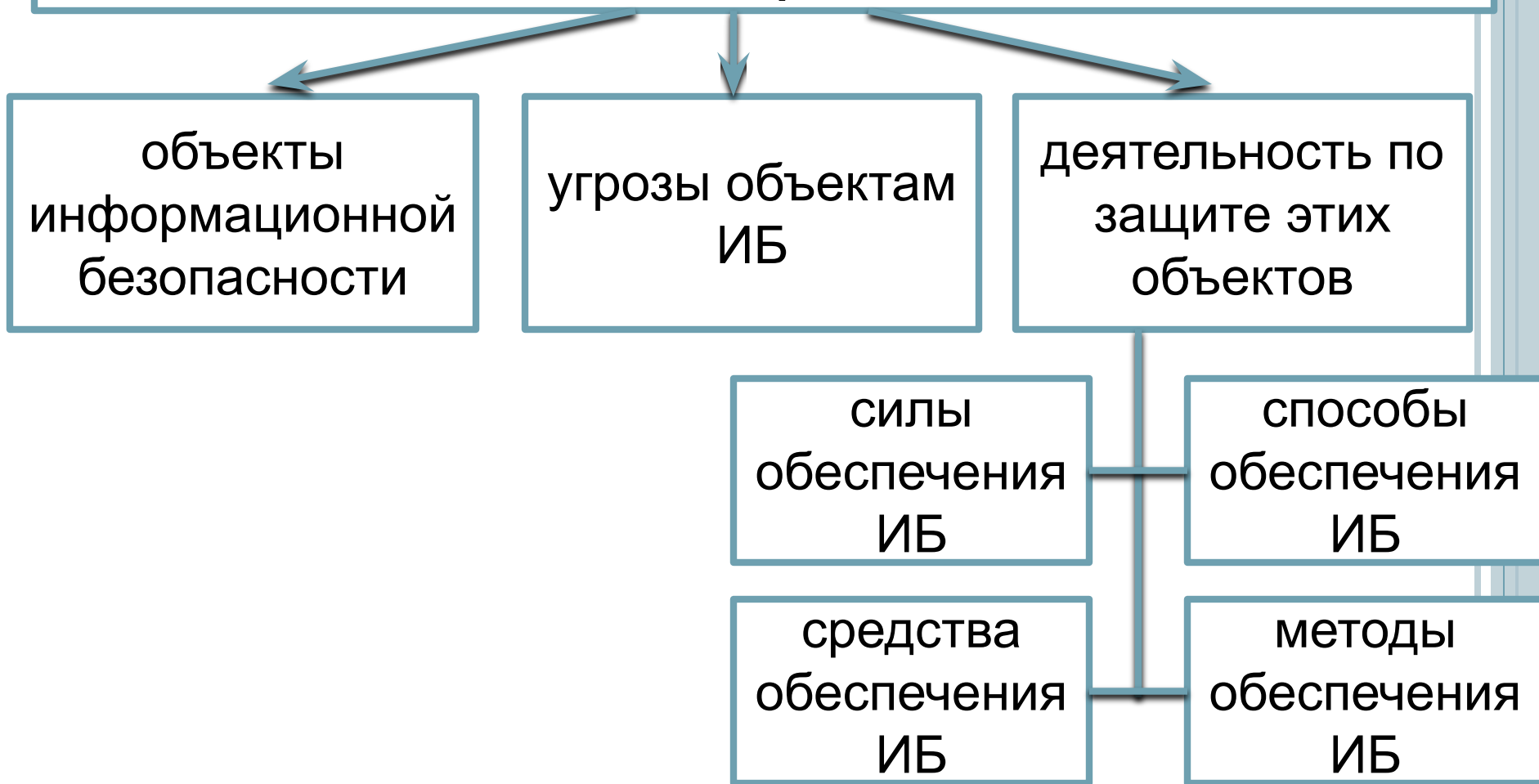


# УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



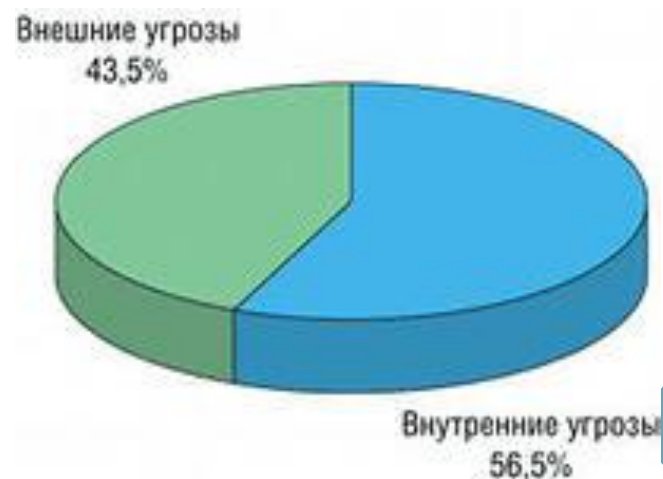
# УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

## ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



# УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Цель деятельности по обеспечению информационной безопасности:** ликвидация угроз объектам информационной безопасности и минимизация возможного ущерба, который может быть нанесен вследствие реализации данных угроз.



**В Доктрине ИБ: «угроза информационной безопасности Российской Федерации (далее – информационная угроза) – совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере»**



# УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

## СВОЙСТВА УГРОЗЫ

### Избирательность

нацеленность угрозы на нанесение вреда тем или иным конкретным свойствам объекта безопасности

### Предсказуемость

наличие признаков возникновения, позволяющих прогнозировать возможность появления угрозы и определять конкретные объекты безопасности, на которые она будет направлена

### Вредоносность

возможность нанесения вреда различной тяжести объекту безопасности

## Основные определения и критерии классификации угроз

? **Угроза** - это потенциальная возможность определенным образом нарушить информационную безопасность.

? **Атака** - попытка реализации угрозы.

Тот, кто предпринимает такую попытку, называется **злоумышленником**.

**Источники угроз** - потенциальные злоумышленники



# УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Чаще всего *угроза* является следствием наличия **уязвимых мест** в защите информационных систем.

**Опасность** - состояние, в котором находится объект безопасности вследствие возникновения угрозы этому объекту.

**Возможный вред определяет величину опасности.**

**Окно опасности** - промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется.



## Основные определения и критерии классификации угроз

Для характеристики **угрозы информационной безопасности** используются следующие **параметры**:

