УДК 343.98

О.Ю. Зеленкина

ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

В статье рассматриваются особенности расследования преступлений в сфере компьютерной информации. Раскрывается понятие преступлений в сфере компьютерной информации, дается характеристика состояния преступности в данной сфере. Рассматриваются некоторые элементы криминалистической характеристики: личность преступника, типичная обстановка, личность потерпевшего, способ совершения преступления. Уделено внимание характеристике следов преступления. Кроме этого, дается классификация типичных следственных ситуаций. Приводится алгоритм производства отдельных следственных действий, наиболее характерных для данной категории дел и указывается их специфика. Предлагаются практические рекомендации по производству следственных действий, позволяющие не допустить уничтожения или сокрытия следов преступления. Отмечается необходимость участия специалиста при производстве следственных действий. Сформированы предложения по использованию новых форм специальных знаний при производстве расследования.

Ключевые слова: расследование преступлений, компьютерная информация, криминалистическая характеристика, следы преступления.

O.Y. Zelenkina

SPECIFIC FEATURES OF INVESTIGATING CRIMES IN THE SPHERE OF COMPUTER INFORMATION

The article is devoted to specific features of investigating crimes in the sphere of computer information. The concept of such a crime is described and the criminal situation is this area is examined. The author analyzes some elements of criminalistic characteristic: the personality of the criminal, typical conditions, the personality of the victim, means of committing a crime. Special attention is paid to characterizing the traces of crime. Besides, the author gives a classification of typical investigation situations, presents the algorithm of performing specific investigation actions most typical of this category of cases and points out their specific features. The author also offers practical recommendations on performing investigation actions that prevent the destruction or hiding of traces of crime. The necessity of involving a specialist in investigation actions is stressed. The author presents suggestions on using new types of special knowledge in the process of investigation.

Keywords: investigation of crimes, computer information, criminalistic characteristic, traces of crime

В последние десятилетия информация стала неотъемлемой частью таких важных сфер деятельности государства, как связь, транспорт, энергетика, добыча и хранение стратегически важных ресурсов, банковская система, системы жизнеобеспечения населения, оборона, структуры обеспечения устойчивой работы государственного аппарата, что закономерно привело к проникновению преступности в сферу компьютерной информации. Возможность совершать противоправные действия, находясь на значительном удалении от места совершения преступления, оставаясь при этом не только не замеченным, но и не обнаруженным впоследствии привлекает все больше преступников.

Под преступлениями в сфере компьютерной информации мы понимаем виновно совершенное общественно опасное деяние, совершенное в сфере информационных технологий путем воздействия на сведения (сообщения, данные), представленные в электронно-цифровой форме, независимо от средств их хранения, обработки и передачи. Традиционно, к числу преступлений рассматриваемой категории относят, прежде всего, составы 28 главы Уголовного кодекса. Однако они часто являются лишь способом совершения других преступлений. Так, по статистике МВД[1] о состоянии преступности за 2018 год, 8,4% всех зарегистрированных преступлений за отчетный период совершены с использованием компьютерных и телекоммуникационных технологий.

[1]Состояние преступности в России за январь-ноябрь 2018 года Министерство Внутренних дел Российской Федерации ФКУ «Главный информационно-аналитический центр» [Электронный ресурс] // URL: https://мвд.рф;

Общее количество зарегистрированных преступлений в сфере высоких технологий с каждым годом возрастает, при этом раскрываемость преступлений остается на крайне низком уровне. По данным МВД на 2017 год зарегистрировано 90587 таких преступлений, из них раскрыто 20424. За 2018 год зарегистрировано уже 156307 преступлений, из них раскрыто только 38773. Основными причинами, на наш взгляд, является недостаточность специальных знаний следователей, отсутствие видимых материальных следов преступлений, а так же обезличенный характер информации, не позволяющий указать на преступника. В сложившейся ситуации, особое внимание правоохранительных органов должно быть сосредоточено на уточнении и повышении эффективности применения частной методики расследования преступлений в сфере компьютерной информации.

