Секция «Криминалистика»

**Способы сокрытия преступной деятельности в сфере незаконного оборота наркотиков в сети «Интернет».**

***Андриянов Андрей Валерьевич***

*Студент (специалист)*

Омская академия Министерства внутренних дел Российской Федерации, Омская область, Россия

*E-mail: sfm21@yandex.ru*

31 декабря 2015 г. вступила в силу Стратегия национальной безопасности РФ, в которой говорится, что одной из основных угроз государственной и общественной безопасности является деятельность преступных организаций, связанная с незаконным оборотом наркотических средств и психотропных веществ [1]. Данная деятельность сопровождается тщательно продуманной «системой безопасности», целью которой является ее сокрытие. Для расследования необходима детальная проработка методов раскрытия, в частности, методов преодоления «системы безопасности» преступных организаций, активно использующих сеть «Интернет».

Изученными приговорами были установлены следующие основные способы сокрытия преступной деятельности в сфере НОН в сети «Интернет» [3][4].

1) *Наличие сложной структуры.* Преступные организации обладают строгой иерархической структурой, состоящей из отдельных звеньев, действующих обособленно в различных регионах и выполняющих определенные функции. Наличие данной структуры является мощнейшим способом сокрытия всей преступной деятельности, так как сама ее организация направлена на обеспечение конспирации.

2) *Отсутствие личных контактов.* Все общение, как внутри организации, так и с заказчиками происходит посредством использования сети «Интернет», не допуская личных контактов.

3) *Тщательный подбор участников и контроль за их деятельностью.* При вступлении в организацию тщательно собираются и проверяются персональные данные участников (фотографии, паспортные данные), которые, в случае, если участник не соблюдал «должностной регламент», размещались в открытом доступе в сети, либо применялись иные санкции. Как у вновь принимаемых «закладчиков», так и уже принятых, регулярно проводятся проверки качества организации тайников как с помещенными муляжами («пробными кладами»), так и с наркотическими средствами.

Данный элемент «системы безопасности» хотя непосредственно и не выполняет функцию конспирации, однако является одним из способов недопущения разглашения данных как от самих участников, так и от заказчиков, работа с которыми предполагает урегулирование любых конфликтов.

*4) Использование сети «Интернет» и мессенджеров с шифрованием передаваемой информации.*

Штат программистов обеспечивает создание форумов в сети «Интернет», а также бесперебойное функционирование программ мгновенного обмена сообщениями (мессенджеров), с шифрованием передаваемой информации. В частности, BROSIX, Telegram, WhatsApp. По заверениям создателя Telegram, получить доступ к переписке пользователей невозможно. К тому же, сервер находится не на территории РФ, в связи с чем, физическое изъятие невозможно. К примеру, одними из функций являются: создание секретных чатов с возможностью автоматического удаления переписки спустя указанный

промежуток времени, что ограничивает возможности последующего осмотра электронных устройств. Это подтверждается и регулярными сообщениями в СМИ: В Госдуме попросили ФСБ ограничить доступ к Telegram[5].

Еще одним элементом является использование интернет-кошельков, регистрация в которых, в отличие от банковских счетов, является более лояльной для использования. Наиболее распространенные: Яндекс.Деньги, Qiwi.

В целом, с помощью указанных средств операторы осуществляют связь с приобретателями наркотиков, а вышестоящие участники контролируют деятельность нижестоящих членов, поступление денежных средств от приобретателей и получение последними «закладок», сохраняя полную конфиденциальность.

5) *Использование способа передачи - закладки.* Само использование закладок является способом совершения преступления, однако им обеспечивается сокрытие деятельности, т.к. сохраняется анонимность передачи.

6) *Регистрация абонентских номеров на подставных лиц и их регулярная замена.* Так, в одной из преступных групп, не реже двух раз в месяц менялись абонентские номера всех участников и регистрировались на подставных лиц, запрещая использование зарегистрированных на участников организации.

7) *Использование при разговорах псевдонимов и общедоступных но понятных в преступной среде «слов».* Одним из способов сокрытия также является использование во время переговоров между собой и приобретателями терминов, дающих возможность двоякого толкования, но понятных и используемых в их среде.

*8) Регулярная смена жилых помещений и обеспечение безопасности имеющихся.* В целях сокрытия, преступники систематически меняют дислокацию мест сбыта и проживания. Для деятельности «складов» снимают обособленные помещения и оборудуют их системами видеонаблюдения.

9) *Уничтожение финансовых документов.* После сверки за учетный период финансовых документов, преступные группы стараются уничтожать всю учетную документацию.

Возможные варианты преодоления следователем.

*Допрос.* Подходит для всех способов, указанных в п. 1-9, при наличии подозреваемых лиц.

*Обыск.* Необходим для преодоления способов, указанных в п. 4,5,6,8, прежде всего, для поиска наркотиков, средств связи, документов.

*Контроль и запись переговоров. Получение информации о соединениях.* При возможности их проведения, целесообразно применять в случаях, указанных в п. 1,4,6, для установления участников группы, заказчиков, а также возможного района их местонахождения (биллинг).

*Осмотр электронных носителей информации.* Целесообразно применять осмотр устройств, используемых для выхода в сеть «Интернет» (смартфоны, компьютерная техника), историю просмотра, сохраненные пароли, мессенджеры и т.д. Однако, ряд авторов рекомендуют использовать судебно-компьютерную экспертизу [2].

*Поручение органу дознания.* На наш взгляд, для преодоления данной системы защиты необходимо комплексное применение ОРМ и следственных действий. Следует выделить следующие ОРМ: проверочная закупка; наблюдение; ПТП; контролируемая поставка; СИТКС и др.

**Источники и литература**

1) Указ Президента Российской Федерации от 31 декабря 2015 года № 683 «О Стратегии национальной безопасности Российской Федерации» // СПС Консультант плюс.
2) Клевцов В.В. Проблемные аспекты изъятия электронных носителей информации при расследовании распространения «дизайнерских» наркотиков с использованием сети Интернет // Российский следователь. 2015. № 6.
3) Приговор Нововятского районного суда г. Кирова по делу № 1-118/2015 г. от 22 октября 2015 г.: https://rospravosudie.com/court-novovyatskij-rajonnyj-sud-g-kirova-kirovskaya-oblast-s/act-499950732/
4) Приговор Приморского краевого суда по делу № 2-7/2010 от 27 октября 2010 года: https://rospravosudie.com/court-primorskij-kraevoj-sud-primorskij-kraj-s/act-100596314/
5) Российская газета : http://www.rg.ru/2015/11/16/telegram-site-anons.html