Администрирование системы защиты информации ViPNet версия 4.x

НОЧУ ДПО ЦПК «Учебный центр «ИнфоТеКС»

ЛЕКЦИЯ 1

«Виртуальные защищенные сети VPN. Технология защиты информации VipNet»

ОАО «ИнфоТеКС»

открытое акционерное общество
«**Инфо**рмационные **те**хнологии и **к**оммуникационные **с**истемы»

Компания основана в 1991г.

- Является одним из лидеров рынка VPN решений и средств защиты информации.
- Имеет запатентованные программные продукты в области защиты корпоративных сетевых решений.

1 этап: *1992-1998 годы*

- Создание и развитие DOS версии пакета программ «Корпоративная наложенная сеть ИнфоТеКС».
- Реализован целый ряд крупных проектов в ЦБ РФ и СБ РФ по созданию защищенной почтовой системы с элементами PKI.

2 этап: *1998-2001 годы*

- Создание и развитие технологии ViPNet для построения полноценных корпоративных VPN с развитой клиентской частью в TCP/IP сетях под ОС Windows.
- Проекты: МИД РФ, МПС, МинАтом, ВЭБ, Альфа Капитал, Reuters и др.
- Организация собственных учебных курсов.

3 этап: *с 2001 года по настоящее время*

- Дальнейшее развитие технологии ViPNet в сторону поддержки PKI, включая разработку ПО Удостоверяющий центр, разработка многоплатформенных решений под ОС Linux, FreeBSD, Sun Solaris.
- Проекты: ПФ РФ, ОАО «РЖД», Госкомстат, МЭРиТ, ЮГБАНК, ЮТК и др.
- Разработка приложений для ОС Windows Mobile, Apple iOS, Android.

Лицензии ФСТЭК

1. На деятельность по разработке и (или) производству средств защиты конфиденциальной информации.
2. На деятельность по технической защите конфиденциальной информации.
3. На осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны (в части технической защиты).
4. На проведение работ, связанных с созданием средств защиты информации.

Лицензии ФСБ

1. Лицензия на разработку и производство криптографических средств и информационных систем защищенных с использованием шифровальных (криптографических) средств.
2. На осуществление разработки и производства средств защиты конфиденциальной информации.
3. На осуществление мероприятий и(или) оказание услуг в области защиты государственной тайны.
4. На осуществление разработки, производства:
   - шифровальных (криптографических) средств,
   - защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.
5. На осуществление предоставления услуг в области шифрования информации.
6. На осуществление технического обслуживания шифровальных (криптографических) средств.
7. На распространение шифровальных (криптографических) средств.

Сертификаты ФСБ и ФСТЭК на продукты ViPNet

Продукты компании «ИнфоТеКС» проходят регулярную сертификацию в ФСБ России и ФСТЭК России на соответствие требованиям безопасности для средств защиты конфиденциальной информации, включая персональные данные

Все сертификаты и лицензии представлены в открытом доступе на официальном сайте компании «ИнфоТеКС» по ссылке: http://infotecs.ru/products/cert/

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/525-2883 от "22" января 2016 г.

Действителен до "30" ноября 2017 г.

Выдан Открытому акционерному обществу «Информационные технологии и коммуникационные системы» (ОАО «ИнфоТеКС»).

Настоящий сертификат удостоверяет, что изделие «Программный комплекс ViPNet Client 3.2» (варианты исполнения 1, 2) в комплектации согласно формуляру ФРКЕ.00004-05 30 01 ФО

соответствует требованиям ФСБ России к устройствам типа межсетевые экраны 4 класса защищенности и может использоваться для защиты информации от несанкционированного доступа в информационных и телекоммуникационных системах органов государственной власти Российской Федерации.

Сертификат выдан на основании результатов проведенных ОАО «ИнфоТеКС» сертификационных испытаний образца продукции № 637С-062845.

Безопасность информации обеспечивается при использовании изделия в соответствии с требованиями эксплуатационной документации согласно формуляру ФРКЕ.00004-05 30 01 ФО.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России А.М.Ивашко

Настоящий сертификат зарегистрирован в государственном реестре сертификатов ФСБ России.

Заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России А.Н.Ковалев

Технология защиты информации ViPNet

Технология ViPNet

Технология ViPNet — технология, предназначенная для развертывания защищенных виртуальных частных сетей (VPN) поверх глобальных и локальных сетей.

Технология ViPNet

Технологии защиты конфиденциальной информации

технологии идентификации и аутентификации

- ✔ позволяют подтвердить личность пользователя и источник сетевого пакета

технология межсетевого и персонального экранирования

- ✔ обеспечивает фильтрацию любого вида трафика (входящего, исходящего, транзитного) на основе заданных правил

технологии инкапсуляции и туннелирования

- ✔ позволяют упаковать IP-пакет вместе со служебными полями в IP-пакет стандартного вида для сокрытия информации при ее передаче по открытым каналам связи

Технология ViPNet

Технологии защиты конфиденциальной информации

технология создания виртуальных защищенных сетей (VPN)

- ✔ позволяет соединить защищенными каналами связи компьютеры независимо от их месторасположения

технология криптографического преобразования данных

- ✔ обеспечивает конфиденциальность информации при ее передачи и хранении

технология работы с электронной подписью (ЭП)

- ✔ обеспечивает целостности информации и позволяет установить ее авторство

Архитектура виртуальных защищенных сетей (VPN)

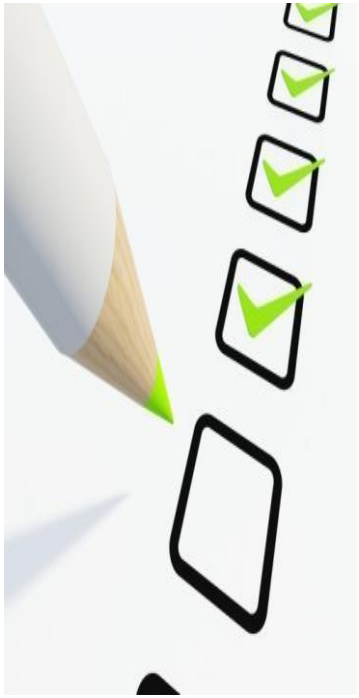
Архитектура VPN

Виртуальные защищенные сети (VPN)

VPN (Virtual Protected Network):

- *это обобщённое название технологий, которые позволяют объединить в виртуальную защищенную сеть произвольное количество локальных сетей и отдельных компьютеров*
- *VPN-сеть строится поверх других сетей передачи данных (в том числе и сети Интернет)*
- *с помощью криптографических методов VPN-сеть позволяет обеспечить конфиденциальность, аутентичность и целостность передаваемой информации*

Преимущества VPN

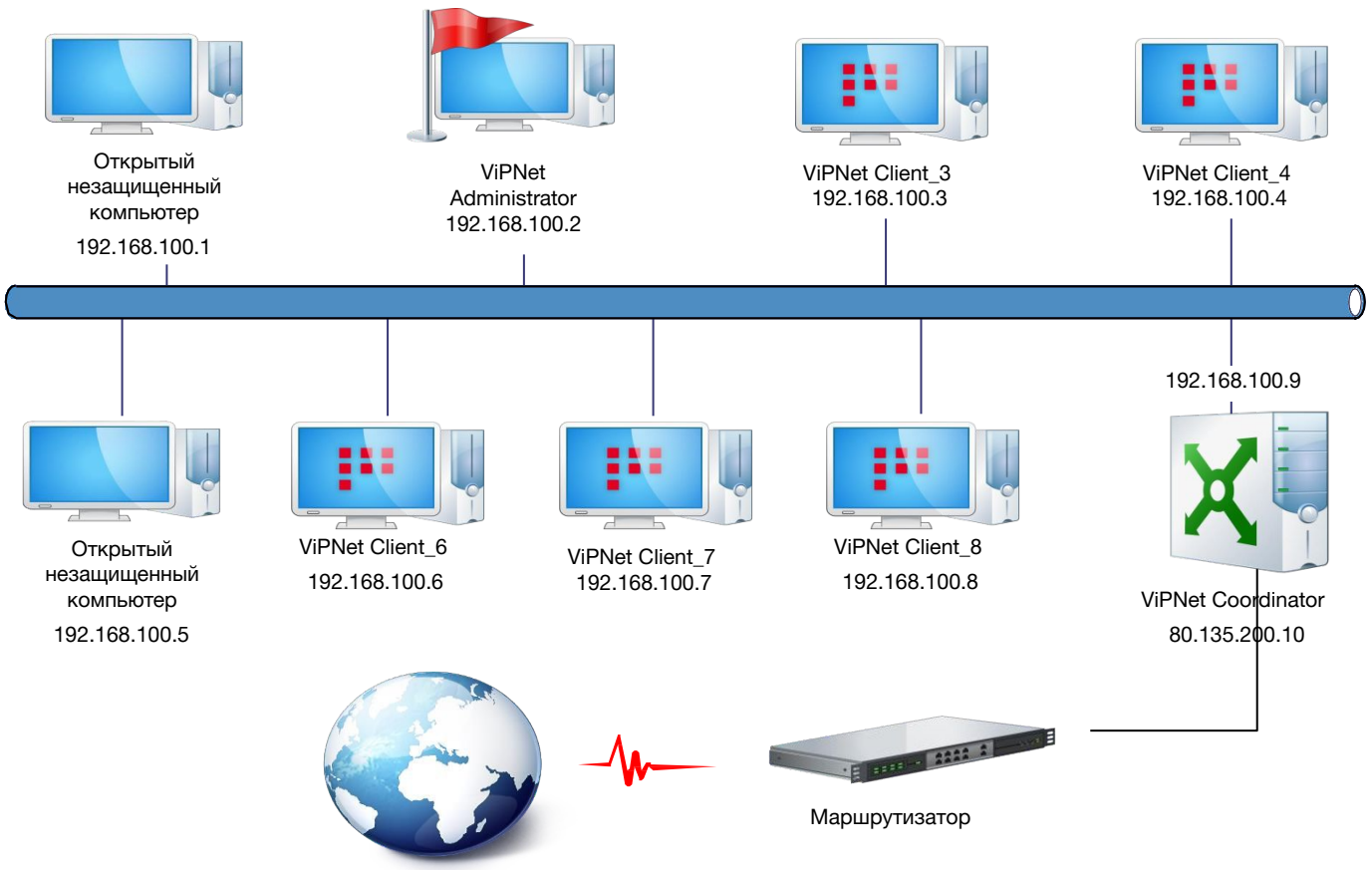


Технологии VPN на основе симметричной криптографии:

- позволяют быстро построить VPN-сеть любой масштабности, не обращая внимания на адресную структуру,
- позволяют размещать VPN-модули, как на компьютерах внутри локальных сетей, защищенных NAT-устройствами, так и на VPN-шлюзах на границе локальных сетей для защиты локальной сети в целом или ее фрагментов.

Предоставляется возможность обеспечить безопасность информации при наличии внутренних и внешних нарушителей.