- Источник угрозы.
- Метод воздействия на объект.
- Уязвимости, которые могут быть использованы.
- Ресурсы, которые могут пострадать от реализации.





# КЛАССИФИКАЦИЯ УГРОЗ

По объектам	По масштабу	По актуализации	По причине
Персонал, финансы, матер. ценности, Информация	Глобальные Региональные Организация	Весьма вероятные Вероятные Маловероятные	Стихийные Преднамеренные Закономерные Случайные
<b>Угрозы</b>			
По характеру ущерба	Расположение источника	По характеру воздействия	По величине ущерба
Материальный Моральный	Внутренние Внешние	Активные Пассивные	Предельный Значительный Незначительный

По аспекту информационной безопасности (доступность, целостность, конфиденциальность), против которого *угрозы* направлены в первую очередь

## Основные определения и критерии классификации угроз

### **Угроза безопасности информации** –

совокупность условий и факторов, создающих потенциальную или реально существующую опасность, в результате которой возможны утечка информации, неправомерное модифицирование (искажение, подмена), уничтожение информации или неправомерное блокирование доступа к ней

Угрозы  
конфиденциальной  
безопасности

Утечка информации

Угрозы  
целостности  
информации

Неправомерное воздействие на  
информацию

Угрозы  
доступности  
информации



## Наиболее распространенные угрозы доступности

Самыми частыми и самыми опасными (с точки зрения размера ущерба) являются **непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы.**

Основной способ борьбы с **непреднамеренными ошибками** - максимальная автоматизация и строгий контроль.



