https://doi.org/10.30764/1819-2785-2025-1-11-22

Уничтожение цифровых следов при сокрытии преступления как вызов судебной экспертологии

А.И. Усов[1,2,3], Ш.Н. Хазиев[1,4], А.Н. Штохов[4]

[1] Федеральное бюджетное учреждение Российский федеральный центр судебной экспертизы имени профессора А.Р. Шляхова при Министерстве юстиции Российской Федерации, Москва 101000, Россия
[2] ФГБОУ ВО «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)», Москва 105055, Россия
[3] ФГБОУ ВО «Всероссийский государственный университет юстиции (РПА Минюста России)», Москва 117638, Россия
[4] Акционерное общество «Научно-производственная компания "Криптонит"», Москва 115114, Россия

Аннотация. Обнаружение, исследование и использование цифровых следов преступления – важнейшие задачи криминалистики. Однако эффективно использовать эти объекты во многих случаях невозможно в связи с их уничтожением самим преступником или иными лицами. На основе отечественного и зарубежного опыта в настоящей статье была впервые осуществлена детальная научная систематизация способов уничтожения цифровых следов и описан общий алгоритм судебного компьютерно-технического экспертного исследования факта уничтожения цифровых следов преступления, а также восстановления утраченной информации. Представляется целесообразным изучить закономерности криминального уничтожения цифровых следов в тесной связи с положениями и результатами разработки отечественными учеными криминалистического учения о сокрытии следов преступления в «доцифровую эпоху». Актуальной задачей является и разработка отечественных технических и программных средств восстановления уничтоженной компьютерной информации.

Ключевые слова: *восстановление информации, криптографическое зашумление, судебная компьютерно-техническая экспертиза, судебная экспертология, цифровая среда, цифровой след*

Для цитирования: Усов А.И., Хазиев Ш.Н., Штохов А.Н. Уничтожение цифровых следов при сокрытии преступления как вызов судебной экспертологии // Теория и практика судебной экспертизы. 2025. Т. 20. № 1. С. 11–22. https://doi.org/10.30764/1819-2785-2025-1-11-22

Destruction of Digital Traces when Concealing a Crime as a Challenge to Forensic Science

Aleksander I. Usov[1,2,3], Shamil N. Khaziev[1,4], Aleksander N. Shtokhov[4]

[1] The Russian Federal Centre of Forensic Science named after Professor A.R. Shlyakhov of the Ministry of Justice of the Russian Federation, Moscow 101000, Russia
[2] Bauman Moscow State Technical University (BMSTU), Moscow 105055, Russia
[3] The All-Russian State University of Justice, Moscow 117638, Russia
[4] Joint Stock Company "Scientific-Production Company "Kryptonite", Moscow 115114, Russia

Abstract. Detection, examination and use of digital traces of crime are important tasks of forensic science. However, the effective use of these objects is impossible in many cases due to their destruction by an offender himself or other persons. For the first time ever this article deals with a detailed scientific systematization of methods for destroying digital traces for the first time basing on domestic and foreign experience and describes a general algorithm for forensic computer-technical expert examination of the fact of destruction of digital traces of a crime as well as lost information recovery. It seems appropriate to study the patterns of criminal destruction of digital traces in close connection with provisions and results of the development of the forensic doctrine of concealment of traces of a crime by domestic scientists in the "pre-digital era". One of the relevant tasks is also the development of domestic technical and software tools for destroyed computer information recovery.

Keywords: *information recovery, cryptographic noise suppression, forensic computer-technical examination, forensic expertology, digital environment, digital trace*

For citation: Usov A.I., Khaziev Sh.N., Shtokhov A.N. Destruction of Digital Traces when Concealing a Crime as a Challenge to Forensic Science. *Theory and Practice of Forensic Science.* 2025. Vol. 20. No. 1. P. 11–22. (In Russ.). https://doi.org/10.30764/1819-2785-2025-1-11-22

Введение

Воздействие преступника или иных лиц на материальные следы, остающиеся в ходе подготовки, совершения и сокрытия преступления, является распространенным способом противодействия раскрытию и расследованию убийств, разбоев, краж, мошенничества и других преступлений. Спектр видов воздействий на материальные следы весьма широк и включает в себя целенаправленное перемещение материальных источников информации о преступлении и преступнике, их маскировку, утаивание, уничтожение, а также различные сочетания этих способов.

Одним из самых распространенных способов воздействия на материальные следы является их уничтожение. Под уничтожением материальных следов преступления традиционно понимается умышленное разрушающее воздействие заинтересованных лиц на материально-фиксированные отражения отдельных элементов события преступления и личности преступника с целью воспрепятствования обнаружению и использованию следов и содержащейся в них информации правоохранительными органами.

Результаты проведенных отечественными криминалистами в начале 1980-х годов исследований свидетельствуют о том, что применение преступниками различных способов сокрытия следов преступлений и приемов их уничтожения подчиняется определенным закономерностям, зависит от вида преступления, обстановки его совершения, личности преступника и множества других факторов, многие из которых способны не только активизировать деятельность по уничтожению следов преступления, но в отдельных случаях и нейтрализовать эти усилия [1, 2]. Дальнейшее комплексное изучение этого способа противодействия субъектов противоправных действий расследованию преступлений позволит разработать конкретные криминалистические рекомендации, направленные на установление индивидуальных признаков искомого преступника, а также механизма происшедшего события в целом и отдельных его элементов.

В последние годы, с учетом цифровой трансформации и появления цифровых следов подготовки и совершения преступлений с использованием компьютерных технологий[1], очевидной становится необходимость дальнейшего развития криминалистического учения о способах сокрытия, в том числе о способах уничтожения следов преступления.

Криминалистическое научное изучение способов уничтожения цифровых следов преступления со временем позволит создать научные предпосылки для:

– более глубокого и полного понимания сложного механизма преступного поведения во всем его многообразии;

– выработки на основе познанных закономерностей и тенденций обоснованных рекомендаций по осмотру мест происшествий и носителей компьютерной информации, позволяющих получать достоверную и ценную информацию как из «остатков» следов, так и из следов действий по их уничтожению;

– создания частных судебно-экспертных методик, приспособленных для исследования подвергшихся уничтожению следов и исследования способов и средств уничтожения источников информации;

– использования данных об особенностях уничтожения следов различными категориями лиц в целях получения максимального объема розыскной и доказательственной информации о неизвестном преступнике;

– осуществления предварительного расчета частоты встречаемости отдельных приемов уничтожения следов и комплексов (совокупностей) таких приемов. На основе этих расчетов в более объективированном виде необходимо определить значимость изменений, возникающих в ходе уничтожения цифровых следов, для выдвижения версий и решения разнообразных следственных и оперативно-розыскных задач.

