

# **Угрозы информационной безопасности и каналы утечки информации**

Лекция 3

# Угроза ИБ

---

Событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации.

---

**Уязвимость информации** - возможность возникновения на каком-либо этапе жизненного цикла КС такого состояния, при котором создаются условия для реализации угроз безопасности информации.

**Атака** – действия нарушителя, для поиска и использования уязвимости системы

# Классификация угроз

## 1. По природе возникновения

---

- **естественные** – возникли в результате объективных физических процессов или стихийных природных явлений (не зависят от человека)

*Пример: пожары, наводнения, цунами, землетрясения и т.д.*

- **искусственные** – вызваны действием человека.

## 2. По степени преднамеренности

---

- ❑ **случайные** – халатность или непреднамеренность персонала.  
(ввод ошибочных данных)
- ❑ **преднамеренные** – деятельность злоумышленника (проникновение злоумышленника на охраняемую территорию)

### 3. В зависимости от источников угроз

---

- ❑ **Природная среда** – природные явления
- ❑ **Человек** - агенты
- ❑ **Санкционированные программно-аппаратные средства** – некомпетентное использование программных утилит
- ❑ **Несанкционированные программно-аппаратные средства** – клавиатурный ШПИОН

## 4. По положению источника

---

### □ **вне контролируемой зоны**

*примеры: перехват побочных маг. излучений (ПЭМИН), данных по каналам связи, информации с помощью микрофона, скрыта фото и видеосъемка)*

### □ **в пределах контролируемой зоны**

*подслушивающие устройства, хищение носителей с конфиденциальной информацией*

## 5. Степени воздействия

---

- ❑ **пассивные** – нет изменений в составе и структуре КС

*Пример: несанкционированное копирование файлов с данными*

- ❑ **активные** – нарушают структуру АС



## 6. По способу доступа к ресурсам КС

---

### ❑ **Используют стандартный доступ**

*Пример: получение пароля путем подкупа, шантажа, угроз, физического насилия*

### ❑ **Нестандартный путь доступа**

*Пример: не декларированные возможности средств защиты*

# Основная классификация угроз

---

- 1. Нарушение конфиденциальности**
- 2. Нарушение целостности данных**
- 3. Нарушение доступности информации**

# Каналы утечки информации

---

## 1. Косвенные

- подслушивающие устройства
- скрытые видеокамеры
- ПЭМИН

## 2. Непосредственные

- хищение носителей
- сбор производственных отходов с информацией
- намеренное копирование файлов других пользователей
- чтение остаточной информации после выполнения действий
- копирование носителей
- НСД
- маскировка под других пользователей для похищения идентифицирующей информации
- обход средств разграничения доступа

# Каналы утечки с изменением элементов КС

---

- ❑ **незаконное подключение регистрирующей аппаратуры**
- ❑ **злоумышленное изменение программ**
- ❑ **злоумышленный вывод из строя средств защиты**

# Выводы:

---

- Надежная защита - это не только формальные методы
- Защита не может быть абсолютной

# Методы и средства защиты

---

- ❑ **Организационно-правовые**
- ❑ **Инженерно-технические**
- ❑ **Криптографические**
- ❑ **Программно- аппаратные**