вирусами, а затем использовать их для распространения вредоносных программ на другие компьютеры или по всей сети. Могут вносить вирусы, которые делают рассылки по пользователям, в которых будет содержаться, например, информация-реклама «дизайнерских наркотиков» или мошеннические сообщения.

Установление направленности личности преступника помогает в первую очередь в квалификации их действий, особенно если имеет место быть подготовка или покушение. Кроме того, деление по направленности позволяет разработать целенаправленные профилактические мероприятия.

УДК 343.98

Р.С. Хамидуллин, А.А. Староверов

ВЫЯВЛЕНИЕ НЕЗАКОННОГО ПРИОБРЕТЕНИЯ И СБЫТА ОГНЕСТРЕЛЬНОГО ОРУЖИЯ, СОВЕРШАЕМОГО ЧЕРЕЗ ТЕНЕВЫЕ РЕСУРСЫ СЕТИ ИНТЕРНЕТ

Стремительное развитие торговли в сети Интернет и социальных сетях приводит к росту количества преступлений в сфере незаконного оборота оружия, оборота наркотических средств, поддельных денежных средств и знаков. Актуальность данной работы связана с быстрым ростом преступлений, совершаемых в теневом секторе сети Интернет, а также с высокой сложностью раскрытия этих преступлений. Так, по данным Главного информационно-аналитического центра МВД России, с января по октябрь 2022 г. совершено 429 245 преступлений с использованием информационно-телекоммуникационной сети Интернет, преступлений, связанных с незаконным оборотом оружия, на территории Российской Федерации зарегистрировано 19 158.

В настоящее время интернет является основной площадкой для продажи наркотиков, оружия, сбыта похищенного имущества. Люди создают множество сайтов и веб-страниц, благодаря которым возможно осуществление покупок и продаж подобных вещей, находясь в любой точке планеты. В связи со сложившейся криминогенной обстановкой в мире отдельное внимание следует уделить преступлениям в сфере незаконного оборота оружия, совершаемым с помощью теневых браузеров (DuckDuckGo, Tor, Whonix). Так, на торговой площадке THIEF можно приобрести оружие любого калибра для любых целей – от простых пистолетов до противотанковых ракетных комплексов (например, ПТРК Javelin). К слову, через эту платформу совершено уже более 2 000 сделок.

Минимальная связь между преступными элементами (покупатель, продавец) доставляет значительные трудности по выявлению, раскрытию и расследованию преступлений, связанных с незаконным оборотом оружия. Это связано с тем, что ни покупатель, ни продавец не видят друг друга и даже не встречаются при осуществлении сделки, в данном случае используется способ демонстрации и бесконтактной оплаты – продавец размещает объявление и прикрепляет к нему фотографии или видео, чтобы покупатель смог увидеть товар, покупатель, в свою очередь, посредством перевода криптовалюты на счет продавца осуществляет покупку. Вследствие чего при задержании покупателя или продавца ни один из них не может дать какой-либо информации о другом.

Серьезную проблему составляет также тот факт, что продажа осуществляется через теневые сектора сети Интернет DarkNet. С помощью этой сети так называемые оружейные бароны осуществляют незаконную продажу огнестрельного оружия и патронов к нему. В сети размещаются специальные платформы, например THIEF, где и находятся объявления по продаже оружия и патронов. Эти площадки позволяют покупателю и продавцу действовать анонимно.

Специалисты в области киберпреступности сходятся во мнении, что в странах с большим количеством интернет-пользователей все чаще для незаконной покупки и продажи оружия используется DarkNet. Такая ситуация складывается вследствие того, что способ оплаты, как и где она производилась, отследить почти невозможно. Цифровизация процессов с помощью blockchain-технологий не в полном объеме дает сотрудникам правоохранительных органов осуществлять физический и юридический контроль по финансовым операциям.

Все расчеты в DarkNet осуществляются при помощи криптовалюты, которую покупатель приобретает на специальном обменнике. После этого покупатель выбирает необходимый ему товар и производит оплату, криптовалюта переводится на счет продавца, который подтверждает оплату. Сам продавец также при помощи обменника должен провести операцию по переводу криптовалюты в фиатную валюту (доллары, евро, рубли и т. д.).

