

КЛАССИФИКАЦИЯ МЕР ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

ГРУППЫ МЕТОДОВ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

- 1) методы и средства организационно-правовой защиты информации;
- 2) методы и средства инженерно-технической защиты информации;
- 3) криптографические методы и средства защиты информации;
- 4) программно-аппаратные методы и средства защиты информации.

ОРГАНИЗАЦИОННО-ПРАВОВАЯ ЗАЩИТА

- ❖ организация режима и охраны;
- ❖ организация работы с сотрудниками;
- ❖ организация работы с документами и документированной информацией;
- ❖ организация использования технических средств сбора, обработки, накопления и хранения конфиденциальной информации;
- ❖ организация работы по анализу внутренних и внешних угроз конфиденциальной информации и выработке мер по обеспечению ее защиты;
- ❖ организация работы по проведению систематического контроля за работой персонала с конфиденциальной информацией, порядком учета, хранения и уничтожения документов и технических носителей.

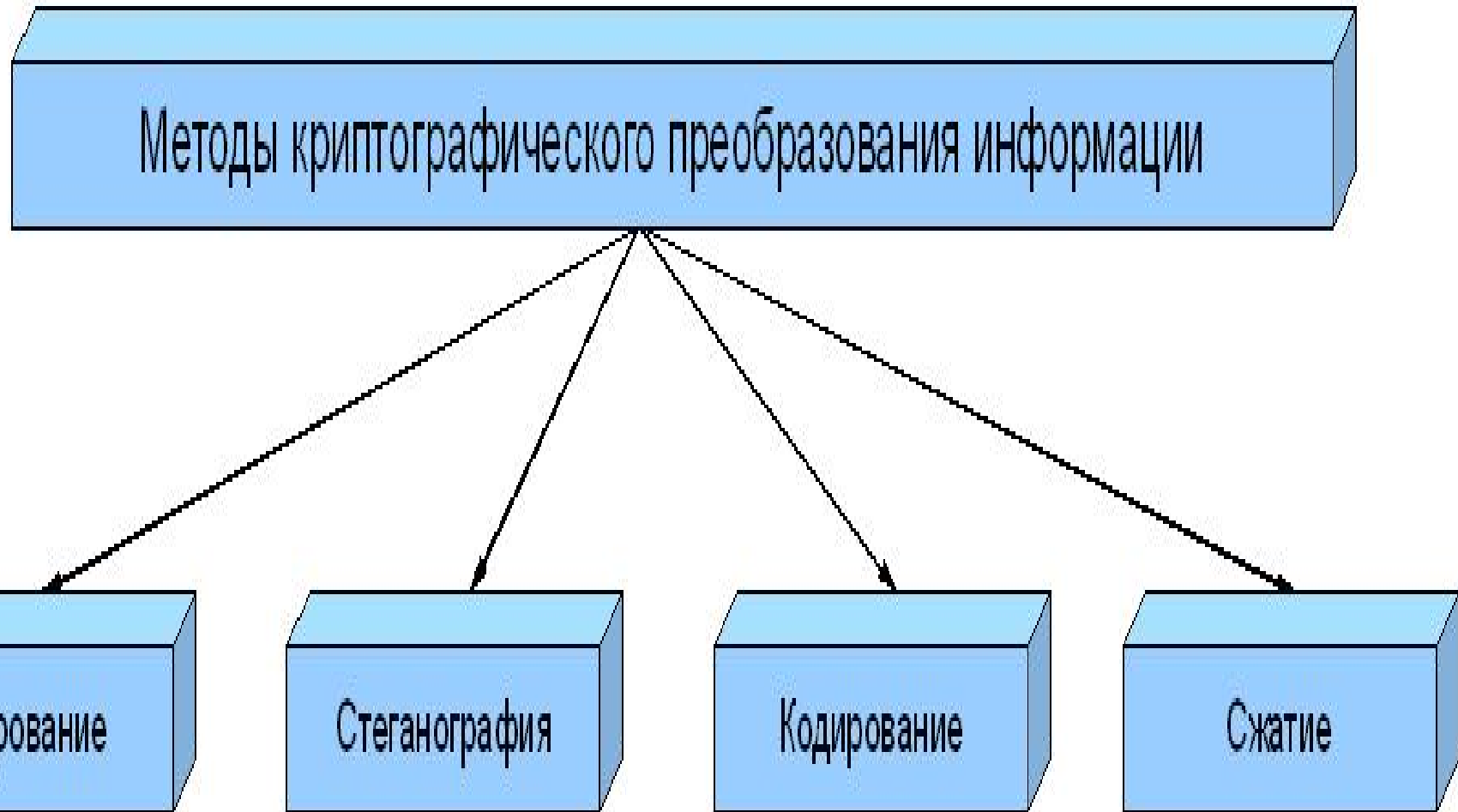
ИНЖЕНЕРНО-ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ

