Краснодарский университет МВД России

А. В. Гусев
Н. И. Старостенко

ВЫЯВЛЕНИЕ МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ, ПРИМЕНЯЕМЫХ В МОШЕННИЧЕСКИХ ЦЕЛЯХ

Методические рекомендации

Краснодар
2023

УДК 343.72
ББК 67.408.121
Г962

Одобрено
редакционно-издательским советом
Краснодарского университета
МВД России

Рецензенты:
М. Н. Кузьмин, кандидат юридических наук (Ростовский юридический институт МВД России);
А. А. Олейников (Главное управление МВД России по Краснодарскому краю).

Гусев А. В.

Г962 Выявление методов социальной инженерии, применяемых в мошеннических целях : методические рекомендации / А. В. Гусев, Н. И. Старостенко. – Краснодар : Краснодарский университет МВД России, 2023. – 42 с.

ISBN 978-5-9266-1934-5

Раскрывается криминалистическая характеристика мошенничества, совершаемого с использованием методов социальной инженерии, анализируется сущность указанных методов, а также их понятие и признаки. Уделяется внимание основным способам совершения такого мошенничества и описанию особенностей механизма их совершения и следообразования.

Для профессорско-преподавательского состава, адъюнктов, курсантов, слушателей образовательных организаций МВД России и сотрудников органов внутренних дел Российской Федерации.

УДК 343.72
ББК 67.408.121

ISBN 978-5-9266-1934-5

Введение

Стремительное развитие информационно-телекоммуникационных технологий оказывает положительное влияние на все сферы жизнедеятельности общества. В то же время оно порождает и комплекс отрицательных последствий, связанных с ростом криминала в стране. Об этом свидетельствуют данные официальной статистики о состоянии преступности в Российской Федерации. Так, в 2020 г. зарегистрировано более 510 396 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий, что на 73,4% (!) больше, чем в 2019 г. При этом более половины таких преступлений совершается с использованием сети Интернет, а более трети – посредством мобильной связи. Четыре таких преступления (80,0%) из пяти совершаются путем кражи или мошенничества – 410 490 тыс. (+83,2%)[1]. По итогам 12-ти месяцев 2021 года количество анализируемых деяний выросло незначительно – на 1,4% (517 222 тыс.). Однако такие данные, несомненно, демонстрируют определенную тенденцию к увеличению показателей рассматриваемой преступности[2].

В ноябре 2021 году в г. Москве состоялось заседание коллегии МВД России, выступая на котором Министр внутренних дел генерал полиции В.А. Колокольцев отметил, что «цифровая революция принесла, не только блага и новейшие технологии, но и возникновение новых угроз – мошенничества с использованием сотовой связи, а также средств IP-телефонии. Преступники научились подменять подлинные телефонные номера кредитных организаций, государственных служб, выдавая себя за их работников. В прошлом году число противоправных деяний, совершенных с применением информационных технологий, увеличилось в два раза, в январе-сентябре текущего года – почти на 70%»[3].

---

[1] Официальный сайт МВД. Краткая характеристика состояния преступности URL: https://мвд.рф/reports/item/22678184/ (дата обращения 10.09.2021г.)

[2] См.: Официальный сайт МВД. Краткая характеристика состояния преступности в Российской Федерации за январь-декабрь 2021 г. URL: https://мвд.рф/reports/item/28021552/ (дата обращения 11.02.2022 г.)

[3] Официальный сайт МВД России. URL: https://мвд.рф/news/item/18808269 (дата обращения 22.11.2021 г.).

Проблема роста преступности в сфере информационно-телекоммуникационных технологий привлекает к себе большое внимание не только правоприменителей, но и ученых. Названное утверждение обуславливается тем, что рассматриваемый вид преступности приобретает серьезные масштабы и представляет одну из главных угроз информационной безопасности, как для отдельной личности, так и для общества в целом. Развитие современных коммуникаций в обществе и использование всеми гражданами информационных технологий позволило преступникам совершать преступления с использованием названной сферы технологического прогресса, в том числе связанных с различными формами мошеннических действий. Новые возможности провоцируют модификацию «традиционных» способов совершения мошенничеств и вызывают появление новых видов.

Сегодня основной тенденцией современной преступности в сфере информационно-телекоммуникационных технологий является совершение хищений с использованием методов социальной инженерии. Отметим, что в Российской Федерации большинство хищений с банковских счетов проводится с помощью техник социальной инженерии (69%). В своем интервью С. Кузнецов (заместитель председателя ПАО «Сбербанк») рассказал о том, «что в 2018 году доля социальной инженерии составляла 75% от всего кибермошенничества, в 2019 – 79%, в 2020 – 89%, а в 2021 году уже достигла 90 также отметил, что в обозримом будущем этот тренд не изменится, и мошенники продолжат пользоваться низкой киберграмотностью[1].

Данные методы предполагают не столько изощренные методы хакерства или навыки использования сложных программно-аппаратных решений, сколько знания и умения пользоваться особенностями человеческой психологии. Они зачастую характеризуются применением определенных техник, направленных на введение человека в заблуждение, а также психологического воздействия и манипулирования для достижения корыстного результата. Рассматриваемые преступления зачастую, по причине не установ-

[1] Официальный сайт ежедневной деловой газеты РБК [Электронный ресурс]. URL:https://www.rbc.ru/technology_and_media/ (дата обращения: 18.01.2022).

ления виновного лица, остаются нераскрытыми, а злоумышленники, совершившие деяние-безнаказанными, что способствует совершению новых преступлений и дальнейшему росту нарушения законности.

Латентность, а также трудность выявления, раскрытия и расследования преступлений данного вида, наличие недостатков при сборе первичного материала и в ходе предварительного расследования, свидетельствует об отсутствии научных разработок тактики и методики расследования хищений, с использованием методов социальной инженерии. В юридических источниках не отражены характеристики способов совершения хищений с использованием методов социальной инженерии, которые зачастую реализуются с использованием информационно-телекоммуникационных технологий.

Предложенные проблемные вопросы расследования таких хищений позволяют сделать вывод о том, что возникла острая необходимость комплексного и всестороннего научного исследования криминалистических особенностей преступности рассматриваемого вида, изучения механизма совершения данных преступлений, его основных способов, проявляющихся в подготовке, непосредственном совершении, а также сокрытии следов преступной деятельности.

ПОНЯТИЕ, ПРИЗНАКИ И ВИДЫ МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ, ПРИМЕНЯЕМЫХ В МОШЕННИЧЕСКИХ ЦЕЛЯХ

Социальная инженерия – в контексте информационной безопасности – психологическое манипулирование людьми с целью совершения определенных действий или разглашения конфиденциальной информации[1]. Иными словами, это искусный метод управления психологией человека без использования технических приемов взлома для получения персональной или конфиденциальной информации[2].

Следует отличать от понятия социальной инженерии в социальных науках – которое не касается разглашения какой-либо информации. В социологии социальная инженерия используется для понимания случаев целенаправленного формирования специфичного группового социального поведения, практической деятельности по преобразованию всех аспектов общественной жизни для успешной адаптации к изменяющимся условиям реальности, научно и технически обоснованное регулирующее действие в сфере социальных отношений[3].

В данном аспекте под социальной инженерией понимается управленческая деятельность, направленная на изменение социальных систем и социальных институтов в соответствии с заданной руководителем целью, от деятельности которого зависит успешность функционирования всей системы.

Что касается понимания механизма использования социальной инженерии при совершении хищений, то здесь необходимо отметить, что ее методы направлены на контроль за поведением человека, выраженный в достижении выполнения им определенных действий с банковским счетом (картой) или сообщении какой-либо персональной или конфиденциальной информации, получе-

[1] Ross J. Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems. – John Wiley & Sons, 2008-04-14. – 1080 с. – ISBN 978-0-470-06852-6.

[2] Созаев С.С., Кунашев Д.А. Социальная инженерия, ее техники и методы её противодействия // Международный журнал «Вестник науки». 2020. №2(23). Т.1. С.85–88.

[3] Веселов А. В. Социальная инженерия: сущность и парадигмальная методология: диссертация … кандидата философских наук: 09.00.11. Москва, 2012.

ние которой позволяет злоумышленнику получать незаконной доступ к чужому имуществу. При этом к чужому имуществу в преступлениях обозначенного вида зачастую относятся электронные, в том числе безналичные, денежные средства.