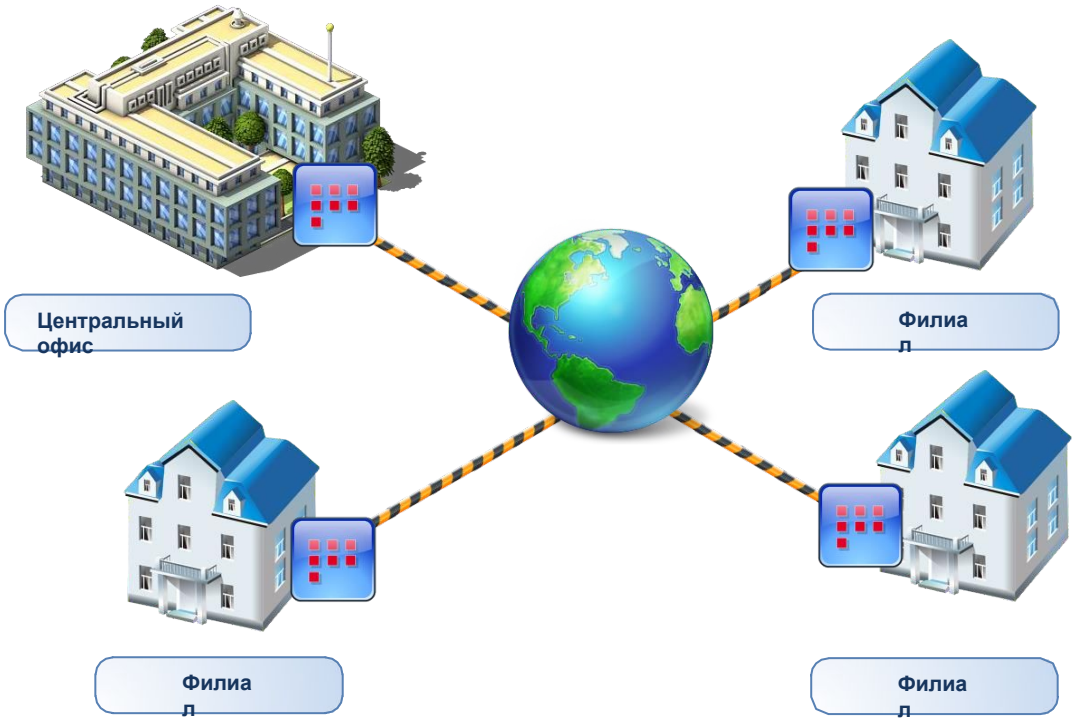
Схема защиты информации средствами ViPNet в ЛВС



Типичная схема организации защиты информации

- С защищенным и незащищенным сегментами;
- С удаленными пользователями;
- С пользователями внутри корпоративной сети;
- В корпоративной сети с удаленными пользователями.

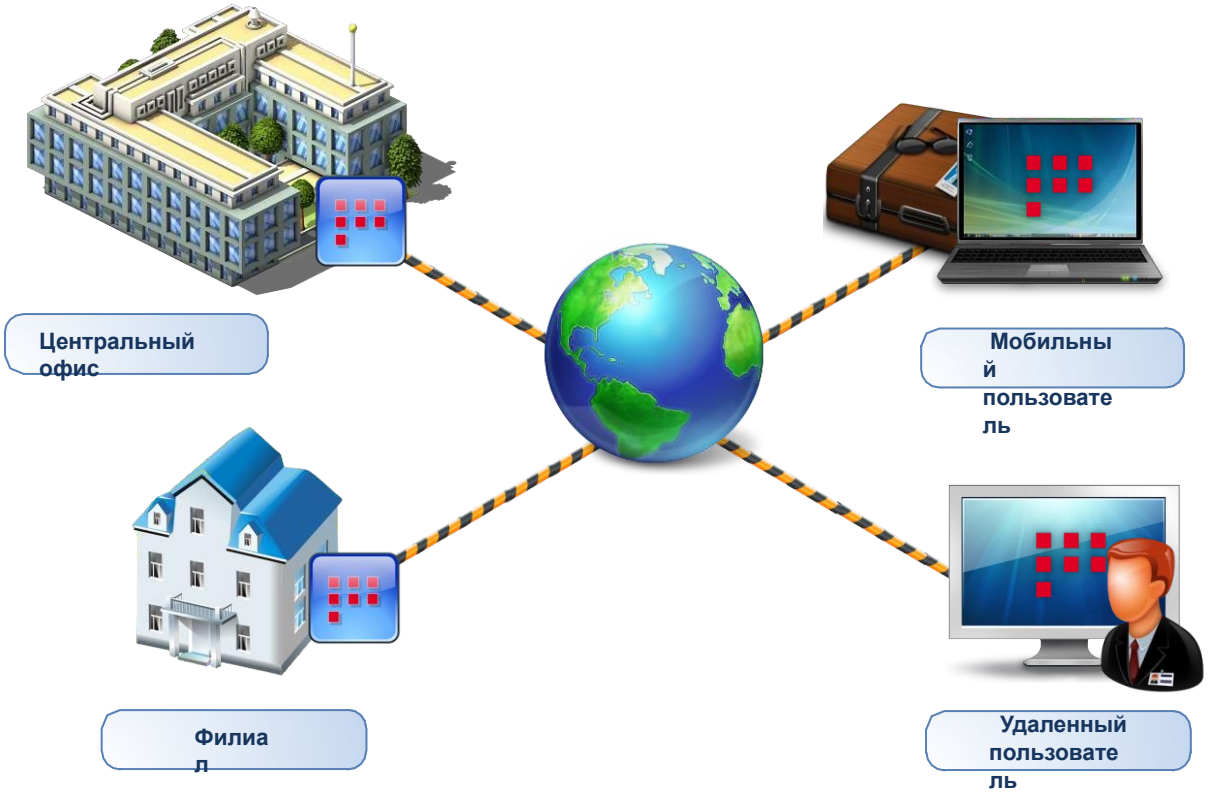
Архитектура VPN Intranet VPN



- *внутрикорпоративная виртуальная сеть*
- *объединяет в единую **защищенную сеть** подразделения одной организации*
- *строится на базе общедоступных сетей связи*

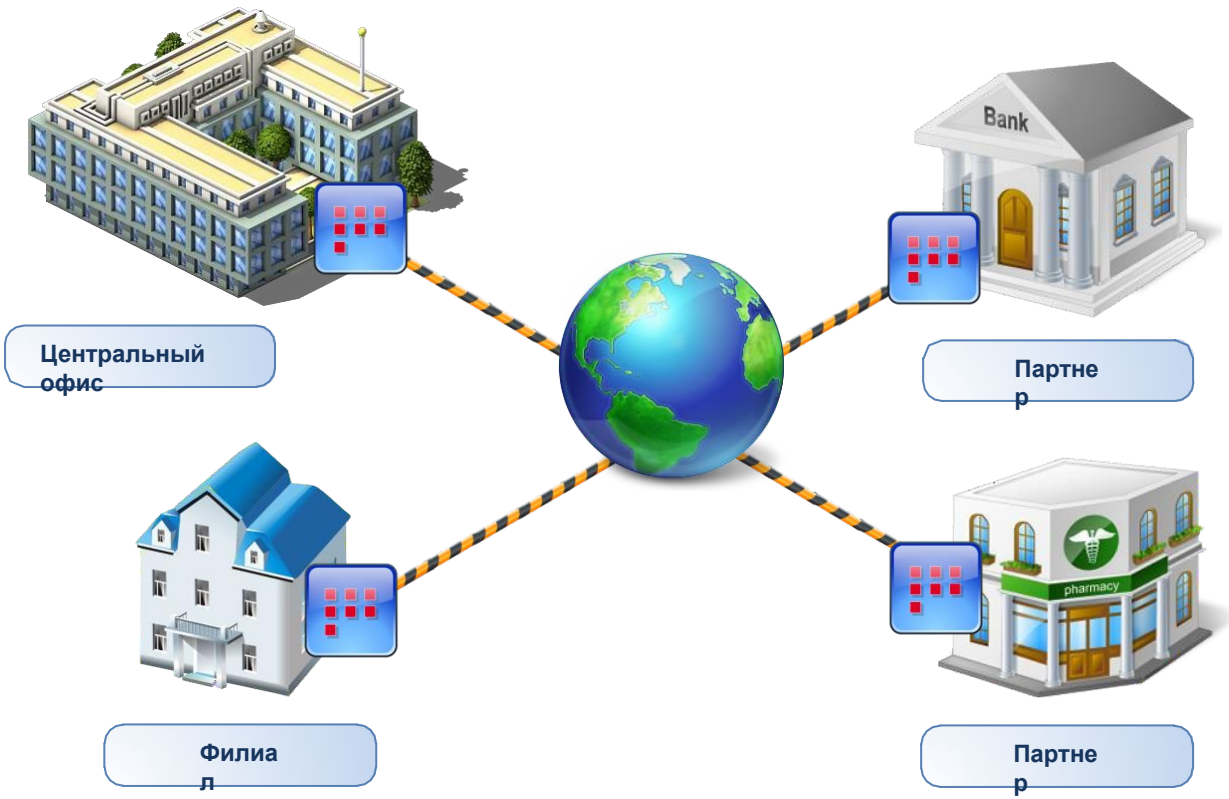
Архитектура VPN

Remote Access VPN



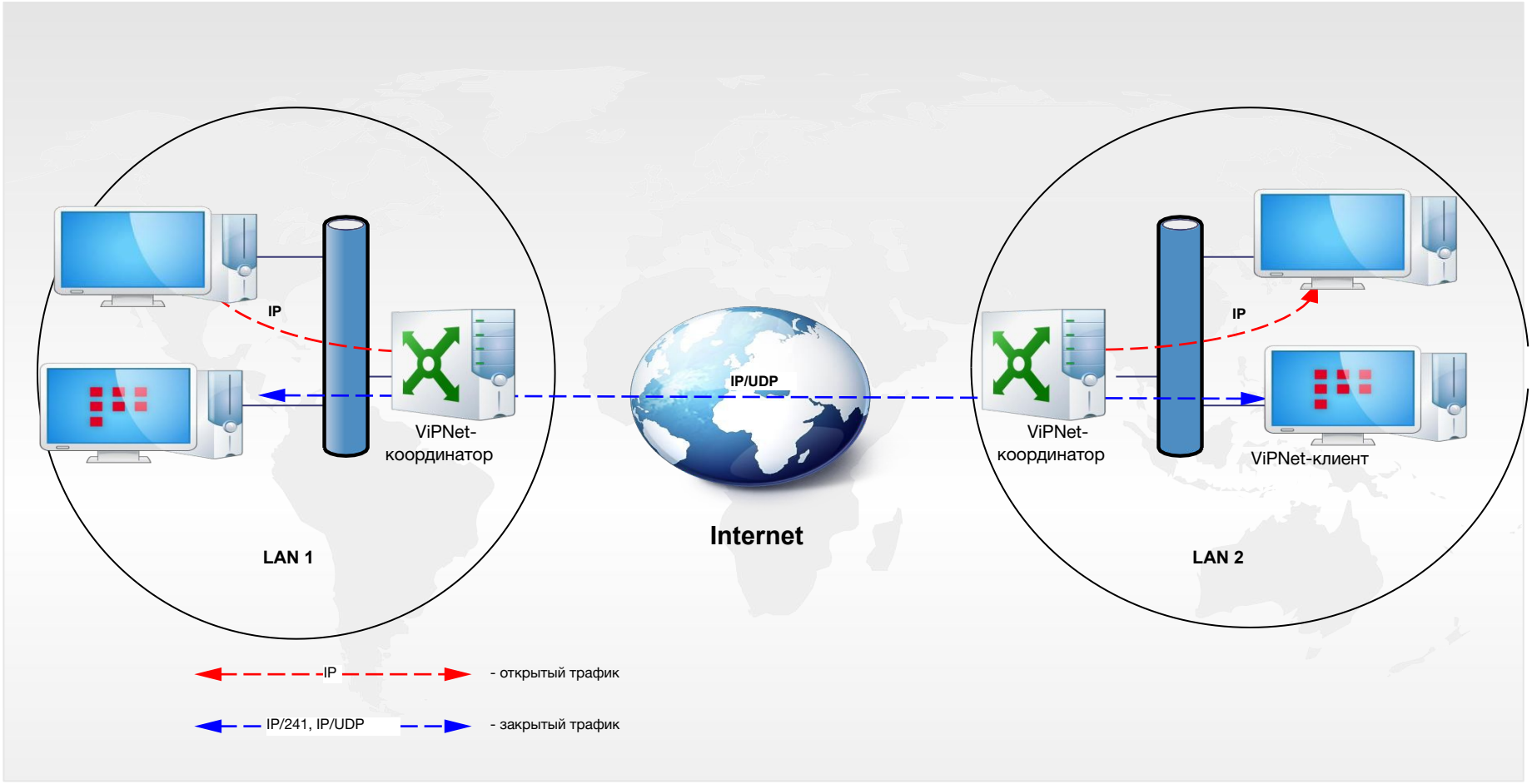
- *виртуальная сеть с удаленным доступом*
- *обеспечивает **защищенное взаимодействие** между сегментом корпоративной сети и внешними пользователями*
- *строится на базе общедоступных сетей связи*

