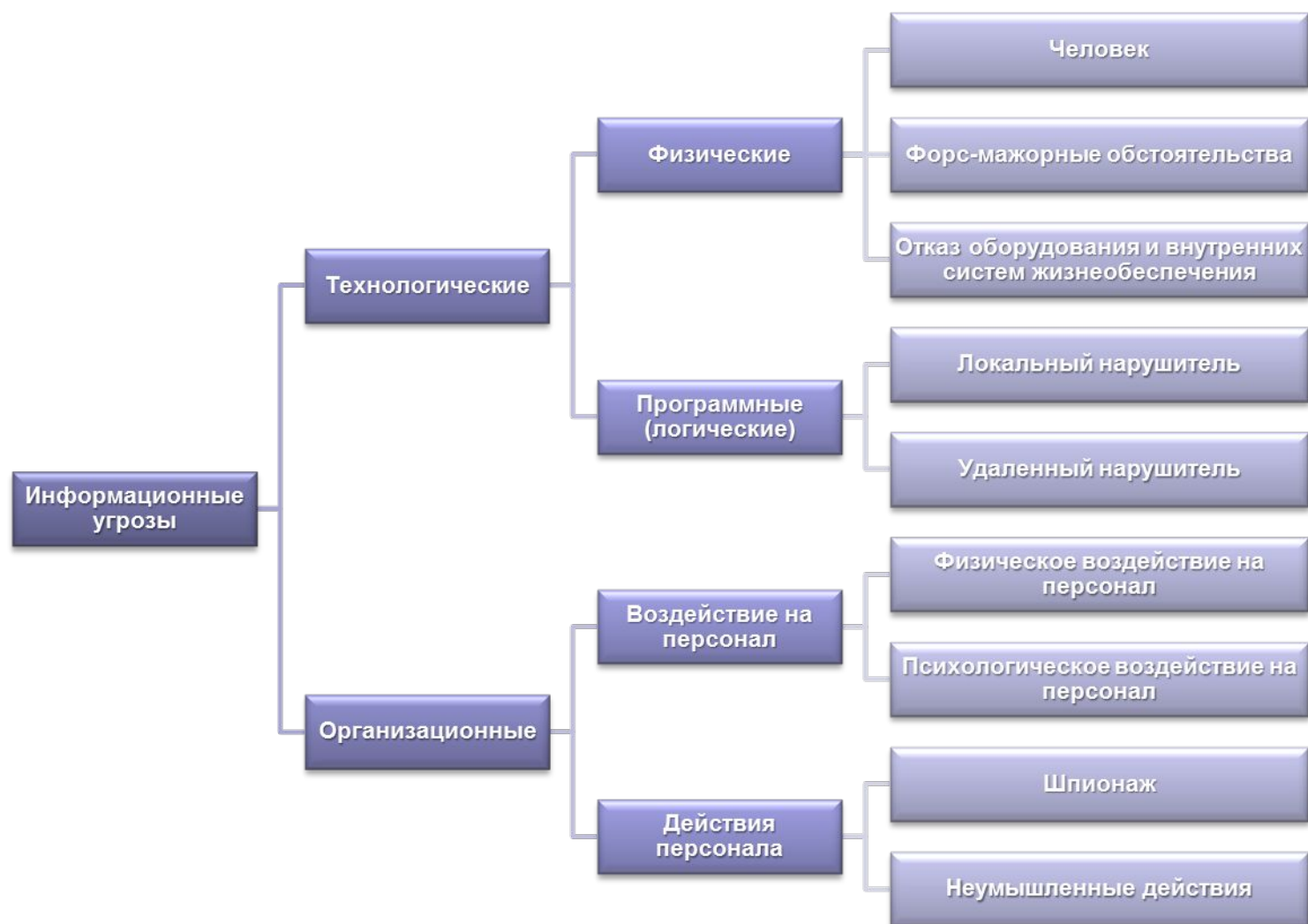


Виды информационных угроз



Организационная защита

- **организация режима и охраны.**
- **организация работы с сотрудниками** (подбор и расстановка персонала, включая ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и др.)
- **организация работы с документами** и документированной информацией (разработка, использование, учет, исполнение, возврат, хранение и уничтожение документов и носителей конфиденциальной информации)
- **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.

Технические средства защиты информации

Для защиты периметра информационной системы создаются:

- системы охранной и пожарной сигнализации;
- системы цифрового видео наблюдения;
- системы контроля и управления доступом (СКУД).

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.

Аппаратные средства защиты информации

- Специальные регистры для хранения реквизитов защиты: паролей, идентифицирующих кодов, грифов или уровней секретности;
- Устройства измерения индивидуальных характеристик человека (голоса, отпечатков) с целью его идентификации;
- Схемы прерывания передачи информации в линии связи с целью периодической проверки адреса выдачи данных.
- Устройства для шифрования информации (криптографические методы).
- Системы бесперебойного питания:
 - Источники бесперебойного питания;
 - Резервирование нагрузки;
 - Генераторы напряжения.

Программные средства защиты информации

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

Программные средства защиты информации

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