УДК 343.98

DOI 10.51980/2542-1735_2023_4_27

Ильнур Асгатович ГУМАРОВ,
доцент кафедры
оперативно-разыскной деятельности
Казанского юридического института МВД России,
кандидат юридических наук, доцент
ilnur_gumar@mail.ru

Виктор Владимирович ТЫРЫШКИН,
заместитель начальника кафедры
административного права и административной
деятельности органов внутренних дел
Барнаульского юридического института МВД России,
кандидат юридических наук, доцент
witsan333@yandex.ru

ДОКУМЕНТИРОВАНИЕ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

DOCUMENTING CRIMES COMMITTED USING INFORMATION AND TELECOMMUNICATION TECHNOLOGIES

Исследование посвящено анализу эффективных направлений документирования киберпреступлений. Документирование – это отражение и фиксация преступных действий проверяемых и разрабатываемых лиц на основе полученных сведений путем проведения оперативно-розыскных мероприятий и установления фактических данных, возможно, имеющих значение для уголовного дела. Наибольшую актуальность, на наш взгляд, такая деятельность приобретает при борьбе с преступлениями, совершаемыми с использованием информационно-телекоммуникационных технологий (ИТТ).

При изучении вопросов документирования следов преступлений, совершенных с использованием ИТТ, были использованы социологические методы опроса и анкетирования сотрудников оперативных подразделений органов внутренних дел, а также материалы уголовных дел и нормативные правовые акты, регламентирующие деятельность оперативных подразделений органов внутренних дел. Применялся контент-анализ научных статей и учебной литературы.

В результате исследования авторами предлагается алгоритм действий и мероприятий, направленный на повышение эффективности документирования преступлений, совершаемых с использованием ИТТ, выделяются наиболее распространенные источники, из которых может быть получена оперативно значимая информация.

The study is devoted to the analysis of effective ways of documenting cybercrimes. Documentation is the reflection and recording of criminal actions of persons under investigation on the basis of information received through operational search activities and the establishment of factual data that may be significant in the criminal case. In authors' opinion, such activities gain the greatest relevance in the fight against crimes committed using information and telecommunication technologies (hereinafter referred to as ITT).

When studying the issues of documenting traces of crimes committed using ITT, sociological methods of surveying and questioning officers of operational units of internal affairs bodies were used, as well as files of criminal cases and normative legal acts regulating the activities of operational units of internal affairs bodies. Content analysis of scientific articles and educational literature was used in this study.

As a result of the study, the authors propose an algorithm of actions and measures aimed at increasing the efficiency of documenting crimes committed using ITT and identified the most common sources from which operationally significant information can be obtained.

Ключевые слова: преступления, использование ИТТ, «виртуальные» следы, классификация виртуальных следов, сбор цифровых следов, оперативные подразделения.

Keywords: *crimes, use of ITT, virtual traces, classification of virtual traces, collection of digital traces, operational units.*

Повсеместное внедрение информационно-телекоммуникационных технологий (далее – ИТТ) значительно облегчает жизнь современного человека, оказывает большое воздействие на модернизацию правоотношений, в которых он участвует. В то же время такие технологии чаще применяются правонарушителями в преступных целях. Перечень исследуемых преступлений закреплен указанием Генпрокуратуры России[1]. К данным правонарушениям, как правило, относятся преступления, совершаемые с использованием сети Интернет, средств мобильной связи, вредоносных компьютерных программ, компьютерной техники и т.п.

Согласно статистическим данным, в 2022 году на территории России зарегистрированы 522 065 преступлений, совершенных с использованием ИТТ, из них: 21046 – экономической направленности, 4516 – с причинением крупного или особо крупного ущерба. Основную массу исследуемых преступлений составляют мошенничества: 309 593 факта (среди них: ст. 159.3 УК РФ (с использованием электронных средств платежа) – 7 288, ст. 159.6 УК РФ (в сфере компьютерной информации) – 334). Кроме того, регистрируются много фактов краж с банковского счета, а равно в отношении электронных денежных средств (п. «г» ч. 3 ст. 158 УК РФ) – 112 348 и правонарушений, связанных с незаконным оборотом наркотиков – 82 661 (среди них: ст. 228 УК РФ (незаконные приобретение, хранение, перевозка, изготовление, переработка наркотических средств, психотропных веществ или их аналогов, а также незаконные приобретение, хранение, перевозка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества) – 19 643, п. «б» ч. 2, чч. 3, 4, 5 ст. 228.1 (незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов…) – 62 209) соответственно.

