УДК 004.06; УДК 343.98.06

МЕТОДЫ ВЫЯВЛЕНИЯ ЦИФРОВОГО СЛЕДА ПРИ РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ

Ф. П. ЦЫБУЛЬСКИЙ
(Представлено: канд. техн. наук, доц. И. Б. БУРАЧЁНОК)

Осуществлен анализ основных классификаций цифрового следа. Рассмотрены методы обнаружения цифрового следа, рекомендуемые для использования правоохранительными органами в расследовании киберпреступлений и предотвращении противозаконной деятельности с использованием цифровых устройств.

Ключевые слова: *информационная безопасность, кибербезопасность, киберпреступления, электронно-цифровой след, цифровая тень, цифровой отпечаток, виртуальный след, цифровой след, трасология, цифровая ДНК.*

Введение. Быстрый рост уровня технологий, внедрение цифровых устройств во все сферы жизнедеятельности человека, переход от индустриальной и постиндустриальной экономики к так называемой цифровой экономике или экономике, базирующейся на сетевом использовании информационно-коммуникационных технологий [1] открыла новые возможности для преступной деятельности в области информационных технологий. Согласно статистике, только по Витебской области за январь-июнь 2024 года зарегистрировано 985 киберпреступлений. Совершение противоправных деяний в области с использованием сети интернет, средств мобильной связи и компьютерной техники с аналогичным периодом прошлого года выросло на 15%. В общей сложности ущерб жителям области от таких преступлений за указанный период составил 1,8 миллиона белорусских рублей [2]. Для сотрудников правоохранительных органов расследования противозаконной деятельности с использованием цифровых устройств является трудоёмкой работой. Специфика деяния и уникальность каждого процесса установления источников доказательной информации не позволяет создать единую практику ведения следствия. Одним из основополагающих инструментов, находящихся на службе у современного специалиста, является изучение цифрового следа интересующего человека. Таким образом, анализ сетевых ресурсов с использованием методов выявления цифрового следа и разработка практических, научно обоснованных рекомендаций и инновационных методик для использования правоохранительными органами в расследовании и предотвращении противозаконной деятельности с использованием цифровых устройств являются **актуальными**.

Основной целью представленной работы является изучение понятия цифрового следа, его классификаций с учётом мнений специалистов в области кибербезопасности и юриспруденции, а также исследование практической применимости методов выявления цифрового следа при расследовании киберпреступлений.

Первоначально рассмотрим само понятие цифрового следа. Электронно-цифровой след, цифровая тень, цифровой отпечаток, виртуальный след, электронный след или цифровой след (англ. digital footprint) – совокупность отслеживаемых цифровых данных, генерируемых в результате взаимодействия человека с техническими устройствами и другими элементами информационной инфраструктуры [3]. Под информационной инфраструктурой понимают комплекс технических средств, программного обеспечения и коммуникационных сетей, предназначенных для получения, хранения и обработки информации [4]. Данными, интерпретируемыми как цифровой след, могут являться любые отслеживаемые цифровые сведения о человеке, такие как, например, статистика изменения геолокации, количество звонков за день или хранимые сведения об учётной записи и пр.

Следует отметить, что согласно проведенного анализа известных источников из описания понятия цифрового следа, возникает проблема единой классификации из-за большого разброса по содержанию и типу объёма данных для представления. В результате проведенных исследований известных подходов по дифференциации цифрового следа на виды, можно указать известные пять: классификация А.Г. Себякина, классификация А.А. Жижелевой, классификация Е.М. Черешнева, классификация А.Н. Колычевой и классификация с точки зрения трасологии.

Исследователь А.Г. Себякин [5] предлагает спецификацию цифровых следов на основе фактора опосредованности воздействия пользователя на элементы компьютерной системы, разделяя его на две группы: опосредованную и непосредственную.

