

# Основы информационной безопасности (ИБ)

**Безопасность информации  
(данных) — состояние  
защищенности информации  
(данных), при котором  
обеспечены её (их),  
*доступность,  
целостность,  
Конфиденциальность.***

**Защита информации** —  
комплекс мероприятий,  
направленных на обеспечение  
важнейших аспектов  
информационной безопасности

# Три главных аспекта (категории) ИБ

◆ **доступность информации** – возможность субъекта осуществлять определенные действия с информацией (избежание временного или постоянного сокрытия информации от пользователей, получивших права доступа);



# Три главных аспекта (категории) ИБ

◆ **целостность информации** – свойство сохранять свою структуру и содержание в процессе хранения, использования и передачи (избежание несанкционированной модификации информации).



# Три главных аспекта (категории) ИБ

◆ **конфиденциальность информации** – свойство информации быть доступной только ограниченному кругу пользователей, прошедших соответствующую проверку и допущенных к ее использованию.



# Другие категории ИБ

Выделяют и другие не всегда обязательные категории модели безопасности:

***аутентичность*** или ***подлинность*** —

возможность установления автора информации;

***неотказуемость*** или ***апеллируемость*** —

возможность доказать, что автором является именно заявленный человек, и никто другой;

ИБ по уровню применения разделяется на:

- ИБ предприятия
- личная ИБ
- ИБ государства

**Информационная безопасность организации** — состояние защищённости информационной среды организации, обеспечивающее её формирование, использование и развитие.



**Человек – член общества**

**Человек – живой организм**

Правовая  
безопасность

Защищенность систем  
жизнеобеспечения

**Информационная безопасность государства** — состояние сохранности информационных ресурсов государства и защищенности законных прав личности и общества в информационной сфере.

## Государственные органы РФ, контролирующие деятельность в области защиты информации:

- ❑ Комитет Государственной думы по безопасности;
- ❑ Совет безопасности России;
- ❑ Федеральная служба по техническому и экспортному контролю (ФСТЭК России);
- ❑ Федеральная служба безопасности Российской Федерации (ФСБ России);
- ❑ Служба внешней разведки Российской Федерации (СВР России);

## Государственные органы РФ, контролирующие деятельность в области защиты информации:

- ❑ Министерство обороны Российской Федерации (Минобороны России);
- ❑ Министерство внутренних дел Российской Федерации (МВД России);
- ❑ Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

## Службы, организующие защиту информации на уровне предприятия:

- ❑ Служба экономической безопасности;
- ❑ Служба безопасности персонала (Режимный отдел);
- ❑ Отдел кадров;
- ❑ Служба информационной безопасности.

# Классификация угроз

Угроза – потенциально возможное или реальное действие злоумышленников, способное нанести моральный или материальный ущерб.

## По объектам

Персонал  
Материальные и  
финансовые  
ценности

## По величине ущерба

Предельный  
Значительный  
Незначительный

## По ущербу

Материальный  
Моральный

## По причинам появления

Стихийные  
преднамеренные

## По вероятности возникновения

Весьма вероятные  
Вероятные  
Маловероятные

## По отношению к объекту

Внутренние  
Внешние

## По характеру воздействия

Активные  
Пассивные

# Классификация угроз информационной безопасности в зависимости от их источника

Природные угрозы	Угрозы техногенного характера	Угрозы, созданные людьми (антропогенные)
<ul style="list-style-type: none"><li>▪ <b>Магнитные бури</b></li><li>▪ <b>Радиоактивное излучение и осадки</b></li><li>▪ <b>другие</b></li></ul>	<ul style="list-style-type: none"><li>▪ <b>Отказы и сбои в работе аппаратно-программных средств</b></li><li>▪ <b>Электромагнитные излучения и наводки</b></li><li>▪ <b>Утечки через каналы связи: оптические, электрические, звуковые и т.д.</b></li><li>▪ <b>Другое</b></li></ul>	<ul style="list-style-type: none"><li>— <b>Преднамеренные и непреднамеренные действия:</b><ul style="list-style-type: none"><li>▪ <i>обслуживающего персонала</i></li><li>▪ <i>управленческого персонала</i></li><li>▪ <i>программистов</i></li><li>▪ <i>пользователей</i></li><li>▪ <i>архивной службы</i></li><li>▪ <i>службы безопасности</i></li></ul></li></ul>

- Отказы пользователей  
(непреднамеренные, намеренные)
- Отказ системы
- Сетевые атаки и прочее.

