Дисциплина: «Основы информационной безопасности»

Раздел 3. Методы и средства обеспечения безопасности

§ 7. Злоумышленники

План:

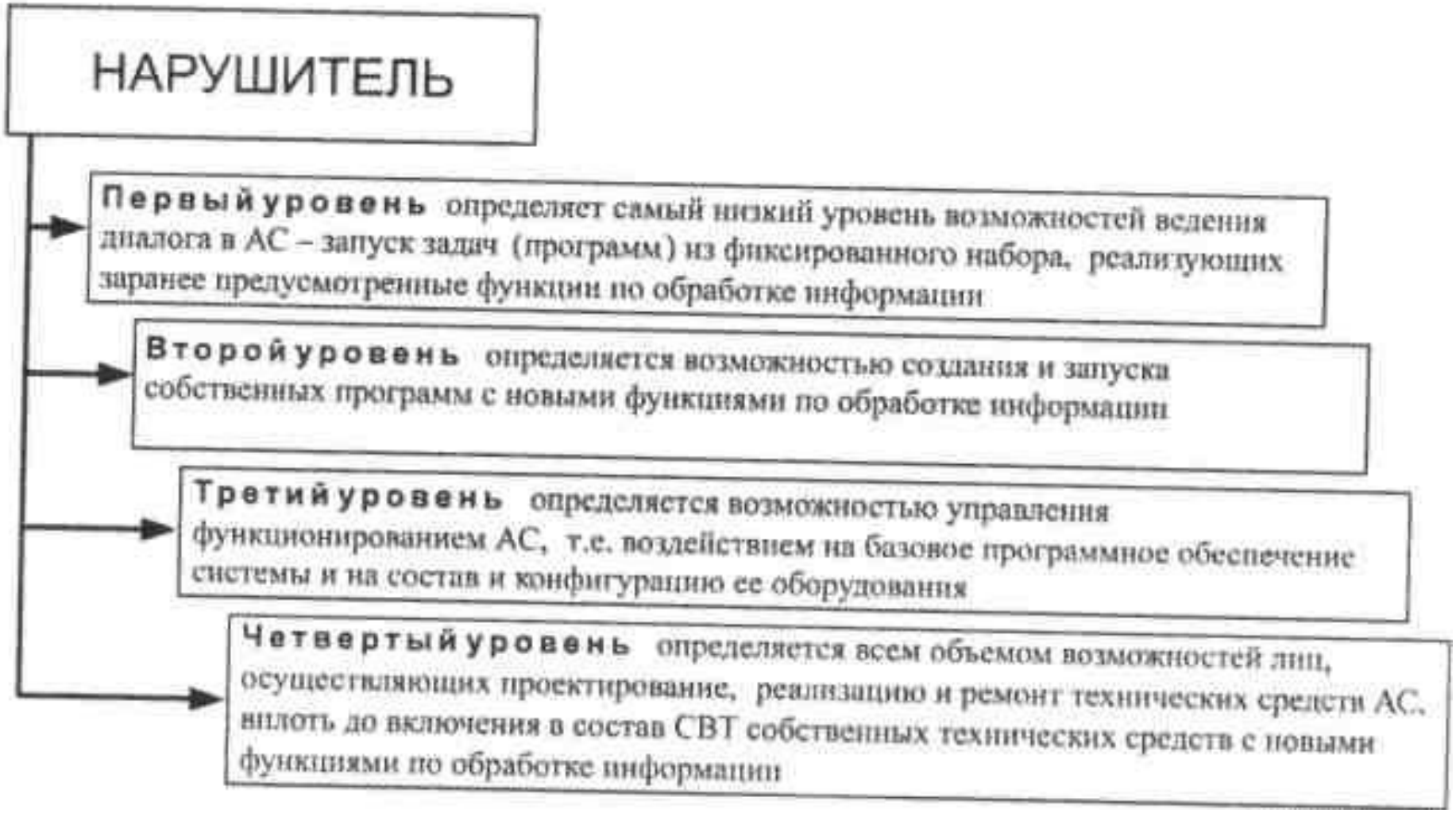
1. Модель нарушителя
2. Категории злоумышленников
3. Классы злоумышленников
4. Степени БИ – Д/З

