ПРОТИВОДЕЙСТВИЕ СОВЕРШЕНИЮ БЕСКОНТАКТНЫХ ПРЕСТУПЛЕНИЙ С ИСПОЛЬЗОВАНИЕМ ЦИФРОВЫХ ТЕХНОЛОГИЙ

В статье рассмотрены вопросы выявления способов совершения преступлений, связанных с незаконным оборотом наркотических веществ, а также приведены типичные схемы контактного и бесконтактного распространения наркотических веществ на территории РФ. Более подробное внимание обращено на схему бесконтактного распространения наркотических веществ и на проблемы противодействия совершению бесконтактных преступлений с использованием цифровых технологий. Кроме того, в статье предложены современные организационно-правовые и технические направления борьбы с незаконным оборотом наркотических веществ с применением цифровых технологий. Был сделан важный вывод, что успешное противодействие совершению бесконтактных преступлений возможно в тех случаях, в которых будет применяться аналитическая система, позволяющая проводить оперативно-розыскные мероприятия с применением цифровых технологий, машинного обучения и технологии Больших данных.

Ключевые слова: незаконный оборот наркотических веществ, бесконтактный способ сбыта наркотических веществ, цифровые технологии, Интернет, Большие данные, машинное обучение.

COUNTERACTION TO THE COMMISSION OF CONTACTLESS CRIMES USING DIGITAL TECHNOLOGY

The article discusses the issues of identifying methods of committing crimes related to the illicit trafficking of narcotic substances, as well as typical schemes of contact and contactless distribution of narcotic substances in the Russian Federation. More detailed attention is paid to the scheme of contactless distribution of narcotic substances and to the problems of counteracting the commission of contactless crimes using digital technologies. In addition, the article proposes modern organizational, legal and technical directions of the fight against drug trafficking using digital technologies. An important conclusion was made that successful counteraction to the commission of contactless crimes is possible in those cases in which an analytical system will be used to conduct operational-search measures using digital technologies, machine learning and Big Data technology.

Keywords: drug trafficking, non-contact way of selling drugs, digital technology, Internet, Big data, machine learning.

Наркотическим веществом называют вещество естественного или искусственного происхождения, которое влияет на психические функции организма с целью его изменения, а при многочисленном и продолжительном употреблении приводит к химической, физической и психической зависимости[1].

В настоящее время ситуация по употреблению наркотиков в РФ складывается катастрофическим образом [2]. Удельный вес синтетических наркотиков в общей массе изымаемых наркотических средств и психотропных веществ на протяжении последних 10 лет увеличился в 13 раз [3].

В связи со стремительным развитием цифровых технологий, глобальной информационной сети Интернет и современных операторов сотовой связи в последние годы злоумышленники начали активно использовать совершенно новые преступные схемы [4-6].

Если рассматривать контактную схему распространения наркотических веществ на территории РФ, то чаще всего их продажа происходит следующим образом [7]: поставщики наркотических средств организуют их поставку в Россию, затем специально обученные для этих целей операторы, которые географически находятся в другом реги-

оне, сообщают о прибытии «товара». Одновременно с этим они сообщают номера телефонов и счетов, на которые следует перевести деньги. Потенциальные покупатели переводят средства на полученный счет. Участники группировки создают тайник, адрес нахождения которого диспетчер отправляет сообщением уже самому потребителю. Непосредственного контакта при такой схеме «работы» между участниками группировки, покупателями и диспетчерами не происходит. Для дальнейшего сокрытия следов номера телефонов и счетов, на которые перечисляются деньги, заменяются не реже, чем раз в неделю [7].

Подробная схема бесконтактного распространения наркотических веществ описана в работах[8,9]. В этой схеме существуют должности, занявшие свои места по порядку подчинения. Должностные инструкции сотрудников подробно прописаны, соблюдаются меры безопасности. Названия должностей звучат следующим образом: кураторы, хакры, кладовщики, закладчики или дропы, операторы, директор и другие.