[1] В качестве синонимов слова «цифровой след» часто используются слова «виртуальный след», «электронный след», «электронно-цифровой след», «цифровой артефакт», «компьютерный след», «компьютерно-технический след», «информационный след» и др.

В настоящей статье под цифровыми следами преступления (*digital traces, digital footprints*) подразумеваются изменения, возникающие в цифровой среде в результате действий преступника, а также компьютерная информация в виде файлов и сообщений, содержащих сведения о подготовке и реализации преступного замысла. К ним относятся электронные письма, текстовые файлы, цифровые фотографии, цифровые аудио- и видеофайлы, документы по обработке текстов, файлы бухгалтерских программ, электронные таблицы, истории интернет-браузеров, базы данных, содержимое памяти компьютера или мобильного устройства связи, резервные копии компьютеров, компьютерные распечатки, треки глобальных систем позиционирования, журналы электронных дверных замков помещений (в частности, отелей), календари, записи чатов, адресные книги (например, Outlook) и др.

Основными носителями компьютерной информации и цифровых следов, представляющих интерес для следствия и суда, являются:

1. Компьютеры и ноутбуки. Они содержат различные цифровые объекты, такие как электронные письма, документы, историю просмотров и даже удаленные файлы, которые можно восстановить.

2. Мобильные устройства: смартфоны (выполняют функцию миниатюрных цифровых журналов, хранящих текстовые сообщения, записи вызовов, информацию GPS и информацию о действиях в социальных сетях), а также планшеты.

3. Оптические носители (CD и CD-ROM, DVD и DVD-ROM, Blu-ray и HD-DVD).

4. Магнитные резервные ленты (любые виды DLT, мини-картриджи и многое другое).

5. Облачные хранилища.

6. Социальные сети. Эти платформы могут служить ценным источником информации, раскрывая сообщества, обсуждения и потенциально компрометирующий контент в онлайн-профилях.

7. Камеры видеонаблюдения и видеофиксации. Визуальные записи, сделанные как государственными, так и частными камерами, могут служить ценными доказательствами в случаях преступной деятельности и даже помогать в выявлении потенциальных преступников или фактов подготовки к совершению преступления.

8. Объекты интернета вещей (IoT – Internet of Things).

Цифровые следы являются латентными (скрытыми), они могут быть изменены, повреждены или уничтожены без особых усилий.

Сам факт уничтожения преступником или другими лицами материальных или цифровых следов и использованные при этом средства могут быть установлены при осмотре места происшествия, осмотре компьютерной техники и гаджетов, при допросе потерпевшего, свидетелей, подозреваемого (обвиняемого), при личном обыске и обыске жилища обвиняемого, осмотре одежды обвиняемого, а также путем проведения различных судебных экспертиз.

1. Программные способы и средства уничтожения цифровых следов преступления

К программным способам и инструментам уничтожения цифровых следов преступления относятся:

– удаление файлов обычными (штатными) программными средствами;

– стирание данных со всего жесткого диска или внешнего носителя установленными на компьютере инструментами;

– стирание данных специальными средствами;

– полная перезапись диска;

– форматирование;

– криптографическое уничтожение (зашумление, стирание);

– удаление следов действий субъекта в цифровой среде.

1.1. Удаление файлов обычными (штатными) программными средствами

Удаление файлов предусмотрено программным обеспечением любого компьютера и является самым доступным способом уничтожения компьютерной информации, файлы обычно отправляются в корзину, но могут быть восстановлены. Существуют программы дистанционного удаления файлов и иной компьютерной информации.

Как правило, поиск и восстановление удаленных штатными программными средствами файлов не вызывает больших трудностей. Есть десятки доступных программ восстановления удаленных (а также утерянных) файлов[2]. При проведении судебной компьютерно-технической экспертизы с этой задачей успешно справляются такие

[2] Например, Recuva, Puran File Recovery, Transcend RecoveRx, R.Saver, Hasleo Data Recovery Free, Disk Drill, Wise Data Recovery, Undelete 360, MiniTool Power Data Recovery, SoftPerfect File Recovery, CD Recovery Toolbox и др.

аппаратно-программные криминалистические средства, как EnCase ® Forensic и некоторые другие. Наиболее эффективные аппаратно-программные средства судебной компьютерно-технической экспертизы, используемые в России, описаны в статье И. Михайлова [3].

1.2. Стирание данных со всего жесткого диска или внешнего носителя установленными на компьютере инструментами

Программное стирание данных использует имеющее доступ к диску приложение для записи комбинации единиц, нулей и любых других буквенно-цифровых символов, также известных как «маска», на каждый сектор жесткого диска. Уровень безопасности при использовании программных средств уничтожения данных значительно повышается за счет предварительного тестирования жестких дисков на предмет аномалий секторов и обеспечения полностью рабочего состояния диска.

Понятие «количество стираний» устарело с недавним включением «проверочного прохода», который сканирует все сектора диска и проверяет, какой символ должен там быть. За один проход заполняются все записываемые сектора жесткого диска, в связи с чем последующее повторение этого процесса будет оказывать разрушительное действие, особенно в случае больших, многотерабайтных, дисков.

Носители на основе флеш-памяти, такие как твердотельные накопители (SSD) или USB-флеш-накопители, могут привести к сбою стирания данных, что нередко позволяет восстановить потенциально хранимые на устройстве остаточные данные, которые недоступны для техники стирания и могут быть извлечены из отдельных чипов флеш-памяти внутри устройства. Стирание данных путем перезаписи работает только на жестких дисках (HDD), которые функционируют и записывают во все сектора. Поврежденные сектора (bad blocks) обычно не подлежат перезаписи, но могут содержать восстанавливаемую информацию и при этом быть невидимы для хост-системы и, следовательно, для программы стирания.

