УДК 343.985.1

О. А. Решняк
доцент кафедры криминалистики
учебно-научного комплекса по предварительному следствию
в органах внутренних дел Волгоградской академии МВД России,
кандидат юридических наук, доцент

ПЛАНИРОВАНИЕ РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ СОЦИАЛЬНЫХ СЕТЕЙ

С развитием современных технологий совершенствуются навыки и познания преступников, совершающих мошенничества с использованием социальных сетей, в связи с чем с этим видом преступлений не только сложно бороться, но и выявлять и предупреждать их совершение. В связи с информатизацией жизни общества отмечается динамичность роста преступлений, совершаемых с использованием сети Интернет, что требует более качественного исследования вопросов методики и особенностей расследования мошенничеств данного вида.

В расследовании преступлений важным организационным моментом является планирование, от качества которого зависит ход выявления преступника. Планирование зависит от следственной ситуации, сложившейся на момент начала расследования. По мошенничествам, совершаемым с использованием социальных сетей, приведем три наиболее типичные следственные ситуации и планирование расследования по каждой из них.

Ситуация 1. Сведения о мошенничестве, совершенном в социальных сетях, получены из заявления потерпевшего или иных неофициальных источников, данные о лице, совершившем преступление, отсутствуют, цифровые следы отсутствуют. Планирование расследования предполагает:

1. Допросы заявителя и других лиц, которые могут быть свидетелями совершенных обстоятельств. Это поможет установить более полную картину произошедшего и получить дополнительные данные для расследования.

2. Истребование выписки о движении денежных средств с банковского счета потерпевшего. Анализ этих данных может раскрыть подробности финансовых операций, связанных с преступлением, и помочь в установлении личности преступника.

3. Осмотр места происшествия, компьютерных и других устройств с целью выявления и фиксации данных, свидетельствующих о совершении преступления. Особое внимание уделяется обнаружению цифровых следов,

данных аккаунта пользователя социальных сетей, переписки жертвы с преступником, данных истории интернет-браузера.

4. Анализ цифровых следов, обнаруженных на компьютерах и мобильных устройствах потерпевших. Могут быть восстановлены удаленные файлы, изучены системные журналы и реестры, а также проанализированы сетевые данные.

5. Сотрудничество с интернет-провайдерами социальных сетей других онлайн-платформ для получения информации о действиях мошенника. Это могут быть запросы на предоставление данных о подключениях к Интернету.

6. Сотрудничество с другими правоохранительными органами и международными организациями, так как мошенничество в социальных сетях может иметь трансграничный характер. Обмен информацией и опытом позволяет эффективнее идентифицировать преступников [1].

Ситуация 2. Прямые данные о преступнике отсутствуют, однако установлены потерпевший и свидетели, а также выявлены цифровые следы.

В данной ситуации цифровые следы могут стать важным источником информации. Такие следы включают следы неправомерного доступа к аккаунту в социальных сетях, соединений между устройствами и следы вывода денежных средств с банковских счетов и т. д.

При данных обстоятельствах необходимо провести ряд действий:

1. Допрос потерпевшего для получения информации о преступлении. Выясняется наличие у потерпевшего компьютера, мобильного телефона или планшета с доступом в Интернет, есть ли у кого-либо, кроме него, доступ к его устройствам, наличие регистрации в социальных сетях, какой учетной записью он пользуется, необходимо установить информацию о банковских счетах и картах, в каких банках они открыты, подключены ли услуги «Онлайн-банк» или «Мобильный банк» и известны ли реквизиты карты или счета третьим лицам. Выяснить виды технических средств, с помощью которых осуществлялась оплата за товар, и каким образом потерпевший и мошенник поддерживали связь [1].

2. Получить выписки с банковского счета потерпевшего.

3. Проанализировать и выявить связи между различными следами. Сопоставить данные о неправомерном доступе к аккаунту в социальных сетях с данными о платежах, совершенных с банковского счета потерпевшего. Это может помочь установить, каким образом мошенник получил доступ к аккаунту и какие действия он предпринимал после этого. Таким образом, цифровые следы могут стать ценным источником для расследования и помочь в установлении личности преступника.

Ситуация 3. Установлен способ совершения мошенничества, выявлены цифровые следы, свидетели, потерпевшие, данные о преступнике известны, но неизвестно его местонахождение.

В указанной ситуации первоначальные данные о преступнике могут быть получены из его профиля в социальной сети или по номеру банковской карты/счета, куда переводились деньги через онлайн-банкинг. Использование специальных знаний и возможностей применения технических средств, а также сотрудничество с различными организациями позволяют повысить шансы на успешное расследование и установление личности мошенника.

Для этого проводятся следующие мероприятия:

1. Допрос потерпевшего и свидетелей с целью получения информации о преступнике и возможном месте его нахождения.

2. При наличии номера телефона преступника необходимо запросить у оператора связи информацию о лице, на которое зарегистрирован данный номер, а также о соединениях.

3. Проверка по базам данных установленного лица (судимости, местожительства).

4. Направление поручения органам дознания о проведении мероприятий по розыску мошенника.

5. Задержание и допрос лица, совершившего мошенничество с использованием социальных сетей.

6. Проведение осмотра мест, где использовалось компьютерное оборудование, а также осмотра самих устройств, чтобы найти дополнительные доказательства. При осмотре обращается внимание на компьютеры и мобильные устройства, которые могут содержать важную информацию. Также необходимо проверить устройства, используемые для подключения к Интернету, такие как модемы и роутеры. Кроме того, следователям стоит обратить внимание на специальную литературу, посвященную интернет-технологиям, которая может содержать полезные сведения о мошеннической деятельности. Важно также обнаружить и сохранить платежные документы, а также распечатанные на бумажных носителях реквизиты банковских карт. Кроме компьютерных устройств, следователям необходимо осмотреть и другие предметы, связанные с интернет-услугами и услугами сотовой связи. Это могут быть документы, подтверждающие предоставление таких услуг. Важно также провести тщательный осмотр компьютерных устройств и их аксессуаров, таких как клавиатура, мышь, сканеры, принтеры. При этом необходимо выявить следы рук, а также биологические следы, которые могут помочь в идентификации подозреваемого.

Список основных источников

1. Малыхина Н. И., Кузьмина С. В. Алгоритм действий следователя в типовых ситуациях расследования мошенничеств, совершенных с использованием сети Интернет // Вестн. Том. гос. ун-та. 2021. № 462. С. 238–247. Вернуться к статье