s·terra
c s p

Сетевая безопасность персональных данных

СТАНДАРТ СЕТЕВОЙ БЕЗОПАСНОСТИ ДЛЯ РОССИЙСКОГО БИЗНЕСА

- Техническое регулирование
- Технические требования
- Сценарии защиты ИСПДн
- Архитектура защиты ИСПДн

Техническое регулирование

Структура нормативов

КОНСТИТУЦИЯ РФ. Глава 2. Статья 23

(«Каждый имеет право на неприкосновенность частной жизни ... тайну переписки, ... переговоров ... и иных сообщений»)

ФЗ № 152 от 26.07.2007 «О персональных данных»

(«Операторами ... должна обеспечиваться конфиденциальность [персональных] данных. Оператор ... обязан принимать необходимые организационные и технические меры ... для защиты персональных данных»)

Постановление Правительства №781 от 17.11.2007

(Утверждает «Положение об обеспечении безопасности ПДн...» Определяет органы надзора и технического регулирования)

Приказ ФСБ, ФСТЭК, Минсвязи России от 13.02.2008

(Устанавливает порядок классификации ПДн)

«Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» (21.02.2008, № 149/5-144)

«Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных» (21.02.2008, № 149/6/6-622)

«Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (14.02.2008)

«Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (14.02.2008)

«Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» (14.02.2008)

«Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (14.02.2008)

Что требуется от оператора ИСПДн?

- Уведомительная регистрация о деятельности оператора
- Лицензирование деятельности
- Классификация ИСПДн
- Разработки и согласование модели угроз
- Построение системы информационной безопасности ИСПДН
- Оценка системы информационной безопасности ИСПДн
  - Для классов ИСПДн К1, К2 – *аттестация*
  - Для класса ИСПДн К3 – *декларируемая оператором оценка соответствия* (может являться объектом проверки со стороны органов регулирования) или *аттестация* (по усмотрению оператора)
  - Для класса ИСПДн К4 – оценка соответствия *относится на усмотрение оператора*

Без ... инструмента – не разберешься!

Технические требования

s·terra
csp
Cisco Solution Technology Integrator

Классификация ИСПДн

- **Ваша цель: установить минимальный обоснованный для Вашего бизнес-процесса класс ИСПДн – это мера способствует снижению информационных рисков ПДн, снижению затрат и, в конечном итоге, упрощению аттестации системы и согласию с органами технического регулирования при проверке соответствия**
  - **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]**

Модель угроз, рекомендации регуляторов

- **При разработке модели угроз [1] принимают во внимание**
  - ***Оценку возможности реализации***
    - **Уровень исходной защищенности ИСПДн**
    - **Частота (вероятность) реализации рассматриваемой угрозы**
  - ***Вероятность реализации* угрозы**
  - **По этим показателям рассчитывается *коэффициент реализуемости угрозы* и с учетом *опасности угрозы* выносится решение об *актуальности* (т.е. необходимости компенсации рисков) угрозы или ее *неактуальности* (возможности принятия рисков)**
- **В соответствии с документом [2], проведите разработку «Модели нарушителя информационной безопасности»**
  - **Технический анализ должен учитывать, *кто* нападает, *на что* нападает (ИСПДн) и *как* нападает (метод реализации угрозы – канал атаки)**
  - **Понятие «атака» также весьма ценно проектировании системы защиты, причем в сети необходимо анализировать как *логические* (сетевой протокол, контекст данных, цепочка событий атаки), так и *топологические* аспекты понятия «канал атаки»**

1. **«Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (14.02.2008)**
2. **«Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» (21.02.2008, № 149/5-144)**

Технические требования, формат описания

- Ниже приведен анализ технических треований по защите ИСПДн
- В анализ не включены:
  - ИСПДн К4, как не требующие высокого уровня защищенности
  - Однопользовательские ИСПДн, как не требующие распределенной обработки ПДн
- Требования представлены в виде таблицы

Требование	ИСПДн К3		ИСПДн К2		ИСПДн К1	
	=	≠	=	≠	=	≠
<Содержание требования>				+	+	+

где приняты обозначения:

=	многопользовательская ИСПДн с равными правами доступа пользователей
≠	многопользовательская ИСПДН с различными правами доступа пользователей
	требование не установлено для ИСПДн данного класса
+	требование установлено для ИСПДн данного класса
	выполнение требования усиливается в случае применения средств сетевой информационной безопасности *(см. доп. информацию в примечаниях)*
	выполнение требования полностью обеспечивается применением продуктов CSP VPN [и инфраструктуры их эксплуатации] *(см. доп. информацию в примечаниях)*

Идентификация, аутентификация, контроль доступа

Требование		ИСПДн К3		ИСПДн К2		ИСПДн К1	
		=	≠	=	≠	=	≠
Идентификация и аутентификация при входе в ОС	(1)	+	+	+	+	+	+
Регистрация входа/выхода в ОС			+		+		+
Идентификация ТС, каналов связи по адресам (номерам)	(2)				+		+
Идентификация программ, томов, каталогов, файлов, записей					+		+
Ролевое управление доступом к СЗИ и функциям управления	(3)						+
Защита данных аутентификации от НСД	(4)						+
Автоматическая идентификация и аутентификация ТС ИСПДн	(5)						+

ПРИМЕЧАНИЯ:

1. Средства сетевой безопасности могут включаться в цепь событий аутентификации при доступе к ОС и использовать общую с ОС инфраструктуру аутентификации.
2. Средства сетевой защиты поддерживают развитую систему способов идентификации и именования сетевых объектов. Имена объектов могут использоваться в правилах политики безопасности сетевых СЗИ, контролирующих доступ к отдельным ТС.
3. Продукты CSP VPN могут быть использованы для построения выделенных защищенных сетей управления (out of band management network), в которых для отдельных операторов могут быть реализованы индивидуальные правила доступа.
4. Данные серверов систем аутентификации и каналы доступа к ним могут быть изолированы оо постороннего доступа путем включения их в выделенную виртуальную защищенную сеть аутентификации.
5. Средства сетевой защиты поддерживают системы управления IP-адресами, службы имен, доменов, identity management и способны динамически управлять этими параметрами и выступать как средства автоматизации идентификации и аутентификации.

Сетевой контроль доступа, МЭ (*)

Требование	ИСПДн К3		ИСПДн К2		ИСПДн К1	
	=	≠	=	≠	=	≠
Конфиденциальность ПДн в распределенных ИСПДн вне К3 (1)	+	+	+	+	+	+
Использование МЭ при взаимодействии с открытыми сетями	+	+	+	+	+	+
Класс МЭ при взаимодействии с открытыми сетями (2)	5	5	4	4	3	3
Система трансляции сетевых адресов (NAT)					+	+
Управление потоками информации на основе меток конфиденц. (3)					+	+

(*) **МЭ – межсетевой экран**

ПРИМЕЧАНИЯ:

1. Обеспечивается применением VPN. Помимо свойства конфиденциальности (для типовых ИСПДн), VPN может обеспечивать целостность данных и потока данных а также эффективный сетевой контроль доступа (изоляцию информационного пространства ИСПДн).
2. Указан класс МЭ в соответствии с Руководящим документом «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации», Гостехкомиссия России, 1997
3. Средства сетевой безопасности могут как непосредственно поддерживать механизмы контроля доступа на основе меток конфиденциальности, так и применяться, как эффективный механизм управления сетевыми потоками, косвенно связанный с метками безопасности или другими механизмами целостности и аутентификации источника данных.

