Научная статья
УДК 34
https://doi.org/10.24412/2073-0454-2023-5-43-47
EDN: https://elibrary.ru/zyldmm
NIION: 2003-0059-5/23-776
MOSURED: 77/27-003-2023-05-975

Документирование лиц, совершающих преступления с использованием компьютерной техники

Евгений Александрович Виноградов
Московский университет МВД России имени В.Я. Кикотя, Москва, Россия, 40mvd@bk.ru

Аннотация. Рассмотрены практические аспекты документирования лиц, совершающих компьютерные преступления с использованием компьютерной техники. Дана оценка имеющимся правовым нормам, связанным с регламентацией расследований, связанных с компьютерными технологиями преступлений. Проведен анализ ключевых проблем при использовании компьютерных технологий при ведении расследования.

Ключевые слова: киберпреступность, технологии, расследование преступлений, цифровая криминалистика, кибербезопасность, цифровой след

Для цитирования: Виноградов Е. А. Документирование лиц, совершающих преступления с использованием компьютерной техники // Вестник Московского университета МВД России. 2023. № 5. С. 43–47. https://doi.org/10.24412/2073-0454-2023-5-43-47. EDN: ZYLDMM.

Original article

Documenting persons who commit crimes using computer technology

Evgeny A. Vinogradov
Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot', Moscow, Russia, 40mvd@bk.ru

Abstract. Practical aspects of documenting persons committing computer-related crimes using computer technology are considered. The available legal norms related to the regulation of investigations of computer-related crimes are assessed. The key problems in the use of computer technology in conducting investigations are analyzed.

Keywords: cybercrime, technologies, crime investigation, digital forensics, cybersecurity, digital footprint

For citation: Vinogradov E. A. Documenting persons who commit crimes using computer technology. Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia. 2023;(5):43–47. (In Russ.). https://doi.org/10.24412/2073-0454-2023-5-43-47. EDN: ZYLDMM.

Компьютерные технологии прочно вошли в нашу жизнь. Без постоянного обмена огромными потоками информации трудно представить современное общество. Поэтому нет ничего удивительного, что компьютеризация, охватывающая все проявления социальных отношений, не обошла стороной и такое печальное их проявление, как преступность. Использование информационных технологий преступниками с каждым годом набирает все большие обороты. Соответственно, правоохранительным органам для борьбы с ними необходимо также развиваться, внедряя новые технологии, собирая все больше знаний о них. В связи с этим услуги экспертов в данной области все чаще используются для проведения оперативно-розыскных, следственных мероприятий, для получения экспертной оценки.

Особенно ярко подобные тенденции проявились в 2021 г. Согласно имеющимся данным статистических исследований и опросов, применение компьютеров и связанных технологий для совершения преступных деяний в этом году было чрезвычайно высоким. Специалисты по информационной безопасности заявляют, что это первый год за все время ведения наблюдений, когда к их услугам прибегали для помощи в расследовании традиционных преступлений в 1,5 раза чаще, чем к раскрытию именно преступлений, связанных с информационной сферой. При этом, если сравнивать не соотношение, а абсолютные значения, то можно отметить, что и связанные с информационной деятельностью преступления, в которых потребовалось помощь опрошенных экспертов, совершались чаще. Это наглядные доказательства как роста компьютеризированной преступности, так и ее активного проникновения в смежные сферы [1].

Также наблюдение следственных и оперативно-розыскных мероприятий с помощью опросов этих экспертов наглядно продемонстрировало, что их помощь потребовалась не только в делах, связанных с незаконным доступом к информации или использованием вредоносных компьютерных программ, но и

при практическом использовании оперативных мер в делах, связанных с азартными играми, мошенничеством, наркоторговле, организации и заказе убийств, ложном информировании о готовящихся террористических актах. Причем касались они, в основном, их традиционных разновидностей, т. е. компьютерные средства являлись не основным способом и объектом преступлений, а лишь вспомогательным средством, что указывает на их все большее распространение. Анализ этих данных позволяет прийти к уверенному выводу, что потребность правоохранительных органов в специализированной компьютерной поддержке и экспертных знаниях в этой области сильно выросла.

