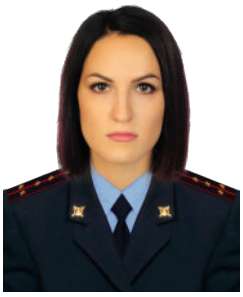
УДК 343.9



Марина Олеговна ЯНГАЕВА,
преподаватель кафедры криминалистики Барнаульского юридического института МВД России,
кандидат юридических наук
marina-ymo@mail.ru

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ КАК СПОСОБ СОВЕРШЕНИЯ КИБЕРПРЕСТУПЛЕНИЙ

SOCIAL ENGINEERING AS A WAY OF COMMITTING CYBER CRIMES

В статье социальная инженерия рассматривается как способ совершения преступлений в сфере компьютерной информации. Проанализированы мнения ученых и специалистов в сфере компьютерных технологий по вопросу содержательного определения социальной инженерии, выделены и проиллюстрированы восемь наиболее популярных методов (техник) применения социальной инженерии: фишинг, претекстинг, «Троянский конь», вымогатель, кви про кво, вишинг, «дорожное яблоко», обратная социальная инженерия.

The article considers social engineering as a method of committing crimes in the field of computer information. The opinions of scientists and specialists in the field of computer technologies on the issue of a meaningful definition of social engineering are analyzed, the eight most popular methods (techniques) of using social engineering are highlighted and illustrated: phishing, pre-texting, «Trojan horse», extortionist, qui pro quo, vishing, «Road apple», reverse social engineering.

Ключевые слова: социальная инженерия, киберпреступления, киберпреступник, способ совершения преступления, компьютерная информация.

Keywords: *social engineering, cybercrimes, cybercriminal, method of committing a crime, computer information.*

«Кто владеет информацией, тот владеет миром»
Н. Ротшильд

Современный мир невозможно представить без информационно-телекоммуникационных технологий. Государства окутаны между собой информационными потоками, назначение которых – передача, сбор, анализ и хранение информации. Приоритетной задачей любого государства является обеспечение информационной безопасности его граждан.

С каждым годом киберпреступлений[1] становится все больше. По данным статистики Министерства внутренних дел РФ в 2017 году были зарегистрированы 90587 преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, в 2018 г. – 174674, в 2019 г. – 294409, направлены в суд – 57221, а в январе-июле 2020 г. – 272737, направлены в суд – 47098, остальные 87% так и остаются не раскрытыми[2].

1 Под киберпреступлениями в данной статье понимаются все преступления, совершенные с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации.

2 Состояние преступности в России // Официальный сайт МВД России. URL: https://mvd.ru.

Проанализировав статистические данные Министерства внутренних дел РФ, констатируем, что сфера киберпреступлений развивается с высокой скоростью, чего нельзя сказать о показателях направления уголовных дел в суд. Считаем, что преступления, связанные с киберпреступностью, сложны в расследовании, а правоохранительные органы нуждаются в кадрах с достаточно интеллектуальным потенциалом в сфере компьютерных технологий.

Необходимо заметить, что в большинстве случаев киберпреступлений технические средства защиты информации исправно выполняют свои функции, чего нельзя сказать о некомпетентном пользователе.

Люди – социальные существа. Мы не представляем себе, как можно жить в одиночестве, без общения. Нам нравится помогать друг другу. Мы склонны доверять авторитетным людям. В нас с детства закладывают информацию о том, что необходимо быть честными по отношению друг к другу, а подвергать сомнению сказанное другим человеком без уважительной причины – это неправильно.

К сожалению, эти социальные тонкости могут превратить нас в самое слабое звено в системе информационной безопасности. Слишком часто взломы возникают не из-за технических недостатков, а из-за того, что люди позволяют киберпреступникам убедить себя в чем-то и тем самым ослабить бдительность и собственную охрану.

Компьютерная система, которую взламывает преступник, не существует сама по себе. Она всегда содержит в себе еще одну составляющую: человека. Схематично современную компьютерную систему можно представить следующим образом.