К *непосредственной группе следов* А.Г. Себякин относит компьютерные данные, образованные или скопированные в результате непосредственного воздействия пользователя (причины) на компьютерную систему. К такому виду причислены данные, генерируемые пользователем путем устройств ввода: созданные файлы, почтовые отправления, фотографии, фонограммы, история поисковых запросов

интернет-браузера и прочая информация, создаваемая при взаимодействии пользователя с программным обеспечением.

К *опосредованной группе* стоит относить следы, которые создаются без наличия прямой связи с причиной (целью) воздействия субъекта (пользователя) на систему, но инициированные этим воздействием, обусловленные особенностями программного обеспечения. Опосредованными следами могут служить таблицы размещения файлов, метаданные пользовательских файлов, записи служебных баз данных и записи реестра.

Опосредованные и непосредственные цифровые следы бывают локальными, то есть храниться на носителе пользователя, так и удалёнными, хранящимися на сетевых каналах, доступ к которым осуществляется с помощью средств коммуникации.

Типичным примером непосредственной группы следа является изображение, созданное пользователем. Изображение генерируется непосредственно в результате воздействия пользователя как причины. Современные фоторедакторы совместно с изображением сохраняют различные метаданные: место съемки, дату съемки, значение выдержки и т.п. Примеры непосредственных следов в виде метаданных изображения показаны на рисунке 1. Эти данные являются опосредованными, так как пользователь только косвенно инициирует создание таковых. Получить основные сведения о файле можно стандартными средствами просмотра свойств Windows.

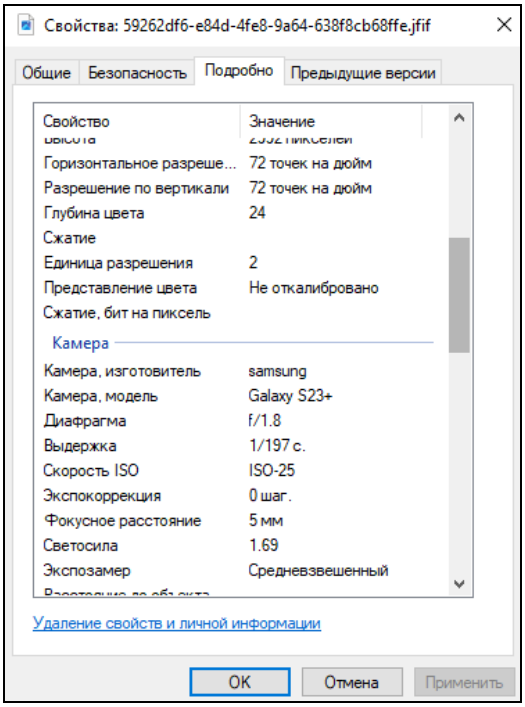

Рисунок 1. – Пример непосредственных следов в виде метаданных фотографии

Классификация А.А. Жижелевой [6], представляет собой разбиение цифровых следов на активные и пассивные.

Активными видами следов являются все цифровые данные, сгенерированные в результате полной сознательной деятельности пользователя в компьютерной системе. К ним можно отнести создаваемые напрямую пользователем с помощью устройств ввода файлы, текстовые сообщения, фотографии, видео и другие виды цифровой информации.

К пассивным видам исследователь причисляет совокупность данных, созданных или измененных непреднамеренно для пользователя самой компьютерной системой. Процессы, совершаемые без прямого участия пользователя: сохраняемые журналы событий, история посещённых сайтов, cookie-файлы и т.п.

Представителями пассивного вида являются журналы событий Windows, которые хранят записи о событиях в Windows. Пример, журнала событий Windows представлен на рисунке 2. Dpkg.log прекрасно подойдет для примера пассивного вида данных для систем, подобных Linux. Dpkg.log содержит записи журнала об установленных пакетах (см. рисунок 3).

