«Методы защиты межсетевого обмена данными»

Вопросы темы:

1. Удаленный доступ. Виды коммутируемых линий.
2. Основные понятия и виды виртуальных частных сетей.
3. Классификация сетей VPN
4. Основные варианты архитектуры VPN

1. Удаленный доступ. Виды коммутируемых линий.

Различают два основных вида удаленного доступа:

- – **соединение по коммутируемой линии** (dial-up connection);
- – **соединение с использованием виртуальных частных сетей** (Virtual Private Networks, VPN).

Виды коммутируемых линий

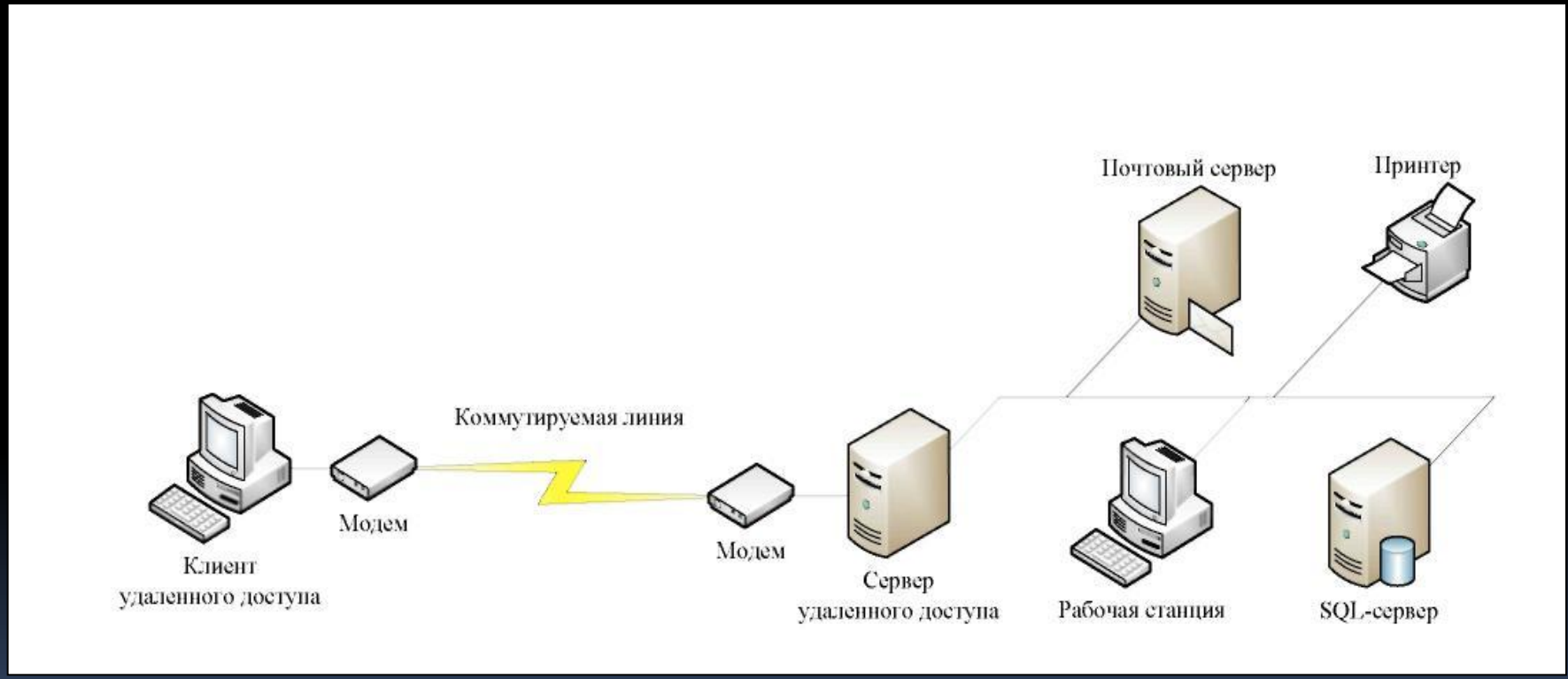
- Телефонные сети
- Сети ISDN (Integrated Services Digital Network – цифровая сеть с комплексными услугами)
- ATM поверх ADSL – передача трафика ATM (Asynchronous Transfer Mode – асинхронный режим передачи) посредством линий ADSL (Asymmetric Digital Subscriber Line – асимметричная цифровая абонентская линия).