Режим защиты носителей информации

Требование	ИСПДн К3		ИСПДн К2		ИСПДн К1	
	=	≠	=	≠	=	≠
Учет и маркировка всех защищаемых носит	+	+	+	+	+	+
Регистрация и маркировка печатных носителей					+	+
Дублирование учета операций с носителями информации					+	+
Очистка оперативной памяти и внешних накопителей					+	+
Автомат. учет созд. защ. файлов и исп. маркировки в СКД					+	+
Контр. соотв. уровня метки и носителя при управлении потоками на основе меток (1)					+	+

ПРИМЕЧАНИЕ:

1. Средства сетевой безопасности могут как непосредственно поддерживать механизмы контроля доступа на основе меток конфиденциальности, так и применяться, как эффективный механизм управления сетевыми потоками, косвенно связанный с метками безопасности или другими механизмами целостности и аутентификации источника данных.

Применение СКЗИ

Требование	ИСПДн К3		ИСПДн К2		ИСПДн К1	
	=	≠	=	≠	=	≠
Шифрование съемных носителей ПДн					+	+
Шифрование долговр. носителей за пределами сеанса работы					+	+
Шифрование ПДн при передаче по каналам связи (1)					+	+
Контроль доступа к СКЗИ (2)					+	+
Применение сертифицированных СКЗИ					+	+

ПРИМЕЧАНИЕ:

1. Обеспечивается средствами VPN. Для специфических ИСПДн могут обеспечиваться также свойства целостности данных, целостности потока данных, аутентификации источника данных.
2. Для части задач управления СКЗИ и ключевыми документами средствами сетевой защиты и VPN может быть создана изолированная сеть управления (out of band management network)/

Требования к анти-вирусной защите

Требование	ИСПДн К3		ИСПДн К2		ИСПДн К1	
	=	≠	=	≠	=	≠
Автоматическая антивирусная проверка	+	+	+	+	+	+
Автоматическое удаление или блокирование вирусов	+	+	+	+	+	+
Автоматическая регулярная проверка СЗИ	+	+	+	+	+	+
Автоматический запуск антивируса при обнаружении атаки (1)	+	+	+	+	+	+
Автоматическая а/в проверка взаимодействий с внешними ИС			+	+	+	+

ПРИМЕЧАНИЕ:

1. Выполняется средствами обнаружения проникновения.

Требования к системе защиты от ПМВ

Требование	ИСПДн К3		ИСПДн К2		ИСПДн К1	
	=	≠	=	≠	=	≠
Идентификация и аутентификация при доступе к СЗ ПМВ	+	+	+	+	+	+
Автоматический непрерывный мониторинг проявлений ПМВ (1)	+	+	+	+	+	+
Регистрация запуска/останова, входа/выхода в/из СЗ ПМВ	+	+	+	+	+	+
Регистрация событий доступа программных средств к СЗ ПМВ	+	+	+	+	+	+
Регистрация попытки обнаружить СЗ ПМВ (2)	+	+	+	+	+	+
Регистрация обновлений и событий отката СЗ ПМВ	+	+	+	+	+	+
Автомат. контроль проявления ПМВ в каналах связи ИСПДн (1)			+	+	+	+

(*) **ПМВ – программно-математическое воздействие**

ПРИМЕЧАНИЕ:

1. Выполняется средствами обнаружения проникновения.
2. Попытки обнаружения системы защиты от программно-математических воздействий могут быть также выявлены средствами сетевого контроля доступа.

Требования к системе защиты от ПМВ (продолжение)

Требование	ИСПДн К3		ИСПДн К2		ИСПДн К1	
	=	≠	=	≠	=	≠
Контроль исполняемых модулей для каждого субъекта доступа (1)					+	+
Применение контроля доступа по группам операций СЗ ПМВ					+	+
Автомат. проверка ПО на ПМВ путем проверочной активации					+	+

ПРИМЕЧАНИЕ:

1. При сетевом доступе средства сетевой защиты могут контролировать объекты доступа (идентифицируя программные модули по адресу и порту). Также средствами VPN можно построить правила доступа для всех разрешенных для данного субъекта соединений и исключить его доступ к другим (запрещенным) сетевым объектам.

Требования к системе регистрации событий

Требование	ИСПДн К3		ИСПДн К2		ИСПДн К1	
	=	≠	=	≠	=	≠
Регистрация входа/выхода в/из ОС, ее запуск и останов	+	+	+	+	+	+
Защита данных регистрации от уничтожения и модификации (1)	+	+	+	+	+	+
Регистрация печатаемых документов				+	+	+
Регистр. запуска/завершения процессов обработки защ. файлов				+	+	+
Регистрация попыток доступа ПО к защищаемым файлам				+	+	+
Регистр. попыток доступа ПС к узлам сети, линиям связи (2)					+	+
Регистр. попыток доступа ПС к периферии, программам, файлам, записям					+	+
Регистрация изменений полномочий субъектов доступа						+

ПРИМЕЧАНИЯ:

1. Обеспечивается применением VPN. Помимо свойства конфиденциальности (для типовых ИСПДн), VPN может обеспечивать целостность данных и потока данных а также эффективный сетевой контроль доступа (изоляцию информационного пространства ИСПДн).
2. Указан класс МЭ в соответствии с Руководящим документом «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации», Гостехкомиссия России, 1997
3. Средства сетевой безопасности могут как непосредственно поддерживать механизмы контроля доступа на основе меток конфиденциальности, так и применяться, как эффективный механизм управления сетевыми потоками, косвенно связанный с метками безопасности или другими механизмами целостности и аутентификации источника данных.

Мониторинг и аудит

Требование		ИСПДн К3		ИСПДн К2		ИСПДн К1	
		=	≠	=	≠	=	≠
Мониторинг аномалий (проявлений ПМВ)	(1)	+	+	+	+	+	+
Автоматический аудит данных регистрации по сигнатурам атак		+	+	+	+	+	+
Блокирование атак и уведомление администратора	(2)	+	+	+	+	+	+
Периодическое применение сканеров безопасности		+	+	+	+	+	+
Выявление попыток нарушения и сигнализация	(1)						+

ПРИМЕЧАНИЕ:

1. Выполняется средствами обнаружения проникновения.
2. Выполняется сетевыми средствами противодействия атаке.

Целостность системно-технических средств и СЗИ

Требование	ИСПДн К3		ИСПДн К2		ИСПДн К1	
	=	≠	=	≠	=	≠
Неизменность программной среды	+	+	+	+	+	+
Проверка целостности ОС, обновлений при загрузке	+	+	+	+	+	+
Наличие резервных копий СЗИ	+	+	+	+	+	+
Процессы тестирования, восстановления, обновления СЗИ	+	+	+	+	+	+
Резервное копирование ПДн на отчуждаемые носители			+	+	+	+
Автомат. контроль корректности функционирования ТС ИСПДн (1)					+	+
Автомат. восстановление ТС СЗ ПМВ после сбоев					+	+

ПРИМЕЧАНИЕ:

1. Некорректное сетевое поведение ТС ИСПДн может выявляться, помимо прочего, детекторами аномалий средств обнаружения проникновений и средствами сетевого контроля доступа.

Требования по режиму эксплуатации ИСПДн

Требование	ИСПДн К3		ИСПДн К2		ИСПДн К1	
	=	≠	=	≠	=	≠
Физическая охрана ТС ИСПДн	+	+	+	+	+	+
Физическая охрана носителей ПДн, в т.ч. хранилищ носителей	+	+	+	+	+	+
Постоянное наличие охраны, строгий пропускной режим					+	+
Специальное оборудование помещений ИСПДн					+	+
Выделенный администратор ИБ					+	+
Блокирование терминалов, в т.ч. по периоду неактивности (1)						+

ПРИМЕЧАНИЯ:

1. Обеспечивается применением VPN. Помимо свойства конфиденциальности (для типовых ИСПДн), VPN может обеспечивать целостность данных и потока данных а также эффективный сетевой контроль доступа (изоляцию информационного пространства ИСПДн).
2. Указан класс МЭ в соответствии с Руководящим документом «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации», Гостехкомиссия России, 1997
3. Средства сетевой безопасности могут как непосредственно поддерживать механизмы контроля доступа на основе меток конфиденциальности, так и применяться, как эффективный механизм управления сетевыми потоками, косвенно связанный с метками безопасности или другими механизмами целостности и аутентификации источника данных.

