

Научная статья
УДК 343.98
EDN RUAXMF
DOI 10.17150/2411-6122.2025.2.70-81



Особенности элементов механизма образования электронных следов в сети Интернет

И.С. Поляков

Московская академия Следственного комитета Российской Федерации имени А.Я. Сухарева,
г. Москва, Российская Федерация, polyakov_is@sledcom.ru

Аннотация. В настоящем исследовании освещены отдельные особенности следующих элементов механизма образования электронных следов в информационно-телекоммуникационных сетях (частным примером которой является Интернет): следовоспринимаемые и следовоспринимающие (отражающие) объекты, среда воздействия и преобразование (контактное взаимодействие, которое в отдельных случаях следует обозначать как воздействие). Рассмотрены основные составляющие сети Интернет, исходя из отечественного нормативного регулирования, а также принцип ее функционирования с помощью периферийного оборудования, которое участвует в слеодообразовании. Кратко охарактеризованы модели воздействия, исходя из нацеленности деятельности пользователя и ее порядка, с раскрытием примеров криминалистически значимой информации, которая может быть при этом обнаружена. Схематично описан механизм образования электронных следов в сети Интернет (следов преступной деятельности, образуемых с помощью информационно-телекоммуникационных технологий).

Ключевые слова: электронные следы, механизм слеодообразования, информационно-телекоммуникационные сети, Интернет, виртуальное пространство, следовоспринимающие объекты, следовоспринимаемые объекты.

Для цитирования: Поляков И.С. Особенности элементов механизма образования электронных следов в сети Интернет / И.С. Поляков. — DOI 10.17150/2411-6122.2025.2.70-81. — EDN RUAXMF // Сибирские уголовно-процессуальные и криминалистические чтения. — 2025. — № 2. — С. 70–81.

Original article

Special Features of Electronic Trace-Formation Mechanism on the Internet

I.S. Polyakov

Sukharev Moscow Academy of the Investigative Committee of the Russian Federation,
Moscow, the Russian Federation, polyakov_is@sledcom.ru

Abstract. The presented study highlights specific features of the following element of electronic trace-formation mechanism in information and telecommunication networks (of which the Internet is a particular example): traceable and trace-receptive (reflecting) objects, the impact medium and the transformation (contact interaction, which in certain cases should be labelled as impact). The author examines key components of the Internet from the standpoint of Russian normative regulation, as well as the principle of the Net's functioning via peripheral equipment, which is involved in trace formation. The models of impact are briefly described based on the targeting and the order of the user's activities, and examples of forensically significant information that could be detected are presented. The author also

offers a schematic description of the mechanism of electronic trace formation on the Internet (traces of criminal actions formed with the use of information-telecommunication technologies).

Keywords: electronic traces, the mechanism of trace formation, information and telecommunication networks, Internet, virtual space, trace-receptive objects, traceable objects.

For citation: Polyakov I.S. Special Features of Electronic Trace-Formation Mechanism on the Internet. *Sibirskie Ugolovno-Processual'nye i Kriminalisticheskie Chteniya = Siberian Criminal Procedure and Criminalistic Readings*, 2025, no 2, pp. 70–81. (In Russian). EDN: RUAXMF. DOI: 10.17150/2411-6122.2025.2.70-81.

Введение

В юридической литературе давно ведутся дискуссии о выработке единого (или хотя бы единообразного) подхода к описанию механизма образования электронных следов или следов преступной деятельности, образуемых с помощью информационно-телекоммуникационных технологий [1; 2, с. 223]. Сложность заключается в необходимости его интеграции в механизм преступления, которое в свою очередь может не ограничиваться сферой компьютерной информации, однако требует изучения с технической стороны [3, с. 74]. При этом отмечается несовершенство понятийно-категориального аппарата криминалистики и проблемы критериев разграничения преступлений в сфере информационных технологий [4, с. 20; 5, с. 47]. Тем не менее именно использование информационных технологий, предполагающих наличие субъекта и объекта воздействия (контактного взаимодействия), производящие мощности и алгоритмы обработки, являются предопределяющими для механизма образования электронного следа. При его изучении в информационно-телекоммуникационных сетях следует выделить особенности элементов его механизма: объектов, пространства и преобразования (контактного взаимодействия).

Объекты и отражение

Следовоспринимающие и следовоспринимаемые объекты имеют физическую форму, однако их взаимодействие имеет место в электронной среде (виртуальном пространстве). Изменение данной среды (отражение следа) происходит посредством передачи сигналов — электрического тока (электрических импульсов) или радиоволн с заранее известными характеристиками. Электрические импульсы используются для хранения, пересылки, передачи, транзита и обмена данных и выступают в качестве средства переноса информации.

