

# *Защита информации в современных ОС*

Тема 1. Основные понятия и положения защиты информации в информационно-вычислительных системах

**Под информационной безопасностью** будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

**Защита информации** – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

**Информационная безопасность** – многогранная область деятельности, в которой успех может принести только систематический, комплексный подход. Для решения данной проблемы рассматриваются меры законодательного, административного, процедурного и программно-технического уровня.



# Основные направления ИБ

```
graph TD; A[Основные направления ИБ] --> B[Доступность информации]; A --> C[Конфиденциальность информации]; A --> D[Целостность информации];
```

**Доступность  
информации**

**Конфиденциальность  
информации**

**Целостность  
информации**

# ПРЕДМЕТ ЗАЩИТЫ ИНФОРМАЦИИ

В законе РФ "Об информации, информатизации и защите информации" определено:

- "информационные ресурсы являются объектами собственности граждан, организаций, общественных объединений, государства";
- "информация – сведения о лицах, предметах, событиях, явлениях и процессах (независимо от формы их представления), отраженные на материальных носителях, используемые в целях получения знаний и практических решений".

Информация имеет ряд особенностей:

- не материальна;
- хранится и передается с помощью материальных носителей;
- любой материальный объект содержит информацию о самом себе либо о другом объекте.



## Свойства информации

- Ценность
- Достоверность
- Своевременность

**Предметом защиты** является информация, хранящаяся, обрабатываемая и передаваемая в компьютерных (информационных) системах.

*Особенностями данного вида информации являются:*

- двоичное представление информации внутри системы, независимо от физической сущности носителей исходной информации;
- высокая степень автоматизации обработки и передачи информации;
- концентрация большого количества информации в КС.

## ОБЪЕКТ ЗАЩИТЫ ИНФОРМАЦИИ

Объектом защиты информации является компьютерная (информационная) система или автоматизированная система обработки информации (АСОИ).

**Информационная система** – это организационно-упорядоченная совокупность информационных ресурсов, технических средств, технологий и персонала, реализующих информационные процессы в традиционном или автоматизированном режиме для удовлетворения информационных потребностей пользователей.

**Информационная безопасность АСОИ** – состояние рассматриваемой автоматизированной системы, при котором она, с одной стороны, способна противостоять дестабилизирующему воздействию внешних и внутренних информационных угроз, а с другой – ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды. *Информационная безопасность достигается проведением соответствующего уровня политики информационной безопасности.*

Под **политикой информационной безопасности** понимают совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты АСОИ от заданного множества угроз безопасности.

**Система защиты информации** – совокупность правовых норм, организационных мер и мероприятий, технических, программных и криптографических средств и методов, обеспечивающих защищенность информации в системе в соответствии с принятой политикой безопасности.



# ОСНОВНЫЕ ПОЛОЖЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

## Методика организации защитных мер

- определение состава средств информационной системы;
- анализ уязвимых элементов ИС;
- оценка угроз ;
- анализ риска

- Какие угрозы должны быть устранены и в какой мере?
- Какие ресурсы системы должны быть защищаемы и в какой степени?
- С помощью каких средств должна быть реализована защита?
- Какова должна быть полная стоимость реализации защиты и затраты на эксплуатацию с учетом потенциальных угроз?

Определение функций, процедур и средств безопасности, реализуемых в виде некоторых механизмов защиты.

## **ОСНОВНЫЕ ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АСОИ**

- Принцип системности
- Принцип комплексности
- Принцип непрерывности защиты
- Разумная достаточность
- Гибкость системы защиты
- Открытость алгоритмов и механизмов защиты
- Принцип простоты применения средств защиты



# Этапы развития концепций обеспечения безопасности данных

## **1 этап 1960 – 1970 гг.**

Попытки обеспечить безопасность данных чисто формальными механизмами, содержащими, главным образом, технические и программные средства. Сосредоточение программных средств в рамках операционных систем и систем управления базами данных

## **2 этап 1970 – 1976 гг.**

Развитие формальных механизмов защиты данных. Выделение управляющего компонента защиты данных – ядра безопасности. Развитие неформальных средств защиты. Формирование основ системного подхода к обеспечению безопасности данных

## **3 этап 1976 – 1990 гг.**

Дальнейшее развитие механизмов второго этапа. Формирование взгляда на обеспечение безопасности данных как на непрерывный процесс. Развитие стандартов на средства защиты данных. Усиление тенденции аппаратной реализации средств защиты данных. Формирование вывода о взаимосвязи обеспечения безопасности данных, архитектуры ИВС и технологии ее функционирования. Формирование системного подхода к проблеме обеспечения безопасности данных

## **4 этап 1990 г. – по настоящее время**

Дальнейшее развитие механизмов третьего этапа. Формирование основ теории обеспечения безопасности данных в ИВС. Разработка моделей, методов и алгоритмов управления защитой данных в ИВС

## **Вопросы**

1. Охарактеризуйте информацию и ее свойства.
2. Что является предметом и объектом защиты информации?
3. Чем определяется ценность информации? Приведите классификацию конфиденциальной информации.
4. Охарактеризуйте свойства достоверности и своевременности информации.
5. Дайте определения информационной безопасности АСОИ и политики информационной безопасности.