Среди рассматриваемых преступлений были зарегистрированы 6598 фактов изготовления, хранения, перевозки или сбыта поддельных денег или ценных бумаг (ст. 186 УК РФ); 9308 фактов неправомерного доступа к компьютерной информации (ст. 272 УК РФ); 21 424 факта заведомо ложного сообщения об акте терроризма (ст. 207 УК РФ); 2647 фактов неправомерного оборота средств платежей (ст. 187 УК РФ); 200 фактов создания, использования и распространения вредоносных компьютерных программ (ст. 273 УК РФ)[2].

Нормативная правовая основа отражена в Уголовном и Уголовно-процессуальном

1 О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности : указание Генпрокуратуры России N 401/11, МВД России N 2 от 19.06.2023 // Документ опубликован не был. СПС «КонсультантПлюс» (дата обращения: 10.06.2023).

2 Состояние преступности в России. URL: https://xn--b1aew.xn--p1ai/dejatelnost/statistics (дата обращения: 10.06.2023).

кодексах РФ, Федеральных законах «О полиции»[1], «Об оперативно-розыскной деятельности»[2], Указе Президента РФ «О развитии искусственного интеллекта в Российской Федерации»[3], указании Генеральной Прокуратуры РФ «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности»[4], решении Коллегии МВД России «О мерах по совершенствованию организации работы по выявлению, раскрытию и расследованию преступлений, совершаемых с использованием информационно-телекоммуникационных технологий»[5].

Следует отметить, что исследований, посвященных раскрытию преступлений, связанных с использованием ИТТ, в последние годы стало много. Только в последние пять лет об этом писали А.А. Битов [1], Ю.В. Гаврилин [2], А.В. Комов [3], Е.А. Пидусов [4], Е.А. Русскевич [5], А.Б. Смушкин [6] и др.

Документирование исследуемых преступлений не привязано только к процессуальной форме борьбы, поэтому существует свобода выбора при определении инструментов, средств и способов получения и фиксации информации в информационно-телекоммуникационной среде.

На наш взгляд, изменения в компьютерной информации, являющиеся следами преступления, в подавляющем большинстве случаев доступны восприятию не в виде бинарного следа (двоичных кодов), а в редактированной форме: записи в файле реестра, изменении атрибутов файла, цифровом сообщении. Данные следы следует называть «виртуальными». Е.А. Пидусов под виртуальными следами понимает «информацию, представленную в виде машинного кода, записанную компьютером или человеком и представляющую определенную ценность для раскрытия и расследования преступлений в сфере информационных технологий» [4, с. 11].

Любые манипуляции на техническом устройстве фиксируются в его памяти (информация о включении и выключении персонального компьютера, вход/выход из браузера, действия в мессенджерах, социальных сетях, изменение или создание файлов и др.). При этом есть возможность проанализировать время таких манипуляций [6, с. 145]. Обнаруженные следы позволяют установить механизм следообразования и построить примерную последовательность противоправных действий правонарушителя.

Существуют различные критерии классификации виртуальных следов, к примеру: в зависимости от физического носителя «виртуального следа» (на жестком диске, оптическом диске (*CD, DVD*); в оперативных запоминающих устройствах; на периферийных устройствах (например, сканер или распечатывающее устройство); в сетевых устройствах; в проводных, радиооптических и других электромагнитных системах и сетях).