Отражение подразумевает собой воздействие одной материальной системы на другую и выражается в диалектической связи этих двух объектов и проявляется через их различие [6, с. 32; 7, с. 233]. Данное отражение потенциально отчуждаемо и становится отображением при его фиксации на материальном носителе или копировании на него. На материальном носителе фиксируется лишь электронный образ модели реального объекта или процесса, вернее, как пишет Агибалов В.Ю., цифровое значение параметров математической модели, на основании которой при определенных условиях сигнал преобразуется в физический процесс, подобный исходному следообразующему объекту [8, с. 60].

Само по себе отражение еще не является следом, поскольку пока сигнал не принят конечным устройством, именно результат процесса отражения, восприятие компьютерной системой — массивом памяти устройства — является следом.

Исходя из начал частной криминалистического учения о механизмах следообразования), отметим большее количество следовоспринимающих и следообразующих объектов в сравнении с разработанными отечественными подходами к механизму следообразования в компьютерной системе [9–11].

Доступ к информационно-телекоммуникационным сетям, в частности к сети Интернет, обеспечивает периферийное оборудование по типу роутера, коммутатора, маршрутизатора — внешние электронные устройства, помимо компьютерного (электронно-вычислительной машины).

Интернет, иногда именуемый как глобальная компьютерная сеть и классифицируемый как пример сети широкой зоны, является системой сетей, использующих определенные общие протоколы и предоставляющих доступ к определенным сервисам, функционирует за счет маршрутизации пакетов данных (коммутации; англ. «packet switching») и базируется на стеке протоколов передачи данных (наборов правил) модели TCP/IP (англ. «Transmission Control Protocol (TCP)» и «Internet Protocol (IP)»). В соответствии с ней работает аппаратное и программное обеспечение.

При соединении посредством сигналов направляется запрос на подключение (пакет); при подтверждении соединения далее направляется запрос данных, в ответ на который направляются запрашиваемые сведения — имеет место так называемое рукопожатие (см. рис. 1).

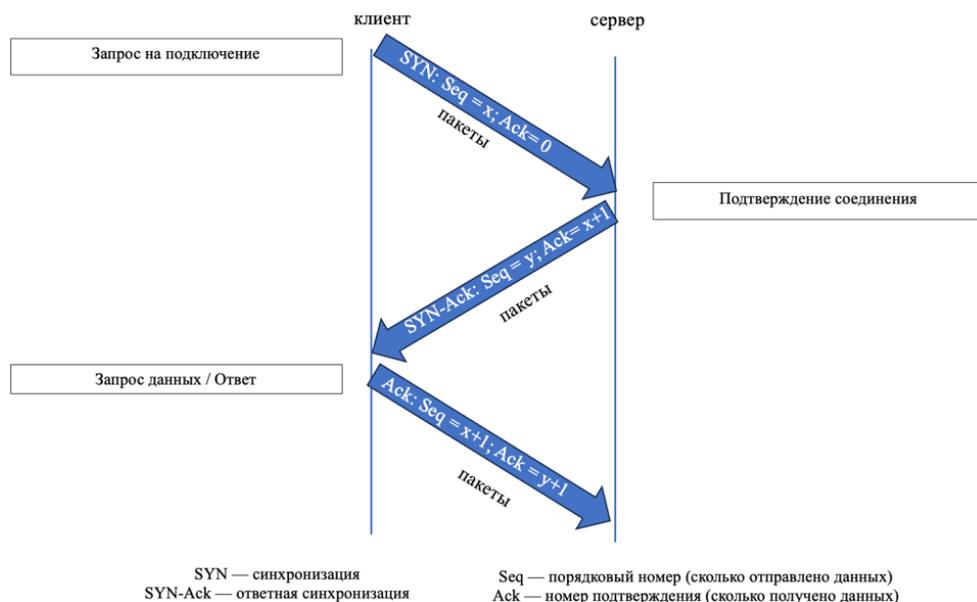


Рис. 1. Рукопожатие при защищенном соединении

Пользователь, использующий компьютерную систему, выступает в качестве отражаемого объекта. В качестве объектов, которые отражают его действия в системе, последовательно при направлении запроса выступают элементы, необходимые для доступа в информационно-телекоммуникационную сеть (далее — ИТС): коммутатор, оборудование провайдера Интернет-услуг, точка обмена трафиком (сервис), где хранится закодированная информация (Интернет-ресурс). При осуществлении рукопожатия (передачи пакетов) каждый из перечисленных элементов как воспринимает отражение от предыдущего, так и последовательно образует его при взаимодействии со следующим.

Пространство

Среда взаимодействия по-разному определяется в юридической литературе. Например, условным местом совершения уголовно-наказуемого деяния называют часть «кибернетического пространства» (киберпространства) — совокупность ЭВМ, системы ЭВМ и сети [12]. Также под средой взаимодействия предлагается понимать виртуальное пространство информационной системы или электронную среду [13].