Методы социальной инженерии:

1. «Фишинг» – получение конфиденциальных данных с помощью выполнения рассылки. Целью «фишинга» является незаконное получение конфиденциальных данных пользователей, например, логина и пароля, номера банковского счета или личного идентификационного кода при рассылке по электронной почте или смс на мобильное или компьютерное устройтсво.

Как правило, письмо, подготовленное к рассылке, для совершения хищений содержит официальный стиль изложения текста, обращение от имени какой-либо организации с просьбой сообщить данные или выполнить переход по ссылке. Указанная ссылка зачастую ведет на поддельную страницу, которая адаптирована для кражи конфиденциальной информации, в том числе банковских сведений.

Пример использования «фишинга» при совершении хищений.

Так, 23.01.2021 неустановленное лицо, находясь в неустановленном месте, под предлогом продажи телефона на сайте объявлений «Авито», якобы для совершения сделки предоставило ссылку в сети Интернет на поддельный сайт, используя которую произвело списание денежных средств в размере 15690 рублей с банковской карты № ..., принадлежащей Н., причинив последней значительный ущерб на указанную сумму[1].

2. «Вишинг» – получение конфиденциальных данных при телефонном звонке. Данный метод социальной инженерии характеризуется применением психологического воздействия при общении с жертвой во время телефонного звонка для получения недостающих конфиденциальных данных. Обычно, злоумышленник обращается к жертве по телефону от имени сотрудника банка и сообщает о возникшей хакерской или мошеннической атаке на ее

[1] Материалы уголовного дела № 12101030053000193, возбужденного 23.01.2021 СО ОП (Карасунский округ) УМВД России по г. Краснодару по признакам преступления, предусмотренного ч.2 ст. 159 УК РФ.

банковский счет, избежать которую возможно, сообщив код, пришедший из СМС от банка.

Пример использования «вишинга» при совершении хищений.

Так, следствием ОМВД РФ по г. Анапе установлено, что 08.04.2021г. в период времени с 16часов 00 минут до 16часов 30минут., неустановленное лицо путём обмана, под предлогом приостановления операции по смене номера телефона привязанного к банковской карте банка «Альфа-банк», убедило К. сообщить код из смс-сообщения, в результате чего похитило принадлежащие ей денежные средства[1].

3. «Претекстинг» – действие по подготовленному сценарию. Указанный метод социальной инженерии подразумевает использование при общении с жертвой заранее подготовленного текста или сценария, успешное соблюдение которого позволяет злоумышленнику незаконно завладеть денежными средствами. При этом особо значение при соблюдении такого сценария имеет оказание психологического влияния на жертву таким образом, чтобы она осуществляла действия под строгим руководством злоумышленника.

Пример использования «претекстинга» при совершении хищений.

Так, 24.01.2021 в период времени с 16 часов 30 минут до 16 часов 52 минут, неустановленное лицо, находясь в неустановленном месте, используя социальную сеть «Вконтакте», действуя от имени «Наталья Т.», сообщило Г. ложные сведения о ДТП с участием Т., после чего умышленно и из корыстных побуждений, путем обмана похитило со счета № ..., открытого на имя последней в АО «Альфабанк», денежные стредства в размере 65 000 рублей, которые последняя перечислила посредством мобильного приложения на банковскую карту № .... Таким образом, своими действиями неустановленное лицо причинило Г. значительный ущерб на указанную сумму[2].

---

[1] Материалы уголовного дела № 12101030004000691, возбужденного 09.04.2021 г. СО ОМВД РФ по г. Анапе по признакам преступления, предусмотренного ч.2 ст. 159 УК РФ.

[2] Материалы уголовного дела № 12101030048000079, возбужденного 25.01.2021 СО ОП (мкр. «Юбилейный») УМВД РФ по признакам преступления, предусмотренного ч.2 ст. 159 УК РФ.

4. «Троянская программа» – убеждение в необходимости скачать программу. Рассматриваемый метод социальной инженерии выражен в убеждении жертвы в необходимости скачать программу (содержащую вредоносное программное обеспечение или служащую для удаленного администрирования в компьютерном или мобильном устройстве), которая, как правило, замаскирована под важное обновление или полезную утилиту и др.

Пример использования «троянской программы» при совершении хищений.

Так, 08.05.2021 г. в 10 часов 35 минут., неустановленное лицо, находясь в неустановленном месте, умышленно ввело в заблуждение Н. относительно совершения мошеннических действий с её банковским счетом, после чего убедило скачать обновления программы ВТБ банка, предоставив удаленный доступ к мобильному устройству, после чего мошенническим путем похитило с банковского счета в ПАО банк «ВТБ», принадлежащие ей денежные средства на общую сумму 36 070 рублей, чем ей был причинен значительный ущерб[1].

К признакам использования методов социальной инженерии при совершении хищений можно отнести:

– официальный стиль обращения к жертве для создания авторитетного образа для жертвы;

– действие от имени представителя какой-либо организации, сотрудника государственного органа (сотрудник безопасности банка, специалист из пенсионного фонда, сотрудник правоохранительных органов либо из социальных служб, близкий родственник или друг, представитель интернет-магазина и др.);

– использование психологических методов воздействия для создания стрессовой ситуации;

– создание условий ограниченности времени, отпущенного на принятие решения;

– сообщение информации, несоответствующей действительности, которую потерпевший воспринимает за действительную;

[1] Материалы уголовного дела № 12101030006000780, возбужденного 12.05.2021 СО ОМВД РФ по г. Геленджику по признакам преступления, предусмотренного ч.2 ст. 159 УК РФ.

– выдвижение неотложного требования сообщить какую-либо личную информацию о себе, конфиденциальные данные о реквизитах банковской карты, счета, пароля от сервиса дистанционного банковского обслуживания, секретного кода от банка из СМС и т. д.;

– выдвижение неотложного требования совершить определенные действия с денежными средствами на карте, которые, например, будут способствовать предотвращению мошеннической операции;

– достижение цели по добровольному переводу денежных средств жертвой на счета третьих лиц, сообщению конфиденциальных данных или выполнения иных действий, которые могут привести к материальному ущербу собственника.

Таким образом, криминалистический аспект методов социальной инженерии, используемых при мошенничествах заключается в понимании криминалистического механизма совершения данных преступлений, проявляющегося в описании динамически связанных элементов таких, как характеристика личности лица, совершающего мошенничества, а также лица, которому был причинен материальный (моральный) вред, обстановка совершения мошеннических действий, механизм следообразования и способы совершения преступления, выраженные в применении методов социальной инженерии – дистанционных приемов психологического воздействия.

КРИМИНАЛИСТИЧЕСКОЕ ПОНИМАНИЕ МЕХАНИЗМА МОШЕННИЧЕСТВ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

В криминалистических учениях механизм совершения преступления подобен составу преступления в уголовном праве, является основой в деятельности лиц, осуществляющих расследование преступлений и криминалистическую деятельность.

Механизм преступления в криминалистике рассматривается как сложная динамичная система, взаимосвязанными элементами которой являются: лицо (лица), которое осуществляет действия по подготовке, совершению и сокрытию преступления; связи и отношения между участниками события; используемые объекты, свойства и признаки этих объектов; явления, отражающие процессы, имевшие место при совершении преступления; пространственно-временные факторы материальной обстановки события преступления и др. Механизм преступления охватывает способ совершения преступления, включает систему действий преступника (преступников).

Субъект, а также характеристика его деятельности играют основополагающую роль в механизме мошенничества обозначенной категории. Личность мошенника, совершающего деяния с использованием методов социальной инженерии характеризуется, в первую очередь, наличием высокого уровня знаний в области человеческой психологии и умениями их использовать при реализации преступных схем. Злоумышленник обладает профессиональными навыками обращения с компьютерной техникой, умениями создания сайтов-подделок, осуществления взлома баз данных, хранящих персональные сведения пользователей, рассылки фишинговых писем на электронною почту. Большой интеллектуальный потенциал преступника, характеризующийся умением осуществлять поиск конфиденциальных сведений из открытых источников в сети Интернет, владеть техникой воспроизведения голоса, напри-

мер специалиста банка или сотрудника государственной организации, позволяет маскировать свои реальные противоправные намерения под правомерные действия[1].

Основой механизма мошенничества выступают действия, слова, те или иные манипуляции преступников, направленные на вхождение в доверие к потерпевшим и вовлечение их в обман. Злоумышленники, используя особенности психологии человека при совершении преступлений, добиваются получения от жертв конфиденциальной информации.

