Секция «Уголовный процесс»

Особенности производства отдельных следственных действий на начальном этапе расследования преступлений в сфере информационно-телекоммуникационных технологий

Научный руководитель – Соколова Марина Владимировна

Симакова Юлия Сергеевна
Студент (специалист)
Московский университет Министерства внутренних дел Российской Федерации,
Факультет подготовки следователей, Москва, Россия
E-mail: 2d_sled-ipsopr@mail.ru

Первоначальный этап расследования информационных преступлений отличается от привычных преступлений общеуголовной направленности. В частности, отсутствует такой привычный для следователя объект криминалистически значимой информации, как место происшествия (преступления).

Большинство преступлений, совершаемых с использованием информационных технологий, связано с непосредственным причинением ущерба гражданам и юридическим лицам. В этой связи на первоначальном этапе расследования задача следователя стоит в признании соответствующих лиц потерпевшими с последующим допросом [2].

Наиболее сложным представляется допрос потерпевшего от интернет-мошенничества - фишинг.

Фишинг - вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей - логинам и паролям. Злоумышленники посредством сети Интернет проводят массовую рассылку электронных писем под видом популярных брендов (онлайн-магазины одежды, техника, телефонные операторы, банки) [1]. В данных письмах содержится прямая ссылка на поддельный сайт. Переходя на данный сайт лицу, как правило, предлагается приобрести какой-нибудь брендовый товар на выгодных условиях или с большой скидкой. От ничего не подозревающего гражданина лишь требуется ввести свои данные - данные о банковской карте. Далее: 1) гражданину предлагается оплатить псевдопокупку, но обещанного товара он так и не получает; 2) получая данные карты, злоумышленники предпринимают попытку хищения с нее денежных средств. Трудность заключается в том, что у допрашиваемого лица необходимо узнать обстоятельства, связанные с интернет-сайтами, на которые последний, как правило, не обращает внимания, либо не может в полной мере пояснить требующуюся от него информацию. Примерный перечень вопросов здесь будет следующий:

- как узнали про сайт, на котором совершили псевдопокупку?

- предшествовала ли покупке интернет-рассылка через социальные сети, мессенджеры, онлайн-почту, от имени магазина о больших скидках или выгодных акциях, если да, то указать откуда именно поступала такая информация, ее точное содержание;

- как назывался онлайн-магазин, помните ли домен сайта, если да, то указать в допросе.

По окончании допроса, следователь, чтобы не затягивать срок следствия, сразу может принять решение об изъятии предметов у потерпевшего, которые могут служить доказательствами по уголовному делу. В частности, это может быть сотовый телефон, он будет иметь значимую информацию в плане переписки с мошенниками. Для того чтобы не лишать потерпевшего надолго телефона, следователь может сразу принять решение о его осмотре вместе с самим потерпевшим, чтобы последний со своего согласия показал следователю нужную ему информацию. При оформлении протокола осмотра предмета в качестве иллюстраций лучше всего использовать скриншоты, сделанные на телефоне,

они имеют большую наглядность по сравнению с фотографиями. Осмотреть можно также онлайн-банк, если он присутствует и входящие (исходящие) звонки и СМС-сообщения, опять-таки с разрешения самого потерпевшего. На основании осмотренной информации в последующем перед судом будет выноситься ходатайство о получении информации о соединениях между абонентами и (или) абонентскими устройствами в порядке ст. 168.1 УПК РФ, а также направляться запросы в банки и иные организации.

Зачастую преступники используют до нескольких десятков поддельных сотовых номеров и подставных банковских счетов, и процессуальные и криминалистические требования сходятся в данном случае в одном - отрабатывать необходимо всю имеющуюся информацию, в этой связи возрастает актуальность создания следственных групп по информационным преступлениям.

Источники и литература

1) 1. Бозиева Ю. Г., Коркмазов А. В. Криминалистическая характеристика преступлений, совершаемых в глобальном информационном пространстве // Журнал прикладных исследований. 2021. №3.
2) 2. Сафронкина О. В., Мещеряков В. А Особенности подготовительного этапа допроса при расследовании мошенничества в сфере компьютерной информации // Вестник ВИ МВД России. 2019. №2.