Сетевая безопасность персональных данных

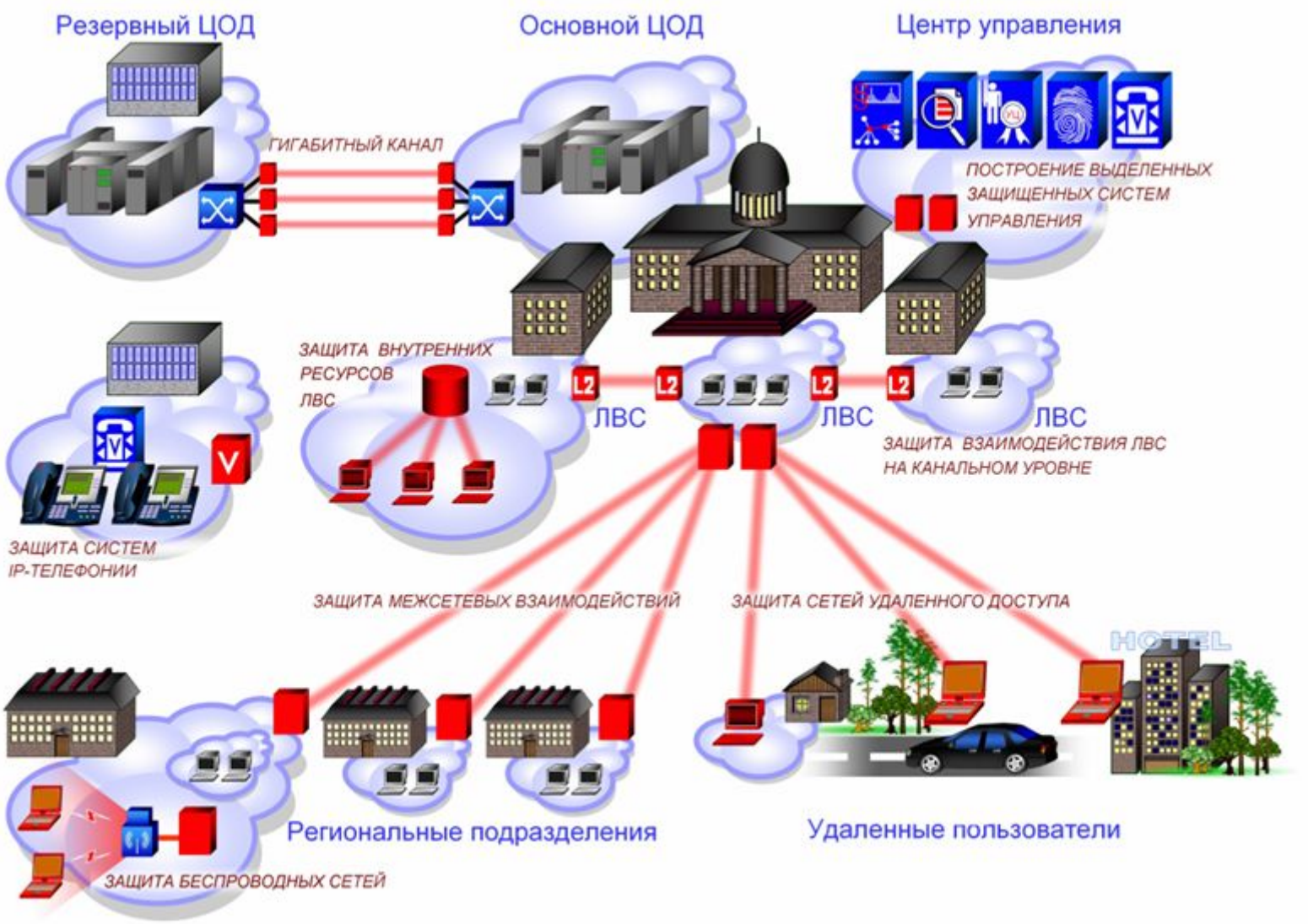
Техническое регулирование
Технические требования
Сценарии защиты ИСПДн
Архитектура защиты ИСПДн

Сценарии
и практические приемы сетевой
защиты ИСПдн

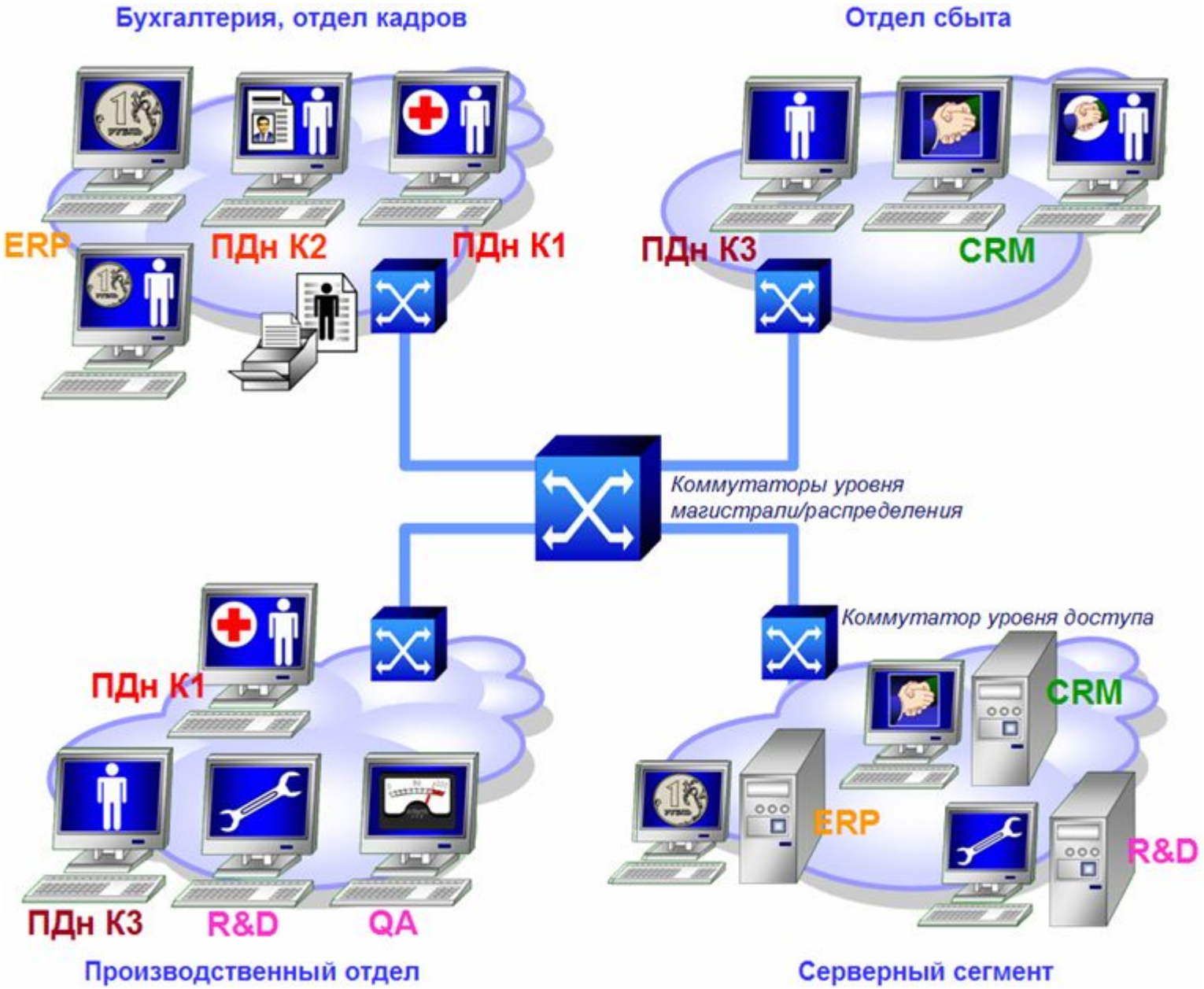
s·terra
csp
Cisco Solution Technology Integrator