При совершении рассматриваемых хищений имеют место направленные действия преступников на органы чувств потерпевшего для введения их в заблуждение и побуждения их к выполнению определенных действий. Обман и злоупотребление доверием, являясь способами получения конфиденциальной информации или совершения преступления, выступают основой психологической манипуляции потерпевших.

Под криминальным манипулированием при совершении мошеннических действий понимается система средств направленного, скрытого психологического воздействия на жертву с целью завладения чужим имуществом или приобретением права на имущество.

При этом рост изобретательности мошенником, техник, средств и приемов криминального манипулирования сознанием жертв расширяется. В ходе осуществления преступного замысла мошенники очень часто используют те техники психологического воздействия, которые имеют манипулятивную направленность по отношению к психической сфере жертвы и способны против ее воли влиять на особенности поведения, установки, убеждения[2].

Следовательно, лицо, используя методы социальной инженерии, применяет систему средств направленного психологического воздействия, успешная реализация которой способствует достижению преступного замысла.

---

[1] Старостенко, Н. И. Криминалистическое понимание механизма совершения мошенничества с использованием методов социальной инженерии // Общество и право. 2021. № 1(75). С. 71-76.

[2] Куклина А.Ю. Криминальное манипулирование сознанием на примере мошенничества // Организация работы с молодежью. 2018. № 3. С. 55-62.

Немаловажное значение при оказании внушаемости на потерпевших занимает психологическая направленность текстов или обращений злоумышленников[1]. Грамотный выбор слов позволяет реализовать при общении с жертвой такое общение, в результате которого высказанные слова наполняются специальным смыслом и незаметно искажают реальную действительность в представлениях адресата[2].

Особая организация текста позволяет злоумышленнику добиться иллюзии самостоятельности сделанных жертвой выводов, на основе получения важной информации и завуалированности реальности противоправных действий. Использование названных психологических манипуляций и других приемов воздействия формирует у жертвы иллюзию свободы выбора поведения[3].

Анализ уголовных дел, а также эмпирических данных позволил выделить основные приемы криминального манипулирования сознанием и поведением жертв при совершении хищений денежных средств с использованием методов социальной инженерии, реализуемых при помощи информационно-телекоммуникационных технологий:

изучение психологического состояния и индивидуальных особенностей потенциальной жертвы;

установление психологического контакта и доверительных отношений;

манипулятивное воздействие, нацеленное на создание ложного представления о ситуации;

сокрытие направленности психологического воздействия;

контроль формой и темпом подачи информации (манипулятивная направленность текстов и обращений к жертвам) и др.

Обстановка мошенничеств, совершенных с использованием методов социальной инженерии, обусловлена определенным местом и временем. Согласно ст. 152 УПК РФ местом совершения является непосредственно место совершения деяния либо его

---

[1] Старостенко О. А. Взаимодействие жертвы и преступника в процессе совершения хищений с использованием IT-технологий // Российский следователь. 2022. № 1. С. 60-63. – DOI 10.18572/1812-3783-2022-1-60-63.

[2] Ortega, R. (2009) The emotional impact on victim of traditional bullying and cyberbullying a study of Spanish adolescents // *Journal of Psyhology.* 217 (4), pp. 197-204.

[3] Дворянчиков Н. В., Соловьева Ю. А. Психологические механизмы манипуляции поведением потребителя // Психология и право. 2011. № 1. С. 1-10.

окончания, а также место нахождения обвиняемого. Однако определение места киберпреступлений вызывает некоторые трудности, так как ключевой особенностью обстановки таких преступных явлений считается, что в совершении противоправных деяний задействовано несколько технических устройств (устройство злоумышленника, жертв), которые находятся удаленно друг от друга. Отсюда, можно сделать вывод о том, что в данном вопросе необходимо учитывать физическое месторасположение виновного и его жертв. Отметим, что преступность анализируемого вида отличается обстановкой ее совершения, образованной электронным устройством, виртуальной средой, а также дистанционностью противоправных деяний. При этом под виртуальной средой следует понимать созданный, с помощью технических средств, мир, передаваемый пользователю через органы чувств.

Обстановка оказывает существенное влияние на способ совершения преступлений данного вида, предопределяет схемы противоправного поведения. Исследуя особенности обстановки рассматриваемых преступлений, возможно предположить, что при расследовании подобных преступлений требуется привлечение специалистов, обладающих знаниями в соответствующей области, позволяющих точно определять место и время совершения мошенничества.

Следует отметить, что преступник действует не только в конкретной обстановке, но и в определенное время, порой в значительной мере влияющее на его поведение. Работа некоторых программ связана со временем, установленным на компьютере или мобильном телефоне, которое может быть изменено по желанию мошенника.

Таким образом, обстановка совершения мошенничеств с использованием методов социальной инженерии – это система взаимосвязанных элементов, протекающих в виртуальной среде и пространственно-временных условиях, в которых удаленно совершаются мошеннические действия, сопровождающиеся использованием техник социальной инженерии.

Традиционно в криминалистическом учении предметами мошенничеств являются объекты материального мира, представляющие экономическую ценность. При совершении мошеннических

действий с использованием методов социальной инженерии предметами преступного посягательства в основном выступают электронные денежные средства жертвы.

Электронные деньги обладают экономической и юридической значимостью, однако их нельзя потрогать, поскольку они лишены какого-либо материального выражения – это лишь денежное обязательство, запись о котором хранится в электронной форме. В связи с этим совершить хищение электронных денег нельзя, поскольку их физически невозможно изъять, однако их можно обратить. При этом причиняется реальный ущерб отношениям собственности, а значит, электронные деньги могут быть предметом хищения[1].

Федеральный закон № 111-ФЗ от 23.04.2018 г. закрепляет, что электронные (безналичные) денежные средства являются самостоятельным предметом хищения[2].

Определение электронных денежных средств содержится в п.18 ст. 3 Федерального закона № 116-ФЗ от 27.06.2011 г. «О национальной платежной системе», где указано, что они являются денежными средствами, которые предварительно предоставлены одним лицом (лицом, предоставившим денежные средства) другому лицу, учитывающему информацию о размере предоставленных денежных средств без открытия банковского счета (обязанному лицу), для исполнения денежных обязательств лица, предоставившего денежные средства, перед третьими лицами и в отношении которых лицо, предоставившее денежные средства, имеет право передавать распоряжения исключительно с использованием электронных средств платежа[3].

Таким образом, электронные (в том числе безналичные) денежные средства признаются самостоятельным элементом и служат предметом в преступлениях анализируемого вида.

---

[1] Ищук Я. Г., Пинкевич Т. В., Смольянинов Е. С. Цифровая криминология: учебное пособие. М.: Академия управления МВД России, 2021. С. 173.

[2] Федеральный закон «О внесении изменений в Уголовный кодекс Российской Федерации» от 23.04.2018 № 111-ФЗ URL: http://www.consultant.ru/document/cons_doc_LAW_296451/ (дата обращения: 10.11. 2020)

[3] Федеральный закон «О национальной платежной системе» от 27.06.2011 № 161-ФЗ (ред. от 02.07.2021 № 343 ФЗ) URL: http://www.consultant.ru/document/cons_doc_LAW_115625/4f41fe599ce341751e4e34dc50a4b676674c1416/ (дата обращения : 10.10. 2021 г.

В преступлениях рассматриваемого вида участие жертвы является неизбежным. Общеизвестно, что именно поведение человека детерминирует противоправные деяния злоумышленника.

Люди, подверженные мошенничеству с использованием техник социальной инженерии, обладают излишней доверчивостью, беспечностью, они легко поддаются обману и убеждению со стороны посторонних лиц. Поведение, особенности морально-психологического состояния личности, ее профессиональная деятельность позволяют злоумышленникам получать необходимую информацию и применять ее в корыстных целях.

Немаловажную роль играет социальный статус, должность, которую занимает жертва в организации, в связи с которой располагает конфиденциальными сведениями, персональными данными пользователей. Наибольшей опасности подвергаются сотрудники и клиенты банков, так как зачастую именно данные организации строят киберзащиту, ориентируясь, прежде всего, на технические векторы атак, а не человеческие. Кроме того, жертву преступления характеризует уровень ее образования. Зачастую потерпевшими от мошенничеств, совершаемых с использованием техник социальной инженерии, становятся люди с низким уровнем правовой и финансовой грамотности. Однако часть из них является образованными людьми, окончившими высшие учебные заведения. Уровень их образования объясняет широкий круг деловых контактов и во многих случаях стабильное материальное положение, что вызывает наибольший интерес у мошенников[1].

