Научная статья
УДК: 343.985.7
DOI: 10.55001/2587-9820.2024.80.56.004

ОБНАРУЖЕНИЕ И ИЗЪЯТИЕ ЦИФРОВЫХ СЛЕДОВ ПРЕСТУПЛЕНИЙ ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ

Денис Михайлович Владимиров
Рязанский филиал Московского университета МВД России имени В.Я. Кикотя, г. Рязань, Российская Федерация, den.vladimirov94@mail.ru

Аннотация. Исследование посвящено особенностям собирания цифровых следов преступлений экстремистской направленности. Обозначены основные способы и методы обнаружения и изъятия исследуемой категории следов преступлений. Отдельное внимание уделено современным автоматизированным поисковым системам, программному обеспечению и аппаратно-программным комплексам отечественного производства, которые в условиях санкционного давления активно развиваются и с их помощью, правоохранительные органы добиваются высоких результатов в деятельности, связанной с собиранием цифровых следов преступлений. В завершение автором обозначены основные векторы совершенствования работы по обнаружению, фиксации и изъятию цифровых следов преступлений экстремистской направленности.

Ключевые слова: преступления экстремистской направленности, цифровые следы, аппаратно-программные комплексы, darknet, информационно-телекоммуникационные технологии

Для цитирования: Владимиров, Д.М. Обнаружение и изъятие цифровых следов преступлений экстремистской направленности // Криминалистика: вчера, сегодня, завтра : сб. науч. тр. Иркутск : Восточно-Сибирский институт МВД России. 2024. Т. 31. № 3. С. 38–44. DOI: 10.55001/2587-9820.2024.80.56.004

DETECTION AND REMOVAL OF DIGITAL TRACES OF EXTREMIST CRIMES

Denis M. Vladimirov
Ryazan Branch of the Moscow University of the MIA of Russia named after V.Ya. Kikot, Ryazan, den.vladimirov94@mail.ru

Abstract. The study is devoted to the peculiarities of collecting digital traces of extremist crimes. The main methods and methods of detection and seizure of the investigated category of crime traces are outlined. Special attention is paid to modern automated search engines, software and hardware and software complexes of domestic production, which are actively developing under the conditions of sanctions pressure and show high results in the activities of law enforcement agencies in collecting digital traces of crimes. In conclusion, the author identifies the main vectors for improving the work on detecting, fixing and removing digital traces of extremist crimes.

Keywords: extremist crimes, digital traces, hardware and software complexes, darknet, information and telecommunication technologies

For citation: Vladimirov, D.M. Obnaruzhenie i iz"yatie cifrovyh sledov prestuplenij ekstremistskoj napravlennosti [Detection and removal of digital traces of extremist crimes]. Kriminalistika: vchera segodnya, zavtra = Forensics: yesterday, today, tomorrow. 2024, vol. 31, no 3, pp. 38–44. (in Russ.) DOI: 10.55001/2587-9820.2024.80.56.004

Введение

Настоящее время характеризуется высоким уровнем погружения человечества в цифровой мир. Развитие высоких технологий, а вместе с тем и способов передачи, обмена и хранения информации послужило толчком к созданию беспроводных систем передачи данных, таких как ИК-порт, Bluetooth, Wi-Fi и, конечно же, информационно-телекоммуникационных сетей, самой распространенной из которых стала всемирно известная сеть Интернет. Согласно исследованиям одной из ведущих мировых компаний, занимающихся медиа-аналитикой «Meltwater», по состоянию на январь 2023 года из 8,01 млрд человек, проживающих на нашей планете, 5,16 млрд (64,4 %) являются интернет-пользователями[1], и из года в год их количество только растет. Интернет повлиял практически на все сферы жизнедеятельности человека благодаря своим функциональным возможностям. В процессе развития он очень активно стал внедряться в профессиональную деятельность людей, многие его ресурсы связаны с коммерцией, маркетинговыми исследованиями, электронными платежами, а также управлением банковскими счетами и т. д. Помимо этого Интернет чаще стал применяться человечеством в быту для коммуникации, проведения досуга, а также получения информации от Интернет-СМИ.