Одной из наиболее значимых структурных частей в системе частной криминалистической методики обоснованно считают криминалистическую характеристику преступления. Рассмотрим некоторые элементы, входящие в вышеназванную характеристику.

Криминалистическая характеристика личности преступника дается в научной литературе достаточно подробно, однако, она не в полной мере соответствуют действительности, поскольку статистика исходит только из тех случаев, которые удалось раскрыть [1; 2]. Достаточно высокая степень сложности современной компьютерной техники и программных средств ее защиты, предполагает высокий образовательный уровень преступников и нетривиальное мышление. К примеру, если рассматривать преступления против безопасности критической инфраструктуры Российской Федерации, то в силу высокой степени защиты объектов, круг профессионалов соответствующего класса даже на сегодняшний день не велик. Следует особо обратить внимание, что субъектом данного состава в соответствии с положениями уголовного закона может выступать иностранный гражданин, совершивший преступление вне пределов Российской Федерации.

Обобщая информацию из различных источников, можно предположить, что типичный преступник - молодой человек, имеющий среднее - специальное или высшее образование, преимущественно техническое. Поскольку под данное описание на сегодняшний день попадет каждый второй представитель молодого поколения, считаем разумным обращать большее внимание на психологические аспекты характеристики личности. Будущий преступник, скорее всего, начал увлекаться программированием еще в школьные годы. В этом возрасте молодые люди, имея ряд комплексов и проблемы с общением или столкнувшись с непониманием со стороны окружающих, активно ищут пути самовыражения в виртуальном пространстве. Постепенно происходит психологическая трансформация, выраженная в подмене реальности, компьютерная сеть становится средой обитания. Таким образом, мотивами совершения противоправных действий в информационном пространстве могут быть и такие, как месть, желание самоутвердиться, сделать вызов обществу и т.п.

Потерпевшим в свою очередь может выступать как физическое, так и юридическое лицо, в том числе государственные органы и государство в целом.

В качестве типичных предметов посягательств можно рассматривать электронные базы данных, серверы коммерческих организаций, государственных органов и учреждений, в том числе объектов критической информационной инфраструктуры РФ, банковские карты, электронные почтовые ящики, страницы в социальных сетях.

Как известно, обстановка преступления традиционно рассматривается как система условий места и времени, с находящимися в них людьми, материальными предметами, в которых совершается уголовно наказуемое деяние. Данные преступления происходят в специфической среде — виртуальном кибернетическом пространстве, где в одном преступлении одновременно могут быть задействованы множество территориально удаленных друг от друга компьютеров. Каждое из мест нахождения электронного устройства имеет свою обстановку. Для характеристики времени совершения преступления используется астрономическое время, то есть определенная временная точка и продолжительность осуществления способа посягательства от его начала до окончания в виде наступления общественно опасных последствий. Работа некоторых программ непосредственно связана со временем, установленным на компьютере вручную и не всегда соответствующим действительности. Неправомерные действия часто происходит ночью в связи с уменьшением нагрузки на каналы связи и возможностью быть незамеченным сразу. На обстановку оказывают влияние и состояние средств защиты объекта преступления. Судебно-следственная практика показала, что в большинстве случаев преступники самостоятельно создают условия совершения преступления. Так, могут создаваться компьютерные вирусы и специальные программы взлома, направленные на снижение уровня защиты. Обстановка является динамичной категорией. Даже опытный киберпреступник не всегда способен верно оценить ее изменения как благоприятные или неблагоприятные. В результате поспешных или ошибочных действий остаются следы преступления, которые в большинстве случаев являются единственной возможностью восстановить механизм совершения преступления.

Следы такого типа не вписывается в общую теорию трасологии, поэтому учеными-криминалистами была предпринята попытка определения их понятия и сущности. К единому мнению относительно этой категории исследователи не пришли до сих пор, поэтому в литературе можно встретить понятия «бинарные следы» [3], «виртуальные следы» [4, с. 52]. В.Б. Вехов предлагает понятие «электронно-цифровой след», под которым понимает любую криминалистически значимую компьютерную информацию, то есть сведения, находящиеся в электронно-цифровой форме, зафиксированные на материальном носителе либо передающиеся по каналам связи посредством электромагнитных сигналов [5, с. 30].