Модель нарушителя – определяется концепцией ИБ

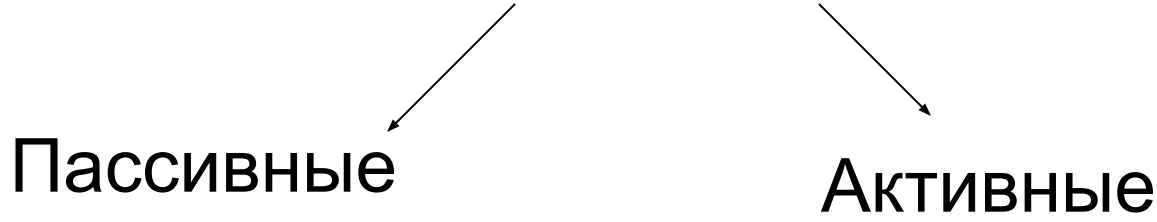
Нарушитель - субъект, имеющий доступ к работе со штатными средствами АС и СВТ, как части АС.

Нарушители классифицируются по уровню возможностей, предоставляемых им штатными средствами АС и СВТ.

Классификация является иерархической, т. е. каждый следующий уровень включает в себя функциональные возможности предыдущего.


НАРУШИТЕЛЬ
Первый уровень определяет самый низкий уровень возможностей ведения диалога в АС – запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации
Второй уровень определяется возможностью создания и запуска собственных программ с новыми функциями по обработке информации
Третий уровень определяется возможностью управления функционированием АС, т.е. воздействием на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования
Четвертый уровень определяется всем объемом возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств АС, вплоть до включения в состав СВТ собственных технических средств с новыми функциями по обработке информации

7.2. Злоумышленники



Категории злоумышленников

- Случайные любопытные пользователи не применяющие серьёзных технических средств.
- Члены организации, занимающиеся комерческим и военным шпионажем.
- Те, кто совершают решительные попытки личного обогащения.
- *Вирусы- не человек, а программа. Действуют не так направленно, как злоумышленник.*

7.3. Классы злоумышленников

Тайный пользователь- лицо, завладевшее управлением в режиме суперпользователя и использующее его, чтобы избежать аудита и преодолеть контроль доступа.

Притворщик- лицо, не обладающее полномочиями по исследованию системы, которое проникает в систему, несмотря на контроль доступа системы и использует учётную запись законного пользователя

Правонарушитель- законный пользователь, получающий доступ к данным, к которым у него нет доступа или есть доступ, но пользователь злоупотребляет своими полномочиями

Причины ведущие к возникновению проблем безопасности по вине людей

- Непонимание что такое безопасность
- Недооценка опасности
- Неумение соблюдать меры безопасности в качестве рабочего навыка
- Люди забывают о безопасности вне рабочей обстановки
- Пассивное участие в мероприятиях по безопасности

Социальная инженерия — это метод несанкционированного доступа к информации или системам хранения информации без использования технических средств.
Метод основан на использовании слабостей человеческого фактора и считается крайне разрушительным, так как злоумышленник получает информацию, например, путем сбора данных о служащих объекта атаки, с помощью обычного телефонного разговора или путем проникновения в организацию под видом ее служащего.

Ключевая особенность - в роли объекта атаки выбирается не машина, а ее оператор.

Процесс получения информации злоумышленниками основан на различных способах психологического воздействия на человека

Основоположник - Кевин Митник.

Будучи всемирно известным компьютерным хакером и консультантом по безопасности, Митник также является автором многочисленных книг по компьютерной безопасности, посвященным, в основном, социальной инженерии и методам психологического воздействия на человека.