- 1) Для защиты периметра информационной системы создаются:
 - системы охранной и пожарной сигнализации;
 - системы цифрового видео наблюдения;
 - системы контроля и управления доступом (СКУД).
- 2) Защита информации от ее утечки техническими каналами связи обеспечивается следующими средствами и мероприятиями:
 - использованием экранированного кабеля и прокладка проводов и кабелей в экранированных конструкциях;
 - установкой на линиях связи высокочастотных фильтров;
 - построение экранированных помещений («капсул»);
 - использование экранированного оборудования;
 - установка активных систем зашумления;
 - создание контролируемых зон.

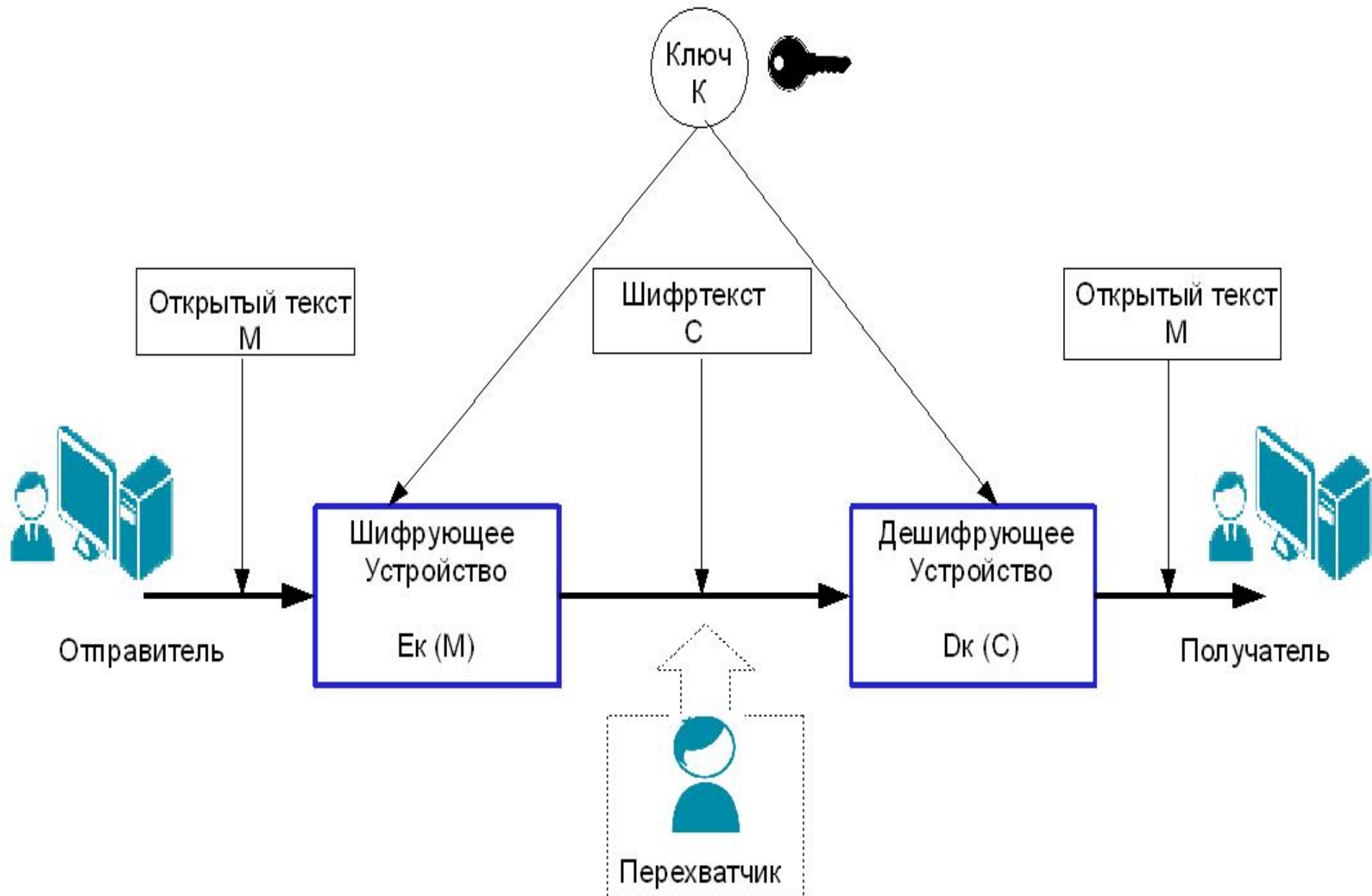
КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ

