



*Ходоева Эржена Дашиевна  
магистрант кафедры криминалистики,  
судебных экспертиз и юридической психологии,  
Байкальский государственный университет,  
г. Иркутск, Россия  
e-mail: erzhenkk@gmail.com*

## **ПОНЯТИЕ И СПОСОБЫ СОКРЫТИЯ ЭЛЕКТРОННЫХ СЛЕДОВ ПРЕСТУПЛЕНИЯ**

**Аннотация.** В статье рассмотрены специфические следы преступления, совершенного с помощью компьютерных и иных цифровых электронных устройств, которые правонарушитель стремится скрыть. Известность способов сокрытия электронных следов обеспечивает своевременную раскрываемость преступлений правоохранительными органами. В статье анализируются такие способы сокрытия электронных следов, как распространение «вируса», «хакерская атака», использование программ-анонимизаторов, «ремейлов», VPN-сервисов, VPN-прокси-серверов, «Onion Routing, TOR — луковичной маршрутизации второго поколения», а также криптование и обфускация.

**Ключевые слова:** электронный след, следообразование, сокрытие следов преступления, киберпреступность, информационно-компьютерное обеспечение, вредоносная программа, «бестелесная» технология.

## **CONCEPT AND METHODS OF COVERING ELECTRONIC TRACES OF CRIME**

**Abstract.** The article deals with specific traces of a crime committed with the help of computer and other digital electronic devices, which the offender seeks to hide. The popularity of methods for hiding electronic traces ensures timely detection of crimes by law enforcement agencies. The article discusses and analyzes such methods of hiding electronic traces as the spread of a «virus», «hacker attack», the use of anonymizer programs, «remails», VPN services, VPN proxy servers, Onion Routing, TOR- of the second generation», as well as cryptography and obfuscation.

**Keywords:** Electronic trace, trace formation, concealment of traces of crime, cybercrime, information and computer software, malicious software, «disembodied» technology.

Изучение научных источников позволило выделить разные суждения авторов относительно термина, применяемого к следам, оставляемым в результате использования информационно-компьютерных технологий. Исследователи используют понятия виртуальный, бинарный, электронный

след. А.А. Бессонов в своей работе отразил понятие «электронный след — это информация, зафиксированная в цифровом формате, содержащаяся в электронно-вычислительных машинах и иных цифровых устройствах, созданных на основе их технологий, в средствах подвижной радиотелефонной связи и на различных носителях цифровой информации, причинно связанная с событием преступления, позволяющая установить обстоятельства совершенного преступления и преступника» [1, с. 47].

В.А. Мещеряков под «виртуальным следом» понимает различное изменение автоматизированной системы, сопряженное с преступлением и зафиксированное как компьютерная информация. А также данные следы занимают промежуточную позицию между материальными и идеальными следами. Некоторые авторы против применения термина «виртуальный след», так как это устоявшийся термин, применяющийся в квантовой теории поля для характеристики частиц, находящихся в промежуточном состоянии или в состоянии неопределенности [2, с. 21].

С одной стороны, выявление и изъятие рассматриваемых следов возможна только благодаря программно-техническому средству, что предполагает отнесение данных следов к материальным, однако, это утверждение ошибочно, в связи с отсутствием неразрывной связи с устройством. С другой стороны, следы запечатлены на материальном объекте, что противоречит главному признаку идеальных следов — сохранение в памяти человека. Следовательно, рассматриваемые следы дифференцированы от иных видов следов.

В.А. Милашев определяет данный след, как «бинарный», иными словами, как «результат логических и математических операций с двоичным кодом» [3, с. 41]. Однако следует отметить тот факт, что в преобладающей части, восприятие следа представляется не в виде двоичного кода, чем и является бинарный след, а в ином виде: записи в файле реестра, трансформации атрибута файла, электронном почтовом сообщении. В связи с вышеизложенным, следует обратить внимание на общий признак рассматриваемых терминов, заключающийся в том, что данный след — это компьютерная информация, находящаяся в электронно-цифровой или же кодовой форме. Наиболее близкими по определению данного следа являются «электронный» и «виртуальный». «Виртуальным» принято считать объект реально не существующий, но возможный. Согласно толковому словарю Д.В. Дмитриева, «электронное есть все, что относится к свойствам, взаимодействия, влияния и так далее, электронов. Термин охватывает все устройства, или системы, действующие на основе электричества» [4, с. 1341]. Следовательно, «электронный» из всего многообразия терминов в полном объеме охватывает понятие рассматриваемого следа.

