УДК 343.985.7:343.57
ББК 67.523.13
DOI 10.25724/VAMVD.RPQR

О. А. Решняк, А. П. Резван

ФИКСАЦИЯ СЛЕДОВ НЕЗАКОННОГО СБЫТА НАРКОТИЧЕСКИХ СРЕДСТВ В СЕТИ ИНТЕРНЕТ

Значительное место в преступной структуре занимают деяния, связанные с незаконным оборотом наркотических средств, психотропных веществ и их аналогов. Половину из зарегистрированных преступлений данной категории составляет сбыт.

В последнее время наибольшую популярность приобрели синтетические наркотики, которые имеют приемлемую стоимость и быстрое действие. Их употребление приводит к расширению масштабов наркотизации населения страны, находящегося, как правило, в репродуктивном и работоспособном возрасте.

Большое влияние на рост преступности, в том числе в сфере незаконного сбыта наркотических средств, оказало массовое внедрение во все сферы жизни современного общества информационно-телекоммуникационных технологий, включая электронные платежные средства и системы быстрого обмена информацией. Преступления стали совершаться с использованием Интернета. Компьютерная информация и содержащие ее электронные носители, а также ресурсы сети Интернет все чаще стали выступать в качестве вещественных доказательств. Это обусловило внесение ряда изменений в отечественное уголовно-процессуальное законодательство, которые породили много проблем теоретического и прикладного характера, требующих незамедлительного реагирования.

В статье рассматриваются вопросы, связанные с обнаружением и фиксацией следов преступной деятельности, оставленных в результате незаконного сбыта наркотических средств с использованием сети Интернет, а также проблемы, с которыми сталкивается следственная практика при фиксации указанных следов, и пути их решения.

Ключевые слова: наркотические средства, Интернет, незаконный сбыт, компьютерные технологии, электронные следы.

O. A. Reshnyak, A. P. Rezvan

FIXATION OF TRACES OF ILLEGAL SALES OF NARCOTIC DRUGS ON THE INTERNET

Criminal acts related to the illegal trafficking in narcotic drugs, psychotropic substances and their analogues hold a significant place in the criminal structure. Half of the crimes reported in this category are related to illegal sales.

Furthermore, in recent years, synthetic drugs have reach the height of popularity due to their acceptable cost and fast action. The consumption of such drugs increases the drug addiction, most commonly among the reproductive and working-age population.

The massive adoption of information and telecommunication technologies into every area of modern society, including electronic means of payment and rapid exchange of information systems, had a great influence on the rise in crime and specifically on the illegal sale of narcotic drugs. Crimes using the Internet had become more frequent. Therefore, computer information and electronic media containing it, as well as Internet resources, begin to act as material evidence more and more often. This led to the introduction of several modifications in the domestic criminal procedural legislation, which caused many theoretical and applicable problems requiring an immediate response in the field of forensic science.

The article discusses issues related to the detection and fixation of traces of criminal activity left as a result of illegal sale of drugs on the Internet, as well as the problems that investigative practice faces when fixing these traces, and suggests ways to solve them.

Key words: narcotic drugs, Internet, illegal sale, computer technologies, electronic traces.

Развитие информационно-телекоммуникационных технологий обусловливает стремительный темп эволюции современного общества. Цифровизация уже охватила различные сферы человеческой деятельности: бизнес, досуг, производство и др. Но, несмотря на все это, приходится с сожалением констатировать тот факт, что криминалистическая и правоохранительная деятельность за этим процессом не успевают. В криминалистической науке выработано недостаточно способов, средств и методик, помогающих правоохранительным органам в сборе доказательственной информации по преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий, одними из которых является сбыт наркотических средств (так называемый бесконтактный сбыт). Особенность данного преступления — следы, образованные в результате его совершения: их нужно искать не на традиционных объектах, а на средствах обмена информацией либо в информационно-телекоммуникационном пространстве. Чтобы деятельность следственных подразделений, расследующих преступления в сфере незаконного оборота наркотических средств, совершенных с использованием сети Интернет, стала более эффективной, необходимо понимать, где можно обнаружить следы, оставленные в результате совершения преступления, в какой форме они могут быть образованы и как правильно
их зафиксировать, чтобы в дальнейшем они могли быть использованы в качестве доказательств по уголовному делу и положены в основу обвинения.