# Угрозы доступности по компонентам ИС

## Отказ пользователей

- нежелание работать с ИС
- невозможность работать с ИС в силу отсутствия соответствующей подготовки
- невозможность работать с ИС в силу отсутствия технической поддержки

## Внутренний отказ ИС

- отступление от установленных правил эксплуатации
- выход системы из штатного режима
- ошибки при конфигурировании системы
- отказы ПО и аппаратного обеспечения
- разрушение данных
- повреждение аппаратуры

## Отказ поддерживающей инфраструктуры

- нарушение работы систем связи
- электропитания
- водо- и/или теплоснабжения, кондиционирования
- разрушение или повреждение помещений
- нежелание обслуживающего персонала выполнять свои обязанности

## Наиболее распространенные угрозы доступности

Опасны так называемые *"обиженные" сотрудники* - нынешние и бывшие.

Как правило, они стремятся нанести вред организации-"обидчику", например:

- ❑ испортить оборудование;
- ❑ встроить логическую бомбу, которая со временем разрушит программы и/или данные;
- ❑ удалить данные.

Необходимо следить за тем, чтобы при увольнении сотрудника его права доступа (логического и физического) к информационным ресурсам аннулировались.

## *МЕРЫ ПРИ УЛИЧЕНИИ СОТРУДНИКА В ПРОМЫШЛЕННОМ ШПИОНАЖЕ*

- немедленно лишить его всех прав доступа к ИТ;
- немедленно скорректировать права доступа к общим информационным ресурсам (базам данных, принтерам, факсам), перекрыть входы во внешние сети или изменить правила доступа к ним;
- все сотрудники должны сменить личные пароли, при этом до их сведения доводится следующая информация: «Сотрудник N с (дата) не работает. При любых попытках контакта с его стороны немедленно сообщать в службу безопасности»;
- некоторое время контроль ИС осуществляется в усиленном режиме.



## 1) Кражи и подлоги

С целью нарушения **статической целостности** **злоумышленник** (как правило, штатный сотрудник) может:

- ? ввести неверные данные;
- ? изменить данные.

## 2) Внедрение вредоносного ПО

**Угрозами динамической целостности** являются переупорядочение, кража, дублирование данных или внесение дополнительных сообщений (сетевых пакетов и т.п.).

Соответствующие действия в сетевой среде

## Основные угрозы конфиденциальности

Угрозы конфиденциальности информации могут носить **некомпьютерный и вообще нетехнический характер.**

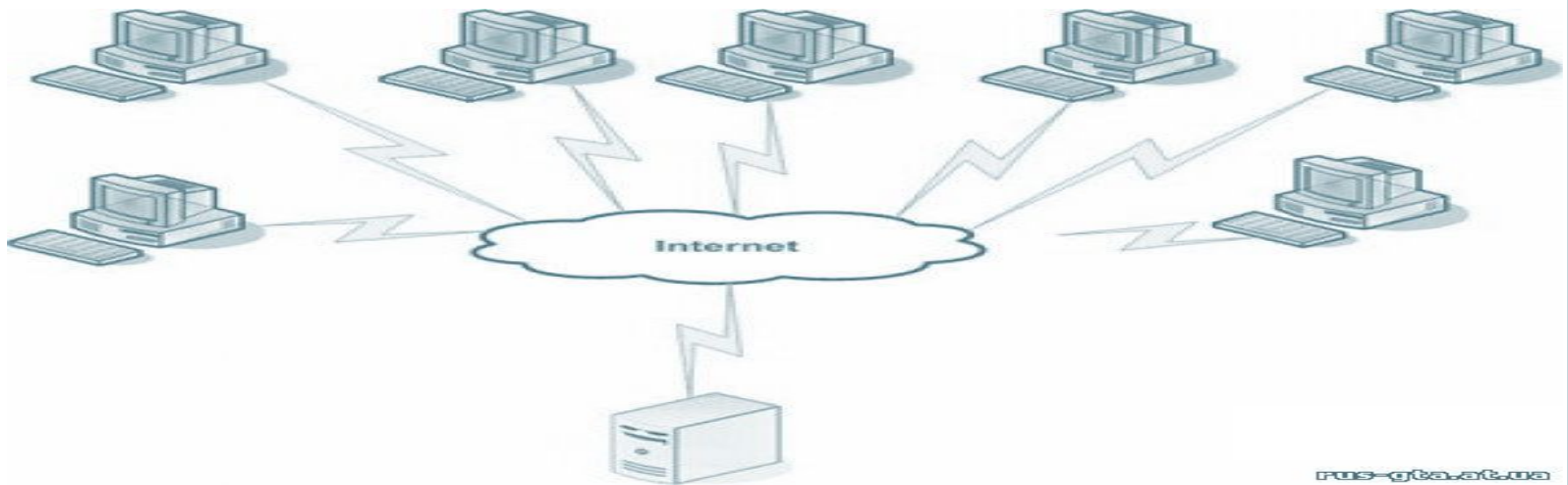
1. **Неправильное хранение данных на резервных носителях.**
2. **Перехват данных** (данные передаются по многим каналам, их защита может оказаться весьма сложной и дорогостоящей)
3. **Злоупотребление полномочиями.**





