Обеспечение информационной безопасности при работе на персональном компьютере и в вычислительных сетях

Обеспечение информационной безопасности информационной системы:

- информационная безопасность на программно-техническом уровне
- информационная безопасность на социально-бытовом и личностном уровне (социальная инженерия)

Информационная безопасность на программно-техническом уровне:

Средства защиты:

- аппаратные (генераторы шума)
- программные (идентификация пользователей)
- аппаратно-программные (secretdisk)

Нормативно-методическая база по их применению

Информационная безопасность на социально-бытовом и личностном уровне:

Самое слабое звено в автоматизированной информационной системе – человек (оператор, пользователь)

Информационная безопасность на социально-бытовом и личностном уровне:

- Деятельность человека не подчинена логике выполнений итераций вычислительного процесса

- Сторонние факторы
- Человеческие слабости

Социальная инженерия –
средства несанкционированного доступа
к информационным ресурсам,
основанные на особенностях психологии
человека

Методы социальной инженерии:

- Метод прямого воздействия
- Введение в заблуждение
- Метод обратной инженерии
- Претекстинг
- Сбор и анализ информации из открытых источников

Метод прямого воздействия:

В основе – желание доверять коллегам и оказывать при необходимости помощь

Следует свободно ориентироваться в терминологии и проблемах, связанных с деятельностью организации

В момент постановки вопроса социальный инженер вводит «атакуемого» сотрудника в режим экстренного принятия решения

Метод введения в заблуждение (фишинг):

В основе – доверие человека используемым на протяжении определенного интервала времени предметам, ресурсам

Социальный инженер создает в сети «Интернет» информационный ресурс-близнец с привычным для пользователя интерфейсом

Метод введения в заблуждение (фишинг):

Отличие ресурса-близнеца – отсутствие элементов функциональной части информационного ресурса, замена на другие с дополнительными функциями

Компьютер атакуемого может запомнить адрес ресурса в сети «Интернет» и вводимую пользователем информацию

Метод введения в заблуждение (фишинг):

Пример:

Администрация информационного ресурса проводит расследование фактов несанкционированного использования учетных данных пользователя и просит подтвердить введенную информацию

Фишинг – метод социальной инженерии, основанный на незнании пользователями основ безопасности в сети «Интернет»

Метод обратной инженерии:

Метод получения информации злоумышленником, при котором атакуемый самостоятельно предоставляет необходимые сведения

Предварительно следует собрать полную информацию об объекте:

- жизненные позиции
- увлечения
- личная жизнь

Метод обратной инженерии:

Социальный инженер: становится:

болельщиком любимой команды атакуемого

другом семьи

Особенность:

- большие временные затраты
- за этот период ситуация может измениться - информация потеряет актуальность

Претекстинг:

Предполагает общение с атакуемыми по телефону, Скайпу

В результате - получение интересующей информации

Метод сбора и анализа информации из открытых источников:

Социальная сеть – интернет-ресурс, предназначенный для обмена текстовыми сообщениями, медиа-ресурсами

Анализ представленной информации в социальных сетях позволяет составить морально-психологический портрет атакуемого

Метод сбора и анализа информации из открытых источников:

Исходная информация из социальных сетей:

- увлечения
- обычаи
- запланированные мероприятия
- семейное положение

Основы методов социальной инженерии:

- человеческие слабости
- особенности:
  - воспитания
  - мировоззрения
  - миропонимания

Противодействие методам социальной инженерии:

- проведение проверочных мероприятий при приеме сотрудников на работу
- контроль входящей корреспонденции
- проверка наличия служебной информации конфиденциального характера в открытых информационных сетях

Противодействие методам социальной инженерии:

- Регулярное проведение занятий по правилам работы с информацией конфиденциального характера
- Контроль соблюдения технологии обработки информации на технических средствах организации
- Запись и анализ телефонных переговоров сотрудников с использованием служебных средств связи

Противодействие методам социальной инженерии:

- Проведение воспитательной работы с целью повышения мотивации сотрудников
- Проведение периодических проверок профессиональной пригодности сотрудников в части обеспечения информационной безопасности