Сценарии защиты распределенных ИСПДн

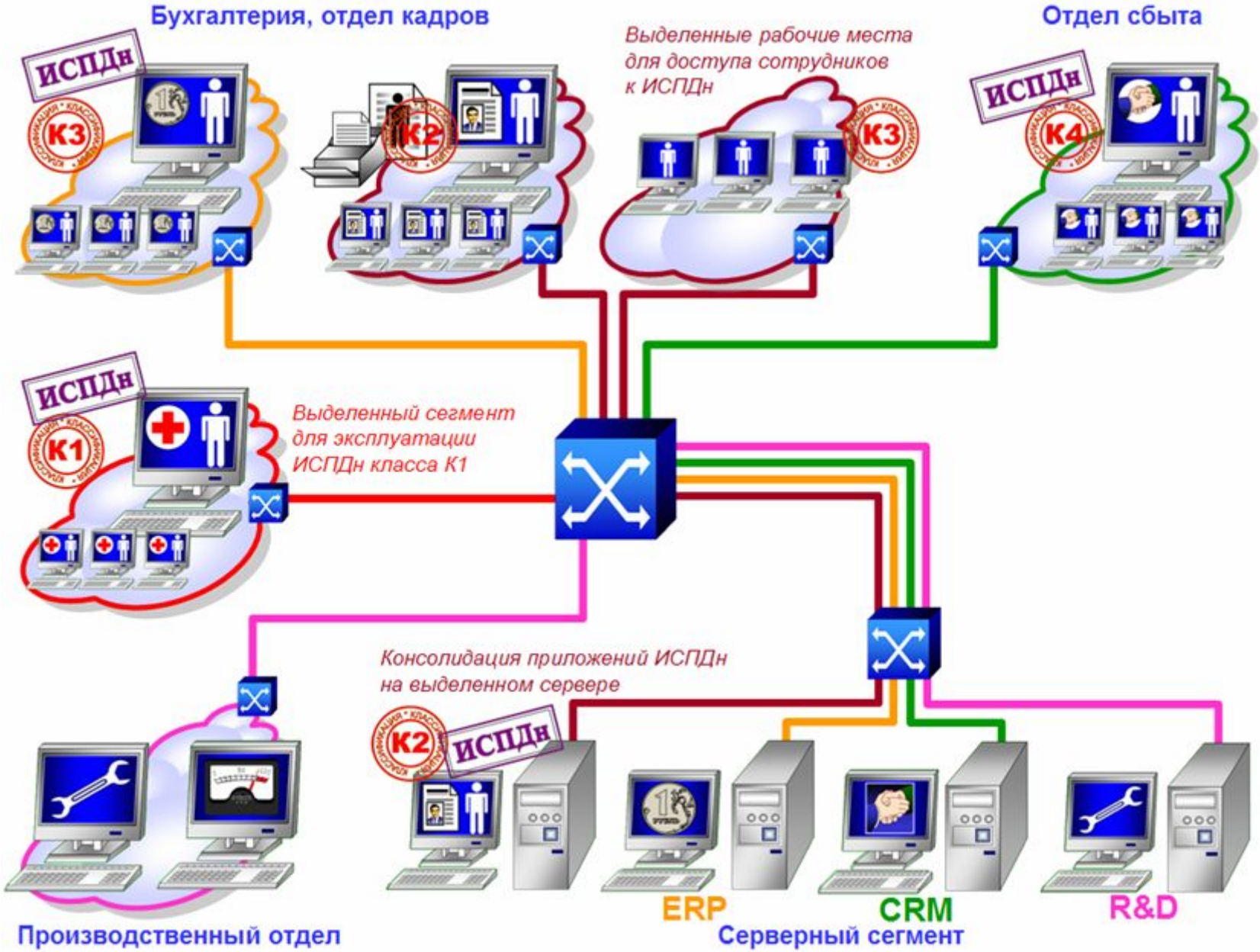
Для защиты ПДн могут применяться, в зависимости от структуры ИСПДн, любые сценарии построения VPN



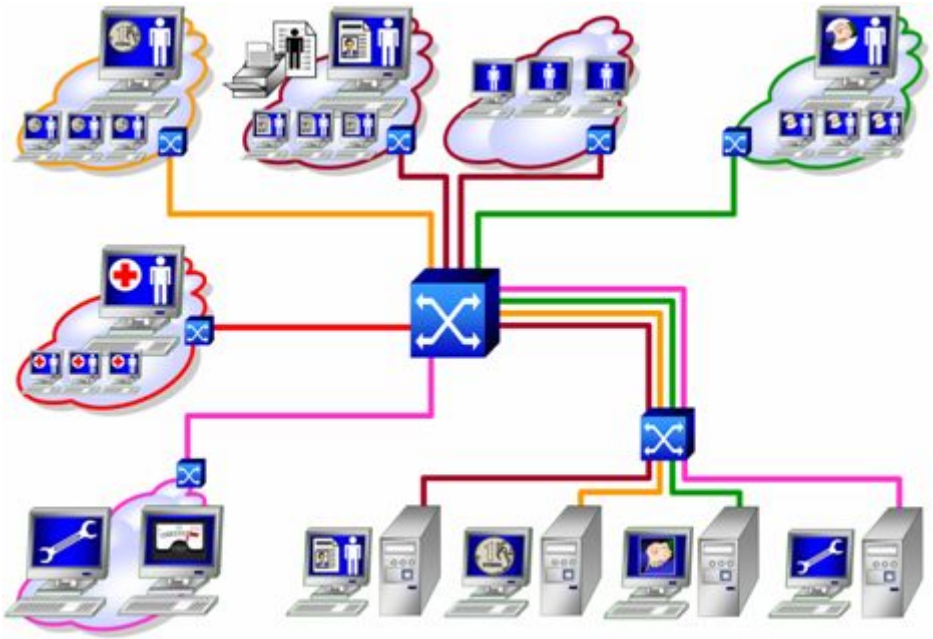
Практические приемы защиты. Исходная сеть