Лица, совершающие преступления с использованием ИТТ, пытаются анонимизировать свои данные посредством сокрытия следов преступления. Так, для сокрытия следов преступления они используют: «руткиты» (программное обеспечение, которое обеспечивает маскировку, управление и сбор сведений), сохранение доступа к «скомпрометированным системам», сокрытие своего существования путем «инъекции» (внедрения) нового процесса, манипуляции с «логами», изменение временных меток на устройстве потерпевшего, сокрытие файлов на отдельных секторах жесткого диска («склеивание» дисков путем создания *RAID* массивов, со-

1 О полиции : Федеральный закон от 07.02.2011 N 3-ФЗ // Собрание законодательства РФ. 2011. N 7. Ст. 900.

2 Об оперативно-розыскной деятельности : Федеральный закон от 12.08.1995 N 144-ФЗ // Собрание законодательства РФ. 1995. N 33. Ст. 3349.

3 О развитии искусственного интеллекта в Российской Федерации : Указ Президента РФ от 10.10.2019 N 490 // Собрание законодательства РФ. 2019. N 41. Ст. 5700.

4 О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности : указание Генпрокуратуры России N 401/11, МВД России N 2 от 19.06.2023.

5 Об объявлении решения коллегии Министерства внутренних дел Российской Федерации от 01.11.2019 N 3км : приказ МВД России от 25.11.2019 N 878 // Документ опубликован не был. СПС «КонсультантПлюс» (дата обращения: 10.06.2023).

здание «теневого» копирования через файл *volsnap.sys* и др.), физическое уничтожение носителя информации, удаление истории и обфускация[1].

Несмотря на различные манипуляции правонарушителей, следы остаются в памяти устройств потерпевших и правонарушителей, на серверах операторов связи, в облачных хранилищах, а также на других носителях информации, которые использовались в момент совершения преступления.

Анализ рассматриваемых преступлений показывает, что в киберпространстве совершаются в большей части корыстные преступления. Появляются новые вредоносные программы, *DoS*-, *DDoS*-атаки, бот-сети, кибершпионаж, мошенничество в сети, специальные сервисы по созданию вредоносных программ (например, «*BLOWMIND*»), по поиску персональных данных будущих жертв, в том числе биометрических (например, *Open source intelegent (OSINT), Shodan, cenys, Maltego, Remini, timber*; веб-сайты: *nomerogram, imgon line.com, iknowwhatyoudownload.com, temp-mail.org* и др.).

Интервьюирование сотрудников АНО ВО «Университет Иннополис», привлекаемых в качестве специалистов при раскрытии преступлений, совершаемых с использованием ИТТ, показало, что для получения доступа к «гаджету» потерпевших чаще всего применяются программа *Mimikatz*[2] *(для преодоления паролей), технологии повышения привилегий программы, использование «скомпрометированной системы» для получения доступа к другим информационно-телекоммуникационным ресурсам, создание поддельного домена через DCShadow* (путем репликации), технологии *Kill chain* и др.

К первоочередным мероприятиям и мерам в процессе выявления следов и документирования противоправных действий необходимо относить: опрос заявителя о совершенных в отношении него противоправных действиях; наведение справок, а именно: запрос выписки об операциях по банковским (лицевым) счетам в банковских организациях; установление возможности видеофиксации факта совершения действия с электронными средствами платежа и изъятие соответствующей видеозаписи; опрос уполномоченных сотрудников банковских организаций; установление и приобщение к материалам проверки: документов, регулирующих отношения между держателем счета (ов) и банковской организацией, сведения о владельце электронного кошелька, регистрационные данные доменных имен, *IP*-адрес владельца сайта и др.

Для эффективного документирования преступлений, совершаемых с использованием ИТТ, сотрудникам оперативных подразделений необходимо применять поисковые программные средства и разрабатывать конкретные устройства выявления информации о преступных посягательствах. Они позволяют установить фактические данные как до возбуждения уголовного дела, так и на последующих этапах расследования. Основная цель данных устройств (программных обеспечений) – деанонимизировать преступников (киберпреступников).

Наибольшую сложность представляет привлечение к ответственности посредников преступной деятельности, которые занимаются обналичиванием доходов, полученных преступным путем, с использованием банкоматов[3]. Их часто используют преступники для обеспечения конспирации противоправ-

1 Обфускация – процесс изменения кода программы, в результате которого он приобретает вид, трудный для понимания, при этом программа сохраняет свои функции. Применяется в целях защиты программного кода и его алгоритмов, для конфиденциальности разработки, а также от действий «атакующих» через уязвимости в коде.

