



Сложные вопросы работы с ИСПДн при построении защиты распределенных компаний с учетом современных требований регуляторов

ДОКЛАД

на 5й межрегиональной конференции «Концептуальные проблемы информационной безопасности.

Современные технологии защиты персональных данных»

11-12 марта 2010г., г. Ростов-на-Дону

Сетевая безопасность ИСПДн
Механизмы безопасности
Сценарии защиты
Вопросы аттестации

Сетевая безопасность ИСПДн

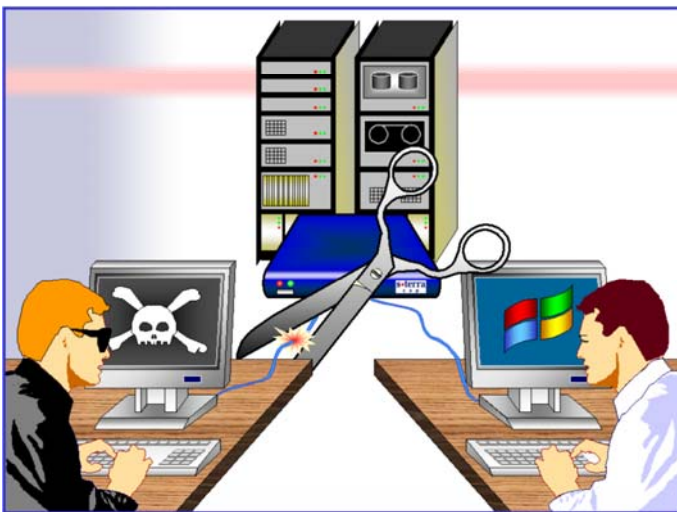
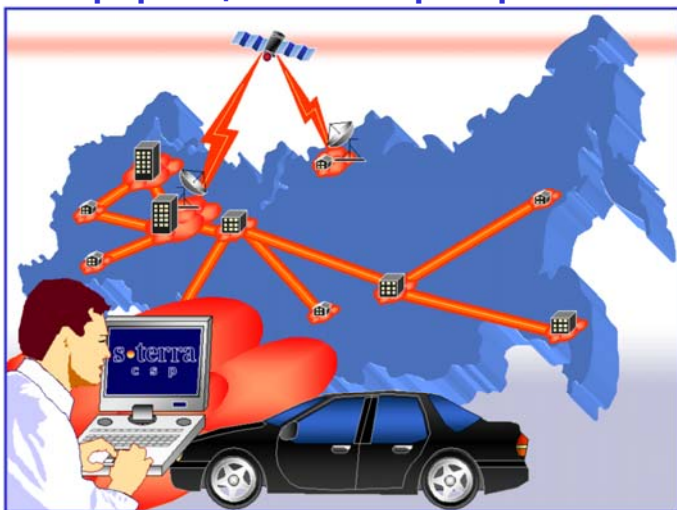
s•terra

с с р

Cisco Solution Technology Integrator

● Доверенное пространство обработки ПДн

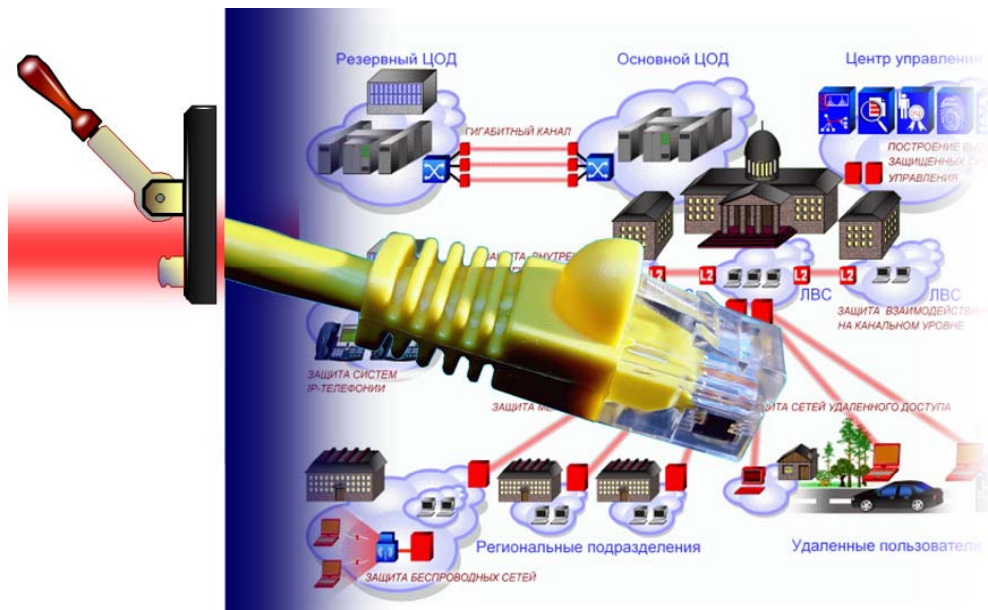
Изоляция корпоративного информационного пространства



Криптографически стойкий контроль доступа

- Базовая технология: фундаментальная архитектура сетевой защиты IPsec
- Механизмы безопасности IPsec:
 - конфиденциальность и целостность информации
 - каждый пакет шифруется при помощи стойких криптоалгоритмов
 - ключевая информация надежно защищена за счет использования временных сеансовых ключей с ограниченным временем жизни
 - целостность информации обеспечивается для данных, для заголовков IP-пакетов и для потока пакетов
 - поддерживается много механизмов аутентификации
 - для отдельного пользователя можно реализовать него индивидуальную политику
 - криптографически стойкий контроль доступа
 - **в сеть может проникнуть только владелец секретного ключа**
 - **это обеспечивает полную изоляцию корпоративного информационного пространства**

● Позиционирование средств сетевой защиты



● Средства сетевой безопасности позволяют принять решение о доступе для каждого сетевого пакета на каждом сетевом интерфейсе

- **Вопрос в том, как оптимальным образом применить средства сетевой защиты в ИСПДн**

ЗА:

- **Возможность построить изолированную среду обработки ПДн, структурировать периметры различных ИСПДн**

ПРОТИВ:

- **Сетевой пакет – не документ и не запись в базе данных, т.е средства сетевой безопасности не применяются к ПДн непосредственно**
- **Средства VPN, как технология, косвенно представлены и в регулировании ФСТЭК и в регулировании ФСБ России**


Сетевая безопасность ИСПДн
Механизмы безопасности
Сценарии защиты
Вопросы аттестации

Механизмы безопасности

s•terra

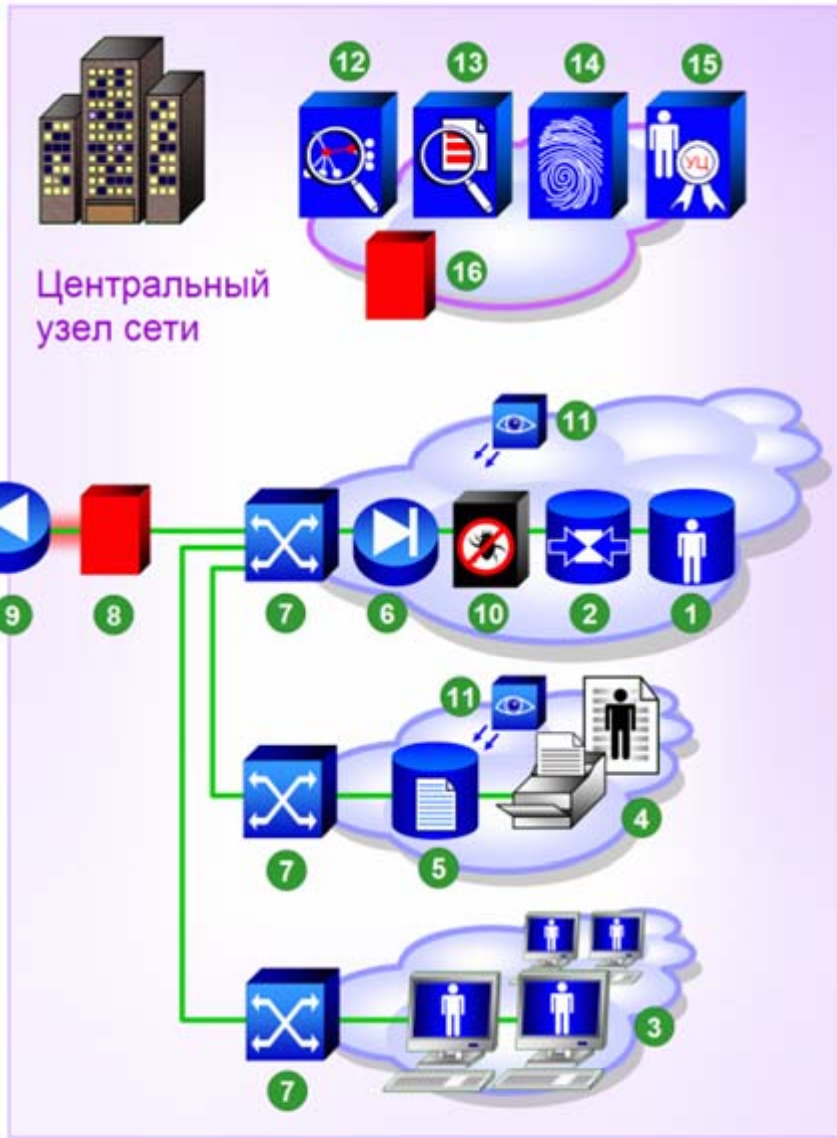
с s p

Cisco Solution Technology Integrator

-  Ниже приведен анализ технических требований по защите ИСПДн 1 класса при многопользовательском режиме обработки персональных данных и разных правах доступа к ним пользователей в соответствии с «Положением о методах и способах защиты информации в информационных системах персональных данных» от 5 марта 2010 г.

