правило, мошеннические счета, номера телефонов действуют одну-две недели, потом их обнуляют и блокируют, после чего регистрируют новые уже на новых лиц.

Многие граждане думают, что с ними не может произойти такое происшествие. В беседе они сами признаются, что неоднократно слышали о таких способах мошенничества из средств массовой информации, их предупреждал об этом участковый уполномоченный полиции, но они не примеряют это на себя и не соблюдают те правила безопасности при обращении с электронным кошельком, которые предписаны в различных профилактических мероприятиях.

Исходя из вышесказанного, можно прийти к выводу, что способ совершения преступления, а также личность потерпевшего и в теоретическом, и в практическом плане должны изучаться самостоятельно и достаточно подробно, от этого в дальнейшем будет зависеть результативность раскрытия и расследования преступления.

Литература

1. Решняк О.А., Ковалев С.А. Организация расследования мошенничеств, совершенных с использованием сети «Интернет», на первоначальном и последующем этапах // Вестник Волгоградской академии МВД России. 2020. № 2 (53). С. 106-109.

2. Смагоринский Б.П., Сычева А.В. Новые способы совершения мошенничеств, связанных с распространением коронавирусной инфекции // Вестник Волгоградской академии МВД России. 2020. № 2 (53). С. 111-116.

Г.М. Семененко, *канд. юрид. наук, доцент*
Волгоградская академия МВД России

Проблемы раскрытия и расследования незаконного сбыта наркотических средств, совершаемого бесконтактно

В условиях научно-технического прогресса информационные технологии становятся ключевым фактором реализации и оптимизации деятельности человека. Сегодня роль информации и информационного пространства стала более значимой и для отдельного гражданина, и для государства в целом [5, с. 65].

Исследование криминогенной обстановки в Российской Федерации показывает, что количество преступлений, связанных с использованием информационно-телекоммуни-кационных технологий, имеет тенденцию к росту. По данным МВД России, в 2019 г. в стране было совершено почти 300 тысяч так называемых IT-преступлений (в 2018 г. кибермошенничеств было совершено на 68,5% меньше) [2].

Такая ситуация наблюдается практически в каждом регионе Российской Федерации. Об этом же говорит и Банк России. В 2019 г. им было заблокировано более 13 тысяч телефонных номеров, которые использовались в мошеннических целях, что в 29 раз больше, чем в 2018 г.; ограничены 1107 ресурсов, распространяющих вредоносное программное обеспечение, 10 683 фишинговых ресурса (их стало в пять раз больше), 370 массовых фишинговых рассылок. Информация о более чем 250 доменах в целях ограничения доступа направлена в Генеральную прокуратуру Российской Федерации [1]. Действительные размеры преступной активности в данной области остаются скрытыми. В 2019 г. в России со счетов физических лиц совершено несанкционированных переводов на сумму 5,7 млрд рублей [1].

Развитие современных цифровых технологий привело к тому, что в настоящее время для незаконного приобретения наркотических средств потребитель и сбытчик практически не встречаются. В последние годы получило широкое распространение использование сети Интернет для распространения наркотических средств бесконтактным способом, что в значительной степени затрудняет задержание продавца с поличным в момент сбыта наркотика. Информация о наличии наркотического средства распространяется на различных ресурсах в интернет-пространстве, а сам наркотик поступает потребителю через тайники-закладки [4, с. 26].

В связи с совершенствованием законодательства Российской Федерации в области контроля сетей электродокументальной связи, в т.ч. интернета, большинство сайтов, осуществляющих реализацию наркотических средств, внесено в список запрещенных, и к ним ограничен доступ из сети Интернет. Однако для обхода

запретов и ограничений в интернете имеется большое количество сайтов, в основном зарубежных, обеспечивающих анонимный доступ к указанным ресурсам. Более того, широкое распространение имеет сегодня программное обеспечение, основанное по принципу соединения с зарубежными серверами и создания сети анонимных пользователей. Запретить такое программным обеспечением или ограничить использование на данный момент не представляется возможным, т.к. они расположены за пределами Российской Федерации. Также следует отметить, что оплата наркотиков осуществляется с использованием электронных платежных систем, при этом зачастую используются счета, зарегистрированные на подставных лиц.

Сложность в раскрытии преступлений представляет тот факт, что преступники редко совершают преступления в том регионе, в котором они сами находятся. С целью сокрытия следов преступники зачастую используют симкарты для сотовых телефонов и банковские счета, зарегистрированные на подставных лиц, чужие документы и их копии. Преступниками используются и виртуальные платежные системы, и карты банков зарубежных государств, не выдающих России сведения об их владельцах.

Так, в ходе проведения оперативно-разыскных и следственных действий установлено, что в октябре 2016 г. неустановленные лица, являясь организаторами и руководителями организованной группы, осуществляли незаконный сбыт наркотических средств синтетического происхождения с использованием сети Интернет. Преследуя цель незаконного обогащения, вовлечения в преступную деятельность новых участников, расширения рынка сбыта наркотиков, получения стабильного дохода и увеличения прибыли, создали на территории Российской Федерации преступное сообщество (преступную организацию), а именно интернет-магазин «Радуга» для длительного, систематического совершения особо тяжких преступлений, связанных с незаконным сбытом наркотических средств.