2 Mimikatz – это приложение с открытым исходным кодом, которое позволяет пользователям просматривать и сохранять учетные данные аутентификации, такие как тикеты Kerberos. Злоумышленники обычно используют Mimikatz для кражи учетных данных и повышения привилегий: в большинстве случаев программное обеспечение для защиты конечных точек и антивирусные системы обнаруживают и удаляют его. И наоборот, специалисты по тестированию на проникновение используют Mimikatz для обнаружения и тестирования уязвимостей в сетях, чтобы можно было их исправить.

3 Дроппер/дроп – лицо, которое выполняет указания преступников, получая за вознаграждение,

ных действий. Проведенное анкетирование[1] показывает, что при задержании дропперов (дропов) они не могут указать на лицо, которое поставило перед ними данное здание. Чаще всего их оправдывают в связи с отсутствием субъективной стороны преступления, если они документально поясняют о том, что не подозревали о противоправности своих действий.

62,5% опрошенных сотрудников органов внутренних дел Республики Татарстан указывают на недостаточную подготовленность сотрудников органов внутренних дел к борьбе с преступлениями в киберпространстве; остальные отметили необходимость получения специальных знаний; 75% сотрудников считают, что рассматриваемые преступления практически не удается раскрыть.

Фактически следователю и оперуполномоченному для грамотного использования данных, полученных в ходе осуществления оперативно-розыскных мероприятий по исследуемым преступлениям, базовой юридической подготовки недостаточно. На практике возникают сложности при взаимодействии как между подразделениями органов внутренних дел, так и с иными правоохранительными органами в процессе определения направлений документирования, реализации получаемой информации и сбора доказательств.

Созданные в системе МВД России подразделения по организации борьбы с противоправным использованием информационно-коммуникационных технологий вынуждены постоянно разъяснять новые способы сбора и фиксации фактических данных, разрабатывать специальные тактико-практические рекомендации, разрабатывать с сотрудниками правоохранительных органов методические мероприятия, направленные на повышение эффективности выявления и документирования новых виртуальных следов.

При этом 25% опрошенных сотрудников органов внутренних дел Республики Татарстансчитают, что в органах внутренних дел работают сотрудники с недостаточным уровнем профессионализма в исследуемой проблеме, а остальные 75% говорят о недостаточном оснащении для борьбы с преступлениями в киберпространстве. Очевидно, что повышение технической оснащенности, применение современных средств мониторинга, средств обеспечения безопасности, механизмов анализа, накопленных данных и оперативного реагирования способны принести значительный результат для борьбы с преступлениями, совершаемыми с использованием ИТТ.

Сотрудникам оперативных подразделений следует обратить внимание на источники получения информации о преступлении, совершенном с использованием ИТТ. Данная оперативно значимая информация может быть получена из следующих основных источников:

– технического средства потерпевшего (заявителя);

– от операторов *IP*-телефонии (сведения об *IP*-адресе, *MAC*-адресе, времени и продолжительности связи, точке доступа к сети Интернет);

– от операторов сотовой связи;

– от операторов платежных систем, банковских организаций и иных кредитных учреждений;

– технического средства подозреваемого (обвиняемого);

– из информационных ресурсов сети Интернет и др.

Обладая сведениям об источнике, следует принимать во внимание алгоритм фиксации (документирования) виртуальных следов. Нами предлагается следующий алгоритм действий:

1) не рекомендуется выключать технические устройства, направленные на сбор оперативно значимой информации. Исключением может являться ситуация, когда у преступника имеются пособники. В данной ситуации могут использоваться специальные уничтожители информации (в том числе термические).

2) в протоколе следственного действия подлежат документированию: в памяти какого устройства обнаружены виртуальные

1 Руководители Управления уголовного розыска МВД по Республике Татарстан на всех уровнях и сотрудники отдела «К» МВД по Республике Татарстан.

