УДК 343.98.06:004
DOI: 10.19073/2658-7602-2025-22-3-455-468
EDN: KOOMRY

Оригинальная научная статья

Новые информационные компоненты в формировании электронных доказательств по уголовным делам (современная дорожка электронно-цифровых следов)

А. Б. Смушкин
Саратовская государственная юридическая академия, Саратов, Российская Федерация
✉ *skif32@yandex.ru*

Аннотация. Данная работа нацелена на рассмотрение следовой картины в киберпространстве в современных условиях. Концепцию дорожки цифровых следов (в нашей трактовке – электронно-цифровых) предложил В. Б. Вехов еще в 2008 г., доработав в более поздних публикациях. Отслеживание дорожки электронно-цифровых следов имеет ключевое значение при расследовании преступлений, связанных с использованием информационно-технологических устройств. Однако в настоящее время появилось множество новых форм информации, средств сокрытия следов в киберпространстве. Некоторые современные концепты в области электронной техники оказывают существенное влияние на трансформацию дорожки электронно-цифровых следов, внося существенные изменения в ее цепочку, образуя разрывы, уводя в сторону, анонимизируя точку старта и/или финиша запроса, дробя и пряча следы. В этой связи целью работы является раскрытие специфики следовой дорожки в контексте неклассических форм размещения и использования электронной информации. Анализируется изменение дорожки электронно-цифровых следов при использовании виртуальных машин с многоуровневой вложенностью и средств виртуализации (например, VPN-сервисов), полиморфных программ, распределенной и облачной информации, блокчейна, RAID-массивов, средств сокрытия дорожки электронно-цифровых следов, отдельных перспективных разработок в области компьютерной техники. Статья основана на использовании материалистической диалектики как всеобщего метода, так и общенаучных методов (анализа, синтеза, моделирования, экстраполяции и др.). В результате исследования определены специфические свойства и характеристики дорожки электронно-цифровых следов при использовании рассмотренных концептов в области электронной информации. Констатируется, что новые концепты в области электронной информации существенно меняют следовую картину в киберпространстве и требуют специфических подходов, поэтому особое значение приобретают исследования на стыке технических наук, программирования и криминалистики, раскрывающие особые характеристики новых технологий и форм информации, требующих разработки специфических криминалистических рекомендаций. При этом, в связи с непрерывным научно-техническим прогрессом, эти исследования должны перманентно сопровождать новинки технологий, а в некоторых случаях (например, квантовых технологий) носить перспективный характер, дающий в руки правоохранительных органов действенные инструменты еще до широкого распространения самих технологий и использования их в преступных целях.

Ключевые слова: электронно-цифровой след; дорожка электронно-цифровых следов; виртуализация; многоуровневая вложенность; луковичная маршрутизация; распределенная информация; облачные сервисы; RAID-массивы; блокчейн; полиморфные программы

Финансирование. Исследование выполнено за счет гранта Российского научного фонда № 24-28-00312, https://rscf.ru/project/24-28-00312/

Конфликт интересов. Автор заявляет об отсутствии конфликта интересов.

Для цитирования: Смушкин А. Б. Новые информационные компоненты в формировании электронных доказательств по уголовным делам (современная дорожка электронно-цифровых следов) // Сибирское юридическое обозрение. 2025. Т. 22, № 3. С. 455–468. DOI: https://doi.org/10.19073/2658-7602-2025-22-3-455-468. EDN: https://elibrary.ru/koomry

Original scientific article

New Information Components in the Formation of Electronic Evidence in Criminal Cases (the Modern Trail of Electronic-Digital Traces)

A. B. Smushkin

Saratov State Law Academy, Saratov, Russian Federation

✉ *skif32@yandex.ru*

Abstract. This work aims to examine the trace picture in cyberspace under contemporary conditions. The concept of a digital trail (in our treatment—electronic-digital) was proposed by V. B. Vekhov back in 2008 and refined in later publications. Tracking the trail of electronic-digital traces is of key importance in investigating crimes involving the use of information-technology devices. However, numerous new forms of information and means of concealing traces in cyberspace have now emerged. Certain modern concepts in electronics substantially influence the transformation of the electronic-digital trail, introducing significant changes into its chain, creating gaps, diverting it, anonymizing the start and/or end point of a request, fragmenting and hiding traces. The aim of the paper is to reveal the specifics of the trail in the context of non-classical forms of placement and use of electronic information. The article analyzes how the trail changes when using virtual machines with multi-level nesting and virtualization tools (e.g., VPN services), polymorphic programs, distributed and cloud information, blockchain, RAID arrays, means of concealing the electronic-digital trail, and certain promising developments in computer technology. The study relies on dialectical materialism as a general method and on general scientific methods (analysis, synthesis, modeling, extrapolation, etc.). As a result, specific properties and characteristics of the electronic-digital trail are identified for the concepts considered in the sphere of electronic information. It is established that new concepts in the field of electronic information significantly alter the trace picture in cyberspace and require specific approaches; therefore, research at the intersection of technical sciences, programming, and criminalistics is of particular importance—research that reveals the distinctive features of new technologies and forms of information and that requires the development of specific forensic recommendations. Given ongoing scientific and technological progress, such research must accompany technological innovations on a permanent basis and, in some cases (e.g., quantum technologies), be forward-looking, providing law-enforcement authorities with effective tools even before the technologies themselves are widely disseminated and used for criminal purposes.

Keywords: electronic-digital trace; trail of electronic-digital traces; virtualization; multi-level nesting; onion routing; distributed information; cloud services; RAID arrays; blockchain; polymorphic programs

Funding. The research was carried out with the support of a grant from the Russian Science Foundation No. 24-28-00312, https://rscf.ru/project/24-28-00312/

Conflict of interest. The Author declares no conflict of interest.