Практически все следы можно условно разделить на следующие категории:

1) следы, которые создаются в технических средствах пользователя;
2) следы прохождения информации по самим техническим каналам связи;

3) на носителях компьютерной информации, где непосредственно наступил результат неправомерного доступа.

Для сокрытия указанных следов преступники широко применяют последние достижения в области шифрования информации, специальные программно-аппаратные средства для уничтожения значимой для следствия информации при попытке доступа к ней третьих лиц. Такие защитные средства могут быть приобретены у компьютерных фирм или созданы преступником самостоятельно, что значительно осложняет их нейтрализацию.

Несмотря на специфику совершаемых действий, в некоторых случаях, могут быть вполне реальные непосредственные гомеоскопические следы - отпечатки рук на технике, используемой преступником (отпечатки пальцев на экране планшетных компьютеров или на стандартных средствах ввода информации), следы биологического происхождения. В этом случае совокупность бинарных и материальных следов значительно облегчает процесс доказывания.

В юридической литературе существует множество классификаций способов совершения преступлений в сфере компьютерной информации. Однако, на наш взгляд, ни одна из них не является исчерпывающей. Это объясняется, во-первых многообразием составов, во-вторых стремительным развитием информационной сферы. В целом, можно согласиться с классификацией, представленной Д.С. Будаковским. К первой группе способов можно отнести способы непосредственного воздействия на компьютерную информацию, ко второй - способы опосредованного (удаленного) воздействия на компьютерную информацию [6]. Среди наиболее часто встречающихся способов можно назвать: распространение вредоносных программ, подбор нужного пароля, в том числе с использованием специальных программ автоматического подбора, получение паролей доступа обманным путем, подключение к линии связи законного пользователя и получение тем самым доступа к его системе, использование различных программных средств специального назначения, направленных, к примеру, на восстановление удаленных файлов.

На первоначальном этапе расследования преступлений в сфере компьютерной информации чаще всего встречаются следующие следственные ситуации, классифицируемые по субъекту выявления преступления:

1. Собственник компьютерной информации обнаружил факт преступления и самостоятельно выявил преступника.

2. Собственник компьютерной информации обнаружил факт преступления, но преступник остается невыявленным.

3. Преступление выявлено правоохранительными органами.

Роль и значение следственных ситуаций определяется тем, что они выступают в качестве основы для построения общих и частных криминалистических версий. Их содержание в первую очередь зависит от этапа расследования и объема данных, которыми располагает следователь в конкретный момент времени.

Рассмотрим вопросы производства отдельных следственных действий, наиболее характерных для данной категории дел.

На первоначальном этапе, прежде всего, следует провести осмотр места происшествия с целью выявления и фиксации данных, позволяющих сделать вывод об обстоятельствах, имеющих значение для уголовного дела, а именно о наличии виртуальных следов, трасологических следов, особенностей доступа, организации, функционирования и устройства различных видов сетей.

По прибытии на место происшествия, следователь должен обеспечить неприкосновенность предполагаемых носителей следов преступления, т.е. исключить до окончания следственного действия контакт потерпевшего и иных лиц с электронными устройствами и каналами связи, общение и выход за пределы осматриваемой территории (помещения) всех присутствующих лиц. Не стоит пытаться самостоятельно проводить какие бы то ни было манипуляции с техникой, если результат заранее не известен. Дополнительно следует произвести осмотр любой документации, находящейся непосредственно рядом с осматриваемым устройством.

Следователь также определяет круг лиц, имевших доступ к определенным устройствам, и обеспечивает добровольную выдачу потерпевшим паролей и кодов доступа до начала производства осмотра [7, с. 149]. На практике могут встречаться случаи препятствования потерпевшего активными или пассивными действиями ходу расследования с целью сокрытия обстоятельств преступления, например, в случае опасений по привлечению его самого к ответственности [8, с. 23].

