ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ

Лекция 3:

«Методы и средства защиты информации в обеспечении безопасности предприятия»

Вопросы:

1. Понятие методов и средств защиты информации.
2. Техника защиты информации и ее использование.
3. Особенности применения электронной подписи.
4. Порядок разработки комплексной системы защиты информации

Вопрос № 1: «Понятие методов и средств защиты информации»

- **Метод (способ) защиты информации** - порядок и правила применения определенных принципов и средств защиты информации.
  - (*ГОСТ Р 50922-2006 Защита информации. Основные термины и определения*)

К основным методам защиты информации относятся:

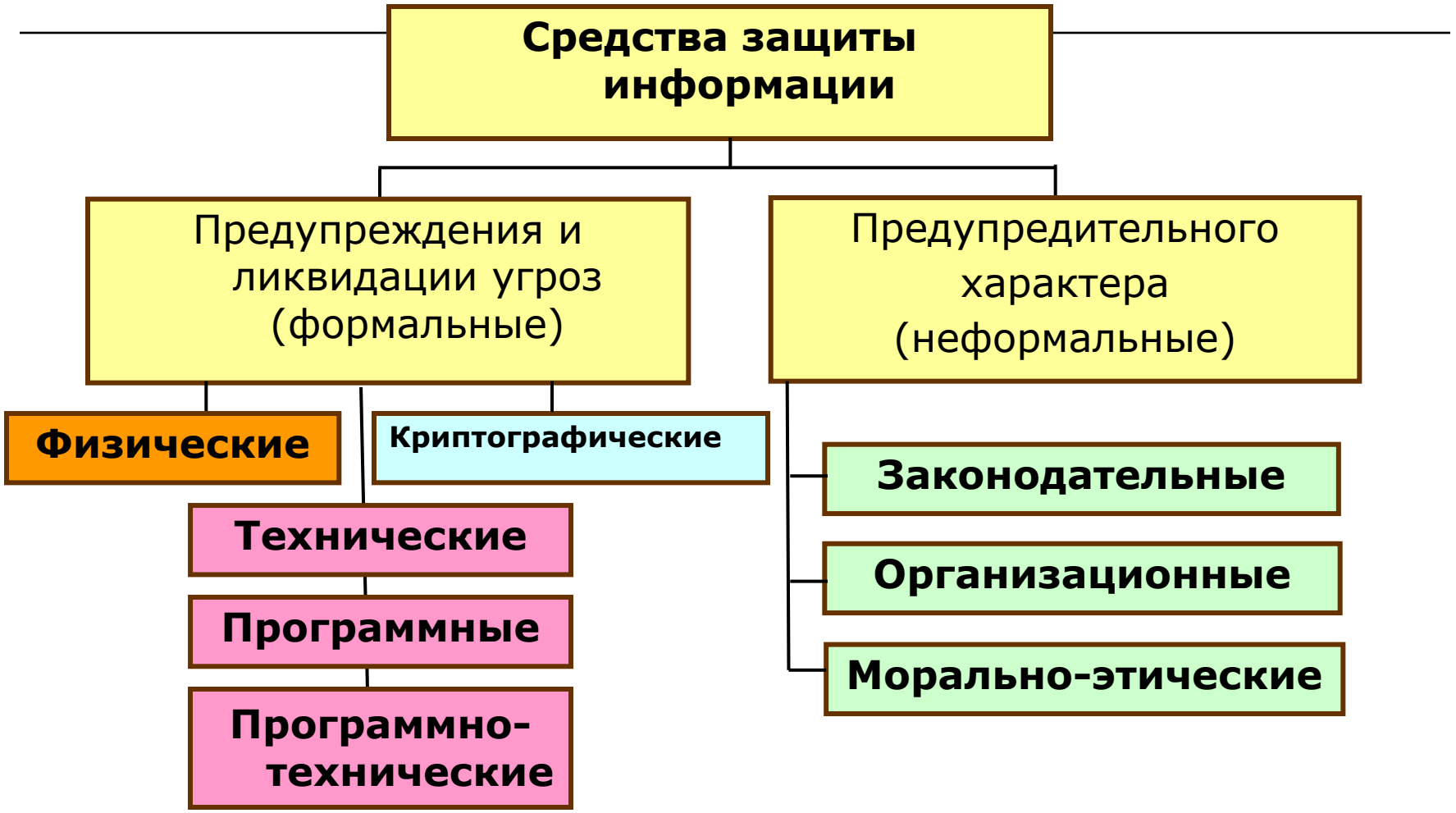
1. **Маскировка информации.**
2. **Препятствие на пути злоумышленника.**
3. **Мотивация.**
4. **Принуждение.**
5. **Регламентация доступа к информации.**
6. **Управление силами и средствами защиты.**

Средства защиты информации

- **Средство защиты информации:** **техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.**
  - ***ГОСТ Р 50922-2006 Государственный стандарт РФ. Защита информации. Основные термины и определения***


ФОРМАЛЬНЫЕ
Физические
Криптографические
Технические
Программные
Управление
Препятствие
Маскировка
Регламентация
Побуждение
Принуждение
Методы защиты данных
НЕФОРМАЛЬНЫЕ
Организационные
Законодательные
Морально-этические
Средства защиты данных

