Анализ понятия «угроза безопасности» и его употребления в нормативных правовых актах позволяет согласиться с пониманием данной категории, приведенной в Концепции нацбезопасности, в соответствии с которой угроза – потенциальная или реально существующая возможность нанесения ущерба.

Вместе с тем некоторые положения данного нормативного правового акта не в полной мере соответствуют определению рассматриваемого понятия. Так, к числу основных угроз национальной безопасности причислены: деструктивное информационное воздействие, наносящее ущерб национальным интересам; нарушение функционирования критически важных объектов информатизации. Иными словами, к угрозам отнесены воздействия уже причинившие ущерб, что, по своей сути, не соответствует представленному выше подходу к пониманию угрозы как возможности нанесения ущерба.

Следует отметить, что в гл. 19 «Противодействие киберпреступности» Концепции инфбезопасности не используются рассмотренные в настоящей статье понятия, что, в определенной степени, может объясняться относительной новизной борьбы с данными преступлениями, отсутствием устоявшихся понятий и категорий, что естественно для этой интенсивно развивающейся сферы. Однако, как и для всех сфер человеческой длительности, построение эффективной системы противодействия киберпреступности возможно только при наличии сформированной теоретической и правовой основы функционирования. Соответственно, решение обозначенных и иных теоретико-прикладных проблем понятийно-категориального ряда информационной безопасности положительно отразится на решении задач обеспечения информационной безопасности и противодействии киберпреступности.

УДК 342.9

М.В. Губич, Д.А. Шкурко

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ НАРКОПРЕСТУПНОСТИ В СЕТИ ИНТЕРНЕТ

Интернет является практически идеальной площадкой для обеспечения коммуникации поставщиков и потребителей наркотических средств, координации деятельности и отмывания денег, что порождает ряд проблем в сфере противодействия наркопреступности в сети Интернет.

Так, виртуализация наркопреступности проявляется в создании интернет-магазинов по продаже наркотиков, оплате посредством электронных платежных систем, криптовалют, общении при помощи различных интернет-мессенджеров и интернет-приложений, осуществляющих шифрование получаемых и передаваемых данных, и т. д.

В докладе Международного комитета по контролю над наркотиками за 2021 г. неоднократно отмечается, что рост наркопреступности во многом связан с использованием перечисленных нами выше возможностей интернета [1].

Стремительное развитие сети Интернет превратило его использование в преступной деятельности в основной ресурс для распространения наркотиков, позволило перейти на бесконтактные способы сбыта наркотиков, что существенным образом изменило весь преступный наркобизнес, а также деятельность правоохранительных органов по противодействию рассматриваемым преступлениям.

Наиболее проблемным полем в сфере противодействия наркопреступности является деанонимизация лиц, причастных к совершению преступлений, связанных с незаконным оборотом наркотиков в сети Интернет, особенно в его теневом сегменте сети – DarkNet, доступ к которому возможен только посредством использования специализированных браузеров и программного обеспечения, например Tor – одна из самых популярных технологий для доступа в DarkNet, представляющая собой систему прокси-серверов, позволяющих устанавливать анонимное сетевое соединение. Данная сеть рассматривается как анонимная сеть виртуальных туннелей, предоставляющая передачу данных в зашифрованном виде.

Программное обеспечение Tor обеспечивает анонимность пользователя в сети Интернет, защищает его от анализа, скрывает IP-адрес используемого технического устройства, что затрудняет для представителей правоохранительных органов обнаружение следов, оставляемых преступниками в сети Интернет. Названные свойства достигаются за счет многоуровневого шифрования передаваемого трафика для нескольких произвольно выбранных узлов сети Tor и последовательной трансляции через эти узлы к получателю. Именно в сети Tor созданы и действуют онлайн-магазины, в которых предлагаются для продажи различные виды запрещенных веществ.

Активное использование в преступной деятельности интернет-мессенджеров, осуществляющих шифрование получаемых и передаваемых данных (Signal, Telegram, Vipole, Jabber и др.), также существенным образом трансформирует деятельность подразделений правоохранительных органов, осуществляющих борьбу с рассматриваемыми преступлениями. Это связано со следующими особенностями рассматриваемых мессенджеров: электронные ключи для расшифровки сооб-

щений создаются и хранятся на устройствах пользователей, а не на внешних серверах; в процессе отправки сообщения программным обеспечением отправителя и получателя по специальным алгоритмам генерируется уникальный ключ, дешифрование которого за разумное время представляется затруднительным, что делает передаваемую информацию труднодоступной для третьих лиц.

