Семинарское занятие 2/4

# «Социальная инженерия как способ совершения компьютерного преступления»

## Вопрос 1. Социальная инженерия

**Социальная инженерия (СИ) –**

это группа методов управления действиями человека с учетом психологических основ поведения человека в обществе и принятия им решений. В частности, может быть использована для получения от человека какой-либо информации, для того, чтобы побудить выполнить какие-либо действия

Примеры ниже – из сообщений телефона

- **«Для получения пароля ответьте на это смс с текстом...»**
- **«Ваш номер телефона выиграл ... для получения выигрыша …»**
- **«Привет, это Лена, брось мне на этот новый телефон рублей двести»**

Каждый раз у пришедшего сообщения небольшие шансы на ответ. Но массовость рассылки умножает эти шансы на вполне ощутимую величину, давая вполне ощутимый средний выигрыш.

В первых двух случаях человек будет ожидать что-либо получить.

В третьем случае тон сообщения может заставить поверить, что сообщение от знакомого тебе человека, если у тебя среди знакомых есть с таким именем.

Сообщение, пришедшее с известного адреса, тоже не вызывает сомнений. Поэтому люди в социальных компьютерных сетях часто доверчиво реагируют на сообщения от друзей типа: **«Смотри, какой я нашел классный сайт...»** и щелкают по ссылке на этот сайт.

Наиболее вероятно, что страничка этого друга была скомпрометирована, его пароль стал известен злоумышленнику, который, используя программу-робота рассылает друзьям жертвы то, что ему надо.

## Телефон

Самое простое средство СИ – телефон. Опытные социальные инженеры действуют экспромтом, полагаясь на свое чутье. По наводящим вопросам, по интонации голоса они могут определить комплексы и страхи человека и, мгновенно сориентировавшись, сыграть на них. К каждому подбирается свой ключ, воздействуя на его эмоции и чувства, которые могут быть разными:

1. в общении человек может испытывать неловкость, дискомфорт, от которых хочется поскорее избавиться;
2. может, напротив, испытывать желание подольше говорить, например, с молодой собеседницей;
3. почувствовать свою значимость и важность в решении вопросов и оказании помощи.

Приведем несколько примеров явления из Интернета.

***То, что по телефону можно воздействовать на эмоции человека, показывает следующий пример.***

Некоторые в детстве баловались с телефонами, например с такой шуткой:

– Алло, это зоопарк?

– Нет.

– А почему обезьяна у телефона?

***Безобидный пример издевательства над людьми. А вот еще один подобный, тоже детский, но с элементами СИ:***

– Алло! Вас беспокоят с телефонной станции. Измерьте, пожалуйста, длину шнура от трубки к телефону.

– Метр.

– Хорошо, для того, чтобы повеситься, хватит.

Следующий звонок.

– Алло! Это милиция. Вам сейчас хулиганы не звонили?

– Да, да! Звонили! Разберитесь с ними, пожалуйста!

– Про трубку и провод спрашивали?

– Да!

– И он у вас метр?

– Да!

– А почему до сих пор не висим?

***Простейший пример СИ для проникновения в систему.***

Звонок администратору системы.

– Здравствуйте, вы администратор?

– Да.

– Я понимаю, что вы ужасно заняты, извините, что отрываю вас от дел, но я не могу войти в сеть.

– *(Про себя: Поработать не дают!)* А что компьютер говорит по этому поводу?

– Как это – «говорит»?

– *(Ха!)* Ну, что там написано?

– Написано «вронг пассворд».

– *(Ну-ну, еще бы...)* А-а-а-а... А вы пароль правильно набираете?

– Не знаю, я его не совсем помню.

– Какое имя пользователя?

– Anatoly.

– Ладно, ставлю вам пароль... мммм... *art*25. Запомнили? *(Если опять не войдет – убью!)*

– Постараюсь... Спасибо. *(Вот дурак-то!)*

Конец разговора. Все!