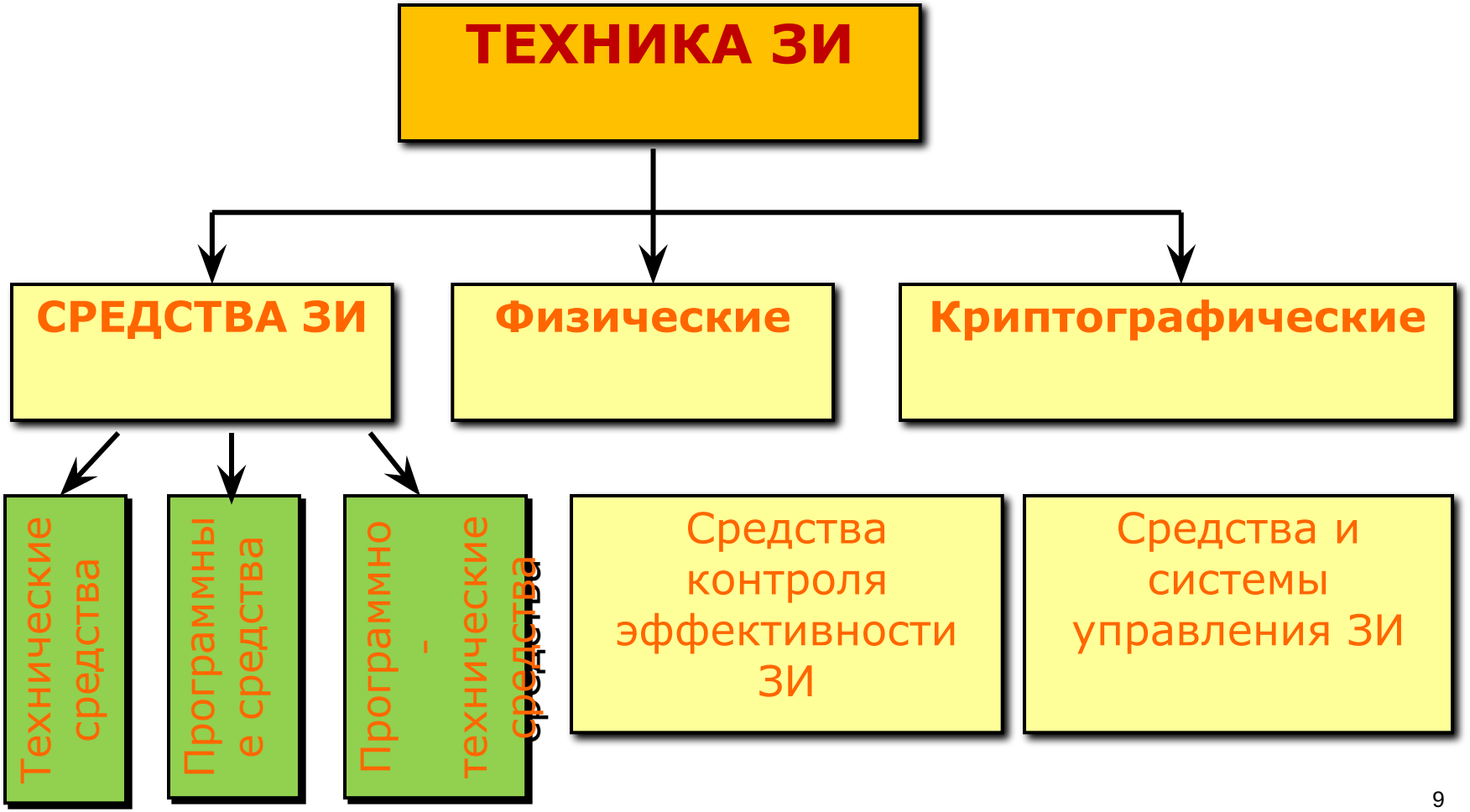
Средства защиты информации



Вопрос № 2: «Техника защиты информации и ее использование»

- **Техника защиты информации** - средства защиты информации, в том числе средства **физической** защиты информации, **криптографические средства** защиты информации, средства **контроля эффективности** защиты информации, средства и системы **управления**, предназначенные для обеспечения защиты информации.

Техника защиты информации (ГОСТ Р 50922-2006)



- **Средство физической защиты информации** - средство защиты информации, предназначенное или используемое для обеспечения физической защиты объекта защиты информации.

Средство физической защиты информации

- **Криптографическое средство защиты информации** - средство защиты информации, реализующее алгоритмы криптографического преобразования информации.