Для начала рассмотрим следы, которые могут образовываться в результате совершения преступных действий с использованием компьютерных технологий. В криминалистической литературе вокруг их определения развернулась острая дискуссия. О них писали В. А. Мещеряков [1],
А. Г. Волеводз [2], В. Е. Козлов [3], В. Н. Черкасов, А. Б. Нехорошев [4], Е. Р. Россинская, И. А. Рядовский [5] и др. Не вступая в спор, отметим, что нам ближе дефиниция, сформулированная профессором В. Б. Веховым. Исследуя информационную сущность фиксации доказательств, находящихся в электронно-цифровой форме, он предлагает называть такие следы «электронно-цифровыми следами», под которыми понимает «…любую криминалистически значимую компьютерную информацию, т. е. сведения (сообщения, данные, видео-, фотоматериалы), находящиеся в электронно-цифровой форме, зафиксированные на материальном носителе либо передающиеся по каналам связи посредством электромагнитных сигналов. Эти следы являются материальными невидимыми сигналами» [6, с. 22—23].

Примерно такую же позицию занимает профессор А. Л. Осипенко: «…подобно записям, выполненным на бумаге, компьютерные записи неоднородны, и их доказательственная ценность определяется целым рядом обстоятельств » [7, с. 32]. А. Л. Осипенко предлагает разделить компьютерные файлы на несколько типов в зависимости от того, каким образом формируются записи:

«1. Файлы, созданные человеком и сохраненные на компьютерном носителе. Это аналоги обычных документов, только содержащих записи в электронной форме (например, почтовые сообщения, служебные записи и т. п.).

2. Файлы, созданные компьютером в автоматическом режиме без участия человека (например, записи в журнале системных событий, служебные сообщения о доставке электронной почты и т. д.).

3. Файлы, в которых записи могут быть сгенерированы компьютером с учетом управляющих последовательностей, задаваемых человеком (например, файл, созданный программой финансового учета на основе исходных данных, введенных бухгалтером)» [7, с. 32].

Мы согласны с мнением В. Б. Вехова и А. Л. Осипенко о том, что следы, образованные в результате совершения преступных действий с использованием компьютерных технологий, целесообразно относить к электронно-цифровым следам: они представляют собой информацию, оставленную на средстве компьютерной техники, либо в смартфоне, либо на съемных носителях электронной информации, непосредственно связанных с событием преступления, и выражены или в виде информации, отражающей свойства материальных объектов либо результатов работы пользователя, или в виде сведений о процессах ее ввода, обработки и передачи.

Сегодня практически исчез традиционный способ сбыта наркотических средств, когда свертки и деньги передавались из рук в руки. Установление лиц, совершивших такие

преступления,
и доказывание их причастности к преступлению всегда сопровождались трудностями. С появлением новых способов сбыта (помещение заранее подготовленных закладок в тайники, что позволяет исключить личные встречи сбытчика и приобретателя и сохранить конфиденциальность) ситуация еще более осложнилась, поэтому поймать сбытчика за руку практически невозможно. Перед задержанием с поличным нужно провести целый комплекс оперативно-разыскных мероприятий, направленных на установление способа совершения преступления, лиц, участвующих в его совершении, и способа передачи наркотического средства. Оплата осуществляется покупателем переводом по номеру мобильного телефона, который, как правило, обезличен либо зарегистрирован на третье лицо. Современные средства электронных платежей позволяют мгновенно переводить деньги на любые счета или телефонные номера из любой точки мира, при этом стороны друг с другом не встречаются и каких-либо материальных (квитанций, следов пальцев рук) или идеальных следов (признаков внешности сбытчика и приобретателя) не остается, что исключает в дальнейшем возможность опознания. Все сказанное обусловливает тот факт, что большинство преступлений, связанных с бесконтактным сбытом наркотических средств, остаются нераскрытыми.

Таким образом, представляется, что следы, которые образуются в результате бесконтактного сбыта наркотических средств, т. е. электронно-цифровые следы, необходимо искать тогда, когда имеется подозреваемое лицо (задержано при проведении оперативно-разыскных мероприятий либо в момент получения закладки) либо нужно доказать его причастность к совершению преступления уже в процессе расследования.

Для понимания того, где нужно искать электронно-цифровые следы, рекомендуется разделять их на два вида: пассивные и активные. Первые, как правило, пользователь оставляет непредумышленно: данные, которые остаются в результате входа в сеть Интернет (IP-адрес устройства, история посещений сайтов и др.). Вторые являются отражением осознанных действий, производимых в сети Интернет (сообщения в социальных сетях, мессенджерах, комментарии, посты, блоги и т. д.).

