УДК 343.98
Базаров А.А.
Базаров Андрей Андреевич (xoocki@yandex.ru)студент, бакалавр 4 курса, Юго-Западный государственный университет, г. Курск

ВИРТУАЛЬНЫЕ СЛЕДЫ В КРИМИНАЛИСТИКЕ

В рамках данной статьи автором были рассмотрены проблемные вопросы, связанные с определением понятия виртуальных следов и возможностями их исследования и использования в криминалистической теории и практике. Отдельно автором рассмотрены различные варианты классификации виртуальных следов.

Ключевые слова: криминалистика, виртуальные следы, компьютерные преступления, расследование киберпреступлений.

За последние годы в России было совершенно десятки тысяч преступлений в сфере телекоммуникационной и компьютерной информации. Только за 2017 год таких преступлений зарегистрировано более одиннадцати тысяч. Преступники сегодня все более активно используют информационные технологии для достижения криминальных целей. При этом характер преступности меняется с каждым годом не только в количественном, но и качественном плане.

Информационные технологии - неотъемлемая часть современного общества. Телекоммуникационная сфера настолько тесно сплелась с реальной жизнью людей, что современное общество невозможно без нее представить. Например, интернет просочился буквально во все сферы жизнедеятельности человека [1].

Использование информационных технологий, повышение ценности информации влечет не только качественное улучшение общественной жизни, но появление новых преступлений, создающих трудности в использовании разнообразных информационных сервисов для быстрого решения тех или иных задач в повседневно-деловой сфере каждого человека. Новые технологии влияют не только на хранение и использование информации, они так же выступают способом получения такой информации. Преступники активно используют вирусы и троянские программы для хищения информации других лиц или безналичных денежных средств с лицевых и банковских счетов. Они, используя имеющиеся технологии и возможности, совершают «атаки» на других пользователей в целях дестабилизации их деятельности или полной ее уничтожения. Уголовное законодательство отдельно выделило такие преступления как мошенничество с использованием информационных технологий, платежных карт, в сфере страхования или компьютерной информации и ряда других преступлений, непосредственно связанных с информационной деятельностью и использованием вычислительной техники. Однако данные способы совершения преступлений характерны не только для составов прямо на это указывающих, но и огромное множество других деяний, подпадающих не только под деятельность статей Уголовного кодекса.

Подготовка и совершение преступления всегда порождает возникновения определенных следов в материальном мире, изучая которые следователь, дознаватель могут решать общие и частные задачи расследования. Аналогичным образом происходит и в рамках виртуального пространства, где злоумышленник, используя информационные технологии оставляет особый вид следов, которые в науке принято называть «виртуальными следами».

Признаки преступлений в сфере информационных технологий в большинстве случаев, в материальном виде не существуют. Они находят свое отражение в телекоммуникационных или компьютерных сетях. Такие виртуальные следы могут иметь доказательственное значение при исследовании закономерности приготовления, совершения и раскрытия преступлений.

В теории криминалистики существуют различные мнения о том, что следует понимать под виртуальными следами: 1) виртуальные следы, как изменение автоматизированной информационной системы [2] 2) виртуальные следы, с точки зрения физической и квантовой теории [1] 3) виртуальные следы как результат логических и математических операций с двоичным кодом [4] и многие другие. До сих пор нет точного определения виртуальных следов. Различные авторы рассматривают поставленный вопрос с различных точек зрения: одни с точки зрения влияния человека на компьютерные системы [3], другие с точки зрения физических связей компьютерных систем, третьи, с точки зрения осуществления определенных операций.

Масштабное исследование по вопросу определения сущности и понятия виртуальных следов провела известный российский процессуалист и специалист в области криминалистики и судебной экспертизы Е. Р. Россинская [5]. По ее мнению, виртуальные следы являются исключительно материальными следами, так как были зафиксированы на материальных носителях путём изменения свойств или состояния отдельных их элементов и отмечает, что данный вид информации не отделим от материального носителя, поэтому к материалам дела приобщается именно носитель [5]. Данную точку зрения трудно назвать верной. Например, энергозависимая память, о существовании которой говорит сам автор [5], компьютерной системы или по-другому оперативное запоминающее устройство (далее ОЗУ) выполняет лишь функцию временного хранилища данных, промежуточного хранилища и в случае прекращения подачи питания на данный тип памяти, вся информация, а это основные данные работы программных средств в которых могут находится определенные следы, фактически подтверждающие действия преступника, полностью уничтожается. Исходя из выше сказанного получается, что на ОЗУ в рамках компьютерных систем ничего не фиксируется на постоянной основе, а лишь носит временный характер. Продолжая говорить о энергозависимой памяти так же стоит вспомнить о таком значимом виде, как память BIOS (*с англ.* базовая система ввода вывода). Широко известно, что данный тип памяти, в котором сохраняются абсолютно все действия с аппаратного обеспечения компьютерной системы, работает в современных персональных компьютерах с использованием батареи или встроенного аккумулятора и отключение которых приведет к полному стиранию всех записей о событиях в хронологическом порядке (файл регистрации или *англ*. log) и настроек пользователя, которые хранились в данном типе памяти. А ведь данные записи позволят подтвердить или опровергнуть факт включения или выключения компьютерной системы, использования того или иного подключенного оборудования. К такому типу памяти может и отнестись кеш – промежуточный буфер с быстрым доступом, который активно используется в центральных процессорах, внешних накопителях для увеличения скорости работы компьютера. Поэтому уже сейчас можно с уверенностью признать несостоятельность предположения о необходимости постоянной привязки виртуальных следов, электронной информации к материальным носителям.