Эксперт в области кибербезопасности Е.М. Черешнев придерживается схожим с А.А. Жижелевой подходом. Однако, помимо выделения активных и пассивных видов данных, Е.М. Черешнев разбивает

их на 15 типов, отражающих содержание и то, насколько сознательно для пользователя система генерирует информацию. В книге [7] Е.М. Черешнева выделяются следующие типы цифрового следа:

– *автоматически генерируемые данные о местонахождении* – информация о географическом местонахождении устройства, с которого пользователь или система цифрового устройства осуществляет вход в сеть;

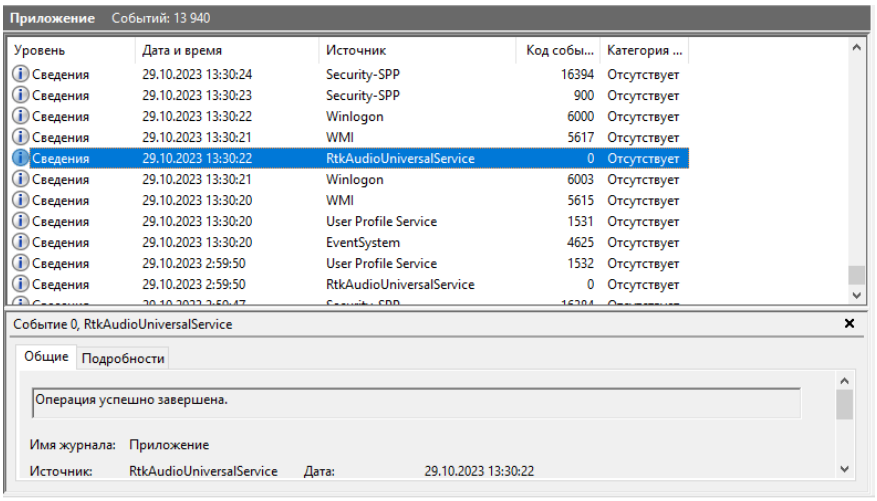

Рисунок 2. – Журнал событий Windows

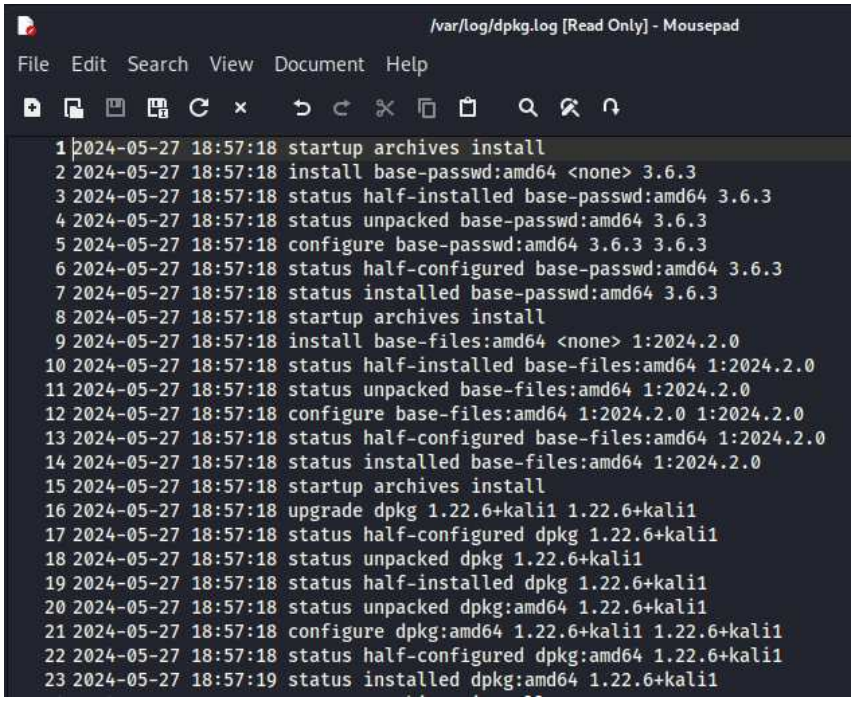

Рисунок 3. – Записи журнала Dpkg.log

– *сервисные данные* – данные, которые необходимы конкретному сервису для осуществления услуг;