Архитектура VPN Extranet VPN

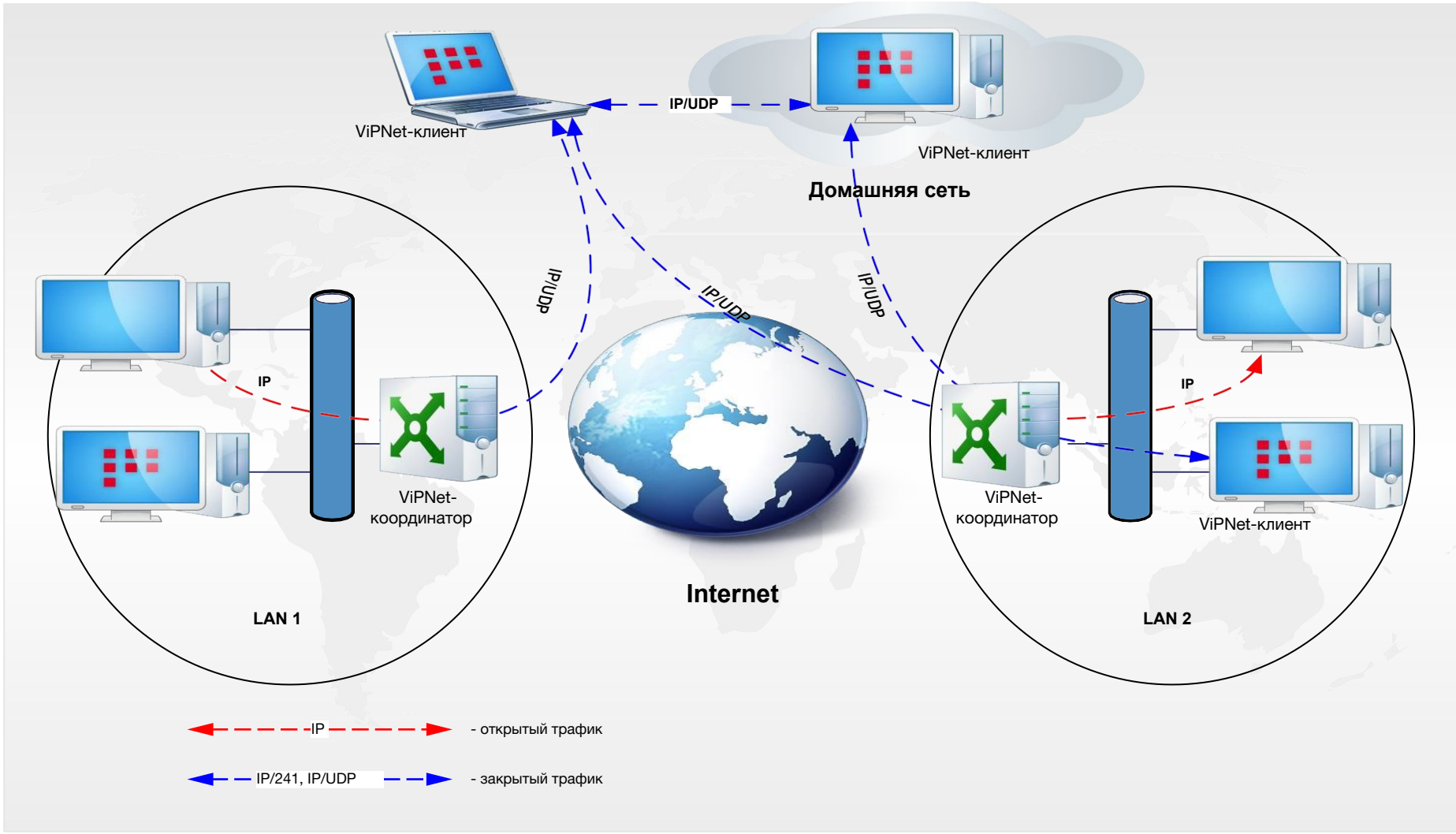


- *межкорпоративная виртуальная сеть*
- *обеспечивает **защищенное соединение** сети компании с сетями ее деловых партнеров и клиентов*
- *строится на базе общедоступных сетей связи*

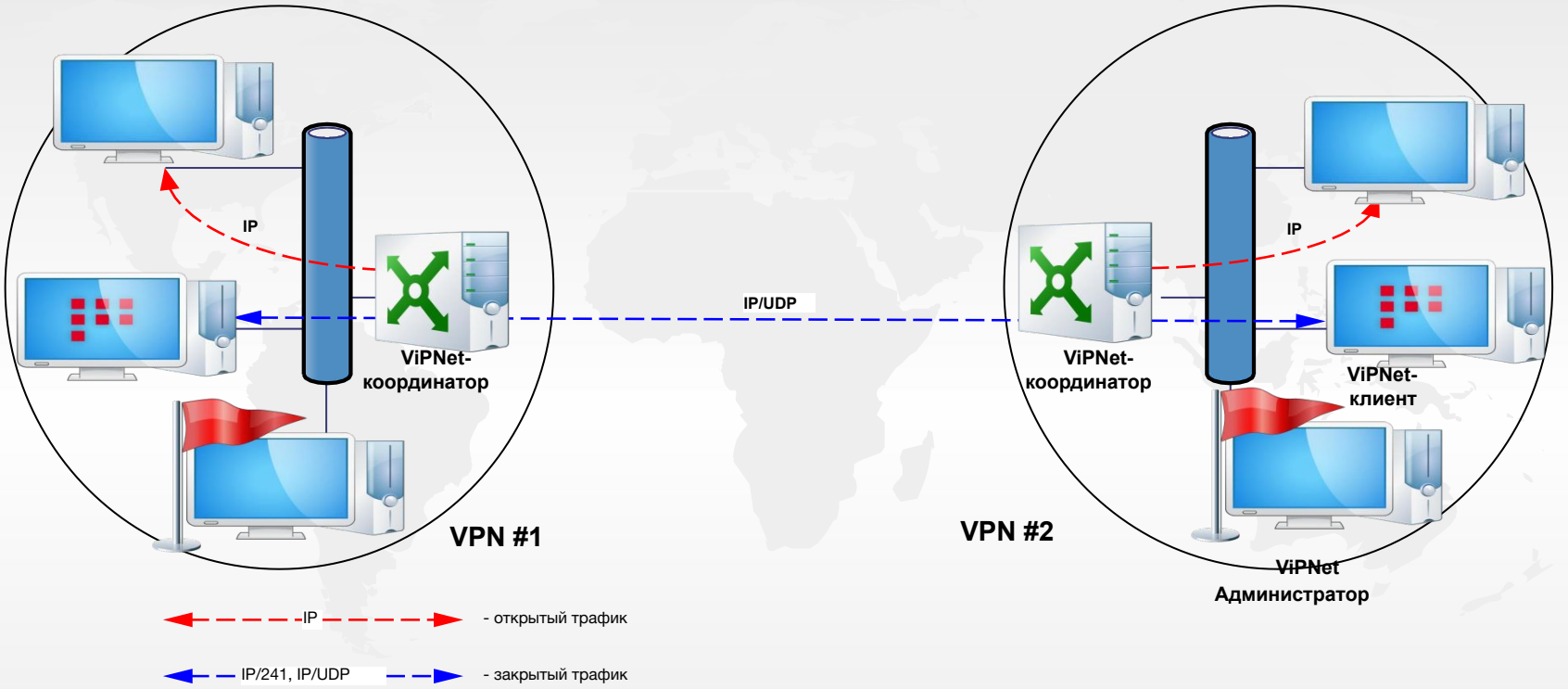
Защита канала связи
LAN–LAN



Защищенный удаленный доступ



Межсетевое взаимодействие



Технология ViPNet

Туннелирование IP-трафика

Туннель – защищенное соединение, созданное для передачи конфиденциальной информации через открытую сеть

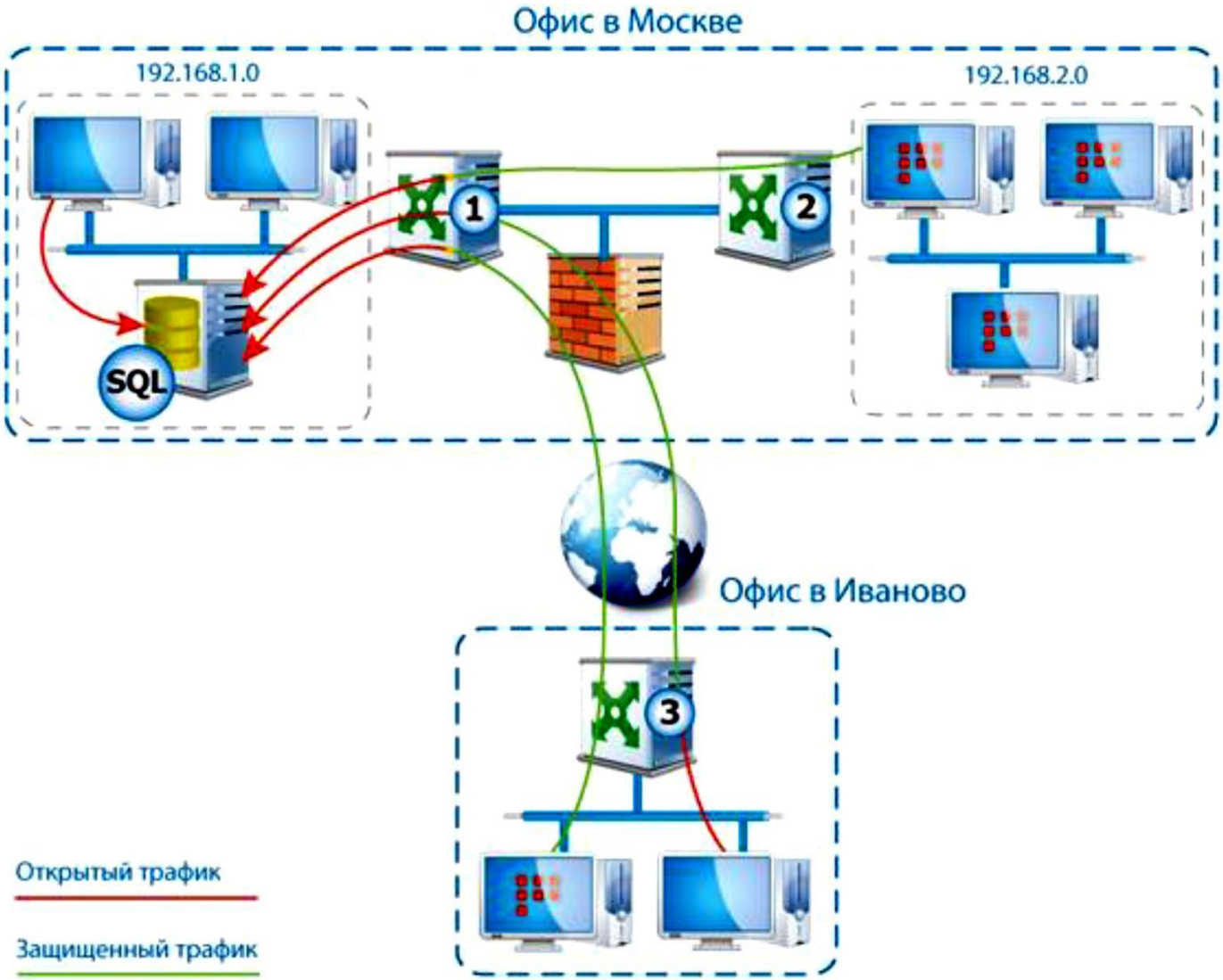
Туннель создается с помощью технологий инкапсуляции и туннелирования Туннель обладает свойствами защищенной выделенной линии