Важной особенностью при покупке оружия через теневые сети является способ общения покупателя и продавца. Сегодня существует множество разных мессенджеров, однако наиболее часто используемым для таких целей является Telegram. Он представляет собой анонимную среду с огромным функционалом, одним из которых является возможность создавать ботов, выполняющих определенные функции. В сети Telegram применяется несколько протоколов шифрования (MTProto 2.0 и MTProxy), что обеспечивает шифрование сообщений при их передаче и получении, а также лиц, их отправляющих. Так, в 2019 г. гражданин за-

казал автомат Калашникова через теневую интернет-платформу DarkNet. Связь с продавцом осуществлялась посредством использования сети Telegram. После проведения оплаты товара продавец отправил покупателю сообщение с координатами тайника оружия, сам же автомат был закопан рядом с деревом, которое служило ориентиром. По прибытии на место покупатель выкопал тайник с автоматом и наглядно продемонстрировал его на видеокамеру.

Рис. 1. Гражданин П. получил координаты от продавца и направляется к месту нахождения тайника

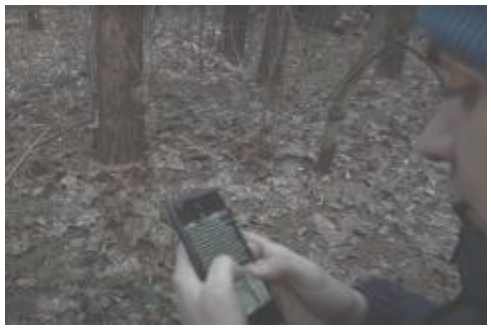

Рис. 2. Гражданин П. прибыл к месту, где находится тайник

Рис. 3. Гражданин П. выкапывает автомат. Автомат завернут в тряпку

Рис. 4. Гражданин П. демонстрирует на видеокамеру автомат АК-47

Особенностью при проведении оперативно-розыскных мероприятий при пресечении незаконного оборота оружия через теневые браузеры является возможность их проведения на первоначальном этапе стадии возбуждения уголовного дела. Если в ходе проведения оперативно-розыскных мероприятий удается установить данные Telegram-аккаунта лица, то оперативные сотрудники могут установить все проводимые лицом операции (отправление и получение фиатных денежных средств, сообщения с покупателем или продавцом, данные о местонахождении тайников-закладок). Следовательно, проведение оперативно-розыскных мероприятий способствует полному, всестороннему и качественному получению информации и сбору доказательственной базы для расследования уголовного дела.

Для полного, своевременного и всестороннего раскрытия и расследования преступлений в области незаконного оборота оружия через теневые браузеры необходимо сочетание оперативно-розыскных и уголовно-процессуальных методов фиксации следов преступления и собирания доказательственной базы по делу. Необходимой мерой является также привлечение специалистов из соответствующих отраслей знаний при осуществлении документирования и последующего расследования рассматриваемых преступлений на всех стадиях оперативно-розыскной и процессуальной деятельности [1].

Итак, продуктивной мерой повышения эффективности работы правоохранительных органов в борьбе с незаконным оборотом оружия, совершаемым посредством теневых сетей, будет пересмотр организационно-тактических мер в отношении дел такой категории. Оперативно-розыскное обеспечение должно осуществляться безотрывно, как в рамках расследования уголовного дела, так и в рамках последующего судебного сопровождения.

Список использованных источников

1. Петухов, А.Ю. Современные тенденции использования средств теневого Интернета при совершении преступлений в сфере незаконного оборота наркотиков / А.Ю. Петухов, К.С. Куликов // Науч. компонент. – 2019. – № 1(1). – С. 22.