For citation: Smushkin A. B. New Information Components in the Formation of Electronic Evidence in Criminal Cases (the Modern Trail of Electronic-Digital Traces). *Siberian Law Review.* 2025;22(3):455-468. DOI: https://doi.org/10.19073/2658-7602-2025-22-3-455-468. EDN: https://elibrary.ru/koomry (In Russ.)

Введение

XXI век становится веком сетевого взаимодействия. Компьютерные сети нивелируют расстояния, сближая людей, позволяя решать многие вопросы и реализовывать свои права в дистанционном режиме. Ряд функций государственных органов также инициируется и выполняется в режиме сетевого взаимодействия. Однако обратной стороной медали выступает также и переход части преступности в киберпространственную среду. Все больше преступлений совершается в самих компьютерных сетях или с их использованием. Ученые уже начинают выделять не просто компьютерные преступления, а киберзависимые, совершение которых невозможно без использования информационно-компьютерной техники, и традиционные преступления, при совершении которых была использована информационно-коммуникационная технология [1, с. 22].

Киберпространство, аналогично обычному пространству, реализует принцип обмена Э. Локарда: любой контакт оставляет следы. Следы в киберпространстве являются отражением как прямых действий человека, так и автоматизированных действий электронного устройства. Подобное отражение можно рассматривать и как «основу ретроспективного уголовно-процессуального познания преступной деятельности» [2, с. 191]. Как отмечается, «след – это интегративная система, отражающая особенности личности киберпреступника, процесса или действия компьютерной системы при совершении киберпреступлений; след как процесс и результат взаимодействия субъекта с объектом находит свое отражение как на материальных объектах, так и в сознании людей, а также и в киберпространстве» [3, с. 295].

Еще в 2008 г. В. Б. Вехов предложил концепцию дорожки электронно-цифровых следов, под которой понимается «система образования следов в компьютерной сети, состоящая из нескольких последовательно расположенных по времени и логически взаимосвязанных записей о прохождении компьютерной информации по линиям связи через коммутационное оборудование оператора (-ов) связи от компьютера преступника (передатчика) до компьютера потерпевшего (приемника)»[1]. В 2019 г. он же, развивая свои предыдущие теории, указал на следующие элементы дорожки электронно-цифровых следов в компьютерной сети:

«1) технические данные, содержащиеся в файловой системе (реестре операционной системы и др.) компьютера преступника, свидетельствующие о подключении и использовании модема, либо записи, содержащиеся в модуле идентификации мобильного абонента и терминала, например, IMEI, Ki, IMSI-код, MIN, ESN и другие идентификаторы;

2) электронные данные, находящиеся в памяти компьютера или мобильного терминала преступника, подтверждающие факт отправки в адрес потерпевшего той или иной криминалистически значимой информации либо сеанс работы атакующего компьютера;

3) записи в памяти коммутационного устройства контроля, авторизации и аутентификации абонентов в сети оператора (-ов) связи и (или) провайдера услуг Интернет (контроллера сигналов, гейткипера для протокола H.323, сервера регистрации соединений абонентов и сервера определения месторасположения абонентов для протокола SIP – proxy-сервера);

4) записи в системе учета данных о начислении платы за оказанные услуги связи и (или) по доступу к компьютерной сети, а также о дате, времени, месте, способе и реквизитах их оплаты…

5) записи, автоматически регистрируемые в журнале событий компьютерной

[1] *Вехов В. Б.* Криминалистическое учение о компьютерной информации и средствах ее обработки : дис. … д-ра юрид. наук. Волгоград, 2008. С. 335.

сети, который находится на сервере оператора связи;

6) записи, автоматически образующиеся в памяти транзитных устройств различных операторов (провайдеров) при передаче по ним информации по протоколу IP (от англ. Internet Protocol);

7) записи в памяти серверов (FTP, SMTP, POP3 и др.) оператора связи (провайдера услуг Интернет), обслуживающего абонентский терминал потерпевшего, о входящих на него вызовах, соединениях и передачах компьютерной информации (электронных сообщений, почтовых отправлений и др.), а также о дистанционном управлении его информационными ресурсами;

8) записи в файловой системе (реестре операционной системы и др.) компьютера потерпевшего, в том числе мобильного терминала, о параметрах изменения подключения модема, настроек браузера, а также о нарушении режима работы или дезактивации средств защиты портов и компьютерной информации;

9) записи в памяти компьютера потерпевшего, содержащие сведения о полученной компьютерной информации, вредоносных программах, несанкционированном изменении системного и прикладного программного обеспечения, сбоях в их работе» [4, с. 19].

Впоследствии идею дорожки электронно-цифровых следов подхватили и другие авторы [5].

Разработка вопросов отслеживания дорожки электронно-цифровых следов имеет несомненное практическое значение. Е. Р. Россинская в ходе изучения последствий сетевого инцидента также отметила необходимость применения субъективного метода осмотра, выражающегося в данном случае в движении по цифровым следам, оставленным в Сети, начиная от скомпрометированной станции, далее по цепочке других компьютеров и серверов до устройства с которого началось проникновение [1, с. 95].

Фактически при обычном использовании компьютера в Сети дорожка электронно-цифровых следов при выполнении запроса (работе в Сети) отображается на следующих устройствах: компьютер пользователя – аппаратура провайдера – аппаратура адресата – ответ через аппаратуру провайдера – на аппаратуру пользователя. Однако с развитием компьютерной техники и сетевых технологий, а также цифровой трансформации раскрытия, расследования и предупреждения преступлений происходит существенная модификация дорожки электронных цифровых следов.