Туннелирующий VPN-шлюз – VPN-шлюз за которым находится открытый узел и который с помощью туннелирования защищает трафик открытого узла

Туннелируемый ресурс – незащищенный компьютер, трафик которого защищается при передаче через открытые сети с помощью процедуры туннелирования

Технология ViPNet

Туннелирование IP-трафика



Технология ViPNet

Инкапсуляция IP-трафика

Инкапсуляция:

- ✔ способ передачи защищаемой информации через открытую сеть при котором передаваемый IP-пакет вместе со служебными полями упаковывается в новый пакет

- ✔ при инкапсуляции любые IP-пакеты с использованием шифрования преобразуются в IP-пакеты единого типа.
  Это позволяет полностью скрыть структуру информационного обмена

Технология ViPNet

Инкапсуляция IP-трафика

Технология ViPNet

Инкапсуляция IP-трафика

- При инкапсуляции пакеты любых IP-протоколов упаковываются в пакеты IP-протоколов двух типов: (IP/241 и IP/UDP)

используется протокол IP/241

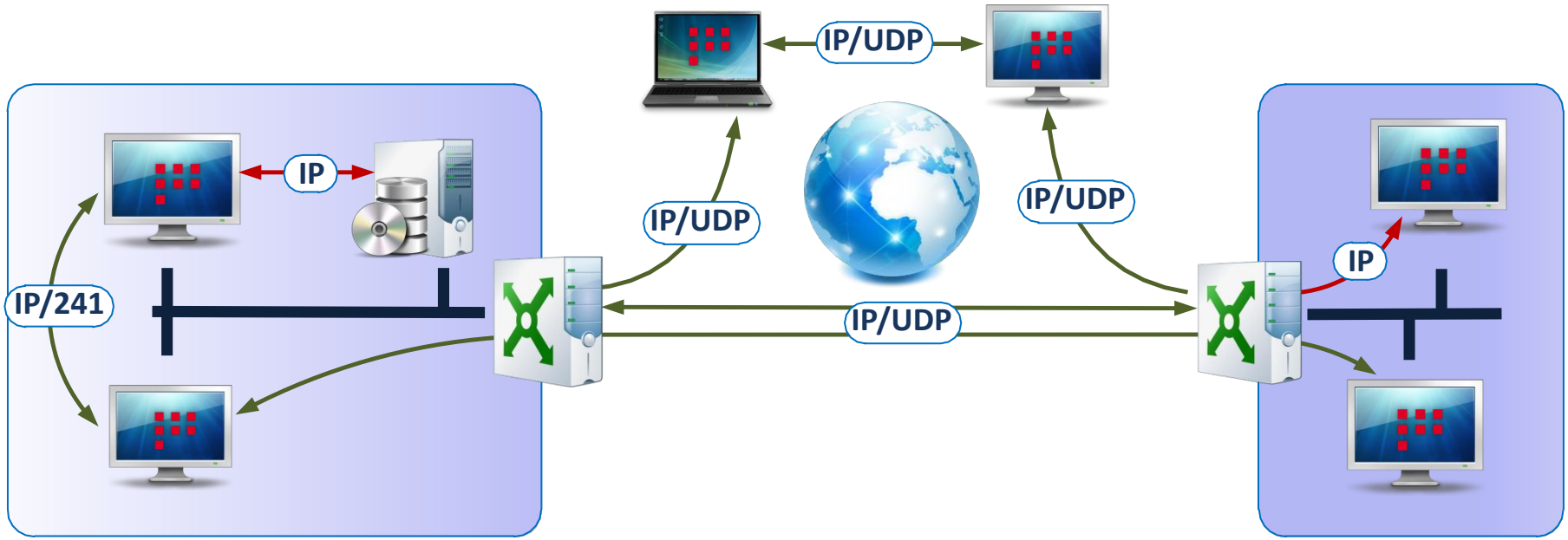
- ✔ *если по пути следования пакета нет преобразования IP-адресов (узлы доступны по реальным IP-адресам)*
- ✔ *если узлы расположены в одном маршрутизируемом сегменте*

используется протокол IP/UDP (порт 55777)

- ✔ *если по пути пакета выполняется преобразование IP-адресов (на пути следования IP-пакета расположено устройство NAT)*

Технология ViPNet

Инкапсуляция IP-трафика



Технология ViPNet

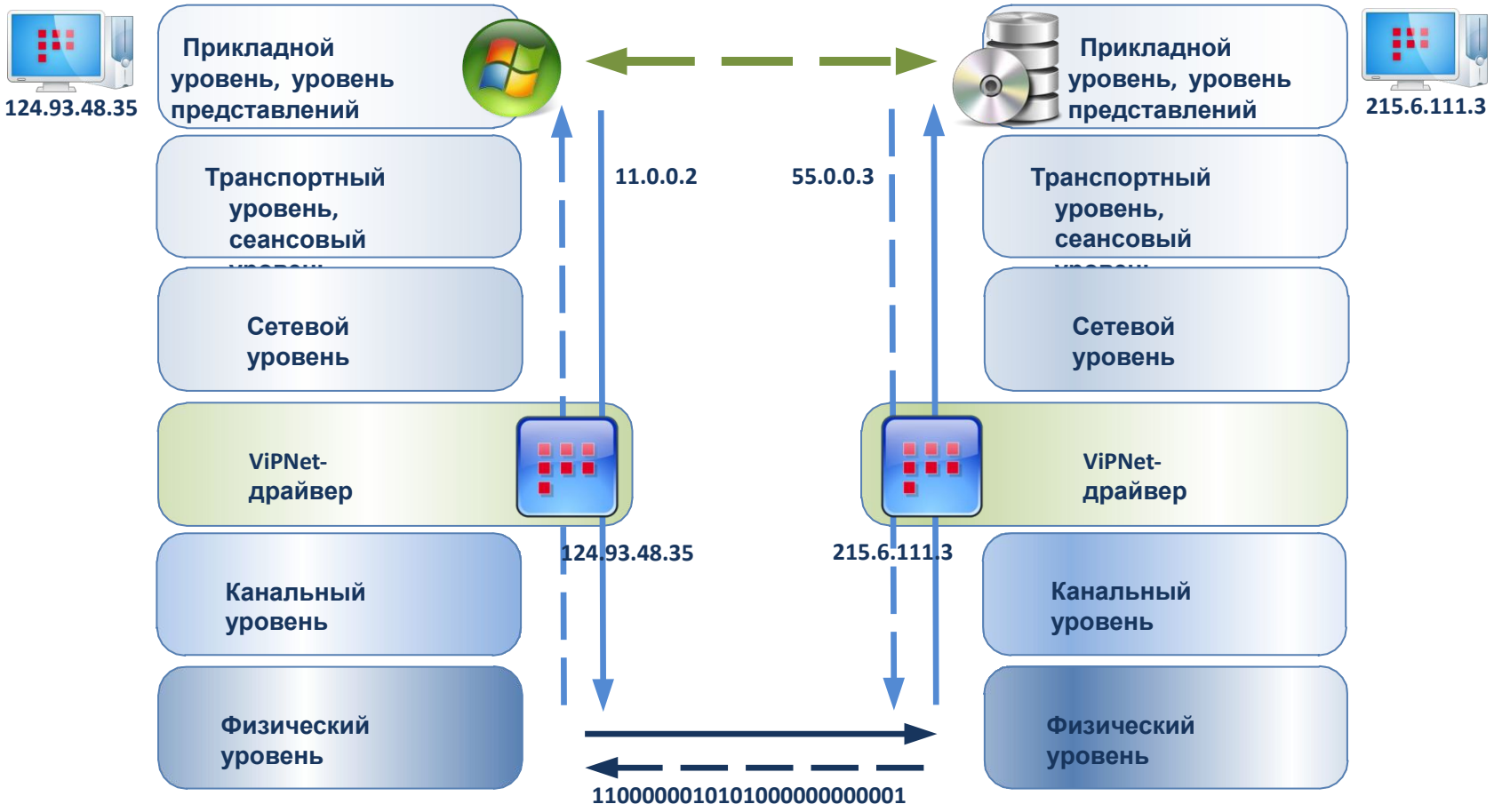
infotecs

ViPNet-драйвер: **ViPNet-драйвер**

- *обеспечивает контроль всего IP-трафика, шифрование (расшифрование) трафика*
- *работает между канальным и сетевым уровнем модели OSI*
- *обрабатывает IP-пакеты до того как они будут обработаны стеком протоколов TCP/IP и переданы на прикладной уровень*
- *активизируется только после авторизации в ПО ViPNet до загрузки прикладных сервисов и системных служб операционной системы*

Технология ViPNet

Принцип работы ViPNet-драйвера



ЛЕКЦИЯ 2

«Модули и объекты защищенной сети VipNet»

Модули защищенной сети ViPNet

ViPNet Network Security 4.x

VPN ViPNet — *это линейка продуктов компании «ИнфоТеКС», предназначенных для защиты информации ограниченного доступа, в том числе персональных данных*

Внимание! Все программно-аппаратные комплексы, программные средства из состава ViPNet Network Security имеют сертификаты соответствия ФСТЭК России и ФСБ России

