УДК 343.9

Е. А. Наборщикова
слушатель 511 учебной группы
факультета подготовки сотрудников полиции
Уральского юридического института МВД России
Р. С. Хамидуллин
начальник кафедры оперативно-розыскной деятельности
органов внутренних дел
Уральского юридического института МВД России,
кандидат юридических наук

КРИМИНАЛИСТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРОТИВОДЕЙСТВИЯ МОШЕННИЧЕСТВАМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ СОТОВОЙ СВЯЗИ И СЕТИ ИНТЕРНЕТ

Сеть Интернет, сотовая связь и средства платежа стали инструментами в руках преступников. Данные преступления осложняются не только тем, что совершаются в век стремительно развивающихся информационных и коммуникационных технологий, но и тем, что являются наиболее латентными. Использование ИТТ позволяет злоумышленникам дистанцироваться от потерпевшего, скрывая свои настоящие данные, что дает им возможность уйти от уголовной ответственности.

Наиболее часто встречающиеся преступления в сфере информационно-телекоммуникационных технологий, совершенные с использованием сотовой связи и сети Интернет, — мошенничества.

На сегодняшний день большинство сотрудников полиции при встрече с подобными преступлениями испытывают трудности в их раскрытии и расследовании, так как отсутствует наличие элементарных базовых знаний, позволяющих получить значимую информацию.

Разумеется, что в зависимости от ситуации действия сотрудников будут различаться, но на первоначальном этапе в ходе опроса потерпевшего необходимо установить максимум возможной информации.

Приведем два примера популярных в современной России типичных ситуаций с дистанционным мошенничеством и действия по ним сотрудников полиции. В рамках первой приведем пример мошенничества, совершенного с использованием сети Интернет (сайта), а во втором случае — с использованием сотовой связи (звонок).

Первая ситуация заключается в том, что злоумышленник создает и размещает сайт на хостинге с предварительной оплатой, затем присваивает ему

доменное имя, размещает для связи абонентский номер (как правило, с IP-телефонии), а также для создания большего доверия у потенциальной «жертвы» размещает еще чат. Наиболее часто встречаются такие виды мошеннических сайтов, как сайты турагентств и отелей, интернет-магазинов, автозапчастей и другие. Продвижение таких сайтов может быть различным: от всплывающих окон (реклама) в браузере сети Интернет до рассылки информации на персональную электронную почту либо в мессенджерах социальных сетей. Таким образом, «жертва» переходит на сайт злоумышленников, выбирает интересующий товар или услугу и производит оплату одним из двух способов: по реквизитам банковской карты или по номеру лицевого счета (абонентскому номеру, привязанному к нему). После получения оплаты организация исчезает или перестает отвечать, товар не поставляется или услуга не оказывается, оплаченные деньги не возвращаются потерпевшему.

В данной ситуации сотруднику полиции следует более подробно опросить потерпевшего по всем обстоятельствам произошедшего (какой сайт посещал (возможно сохранилась ссылка), способ общения с мошенником, а главное — на какие банковские карты или счета осуществлял переводы денежных средств). С целью установления лица, причастного к совершению преступления, необходимо выполнить ряд общих мероприятий, направленных на получение представляющей интерес информации:

1. С помощью находящихся в свободном доступе специальных сервисов в сети Интернет необходимо установить принадлежность сайта хостингу (например, 2ip.ru), а также регистратора доменного имени (например, reg.ru). При наличии данной информации сформировать и направить запросы по соответствующим адресам.

2. Установить оператора сотовой связи абонентского номера, указанного на сайте злоумышленника, с использованием общедоступных сервисов сети Интернет (например, xinit.ru). По получении этих данных сформировать соответствующие запросы и направить их в адрес.

3. Направить запросы в банки или иные коммерческие организации для получения информации по движению денежных средств на счетах от потерпевшего к злоумышленнику. Далее систематизировать полученную информацию в схему для анализа движения денежных средств. В случае обналичивания направить запрос на получение видеозаписей с банкоматов (АТМ). После получения информации в местах расположения банкоматов провести оперативно-технические мероприятия.

4. В связи с тем, что цифровое мошенничество имеет глобальные масштабы, а не фокусируется в одном регионе, необходимо с помощью

интегрированного банка данных федерального уровня (ИБД-Ф) в разделе «Дистанционное мошенничество» посмотреть совпадения по банковским картам, лицевым счетам и сайтам, указанным потерпевшим. При наличии совпадений связаться с соответствующим регионом для получения дополнительных данных.

5. С помощью общедоступных сервисов в сети Интернет проанализировать отзывы установленного сайта, а в случае, если он уже не функционирует, — найти его в ВЭБ-Архиве.

6. При установлении IP-адресов направить запросы в указанные адреса.

Вторая ситуация заключается в том, что злоумышленник осуществляет звонки потенциальной «жертве», представляясь сотрудником банка (родственником, сотрудником правоохранительных органов, сотрудником сервиса госуслуг, менеджером инвестиционной компании, менеджером по трудоустройству и т. д.), и под разнообразными предлогами заставляет сообщить персональные данные или сделать определенные действия. В результате потерпевший под влиянием мошенника сообщает данные реквизитов своей банковской карты, привязывает к бесконтактной оплате свою банковскую карту или просто переводит денежные средства на продиктованный счет или номер банковской карты. Следовательно, полученные денежные средства мошенниками переводятся да различные банковские карты или обменные площадки.

Мероприятия для установления причастных лиц:

1. С помощью абонентских номеров мошенника путем направления запроса можно установить информацию об IP-адресах и реальный номер злоумышленника (если звонок совершен через IP-телефонию).

2. Так же как и в случае с сайтом, необходимо установить информацию по движению денежных средств и составить схему транзакций, а при обналичивании — установить место. Для получения соответствующей информации подготовить и направить запросы.

3. При использовании потерпевшим бесконтактной оплаты через банкомат нужно провести осмотр места происшествия и подготовить запрос в финансовую организацию, которой принадлежит АТМ, в целях установления счета или реквизитов банковской карты, а также абонентских номеров, на которые начислялись средства.

4. В случае если мошенник действует от инвестиционной компании, необходимо установить сайт и дальнейшие действия осуществлять, как в первой первой ситуации.

5. Так же как и с сайтом, необходимо проверить информацию с помощью ИБД-Ф.

Таким образом, за 2022 год каждое четвертое преступление совершалось с использованием IT-технологий. Следовательно, наличие соответствующих знаний в области цифровых технологий помогает сотрудникам полиции в выборе методики и тактики для выявления, раскрытия и расследования дистанционных мошенничеств.