Протоколы удаленного доступа

Подключение клиента к серверу удаленного доступа по коммутируемым линиям состоит из следующих основных этапов:

- установка соединения;
- аутентификация и авторизация клиента удаленного доступа;

Подключение клиента к серверу удаленного доступа по коммутируемым линиям



Протоколы удаленного доступа

- протокол SLIP
- протокол PPP

Соединение «точка-точка» устанавливается в четыре этапа:

1. Настройка параметров канального уровня.
2. Аутентификация клиента.
3. Обратный вызов (callback).
4. Настройка протоколов верхних уровней.

Протоколы аутентификации

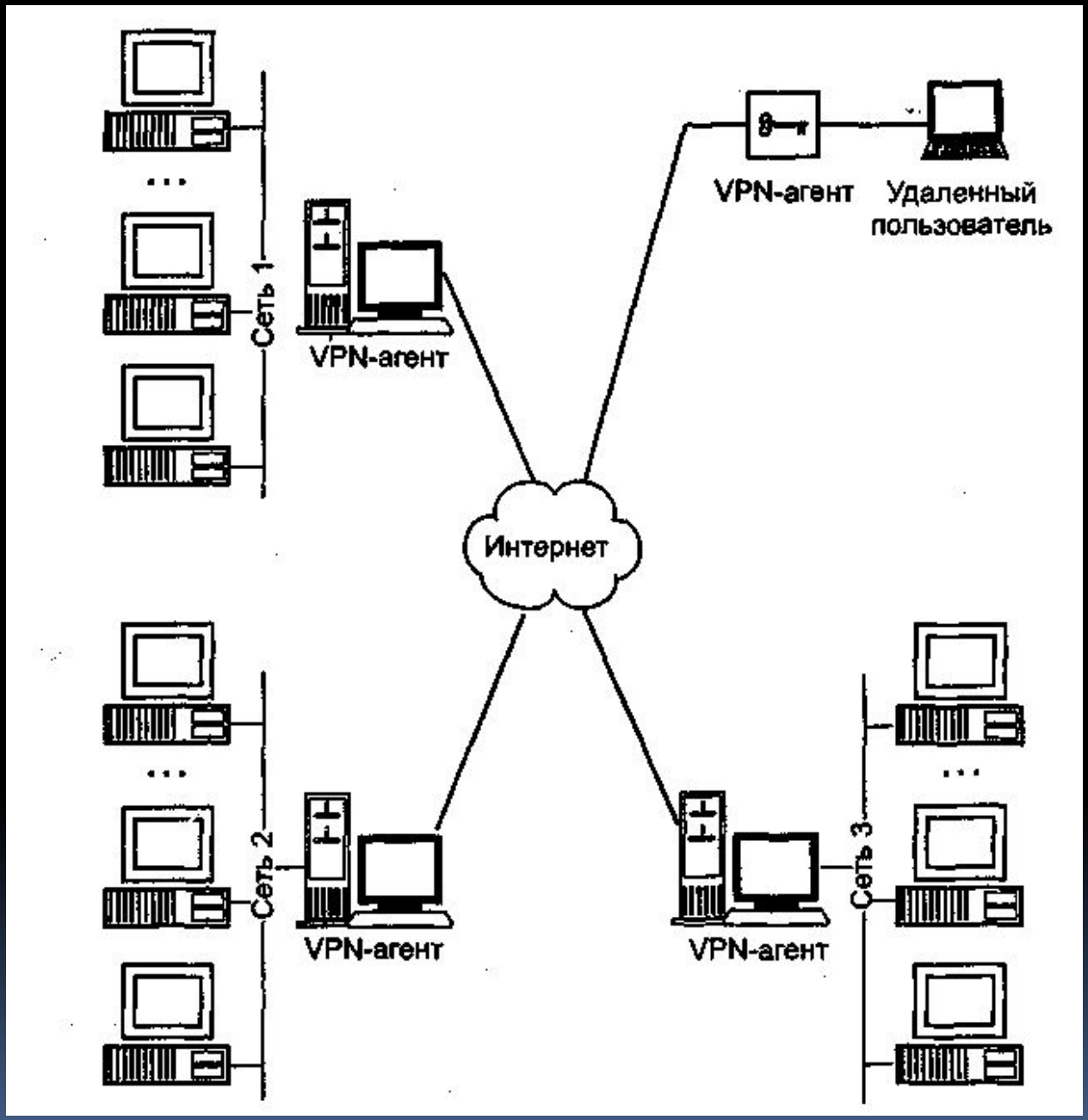
- PAP (Password Authentication Protocol) – протокол аутентификации по паролю
- CHAP (Challenge Handshake Authentication Protocol) – протокол аутентификации с предварительным согласованием вызова
- MS-CHAP (Microsoft Challenge Handshake Authentication Protocol)
- MS-CHAP v2
- EAP (Extensible Authentication Protocol) – расширяемый протокол аутентификации