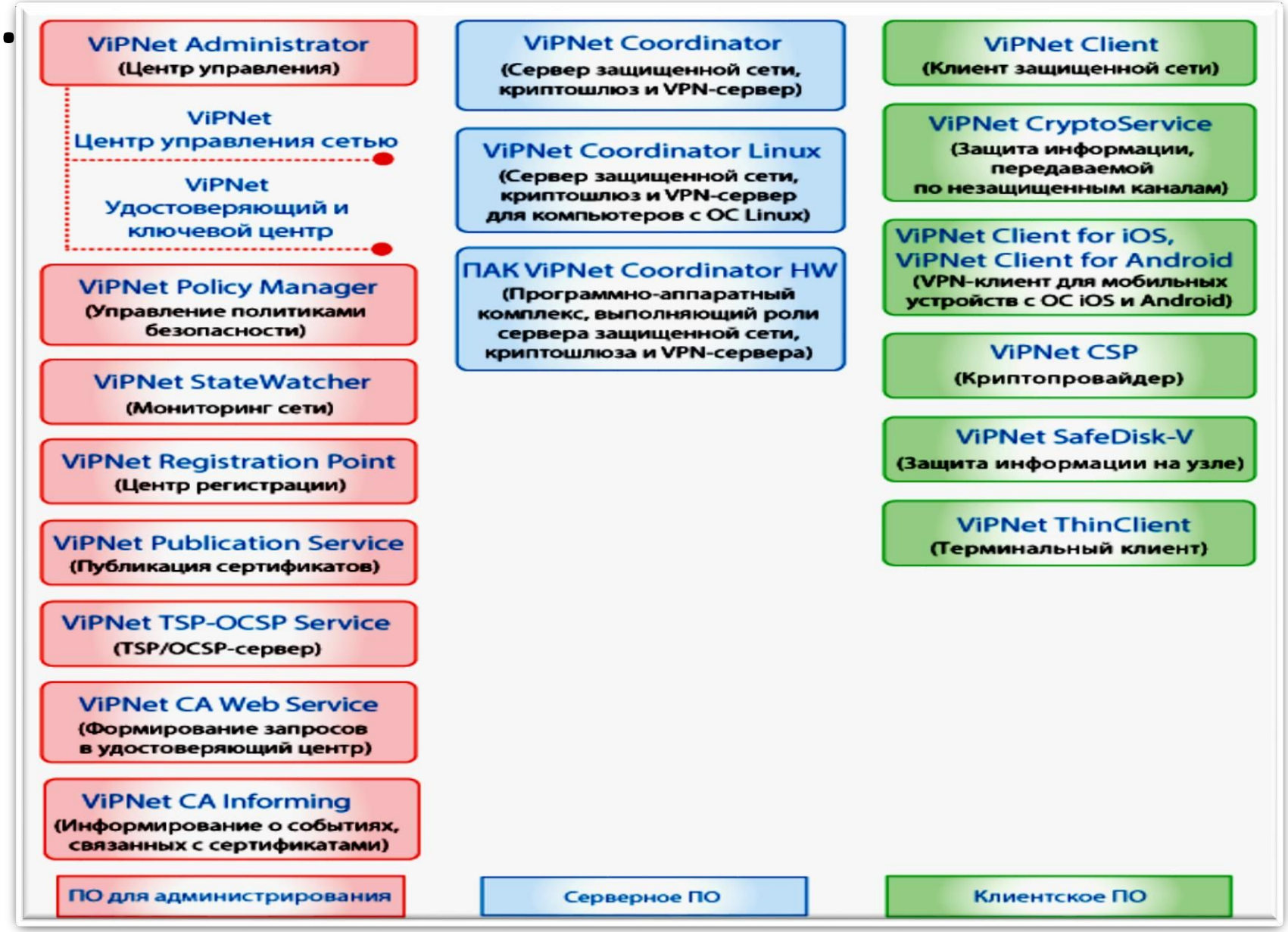
ViPNet Network Security 4.x

Назначение VPN ViPNet

VPN ViPNet позволяет организовывать защиту информации в различных информационных системах и нацелен на решение двух задач информационной безопасности:

- *создание защищенной среды передачи данных с использованием публичных и выделенных каналов связи путем организации сети VPN*
- *развертывание инфраструктуры открытых ключей (PKI) и организация Удостоверяющего центра, что позволит использовать ЭП в прикладном ПО Заказчика (системах ЭДО, электронной почте, ЭТП и т.д.)*

Состав ViPNet Network Security 4.



ViPNet Network Security 4.x

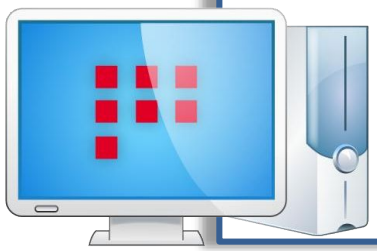
Базовые модули ViPNet 4.x

ViPNet Administrator

- ✔ *предназначен для создания и управления защищенной сетью ViPNet*

ViPNet Coordinator

- ✔ *предназначен для защиты сегментов IP-сетей, координации работы узлов защищенной сети*



ViPNet Client

- ✔ *предназначен для защиты отдельных компьютеров*

ViPNet Network Security 4.x

ViPNet Administrator

предназначен для:

- ✔ *создания VPN-сети на основе технологии ViPNet администрирования VPN-сети (добавление, удаление, изменение объектов сети, настройка параметров работы, контроль работоспособности и др.)*
- ✔ *обновления ПО ViPNet, установленного на узлах защищенной сети*

состоит из:

- ✔ *серверного приложения ЦУС*
- ✔ *клиентского приложения ЦУС*
- ✔ *базы данных SQL*
- ✔ *удостоверяющего и ключевого центра*

ViPNet Network Security 4.x

Состав ViPNet Administrator

ViPNet Центр управления сетью

- *выполняет следующие функции:*
  - ✔ *создание и модификация структуры сети ViPNet*
  - ✔ *разграничение уровней полномочий пользователей сети ViPNet*
  - ✔ *отправка ключевой и справочной информации, обновлений ПО ViPNet на сетевые узлы*

ViPNet Удостоверяющий и ключевой центр

- *выполняет следующие функции:*
  - ✔ *формирование и управление ключевой структурой сети*
  - ✔ *издание и управление сертификатами пользователей*

ViPNet Network Security 4.x

ViPNet Coordinator

предназначен для:

- ✔ *защиты сегментов IP-сетей*
- ✔ *защиты трафика, передаваемого по открытым каналам связи*
- ✔ *координации работы узлов защищенной сети*

может быть установлен на:

- ✔ *стационарные компьютеры*
- ✔ *серверные платформы*
- ✔ *виртуальные машины*
- ✔ *…*

ViPNet Network Security 4.x

Функции ViPNet Coordinator

- *выполняет функции персонального и межсетевого экрана*
- *создает туннели для организации защищенных соединений с открытыми узлами*
- *осуществляет трансляцию адресов (NAT) для проходящего через координатор открытого трафика*
- *позволяет разделить доступ защищенных узлов в Интернет и к ресурсам локальной сети*
- *позволяет исключить любые атаки в реальном времени на компьютеры локальной сети*

ViPNet Network Security 4.x

Функции ViPNet Coordinator

- ✔ *обеспечивает обмен служебными и прикладными транспортными конвертами между узлами сети ViPNet*
- ✔ *сообщает защищенным узлам информацию об IP-адресах и параметрах доступа других узлов*
- ✔ *обеспечивает маршрутизацию транзитного VPN-трафика, проходящего через координатор на другие защищенные узлы*

ViPNet Network Security 4.x

ViPNet Client

предназначен:

- ✔ *для защиты рабочих компьютеров пользователей сети ViPNet*

выполняет:

- ✔ *фильтрацию всего IP-трафика*
- ✔ *шифрование соединений между защищенными узлами. Для шифрования трафика используются симметричные ключи, которые создаются и распределяются централизованно*

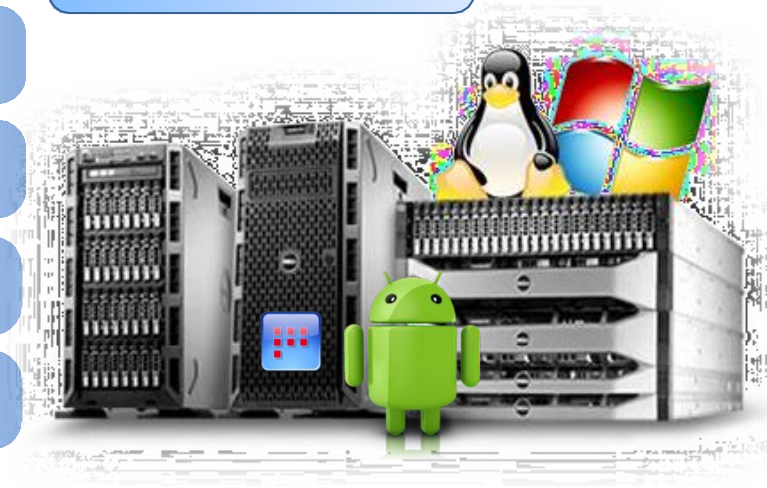
может быть установлен:

- ✔ *на стационарные компьютеры, виртуальные машины, мобильные устройства…*

ViPNet Network Security 4.x

Поддерживаемые операционные системы

ViPNet Client	ViPNet Coordinator	ViPNet Administrator
Windows XP (32-разрядная)	Windows XP (32-разрядная)	Windows 7 (32/64-разрядная)
Windows Server 2003 (32-разрядная)	Windows Server 2003 (32-разрядная)	Windows Server 2008 R2 (64-разрядная)
Windows Vista (32/64-разрядная)	Windows Vista (32/64-разрядная)	Windows 8 (32/64-разрядная)
Windows Server 2008 (32/64-разрядная)	Windows Server 2008 R2 (64-разрядная)	Windows Server 2012 (64-разрядная)
Windows 7 (32/64-разрядная)	Windows 7 (32/64-разрядная)	Windows 10 (64-разрядная)
Windows 8 (32/64-разрядная)	Windows 8 (32/64-разрядная)	
Windows Server 2012 (64-разрядная)	Windows Server 2012 (64-разрядная)	
ОС Android	ОС семейства Linux	



ViPNet Network Security 4.x

Дополнительные модули ViPNet Network Security 4.x

ViPNet StateWatcher

- ✔ *предназначен для централизованного мониторинга защищенных сетей и анализа событий, произошедших на узлах сети*

ViPNet Registration Point

- ✔ *предназначен для регистрации и обслуживания внешних и внутренних пользователей ViPNet и хранения их регистрационных данных; является посредником между внешними пользователями и удостоверяющим центром*

ViPNet Policy Manager

- ✔ *предназначен для централизованного управления политиками безопасности на сетевых узлах ViPNet*

ViPNet Network Security 4.x

Дополнительные модули ViPNet Network Security 4.x

ViPNet SafeDisk (ViPNet SafeDisk-V)

предназначен для защиты конфиденциальной информации, которая хранится на жестком диске компьютера или съемном носителе

ViPNet CSP

- ✔ *представляет собой крипто-провайдер, обеспечивающий вызов криптографических функций через интерфейс Microsoft CryptoAPI 2.0*

ViPNet CryptoService

- ✔ *предназначен для встраивания в прикладные системы криптографических функций ViPNet и функций Криптопровайдера ViPNet; работы PKI, построенной на базе технологий ViPNet*

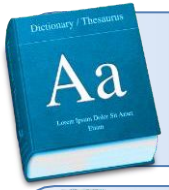
ViPNet Network Security 4.x

Новые возможности ViPNet Network Security 4.x

клиент-серверная архитектура ViPNet ЦУС

возможность многопользовательского режима работы с ViPNet ЦУС

единая база данных SQL, через которую происходит взаимодействие компонентов ViPNet Administrator



изменение в терминологии ViPNet

назначение права подписи и выбор узлов для рассылки САС перенесено из ViPNet ЦУС в ViPNet УКЦ

упрощена организация межсетевого взаимодействия

ViPNet Network Security 4.x

Новые возможности ViPNet Network Security 4.x

настройки сетевых объектов можно выполнять непосредственно при их создании в ЦУС

типы коллектива больше не используются

появилась возможность объединять сетевые узлы и пользователей в группы

связи задаются между сетевыми узлами и между пользователями

отправка обновлений на узлы ViPNet осуществляется с помощью мастера обновления

упрощена процедура создания ключей пользователей и ключей узлов

Объекты защищенной сети ViPNet

Сетевой узел ViPNet

Сетевой узел ViPNet

Сетевой узел ViPNet:

компьютер, на котором установлено программное обеспечение ViPNet

Клиент:

компьютер, на котором установлено клиентское ПО ViPNet

Координатор:

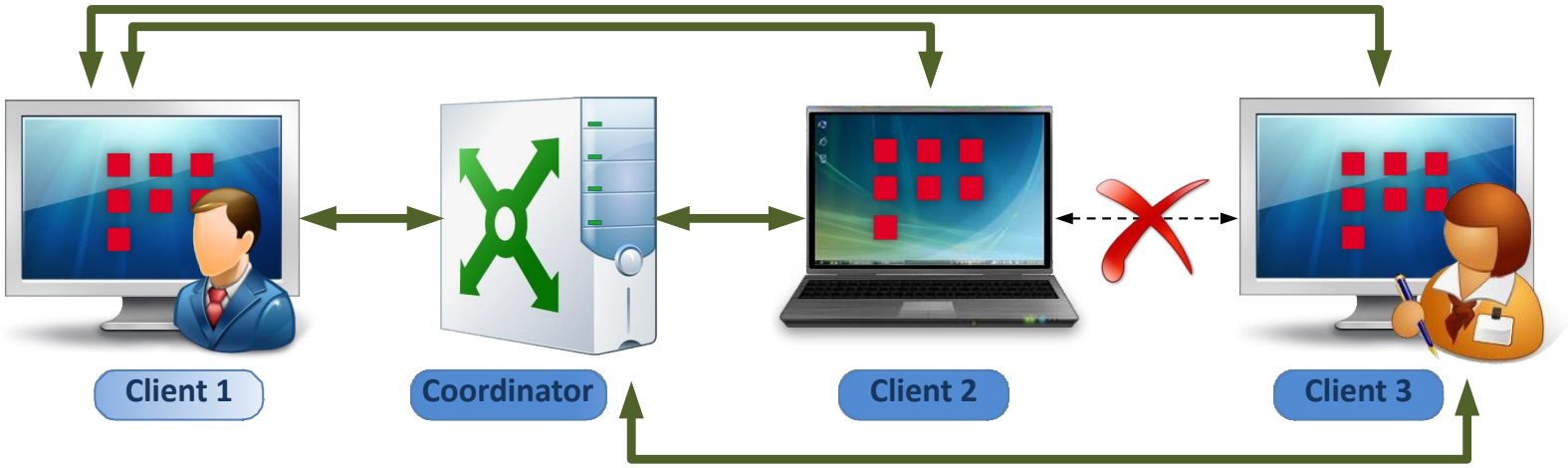
компьютер, на который установлено ПО ViPNet Coordinator или специальный программно-аппаратный комплекс

Сетевой узел ViPNet

Связи между сетевыми узлами

Связь:

- ✔ *обеспечивает возможность создания защищенного канала между узлами ViPNet*
- ✔ *задается администратором ViPNet в клиентском приложении ЦУС*
- ✔ *некоторые связи создаются автоматически и являются обязательным*



Сетевой узел ViPNet

Связи между сетевыми узлами

обязательные связи

- *связь узла с ЦУС*
- *между координатором и зарегистрированными на нем клиентами*
- *между клиентами и их сервером IP-адресов*
- *между сетевым узлом и координатором, выбранным для организации соединений с внешними узлами*
- *между координаторами, которые образуют межсерверный канал*
- *между ViPNet Policy Manager и подчиненными ему сетевыми узлами*

связи, заданные

Сетевой узел ViPNet

Группа сетевых узлов

Группа узлов:

- ✔ *множество сетевых узлов ViPNet, объединенное под общим именем для удобства администрирования*
- ✔ *группы сетевых узлов настраиваются администратором ViPNet в клиентском приложении ЦУС*
- ✔ *группа «Вся сеть» создается по умолчанию и объединяет все узлы сети ViPNet. Эту группу невозможно удалить*
- ✔ *в одну группу можно объединить одновременно координаторы и клиенты*

Пользователь ViPNet

Пользователь ViPNet

Пользователь:

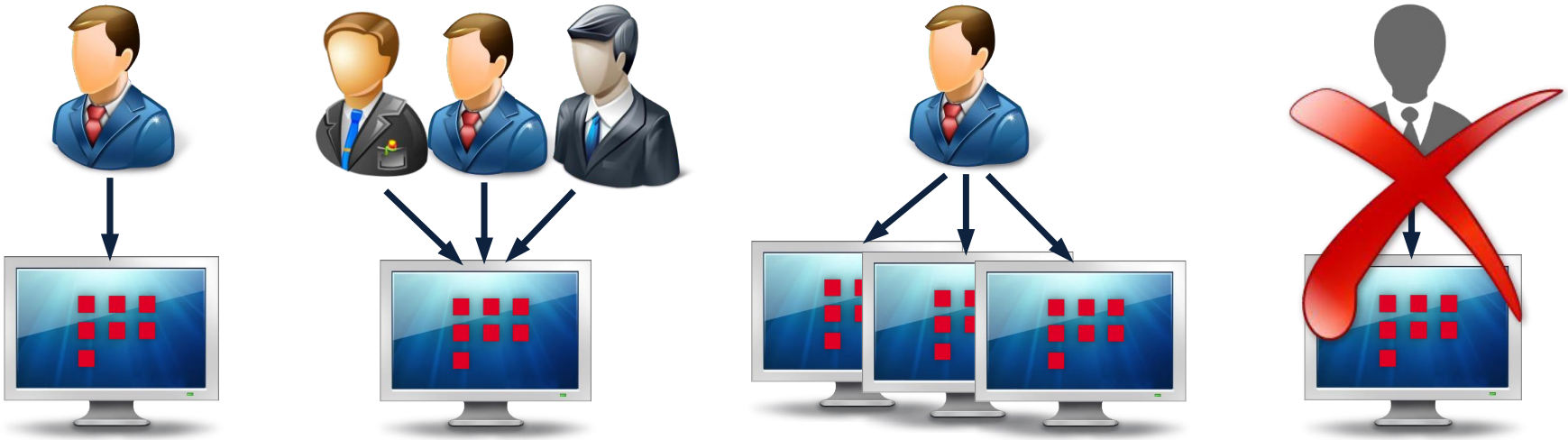
- *владелец ключевой информации для доступа в защищенную сеть*
- *параметры пользователя настраиваются администратором ViPNet в клиентском приложении ЦУС*

Группа пользователей:

- *упрощает управление связями между пользователями. При добавлении пользователя в группу автоматически создается связь между пользователем и каждым членом группы*

Пользователь ViPNet

Регистрация пользователей на СУ



Внимание! *Если пользователь зарегистрирован на нескольких сетевых узлах, его ключевая информация может быть отправлена только на первый узел, на который он был добавлен*

Пользователь ViPNet

Связи между пользователями ViPNet

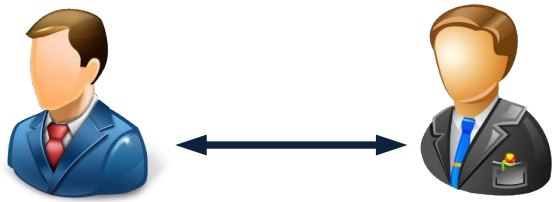
Связи между пользователями:

- ✔ *позволяют пользователям обмениваться друг с другом персональными зашифрованными сообщениями в программе ViPNet Деловая почта. Сообщение сможет прочесть только тот пользователь, которому оно адресовано*

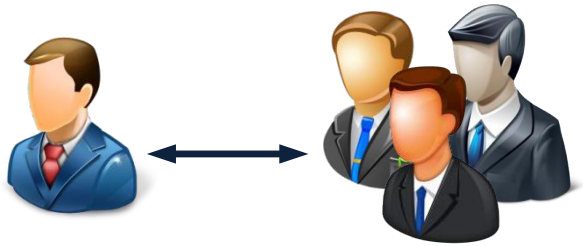
Пользователь ViPNet

Связи между пользователями ViPNet

пользователь – пользователь:



пользователь - группа пользователей:



- *создание связи пользователя с группой эквивалентно созданию связей пользователя с каждым участником группы*
- *при добавлении пользователя в группу автоматически создается связь между пользователем и этой группой*

Роли сетевых узлов

Роли сетевых узлов

Роль:

- *это атрибут сетевого узла ViPNet, который определяет возможность использования на сетевом узле программного обеспечения ViPNet или выполнения на узле служебных задач сети ViPNet*
- *набор ролей для каждого сетевого узла задается администратором ViPNet в клиентском приложении ЦУС*
- *список ролей, которые можно использовать в сети ViPNet, и количество узлов на которых их можно использовать содержатся в лицензионном файле infotecs.reg*

Примеры ролей сетевых

0004 "Network Control Center"

- *Позволяет установить на клиенте серверное приложение ViPNet Центр управления сетью (автоматически добавляется на первый клиент сети ViPNet и не может быть добавлена на другие клиенты)*

0017 "VPN-клиент"

- *позволяет использовать на сетевом узле программное обеспечение ViPNet Client. Может быть добавлена только на клиент.*

0018 "VPN-

- *позволяет использовать на сетевом узле программное обеспечение ViPNet Coordinator (Win или Lin). Может быть добавлена только на координатор. Не совместима с ролями для ПАК (Coordinator HW, KB)*

0000 "Business Mail"

- *позволяет использовать на клиенте программу ViPNet Деловая почта*

Примеры ролей сетевых узлов

infotecs

001E "SafeDisk"

- *позволяет использовать на сетевом узле программу ViPNet SafeDisk-V. Может быть добавлена на клиент или координатор*

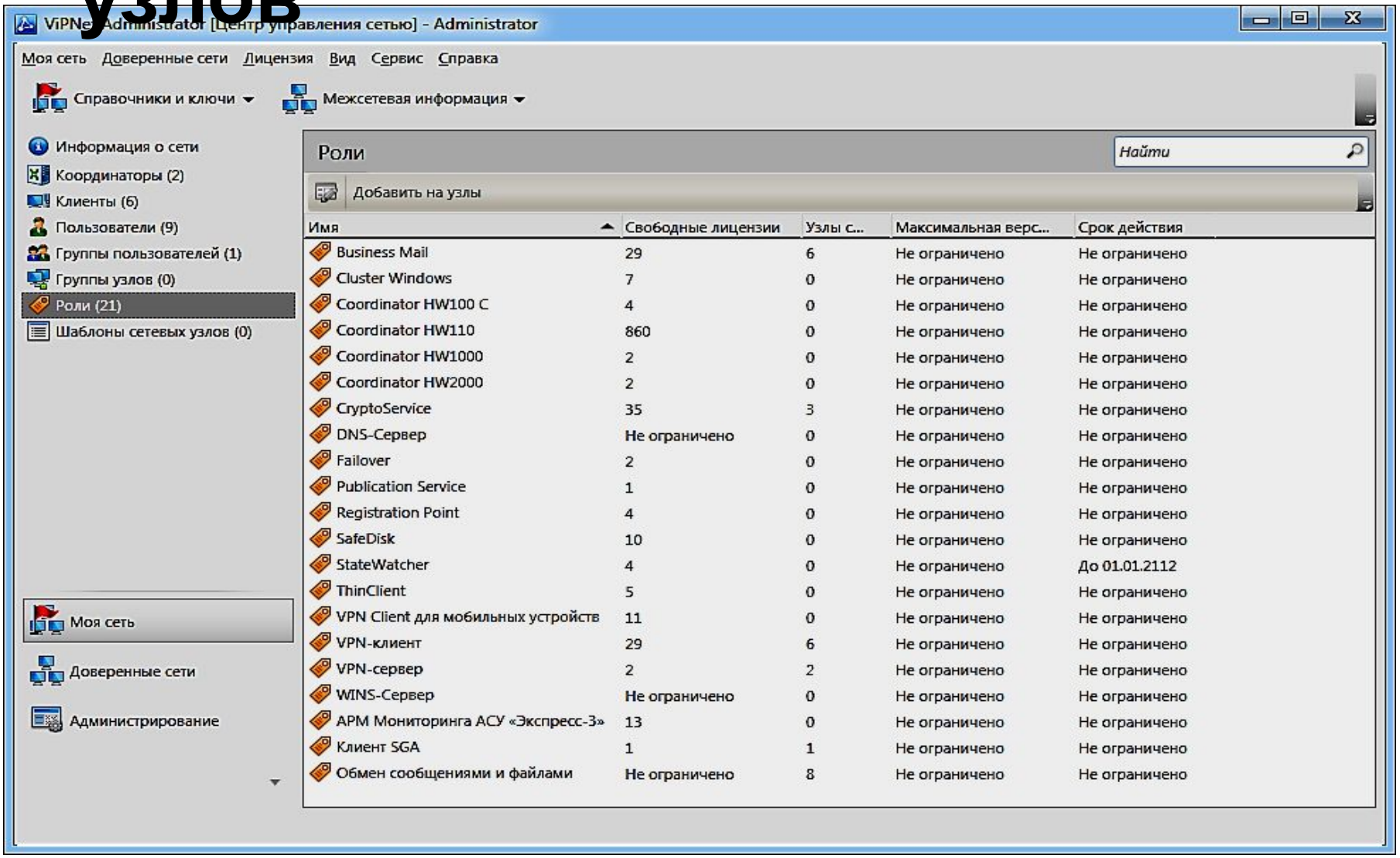
0020 "CryptoService"