1.3. Стирание данных специальными средствами

В IT-индустрии имеется направление, обеспечивающее изготовление аппаратно-программных средств (инструментов) для эффективного стирания данных. Такие средства могут использоваться не только в правомерных целях для очистки компьютеров, но и преступниками для уничтожения цифровых следов.

К числу таких инструментов относится, в частности, Privacy Eraser («ластик конфиденциальности»[3]). Этот продукт предназначен для защиты конфиденциальности пользователя путем удаления истории просмотров и других действий на компьютере, поддерживает несколько веб-браузеров, таких как Internet Explorer, Microsoft Edge, Firefox, Google Chrome, Safari и Opera.

Privacy Eraser стирает все цифровые следы: кэш веб-браузера, файлы cookie и index.dat[4], а также временные файлы и файлы журналов; охраненные пароли; последние документы; корзину; буфер обмена; кэш DNS; отчеты об ошибках; истории просмотров, адресной строки, автозаполнения форм, ввода URL-адресов, запуска Windows, поиска, открытия/сохранения.

Privacy Eraser поддерживает плагины для расширения возможностей очистки программного обеспечения и некоторые программы, такие как ACDSee, Adobe Reader, Microsoft Office, WinZip, WinRAR, Windows Media Player, VLC Player, BitTorrent и панель инструментов Google. Он работает с Windows 10/8.x/7/Vista/2012/2008 (32/64-бит) и с файловыми системами WindowsFAT16/FAT32/exFAT/NTFS. Как указывают производители, это программное обеспечение реализует стандарты очистки Министерства обороны и Агентства национальной безопасности США и даже превосходит их[5].

Кроме этого, для уничтожения компьютерной информации (или цифровых следов преступления) применяют программы-шредеры (иногда их называют утилитами),

[3] Cybertron Software, ранее известная как Privacy Eraser Computing (© 2002–2012), является ведущей компанией, которая специализируется исключительно на защите конфиденциальности, очистке ПК и решениях по оптимизации производительности для домашних и офисных пользователей компьютеров. С момента основания в 2002 году поставляет профессиональные и инновационные решения миллионам клиентов по всему миру, особенно в США, Великобритании, Канаде, Австралии, Германии, Франции, Италии, Испании. Располагается в городе Миннетонка (США, штат Минесота).

[4] Файл index.dat – это файл базы данных, содержащий информацию о веб-URL-адресах, поисковых запросах и недавно открывавшихся файлах. Его цель – обеспечить быстрый доступ к данным, используемым Internet Explorer.

[5] Anti-Forensics Countermeasures.
https://info-savvy.com/anti-forensics-countermeasures/

которые позволяют безвозвратно удалять папки и файлы с жесткого диска или внешних носителей информации.

Для предотвращения восстановления удаленных файлов утилита записывает поверх данных случайные байты, дату и время их модификации, тем самым обеспечивая недоступность информации. Программа может быть интегрирована в систему с доступом из контекстного меню.

Наиболее популярные программы-шредеры – это CCleaner, Eraser, File Shredder и Freeraser.

1. CCleaner – продукт компании Gen Digital Inc.[6], выпущенный в 2004 году и предназначенный для удаления информации из настольных ПК, мобильных устройств, очистки информации в облаке и в сложных корпоративных сетях. В начале 2024 года компания Avast, владелец CCleaner, перестала оказывать услуги в России и Белоруссии в связи с санкциями Евросоюза.

2. Eraser – программа стирания файлов для Windows. Удаляет файлы безошибочно и безопасно. Скорость процесса стирания зависит от размера данных и типа стирания. В настройках доступен огромный список параметров стирания, в том числе методы с такими впечатляющими названиями, как перезапись методом Гутмана (Gutmann [35 passes]) и ВВС США (Air Force). По сути, чем больше «проходов» выполняет Eraser, тем надежнее стираются данные и тем больше времени это занимает.

В литературе отмечается, что в современных дисках старые методы кодирования не используются, что делает многие проходы перезаписи методом Гутмана лишними. Кроме того, уже более 20 лет в конструкцию жестких дисков ATA IDE и SATA включается поддержка стандарта «Secure Erase», что устраняет необходимость применения метода Гутмана при очистке всего диска. По мнению экспертов, данный метод также неприменим к твердотельной памяти, что признает в том числе и сам Гутман [4]. Исходя из вышеизложенного, перезапись методом Гутмана эффективна только с накопителями на жестких магнитных дисках.

Самая «полезная» функция Eraser – запланированное стирание содержимого жесткого диска. Eraser даже заменит стертые файлы файлами по выбору, чтобы обеспечить «правдоподобное отрицание».

3. File Shredder – быстрый, безопасный и надежный инструмент для уничтожения корпоративных файлов. Поскольку программа была выпущена бесплатно под лицензией GNU, ее без ограничений может использовать кто угодно. Это простая программа превосходит множество коммерческих файловых шредеров. В File Shredder возможен выбор одного из пяти алгоритмов уничтожения, каждый из которых мощнее предыдущего. Программа имеет интегрированный Disk Wiper, который использует алгоритм уничтожения для очистки неиспользуемого дискового пространства.

4. Freeraser – альтернативная корзина для Windows, в которой возможно безопасно стирать файлы без возможности восстановления. Имеет красиво оформленную иконку с изменяемым размером и эффектом прозрачности (с более совершенным дизайном по сравнению со стандартной корзиной Windows). Поддерживает три метода удаления (быстрый, принудительный и окончательный) и работает очень эффективно.

Кроме упомянутых имеется несколько десятков программ для стирания файлов и другой компьютерной информации. В них комбинируют такие методы, как запись нуля, случайные данные, стирание по стандарту DoD 5220.22-M, Gutmann, Schneier. Разработчики заявляют, что большинство программ позволяет безвозвратно удалять информацию с жесткого диска или иного носителя.

1.4. Полная перезапись диска

Существует множество программ перезаписи, но полную безопасность обеспечивают только уничтожающие данные во всех областях жесткого диска. Без полного доступа к диску, включая скрытые/заблокированные области (например, защищенную область хоста [HPA], переназначенные сектора), программы выполняют неполное стирание, оставляя часть данных нетронутыми.