● Позиционирование средств сетевой защиты

Справочная архитектура подсистемы сетевой безопасности системы обработки персональных данных



Подсистема приложений

1. Хранилище персональных данных

- Для крупных систем (Хнд-1,2) и для систем высокой ответственности (К1,2) можно рекомендовать разделение функций хранилища (базы) данных и сервера приложений, реализующего прикладную логику. Это позволит реализовать дополнительный уровень контроля доступа (на интерфейсе между сервером приложений и базой данных) а также применить более гибкую архитектуру, в которой можно более эффективно реализовать механизмы защиты информации

2. Сервер приложений

- Может иметь более сложную, нежели монолитное приложение на единственном сервере, структуру
- Рекомендуются архитектурные решения, в которых обработка персональных данных реализуется преимущественно в серверной части системы, без передачи или с передачей минимального объема информации на терминалы обработки персональных данных (3)
- В рамках приложений, обладающих персональные данные высокой ответственности (К1,2) должен быть реализован ряд механизмов безопасности:

- Строгая аутентификация администраторов и пользователей
- Контроль доступа на уровне прикладных операций
- Регистрация действия администраторов и пользователей, связанных с созданием, уничтожением и модернизацией персональных данных

- В или вне рамок прикладного сервера для систем высокой ответственности (К1,2) должны быть реализованы функции резервного копирования и восстановления персональных данных. При этом должны обеспечиваться:

- Учет резервных копий
- Защищенное хранение резервных копий. Для данных категории Хнд-1 рекомендуется применение криптографических методов защиты резервных копий
- Регламент безопасности хранения и восстановления резервных копий

3. Терминалы обработки персональных данных

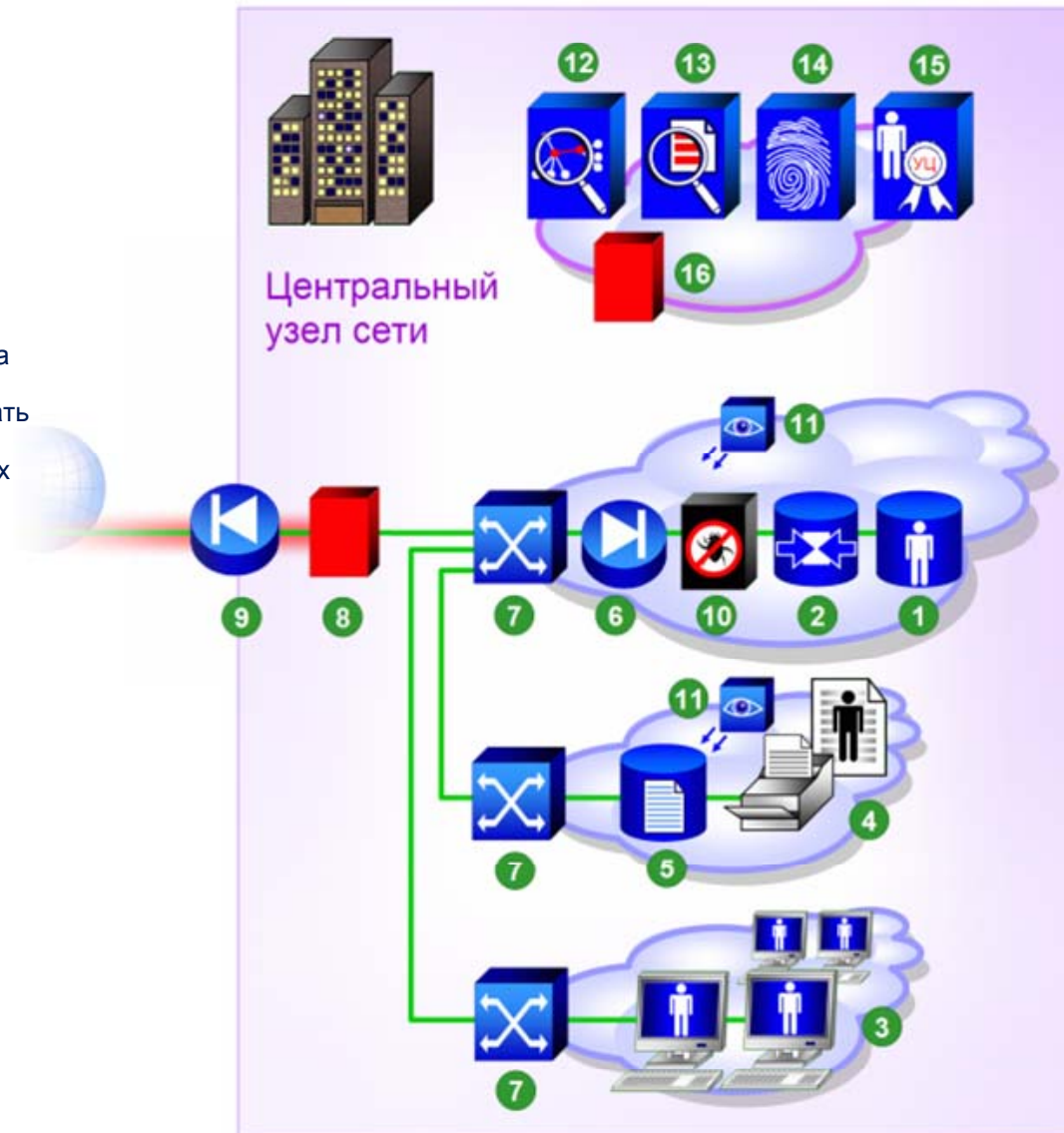
- Логика по распределению обработки персональных данных может в различных пропорциях распределяться между компонентами «клиент», «сервер», «промежуточное программное обеспечение (middleware)»
- Для систем высокой ответственности (К1,2) можно рекомендовать терминальный режим доступа к персональным данным
- Детали организации терминальных систем приведены в разделе «Справочный состав программного обеспечения терминала обработки персональных данных»



● Система печати персональных данных

Система печати персональных данных должна обеспечивать контролируемый процесс вывода информации на печать, контролируемого использования и распространения печатной информации, надежного уничтожения печатных материалов, содержащих персональные данные. Ее компоненты:

4. Система печати
5. Принт-сервер. Назначение принт-сервера состоит в том, чтобы:
 - Обеспечивать контроль доступа к выводу на печать
 - Регистрировать вывод информации на печать в системе событийного протоколирования
 - Снабжать печатные материалы в различных форматах метками о классе конфиденциальности данных



Сетевая инфраструктура

Безопасная сетевая инфраструктура обработки персональных данных должна обеспечивать защиту данных от атак, осуществляемых методами сетевого доступа.

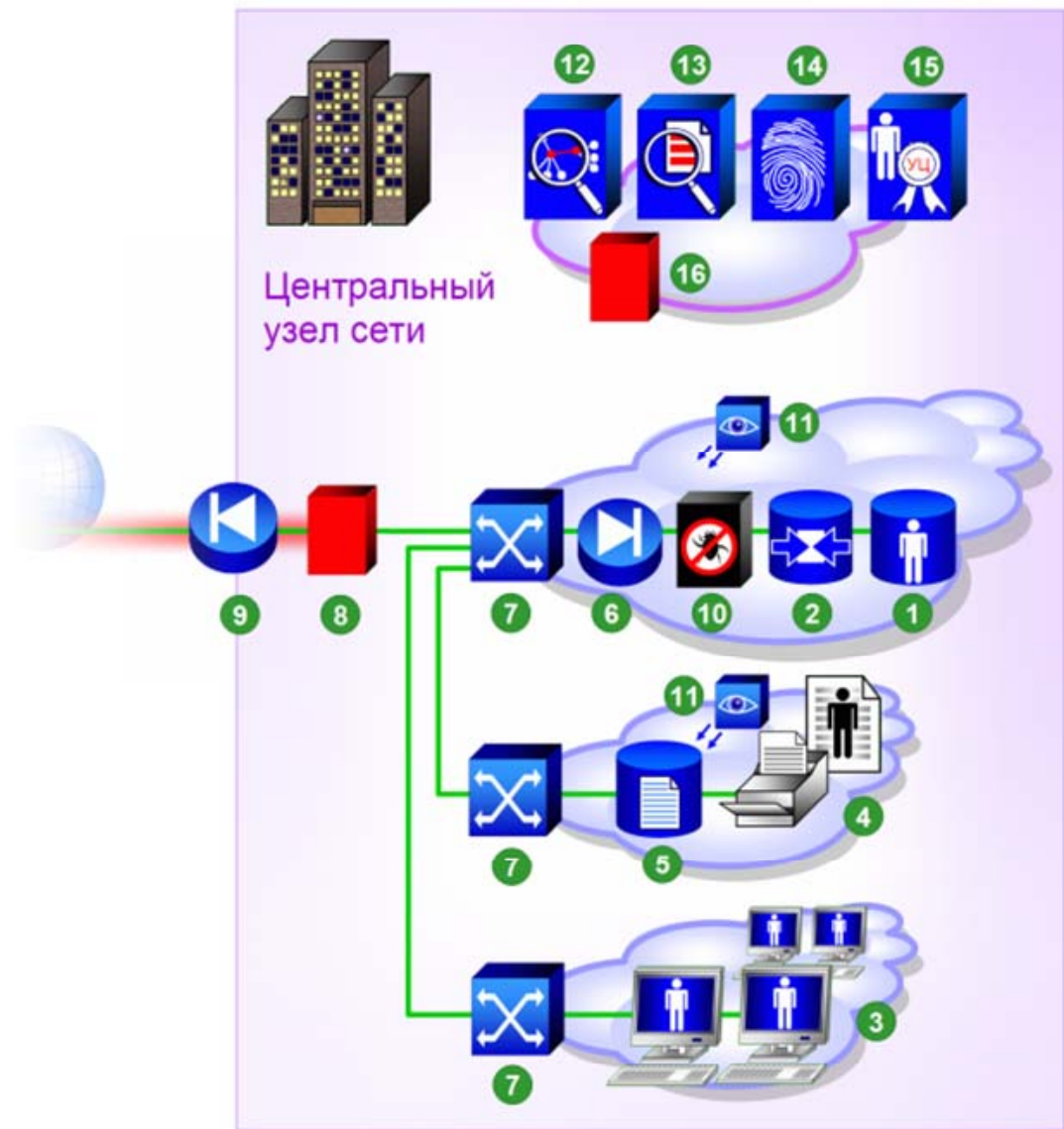
Сетевая инфраструктура должна быть иерархизирована (защита должна быть реализована на различных уровнях модели OSI/ISO) и структурирована (в частности, ЛВС, в которых ведется обработка данных должны быть сегментированы, серверные подсистемы, подсистемы ввода/вывода, терминальные системы должны быть размещены в различных сегментах ЛВС). В ее состав должны входить:

6. Межсетевой экран для контроля доступа к прикладным системам
 - Обеспечивает контроль доступа к приложениям
7. Безопасная инфраструктура ЛВС
 - Строится на основе коммутаторов. Обеспечивает ролевой контроль доступа на всем тракте их распространения (с применением технологий IEEE 802.1q VLAN) и, возможно, контроль доступа к портам ЛВС (IEEE 802.1x)
8. VPN-шлюз
 - Обеспечивает изоляцию сетевого пространства, в котором распространяются персональные данные, аутентификацию источника, конфиденциальность и целостность данных при их распространении. Технологии VPN могут применяться также для защиты персональных данных высокой ответственности (K1, 2) при их распространении внутри ЛВС с целями защиты от инсайдеров, в том числе с высокими правами доступа (например, системных администраторов)
9. Межсетевой экран на периметре ЛВС (узел доступа в открытые сети)
 - Предназначен для защиты системы от несанкционированного доступа из открытых сетей связи
10. Контентный фильтр
 - Обеспечивает фильтрацию опасного, активного сетевого прикладного контента (вирусов, червей, зараженных документов и т.п.)
11. Система контроля аномальных активностей и обнаружения вторжений
 - Датчики системы должны устанавливаться в зонах коммутации трафика и в зонах дислокации серверных ресурсов