Рассмотрим основные новые концепты, влияющие на трансформацию и появление качественно иных свойств у дорожки электронно-цифровых следов.

Многоуровневая вложенность и системы виртуализации

Под многоуровневой вложенностью понимается возможность программного создания в рамках физического компьютера, виртуальной машины алгоритмической модели, имитирующей работу компьютерного устройства. Для создания виртуальных машин может быть использовано различное программное обеспечение, например, гипертерминал (Microsoft Hyper-V), Oracle VM VirtualBox и прочие.

В рамках одной виртуальной машины могут быть созданы и другие, внутри которых, в свою очередь, имеются еще слои. Глубина подобной виртуальной «матрешки» ограничивается фактически только объемом памяти и мощностью аппаратного обеспечения физического устройства. То есть следовая картина данных систем будет характеризоваться вложением следовой картины одного устройства в другое. В этой связи следы могут появиться на различных уровнях и в отдельных компонентах операционной системы и программного обеспечения. После завершения работы виртуальная машина может

быть удалена злоумышленником, что приведет также к стиранию расположенных в ней следов. При этом, вследствие отсутствия опыта или времени, злоумышленник по ошибке вместо полного удаления виртуальной машины с диска (команда «Удалить с диска») может лишь исключить ее запись из оснастки гипервизора, то есть сохранить следы ее использования, сохранить виртуальный диск на сервере. Подобные следы, в частности, могут быть обнаружены по пути C:\ProgramData\Microsoft\Windows\Hyper-V, где хранятся файлы конфигурации виртуальной машины при использовании гипервизора. Факт того, что на физическом устройстве ранее была установлена виртуальная машина, можно определить по следам в реестре, системных каталогах и файлах, а также каталогах, создаваемых самой виртуальной машиной.

Файлы, расположенные на виртуальном диске виртуальной машины, могут быть восстановлены при восстановлении самой виртуальной машины, к примеру, с использованием программы для восстановления удаленных данных Hetman Partition Recovery. Для этого диск, на котором, возможно, была установлена виртуальная машина, сканируется с использованием указанной программы, и при обнаружении соответствующих файлов таких форматов, как VDI, VMDK, VHD, VHDX, HDD, QED, QCOW, производится восстановление. Даже собственно файлы виртуальных машин имеют большое криминалистическое значение. Так, по данным П. А. Олейниковой и А. В. Караваевой, «файл *.vbox хранит в себе информацию об ОС, дате и времени создания ВМ, MAC-адресе. А файл *.vdi содержит полностью образ ВМ, включая в себя все программы, установленные на ВМ, пользовательские файлы (документы, изображения, видео и т. д.), системные файлы и другое» [6, с. 194]. Кроме того, при помощи программы Microsoft SQL Server Management Studio Express может быть установлено имя пользователя (Username), запустившего удаление виртуальной машины.

Следует также отметить, что модули программно-аппаратного комплекса «Мобильный криминалист», например «Скаут-МК», позволяют эффективно исследовать виртуальные машины, восстанавливая доступ даже к удаленной информации.

Системы виртуализации не ограничены только упомянутыми виртуальными машинами. Так, В. А. Мещеряков называет следующие:

– виртуализация операционных систем – развертывание на одной аппаратной основе нескольких одинаковых или разнородных и функционирующих независимо друг от друга операционных систем (фактически виртуальных компьютеров);

– виртуализация серверов приложений, как правило, выражается в виде интеллектуальной балансировки нагрузки, когда специальный балансировщик нагрузки управляет несколькими вебсерверами и приложениями как единой системой;

– виртуализация отдельных приложений – эксплуатация определенной совокупности программных продуктов в рамках изолированной виртуальной компьютерной среды (как программной, так и аппаратной);

– виртуализация сети – объединение аппаратных и программных ресурсов в единую виртуальную сеть;

– виртуализация аппаратного обеспечения и систем хранения информации, когда в виртуальных машинах могут создаваться представления аппаратных устройств, которых физически нет (эмуляция устройств), кроме того, в качестве параметров виртуальной машины (объем и тип оперативной памяти, процессор и т. п.) можно указать значения и типы, отличающиеся от реальной физической

конфигурации компьютера, подстраивая ее образ под желаемый вид [7, с. 147–148].

Появление подобных систем вносит существенные изменения в формирование дорожки электронно-цифровых следов. Так, на виртуальных машинах верхнего уровня, несмотря на нахождение на той же физической машине, не будут проявляться виртуальные следы терминала нижнего уровня. Следовательно, при обнаружении физического устройства с признаками многоуровневой вложенности виртуальной машины следует пытаться выявить и проверить каждый слой каждой эмулированной машины.

Эмулированные на устройстве виртуальная операционная система или иное компьютерное устройство могут быть созданы конкретно для совершения определенных деяний. После них на первичном устройстве можно будет обнаружить лишь виртуальные следы программы гипервизора, но не самих эмулированных устройства или операционной системы.

Особо хотелось бы отметить взаимосвязь подобной виртуальной вложенности, а также эмуляции одних устройств на других применительно к цифровым отпечаткам компьютерного устройства (device fingerprint – *англ.*), используемым, прежде всего, в банковской деятельности. Цифровой отпечаток представляет собой «цифровой след, который сформирован в виде производного значения параметров, конфигурации программного и аппаратного обеспечения конкретного компьютерного устройства»[2]. Использование цифровых отпечатков компьютерного устройства (отраженных в формуле, вычисленной с определенной функцией хеширования с длиной хеш-кода 512 бит, которая представляет собой строку фиксированной длины) дает достаточно высокую степень его идентификации. При этом цифровой отпечаток учитывает системные и аппаратные параметры устройства, версию браузера, идентификаторы аппаратной части устройства, версию операционной системы и т. д. Использование указанных выше методов эмуляции и виртуальной вложенности подменяет считываемую картину следов на следы эмулируемого устройства или операционной системы, что при обнаружении самого физического устройства может повести следствие в неверном направлении.