Участники группировки общаются с помощью приложений-мессенджеров, например, таких как Viber, Telegram, WhatsApp, ICQ и

менее распространенных – XMPP (более известный, как Джабер), Brosix [10].

Сотрудники, «добросовестно» выполняющие свои функции, могут быть переведены на следующую по ступени должность с другим окладом. Также как и члены, допустившие ошибки в своей работе, подвергаются штрафу.

Все «работники» команды имеют подробные инструкции, где описывается, как вести себя в случае, если произошло задержание сотрудниками полиции. Также там имеется обучающая информация, касающаяся хранения, транспортировки, фасовки, пользования счетами, электронными платежами. Особое внимание уделяется использованию анонимных методов общения в Интернете, а также посещению опасных или запрещенных страниц.

Среднестатистический пользователь персонального компьютера может зайти в интернет и установить специальные программы anonymizer и прокси-серверы для скрытия информации о компьютере и его IP-адресе. Самые часто используемые для этих целей являются такие программы, как hideme, webwarper, Zip. Данные сервисы позволяют скрывать не только IP-адреса, но и информацию о географическом месте нахождения пользователя; браузер, который используется, а также переходить на запрещенные сайты, ранее заблокированные надзорными органами. Также программы-анонимайзеры позволяют загружать данные с файлообменников без временных требований и платной регистрации, посещать форумы и социальные сети, даже если они имеют статус заблокированных за нарушение правил сообществ.

С появлением сети VirtualPrivateNetwork или VPN, которая позволяет объединить несколько компьютеров, находящихся в разных концах мира, появилась такая возможность, как осуществление запрещенного доступа к ранее заблокированным платным и бесплатным сайтам. Суть использования этой сети в том, что зашифрованный секретный трафик с компьютера пользователя и интернет-провайдера отправляется на VPN-сервер, а далее происходит анонимный переход на заблокированный сайт. Пользователь может изменять IP-адрес своего компьютера, то есть со стороны он будет выглядеть как посетитель из другой страны, так как некоторые сервисы работают только для пользователей США и Европы.

Прокси-сервер – это промежуточный сервер, позволяющий клиентам осуществлять косвенные запросы к разным сетевым службам. То есть пользователь подключается в цепочку прокси-серверов и запрашивает какой-либо ресурс, расположенный на другом сервере. При этом сам запрос клиента или ответ сервера может быть изменен прокси-сервером для сохранения анонимности клиента. Разные прокси-серверы располагают разными возможностями. Например, одни из них позволяют скрыть данные об источнике запроса, другие – IP-адрес. Третьи изменяют адрес источника запроса. И если изначально эти серверы были направлены на использование в целях сохранения конфиденциальной информации о пользователе, то в последнее время их использование часто связано с получением доступа к запрещенным сайтам. Это объясняет популярность использования прокси-серверов для получения доступа к информационным ресурсам, запрещенным законом.

Отметим, что наркодилеры выделяют крупные суммы на покупку транспорта, устройств для использования сотовой и другой необходимой для работы связи, техники, оружия, разработки новых программ, аренду помещений, содержание «своего» персонала (охрана, водители, упаковщики), собственных лабораторий и т.п.

Незадолго до настоящего момента на территории Российской Федерации организационные моменты в схемах сбыта бесконтактными способами с использованием Интернета значительно изменились. Теперь буквально вся информация о разновидностях, массе, стоимости предлагаемого для продажи наркотических веществ, а также способах связи и оплаты размещается на определенных сайтах. Передача самого наркотического средства происходит посредством «закладок». Оплата осуществляется через разные электронные платежные сервисы (QIWI-кошелек, Яндекс.Деньги, WebMoneyTransfer, E-port.ru), на которые перечисляются виртуальные деньги.