Подсистема управления

- 12. Центр управления политиками безопасности сети
- 13. Центр событийного протоколирования и мониторинга
 - Должен обеспечивать сбор событийной информации, в том числе с датчиков аномальных активностей и
- 14. Серверы аутентификации
- 15. Удостоверяющий центр
- 16. Выделенная защищенная подсеть управления



Терминал оператора ИСПДн

Справочный состав программного обеспечения терминала обработки персональных данных

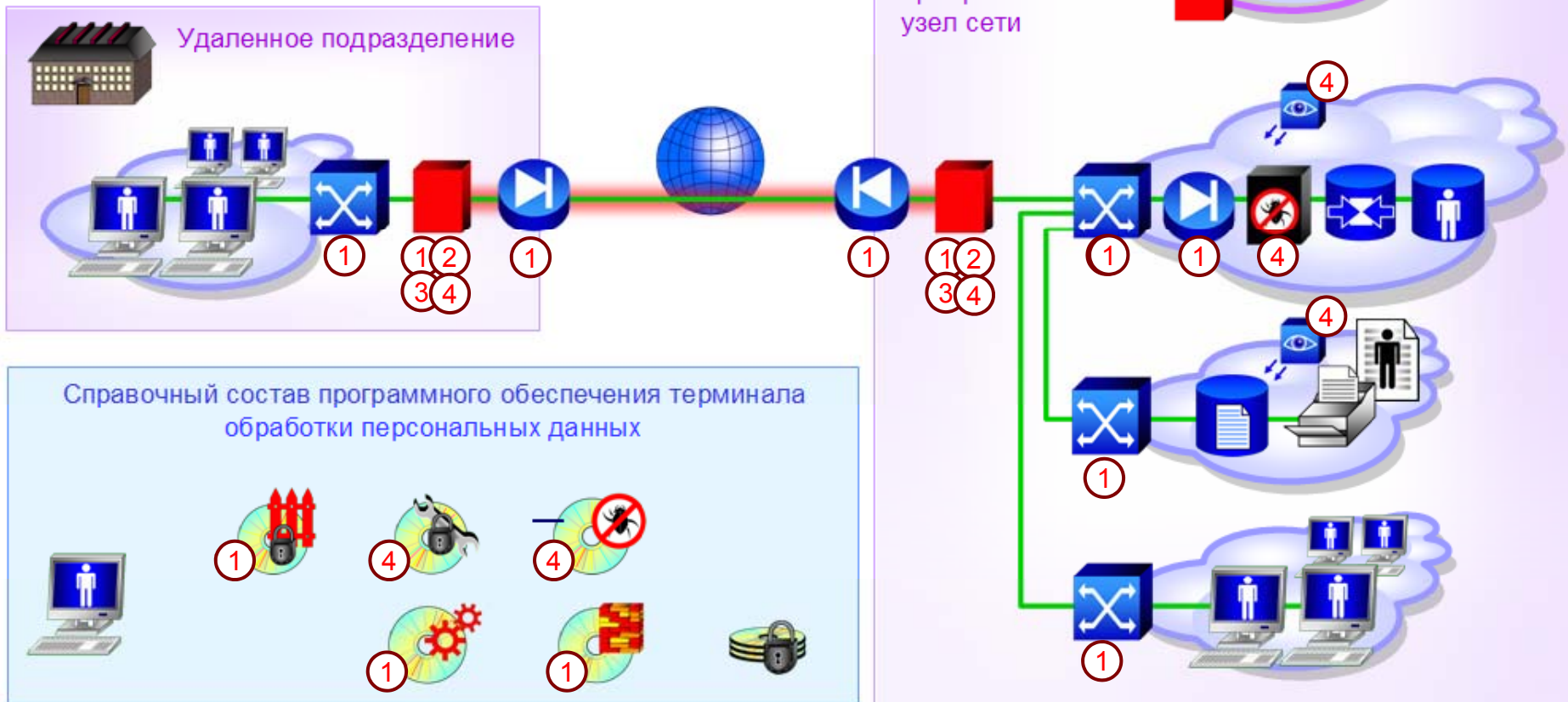
1. Система аутентификации пользователя и контроля доступа
2. Система контроля за конфигурацией терминала и устройств ввода-вывода
3. Анти-вирусное ПО
4. ПО защиты файловой системы
5. VPN-клиент
6. Персональный межсетевой экран



2.1 методы и способы защиты ПДн от НСД

1. реализация разрешительной системы допуска, разграничение доступа пользователей к информационным ресурсам, программным средствам
2. регистрация действий пользователей
3. использование защищенных каналов связи;
4. предотвращение внедрения в ИСПДн вредоносных программ, вирусов и программных закладок

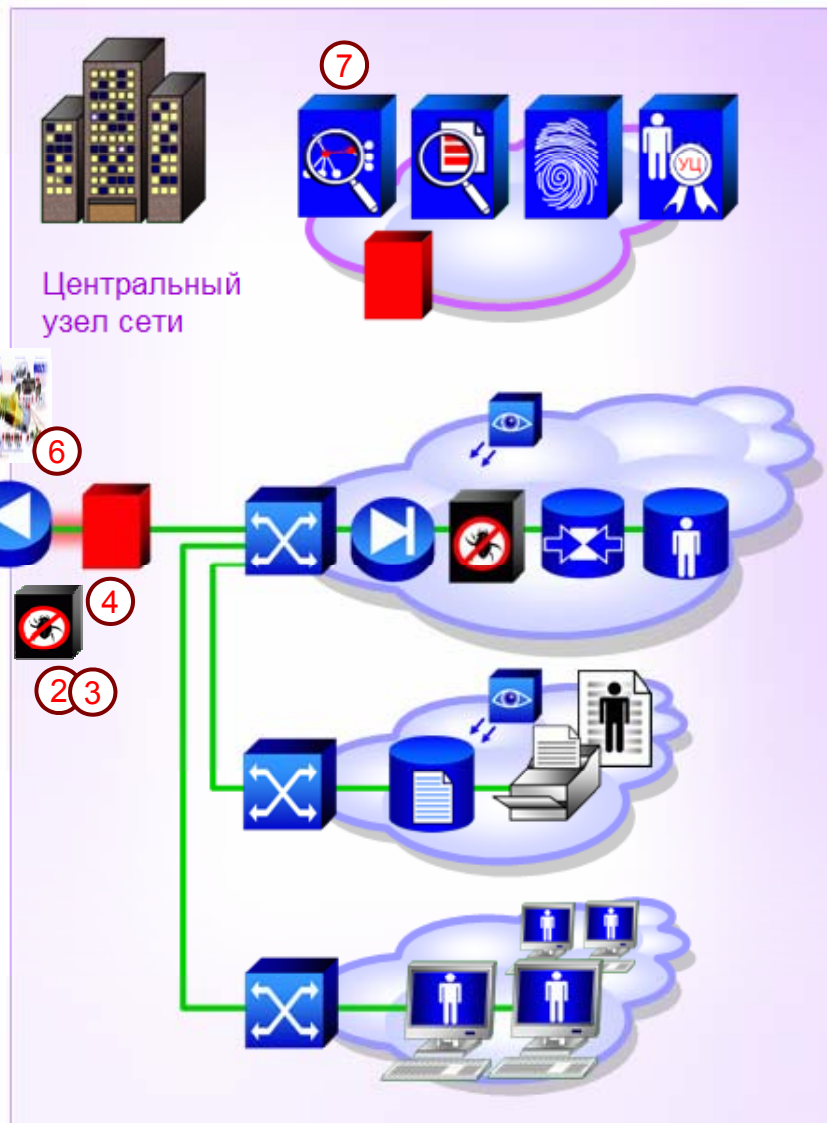
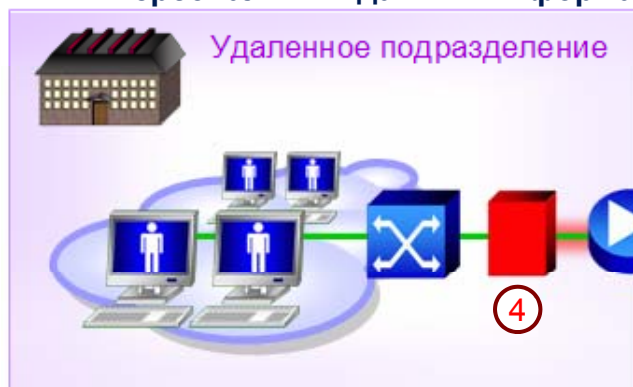
Также средства сетевой безопасности обеспечивают резервирование технических средств и подвержены оценке соответствия



2.4 защита при взаимодействии с открытыми сетями

1. межсетевое экранирование
2. обнаружение вторжений в информационную систему
3. анализ защищенности при помощи сканеров безопасности)
4. защита информации при передаче по каналам связи
5. использование смарт-карт ... для аутентификации пользователей
6. использование средств антивирусной защиты
7. централизованное управление системой защиты персональных данных информационной системы

