Обеспечение информационной безопасности

- Обеспечение безопасности информации в КИС подразумевает не просто внедрение каких-то средств защиты, а грамотное и последовательное построение подсистем, входящих в систему обеспечения безопасности информации (СОБИ), причем само построение должно осуществляться в соответствии с результатами анализа актуальных угроз безопасности информации, комплексным подходом при проектировании СОБИ и учитывать необходимость централизованного управления средствами защиты информации.
- СОБИ должна строиться как иерархическая, многоуровневая система.
- Комплексный подход, применяемый при построении СОБИ, предусматривает наличие нескольких уровней защиты, которые определяют требования по обеспечению безопасности информации на всех этапах ее обращения в КИС: технологического, пользовательского, сетевого и канального.

Подсистемы системы информационной безопасности

- **Подсистема поддержки доверенной информационной среды** (ДИС) предназначена для поддержания целостной программно-аппаратной среды КИС, обеспечения гарантий доверительности пользователей КИС к предоставляемой системой информации и сервисам.
- **Подсистема аутентификации и идентификации** предназначена для проведения процедур аутентификации/идентификации сетевых сущностей, входящих в состав КИС, на всех этапах обработки и обращения информации в КИС. Подсистема тесно взаимодействуете подсистемой контроля доступа.

Подсистемы системы информационной безопасности

- **Подсистема контроля доступа** предназначена для управления и контроля за доступом пользователей к АРМ, серверам, прикладным системам, системным и сетевым сервисам и др., входящим в состав КИС, на базе многоуровневой Политики безопасности.
- **Подсистема защиты потоков** предназначена для создания доверенных каналов связи между структурными составляющими КИС.
- **Подсистема аудита и регистрации** осуществляет сбор и хранение информации об общем состоянии программных и технических компонентов, функционирующих отдельно или входящих в состав подсистем безопасности, и предназначена для предварительного анализа данной информации.

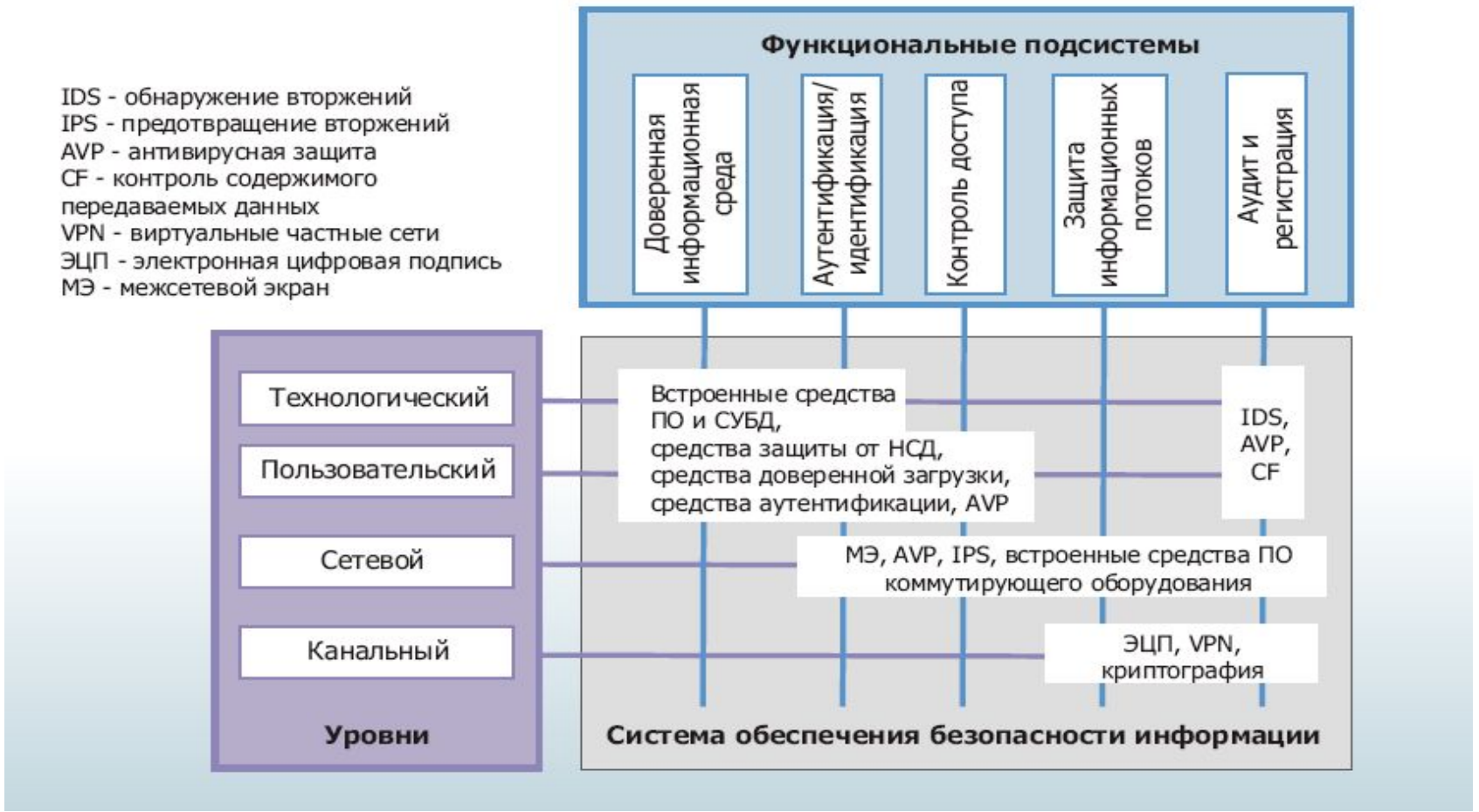
Подсистемы системы информационной безопасности