# Программные атаки на доступность

- ? **Атака** – любое действие или последовательность действий, использующих уязвимости информационной системы и приводящих к нарушению политики безопасности.
- ? **Механизм безопасности** – программное и/или аппаратное средство, которое определяет и/или предотвращает атаку.
- ? **Сервис безопасности** - сервис, который обеспечивает безопасность систем и/или передаваемых данных, либо определяет осуществление *атаки*.



## Классификация сетевых атак

При описании сетевых атак в общем случае используется следующее представление:

- существует информационный поток от отправителя (файл, пользователь, компьютер) к получателю (файл, пользователь, компьютер):



# Классификация атак

Классификация атак на информационную систему может быть выполнена по нескольким признакам:

- **По месту возникновения:**

- ? **Локальные атаки** (источником данного вида атак являются пользователи и/или программы локальной системы);

- ? **Удаленные атаки** (источником атаки выступают удаленные пользователи, приложения)



## По воздействию на информационную систему:

? Активные атаки (результатом воздействия которых является нарушение деятельности информационной системы);

? Пассивные атаки (ориентированные на получение информации из системы, не нарушая функции системы)



## Сетевые атаки

? **Пассивной** называется такая атака, при которой противник не имеет возможности модифицировать передаваемые сообщения и вставлять в информационный канал между отправителем и получателем свои сообщения.

? **Целью пассивной атаки** может быть только прослушивание передаваемых сообщений и анализ трафика.



? **Активной** называется такая атака, при которой противник имеет возможность модифицировать передаваемые сообщения и вставлять свои сообщения.

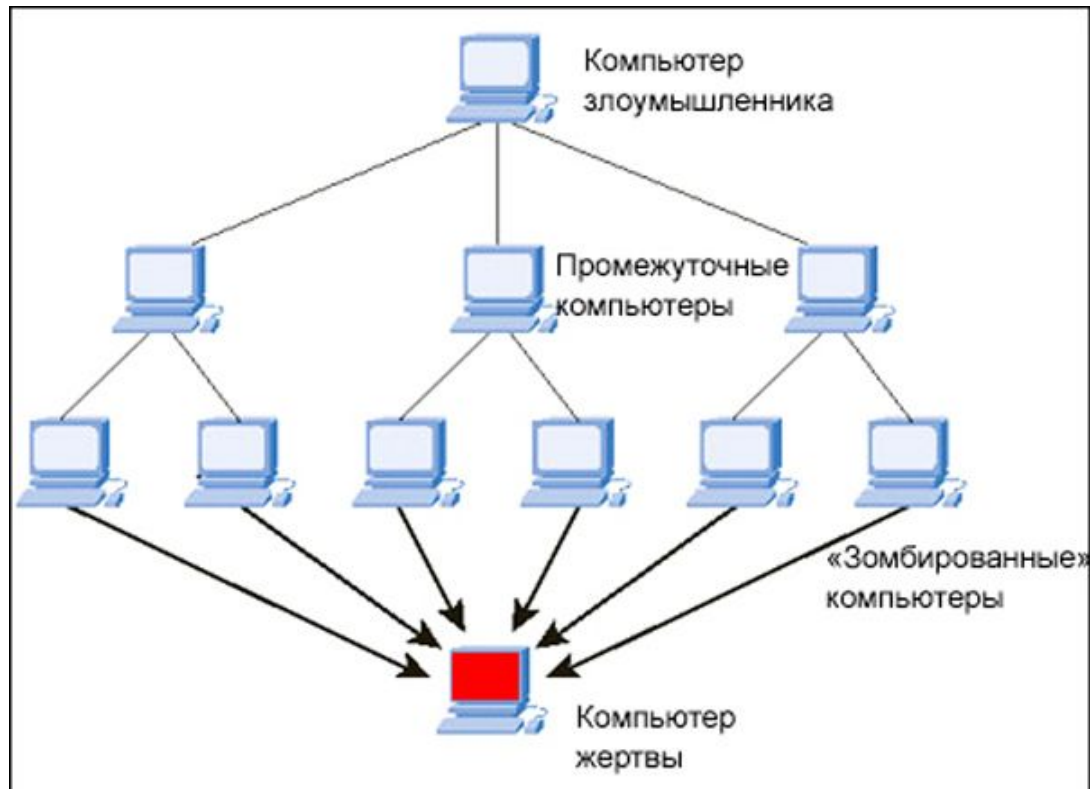
Различают следующие типы активных атак:

