

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ОБЪЕКТ МОДЕЛИРОВАНИЯ

Занятие 1

Маковецкая-Абрамова О.В.

# Вопросы по теме

- Сущность и основные вопросы информационной безопасности
- Виды угроз информационной безопасности
- Методы и средства защиты информации

# Что есть информация?



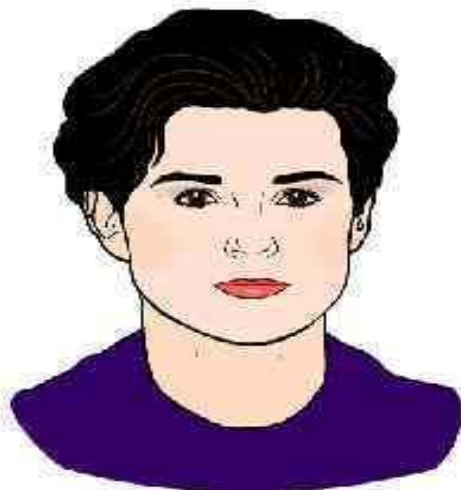
# Сенсорная информация

## *Виды информации*

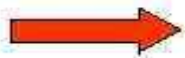
---

### По способам восприятия

У человека пять органов чувств:



Зрение



Слух



Вкус



Обоняние



Осязание

# Сенсорная информация



# Типология информации

## Информация

По способу  
восприятия

- Зрительная
- Слуховая
- Тактильная
- Обонятельная
- Вкусовая

По форме  
представления

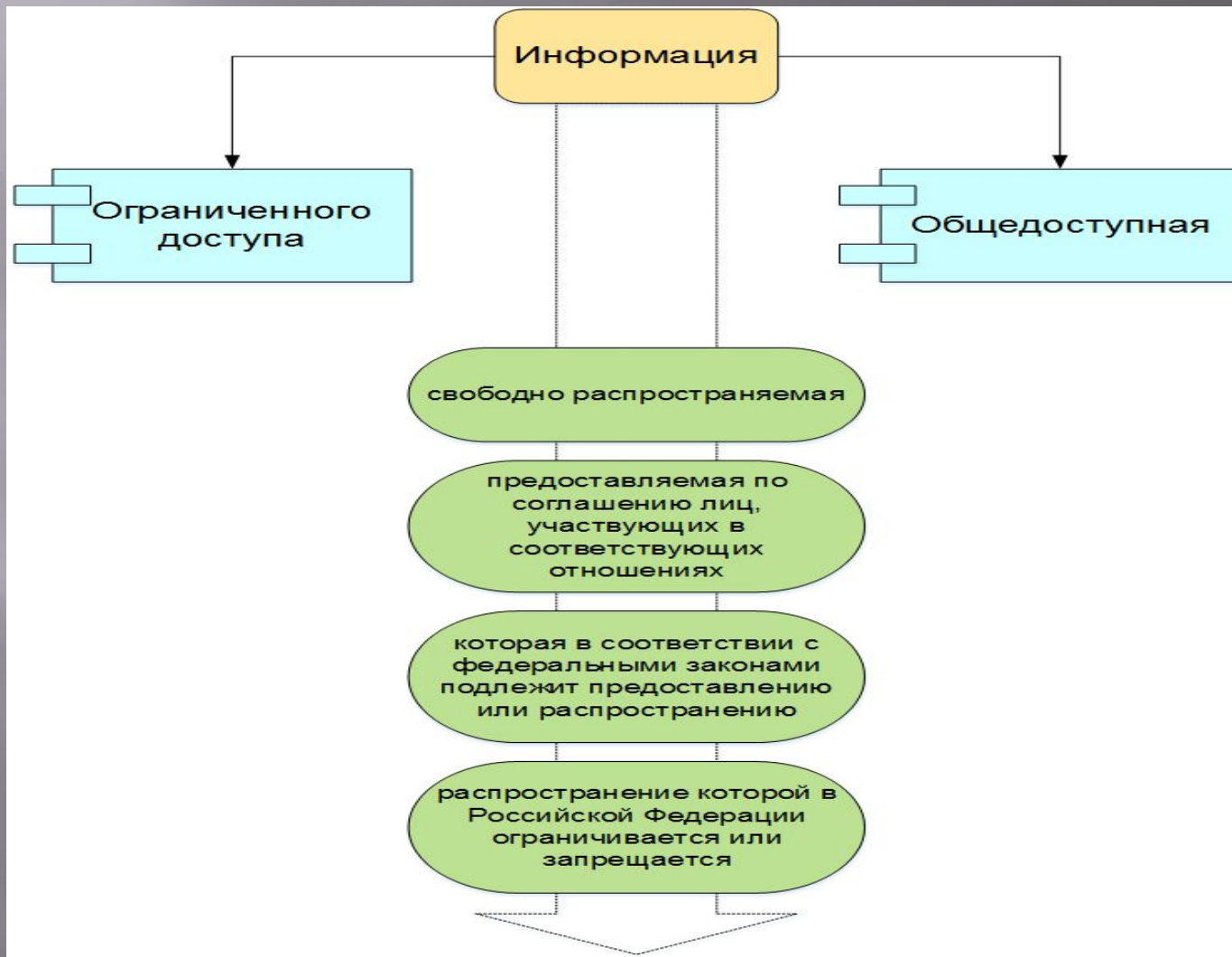
- Текстовая
- Числовая
- Графическая
- Музыкальная
- Комбинированная

