Старостенко Нина Игоревна,
начальник кабинета специальных дисциплин
кафедры уголовного процесса
Краснодарского университета МВД России

СОВЕРШЕНСТВОВАНИЕ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Эффективность расследования преступлений в сфере информационно-телекоммуникационных технологий сегодня является предметом особого внимания. По мнению Кузнецова С.В., заместителя Председателя Правления Сбербанка России, более 80% случаев таких преступлений в Российской Федерации совершается при помощи методов социальной инженерии[1].

Известный ученый Овчинский В.С., в своей книге «Мафия. Новые мировые тенденции», отметил, что социальная инженерия «превратилась в один из самых распространенных векторов атак на информацию, от которых сложнее всего защититься»[2]. Она представляет собой систему «различных психологических методик и мошеннических приемов, целью которых является получение конфиденциальной информации о человеке обманным путем»[3]. Это своеобразный метод (атак) несанкционированного доступа к информации или системам хранения информации «с помощью техник, основанных на использовании слабостей человеческого фактора. Кроме того, данные техники являются очень эффективным оружием мошенников на сегодняшний день»[4].

Большой объем работы, нехватка кадрового состава следственных подразделений, длительность проведения следственных действий, а также незнание сотрудниками правоохранительных органов приемов социальной инженерии интернет-мошенников, совершающих преступления информационно-телекоммуникационным способом, не позволяют поддерживать степень раскрываемости и расследования данных преступлений на высоком уровне.

---

[1] Официальный сайт Новости России. Комсомольская правда в РФ [Электронный ресурс] URL: https://www.kp.ru (дата обращения: 01.02.2020).

[2] Овчинский В.С. Мафия. Новые мировые тенденции «Коллекция изборского клуба» – М.: Книжный мир 2016. – С. 37.

[3] НИЦ корпоративной безопасности в Москве – Артемов Н. Социальная инженерия – технология «взлома» человека [Электронный ресурс] URL: https:// srccs.su/tag/nikita-artemov/ (дата обращения: 01.02.2020).

[4] Официальный сайт Хабр [Электронный ресурс] URL: https:// habr.com/ru/post/83415/ (дата обращения: 23.12.2019).

Справедливо отмечает доктор юридических наук, профессор Шаталов А.С., что «одной из наиболее существенных причин низкого качества предварительного расследования преступлений, совершаемых в киберпространстве, является отсутствие качественных методических разработок, в реализации которых были бы в полной мере задействованы современные информационные технологии»[1].

С мнением Шаталова А.С. нельзя не согласиться. Ведь, несомненно, указанная проблема является весьма актуальной на сегодняшний день. Согласно официальной статистике МВД преступления, совершенные информационно-телекоммуникационным способом, набирают большую популярность среди мошенников. Так в январе – декабре 2019 года зарегистрировано 294,4 тыс. преступлений, совершенных с использованием информационно – телекоммуникационных технологий или на 68,5 % больше, чем за аналогичный период прошлого года. В общем числе зарегистрированных преступлений их удельный вес увеличился с 8,8 % в январе–декабре 2018 года до 14,5 %. Практически все преступления данного вида (98,4 %) выявляются органами внутренних дел. Из общего числа преступлений указанного вида 294,4 тыс. преступлений раскрыто 65,2, а 229,2 остаются нераскрытыми. Краснодарский край указан на позиции «Регионы с наименьшей раскрываемостью», процентная доля составляет – 14,6 %[2].

Полагаем, что такая ситуация обуславливается следующими причинами:

Во-первых, на показатели раскрываемости преступлений влияет правовая и информационная подготовленность сотрудников в сфере изучения методики расследования преступлений социальной инженерии. Кроме того, значительными проблемами является отсутствие специализированных подразделений, расследующих дела указанного вида преступлений, а также длительное (2–3 месяца) проведение следственных действий таких, как получение информации о соединениях между абонентами и (или) абонентскими устройствами, контроль и запись переговоров и др.

Во-вторых, на качественное и своевременное расследование преступлений влияет сложность идентификации мошенников, которые дистанционно оказывают влияние на жертву для достижения корыстного результата, а также удаленно используют средства конспирации в

[1] Шаталов А.С. Разработка методических основ расследования преступлений, совершаемых с помощью компьютерных и сетевых технологий: проблемы, перспективы и тенденции //Вестник сибирского юридического института МВД России. 2018. № 3(32).

[2] Официальный сайт МВД России [Электронный ресурс] URL: https:// мвд.рф/reports/item/19412450/ (дата обращения: 10.12.2020).

преступной деятельности: сим-карты, зарегистрированные на других лиц, мобильные телефоны, добытые преступным путем.

Таким образом, для совершенствования расследования преступлений, совершенных с использованием техник социальной инженерии для неправомерного доступа к информации или системам хранения информации необходимо:

В связи с тем, что курс подготовки сотрудников не предусматривает системного знания о техниках социальной инженерии, используемых при совершении преступлений необходимо создать учебную методику и рекомендации по расследованию данных преступлений, содержащие основные приемы и способы интернет-мошенничеств. Данное знание должно включать понятие социальной инженерии, ее виды, признаки техник, методы и способы их выявления, фиксирования и использования в раскрытии и расследовании преступлений. Также немаловажным будет являться введение в курс повышения квалификации и обучения сотрудников правоохранительных органов дисциплины, в которой будут отражены алгоритмы действий при возникновении различных следственных ситуаций.

Необходимо отметить, что предотвращение таких преступлений невозможно без использования современных информационных технологий. Следовательно, требуется привлечение более подготовленных специалистов для борьбы с мошенничествами в сфере информационно-телекоммуникационных технологий. Кроме того, учитывая большой объем работы сотрудников правоохранительных органов, важно создать специализированные подразделения, конкретно расследующие мошенничества указанного вида. А в состав данных подразделений включить следователей, оперативных сотрудников, экспертов, обладающих познаниями в сфере информационных технологий.

Также необходимо определить организационную составляющую тактики расследования преступлений. Для своевременного и оперативного реагирования на указанные преступления установить более тесное взаимодействие данных подразделений с организациями, оказывающие услуги связи.

Таким образом, при осуществлении названных тезисов, полагаю, возможно достичь более эффективного и качественного раскрытия и расследования преступлений, оперативного сбора и фиксации вещественных доказательств, а также подготовки сотрудников правоохранительных органов на высоком уровне.