Научная статья
УДК 343.98
DOI: 10.55001/2587-9820.2024.40.33.008

КЛАССИФИКАЦИЯ ЭЛЕКТРОННО-ЦИФРОВЫХ СЛЕДОВ, ВОЗНИКАЮЩИХ ПРИ СОВЕРШЕНИИ ПРЕСТУПЛЕНИЙ ЭКСТРЕМИСТСКОЙ И ТЕРРОРИСТИЧЕСКОЙ НАПРАВЛЕННОСТИ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Роман Александрович Дерюгин
Уральский юридический институт МВД России, г. Екатеринбург, Российская Федерация, deryugin.r.a@mail.ru

Аннотация. В статье проанализированы самые распространенные виды электронно-цифровых следов, которые могут быть оставлены при совершении преступлений экстремистской и террористической направленности с использованием информационно-телекоммуникационных технологий. На основе выработанных в криминалистической науке критериев предложена авторская классификация электронно-цифровых следов, возникающих в процессе совершения указанных преступлений. Приведены примеры специализированных программных продуктов и аппаратно-программных комплексов, используемых в рамках работы с электронно-цифровыми следами при расследовании преступлений экстремистской и террористической направленности.

Ключевые слова: информация, экстремизм, терроризм, электронно-цифровые следы, классификация, мобильный криминалист

Для цитирования: Дерюгин, Р. А. Классификация электронно-цифровых следов, возникающих при совершении преступлений экстремистской и террористической направленности с использованием информационно-телекоммуникационных технологий // Криминалистика: вчера, сегодня, завтра : сб. науч. тр. Иркутск : Восточно-Сибирский институт МВД России. 2024. Т. 32. № 4. С. 78–85. DOI: 10.55001/2587-9820.2024.40.33.008

CLASSIFICATION OF ELECTRONIC DIGITAL TRACES ARISING WHEN COMMITTING EXTREMIST AND TERRORIST CRIMES USING INFORMATION AND TELECOMMUNICATION TECHNOLOGIES

Roman A. Deryugin
Ural Law Institute of the MIA of Russia, Yekaterinburg, Russian Federation, deryugin.r.a@mail.ru

Abstract. The article analyzes the most common types of electronic and digital traces that can be left when committing crimes of extremist and terrorist orientation using information and telecommunication technologies. Based on the criteria developed in forensic science for classification, the author's classification of electronic and digital traces arising in the course of committing these crimes is proposed. Examples of specialized software products and hardware and software complexes used in the framework of working with electronic digital traces in the investigation of crimes of extremist and terrorist orientation are given.

Keywords: information, extremism, terrorism, electronic digital traces, classification, mobile criminologist

For citation: Deryugin, R. A. Klassifikaciya elektronno-cifrovyh sledov, voznikayushchih pri sovershenii prestuplenij ekstremistskoj i terroristicheskoj napravlennosti s ispol'zovaniem informacionno-telekommunikacionnyh tekhnologij [Classification of electronic and digital traces arising from the commission of crimes of extremist and terrorist orientation using information and telecommunication technologies]. Kriminalistika: vchera, segodnya, zavtra = Forensics: yesterday, today, tomorrow. 2024, vol. 32. no. 4, pp. 78–85 (in Russ.). DOI: 10.55001/2587-9820.2024.40.33.008

Введение

Для современного общества характерно качественно новое состояние, в котором все больше возрастает влияние информационно-телекоммуникационных технологий на все виды деятельности человека. Интернет, 3D-технологии, виртуальная реальность, искусственный интеллект стали неотъемлемой частью нашей жизни и подтверждают статус информационного общества.

К сожалению, нельзя не отметить, что интернет-пространство и информационные технологии активно используют различные экстремистские и террористические организации, которые вербуют молодежь, пропагандируют радикальные настроения и распространяют идеологии экстремистской направленности. Данный факт находит отражение в Стратегии противодействия экстремизму в России, где подчеркивается, что информационно-телекоммуникационные сети, включая сеть «Интернет», стали основным средством связи для экстремистских организаций, которое используется ими для привлечения в свои ряды новых членов, организации и координации совершения преступлений экстремистской направленности[1].

