3. *Соловьянова И. П.*, *Наймушин М. П.* Теория волновых процессов. Электромагнитные волны : учеб. пособие. Екатеринбург : ГОУ ВПО УГТУ–УПИ, 2005. 131 с.

4. SIM7100 GPS Application Note/ Shanghai SIMCom Wireless Solutions Ltd., 2015. 13 с.

5. SIM7100 Series Hardware Design V1.09 / Shanghai SIMCom Wireless Solutions Ltd., 2017. 66 с.

УДК 004.056.53

И. А. Бойко, К. Л. Стойчин
Научный руководитель: д-р тех. наук, проф. С. В. Поршнев
Уральский федеральный университет, Екатеринбург

ПРОБЛЕМА СОВРЕМЕННЫХ МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Аннотация. В настоящей статье рассмотрены проблемы современных методов социальной инженерии. Данное исследование имеет цель рассмотреть методику работы людей, владеющих навыками социальной инженерии. Результатами данной работы являются рекомендации, помогающие предотвратить утечку информации людям, владеющими навыками социальной инженерии.

Ключевые слова: социальная инженерия; VPN; схема; лицо; владеющее методами социальной инженерии.

В современном мире большую ценность имеет такой ресурс, как информация. Она имеет ценность для человека или предприятия, которые владеют ею. Несложно догадаться, что в случае утечки ценной информации владельцу будет нанесен ущерб, который в большинстве случаев принесет материальные убытки, а также изменит нормальный ритм работы персонала. Для сохранности ценной информации в тайне разрабатываются различные программные и аппаратные средства защиты информации, позволяющие минимизировать шансы ее утечки с системы электронно-вычислительных устройств. Но как бы надежно ни была защищена система, главной уязвимостью в утечке защищенной информации является человек. Он является слабым звеном в системе защиты информации. При правильном подходе злоумышленника посвященный человек способен выдать ему всю защищенную информацию, которую он потребует. Такой подход к получению защищенной информации имеет название

«социальная инженерия». В данной статье рассматриваются виды социальной инженерии, а также современные методы ее реализации [1].

В самом начале стоит разобраться, что такое социальная инженерия и дать определение этому понятию. Социальная инженерия — метод доступа к защищенной информации без использования технических средств. Ключевой фразой в данном определении является «отсутствие технических средств», то есть получение информации происходит с помощью человека, который имеет доступ к ней. Для этого используются методы воздействия на человеческую психику, позволяющие заслужить у него доверие, а затем использовать его для своих нужд. Помимо доверия, также можно использовать такие качества человека, как жалость, желание помочь, невнимательность, а также незнание механизмов работы различных систем. Все эти факторы в руках социального инженера позволяют производить манипуляцию над человеком и добыть с его помощью нужную информацию таким образом, что этого даже не заподозрит. На данный момент в большинстве случаев социальную инженерию используют для получения материальных ценностей [2].

В современном обществе почти каждый пользуется Интернетом, поэтому большинство лиц, использующих методы социальной инженерии, работают именно там. Для себя они создают такие условия анонимности, что в случае их розыска обнаружение почти невозможно. Для этого лица, использующие социальную инженерию, работают с виртуальными приватными сетями (VPN), анонимным браузером Tor, а также операционными системами, созданными для анонимности, устанавливаемыми на виртуальные машины. Настройка рабочего места лица, использующего социальную инженерию, выглядит следующим образом:

1. С помощью загрузочного устройства запускается операционная система для анонимности пользователя (к примеру Tails OS).

2. Происходит подключение к VPN (в большинстве своем покупаются платные доступы к заграничным сетям тех стран, которые ставят конфиденциальность пользователя на первое место, тем самым вероятность разглашения правоохранительным органам подключенного истинного IP-адреса минимизируется).

3. Из VPN происходит подключение к серверам Tor Browser. Tor Browser осуществляет подключение к трем серверам разных стран, причем каждый сервер имеет иерархию, построенную таким образом, что с сервера нижнего уровня нельзя выйти на сервер вышестоящего уровня. Таким подходом достигается усиление анонимности в большое число раз.

4. После подключений к серверам Tor производится подключение к другой VPN, находящейся в другой стране.

Таким образом, рабочее место лица, использующего социальную инженерию, готово. Стоит учесть, что весь трафик, который циркулирует в данной цепочке, является зашифрованным, что усиливает анонимность пользователя.

В настоящее время лица, использующие социальную инженерию, работают по так называемым схемам. Схема — описанный алгоритм, в котором содержатся аспекты, позволяющие найти и осуществить обман жертвы. Схемы бывают публичными (содержатся в открытом доступе), а также приватные (продаются создателями за деньги). Выделяется три типа схем:

1. Белая схема.
2. Серая схема.
3. Черная схема.

Необходимо рассмотреть каждый вид схемы подробнее.

Белая схема. Характеризуется простотой своих действий. Анонимность для реализации не требуется. Как правило, для выполнения белой схемы достаточно убедить жертву, что ваши действия принесут ему пользу.

Рассмотрим пример белой схемы. Требуется распространить вирус удаленного доступа к компьютеру жертвы. Для этого люди, использующие методы социальной инженерии, ищут людей, которые используют компьютеры на уровне простого пользователя и не смогут понять, что скачанный файл нужного им разрешения является исполняемым файлом. К примеру, берутся пользователи Photoshop, которые ежедневно скачивают дополнительный контент для обработки фотографий. Лицо, использующее социальную инженерию, ищет группы в социальной сети «ВКонтакте», где выкладываются такие дополнения, а затем выкладывает туда файл, созданный с помощью специального софта, разрешение которого соответствует файлу Photoshop, а на деле это исполняемый *.exe файл (чаще всего с использованием криптографии, чтобы антивирусы не воспринимали его как вирус). Успехом в количестве скачиваний является правильно написанное и увлекательное описание. Тем самым используются навыки социальной инженерии. После установки дополнения лицо, использующее навыки социальной инженерии, имеет доступ к компьютеру жертвы и использует его для своих нужд. Материального ущерба в данном случае для жертвы нет [3].