По общественному  
значению

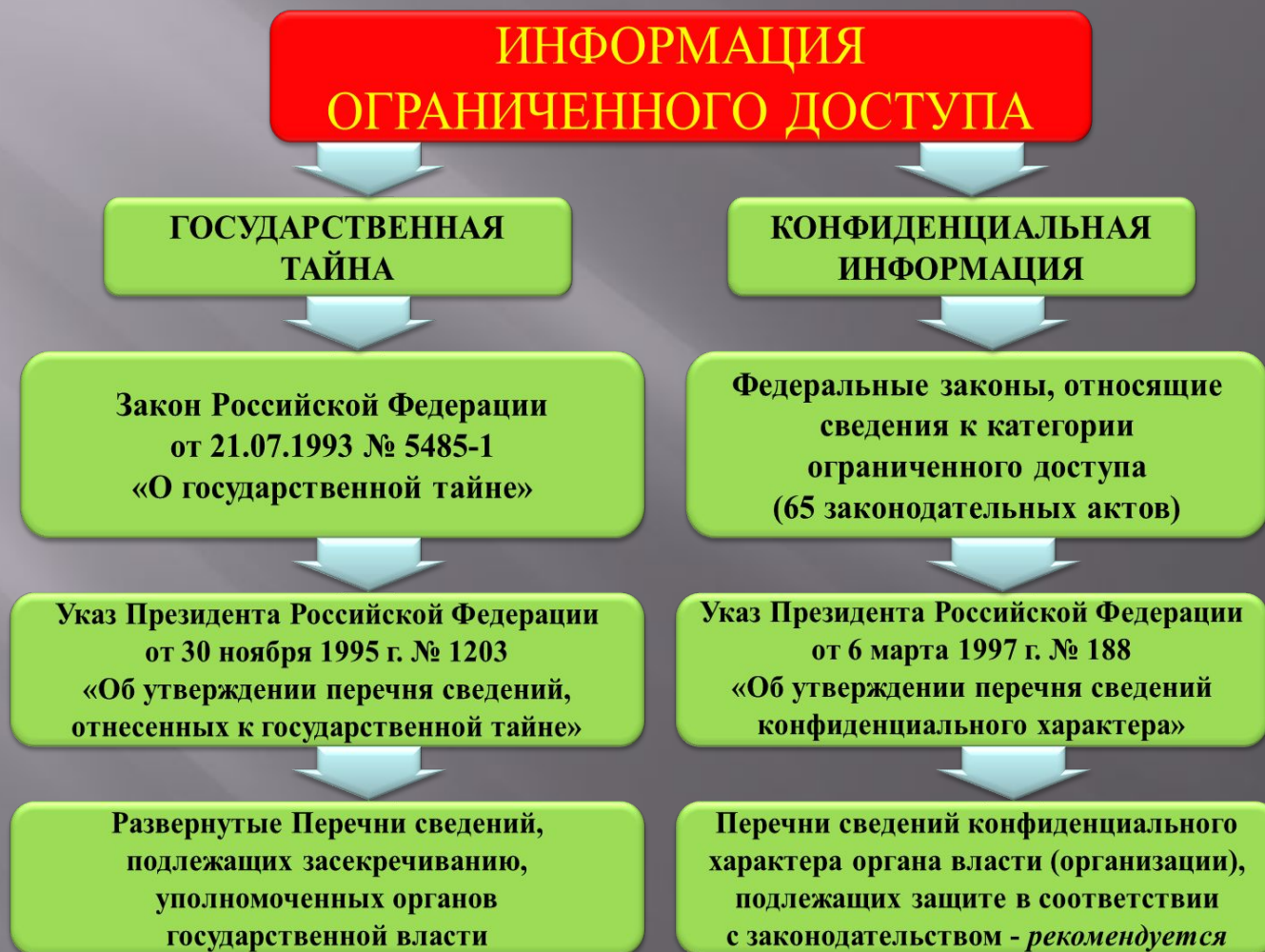
- Массовая (общ.-полит.)
- Специальная (научная, техническая)
- Личная (знания, умения, интуиция)
- Эстетическая
- Обыденная



# Доступность информации



# Ограниченный доступ





# Информация- предмет защиты

## Информация, как предмет защиты

- ❑ от разглашения – деятельность по предотвращению несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.
- ❑ от несанкционированного доступа – защита информации от НСД: деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации.