Согласно статистическим показателям глобального индекса терроризма, в 2024 году число смертей в результате терактов увеличилось на 22 % и составило 8 352 человека, что является самым высоким показателем с 2017 года. При этом количество террористических актов сократилось на 22 % (до 3 350), а количество стран, сообщивших об инцидентах, сократилось до 50. В 2023 году и в первую половину 2024 года на США пришлось 76 % смертей, связанных с терроризмом, несмотря на 15-летний спад числа инцидентов. Эпицентр терроризма переместился с Ближнего Востока в регион Центрального Сахеля в Африке к югу от Сахары, на который сейчас приходится более половины всех смертей от терроризма. Более 90 % терактов и 98 % смертей в результате терактов в 2023 году и в первую половину 2024 года произошли в зонах конфликтов, что подчеркивает тесную связь вооруженных конфликтов и и терроризма[2].

По данным МВД России, в январе – сентябре 2024 года зарегистрировано 2,6 тыс. преступлений террористического характера (+49,0 %) и 1,4 тыс. преступлений экстремистской направленности (+34,7 %). Если обратиться к более ранним показателям, то в январе 2023 года МВД России зарегистрировало 134 преступления экстремистской направленности, что на 157,7 % больше, чем за аналогичный период 2022 года. К тому же по сравнению с январем

[1] Стратегия противодействия экстремизму в Российской Федерации до 2025 года : утв. Указом Президента Российской Федерации от 29 мая 2020 г. № 344 // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_353838/ (дата обращения: 11.12.2024). Режим доступа: для зарегистрир. пользователей.

[2] Глобальный индекс терроризма 2024 // Международные частные инвестиции : сетевой журнал. URL: https://internationalinvestment.biz/analytics/4701-globalnyj-indeks-terrorizma-2024.html (дата обращения: 11.12.2024).

2019 года зафиксировано 35 экстремистских преступлений, а в 2023 г. их число выросло почти в четыре раза. При этом в настоящее время уточняется, что большая часть таких преступлений совершается с использованием информационно-телекоммуникационных технологий[3].

Очевидно, что при таком росте преступлений данного вида требуется выработка современных действенных мер по противодействию преступности экстремистской и террористической направленности с учетом специфики новых способов совершения преступлений и механизма следообразования, где ключевыми стали электронно-цифровые следы.

Основная часть

Одной из особенностей расследования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, является работа с электронно-цифровыми следами, образующимися в рамках преступной деятельности. Не стала исключением и деятельность экстремистов и террористов, преимущественно совершающих определенные действия в сети Интернет, посредством мобильной связи, мобильных приложений, программ для быстрого обмена сообщениями (приложений-мессенжеров).

Несмотря на всестороннее исследование классификации электронно-цифровых следов для целей настоящей работы считаем целесообразным уделить этому внимание и при этом учесть виды электронно-цифровых следов, образующихся при совершении преступлений экстремистской и террористической направленности.

Так, по мнению В. А. Мещерякова, электронно-цифровые следы подразделяются в зависимости от места их обнаружения: на носителях, которые использовались при совершении преступлений; носителях, используемых для связи с сетями; носителях, которые подверглись изменению в результате действий подозреваемого [1, с. 103].

А. Г. Волеводз выделяет локальные и сетевые следы [2, с. 205].

А. Ю. Семенов классифицировал электронно-цифровые следы по месту их нахождения на следы в компьютере преступника и следы в компьютере потерпевшего [3].

В. Б. Вехов подразделяет электронно-цифровые следы в зависимости от особенностей компьютерной информации, зафиксированной на машинном носителе в форме, доступной для восприятия ЭВМ [4, с. 43].

Каждая из указанных классификаций представляет определенное теоретическое и практическое значение, что подтверждается целым рядом научных исследований. Основываясь на перечисленных критериях и учитывая специфику совершения преступлений экстремистской и террористической направленности в современных реалиях, для классификации электронно-цифровых следов дополнительно предлагаем отметить электронно-цифровые следы по характеру пребывания лица в виртуальном пространстве. Например, если рассматривать электронно-цифровой след как деятельность личности («преступника экстремиста») в виртуальном пространстве, то его действия и оставляемые следы могут быть как активными, так и пассивными.

Активные следы – это те, которые создаются пользователем намеренно, например при авторизации на сайте с помощью логина и пароля, размещения публикаций в социальной сети, заполнении онлайн-форм и т. п.

Пассивные следы остаются случайно, например в виде истории посещений сайтов, IP-адресов, что позволяет без его уведомления пользователя собирать информацию о нем.

[3] Сапожников, А. В России на 160 % за год выросло число экстремистских преступлений // Коммерсантъ : сайт. URL: https://www.kommersant.ru/doc/5861839 (дата обращения: 11.12.2024).