Чтобы скрыть электронно-цифровые следы, люди часто прибегают к различным ухищрениям: переезжают с одного места на другое, меняют технические устройства (смартфоны, планшеты, ноутбуки), используют анонимайзеры (специальные сервисы, позволяющие пользователю не только скрывать данные о своем местоположении, оборудовании, интернет-браузере и другую конфиденциальную информацию, но и посещать различные интернет-ресурсы, свободный доступ к которым по каким-либо причинам закрыт) [8]. Кроме того, для введения в заблуждение сотрудников правоохранительных органов и отведения от себя подозрений преступники осуществляют незаконное подключение к Wi-Fi роутерам незапароленных пользователей, находящихся в зоне доступа сети, либо подгадывают момент, когда пользователь, только подключившийся к сети Интернет, устанавливает пароль для ограничения подключения к Wi-Fi роутеру, перехватывают сигнал и взламывают пароль. Необходимо также отметить, что сегодня во многих общественных местах (торговых центрах, кафе, ресторанах, вокзалах, аэропортах и т. д.) можно свободно подключиться к Wi-Fi, что делают, в том числе, злоумышленники. Данное обстоятельство существенно затрудняет расследование преступления, поскольку в таких условиях установить преступника невозможно.

Однако, несмотря на все ухищрения, полностью скрыть свое пребывание в Интернете нельзя. Даже малозначительные действия любой давности могут дать информацию о личности пользователя. Лицо, которое причастно к совершению сбыта наркотических средств в сети Интернет, наверняка осуществляло вход и на другие сайты, форумы, в социальные сети, пользовалось поисковыми системами Google, Yandex, Mozilla Firefox и т. д. Электронно-цифровой след подобен отпечатку пальцев, поскольку является цифровой идентификацией человека. Он определяет контент, который будет показан пользователю, и сервисы, которые будут ему доступны. Время, проведенное в приложениях или сервисах, также фиксируется в информационной среде.

Отследить пассивный цифровой след, например установить IP-адрес пользователя сети Интернет, сегодня совсем не сложно. Для этого существует множество различных программ (Whois, REG.RU, Speed-tester, IpGeoBase и др.) [9, с. 110—114]. Но, как было сказано ранее, преступники могут использовать анонимайзеры. В данных случаях в истории посещения сайтов будет показан IP-адрес пользователя, не соответствующий реальному.

При взаимодействии с сотрудниками отдела «К» МВД России у владельцев, предоставляющих услуги анонимизации, можно запросить информацию о реальном IP-адресе пользователя, который заходил в Интернет в определенную дату и время. Однако не все сервисы анонимизации ведут журналы посещений, поэтому получить нужную информацию удается не всегда. Чтобы установить, реальный IP-адрес у злоумышленника или нет, можно воспользоваться сервисом https://2ip.ru/whois/. Ввести в строке IP проверяемый адрес, после чего программа выдаст хост, город, страну, название провайдера, которому принадлежит этот IP-адрес (рис. 1).

Рис. 1. Страница сайта Whois

Если IP-адрес принадлежит какой-либо хостинговой (имеет имя XX.XXX.XX.XXX.site.ru) или известной компании, то, вероятнее всего, это адрес анонимайзера или прокси-сервера. В случае когда адрес принадлежит одному из интернет-провайдеров (Билайн, Ростелеком и т. д.), он наверняка является реальным. В дальнейшем по нему можно установить данные лица, на которое зарегистрирован договор с компанией, предоставляющей услуги интернет-связи, и точное место пользователя в момент его выхода в сеть [10].

Для фиксации активных цифровых следов незаконного сбыта наркотических средств в сети Интернет следует прибегать к помощи специалиста. С его участием необходимо осмотреть техническое средство (смартфон, планшет, ноутбук, компьютер) подозреваемого либо в момент получения закладки покупателем, либо при ее помещении в тайник курьером. Если нужно доказать причастность лица к совершению преступления уже в процессе расследования, в протоколе следственного действия необходимо зафиксировать историю переписки, относящейся к событию преступления (сообщения в социальных сетях, мессенджерах, комментарии, посты, блоги и т. д.). Рекомендуется также обращать внимание на то, установлены на техническом средстве подозреваемого приложения для осуществления электронных платежей или нет. Если таковые имеются, их нужно просмотреть, а в протоколе зафиксировать сведения о переводах денежных средств, номерах телефонов либо счетах, куда были переведены деньги. Эта информация поможет установить владельцев указанных счетов и даст направление дальнейшему расследованию.

При обнаружении и фиксации следов незаконного сбыта наркотических средств в сети Интернет сотрудники следственных подразделений часто сталкиваются с многочисленными трудностями, обусловленными недостаточностью специальных знаний в области компьютерных технологий. Чтобы избежать их, следователям необходимо организовывать взаимодействие с оперативными подразделениями отдела «К» МВД России, непосредственно занимающимися выявлением, пресечением и раскрытием компьютерных преступлений. Следственные действия по обнаружению и фиксации информации в компьютерной технике либо информационно-телекоммуникационном пространстве нужно проводить с участием специалиста, который поможет обнаружить всю имеющуюся информацию и правильно ее зафиксировать. Перечисленные мероприятия будут способствовать
не только полному и своевременному обнаружению следов и их фиксации, но и качественному раскрытию и расследованию преступлений.