**Цели защиты информации:** выявление, предотвращение, нейтрализация, пресечение, локализация, отражение и уничтожение угроз.

# Обработка информации

## Обработка информации.

### Изменение формы представления

Обработка информации – это действие с информацией, решение некоторой информационной задачи.



# Свойства информации

## Свойства информации

Объективность

Информация **объективна**, если она не зависит от чьего-либо мнения.

Достоверность

Информация **достоверна**, если она отражает истинное положение дел.

Полнота

Информация **полна**, если ее достаточно для принятия решения.

Актуальность  
(своевременность)

Информация **актуальна**, если она важна, существенна для настоящего времени.

Полезность

**Полезность** информации оценивается по тем задачам, которые мы можем решить с ее помощью.

Понятность

Информация **понятна**, если она выражена на языке, доступном для получателя.

# Свойства информации

## Свойства информации

Объективность

Субъективность

Достоверность

Недостоверность

Полнота

Неполнота, избыточность

Актуальность  
(своевременность)

Устаревание или  
преждевременность

Полезность

Бесполезность

Понятность

Непонятность



# Значение искусственного интеллекта

- Человеческий мозг получает значительно больше информации, чем может её обработать.
- Не может воспринять непонятную ему информацию.
- Необъективен, т.е. зачастую воспринимает информацию не такой, какая она есть, а такой, какой она ему кажется.
- Быстро устаёт и может ошибаться, обрабатывая информацию.



# ИНФОРМАЦИЯ

Это информация по **Шеннону**.

**Хартли** предложил мерить информацию как  $\log M$ , где  $M$  – количество сообщений в алфавите (элементов в ансамбле). Информация по **Хартли** и по **Шеннону** совпадает, когда события **равновероятны**. В отличие от Хартли **Шеннон** учел **статистическую природу сообщений**.

**Энтропия**  $H(X)$  - это среднее значение информации на одно сообщение.

**Энтропия**  $H(X)$  - это мера «неопределенности» сообщения до того, как оно было принято.

**Энтропия неотрицательна**, поскольку неотрицательна  $I(X)$ .

# ИНФОРМАЦИЯ

**Вероятностно-статистическое понятие (по Шеннону):** информация – сведения, сообщения, которые снимают существовавшую до их получения неопределенность полностью или частично.

*Сообщение* – это форма представления информации в виде речи, текста, изображения, цифровых данных, графиков, таблиц и т.п.



# ИНФОРМАЦИЯ – это снятая неопределенность

## ФОРМУЛА ШЕННОНА

Количество информации для событий с различными вероятностями определяется по формуле:

$$I = - \sum_{i=1}^N p_i \log_2 p_i$$

*I* – количество информации,  
*N* – количество возможных событий  
*p<sub>i</sub>* – вероятности отдельных событий

Если события равновероятны ( $p_i = 1/N$ ):

$$I = - \sum_{i=1}^N \frac{1}{N} \log_2 \frac{1}{N} = \log_2 N$$

# ИНФОРМАЦИЯ



## Расчет количества информации по Хартли

Частный случай формулы Шеннона для равновероятных событий

$$I = \log_2 N$$

$$N = 2^I$$

где

$I$  – количество информации, бит

$N$  – число возможных состояний системы

# Безопасность





# Информационная безопасность



# Цифровая информация

**Цифровая информация** –

информация, хранение, передача и обработка которой осуществляется средствами ИКТ.