Недоступные взору материальные следы и есть электронные следы. При разрешении вопроса о возникновении данных следов, следует вывод о том, что их образование происходит благодаря электромагнитному воздействию материальных объектов, которые являются объективной формой

существования компьютерной информации. Из вышеизложенного следует, что компьютерная информация независима и представляется в объективной форме. Существует теория отражения, согласно которой, изменения в окружающей человека обстановке, образуются во всех случаях происхождения в материальном мире факультативных признаков объективной стороны совершения правонарушения. Иными словами, подготовка, совершение и сокрытие преступления абсолютно во всех случаях приносят изменения в окружающую обстановку, оставляя любое материально фиксированное отражение [5, с. 51]. Как правило, отражение образуется во время взаимодействия следообразующего и следовоспринимающего объектов следообразования. Что же касается электронных следов, то средством для передачи компьютерной информации о способе совершения правонарушения и информации о субъекте преступления является отображающийся объект следообразования [6, с. 48]. Использование материальных носителей позволяет передачу компьютерной информации, содержащую в себе факультативные признаки объективной стороны преступления, между системами, однако, обнаружение и изъятие электронных следов из компьютерной системы — следообразователя порой невозможно, в связи с предусмотрительностью правонарушителя, заключающейся в сокрытии электронных следов.

Как отмечает профессор Р.С. Белкин, детально исследовавший проблему сокрытия следов преступления, «сокрытие преступления — это деятельность (элемент преступной деятельности), направленная на воспрепятствование расследованию путем утаивания, уничтожения, маскировки или фальсификации следов преступления и преступника и их носителей» [7, с. 358]. Сокрытие электронных следов преступления осложнено тем, что одной из особенностей данного деяния является то, что способ и механизм совершения, заблаговременно скрываются преступником. Именно для этой цели используются технически сложные средства совершения преступления. Постоянное совершенствование операционных систем, создание программистами новых программ, вирусов, системных атак является особенностью сокрытия электронных следов преступления. В частности, динамика развития киберпространства и сложность средств совершения преступления, являются обеспечением анонимности правонарушителя.

Использование технических возможностей всемирной информационной компьютерной сети, особых компьютерных программ при киберпреступности обеспечивает анонимность лицу, совершившему правонарушение, путем обнаружения правоохранительными органами иного лица, не имеющего отношения к рассматриваемому событию [8, с. 47]. В данном случае правонарушитель достигает желаемого для него результата — анонимности, а такое обстоятельство обеспечивает его безнаказанность, что приводит к совершению новых аналогичных преступлений. Практически закономерностью является то, что такие преступления совершаются и в

дальнейшем, все это приводит к тому, что с течением времени уровень раскрываемости данных правонарушений понижается.

Информационные компьютерные сети и сервисы, разработанные специалистами программы, способствуют киберправонарушителю в сокрытии своей личности. Например, компьютерная программа, созданная с учетом принципа «Onion Routing, TOR — луковичной маршрутизации второго поколения», необходимая для предоставления компьютерной информации в информационно-телекоммуникационную сеть «Интернет». Указанная компьютерная технология позволяет сохранять состояние инкогнито при посещении различных компьютерных сайтов, отправке различных сообщений, публикации какого-либо материала. Безадресованность данной информации обеспечивается путем создания сети маршрутизаторов, по которым устанавливается соединение. В этом случае компьютерные серверы являются посредниками, по которым устанавливается соединение, иными словами, происходит многослойное шифрование с помощью системы прокси-серверов. Именно благодаря данным «посредникам» компьютерно-информационного соединения усложняется установление источника компьютерной информации. Задача установления источника более усложнится тем, что «посредников» может быть много и высока вероятность нахождения их вне пределов одного государства [9, с. 44]. Важно также отметить и то, что устанавливаемая цепочка компьютерно-информационного соединения шифруется, и, данное обстоятельство осложняет установление лица, который использовал ранее указанную компьютерную программу.