2. Основные понятия и виды виртуальных частных сетей

Virtual Private Network, VPN – это защищенное соединение двух узлов через открытые сети,

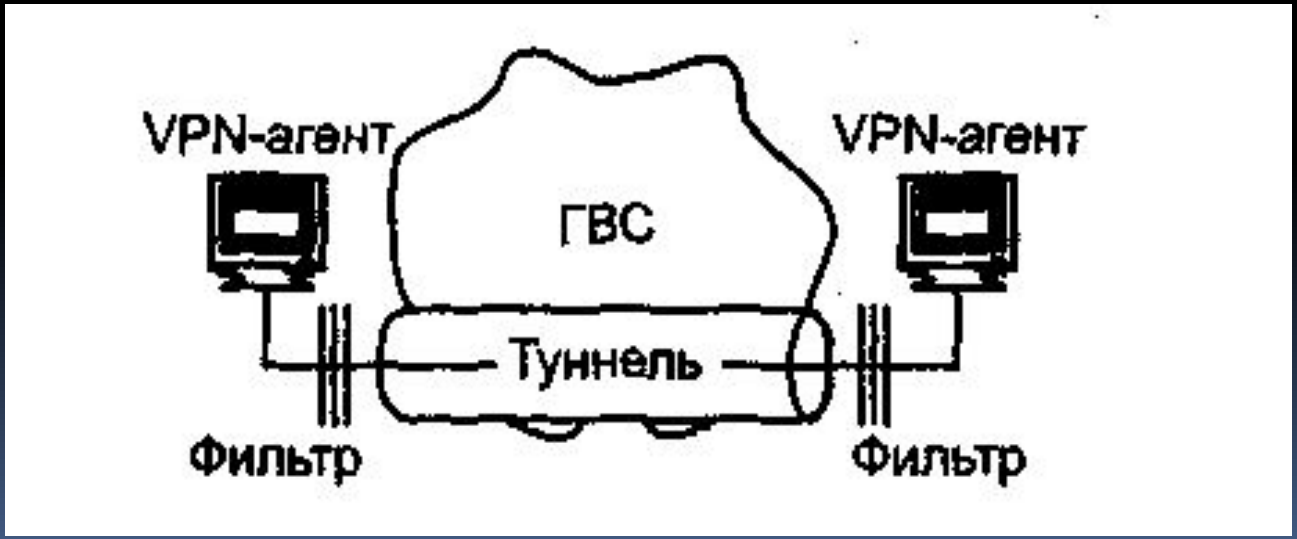
при котором организуется виртуальный канал, обеспечивающий безопасную передачу информации,

а узлы, связанные VPN, могут работать так, как будто соединены напрямую.