**Защита информации** – деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.



# Модель информационной безопасности



Модель информационной безопасности

## Ключевые вопросы ИБ



Субъекты  
нелегального доступа  
Вредоносные  
программы

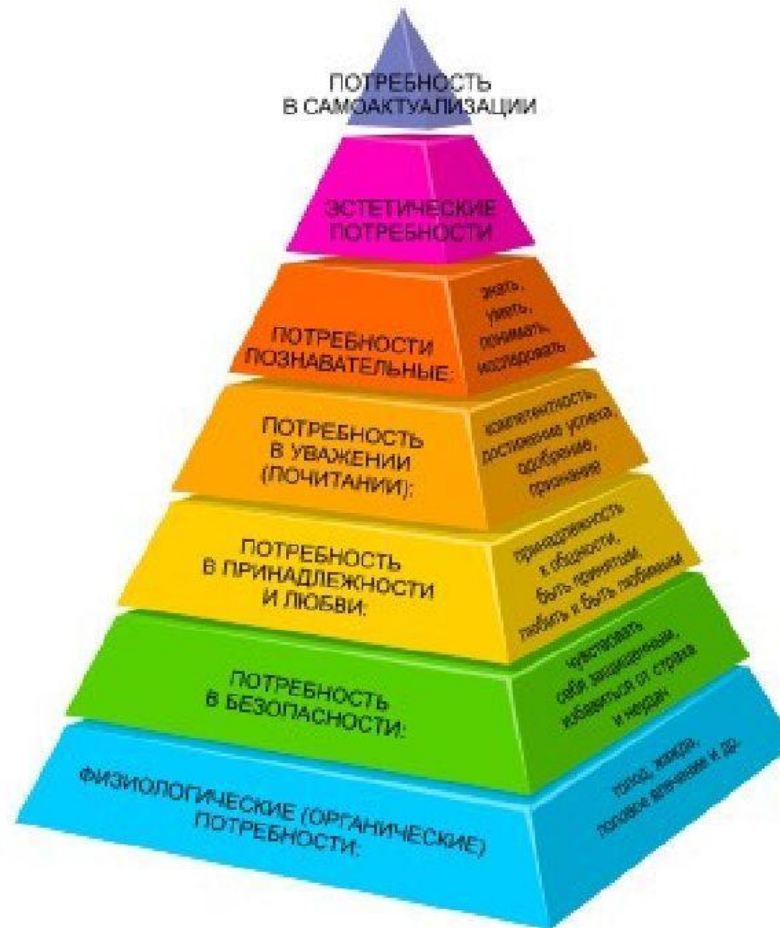
*Что  
защищать?*

*От кого  
защищать?*

*Как и чем защищать?*

# Пирамида Маслоу

**Безопасность**  
общества и пр  
Безопасность  
человека наря  
духовными пс



ИЦ,  
1.

И И



# Определение информационной безопасности

- Информационная безопасность — состояние сохранности информационных ресурсов и защищенности законных прав личности и общества в информационной сфере; это процесс обеспечения конфиденциальности, целостности и доступности информации



# Категории ИБ

**Информационная безопасность** - многогранная, многомерная область деятельности, в которой успех может принести только систематический, комплексный подход.

Спектр интересов субъектов, связанных с использованием информационных систем, можно разделить на следующие категории: обеспечение **доступности, целостности и конфиденциальности** информационных ресурсов и поддерживающей инфраструктуры.

# Правовая защита

## Правовые основы информационной безопасности

Наказания за создание вредоносных программ

штраф  
и конфискация  
компьютерного  
оборудования

тюремный  
срок

смертная  
казнь  
(Филлипины)

# Какие угрозы безопасности существуют?

## **Информационная безопасность –**

состояние защищенности информационной среды.

## **Защита информации –**

действия по предотвращению  
возможного повреждения или уничтожения информации, а также  
несанкционированного доступа к ней (но вместе с тем –  
обеспечение беспрепятственного доступа к информации  
со стороны легитимных пользователей)



# Угрозы

Угрозы конфиденциальной информации - потенциальные или реально возможные действия по отношению к информационным ресурсам, приводящие к неправомерному овладению охраняемыми сведениями.