В 2002 году выходит книга "The Art of Deception" под его авторством, повествующая о реальных историях применения социальной инженерии.

Домашнее задание:

1. Охарактеризовать возможные злоупотребления, указать средства и методы борьбы с ними:

- Программы открытия паролей
- Программы захвата паролей
- «Люки»
- Логические бомбы
- Репликаторы
- Программные закладки
- Работа между строк
- Анализ трафика
- «Маскарад»

2. Охарактеризовать техники социальной инженерии, приведите примеры:

- Претекстинг
- Фишинг
- Кви про кво
- Троянский конь
- Сбор информации из открытых источников

3. «Теория шести рукопожатий» - это?

Принципы социальной инженерии

Техники социальной инженерии

Претекстинг

- **Претекстинг - это набор действий, проведенный по определенному сценарию и заставляющий цель совершить определенное действие или предоставить определенную информацию.** Данный вид атак применяется в основном по телефону или по переписке. В большинстве случаев данная техника требует каких-либо изначальных данных о цели (например, персональных данных: даты рождения, номера телефона, номеров счетов и др.)

Фишинг

- Ни одна крупная утечка персональных данных уже не обходится без волны фишинговых рассылок, следующих за ней. **Фишинг — техника, направленная на незаконное получение конфиденциальной информации**. Обычно мошенник посылает цели сообщение по электронной почте, подделанное 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, и содержащую форму, требующую ввести конфиденциальную информацию.

Принципы социальной инженерии

Техники социальной инженерии

Кви про кво

- **Кви про кво — вид атаки подразумевает звонок злоумышленника в компанию по корпоративному телефону.** Представляясь сотрудником техподдержки, опрашивающим, есть ли какие-либо технические проблемы, в процессе общения, мошенник "заставляет" цель вводить команды, которые позволяют хакеру запустить вредоносное программное обеспечение.

Троянский конь

- Троянский конь — эта техника зачастую эксплуатирует любопытство, либо другие эмоции цели. Злоумышленник отправляет **электронное сообщение, содержащее "интересный" контент, новый апгрейд антивируса, или другую информацию, способную заинтересовать цель.** Открывая прикрепленный к письму файл, цель устанавливает себе на машину вредоносное программное обеспечение, позволяющее мошеннику получить доступ к конфиденциальной информации.

Принципы социальной инженерии

Техники социальной инженерии

Сбор информации из открытых источников

- Принципиально новым способом **получения различной информации стал её сбор из открытых источников**, и в первую очередь из многочисленных социальных сетей. Люди, не уделяющие должного внимания вопросам безопасности, зачастую оставляют в свободном доступе сведения, которыми могут воспользоваться злоумышленники.

Показательным примером, в этом плане, может служить история с похищением сына Евгения Касперского. В ходе следствия удалось установить, что преступники узнали примерное расписание дня и маршруты следования подростка из его записей на странице в социальной сети.

Принципы социальной инженерии

Известная «теория шести рукопожатий» гласит, что любые два человека на нашей планете, в среднем, разделены лишь небольшой цепочкой из пяти общих знакомых.

Как показывает практика, именно на это и полагаются злоумышленники. Доказано, что если жертва видит, что у человека, подавшего заявку на дружбу, есть с ней общие знакомые, подозрения к нему существенно уменьшаются.

В реальной жизни этот принцип доказал бразильский исследователь по вопросам компьютерной безопасности.

Он показал, что существует возможность стать другом любого пользователя Facebook в течение 24 часов, используя методы социальной инженерии.

В ходе эксперимента исследователь Нельсон Новаес Нето выбрал «жертву» и создал фальшивый аккаунт человека из ее окружения - ее начальника. Сначала Нето отправлял запросы на дружбу друзьям друзей начальника жертвы, а затем и непосредственно его друзьям. Через 7,5 часа исследователь добился добавления в друзья от «жертвы». Тем самым, исследователь получил доступ к личной информации пользователя, которой тот делился только со своими друзьями.