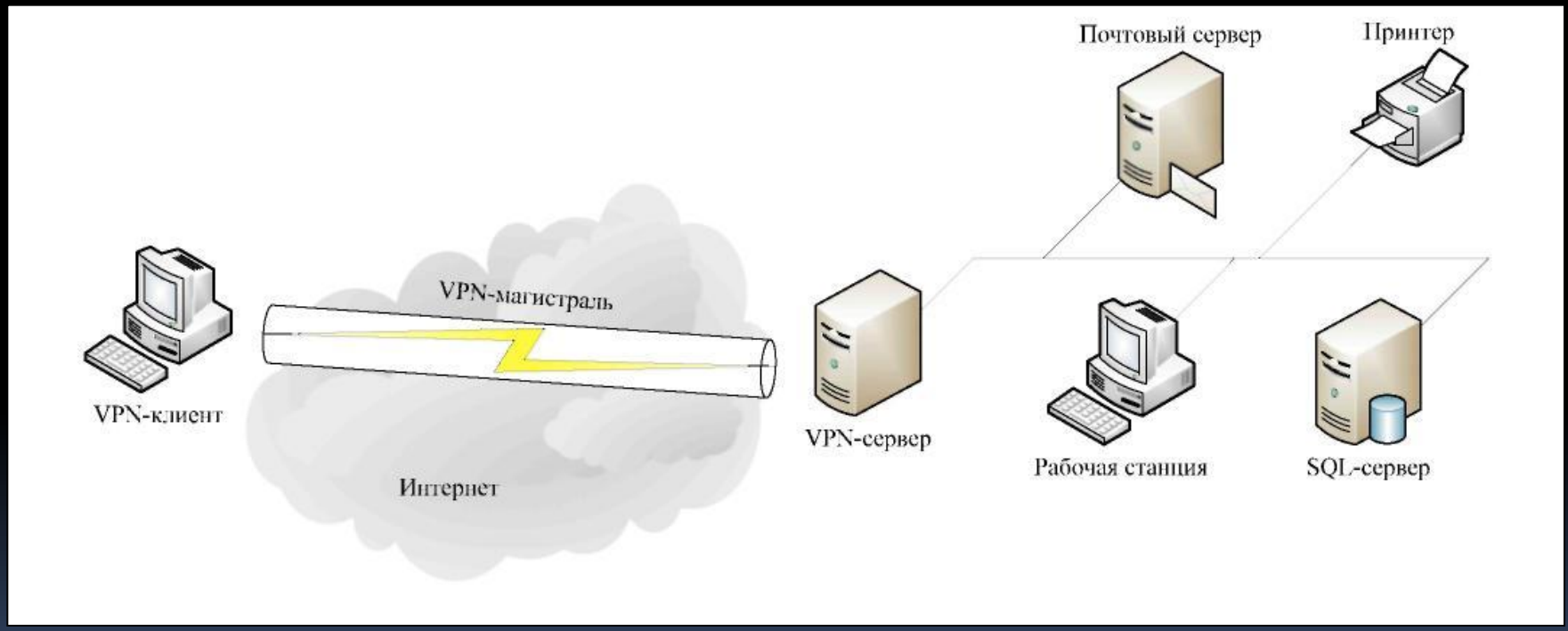

Сеть 1
VPN-агент
VPN-агент
Удаленный пользователь
Интернет
Сеть 2
VPN-агент
VPN-агент
Сеть 3

VPN - это совокупность сетей, на внешнем периметре которых установлены VPN-агенты.