Уголовно-процессуальный кодекс в настоящее время не предусматривает участия специалиста по компьютерной технике в осмотре места преступления в обязательном порядке, однако требует его участия в других случаях изъятия электронных носителей информации. Например, в ходе производства обыска. Поскольку осмотр места происшествия чаще всего сопровождается изъятием электронных носителей информации, считаем целесообразным привлекать специалиста и к осмотру. Каким бы уровнем компьютерных знаний следователь не обладал, скорее всего, их будет недостаточно для обнаружения искомой информации, безошибочного изъятия следов преступления и обеспечения сохранности доказательств. Так же необходимо позаботиться об участии понятых. Исходя из общих принципов уголовного судопроизводства, они должны обладать некоторым объемом знаний, достаточным для понимания сути проводимого следственного действия. Если по объективным причинам это невозможно, ход следственного действия в таком случае может фиксироваться с помощью технических средств. Кроме этого, следователь должен заблаговременно подготовить специализированные средства для изъятия виртуальных следов путем копирования – портативные криминалистические накопители, стандартные паспортизированные программы, предназначенные для копирования данных, с соответствующим документальным приложением, блокаторы записи, позволяющие предотвратить случайное или преднамеренное внесение изменений в данных, мобильную лабораторию [9]. По ходатайству законного владельца изымаемых электронных носителей информации или обладателя содержащейся на них информации специалист осуществляет копирование изымаемых электронных носителей информации на другие

электронные носители информации. Если специалист сделает вывод о том, что копирование информации может повлечь утрату или изменение информации или иным образом может негативно отразиться на ходе расследования, копирование информации не допускается.

При отсутствии возможности проанализировать относимость доказательств к данному делу ввиду большого объема информации, отсутствии доступа или потенциальной опасности копирования информации, следователь вправе изъять электронное устройство, его часть, непосредственно содержащую информацию, а так же несколько устройств, если они соединены между собой. При этом необходимо корректно завершить работу в строго определенной последовательности. Каждый этап осмотра должен фиксироваться в протоколе. Изъятые электронные устройства должны быть упакованы должным образом, исключающим попадание влаги и механические повреждения, опечатаны и заверены подписями следователя и понятых при их наличии на месте проведения осмотра. Подписывать упаковку нужно перед помещением в нее электронного носителя во избежание повреждения надписью.

Если в результате произведенных следственных действий появились достаточные данные, дающие основание подозревать лицо в совершении преступного деяния, при наличии предусмотренных законом оснований и мотивов, может быть произведено задержание. Традиционно, сущность задержания с позиций криминалистики заключается в выполнении комплекса действий, составляющих тактическую операцию: физический захват подозреваемого, неотложное производство личного обыска, конвоирование и доставление задержанного в соответствующий орган предварительного следствия. Ситуация часто осложняется фактом нахождения подозреваемого за пределами Российской Федерации.

В связи с частым отсутствием прямых доказательств по делу, при производстве допроса необходимо уделить особое внимание сбору данных о личности допрашиваемого, что позволит правильно определить наиболее эффективные тактические приемы проведения допроса, способствующие установлению психологического контакта с допрашиваемым и преодолению позиции, направленной на дачу ложных показаний. Поскольку сфера деятельности предполагаемого преступника достаточно сложна и плохо известна следователю, допрашиваемый достаточно легко может ввести его в заблуждение. Во избежание такой ситуации следователь должен обратиться за консультацией к специалисту, а при необходимости обеспечить его участие в допросе. Именно специалист поможет определить относимость информации к расследуемому событию. Главной проблемой фиксации показаний по делам данного вида является значительный объем специальной терминологии. Целесообразно в протоколах более подробно фиксировать значения терминов, используемых допрашиваемым, дополнять протокол различными схемами, ключами языков программирования и т.п.

При наличии достаточных оснований полагать, что оборудование или иные средства совершения преступления могут находиться в определенном месте или у определенного лица следователем может быть принято решение о

производстве обыска. Отметим, что при производстве указанного следственного действия в целом следует руководствоваться теми же рекомендациями, что и при осмотре места происшествия. Не стоит забывать о возможностях сбора традиционных доказательств, например, невидимых следов пальцев на устройствах ввода информации и корпусе техники.