Использование VPN-сервисов (англ. Virtual Private Network- виртуальная частная сеть) обеспечивает шифрование сетевого трафика между компьютером лица, желающего стать анонимом, и VPN-прокси-сервером (представляет собой шлюз выхода в Интернет), обеспечивающим анонимность реального IP-адреса пользователя [10, с. 91]. При необходимости высокого уровня конфиденциальности возможен такой вариант как, аренда у провайдеров хостинговых услуг вычислительные мощности практически в любой точке мира, далее настраиваются собственные VPN-серверы, с помощью которых, при использовании сторонних VPN-сервисов, протекает выход в Интернет.

Существуют иные способы анонимности пользователей компьютера в информационно-компьютерной сети «Интернет», например, сокрытие IP-адреса с помощью автоматизированной сети (бота-сети) из компьютеров, которая создана троянской программой, имеющей функционально схожие возможности с VPN-прокси-сервером [10, с. 92]. Также необходимо рассмотреть и такой способ как, заражение компьютерным вирусом, позволяющим добиться необходимого преступного результата и анонимности. Распространение вирусов возможно следующими способами:

А) «фейк» — в широком смысле это подделка. Из одного названия есть возможность определить сущность способа, которая заключается в том, что пользователь по ошибке может «войти» на схожую с оригиналом, социальную

сеть или платежную систему. Благодаря невнимательным действиям пользователя в информационно-компьютерной сети, в его устройство проникает компьютерный вирус. Данный вирус может сохранять и передавать личные данные пользователя, пароли и логины для входа в социальные сети или электронную почту, а также блокировать некоторые функции устройства из-за системных ошибок, в большинстве случаев, приоритетной функцией вируса является распространение;

Б) «письмо счастья или спам» — данные электронные сообщения рекламного или религиозно-мистического и иного характера информацией, общность которых заключается в требовании переслать копии письма другим лицам. В пересылаемых электронной почтой письмах содержится средство для перехода на другой сайт (ссылка). В данном случае вирусификация устройства происходит путем перехода пользователя по ссылке, указанной в письме, дальнейшие действия вируса зависят от его созданных целей. В компьютерной системе жертвы в случае использования вышеуказанных способов заражения вирусом, имеет место быть вредоносная компьютерная программа с хранящейся в ней зашифрованной личной информацией пользователя. Соккрытие существования ранее рассмотренной программы в устройстве пользователя возможно ее самоликвидацией по команде, которая поступила от управляющего ею лица, либо автоматически [11, с. 213].

Заинтересовывает и такое действие, предусматривающее захват контроля над удаленной информационно-компьютерной техникой, либо ее дестабилизация («хакерская атака») [12, с. 90]. Участники данной атаки, хакеры — программисты намеренно обходящие системы компьютерной безопасности, способствуют сокрытию следов совершенного правонарушения. Как правило, хакерская атака является отвлекающим маневром от самих действий, направленных на совершение преступлений, то есть возникает ситуация, когда преступники используют иных лиц, не обладающих информацией о совершаемом преступлении для достижения своих целей.

Необходимо отметить и такие способы анонимности, как использование программ-анонимизаторов и ремейлов. Рассматриваемые способы позволяют осуществить переадресацию электронной почты, направляя ее с иного компьютера или изменить данные об обратном адресе и службе электронной почты отправителя, из этого следует, что конечный получатель лишен возможности идентификации отправителя письма. В качестве ремейлеров могут выступать специализированные веб-сайты, открытые SMTP-серверы и анонимные сети, например, Mixminion [13, с. 43]. SMTP-сервер (протокол простой передачи почты) — это обширно используемый сетевой протокол, который предназначен для передачи электронной почты в сетях TCP/IP, а mixminion основан на пересылаемых защищенных одноразовых блоках, может принимать и отсылать анонимные сообщения электронной почты [3, с. 44].

В случаях сокрытия следов несанкционированного доступа и вредоносной активности, применяются различные меры технического

характера такие как, шифрование (криптование), обфусикация (obfuscate — делать запутанным, неочевидным) а также относительно новые приемы и методы — «бестелесная» технология [10, с. 92].