Отдельно необходимо рассмотреть следовую картину виртуальной частной сети (Virtual Private Network, VPN – *англ.*). VPN – это «сетевая технология, которая обеспечивает безопасное расширение локальной сети посредством публичной сети (такой, как интернет), с помощью инкапсуляции, шифрования пакетов данных в различных удаленных точках, публичной инфраструктуры передачи данных» [8, с. 24]. Существует множество технологий и протоколов VPN – от подмены источника запроса, аналогичного прокси-серверу, до туннелирования запроса.

С учетом подмены виртуальной сетью IP-адреса первоначального компьютера коренным образом меняется дорожка электронно-цифровых следов. В обычном режиме применяется следующая схема: используемое интернет-устройство пользователя делает запрос провайдеру, который направляет в глобальную сеть Интернет, получает ответ от Сети и направляет пользователю. Таким образом, имеется возможность непрерывного отслеживания дорожки электронно-цифровых следов с участием провайдера, который выполнит требования закона по предоставлению соответствующей информации правоохранительным органам. В случае использования VPN пользователь отправляет зашифрованный запрос на подключение к VPN-серверу своему провайдеру, далее проводится соединение

[2] *Цифровая* криминалистика : учеб. для вузов / В. Б. Вехов [и др.] ; под ред. В. Б. Вехова, С. В. Зуева. 2-е изд., перераб. и доп. М. : Юрайт, 2024. С. 292–304.

с данным сервером, и с этого момента дорожка следов прерывается для внешнего наблюдателя. Дальнейшее взаимодействие пользователя с сетью Интернет происходит через VPN-сервер и от его имени. Следовательно, IP направившего запрос пользователя меняется – следы пропадают из поля зрения провайдера. Серверы виртуальной частной сети чаще всего недоступны правоохранительным органам, и их владельцы редко будут предоставлять информацию по запросу.

При использовании шифрования и тоннельной маршрутизации вероятность установления дорожки электронно-цифровых следов еще меньше. Тоннельная маршрутизация представляет собой построение сетей, при котором один протокол инкапсулируется в другой и за счет этого не подвержен мониторингу. Это можно назвать даже не виртуальной частной, а виртуальной защищенной сетью.

Как отметил В. А. Мещеряков, «внедрение виртуальных сетей приводит к возможности динамической миграции приложений и сервисов по территориально и географически распределенной информационной инфраструктуре, при которой начало работы с сервисом может быть реализовано вычислительными мощностями, расположенными в одном месте, продолжены в другом, а завершены в третьем. Вместе с тем предоставление сервиса не прерывается, а его миграция абсолютно незаметна для конечных пользователей. Фактически единый логически законченный след работы прикладного сервиса становится распределенным как во времени, так и в пространстве» [7, с. 149].

Однако полностью гарантировать отсутствие следов при использовании VPN не всегда возможно. Некоторые виртуальные частные сети ведут журналы, которые фиксируют данные, позволяющие идентифицировать пользователя (логин и пароль для входа, электронный адрес, пропускную способность, данные соединения и т. д.). Операторы VPN-сервиса могут вести логирование трафика, зачастую не предупреждая об этом пользователей.

Следующим элементом, несущим на себе следы работы в Сети даже при использовании VPN, являются сторонние cookie-файлы, с помощью которых осуществляется таргетирование рекламы. Не все сайты предупреждают об установке на устройство пользователя этих файлов. Многие cookie-файлы даже после их удаления и перезагрузки устройства автоматически восстанавливаются. Значительное количество сайтов мониторит отпечатки браузера, что позволяет установить терминал, с которого осуществлялся вход, даже при использовании VPN.

Использование луковичной маршрутизации Tor

Большое количество преступлений в последнее время совершается с использованием теневого сегмента сети Интернет – Даркнета [9]. При этом исследование дорожки электронно-цифровых следов существенно осложняется средствами анонимизации, в первую очередь луковичным шифрованием Tor (The Onion Router – *англ.*). При его использовании применяется многослойное шифрование запроса, где каждый слой шифров вскрывается на новом узловом устройстве, оставляя анонимными и скрытыми другие следы. Дорожка виртуальных следов в случае использования луковичной маршрутизации Tor представляется дискретной линией с более или менее отрезанными от следов на предшествующих или последующих устройствах отрезками с размытыми временем доступа и корреляцией событий. Выбор промежуточных узлов, добровольно предоставленных для использования, осуществляется на основании случайного маршрута. При этом в сети Tor входной узел не видит адресата запроса, центральный узел – автора и адресата, выходной – автора запроса.

Следует учитывать, что использование промежуточных узлов приводит и к появлению в рамках дорожки множества IP-адресов устройств. Практика ошибочных задержаний владельцев выходных узлов, как оставивших итоговые электронно-цифровые следы при совершении преступлений в киберпространстве, уже имеется. Вместе с тем на компьютере подозреваемого пользователя узлов сети Tor (причем выявить этого подозреваемого – нелегкая задача) могут быть обнаружены только установленный Tor-клиент, а также следы использования сети Tor в записях реестра. Подобная сложная трассировка и многоуровневое шифрование делают практически невозможным отслеживание дорожки до пользователя – источника действий. Следует также учитывать, что браузер Tor предоставляет доступ к ряду скрытых в Даркнете сервисов и доменов (.onion), невозможный из обычных браузеров, при этом не сохраняя историю посещений, что даже в случае идентификации пользователя и получения доступа к его устройству осложняет изучение дорожки следов. Одновременно с этим для доступа к указанным доменам используется особый протокол Tor Hidden Services Protocol и отсутствуют обычные DNS-запросы, которые позволили бы отследить пользователя.