Сегментирование ИСПДн

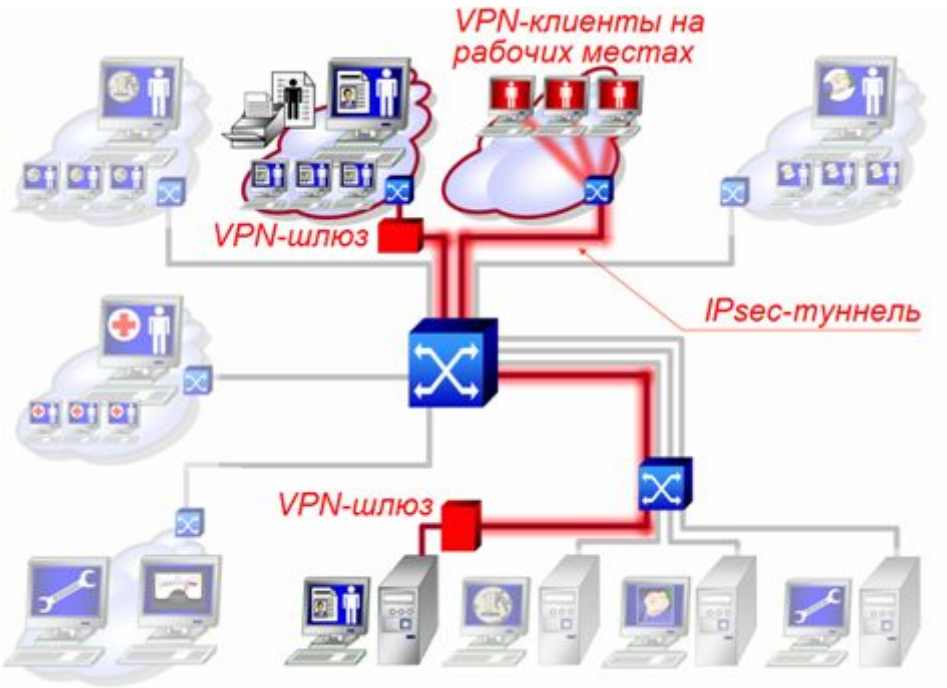


Технологии защиты сегментов ИСПДн



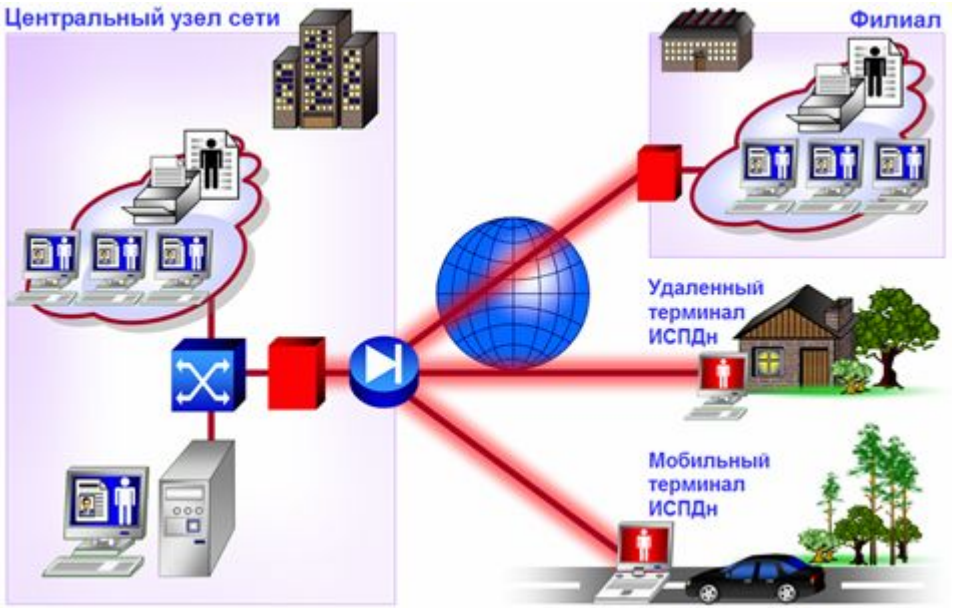
- Сегментирование ИСПДн выполняется путем перегруппировки приложений серверов и терминалов ИСПДн в отдельные сетевые сегменты и осуществления контроля доступа между сегментами
- Для этих целей могут применяться технологии:
  - физической перекоммутации устройств
  - построения виртуальных локальных сетей (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



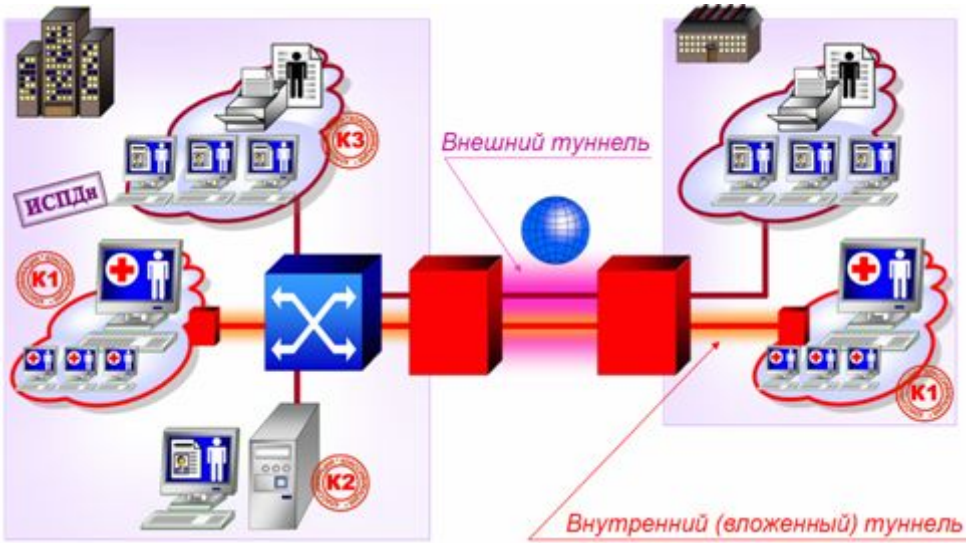
- **Изолировать ресурсы отдельной ИСПДн на сетевом уровне можно при помощи технологии IPsec VPN**
  - **для этого на терминалах ИСПДн должны быть установлены VPN-клиенты, а серверы – защищены при помощи программных VPN-продуктом или выделенных шлюзов безопасности**
    - **выделенный шлюз можно рекомендовать в тех случаях когда:**
      - **сервер обслуживает большое количество пользователей и разнородных приложений, контроль за безопасностью среды функционирования VPN затруднен и и эксплуатация криптографического приложения на нем нежелательна**
      - **сервер работает в условиях высоких пиковых нагрузок и разделение процессорной мощности в криптографическим приложением 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



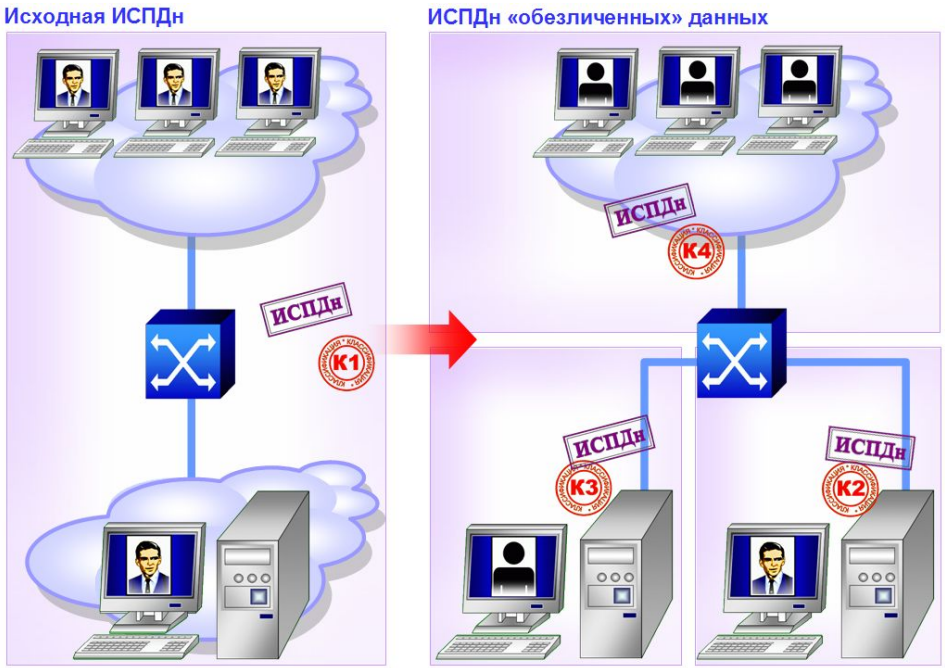
- Для распределенных ИСПДн, сегменты которых географически дистанцированы и объединены при помощи сетей связи общего пользования, технологии VPN являются естественным способом защитить данные в канале связи от их перехвата и компрометации
  - при этом целесообразно защищать корпоративную сеть в целом, 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