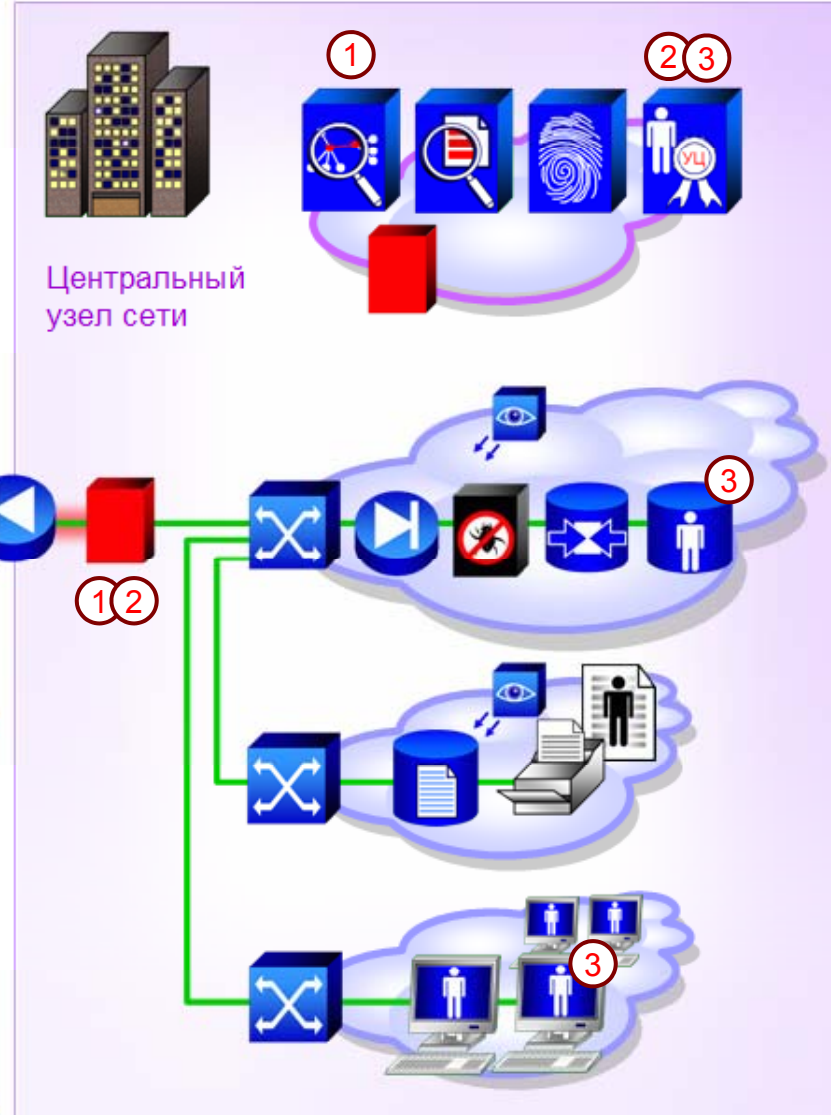
**) – дополнительно к 2.1*



2.8-2.9 взаимодействие через открытые сети

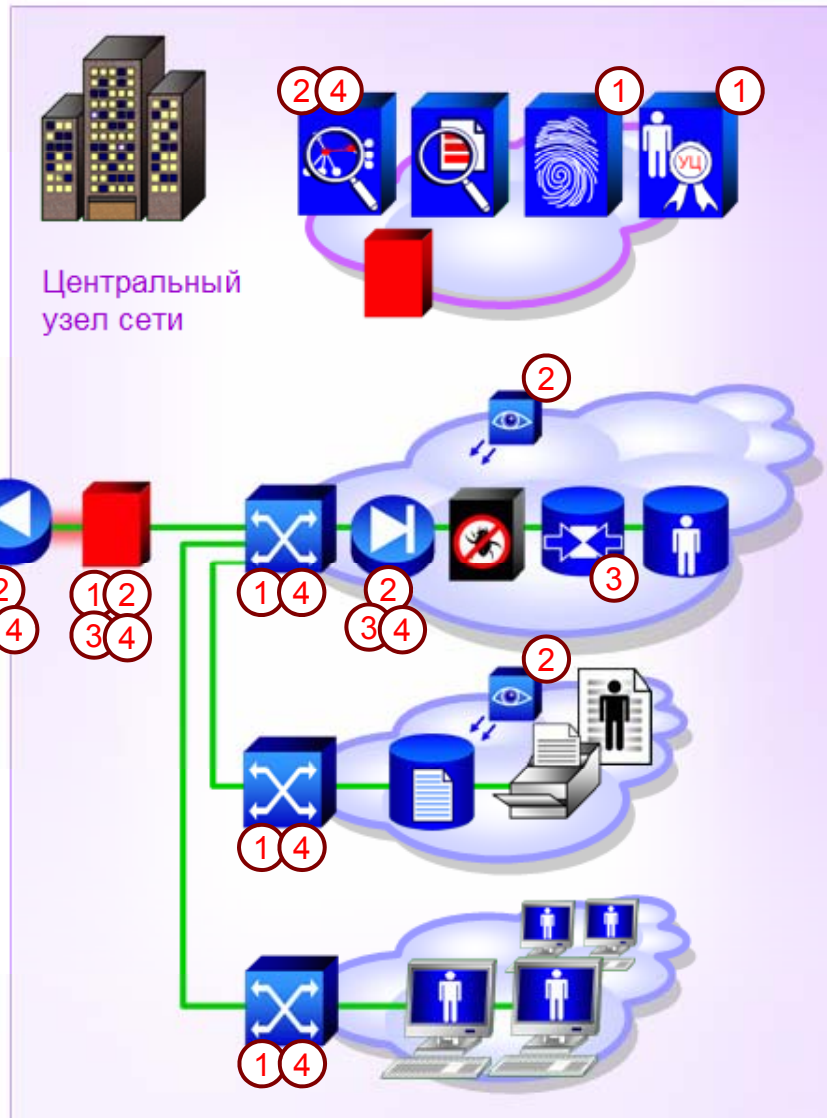
1. создание канала связи, обеспечивающего защиту передаваемой информации
2. осуществление аутентификации взаимодействующих систем и пользователей, целостность передаваемых данных
3. неотказуемость *) – для взаимодействия различных операторов

*) – дополнительно к 2.1, 2.4



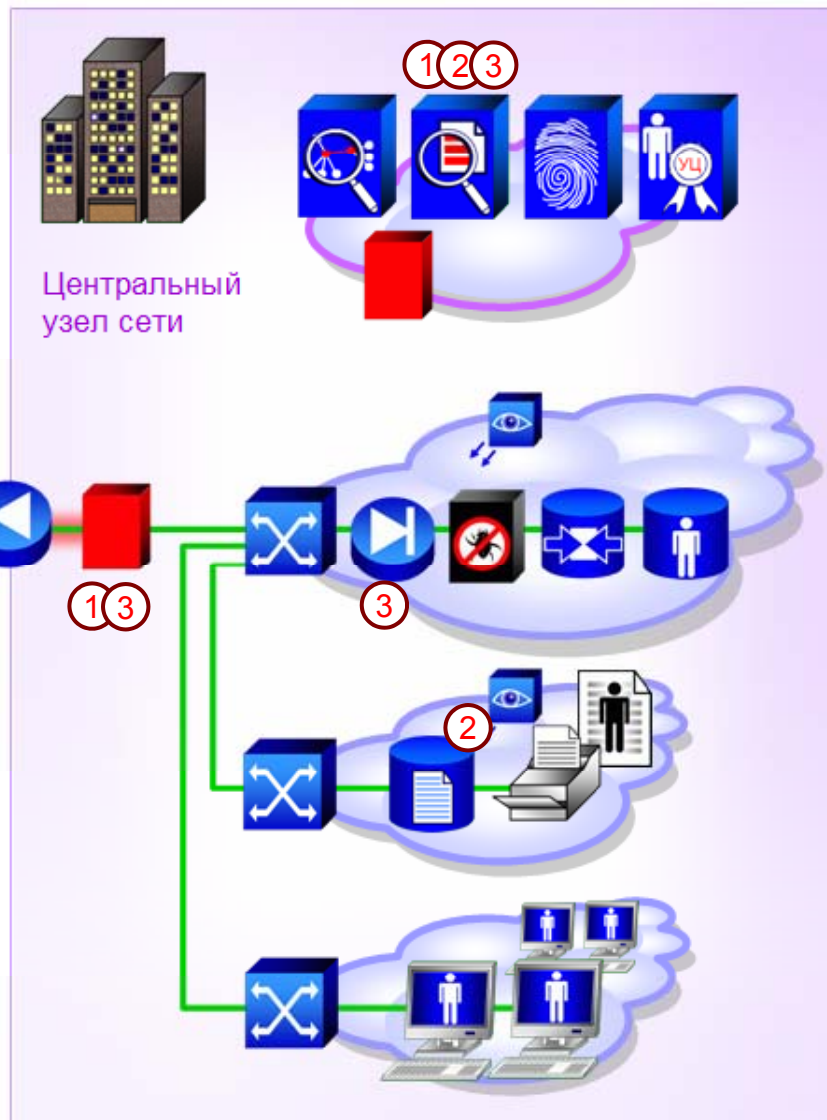
4.3 (а) управление доступом

1. идентификация и проверка подлинности (VPN: аутентификация) пользователя
2. идентификация терминалов, технических средств, узлов сети, каналов связи, внешних устройств по логическим именам *) - по DNS-имени, адресу; VPN: аутентификация
3. идентификация программ *) – по порту
4. контроль доступа пользователей к защищаемым ресурсам в соответствии с матрицей доступа *) - правила



4.3 (б) регистрация и учет

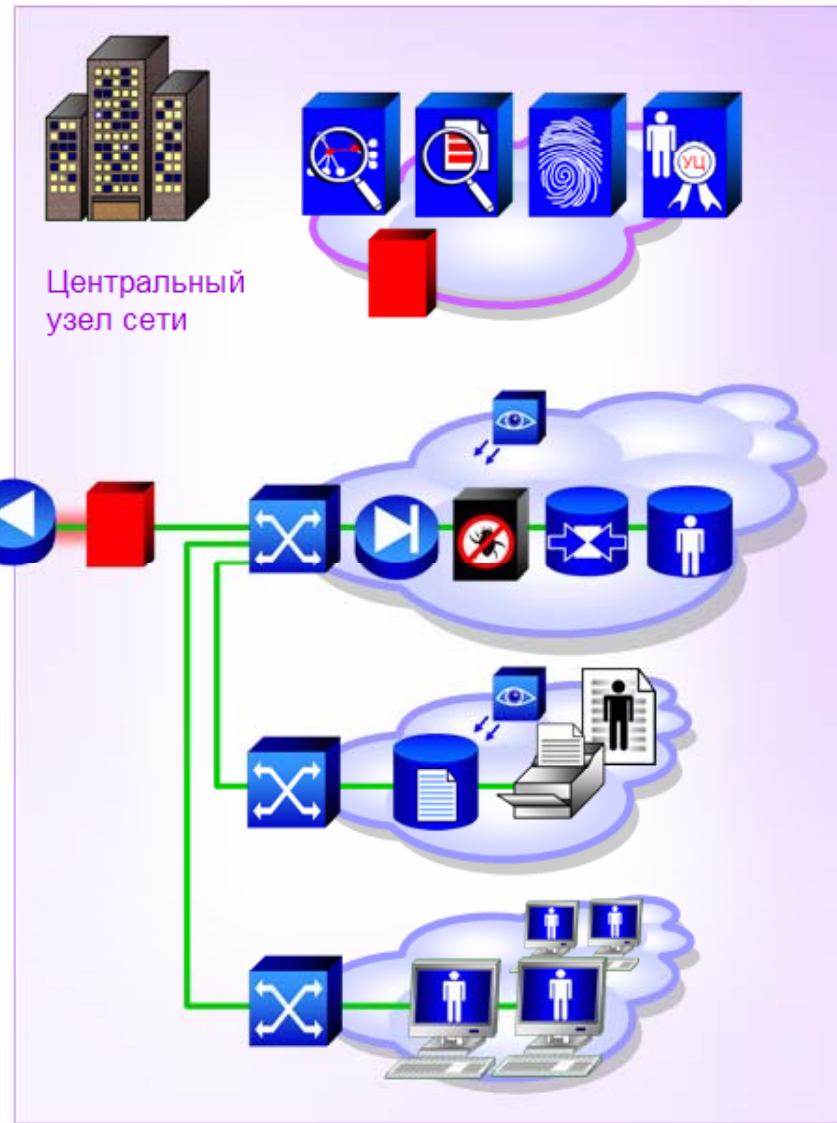
1. регистрация входа (выхода) пользователей *) – в сеть
2. регистрация выдачи печатных (графических) документов на бумажный носитель
3. регистрация попыток доступа программных средств к файлам и защищаемым объектам доступа