***С первоначальными нулевыми знаниями. Выбирается цель по телефонной книге – организация, где есть телефон секретаря.***

- Звоним секретарю и узнаем имя персоны, с которой можно проконсультироваться по поводу некоторых проблем с работой системы.
- Звоним любому другому человеку, чей номер телефона имеется в книге, предполагая, что он имеет доступ к системе.
- Представляемся (вымышленным именем) помощником той персоны, имя которой мы узнали из первого звонка. Говорим, что в связи с перестановкой системы администратор дал задание поменять пароли всем пользователям.
- Узнаем имя входа, прежний пароль, говорим новый пароль. Все!
- В этом примере есть большая вероятность получения доступа в систему вследствие оперирования в разговоре конкретными именами и должностями. Их возможно получить в различных справочниках, из рекламы, из мусора, который выбрасывается организацией.
- Иногда получение доступа к системе в виде простого пользователя бывает для целей злоумышленника недостаточным. Однако, используя те же методы СИ можно получить более полные права.

***Получения привилегий администратора в Unix-системе.***

Звонок администратору.

– Здравствуйте, вы администратор?

– Да.

– Извините, что отвлекаю. Не могли бы вы мне помочь?

– (Ну что еще ему надо?) Да, конечно.

– Я не могу в своем каталоге выполнить команду *ls* (аналог команды *dir Windows*).

– (Как будто ему это надо!) В каком каталоге?

– /home/Anatoly.

– (Вот ведь глупый юзер!) Сейчас посмотрю. (Заходит в этот каталог и набирает команду *ls*, которая успешно выполняется и показывает наличие нормальных прав на каталог).

– Все у вас должно работать!

– Хм... Подождите... О! А теперь работает... Странно...

– *(Рррррр!!!)* Да? Хорошо!

– Спасибо огромное. Еще раз извиняюсь, что помешал.

– (Ну, наконец!) Да не за что. До свидания.

***Пример сбора информации о жертвах.***

Звонок на совершенно незнакомый номер.

– Алло, извините, вас беспокоят с телефонной станции. Это номер такой-то?

– Да.

– У нас идет перерегистрация абонентов, не могли бы вы сообщить, на кого у вас зарегистрирован телефон? Имя, фамилию и отчество, пожалуйста.

– (Сообщает информацию).

– Спасибо! Так... секундочку... Хорошо, ничего не изменилось. А место работы?

– (С некоторым сомнением называет, а если человек очень подозрительный, то спрашивает, зачем).

– Это сведения для новой телефонной книги. По вашему желанию можем внести не одно имя, а всех, кого можно найти по этому телефону.

– (Тут с радостью называются имена всех членов семьи с их положением в ней, хотя это и не требовалось).

Информации уже достаточно для попытки взлома. Таким же образом становятся известными номера паспортов и т.д. После такого разговора можно звонить сотрудникам хозяина телефона от имени его родственников и получать дальнейшую информацию.

***Звонок от имени администратора.***

– Алло, это приемная?

– Да.

– Это администрация сети. Мы сейчас меняли сетевую систему защиты. Необходимо проверить, все ли у вас нормально работает. Как вы обычно регистрируетесь в системе?

– Ввожу свои имя и пароль.

– Хорошо... Так... (Пауза) Какое имя?

– *Anna*.

– *Anna*... (Пауза) Так... какой у вас раньше был пароль?

– *aa*62.

– Та-а-а-ак... Хорошо. Попробуйте сейчас перерегистрироваться.

– *(Пауза)* Все нормально. Работает.

– Отлично. Спасибо!

**В маленьких организациях, где все знают администратора, это не сработает, зато в больших есть все шансы.**

**Электронная почта**

Использование СИ с помощью электронной почты имеет некоторые особенности:

- письма должны иметь соответствующий вид;
- подпись в конце письма – стандартная для организации: имя, фамилия, должность, название организации, адрес и телефон;
- письмо не посылается напрямую, а использует поддельный адрес и/или скрывает *IP*-адрес отправителя.

В любом электронном письме существует заголовок, содержащий служебную информацию, такую как дата и время отправки, *IP*-адрес машины, с которой отправили письмо, название отправляющей программы, адрес отправителя и т.д.

Эту информацию обычно можно просмотреть либо в почтовой программе, либо с помощью любого текстового редактора.

Что здесь может заинтересовать получателя письма?