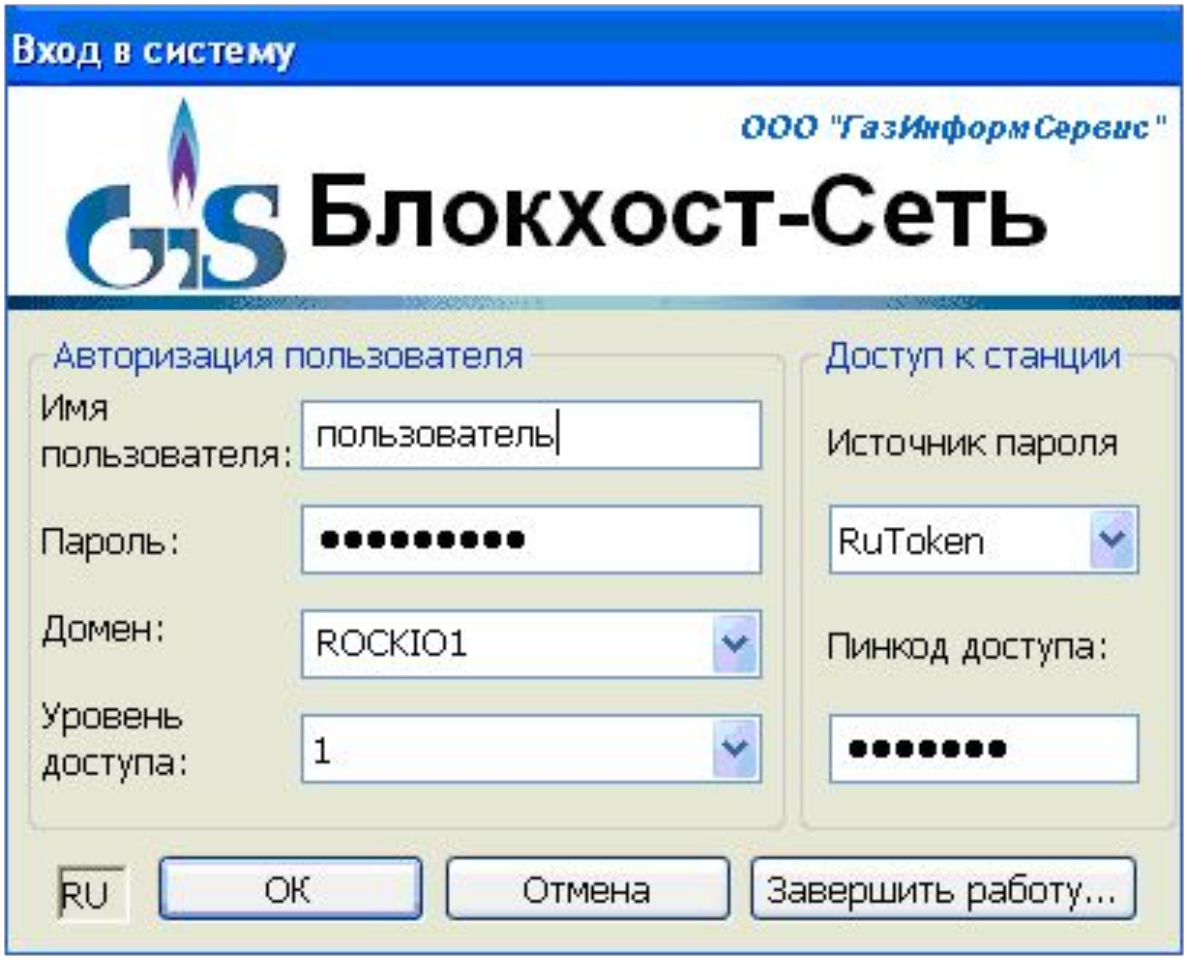
Криптографическое средство защиты информации

КриптоПро
РУТОКЕН CSP

- **Техническая защита информации (ТЗИ) –** защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

Техническое средство защиты информации

Программное средство защиты информации



Программно-техническое средство защиты информации

- **Средство контроля эффективности защиты информации -** средство защиты информации, предназначенное или
  нтроля
  ты информации.

Сетевые сканеры безопасности

- для инвентаризации сетевых ресурсов;
- в ходе проведения «тестов на проникновение»;
- в процессе проверки систем на соответствие различным требованиям.
  - **Nessus**
  - **MaxPatrol**
  - **Internet Scanner**
  - **Retina Network Security Scanner**
  - **Shadow Security Scanner (SSS)**
  - **NetClarity Auditor**

Предотвращение утечек информации

- **DLP (*Data Loss Prevention*)** — технологии предотвращения утечек КИ из информационной системы.
- Строятся на анализе потоков данных, пересекающих периметр защищаемой системы.
- При детектировании в потоке конфиденциальной информации срабатывает **активная компонента** системы, и передача сообщения (пакета, потока, сессии) блокируется.