Отдельно стоит выделить обнаружение и фиксацию цифровых следов. Это область технических знаний занимает особо востребованное место в структуре технических знаний, необходимых для эффективной следственно-розыскной работы. Профессор Е. Р. Россинский к данным следам, как и другие авторы, относит компьютерную информацию с криминалистической значимостью, которая касается событий или действий и отражается в материальной форме в результате процессов ее формирования, обработки, передачи и хранения. Результаты двухлетних исследований и опросов, в которых приняли 100 следователей и свыше 200 оперативных сотрудников, указывают, что в связанных с выездом на место совершения преступления мероприятиях по сбору улик самые важные улики не зависят от типа произошедшего преступления. Они все касаются нескольких общих категорий: получение доступа к персональному компьютеру и другим цифровым устройствам подозреваемого при обыске (или, в некоторых случаях, жертвы), изъятие и исследование компьютерной техники потерпевшего лица, исследование локальных компьютерных сетей.

Опрошенные эксперты, отвечая на вопрос о видах следственных действий, в которых нужна была их помощь, ответили так:

♦ 43 % вызовов были связаны с обыском;

♦ 31 % вызовов касался осмотра места совершения преступления;

♦ в 16 % случаев нужно было изучить уже найденные улики — предметы, документы и т. д.;

♦ и в 10 % нужно было провести изъятие улик.

Как и другие виды оперативно-розыскной деятельности, мероприятия, вроде изъятия информации с электронных устройств и каналов связи, а также другие действия, связанные с использованием компьютерных технологий для поиска следов преступления цифрового характера, регламентированы ФЗ № 144 «Об оперативно-розыскной деятельности», принятом в 1995 г.

Данные, полученные посредством опроса IT-специалистов, сотрудничавших с полицией, а также оперативного персонала МВД России, чаще всего такая экспертная помощь была нужна в следующих видах мероприятий:

♦ в 36 % случаев при проведении исследований;

♦ в 28 % случаев при изъятии информации из каналов связи;

♦ в 17 % случаев при изъятии информации из других устройств;

♦ в 12 % случаев при сборе иных видов улик и образов для проведения исследований;

♦ и в 7 % случаев для организации и проведения следственного эксперимента.

Тем не менее, были выявлены и некоторые проблемы. Анализ собранных анкет, результатов опросов сотрудников оперативно-розыскной и следственной деятельности, показывает, что существуют трудности при работе с получением, передачей и демонстрацией цифровых улик посредством удаленных компьютерных систем. Корнем проблемы являются процессуальные сложности. Уголовное законодательство не предусмотрело регламентов для следственных мероприятий, связанных с цифровыми уликами в компьютерных системах удаленного типа. Из-за этого их получение вменяется в обязанности оперативно-розыскных органов, и они занимаются воплощением соответствующих мер.

Чаще всего подобные трудности связаны с получением и фиксацией данных, находящихся на ресурсах мировой сети Интернет. Ими обычно пользуются для нелегальных форм коммерческой деятельности, связанных с распространением порнографической информации, оборотом наркотических средств или иными товарами и информациями, запрещенными к реализации и распространению на территории нашей страны.

Уже целый ряд авторов указывал в своих работах на необходимость улучшить имеющиеся правовые нормы, связанные с регламентацией расследований, связанных с компьютерными технологиями преступлений, а также на то, что наши законодатели внесли в УПК РФ [2] ст. 164.1, касающуюся копирования важной для следствия информации. Тем не менее, все участники опросов с жалобой указывали на недостатки законодательства, проявляющиеся в том, что в списке следственных действий не указан целый ряд нужных для успешной работы процессуальных ин-

струментов, которые бы охватывали своими определениями и рамками именно работу с удаленными системами и сетями для получения компьютерной информации.