Анализируя личностные качества жертв, необходимо указать на степень их влияния на выбор предмета, места, времени и способа совершения преступления. Для определения характера взаимосвязи между преступником и потерпевшим, личность последнего изучается не в меньшем объеме, чем личность обвиняемого. Немаловажным при расследовании преступлений данного вида является диагностика психического состояния потерпевшего. Совокупность особенностей личности жертвы рассматриваемой категории мошенничеств позволяет сделать вывод о том, что мошенни-

[1] Старостенко Н. И. Криминалистическое понимание механизма совершения мошенничества с использованием методов социальной инженерии // Общество и право. 2021. № 1(75). С. 71-76.

чества с применением методов социальной инженерии совершаются в связи с созданием специальных неблагоприятных условий, которые в настоящее время ни один комплекс технической информационной защиты не способен в полной мере предотвратить[1].

В завершении еще раз отметим, что механизм совершения мошенничеств с использованием методов социальной инженерии представляет собой совокупность взаимосвязанных элементов таких, как субъект преступного события, с дифференцированными способами социальной инженерии, его отношение к деянию, обстановка и предмет преступления, характеристика личности жертвы. Выработка криминалистического понимания механизма данного преступного явления поможет выработать научные рекомендации, повышающие эффективность деятельности правоохранительных органов, а также способствующие решению проблемных ситуаций, возникающих при раскрытии и расследовании преступлений рассматриваемой категории.

[1] Старостенко Н. И. Указ. соч. С. 71–76.

СПОСОБЫ СОВЕРШЕНИЯ МОШЕННИЧЕСТВ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Структуру деяния (способа) практически все криминалисты представляют в виде комплекса действий, которые делятся на следующие группы: по подготовке, совершению (исполнению), посткриминальные и по сокрытию. Все перечисленные группы действий входят в предмет криминалистики, являются объектом ее познания[1].

Способы подготовки к совершению мошенничеств с использованием методов социальной инженерии следующие:

объединение в группы лиц, которые по своим личностным качествам могут оказывать психологическое воздействие на людей, воздействовать на поведение людей;

распределение ролей каждого участника группы (роли распределяются согласно характеру выполнения действий, например часть участников группы выполняет «обзвон» граждан, часть осуществляет рассылки смс сообщений, другая часть злоумышленников выполняет поиск и сбор информации о пользователях в открытых источниках, остальные организовывают проведение финансовых операций по банковским счетам в целях стремительного перечисления денежных средств, добытых преступным путем, на счета третьих лиц и т. д.);

приискание офисов, так называемых колл-центров, в которых имеется возможность организации технического оснащения преступной деятельности;

приискание средств совершения хищений (мобильных телефонов, смартфонов, ноутбуков, наушников, микрофонов, диктофонов, сим-карт, банковских карт и др.);

обеспечение подключения услуг сотовой связи и сети Интернет, открытие счетов в банке от имени третьих лиц;

изучение специальной литературы о психологии человека, об искусстве обмана и манипулирования, изучение психологических слабостей человека, выработка официального стиля изложения речи, создание клеше (текста), сценариев, алгоритмов действий по

[1] Криминалистика: учебник / под ред. В.А. Образцова М., 1997.

успешному достижению корыстного результата, отработка данных навыков и др.

Стадии преступной деятельности, характеризующие способ совершения преступлений рассматриваемого вида:

1. Подготовка к совершению преступления (выбор и изучение преступной схемы поведения, избрание действующих приемов оказания психологического воздействия и т. д.).

2. Исследование цели (сбор и изучение необходимых конфиденциальных данных о потенциальной жертве, поиск информации о ее Ф.И.О., номере телефона, банковских сведений и данных, размещенных на страницах социальной сети, исследование материального положения, круга интересов, информации о близких и родственниках).

3. Взаимодействие с жертвой (на данном этапе мошенник инициирует общение с выбранной жертвой по разработанной преступной схеме таким образом, чтобы она добровольно предоставила свою конфиденциальную информацию либо самостоятельно совершила действия по переводу денежных средств злоумышленнику).

4. Непосредственное совершение преступления (этап характеризуется возникновением последствий применения методов социальной инженерии и достижением корыстной цели, предполагающей неправомерное получение денежных средств либо доступа к сервису дистанционного банковского обслуживания жертвы).

5. Сокрытие преступления. Способы сокрытия преступления мошенником: выезд преступника из населенного пункта, перевод денежных средств на подконтрольные банковские счета, уничтожение следов преступлений, укрытие орудий совершения преступлений (уничижение сим-карт, технических устройств, смена IP-адресов и др.).

Далее перечислим основные способы непосредственного совершения мошенничества с использованием методов социальной инженерии.

1. Убеждение в необходимости оформить кредит и перевести денежные средства.

Так, 14.01.2021 неустановленное лицо позвонил К. и представился сотрудником безопасности «Сбербанка». Далее, предупре-

див об угрозе списания денежных средств, сообщил о необходимости сделать следующие операции: через личный кабинет «Сбербанк онлайн» оформить на себя кредит, после чего в банкомате снять денежные средства в сумме 215000 руб. и положить их в банкомат «Тинькоф банк». В результате выполнения указанных действий под контролем неустановленного лица потерпевшей был причинен значительный ущерб[1].

Рассматриваемый способ мошенничества сопровождается использованием метода социальной инженерии «Претекстинг» и проявляется в использовании при общении с потерпевшей специально подготовленного сценария и выполнения определенной последовательности действий, которые были выполнены потерпевшей под контролем преступника. Достижение корыстных целей неустановленным лицом произошло за счет выдачи себя за представителя банка и создания стрессовой ситуации, возникшей в связи с угрозой списания денежных средств со счета.

2. Убеждение в необходимости выполнить перевод денежных средств для помощи близким;

С 17 часов 30 минут по 17часов 58 минут 30.08.2021 неустановленные лица, путем обмана, позвонив по номеру телефона (812) .., представившись племянником Т. и сообщили ему информацию, не соответствующую действительности о том, что он стал виновником ДТП, и о необходимости уплаты денежных средств для разрешения ситуации в его пользу, тем самым ввели Т. в заблуждение. Т. указанные неустановленными лицами действия выполнил. В результате Т. был причинен материальный ущерб на сумму 30 000 рублей[2].

В рассматриваемом случае также наблюдается использование мошенником метода социальной инженерии «Претекстинг». Преступник, реализуя корыстный мотив, осуществлял манипуля-

[1] Материалы уголовного дела № 12101400019000147, возбужденного 18.01.2021г. СУ МВД России по Выборгскому району г. Санкт-Петербурга по признакам преступления, предусмотренного ч. 2 ст. 159 УК РФ.

[2] Материалы уголовного дела № 12101400016000532, возбужденного 30.08.2021г. СО ОМВД по Курортному району г. Санкт-Петербурга по признакам преступления, предусмотренного ч. 2 ст. 159 УК РФ.

тивное воздействие, нацеленное на создание ложного представления о сложившейся ситуации и оказание неотложной помощи близкому родственнику (племяннику).

3. Обман при осуществлении сделки купли-продажи.

Так, 01.04.2021 года на сайте объявлений «Авито» при продаже женского комбинезона, гр-ке Б. с телефона +7960.. позвонило неустановленное лицо и сообщило о готовности приобрести комбинезон, после обсуждения деталей попросило отправить его с помощью сервиса «Авито доставки», далее прислало ссылку на «Вотсапп», по которой потерпевшая Б. перешла и ввела данные своей банковской карты для получения оплаты. В результате действий неустановленного лица Б. был причинен материальный ущерб на сумму 25 000 рублей[1].

В рассматриваемом случае мошенник, выдавая себя за покупателя, использовал метод социальной инженерии «Фишинг», а именно создал фиктивную ссылку, при использовании которой потерпевший осуществил переход на поддельный сайт, идентичный оригинальному сайту «Авито», где востримая данный сайт за реальный, ввел данные банковской карты, тем самым предоставил мошеннику доступ к своим денежным средствам.

4. Обман при получении выигрыша.

07.01.2021 г. неустановленные лица, путем обмана и злоупотребления доверием, завладели денежными средствами С. на сумму 12000 рублей, а именно 07.01.2021г. отправили сообщение на электронную почту о том, что С. выиграл денежный приз в размере 3 000 долларов США и для получения выигрыша необходимо перейти по ссылке и ввести данные банковской карты, что С. и сделал. Однако после перехода по ссылке и введения данных банковской карты выигрыш зачислен не был, а с банковского счета произошло списание денежных средств в размере 12 000 рублей[2].