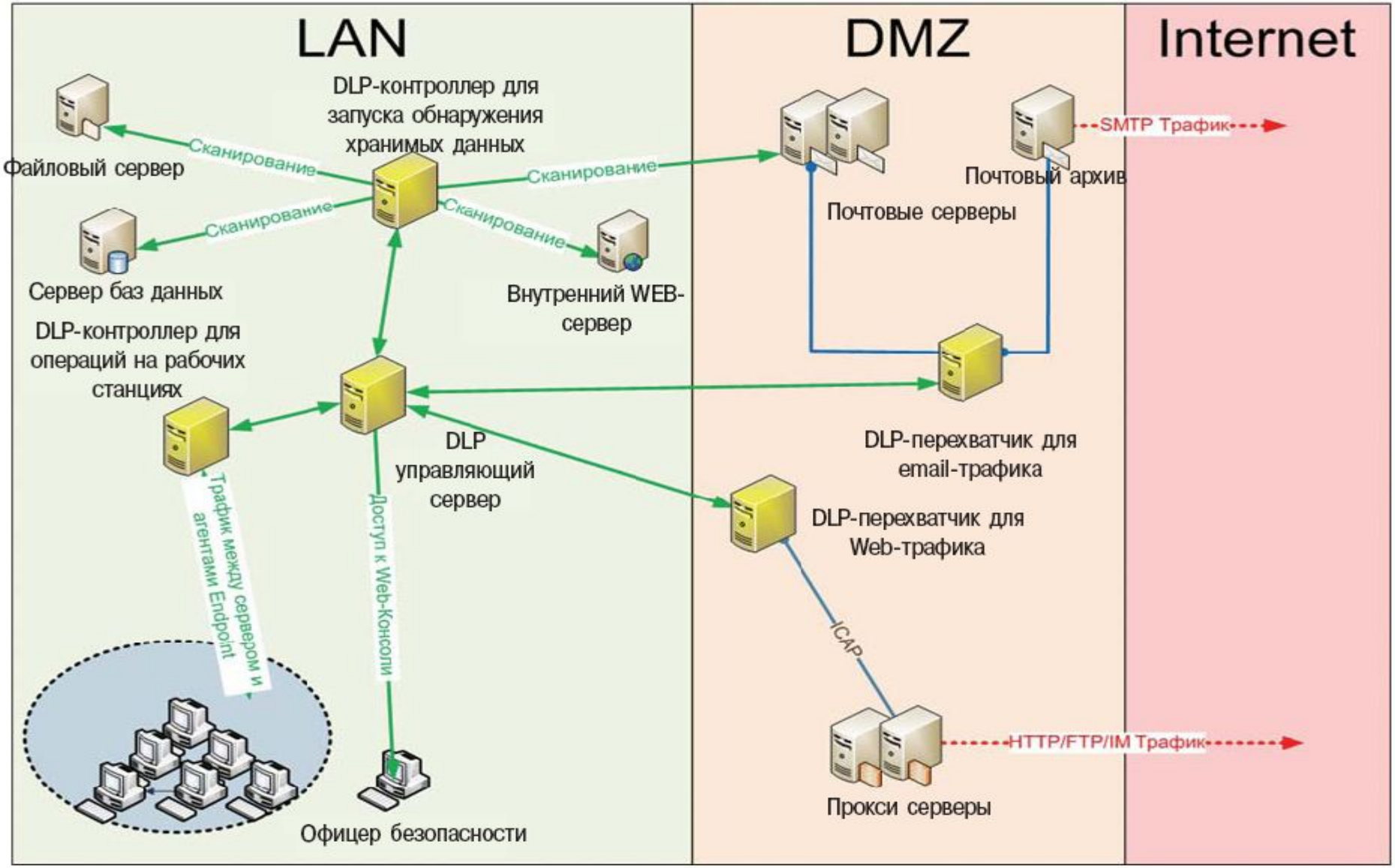
Антивирусные программные средства

- Acronis AntiVirus • AVS • AhnLab Internet Security • AOL Virus Protection • ArcaVir • Ashampoo AntiMalware • Avast! • AVG • Avira AntiVir • AVZ • A-square anti-malware • BitDefender • CA Antivirus • Clam Antivirus • ClamWin • Command Anti-Malware • Comodo Antivirus • Dr.Web • eScan Antivirus • F-PROT Antivirus • F-Secure Anti-Virus • G-DATA Antivirus • Graugon Antivirus• IKARUS virus.utilities • Антивирус Касперского • McAfee VirusScan • Microsoft Security Essentials • mks_vir • Moon Secure AV • Multicore antivirus • NOD32 • Norman Virus Control • Norton AntiVirus • Outpost Antivirus • Panda Cloud Antivirus • PC-cillin • TrustPort Antivirus • PC Tools Antivirus • Quick Heal AntiVirus • Rising Antivirus • Safe`n`Sec • Simple Antivirus • Sophos Anti-Virus • ВирусБлокАда • ViRobot • VirusBuster Personal • WinPooch • Zillya! • ZoneAlarm AntiVirus

Средства межсетевого экранирования

- **Бесплатные:** Outpost Security Suite Free • Ashampoo FireWall Free • Comodo • Core Force (англ.) • Online Armor • PC Tools • PeerGuardian (англ.) • Sygate (англ.)
- **Проприетарные:** Ashampoo FireWall Pro • AVG Internet Security • CA Personal Firewall • Jetico (англ.) • Kaspersky • Microsoft ISA Server • Norton • Outpost • Trend Micro (англ.) • Windows Firewall • Sunbelt (англ.) • Kerio Control
- **Для Linux:** Netfilter (Iptables • Firestarter • Iplist • NuFW • Shorewall) • Uncomplicated Firewall

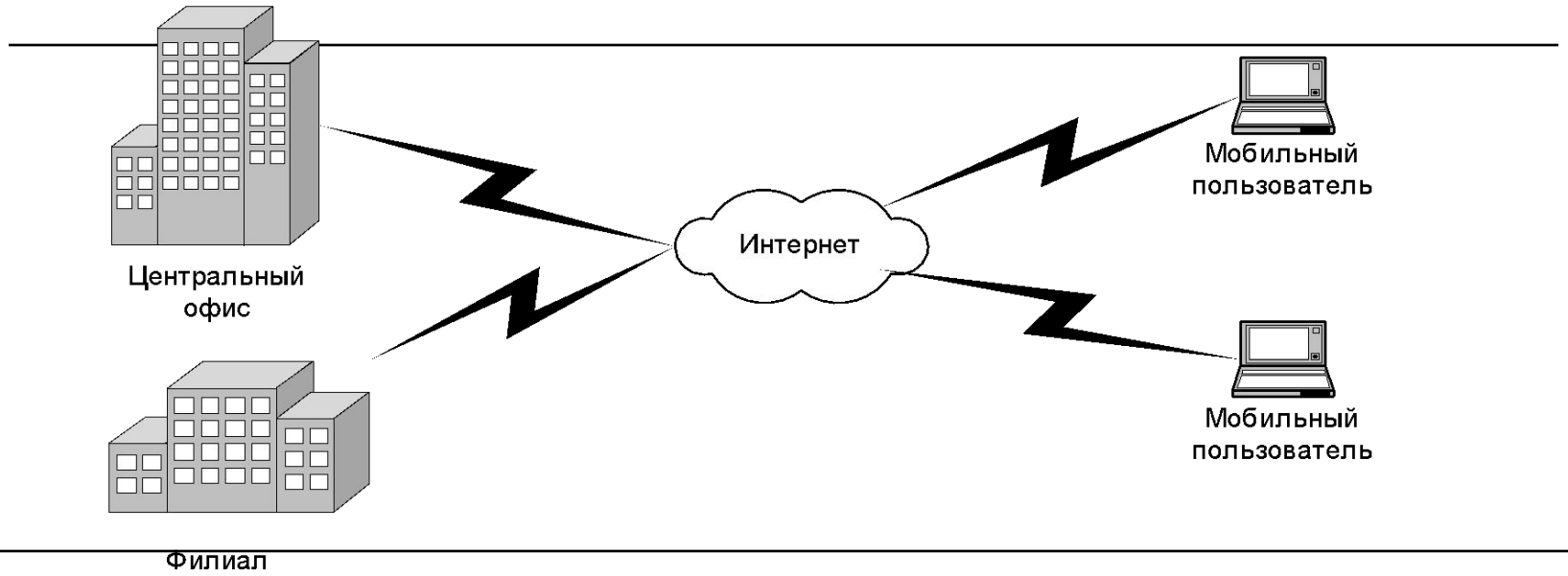
Типовая архитектура построения системы защиты информации на основе DLP технологии