Опрошенные эксперты считают, что такая правовая норма необходима при расследовании преступлений с использованием компьютеров, касающихся шифрования информации. Так как у информации в компьютере нет строгой связи с физическим носителем и ее можно без труда изменить, уничтожить или зашифровать, умные преступники часто прибегают к подобным методам, чтобы в случае опасности уничтожить улики, скрыть их от следствия. Тем, кто хочет уделять внимание средствам конспирации и сокрытия, не нужно даже обязательно быть профессиональными программистами. Существуют достаточно большое количество специализированных программных продуктов, вроде TrueCrypt, которые позволяют зашифровать данные даже без особых профессиональных познаний. Получить доступ к зашифрованным данным, даже если компьютер изъят, может быть затруднительно из-за необходимости использования пароля или иного криптографического ключа. Как правило, если преступник подошел к своей деятельности организованно и осторожно, у следствия доступа к таким ключам нет.

Поэтому часто для обхода подобной защиты часто используется другой способ, который заключается в удаленном подключении прямо во время работы компьютера. На сегодняшний момент, чтобы реализовать этот метод, необходимо прямое поручение от следователя на проведение оперативно-розыскных действий.

По этой причине, в ответ на просьбу назвать главные задачи IT-специалиста при следственных и оперативно-розыскных действиях, 64 % опрошенных назвали «обеспечение доступа к значимым для расследования компьютерным данным, которые могут быть зашифрованы.

Проведение анализа различных уголовных дел с учетом результатов проведенных опросов сотрудников оперативных и следственных органов позволяет прийти к выводу, что привлечение к следствию лиц со специальными, экспертными познаниями в информационной сфере и компьютерах — важная часть еще планирования и подготовки будущих следственных мероприятий. При поставленной цели получения не только цифровых улик и их фиксации, но и компетентного объяснения меры доступности, точности и надежности полученных доказательств, а также требований к сохранению их в целостности. Но если обобщить полученные результаты опросов, то окажется, что наиболее частой и при этом важной ошибкой является поверхностный, формализованный подход к подготовке следственных мероприятий и оперативно-розыскных действий, либо вообще отсутствие таковой, хотя все респонденты признают, что она значима и необходима.

Это подтверждается их ответом на вопрос об идеальном следственном мероприятии с их участием. Ключевым признаком такового они назвали именно наличие хорошей подготовки.

Личные беседы с участниками опросов затронули и различные показательные примеры, имевшие место в их практике. На их основании можно прийти к выводу, что подготовка часто проводится в общих чертах, без учета специфики компьютерной преступности. Как пример приводят случай, когда место для обыска было выбрано ошибочно: квартиру или офис установили как место совершения преступления, ориентируясь на входящий канал провайдера на основании признаков противоправной активности в соответствующем сетевом трафике. При этом не была рассмотрена версия, что доступ к WiFi был скомпрометирован, что можно было сделать и извне данного помещения — из соседней жилой или рабочей комнаты, например.

Также часто не хватает предварительного брифинга с инструктажем для всех участников запланированных оперативно-розыскных мероприятий. Во многих ситуация это приводит к утере ключевых для расследования данных непосредственно при проведении обыска из-за незнания или плохой подготовки к подобным мероприятиям сотрудников. Не имеющие опыта работы в IT-сфере или расследования преступлений с использованием компьютеров, сотрудники оперативных и следственных органов не имеют полного представления и понимания легкости и способов, с помощью которых подозреваемые могут избавляться от компрометирующей информации. Порой достаточно захлопнуть крышку ноутбука или выдернуть из электросети кабель персонального компьютера. Все это указывает на недостаток знаний и подготовки в области компьютеров.

Утратить компьютерную информацию можно намного быстрее и с куда большим риском, нежели более традиционные виды улик. Поэтому осмотром техники должны заниматься, в первую очередь, специалисты, а также обученные необходимым мерам предосторожности сотрудники [3].