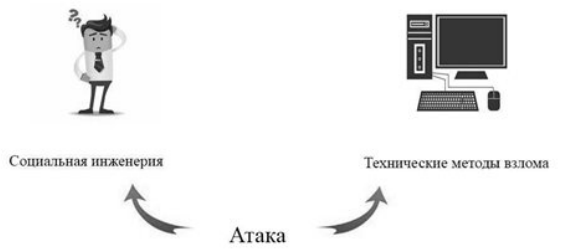


Рис. 1. Система человек – компьютер

Задача преступника состоит в том, чтобы взломать компьютерную систему. Так как у этой системы две составляющие, соответственно, и основных путей ее взлома два. Первый путь, когда «взламывается персональный компьютер» с помощью технических методов взлома. Второй путь, когда с помощью методов социальной инженерии преступник атакует пользователя компьютера [2, с. 10-11].

По мнению многих ученых и IT-специалистов, в следующее десятилетие именно социальная инженерия будет представлять наибольшую угрозу информационной безопасности.

В связи с чем такое возможно? Ответ очевиден. Технические системы защиты с каждым годом совершенствуются, а люди так и будут оставаться самым слабым звеном в системе информационной безопасности со своими стереотипами, слабостями, предрассудками и т.д.

Впервые понятие «социальная инженерия» применил американский социолог Роско Паундом. Кевин Митник (известный киберпреступник, а ныне консультант по безопасности) еще в 1990-е гг. стал популяризировать данный термин. Он считал, что ни один технический код не сможет так обмануть человека, как психологические умения преступника [3, с. 55-60].

Так что же такое социальная инженерия? К сожалению, данное понятие не рассматривается ни в одном нормативном правовом акте, однако многие ученые и специалисты в области информационных технологий предлагают свои варианты определения данного термина.

К.Д. Митник и В.Л. Саймон считают, что социальная инженерия – это совокупность подходов прикладных социальных наук, приемов и технологий, ориентированных на создание организационных структур для регулирования и управления действиями человека [3].

По мнению П.В. Ревенкова и А.А. Бердюгина, социальная инженерия – это метод хищения конфиденциальной информации пользователей [4, с. 1749].

Социальная инженерия также часто рассматривается как «манипулирование поведением человека с помощью использования социальных и психологических навыков» в целях достижения корыстного результата [6, с. 81].

С.С. Созаев и Д.А. Кунашев предлагают под социальной инженерией рассматривать искусный метод управления психологией человека без использования технических приемов взломов для получения персональной информации, доступа к чему-либо [5, с. 86].

На наш взгляд, данные определения не дают реального понимания сущности социальной инженерии в связи с полным отсутствием конкретики.

Мы считаем определение социальной инженерии, сформулированное В.В. Суворовой и Л.А. Суворовой, наиболее информативным на сегодняшний день. Они предлагают определять социальную инженерию как «вид совершения компьютерных преступлений, направленный на несанкционированное получение информации путем использования слабых мест в психике человека» [7, с. 73].

По данным Центрального банка Российской Федерации, в 2019 г. большинство хищений с банковских счетов проводились с помощью техник социальной инженерии (69%). С. Кузнецов (заместитель председателя ПАО «Сбербанк») рассказал, «что в 2017 году доля социальной инженерии составляла 75% от всего кибермошенничества, в 2018 – 79%, в 2019 – 89%, а в 2020 году уже достигла 90%»[3]. Он также отметил, что в обозримом будущем этот тренд не изменится и мошенники продолжат пользоваться низкой киберграмотностью населения.

В связи с этим Сбербанк выступил с инициативой криминализировать в Уголовном кодексе Российской Федерации нормы, содержащие ответственность за кражу SIM-карт, фишинг и социальную инженерию.

Министерство внутренних дел Российской Федерации, напротив, считает нецелесообразным перегружать уголовный закон РФ новыми статьями, и с ним солидарно адвокатское сообщество, так как нормы, содержащиеся в действующем УК РФ, в полной мере охватывают такие социальные явления, как фишинг, кражу SIM-карт и социальную инженерию (ст. 158 УК РФ «Кража», ст. 159 УК РФ «Мошенничество», ст. 159.3 УК РФ «Мошенничество с использованием электронных средств платежа» и ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации»)[4].

Традиционно в криминалистике под способом совершения преступления понимают «систему действий по подготовке, совершению и сокрытию общественно опасного деяния, детерминированных условиями внешней среды и свойствами личности, которые могут быть связаны с использованием соответствующих орудий, средств, условий места и времени» [1, с. 16-17].

