ОПЕРАТИВНО-РОЗЫСКНАЯ ДЕЯТЕЛЬНОСТЬ

УДК 343.98

Д. С. Зинченко
научный сотрудник отделения организации
научно-исследовательской работы научно-исследовательского отдела
Белгородского юридического института МВД России имени И. Д. Путилина

ОПЕРАТИВНО-РОЗЫСКНАЯ ДЕЯТЕЛЬНОСТЬ В СФЕРЕ МОШЕННИЧЕСТВА В СОЦИАЛЬНЫХ СЕТЯХ

В XXI веке констатируется динамичное развитие компьютерных и информационно-коммуникационных технологий, которые прочно вошли в повседневную жизнь населения. Так, около 85 % населения планеты зарегистрировано в различных социальных сетях и сети Интернет. На сегодняшний день наибольшую популярность среди пользователей социальных сетей приобрели такие сервисы, как: «ВКонтакте» — 53,8 млн чел., Instagram — 48,9 млн чел., «Одноклассники» — 35 млн чел., Facebook — 26,7 млн чел., а также Viber и WhatsApp — около 19,2 млн чел. [1].

При всех положительных характеристиках реализации данных технологий в практической деятельности и экономической глобализации и интеграции государств прослеживается положительный потенциал прогрессивного развития. Однако существует и ряд негативных последствий. Одним из них выступает современная преступность, а именно мошенничество в социальных сетях. Например, анализ статистики, приведенной Министерством внутренних дел Российской Федерации «О состоянии преступности за май – ноябрь 2020 года», показал, что за данный период было зарегистрировано 1,29 млн преступлений, квалифицируемых по ст. 159.6 Уголовного кодекса Российской Федерации «Мошенничество в сфере компьютерной информации». Для сравнения, в 2010 году их доля составила всего лишь 9,6 тыс. [2]. Общий объем ущерба, который ежегодно наносится данными преступлениями, составляет около 34 млрд долларов. С октября по декабрь 2021 года в России было зарегистрировано 10,3 тыс. преступлений, связанных с мошенничеством в сети Интернет [3]. Это серьезная проблема, которая все больше и больше волнует мировое сообщество. Борьбой с указанным видом мошенничества занимаются практически все страны, в том числе и Россия.

Ввиду этого правоохранительными органами Российской Федерации ведется усиленная борьба с мошенничеством в социальных сетях. Для этого не только проводятся мониторинг социальных сетей, анализ и выработка

путей предупреждения и предостережения от указанного вида преступлений, но и осуществляется оперативно-розыскная деятельность (далее — ОРД) посредством проведения оперативно-розыскных мероприятий (далее — ОРМ). Для того чтобы детально разработать методы и приемы ОРД для борьбы с интернет-мошенничеством, необходимо иметь представление об их видах. На современном этапе развития правоохранительные органы преследуют следующие разновидности мошенничества в социальных сетях: 1) проведение различных аукционов и онлайн-торговля; 2) деловые возможности, т. е. противоправное получение данных банковских карт под вымышленными предлогами; 3) кража личных персональных данных.

Анализ ОРД показал, что наиболее эффективными ОРМ для раскрытия и расследования преступлений, связанных с мошенничеством в социальных сетях и сети Интернет, являются: оперативное внедрение, оперативный эксперимент, снятие информации с технических каналов связи и получение компьютерной информации [4, с. 124].

Существует ряд особенностей проведения вышеуказанных ОРМ. На практике складываются несколько следственных ситуаций — благоприятная и неблагоприятная. Благоприятная следственная ситуация складывается в тех случаях, когда в ходе ОРМ подозреваемый готов сотрудничать и добровольно предоставляет интересующую следствие информацию. К примеру, в Краснодарском крае мошенник, представляясь сотрудником службы безопасности, совершал рассылки сообщений в социальных сетях и сообщал лицам, что их привязанная к аккаунту банковская карта подверглась взлому, в связи с чем необходимо было указать данные банковской карты для безопасности. Данная преступная схема «успешно» им применялась в течение трех месяцев, за которые он похитил около 3 млн рублей [5]. В ходе проведения ОРМ злоумышленник сам предоставил технику и все данные (пароли от аккаунтов, переписки и т. д.), при помощи которых совершал мошеннические действия.

Но правоприменительной практике известны и неблагоприятные ситуации, связанные с активным противодействием со стороны злоумышленников расследованию. Например, в ходе проводимых ОРМ злоумышленники пытаются уничтожить или повредить технику, изменить или удалить значимую для следствия информацию и данные и т. д.

В то же время для недопущения возникновения указанных выше ситуаций законодательно закреплена за провайдерами и владельцами интернет-сервисов обязанность сохранять историю посещений и личную информацию в облачном хранилище данных, которые пригодны к использованию в качестве доказательств. Но и здесь возникают проблемы. Дело в том, что большинство

компаний, которые обеспечивают работу мессенджеров и социальных сетей, находятся за рубежом (США, страны Европы). А это значит, что при проведении ОРМ органы, осуществляющие ОРД, направляют запросы этим зарубежным компаниям, в результате которых в большинстве случаев получают отрицательные ответы или не получают их вообще [6, с. 18].

Таким образом, ОРМ играют важнейшую роль в борьбе с мошенничеством в социальных сетях и сети Интернет, так как в процессе их проведения можно получить оперативные данных о подготовке и совершении мошенничества, установлении криминальных связей, данных, имеющихся на технических устройствах и аккаунтах, однако ввиду своих особенностей при проведении указанных ОРМ нередко возникают проблемы, связанные с рисками потери информации или неполучении ее вообще.

Список основных источников

1. Энциклопедическая статья «Социальная сеть» [Электронный ресурс] // Свободная энциклопедия Википедия. — Режим доступа: https://ru.wikipedia.org/wiki/Социальная_сеть. — Дата доступа: 20.12.2021. Перейти к источнику Вернуться к статье

2. Состояние преступности в России за 2020 год [Электронный ресурс] // М-во внутр. дел Рос. Федерации. — Режим доступа: https://mvd.ru/upload/site1/. — Дата доступа: 21.12.2021. Перейти к источнику Вернуться к статье

3. Статистические данные Федеральной службы государственной статистики Российской Федерации [Электронный ресурс]. — Режим доступа: https://rosstat.gov.ru/statistic. — Дата доступа: 01.12.2021. Перейти к источнику Вернуться к статье

4. Особенности расследования сетевых компьютерных преступлений / А. Л. Осипенко // Рос. юрид. журнал. — Екатеринбург : Урал. гос. юрид. ун-т. — 2019. — № 2. — С. 121–126. Вернуться к статье

5. Мошенник обманул жителей Краснодарского края в социальных сетях [Электронный ресурс] // Аргументы и Факты. Социальная сеть [Электронный ресурс]. — Режим доступа: https://kuban.aif.ru/incidents/criminal/internet-moshennik_obmanul_neskolko_zhiteley_sochi-v-socialnyh-setyah. — Дата доступа: 10.01.2022. Перейти к источнику Вернуться к статье

6. Батоев, В. Б. Использование мессенджеров в преступной деятельности: проблемы деанонимизации пользователей и дешифрования информации / В. Б. Батоев // Оперативник (сыщик) : науч. журнал. — 2017. — Вып. 2 (51). — С. 15–20. Вернуться к статье