---

[1] Материалы уголовного дела № 12101400019001475, возбужденного 07.04.2021 г. СУ МВД России по Выборгскому району г. Санкт-Петербурга по признакам преступления, предусмотренного ч. 2 ст. 159 УК РФ.

[2] Материалы уголовного дела № 12101400019001648, возбужденного 15.04.2021 г. СУ МВД России по Выборгскому району г. Санкт-Петербурга по признакам преступления, предусмотренного ч. 2 ст. 159 УК РФ.

Указанный способ мошенничества был реализован за счет использования метода социальной инженерии «Фишинг». Преступники, используя желание потерпевшего улучшить свое материальное положение и получить денежное вознаграждение, убедили последнего в необходимости ввести данные банковской карты для получения выигрыша.

5. Обман на сайтах знакомств.

Так, в Приговоре № 1-22/2020 1-673/2019 от 3 февраля 2020 г. по делу № 1-22/2020 *Г. разработала план совершения преступления, согласно которому используя имевшиеся в ее распоряжении мобильные телефоны оснащенные доступом к информационно-телекоммуникационной сети «Интернет» (далее - сеть «Интернет») и сим - карты, на интернет сайте «tamba.ru», предназначенном для знакомств , для привлечения потенциальных потерпевших она создала свою учетную запись, в которой разместила фотографии как свои так и третьих лиц, в том числе интимного характера. В ходе переписки с потерпевшими, в зависимости от ситуации, Г. намеревалась сообщать заведомо ложную информацию о себе, а именно о своем семейном положении, образе жизни и финансовом положении, намереваясь тем самым убедить потерпевшего в необходимости оказания ей финансовой помощи. Убедившись, что потерпевший поверил и воспринял сообщенные ему ложные сведения, как соответствующие действительности, Г. должна сообщить номер, находящийся в ее пользовании банковской карты ПАО «Сбербанк России» для перечисления потерпевшими денежных средств. После перечисления потерпевшими денежных средств на подконтрольную Г. банковскую карту, последняя, в зависимости от ситуации намеревалась вновь сообщить ему несоответствующие действительности сведения в необходимости оказания ей дополнительной финансовой помощи*[1].

В рассматриваемом способе совершения мошенничества использовался метод социальной инженерии «Претекстинг», представляющий собой действие по заранее спланированному сценарию, включающему поиск и подготовку фотографий третьих лиц,

[1] Приговор Бийского городского суда Алтайского края № 1-22/2020 1-673/2019 от 3 февраля 2020 г. по делу № 1-22/2020.

создание Интернет-страницы с размещением указанных фотографий на сайте знакомств от своего имени, формирование текстовых клеше для организации взаимодействия с потенциальными жертвами и т. д.

6. Получение банковских данных во время телефонного звонка.

Так, 02.04.2020 в 15 часов 20 минут неустановленное лицо, находясь в неустановленном месте, путем обмана, представившись сотрудником «Сбербанка» под предлогом угрозы выполнения по счету подозрительных операций на банковской карте, убедило Ж. предоставить данные смс-кода, пришедшего от банка на мобильный телефон, тем самым вынудило Ж. добровольно выполнить перевод денежных средств в сумме 21 010 рублей со своего банковского счета на счет неустановленного лица.[1]

В данном способе мошенничества был использован метод социальной инженерии «Вишинг», выраженный в действии неустановленного лица от имени сотрудника банка, сообщающего информацию о подозрительных операциях по счету, провоцирующих стрессовую ситуацию для потерпевшего и создание условий ограниченности времени, отпущенного на принятие им обдуманного решения. Таким образом, жертвы преступлений, совершенных подобным приемом, доверяя «сотрудникам банка», сообщивших новость об угрозе списания денежных средств передуют свои конфиденциальные (банковские) данные мошенникам, не подозревая об истинности их противоправных намерений.

Как уже было отмечено, мошенники при совершении изучаемых поступлений действуют не от своего имени, а выдают себя за представителя какой-либо государственной или негосударственной организации, близкого родственника или другого человека, который может вызвать доверие у потерпевшего. В связи с этим мы рассмотрели способы совершения мошенничеств с использованием методов социальной инженерии, сформулированные в зависимости от схемы преступного поведения:

[1] Материалы уголовного дела № 12001450299000338, возбужденного 03.04. 2020 г. СУВД по Троицкому и Новомосковскому АО г. Москвы по признакам преступления, предусмотренного ч. 2 ст. 159 УК РФ.

«сотрудник банка» – наиболее популярная схема у мошенника, когда он представляется специалистом банка или сотрудником службы безопасности банка и, играя на страхе жертвы потерять деньги, получает данные банковской карты, в том числе и ее секретный пароль;

«представитель пенсионного фонда» – суть данной схемы заключается в убеждении жертвы о возможности получить выплаты, а затем завладеть ее денежными средствами;

«друг или родственник» – данная схема подразумевает действия мошенника, когда он представляется другом, товарищем или родственником с просьбой о неотложной помощи в беде или денежном переводе на лечение;

«бесплатный помощник» – в названной схеме деяния злоумышленника выражены в скрытых мошеннических действиях под видом бесплатной финансовой или правозащитной консультации, а предложенные им услуги оказываются за определенную сумму. Расчет преступника направлен на то, что данные услуги фактически не будут осуществлены, а денежные средства спишутся с банковского счета;

«покупатель по объявлению» – суть данной схемы выражена в том, что мошенник под видом покупателя сообщает жертве о готовности купить у нее тот или иной товар на интернет-сайте «Авито» или «Юла», однако для этого ему понадобятся данные банковской карты для перевода денежных средств, включая секретный код этой карты или проверочный код из СМС;

«продавец с интернет-сайта» – в названной схеме злоумышленник наоборот размещает заманчивое предложение о продаже какого-либо товара. Зачастую мошенник создает поддельный сайт под видом известного магазина, надеясь заинтересовать жертву выгодным предложением. Такой способ мошенничества подразумевает, что жертва при покупке данного товара переведет преступнику предоплату или полную сумму за этот товар[1];

«сотрудник правоохранительных органов» – при реализации корыстного умысла мошенник выдает себе за сотрудника поли-

[1] Старостенко Н.И., Старостенко О.А. Криминалистическая характеристика способов мошенничества, совершенного с использованием методов социальной инженерии // Проблемы правовой и технической защиты информации. 2020. № 8. С. 107-110.

ции, прокуратуры, ФСБ и др. Во время звонков мошенник сообщает жертве, что в отношении нее якобы возбуждено уголовное дело по заявлению Банка России. Для выявления обстоятельств дела преступники просят человека уточнить информацию по карте – сообщить полные реквизиты, включая срок действия и три цифры, находящиеся на обороте карты.

Таким образом, нами были сформулированы основные способы совершения мошенничеств, в которых были применены методы социальной инженерии, реализуемые с помощью информационно-телекоммуникационных технологий. Данный анализ позволяет выделить основные особенности способов совершения указанных преступлений. К числу таких особенностей можно отнести: предварительная подготовка к совершению мошеннических действий и сбор конфиденциальной информации о потенциальных жертвах, выдача за другое лицо (сотрудника организации), использование в ходе реализации корыстного умысла мобильного или компьютерного устройства, позволяющего дистанционно оказывать психологическое воздействие на личность и способствующего сообщению или распространению ложной информации, которую жертва воспринимает за действительную.

МЕХАНИЗМ СЛЕДООБРАЗОВАНИЯ ПРИ СОВЕРШЕНИИ МОШЕННИЧЕСТВ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Основными источниками криминалистически значимой информации о виновных лицах являются следы преступления. Благодаря названой информации, правоохранительные органы получают данные о событии преступления, позволяющие установить и изобличить преступника. Именно поэтому изучение механизма образования следов преступления и работа следователя (суда), связанная с их обнаружением и анализом, составляют основу науки криминалистики.

Тенденция механизма следообразования мошенничеств, совершенных с использованием методов социальной инженерии, существенно отличается от хищений традиционных видов. Данный факт обуславливается тем, что в процессе проведения следственных действий, обнаруживаются, исследуются и фиксируются как общеизвестные следы (материальные и идеальные), так и электронно-цифровые, образованные благодаря использованию информационно-телекоммуникационных технологий.