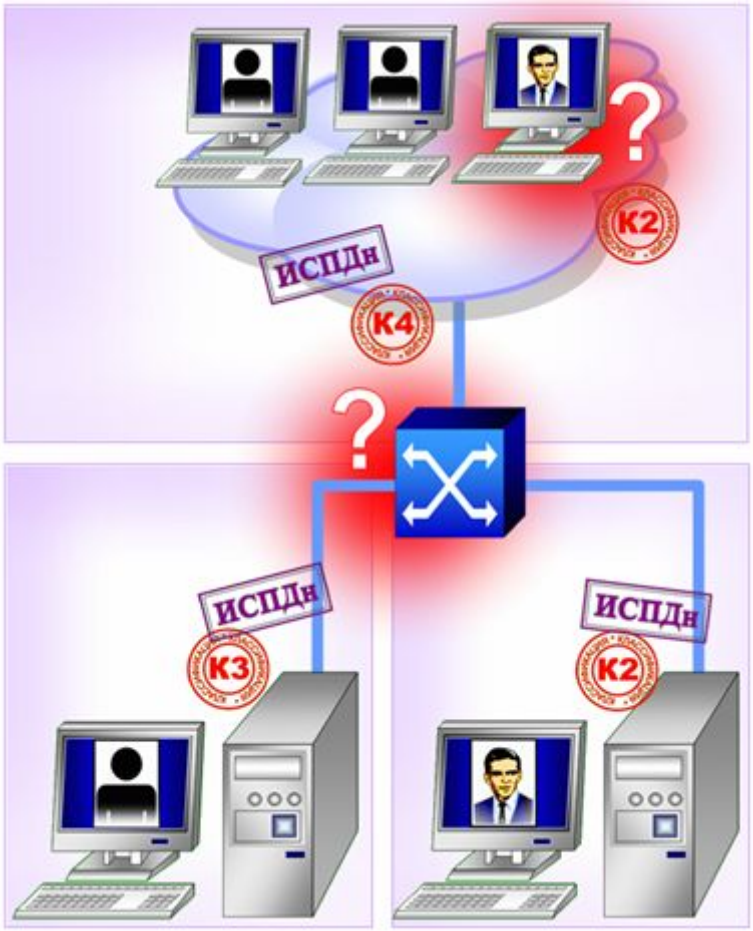
- **Для ИСПДн, где присутствует четырехуровневая иерархия требований защиты, могут быть полезны сценарии построения «вложенных» VPN**
  - **на рисунке показан пример в котором трафик ИСПДн К1, изолированный внутри периметра корпоративной сети, передается внутри «внешнего» туннеля, защищающего корпоративную 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



- 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»



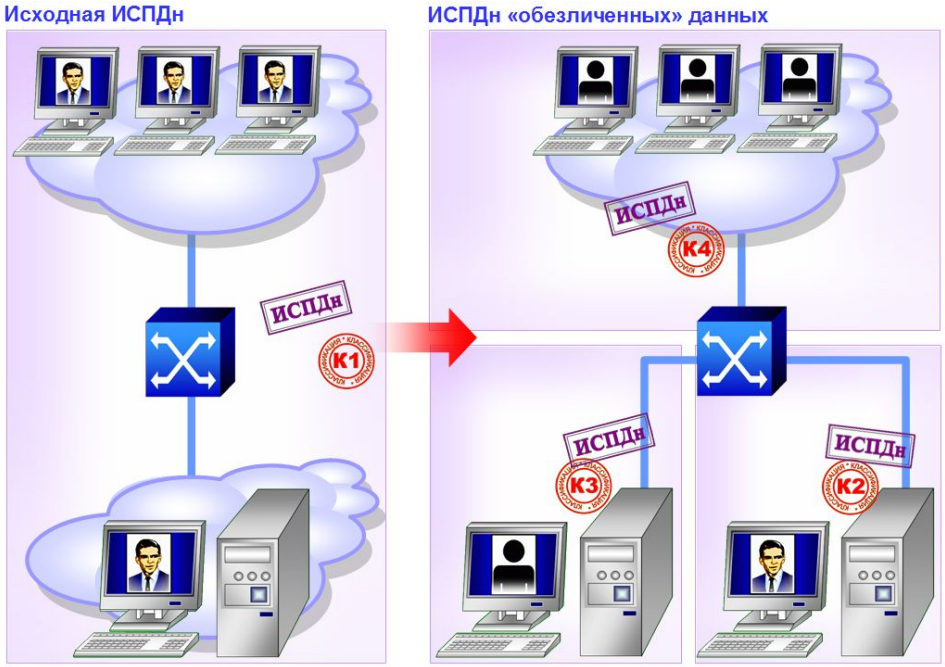
- **Несмотря на наличие такой практики, использование обезличивания персональных данных с целями снижения класса защиты системы (и, как следствие, снижения стоимости и стойкости применяемых мер защиты) вызывает вопросы:**
  1. **Можно ли трактовать ли декомпозированную систему (ИСПДн с идентификационными 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 производиться одновременная работа с той и с другой системой?**
     - **поскольку обезличенные персональные данные приобретают ценность только во взаимоувязке 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 К1)**

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 К1, в соответствии с действующим регулированием, должна быть надежно защищена, то требования на защиту систем класса К4 («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 К1**
- **Вывод заключается в том, что как минимум один из трех элементов:**
  - **ИСПДн «обезличенных» контекстных данных**
  - **ИСПДн идентификационных данных**
  - **или связь между ними**

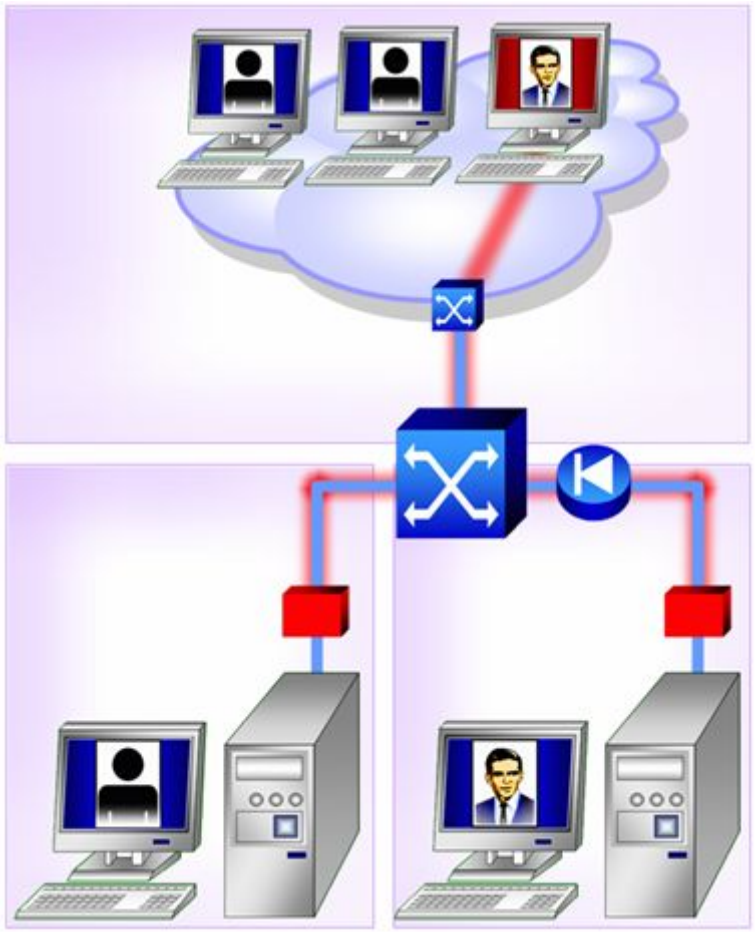
  должен иметь класс защиты не ниже и исходной ИСПДн, в которой контекстные и идентификационные данные были интегрированы

«Обезличивание» - to be or not to be?