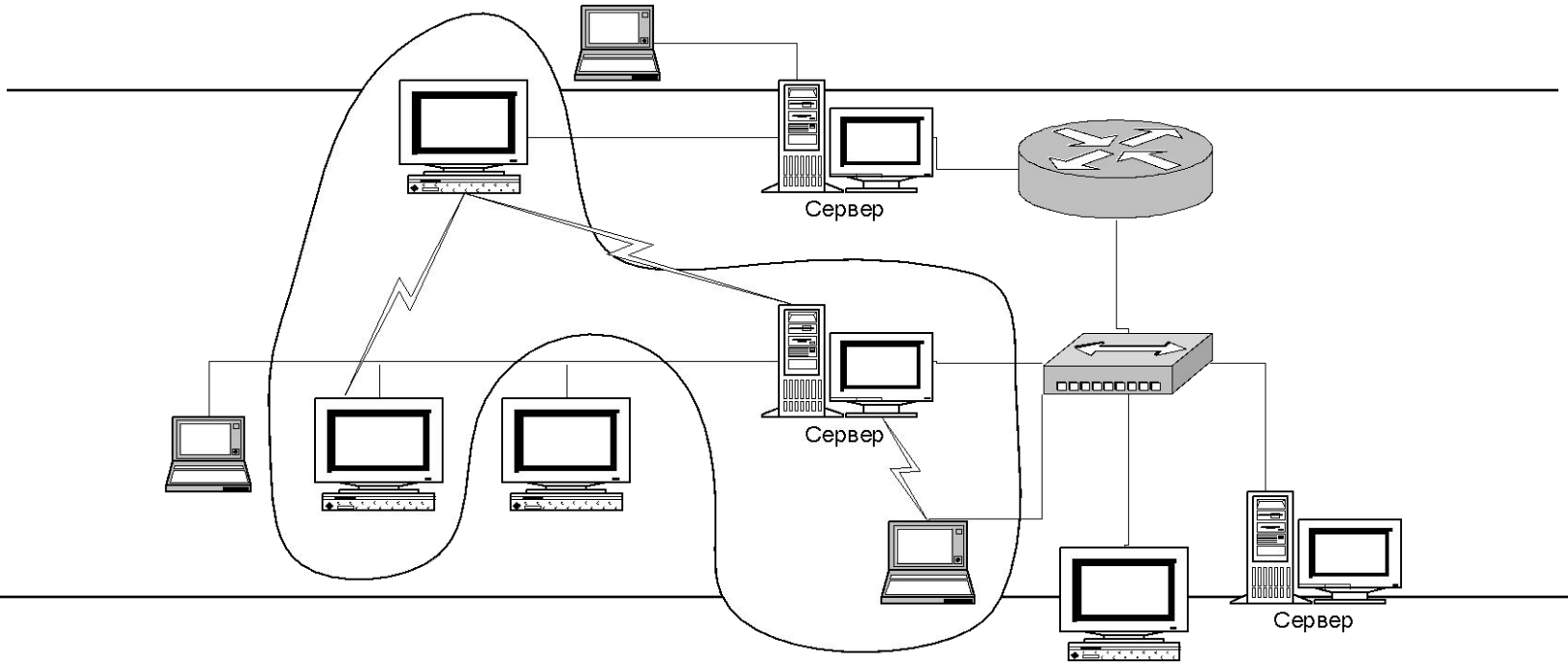
Технология VPN

Intranet VPN – объединяет в единую защищенную сеть несколько распределенных филиалов одной организации, взаимодействующих по открытым каналам связи.