Наиболее специфичными следами в данном случае могут быть следующие:

- регистрационные данные на доменное имя; логин от взаимодействия с регистратором доменных имен; следы проведения платежа этому регистратору;
- следы при настройке DNS-сервера, поддерживающего домен преступников (например, вербовщиков);
- следы от взаимодействия с хостинг-провайдером, у которого размещен веб-сайт: заказ, оплата, настройка, залив контента;
- следы, оставленные пользовательским оборудованием при посещении сайта (например, файлы cookie, данные записи сессии, рекламных трекеров, сведения об IP-адресе и т. п.).

При взаимодействии с преступниками могут оставаться такие следы, как данные почтового адреса при приеме заказов по электронной почте, через веб-форум; переписка в диалоговом окне сайта или в приложении с потенциальными жертвами.

В ходе совершения преступлений экстремистского и террористического характера с использованием вредоносного программного обеспечения могут быть оставлены следующие следы:

- файлы (исполняемые и различные скрипты, файлы динамически загружаемых библиотек, log-файлы, архивы, файлы электронной почты);
- программы, предназначенные для удаленного или локального управления системой, для удаления системных данных, а также для кражи пользовательских данных и сбора сведений о системе;
- записи журналов системных событий и событий информационной безопасности;
- список запущенных процессов и служб;
- список действующих и недавно установленных сетевых соединений;
- информация о событиях информационной безопасности антивирусного программного обеспечения, экрана SIEM-систем;
- список локальных и доменных пользователей;
- артефакты и метаданные запуска программ (Prefetch, Amcache, Shimcache).

Учитывая практику расследования рассматриваемых преступлений, наиболее распространенными видами электронно-цифровых следов, с которыми приходится работать сотрудникам правоохранительных органов, являются текстовые, аудио- и графические файлы. В связи с этим целесообразно выделить также классификацию следов по их формату. Помимо указанных, в зависимости от форматов файлов, встречаются видеофайлы, архивные файлы, исполняемые файлы, лог-файлы, системные файлы.

Так, в 2023 году сотрудники регионального управления ФСБ по Тюменской области задержали гражданина России за «целенаправленное финансирование» Вооруженных сил Украины (далее по тексту – ВСУ). По данному факту было возбуждено уголовное дело о содействии террористической деятельности[4].

Также в Новокузнецке сотрудники ФСБ задержали жителя Новокузнецка за перевод личных средств на покупку снаряжения для ВСУ[5].

В обоих случаях одними из доказательств выступили электронные чеки о денежных переводах и проводимых финансовых операциях.

---

[4] Ткаченко, Н. Россиянина задержали по делу о финансировании ВСУ // Московский комсомолец : сайт. URL: https://www.mk.ru/incident/2023/12/07/rossiyanina-zaderzhali-po-delu-o-finansirovanii-vsu.html (дата обращения: 11.12.2024).

[5] Добрунов, М. Жителя Новокузнецка арестовали по делу о финансировании ВСУ // РБК : новостной портал. URL: https://www.rbc.ru/politics/22/01/2024/65ae193c9a794708c735bb2e (дата обращения: 11.12.2024).

Приведем еще пример, где в качестве электронно-цифровых следов выступили аудио- и видеофайлы. Р. с помощью своего персонального компьютера, подключенного к сети Интернет, на официальном сайте «www.vkontakte.ru» в учетной записи разместил видеоролик «Россия 88 ….», содержащий призывы к действиям, направленным на возбуждение национальной розни, нарушение прав, свобод и законных интересов человека и гражданина в зависимости от его национальной принадлежности. Кроме того, Р. разместил композицию «Слава ****» группы «********», содержащую призывы к действиям, направленным на возбуждение национальной розни, нарушение прав, свобод и законных интересов человека и гражданина в зависимости от его национальной принадлежности[6]. Тем самым Р. совершил не только действия террористического и экстремистского характера, но и распространил данную информацию в сети «Интернет», где данными могли воспользоваться десятки людей, которые в последующем могли возобновить и продолжить преступную деятельность.

Обобщая вышесказанное, предлагаем авторскую классификацию электронно-цифровых следов, образующихся в процессе совершения преступлений террористического и экстремистского характера:

1) следы телефонных переговоров с использованием средств мобильной связи (IMEI, сведения об абоненте и абонентском номере, биллинговые данные о SIM-карте, записанные аудиофайлы телефонного разговора и др.);

2) следы передачи и приема текстовых сообщений с использованием средств мобильной связи и иных технических средств;

3) следы доступа в сеть Интернет и использования предоставленных там услуг;

4) следы, образуемые в результате внесения записей об абонентах и абонентских номерах в записную книгу устройства;

5) следы, содержащиеся в аудио-, фото- и видеозаписи;

6) следы финансовых операций;

7) следы в специальных программных средствах для прошивки мобильных телефонов и SIM-карт;

8) следы в приложениях Viber, Skype, WhatsApp, Telegram, Vkontakte и др.