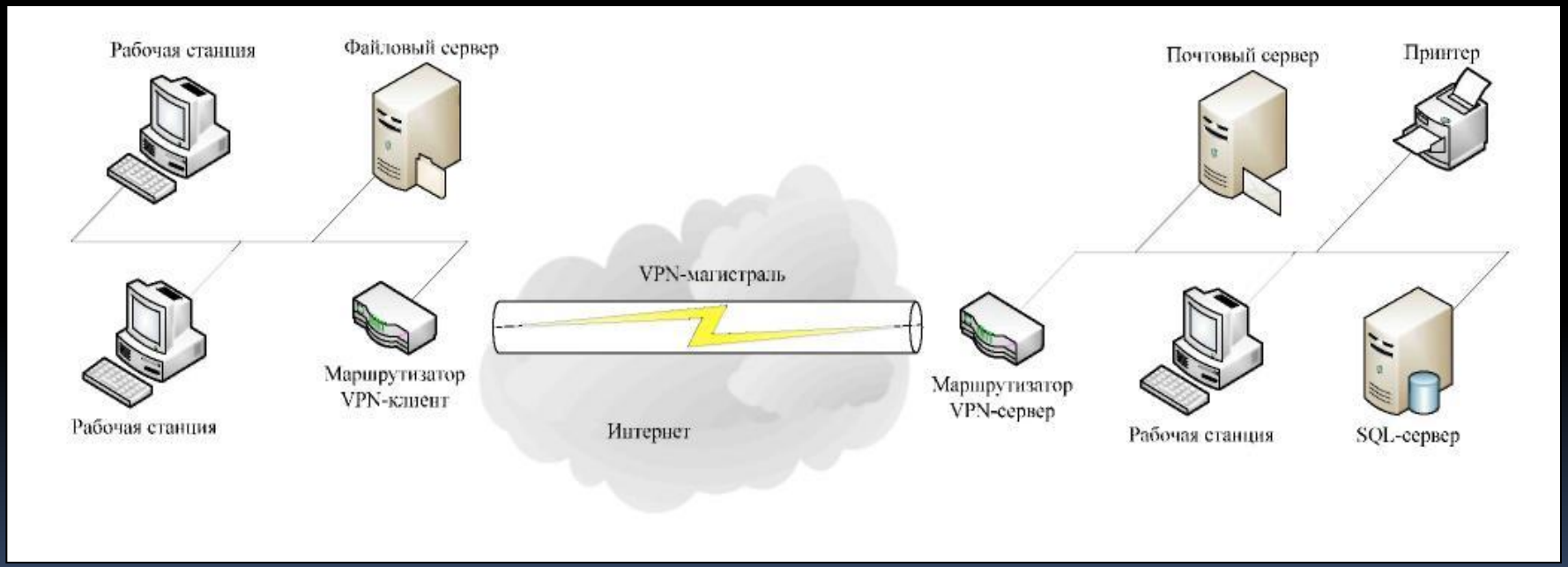
VPN-агент - это программа или программно-аппаратный комплекс, выполняющий действия по безопасной передачи данных VPN



VPN-соединение с удаленными пользователями



VPN-соединение между маршрутизаторами



3. Классификация сетей VPN

Наиболее часто используются:

- «рабочий» уровень модели OSI;
- архитектура технического решения VPN;
- способ технической реализации VPN.

Классификация VPN по «рабочему» уровню модели OSI

По признаку «рабочего» уровня модели OSI различают следующие группы VPN:

- VPN канального уровня;
- VPN сетевого уровня;
- VPN сеансового уровня.

VPN канального уровня

Основаны на применении следующих протоколов:

- PPTP (Point-to-Point Tunneling Protocol);
- L2F (Layer 2 Forwarding);
- L2TP (Layer 2 Tunneling Protocol).

VPN сетевого уровня

Основаны на применении следующих протоколов:

- SKIP (Simple Key Management for Internet Protocol);
- IKE (Internet Key Exchange);
- IPSec (Security Architecture for IP).