- ◆ **Утечка** — бесконтрольный выход КИ за пределы организации или круга лиц, которым, она была доверена.
- ◆ **Несанкционированный доступ** — это противоправное преднамеренное овладение КИ лицом, не имеющим права доступа к охраняемым секретам

## Угрозы конфиденциальной информации (КИ)

- ◆ **Разглашение** - это умышленные или неосторожные действия с КИ, приведшие к ознакомлению с КИ лиц, не допущенных к ней;
- ◆ **Модификация** информации в криминальных целях –частичное или значительное изменение состава и содержания сведений;
- ◆ **Разрушение** (уничтожение) информации - акт вандализма с целью прямого нанесения материального ущерба.

# Основные виды защищаемой информации

- государственная, коммерческая, служебная, банковская тайна;
- персональные данные
- интеллектуальная собственность.

# ***Классификация методов защиты информации в вычислительных системах***



**Правовая защита –  
специальные правовые акты,  
правила, процедуры и  
мероприятия,  
обеспечивающие защиту на  
правовой основе.**

**Организационные методы защиты информации обеспечивают организацию :**

♦ охраны, режима, работы с кадрами, с документами;

♦ работы по анализу внутренних и внешних угроз КИ и т.п.

**Физические средства защиты** — это разнообразные устройства, приспособления, конструкции, аппараты, изделия, предназначенные для создания препятствий на пути движения злоумышленников

- **средства предупреждения** (заборы вокруг объектов, укрепление стен, дверей и пр. )
- **средства обнаружения угроз** (охранная сигнализация и охранное телевидение)
- **системы ликвидации угроз** (средства пожаротушения)

различные технические конструкции, обеспечивающие пресечение разглашения, защиту от утечки и противодействие несанкционированному доступу к источникам КИ

- специальные регистры для хранения реквизитов защиты (паролей, кодов, грифов);
- генераторы кодов для автоматического генерирования идентифицирующего кода устройства;
- устройства измерения индивидуальных характеристик человека (голоса, отпечатков) с целью его идентификации;

## **Основные направления:**

- 1) защита информации от несанкционированного доступа;**
- 2) защита информации и программ от копирования, от вирусов;**
- 3) программная защита каналов связи.**

# Защита информации от несанкционированного доступа

1) **Идентификация** позволяет субъекту (пользователю, процессу) назвать себя (сообщить свое имя).

**Аутентификация** – подтверждение (проверка) подлинности. (**Аутентичность** — гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор. )

- 1) **Шифрование заменой** (подстановка). Символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов.
- 2) **Шифрование методом перестановки**. Символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов.
- 3) **Шифрование с использованием открытых ключей**. Для шифрования данных используется один ключ, он не является секретным. Для дешифровки используется другой ключ, он засекречен и не может быть выведен из ключа-шифровщика.

## ***4) Использование хэш-функций***

Хэш-функции отображают сообщение любой длины в строку фиксированного размера.

Особенностью ее применения является тот факт, что не существует функции, которая бы могла по сжато отображению восстановить исходное сообщение

**Электронная цифровая подпись  
(ЭЦП)— реквизит)— реквизит  
электронного документа,  
предназначенный для защиты  
данного электронного документа от  
подделки**

На этапе формирования цифровой подписи генерируется два ключа: секретный и открытый.