следы; кому принадлежит устройство; имеет ли устройство выход в сеть Интернет, иные телекоммуникационные или локальные сети; какая оперативная система функционирует на устройстве; в каких файлах обнаружены следы вмешательства, их описание; история создания файла, его изменение. Целесообразно привлекать IT-специалиста;

3) целесообразно осуществлять фотовидеофиксацию экрана с исходной информацией о файлах. Рекомендуется последующая распечатка (запись на CD-диск);

4) производить изъятие для исследования всего объекта – носителя оперативно значимой информации для последующего исследования специалистами-экспертами в сфере компьютерной информации.

Для проведения различных операций с виртуальными следами используют два вида технических средств: общеупотребительные и специализированные. К первому виду относятся программы, которые могут быть известны любому пользователю сети Интернет, например, для просмотра подключений к компьютеру применяется программа-анализатор трафика для компьютерных сетей *Wireshark*; вся информация о процессах на компьютере хранится в разделе *memory damp*, в *swap*-файлах можно найти отпечатки разных программ подключения, а также ряд специализированных прикладных программ (например, *Volatility* – для поиска вирусов и скрытых процессов). При этом необходимо принимать во внимание, что в некоторых файлах содержится информация «в миниатюре», например, в файлах *samp.db*.

В экспертную деятельность внедряются программно-аппаратные комплексы, позволяющие комплексно решать целый ряд задач по исследованию компьютерной информации и техники (например, *EnCase Forensic Edition*, *UFED, X-Ways Forensics, Belkasoft*, Мобильный криминалист-эксперт и др.). Так, «Мобильный криминалист-эксперт» способен извлечь необходимый пласт физических данных. Облачная криминалистика является важным направлением при работе с извлечением данных, поскольку на современных мобильных устройствах пользователь содержит необходимую информацию в облачном сервисе приложений. *X-Ways Forensics* – это программный комплекс, позволяющий исследовать носители информации и снимать с них необходимые для расследования уголовного дела сведения.

Кроме этого следует использовать специальные инструменты по получению оперативно значимой информации, такие как: *Zimmerman tools*, *Elcomsoft, MOBILed.it*, с использованием уязвимости *BootROM* («загрузчик» устройства) – *checkm8*.

Для документирования следов преступления с применением ИТТ наиболее эффективными оперативно-розыскным мероприятиям являются исследование предметов и документов, наблюдение и сбор образцов для сравнительного исследования. В процессе осуществления вышеуказанных оперативно-розыскных мероприятий важно грамотно задокументировать результаты их проведения. В целях фиксации оперативно значимой информации можно использовать фотоаппарат и видеокамеру, такие функции на компьютере, как сочетания клавиш «*PrtSc*», «*Alt PrtSc*», «*Win Shift S*».

В настоящее время имеются недостатки в практическом применении криминалистической техники в процессе документирования исследуемых преступлений: чаще всего применяются лишь часть имеющихся средств (*UFED* и Мобильный криминалист-эксперт), не используют возможности *IT*-специалистов по сбору информации через *Big data*, программные возможности изучения разделов *memory damp*, *swap*-файлов. Это связано с несовершенством организации и правового регулирования использования криминалистической техники, научно-методического и технико-криминалистического обеспечения ее применения. Несмотря на направляемые в территориальные органы внутренних дел алгоритмы действий по линии борьбы с исследуемыми преступлениями, изменить ситуацию не получается.

Сегодня имеется необходимость в формировании отечественных специальных программ в целях выявления злоумышленников в киберпространстве по аналогии с другими

государствами (например, зарубежное специальное программное обеспечение *Magnet Forensics* позволило обнаружить необходимую оперативно значимую информацию на более тридцати электронных устройствах, принадлежащих террористам, ответственных за атаку во время Бостонского марафона (братья Царнаевы, 2013 г.); в 2018 г. МВД Великобритании доложило о создании лондонской технологической компанией *ASI Data Science* комплексного инструмента искусственного интеллекта для обнаружения в 95% террористического контента в онлайн-видео, с вероятностью выявления 99,9%)[1].