Прежде всего, это поля

«*From:*» (От) «*To:*» (Кому), «*Received*:», где содержится информация о маршруте, который прошло письмо.

Как правило, последнее поле «*Received*:» показывает адрес машины, с которой это сообщение было отправлено.

В самом простом случае будет написан *IP*-адрес.

Существует несколько способов сделать так, чтобы эти поля не записывались, или чтобы туда записалась ложная информация.

***Во-первых,*** можно использовать распространенные в Интернете программы, позволяющие заполнить поля *From*, *To* и *Host* – адрес сервера, через который будет отправлена почта.

- ***Во-вторых,*** можно перенастроить почтовую программу (*Outlook Express*, *The Bat*) на другое имя отправителя и другой адрес почтового сервера или создать для этого отдельную учетную запись.

- В-третьих, можно использовать серверы, переправляющие почту, но стирающие всю информацию о пути прохождения сообщения, – так называемые *remailers*.

Мало того, что вы подмените адрес, в некоторых случаях придется поменять и имя программы-отправителя

«*X-Mailer*:».

***Например***, получатель знает, что его друг питает отвращение к *Outlook Express*, а тут вдруг пользуется им. **Ошибка! Источник ссылки не найден.** содержит пример отправки письма через Web-интерфейс сервера *mail.ru*.

Возможно, придется изменить даже ***дату отсылки сообщения.***

Если отправитель находится в противоположной точке земного шара и разница во времени составляет 12 часов (дата отправки обычно показывается всеми почтовыми программами), то отправление письма в 5 утра может насторожить получателя. Вопрос с датами в любом случае нужно рассмотреть подробнее, так как некоторые серверы ее изменяют, некоторые пишут ее относительно *GMT* и т. д.

Добавим только, что обычно проверкой подлинности письма никто не занимается, да и осуществить такую процедуру сможет далеко не каждый. Поэтому при «работе» с обыкновенными пользователями об этом, как правило, не задумываются, но иногда все же стоит перестраховаться.

**С электронной почтой связаны несколько специальных методов.**

***Фишинг*** – метод, направленный на получение конфиденциальной информации.

Обычно злоумышленник посылает цели *e-mail*, подделанный под официальное письмо – от банка или платёжной системы – требующее «проверки» определённой информации, или совершения определённых действий.

Это письмо обычно содержит ссылку на фальшивую веб-страницу, имитирующую официальную, с корпоративным логотипом и содержимым, и содержащую форму, требующую ввести конфиденциальную информацию – от домашнего адреса до *PIN*-кода банковской карты.

***Троянский конь*** – метод, который эксплуатирует любопытство, либо алчность цели.

Злоумышленник отправляет *e-mail*, содержащий во вложении «красивые обои», «хранитель экрана», «обновление антивируса» и т.д. Такой метод остаётся эффективным, пока пользователи будут слепо кликать по любым вложениям.

**Атака с помощью носителей информации**

Существует метод атаки, который представляет собой адаптацию троянского коня, и состоит в использовании физических носителей.

Злоумышленник может подбросить инфицированные CD или флешку, в месте, где носитель может быть легко найден. Носитель подделывается под официальный, и сопровождается подписью, призванной вызвать любопытство.

**Обратная социальная инженерия**

Целью обратной социальной инженерии является заставить жертву саму обратиться к злоумышленнику за «помощью». С этой целью применяют следующие два метода:

- ***Диверсия***: создание обратимой неполадки на компьютере жертвы.
- ***Реклама***: злоумышленник подсовывает жертве объявления вида «При неполадках с компьютером, звоните по такому-то номеру».

То, что специалиста вызвали сами, не дает оснований предполагать у него какой-либо интерес к системе безопасности или злой умысел.

**Вопрос 2.**

**Защита от социальной инженерии**

Основные рекомендации для усиления безопасности компьютерных систем организации.

1. Привлекайте внимание людей к вопросам безопасности. Сотрудники должны осознавать серьезность проблемы и причины принятия политики безопасности организации.
2. Требуйте от сотрудников проверять личность и делать встречные звонки любому, кто просит сообщить персональную или конфиденциальную информацию.
3. Реализуйте программу обучения пользователей в области безопасности. Хорошая программа обучения пользователей может быть реализована с минимальными затратами и сохранить организации миллионы.
4. Назначьте ответственных за техническую поддержку. Каждый сотрудник организации обязан лично познакомиться с ответственным за техническую поддержку и обращаться исключительно к нему.