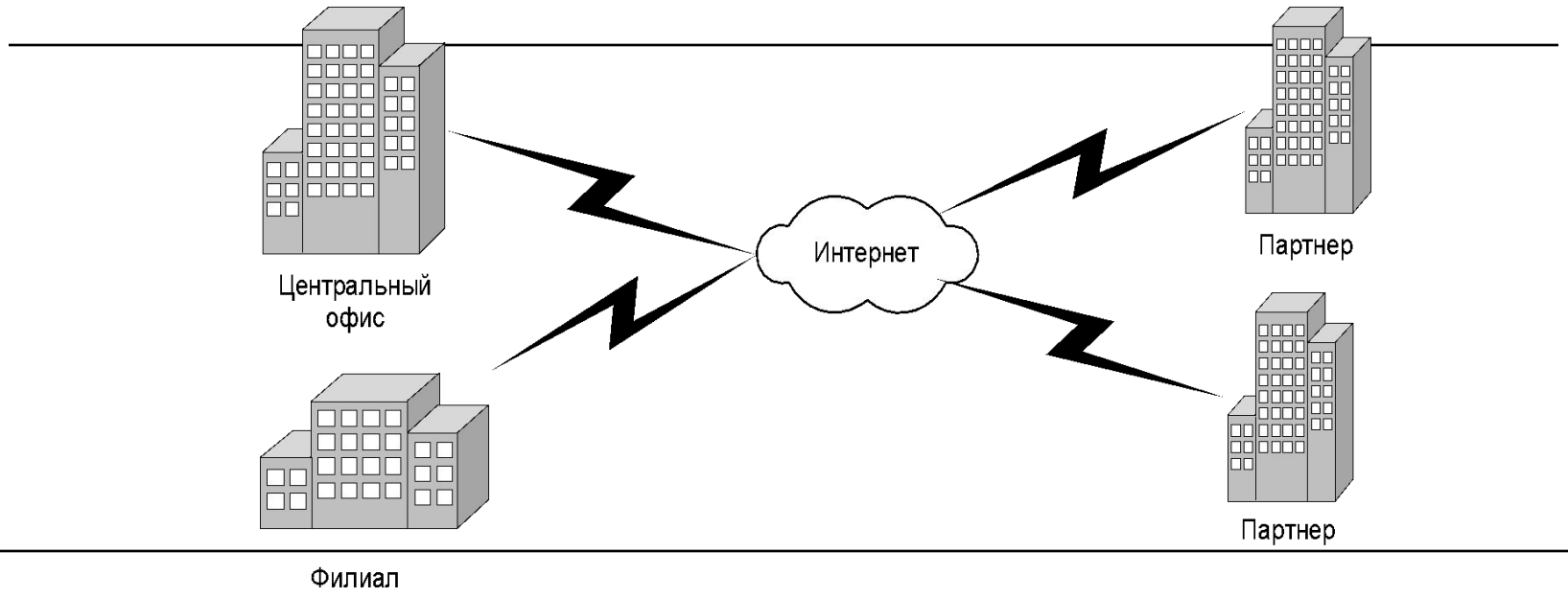
Remote Access VPN – реализует защищенное взаимодействие между сегментом корпоративной сети и одиночным пользователем.



Client-Server VPN – обеспечивает защиту передаваемых данных между двумя узлами корпоративной сети.



Extranet VPN – реализует защищенное соединение со сторонними пользователями (партнеры, заказчики, клиенты и т.д.), уровень доверия к которым ниже, чем к своим сотрудникам.



Вопрос 3: «Особенности использования электронной подписи»

- **Электронная подпись** - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая **используется для определения лица**, подписывающего информацию.
  - ***Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи»***

Виды электронных подписей

Средства электронной подписи -

- шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций: **создание, проверка ЭП, создание ключа ЭП и ключа проверки ЭП.**

Электронная цифровая подпись

Госдума РФ приняла новый закон «Об электронной подписи»

Электронная цифровая подпись (ЭЦП) — реквизит электронного документа, позволяющий установить отсутствие искажения информации в документе и проверить принадлежность подписи конкретному лицу

Простая ЭЦП *

Подтверждает, что электронное сообщение отправлено конкретным лицом. Предназначена для подписания электронных сообщений, направляемых в государственный орган, орган местного самоуправления или должностному лицу

Иванов

Усиленная ЭЦП *

Позволяет не только идентифицировать отправителя, но и подтвердить, что с момента подписания документ не менялся. Применяется во всех видах отношений, если иное не установлено нормативным правовым актом или соглашением участников отношений

** Сообщение с простой или усиленной ЭЦП может быть приравнено к бумажному документу, подписанному собственноручно (по предварительной договоренности сторон), а также в специально предусмотренных законом случаях*

Иванов

Квалифицированная ЭЦП **

Предназначена для взаимодействия госорганов с использованием государственных информационных систем

*** Дополнительно подтверждается сертификатом от аккредитованного удостоверяющего центра, а сообщение во всех случаях приравнивается к бумажному документу с собственноручной подписью*

Иванов

Кто может получить ЭЦП?

- Юридические лица
- Индивидуальные предприниматели
- Физические лица

Как получить ЭЦП?

ЭЦП выдается центром сертификации (удостоверяющим центром)

ПРИНЦИП ДЕЙСТВИЯ ЭЛЕКТРОННОЙ ПОДПИСИ

Подготовка ключей

Закрытый ключ — *Остаётся у владельца подписи*

Программно-технический комплекс

Открытый ключ — *Передаётся адресату*

001100
110011
100

Хеш-функция *(Идентификатор документа, математически рассчитываемый на основании текста самого документа, позволяющий сравнивать документ на соответствие)*

Подписание

Электронный документ

Создание хеш-функции

001100
110011
100

Шифрование хеш-функции закрытым ключом

001100
110011
100

Создание электронной подписи

Соединение подписи с документом

Проверка

Подписанный электронный документ, переданный адресату

Считывание документа

Расшифровка хеш-функции открытым ключом

Создание хеш-функции

Восстановление хеш-функции

001100
110011
100

001100
110011
100

001100
110011
100

001100
110011
100

Сравнение хеш-функций, если они одинаковые, электронная подпись верна

Источник: uc.credos.ru

ТАСС Телеком

ИТАР ТАСС

Нормативные документы по использованию ЭП

- **ПП РФ от 25 июня 2012 г. N 634 «О видах электронной подписи, использование которых допускается при обращении за получением государственных и муниципальных услуг».**
- **ПП РФ от 25.01.13 N 33 «Об использовании простой электронной подписи при оказании государственных и муниципальных услуг»**

ЭП используются для:

- **подписания отчетов в государственные контролирующие органы** (ФНС, ПФР, ФСС, Росстат, Росалкогольрегулирование, ФСТ, Росприроднадзор, Роскомнадзор, Росфинмониторинг и др.)
- **доступа и работы на электронных торговых площадках** (Госторги (5 площадок), реализация имущества предприятий-банкротов, коммерческие торги),
- **обмена электронными документами** между разными юридическими лицами (Диадок)

ЭП используются для:

- **доступа к ГИС** (fedresurs.ru, zakupki.gov.ru, Единый федеральный реестр сведений о банкротстве, Росаккредитация),
- **работы на особых площадках** (loanberry.ru – взятие и дача взаймы денежных средств онлайн),
- **Интернет-банкинг** (системы ДБО).

