


ТЕМА: Угрозы безопасности

A silhouette of a runner in a starting crouch on a track, positioned to the left of the key words text.

Ключевые слова: угроза,
атака, окно опасности,
злоумышленник.

План урока:

1. Основные определения и критерии классификации угроз
2. Виды угроз, возникающие в ИС.

Цели и задачи урока: научиться определять угрозы безопасности и устранять угрозы.



1. Основные определения и критерии классификации угроз

Под **угрозой** 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**.

ЗАЩИТИ ИНФОРМАЦИЮ ОТ УТЕЧКИ!

Каналы утечки информации

Съемные носители информации
Электронная почта
Интернет
Бумажные документы
Настольные ПК
Мобильное оборудование



Угрозы

Случайное или преднамеренное копирование информации



Разглашение информации вследствие случайного или преднамеренного вывода на печать



Передача информации с использованием сети Интернет



- Утечка клиентской базы
- Распространение персональных данных
- Утечка методик, разработок, чертежей
- Утечка финансовой информации

Инциденты



Нарушители

Менеджеры высшего и среднего звена, административно-хозяйственный персонал
Персонал, имеющий легитимный доступ к защищаемой информации

Системные администраторы
Персонал, осуществляющий администрирование оборудования

Способы защиты

DLP-системы
Технические средства защиты

Защита от несанкционированного физического доступа к компьютерным системам
Организационные способы защиты



Последствия утечки информации

Утечка интеллектуальной собственности
Потери репутации Компании
Банкротство Компании
Судебные разбирательства



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.

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 (копирование, удаление, изменение):
2. Некорректное использование ресурсов:
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.

Закрепление материала:

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?

Домашнее задание:

1. Уровни защиты.
2. Основные задачи защиты.