Необходимо пояснить, что преступлениям, совершаемым в сфере компьютерной информации способом «социальная инженерия», свойственна трехзвенная структура совершения преступления. Такие преступления тщательно готовятся (собирается информация, подготавливается программное обеспечение, подыскиваются соучастники и т.д.), в момент подготовки также продумываются способы сокрытия преступления.

Рассмотрим наиболее распространенные способы (техники) социальной инженерии, используемые киберпреступниками.

1. Фишинг (электронной почты, текстовых сообщений, «подводная охота»). Является наиболее популярным способом социальной инженерии.

Целенаправленные фишинговые атаки являются главной угрозой информационной безопасности, так считают 56% лиц, работающих в сфере IT[5].

Компания «Purplesec» проанализировала мнения респондентов всего мира по поводу фишинговых атак и пришла к выводу, что в

3 Официальный сайт ежедневной деловой газеты РБК. URL: https://www.rbc.ru/technology_and_media/17/04/2020/5e988cc29a7947ff6c7b4e6eПРО СБЕРБАНК (дата обращения: 18.08.2020).

4 Официальный сайт ежедневной деловой газеты РБК. URL: https://www.rbc.ru/technology_and_media/19/05/2020/5ec2e5259a7947b2c1755c59?utm_source=amp_full-link (дата обращения 18.08.2020).

5 Purplesec. URL : https://purplesec.us/resources/cyber-security-statistics/ (дата обращения: 24.08.2020).

2017 г. 76% опрошенных были подвержены фишинговым атакам, а в 2018 г. – 83%. Наиболее распространенные типы вредоносных вложений: офис – 38%, архив – 37%, PDF-файлы – 14%, исполняемые файлы – 4%[6].

Задачей *фишинга электронной почты* является отправка большому количеству человек спам-сообщений на адрес электронной почты так, чтобы сообщение выглядело, как будто оно было отправлено компанией или организацией, которой человек доверяет. Подобные электронные письма легко создавать в настоящее время, используя готовые фишинговые наборы, которые содержат предварительно разработанные шаблоны электронных почт, известных компаний. В спам-письме содержится ссылка на фишинговый сайт, предназначенный для сбора имен пользователей и паролей.

Согласно данным компании Symantec, которая занимается разработкой программного обеспечения в области информационной безопасности и защиты информации, 55% всех электронных писем являются спамом[7]. Многим пользователям удается обнаружить спам, но из-за большого потока писем ослабляется способность обнаруживать более тонкие уловки киберпреступников, встроенные в сообщения.

Пользователями открываются около 30% фишинговых сообщений, а 12% этих пользователей все же кликают на вредоносные вложения или ссылки. 66% вредоносных программ устанавливаются через вредоносные вложения электронной почты[8].

Фишинг текстовых сообщений SMS – это тип фишинга, который распространяют на планшет, смартфон или смарт-часы. Потерпевшие обычно получают текстовое сообщение от неизвестного отправителя, информирующее их о каком-либо специальном предложении, конкурсе, в котором они выиграли. Текст содержит ссылку на поддельный сайт, предназначенный для сбора учетных данных для входа.

Например, в 2003 г. была осуществлена фишинговая атака, большое количество пользователей получили сообщения от компании eBay, в которых говорилось, что их учетная запись будет заблокирована, если они не перейдут по ссылке для обновления информации о банковской карте.

«Подводная охота» – это фишинговая атака, нацеленная на одного человека или небольшую группу людей, в отличие от типичного фишинга, который преднамеренно универсален и в котором электронные письма рассылаются большому количеству пользователей в случайном порядке. В случае с «подводной охотой» киберпреступники заранее ищут учетные записи конкретных пользователей в социальных сетях и используют информацию, полученную из фотографий, статуса, семейного положения, дат рождения, мест проживания, работы и любой другой общедоступной информации, в своих преступных целях.

2. Не менее популярный способ социальной инженерии – **претекстинг**. Это заранее грамотно написанный сценарий действий преступника, результатом которого является в 80% случаев полученная от потерпевшего информация, необходимая киберпреступнику. Данный способ осуществим при помощи телефонного звонка.