- **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 могут 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, там 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

Техническое регулирование
Технические требования
Сценарии защиты ИСПДн
Архитектура защиты ИСПДн

Архитектура системы сетевой защиты ИСПдн

s-terra
csp
Cisco Solution Technology Integrator

Позиционирование средств сетевой защиты

Подсистема приложений

1. Хранилище персональных данных

   Для крупных систем (Хнпд-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:

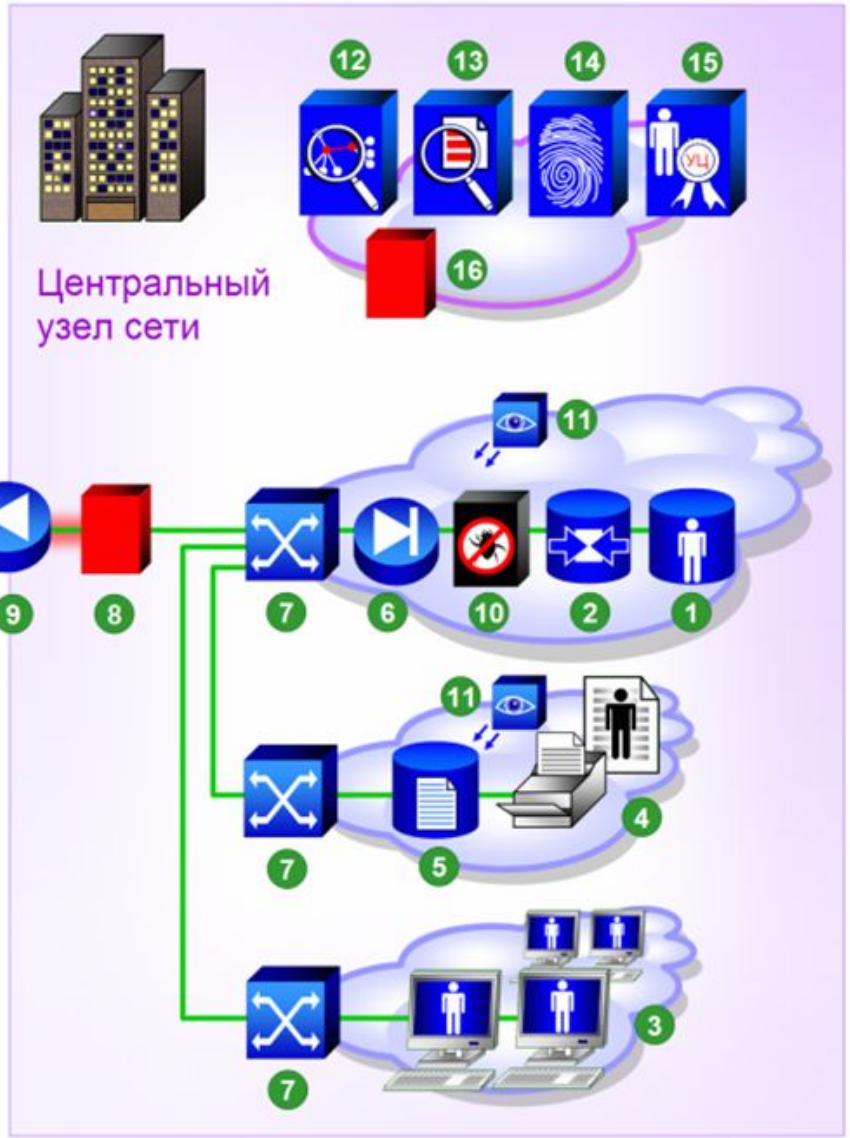
   - Учет резервных копий
   - Защищенное хранение резервных копий. Для данных категории Хпдн-1 рекомендуется применение кпритографических методов защиты резервных копий
   - Регламент безопасности хранения и восстановления резервных копий

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

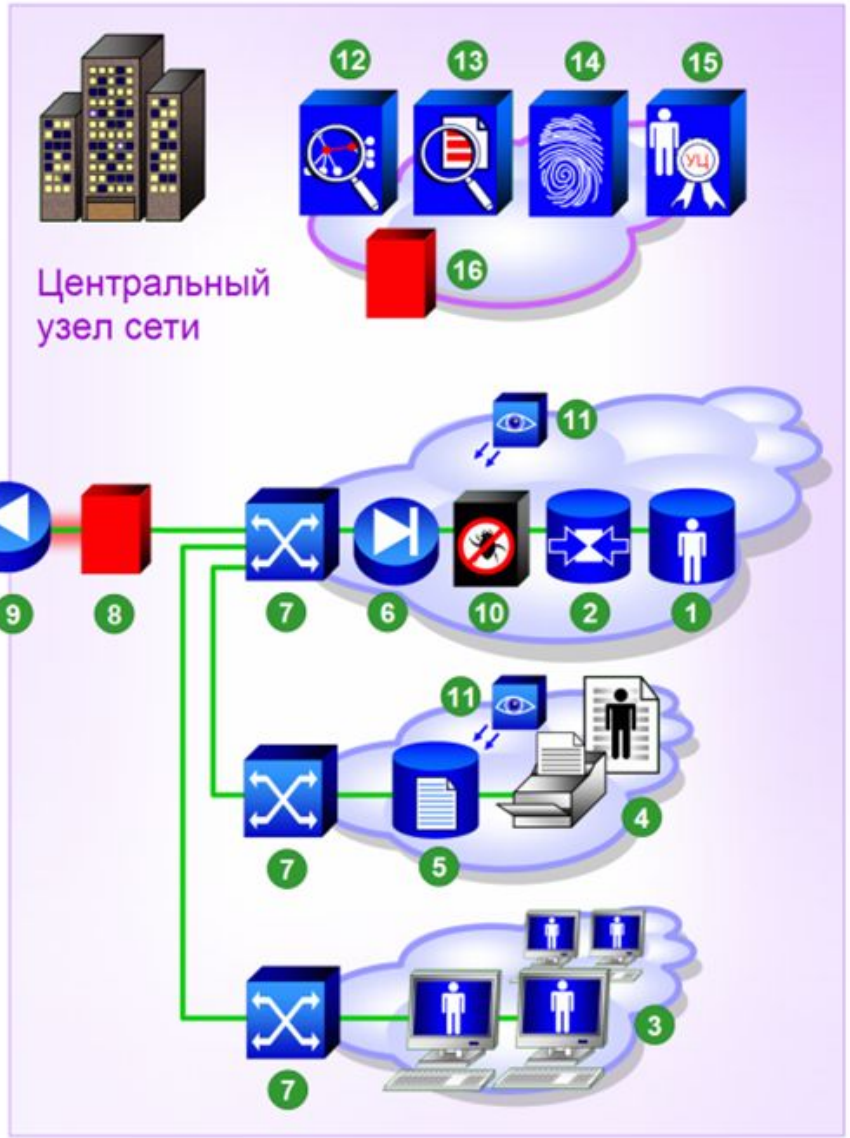
   Детали организации терминальных систем приведены в разделе «Справочный состав программного обеспечения терминала обработки персональных данных»