- 1) Специальные регистры для хранения реквизитов защиты: паролей, идентифицирующих кодов, грифов или уровней секретности;
- 2) Устройства измерения индивидуальных характеристик человека (голоса, отпечатков) с целью его идентификации;
- 3) Схемы прерывания передачи информации в линии связи с целью периодической проверки адреса выдачи данных.
- 4) Системы бесперебойного питания: источники бесперебойного питания, резервирование нагрузки, генераторы напряжения.

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ



КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ



АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ

- 1) Специальные регистры для хранения реквизитов защиты: паролей, идентифицирующих кодов, грифов или уровней секретности;
- 2) Устройства измерения индивидуальных характеристик человека (голоса, отпечатков) с целью его идентификации;
- 3) Схемы прерывания передачи информации в линии связи с целью периодической проверки адреса выдачи данных.
- 4) Системы бесперебойного питания: источники бесперебойного питания, резервирование нагрузки, генераторы напряжения.

СМАРТ-КАРТЫ



RFID-ИДЕНТИФИКАТОР



IBUTTON

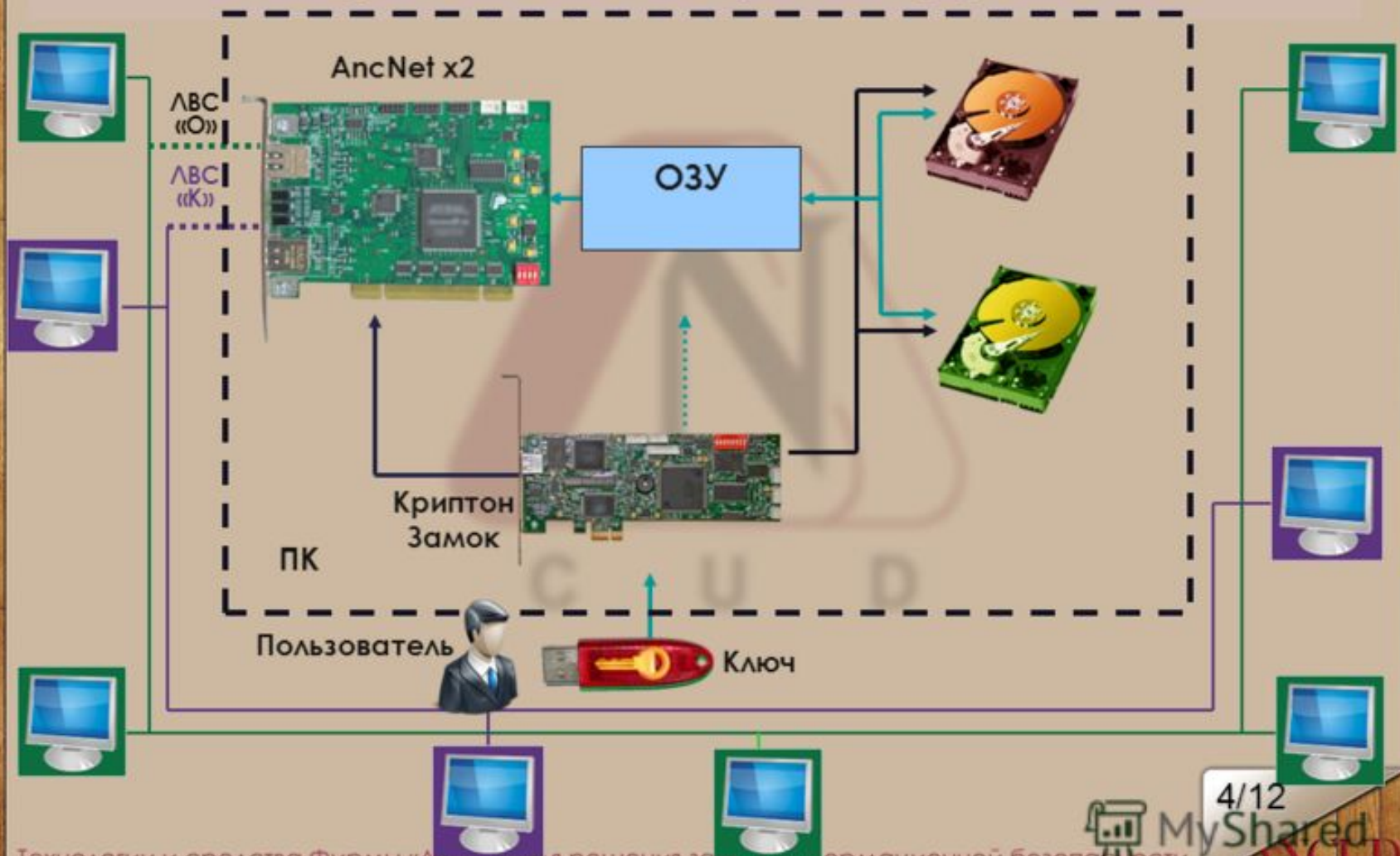


USB-TOKEN



КРИПТОН-Замок/РСИ

Структура аппаратно-программных средств ПК для работы конфиденциальной и открытой информации



СЗИ «Страж NT»



РЕГИСТРАЦИЯ ПОЛЬЗОВАТЕЛЯ В СИСТЕМЕ

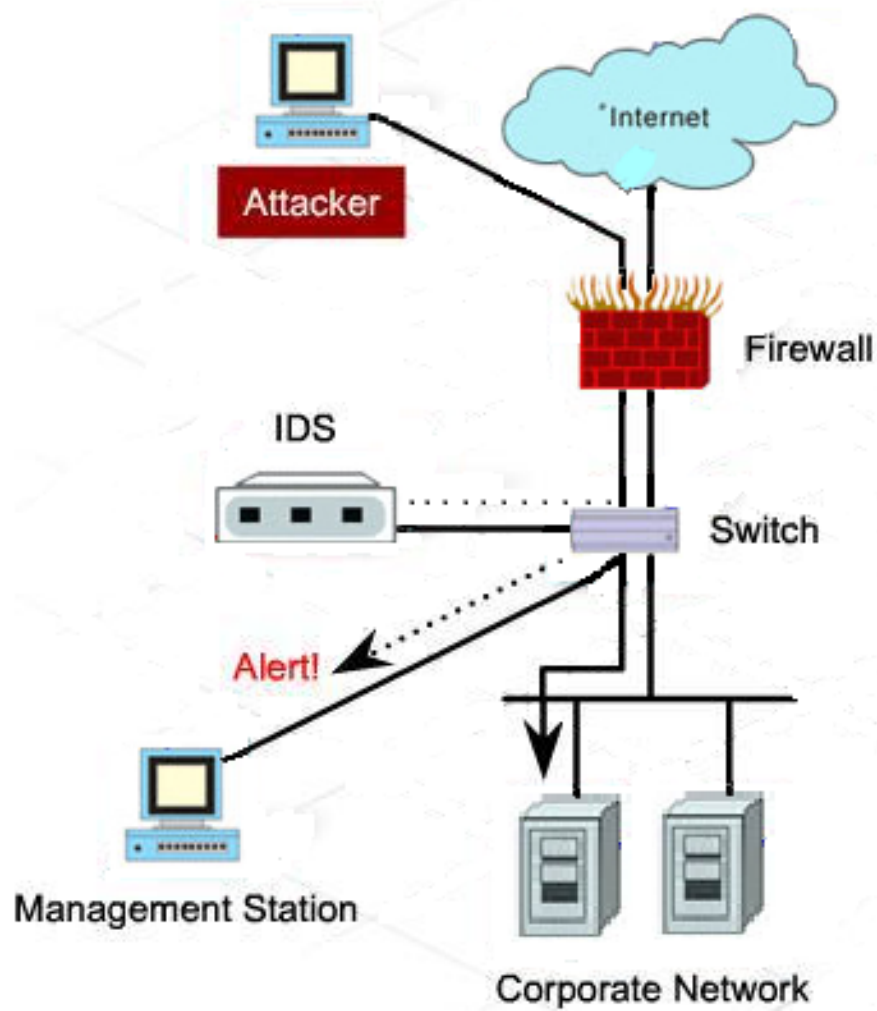
- 1) **Идентификация** — это называние лицом себя системе;
- 2) **Аутентификация** — это установление соответствия лица названному им идентификатору;
- 3) **Авторизация** — предоставление этому лицу возможностей в соответствии с положенными ему правами или проверка наличия прав при попытке выполнить какое-либо действие

ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ

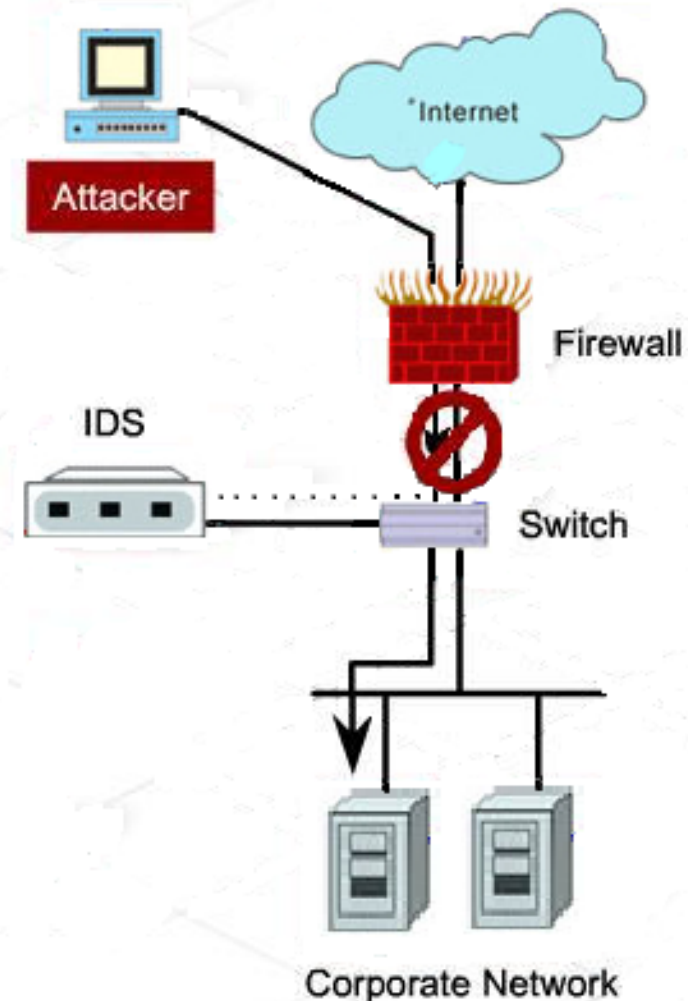
- 1) Средства защиты от несанкционированного доступа (НСД):
 - ✓ Мандатное управление доступом;
 - ✓ Избирательное управление доступом;
 - ✓ Управление доступом на основе ролей;
 - ✓ Журналирование (так же называется Аудит).
- 2) Системы анализа и моделирования информационных потоков (CASE-системы).
- 3) Системы мониторинга сетей:
 - ✓ Системы обнаружения и предотвращения вторжений (IDS/IPS).
 - ✓ Системы предотвращения утечек конфиденциальной информации (DLP-системы).
- 4) Анализаторы протоколов.
- 5) Антивирусные средства.

СИСТЕМЫ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ (IDS/IPS)

Intrusion Detection System



Intrusion Prevention System



ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ

- 1) Межсетевые экраны.
- 2) Криптографические средства:
 - ✓ Шифрование;
 - ✓ Цифровая подпись.
- 3) Системы резервного копирования.
- 4) Программные системы аутентификации:
 - ✓ Пароль;
 - ✓ Ключ доступа (физический или электронный);
 - ✓ Сертификат;
 - ✓ Биометрия.
- 5) Инструментальные средства анализа систем защиты:
 - ✓ Мониторинговый программный продукт.

КОМПОНЕНТЫ АНТИВИРУСОВ

- Антивирусный монитор\проактивная защита\контроль программ
- Антивирусный сканер.
- Веб-экран\брандмауэр\фаервол\атихакер.
- Модуль защиты электронной\антиспам.
- Контроль доступа к устройствам.
- Безопасные платежи.
- Антибанер.
- Анализ уязвимостей.

ПРИМЕРЫ АНТИВИРУСОВ