ПРАВЛЕНИЕ ПЕНСИОННОГО ФОНДА РОССИЙСКОЙ ФЕДЕРАЦИИ

РАСПОРЯЖЕНИЕ

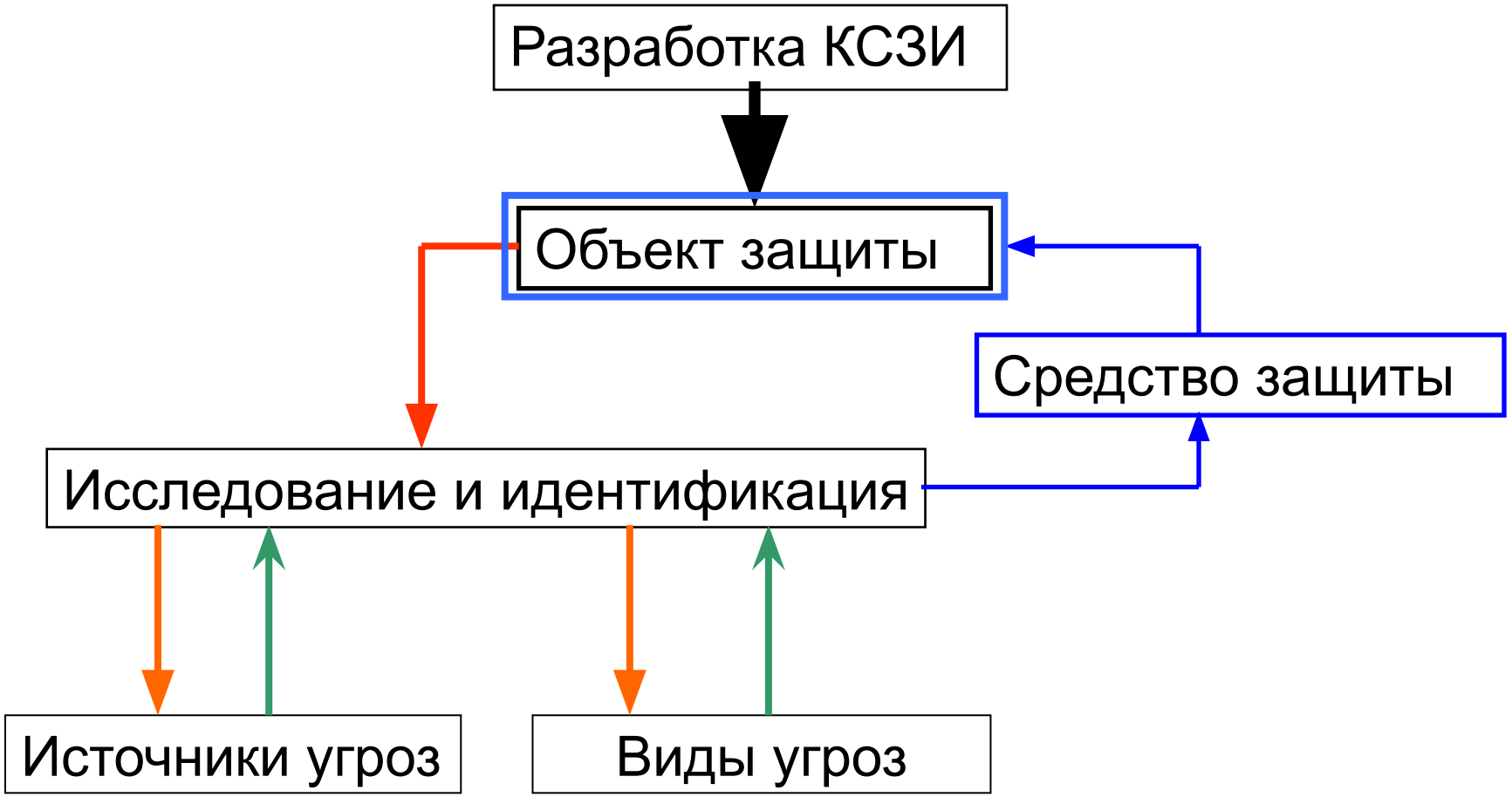
О внедрении защищенного электронного документооборота в целях реализации законодательства Российской Федерации об обязательном пенсионном страховании

- **от 11 октября 2007 г. N 190р** (в ред. распоряжений Правления ПФ РФ от 10.06.2009 N 116р, от 19.03.2010 N 75р)

