сбыта наркотических средств, запрещен, в связи с чем блокируется интернет-провайдерами. Однако есть обход данного запрета с помощью использования VPN-ресурса. В ходе производства следственного эксперимента наркосбытчик (подозреваемый, обвиняемый) должен продемонстрировать навык по умению пользования данным ресурсом.

VPN (англ. Virtual Private Network – виртуальная частная сеть) – обобщенное название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет). Несмотря на то, что коммуникации осуществляются по сетям с меньшим или неизвестным уровнем доверия (например, по публичным сетям), уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии (шифрования, аутентификации, инфраструктуры открытых ключей, средств для защиты от повторов и изменений, передаваемых по логической сети сообщений)[1]. Подозреваемый, при производстве следственного эксперимента должен указать, каким образом он получил доступ к ресурсу VPN (название сайта, с которого был скачан, и название VPN), а также умение настроить данный ресурс для соединения с интернет-ресурсом для его последующего использования.

Таким образом, нельзя недооценивать значимость следственного эксперимента на стадии предварительного расследования наркопреступлений, совершенных с использованием информационно-телекоммуникационных сетей и цифровой валюты, так как с его помощью появляется возможность выявления умений и навыков подозреваемого по реальному совершению каких-либо действий, которые позволят установить механизм совершенного преступления.

*Даниленко А.В.*

Могилевский институт МВД Республики Беларусь
Научный руководитель Д.И. Шнейдерова

## Криминалистический анализ способов сокрытия электронно-цифровых следов

Ежегодный прирост пользователей сети Интернет по всему миру и увеличение суточного интервала активности при использовании его ресурсов свидетельствуют о прочной взаимосвязи жизни людей современного общества с компьютерными технологиями. Действия в сети Интернет, в том числе противоправного характера, как и любое преступление, совершаемое в условиях материальной среды, не могут оставаться бесследными. В рамках криминалистичес-

[1] Там же. С. 154.

кого исследования киберпреступлений, связанных с хищением имущества, компьютерной безопасностью, отдельное внимание уделяется видовому разнообразию электронно-цифровых следов, образуемых в памяти устройств при активности пользователя как в сети Интернет, так и в системе самого устройства.

Значимость электронно-цифровых следов определяется в первую очередь возможностью установления по их совокупности личности лица, совершившего преступление, использования их в доказывании виновности или невиновности, помимо этого следы способствуют установлению обстоятельств совершенного преступления, в частности способа реализации преступного умысла, сокрытия личности пользователя и похищенного имущества (если совершено хищение). По механизму образования электронно-цифровые следы разделяют на активные и пассивные. Активные следы образуются за счет целенаправленного воздействия пользователя на компьютерную систему, намеревающегося опубликовать личные или иные данные, и имеют выраженный публичный характер (например, аккаунты с личной информацией в социальной сети, фотографии, объявления о продаже товара, сообщения на форуме и т.д.). Пассивные следы формируются системой в фоновом режиме, независимо от желания пользователя, и отражают каждое производимое им действие (например, при посещении веб-страниц сервер сайта регистрирует IP-адрес устройства, которое запрашивало к ним доступ, в какое время, сколько раз, какие действия производились и т.д.).

Как правило, важное криминалистическое значение при решении задачи поиска лица, совершившего киберпреступление, имеют пассивные следы, которые позволяют связать личность с определенными техническими устройствами и местом их использования. Однако на практике данная задача является трудновыполнимой или нереализуемой вовсе по нескольким причинам: во-первых, при совершении каких-либо действий в сети Интернет преступники используют сервисы-анонимайзеры, позволяющие скрыть реальный IP-адрес устройства; во-вторых, некоторые провайдеры сети применяют технологии преобразования сетевых адресов, за счет которых несколько пользователей имеют один внешний адрес и, наоборот, один пользователь имеет несколько внешних адресов; в-третьих, поскольку большинство киберпреступлений совершаются лицами, находящимися на территории иностранных государств, либо ими используются сетевые ресурсы, серверы которых принадлежат зарубежным компаниям, то возникают трудности при получении криминалистически значимой информации в рамках международных запросов по материалам проверки и уголовным делам (на такое положение влияют низкая оперативность, отказ в предоставлении информации ввиду политики конфиденциальности организации, либо если преступление не является уголовно наказуемым на территории государства-адресата и по иным причинам).