5. Создайте систему оповещения об угрозах. Атакующие знают, что, даже если их обнаружат, у служащего нет возможности предупредить других сотрудников об атаках. В результате атака может быть продолжена с минимальными изменениями и после компрометации. По существу, компрометация только улучшит атаку, так как атакующие узнают, что именно не срабатывает.
6. Создайте различные варианты политики безопасности, определите правила корректного использования телефонов, компьютеров и т.д.
7. Социальная инженерия является единственным подходящим методом проверки эффективности политики безопасности. Хотя многие тесты проверяют физические и электронные уязвимые места, но лишь некоторые анализы безопасности исследуют бреши, создаваемые людьми.

***Тестирование системы защиты*** – это метод выявления недостатков безопасности с точки зрения постороннего человека (взломщика). Он позволяет протестировать схему действий, которая раскрывает и предотвращает внутренние и внешние попытки проникновения и сообщает о них. Используя этот метод, можно обнаружить даже те недостатки защиты, которые не были учтены в самом начале при разработке политики безопасности.

***Тест должен разрешить два основных вопроса:***

- все ли пункты политики безопасности достигают своих целей и используются так, как это было задумано;
- существует ли что-либо, не отраженное в политике безопасности, что может быть использовано для осуществления целей злоумышленника.

Необходимо свести к минимуму количество людей, знающих о проведении эксперимента. При тестировании могут быть затронуты деликатные вопросы частной жизни сотрудников и безопасности организации, поэтому желательно получить предварительное разрешение на проведение такой акции. Непосредственное начальство обязательно должно быть в курсе происходящего.

Профессионалам в области безопасности при проведении теста необходимо иметь такое же положение, как и у потенциального злоумышленника:

в их распоряжении должны быть время, терпение и максимальное количество технических средств, которые могут быть использованы взломщиком.

Более того, проверяющим следует расценить это как вызов своему профессионализму, а значит, проявить столько же рвения, сколько и взломщик, иначе тесты могут не достичь необходимого результата.

Таким образом, мы рассмотрели основные вопросы информационной безопасности, которыми должен владеть руководитель подразделения, отдела, учреждения и т. п. для постановки задачи защиты информации

Успехи хакеров настолько велики, что, например, США намерены использовать их в информационной войне.

С момента официального признания в 1993 году военно-политическим руководством США «информационной войны» в качестве одной из составляющих национальной военной стратегии, ускоренными темпами идут поиски методов, форм и средств ее ведения.

Так, в последние годы все чаще говорят о целесообразности привлечения хакеров на различных стадиях «информационной войны».

Спецслужбы США и некоторых европейских стран уже прибегают к услугам этой категории компьютерщиков.

**Контрольные вопросы**

1. Сформулируйте понятие социальной инженерии.
2. Назовите средства социальной инженерии.
3. Сформулируйте отличие социальной инженерии от обратной социальной инженерии.
4. Рассмотрите систему мер защиты от социальной инженерии.

**Литература**

***Основная:***

1. Аполлонский А. В., Домбровская Л. А., Примакин А. И., Смирнова О. Г., Основы информационной безопасности в ОВД: Учебник для вузов. – СПб.: Университет МВД РФ, 2010.
2. Лопатин В. Н. Информационная безопасность России: Человек. Общество. Государство. Фонд «Университет». СПб 2000.

***Дополнительная***:

1. Васильев А.И., Сальников В.П., Степашин С.В. Национальная безопасность России: конституционное обеспечение. Фонд «Университет». СПб 1999.
2. Исмагилов Р.Ф., Сальников В.П., Степашин С.В. Экономическая безопасность России: концепция – правовые основы – политика. Фонд «Университет». СПб 2001.
3. Доценко С.М., Примакин А.И. Информационная безопасность и применение информационных технологий в борьбе с преступностью: Учебник для вузов. – СПб.: Университет МВД РФ, 2004.