1. Мещеряков В. А. Основы методики расследования преступлений в сфере компьютерной информации: автореф. дис. … д-ра юрид. наук. Воронеж, 2001. 387 с.

2. Волеводз А. Г. Следы преступлений, совершенных в компьютерных сетях // Российский следователь. 2002. № 1. С. 4—12.

3. Козлов В. Е. Теория и практика борьбы с компьютерной преступностью. М.: Горячая линия — Телеком, 2002. 336 с.

4. Черкасов В. Н., Нехорошев А. Б. Кто живет в «киберпространстве»? Управление защитой информации. 2003. Т. 7. № 4. С. 468.

5. Российская Е. Р., Рядовский И. А. Концепция цифровых следов в криминалистике // Аубакировские чтения: материалы междунар. науч.-практ. конф. (Алматы, 19 февраля 2019 г.). Алматы, 2019. С. 6—9.

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

7. Осипенко А. Л. Проблемы вовлечения электронно-цифровых следов в уголовный процесс // Научный вестник Омской академии МВД России. 2009. № 4 (35). С. 31—34.

8. Что такое анонимайзер? URL: http://cameleo.xyz/chto-takoe-anonymizer.html (дата обращения: 09.09.2020).

9. Решняк О. А. Использование компьютерных технологий при расследовании преступлений в сфере незаконного оборота опасных психоактивных веществ: дис. … канд. юрид. наук. Волгоград, 2020. 229 с.

10. Я тебя по IP вычислю, или Можно ли найти человека, имея его IP адрес. URL: https://2ip.ru/article/findaddress (дата обращения: 09.09.2020).

1. Meshcheryakov V. A. Fundamentals of methods of crime investigation in the field of computer information. Abstract of dissertation of the doctor of juridical sciences. Voronezh; 2001: 387.

2. Volevodz A. G. Traces of crimes committed in computer networks. Russian investigator. 2002; 1: 4—12.

3. Kozlov V. E. Theory and practice of combating cyber-crime. Moscow: Goryachaya linia — Telecom; 2002: 336.

4. Cherkasov V. N., Nekhoroshev A. B. Who lives in "cyberspace"? Information security management. 2003; 7; 4: 468.

5. Rossiyskaya E. R., Ryadovsky I. A. The concept of digital traces in forensic science. In: Aubakirov's readings: materials of the International scientific and practical conference, 19 February 2019, Almaty, Kazakhstan. Almaty; 2019: 6—9.

6. Vekhov V. B. Forensic doctrine of computer information and means of its processing. Abstract of dissertation of the doctor of juridical sciences. Volgograd; 2008: 45.

7. Osipenko A. L. Problems of involving electronic digital traces in the criminal process. Scientific Bulletin of the Omsk Academy of the MIA of Russia. 2009; 35 (4): 31—34.

8. What is anonymizer? Available from: http://cameleo.xyz/chto-takoe-anonymizer.html. Accessed: 9 September 2020.

9. Reshnyak O. A. Use of computer technologies in the investigation of crimes in the field of illegal trafficking in dangerous psychoactive substances. Dissertation of the candidate of juridical sciences. Volgograd; 2020: 229.

10. I'll track you down by your IP, or Is it possible to find a person with his IP address. Available from: https://2ip.ru/article/findaddress. Accessed: 9 September 2020.

Решняк Ольга Александровна,
старший преподаватель
кафедры криминалистики
учебно-научного комплекса
по предварительному следствию
в органах внутренних дел
Волгоградской академии МВД России;
e-mail: volakdm@va-mvd.ru

Резван Александр Павлович,
профессор кафедры криминалистики
учебно-научного комплекса
по предварительному следствию

Reshnyak Olga Alexandrovna,
senior lecturer at the criminology department
of the training and scientific complex
of preliminary investigation
in law-enforcement bodies
of the Volgograd Academy of the Ministry
of the Interior of Russia;
e-mail: volakdm@va-mvd.ru

Rezvan Alexander Pavlovich,
professor at the criminology department
of the training and scientific complex
of preliminary investigation

в органах внутренних дел
Волгоградской академии МВД России,
доктор юридических наук, профессор;
e-mail: volakdm@va-mvd.ru

in law-enforcement bodies
of the Volgograd Academy of the Ministry
of the Interior of Russia,
doctor of juridical sciences, professor;
e-mail: volakdm@va-mvd.ru