На наш взгляд, в целях повышения эффективности документирования исследуемых преступлений, необходимо:

1) своевременно внедрять в практику правоохранительных органов специальные знания о возможности отдельных программных обеспечений и ресурсов по получению цифровых следов преступлений;

2) детально проработать механизм привлечения посредников преступной деятельности (дропов), которые занимаются обналичиванием преступных доходов, и разъяснить порядок их привлечения к ответственности за соучастие в исследуемых преступлениях. Прежде всего, на наш взгляд, это возможно в рамках разработки методических рекомендаций по документированию субъективной стороны.

Принимая во внимание большое количество киберпреступлений, напрашивается вывод о недостаточности отдельных подразделений в системе органов внутренних дел, к примеру, подразделения по организации борьбы с противоправным использованием информационно-коммуникационных технологий. По нашему мнению, требуется создание специальной службы (органа) на федеральном уровне по аналогии с ранее действовавшей Федеральной службой Российской Федерации по контролю за оборотом наркотиков, со своими следователями, оперуполномоченными, специальными техническими и поисковыми подразделениями, а также учебными и научными организациями.

Следует отметить, что в связи с нехваткой специалистов требуется стимулирование деятельности IT-специалистов в органах внутренних дел по линии борьбы с преступлениями, совершенными с использованием ИТТ, в том числе премирование за разработку новой тактики, методики или программы по раскрытию исследуемых преступлений. Одним из вариантов стимулирования следует рассмотреть помощь руководителей органов внутренних дел в получении специалистами патента на разработанную программу.

Анализ рассматриваемых нами преступлений показывает, что в киберпространстве совершаются в большей части корыстные преступления. Данный факт необходимо принимать во внимание при формировании психологического образа преступника. Последние при этом, используя ИТТ, наносят не только материальный вред, похищая денежные средства, иные финансовые активы граждан, но и получают персональные данные для дальнейшей противоправной деятельности. Такие преступные действия осуществляются посредством специального программного обеспечения, доступа к гаджетам потерпевшего, сети Интернет, вовлечения IT-специалистов. Для выявления виртуальных и цифровых следов преступной деятельности требуется знание основных источников получения оперативно значимой информации, применение комплекса программного обеспечения, техники и ресурсов.

1 Counter-terrorism strategy embraces tech, but warns of future extremist digital capabilities. URL: https://www.itpro.co.uk/cyber-terrorism/31247/quantum-computing-could-help-fight-terrorism-says-uk-gov (дата обращения: 13.06.2023).

Библиографический список

1. Битов, А.А. Некоторые особенности взаимодействия следственных и оперативных подразделений ОВД при выявлении, раскрытии и расследовании наркопреступлений, совершаемых с использованием информационных технологий / А. А. Битов // Пробелы в российском законодательстве. – 2022. – Т. 15. – N 4. – С. 49-53.

2. Гаврилин, Ю.В. О научных подходах к проблеме использования информационно-телекоммуникационных технологий в преступных целях : научно-практическое пособие / Ю.В. Гаврилин. – М.: Академия управления МВД России, 2021. – 72 с.

3. Комов, А.В. Организация и тактика работы с компьютерными следами на стадии поисково-познавательной деятельности / А. В. Комов // Пробелы в российском законодательстве. – 2022. – Т. 15. – N 1. – С. 131-136.

4. Особенности обнаружения и изъятия виртуальных следов при расследовании преступлений против собственности в сфере информационных технологий : методические рекомендации / под ред. Е.А. Пидусова. – Воронеж: Воронежский институт МВД России, 2021. – 35 с.

5. Русскевич, Е.А. Преступления, связанные с обращением криптовалют: особенности квалификации / Е.А. Русскевич, И.И. Малыгин // Право. Журнал Высшей школы экономики. – 2021. – N 3. – С. 106-125.

6. Смушкин, А.Б. О структуре электронной цифровой криминалистики / А.Б. Смушкин // Криминалистика: вчера, сегодня, завтра. – 2020. – N 3 (15). – С. 140-148.