VPN сеансового уровня

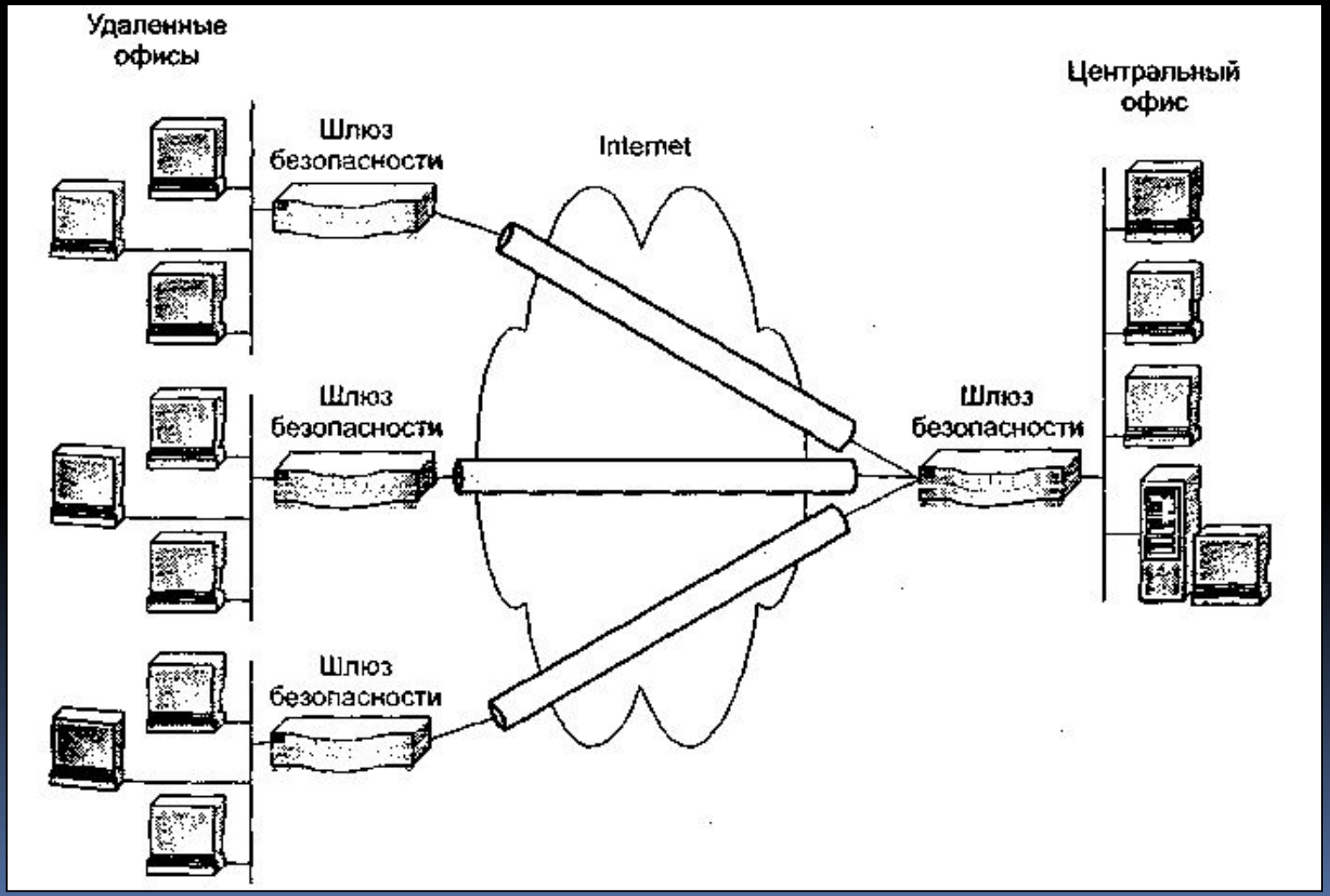
Основаны на применении следующих протоколов:

- SOCKS;
- SSL/TLS - протоколы защиты транспортного уровня, используемые в паре с протоколом SOCKS.

