

ОСНОВНЫЕ НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ СЛЕДОВАТЕЛЯ ПО УСТАНОВЛЕНИЮ ЛИЦ, СОВЕРШИВШИХ НЕЗАКОННЫЙ СБЫТ НАРКОТИЧЕСКИХ СРЕДСТВ ПОСРЕДСТВОМ СЕТИ «ИНТЕРНЕТ»

А.Б. Соколов, Н.А. Яковлева
Омская академия МВД России, г. Омск
email: Andrey.perm@mail.ru

Аннотация. Определено, что стремительное развитие цифровых устройств и информационных технологий характеризуется не только положительными, но и негативными последствиями в виде активного использования достижений цифрового прогресса при совершении различных преступлений. Анализ статистических данных показал, что к числу наиболее распространенных преступлений, совершаемых с использованием информационно-телекоммуникационных технологий (включая сеть «Интернет») относится незаконное производство, сбыт или пересылка наркотических средств, психотропных веществ, а также незаконные сбыты или пересылка растений, содержащих наркотические средства или психотропные вещества (ст. 228.1 УК РФ). Определены основные направления деятельности следователя по установлению лиц, совершивших незаконный сбыт наркотических средств посредством сети «Интернет». Сделан вывод о том, что оптимальными способами получения информации в рамках указанных направлений являются: производство следственных действий (осмотр места происшествия, осмотр предметов, обыск и др.), направление запросов, а также самостоятельный мониторинг.

Ключевые слова: незаконный сбыт наркотических средств, информационно-телекоммуникационные технологии, сетевой наркомаркетинг, планирование расследования преступлений, IP-адрес, VPN-технологии, провайдер.

Мы и сами того не заметили, как нашу повседневную жизнь наполнили достижения науки и техники. Ежедневно каждый из нас сталкивается с «цифровыми произведениями». По пути в кофейню мы отправляем сообщение в полюбившимся нам мессенджере и имеем возможность заказать пряный латте в кофейном автомате; покоряя электросамокат, направляемся на прогулку по городу, не забыв настроить в мобильном телефоне аудиокнигу; приходя домой, с порога слышится «Привет, Алиса, включи что-нибудь повеселее...». И это лишь небольшая часть использования достижений технического прогресса в настоящее время. В желании отгородиться от повседневной суеты и высокого ритма жизни, люди создают виртуальный мир, в котором позволяют себе находиться без счета времени. К сожалению, достижения науки и техники нередко становятся предметом внимания со стороны криминального элемента. Соответствующие возможности адаптируются для достижения преступных целей, в том числе посредством информационно-телекоммуникационных технологий (далее – ИТТ)¹.

Стремительное развитие цифровых устройств и информационных технологий характеризуется не только положительными эффектами при решении задач стоящих перед обществом, но и негативными последствиями в виде активного использования достижений цифрового прогресса при совершении различных преступлений. Сложность выявления и дальнейшего расследования противоправных деяний, совершенных посредством ИТТ сопровождается высокой степенью анонимности использования сети Интернет. Примером, рассматриваемой ситуации, может послужить так называемый «сетевой наркомаркетинг». Интересным в этой части представляется мнение Л.С. Кузиной, указывающей на то, что «"Сетевой

¹ Совокупность методов и средств передачи различной информации.

наркомаркетинг" представляет собой преступную схему, которая заключается в реализации активного внедрения и распространения наркотических средств, психотропных веществ или их аналогов среди населения» [1, с. 287]. Результаты анализа состояния уровня преступности в России показывают, что количество зарегистрированных преступлений, предусмотренных ст. 228.1 УК РФ, совершенных с использованием ИТТ (включая сеть «Интернет») растет. Так за 2019 год зарегистрировано 24 677 (+31,2%) указанных преступлений; за 2020 год – 47 060 (+90,7%); за 2021 год – 51 444 (+9,3%); за период с января по сентябрь 2022 года зарегистрировано 46 315 (+8,4%)¹. Приведенные данные позволяют отметить, что незаконное производство, сбыт или пересылка наркотических средств, психотропных веществ, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества (ст. 228.1 УК РФ) совершенных с использованием ИТТ (включая сеть «Интернет») характеризуется постоянным ростом.

