УДК 343(575+14) : 004.7

ОТДЕЛЬНЫЕ ВОПРОСЫ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ В СФЕРЕ НЕЛЕГАЛЬНОГО ОБОРОТА НАРКОТИКОВ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ СЕТИ ИНТЕРНЕТ

PARTICULAR ISSUES OF COUNTERACTING CRIMES IN THE SPHERE OF ILLICIT DRUG TRAFFICKING COMMITTED BY MEANS OF THE INTERNET NETWORKS

Молоков Вячеслав Витальевич,
начальник кафедры информационно-правовых дисциплин и специальной техники Сибирского юридического института МВД России (г. Красноярск), кандидат технических наук, доцент

vvmolokov@mail.ru

Ключевые слова:
незаконный оборот наркотиков, раскрытие и расследование преступлений, специальные технические знания, оперативно значимая информация, Интернет.

В статье рассматриваются отдельные задачи, которые необходимо решать в процессе выявления, раскрытия и расследования преступлений в сфере незаконного оборота наркотиков, совершаемых посредством сети Интернет. Поэтапно раскрываются мероприятия по получению оперативно и криминалистически значимой информации. Предлагаются варианты решения оперативно-технических задач противодействия наркопреступлениям.

Keywords:
illegal drug trafficking, investigation and solution of crimes, specific technical knowledge, operational and significant information, the Internet.

The article considers the certain tasks that should be solved while detecting, solving and investigating crimes in the sphere of illicit drug trafficking by means of the Internet networks. The activities of getting operational and forensic significant information are represented in stages. The ways of solving operational and technical tasks of counteracting drug crimes are suggested.

Современная ситуация развития интернет-технологий намного расширяет возможности всемирной паутины, предлагая различные сервисы, приложения, инструменты проектирования, ориентированные на широкие массы пользователей сети. Не надо обладать специализированным техническим образованием, чтобы легко пользоваться готовыми решениями, по умолчанию установленными на популярных устройствах, таких как смартфоны, планшеты и другие умные гаджеты. Виртуальный мир Интернета интегрировался с реальной жизнью, с ее социальными проявлениями и экономическими отношениями. Вместе с положительной реальностью в сеть Интернет проникла угроза противоправной деятельности, ставшая изнанкой виртуализации денежных отношений, безграничной коммуникации между пользователями, автоматизации товарных операций. На текущий момент наиболее остро стоят проблемы мошенничества, использования сети Интернет в незаконном обороте наркотиков, распространения идеологии экстремизма и терроризма, легализации доходов, добытых преступным путем. Таким образом, актуально противостоять преступности не только в реальном мире, но и на просторах Интернета.

В направлении противодействия преступлениям, совершаемым с использованием сети Интернет, находятся правоохранительные органы, регуляторы в сфере связи, информационных технологий и коммуникаций, общественные организации, кибердружины. Государство прилагает усилия для ограждения информационно-телекоммуникационного пространства сети Интернет от преступных проявлений. Революционным шагом стал разработанный законопроект о суверенном Интернете [6], предполагающий ряд организационно-технических мер по обеспечению комплексной безопасности российского сегмента сети Интернет. Тем не менее на переднем фронте борьбы всегда находятся правоохранительные органы, и им необходимо решать различного рода задачи по выявлению, раскрытию и расследованию преступлений, совершаемых посредством сети Интернет.

Раскроем возможности и механизмы противодействия преступлениям в сфере незаконного оборота наркотиков, совершаемым с использованием сети Интернет. Обратим внимание на мероприятия по получению оперативно и криминалистически значимой информации, доступной в открытых источниках.

Бесконтактный сбыт наркотических средств и психотропных веществ, как правило, имеет типовую структуру организованной преступной группы и схему сбыта. Для формирования предложения наркотиков на просторах всемирной паутины создаются различные информационные ресурсы в виде сайтов, форумов, сообществ в социальных сетях, групп пользователей и каналов в мессенджерах. Все контакты и обмен информацией поддерживаются приложениями интернет-коммуникаций, при этом используются средства анонимизации и закрытия передаваемого трафика. [2] Место закладки наркотиков сообщается

после перечисления денег на виртуальные счета организаторов. Легализация преступных доходов осуществляется с использованием алгоритмов перевода в различных электронных финансовых системах.