Перезаписывающие программы, работающие через операционную систему, не всегда выполняют полное стирание, поскольку не могут изменять содержимое жесткого диска, активно этой системой используемого. Из-за этого многие программы предоставляются в загрузочном формате с запуском live CD, который имеет все необходимое программное обеспечение для стирания диска.

[6] Gen Digital Inc. предоставляет решения, которые позволяют потребителям защищать свои устройства, онлайн-конфиденциальность, личность и домашние сети. Gen Digital обслуживает клиентов по всему миру. Располагается в городе Темпе (США, штат Аризона).

В Специальной публикации Национального института стандартов и технологий США SP 800-88 Rev. 1 от 2014 года, раздел 2.4 указано следующее: «Для устройств хранения данных, содержащих магнитные носители, один проход перезаписи с фиксированным шаблоном, таким как двоичные нули, обычно препятствует восстановлению данных, даже если для попытки извлечь данные применяются самые современные лабораторные методы» [5, с. 7]. В качестве более общего механизма рекомендуется криптографическое стирание.

Согласно «Учебнику по очистке данных на дисках» (Tutorial on Disk Drive Data Sanitization) Центра исследований памяти и записи Калифорнийского университета в Сан-Диего (CMRR), «…Безопасное стирание достигается однократным стиранием данных на дорожке. Агентство национальной безопасности США опубликовало одобрение по обеспечению безопасности информации для однопроходной перезаписи после того, как технические испытания в CMRR показали, что многократные проходы перезаписи на дорожке не дали дополнительного стирания» [6, с. 8]. Безопасное стирание – это функция, встроенная в современные жесткие диски и твердотельные накопители, которая перезаписывает все данные на диске, включая переназначенные (ошибочные) сектора.

Форматирование носителя не гарантирует уничтожение компьютерной информации. Как и в случае удаления файла, форматирование жесткого диска или USB-накопителя удаляет только указатели на место хранения информации, но фактическая информация остается и не уничтожается. Поэтому относить форматирование к самостоятельному и значимому способу уничтожения цифровых следов не следует.

Анализ возможностей криминалистического (судебно-экспертного) восстановления уничтоженных программными средствами цифровых следов периодически проводится зарубежными исследователями, и его результаты находят свое отражение в соответствующих научных публикациях. (статьях, аналитических обзорах, диссертациях) [7–9].

1.5. Криптографическое уничтожение

При шифровании файла и последующем уничтожении ключей шифрования восстановить его содержание не представляется возможным, поэтому данный способ сокрытия, по нашему мнению, целесообразно также отнести к категории «уничтожение». Этому способу безвозвратного сокрытия информации посвящен ряд научных исследований, в которых он также именуется как «криптографическое стирание», «криптографическое удаление», «крипто-шреддинг», «кодовое зашумление» [10].

Криптографическое стирание – это особая форма перезаписи, иногда называемая удалением-шифрованием, которая заменяет сохраненную информацию сильно зашифрованными данными. После того, как изначальные данные зашифрованы и криптографические ключи надежно стерты, информация становится невосстановимой. Если применяется опция криптографического стирания, рекомендуется выполнить процедуру криптографического стирания блоков однократно, а затем провести процедуру стирания с опцией Block Erase.

Устройства iOS и компьютеры Macintosh с чипом Apple T2 или Apple Silicon используют криптографическое стирание при выполнении действия «Стереть весь контент и настройки», удаляя все ключи в «стираемом хранилище». Это делает все пользовательские данные на устройстве недоступными за очень короткий промежуток времени.

Производители накопителей, например, компании Seagate и Western Digital [11, 12], подобные методы традиционно называют Instant Secure Erase,

Криптографическое стирание особенно эффективно в случае уничтожения данных, находящихся в облачных хранилищах или виртуальных машинах. Его можно использовать на любом типе устройства хранения, включая жесткие диски, SSD, USB-накопители и карты памяти, но оно неприменимо к CD и DVD-дискам, поскольку последние обычно не используют шифрование подобно цифровым устройствам хранения данных.

Время, необходимое для завершения криптографического стирания, зависит от размера устройства хранения и объема данных.

Одним из недостатков метода является то, что надежность удаления трудно проверить путем проверки носителя, поскольку невозможно подтвердить, что все криптографические ключи (основные и дополнительные резервные) были действительно стерты.

1.6. Удаление следов действий субъекта в цифровой среде

Следы действий субъекта в цифровой среде, иначе называемые следами активности на компьютере, могут служить важными доказательствами совершения преступления. К ним относятся:

– подробная информация о поисковых запросах, введенных пользователями;

– информация о посещенных веб-сайтах;

– информация о запущенных приложениях, а также открытых и сохраненных файлах;

– информация о создании и последующем удалении учетных записей;

– записи журнала событий Microsoft Windows.

Следы действий субъекта уничтожаются путем внесения изменений (главным образом удаления или маскировки) в автоматически создаваемые компьютерные сведения в журналах, реестрах и т. п. Очистка истории браузера, cookie и кэш, удаление данных для автозаполнения также могут снизить возможность получения интересующей следствие информации о действиях субъекта. Использование режима «инкогнито» или «приватного режима» минимизирует образование следов онлайн-активности, не удаляя их, но предотвращая накопление в локальной истории браузера.

Многие программы, предназначенные для обеспечения компьютерной безопасности, содержат средства очистки конфиденциальных данных, которые удаляют следы действий пользователя в операционной системе. Тем не менее в процессе судебной компьютерно-технической экспертизы целесообразно осуществлять анализ изменений таких блоков, как журналы событий Windows (журнал приложений, системный журнал, журнал безопасности), реестр Windows, оперативная память (ОЗУ), файлы подкачки, файлы предварительной загрузки Windows Prefetch, файлы Windows Superfetch, кэш-миниатюр Windows, списки переходов Windows, история и файлы кэша в веб-браузере.

2. Физические способы уничтожения цифровых следов преступления

К физическим способам уничтожения цифровых следов преступления относят:

– размагничивание жесткого диска;

– механическое повреждение или разрушение (измельчение жесткого диска, флешкарты, CD или DVD дисков);

– химическое воздействие на диск или накопитель;

– расплавление термическое или сжигание магнитных дисков или магнитных лент;

– взрывное (пиротехническое) уничтожение носителя.