К документу добавляется подпись, содержащая:

- дату подписи;
- информацию об отправителе;
- имя открытого ключа.

Ко всему документу применяется хэш-функция, получается число. Это число шифруется закрытым ключом – это и есть **ЭЦП**.

Получателю пересылается документ и ЭЦП.

При проверке ЭЦП расшифровывается открытым ключом.

К полученному документу применяется преобразование хэш-функцией.

Результат сравнивается с присланной ЭЦП. Если оба числа совпадают, то полученный документ – подлинный.

**Электронный ключ** разграничивает права пользователей по использованию определяемых ключом ресурсов, но не контролирует поступающие на компьютер данные.

**Защищенным сеансом связи** называют ситуацию, когда обе стороны диалога могут быть уверены в авторстве и неизменности пересылаемых документов и конфиденциальности переписки. Такой сеанс связи достигается различными методами шифрования пересылаемых данных.

Наиболее популярным сегодня является несимметричное шифрование, когда каждая сторона имеет по два ключа шифрования (секретный и открытый). И отправка сообщений, и их чтение осуществляются своим секретным ключом и открытым ключом адресата.

Объединение локальных сетей и отдельных компьютеров через открытую внешнюю среду передачи информации в единую сеть, обеспечивающую безопасность циркулирующих данных, **называют защищенной виртуальной сетью.**

# Определения

**Несанкционированный доступ** – доступ к информации со стороны лиц, не имеющих разрешения на доступ к этой информации.

**Цифровая информация** – информация, хранение, передача и обработка которой осуществляются средствами ИКТ.

**Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.  
(ГОСТ Р 50922-2006 )**

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

# Два основных вида угроз для цифровой информации

## Кража (утечка)

- Копирование документов
- Кража документов
- Прослушивание телефонных разговоров
- Новые каналы утечки – компьютерные сети, сотовая связь

## Разрушение (уничтожение)

### Преднамеренное – несанкционированное

- Создание вирусов
- Деятельность хакеров (взломщиков информационных систем)

### Непреднамеренное

- Ошибки пользователя
- Сбой в работе оборудования
- Аварии и прочее

# Меры по защите информации отдельного пользователя ПК и группы пользователей



- ▶ Периодическое резервное копирование
- ▶ Регулярная антивирусная проверка
- ▶ Использование блока бесперебойного питания

## Меры по защите информации группы пользователей ПК



- ❖ Разграничение доступа для разных пользователей (создаются учетные записи, устанавливаются пароли)

# Меры по защите компьютера, подключенного к сети

❖ Использование защитных программ –  
**брандмауэров**

❖ Брандмауэры, защищающие сети,  
подключенные к другим сетям,  
называются **межсетевыми экранами**.

# Криптография и защита информации

Криптография – в переводе - тайнопись

Современные методы  
шифрования (криптографии)

```
graph TD; A[Современные методы шифрования (криптографии)] --> B[Симметричные (с закрытым ключом)]; A --> C[Асимметричные (с открытым ключом)];
```

Симметричные  
(с закрытым  
ключом)

Асимметричные  
(с открытым  
ключом)

**Закрытый ключ** – это ключ, которым обмениваются два абонента, ведущие секретную переписку. Это единый ключ, с помощью которого происходит как шифрование, так и дешифрование.

**Открытый ключ** – это алгоритм шифрования, который базируется на использовании отдельных шифровального (открытого) ключа и дешифровального (закрытого) ключа.

**Цифровая подпись** – это индивидуальный секретный шифр, ключ которого известен только владельцу.

Наличие цифровой подписи свидетельствует о том, что ее владелец подтвердил подлинность содержимого переданного сообщения.

**Цифровой сертификат** подтверждает, что открытый ключ действительно относится к владельцу подписи.

Криптография

Шифрование

Дешифрование

Открытый ключ

Закрытый ключ

Дешифрование

Шифрование

Цифровая подпись