Первым этапом противодействия нелегальному обороту наркотиков, осуществляемому посредством сети Интернет, является выявление информационных ресурсов, так или иначе использующихся для их сбыта. Это могут быть сайты, на которых формируется предложение наркотиков, публикуется прайс-лист и работает личный кабинет покупателя, через который осуществляется взаимодействие с продавцом. Причем интернет-магазин работает в бот-режиме, то есть администратор не участвует в общении с потребителем, а только формирует базу мест закладок. Координаты закладки сообщаются покупателю только после перевода обозначенной суммы на электронный кошелек. На просторах Интернета до сих пор существуют форумы, посвященные вопросам организации бесконтактного сбыта и предоставляющие платформу для размещения новых интернет-магазинов. [3] Социальные сети нередко содержат информацию, пропагандирующую потребление наркотических средств и психотропных веществ, в закрытых группах обсуждаются вопросы, связанные с источниками приобретения наркотиков. Пользуясь анонимностью, которую предоставляют некоторые каналы в мессенджерах, они также используются для организации бот-магазинов.

Таким образом, речь идет об интернет-площадках, которые содержат следующие ключевые признаки:

– пропаганда потребления наркотических средств и психотропных веществ;

– предложения о продаже тех или иных наркотиков;

– сервисы организации бесконтактного сбыта;

– предложения о найме на работу в составе организованных преступных групп.

Остановимся на методах выявления таких интернет-ресурсов. Так как сеть Интернет не является формализованным источником информации, ее поиск осуществляется обычно с использованием поисковых машин, типа Яндекс, Google, Rambler и т.п. Значит, для обнаружения противоправного контента, содержащего обозначенные ранее признаки, необходимо использовать ключевые слова, содержащие сленговые названия наркотических средств, признаки сбыта и пропаганды. Для эффективного поиска следует применять язык запросов – специальные операторы поисковых машин, значительно сужающие круг поисковой выдачи и повышающие релевантность ответов. Подобно осуществляется поиск в социальных сетях, причем многие из них обладают собственным языком запросов, например сеть «ВКонтакте». Уместно легендированное посещение специализирующихся на сбыте наркотиков интернет-форумов.

После обнаружения таких ресурсов следует зафиксировать факт распространения противоправной информации, а именно сделать скриншот экрана страницы и сохранить из адресной строки браузера универсальный указатель страницы в сети Интернет (URL). Также рекомендуется документировать и иную информацию, которая в дальнейшем может быть использована в оперативных целях или при доказывании факта незаконного сбыта.

Затем следует оградить остальных пользователей всемирной паутины от нежелательного контента. Регулятором этого процесса выступает Роскомнадзор. На его сайте находится форма для подачи жалобы, где указываются признаки противоправной информации, адрес ресурса и прикрепляется по возможности скриншот изображения. В случае обнаружения признаков противоправной информации эксперты Роскомнадзора применяют алгоритм блокировки указанного адреса или страницы в сети Интернет. Работает он предельно просто. Указатели страницы или IP-адрес ресурса, содержащего запрещенную информацию, помещаются в единый реестр, затем все интернет-провайдеры российского сегмента сети обязаны читать его не реже двух раз в сутки и на основе специальных фильтров ограничивать доступ своих абонентов к этим сайтам. Если противоправная информация распространяется в социальной сети, то рекомендуется направить жалобу администраторам этой сети.

Процесс дальнейшего раскрытия преступной группы неразрывно связан с получением оперативно и криминалистически значимой информации. Собирать ее можно как аналитически с использованием все тех же инструментов эффективного поиска, так и техническим путем, формируя задания для подразделений бюро специальных технических мероприятий (БСТМ).

В первом случае следует исследовать сайты, социальные сети, форумы на предмет нахождения информации, так или иначе относящейся к возможным фигурантам дела. [4] Современный человек оставляет в Интернете различные следы своего пребывания, регистрируясь в социальных сетях, форумах, сервисах электронного взаимодействия, почтовых ресурсах, сохраняя свои заметки, фотографии, контакты. Процесс поиска сравним с интернет-разведкой, которую можно осуществлять с любого компьютера, подключенного к Интернету. Безусловно, должны соблюдаться правила обеспечения информационной безопасности, в частности использоваться фейковые аккаунты, анонимные прокси-серверы или VPN-туннели и т.п.