Как указано в п. 4.2.10 ГОСТ 52292-2004, под электронной средой понимается среда технических устройств или аппаратных средств, функционирующих на основе физических законов и используемых в информационной технологии при обработке, хранении и передаче данных. Для ее описания может использоваться среда логических объектов на основе математических законов — цифровая среда. Они в свою очередь продуцируются на основе электронной среды в виде распределенных систем. Частным случаем электронной среды является Интернет-

инфраструктура, включающая персональные, связанные и сетевые устройства, на основе которых формируются электронно-цифровые платформы.

Элементом ИТС Интернет является Интернет-ресурс. Например, веб-страница (электронный файл, размещенный на сервере), почтовый сервер или поисковая система (машина), как указывалось в ГОСТ Р 52872-2012. Однако согласно Федеральному закону № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации» (ред. от 23.11.2024 г.)¹, поисковая система — это информационная система, а веб-страница или Интернет-страница является лишь частью (веб-)сайта — узла сети Интернет. В свою очередь (веб-)сайт — это совокупность программ и иной информации, содержащейся в информационной системе (хранящейся на сервере).

Учитывая положения ГОСТ Р 52872-2019 и ГОСТ Р 57723-2017, сформируем собственное определение ресурса — место для размещения адресуемой поставщиком контента информации и иного содержимого в текстовой, графической и мультимедийной форме, доводимого до пользователя через его органы чувств и доступного с помощью устройства и ИТС. Оно состоит из программно-технических средств, позволяющих осуществлять публикацию информации. Поставщиком контента выступает пользователь, под которым подразумевается как пользователь ИТС, использующий устройство (клиент), так и организация (работник), администрирующая

¹ Об информации, информационных технологиях и о защите информации : Федер. закон № 149-ФЗ от 27 июля 2006 г. // Собрание законодательства Российской Федерации. 2006. № 31 (часть I). Ст. 3448.

Интернет-ресурс — зачастую владелец сайта. При этом для обеспечения передачи информации и ее размещения в информационной системе, постоянно подключенной к сети Интернет, нужна вычислительная мощность, предоставляемая провайдером хостинга.

Преобразование

При рассмотрении такого элемента механизма слеодообразования в сети Интернет, как преобразование, необходимо разграничить контактное взаимодействие и воздействие. Воздействие имеет негативную коннотацию, подразумевает внесение изменений и может относиться к неправомерной деятельности. Взаимодействие же характеризуется нейтральными действиями, которые включают в себя, например, открытие Интернет-страницы или новой вкладки в веб-браузере, сохранение закладок и электронных файлов на рабочий стол.

Виды преобразований можно сгруппировать следующим образом. Во-первых, фундаментальным основанием выступает воля и желание пользователя (отражаемого объекта): *прямое / активное* взаимодействие происходит по воле и желанию субъекта; *пассивное* — помимо воли и желания субъекта. Во-вторых, в качестве как самостоятельной, так и производной классификации выступает группа взаимодействия по направленности: *социальное*, то есть взаимодействие с другими пользователями, и *техническое*, то есть взаимодействие с системой / сетью или воздействие на них [14], а также *смешанное* — при направленности на других пользователей происходит фиксация технологических событий). В-третьих, можно выделить *материальное* преобразование, которое включает в себя физическое воздействие на компьютерную систему или устройство

потерпевшего, а равно и физическое взаимодействие; *виртуальное* преобразование охватывает воздействие на устройство или систему посредством дистанционного доступа и взаимодействия с ними). Иначе их можно обозначить как *непосредственное* (прямое воздействие на компьютерную систему или устройство потерпевшего) и *опосредованное* (воздействие на устройство или систему с использованием командной строки).

Указанные классификации не являются исчерпывающими. В сущности, они подразумевают нацеленность деятельности субъекта и ее порядок: лицо взаимодействует с компьютерной системой и информационной сетью непосредственно, в частности с целью воздействия на них, а равно использует их для взаимодействия с другим лицом. След отражает поведение лица в Интернете, его взаимодействие с другими лицами и технологическое событие (состояние функционирования устройства, системы и сети, а равно продуктов их функционирования).

Прямое или активное взаимодействие

При непосредственном контакте или общении лицо отправляет сообщения с помощью электронного почтового ящика, социальных сетей, мессенджеров, иных приложений или программ, ставит реакции, лайки и оставляет комментарии под публикациями в администрируемом аккаунте, а также в аккаунтах других лиц или групп (сообществ). Последние воспринимаются в качестве так называемых социальных кнопок или знаков социального взаимодействия (англ. «social buttons», «social media buttons») [15, с. 141–142].

Размещение комментариев (текстового, мультимедийного характера) может расцениваться как использова-

ние социальной кнопки и признаваться электронным следом, который был оставлен для воздействия на неопределенный круг лиц². Публикации фото, аудио- и видеозаписи, а равно файлов иных форматов являются также объектом социального взаимодействия³.