При криптовании исполняемый код вредоносной программы шифруется, в случае обфусикации становится затруднительным познание и анализирование алгоритма работы. Рассмотренные виды сокрытия электронных следов осложняют выявление данных программ антивирусным программным обеспечением и исследование специалистами информационной безопасности. «Бестелесными» называются программы, функционирующие только в оперативной памяти и не сохраняющиеся на энергопотребляющих запоминающих устройствах. Данная программа самоликвидируется с устройства при перезагрузке или отключении питания. Лица, совершающие неправомерные действия используют вышерассмотренные программы для сокрытия своей активности.

Важно обратить внимание на то, что приведенные примеры программ, способствующие анонимности в сети, не являются единственными. Преступления, где средством являются информационно-компьютерные технологии, постоянно развиваются, создаются новые программные обеспечения и средства, иные средства сокрытия следов. Необходимо выделить, что важной криминалистической закономерностью является обстоятельство, при котором, во время планирования и непосредственно осуществления киберпреступником выбранного способа совершения преступления, с использованием информационно-компьютерных технологий является то, что лицо при подготовке к совершению преступления предпринимает действия по сокрытию своих следов. Иными словами, лицо, совершающее неправомерные действия с использованием информационно-компьютерных технологий, заблаговременно осуществляет комплекс мер по сокрытию электронных следов, непосредственно перед совершением преступления.

#### **Список использованной литературы**

1. Бессонов А.А. О некоторых возможностях современной криминалистики в работе с электронными следами // Вестник Университета имени О.Е. Кутафина. — 2019. — № 3 (55). — С. 46-52.
2. Шаталов А.С. Разработка методических основ расследования преступлений, совершаемых с помощью компьютерных и сетевых технологий: проблемы, перспективы и тенденции. // Вестник Сибирского юридического института МВД России. — 2018. — № 3 (32). — С. 7-15.
3. Милашев В.А. Неправомерный доступ к компьютерной информации в сетях ЭВМ // Правовые вопросы связи. — 2004. — № 2. — С. 40-46.
4. Дмитриев Д.В. Толковый словарь русского языка. — М.: Астрель: АСТ, 2003. — 1578 с.
5. Карепанов Н.В. Некоторые вопросы выявления и исследования следов преступлений // Российское право: Образование. Практика. Наука. — 2019. — № 3 (111). — С. 49-59.

6. Глушков Е.Л. Емельянов Д.Е. Оперативно-розыскная деятельность при расследовании и раскрытии преступлений в сфере компьютерной информации // Вестник Белгородского юридического института МВД России имени И.Д. Путилина. — 2019. — № 2. — С. 45-50.
7. Белкин Р.С. Курс криминалистики: учеб. пособие для вузов. — 3-е изд., дополненное. — М.: ЮНИТИ-ДАНА, Закон и право, 2001. — 837 с.
8. Малышкин П.В. Особенности сокрытия следов совершенных преступлений, совершаемых с применением информационных компьютерных технологий // Мир науки и образования. — 2016. — № 4 (8). — С. 42-47.
9. Россинская Е.Р., Рядовский И.А. Современные способы компьютерных преступлений и закономерности их реализации // Lex Russica. — 2019. — № 3 (148). — С. 87-99.
10. Введенская О.Ю. Особенности следообразования при совершении преступлений посредством сети интернет // Юридическая наука и правоохранительная практика. — 2015. — №4 (34). — С. 209-216.
11. Толпекин К.А. Международные и интеграционные нормы ЕАЭС об использовании информационных приемов цифровой криминалистики в противодействии киберпреступлениям // Международное сотрудничество евразийских государств: политика, экономика, право. — 2017. — № 4. — С. 87-96.
12. Распопова А.В. Организационно-методическое обеспечение первоначального этапа расследования преступлений, совершаемых в сфере экономики с использованием средств компьютерной техники: автореф. дисс. ... канд. юрид. наук: 12.00.09 — М., 2007. — 180 с.
13. Кадатенко Е.П. Неправомерный доступ к компьютерной информации в сфере банковской деятельности: проблема производства осмотра места происшествия по делам о хищениях // Вестник экономической безопасности. — 2009. — № 8. — С. 42-46.