- *позволяет использовать на сетевом узле программу ViPNet CryptoService. Может быть добавлена на клиент или координатор*

000C "Policy Manager"

- *позволяет использовать на клиенте программу ViPNet Policy Manager для централизованного управления политиками безопасности сетевых узлов.Может быть добавлена только на клиент, который не контролируется другим ViPNet Policy Manager.*

Примеры ролей сетевых узлов



Имя	Свободные лицензии	Узлы с...	Максимальная верс...	Срок действия
Business Mail	29	6	Не ограничено	Не ограничено
Cluster Windows	7	0	Не ограничено	Не ограничено
Coordinator HW100 C	4	0	Не ограничено	Не ограничено
Coordinator HW110	860	0	Не ограничено	Не ограничено
Coordinator HW1000	2	0	Не ограничено	Не ограничено
Coordinator HW2000	2	0	Не ограничено	Не ограничено
CryptoService	35	3	Не ограничено	Не ограничено
DNS-Сервер	Не ограничено	0	Не ограничено	Не ограничено
Failover	2	0	Не ограничено	Не ограничено
Publication Service	1	0	Не ограничено	Не ограничено
Registration Point	4	0	Не ограничено	Не ограничено
SafeDisk	10	0	Не ограничено	Не ограничено
StateWatcher	4	0	Не ограничено	До 01.01.2112
ThinClient	5	0	Не ограничено	Не ограничено
VPN Client для мобильных устройств	11	0	Не ограничено	Не ограничено
VPN-клиент	29	6	Не ограничено	Не ограничено
VPN-сервер	2	2	Не ограничено	Не ограничено
WINS-Сервер	Не ограничено	0	Не ограничено	Не ограничено
АРМ Мониторинга АСУ «Экспресс-3»	13	0	Не ограничено	Не ограничено
Клиент SGA	1	1	Не ограничено	Не ограничено
Обмен сообщениями и файлами	Не ограничено	8	Не ограничено	Не ограничено

Полномочия пользователей

Полномочия пользователей

ViPNet Полномочия пользователя ViPNet :

- ✔ *это права, которые дают возможность изменять пользователю установленного на сетевом узле настройки ПО ViPNet,*
- ✔ *задаются администратором ViPNet в клиентском приложении ЦУС в в свойствах ролей*
- ✔ *изменить уровень полномочий пользователя можно для сетевых узлов, на которые добавлены роли:*
  - ***VPN-сервер***
  - ***VPN-клиент***
  - ***CryptoService***
  - ***Business Mail***
  - ***VPN Client для мобильных устройств***

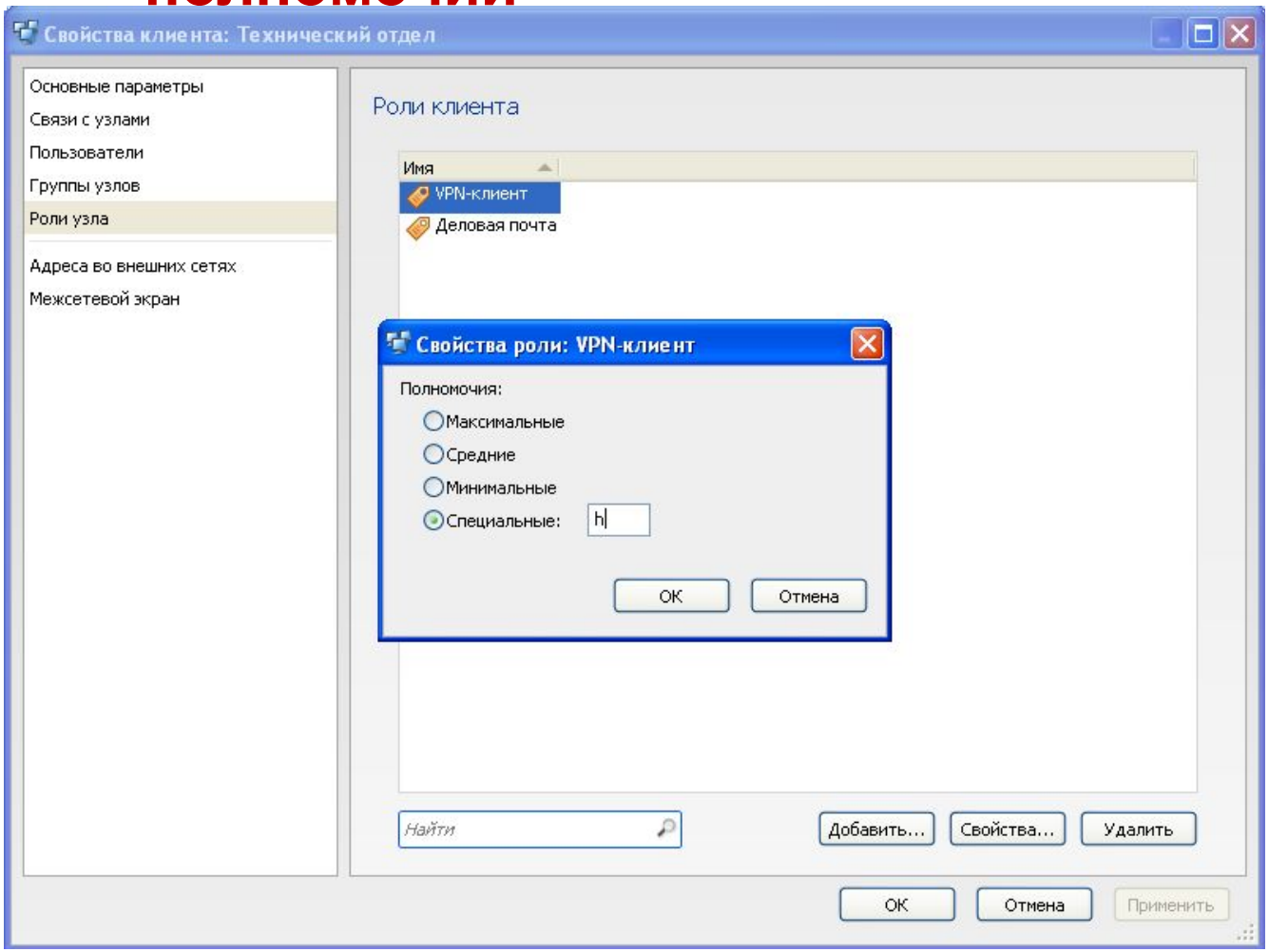
Полномочия пользователей

Уровни полномочий

Минимальные полномочия	пользователь не может изменять настройки ПО ViPNet
Средние полномочия	пользователь может изменять некоторые параметры работы ПО ViPNet
Максимальные полномочия	пользователь не имеет ограничений по настройкам и использованию различных функций ПО ViPNet
Специальные полномочия	зависят от роли, добавленной на сетевой узел. Позволяют сделать специальные настройки ПО ViPNet

Полномочия пользователей

Назначение уровня полномочий



Лицензирование сети ViPNet

Файл лицензии

Файл лицензии:

- файл **infotecs.reg** **.itcslic*, в котором содержатся или параметры сети ViPNet
- файл лицензии необходим при серверного установке приложения ViPNet Центр управления сетью
- необходимо обратиться в ОАО «ИнфоТеКС» и получить новый файл лицензии

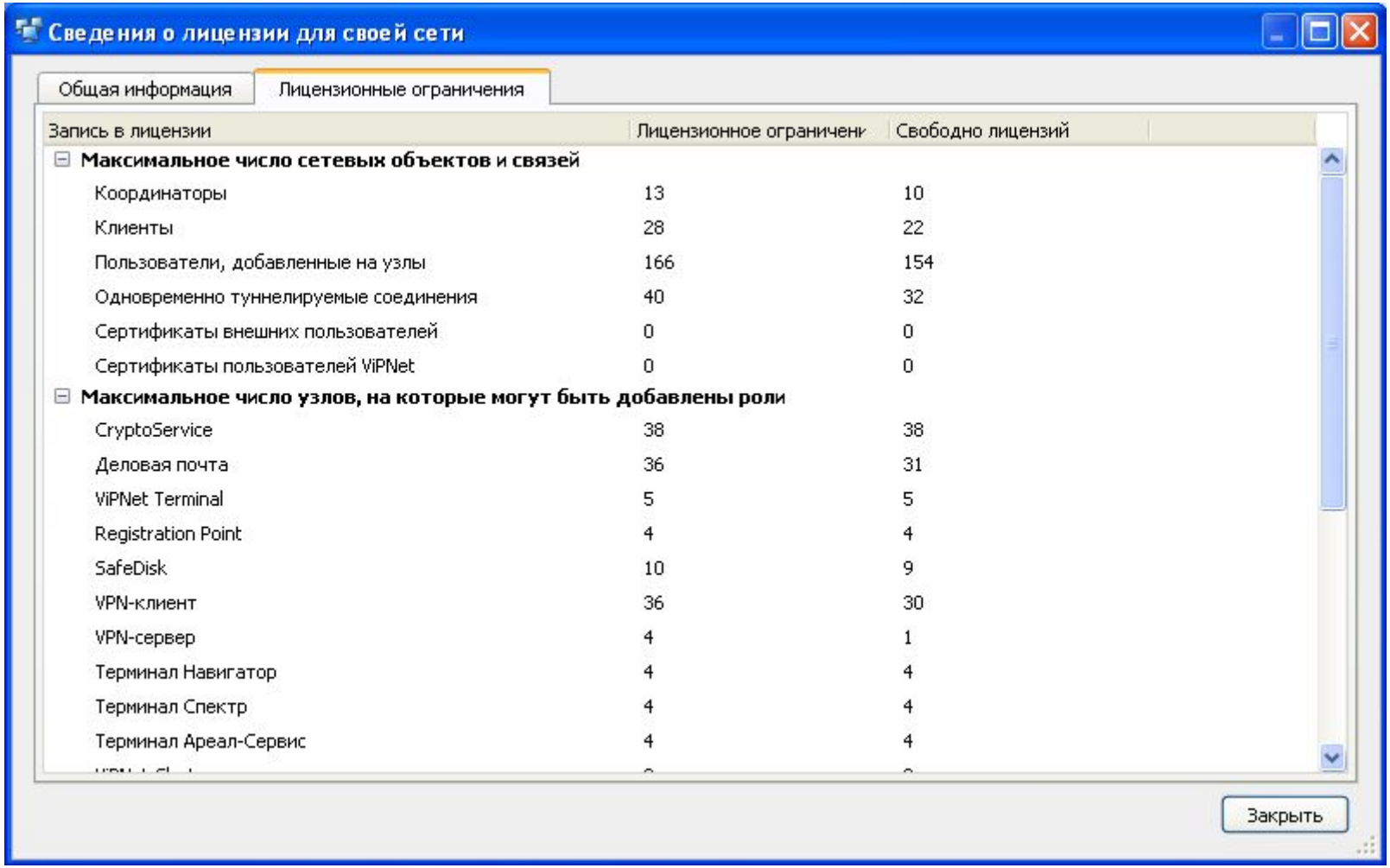
Лицензирование сети ViPNet

Файл лицензии содержит:

- ✔ Номер сети ViPNet и номера подчиненных сетей (если лицензия предполагает создание иерархии сетей ViPNet).
- ✔ Сведения о владельце сети.
- ✔ Возможность использования функций удостоверяющего центра и максимальное число сертификатов ключа проверки электронной подписи, которое может быть издано в УКЦ для внешних пользователей и пользователей ViPNet.
- ✔ Список ролей, разрешенных для использования в сети ViPNet и ограничения на количество узлов с различными ролями.
- ✔ Ограничения на версии и период использования программного обеспечения для ролей.
- ✔ Общий срок действия лицензии.