Обширная судебная практика различных субъектов РФ указывает на то, что при расследовании не только киберпреступлений, но и традиционных преступлений электронные сообщения (переписка), по которым возможно установить факты, связанные с событием преступления, можно признать в качестве электронного следа, оставленного пользователем в сети Интернет, и в последующем при надлежащем процессуальном оформлении облечь в форму доказательства⁴.

² Обвинительный приговор по ст. 354.1 УК РФ. Брянский областной суд. Приговор № 2-14/2023 от 10 нояб. 2023 г. по делу № 2-14/2023 // Судебные и нормативные акты РФ. URL: <https://sudact.ru/regular/doc/YenUobHR2tVq/> (дата обращения: 04.01.2025).

³ Обвинительный приговор по ст. 207.3 УК РФ. Челябинский областной суд. Апелляционное постановление № 10-5246/2023 от 21 авг. 2023 г. по делу № 1-402/2023 // Судебные и нормативные акты РФ. URL: <https://sudact.ru/regular/doc/Nrgz6Fqcc8f/> (дата обращения: 04.01.2025).

⁴ Кировградский городской суд (Свердловская область). Приговор № 1-128/2023 от 22 сент. 2023 г. по делу № 1-128/2023 // Судебные и нормативные акты РФ. URL: <https://sudact.ru/regular/doc/No1kug5QU3VQ/> (дата обращения: 04.01.2025), Няганский городской суд (Ханты-Мансийский автономный округ-Югра). Приговор № 1-208/2022 1-30/2023 от 28 сент. 2023 г. по делу № 1-208/2022 // Судебные и нормативные акты РФ. URL: <https://sudact.ru/regular/doc/WODkj4LZsSU5/> (дата обращения: 04.01.2025), Первомайский районный суд г. Ижевска (Удмуртская Республика). Приговор № 1-476/2023 от 16 авг. 2023 г. по делу № 1-476/2023 // Судебные и нормативные акты РФ. URL: <https://sudact.ru/regular/doc/1SIRrUV3YW6O/> (дата обращения: 04.01.2025).

Пассивное взаимодействие

В процессе использования ИТС субъектом данные могут формироваться вне зависимости от воли субъекта ввиду его деятельности по типу геолокационных данных и метаданных (с англ. «observed data» — наблюдаемые данные), то есть сведения о создателе, месте, дате и времени создания и модификации, элементах управления доступом, формате, объеме. К ним также можно отнести, например, и ID страницы в социальной сети — часть указателя страницы сайта, который содержит помимо доменного имени числовой или буквенный набор символов и может формироваться как системой в автоматическом режиме, так и самим пользователем.

Данные могут формироваться по воле и желанию субъекта воздействия (отражаемого объекта) и являются предоставляемыми (англ. «volunteered data»). Например, в случае заполнения пользователем профиля в социальной сети или экосистеме криминалистически значимой информацией признаются регистрационные данные. В случае если лицо осуществило вход под конкретной учетной записью, фиксируются данные о заказах и местах: Такси, Еда, Афиша, Лавка, Маркет, Услуги, Доставка, Аренда, Деливери, Отели, Карты — которые могут позволить установить местонахождение лица⁵ и географию перемещений с точным временем и датой,

⁵ Николаевский районный суд (Ульяновская область). Приговор № 1-1-31/2023 от 28 июля 2023 г. по делу № 1-1-31/2023 // Судебные и нормативные акты РФ. URL: <https://sudact.ru/regular/doc/pAtPlcUJY4YK/> (дата обращения: 04.01.2025 г.) и Пензенский областной суд. Приговор № 22-1299/2023 от 22 нояб. 2023 г. по делу № 1-102/2023 // Судебные и нормативные акты РФ. URL: <https://sudact.ru/regular/doc/86aAfsngDPL1/> (дата обращения: 04.01.2025).

используемый транспорт, состав семьи, семейное положение.

Социальное взаимодействие

Социальное взаимодействие имеет место при публичном распространении сведений посредством размещения материала (публикации фото, аудио- и видеозаписи) на личной странице, а равно в группах, сообществах, открытых и закрытых каналах, групповых и личных чатах (беседах), в частности в мессенджерах (системах мгновенного обмена сообщениями) «WhatsApp» и «Telegram» и социальных сетях по типу «ВКонтакте» и «Одноклассники».

С целью незаконного сбора персональных данных и хищения путем обмана денежных средств пользователями могут создаваться сообщества (группы), содержащие такую криминалистически значимую информацию, как контактные данные (абонентские номера, в том числе подменные, электронные почтовые ящики), сфальсифицированные бланки и документы (электронные файлы) государственных органов власти, формы для заполнения персональных данных.