УДК 343.985

Д.Л. Харевич

О ПОРЯДКЕ ОСУЩЕСТВЛЕНИЯ НЕКОТОРЫХ ДЕЙСТВИЙ ИНФОРМАЦИОННОГО ХАРАКТЕРА В ХОДЕ НЕГЛАСНОГО РАССЛЕДОВАНИЯ В ФЕДЕРАТИВНОЙ РЕСПУБЛИКЕ ГЕРМАНИЯ

Негласное расследование (verdeckte Ermittlung) в Федеративной Республике Германия (ФРГ) представляет собой собирательный термин, означающий негласные виды деятельности, осуществляемые в целях превенции (предотвращения опасности) либо в целях преследования и предупреждения уголовно наказуемых деяний (в репрессивных целях). Негласное расследование, проводимое в превентивных целях, регламентируется полицейским правом. Основу законодательной базы негласного расследования, осуществляемого в репрессивных целях, составляет уголовно-процессуальное законодательство. Содержание негласного расследования составляют негласные методы, направленные на получение информации. Нормативно регламентированы лишь те методы, которые затрагивают основные права граждан.

Длительное время действия, связанные с обработкой персональных данных, не рассматривались как вторжение в основные права гражданина и требующие законодательной регламентации. В настоящее время решениями высших судебных инстанций признано, что подобные действия затрагивают право граждан на информационное самоопределение. В толковании Федерального конституционного суда ФРГ оно включает в себя право каждого гражданина принимать решение о предоставлении и использовании сведений о своей личности и о том, как он желает быть представленным в глазах других людей. Совершение указанных действий без согласия лица является нарушением рассматриваемого конституционного права. Исключения из данного правила возможны лишь в случаях, оговоренных в законе, например, если гражданин нарушает права других или посягает на конституционный строй или нравственные нормы. В этой связи в законодательстве ФРГ существует достаточно детальная правовая регламентация действий, связанных с получением и обработкой персональных данных, неоднократно являвшаяся предметом научной дискуссии и рассмотрения в Федеральном конституционном суде и конституционных судах федеральных земель.

К действиям указанного рода относятся растровый поиск и полицейское наблюдение.

Под растровым поиском (Rasterfahndung) понимается сквозной поиск по базам данных и автоматизированное сопоставление машинным способом персональных данных о лицах, которые соответствуют проверочным признакам, предположительно указывающим на определенное лицо, с другими данными, хранящимися в иных организациях, осуществляемое с тем, чтобы исключить непричастных лиц или установить лиц, представляющих интерес для расследования.

Одним из примеров успешного проведения растрового поиска является установление местонахождения и задержание члена одной из опасных террористических организаций. Во время расследования было установлено, что террористы, снимавшие квартиры от имени несуществующих лиц, оплачивали счета за электричество наличными деньгами во избежание своей идентификации по номеру счета при безналичной оплате. В связи с этим полицией были истребованы адреса, по которым осуществлялась оплата за электроэнергию деньгами. Из полученных примерно 16 000 совпадений были исключены реально существующие лица: те, кто был зарегистрирован по адресу проживания, имел местную регистрацию автотранспорта или получал пособие либо пенсию. В результате было выделено лишь два лица, при проверке оказавшихся: первый – наркодилером, второй – искомым террористом.

С тех пор существенно расширились возможности получения информации, однако алгоритм действия при проведении мероприятия остался неизменным. На первоначальном этапе растрового поиска из признаков, ставших известными в ходе расследования, осуществляется составление профиля лица (растр). После этого по относящимся к нему признакам организуются запросы в различные банки данных, содержащие соответствующую информацию. По результатам ее обработки выделяются те наборы сведений, которые удовлетворяют всем признакам. Каждое лицо, попавшее таким образом в указанный растр, подлежит более тщательной проверке.

Выделяют две разновидности растрового поиска: «позитивный» и «негативный». Примером «позитивного» растрового поиска может являться сопоставление банка данных разыскиваемых лиц с реестром регистрации граждан. На основе совпадений возможно установление места проживания таких лиц. Данный вид поиска направлен на ограничение круга лиц, подлежащих проверке иными методами. «Негативный» растровый поиск представляет собою более уникальный способ, при котором