Полиморфные программы

В. А. Мещеряков рассматривает также особенности следообразования при выявлении полиморфных вредоносных программ и вирусов [7, с. 144–146]. Очевидно, что необходимо исследовать как полиморфные вирусы, так и любые полиморфные программы, не только зловредного характера (например, в европейских странах активно используются так называемые служебные вирусы – специальные программы получения скрытого доступа к пользовательским устройствам для проведения тайного онлайн-обыска).

Сущность подобной программы заключается в ее применении к самой себе с целью трансформации программного кода путем подстановки синонимических элементов. Полиморфные программы могут изменять свою структуру, характеристики (включая даже хеш-сумму), порядок выполнения операций, маскировать цифровые следы. В то же время может использоваться различная техника мутаций. За каждым экземпляром вроде однотипных полиморфных программ могут стоять различные паттерны изменения и поведения. Некоторые полиморфные программы могут дробиться на части, каждая из которых будет отдельно загружаться и самостоятельно выполняться. Сетевые протоколы соединения с серверами у полиморфных программ тоже могут отличаться от обычных.

Указанные обстоятельства существенно осложняют выявление и исследование дорожки электронно-цифровых следов вследствие перманентного изменения программы в ходе работы. Получается, различные элементы цепочки электронно-цифровых следов могут соответствовать состояниям программы в разные периоды ее трансформации, могут быть фрагментированы, а также иметь отличающиеся от обычных взаимосвязи с другими элементами.

Распределенная информация

При использовании распределенной информации один информационный объект дробится на некоторое количество частей, размещаемых в множестве узлов Сети. В некоторый момент времени может не оказаться ни одного пользователя, владеющего информационным объектом целиком, но при этом совокупность частей, размещенных в Сети, будет составлять единый объект.

Специфика следообразования при использовании распределенных сетей будет заключаться в наличии следов не целого

объекта, а лишь его части, которая не может дать полное представление о содержании целого объекта. Фактически в данном случае должно происходить восстановление целого по частям, в связи с чем необходимо использовать специализированные программы-клиенты. Без их применения файлы так и будут оставаться разрозненными элементами, не позволяющими восстановить не только содержание, но и формат и иные метаданные целого объекта. Применение подобных программ-клиентов может оставлять следы в системном реестре устройства пользователя, временных файлах, удаленных файлах, месте установки программы, месте нахождения ярлыка программы, реестре автозагрузок, папках недавно использованных программ и файлов, а также в самих программах-клиентах, свидетельствующих о поиске и перекачке определенной информации, и т. д. При работе программы-клиента следы остаются на устройстве скачивающего пользователя (причем иногда, удалив скачанную информацию с устройства, он может забыть стереть ее из памяти программы), на оборудовании провайдера, в программе-клиенте раздающего пользователя. Использование торрентов представляет собой частично децентрализованную информацию, то есть имеются централизованные серверы, на которых можно обнаружить список раздающих определенный цифровой объект. Пользователи, скачав этот список, соединяются напрямую. На компьютере пользователя при этом могут быть обнаружены сами торрент-файлы (списки), программы-клиенты (оставившие следы в виде ярлыков, следов установки, удаления, следов в автозагрузке, в папках недавно использованных программ), частично скачанные информационные объекты, полностью скачанные объекты, следы удаленных объектов. В программах-клиентах также могут быть обнаружены соответствующие следы. В них содержится URL трекера, имя, размер файла и контрольные хеш-суммы SHA1-сегментов раздаваемых файлов. В программах-клиентах торрентов может быть выявлена следующая информация: список скачиваемых, скачанных и раздающихся файлов, настройки раздачи (ограничения или полный запрет на раздачу), IP-адреса, с которых происходит скачивание, адреса трекеров, с которых производился поиск определенных файлов. Таким образом, следовая картина при использовании систем распределенного хранения информации будет существенно отличаться от классических электронно-цифровых следов. Дорожка следов будет содержать элементы логически законченных, но нечитаемых объектов (пока не завершится процесс скачивания), следы одного и того же объекта (с одинаковой хеш-суммой) будут находиться у нескольких пользователей.

Специфика дорожки электронно-цифровых следов в RAID-массивах

RAID-массивы представляют собой несколько физических дисков, объединенных в один логический. Связь между физическими дисками может быть как проводной, так и беспроводной. Операционная система воспринимает этот комплект как один диск, вне зависимости от типа связи и места расположения. В связи с этим возникает специфическое воплощение дорожки электронно-цифровых следов. Поскольку операционная система воспринимает RAID-массив как один логический диск, то и запись ведется как на обычный винчестер не последовательно, а по свободным секторам любого физического диска. Следовательно, электронно-цифровой след может быть распределен по нескольким физическим дискам, и его сборка может зависеть от последовательности расположения (подключения) дисков в массиве. Как отмечает В. А. Мещеряков, «с точки

зрения криминалистики подобная ситуация порождает эффекты распределения единого следового объекта на несколько взаимосвязанных частей, которые могут формироваться, храниться, обрабатываться, передаваться и уничтожаться абсолютно независимо друг от друга. При этом уголовно-релевантные свойства этого следового объекта будут проявляться только при совместном комплексном использовании образующих его частей, а каждая из его частей вообще не может быть соотнесена с уголовно-релевантными событиями или соотнесена с большими технологическими трудностями» [7, с. 143].

