тельности – банки, крупные корпорации, операторы сотовой связи, организации, занимающиеся разработками IT-продуктов, другие организации и физические лица, так или иначе заинтересованные в информационной безопасности в сети Интернет.

Список использованных источников

1. Послание Главы государства Касым-Жомарта Токаева народу Казахстана [Электронный ресурс] // Президент Республики Казахстан : офиц. сайт. – URL: http://https://www.akorda.kz/ru/poslanie-glavy-gosudarstva-kasym-zhomarta-tokaeva-narodu-kazahstana-183048 (дата обращения: 01.09.2022).

2. Кецко, К.В. Преступность в сфере электронной коммерции / К.В. Кецко // Рос. следователь. – 2021. – № 9. – С. 58–63.

3. Уваров, А.А. Проблемы использования цифровых технологий при реализации прав и свобод граждан / А.А. Уваров // Право и цифровая экономика. – 2020. – № 2. – С. 5–11.

УДК 343.918.2

И.А. Фомина

ТИПОЛОГИЯ ЛИЧНОСТИ КИБЕРПРЕСТУПНИКА ПО ПАРАМЕТРАМ НАПРАВЛЕННОСТИ

Киберпреступность как правовая, практическая и политическая проблема представляет собой прямую угрозу правам человека, общества и государства. Ее большая опасность в том, что современное развитие мира немыслимо без телекоммуникационных систем. Наш современный мир – цифровой мир, где есть место не только новым возможностям, но и рискам. Рост и прогресс цифровых технологий создали совершенно новую платформу для преступной деятельности. Соответственно, перемещение преступности в киберпространство вполне закономерно – это диктует необходимость перепрофилирования не только правоохранительных органов, но и изменения научных исследований в этом направлении, с учетом особенностей киберпространства. Из-за технологических достижений киберпреступность обычно относится к преступлениям, в которых компьютерная сеть используется в незаконных целях, таких как кража конфиденциальных данных, мошенничество, отмывание денег и детская порнография. С развитием технологий появляются и виды киберпреступлений, которые совершают преступники. При этом киберпреступность принимает различные формы, включая хакерство, распространение вредоносного программного обеспечения, программ-вымогателей, фишинг и др. Многие виды ки-

берпреступности являются продолжением существующей офлайн преступной деятельности, поскольку компьютеры и интернет отделили их от географического местоположения преступника, обеспечивая анонимность и защиту от судебного преследования.

Лица, активно использующие киберпространство в своих преступных целях, обладают специфическими, характерными для них характеристиками целей и мотивов, позволяющими классифицировать (объединить) их по параметрам направленности. Благодаря точной типизации потенциальных киберпреступников, сотрудники правоохранительных органов, занимающиеся предупреждением киберпреступлений, лучше понимают, кто такие киберпреступники, какие методы они используют и какие контрмеры могут быть приняты для защиты и предотвращения будущих киберпреступлений.

Следует иметь в виду, что киберпреступники – это, обычно, отдельные лица или небольшие группы. Однако существуют также крупные и высокоорганизованные группы, которые способны проводить массовые целенаправленные атаки. Они относятся к киберпреступности как к бизнесу, даже формируя глобальные сообщества, которые разделяют стратегии и инструменты. Они могут объединять силы для проведения скоординированных атак и обмена украденными личными данными и информацией на своем подпольном рынке.

Киберпреступники широко представлены в так называемой Dark Web, где они в основном предоставляют свои незаконные услуги или продукты. При этом, так как киберпреступность представлена в двух разновидностях: как преступная деятельность, нацеленная на компьютеры, использующие вирусы и другие типы вредоносных программ, и как преступная деятельность с использованием компьютеров для совершения других преступлений, то в рамках деления киберпреступников по параметрам направленности целесообразно выделять:

киберпреступников, нацеленных на компьютеры (могут например, заражать их вредоносными программами, чтобы повредить устройства или остановить их работу; могут использовать вредоносные программы для удаления или кражи данных; могут помешать пользователям использовать интернет или помешать бизнесу предоставлять программные услуги своим клиентам, т. е. атака по типу «отказ в обслуживании» (DoS));

киберпреступников, которые используют компьютер для совершения других преступлений, когда происходит использование компьютеров или сетей для распространения вредоносных программ, незаконной информации, предметов или незаконных изображений (например, наркопреступление, детская порнография, кибертерроризм и др.);

киберпреступников, которые совмещают в себе два типа: делают и то, и другое одновременно. Они могут сначала заражать компьютеры

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-