Техническое получение информации основано на владении специальными знаниями в области сетевых технологий. [5] Здесь важно представлять, что основным идентифицирующим признаком сетевого устройства (компьютер, смартфон, модем и т.п.) является его IP-адрес. Он используется для идентификации устройства в сети и маршрутизации к нему данных. За счет указания IP-адреса осуществляется доставка пакетов в пункт назначения. Сетевой па-

кет обязательно содержит в заголовке IP-адрес отправителя и получателя. По сути, от источника данных до приемника организуется некоторая цепочка связи, в которой всегда есть непосредственно само сетевое устройство, которым пользуется пользователь, затем его интернет-провайдер и далее узел назначения. Раскрытие такой цепочки способствует установлению личности подозреваемого лица. Следует собрать как можно больше сведений о маршрутах и IP-адресах прохождения пакетов, времени их продвижения, адресах портов соединения. Для этого могут быть использованы системы обеспечения оперативно-розыскных мероприятий (СОРМ), установленные на оборудовании каждого оператора связи. Максимально объективной информацией об абонентском устройстве обладает интернет-провайдер. В соответствии с законодательством Российской Федерации оператор связи обязан хранить шесть месяцев все передаваемые от абонентов данные и три года факты таких сообщений. [7] Кроме этого информацию об IP-адресе любого ресурса и его возможном хостинге можно установить самостоятельно с использованием простых сетевых сервисов типа 2ip.ru или xinit.ru. Полезную информацию о домене может дать сервис Whois. Криминалистически значимой информацией является физический адрес устройства (MAC-адрес), его получение способствует расширению доказательной базы причастности пользователя к осуществлению противоправных действий с помощью имеющихся компьютерных средств.

Контроль и документирование интернет-мессенджеров – основные задачи, которые необходимо решать в процессе раскрытия участников организованной группы. Заявление разработчиков, что наиболее популярные мессенджеры типа Viber, WhatsApp или Telegram используют алгоритмы шифрования на уровне контактирующих абонентов (end-to-end), делают их популярными в криминальной среде. Есть основания предполагать, что в законном порядке документирование сообщений возможно, как и определение конкретного географического положения устройства на местности. В настоящее время действуют правила о предоставлении сервисами интернет-коммуникаций номеров телефонов, соответствующих определенным контактам. [8] Часто фигуранты преступных групп используют IP-телефонию (VoIP). Подходы к документированию и отслеживанию источника звонка также основаны на анализе трафика интернет-провайдеров и запросов к операторам электронной связи.

Несмотря на открытость стандартного механизма маршрутизации интернет-трафика злоумышленники используют методы анонимизации. Наиболее популярные из них: анонимные прокси-серверы, виртуальные частные сети (VPN), децентрализованные сети типа Tor. Это значительно противодействует процессу раскрытия и расследования такого рода преступлений. Однако следует ожидать расширение возможностей аппаратуры СОРМ за счет внедрения систем глубокого анализа трафика (DPI). Деанонимизации по-

добного рода пользователей может содействовать принятие законопроекта об обеспечении комплексной безопасности российского сегмента сети Интернет. Многие технические мероприятия, которые должны будут осуществлены, способны выявлять и отслеживать трафик, принадлежащий анонимным сервисам.

В финансовом обороте нелегального наркорынка задействованы различные электронные платежные системы. Для установления каналов получения прибыли следует фиксировать электронные адреса и IP-адреса входа-выхода всех кошельков, счетов и иных платежных систем. Официальное обращение в администрацию таких сервисов позволяет запрашивать транзакции движения денежных средств и выстраивать схемы легализации преступных доходов.

Определенную трудность в целях расследования преступлений составляют криптовалюты. [1] Они базируются на децентрализованных вычислениях, защищены криптографией и анонимны. Все транзакции в системе открыты, база операций хранит их с самого создания криптовалюты. Криминалистически значимую информацию о принадлежности адресов и паролей можно получить только от пользователя, либо с помощью компьютерно-технической экспертизы. Монетизация виртуальных денег осуществляется на специальных биржах, если контролировать операции вывода на реальные счета, то можно устанавливать криминальные схемы легализации.