Следует также учитывать, что массивы типа RAID1, а также производные составные массивы RAID10 и RAID01 (то есть массивы типа RAID0, организованные из массивов RAID1, или наоборот) построены по принципу отзеркаливания, так что информация дублируется на физических дисках, входящих в массив, при этом также дублируются и следы.

Следы в системе блокчейн

Блокчейн является системой криптографических блоков распределенного хранения информации без единого сервера. Степень отслеживаемости следов в блокчейне зависит от его алгоритма и типа. Самым распространенным методом работы блокчейна является доказательство работы (Proof of Work, PoW – *англ.*) – алгоритм консенсуса при подтверждении транзакции. А. В. Аносов пишет: «По условиям функционирования блокчейна функцию защиты единицы информации от изменения или замены целиком выполняет распределение транзакций в блоки со строгой привязкой ко времени осуществления транзакции и с расчетом криптографической хеш-функции для каждого из блоков… Сформированные блоки организуются в упорядоченную цепь (собственно блокчейн), при этом ключевые свойства блоков (такие как хеш-код и время прохождения транзакции) выделяются в заголовок блока, что позволяет значительно упростить процедуру проверки корректности блокчейна. Кроме того, каждый заголовок блока содержит указатель на предыдущий блок. Таким образом, все блоки в блокчейне оказываются тесным образом взаимосвязаны между собой несколькими ключевыми значениями, исключающими подмену или модификацию отдельного блока» [10, с. 214]. Следовательно, каждый новый блок содержит в себе информацию о всех предыдущих транзакциях, то есть о предшествующих частях дорожки электронно-цифровых следов. Посредством блокчейна информация через распределенные записи децентрализуется, последовательно хешируется (англ. *hashing* – «перемешивание, преобразование») и зашифровывается[3]. Следует отметить открытость информации блокчейна только в отношении транзакций, но не пользователей. Можно установить историю, транзакции каждого блока информации, но не его пользователя.

Однако не все так легко. Среди тех же криптовалют выделяются анонимные криптовалюты (например, Monero, Firo, Zcash). Кроме того, существуют разработки в области блокчейн-миксера, в котором информация на некоторое время «зависает» в миксере и потом направляется в перемешанных информационных потоках и в разное время. В ходе анализа изъятого оборудования, использованного для совершения блокчейн-транзакций, можно установить соответствующее программное обеспечение (или следы его удаления), следы в реестре, использовать разработки в области методов анализа транзакций,

[3] *Usher V.* Cybersecurity and the future of blockchain technology // GingerMay. 2017. URL: https://teamgingermay.com/cybersecurity-blockchain-technology/ (дата обращения: 08.04.2025).

кластеризации адресов, распознавания образов и т. д. Особое значение приобретает исследование электронно-цифровых следов при хищениях в сфере криптовалют [11].

Облачные сервисы

Облачные сервисы и системы синхронизации информации облачных сервисов представляют собой комплекс услуг, связанных с удаленной деятельностью. В большинстве случаев при применении облачных сервисов устройство пользователя используется только как терминал, то есть, в зависимости от типа сервиса, необходимости сокрытия информации и т. д., на устройстве пользователя могут быть обнаружены только следы, связанные с программой удаленной работы с облачным сервисом. Устройство злоумышленника может входить в облачные сервисы с помощью токена, удаление и выбрасывание которого может составлять 3–4 движения, что к моменту осмотра устройства явно оставит обрезанной дорожку электронно-цифровых следов.

Кроме того, рассматривая дорожку электронно-цифровых следов при использовании облачных сервисов, необходимо обратить внимание на ряд специфических черт. Во-первых, облачные сервисы используют принцип распределенного хранения информации, что приводит к распределению частей каждого элемента дорожки между многими серверами. Во-вторых, пользователь может входить в облачный сервис с разных устройств и из разных мест, что может привести к перманентной изменчивости даже последовательных элементов дорожки. В-третьих, некоторые провайдеры облачных сервисов предоставляют пользователям возможность выбора географического расположения серверов (например, вне российской юрисдикции, в странах, не имеющих договоров о взаимной правовой помощи с РФ или умышленно игнорирующих российские запросы). Провайдеры облачных хранилищ могут сохранять информацию об IP-адресах пользователей, местоположении устройств, цифровых отпечатках устройств и браузеров, пользовательских запросах в поисковых системах, действиях пользователей в Интернете, связанных с применением облачного сервиса, однако и сами провайдеры часто расположены за рубежом, и пользователи обычно уведомляются о подобных условиях использования. Именно облачные элементы дорожки представляют собой следы регистрации, доступа к данным, взаимодействия пользователей, использования API-вызовов, информацию о всех сбоях и ошибках. Указанные данные собираются и анализируются сервером автоматизированно. При этом серверы облачных сервисов периодически проходят процедуру резервного копирования, при которой в том числе копируются и элементы дорожки следов, но сохраняются в разных местах. Следует также учитывать дублирование следов с некоторых устройств в облачных сервисах. Так, облачные сервисы Google и «Яндекс», технологии iCloud могут сохранять ряд объектов, настройки, треки навигатора и т. п. в рамках одного аккаунта на разных носителях одновременно, что дает возможность доступа, например к фотографиям или иным объектам, с любого устройства с авторизованным аккаунтом.