Серая схема. Требуется незначительная анонимность (достаточно VPN). Отличием серой схемы от черной является ущерб жертве в размере до 2 500 рублей. Как правило, в данной схеме жертва не понимает, что ее обманули, поэтому наказания ждать не стоит.

Рассмотрим пример данной схемы. Создается группа в социальной сети «ВКонтакте», в которой выкладываются фотографии одежды и прейскурант цен на нее гораздо ниже, чем на такую же, но оригинальную. Лицо, использующее методы социальной инженерии, рекламирует группу таким образом,

чтобы люди ему доверяли и производили оплату. Для этого создаются поддельные скриншоты довольных покупателей и покупается реклама данного магазина в других группах. После набора аудитории лицо, использующее методы социальной инженерии, производит продажи несуществующего товара, убеждая покупателей, что их заказ отправлен и прибудет через определенное количество дней. После того, как наберется достаточная сумма денег, которую требовалось собрать, лицо, использующее методы социальной инженерии, перестает отвечать на сообщения и всячески забывает об этой группе. Деньги получены, пользователи ждут и не понимают, что они обмануты [4].

Черная схема. Требуется полная анонимность. Фигурируют большие суммы денег. Будут написаны заявления в органы, будет производиться розыск лица, использующего методы социальной инженерии.

Рассмотрим пример черной схемы. В данном случае будет представлена тема с «безвозвратными» кредитами. Человек очень любит получить деньги, ничего для этого не предпринимая, поэтому найти жертву не составляет проблем. Лицо, использующее методы социальной инженерии, найдя жертву, представляется сотрудником банка и предлагает взять «безвозвратный» кредит, убеждая, что после взятия кредита он удалит его данные из базы и возвращать ничего не придется. При этом лицо, использующее методы социальной инженерии, возьмет себе плату в размере 50 % от суммы. Жертва соглашается деньгам и присылает все нужные сканированные данные для оформления кредита лицу, использующему методы социальной инженерии. Он с помощью кредитных организации в Интернете оформляет кредитную карту на сумму, к примеру 300 000 рублей, при этом используя свою поддельную сим-карту для ее регистрации. Карта с взятым кредитом приходит к жертве домой курьером, производится обращение к лицу, использующему методы социальной инженерии. Он убеждает, что нужно передать ему все данные о карте, иначе карту из базы удалить невозможно. Жертва передает все данные о карте, лицо, использующее методы социальной инженерии, обналичивает деньги через различные криптовалюты, виртуальные деньги и скрывается. В итоге жертва долгое время выплачивает кредит, а лицо, использующее методы социальной инженерии, получает большую сумму денег [5].

Подводя итог, стоит сказать, что схем работы лиц, использующих методы социальной инженерии, огромное количество, и давать гарантии за чью-либо безопасность невозможно. Стоит быть бдительным, не пытаться получить деньги просто так, не устанавливать стороннего ПО. Всех поставленных целей стоит добиваться только своим трудом. Ведь, легко получив деньги, в итоге может оказаться так, что необходимо будет отдать в разы превосходящую полученную сумму, либо ваш компьютер будет выполнять незаконные действия в пользу лица, использующего методы социальной инженерии.

Список литературы

1. Защита информации в Интернете. URL: https://camafon.ru/informatsionnaya-bezopasnost/zashhita-v-internete.
2. *Митник К.* Искусство обмана. М., 2001.
3. Форум социальной инженерии. URL: https://darkwebs.ws/.
4. Форум заработка в сети. URL: http://blackforum.biz/.
5. Форум социальной инженерии. URL: https://lolzteam.net/.

УДК 004.056.2+ 65.011.56

Е. Е. Ерофеева, Е. А. Терентьева, Е. Н. Полякова, Д. И. Дик
Научный руководитель: канд. пед. наук, доц. Е. Н. Полякова,
канд. тех. наук, доц. Д. И. Дик
Курганский государственный университет, Курган

ПРЕДОСТАВЛЕНИЕ УСЛУГ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ПОМОЩЬЮ ОНЛАЙН-СЕРВИСА

Аннотация. В данной статье показан разработанный онлайн-сервиса SofI, с помощью которого можно автоматизировать процесс построения системы защиты информации в организации. Перечислены качественные показатели работы онлайн-сервиса: снижение вероятности возникновения случайных ошибок и неоптимального выбора средств защиты информации при построении системы защиты, снижение финансовых затрат в информационных системах и др. Данный сервис предназначен для обладателя информации, специалистов по защите информации, преподавателей и обучающихся средних и высших учебных заведений.

Ключевые слова: защита информации; информационная система; класс защищенности; уровень защищенности; персональные данные.

Термин «национальная безопасность» впервые был использован в 1995 году в Федеральном законе «Об информации, информатизации и защите информации». В Послании по национальной безопасности Президента Российской Федерации Федеральному Собранию от 13 июня 1996 года понятие «национальная безопасность» получило следующее определение: «…национальная безопасность понимается как состояние защищенности национальных интересов от внутренних и внешних угроз, обеспечивающее прогрессивное развитие личности, общества и государства» [1].

Национальная безопасность России напрямую зависит от степени защищенности государственных информационных систем (далее ГИС), так как