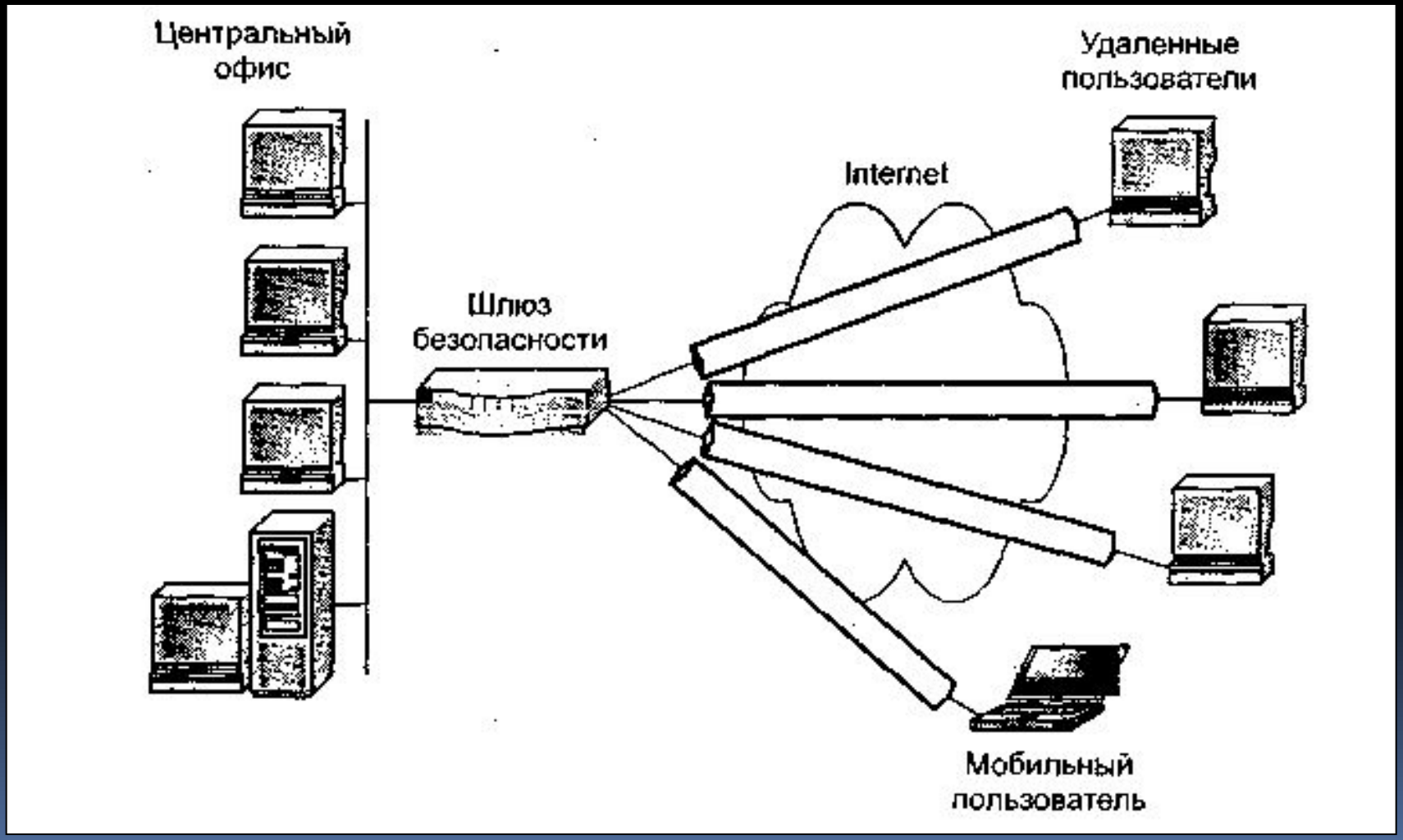
Классификация VPN по архитектуре технического решения

- внутрикорпоративные VPN (Intranet VPN);
- VPN с удаленным доступом (Remote Access VPN);
- межкорпоративные VPN (Extranet VPN).