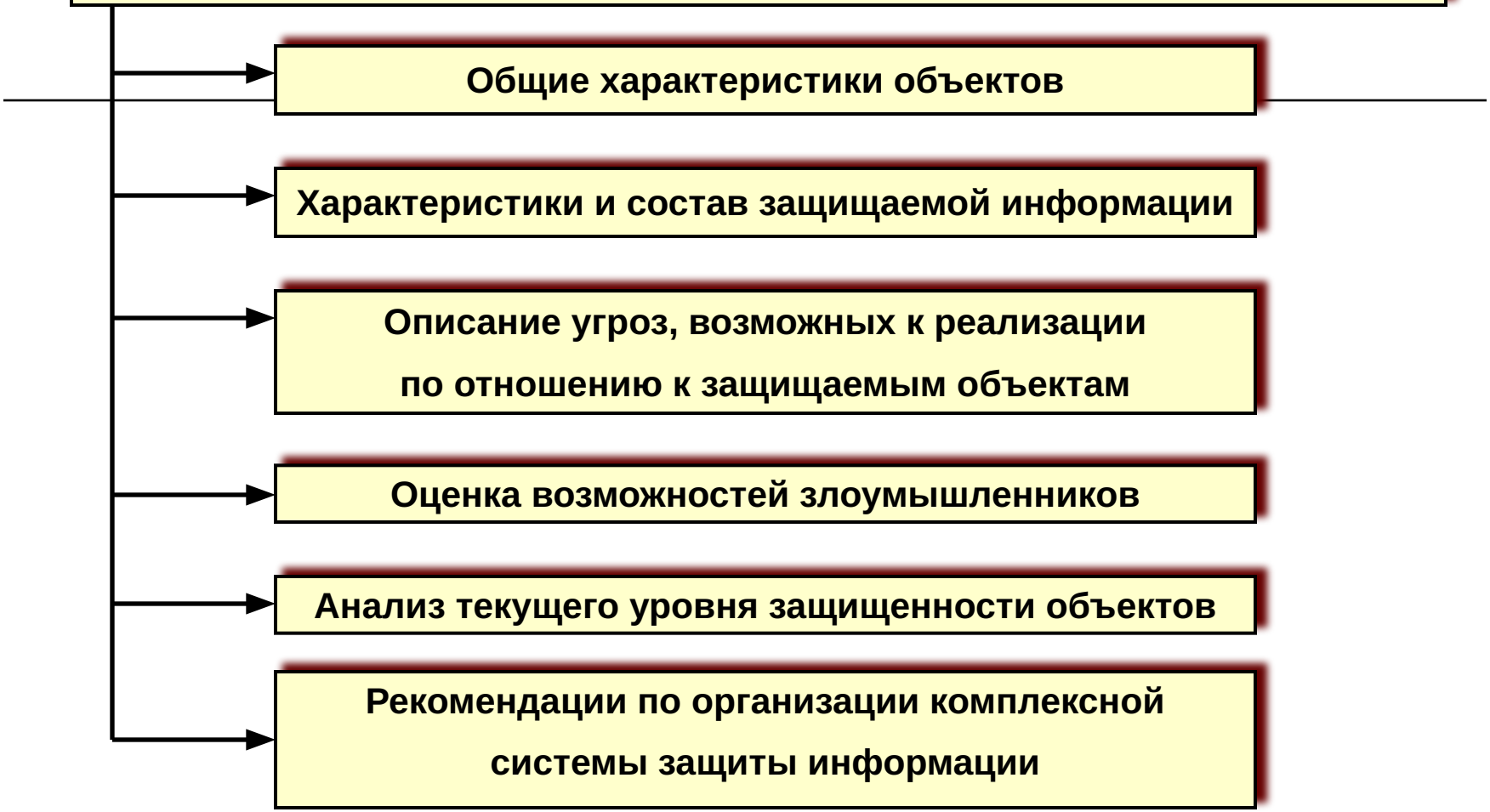
Средства криптографической защиты информации

- Для организации юридически значимого документооборота используются СКЗИ:
- В органах ПФР - "Домен-К", версии не ниже v.2.0 или "Верба-OW", версии не ниже v. 6.1;
- Абонент Системы может использовать СКЗИ КриптоПРО не ниже v.2.0, "Домен-К" версии не ниже v.2.0 или "Верба OW" версии не ниже 6.1.
- СКЗИ используются для формирования и проверки подлинности ЭЦП и шифрования/расшифрования данных.

Вопрос № 4: «Порядок разработки комплексной системы защиты информации»



Концепция информационной безопасности организации



Общие характеристики объектов

- Особенности расположения объектов (зданий и сооружений, кабинетов и рабочих комнат, автоматизированных систем)
- Анализ конструктивных особенностей зданий
- Анализ инженерно-технических коммуникаций объектов
- Анализ особенностей построения силовых и слаботочных сетей
- Анализ построения сетей связи и передачи данных

Характеристики и состав защищаемой информации

- Перечень видов защищаемой информации
- Принципы классификации защищаемой информации по уровням конфиденциальности
- Анализ особенностей хранения и обработки защищаемой информации

Оценка возможностей злоумышленников

- Анализ технических возможностей
- Разработка «моделей» злоумышленников
- Разработка общих технических требований (норм) к средствам защиты информации применяемым в организации

ЭТАПЫ РАБОТ ПО СОЗДАНИЮ КОМПЛЕКСНОЙ СИСТЕМЫ БЕЗОПАСНОСТИ

- Экспертное обследование
- Предпроектные изыскания на объекте
- Разработка технических решений
- Проведение специальных исследований
- Проектирование систем
- Поставка оборудования и материалов
- Монтаж подсистем и средств защиты, кабельных сетей и оборудования
- Пуско-наладочные работы, настройка систем
- Обучение эксплуатационных служб и служб безопасности

Контрольная работа

- **Критерии оценки:**
- **Соответствие тематике**
- **Необходимый объем и оформление**
- **Содержание необходимых мер по защите информации**
- **Shans.ISE@mail.ru**
- **проверка на наличие плагиата**