# Классификация угроз

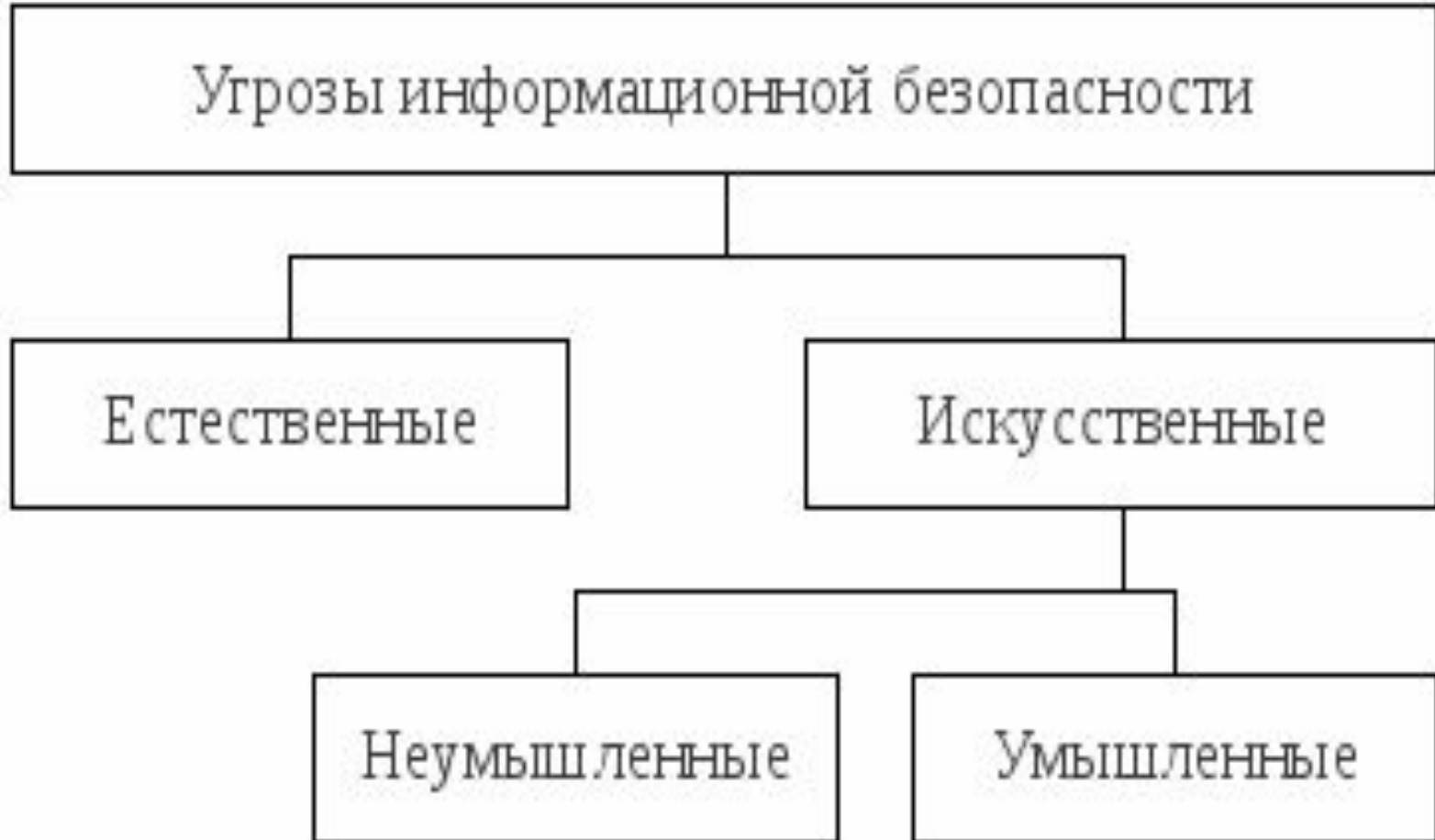
## Классификация угроз информационной безопасности