Применительно к рассматриваемой категории мошенничеств будет вполне обосновано выделить следующие материальные следы-предметы:

портативные, многофункциональные или микропроцессорные электронные устройства: персональные компьютеры, ноутбуки, смартфоны, планшеты и др. гаджеты;

электронные носители информации устройства вывода информации;

оборудование компьютерных и беспроводных сетей;

детали электронных устройств документы, рукописные и машинописные записи конфиденциальных сведений, данные банковских карт потенциальных жертв;

SIM-карты, используемые мошенниками и SIM-карты жертв;

банковские карты, используемые мошенниками и банковские карты жертв;

личные вещи мошенника;

блокноты, записные книжки;

машинописные алгоритмы и сценарии (тексты) взаимодействия с жертвами;

различные документы, свидетельствующие о заключении договоров на получение услуг связи, сети Интернет, банковских услуг и др.

Поскольку речь идет о работе с объектами материального мира, то следует учитывать необходимость сбора следов человека, которые можно обнаружить на следах-предметах. Среди них приобретают существенную ценность и криминалистическую значимость: следы папиллярных линий рук и ног; следы зубов; следы частей тела; следы одежды; вещественные следы биологического происхождения: следы слюны, крови, волос, пота, запаха и прочих выделений человеческого организма (перхоть, подногтевое содержимое) и др.

Идеальные следы выступают как субъективные образы материальной действительности, отображенные в памяти человека, и позволяют выявить важные элементы в его сознании. Идеальные следы преступления – криминалистически значимая уголовно-релевантная информация, воспринятая и запечатленная человеком в виде мысленных (памятных) образов, и которая может быть им воспроизведена в вербальной форме либо извлечена из его памяти средствами, допустимыми для использования в уголовном судопроизводстве[1].

Отметим, что идеальные следы возникают в памяти потерпевшего, подозреваемого (обвиняемого), свидетеля, эксперта, специалиста и других лиц, в связи с вовлечением их в процесс уголовно-правовых и процессуальных правоотношений, а также собиранием, исследованием, использованием и оцениванием полученной информации.

Особенностью идеальных следов рассматриваемой категории преступности является практическая невозможность потерпевшего запечатлеть в памяти внешний облик злоумышленника в связи с дистанционным характером совершения преступления.

---

[1] Суворова Л.А. Идеальные следы в криминалистике: канд. юрид. наук: 12.00.09. Воронеж, 2005. 245 с.

Принимая во внимание вышеизложенное, стоит подчеркнуть, что мошенничества, совершенные с использованием методов социальной инженерии, реализуются удаленно от жертв, что подтверждает сложность построения обвинения только на материальных и идеальных следах преступления, так как они не отражают в полной мере всю картину произошедшего события.

В научных изданиях неоднократно рассматривался вопрос о значимости следов, образованных в связи с использованием информационно-телекоммуникационных технологий и принимающих важнейшее участие в воссоздании механизма совершения преступления, а также служащих одним из основных источников доказательственной информации при расследовании компьютерных преступлений или преступлений, совершенных в сети Интернет.

В настоящее время обозначенный элемент механизма следообразования определяют как «цифровые следы», «виртуальные следы», «компьютерные следы». В криминалистических учениях нет единого мнения о том, какое из понятий верно и какое необходимо использовать для обозначения категории следов, образованных в результате использования информационно-телекоммуникационных технологий.

Мы придерживаемся позиции, что следы, образованные при помощи информационно-телекоммуникационных, необходимо рассматривать в качестве «электронно-цифровых следов», поскольку данная формулировка свидетельствует о том, что эти следы образованы в результате движения электронов, которые оставляют в памяти электронных устройств криминалистически значимую информацию, которая в свою очередь представлена в виде двоичного (цифрового) кода[1].

По нашему мнению, электронно-цифровые следы преступления – это изменение состояния автоматизированной системы, а также информации, которая содержится в памяти электронно-вычислительных устройств или создана в сети Интернет с помощью

[1] Старостенко Н. И. Особенности механизма следообразования при совершении хищений с использованием информационно-телекоммуникационных технологий и методов социальной инженерии // Вектор науки Тольяттинского государственного университета. Серия: Юридические науки. 2021. № 4(47). С. 48-54. DOI 10.18323/2220-7457-2021-4-48-54.

названных устройств, непосредственно связанных с преступной деятельностью.

Кроме того, необходимо добавить, что совершенствование технологий передачи и хранения информации, особенности ее обработки, передачи и воспроизведения обусловили изучение электронно-цифровых следов в качестве самостоятельного элемента механизма следообразования. Именно поэтому механизм следообразования преступлений рассматриваемой категории ровно, как и деятельность по собиранию, фиксации и исследованию в процессе доказывания таких следов, отличается ярко выраженной спецификой.

По нашему мнению, установление особенностей следовой картины, в частности, той ее части, которая включает электронно-цифровые следы, позволит правильно квалифицировать деяние, определить способ и механизм совершения преступления, верно и в полной мере осуществить сбор доказательственной базы, а также своевременно изобличить виновного в совершении преступления.

Поэтому считаем необходимым рассмотреть электронно-цифровые следы мошенничеств анализируемого вида в зависимости от применяемых методов социальной инженерии и информационно-телекоммуникационных технологий:

1)Осуществление фишинговых рассылок в сети Интернет от имени известных кампаний/организаций с просьбой предоставить конфиденциальные данные или скачать вредоносную программу, предварительно замаскированную под полезное приложение, графический файл.

К указанной группе методов социальной инженерии можно отнести следующие электронно-цифровые следы:

программы для создания сайтов (интернет-магазинов), приложения социальных сетей и сервисов электронной почты, программы, осуществляющие удаленное администрирование;

анкетные данные пользователя (злоумышленника), указанные в названных программах и приложениях при регистрации;

текстовые клише, содержащие обращения от имени государственных учреждений, банковских организаций, администраторов социальных сетей, например, «Госуслуги», «СберБанк», «Авито», покупателей/продавцов в интернет-магазинах и др.;

черновики электронных писем, содержащих форму на предоставление жертвой конфиденциальной информации либо ссылку

для перехода на фишинговый сайт (сайт-клон известной организации/кампании);

списки рассылки сообщений;

входящие/исходящие электронные сообщения в сети Интернет, а также вся информация их характеризующая (содержание, дата, время, email адреса, с которых были отправлены/получены сообщения, имя отправителя/имя получателя, фотография (изображение, которое было размещено в качестве фотографии пользователя интернет-ресурса) и др.);

электронные базы персональных и банковских данных жертв;

информация о веб-браузере компьютера или сотового телефона преступника, содержащем ссылки, истории посещения вебсайтов, свидетельствующие о способности злоумышленника осуществлять рассылки, сбор и анализ конфиденциальных сведений жертвы;

ссылки на фишинговый сайт, снимки экрана страниц сайта (изображение, полученное устройством и показывающее в точности то, что видит пользователь на экране монитора или другого визуального устройства вывода, например, фрагмент веб-страницы);

снимки экрана устройства, свидетельствующие о криминалистически значимой информации о сайте (название, характеристика интерфейса, целевое назначение, адресная строка, дата и время посещения, описание конфиденциальных данных, которые на указанном сайте требуется вводить или какие действия выполнить и т. д.);

специально созданные цифровые фотографии и видео файлы, например для отправки сообщений на сайтах бесплатных объявлениях «Авито»/«Юла», способствующие осуществлению фиктивных сделок;

снимки экрана, свидетельствующие о продаже какого-либо товара или оказания услуги (фиксирующие информацию о наименовании товара (услуги), его описании, стоимости, адресе, указанном в качестве места встречи с покупателем, номере телефона и др.);

снимки экрана, свидетельствующие о переписке злоумышленника с жертвой (содержание просьб или требований, которые были выдвинуты злоумышленником, ссылки, которые направил

для перехода на сайт, характеристика конфиденциальных данных, необходимых для осуществления какой-либо операции и др.)

электронно-цифровые данные от провайдера сети Интернет (информация об IP-адресах злоумышленников, сведения о доменном имени, сведения о регистрации домена при создании фишингового интернет-сайта и др.).

образцы шпионских или вредоносных программ. Инструкции по их использованию и внедрению в персональный компьютер или сотовый телефон для кражи конфиденциальных данных жертвы или электронных денежных средств и др.[1]

2)Выдача за другое лицо при телефонном звонке и использование при общении с жертвой предварительно подготовленного сценария (текста) или алгоритма взаимодействия с жертвой для получения конфиденциальных данных или склонения к осуществлению каких-либо действий с банковским счетом (картой).