Для наглядности рассмотрим в качестве примера одну из ситуаций, описанных в ходе опроса одним из

респондентов в личном порядке. Предстояло провести обыск в офисе. В нем рабочие места были компьютеризированы и использовались участниками организованной преступной группы. Их криминальная деятельность была связана с компьютерной информацией. Следователь, ответственный за ведение дела, разработал план обыска помещения с осмотром, изъятием и изучением найденных улик. Первыми по очереди на исследование рабочих мест были поставлены криминалисты, чтобы они могли обнаружить отпечатки пальцев, потожировые следы, генетический материал. Лишь после них к работе допускались IT-специалисты. Но они не учли, что для дактилоскопии — снятия отпечатков пальцев — используется специальный порошок и магнитная кисть. Встроенные в ноутбук датчики закрытия крышки отреагировали на контакт с ней, и оперативная система инициировала переход в энергосберегающий режим. Фактически, ноутбук выключился, и после включения обратно доступ к программам и данным был уже заблокирован. Это наглядно демонстрирует, как специалист по криминалистике, не зная особенностей компьютерной техники и собственного инструментария, по неосторожности многократно усложнил получение улик другими специалистами.

Этого можно было бы избежать, если бы к подготовке подошли более тщательно, всем участникам разъяснили бы особенности работы с цифровыми устройствами, изменили очередность и в полной мере проконсультировались у специалистов. Чувствительность приборов к магнитным полям — широко известный факт, и для того, чтобы не совершить ошибку, достаточно было бы правильно организовать подготовительный этап.

Есть и другие проблемы, выявленные в ходе этих опросов специалистов. Они связаны с законодательством или, скорее, его интерпретацией. Дело в том, что оно требует привлекать специалистов для поиска и изъятия цифровых следов. При этом большинство сотрудников следственных и оперативно-розыскных органов признались, что обычно исполняли это требование, пользуясь лазейкой в определении, используя в качестве «специалиста» сотрудника другой сферы — например, того же криминалиста. Или же специалиста в сфере компьютерной техники, но стороннего сотрудника вообще. Хотя закон не говорит об этом напрямую, подразумевается, что изымать, копировать и проводить другие манипуляции с электронными носителями информации также должны соответствующие специалисты. Как правило, следователи, оперативные сотрудники не совсем понимают, каким компетенциям согласно этому закону должны соответствовать специалисты, какую конкретную область в широкой информационной сфере должен знать и понимать нужный им человек. В отличие от них, сами специалисты при опросе объяснили, что требования к знаниям используемых экспертов при поиске цифровых улик очень широкие. Они должны разбираться и в программировании, и в конструкции устройств, и в сетевых структурах и их взаимодействии и т. д. Либо же приходится привлекать помощь сразу несколько специалистов, обладающих узкоспециализированными, но глубокими познаниями в своих соответствующих областях IT-технологий. Но чтобы это сделать, организующий соответствующие мероприятия следователь сам должен, в первую очередь, иметь представление, какая помощь ему понадобится, с чем предстоит иметь дело и, соответственно, какие методы, знания, технические средства требуются от привлекаемого к делу специалиста.

Другая проблема — трудности, связанные с поиском и выявлением источника важных для расследования данных. Они возникают при изучении крупных компьютерных сетей. Как правило, их функционирование приостановить не представляется возможным из-за их критической важности для производственных процессов, которые идут непрерывно. Более того, изъять их целиком с места преступления, как правило, технически невозможно, и даже если бы это можно было как-то осуществить, огромные объемы подлежащей изучению информации делали бы это нецелесообразным. В такой ситуации следует выявить конкретные устройства в сети с нужной информацией, локализовать их и исследовать отдельно. При этом следователи не обладают нужными знаниями — за исключением сотрудников специализированных подразделений — не смогли дать точных критериев и определений того, как объекты нужно искать, какие процессы в системах отслеживать для выполнения такой задачи.

Результаты исследования показывают, что очень часто отсутствуют даже самых основные понятия о работе и конструкции современных компьютеров и соединяющих их сетях. Это негативно влияет на качество и успешность раскрытия связанных с информационными технологиями преступлений, а также преступлений, совершенных с их помощью. В большинстве случаев это прямо или косвенно ведет к потере ценных улик, не подлежащих восстановлению.