---

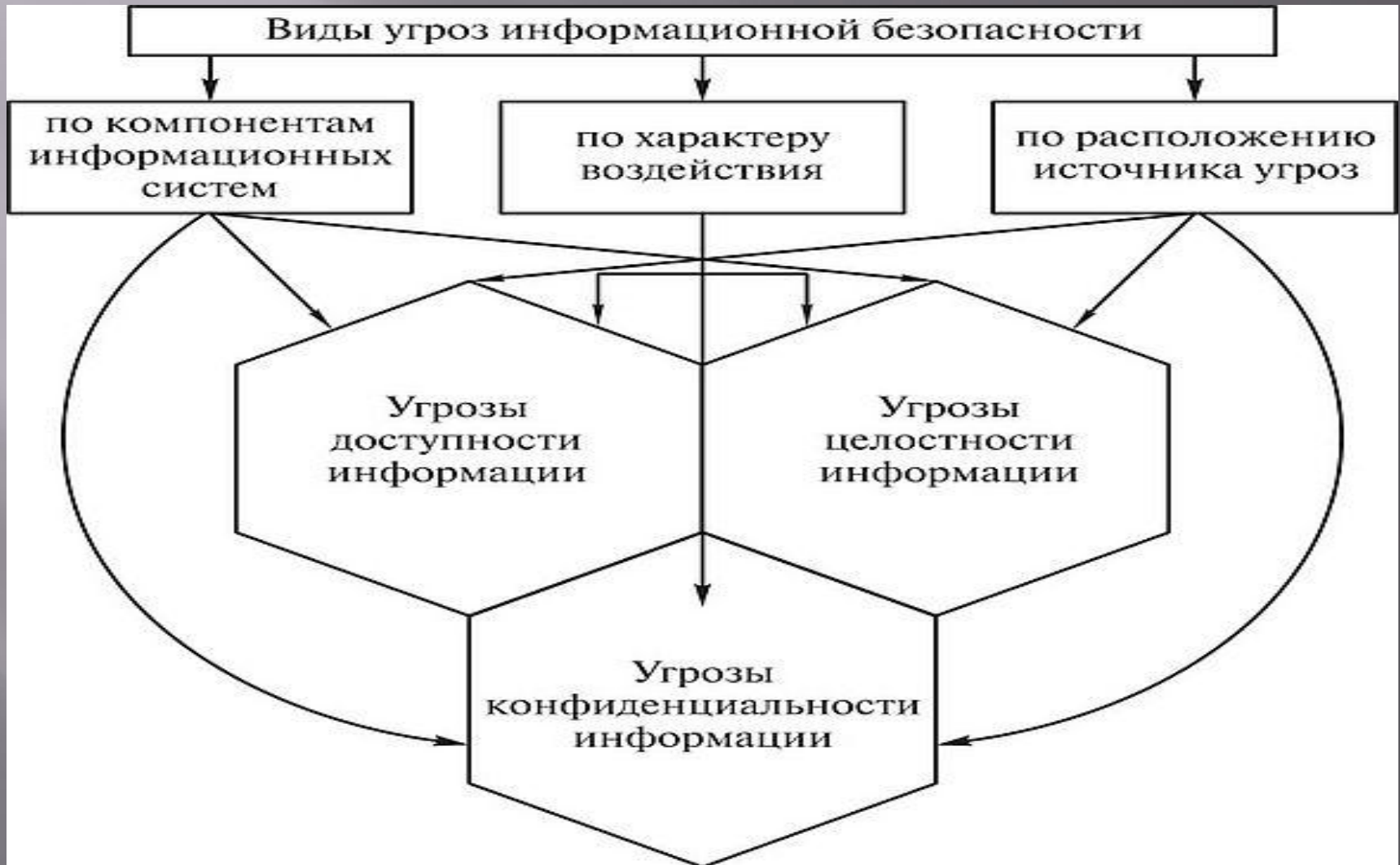
- **Угроза информационной безопасности (ИБ)** – потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам.
- Попытка реализации угрозы называется **атакой**.
- Классификация угроз ИБ можно выполнить по нескольким критериям:
  - **по аспекту ИБ** (доступность, целостность, конфиденциальность);
  - **по компонентам ИС**, на которые угрозы нацелены (данные, программа, аппаратура, поддерживающая инфраструктура);
  - **по способу осуществления** (случайные или преднамеренные действия природного или техногенного характера);
  - **по расположению источника угроз** (внутри или вне рассматриваемой ИС).



# Типы угроз

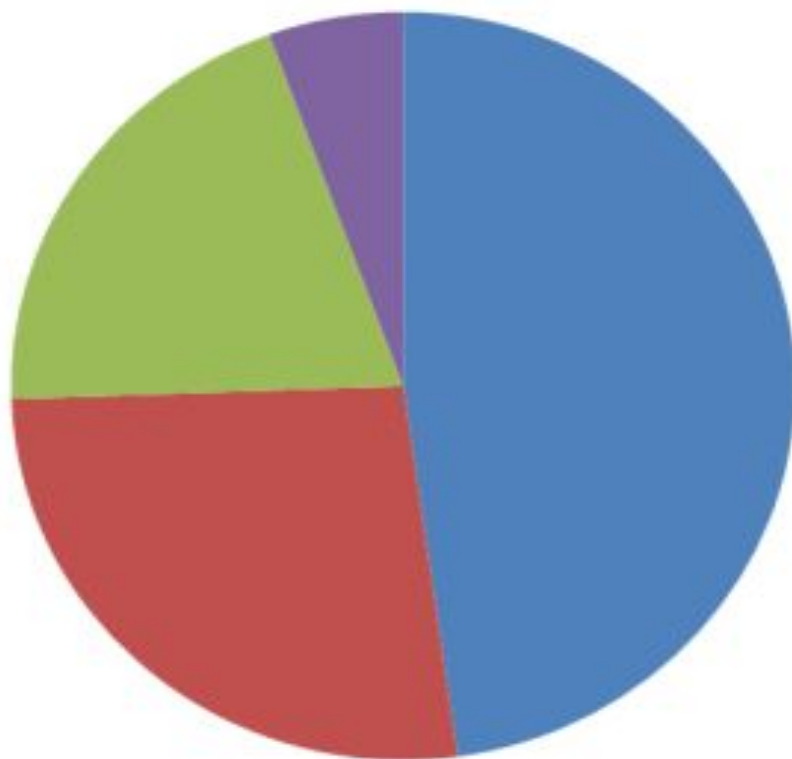


# Виды угроз



# Процентное соотношение

## угрозы информационной безопасности



- разглашение информации в результате подкупа работников 43%
- копирование программ и данных 24%
- проникновение в ПЭВМ 18%
- подслушивание переговоров 5%