Техническое взаимодействие

Компьютерная система фиксирует активность пользователя, помимо его воли и желания, в частности, например, историю браузера, так называемые «cookies», посещенные Интернет-ресурсы с использованием IP-адресов, в том числе арендованных у проху-сервисов [16, с. 113].

Текстовые файлы «cookies» содержат информацию о сеансе пользователя. Хотя они хранятся на компьютере пользователя, именно сервер сайта (Интернет-ресурса) формирует и использует их. Обычно к ним относят персональные данные, применимые настройки,

данные авторизации и активности, информация об используемом для входа устройстве.

В рамках отдельных экосистем по типу «Яндекс» и «VK» возможно создание веб-сайтов с привязкой к объекту или сообществу. При этом «Яндекс метрика» фиксирует характеристику посетителя веб-сайта и его поведения на страницах с помощью технологии «Крипта»: просмотр, нажатие на кликабельные элементы по типу кнопки, размещенные адреса, номера телефонов, переход по ссылкам, в том числе в мессенджеры, социальные сети, скачивание файлов, поиск по сайту, возврат из платежной системы (проведенные транзакции), осуществление звонков, событий, о совершении которых передается информация с помощью JavaScript по типу заполнение и отправка формы и иные действия.

При совершении преступления с использованием веб-ресурса для незаконного сбора персональных данных и хищения денежных средств, в качестве криминалистически значимой информации в первую очередь выступает доменное имя ресурса, а также сведения, опубликованные на нем (адреса электронных почтовых ящиков, абонентских номеров). Регистратор доменного имени может предоставить регистрационные данные: дату и время регистрации/авторизации, адрес электронного почтового ящика; сведения об оплате, IP-адреса, используемые при подключении к веб-ресурсу. При получении и анализе указанных сведений, возможно установить Интернет-провайдера, его географическое положение, дату и время совершения авторизаций, а также получить информацию о проведении транзакций об оплате услуг аренды доменного имени.

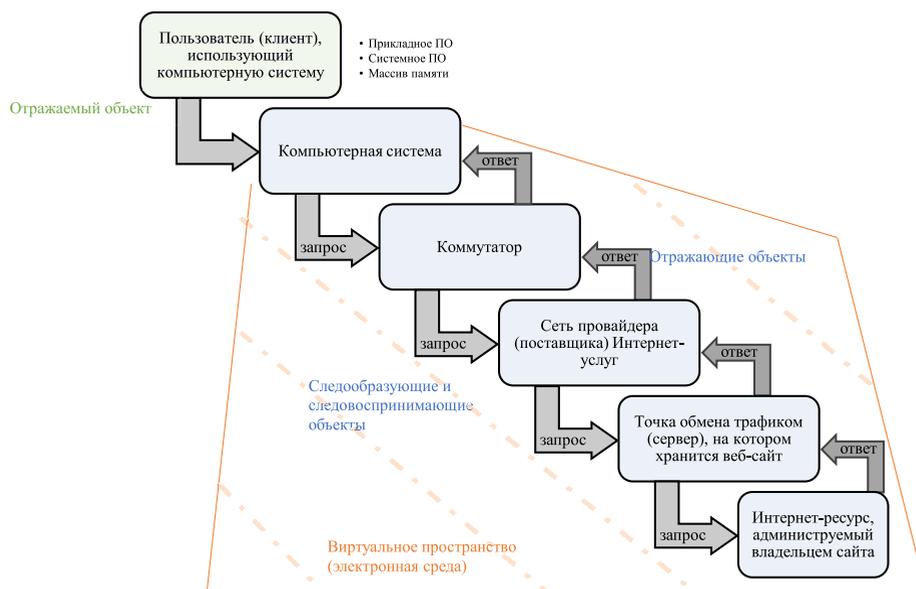


Рис. 2. Механизм отражения в сети Интернет

Смешанное взаимодействие

Возьмем в пример стриминговые сервисы («Twitch.tv» и «GoodGame.ru») и видеохостинговые платформы по типу «Youtube» — платформы, позволяющие пользователям осуществлять вещание (трансляции) с использованием протоколов потоковой передачи данных, то есть в режиме реального времени, а также размещать видеозаписи. При этом оказывать воздействие на пользователей, которые смотрят трансляции, что подразумевает социальное воздействие. В то же самое время в ходе технического взаимодействия, помимо воли и желания пользователя, но в связи с социальным взаимодействием фиксируется количество зрителей, подписчики, содержание чата (публичной переписки) и формируются отчеты о них.

Криминалистически значимой информацией могут выступать содержание трансляций, реакции пользовате-

лей, электронные сообщения в чатах, донаты (направление денежных средств пользователями) и отчеты о проведенных трансляциях, количестве зрителей, участников чата, подписчиков.