Использование методов сокрытия дорожки следов

Использование методов сокрытия электронно-цифровых следов существенно влияет на особенности дорожки следов. Среди подобных средств можно назвать сокрытие и запутывание следов.

В ходе сокрытия данных могут использоваться методы стеганографии, обратимого шифрования или сокрытия файлов в менее доступных областях диска. Каждый из этих методов меняет дорожку

электронных следов или ее свойства. В первом случае данные одного типа скрываются в данных другого типа (например, фотография в аудиофайле), что, не меняя расположения элементов дорожки следов, запутывает и скрывает их наличие. Шифрование, в отличие от стеганографии, не скрывает сам факт наличия данных (следов), но делает невозможным их изучение без ключа шифрования или взлома кода. В третьем случае след может размещаться в неразмеченной области диска, недоступной для файловой системы и пользователя, что препятствует его прямому выявлению и исследованию. Без специальных программ ни размещение в неразмеченной области диска, ни выявление наличия там следа невозможно.

При запутывании следов возможны изменение расширения файла вручную, изменение сигнатуры файла (данных, необходимых для его программной идентификации), манипуляция с метаданными файла и временными метками, что осложнит его идентификацию как элемента дорожки электронно-цифровых следов преступления (например, изменение временных меток файла выведет его за пределы заданной специалистами временной шкалы и воспрепятствует его обнаружению). В современных версиях операционных систем возможно отключение ведения некоторых журналов, что не дает отразиться в них элементам дорожки следов, предотвращая само их появление.

Перспективные разработки

В последнее время активизируются разработки в области квантовых компьютеров. В. Поляков отмечает: «В современных компьютерных устройствах запись и обработка информации проводится путем кодирования электромагнитных сигналов. В квантовом компьютере это происходит на основе иных физических принципов, основанных на использовании особенностей квантовых состояний микрочастиц. Применение квантовых компьютеров может привести к резкому ускорению развития технологий искусственного интеллекта. Полагаем, что использование квантовых компьютеров в криминалистическом аспекте проявится в появлении нового по своему техническому содержанию вида следов, возникающих при воздействии на компьютерную информацию. Таким образом, механизм следообразования, в начале 2000-х годов относительно изученный криминалистикой, для случаев электронно-цифровых следов потребует, на наш взгляд, нового переосмысления и дополнения» [12, с. 24]. Следует также учитывать, что квантовая теория основана не на детерминизме и закономерностях, а на вероятности – это существенно меняет всю концепцию виртуальной следовой картины и принципы работы с виртуальными следами. В данном случае мы умышленно оперируем термином «виртуальный след», поскольку полагаем, что он обладает более высоким уровнем обобщения, чем «электронно-цифровой след». Последний входит в виртуальные следы как один из видов. Как уже было указано ранее, «данное наименование обусловлено универсальностью термина, охватывающего искусственное инцидентное пространство формализованных моделей (созданного путем информационных (математических) преобразований) описания реальных объектов или явлений. Кроме того, в данном контексте виртуальность означает нечто дополняющее физическую реальность (аналогично виртуальной памяти, использующей ресурсы жесткого диска при недостаточности физической оперативной памяти)»[4].

[4] *Смушкин А. Б.* Цифровизация криминалистической деятельности : + еПриложение: дополнительные материалы : учеб. пособие для студентов магистратуры, обучающихся в юрид. вузах, специалистов / под ред. В. Б. Вехова. М. : КноРус, 2024. С. 93.

Заключение

Таким образом, представляется необходимым перманентное изучение влияния новых концептов на дорожку электронно-цифровых следов для разработки эффективных, отвечающих последним достижениям науки и техники криминалистических рекомендаций по ее выявлению, фиксации и исследованию в целях скорейшего раскрытия и расследования уголовных дел. Качественно иные концепты в области электронной информации существенно меняют следовую картину в киберпространстве и требуют специфических подходов.

Список литературы

1. Теория информационно-компьютерного обеспечения криминалистической деятельности : моногр. / Е. Р. Россинская, А. И. Семикаленова, И. А. Рядовский, Т. А. Сааков ; под ред. Е. Р. Россинской. М. : Проспект, 2022. 256 с.
2. Давлетов А. А. Основы уголовно-процессуального познания. [2-е изд., испр. и доп.]. Екатеринбург : Изд-во Гуманитар. ун-та, 1997. 191 с.
3. Даниленко Ю. А. Криминалистическое распознавание в тактике производства следственных действий при расследовании преступлений в сфере компьютерной информации // Ученые записки Крымского федерального университета имени В. И. Вернадского. Юридические науки. 2023. Т. 9 (75), № 2. С. 294–298.
4. Вехов В. Б. Дорожка электронных следов: понятие и особенности судебного компьютерно-технического исследования // Уголовное производство: процессуальная теория и криминалистическая практика : материалы VII междунар. науч.-практ. конф., 25–26 апр. 2019 г., Симферополь–Алушта / отв. ред.: М. А. Михайлов, Т. В. Омельченко. Симферополь : Ариал, 2019. С. 18–20.
5. Карепанов Н. В. Особенности технологии агрегирования, исследования и использования электронно-цифровых следов преступления // Технологии XXI века в юриспруденции : материалы четвертой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 г.) / отв. ред. Д. В. Бахтеев. Екатеринбург : Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 86–104.
6. Олейникова П. А., Караваева А. В. Поиск следов применения виртуальной машины Oracle VM VirtualBox на предмет наличия криминалистически значимой информации // Вестник Алтайской академии экономики и права. 2022. № 10-1. С. 189–195. DOI: https://doi.org/10.17513/vaael.2448
7. Мещеряков В. А. Теоретические основы механизма следообразования в цифровой криминалистике : моногр. М. : Проспект, 2022. 176 с.
8. Хесус Назарет Бенитес Гонсалес. Технологии создания виртуальных частных сетей // Молодой исследователь Дона. 2016. № 2 (2). С. 24–26.
9. Вехов В. Б. Проблемы борьбы с экстремизмом в «Даркнет» // Шумиловские чтения : сб. материалов междунар. науч.-практ. конференции, 30 нояб. 2023 г. / отв. ред.: Д. А. Бражников, Л. Е. Калинина. М. : Рос. таможн. Акад., 2023. С. 47–53.
10. Аносов А. В. Использование технологии блокчейн в процессе формирования и учета криминологической информации // Вестник Казанского юридического института МВД России. 2018. №. 2 (32). С. 211–216. DOI: https://doi.org/10.24420/KUI.2018.32.13968
11. Шнейдерова Д. И. Цифровые следы в системе следов по делам о хищениях в сфере оборота криптовалют // Вестник Дальневосточного юридического института МВД России. 2024. № 2 (67). С. 102–111.
12. Поляков В. К проблеме использования понятия «искусственный интеллект» в криминалистике // Юрислингвистика. 2022. № 25 (36). С. 21–28. DOI: https://doi.org/10.14258/leglinleglin(2022)2504