К сожалению, и представители криминальной субкультуры смогли адаптироваться к новым реалиям, что позволило им открыть новые возможности реализации своих противоправных целей. Не исключением стали и экстремистские организации, а также отдельные представители экстремистской идеологии. Согласно статистическим данным МВД России о состоянии преступности, в 2019 г. было зарегистрировано 585 преступлений экстремистской направленности, в 2020 г. – 833 (+30 %), в 2021 г. – 1 057 (+22 %), в 2022 г. – 1 566 (+48 %), и в 2023 г. – 1 340 (-14,4 %)[2], большая часть из которых совершается с использованием сети Интернет.

Генеральный прокурор Российской Федерации И. В. Краснов отмечает, что Интернет является основным источником распространения экстремистской идеологии[3], в связи с чем перед специалистами стоит задача по выработке и совершенствова-

[1] The changing world of digital in 2023 // we are social : сайт. URL: https://wearesocial.com/uk/blog/2023/01/the-changing-world-of-digital-in-2023/ (дата обращения: 29.02.2024).

[2] Состояние преступности в России за 2019 –2022 гг. // Министерство внутренних дел Российской Федерации : офиц. сайт. URL: https://мвд.рф/reports/item/35396677/ (дата обращения: 13.03.2024).

[3] Из доклада Генерального прокурора Российской Федерации И. В. Краснова на расширенном заседании Коллегии, посвященной итогам работы органов прокуратуры за 2022 год и задачам по укреплению законности и правопорядка на 2023 г. // Генеральная прокуратура Российской Федерации : офиц. сайт. URL: https://epp.genproc.gov.ru/web/gprf/mass-media/news?item=86293561 (дата обращения: 10.03.2025).

нию методик обнаружения, фиксации и изъятии цифровых следов преступлений, или, как их еще называют, «виртуальных следов» [1, с. 173], или «электронно-цифровых» [2, с. 10].

Основная часть

Преобладающее большинство преступлений экстремистской направленности совершаемых с использованием сети «Интернет» осуществляются посредством размещения текста, фото-, аудиоматериалов, картинок либо рассылки сообщений в чатах мессенджеров, содержащих призывы к осуществлению экстремистской деятельности (ч. 2 ст. 280 УК РФ[4], ч. 2 ст. 280.1 УК РФ) или направленных на возбуждение ненависти, вражды либо унижение чести и достоинства по экстремистскому мотиву (ст. 282 УК РФ). С учетом специфики исследуемой категории преступлений обнаружение цифровых следов и криминалистически значимой информации осуществляется преимущественно следующими способами:

1. Поиск информации экстремистского толка путем мониторинга социальных страниц, мессенджеров или интернет-сайтов посредством использования персонального компьютера, ноутбука, сотового телефона и т. д. Однако такой поиск возможен, когда информация находится в открытом доступе либо получилось оперативным путем получить право посещения закрытой страницы, чата, канала или сайта.

Стоит отметить, что с конца 2022 – начала 2023 года Роскомнадзор протестировал и запустил систему «Окулус», предназначенную для автоматического поиска запрещенного контента, в том числе экстремистского содержания. Данная система обрабатывает данные, отобранные единым модулем анализа (ЕМА), в том числе в расшифровке QR-кодов, переписке в чатах и каналах мессенджеров, URL-адресах, субтитрах и т. д., причем на достаточно высокой скорости: в сутки «Окулус» способен обработать свыше 200 000 фотографий, на один файл в среднем тратится около трех секунд[5]. Для обычных операторов, действующих в ручном режиме, такая скорость мониторинга, естественно, недостижима, либо будет требовать задействования большого количества человеческих ресурсов.

Компания «СЕУЛАБ» активно развивает поисковую систему «СЕУС», которая специализируется на анализе криминалистически значимой информации в социальных сетях. Применение поисковой системы «СЕУС» позволяет экспертам эффективно решать задачи противодействия терроризму и экстремизму в Интернете[6]. Это лишний раз показывает наличие стремления российских производителей к совершенствованию отечественных цифровых поисковых систем, предназначенных для выявления противоправной информации, размещаемой в сети Интернет.

2. Обнаружение цифровых следов преступлений путем непо-

[4] Уголовный кодекс Российской Федерации : УК : принят Гос. Думой 24 мая 1996 года : одобрен Советом Федерации 5 июня 1996 года : послед. ред. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 18.05.2024).