Материальное и виртуальное взаимодействие (воздействие)

Представляется возможным говорить о комбинации двух моделей преобразования: материальной и виртуальной [17]. В первом случае лицо непосредственно само воздействует на компьютерную систему или устройство потерпевшего, имея физический доступ к ним, а во втором — посредством удаленного доступа к компьютерному устройству, например, осуществляет запуск вредоносной программы, которое фактически выполняет процесс воздействия. При этом происходит кодовое преобразование информации, отражающей преступную деятельность и существующей объективно в потен-

циальной форме, и обратное преобразование позволяющее понять механизм этой деятельности [18, с. 11]. Это согласуется с позицией Торбина Ю.Г. о корректности использования следов, которые могут быть следствием совершения преступных действий [19, с. 45]. Любые действия с электронными устройствами или компьютерными системами получают свое непосредственное отражение в их памяти [20, с. 266–267].

Выводы

Во-первых, каждый из элементов механизма образования электронных следов (объекты, пространство и преобразование) имеет свои особенности. При использовании ИТС, частным примером которой является Интернет, количество отражающих (следообразующих) и следовоспринимающих объектов, функционирующих в электронной среде, увеличивается в сравнении с механизмом следообразования в компьютерной системе. При этом следовоспринимающим объектом является не только массив памяти используемой компьютерной системы или электронного устройства, но и иных элемен-

тов, необходимых для доступа в ИТС (коммутатор, оборудование сети провайдера Интернет-услуг, точки обмена трафиком или сервис) ввиду принципа действия «рукопожатия» при установлении соединения (см. рис. 1). Схематично механизм отражения следов в сети Интернет можно представить следующим образом (см. рис. 2).

Во-вторых, контактное взаимодействие (воздействие) имеет место в электронной среде и может быть классифицировано на прямое или активное и пассивное, а также социальное, техническое и смешанное; виртуальное и материальное. Фактически любые данные могут считаться электронным следом, если они отображают воздействие в определенном месте электронной среды (виртуального пространства) в определенный момент времени действия субъекта (например, поставщика контента: пользователя или администратора сайта), а равно технологическое событие, имеющие связь с преступлением. При этом криминалистически значимой информацией обычно выступают как предоставляемые пользователем, так и собираемые вопреки его воли.

Список использованной литературы

1. Малыхина Н.И. Криминалистическое учение о механизмах следообразования: современное состояние, направления развития / Н.И. Малыхина. — DOI 10.17150/2411-6122.2022.1.127-134 // Сибирские уголовно-процессуальные и криминалистические чтения. — 2022. — № 1. — С. 127–134.
2. Информационные технологии в уголовно-правовой сфере: монография / О.Ю. Антонов, А.И. Бастрыкин, А.А. Бессонов [и др.]. — Москва : Юнити Дана, 2023. — 279 с.
3. Фойгель Е.И. К вопросу о проблемах практической реализации нового оперативно-розыскного мероприятия («получение компьютерной информации» при раскрытии преступлений в сфере компьютерной информации) / Е.И. Фойгель, А.Г. Проценко. — EDN XRNDJJ // Сибирские уголовно-процессуальные и криминалистические чтения. — 2016. — № 6(14). — С. 73–82.
4. Валькирия Н.И. Общая теория криминалистики в эпоху развития цифровых технологий: некоторые актуальные проблемы / Н.И. Валькирия. — DOI 10.17150/2411-6122.2024.4.15-25. — EDN СТУНJA // Сибирские уголовно-процессуальные и криминалистические чтения. — 2024. — № 4(46). — С. 15–25.
5. Варданян А.В. Криминалистическая характеристика посткриминальной деятельности по делам о преступлениях в сфере информационных технологий / А.В. Варданян. —