Безусловно, данному негативному явлению способствует применение различных видов VPN-программ², особенно пользующихся спросом за последнее время. Их ключевая задача состоит в сохранении «образа невидимки». Взаимодействие субъектов «сетевого наркомаркетинга» происходит посредством мессенджеров, к числу наиболее распространенных из них можно отнести Telegram, WhatsApp, либо через социальные сети, такие как Facebook, Twitter, «Вконтакте».

Что позволит идентифицировать лицо, использующее сеть «Интернет» для незаконного сбыта наркотических средств? Какие меры для этого целесообразно предпринять правоохранительным органам? Учитывая поставленные вопросы, интересным представляется определение направлений деятельности следователя по установлению лиц, совершивших незаконный сбыт наркотических средств посредством сети «Интернет».

Исходной точкой разгадывания «сетевой головоломки» является тот факт, что указанные нами ранее средства взаимодействия используются в онлайн режиме, соответственно, связаны с подключением к сети «Интернет». Выход во всемирную глобальную паутину происходит через IP-адреса (Internet Protocol Address), что является нашим местоположением в киберпространстве или иначе киберлокацией. Цепочка цифр, указанных в этом адресе, может позволить получить ценную информацию, например, фактический адрес лица, пользующегося услугами «Интернета», либо его персональные данные.

Таким образом, первостепенной задачей правоохранительных органов является определение IP-адреса, который был присвоен пользователю (сбытчику) провайдером. Указанная информация может быть получена путем производства следственных и иных процессуальных действий (например, запросом). Рассмотрим возможности получения IP-адреса в рамках следственных действий, при этом существенное значение будет иметь наличие либо отсутствие возбужденно уголовного дела. Перечь следственных действий, которые могут быть произведены до возбуждения уголовного дела, представлен в ч. 1 ст. 144 УПК РФ. Из числа указанных оптимальным способом определения IP-адреса может быть осмотр места происшествия и (или) осмотр предмета. При наличии возбужденного уголовного дела следует отнести обыск. О назначении и возможностях, а также соотношении осмотра и обыска, с целью получения информации, содержащейся на электронных носителях информации (в том числе и IP-адреса) уже упоминалось на страницах юридической печати [2, 3, 4 и др.]. Опираясь на сущность рассматриваемых

¹ Статистика. Состояние преступности в России за январь-декабрь 2019, 2020, 2021, январь-сентябрь 2022 гг. URL: <https://мвд.рф/folder/101762> (дата обращения: 11.11.2022).

² Virtual Private Network – виртуальная частная сеть, основной задачей которой является зашифровка IP-адреса.

следственных действий, может складываться ощущение, что просмотр информации, находящейся на электронном носителе ассоциируется с деятельностью по отысканию (носит активный поисковый характер) и, соответственно, выходящей за рамки осмотра. Учитывая специфический характер электронной информации, полагаем, что это не совсем так. С технической точки зрения просмотр файлов (их наименования) содержащихся на электронном носителе информации является действием по обнаружению (в сравнении с отысканием носит пассивный характер). Но не стоит забывать о специфике электронной информации, которая сконструирована в виде файловой системы. Именно данный аспект является логическим обоснованием того, что просмотр файлов носит пассивный характер и является лишь обнаружением информации.

К наиболее распространенному типу файловых систем относится семейство FAT. Для него характерно деление дискового пространства на системную область и область данных, расположенных последовательно. В последней находятся каталоги и файлы, и ее структура сравнима с методом «дерева целей». Таким образом, видится взаимосвязь файлов в виде цепочки, и, обращаясь к нужному нам файлу, считывание происходит с первого номера (с первого звена цепочки). Следовательно, просматривая сведения на носителе информации, мы лишь перемещаемся от «узла к узлу» различных ветвей. Данные действия не являются отысканием, что характерно для обыска. Сведения, которые нам необходимо получить: полное имя файла (местоположение), даты создания, редактирования и последнего открытия, а также его размер.