2.1. Размагничивание жесткого диска

Наиболее эффективным методом уничтожения считается размагничивание жестких дисков путем воздействия на них мощными электромагнитными установками или приборами [13]. При этом применяют магнитную силу, намного превышающую силу головок чтения/записи. Размагничивание – отнюдь не новый инструмент, он развивался одновременно с совершенствованием магнитных носителей; в первые годы его применяли в основном для переработки дорогостоящей ленты для повторного использования.

Размагничиватель с достаточной силой и ориентацией поля способен устранить все магнитные домены накопителя или ленты, в результате на пластине диска не остается самых глубоких магнитных схем – серводорожек. Сила размагничивающего устройства должна оцениваться по мощности, которая постоянно поддерживается в камере размагничивания, а не по ее максимальным отметкам. Ориентация привода или ленты по отношению к пути магнитного поля стирания также важна. Привод, проходящий внутри направленного магнитного поля, будет иметь лучшие результаты стирания, чем привод, проходящий над магнитным полем. Цель – удалить все данные и как можно большую часть базовой структуры с жесткого диска или ленты.

Единственный недостаток размагничивания жестких дисков и некоторых новых магнитных лент заключается в том, что они не подлежат повторному использованию. По сравнению с многочасовыми сеансами перезаписи или безопасного стирания для повторного использования старых дисков размагничивание и замена на новый диск все еще намного более экономически выгодны. Кроме того, жесткие диски компьютеров выходят из строя с большой регулярностью, и в будущем этот показатель будет только расти.

В практике судебной компьютерно-технической экспертизы факты размагничивания жестких дисков, представленных на исследование, встречаются довольно редко. Размагниченный жесткий диск в таких случаях не определяется при включении компьютера или при его подключении к компьютеру эксперта. В заключении эксперта

при этом делается вывод о невозможности восстановления содержания жесткого диска (или внешнего накопителя) и перечисляются возможные причины этого, в том числе его размагничивание.

Следует иметь в виду, что размагничивание SSD для уничтожения данных неэффективно, поскольку такие диски основаны на интегральных схемах. Размагничивание неэффективно и в случае USB-флеш-накопителей, поскольку они не используют магнитную память.

2.2. Механическое повреждение или разрушение

Механическое повреждение или разрушение носителей цифровых следов осуществляют путем нанесения ударов рубящими или тупыми твердыми предметами, разрезания, измельчения, переезда транспортными средствами.

Многие компании и государственные учреждения до сих пор сверлят отверстия или повреждают жесткие диски молотком перед их утилизацией. Помимо риска для сотрудников, использующих дрель или молоток, эффективность этого способа не слишком значительна. Повреждения, безусловно, затрудняют восстановление данных, но, тем не менее, это возможно при наличии необходимого оборудования и узкоспециализированных экспертов. К числу компаний, предлагающих услуги по восстановлению данных, уничтоженных путем механического повреждения, принадлежат Secure Data Recovery (Калифорния, США), DriveSavers (Калифорния, США), Ontrack Data Recovery (Лондон, Великобритания) и некоторые другие.

Популярное электронное издание WikiHow приводит следующий способ механического разрушения диска: «Разбейте диск молотком. Перед тем как сделать это, поместите диск в тканевый мешок, чтобы осколки не разлетелись во все стороны. Возьмите молоток и разбейте им диск, пока он не разлетится на тысячи мелких кусочков. После этого разделите остатки на несколько пакетов и выбросьте каждый по отдельности, чтобы их нельзя было собрать вместе»[7].

Иногда данные можно восстановить и со сломанного жесткого диска. Однако, если пластины на жестком диске повреждены, например, просверлено отверстие в диске (и пластинах внутри), то данные теоретически можно восстановить только путем побитового анализа каждой пластины с использованием специальных криминалистических технологий.

Промышленность предлагает различные устройства для измельчения не только жестких дисков, но и разнообразных устройств (флеш-карт, CD или DVD дисков), содержащих компьютерную информацию и цифровые следы. Примером является измельчитель твердотельных накопителей Kobra, выпускаемый американской компанией Media Duplication Systems.

Kobra SSD специально разработан для твердотельных устройств: он эффективно уничтожает твердотельные SIM-карты, флеш-накопители, печатные платы, корпоративные твердотельные накопители, мобильные телефоны, планшеты, USB-флешки, USB-устройства памяти, микросхемы флеш-памяти и микросхемы ЦП с внутренним ПЗУ и/или флеш-памятью. Делая эти устройства невосстановимыми, Kobra SSD обеспечивает полную защиту конфиденциальной информации[8].

На оптических дисках (CD, DVD, Blu-ray) несущие информацию слои удаляют с помощью шлифовальной машины. При этом измельчение является единственным достаточным методом уничтожения информации на оптических носителях.

2.3. Химическое воздействие

Одним из способов разрушающего воздействия является помещение носителей компьютерных следов в агрессивную среду некоторых жидкостей, при этом наиболее доступной и популярной является соляная кислота. Считается, что для уничтожения магнитного слоя блина жесткого диска достаточно вылить на него любую жидкость, которая способна изменить свойства ферромагнетиков. Чтобы изменить состав оксида хрома (ферромагнетик, которым покрывают блины жестких дисков, – магнитный слой диска) необходимо вылить на него соляную кислоту или воду температурой 100° С. Иногда используют и азотную кислоту. Кислоты разъедают механические компоненты и снимают пленку с пластины.

Соляная кислота быстро расправляется с двигателем и корпусом жесткого диска, при этом пластина остается нетронутой.

[7] How to Destroy a Hard Drive & Prevent Data From Being Recovered // wikiHow. 19.02.2025. https://www.wikihow.com/Destroy-a-Hard-Drive

[8] Media Duplication Systems (MDS). https://www.mediaduplicationsystems.com/

Некоторые исследователи рекомендуют поместить пластину и в соляную, и в азотную кислоту. Первая разрушает алюминий в пластине, а вторая стирает тонкую пленку данных с диска. При этом выделяются опасные газы, поэтому для осуществления этих действий необходимы специальная стеклянная посуда и оборудование.

