

# Угрозы информационной безопасности

Выполнил: обучающийся  
гр. № 23 Бартель Г.В.

Проверила: Турусинова И.П.

# ОГЛАВЛЕНИЕ

1. Основные определения
2. Классификация угроз
  - 2.1. По виду источника угроз
    - 2.1.1. Антропогенные источники
    - 2.1.2. Техногенные источники
    - 2.1.3. Стихийные бедствия
  - 2.2. По признаку топологии
  - 2.3. По признаку воздействия
3. Соотношение опасности от общих внутренних и внешних угроз
4. Фишинг
5. Модель нарушения
6. Литература

# 1. ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ

**Уязвимость** - это причины, обусловленные особенностями хранения, использования, передачи, охраны и ресурсов, приводящие к нарушению безопасности конкретного ресурса.

**Угроза безопасности** - потенциальное нарушение безопасности, любое обстоятельство, которое может явиться причиной нанесения ущерба предприятию.

**Атака** - реализация угрозы.

**Ущерб** - последствия, возникшие в результате правонарушения. Ущерб бывает материальный, физический, моральный.

**Нарушитель** - это лицо, предпринявшее попытку выполнения запрещенных операций и использующее для этого различные возможности

## 2. КЛАССИФИКАЦИЯ УГРОЗ

1. По виду источника угроз
  - 1.1. Антропогенные источники угроз
  - 1.2. Техногенные источники
  - 1.3. Стихийные бедствия
2. По внутренним признакам топологии
3. По внешним признакам топологии
4. По признаку воздействия

## 2.1. ВИДЫ ИСТОЧНИКОВ УГРОЗ

- 2.1.1. Антропогенные источники
- 2.2.2. Техногенные источники
- 2.2.3. Стихийные бед



## 2.1.1. АНТРОПОГЕННЫЕ ИСТОЧНИКИ

- Криминальные структуры
- Потенциальные преступники и хакеры
- Недобросовестные партнеры
- Представители надзорных организаций и аварийных служб
- Представители силовых структур
- Основной персонал (пользователи, программисты, разработчики)
- Представители службы защиты информации (администраторы)
- Вспомогательный персонал (уборщики, охрана)
- Технический персонал (жизнеобеспечение, эксплуатация)

## 2.1.2.ТЕХНОГЕННЫЕ ИСТОЧНИКИ

### Внешние

- Средства связи (передачи информации)
- Сети инженерных коммуникаций (энергоснабжения, водоснабжения, отопления, вентиляции, канализации)

### Внутренние

- Некачественные технические средства обработки информации
- Некачественные программные средства обработки информации
- Вспомогательные средства (охраны, сигнализации, телефонии)
- Другие технические средства, применяемые в учреждении

## 2.1.3. СТИХИЙНЫЕ БЕДСТВИЯ

- Пожары,
- Землетрясения,
- Наводнения,
- Ураганы,
- Различные непредвидимые обстоятельства,
- Необъяснимые явления,
- Другие форс-мажорные обстоятельства





## 2.2. ПО ПРИЗНАКУ ТОПОЛОГИИ

### Внутренние угрозы:

- неквалифицированная внутренняя политика компании по организации
- информационных технологий и управлению безопасностью;
- отсутствие соответствующей квалификации персонала по обеспечению деятельности и управлению объектом защиты;
- преднамеренные и непреднамеренные действия персонала по нарушению безопасности;
- предательство персонала;
- техногенные аварии и разрушения, пожары.

## 2.2. ПО ПРИЗНАКУ ТОПОЛОГИИ

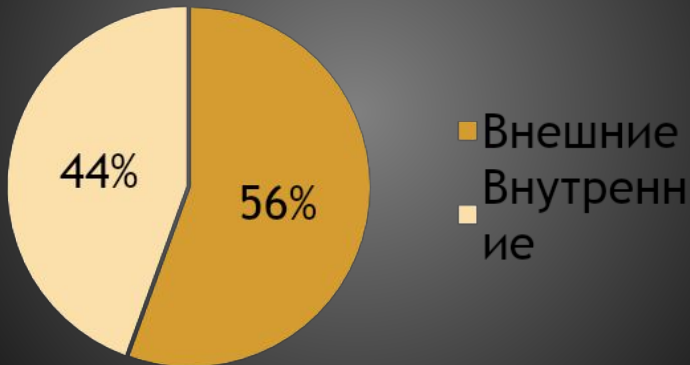
### Внешние угрозы

- ⊙ негативные воздействия недобросовестных конкурентов и государственных структур;
- ⊙ преднамеренные и непреднамеренные действия заинтересованных структур и физических лиц;
- ⊙ утечка конфиденциальной информации на носителях информации и по каналам связи;
- ⊙ несанкционированное проникновение на объект защиты;
- ⊙ несанкционированный доступ к носителям информации и каналам связи с целью хищения, искажения, уничтожения, блокирования информации;
- ⊙ стихийные бедствия и другие форсмажорные обстоятельства;
- ⊙ преднамеренные и непреднамеренные действия поставщиков услуг по обеспечению безопасности и поставщиков технических и программных продуктов.

## 2.3. ПО ПРИЗНАКУ ВОЗДЕЙСТВИЯ

- ⊙ Угрозы конфиденциальности данных и программ
- ⊙ Угрозы целостности данных, программ, аппаратуры
- ⊙ Угрозы доступа к информационным ресурсам

### 3. СООТНОШЕНИЕ ОПАСНОСТИ ПО ПРИЗНАКУ ТОПОЛОГИИ ОТ ОБЩИХ ВНУТРЕННИХ И ВНЕШНИХ УГРОЗ



## 4. ФИШИНГ

Фишинг - это особый вид компьютерного мошенничества.

Фишинг-атаки организуются следующим образом: киберпреступники создают подложный сайт, который выглядит в точности так же, как сайт банка или сайт, производящий финансовые расчеты через интернет.

Мошенники пытаются обманным путем добиться, чтобы пользователь посетил фальшивый сайт и ввел на нем свои конфиденциальные данные - например, регистрационное имя, пароль или PIN-код.

Используя их, злоумышленники крадут деньги со счетов попавшихся на удочку пользователей.

## 5. МОДЕЛЬ НАРУШЕНИЯ

Моделирование процессов нарушения информационной безопасности целесообразно осуществлять на основе рассмотрения логической цепочки: «угроза – источник угрозы – метод реализации – уязвимость – последствия»

## 5. МОДЕЛЬ НАРУШЕНИЯ

- **Требования к модели нарушения**

Служба безопасности должна построить модель типичного злоумышленника.

Необходимо оценить, от кого защищаться в первую очередь. Опираясь на построенную модель злоумышленника можно строить адекватную систему информационной защиты. Правильно разработанная модель нарушителя является гарантией построения адекватной защиты.

## 5. МОДЕЛЬ НАРУШЕНИЯ

- **Требования к системе защиты информации**

Система защиты информации должна быть адекватной уровню важности, секретности и критичности защищаемой информации.

Ее стоимость не должна превосходить возможный ущерб от нарушения безопасности охраняемой информации.

Преодоление системы защиты должно быть экономически нецелесообразно по сравнению с возможной выгодой от получения доступа, уничтожения, модификации или блокировки защищаемой информации.



## 6. ЛИТЕРАТУРА

- <http://privetstudent.com/prezentacii/prezentacii-kompiutery/1094-prezentaciya-klassifikacii-ugroz-informacionnoy-bezopasnosti-i-ih-harakteristika.html>