[5] Что такое «Окулус» и зачем он нужен? // Российская газета : сетевое издание. URL: https://rg.ru/2023/02/13/chto-takoe-okulus-i-zachem-on-nuzhen-roskomnadzoru.html (дата обращения: 23.02.2024).

[6] Цифровая криминалистика. Весна-23 // МКО Системы : сайт. URL: http://events.mko-systems.ru/forensics_spring23 (дата обращения: 04.03.2024).

средственного осмотра электронных устройств подозреваемых либо авторизации через их аккаунты в социальных сетях (мессенджерах) с добровольного согласия или разрешения суда [3, с. 108–109].

3. При наличии достоверной информации и положительного решения суда можно обратиться к компаниям – владельцам серверов социальных сетей, мессенджеров и т. д. с просьбой предоставления криминалистически значимой информации о пользователях и их деятельности в цифровом пространстве, хранящейся на принадлежащих им электронно-вычислительных мощностях (например, в компанию VK, в активы которой входят такие социальные сети, как «Вконтакте» и «Одноклассники», почтовый сервис «Почта Mail.ru», мессенджер «ISQ» и др.).

4. Получение информации о фактах размещения файлов экстремистского содержания в сети Интернет от физических и юридических лиц, а также от негласного аппарата (конфидентов) оперативными подразделениями [4, с. 143].

Фиксацию факта размещения информации экстремистского содержания на интернет-странице следует производить незамедлительно, так как злоумышленникам не представляет труда частично или полностью изменить либо полностью удалить опубликованную ими противоправную информацию, находясь на любом расстоянии, только лишь имея доступ к сети. Для этого можно произвести фотофиксацию экрана служебного компьютера, где на фотоснимке будет отражена криминалистически важная информация и место ее размещения, однако рекомендуется делать «скриншот» (Print-screen), который позволяет получить более качественное изображение без бликов и ряби (так называемых «муаровых узоров») [3, с. 118–119].

Что касается обнаружения, фиксации, а также изъятия цифровых следов с электронных носителей информации, в том числе заблокированных или поврежденных, то для этого экспертно-криминалистические подразделения МВД России оснащаются специализированными программно-аппаратными комплексами. Наиболее часто используемым и эффективным до недавнего времени считался комплекс UFED израильского производства фирмы Cellebrite. Изначально он предназначался для работы в полевых и лабораторных условиях с мобильными устройствами, но с течением времени усовершенствовался и стал применяться для работы с некоторыми КПК, ноутбуками и компьютерами. Однако в последние годы, с учетом происходящих геополитических событий и санкционного давления на Россию, программные обновления к данному комплексу перестали предоставляться фирмой Cellebrite. В связи с этим, как справедливо отмечает Я. Г. Варакин, со временем это сделает их бесполезными к использованию правоохранительными органами Российской Федерации [5, с. 85], а для работы со многими новейшими устройствами они уже непригодны.

К счастью, отечественные производители активно развивают собственные программно-аппаратные комплексы, которые показывают хорошие результаты в работе с различными видами электронных устройств и носителей. Так, «Мобильный криминалист» фирмы «МКО Системы» уже давно не только используется для работы с сотовыми телефонами, но и имеет программы для обнаружения, фиксации и изъятия данных с компьютеров («МК Десктоп») и даже

облачных серверов и дронов («МК Эксперт Плюс»). PC-3000 фирмы Acelab специализируется на восстановлении и изъятии информации с жестких дисков компьютеров, а Elcomesoft – на восстановлении доступа к заблокированным и зашифрованным данным.

Существуют и другие методы изъятия криминалистически важной информации с электронных устройств: например, метод «Chip-off», предусматривающий выпаивание чипа памяти и считывание с него данных специализированными устройствами или его перепайку в другое, не поврежденное аналогичное устройство; метод J-tag, предусматривающий получение доступа к данным с помощью отладочного интерфейса, и т. д. В зависимости от производителя и функционала, учитывая каждую конкретную ситуацию и исследуемый объект, эксперт сам определяет, какой метод будет более эффективен.