Следует обратить внимание, что данная классификация не содержит исчерпывающего переченя видов электронно-цифровых следов и может быть дополнена или скорректирована с учетом практического опыта расследования указанных преступлений.

Также важно отметить, что, несмотря на достаточно развернуто представленную классификацию электронно-цифровых следов, образующихся при совершении рассматриваемой группы преступлений, их специфика во многом заключается именно в содержательной составляющей (содержание текста, видеофайла, аудиофайла, изображения и т. п.). В свою очередь перечисленные виды электронно-цифровых следов и отдельные критерии для классификации универсальны и могут быть применимы при исследовании особенностей механизма следообразования других видов преступлений, которые совершаются с использованием информационно-телекоммуникационных технологий.

Таким образом, при расследовании отдельных видов преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, в том числе экстремистской и террористической направленности, особенно важно не только обнаружить, правильно зафиксировать и получить

[6] Морохин, И. Н. и др. Экстремизм «в контакте» (первая инстанция) // Праворуб. Профессиональное сообщество юристов и адвокатов : сайт. URL: https://pravorub.ru/cases/11215.html (дата обращения: 11.12.2024).

сведения об электронно-цифровом следе, но и сохранить его содержание и получить информацию о его происхождении.

Анализ следственной и судебной практики о преступлениях экстремистской и террористической направленности свидетельствует о том, что электронно-цифровые следы наиболее часто можно обнаружить на персональных компьютерах, мобильных телефонах, переносных носителях информации. Отдельно стоит отметить облачные сервисы и хранилища, но с поправкой на тот факт, что доступ к ним осуществляется через вышеуказанные технические устройства. Однако в случае получения электронно-цифровых следов в рамках исследования облачных сервисов путем взлома аккаунта удаленным доступом и сохранением файлов место обнаружения не привязывается к определенному устройству (ПК, планшету или мобильному телефону).

Вне зависимости от места формирования и нахождения электронно-цифровых следов в целях их обнаружения, правильной фиксации и сохранения для дальнейшего исследования необходимо использовать помощь специалиста в области информационных технологий, который в свою очередь выбирает комплекс специальных технических средств, аппаратно-программных комплексов (далее – АПК) и сервисов для работы с устройствами и файлами.

В качестве примера приведем АПК «Мобильный Криминалист Эксперт», основной функционал которого – это мобильные телефоны и мультимедийные устройства, а также персональные компьютеры, с которых возможно:

- извлечь полную файловую структуру и данные Keychain из iOS-устройств;
- создать физические образы устройств под управлением Android, а также логические образы устройств под управлением iOS, Android, BlackBerry, WindowsPhone, Symbian и др.;
- извлечь расшифрованные данные из Android-устройств с пофайловым и полнодисковым шифрованием;
- импортировать физические образы и резервные копии множества устройств;
- получать подробную информацию о событиях на целевой машине благодаря детальному анализу артефактов систем на Windows, macOS и GNU/Linux;
- извлекать переписку, вложения и контакты из приложений-мессенджеров[7].

Данные функции принципиально важны, поскольку представляют достаточно широкие возможности для исследования технических устройств, содержащих электронно-цифровые следы с информацией экстремистского и террористического характера.

Кроме того, АПК «Мобильный Криминалист» позволяет работать с облачным сервисами, что, как отмечалось выше, актуально и представляет важное криминалистическое значение для расследования.

Весьма полезным представляется программный комплекс «SEUS» для поиска, мониторинга и анализа информации в открытом пространстве социальных сетей и мессенджеров. Данный комплекс на основе размещенных когда-либо аккаунтов (в том числе удаленных) в социальных сетях, контента, размещенного пользователем в сети, и других открытых данных из Интернета создает «цифровое досье» на пользователя. Таким образом, у следователя при должном анализе появляется не только полезная ориентирующая информация о лице, но и сведения, имеющие доказательственное значение (например, данные о связи между удаленными и существующими аккаунтами пользователя и сведения экстремистского характера, размещенные этим пользователем с разных устройств и анонимизированных профилей

[7] Мобильный криминалист // МКО Системы : сайт. URL: https://mko-systems.ru/ (дата обращения: 10.12.2024).

в приложениях-мессенджерах и социальных сетях).