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

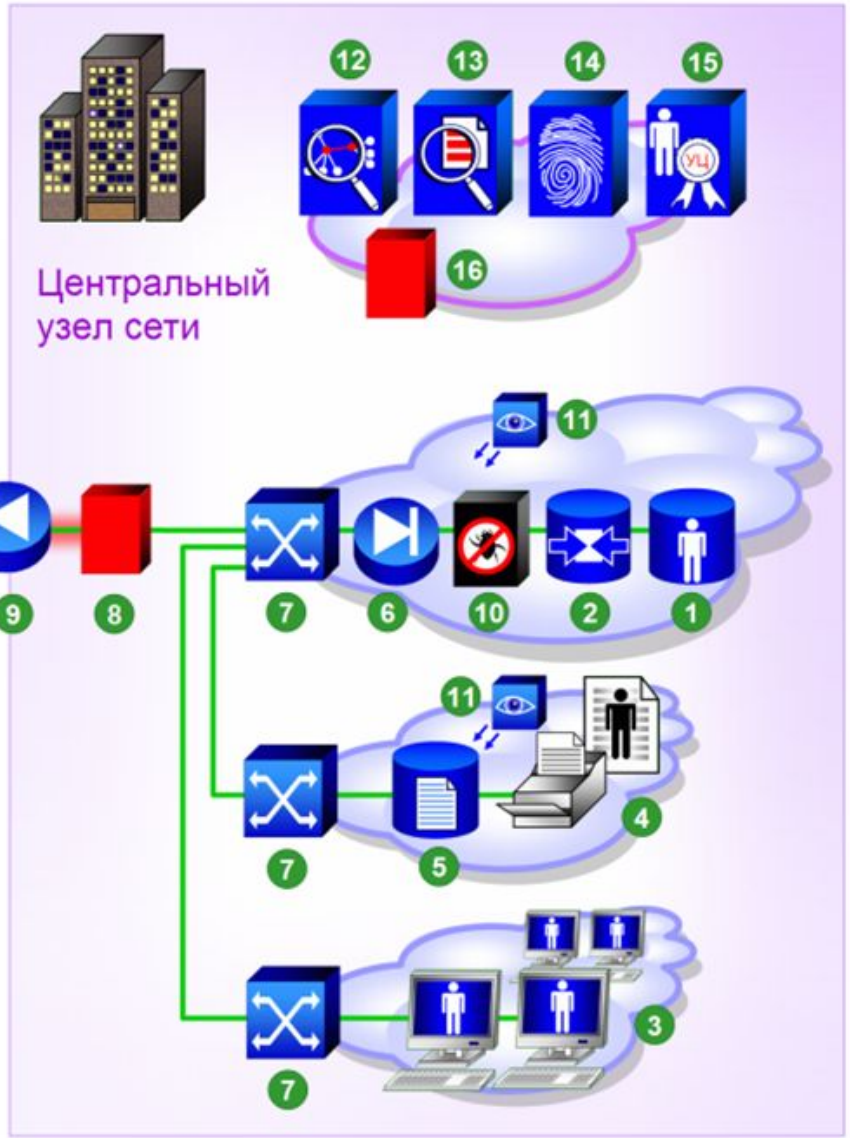


Сетевая инфраструктура

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

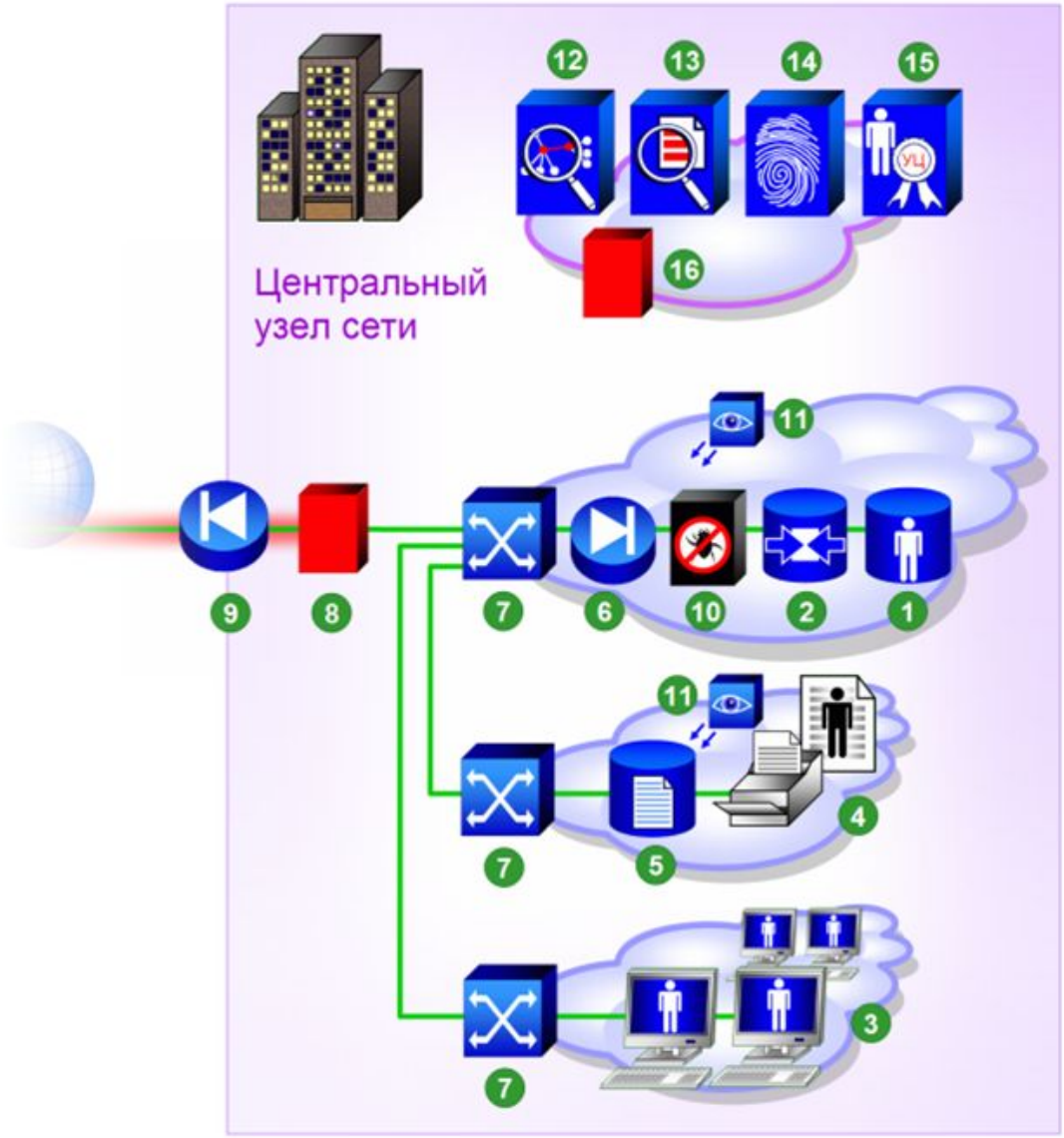
Сетевая инфраструктура должна быть иерархизирована (защита должна быть реализована на различных уровнях модели OSI/ISO) и структурирована (в частности, ЛВС, в которых ведется обработка данных должны быть сегментированы, серверные подсистемы, подсистемы ввода/вывода, терминальные системы должны быть размещены 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 802.1g 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 (К1, 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

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
c s p
Cisco Solution Technology Integrator