Заключение судебной компьютерно-технической экспертизы может сыграть определяющую роль при производстве расследования [10]. Однако при назначении столь важного следственного действия на практике сотрудники сталкиваются с целым рядом проблем, имеющим, в сущности, две причины. Первая заключается в недостаточном уровне не только узкоспециальных, но и общих знаний следователей в области компьютерной информации, что приводит к постановке некорректных вопросов эксперту, а значит и к ответам, отражающим этот факт, но не вносящим никакой ясности в существо проблемы. Выходом из ситуации опять может стать консультирование со специалистом для постановки вопросов, входящих в его компетенцию. Вторая связана с недостаточным количеством экспертных учреждений, способных выполнить различные виды экспертиз такого профиля.

На наш взгляд, еще одной формой применения специальных знаний в рамках расследования преступлений в сфере компьютерной информации может стать использование единого специального криминалистического учета, в котором бы содержались ключи шифрования, данные о программно-техническом обеспечении и другая информация. Создание подобного учета может существенно облегчить процесс расследования, процесс сбора и анализа статистических данных, поскольку, по нашему мнению, программно-технические средства, создаваемые преступником самостоятельно, являются плодом высокоинтеллектуальной деятельности и практически также уникальны как отпечатки пальцев.

Подводя итог, следует сказать, что компьютерная информация, используемая в преступных целях, таит в себе огромную потенциальную угрозу для личности, общества и государства, в виду непредсказуемости последствий, что в свою очередь ставит перед правоохранителями задачу разработать эффективный механизм не только расследования таких преступлений, но и их предотвращения.

Список использованной литературы

1. Потапов С.А. Совершенствование расследования и раскрытия преступлений в сфере компьютерной информации // Социально-экономические явления и процессы. – 2016. – Т. 11. № 10. – С. 90–95.

2. Ефремов К.А. Личность преступника, совершающего преступления в сфере компьютерной информации // Общество: политика, экономика, право. – 2016. – № 6. – С. 92–95.

3. Милашев В.А. Проблемы тактики поиска, фиксации и изъятия следов при неправомерном доступе к компьютерной информации в сетях ЭВМ : автореф. дис. ... канд. юрид. наук. – М., 2004. – 22 с.

4. Шеметов А.К. О понятии виртуальных следов в криминалистике // Российский следователь. – 2014. – № 20. – С. 52–54.

5. Вехов В.Б. Криминалистическое учение о компьютерной информации и средствах ее обработки : автореф. дис. … д-ра юрид. наук. – Волгоград, 2008. – 45 с.

6. Будаковский Д.С. Способы совершения преступлений в сфере компьютерной информации // Российский следователь. – 2011. – № 4. – С. 2–4.

7. Коломинов В.В. Осмотр места происшествия по делам в сфере компьютерной информации // Сибирские уголовно-правовые и криминалистические чтения. – 2017. – №3. – С.145–149.

8. Поляков В.В. Анализ факторов, затрудняющих расследование неправомерного удаленного доступа к компьютерной информации // Проблемы правовой и технической защиты информации: сб. науч. ст. – Барнаул : Изд-во Алт. ун-та, 2008. – С.17–24.

9. Электронные носители информации в криминалистике: монография / под ред. О.С. Кучина. – М. : Юрлитинформ, 2017. – 304 с.

10. Развитие информационных технологий в уголовном судопроизводстве: монография / под ред. С.В. Зуева. – М. : Юрлитинформа, 2018. – 248 с.

Информация об авторе

Зеленкина Ольга Юрьевна – студент, Институт государства и права, Тюменский государственный университет, 625003, г. Тюмень, ул. Ленина, 38; e-mail: o.zelenkina97@gmail.com.

Information about the author

Zelenkina, Olga Yu. – Student, Institute of State and Law, Tyumen State University, 38 Lenin st., Tyumen, 625003; e-mail: o.zelenkina97@gmail.com.