– *добровольно публичные контролируемые данные* – данные, которые пользователь оставляет добровольно и осознанно. При этом пользователь имеет над этими данными полный контроль как производитель;

– *добровольно публичные, но неконтролируемые данные* – данные, которые пользователь оставляет добровольно и осознанно. При этом пользователь не имеет контроля над этими данными;

– *биометрические данные* – данные, генерируемые цифровыми техническими устройствами на основе биометрических показателей активности и уникальных идентификаторов пользователя;

– *атрибутированные данные* – данные, связанные с конкретным пользователем, однако, опубликованные не им, а его окружением;

– *поведенческие данные* – данные, генерируемые программным обеспечением, содержащие аспекты поведения пользователя, такие как скорость печати, время и место курсора на экране в конкретный момент;

– *психологические данные* – данные, генерируемые программным обеспечением в результате психологического профилирования пользователя на базе первичных данных;

– *медицинские данные* – отслеживаемые показатели конкретного человека, снятые с помощью цифровых медицинских устройств;

– *расшифрованная ДНК* – данные, полученные и опубликованные в информационной инфраструктуре, содержащие анализ детально расшифрованной ДНК человека;

– *секретно собираемые данные* – данные, сохраняемые или генерируемые программным обеспечением без прямого участия и согласия пользователя, которые пользователь оставляет неосознанно;

– *данные, основанные на выводах* – результаты математического анализа и интерпретации первичных данных с целью извлечения значимых закономерностей;

– *данные рода* – данные, генерируемые программным обеспечением в результате анализа информации, полученной по обратной связи с цифровыми следами членов семьи конкретного пользователя;

– *служебные данные* – данные пользователя, генерируемые программным обеспечением на базе файлов, записей или документации, связанных с профессиональной и служебной деятельностью пользователя;

– *полученные или доступные знания* – данные, генерируемые программным обеспечением в результате анализа первичных данных, содержащие информацию о знаниях, которые пользователь получил или в теории мог бы.

Более подробная классификация данных позволяет эффективно выделять полезные электронно-цифровые следы, делая их более заметными. Е.М. Черешнев утверждает, что все эти типы данных так или иначе собираются программным обеспечением в режиме реального времени. Полный цифровой след, состоящий из вышеперечисленных типов данных и выводы, которые можно на них построить, исследователь называет цифровой ДНК, или digital DNA (dDNA).

dDNA – структурированная база данных, содержащая записи всей информации об объекте за конкретный промежуток времени, состоящий из 3 частей: фактическая (past & present), легенда описания и разметка базы ячеек (legend), и прогнозы вероятных действий в будущем (future) [7]. Имея доступ к цифровой ДНК, можно узнать увлечения, повседневные взаимодействия с цифровой инфраструктурой, а также определить факт связи цифровой улики с пользователем.

Стоит обратить внимание на классификацию исследователя А.Н. Колычевой. Она, в свою очередь, предлагает спецификацию цифровых следов как возникающих данных в процессе подготовки, совершения и сокрытия преступного деяния, хранящиеся и образующихся в компьютерных системах и интернет-пространстве и дифференцирует явление цифровой тени по виду информации на 7 следующих групп [10]

– файлы системно и прикладного программного обеспечения;

– файлы конфигурации программных приложений и операционных систем;

– файлы-журналы программного обеспечения и технических средств;

– файлы - источники информации, образующиеся в ходе деятельности пользователя, в том числе их резервные копии и удаленные файлы, подлежащие восстановлению;

– файлы, обеспечивающие аутентификацию и конфиденциальность пользователей;

– информация, находящаяся в оперативной памяти или файле подкачки устройства;

– информация, полученная с помощью соответствующих радиоэлектронных или специальных технических средств.

По месту нахождения цифровых следов А.Н. Колычева выделяет 3 группы:

– находящиеся на электронных устройствах потерпевшего;

– находящиеся на электронных устройствах лиц, подготавливающих, совершающих либо совершивших преступление;

– находящиеся на материальных носителях, размещенных в технических устройствах операторов электросвязи.