Анализ предоставленной и собранной с помощью открытых источников информации дает возможность установить следующую схему сбыта наркотических средств, которая состоит из следующих этапов:

1) публикация информации о продаже наркотических веществ на сайтах, форумах в социальных сетях (VKontakte, Ok.ru и др.) на

сайтах знакомств и бесплатных досках объявлений, в даркнете, где в качестве контактных данных указываются никнейм (псевдоним) в программах Skype, Brosix, Jabber, адрес почтового ящика или номер телефона;

2) во время переписки продавец предлагает потенциальному покупателю подготовленный ранее прейскурант, где указано название вещества, стоимость и масса. А также сообщается информация о способах оплаты и получения желаемого вещества;

3) безналичная оплата предполагаемого заказа с помощью электронных платежных систем Qiwi, VisaWallet, WebMoneyTransfer, «Яндекс.Деньги». В последнее время отмечено использование пиринговой платежной системы Биткоин (BitCoin) и другой криптовалюты;

4) после подтверждения перевода денег происходит закладывание наркотического вещества в «тайники» или сообщаются заранее подготовленные точки с закладками;

5) заказчику описывают местонахождения «закладки» также с помощью переписки в интернете.

Также важно рассмотреть основные проблемы противодействия бесконтактного распространения наркотических веществ. Для более детального рассмотрения данного вопроса приведем схему преступной деятельности в межрегиональных и региональных крупных интернет-магазинах по сбыту наркотических веществ [11,12]. Она состоит из следующих пунктов:

1. Наличие самостоятельных структурных подразделений, имеющих свою иерархию, географически и функционально разделенных друг от друга, при этом находящихся под руководством одного лидера. Зачастую в каждом таком подразделении процесс преступной деятельности происходит от производства до незаконного сбыта. Количество структурных подразделений в зависимости от масштаба преступной деятельности может быть от двух до нескольких десятков. Например, у интернет-магазина «ХимПром», функционировавшего в форме организованной преступной группировки с годовым доходом 2,3 млрд рублей, филиалы были расположены в 14 регионах страны.

2. Многочисленный состав участников, доходящий до нескольких сотен человек с четко разделенными обязанностями (закладчики, диспетчеры, кассиры, курьеры, менеджеры по регионам, финансовые директоры,

специалистов в области информационной безопасности и т.д.) При этом руководство группировок может использовать свой, неизвестный до этого в криминальном мире, сленг для еще большей конспирации.

3. Использование мессенджеров для обмена сообщениями и медиафайлами при общении между участниками преступного сообщества. Следует отметить, что если еще несколько лет назад для мгновенного обмена сообщениями наиболее часто использовались такие общедоступные и известные приложения, как Viber, WhatsApp и ICQ, то сейчас для затруднения прослушивания телефонных переговоров правоохранными органами члены преступной группы все чаще применяют программы Telegram, Brosix, Pidgin, Xabber, Vipole, IM+, Psi и др.

4. Разработка и внедрение комплекса правил, позволяющих держать свои действия на высоком уровне секретности. Помимо использования вышеуказанных мессенджеров, также используются такие онлайн-сервисы для загрузки файлов, как Imgur, Radikal, Postimg. А для хранения и передачи покупателям фотографий мест тайников с наркотическими веществами, для передачи покупателям точных координат мест нахождения этих тайников используется картографический сервис GoogleMaps. Сервисы OneTimeSecret, Privnote позволяют после прочтения полученных по ссылкам сообщений безвозвратно удалять их через определенный отправителем непродолжительный период времени.

Вышеперечисленные программы и сервисы позволяют усложнить работу сотрудникам правоохранных органов, предотвратить утечку информации о преступной деятельности его участников и позволяют обезопасить руководство данного бизнеса от прямого участия в преступной деятельности.

В данный момент злоумышленники, распространяющие наркотические вещества, зачастую делают это с помощью площадок для обмена криптовалютой или биржи криптовалют [12]. По данным сайта, предоставляющем информацию об обменных пунктах и курсах обмена электронных денег – bestchange.ru, обходя законодательную сферу, в русскоязычном Интернете функционируют более 500 порталов для обмена криптовалюты на рубли. С помощью криптовалюты Ethereum и Bitcoin гонорары за работу получают сотрудники преступных группировок, кроме того,

при ее использовании для заказа «товара» в интернет-магазине цена товара снижается до 20%.