# Источники угроз

## Классификация угроз по расположению источника угроз

8

- Ко внешним угрозам относятся вирусы шпионские программы , DoS-атаки (атаки с на «отказ в обслуживании» и др. Любые угрозы со стороны внешнего нарушителя, не работающего в компании.
- Ко внутренним угрозам информационной безопасности относятся случайные или намеренные утечки конфиденциальных корпоративных данных, нецелевое (в том числе и в криминальных целях) использование корпоративных ресурсов, намеренное нарушение работы ИС и поддерживающей инфраструктуры, кража и порча носителей информации и т.д. Любые угрозы со стороны внутреннего нарушителя (сотрудника или бывшего сотрудника организации).

Инсайдер – внутренний нарушитель, собственный сотрудник, нашедший способы прохождения всех рубежей авторизации и получивший санкционированный доступ к корпоративной информации за пределами своей компетенции.



# Методы защиты



# Правовая защита



## Структура правовой защиты информации



### Правовая защита информации

Специальные правовые акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе

#### Международное право

Декларации  
Патенты  
Авторские права  
Лицензии

#### Внутригосударственное право

##### Государственные

Конституция  
Законы  
Указы  
Постановления

##### Ведомственные

Приказы  
Руководства  
Положения  
Инструкции ит.д.

# Объекты защиты



# Что защищать?



**Сведения, составляющие государственную тайну**



**Персональные данные**



**Сведения, составляющие коммерческую тайну**



**научно-техническая и технологическая информация, связанная с деятельностью учреждения**



**деловая информация, отражающая деятельность учреждения**



# Что защищать?

## О Б Ъ Е К Т Ы    З А Щ И Т Ы

**Информация** - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

**Документированная информация** (документ) - зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

**Информационная система** (ИС) - организационно упорядоченная совокупность документов (массивов документов и информационных технологий, в том числе с использованием СВТ и связи) реализующих информационные процессы (процессы сбора, обработки, распространения).

**Информационные ресурсы** (ИР) - отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах);

**Общедоступные**

**Доступ к которым запрещено  
ограничивать законом**

**Документы  
ограниченного доступа  
по условиям правового режима**

1. Информация, составляющая **государственную тайну** (определяется законом О государственной тайне)

2 **Конфиденциальная информация** (виды тайн, определенные Указом Президента РФ №188)

# Кого защищать?

## СУБЪЕКТЫ ЗАЩИТЫ

*собственник* информационных ресурсов, информационных систем, технологий и средств их обеспечения - субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения указанными объектами;

*владелец* информационных ресурсов, информационных систем, технологий и средств их обеспечения - субъект, осуществляющий владение и пользование указанными объектами и реализующий полномочия распоряжения в пределах, установленных законом;

*пользователь (потребитель)* информации - субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.

# Как защитить?

## Способы защиты информации

---

**Маскировка** – способ защиты информации путем ее криптографического шифрования.

**Регламентация** – заключается в разработке и реализации комплексов мероприятий, создающих такие условия при которых возможности несанкционированного доступа к защищаемой информации сводились бы к минимуму.

**Принуждение** – пользователи и персонал вынуждены соблюдать правила обработки и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.



# Виды и методы

## Виды и методы защиты информации

### Вид защиты

От преднамеренного искажения, вандализма (компьютерных вирусов)

От несанкционированного (нелегального) доступа к информации (её использования, изменения, распространения)

### Метод защиты

- Общие методы защиты информации;
- профилактические меры;
- использование антивирусных программ

- Шифрование;
- паролирование;
- «электронные замки»;
- совокупность административных и правоохранительных мер





# Методы обеспечения

## Теоретические методы

1. Формализация разного рода процессов, связанных с обеспечением информационной безопасности
2. Строгое обоснование корректности и адекватности функционирования систем обеспечения информационной безопасности при проведении анализа их защищенности

## Правовые и организационные методы

Создание нормативной базы для организации различного рода деятельности, связанной с обеспечением информационной безопасности

## Методы обеспечения информационной безопасности

## Сервисы сетевой безопасности

1. Идентификация и аутентификация
2. Разграничение доступа
3. Протоколирование и аудит
4. Средства защиты периметра
5. Криптографические средства защиты

## Инженерно-технические методы

Защита информации от утечки по техническим каналам

# Объекты информационной безопасности

**К объектам, которым следует обеспечить информационную безопасность, относятся:**

- Информационные ресурсы;
- Система создания, распространения и использования информационных ресурсов;
- Информационная инфраструктура общества (информационные коммуникации, сети связи, центры анализа и обработки данных, системы и средства защиты информации);
- Средства массовой информации;
- Права человека и государства на получение, распространение и использование информации;
- Защита интеллектуальной собственности и конфиденциальной информации

# Понятия ИБ

## Понятия информационной безопасности: что защищать?





# Принципы защиты

## **Принцип непрерывности совершенствования и развития системы информационной безопасности.**

Суть принципа заключается в постоянном контроле функционирования системы, выявлении слабых мест, потенциально возможных каналов утечки информации и ИСП, обосновании и доводении механизмов защиты с учетом изменения характера внутренних и внешних угроз, обосновании и реализации на этой основе наиболее рациональных методов, способов и путей защиты информации.