По источнику информации исследователь подчеркивает еще 3 группы данных:

– следы на материальных носителях;

– следы, находящиеся в оперативной памяти электронных устройств получения, фиксации, обработки и передачи цифровых данных;

– следы в сетевых каналах передачи данных между устройствами.

С точки зрения общей трасологии, электронно-цифровой след единогласно нельзя причислить ни к материальным, ни к идеальным видам следов. С точки зрения В.А. Мещарикова [9] цифровая тень является материальным видом следов, так как информация существует реально на цифровом носителе, а их обнаружение возможно только с применением программного-технического устройств. Другие специалисты (В.Б. Вехов [11], А.Н. Колычева [10]) уточняют это мнение, считая такой вид данных невидимым материальным следом, который человек может воспринять органами чувств в результате преобразования цифровыми устройствами и устройствами вывода компьютерной информации. С другой стороны, материальным следов считается след, который имеет относимость рассматриваемого объекта к материальному миру, а цифровая тень к материальному миру напрямую не относится, человек не способен воспринять информацию непосредственно. Также есть мнения о том, что цифровой след находится между материальными и идеальными следами, при этом заимствуя свойства двух видов.

Анализ и поиск цифровых следов активно используется в криминалистических процессах в комплексе судебной компьютерно-технической экспертизы (далее КТЭ) [12].

Методы обнаружения цифрового следа включают в себя:

– *анализ слепков памяти* (memory dumping) [13] – воспроизведение и анализ состояния слепка оперативной памяти, снятого ранее.

– *анализ общедоступных интернет-ресурсов* [14] – анализ социальной среды интернет-пространства в качестве ориентирующей информации.

– *анализ файловой системы* [15] – анализ файловой системы на предмет наличия следов преступной деятельности.

Также используются методы и алгоритмы информационной интерпретации.

Явление цифрового следа нашло свое применение в OSINT (англ. Open Source Intelligence), которая базируется на анализе открытых источников информации. Более точное определение OSINT сформулировано М.О. Янгаевой и Н.О. Павленко [8]. Также создаются аппаратно-программные комплексы, способные отслеживать открытые источники информации: АПК «Демон Лапласа» [16], Find Face [17] и другие. Эти программные комплексы способны эффективно выявлять, производить мониторинг и анализировать информацию, полученную из мессенджеров, камер наблюдений и прочих цифровых ресурсов. Такого рода меры позволяют прогнозировать противоправные действия и оказывать поддержку в аргументации судебного процесса по деяниям, связанным не только с сферой компьютерных сетей, но и других разделах криминалистики.

Вывод: В связи с быстрым ростом компьютеризации и сравнительно недавним возникновением понятия цифрового следа, заметно отставание правоохранительных органов в области цифровых технологий. Однако любая активность в цифровом пространстве оставляет следы. Эти следы можно найти, интерпретировать и представить суду в определенной процессуальной форме. И несмотря на отсутствие общего подхода к расследованию и недостаточно конкретной спецификацией цифрового следа как технического и юридического объекта, можно сказать, что цифровая криминалистика на сегодня уже активно формируется в современных реалиях киберпространства. Таким образом, научное изучение явления цифрового следа остается актуальным в обеспечении безопасности в сфере информационных технологий. Эффективное решение проблемы сбора данных и их анализа позволят создать более гибкие методики ведения криминалистического следствия и защиты информационных ресурсов.