Попытки повреждения жестких дисков путем помещения их в морскую или просто соленую воду во многих случаях не исключают последующего восстановления информации. Такие объекты сначала аккуратно очищаются органическими растворителями, а затем сверхчистой водой, после чего высушиваются с помощью оборудования для вакуумного испарения [14].

2.4. Термическое расплавление или сжигание

Расплавление термическое или сжигание магнитных дисков, магнитных лент считается вполне эффективным методом уничтожения данных, который, однако, требует длительного поддержания высокой температуры и использования мусоросжигательных печей, в результате чего наносится ущерб окружающей среде. Если диск не сгорает полностью, будет иметь место некоторая потеря данных.

Основной процесс их восстановления включает в себя вскрытие корпуса, затем – очистку извлеченных пластин от сажи, копоти или других частиц, чтобы предотвратить их дальнейшее повреждение. Далее пластины помещают в другой жесткий диск, что может потребовать работы с прошивкой и настройками BIOS из-за проблем совместимости и обеспечения возможности чтения диска.

2.5. Взрывное (пиротехническое) уничтожение носителя

Некоторое время назад для сохранения важной защищенной секретной информации были предложены и внедрены методы экстренного уничтожения носителей компьютерной информации с использованием пиротехнических средств.

Следствию нередко приходится сталкиваться и с такими способами сокрытия следов преступлений, как уничтожение или существенное повреждение преступниками материальных носителей компьютерной информации – персональных компьютеров и (или) их жестких дисков, внешних носителей информации (внешние жесткие диски, флеш-карты, лазерные CD или DVD диски и др.), мобильных телефонов и других гаджетов.

3. Судебно-экспертное исследование компьютерных средств и цифровой среды с целью восстановления уничтоженных данных

Наиболее ценным результатом судебной компьютерно-технической экспертизы, проводимой с целью поиска, обнаружения и фиксации цифровых доказательств (в том числе цифровых следов), является восстановление уничтоженных данных (файлов, писем и т.д.), имеющих значение для расследования и судебного разбирательства.

Последовательность действий эксперта в процессе исследования компьютерных средств или цифровой среды в большинстве случаев выглядит следующим образом:

1) определение типа, вида и технических особенностей представленного на исследование компьютерного средства;

2) создание полной копии (образа) цифрового устройства;

3) систематизация содержания информации, имеющейся на цифровом устройстве на момент начала его исследования;

4) поиск и фиксация сохранившихся следов, имеющих значение для дела;

5) выявление признаков, свидетельствующих об уничтожении цифровых следов;

6) установление способа уничтожения цифровых следов;

7) восстановление уничтоженной компьютерной информации;

8) анализ восстановленной информации и выделение из ее состава совокупности цифровых следов, имеющих значение для расследуемого дела;

9) синтезирование всей совокупности информации, полученной в процессе экспертного исследования;

10) формулирование выводов и оформление заключения эксперта.

Криминалистическое восстановление данных – специализированная область, которая включает в себя извлечение скрытых, утерянных или уничтоженных данных с цифровых устройств. Эти данные могут включать удаленные файлы, электронные письма, историю просмотров в интернете и многое другое. Криминалистическое восстановление данных отличается от традиционного восстановления данных тем, что оно должно выполняться таким образом, чтобы сохранить целостность (обеспечить неиз-

менность) доказательств. Это означает, что данные должны быть восстановлены без их изменения или какой-либо модификации.

В подразделениях (лабораториях, отделах) судебной компьютерно-технической экспертизы в ряде случаев удается восстановить информацию, которую пытались уничтожить на том или ином носителе механическим, химическим, электромагнитным способами. Существует ряд методов, которые возможно использовать для восстановления данных в целях судопроизводства с учетом конкретной ситуации.

Важным этапом анализа содержания компьютерного средства и восстановления удаленных или иным способом уничтоженных данных является клонирование диска, что подразумевает создание точной копии (образа) жесткого диска. Копию затем можно использовать для восстановления данных с исходного диска. Иногда она используется для проведения экспертных экспериментов с целью изучения механизма следообразования, например, механизма следообразования при создании и последующем уничтожении учетных записей [15].

Одним из способов восстановления удаленных файлов является сканирование памяти и компьютерной системы и поиск фрагментов информации (остатков данных), которые были частично стерты в одном месте, но фрагментарно отобразились в другой области исследуемого устройства. Сложить обнаруженные фрагменты можно с помощью таких криминалистических инструментов, как Wise Data Recovery, CrashPlan и др.

Если имеются сведения об уничтожении медиафайлов, целесообразно проводить комплексные судебные видеофонотехнические и компьютерно-технические экспертизы.

Помимо восстановления содержания удаленных данных в ходе проведения судебной компьютерно-технической экспертизы осуществляют поиск следов цифровой активности, предположительно имеющей отношение к расследуемому событию. Такие следы требуют специфического анализа и оценки.

В случаях, когда интересующая следствие информация зашифрована, эксперты используют для доступа к данным и их анализу методы шифрования и дешифрования. Это может включать взлом паролей, восстановление ключей шифрования или использование известных уязвимостей в алгоритмах шифрования.

В настоящее время продолжают разрабатываться и совершенствуются уже существующие методики судебной компьютерно-технической экспертизы, позволяющие решать многочисленные задачи, возникающие в процессе судопроизводства. Опубликовано несколько учебников и учебных пособий по судебной компьютерно-технической экспертизе [16–18], в то же время имеется не так много научных публикаций, посвященных экспертному исследованию следов действий субъекта в цифровой среде [19, 20], до сих пор методы и средства исследования, а также правила юридически значимой фиксации фактов уничтожения цифровых следов не сведены в отдельную судебно-экспертную методику.

Заключение

Представляется целесообразным и своевременным продолжить научное исследование способов уничтожения следов преступлений с учетом цифровой трансформации и появления новых высокотехнологичных способов совершения и сокрытия преступлений и их следов.

Сегодня цифровые следы являются одним из самых распространенных объектов многих родов и видов судебных экспертиз, что обусловливает формирование в судебной экспертологии нового учения о цифровизации судебно-экспертной деятельности [21, 22].

