

---

---

# Методы оценивания угроз



# Методы оценивания угроз

---

- идентификация угроз
- спецификация угроз
- оценивание угроз
  - формирование оценок идентифицированных и специфицированных угроз с точки зрения потерь, ущерба, возможных от реализации (воздействия) соответствующих угроз.
  - Основными факторами оценки являются возможность реализации угрозы и возможный ущерб от реализации угрозы.



# Общая схема оценки угроз



# Оценка угроз. Как оценивать?

---

- Вероятность реализации угроз - естественный параметр и шкала оценки возможности реализации угроз
- 1. Априорный подход** - если природа угроз позволяет вычислять эти вероятности на основе известных соответствующих физических закономерностей (ошибки в наборе данных)
- 2. Апостериорный поход** – основан на накопленной статистике проявления соответствующей угрозы в данной или подобной КС (в подобных условиях)
- 3. Метод экспертных оценок**



# 1. Оценка угроз.

## Метод экспертных оценок

---

- Эксперты на основе профессионального опыта, глубокого представления многокомпонентной природы оцениваемых объектов, дают эвристические оценки по одному или группе параметров
- 1. Отбор экспертов** (метод «снежного кома», 10-12 чел.).
  - 2. Выбор параметров**, по которым оцениваются объекты (сущностные параметры оценивания, выражающие природу объектов и независимые друг от друга, определяются веса параметров)



# 3-1. Оценка угроз.

## Метод экспертных оценок

---

- 1. Выбор шкал оценивания и методов экспертного шкалирования.** Ранжирование объектов (порядковая шкала оценки), попарные оценки сравнительной предпочтительности, непосредственная оценка выраженности оцениваемого параметра

Непосредственной оценкой

	Эксп. 1	Эксп. 2	Эксп. М
Угр. 1			
Угр. 2			
...			
Угр. N			

$$P_i = \sum_{j=1}^M \frac{1}{M} P_{ij}$$



# 3-2. Оценка угроз.

## Метод экспертных оценок

---

1. Выбор шкал оценивания и методов экспертного шкалирования. Ранжирование объектов (порядковая шкала оценки), попарные оценки сравнительной предпочтительности, непосредственная оценка выраженности оцениваемого параметра

**Ранжированием**

	Эксп. 1	Эксп. 2	Эксп. М
Угр. 1	2	1	5
Угр. 2	1	3	1
...			
Угр. N	5	2	2



# 3-3. Оценка угроз.

## Метод экспертных оценок

1. Выбор шкал оценивания и методов экспертного шкалирования. Ранжирование объектов (порядковая шкала оценки), попарные оценки сравнительной предпочтительности, непосредственная оценка выраженности оцениваемого параметра

Парным сравнением

$$p_i = \sum_{j=1}^N \sum_{m=1}^M \frac{1}{MN} p^{m}_{ij}$$

Эксп. $M$	Угр. 1	Угр. 2	Угр. $N$
Угр. 1			
Угр. 2			
...			
Угр. $N$			

Эксп. 2	Угр. 1	Угр. 2	Угр. $N$
Угр. 1			
Угр. 2			
...			
Угр. $N$			

Эксп. 1	Угр. 1	Угр. 2	Угр. $N$
Угр. 1			
Угр. 2			
...			
Угр. $N$			





# 4. Оценка угроз.

## Метод экспертных оценок

---

4. Выбор и осуществление процедуры опроса экспертов
5. Агрегирование оценок, анализ их устойчивости и согласованности



- 
- Человеческий фактор в угрозах безопасности и
  - модель нарушителя



# Человеческий фактор в угрозах безопасности и модель нарушителя

---

## *Роль человека в угрозах безопасности информации:*

- носитель/источник угроз** (*как внутренних, так и внешних, как случайных, так и преднамеренных*)
- средство, орудие осуществления угроз** (*всех преднамеренных и определенной части случайных угроз*)
- предмет, объект, среда осуществления угроз** (*как элемента человеко-машинной КС*)



# Структура потенциальных нарушителей (злоумышленников)

## КС (ИнФС)

Внешняя сторона

Внутренняя сторона

### Сфера сотрудничества

Производственно-технологический аспект  
Общественно-политический аспект

### Сфера противоборства

Конкуренция  
Преступность

### Иные сферы

Сторонние эксперты, конс.

Родственники, друзья

Бывшие работники

### Персонал, непосредственно связанный с КС

- *обслуживающий персонал*
  - администраторы
    - системные
    - безопасности
  - инженеры-программисты
    - системные
    - прикладные
  - руководители служб ИТ
- *обслуживаемый персонал*
  - пользователи
    - индивидуальные
    - члены раб. групп
    - руководители подр-й

### Персонал, не связанный непосредственно с КС

- *руководители*
- *прочие работники*



# Человеческий фактор в угрозах безопасности и модель нарушителя

---

## МОТИВЫ

действий, поступков по осуществлению угроз

- *Осознанные*

- *Корысть, нажива*
- *Политика, власть, шпионаж*
- *Исследовательский интерес*

- *Неосознанные (не вполне, не до конца осознаваемые)*

- *Хулиганство*
- *Мечь*
- *Зависть*
- *Недовольство*
- *Небрежность, недобросовестность*



# Человеческий фактор в угрозах безопасности и модель нарушителя

## Модель нарушителя

**совокупность представлений по человеческому фактору осуществления угроз безопасности**

- *категории лиц, в числе которых может оказаться нарушитель*
- *его мотивационные основания и преследуемые цели*
- *его возможности по осуществлению тех или иных угроз (квалификация, техническая и иная инструментальная оснащенность)*
- *наиболее вероятные способы его действий*

Исходное основание для разработки и синтеза системы защиты информации!!!

# Модель внутреннего нарушителя по РД ГосТехКомиссии

!!! Концепция ориентируется на физически защищенную среду -  
- нарушитель безопасности как "субъект, имеющий доступ к  
работе со штатными средствами АС и СВТ как части АС"

4-й (высший) уровень возможностей нарушителя

Весь объем  
возможностей  
лиц, осуществляющих проектирование, реализацию и ремонт технических средств АС, вплоть до включения в состав СВТ собственных технических средств с новыми функциями по обработке информации

3-й уровень  
Возможность управления функционированием АС, т.е. воздействием на базовое программное обеспечение системы и на состав и конфигурацию оборудования

2-й уровень  
Возможность создания и запуска собственных программ с новыми функциями по обработке информации

1-й уровень  
Запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации

## Основные способы НСД

- непосредственное обращение к объектам доступа
- создание прогр. и техн. средств, выполняющих обращение к объектам доступа в обход средств защиты
- модификация средств защиты, позволяющая осуществить НСД
- внедрение в техн. ср. СВТ или АС программных или технических механизмов, нарушающих предполагаемую структуру и функции СВТ или АС и позволяющих осуществить НСД

- 
- Продолжение следует ...

Политика и модели безопасности в  
компьютерных системах