4.3 (в) обеспечение целостности

- 1. обеспечение целостности программных средств системы защиты персональных данных
- 2. периодическое тестирование функций системы защиты персональных данных
- 3. наличие средств восстановления системы защиты персональных данных

обеспечиваются различными элементами комплекса технических средств сетевой защиты

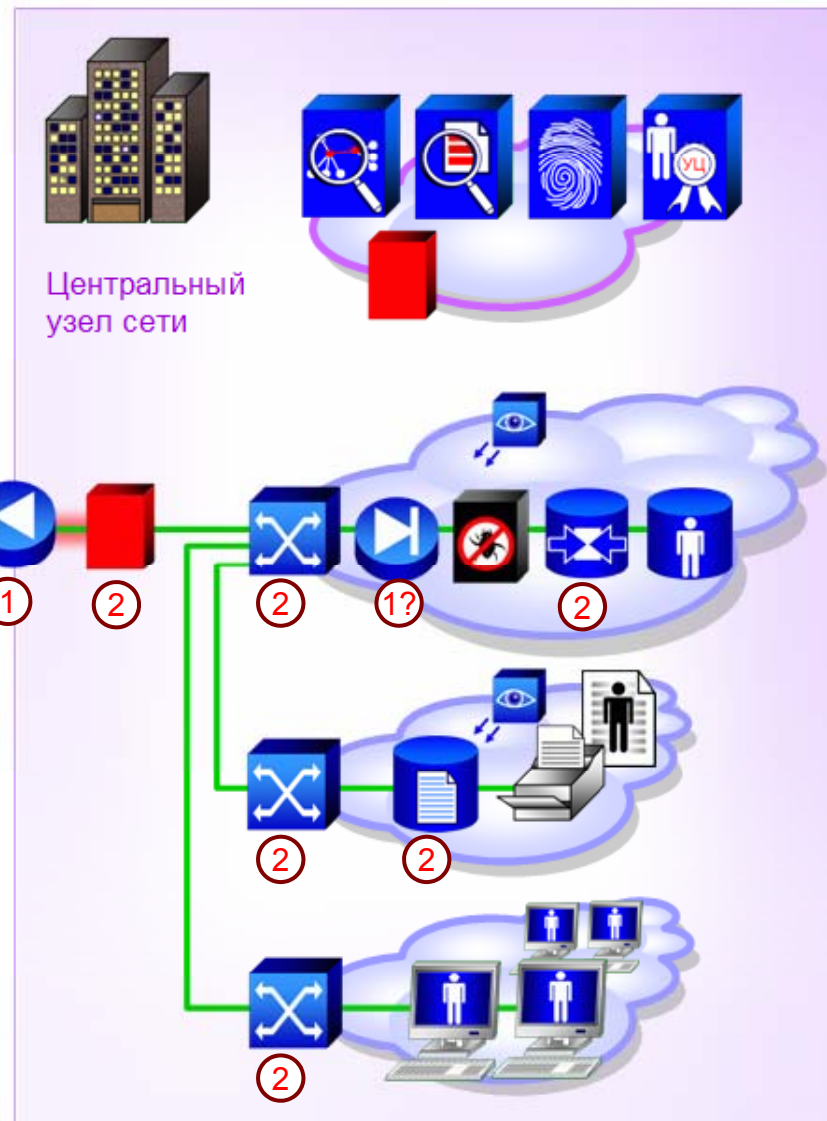
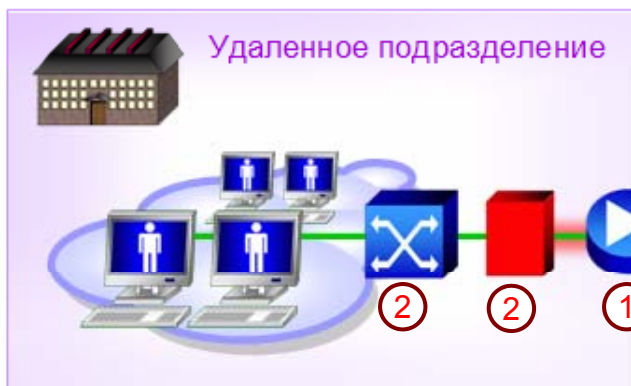


4.4 межсетевое экранирование

1. межсетевые экраны
2. прочие средства сетевого контроля доступа

Вопросы к межсетевому экрану:

- роль МЭ внутри ЛВС
- соответствие класса МЭ задаче доступа в Интернет



Сетевая безопасность ИСПДн
Механизмы безопасности
Сценарии защиты
Вопросы аттестации