Так же является спорным мнение Россинской Е.Р. о неотделимости виртуальных следов от её носителей. Сегодня, активно развиваются «облачные технологии» в рамках которых, пользователь может хранить свои данные и информацию за пределами своего собственного персонального компьютера или компьютерной системы. Для её максимальной сохранности технологические компании располагают её на разных устройствах хранения. Это позволяет, в случае выхода одного из устройств хранения с пользовательской информацией из строя, в кратчайшие сроки его восстановить, а также информацию, которая находилась на нем. Для пользователя данный процесс абсолютно не заметен. Так же возможно экстренное сохранение информации на различные физические носители компьютерной информации. Исходя из этого возникает вопрос, если виртуальные следы, представленные в рамках определенного вида компьютерной информации, являются неотделимыми от их носителя, тогда в случае расследования преступления связанных с этими данными, следователям необходимо изымать все

носители, на которых хранится данная информация. А их число может достигать не просто десятков, но и сотен хранилищ информации. Поэтому рациональным стоит поставить вопрос о разработке и использовании программного обеспечения для изъятия виртуальных следов с физических носителей информации без их изъятия.

Анализируя различные точки зрения относительно понятия виртуальных следов, с учетом юридических и технических аспектов данного вопроса, по нашему мнению, под виртуальными следами следует понимать – определенные сведения, представленные в виде машинного кода или человекочитаемой информации, которые были зафиксированы ЭВМ или человеком на физическом, логическом, синтаксическом, семантическом и прагматическом уровнях, и могут представлять определенную ценность при исследовании закономерности приготовления, совершения и раскрытия преступлений.

Уяснив, что же понимается под виртуальными следами, стоить помнить, что компьютерные сети представляют собой сложные системы взаимодействия различного технического оборудования, в рамках которого возникает огромное многообразие виртуальных следов.

Можно выработать определенную классификацию виртуальных следов: 1) *по происхождению:* 1) электронная информация, созданная ЭВМ в процессе своей работы; 2) электронная информация, созданная в процессе деятельности человека; 3) производная электронная информация, созданная компьютером на основе введенных данных пользователем или наоборот, информация, созданная из данных, сгенерированных компьютерной системой; *по форме представления:* 1) человекочитаемая информация (информация, доступная для восприятия человеком); 2) машиночитаемая информация (информация, представленная в виде машинного кода); *по месту хранения:* 1) данные, хранящиеся в компьютерных системах (ЭВМ, серверы, локальные сети, глобальные сети); 2) данные, скопированные или перемещенные пользователем на электронные носители (жесткие диски, флоппи диски, компакт-диски, стримеры, твердотельные накопители); 3) бумажные копии человекочитаемой или машиночитаемой информации (копии переписок, скриншоты, примеры программного года и др.); *по форме*: 1) исходные данные (информация, введенная человеком); 2) человекочитаемые и машиночитаемые базы данных; 3) коды шифрования; 4) программное обеспечение различных видов; 5) компьютерные системы (ЭВМ, серверы, локальные сети, глобальные сети).

Развитие информационных и компьютерных технологий продолжит оказывать постоянное влияние на расширение перечня видов и подвидов виртуальных следов. Это прогрессирующая система, которой многие правоведы, уже сегодня, должны уделить достаточное внимание, с целью избежать возникновение отрицательных последствий.

Подводя итог, стоит сказать, что в рамках криминалистики необходимо изучить теоретические основы следообразования, закономерности возникновения виртуальных следов, отражающих механизм киберпреступления с целью разработки рекомендации по применению научно-технических средств и специальных методов для обнаружения, изъятия и исследования виртуальных следов с целью установления обстоятельств, имеющих значение для раскрытия, расследования и предупреждения преступлений совершенных в рамках или с использованием компьютерных систем.

Библиографический список

1) Базаров, А. А. Проблемы развития института борьбы с информационными преступлениями в Российской Федерации / А. А. Базаров, А. А. Гребеньков // Проблема модернизации законодательства в условиях глобализации -2016 / А. А. Гребеньков. — Курск, 2016. — С. 67-72.

2) Мещеряков В.А. Электронные цифровые объекты в уголовном процессе и криминалистике // Воронежские криминалистические чтения: сб. науч. тр. Воронеж, 2004. Вып. 5. С. 153–169.

3) Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования // Воронеж, 2002.

4) 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. С. 18.

5) Е.Р. Россинская, Г.П. Шамаев. Криминалистическое исследование компьютерных средств и систем как новый раздел криминалистической техники [Электронный ресурс]. Режим доступа: https://elibrary.ru/download/elibrary_23791198_70740334.pdf (дата обращения 14 ноября 2017).

6) Черкасов В.Н., Нехорошев А.Б. Кто живет в "киберпространстве"? Управление защитой информации. 2003. Т. 7. N 4. С. 468.

Bazarov A.A.

Bazarov Andrey Andreevich (xoocki@yandex.ru) student, bachelor of 4th course of Faculty of Law South-West State University, Kursk

VIRTUAL TRACES IN CRIMINALISTICS

Abstract: In this article, the author considered on the problematic issue of the concept of virtual tracks in criminalistics and considered possible classification of the virtual traces.

Key words: criminalistics, virtual traces, computer crimes, investigation of cybercrimes.