**Обеспечение информационной безопасности не может быть одноразовым актом !!!.**

## **Принцип комплексного использования**

**всего арсенала** имеющихся средств защиты **во всех структурных элементах** производства и **на всех этапах технологического цикла** обработки информации.

Комплексный характер защиты информации проистекает, прежде всего, из характера действий злоумышленников, стремящихся любой совокупностью средств добыть важную для конкурентной борьбы информацию.

**Оружие защиты должно быть адекватно оружию нападения !!!.**



# Основные требования

## Требования к системе защиты информации:

- **централизованность**; процесс управления *всегда централизован*, в то время как *структура системы*, реализующей процесс, должна *соответствовать структуре защищаемого объекта*;
- **плановость**; планирование осуществляется *для организации взаимодействия* подразделений объекта *в интересах реализации принятой политики безопасности*; каждая служба, отдел, направление разрабатывают детальные планы защиты информации в сфере своей компетенции с учетом общей цели организации;
- **конкретность и целенаправленность**; защите подлежат абсолютно конкретные информационные ресурсы, могущие представлять интерес для конкурентов;
- **активность**; защищать информацию необходимо с достаточной степенью настойчивости и целеустремленности. Это требование предполагает наличие в составе системы информационной безопасности *средств прогнозирования, экспертных систем и других инструментариев*, позволяющих реализовать наряду с принципом *“обнаружить и устранить”* принцип *“предвидеть и предотвратить”*;
- **надежность и универсальность**, охват всего технологического комплекса информационной деятельности объекта; методы и средства защиты должны надежно перекрывать все возможные каналы утечки информации и противодействовать способам несанкционированного доступа независимо от формы представления информации, языка ее выражения и вида носителя, на котором она закреплена;
- **нестандартность** (по сравнению с другими организациями), разнообразие средств защиты;
- **открытость** для изменения и дополнения мер обеспечения безопасности информации;
- **экономическая эффективность**; затраты на систему защиты не должны превышать размеры возможного ущерба.

# Моделирование ИБ

- Исследование информационной безопасности существующими в науке методами моделирования следует рассматривать как процесс объективно обусловленный, имеющий целью разработать научное обеспечение для концепции информационной безопасности как составляющей национальной безопасности и путем внедрения новых информационных технологий повысить результативность деятельности по ее реализации.

# Исследование операций

- ▣ Исследование операций — применение математических, количественных методов для обоснования решений во всех областях целенаправленной человеческой деятельности. Исследование операций начинается тогда, когда для обоснования решений применяется тот или другой математический аппарат.
- ▣ *Цель исследования операций — предварительное количественное обоснование оптимальных решений с опорой на показатель эффективности. Само принятие решения выходит за рамки исследования операций и относится к компетенции ответственного лица (лиц).*



# Методы обеспечения ИБ

## Теоретические методы

1. Формализация разного рода процессов, связанных с обеспечением информационной безопасности
2. Строгое обоснование корректности и адекватности функционирования систем обеспечения информационной безопасности при проведении анализа их защищенности

## Правовые и организационные методы

Создание нормативной базы для организации различного рода деятельности, связанной с обеспечением информационной безопасности

## Методы обеспечения информационной безопасности

## Сервисы сетевой безопасности

1. Идентификация и аутентификация
2. Разграничение доступа
3. Протоколирование и аудит
4. Средства защиты периметра
5. Криптографические средства защиты

## Инженерно-технические методы

Защита информации от утечки по техническим каналам



# Теория игр - один из методов определения эффективного поведения.

- ▣ Обеспечение информационной безопасности с помощью теории игр.
- ▣ Для выбора средства эффективной защиты от различного рода атак можно использовать методы теории игр. Теория игр предполагает наличие продавца и покупателя. Взаимосвязь между ними определяется платежной матрицей. Матричная игра, в которой игрок взаимодействует с окружающей средой и решает задачу определения наиболее выгодного варианта поведения, называется статистической игрой.
- ▣ Игрок в таком случае – лицо, принимающее решение

# Информационная безопасность