Наибольшее распространение в преступной деятельности, связанной с незаконным оборотом наркотиков, получило использование интернет-мессенджера Telegram. Преступниками все более активно используются специальные программы (боты), которые автоматизируют процесс продажи наркотиков, минимизируя участие в процессе распространения наркотиков физических лиц.

Следует отдельно отметить, что преступниками, в совокупности с рассмотренным программным обеспечением, активно используются специализированные технические средства, предназначенные для анонимизации пользователей в сети Интернет – анонимайзеры, VPN-сервисы, прокси-серверы.

Таким образом, деанонимизация лиц, причастных к совершению преступлений, связанных с незаконным оборотом наркотиков в сети Интернет, является одной из первоочередных задач, решаемых в ходе противодействия наркопреступности.

Необходимо отметить, что в Республике Беларусь принимаются определенные меры для решения указанной задачи. Так, в соответствии с Законом Республики Беларусь от 17 июля 2008 г. № 427-З (в ред. от 24.05.2021 г.) «О средствах массовой информации» среди оснований для ограничения доступа к интернет-ресурсу, сетевому изданию указывается распространение запрещенной информации (ст. 51^1). Постановлением Оперативно-аналитического центра при Президенте Республики Беларусь, Министерства связи и информатизации Республики Беларусь, Министерства информации Республики Беларусь от 3 октября 2018 г. № 8/10/6 (в ред. от 19.09.2022 г.) «Об утверждении Положения о порядке ограничения (возобновления) доступа к интернет-ресурсу, сетевому изданию» утвержден порядок ограничения доступа к интернет-ресурсам. Принимается ряд других правовых и организационных мер, направленных на недопущение «суперанонимности» пользователей сети Интернет.

Однако на практике применяемые в данном направлении меры являются недостаточно эффективными, что обусловлено многочисленными факторами, в том числе противодействием блокировкам со стороны разработчиков программных продуктов для анонимизации.

Кроме того, следует понимать, что эффективность поиска цифровых следов преступника, способствующих его деанонимизации, в значительной степени зависит от межгосударственного сотрудничества по

вопросам сбора, обработки, анализа, обмена информацией, представляющей оперативный интерес.

Необходимо отметить, что для органов внутренних дел наиболее актуальным является международное сотрудничество в целях получения значимой информации. Данное сотрудничество, как правило, осуществляется в рамках межправительственных и межведомственных договоров, либо при их отсутствии на основе принципа взаимности. При этом в силу имеющихся различий в законодательстве стран, даже при наличии нормативной базы, позволяющей осуществлять обмен информацией, ее получение не всегда возможно в силу объективных причин (короткие сроки хранения информации, усложнение процесса и т. д.).

Анализ международного и национального законодательства в сфере противодействия незаконному обороту наркотиков позволяет утверждать, что отсутствуют единые требования, обязательные для всех государств и иных субъектов, обеспечивающих функционирование сети Интернет и ее сегментов (поставщиков услуг интернета, хостинговых компаний, владельцев продуктов программного обеспечения и т. д.).

В целях разрешения указанной проблемы представляется возможным выстроить модель взаимодействия субъектов противодействия наркопреступности по аналогии с организацией межгосударственного взаимодействия в сфере борьбы с киберпреступностью, осуществляемого главным управлением противодействия киберпреступности МВД Республики Беларусь посредством национального контактного пункта (НКП), деятельность которого организована в соответствии с Положением о национальном контактном пункте МВД (утверждено приказом МВД Республики Беларусь от 12 июля 2021 г. № 201). Посредством НКП осуществляется взаимодействие с правоохранительными органами зарубежных стран и иностранными организациями, являющимися поставщиками интернет-услуг, при предупреждении, выявлении (раскрытии) и пресечении трансграничных и международных преступлений в сфере информационно-коммуникационных технологий.

Работа НКП организуется в режиме «24 часа в сутки 7 дней в неделю». При этом в нерабочее время, выходные и праздничные дни обеспечивается возможность круглосуточного получения сотрудниками, ответственными за функционирование НКП, информации либо запросов о помощи от НКП правоохранительных органов иностранных государств (в настоящее время указанная международная сеть НКП имеется в 89 странах мира).