Осмотр электронных носителей информации происходит с участием специалиста. Ценным является получение информации о переписках посредством SMS либо в мессенджерах, при обнаружении которых следователь производит фотосъемку, о чем обязательно указывает в протоколе осмотра предмета. Учитывая сказанное, следователь вправе беспрепятственно получить информацию, содержащуюся на электронных носителях, в ходе осмотра при отсутствии средств защиты на устройстве (паролей). Отсутствие указанного условия влечет производство такого следственного действия как обыск. В ходе его проведения допускается использование разрушающих методов, направленных на обход или устранение различных паролей, в том числе не исключается возможность применения программно-аппаратных комплексов.

Помимо названных оптимальным способом определения IP-адреса может заключаться в составлении и направлении следователем запроса в адрес администрации сайта в рамках реализации полномочий, предусмотренных ч. 4 ст. 21 и п. 3 ч. 2 ст. 38 УПК РФ. Разберем данную ситуацию на примере. Незаконный сбыт наркотиков осуществляется посредством социальной сети «ВКонтакте». При наличии информации о переписке приобретателя и сбытчика следователь направляет запрос в адрес администрации сайта «ВКонтакте» с целью получения соответствующей переписки. Анализ полученного ответа позволит определить никнейм (nickname) «сбытчика» (абонента). Далее следователь направляет новый запрос о получении логина (login) присвоенный абоненту сайта «ВКонтакте» при регистрации. В данном запросе целесообразно также указать, с каких IP-адресов выходил в сеть соответствующий пользователь, участвующий в переписке (сбытчик). Не исключается возможность установить дополнительные (персональные) данные об интересующем абоненте, которые были указаны им при добровольной регистрации [5, с. 88-92]. Учитывая сказанное, запрашиваемая информация может содержать ответ в виде данных IP-адреса, а также интенсивности

посещения им сайта, фамилии, имени, отчество пользователя, его электронной почты, номера мобильного телефона и др¹.

Получение IP-адреса может быть осложнено использованием различных VPN-программ. Аббревиатура VPN раскрывается как Virtual Private Network – виртуальная частная сеть, функционал которой основан на зашифровке IP-адреса. По общему правилу, информация в сети Интернет передается по схеме Пользователь – Сервер через «туннель движения». При использовании VPN сервисов данная схема добавляется третьим элементом – «виртуальным узлом», в результате чего мы получаем следующую схему: Пользователь – VPN (виртуальный узел) – Сервер. Новый элемент позволяет скрыть IP-адрес пользователя, что скрывает его действительное местоположение и обеспечивает анонимность, то есть все запросы выполняются с мнимого адреса. Определить такого пользователя все же возможно, однако цепочка по установлению его местонахождения будет длиннее обычной.

Получив сведения об IP-адресе, следователь устанавливает провайдера – компанию, предоставляющую услуги Интернета. С современными возможностями это не составляет особого труда, достаточно ввести в поисковую строку браузера соответствующий запрос. Результаты поиска не заставят долго ждать, указывая на такие открытые источники, как «whoer.net», «2IP», «whois» и другие, позволяющие установить провайдера в режиме онлайн. Результаты мониторинга оформляются следователем в виде справки, содержащей последовательно выполненные им действия.

Обладая IP-адресом, установив провайдера, завершающим шагом является получение сведений позволяющих установить лицо, осуществившего незаконный сбыт наркотических средств. Прежде чем провайдер предоставит услуги доступа к сети Интернет, он заключает с клиентом договор, в котором указываются: фамилия, имя, отчество, дата рождения, место регистрации и проживания, серия, номер паспорта, кем и когда выдан и иные данные. С целью их получения, следователь направляет запрос провайдеру о предоставлении таких сведений.