При разработке методов и средств судебно-экспертного исследования способов уничтожения цифровых следов и последующего их восстановления желательно использовать результаты предшествующего многолетнего криминалистического научного исследования традиционных («аналоговых») способов сокрытия следов преступления и накопленный в судебно-экспертной практике соответствующий опыт.

Информацию о способах уничтожения цифровых следов и данные о криминалистических и судебно-экспертных методах их выявления необходимо включить в учебно-методические издания для экспертов и правоприменителей.

СПИСОК ЛИТЕРАТУРЫ

1. Способы сокрытия следов преступлений и криминалистические методы их установления. Сборник трудов. М.: Московский филиал юридического заочного обучения при Академии МВД СССР, 1984. 108 с.

REFERENCES

1. *Methods of Concealment of Traces of Crimes and Criminalistic Methods of Their Identification. Collected Works.* Moscow: Moskovskii filial yuridicheskogo zaochnogo obucheniya pri Akademii MVD SSSR, 1984. 108 p. (In Russ.).

2. Криминалистическая сущность, средства и методы установления способов сокрытия следов преступления. Сборник научных трудов. М.: Московский филиал юридического заочного обучения при Академии МВД СССР, 1987. 78 с.
3. Михайлов И. Ключ на старт: лучшие программные и аппаратные средства для компьютерной криминалистики // Блог компании F6. 10.06.2019. https://habr.com/ru/companies/facct/articles/454672/
4. Gutmann P. Secure Deletion of Data from Magnetic and Solid-State Memory // Proceedings of the Sixth USENIX UNIX Security Symposium (San Jose, July 22–25, 1996). San Jose, 1996. P. 77–90.
5. Kissel R., Regenscheid A., Scholl M., Stine K. Guidelines for Media Sanitization // Computer Security. National Institute of Standards and Technology, 2014. 56 p. https://doi.org/10.6028/NIST.SP.800-88r1
6. Hughes G., Coughlin T. Tutorial on Disk Drive Data Sanitization. San Diego: Center for Magnetic Recording Research, 2006. 15 p.
7. Al Saadi E.A.M. Anti-Computer Forensics Techniques. Zayed University, 2013. 46 p.
8. Garfinkel S. Anti-Forensics: Techniques, Detection and Countermeasures // The 2nd International Conference on i-Warfare and Security. Monterey: Naval Postgraduate School, 2007. P. 77–84.
9. Patel S.A., Yadav S.K., Kumar R., Singh A., Kumar P. Recovery of Deleted Data from Virtual Machine Using Open Source Tools: A Review // International Journal of Research and Analytical Reviews. 2024. Vol. 11. No. 1. P. 764–769.
10. Демидов А.А. Гарантированное уничтожение информации на основе кодового зашумления // Инфокоммуникационные технологии. 2007. Т 5. № 2. С. 75–78.
11. Куц Д.В., Поршнев С.В., Соколов И.П., Куц М.П. К постановке проблемы затирания отдельных файлов на твердотельных накопителях // Инженерный вестник Дона. 2024. № 2 (110). С. 35–51.
12. Куц Д.В., Поршнев С.В., Соколов И.П., Куц М.П. Анализ проблемы надежного удаления файлов на твердотельных накопителях и подходов к ее решению // Вестник УрФО. Безопасность в информационной сфере. 2024. № 1 (51). С. 39–44. https://doi.org/10.14529/secur240105
13. Хлопов Б.В., Самойлович М.И., Митягина А.Б. Устойчивость мультиферроидных материалов НЖМД при воздействии на них внешних магнитных полей // Инновационная наука. 2016. № 4. С. 39–41.
14. Curnett B., Darian T., Wojcik K., McCarthy S. Chemical Restoration of Damaged Hard Drives // Journal of Purdue Undergraduate Research. 2014. Vol. 4. Article 76. http://doi.org/10.5703/1288284315437
15. Al-Saleh M.I., Al-Shamaileh M.J. Forensic Artefacts Associated with Intentionally Deleted User

2. *The Criminalistic Essence, Means and Methods for Establishing Ways to Conceal Traces of Crimes. Collection of Scientific Papers.* Moscow: Moskovskii filial yuridicheskogo zaochnogo obucheniya pri Akademii MVD SSSR, 1987. 78 p. (In Russ.).
3. Mikhailov I. Key to Start: The Best Software and Hardware for Computer Forensics. *The blog of F6 Company.* 10.06.2019. (In Russ.). https://habr.com/ru/companies/facct/articles/454672/
4. Gutmann P. Secure Deletion of Data from Magnetic and Solid-State Memory. *Proceedings of the Sixth USENIX UNIX Security Symposium* (San Jose, July 22–25, 1996). San Jose, 1996. P. 77–90.
5. Kissel R., Regenscheid A., Scholl M., Stine K. Guidelines for Media Sanitization. *Computer Security.* National Institute of Standards and Technology, 2014. 56 p. https://doi.org/10.6028/NIST.SP.800-88r1
6. Hughes G., Coughlin T. *Tutorial on Disk Drive Data Sanitization.* San Diego: Center for Magnetic Recording Research, 2006. 15 p.
7. Al Saadi E.A.M. *Anti-Computer Forensics Techniques.* Zayed University, 2013. 46 p.
8. Garfinkel S. Anti-Forensics: Techniques, Detection and Countermeasures. *The 2nd International Conference on i-Warfare and Security.* Monterey: Naval Postgraduate School, 2007. P. 77–84.
9. Patel S.A., Yadav S.K., Kumar R., Singh A., Kumar P. Recovery of Deleted Data from Virtual Machine Using Open Source Tools: A Review. *International Journal of Research and Analytical Reviews.* 2024. Vol. 11. No. 1. P. 764–769.
10. Demidov A.A. Guaranteed Information Destruction Based on Code Noise Suppression. *Infocommunication technologies.* 2007. Vol. 5. No. 2. P. 75–78. (In Russ.).
11. Kutz D.V., Porshnev S.V., Sokolov I.P., Kutz M.P. On the Issue of Mashing Individual Files on Solid-state Drives. *The Don Engineering Bulletin.* 2024. No. 2 (110). P. 35–51. (In Russ.).
12. Kutz D.V., Porshnev S.V., Sokolov I.P., Kutz M.P. Analyzing the Problem of Reliable File Deletion on Solid-state Drives and Approaches to Its Solution. *Bulletin of Ural Federal District (UrFD). Information security.* 2024. No. 1 (51). P. 39–44. (In Russ.). https://doi.org/10.14529/secur240105
13. Khlopov B.V., Samoylovich M.I., Mityagina A.B. Resiliency of Multiferroid HMDD Materials under Their Exposion to External Magnetic Fields. *Innovative science.* 2016. No. 4. P. 39–41. (In Russ.).
14. Curnett B., Darian T., Wojcik K., McCarthy S. Chemical Restoration of Damaged Hard Drives. *Journal of Purdue Undergraduate Research.* 2014. Vol. 4. Article 76. http://doi.org/10.5703/1288284315437
15. Al-Saleh M.I., Al-Shamaileh M.J. Forensic Artefacts Associated with Intentionally Deleted User