ЛИТЕРАТУРА

1. Головенчик, Г.Г. Цифровая экономика [Электронный ресурс] : учеб.-метод. комплекс / Г.Г. Головенчик. – Минск : БГУ, 2020. – 1 электрон. опт. диск (CD-ROM). ISBN 978-985-566-847-4.
2. Александр Гарус: Схемы кибермошенников и как не попасться на их уловки. Правоохранители Витебской области дали советы [Электронный ресурс]. – Режим доступа: https://www.belta.by/comments/view/shemy-kibermloshennikov-i-kak-ne-popastsja-na-ih-ulovki-pravoohraniteli-vitebskoj-oblasti-dali-sovety-9299. – Дата доступа: 14.08.2024.
3. Нестеров, С.А. Понятие цифрового следа и анализ цифрового следа в образовании / С.А. Нестеров, Е.М. Смолина // SAEC. 2023. №3. [Электронный ресурс]. – Режим доступа: URL: https://cyberleninka.ru/article/n/ponyatie-tsifrovogo-sleda-i-analiz-tsifrovogo-sleda-v-obrazovanii. – Дата доступа: 18.08.2024.
4. Перечень терминов и их определений (приложение 2), утвержденный Указом Президента Республики Беларусь от 14 февраля 2023 г. № 40 «О кибербезопасности».
5. Себякин, А. Г. Тактика использования знаний в области компьютерной техники в целях получения криминалистически значимой информации: дис. канд. юрид. наук : 12.00.12. / А. Г. Себякин. – М., 2021. – 271 с.

6. Жижилева, А.А. О некоторых теоретических аспектах использования в криминалистике понятий цифровые, электронные, виртуальные следы // Вопросы российской юстиции. 2019. №3. – Режим доступа: URL: https://cyberleninka.ru/article/n/o-nekotoryh-teoreticheskih-aspektah-ispolzovaniya-v-kriminalistike-ponyatiy-tsifrovye-elektronnye-virtualnye-sledy. – Дата доступа: 18.08.2024.
7. Черешнев, Е.М. Форма жизни №4: Как остаться человеком в эпоху расцвета искусственного интеллекта. // Е.М. Черешнев. – М.: ООО «Альпина Паблишер», 2022. – 420 с.
8. Янгаева, М.О. OSINT. Получение криминалистически значимой информации из сети Интернет. / М.О. Янгаева, Н.О. Павленко // Алтайский юридический вестник. 2022. № 2 (38). С. 131-135.
9. Мещеряков, В.А. Основы методики расследования преступлений в сфере компьютерной информации: дис. д-ра юрид. наук. / В.А. Мещеряков. – Воронеж, 2001. – 387 с.
10. Колычева, А.Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет: автореф. канд. юрид. наук: 12.00.12 / А.Н. Колычева. – Москва, 2019. – С. 25.
11. Вехов, В.Б. Электронные следы в системе криминалистики. / В.Б. Вехов, Б.П. Смагоринский, С.А. Ковалев. // Судебная экспертиза. – №2. С. 17.
12. Проведение компьютерно-технической экспертизы в Минске (досудебная экспертиза) [Электронный ресурс]. – Режим доступа: https://www.fedkon.by/services/dosudebnaya-ekspertiza/kompyuterno-tekhnicheskaya-ekspertiza/. – Дата доступа: 14.08.2024.
13. Островская, С. Криминалистика оперативной памяти на практике. [Электронный ресурс] : / С. Островская, О. Скулкин. – М. : ДМК-Пресс, 2022. – 256 с.
14. Болвачев, М.А. Социальная сеть как объект криминалистического исследования // Известия ТулГУ. Экономические и юридические науки. / М.А. Болвачев, 2020. №4. – Режим доступа: URL: https://cyberleninka.ru/article/n/sotsialnaya-set-kak-obekt-kriminalisticheskogo-issledovaniya. – Дата доступа: 20.08.2024.
15. Ливак, Е.Н. Особенности криминалистического анализа файловой системы NTFS. [Электронный ресурс]. / Е.Н. Ливак, О.Р. Мысливец. – Режим доступа: https://elib.grsu.by/katalog/553951pdf.pdf?d=true. – Дата доступа: 20.08.24
16. Программа «Демон Лапласа» [Электронный ресурс]. – Режим доступа: https://protestonline.ru. – Дата доступа: 14.08.2024.
17. Распознавание лиц и силуэтов людей, автомобилей и номерных знаков. Платформа мультиобъектной видеоаналитики. [Электронный ресурс]. – Режим доступа: https://ntechlab.ru. – Дата доступа: 14.08.2024.