Подводя итоги, отметим, что к числу основных направлений деятельности следователя по установлению лиц, совершивших незаконный сбыт наркотических средств посредством сети «Интернет», могут быть отнесены:

- определение IP-адреса присвоенного пользователю (сбытчику);
- определение провайдера, предоставлявшего услуги доступа к сети «Интернет» пользователю (сбытчику);
- получение идентифицирующих сбытчика данных.

К типичным способам получения информации в рамках указанных направлений являются: производство следственных действий (осмотр места происшествия, осмотр предметов, обыск и др.), направление запросов, а также самостоятельный мониторинг².

Библиографический список.

1. Кузина Л.С. «Сетевой наркомаркетинг» как один из факторов вовлечения несовершеннолетних в незаконный оборот наркотиков // Вестник ВИ МВД России. 2020. №4. С. 285-290.
2. Соколов А.Б. Собирание доказательственной информации, находящейся на цифровых носителях вычислительной техники. I. Проблемы целеполагания // Проблемы борьбы с преступностью в условиях цифровизации: теория и практика : сборник статей XIX Международной научно-практической конференции «Уголовно-процессуальные и криминалистические чтения на Алтае», посвященные памяти В.К.

¹ Полученные данные могут быть использованы тактически.

² Систематический сбор и обработка информации, которая используется для обеспечения возможности принятия решения.

Гавло. – Вып. XVII / Министерство науки и высшего образования РФ, Алтайский государственный университет; отв. ред. С.И. Давыдов, В.В. Поляков. – Барнаул: Изд-во Алт. ун-та, 2021. С. 429-433.

3. Соколов А.Б., Щербина Р.П. Собирание доказательственной информации, находящейся на цифровых носителях. II. Осмотр, обыск, судебно-компьютерная экспертиза // Проблемы борьбы с преступностью в условиях цифровизации: теория и практика : сборник статей XIX Международной научно-практической конференции «Уголовно-процессуальные и криминалистические чтения на Алтае». – Вып. XIX / Министерство науки и высшего образования РФ, Алтайский государственный университет; отв. ред. С.И. Давыдов, В.В. Поляков. – Барнаул: Изд-во Алт. ун-та, 2021. С. 434-439.

4. Старичков М.В. Тактика осмотра и выемки носителей компьютерной информации // Вестник Восточно-Сибирского института МВД России. 2012. № 2. С. 18-26.

5. Сидорова К.С. Способы установления IP-адреса и сведений о нем при расследовании уголовных дел // Вестник СИБИТА. 2018. №2. С. 88-92.

THE MAIN ACTIVITIES OF THE INVESTIGATOR TO IDENTIFY PERSONS WHO HAVE COMPLETED THE ILLEGAL SALE OF NARCOTIC DRUGS THROUGH THE INTERNET NETWORK

A.B. Sokolov, N.A. Yakovleva

*Omsk Academy of the Ministry of Internal Affairs of Russia, Omsk
email: Andrey.perm@mail.ru*

Annotation: It has been determined that the rapid development of digital devices and information technologies is characterized not only by positive, but also by negative consequences in the form of the active use of digital progress in the commission of various crimes. An analysis of statistical data showed that the most common crimes committed using information and telecommunication technologies (including the Internet) include the illegal production, sale or shipment of narcotic drugs, psychotropic substances, as well as the illegal sale or shipment of plants containing narcotic drugs or psychotropic substances (Article 228.1 of the Criminal Code of the Russian Federation). The main areas of activity of the investigator in identifying persons who have committed the illegal sale of narcotic drugs through the Internet have been determined. It is concluded that the best ways to obtain information within these areas are: the production of investigative actions (inspection of the scene, inspection of objects, search, etc.), sending requests, as well as independent monitoring.

Key words: illegal sale of drugs, information and telecommunication technologies, network drug marketing, crime investigation planning, IP address, VPN technologies, provider.