В указанных случаях целесообразно выделить следующие электронно-цифровые следы:

программные компоненты, позволяющие осуществить подмену абонентского номера, которые способствуют использованию услуг сотовой связи без установления личности абонента и данных о вызове;

фонограммы записи голоса специалиста банковской организации, сотрудника полиции или пенсионного фонда и др.

сценарии взаимодействия с жертвой, алгоритмы оказания психологического воздействия для достижения преступной цели, представленные в электронном виде;

электронные файлы, содержащие сценарий (текст) по неправомерному получению конфиденциальной информации пользователей либо алгоритмы, способствующие достижению выполнения жертвой определенных действий со своим банковским счетом (картой) в интересах злоумышленника.

[1] Старостенко Н. И. Особенности механизма следообразования при совершении хищений с использованием информационно-телекоммуникационных технологий и методов социальной инженерии // Вектор науки Тольяттинского государственного университета. Серия: Юридические науки. 2021. № 4(47). С. 48-54. DOI 10.18323/2220-7457-2021-4-48-54.

электронно-цифровые данные от операторов связи, о лице, на которое зарегистрирована SIM-карта (о входящих и исходящих соединениях; о фактах приема, передачи, доставки и (или) обработки голосовой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей услугами связи – в течение трех лет с момента окончания осуществления таких действий и другая информация),

цифровые фонограммы звукозаписи разговоров злоумышленников с жертвами;

данные списков контактов злоумышленника;

журналы входящих/исходящих вызовов злоумышленника или жертвы и другая информация.

Кроме того, отмечается ряд общих электронно-цифровых следов, которые свойственны всем хищениям, совершенным с использованием информационно-телекоммуникационных технологий и методов социальной инженерии, как сведения о проведенной банковской транзакции по счету (карте), записи с камер видеонаблюдения в банкоматах или банках, в которых было осуществлено обналичивание денежных средств подозреваемыми и др.[1]

Далее сформулируем основные выводы о механизме следообразования мошенничеств, совершенных с использованием методов социальной инженерии:

1. Материальные, представленные в виде следов-предметов (технических устройств, приспособленных для реализации методов социальной инженерии, SIM-карт, банковских карт, документов), следов-отображения (биологических следов, позволяющих установить, что хищение денежных средств совершалось конкретным лицом при помощи определенного технического устройства).

2. Идеальные, являющиеся мысленным образом воспринятого события преступления или его элементов в сознании человека, представлены в показаниях потерпевшего, подозреваемого (обвиняемого), свидетеля, эксперта, специалиста и других лиц, в

[1] Старостенко Н. И. Особенности механизма следообразования при совершении хищений с использованием информационно-телекоммуникационных технологий и методов социальной инженерии // Вектор науки Тольяттинского государственного университета. Серия: Юридические науки. 2021. № 4(47). С. 48-54. DOI 10.18323/2220-7457-2021-4-48-54.

связи с вовлечением их в процесс уголовно-правовых правоотношений, складывающихся в результате противоправных дистанционных действий подозреваемого (обвиняемого) по оказанию психологического воздействия (использования методов социальной инженерии) на потерпевшего в целях осуществления несанкционированного доступа к его конфиденциальной информации и хищения электронных денежных средств.

Важно подчеркнуть, что показания потерпевших и специалистов-психологов представляют наибольший интерес при расследовании рассматриваемых преступлений, так как эти лица могут сообщить информацию о психологической манипуляции, применяемой в отношении них, о механизмах оказанного психологического воздействия, дать характеристику психологического состояния, вызванного целенаправленными действиями подозреваемого, а также дать оценку действиям, побудивших добровольно предоставить конфиденциальную информацию или совершить определенные действия.

3. Электронно-цифровые, выраженные в совокупности информации, которая содержится в памяти электронно-вычислительных средств (устройств), непосредственно связанных с преступной деятельностью злоумышленника, т.е. следы, констатирующие применение методов социальной инженерии в отношении потерпевшего при помощи информационно-телекоммуникационных технологий. Кроме того, отмечается потребность в квалифицированных специалистах, обладающих навыками сохранения электронно-цифровых следов и умениями извлечения из таких следов криминалистически значимой информации, позволяющей интерпретировать ее для понимания ключевых аспектов рассматриваемых преступлений.

Таким образом, сформирована типичная следовая картина мошенничеств, совершенных с методов социальной инженерии, знание которой позволяет получить необходимую информацию о способе совершения преступления, причастных к нему лицах, а также определяет тактику проведения оперативно-розыскных мероприятий и следственных действий.

Заключение

Таким образом, проведенное исследование позволило сформулировать основные теоретические аспекты применения методов социальной инженерии при совершении мошенничеств. В работе освещены вопросы понимания социальной инженерии в качестве объекта криминалистического изучения, раскрыты основные ее признаки и методы. Кроме того, в ходе исследования была сформулирована характеристика криминалистического механизма совершения мошенничеств с использованием методов социальной инженерии, дано описание личности мошенника, жертвы, обстановки совершения мошеннических действий и других элементов. В дополнении на основе судебной и следственной практики были выявлены основные способы и схемы совершения мошенничеств, в которых реализуются указанные методы социальной инженерии. А также с учетом предложенной криминалистически значимой информации сформирована типичная следовая картина анализируемых преступлений.

По нашему мнению, дальнейшее изучение преступности анализируемого вида чрезвычайно важно поскольку мошенничества, реализуемые за счет методов социальной инженерии динамичны, а их показатели в сводках статистических данных демонстрируют тенденции к росту. Тот факт, что грамотность населения в сфере информационной безопасности и сфере оказания банковских услуг находится на достаточно низком уровне, помогает мошенникам использовать методы социальной инженерии в преступных целях. Данная проблема широко обсуждается как в научном сообществе, так и средствах массовой информации, однако действующие нормативные правовые акты не содержат правовых дефиниций социальной инженерии и ее видов[1].

С учетом вышеизложенного, считаем необходимым закрепить криминалистические признаки способа совершения мошенничеств с использованием методов социальной инженерии в кри-

[1] Старостенко Н. И. Криминалистический аспект техник социальной инженерии при совершении преступлений // Вестник Краснодарского университета МВД России. 2020. № 1(47). С. 80-83.

миналистических учениях, дополнить имеющиеся знания о способе совершения мошенничеств с использованием информационно-телекоммуникационных технологий новым способом – с использованием методов социальной инженерии, а также выработать соответствующую криминалистическую методику расследования подобных хищений и тактику проведения отдельных следственных действий.

Литература

Нормативные документы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7- ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ) // Собрание законодательства РФ, 04.08.2014, № 31, ст. 4398.

2. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 29.07.2017) (с изм. и доп., вступ. в силу с 01.09.2017) [Электронный ресурс] // Режим доступа: http://www.consultant.ru (дата обращения: 16.06.2021).

3. Уголовный кодекс Российской Федерации от 13.06.1996 №63-ФЗ (ред. от 29.07.2017) (с изм. и доп., вступ. в силу с 26.08.2017), [Электронный ресурс] // Режим доступа: http://www.pravo.gov.ru (дата обращения: 16.06.2021).

4. Федеральный закон «О банках и банковской деятельности» от 02.12.1990 № 395-1 (ред. от 30.12.2020 № 495-ФЗ) Режим доступа: http://www.pravo.gov.ru (дата обращения: 16.06.2021).

5. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (ред. 30.12.2020 № 530-ФЗ) Режим доступа: http://www.pravo.gov.ru (дата обращения: 16.06.2021).

6. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ (ред. от 30.12.2020) (с изм. и доп., вступ. в силу с 01.03.2021) Режим доступа: http://www.pravo.gov.ru (дата обращения: 16.06.2021).

7. Федеральный закон «О национальной платежной системе» от 27.06.2011 № 161-ФЗ (ред. от 02.07. 2021) URL: http://www.consultant.ru/document/cons_doc_LAW_115625/ (дата обращения 10.09.2021 г.).

Монографии, учебники и учебные пособия

8. Белкин Р.С. Курс криминалистики: в 3 т.; т. 2: Частные криминалистические теории. М.: Юристъ, 1997. 464 с.

9. Белкин Р.С. Криминалистика: проблемы сегодняшнего дня. М. 2001. 304 с.

10. Белкин Р.С. Криминалистика: учебник для вузов / под ред. Р.С. Белкина. М.,2001. 990 с.