Accounts // International Journal of Electronic Security and Digital Forensics. 2017. Vol. 9. No. 2. P. 167–179. http://doi.org/10.1504/IJESDF.2017.083992
16. Молодцова Ю.В., Яковлев А.Н. Судебная компьютерно-техническая экспертиза. Учебно-методическое пособие. М.: МГТУ им. Н.Э. Баумана, 2021. 71 с.
17. Бегларян М.Е., Возняк Г.Н. Судебная компьютерно-техническая экспертиза. М.: Юнити-Дана, 2022. 72 с.
18. Тушканова О.В., Зубков А.А., Вавилин А.Ю., Гудкова М.А. Типовая методика производства информационно-аналитической экспертизы. М.: Следственный комитет Российской Федерации, 2023. 66 с
19. Horsman G. Understanding and Comparing Digital Traces // Australian Journal of Forensic Sciences. 2024. P. 1–11. https://doi.org/10.1080/00450618.2024.2381535
20. Soni N., Soni P. Tracing the Unseen: The Role of Digital Footprints in Modern Forensic Investigations // International Journal of Innovative Research in Technology. 2024. Vol. 11. No. 4. P. 346–352.
21. Россинская Е.Р., Зинин А.М. Экспертиза в судопроизводстве: учебник / Под ред. Е.Р. Россинской. М.: Проспект, 2022. 416 с.
22. Теория информационно-компьютерного обеспечения криминалистической деятельности / Под ред. Е.Р. Россинской. М.: Проспект, 2022. 254 с.

Accounts. *International Journal of Electronic Security and Digital Forensics.* 2017. Vol. 9. No. 2. P. 167–179. http://doi.org/10.1504/IJESDF.2017.083992
16. Molodtsova Yu.V., Yakovlev A.N. *Forensic Computer and Technical Examination. Study Guide.* Moscow: MGTU im. N.E. Baumana, 2021. 71 p. (In Russ.).
17. Beglaryan M.E., Voznyak G.N. *Forensic Computer and Technical Examination.* Moscow: Unity-Dana, 2022. 72 p. (In Russ.).
18. Tushkanova O.V., Zubkov A.A., Vavilin A.Yu., Gudkova M.A. *Typical Methodology for Forensic Information and Analytical Examination.* Moscow: Sledstvennyi komitet Rossiiskoi Federatsii, 2023. 66 p. (In Russ.).
19. Horsman G. Understanding and Comparing Digital Traces. *Australian Journal of Forensic Sciences.* 2024. P. 1–11. https://doi.org/10.1080/00450618.2024.2381535
20. Soni N., Soni P. Tracing the Unseen: The Role of Digital Footprints in Modern Forensic Investigations. *International Journal of Innovative Research in Technology.* 2024. Vol. 11. No. 4. P. 346–352.
21. Rossinskaya E.R., Zinin A.M. *Forensic Examination in Legal Proceedings: Textbook* / E.R. Rossinskaya (ed.). Moscow: Prospekt, 2022. 416 p. (In Russ.).
22. *Theory of Information and Computer Support of Criminalistic Activities* / E.R. Rossinskaya (ed.). Moscow: Prospekt, 2022. 254 p. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Усов Александр Иванович – д. юр. н., профессор, заслуженный юрист Российской Федерации, первый заместитель директора ФБУ РФЦСЭ имени профессора А.Р. Шляхова при Минюсте России, профессор кафедры «Безопасность в цифровом мире» ФГБОУ ВО МГТУ имени Н.Э. Баумана, заведующий кафедрой судебной экспертологии ФГБОУ ВО «Всероссийский государственный университет юстиции» (РПА Минюста России); e-mail: a.usov@sudexpert.ru

Хазиев Шамиль Николаевич – д. юр. н., доцент, главный научный сотрудник отдела научно-методического обеспечения Российского федерального центра судебной экспертизы имени профессора А.Р. Шляхова при Минюсте России, советник по научной деятельности генерального директора АО «Научно-производственная компания “Криптонит”»;
e-mail: sh.khaziev@sudexpert.ru

Штохов Александр Николаевич – заместитель генерального директора АО «Научно-производственная компания “Криптонит”»;
e-mail: a.shtokhov@kryptonite.ru

Статья поступила: 20.12.2024
После доработки: 15.01.2025
Принята к печати: 20.01.2025

ABOUT THE AUTHORS

Usov Aleksandr Ivanovich – Doctor of Law, Full Professor, Honored Lawyer of the Russian Federation, First Deputy Director of the Shlyakhov RFCFS, Professor of “Security of the Digital World” Department, the Bauman Moscow State Technical University; Head of the Department of Forensic Expertology of the All-Russian State University of the Ministry of Justice of the Russian Federation;
e-mail: a.usov@sudexpert.ru

Khaziev Shamil Nikolaevich – Doctor of Law, Associate Professor, Principal Researcher at the Forensic Research Methodology Department of the Russian Federal Centre of Forensic Science named after professor A.R. Shlyakhov of the Ministry of Justice of the Russian Federation; Academic Advisor to the General Director of the Joint Stock Company “Research and Development Company “Kryptonite”;
e-mail: sh.khaziev@sudexpert.ru

Shtokhov Aleksander Nikolaevich – Deputy General Director of the Joint Stock Company “Research and Development Company “Kryptonite”;
e-mail: a.shtokhov@kryptonite.ru

Received: December 20, 2024
Revised: January 15, 2025
Accepted: January 20, 2025