Сценарии защиты

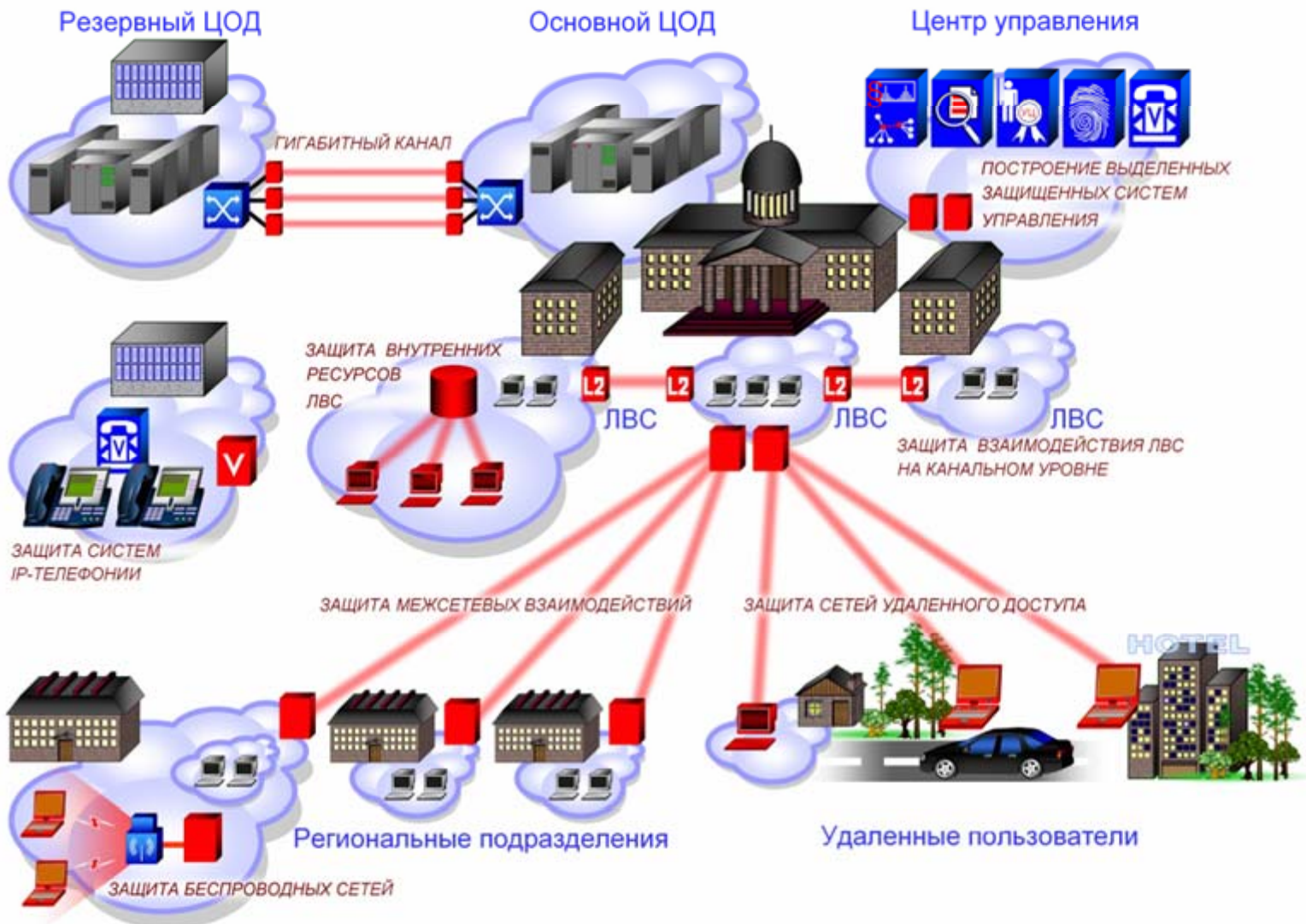
s•terra

c s p

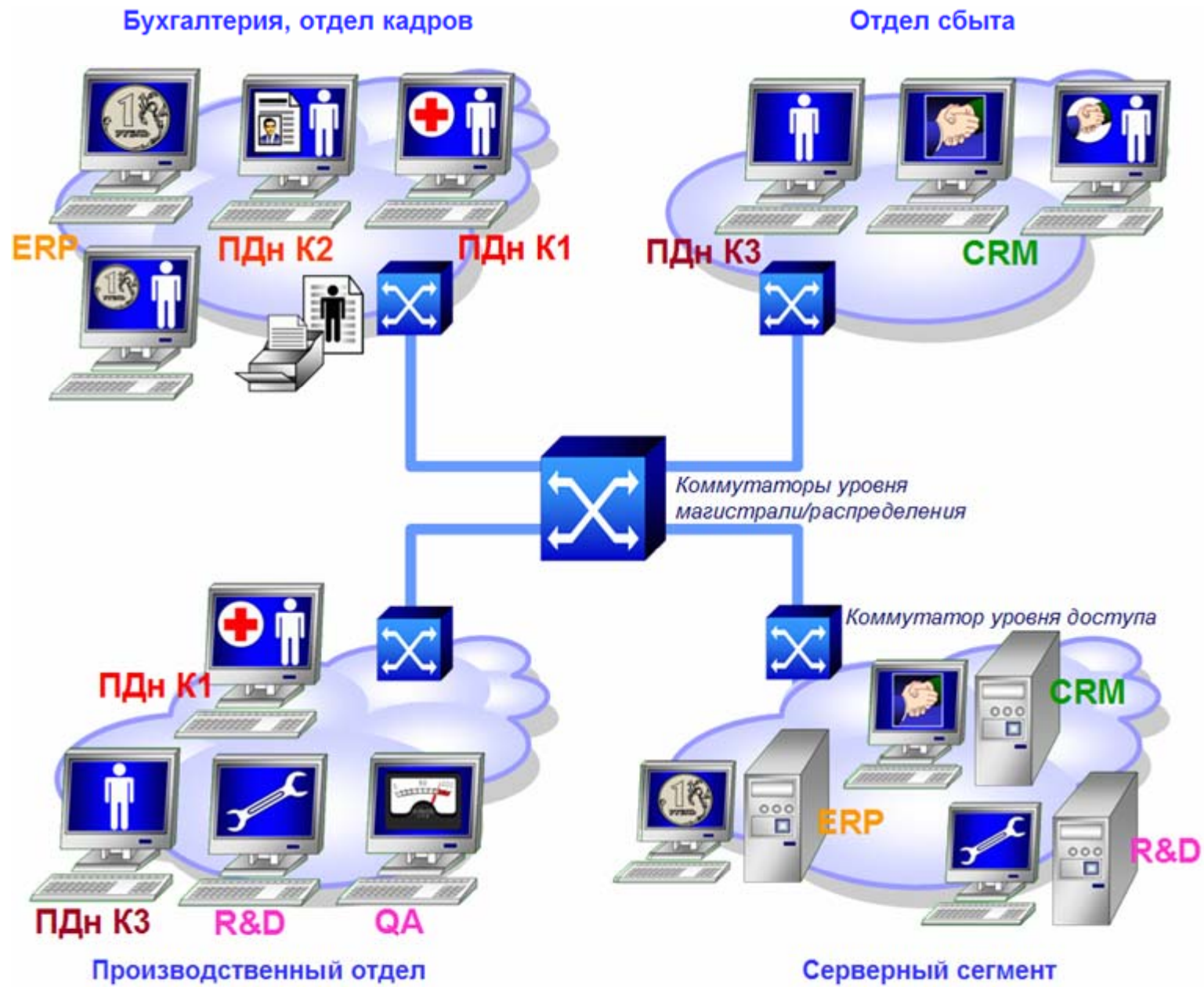
Cisco Solution Technology Integrator

● Сценарии защиты распределенных ИСПДн

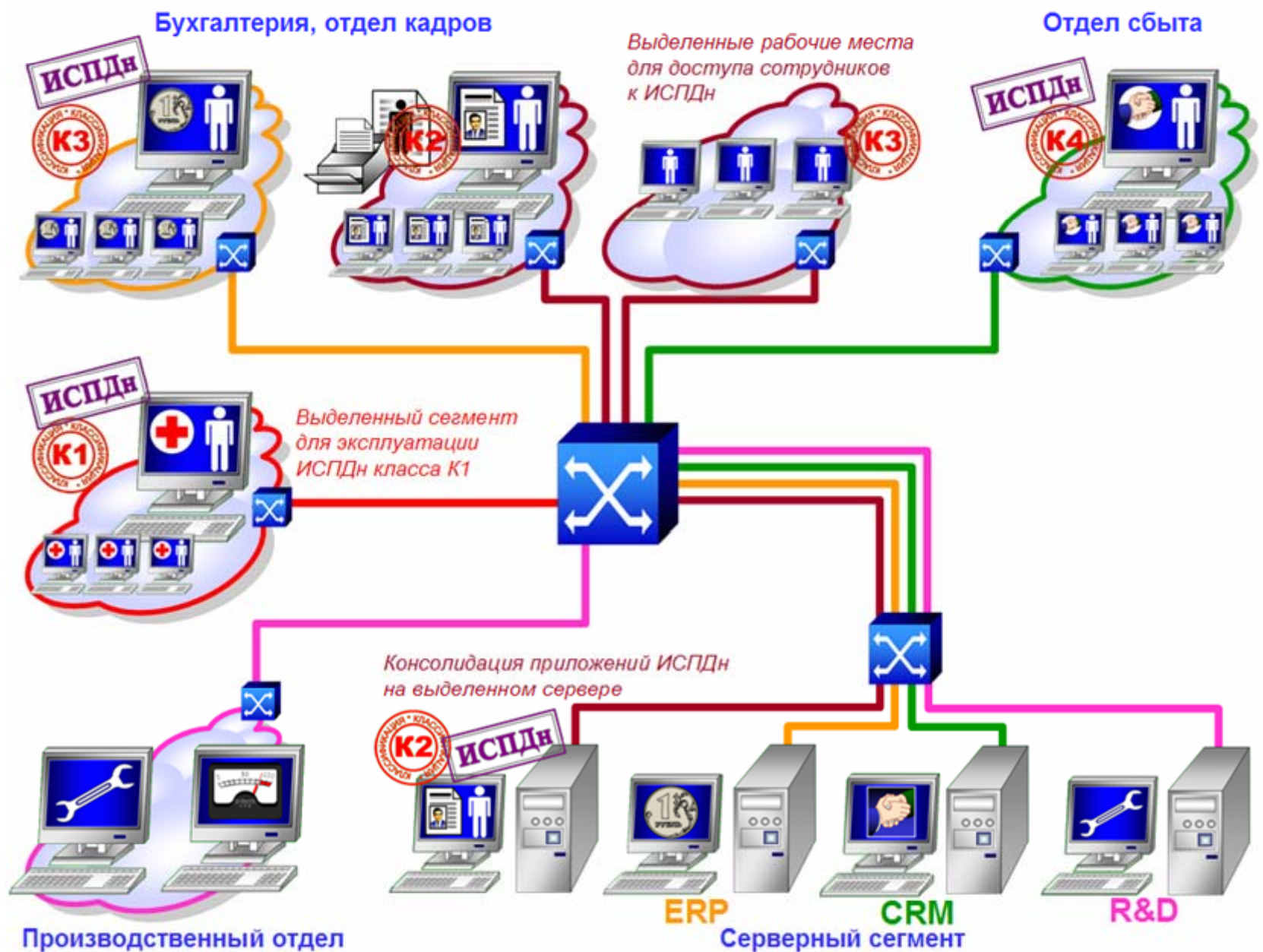
Для защиты ПДн могут применяться, в зависимости от структуры ИСПДн, любые сценарии построения VPN



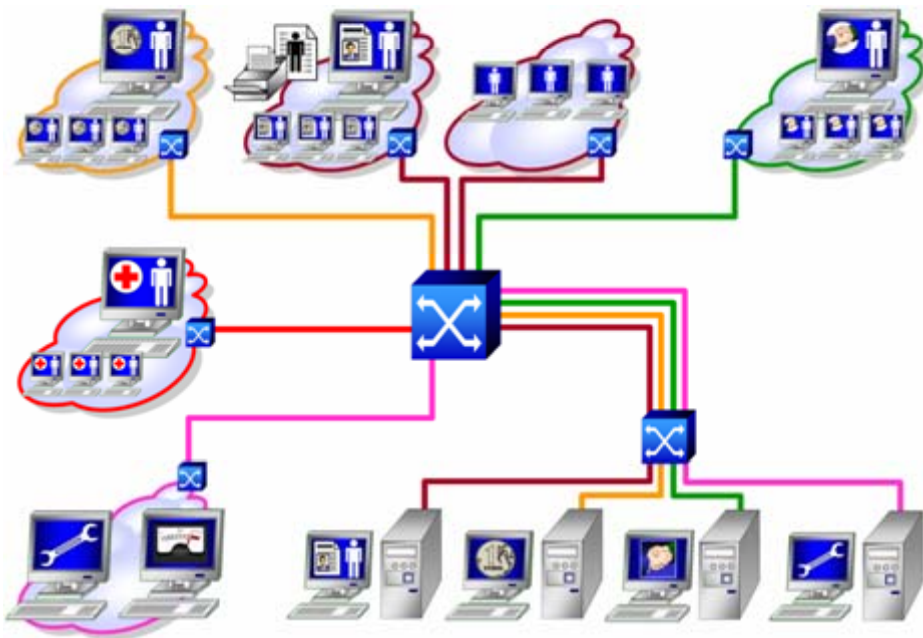
● Практические приемы защиты. Исходная сеть



● Сегментирование ИСПДн



● Технологии защиты сегментов ИСПДн



- Сегментирование ИСПДн выполняется путем перегруппировки приложений серверов и терминалов ИСПДн в отдельные сетевые сегменты и осуществления контроля доступа между сегментами
- Для этих целей могут применяться технологии:
 - физической перекоммутации устройств
 - построения виртуальных локальных сетей (VLAN) на основе протокола IEEE 802.1q и организации контроля доступа при объединении виртуальных сетей
 - организации мониторинга подключений к портам VLAN на основе MAC-адресов и мониторинга протоколов конфигурирования IP-адресов (ARP-мониторинг)
 - обеспечения аутентификации пользователя при подключении к портам VLAN (протокол 802.1x, в качестве систем аутентификации часто используются RADIUS-серверы)
- При необходимости инфраструктура контроля доступа на основе VLAN может быть организована не только в пределах офисного здания, но и транслироваться между локальными сетями по VAN-каналу
 - Для этого используются средства туннелирования канального уровня
 - Защищенный при помощи российских криптоалгоритмов туннель канального уровня можно построить при помощи продукта CSP L2VPN Gate

● Изоляция ИСПДн на сетевом уровне

- Изолировать ресурсы отдельной ИСПДн на сетевом уровне можно при помощи технологии IPsec VPN

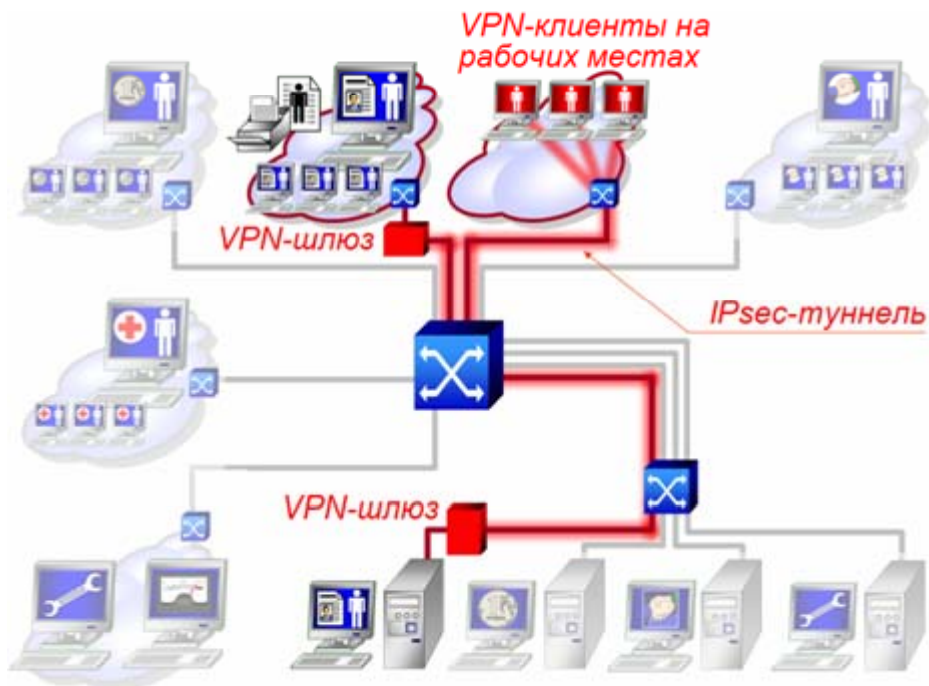
- для этого на терминалах ИСПДн должны быть установлены VPN-клиенты, а серверы – защищены при помощи программных VPN-продуктов или выделенных шлюзов безопасности