- EDN PNHKBW // Сибирские уголовно-процессуальные и криминалистические чтения. — 2021. — № 2(32). — С. 44–51.
6. Тюхтин В.С. О сущности отражения / В.С. Тюхтин // Вопросы философии. — 1962. — № 5. — С. 31–43.
7. Шрейдер Ю.А. Об одной модели семантической теории информации / Ю.А. Шрейдер // Проблемы кибернетики : сб. статей / под ред. А.А. Ляпунова. — Москва, 1965. — Вып. 13. — С. 233–240.
8. Агибалов В.Ю. Виртуальные следы в криминалистике и уголовном процессе : монография / В.Ю. Агибалов. — Москва : Юрлитинформ, 2012. — 152 с. — EDN SYPZGV.
9. Себякин А.Г. Механизм следообразования в компьютерных системах с точки зрения теории отражения / А.Г. Себякин. — EDN JSESDH // Сибирские уголовно-процессуальные и криминалистические чтения. — 2021. — № 2 (32). — С. 89–99.
10. Переверзева Е.С. Механизм следообразования виртуальных следов / Е.С. Переверзева, А.В. Комов. — DOI 10.35750/2071-8284-2022-1-128-133. — EDN FKISRF // Вестник Санкт-Петербургского университета МВД России. — 2022. — № 1 (93). — С. 128–133.
11. Мещеряков В.А. Теоретические основы механизма следообразования в цифровой криминалистике : монография / В.А. Мещеряков. — Москва : Проспект, 2022. — 176 с.
12. Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации : автореф. дис. ... док. юрид. наук : 12.00.09 / В.А. Мещеряков. — Воронеж, 2001. — 39 с.
13. Телешина Н.Н. Виртуальное пространство как объект контрольной деятельности государства : автореф. дис. ... канд. юрид. наук : 12.00.01 / Н.Н. Телешина. — Муром, 2011. — 26 с.
14. Hepp A. Digital Traces in Context / A. Hepp, A. Breiter, T.N. Friemel // International Journal of Communication. — 2018. — № 12. — P. 439–449.
15. Casagrande G. Visible and Invisible Traces: Managing the Self on Social Media Platforms / G. Casagrande // What People Leave Behind. Marks, Traces, Footprints and Their Relevance to Knowledge Society / ed. F. Comunello, F. Martire, L. Sabetta. — Berlin : Springer, 2022. — P. 141–156.
16. Лысенко Е.С. Отдельные вопросы деанонимизации лиц, совершающих преступления в сети интернет / Е.С. Лысенко, Е.Ю. Семенов. — EDN EIKAPF // Проблемы противодействия киберпреступности : материалы Междунар. науч.-практ. конф., Москва, 28 апр. 2023 г. — Москва, 2023. — С. 108–114.
17. Мочагин П.В. Виртуально-информационный и невербальный процесс отражения следообразований как новое направление в криминалистике и судебной экспертизе / П.В. Мочагин. — EDN OKWNEH // Вестник Удмуртского университета. Серия «Экономика и право». — 2013. — № 2. — С. 148–154.
18. Каминский М.К. Что есть, что может быть и чего быть не может для системы «криминалистики» / М.К. Каминский. — EDN YXLYQX // Вестник криминалистики. — 2002. — № 1 (3). — С. 8–14.
19. Торбин Ю.Г. Следы и особые приметы на живых лицах (уголовно-процессуальные и криминалистические аспекты обнаружения и использования) / Ю.Г. Торбин. — Москва : Юрлитинформ, 2006. — 432 с.
20. Долгинов С.Д. Следы электронных устройств в криминалистике / С.Д. Долгинов. — EDN URVGXH // Шестой пермский конгресс ученых-юристов: Российская национальная правовая система: современное состояние, тенденции и перспективы развития : материалы Междунар. науч.-практ. конф., Пермь, 16–17 окт. 2015 г. / ред. О.А. Кузнецова. — Пермь, 2015. — С. 383–389.

References

1. Malykhina N.I. Forensics Doctrine of the Mechanisms of Trace Formation: Current State, Development Directions. *Sibirskie ugolovno-protsessual'nye i kriminalisticheskie chteniya = Siberian Criminal Procedure and Criminalistic Readings*, 2022, no. 1, pp. 127–134. (In Russian). DOI: 10.17150/2411-6122.2022.1.127-134.
2. Antonov O.Yu., Bastrykin A.I., Bessonov A.A., Ermolovich Ya.N., Malikov S.V. *Information Technologies in Criminal Law Sphere*. Moscow, Yuniti Dana Publ., 2023. 279 p.

3. About the Problems of the Practical Implementation of the New Operational Investigative Activity "Getting Computer-based Data" in Solving Crimes in the Sphere of Computer Information. *Sibirskie ugovolno-protsessual'nye i kriminalisticheskie chteniya = Siberian Criminal Procedure and Criminalistic Readings*, 2016, no. 6, pp. 73–82. (In Russian). EDN: XRNDJJ.

4. Valkiriya N.I. The General Theory of Criminalistics in the Era of Digital Technology's Development: Some Topical Problems. *Sibirskie ugovolno-protsessual'nye i kriminalisticheskie chteniya = Siberian Criminal Procedure and Criminalistic Readings*, 2024, no. 4, pp. 15–25. (In Russian). EDN: CTYHJA. DOI: 10.17150/2411-6122.2024.4.15-25.

5. Vardanyan A.V. Forensic Characteristics of Post-criminal Activity in Cases of Information Technology Crimes. *Sibirskie ugovolno-protsessual'nye i kriminalisticheskie chteniya = Siberian Criminal Procedure and Criminalistic Readings*, 2021, no. 2, pp. 44–51. (In Russian). EDN: PHKHWB.

6. Tyukhtin V.S. On the Essence of Reflection. *Voprosy filosofii = Issues of Philosophy*, 1962, no. 5, pp. 31–43. (In Russian).