11. Головин А.Ю., Головина Е.В. Социальная инженерия в механизме преступной деятельности в сфере информационно телекоммуникационных технологий // Известия ТулГУ. Экономические и юридические науки. 2021. №2. С. 3-13.

12. Зеленский В.Д., Меретуков Г.М. Криминалистика. Учебник / под ред. Зеленского В.Д., Меретукова Г.М. М., Издательство «Юридический центр» 2015. 704 с.

13. Жданов Ю.Н., Овчинский В.С. Киберполиция XXI века. Международный опыт/ под ред. С.К. Кузнецова.М:.Международные отношения, 2020. 288 с.

14. Кевин Д. Митник, Вильям Л. Саймон Искусство обмана. М.,-2004. 360 с.

15. Колдин В.Я. Корухов Ю.Г. Криминалистика социалистических стран. М., 1986. 509 с.

16. Криминалистика: Учебник /Под ред. В.А. Образцова М., 1997.

17. Криминалистика. Учебник / Герасимов В.Н., Колдин В.Я., Крылов В.В., Куликов В.И., и др.; Отв. ред.: Яблоков Н.П. М.: БЕК, 1996. 708 с.

18. Криминалистика: учебник / под ред. И. Ф. Пантелеева, Н.А. Селиванова. М.: Юрид. лит., 1988. 672 с.

19. Криминалистика: учебник / под ред. И.Ф. Крылова, А.И. Бастрыкина. М.: Дело,2001. 506 с.

20. Крылов И.Ф. Избранные труды по криминалистике. СПб.: Юрид. фак. СПбГУ, 2006. 998 с.

21. Овчинский В.С. Мафия. Новые мировые тенденции «Коллекция изборского клуба» М.: Книжный мир, 2016. 369 с.

22. Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: международный опыт: монография. М.: Норма, 2004. 432 с.

23. Черемушкин А. В. Информационная безопасность. Глоссарий /под ред. С. Пазизина. М., 2013.

24. Якимов И.Н. Криминалистика. Руководство по уголовной технике и тактике. Новое издание, перепечатанное с издания 1925 г. М.: ЛексЭст, 2003. 496 с.

Научные статьи и иные публикации

25. Давыдов В.О., Головин А.Ю. Значение виртуальных следов в расследовании преступлений экстремистского характера / В.О. Давыдов // Известия Тульского государственного университета. Экономические и юридические науки. 2016. № 3. 485 с.

26. Дворянчиков Н. В., Соловьева Ю. А. Психологические механизмы манипуляции поведением потребителя // Психология и право. 2011. № 1. С. 1-10.

27. Гусев А.В. Медведева С.Н. Использование признаков материального следа для определения компонентов причинно-следственной связи и механизма следообразования // Вестник Краснодарского университета МВД России. № 2 (36). 2017. С. 97-102.

28. Куклина А.Ю. Криминальное манипулирование сознанием на примере мошенничества // Организация работы с молодежью. 2018. № 3. С. 55-62.

29. Кустов А. М. К вопросу о структуре механизма преступления // Пенитенциарная наука. 2009. №5. URL: https://cyberleninka.ru/article/n/k-voprosu-o-strukture-mehanizma-prestupleniya (дата обращения: 16.11.2020).

30. Кустов А.М. Типичная модель механизма преступлений террористического характера. Материалы Всероссийской научно-практической конференции. Москва: ФГБОУ ВО «Российский химико-технологический университет имени Д.И. Менделеева». 2019. С 137-143.

31. Меретуков Г.М. Механизм преступления в структуре криминалистической характеристики // Современные проблемы отечественной криминалистики и перспективы ее развития : Сборник научных статей по материалам Всероссийской научно-практической конференции (с международным участием), посвященной 20-летию кафедры криминалистики, Краснодар, 28–29 сентября 2018 года / Ответственный редактор Г.М. Меретуков. Краснодар:

Кубанский государственный аграрный университет имени И.Т. Трубилина, 2019. С. 97-102.

32. Образцов В.А. Преступление как объект криминалистического познания // Вопросы борьбы с преступностью. № 42. М., 1985. С. 47-48.

33. Осипенко А.Л. Об участии органов внутренних дел в системе обеспечения кибербезопасности Российской Федерации // Общество и право. 2018. №3 (65). С. 35-42.

34. Поляков В.В. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики // Известия АлтГУ. 2013. №2 (78). С. 114-116.

35. Ревенков П.В., Бердюгин А.А. Социальная инженерия как источник рисков в условиях дистанционного банковского обслуживания // Национальные интересы: приоритеты и безопасность. 2017. №9 (354). С. 1747-1760.

36. Резник Ю.М. Социальная инженерия: предметная область и границы применения// Социологические исследования. 1994. № 2. С. 87-96.

37. Россинская Е. Р., Рядовский И. А. Концепция цифровых следов в криминалистике // Аубакировские чтения: материалы Международной научно-практической конференции (19 февраля 2019 г.). Алматы, 2019. С. 6-9.

38. Созаев С.С., Кунашев Д.А. Социальная инженерия, ее техники и методы её противодействия // Международный журнал «Вестник науки». 2020. №2(23). Т.1. С.85-88.

39. Старостенко, Н. И. Криминалистическое понимание механизма совершения мошенничества с использованием методов социальной инженерии // Общество и право. 2021. № 1(75). С. 71-76.

40. Старостенко НИ. Криминалистический аспект техник социальной инженерии при совершении преступлений // Вестник Краснодарского университета МВД России. 2020. № 1(47). С. 80-83.

41. Старостенко Н. И. Особенности механизма следообразования при совершении хищений с использованием информационно-телекоммуникационных технологий и методов социальной инженерии // Вектор науки Тольяттинского государственного университета. Серия: Юридические науки. 2021. № 4(47). С. 48-54. DOI 10.18323/2220-7457-2021-4-48-54.

42. Старостенко О.А. Индивидуальная виктимность жертвы информационно-телекоммуникационного мошенничества // Вестник Краснодарского университета МВД России. 2021. № 1 (51). С. 28-32.

43. Центров Е.Е. Следы как отражение взаимосвязи объектов и их связи с происшедшим событием // Вестник криминалистики. Вып. 1 (3). М., 2002.

44. Blommaert J., Omoniyi T. E-mail fraud: Language, technology, and the indexicals of globalization // Social Semiotics. 2006. №16, P. 573-605.

45. Huang W., Brockman A. Social engineering exploitations in online communications: Examining persuasions used in fraudulent e-mails. In T. Holt (Ed.) // Crime online: Correlates, causes, and context Durham, NC: Carolina Academic Press. 2011. P. 87-111).

46. Mann I. Hacking the human: Social engineering techniques and security measures. Burlington, VT: Gower Publishing Company. 2008.

47. Ortega R. The emotional impact on victim of traditional bullying and cyberbullying a study of Spanish adolescents / R. Ortega, P. Elipe, J. Mora-Merchan, J. Calmaestra, E. Vega // Journal of Psyhology. 2009. Vol. 217 (4). P. 197-204.

48. Ross J. Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems. – John Wiley & Sons, 2008-04-14. – 1080 c.

49. Workman M. Wisecracker: A theory-grounded investigation of phishing and pretext social engineering threats to information security // Journal of personality and Social Psychology. 2009. № 9. P. 1-27.

Диссертации и авторефераты диссертаций

50. Веселов А. В. Социальная инженерия: сущность и парадигмальная методология: дис. кан. фил. наук: 09.00.11. Москва, 2012. 185.

51. Колычева А.Н. Фиксация доказательственной информации, хранящееся на ресурсах сети Интернет: автореф. канд. юрид. наук: 12.00.12 / Колычева Алла Николаевна. М., 2019.С. 25.

52. Суворова Л.А. Идеальные следы в криминалистике: дис. канд. юрид. наук: 12.00.09. Воронеж, 2005. 245 с.

Оглавление

Учебное издание

Гусев Алексей Васильевич
Старостенко Нина Игоревна

ВЫЯВЛЕНИЕ МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ, ПРИМЕНЯЕМЫХ В МОШЕННИЧЕСКИХ ЦЕЛЯХ

Методические рекомендации

В авторской редакции
Компьютерная верстка *Г. А. Артемовой*

ISBN 978-5-9266-1934-5

Подписано в печать 16.03.2023. Формат 60x84 1/16.
Усл. печ. л. 2,5. Тираж 50 экз. Заказ 118.

Краснодарский университет МВД России.
350005, г. Краснодар, ул. Ярославская, 128.