Для комплексной работы по борьбе с незаконным оборотом наркотических средств сотрудникам оперативных служб важно усилить работу по следующим направлениям [13]:

- начать сотрудничать с провайдером интернет-услуг, который на основании судебного решения предоставит следствию данные о посещаемых страницах компьютеров и телефонов подозреваемых;

- привлечь IT-специалиста для сбора и анализа информации сайтов, пропагандирующих незаконный оборот наркотических веществ, а также на установку программ, отслеживающих посещение интересующих интернет-ресурсов;

- подготовку запросов в Федеральную службу по надзору в сфере связи информационных технологий и массовых коммуникаций (Роскомнадзор) о блокировании подозрительных порталов;

- разработать аналитическую систему, которая позволит проводить оперативно-розыскные мероприятия с применением цифровых технологий, машинного обучения и технологии Больших данных.

Для комплексной оперативной работы при борьбе с преступной деятельностью наркодилеров важно систематически и комплексно осуществлять мониторинг сайтов и порталов, публикующих потенциально опасную информацию о наркотических веществах.

Быстроразвивающиеся современные цифровые технологии, доступность интернета для всех слоев населения, всеохватность социальных сетей создают препятствия для оперативной блокировки запрещенного контента. При этом сотрудники оперативных служб в рамках своих возможностей регулярно передают данные в Роскомнадзор для блокирования опасных сайтов посредством работы с провайдерами.

К минусам такого способа можно отнести время, которое приходится тратить, так как работа осуществляется при помощи человеческого ресурса. Поэтому автоматизирование с помощью специально настроенных программ для мониторинга позволило бы ускорить рабочий процесс и увеличить результат [14].

Для оперативного блокирования доступа пользователей интернета к контенту, содер-

жащему противоправную информацию, было бы разумным взаимодействие с отечественными поисковыми сервисами, например, такими как Yandex, Mail.Ru, Rambler, Rutube, Aport, Webalta, Nigma.

Важно признать, что для получения положительного результата в борьбе с наркопреступностью важно выстроить работу с интернет-провайдерами, выяснить, как оперативно получить имеющуюся у них информацию. Еще одну сложность на этом этапе представляют иностранные фирмы, которые предоставляют интернет и при этом территориально находятся за границей.

Большим подспорьем в работе по сбору информации о злоумышленниках является информация, оставленная в Интернете самими участниками преступлений. Сюда относятся случаи, когда пользователи восстанавливают пароль с помощью специальных серверов или оставляют свой номер телефона, а также другие личные данные на странице в социальных сетях.

Для улучшения работы сотрудников оперативных служб и ведомств, занимающихся разоблачением наркопреступлений в Интернет-пространстве, возможны следующие шаги для улучшения функционирования данного процесса [14]:

- 1) введение поправок в Федеральный закон «Об оперативно-розыскной деятельности», а именно дополнение положениями, которые позволят субъектам самостоятельно блокировать денежные переводы и счета (при наличии информации об их вовлеченности в сферу незаконного оборота наркотических веществ);

- 2) предоставление права субъектам оперативно-розыскной деятельности создавать сайты для обнаружения лиц, причастных к незаконному обороту наркотических средств;

- 3) постоянное совершенствование мониторинга и выявление интернет-ресурсов, созданных для сбыта наркотических средств;

- 4) привлечение на постоянной основе IT-специалистов, программистов для отслеживания посетителей сайтов, пропагандирующих незаконный оборот наркотических веществ;

- 5) создание банка данных нераскрытых преступлений, связанных с незаконным оборотом наркотических средств регионального уровня, а также автоматизированной информационной системы «Незаконный оборот

наркотических средств», состоящей из уже существующей и постоянно пополняющейся оперативной информации по части борьбы с незаконным оборотом наркотических средств.