В настоящее время НКП позволяет оперативно обмениваться информацией о готовящихся, совершаемых либо совершенных преступлениях в киберпространстве, а также запрашивать необходимую для проведения оперативно-розыскных мероприятий и следственных действий техническую и иную информацию из аналогичных подразделе-

ний правоохранительных органов государств-участников информационного обмена. Указанные возможности международного обмена информацией, несомненно, способствуют повышению эффективности противодействия киберпреступности.

Таким образом, в настоящее время наиболее актуальными проблемами в противодействии наркопреступности в сети Интернет являются осуществление деанонимизации лиц, причастных к совершению преступлений, связанных с незаконным оборотом наркотиков в сети Интернет, а также повышение эффективности международного сотрудничества с правоохранительными органами и иностранными организациями, являющимися поставщиками интернет-услуг.

В целях решения указанных проблем видится необходимым:

повышение компетенций сотрудников подразделений по наркоконтролю и противодействию торговле людьми в части осуществления деанонимизации лиц, причастных к совершению преступлений, связанных с незаконным оборотом наркотиков в сети Интернет, работы с электронными цифровыми следами, использованию методов поиска и анализа данных из открытых источников;

совершенствование механизмов межгосударственного взаимодействия в части, касающейся своевременного получения информации о сетевом трафике у поставщиков услуг интернета, хостинговых компаний, владельцев продуктов программного обеспечения (в качестве организационно-правовой основы взаимодействия рассмотреть опыт функционирования НКП).

Список использованных источников

1. Доклад Международного комитета по контролю над наркотиками за 2021 год [Электронный ресурс]. – Режим доступа: https://unis.unvienna.org/pdf/2022/INCB/INCB_2021_Report_R.pdf. – Дата доступа: 31.10.2022.

УДК 334

В.Б. Гунько

О КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКЕ СБЫТА НАРКОТИКОВ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Прогресс современных информационно-телекоммуникационных технологий способствует развитию экономики государства, повышению уровня жизни граждан. Однако достижения науки и техники в данной области используются, в том числе, преступным сообществом в целях совершения различного рода противоправных деяний.

Одной из сфер преступного бизнеса, где информационно-телекоммуникационные технологии играют ключевую роль, является незаконный оборот наркотических средств, психотропных веществ или их аналогов. Так, в соответствии с официальными данными МВД России в 2019 г. выявлено 190,2 тыс. преступлений, связанных с незаконным оборотом наркотиков, в 2020 г. – 189,9 тыс. преступлений, в 2021 г. – 179,7 тыс. преступлений. При этом количество зарегистрированных преступлений в данной сфере, совершенных с использованием информационно-телекоммуникационных технологий, составило: в 2019 г. – 24 677, в 2020 г. – 47 060, в 2021 г. – 51 444. Наблюдается более чем двукратный рост за два года. За десять месяцев 2022 г. число выявленных случаев незаконного производства, сбыта или пересылки наркотических средств, психотропных веществ, а также незаконного сбыта или пересылки растений, содержащих наркотические средства или психотропные вещества, совершенных с использованием информационно-телекоммуникационных технологий, превысило показатели 2021 г. и составило 52 913. Неслучайно в Указе Президента Российской Федерации от 2 июля 2021 г. № 400 в числе стратегических национальных приоритетов Российской Федерации названо «предупреждение и пресечение правонарушений и преступлений, совершаемых с использованием информационно-коммуникационных технологий, в том числе … организации незаконного распространения наркотических средств и психотропных веществ…».

В процессе расследования преступлений, в том числе и в сфере незаконного оборота наркотических средств, важное значение имеет криминалистическая характеристика преступления, которую можно определить как систему его значимых элементов и взаимообусловливающих связей между ними.

Вопрос о структуре криминалистической характеристики преступления вообще и сбыта наркотических средств с использованием информационно-коммуникационных технологий в частности является дискуссионным. Исследуя криминалистическую характеристику сбыта наркотиков с использованием информационно-телекоммуникационных технологий, ряд исследователей определяют ее состав традиционно, как содержащий сведения о предмете преступного посягательства, о месте совершения противоправных деяний и о личности типичных преступников. С учетом особенностей рассматриваемого вида преступлений представляется целесообразным при построении структуры их криминалистической характеристики акцентировать внимание на способе совершения преступления, в основе которого лежит использование возможностей, предоставляемых современными информационно-коммуникационными технологиями.