**1. Отказ в обслуживании** - **DoS-атака** (*Denial of Service*)

Атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых правомерные пользователи системы не могут получить доступ к предоставляемым системой ресурсам (серверам).

## Сетевые атаки

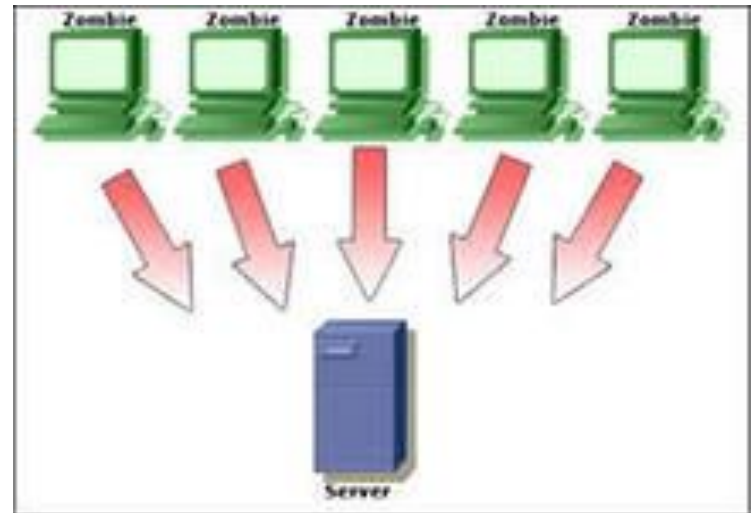
Если атака выполняется одновременно с большого числа компьютеров, говорят о **DDoS-атаке** (*Distributed Denial of Service, распределённая атака типа «отказ в обслуживании»*).



## Сетевые атаки

Классическим примером такой *атаки* в сетях TCP/IP является **SYN-атака**, при которой нарушитель посылает пакеты, инициирующие установление TCP-соединения, но не посылает пакеты, завершающие установление этого соединения.

В результате может произойти переполнение памяти на сервере, и серверу не удастся установить соединение с законными пользователями.





## 2. Модификация потока данных - атака "man in the middle"

**Модификация потока данных означает либо изменение содержимого пересылаемого сообщения, либо изменение порядка сообщений.**



## 3. Создание ложного потока (фальсификация)

Фальсификация (нарушение аутентичности) означает попытку одного субъекта выдать себя за другого



## 4. Повторное использование

Означает пассивный захват данных с последующей их пересылкой для получения несанкционированного доступа - это так называемая *replay-атака*.

На самом деле *replay-атаки* являются одним из вариантов фальсификации, но в силу того, что это один из наиболее распространенных вариантов *атаки* для получения несанкционированного доступа, его часто рассма