Разумеется, само значение привлечения экспертной помощи заключается в том, чтобы они, за счет своих компетенций, могли компенсировать недоста-

ток знаний и навыков следователя, помогли ему выявить улики, зафиксировать цифровых следы, исследовать их. Но это не значит, что минимальная компьютерная грамотность не нужна для сотрудников правоохранительных органов. Чтобы осознать необходимость помощи специалистов, обратиться к ним в соответствии с компетенциями, которые пригодятся в данном конкретном расследовании и наиболее эффективно воспользоваться их услугами, нужно информационное образование.

Другая проблема, связанная с плохой подготовкой к проведению оперативно-розыскных мероприятий относительно преступлений в области компьютерных технологий — материальное обеспечение и оплата труда привлекаемых специалистов. Изъятие информационных улик часто требует использовать специализированную компьютерную технику. Особенно это касается случаев, когда изъятие компьютерной системы со всеми уликами невозможно и приходится создавать ее дубликат.

Более того, удостовериться в компетенциях специалиста до начала работы и нанесения возможного ущерба невозможно, если сам следователь не имеет хотя бы базовых представлений об области, в которой ему нужна помощь. Опрошенные эксперты объяснили, что ввиду многообразия ситуаций и постоянного быстрого развития технологий, составить исчерпывающий и при этом стабильный перечень требуемых компетенций и используемых средств невозможно. Можно лишь выделить обязательный минимум, который, впрочем, часто все равно будет недостаточным:

♦ программы для снимка оперативной памяти, вроде ProcDump;

♦ устройства чтения содержимого файловой системы без внесения изменений;

♦ блокираторы копирования жесткого диска, защищающие его от изменений.

На основе этого исследования можно прийти к следующим выводам о ключевых проблемах при использовании компьютерных технологий при ведении расследования:

♦ недостаточные или отсутствующие подготовительные мероприятия;

♦ невозможность полноценно оценивать компетенции привлекаемых специалистов;

♦ утрата компьютерной информации из-за неправильной очередности использования криминалистических методов;

♦ формализация подхода к организации следственных и оперативно-розыскных действий;

♦ отсутствие у сотрудников следствия и оперативного розыска необходимых минимальных познаний в IT-сфере.

Это все указывает, что тема компьютерного обеспечения криминалистической деятельности слабо разработана, что ведет к отсутствию организованного системного подхода при поиске цифровых улик. Лишь развивая криминалистическую науку и процессуальные нормы в этом направлении можно добиться более оптимизированного подхода к раскрытию компьютерных преступлений.

Список источников

1. Федеральная служба государственной статистики // URL://http://www.gks.ru/wps/wcm/connect/rosstat_main/rosstat/ru/statistics/population/level/#.

2. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ // СЗ РФ. 2022. № 41. Ст. 6946.

3. Семикаленова А. И. Использование специальных знаний при обнаружении и фиксации цифровых следов // Юридические науки. 2020. № 6. С. 34.

References

1. Federal State Statistics Service // URL://http://www.gks.ru/wps/wcm/connect/rosstat_main/rosstat/ru/statistics/population/level/#.

2. The Criminal Procedure Code of the Russian Federation No. 174-FZ of December 18, 2001 // CL RF. 2022. No. 41. Art. 6946.

3. Semikalenova A. I. The use of special knowledge in the detection and fixation of digital traces // Legal Sciences. 2020. No. 6. P. 34.

Информация об авторе

Е. А. Виноградов — соискатель факультета подготовки научно-педагогических кадров по кафедре оперативно-розыскной деятельности и специальной техники Московского университета МВД России имени В.Я. Кикотя.

Information about the author

E. A. Vinogradov — Candidate of the Faculty of Training of Scientific and Pedagogical Personnel in the Department of Operational Investigative Activities and Special Equipment of the Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot'.

Статья поступила в редакцию 25.05.2023; одобрена после рецензирования 12.07.2023; принята к публикации 11.09.2023.
The article was submitted 25.05.2023; approved after reviewing 12.07.2023; accepted for publication 11.09.2023.