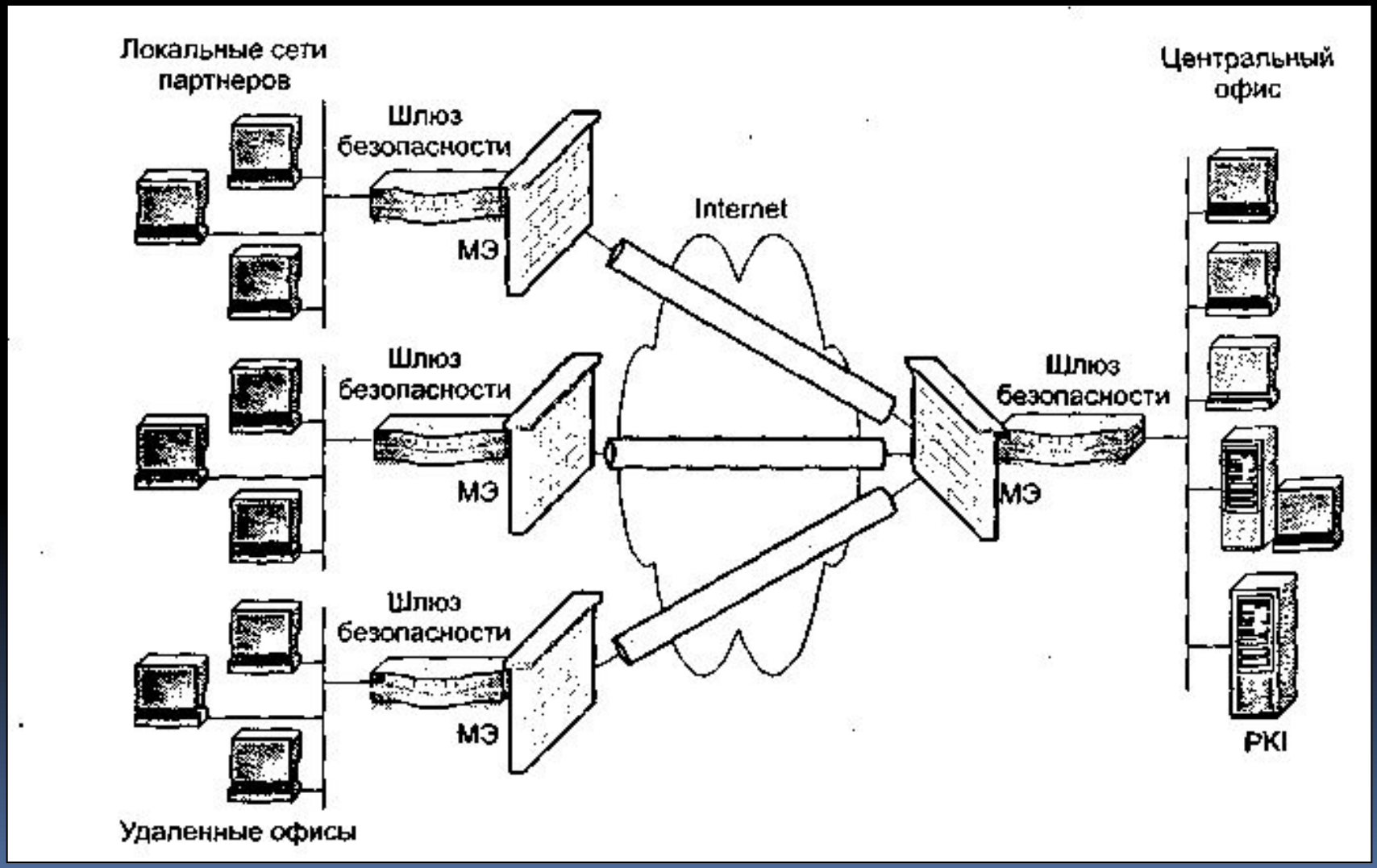
Внутрикорпоративные сети VPN



VPN с удаленным доступом



Межкорпоративные сети VPN



Классификация VPN по способу технической реализации

По способу технической реализации различают VPN на основе:

- маршрутизаторов;
- межсетевых экранов;
- программных решений;
- специализированных аппаратных средств со встроенными шифропроцессорами.

Контрольные вопросы

1. Что такое удаленный доступ?
2. Назовите виды удаленного доступа.
3. Перечислите протоколы удаленного доступа.
4. Для чего нужна аутентификация при удаленном доступе?
5. Каким образом сети VPN обеспечивают безопасную передачу пакетов?
6. Назовите виды VPN-соединений.
7. По каким признакам классифицируют сети VPN ?