Среди популярных сервисов, позволяющих замаскировать реальный IP-адрес используемого преступником устройства, следует отметить VPN и Tor. VPN представляет собой технологию, именуемую как частная виртуальная сеть, которая позволяет своим клиентам передавать и получать зашифрованные пакеты данных в сети Интернет через специальные туннели, проходящие по каналу связи с более низким уровнем. Пользователь, подключаясь к VPN, может осуществлять любые действия в общедоступной сети под IP-адресом, принадлежащим серверу VPN, тем самым не афишируя свой IP, присвоенный провайдером используемой сети. Исходя из механизма функционирования сервисов VPN, следует, что провайдер сети Интернет, услугами которого пользуется преступник, может отследить его действия только на этапе до подключения к VPN, дальнейшая активность доступна только VPN-администратору. Кроме того, имеет место двойное подключение к VPN-серверам, в ходе которого преступник первоначально присоединяется к публичному сервису, а потом перенаправляется к другому, уже не установленному. Такое положение крайне негативно влияет на процесс расследования киберпреступлений и отыскание электронно-цифровых следов пребывания определенного преступника на конкретных интернет-ресурсах, поскольку VPN-провайдеры отказывают в предоставлении необходимой информации по международным запросам, ссылаясь на политику конфиденциальности и деловую репутацию, так как обеспечение анонимности клиентов – главная задача данных ресурсов.

Также следует обратить внимание, что на анонимизирование личности в сети Интернет может быть направлено действие автоматизированной сети компьютеров – бот-сети, которая создается хакерами путем распространения вирусных троянских программ[1]. Так, компьютер любого пользователя может быть использован как проводник для различных атак в сети, при этом провайдер будет видеть только IP используемого устройства добросовестного пользователя, а не преступника, что в последующем направит следствие по ложному следу.

Tor – программное обеспечение, позволяющее осуществлять передачу данных по механизму «луковой» маршрутизации, который представляет собой перенаправление зашифрованных пакетов данных к нескольким случайным узлам сети по очереди с целью их послойного дешифрования и отправки конечному получателю. Такое движение пакетов данных и запросов к иной стороне приводит к смене информации о реальном первичном узле – отправителе, что позволяет пользователю этого узла, т.е. преступнику, оставаться незамеченным в цифровом поле. Однако браузеры и приложения Tor за счет сложной

[1] Россинская Е.Р. Современные способы компьютерных преступлений и закономерности их реализации // Lex Russica. 2019. № 3 (148). С. 91.

многоузловой маршрутизации крайне медлительны, что не позволяет преступникам реализовывать преступные схемы, требующие оперативности. При этом Tor активно применяется для доступа к теневому сегменту – DarkNet, площадки которого специализируются на продаже баз данных, поддельных паспортов, банковских и сим-карт, товаров, запрещенных к обороту, а также методических рекомендаций по реализации различных способов осуществления киберпреступлений.

NAT и DHCP – технологии маршрутизации, изменяющие количество внешних IP-адресов, подключенных к сети устройств, которые применяются крупными провайдерами интернет-сети. NAT позволяет нескольким компьютером использовать один внешний IP, а DHCP – одному внутреннему несколько краткосрочных внешних IP. Такие способы маршрутизации приводят к диссонансу между реальным количеством использованных устройств и количеством внешних IP, отображаемых в анализируемом трафике, что не позволяет правоохранительным органам оперативно установить точный адрес искомого устройства.

Таким образом, с теоретической точки зрения полностью анонимизировать свое присутствие и активность в сети Интернет невозможно, поскольку и владельцы анонимайзеров, и зарубежные интернет-провайдеры, и сетевые ресурсы все же обладают достоверной информацией о своих клиентах. Однако с практической точки зрения получение таких электронно-цифровых следов затруднено и зачастую невозможно ввиду отсутствия налаженного и компромиссного механизма международного взаимодействия, проблемы которого требуют дальнейшего изучения и поиска эффективных решений.

*Биткова А.А.*

Санкт-Петербургский Университет МВД России
Научный руководитель Е.В. Горкина, кандидат юридических наук, доцент

## Криминалистическая характеристика жертв доведения до самоубийства и склонения к его совершению

Самоубийство – это явление социальной жизни, которое существует на протяжении всей истории человечества. В разные времена отношение к людям, совершающим суицид или попытки к нему, было различно: в некоторых культурах существовал и по сей день существует ритуальный суицид, осуществляемый по определенным правилам, во времена императорской России за попытки самоубийства была предусмотрена ответственность действующими в то время законами. Сейчас к людям с суицидальным поведением относятся неоднозначно. С одной стороны, ответственность за самоубийство по