Для достижения своих преступных целей организаторы преступного сообщества обеспечили создание в программе Telegram учетных записей с различными ник-неймами и контактными данными, которые для привлечения покупателей и расширения рынка сбыта наркотических средств разместили в качестве рекламы и в виде интернет-магазина «Радуга», на тематическом интернет-портале www.LegalRC .biz, включенном в Единый реестр интернет-ресурсов, содержащих информацию, распространение которой в Российской Федерации запрещено (утвержден Постановлением Правительства РФ от 26.10.2012 № 1101).

Организаторами преступного сообщества была определена следующая схема незаконного сбыта наркотических средств. На странице учетной записи «операторов» в программе Telegram был представлен прайс-лист с наименованием и стоимостью наркотических средств. Покупатель определял вид и количество приобретаемого наркотика, затем путем переписки с «оператором» в программе Telegram осуществлял заказ наркотика, получая от «оператора» номер виртуального счета (электронного кошелька) платежной системы Visa QIWI Wallet ООО «QIWI-Кошелек» для оплаты приобретаемого наркотика, а также комментарий, который необходимо было указать при оплате для его идентификации и подтверждения оплаты за конкретное наркотическое средство. После зачисления денежных средств на указанный счет покупатель сообщал «оператору» о произведенной оплате. «Оператор», отслеживая в режиме реального времени поступление денежных средств, сообщал покупателю адрес и место тайника с наркотическим средством.

Для поддержания связи, в целях конспирации и безопасности осуществления преступной деятельности, между участниками преступного сообщества было принято решение об использовании программы Xabber, применяемой для быстрого обмена сообщениями в информационно-телекоммуникационной сети Интернет.

Кроме того, при раскрытии и расследовании преступления сотрудники правоохранительных органов зачастую сталкиваются с такими проблемами, как невозможность установить личность абонента IP-телефонии, связанной с отсутствием установленного порядка верификации предоставляемых сведений (как правило, регистрация абонентов производится формально при внесении платежа по присланным по электронной почте персональным данным или скан-копиям паспортов); невозможность установления личности абонента IP-телефонии, использующего технологию подмены вызывающего номера; трудность в установлении данных об электронных платежах, совершаемых с использованием Интернет-ресурсов; невозможность установления данных об электронных платежах, совершаемых с использованием пла-

тежных систем и банковских карт банков-эмитентов, находящихся на территории стран, не поддерживающих международное сотрудничество правоохранительных органов с Российской Федерацией [3, с. 149].

Это далеко не полный перечень технических проблем, с которыми сталкиваются правоохранительные органы в процессе раскрытия и расследования дистанционных преступлений, связанных с незаконным оборотом наркотических средств.

Решение данной проблемы видится нам в выработке алгоритма совместных действий сотрудников правоохранительных органов и Роскомнадзора, Центробанка, операторов связи и провайдеров сети Интернет, средств массовой информации.

Перечень обозначенных нами проблемных вопросов в рамках раскрытия и расследования преступлений, связанных с незаконным сбытом наркотических средств дистанционно с использованием средств сотовой связи, конечно же, не является исчерпывающим. Однако предложенные меры помогут совершенствовать методику раскрытия и расследования преступлений данного вида, предупредить совершение преступлений, а затем и снизить их число на территории Российской Федерации.

Литература

1. Все, что вы публикуете, может быть использовано против вас. Статистика мошенничества с банковскими счетами. URL: https://yarcube.ru/news/economics (дата обращения: 25.06.2020).

2. Мошенники ушли в сеть. URL: https://rg.ru/2020/01/28 (дата обращения: 25.06.2020).

3. Пупцева А.В. Некоторые особенности выявления, раскрытия и расследования преступлений в сфере незаконного оборота наркотиков, совершенных с помощью сети «Интернет» бесконтактным способом // Вестник Волгоградской академии МВД России. 2018. № 3 (46).

4. Пупцева А.В. Проблемные вопросы выявления преступлений в сфере незаконного оборота наркотиков с использованием средств сотовой связи // Результаты научных исследований: сб. статей междунар. научно-практ. конф-ции (Тюмень, 15 февраля 2016 г.). Уфа: Аэтерна, 2016.

5. Семененко Г.М., Чхвимиани Э.Ж. Применение инновационных технологий в целях предупреждения дорожно-транспортных происшествий на территории Российской Федерации // Вестник Волгоградской академии МВД России. 2018. № 4 (47).

А.С. Скоревич
Юридический институт
Томского государственного университета

Устранение вызванных добросовестным заблуждением субъективных искажений в показаниях допрашиваемого

Расследование преступления имеет ретроспективную направленность ввиду того, что связано с уже произошедшим событием. Должностное лицо, выполняющее работу по расследованию произошедшего, преступление непосредственно не наблюдало, поэтому получает информацию о нём опосредованно. Источниками информации могут служить следовая картина преступления либо очевидцы, другие свидетели или сам преступник. Лицо, обладающее информацией о преступлении, допрашивается для получения следователем данных, имеющих криминалистическую ценность.

Таким образом, допрос содержательно представляет собой следственное действие, проведение которого направлено на получение информации о произошедшем событии преступления от лица, которое обладает этой информацией. Возможна ситуация, когда допрашиваемый подвержен добросовестному заблуждению, которое «является результатом неадекватного отражения действительности в силу особенностей протекания познавательных процессов» [5, с. 72]. Для того чтобы определить неправду, прежде всего, «необходимо уяснить, в какой степени мысли говорящего о действительности соответствуют действительности» [4, с. 200]. Отмечается также, что «иногда восприятие может быть искажено вследствие симпатии или предубеждения» [6, с. 320]. Сказанное определяет актуальность способов оптимизации проведения допроса, связанных с устранением субъективных искажений в показаниях допрашиваемого.