Перечисленные программные продукты значительно облегчают следственную работу, но следует помнить, что все полученные результаты должны быть зафиксированы с соблюдением норм уголовно-процессуального законодательства, анализироваться следователем с учетом уже имеющихся в уголовном деле доказательств, всесторонне исследоваться с точки зрения допустимости, относимости и достаточности доказательств.

Выводы и заключение

Выработанные наукой и практикой критерии для классификации и виды электронно-цифровых следов разнообразны и ориентированы на сущность электронно-цифрового следа, его формат, источник формирования и др. Предложенная авторская классификация электронно-цифровых следов сформирована исходя из специфики работы со следами, возникающими при совершении преступлений экстремистского и террористического характера. При этом исследование позволяет сделать вывод о том, что данная классификация может быть расширена и доработана, так как выделенные виды электронно-цифровых следов универсальны и могут подходить под другие виды преступлений, совершаемых с использованием информационно-телекоммуникационных технологий.

В связи с этим еще один вывод заключается в том, что самым важным для расследования рассматриваемых в исследовании преступлений является содержание электронно-цифрового следа (текстовое, изображение, информация в аудиозаписи и т. п.), а не только сведения об электронно-цифровом следе (формате, виде, происхождении и т. п.).

Таким образом, при расследовании преступлений террористической и экстремисткой направленности, совершаемых с использованием информационных технологий, следователь должен обладать знаниями об особенностях формирования таких следов и навыками по работе с ними, учитывать необходимость содействия специалиста в области информационных технологий, уметь правильно фиксировать и анализировать результаты, в том числе полученные при исследовании электронно-цифровых следов с помощью специализированных программных продуктов и АПК.

СПИСОК ИСТОЧНИКОВ

1. Мещеряков, В. А. Преступления в сфере компьютерной информации: основы теории и практики расследования : монография. Воронеж : Издательство Воронежского государственного университета, 2002. 408 с.

2. *Волеводз, А. Г.* Противодействие компьютерным: книга преступлениям. Москва : Юрлитинформ, 2002. 375 с.

3. Семенов, А. Ю. Некоторые аспекты выявления, изъятия и исследования следов, возникающих при совершении преступлений в сфере компьютерной информации // Сибирский юридический вестник. 2004. № 1. С. 53–55.

4. *Вехов, В. Б.* Электронная криминалистика: понятие и система // Криминалистика: актуальные вопросы теории и практики : сб. тр. участников междунар. науч.-практ. конф. Ростов н/Д, 2017. С. 40–46.

REFERENCES

1. *Meshcheryakov V. A.* Prestupleniya v sfere komp'yuternoj informacii: osnovy teorii i praktiki rassledovaniya: monografiya [Crimes in the field of computer information: fundamentals of theory and practice of investigation: monograph]. Voronezh: Izdatel'stvo Voronezhskogo gosudarstvennogo universiteta, 2002. 408 p. (in Russian)
2. *Volevodz A. G.* Protivodejstvie komp'yuternym: kniga prestupleniyam [Countering computer crimes: a book of crimes]. Moscow: Yurlitinform. Moskva: YUrlitinform, 2002. 375 p. (in Russian).
3. *Semenov A. YU.* Nekotorye aspekty vyyavleniya, iz"yatiya i issledovaniya sledov, voznikayushchih pri sovershenii prestuplenij v sfere komp'yuternoj informacii [Some aspects of identifying, seizing and studying traces that arise when committing crimes in the field of computer information]. Siberian Legal Bulletin. – Sibirskij yuridicheskij vestnik. 2004. no 1. Pp 53–55. (in Russian)
4. *Vekhov V. B.* Elektronnaya kriminalistika: ponyatie i sistema [Electronic forensics: concept and system]. Kriminalistika: aktual'nye voprosy teorii i praktiki: sb. trudov uchastnikov mezhdunar. nauch.-prakt. konf. – Forensic science: current issues of theory and practice: collection. tr. participants of the international scientific-practical conf. Rostov n/D., 2017. Pp. 40-46. (in Russian) (in Russian).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Дерюгин Роман Александрович, кандидат юридических наук, доцент, начальник кафедры криминалистики. Уральский юридический институт МВД России. 620057, Российская Федерация, г. Екатеринбург, ул. Корепина, 66.

INFORMATION ABOUT THE AUTHOR

Roman A. Deryugin, Candidate of Law, Head of the Criminalistics Department. Ural Law Institute of the MIA of Russia, 66, Korepina Str., Yekaterinburg, Russian Federation, 620057.