К сожалению, несмотря на то, что методологическое и технико-криминалистическое обеспечение ЭКП МВД России достаточно разнообразное и современное, ни один из аппаратно-программных комплексов как зарубежного, так и отечественного производства не дает гарантий постоянного полного извлечения всех интересующих данных с любого исследуемого устройства. Помимо того, что устройство может быть сильно повреждено либо интересующие цифровые следы были удалены без возможности восстановления, экспертам необходимо иметь в распоряжении только программные комплексы, совместимые аппаратно с версиями операционных систем устройств. К тому же существуют программные обеспечения, специализирующиеся на шифровании. Так, «VeraCrypt» используется представителями криминальной среды для создания шифрованных томов на жестких дисках, электронных носителях и даже облачных сервисах. Данное ПО работает со всеми популярными операционными системами: Windows, Linux, Mac OS. Если устройство подвергается осмотру с помощью аппаратно-программных комплексов, о которых мы говорили ранее, то зашифрованную с помощью VeraCrypt информацию не всегда удается обнаружить и, соответственно, изъять.

Одним из разделов сети «Интернет», который содержит огромное количество запрещенной информации, кинопродукции, товаров и сферы услуг криминального характера, является популяризированная в преступном мире так называемая «теневая, или темная, сеть» – DarkNet [6, с. 302]. Для использования подавляющего большинства теневых сетей требуется установка специализированного программного обеспечения (самым распространенным является «Tor», а также «I2P», «Freenet», «Retroshare» и т. д.). Несмотря на их различные индивидуальные качества, главной особенностью всех теневых сетей, привлекающей представителей криминальной субкультуры, является высокий уровень анонимизации пользователей. Для этого в DarkNete используются собственные домены (т. н. псевдодомены, такие как «.onion»), информация о которых не хранится в корневых серверах DNS, сайты не индексируются поисковыми системами, информация покрывается несколькими слоями шифров, сами сети состоят из нод – огромного количества серверов, созданных анонимными пользователями. Для того чтобы провести осмотр ресурсов DarkNet и зафиксировать интересующую криминалистически важную информацию, необходимо в первую очередь добиться их деанонимиза-

ции. Здесь особое значение имеет эффективность работы оперативных подразделений. Как справедливо отмечает А. Б. Смушкин, многие сайты даркнета требуют так называемых приглашений (инвайтов) от доверенных пользователей для доступа к сайту, и для получения подобного инвайта следует активно использовать работу с негласным аппаратом [7, с. 108]. Также в аудиторию пользователей DarkNet может быть внедрен и оперативный сотрудник.

Выводы и заключение

Аккумулируя вышеизложенное, стоит отметить, что, несмотря на вводимые санкции западных государств в отношении Российской Федерации, отечественные разработчики аппаратно-программных комплексов и программного обеспечения различного типа смогли адаптироваться и усовершенствовать собственные продукты, которые в настоящее время активно применяются сотрудниками правоохранительных органов в работе по собиранию цифровых следов преступлений. Конечно, не стоит останавливаться на достигнутом, необходимо и дальше развивать отечественную продукцию и устранять существующие недостатки. То же самое касается и оперативной работы, особенно в рамках борьбы с преступлениями экстремистской направленности, совершаемыми посредством использования теневых сетей DarkNet. С учетом глобального технического развития необходимо повышать качество и вносить своевременные изменения в тактику и методику работы оперативных подразделений по борьбе с исследуемой категорией преступлений. А на уровне сотрудничества государств, несмотря на геополитические процессы, надо стремиться к разработке, принятию и соблюдению международных правовых норм, направленных на противодействие преступлениям в сфере информационно-телекоммуникационных технологий.

СПИСОК ИСТОЧНИКОВ

1. *Аскольдская, Н. Д.* Виртуальные следы как элемент криминалистической характеристики компьютерных преступлений // Закон и право, 2020. № 5. 173–175.

2. *Колычева, А. Н.* Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет : автореф. дис. … канд. юрид. наук. М., 2019. 25 с.

3. *Россинская, Е. Р., Сааков, Т. А.* Проблемы собирания цифровых следов преступлений из социальных сетей и мессенджеров // Криминалистика: вчера, сегодня, завтра. 2020. № 3 (15). С. 106–123.

4. *Кутузов, А. В.* Методологические основы раскрытия и расследования преступлений экстремистской направленности с использованием информационно-телекоммуникационной сети Интернет : дис. ... канд. юрид. наук. Ростов-на-Дону, 2022. 237 с.