Согласно проведенному исследованию важно на законодательном уровне рассмотреть следующие вопросы:

- введение обязательной регистрации юридических лиц, осуществляющих сделки с использованием цифровой валюты;
- запрет для некоммерческих организаций и банковских учреждений на проведение операций с криптовалютами с незарегистри-

рованными в установленном порядке юрлицами;

- привлечение к уголовной ответственности за теневой оборот криптовалюты;
- арест на оборот криптовалюты в случае следственных и оперативно-розыскных мероприятий, а также закрепление списка требований для обменных пунктов, бирж, банков для порядка изъятия криптовалюты;
- запрет и ответственность на законодательном уровне на массовую рассылку противоправной информации, а также приравливание мессенджеров к организаторам распространения информации.

Литература

1. Кожемякина М.Р. Информационная среда наркозависимых лиц // Сибирские уголовно-процессуальные и криминалистические чтения, 2016, №5(13).
2. Шалагин А.Е., Усманов И.М. Современная наркоситуация в Российской Федерации: тенденции, прогноз, меры противодействия // Вестник Казанского юридического института МВД России, 2016, №1(23).
3. Морозов, А.В. Особенности борьбы с наркопреступностью в сфере информационно-телекоммуникационных технологий / А.В. Морозов // Профессионал: научно-практический альманах МВД России, 2018, №3.
4. Осипенко А.Л., Миненко П.В. Оперативно-розыскное противодействие незаконному обороту наркотических средств, совершаемому с ИС использованием телекоммуникационных устройств // Вестник ВИ МВД России, 2014, №1.
5. Дикарев В.Г., Олимпиев А.Ю. К вопросу о противодействии бесконтактному способу сбыта наркотиков через сеть Интернет // Вестник Московского университета МВД России, 2016, №8.
6. Тимофеев С.В. Использование информационно-телекоммуникационных технологий при бесконтактном сбыте наркотических средств: проблемы противодействия и пути решения // Криминалистика: вчера, сегодня, завтра, 2018, №4(8).
7. Виноградов И.А., Загайнов В.В. Современные схемы «бесконтактного» сбыта наркотических средств и психотропных веществ // Криминалистика: вчера, сегодня, завтра, 2017, №2(2).
8. Богданов А.В., Ильинский И.И., Хазов Е.Н. Информационно-телекоммуникационная сеть Интернет как один из наиболее востребованных ресурсов в противодействии незаконному обороту наркотиков // Вестник Московского университета МВД России, 2018, №3.
9. Кушпель Е.В., Кулешов П.Е. Некоторые аспекты криминалистической характеристики незаконного сбыта наркотических средств, совершенного бесконтактным способом // Международный журнал прикладных и фундаментальных исследований, 2016, №2(1). С. 119–122.
10. Суходолов А.П. Цифровые технологии и наркопреступность: проблемы противодействия использованию мессенджера «Телеграм» в распространении наркотиков / А.П. Суходолов, А.М. Бычкова // Всероссийский криминологический журнал, 2019. Т. 13, № 1. С. 5–17.
11. Земцова С.И. Предмет допроса свидетелей при расследовании незаконного сбыта синтетических наркотических средств, совершенного с использованием интернет-магазинов // Криминалистика: вчера, сегодня, завтра, 2018, №3(7).
12. Земцова С.И. Интернет-магазины, осуществляющие незаконный сбыт синтетических наркотических средств: дифференциация и характерные признаки // Вестник Сибирского юридического института МВД России, 2019, №1(34).
13. Гурьянов К.В., Шатило Я.С. Организация противодействия распространению наркотиков через интернет Антинаркотическая безопасность, 2016, №1(6). С. 101–108.
14. Глушков Е.Л. Сбыт наркотических средств бесконтактным способом посредством сети Интернет: пути выявления и раскрытия // ППД, 2018, №2. С. 45–53.