Таким образом, определим, какие оперативно-технические мероприятия должны быть отработаны в целях раскрытия преступлений в сфере нелегального оборота наркотиков, совершаемых с использованием сети Интернет:

1. Поиск и анализ априорной информации о структуре сбыта, фигурантах преступных групп и используемых средствах интернет-коммуникаций в открытых источниках;

2. Установление исходящих (входящих) IP-адресов интернет-провайдеров, хостинг-провайдеров, операторов телекоммуникационной связи, электронных кошельков, электронных бирж и т.п., используемых в организации бесконтактного сбыта наркотиков;

3. Направление официальных запросов в администрации интернет-компаний или сервисов для уточнения сведений, касающихся лиц, которые используют либо администрируют средства интернет-коммуникаций, использующиеся в преступной деятельности;

4. Технический контроль телекоммуникационных каналов и документирование трафика фигурантов дела.

5. Установление иной криминалистически значимой информации на изъятых компьютерных устройствах.

Следует отметить, что процесс раскрытия подобного рода преступлений не имеет четкого алгоритма действий, которые могут привести к выявлению организаторов бесконтактного сбыта наркотических средств и психотропных

веществ в сети Интернет. Предлагаемые мероприятия являются инструментами для эффективного решения поставленных перед органами внутренних дел задач в сфере противодействия незаконному обороту наркотиков.

Библиографический список

1. Галушин, П.В. Сведения об операциях с криптовалютами (на примере биткойна) как доказательство по уголовному делу / П.В. Галушин, А.Л. Карлов // Ученые записки Казанского юридического института МВД России, 2017. – Т. 2. – №4. – С. 90-100.

2. Молоков, В.В. Средства противодействия раскрытию преступлений в сфере незаконного оборота наркотиков, совершаемых с использованием сети Интернет / В.В. Молоков // Национальный и международный уровни противодействия наркоугрозе и взаимодействие в сфере реабилитации и ресоциализации наркопотребителей : материалы XVIII международной научно-практической конференции. – Красноярск : СибЮИ ФСКН России, 2015. – Ч. 2. – С. 56-60.

3. Молоков, В.В. Интернет и наркотики / В.В. Молоков // Актуальные проблемы профилактики наркомании и противодействия правонарушениям в сфере легального и нелегального оборота наркотиков: материалы XV международной научно-практической конференции : в 3 ч. – Красноярск : СибЮИ ФСКН России, 2012. – Ч. 1. – С. 72-75.

4. Молоков, В.В. Получение криминалистически значимой информации в сети Интернет / В.В. Молоков // Криминалистическое обеспечение расследования преступлений: проблемы, перспективы и инновации : материалы международной науч.-практ. конф., посвященной 45-летию кафедры криминалистики юридического факультета БГУ, Минск, 12-13 октября 2017 г. / БГУ ; редкол. В. Б. Шабанов (отв. ред.) [и др.]. – Минск : изд. центр БГУ, 2017. – С. 205-207.

5. Молоков, В.В., Галушин, П.В. Специальные технические знания, необходимые для эффективного раскрытия и расследования преступлений в сфере незаконного оборота наркотиков, совершаемых посредством сети Интернет / В.В. Молоков, П.В. Галушин // Вестник Сибирского юридического института ФСКН России: научно-практический журнал. – Красноярск : СибЮИ ФСКН России, 2016. – Вып. №2 (23). – С. 138-142.

6. О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации» (в части обеспечения безопасного и устойчивого функционирования сети «Интернет» на территории Российской Федерации) : законопроект №608767-7. – URL: https://sozd.duma.gov.ru (дата обращения: 15.05.2019).

7. О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности : Федеральный закон от 06.07.2016 №374-ФЗ // СПС КонсультантПлюс.

8. Об утверждении Правил идентификации пользователей информационно-телекоммуникационной сети «Интернет» организатором сервиса обмена мгновенными сообщениями : постановление Правительства РФ от 27.10.2018 №1279 // СПС КонсультантПлюс.