3. «Троянский конь» – вид вредоносной программы. Компьютерные трояны содержат в себе разрушительную нагрузку. Вложения электронной почты, содержащие скрытые вредоносные программы, являются формой трояна. Хитрость социальной инженерии заключается в том, что электронная почта, с которой отправляется вредоносный файл, исходит от надежного отправителя (коллега, друг, член семьи или компании, с которой вы ведете бизнес).

4. Вымогатель – это тип вредоносного программного обеспечения, которое удерживает ваши файлы (зашифровывает их) с целью выкупа их у киберпреступников. Людям, которые хотят вернуть (расшифровать) свои

6 Purplesec. URL : https://purplesec.us/resources/cyber-security-statistics/ (дата обращения: 24.08.2020).

7 ISTR. URL: https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf (дата обращения: 24.08.2020).

8 Там же.

ценные данные, преступники предлагают их выкупить.

5. Кви про кво (услуга за услугу). Киберпреступник под видом сотрудника технической поддержки информирует потерпевшего по телефону, что необходимо провести профилактические мероприятия на персональном компьютере или спрашивает у потерпевшего, есть ли какие-либо проблемы с компьютером. Затем преступник решает технические проблемы (или делает вид), а затем предлагает неопытному пользователю установить программу, которая будет передавать ему данные с этого компьютера для осуществления его преступных целей.

6. Вишинг (голосовая запись). Данный способ осуществляется путем телефонного звонка, с помощью которого, например, у клиентов банков выведывается конфиденциальная информация. Главной особенностью данного способа является заранее подготовленные голосовые сообщения от якобы специалистов данной компании (например, Сбербанка).

7. «Дорожное яблоко» – это метод, в основе которого лежат признаки «Троянского коня». Различие лишь в том, что данный метод подразумевает применение физических носителей (внешние накопители информации, подделываемые киберпреступником под официальные), которые преступники намеренно оставляют в местах общего пользования так, чтобы они могли быть быстро обнаружены заинтересованными лицами. Как только лицо, обнаружившее накопитель, подключит его к компьютеру, произойдет передача информации киберпреступнику.

8. Обратная социальная инженерия. Киберпреступниками создается такая ситуация, когда лицо само обращается к нему для решения каких-либо вопросов и сообщает ему свои персональные или иные данные.

Приведенный перечень содержит наиболее популярные техники (методы) социальной инженерии, используемые киберпреступниками в настоящее время, но с учетом быстрого развития информационных технологий он не является исчерпывающим.

Одной из главных задач сегодня является обучение пользователей выявлению атак на начальном уровне. Обнаружение подозрительных ключевых слов в сообщениях, электронных письмах и телефонных разговорах поможет в блокировке потенциальной атаки.

Для информирования граждан о методах социальной инженерии можно воспользоваться социальной рекламой, размещенной в общественном транспорте, на улицах в виде баннеров, на экранах телевизоров и т.д.

Считаем, что необходимо законодательно закрепить категории, рассматриваемые в данной статье. Образовательным организациям высшего и среднего профессионального образования ввести в курс «Криминалистика» информацию о техниках социальной инженерии, а также противодействия им.

Библиографический список

1. Зуйков, Г.Г. Криминалистическое учение о способе совершения преступления : автореф. дис. … д-ра юрид. наук / Г.Г. Зуйков – М., 1970. – 31 с.

2. Кузнецов, М.В. Социальная инженерия и социальные хакеры / М.В. Кузнецов, И.В. Симдянов. – СПб.: БХВ-Петербург. – 2007. – 368 с.

3. Митник, К.Д. Искусство обмана / К.Д. Митник, В.Л. Саймон // Компания АйТи. – 2004. – 360 с.

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

5. Созаев, С.С. Социальная инженерия, ее техники и методы ее противодействия / С.С. Созаев, Д.А. Кунашев // Вестник науки : международный журнал. – 2020. – № 2(23). – Т. 1. – С. 85-88.

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

7. Суворова, В.В. Совершение преступлений с использованием социальной инженерии: постановка проблемы / В.В. Суворова, Л.А. Суворова // Теория и практика приоритетных научных исследований : сборник научных трудов по материалам VIII Международной научно-практической конференции. – Изд. МНИЦ «Наукосфера», 2019. – С. 71-74.