5. *Варакин, Я. Г.* Криминалистические технологии обнаружения, фиксации, изъятия цифровых следов преступлений и иной доказательной информации // Вестник Сургутского государственного университета, 2021. № 4 (34). С. 81–87.

6. *Гасанов, С.Ш.* Сеть «DARKNET» как пространство негативной социализации и совершения преступлений // В сборнике: Социально-гуманитарные проблемы образования и профессиональной самореализации. Сборник материалов Всероссийской конференции молодых исследователей с международном участием, 2019. – С. 301-304.

7. *Смушкин, А. Б.* Криминалистические аспекты исследования даркнета в целях расследования преступлений // Актуальные проблемы российского права. 2022. Т. 17. № 3. С. 102–111. DOI: 10.17803/1994-1471.2022.136.3.102-111.

REFERENCES

1. *Askoldskaya, N. D.* Virtual'nye sledy kak element kriminalisticheskoj harakteristiki komp'yuternyh prestuplenij [Virtual footprints as the element of criminalistic characteristics of computer crimes]. Zakon i pravo – Law and Law, 2020, no. 5, pp. 173-175. (in Russian).

2. *Kolycheva, A.N.* Fiksaciya dokazatel'stvennoj informacii, hranyashchejsya na resursah seti Internet : avtoref. dis. … kand. yurid. Nauk [Fixation of evidentiary information stored on Internet resources: abstract of the cand. Jurid. sciences': 12.00.12]. Moscow, 2019, 25 p. (in Russian).

3. Rossinskaya, E.R., Saakov, T.A. Problems of collecting digital traces of crimes from social networks and messengers [Problemy sobiraniya cifrovyh sledov prestuplenij iz social'nyh setej i messendzherov]. Kriminalistika: vchera, segodnya, zavtra. – Criminalistics: yesterday, today, tomorrow. 2020, no. 3 (15), pp. 106-123. (in Russian).

4. *Kutuzov, A.V.* Metodologicheskie osnovy raskrytiya i rassledovaniya prestuplenij ekstremistskoj napravlennosti s ispol'zovaniem informacionno-telekommunikacionnoj seti Internet : dis. ... kand. yurid. nauk. [Methodological foundations for the disclosure and investigation of extremist crimes using the Internet information and telecommunications network: dis. ... cand. Jurid. sciences']. Rostov-on-Don, 2022, 237 p. (in Russian).

5. *Varakin, Ya.G.* Kriminalisticheskie tekhnologii obnaruzheniya, fiksacii, iz"yatiya cifrovyh sledov prestuplenij i inoj dokazatel'noj informacii [Criminalistic technologies of detection, fixation, seizure of digital traces of crimes and other evidentiary information]. Vestnik of Surgut State University – Vestnik Surgutskogo gosudarstvennogo universiteta. 2021, no. 4 (34), pp. 81-87. (in Russian).

6. *Gasanov, S.SH.* [The "DARKNET" network as a space of negative socialization and the commission of crimes]. Social'no-gumanitarnye problemy obrazovaniya i professional'noj samorealizacii. Sbornik materialov Vserossijskoj konferencii molodyh issledovatelej s mezhdunarodnom uchastiem [Social and humanitarian problems of education and professional self-realization. Collection of materials of the All-Russian Conference of Young Researchers with International Participation]. 2019, pp. 301-304. (in Russian).

7. *Smushkin, A. B.* Kriminalisticheskie aspekty issledovaniya darkneta v celyah rassledovaniya prestuplenij [Criminalistic aspects of darknet research in order to investigate crimes]. Aktual'nye problemy rossijskogo prava – Actual problems of Russian law. 2022, vol. 17, no. 3, pp. 102-111. (in Russian).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Владимиров Денис Михайлович, преподаватель кафедры криминалистики, Рязанский филиал Московского университета МВД России имени В.Я. Кикотя, 390043, Российская Федерация, г. Рязань, ул. 1-ая Красная, 18.

INFORMATION ABOUT THE AUTHOR

Denis M. Vladimirov, Lecturer at the Department of Criminology, Ryazan Branch of the Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot, 18, 1st Krasnaya str., Ryazan, Russian Federation, 390043