- **Подсистема управления** - ключевая подсистема СОБИ, предназначенная для оперативного управления как отдельными составляющими СОБИ, так и системой в целом, в соответствии с Политикой безопасности.
- Подсистема включает в себя такие механизмы, как анализ информации с консолей мониторинга средств защиты, система поддержки принятия решения об оперативном усилении/ослаблении политики безопасности в отдельных элементах или узлах СОБИ и противодействия внешним и внутренним атакам, управление отдельными средствами и комплексами защиты информации и др.

Наборы подсистем защиты

- СОБИ для каждой организации представляет собой различный набор подсистем (решений), который не является стандартным и различен в зависимости от бизнес-задач, решаемых КИС. Однако можно выделить несколько базовых подсистем, составляющих СОБИ корпоративной информационной системы практически любой организации:
  - Подсистема безопасного подключения корпоративной сети к Интернет
  - Подсистема защиты корпоративной электронной почты
  - Подсистема защиты от вредоносных программ и компьютерных вирусов
  - Подсистема защиты внутренних и внешних информационных потоков
  - Подсистема предотвращения вторжений
  - Подсистема защиты информации персональных компьютеров от НСД
  - Подсистема контроля целостности программной среды
  - Подсистема резервного копирования и восстановления данных

Функциональные подсистемы защиты



Идентификация и аутентификация

- Идентификация и аутентификация – основа программно-технических средств ИБ.
- Идентификация позволяет субъекту указать свое имя в ИС.
- Аутентификация является мерой подтверждения введенного идентификатора.
- Аутентификация бывает односторонней (клиент доказывает подлинность серверу) или двусторонней (взаимной).

Парольная аутентификация

- Использование пароля при идентификации субъекта
- **Достоинства**: простота и удобства для человека
- **Недостатки**: обеспечивается слабая защита

Парольная защита

- Меры по обеспечению надежности парольной защиты:
  - Наложение технических ограничений (длина пароля, алфавит пароля)
  - Управление сроком действия пароля, их периодическая смена
  - Ограничение доступа к файлу паролей
  - Ограничение числа неудачных попыток входа в систему
  - Обучение пользователей
  - Использование программных средств генерации паролей