Лекция №3

Виды угроз в информационной системе

Вопросы темы:

1. Основные определения и критерии классификации угроз
2. Виды угроз, возникающие в ИС.
3. Основные задачи защиты.
4. Уровни защиты.

1. Основные определения и критерии классификации угроз

Под **угрозой ИПО** понимается возможность преднамеренного или случайного действия, которое может привести к нарушениям безопасности хранимой и обрабатываемой информации и программ.

Попытка реализации угрозы называется **атакой**, а тот, кто предпринимает такую попытку, - **злоумышленником**.

Чаще всего **угроза** является следствием наличия уязвимых мест в защите информационных систем (таких, например, как возможность доступа посторонних лиц к критически важному оборудованию или ошибки в программном обеспечении).

Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется, называется **окном опасности**, ассоциированным с данным уязвимым местом.

Пока существует **окно опасности**, возможны успешные **атаки** на ИС.

Для большинства уязвимых мест **окно опасности** существует сравнительно долго (несколько дней, иногда - недель), т.к. за это время должны произойти следующие события:

- **должно стать известно о средствах использования пробела в защите;**
- **должны быть выпущены соответствующие заплаты;**
- **заплаты должны быть установлены в защищаемой ИС.**

Угрозы можно классифицировать по нескольким критериям:

- по аспекту информационной безопасности (доступность, целостность, конфиденциальность), против которого угрозы направлены в первую очередь;
- по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);
- по способу осуществления (случайные/преднамеренные действия природного/техногенного характера);
- по расположению источника угроз (внутри/вне рассматриваемой ИС).

2. Виды угроз, возникающие в ИС.

1. Несанкционированное использование ресурсов:
- Использование данных(копирование, модификация, удаление, печать и т.д.)
- копирование и модификация программ
- Исследование программ для последующего вторжения в систему.

2. Некорректное использование ресурсов:
- Случайный доступ прикладных программ к чужим разделам основной памяти
- Случайный доступ к системным областям дисковой памяти
- Некорректное изменение БД (ввод неверных данных, нарушение ссылочной целостности):

- Ошибочные действия пользователей и персонала.

3. Проявление ошибок в программных и аппаратных средствах.
4. Перехват данных в линиях связи и системах передачи.
5. Несанкционированная регистрация электромагнитных излучений.
6. Хищение устройств ВС, носителей информации и документов.
7. Несанкционированное изменение состава компонентов ВС, средств передачи информации или их вывода из строя
8. Несанкционированный доступ к информационным ресурсам.

Угрозы и препятствия, стоящие на пути к достижению ИБ, делятся на две группы:

1. Технические угрозы

- Ошибки в программном обеспечении
- DoS-атаки (Denial of Service – отказ в обслуживании) – вид атак, направленный на выведение сети или сервера из работоспособного состояния.
- Новый тип атак DDoS (Distributed Denial of Service – распределенный DoS) – перегрузка сетевого канала трафиком, которая мешает прохождению полезной информации или полностью блокирует ее.

- Компьютерные вирусы, троянские кони
- Анализаторы протоколов и сниффферы – в данную группу входят средства перехвата передаваемых по сети данных, как аппаратные, так и программные
- Технические средства съема информации – сюда относятся клавиатурные жучки, различные мини-камеры, звукозаписывающие устройства и т.д.

Человеческий фактор

- Уволенные или недовольные сотрудники
- Промышленный шпионаж
- Халатность
- Низкая квалификация.

Возможными последствиями нарушения защиты являются следующие:

1. Получение секретных сведений;
2. Снижение производительности или остановка системы;
3. Невозможность загрузки ОС с жесткого диска;
4. Материальный ущерб;
5. Катастрофические последствия.

3. Основные задачи защиты.

Целью защиты является обеспечение безопасности информации в ВС, которая может быть нарушена (случайно или преднамеренно), поэтому сущность защиты сводится к предотвращению угроз нарушения безопасности.

Исходя из возможных угроз безопасности выделяют следующие задачи защиты:

1. **Защита информации от хищения –** подразумевает предотвращение физического хищения устройств и носителей хранения информации, несанкционированного получения информации (копирования, подсмотра, перехвата и т.д.) и несанкционированного распространения информации

2. **Защита информации от потери –** подразумевает поддержание целостности и корректности информации, что означает обеспечение физической, логической, семантической целостности информации.

3. **Защита ВС от сбоев и отказов аппаратно-программного обеспечения** является одним из необходимых условий нормального функционирования системы.

4. Уровни защиты.

Различают четыре уровня защиты:

1. **Предотвращение** – доступ к информации и технологии имеет только персонал, который получил допуск от собственника информации

2. **Обнаружение** – обеспечивается раннее обнаружение преступлений и злоупотреблений, даже если механизмы защиты были обойдены

Уровни защиты

1. **Ограничение** – уменьшается размер потерь, если преступление все-таки произошло, несмотря на меры по его предотвращению и обнаружению
2. **Восстановление -** обеспечивает эффективное восстановление информации при наличии документированных и проверенных планов по восстановлению.

Контрольные вопросы:

1. Что понимают под угрозой ИПО?
2. Что называется атакой и кто такой злоумышленник?
3. Что такое окно опасности?
4. По каким критериям классифицируют угрозы в ИС?
5. Перечислите основные виды угроз, возникающие в ИС.
6. Каковы возможные последствия нарушения системы защиты?
7. Перечислите основные задачи и уровни защиты.