- выделенный шлюз можно рекомендовать в тех случаях когда:

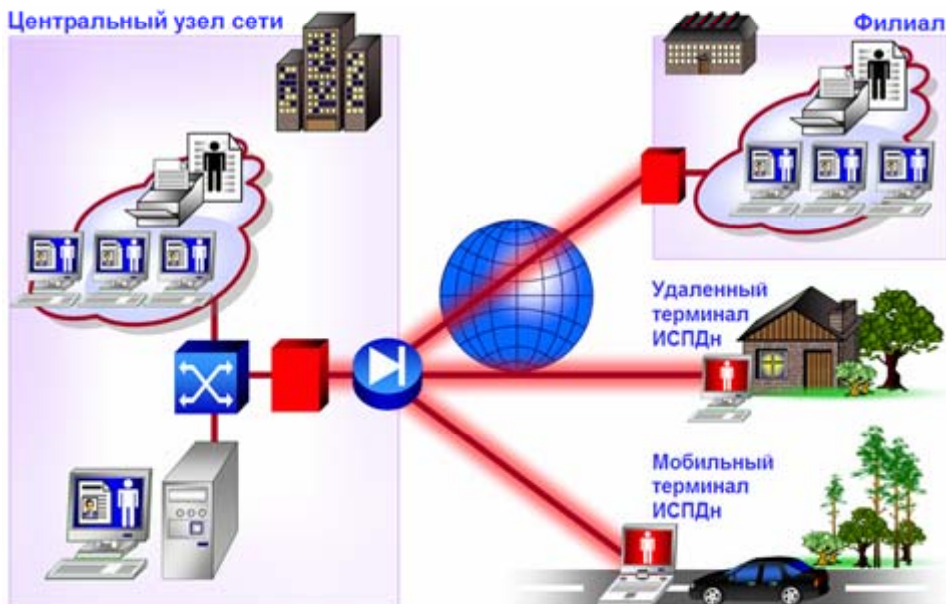
- сервер обслуживает большое количество пользователей и разнородных приложений, контроль за безопасностью среды функционирования VPN затруднен и эксплуатация криптографического приложения на нем нежелательна
- сервер работает в условиях высоких пиковых нагрузок и разделение процессорной мощности в криптографическом приложении может привести к существенному снижению производительности серверной системы

- вместо установки VPN-клиентов на терминалы ИСПДн можно использовать защиту сегмента в целом при помощи VPN-шлюза

- при построении VPN следует придерживаться принципа изоляции ИСПДн: следует минимизировать взаимодействие защищенного сегмента с внешним окружением, а в тех случаях, когда такое взаимодействие реально необходимо – обеспечить эффективный контроль доступа между защищенной ИСПДн и внешними сегментами сети



● Защита трафика ПДн в открытых сетях связи

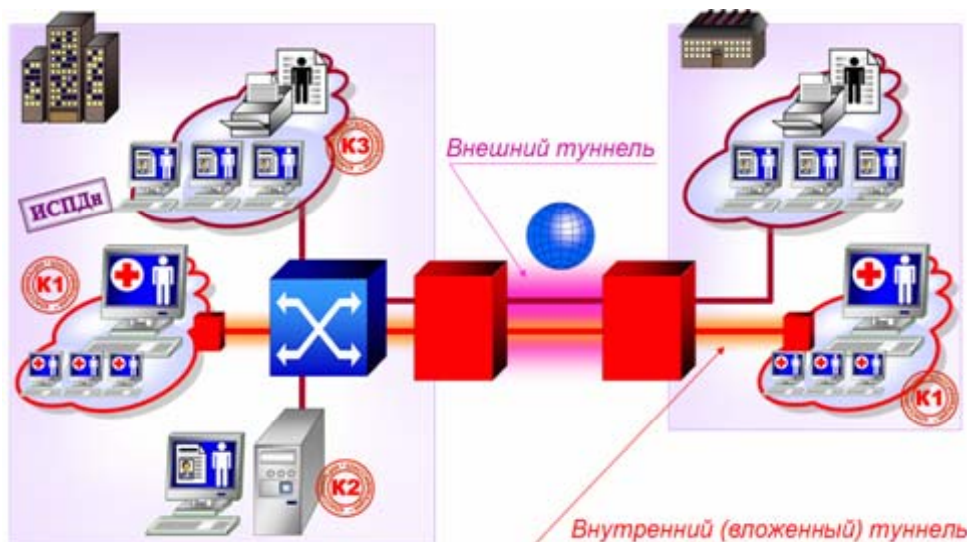


- Для распределенных ИСПДн, сегменты которых географически дистанцированы и объединены при помощи сетей связи общего пользования, технологии VPN являются естественным способом защитить данные в канале связи от их перехвата и компрометации
 - при этом целесообразно защищать корпоративную сеть в целом, поскольку защита только трафика ИСПДн
 - снижает общий уровень защищенности корпоративной сети, ее элементы могут быть компрометированы и служить плацдармом для вторичной атаки на сеть ИСПДн
 - демаскирует трафик ИСПДн
- Принципы дизайна VPN в этом случае – те же, что и в общих сценариях защиты межсетевых взаимодействий, удаленного доступа и т.п.

«Вложенная VPN» для изоляции ИСПДн К1

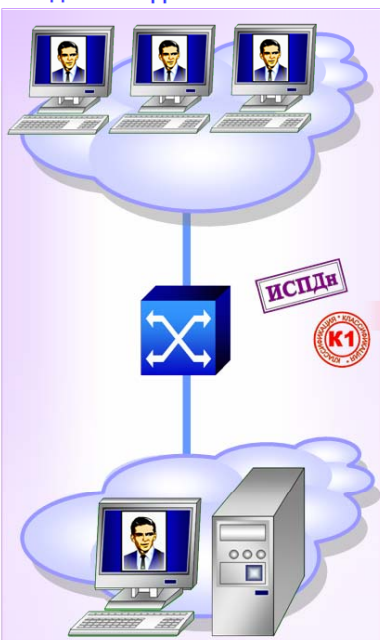
- Для ИСПДн, где присутствует четырехуровневая иерархия требований защиты, могут быть полезны сценарии построения «вложенных» VPN

- на рисунке показан пример в котором трафик ИСПДн К1, изолированный внутри периметра корпоративной сети, передается внутри «внешнего» туннеля, защищающего корпоративную сеть в целом
- для сценариев межсетевых взаимодействий такое туннелирование организуется весьма просто, но для удаленного доступа в ИСПДн К1 понадобится VPN-клиент, поддерживающий одновременно два туннеля: к внешнему периметру и к «вложенной» в него VPN, защищающей ИСПДн К1
 - допуск к «вложенной» VPN, минуя «внешний» контур, например, через межсетевой экран, может быть опасен
 - продукт CSP VPN Client поддерживает функциональность вложенного туннелирования

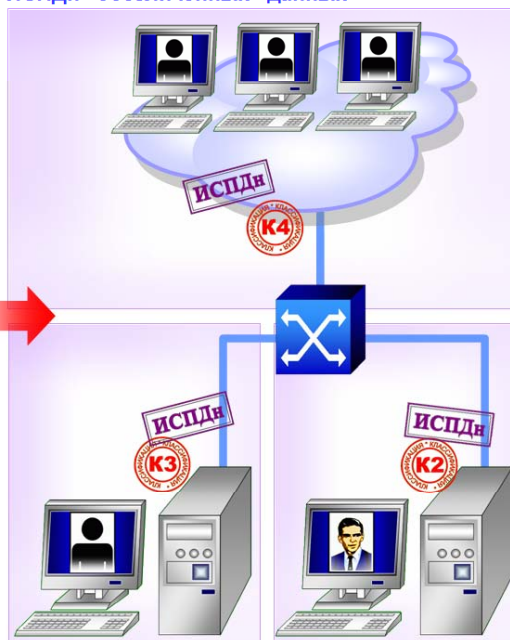


«Обезличивание», как прием защиты ПДн

Исходная ИСПДн

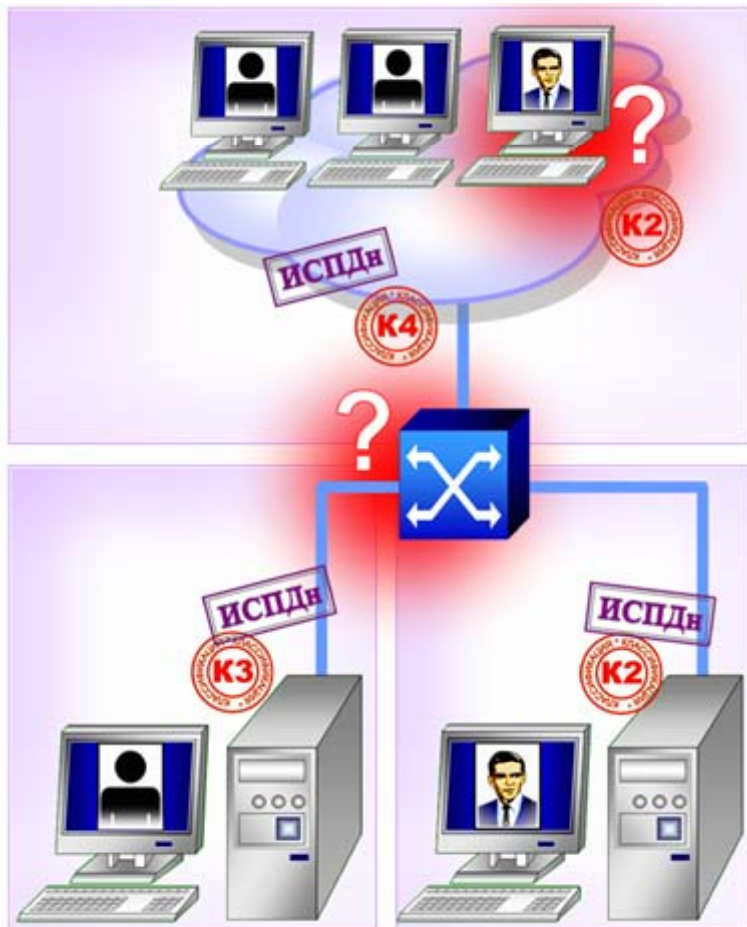


ИСПДн «обезличенных» данных



- Сегодня в среде специалистов активно обсуждаются сценарии технической реорганизации ИСПДн с целями обезличивания персональных данных
- Идея заключается в том, чтобы снизить класс ИСПДн путем отделения контекстной информации от идентификационной информации и разнесения контекстной и идентификационной информации по разным информационными системам (см. ИСПДн К1 в примере на рисунке)
 - это позволит защищать ИСПДн, обрабатывающую «обезличенные» данные, по классу К4, а идентификационную информацию, например, – по классам К2-К3
 - техническая практика разделения контекстной и идентификационной информации в индустрии давно используется в виде карт социального страхования, кредитных карт, подсистем управления персональными идентификаторами (Identity & Access Management, IAM)