References

1. Kozhemyachkina M.R. Informatsionnaya sreda narkozavisimykh lits // Sibirskiy ugolovno-protsessual'nyye i kriminalisticheskiye chteniya, 2016, №5(13).
2. Shalagin A.Ye., Usmanov I.M. Sovremennaya narkosituatsiya v Rossiyskoy Federatsii: tendentsii, prognoz, mery protivodeystviya // Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii, 2016, №1(23).
3. Morozov, A.V. Osobennosti bor'by s narkoprestupnost'yu v sfere informatsionno-telekommunikatsionnykh tekhnologiy / A.V. Morozov // Professional: nauchno-prakticheskiy al'manakh MVD Rossii, 2018, №3.
4. Osipenko A.L., Minenko P.V. Operativno-rozysknoye protivodeystviye nezakonnomu oborotu narkoticheskikh sredstv, sovershayemomu s ispol'zovaniyem telekommunikatsionnykh ustroystv // Vestnik VI MVD Rossii, 2014, №1.
5. Dikarev V.G., Olimpiyev A.YU. K voprosu o protivodeystvii beskontaktnomu sposobu sbyta narkotikov cherez set' Internet // Vestnik Moskovskogo universiteta MVD Rossii, 2016, №8.
6. Timofeyev S.V. Ispol'zovaniye informatsionno-telekommunikatsionnykh tekhnologiy pri beskontaktnom sbyte narkoticheskikh sredstv: problemy protivodeystviya i puti resheniya // Kriminalistika: vchera, segodnya, zavtra, 2018, №4(8).
7. Vinogradov I.A., Zagaynov V.V. Sovremennyye skhemy «beskontaktnogo» sbyta narkoticheskikh sredstv i psikhotropnykh veshchestv // Kriminalistika: vchera, segodnya, zavtra, 2017, №2(2).
8. Bogdanov A.V., Il'inskiy I.I., Khazov Ye.N. Informatsionno-telekommunikatsionnaya set' Internet kak odin iz naiboleye vostrebovannykh resursov v protivodeystvii nezakonnomu oborotu narkotikov // Vestnik Moskovskogo universiteta MVD Rossii, 2018, №3.
9. Kushpel' Ye.V., Kuleshov P.Ye. Nekotoryye aspekty kriminalisticheskoy kharakteristiki nezakonного sbyta narkoticheskikh sredstv, sovershennogo beskontaktnym sposobom // Mezhdunarodnyy zhurnal prikladnykh i fundamental'nykh issledovaniy, 2016, №2(1). S. 119–122.
10. Sukhodolov A.P. Tsifrovyye tekhnologii i narkoprestupnost': problemy protivodeystviya ispol'zovaniyu messendzhera «Telegram» v rasprostraneni narkotikov / A.P. Sukhodolov, A.M. Bychkova // Vserossiyskiy kriminologicheskii zhurnal, 2019. T. 13, № 1. S. 5–17.
11. Zemtsova S.I. Predmet doprosa svideteley pri rassledovanii nezakonного sbyta sinteticheskikh narkoticheskikh sredstv, sovershennogo s ispol'zovaniyem internet-magazinov // Kriminalistika: vchera, segodnya, zavtra, 2018, №3(7).
12. Zemtsova S.I. Internet-magaziny, osushchestvlyayushchiye nezakonnyy sbyt sinteticheskikh narkoticheskikh sredstv: differentsiatsiya i kharakternyye priznaki // Vestnik Sibirskogo yuridicheskogo instituta MVD Rossii, 2019, №1(34).
13. Gur'yanov K.V., Shatilo YA.S. Organizatsiya protivodeystviya rasprostraneni narkotikov cherez internet Antinarkoticheskaya bezopasnost', 2016, №1(6). S. 101–108.
14. Glushkov Ye.L. Sbyt narkoticheskikh sredstv beskontaktnym sposobom posredstvom seti Internet: puti vyavleniya i raskrytiya // PPD, 2018, №2. S. 45–53.

ФЕЛЬДМАН Елена Васильевна, доцент, кафедра «Компьютерной безопасности и прикладной алгебры», Челябинский государственный университет. 454001, г. Челябинск, ул. Бр. Кашириных, 129. E-mail: mila008.is@gmail.com

FELDMAN Elena, Associate Professor, Department of Computer Security and Applied Algebra, Chelyabinsk State University. 454001, Chelyabinsk, ul. Br. Kashirinykh, 129. E-mail: mila008.is@gmail.com