7. Shreider Yu.A. On One Model of the Semantic Theory of Information. In Lyapunov A.A. (ed.). *Problems of Cybernetics. Collected Papers*. Moscow, 1965, iss. 13, pp. 233–240. (In Russian).

8. Agibalov V.Yu. *Virtual Traces in Criminalistics and Criminal Process*. Moscow, Yurлитinform Publ., 2012. 152 p. EDN: SYPZGV.

9. Sebyakin A.G. The Mechanism of Trace Formation in Computer Systems from the Standpoint of the Reflection Theory. *Sibirskie ugovolno-protsessual'nye i kriminalisticheskie chteniya = Siberian Criminal Procedure and Criminalistic Readings*, 2021, no. 2, pp. 89–99. (In Russian). EDN: JSESDH.

10. Pereverzeva E.S., Komov A.V. The Mechanism for Digital Footprints Formation. *Vestnik Sankt-Peterburgskogo universiteta MVD Rossii = Saint Petersburg University of Ministry of Internal Affairs of Russia Bulletin*, 2022, no. 1, pp. 128–133. (In Russian). EDN: FKISRF. DOI: 10.35750/2071-8284-2022-1-128-133.

11. Meshcheryakov V.A. *Theoretical Basis of the Mechanism of Trace Formation in Digital Criminalistics*. Moscow, Prospekt Publ., 2022. 176 p.

12. Meshcheryakov V.A. *Basics of the Methodology of Crime Investigation in the Sphere of Computer Information. Doct. Diss. Thesis*. Voronezh, 2001. 39 p.

13. Telezhina N.N. *Virtual Space as an Object of State Control. Cand. Diss. Thesis*. Murom, 2011. 26 p.

14. Hepp A., Breiter A., Friemel T.N. Digital Traces in Context. *International Journal of Communication*, 2018, no. 12, pp. 439–449.

15. Casagrande G. Visible and Invisible Traces: Managing the Self on Social Media Platforms. In Comunello F., Martire F., Sabetta L. (eds.) *What People Leave Behind. Marks, Traces, Footprints and Their Relevance to Knowledge Society*. Berlin, Springer, 2022, pp. 141–156.

16. Lysenko E.S., Semenov E.Yu. *Specific Issues of De-anonymizing Persons Who Commit Crimes on the Internet. Problems of Counteracting Cybercrimes. Materials of International Scientific Conference, Moscow, April 28, 2023*. Moscow, 2023, pp. 108–114. (In Russian). EDN: EIKAPF.

17. Mochagin P.V. Virtual-information and Nonverbal Reflection Process of Trace Formation as a New Direction in Forensic Science and Criminalistics. *Vestnik Udmurtskogo universiteta. Seriya Ekonomika i pravo = Bulletin of Udmurt University. Series Economics and Law*, 2013, no. 2, pp. 148–154. (In Russian). EDN: OKWNEH.

18. Kaminskiĭ M.K. What is, What Could Be and What Cannot Be for the System of "Criminalistics". *Vestnik kriminalistiki = Bulletin of Criminalistics*, 2002, no. 1, pp. 8–14. (In Russian). EDN: YXLYQX.

19. Torbin Yu.G. *Traces and Distinguishing Features of Living Persons (Criminal Procedure and Criminalistic Aspects of Detection and Use)*. Moscow, Yurлитinform Publ., 2006. 432 p.

20. Dolginov S.D. Traces of Electronic Devices in Criminalistics. In Kuznetsova O.A. (ed.). *The Sixth Perm Congress of Legal Scholars: Russian National Legal System: Modern Condition, Trends and Development Prospects. Materials of International Scientific Conference, Perm', October 16–17, 2015*. Perm', 2015, pp. 383–389. (In Russian). EDN: URVGXH.

Информация об авторе

Поляков Игорь Сергеевич — аспирант, Академия Следственного комитета Российской Федерации имени А.Я. Сухарева; следователь по особо важным делам, отдел по расследованию киберпреступлений и преступлений в сфере высоких технологий, Управление по расследованию отдельных видов преступлений, Главное следственное управление Следственного комитета Российской Федерации, майор юстиции, г. Москва, Российская Федерация, SPIN-код: 5720-8583, AuthorID РИНЦ: 1252780.

Author Information

Polyakov, Igor S. — Ph.D. Student, Sukharev Moscow Academy of the Investigative Committee of the Russian Federation; Special Investigator, Cyber and High-Tech Crimes Investigation Unit, Selected Crimes Investigation Department, Main Investigative Directorate of the Investigative Committee of the Russian Federation, Major of Justice. Moscow, the Russian Federation, SPIN-Code: 5720-8583, AuthorID RSCI: 1252780.

Поступила в редакцию / Received 25.03.2025

Одобрена после рецензирования / Approved after reviewing 31.03.2025

Принята к публикации / Accepted 21.05.2025

Дата онлайн-размещения / Available online 26.06.2025