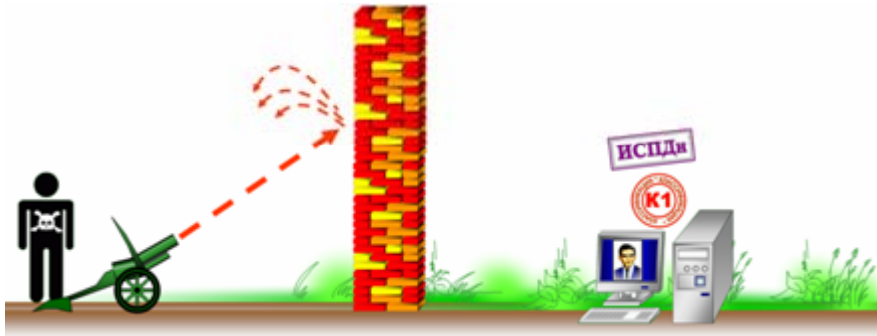
● Неприятные вопросы «обезлички»



- Несмотря на наличие такой практики, использование обезличивания персональных данных с целями снижения класса защиты системы (и, как следствие, снижения стоимости и стойкости применяемых мер защиты) вызывает вопросы:

1. Можно ли трактовать ли декомпозированную систему (ИСПДн с идентификационными данными + ИСПДн с обезличенными контекстными данными), как две независимых и независимо защищаемых ИСПДн?
 - дело в том, что «обезличенные» персональные данные без связи с идентификационной информацией утрачивают ценность: рентгеновский снимок конкретного пациента является критичной информацией категории 1, а «обезличенный снимок» - имел ценность только для записи «музыки на костях» до повсеместного распространения магнитофонов
2. Как классифицировать терминал, с которого производится одновременная работа с той и с другой системой?
 - поскольку обезличенные персональные данные приобретают ценность только во взаимосвязке с идентификационными данными, то в ИСПДн их обработки будут возникать узлы, на которых происходит одновременная обработка и контекстной и идентификационной информации
 - такие узлы, несмотря на усилия по организации «обезличивания» ПДн, могут на время обработки тех и других данных, приобретать классификацию исходной системы (в примере – ИСПДн K1)

● Необходимость сохранения стойкости защиты



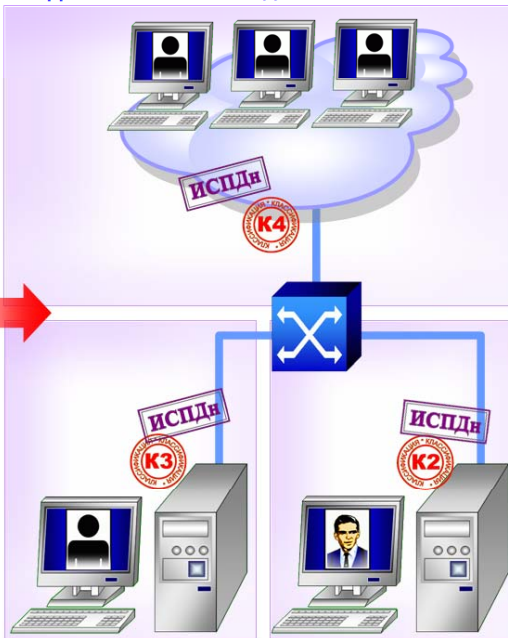
- Таким образом, снижение класса ИСПДн при «обезличивании» персональных данных может вести к катастрофическому снижению уровня защищенности системы в целом
- Если ИСПДн класса K1, в соответствии с действующим регулированием, должна быть надежно защищена, то требования на защиту систем класса K4 («обезличенные» данные) чрезвычайно низки
 - злоумышленник без труда проведет атаки на две слабо защищенные системы подсистемы с контекстными и идентификационными данными и, объединив результат двух атак, «дешево» получит данные 1й категории
 - по сути – он таким образом выполнит двустадийную атаку на ИСПДн класса K1
- Вывод заключается в том, что как минимум один из трех элементов:
 - ИСПДн «обезличенных» контекстных данных
 - ИСПДн идентификационных данных
 - или связь между нимидолжен иметь класс защиты не ниже и исходной ИСПДн, в которой контекстные и идентификационные данные были интегрированы

«Обезличивание» - to be or not to be?

Исходная ИСПДн



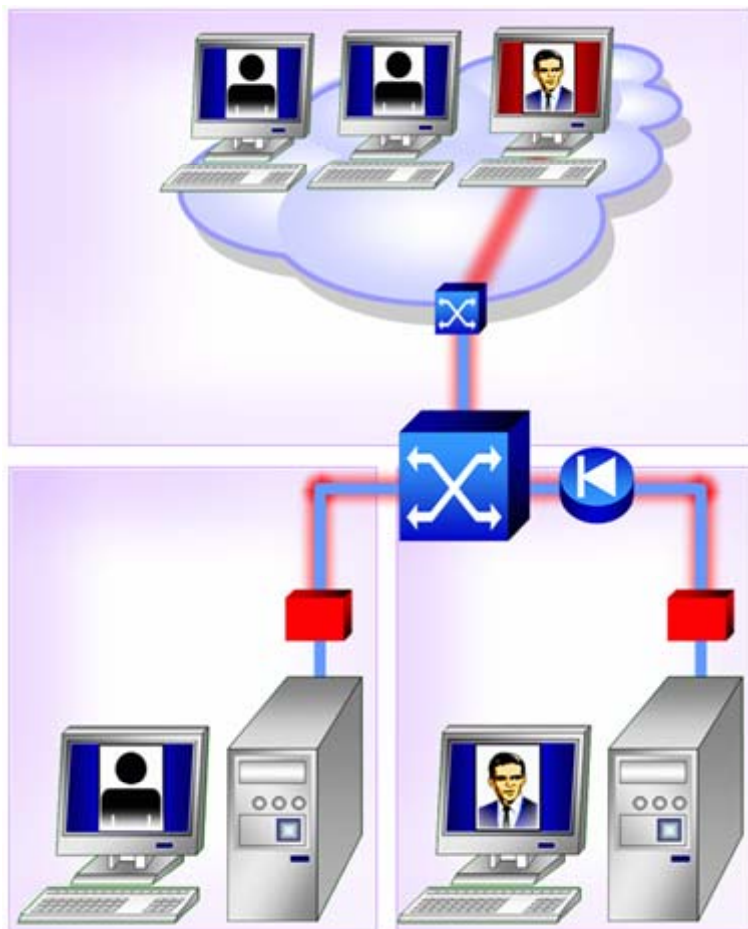
ИСПДн «обезличенных» данных



- Несмотря на необходимость поддерживать достаточно высокий уровень защиты составляющих ИСПД с обработкой «обезличенных» персональных данных, существует ряд доводов в пользу применения приема «обезличивания» ПДн

1. Ряд требований безопасности для отдельных компонентов системы может быть снижен. Например, если связь между контекстной и идентификационной информацией устанавливается только на фазе обработки данных, то требования к защите данных в фазе их хранения или передачи могут быть снижены
2. Структурирование данных может приводить к снижению их объемов, приходящихся на одну ИСПДн, это, в соответствии с действующим регулированием, является основанием для снижения класса системы
3. Задача обеспечения безопасности идентификационных данных в ряде случаев может быть передана в ответственность их владельцу (как это делается, например, в платежных системах). При этом идентификационные данные могут быть разрознены и для их хранения могут применяться специальные носители

● Сетевая защита при «обезличивании» ПДн



- При «обезличивании» персональных данных средства сетевой информационной безопасности могут применяться как для защиты ИСПДн контекстной и идентификационной информации, так и для связи между ними
- Поскольку при взаимодействии контекстной и идентификационной ИСПДн часто возникает задача аутентификации владельца идентификационных данных и подтверждения подлинности идентификационных данных – то средства IPsec VPN, поддерживающие множество механизмов строгой аутентификации, могут быть задействованы, как основные или дополнительные средства аутентификации

Сетевая безопасность ИСПДн
Механизмы безопасности
Сценарии защиты
Вопросы аттестации

Вопросы аттестации

s•terra

C S P

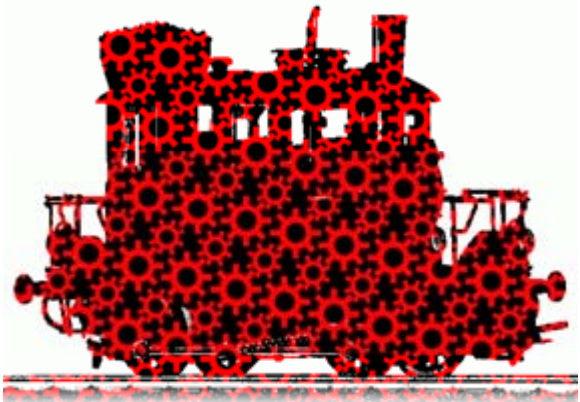
Cisco Solution Technology Integrator

● Классификация, ТЗ, ПСИ и аттестация ИСПДн



- Цель: установить минимальный обоснованный для Вашего бизнес-процесса класс ИСПДн
 - Учитывайте технические возможности снижения класса ИСПДн при построении системы защиты ИСПДн
- Этапы классификации ИСПДн
 - Инвентаризация и категорирование ПДн
 - Оценка объема ПДн
 - [Планирование мероприятий по снижению класса ИСПДн]
 - Обезличивание ПДн с целями снижение категории ИСПДн
 - Структурирование данных, деление систем обработки и сегментирование локальных сетей с целями снижения объема ПДн высоких категорий
 - Определение класса ИСПДн [с учетом плановых мероприятий по снижению класса ИСПДн]
- Требования к аттестации ИСПДн – разделом ТЗ
- Аттестационные испытания – в идеале в едином цикле с ПСИ ИСПДн

● Легитимизация VPN-периметра ИСПДн



- VPN (в функциональности ВЗС)– это коммуникационная среда со встроенным СКЗИ или это СКЗИ?
- Центр ФСБ России отвечает на этот вопрос однозначно:
 - VPN – это средство криптографической защиты
 - Основания для такого взгляда:
 - стойкость сервиса VPN существенно зависит от структуры и корректности реализации криптографического протокола
 - криптографический протокол в целом характеризуется параметрами криптографической стойкости
- Состав сертификатов VPN-продукта:
 - ФСБ России:
 - СКЗИ
 - ФСТЭК России:
 - НДВ

КОНТАКТЫ

e-mail: information@s-terra.com

web: <http://www.s-terra.com/>

Тел.: +7 (499) 940 9001

+7 (495) 726 9891

Факс: +7 (499) 720 6928

Вопросы?

Обращайтесь к нам!

s•terra

с s p

Cisco Solution Technology Integrator