References

1. Rossinskaya E. R., Semikalenova A. I., Ryadovskii I. A., Saakov T. A. *Theory of Information-Computer Support for Criminalistic Activity*. Moscow: Prospekt Publ.; 2022. 256 p. (In Russ.)
2. Davletov A. A. *Foundations of Criminal-Procedural Cognition*. 2nd ed. Yekaterinburg: University for Humanities Publ.; 1997. 191 p. (In Russ.)
3. Danilenko Yu. A. Criminalistic Recognition in the Tactics of Producing Investigative Actions in the Investigation of Crimes in the Sphere of Computer Information. *Scientific Notes of V. I. Vernadsky Crimean Federal University. Juridical Science*. 2023;9(2):294-298. (In Russ.)
4. Vekhov V. B. Digital Trail: Concept and Features of Forensic Computer-Technical Examination. In: Mikhailov M. A., Omel'chenko T. V. (Eds.). *Criminal Proceedings: Procedural Theory and Forensic Practice.* Simferopol: Arial Publ.; 2019. P. 18–20. (In Russ.)
5. Karepanov N. V. Features of the Technology of Aggregation, Research and Use of Electronic Digital Traces of Crime. In: Bakhteev D. V. (Ed.). *21st-Century Technologies in Jurisprudence*. Yekaterinburg: Ural State Law University named after V.F. Yakovlev Publ.; 2022. P. 86–104. (In Russ.)

6. Oleinikova P. A., Karavaeva A. V. Search for Traces of the Use of the Oracle VM VirtualBox Virtual Machine for the Presence of Forensically Significant Information. *Vestnik Altajskoj akademii ekonomiki i prava*. 2022;10-1:189-195. DOI: https://doi.org/10.17513/vaael.2448 (In Russ.)

7. Meshcheryakov V. A. *Theoretical Foundations of the Mechanism of Trace Formation in Digital Criminalistics*. Moscow: Prospekt Publ.; 2022. 176 p. (In Russ.)

8. Jesús Nazareth Benitez González. Virtual Private Networks Design Technologies. *Young Don Researcher*. 2016;2:24-26. (In Russ.)

9. Vekhov V. B. Problems of Combating Extremism on the "Darknet". In: Brazhnikov D. A., Kalinina L. E. (Eds.). *Shumilov Readings*. Moscow: Russian Customs Academy Publ.; 2023. P. 47–53. (In Russ.)

10. Anosov A. V. The Use of Blockchain Technology in the Process of Forming and Accounting Criminological Information. *Bulletin of the Kazan Law Institute of MIA of Russia*. 2018;2:211-216. DOI: https://doi.org/10.24420/KUI.2018.32.13968 (In Russ.)

11. Shneiderova D. I. Digital Traces in the System of Traces in Cases of Theft in the Sphere of Cryptocurrency Turnover. *Vestnik of the Far Eastern Law Institute of the Ministry of Internal Affairs of Russian Federation*. 2024;2:102-111. (In Russ.)

12. Polyakov V. On Using the Concept of "Artificial Intelligence" in Forensic Science. *Legal Linguistics*. 2022;25:21-28. DOI: https://doi.org/10.14258/leglinleglin(2022)2504 (In Russ.)

Информация об авторе

Александр Борисович Смушкин, доцент кафедры криминалистики, ведущий научный сотрудник проектного офиса научных программ и исследований Саратовской государственной юридической академии (ул. Вольская, 1, Саратов, 410056, Российская Федерация), кандидат юридических наук; ORCID: https://orcid.org/0000-0003-1619-8325; ScopusID: 57202012484; ResearcherID: AAM-2853-2020; SPIN-код: 7360-6396, AuthorID: 439039.

About the Author

Aleksandr B. Smushkin, Associate Professor of the Department of Criminalistics, Lead Researcher of the Project Office of Scientific Programs and Research at the Saratov State Law Academy (1 Volskaya str., Saratov, 410056, Russian Federation), Candidate of Legal Sciences; ORCID: https://orcid.org/0000-0003-1619-8325; ScopusID: 57202012484; ResearcherID: AAM-2853-2020; SPIN-code: 7360-6396, AuthorID: 439039.

Поступила | Received 10.04.2025

Поступила после рецензирования и доработки | Revised 09.06.2025

Принята к публикации | Accepted 16.06.2025