Лицензирование сети ViPNet

Просмотр файла лицензии



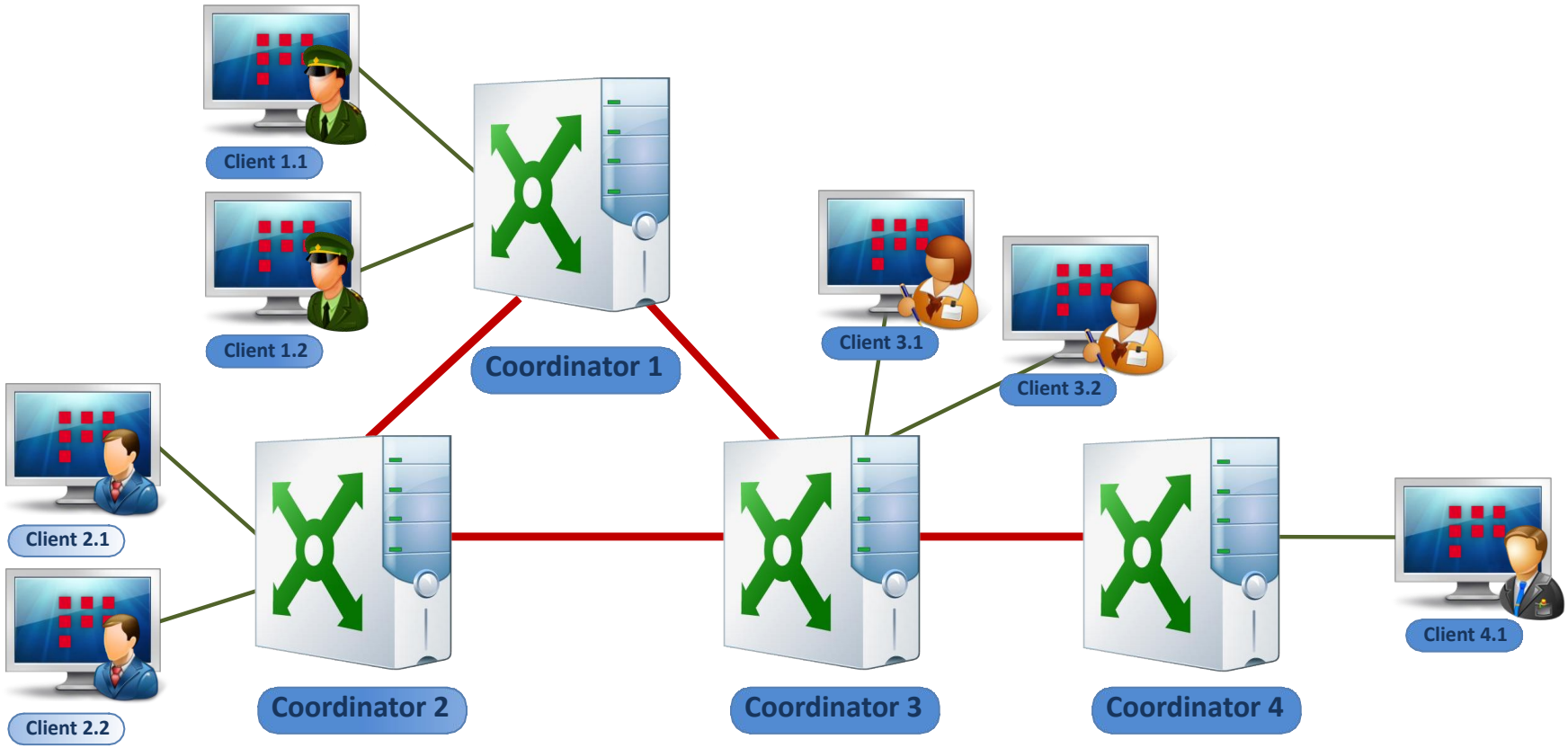
Межсерверные каналы

Межсерверные каналы

- *на основании межсерверных каналов выполняется маршрутизация управляющих, прикладных и транспортных конвертов между координаторами*
- *межсерверные каналы могут быть организованы по любой схеме*
- *если есть несколько маршрутов передачи конвертов между координаторами, будет использован кратчайший из них*

Межсерверные каналы

Межсерверные каналы



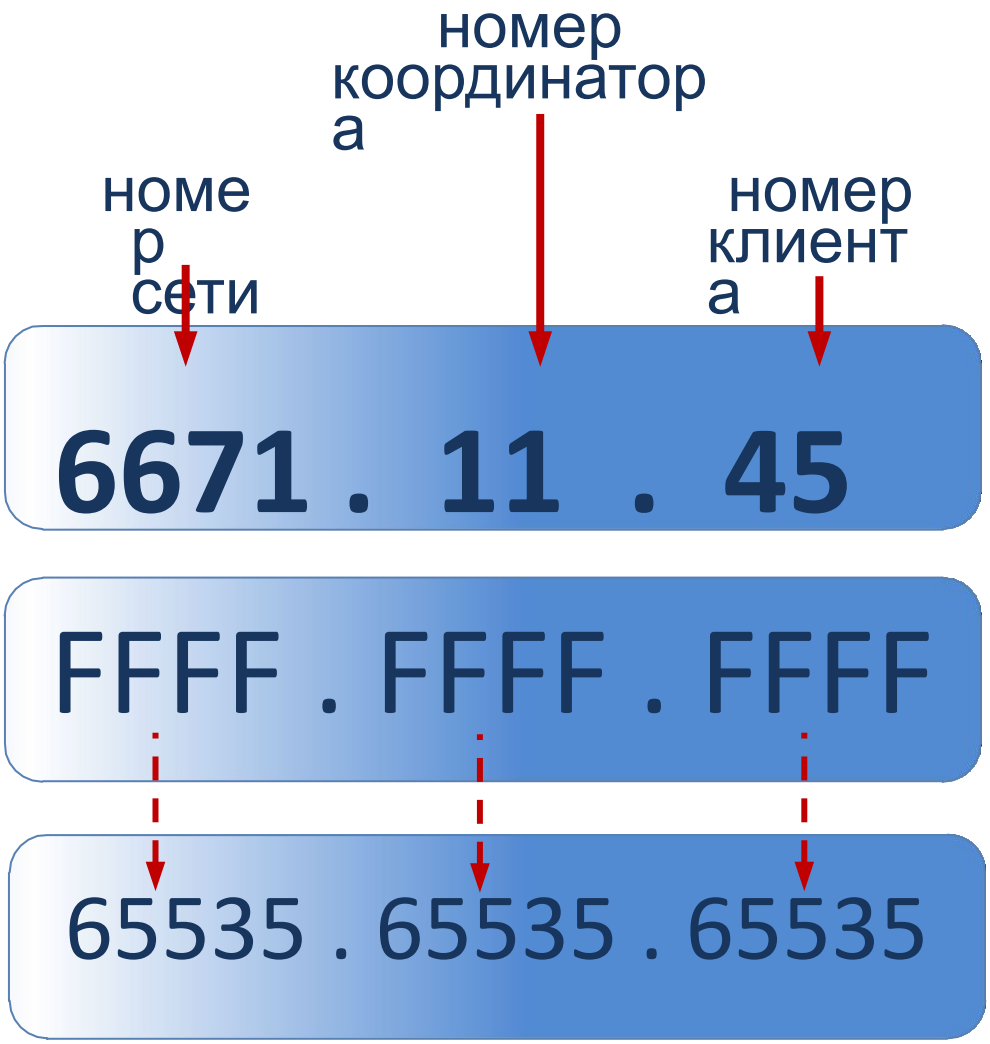
Идентификаторы объектов

Сетевой адрес

- *сетевой адрес состоит из номера сети ViPNet, номера координатора и номера клиента на координаторе*
- *на основе сетевого адреса осуществляется маршрутизация пакетов в сети ViPNet*
- *структура сетевого адреса позволяет иметь до 65535 сетей ViPNet, в каждой сети может быть до 65535 сетевых узлов, на каждом из которых может быть зарегистрировано до 65535 пользователей*

Идентификаторы объектов

Сетевой адрес



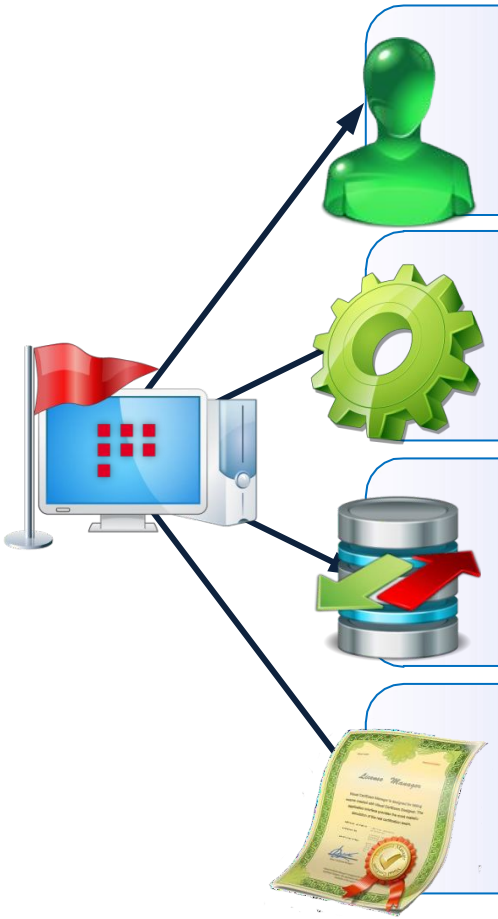
ЛЕКЦИЯ 3

«ViPNet Administrator »

ViPNet Administrator 4.x

ViPNet Administrator 4.x

Состав ViPNet Administrator



клиентское приложение ЦУС:
графический интерфейс для управления структурой сети ViPNet и свойствами сетевых объектов

серверное приложение ЦУС:
приложение с помощью которого осуществляется работа с базой данных SQL

база данных SQL-сервера:
предназначена для хранения полной информации о структуре и объектах сети ViPNet

удостоверяющий и ключевой центр:
предназначен для управления ключевой структурой сети ViPNet и издания и обслуживания сертификатов

ViPNet Administrator 4.x

База данных SQL-сервера

База данных SQL-сервера:

- ✔ *предназначена для хранения информации о структуре и настройках сети ViPNet*
- ✔ *создается автоматически при установке серверного приложения ЦУСа*

Для размещения базы данных можно использовать:

- ✔ *существующий именованный экземпляр SQL-сервера, который установлен на локальный или удаленный компьютер*
- ✔ *SQL-сервер, входящий в комплект поставки ViPNet Administrator*

ViPNet Administrator 4.x

Поддерживаемые версии СУБД

- ✔ Microsoft SQL Server 2008 Express SP3 и выше
- ✔ Microsoft SQL Server 2008 R2 Express SP1 и выше
- ✔ Microsoft SQL Server 2012 Express
- ✔ Microsoft SQL Server 2014 Express

Внимание! По умолчанию устанавливается Microsoft SQL Server 2014 Express и создается именованный экземпляр SQL-сервера WINNCCSQL

ViPNet Administrator 4.x

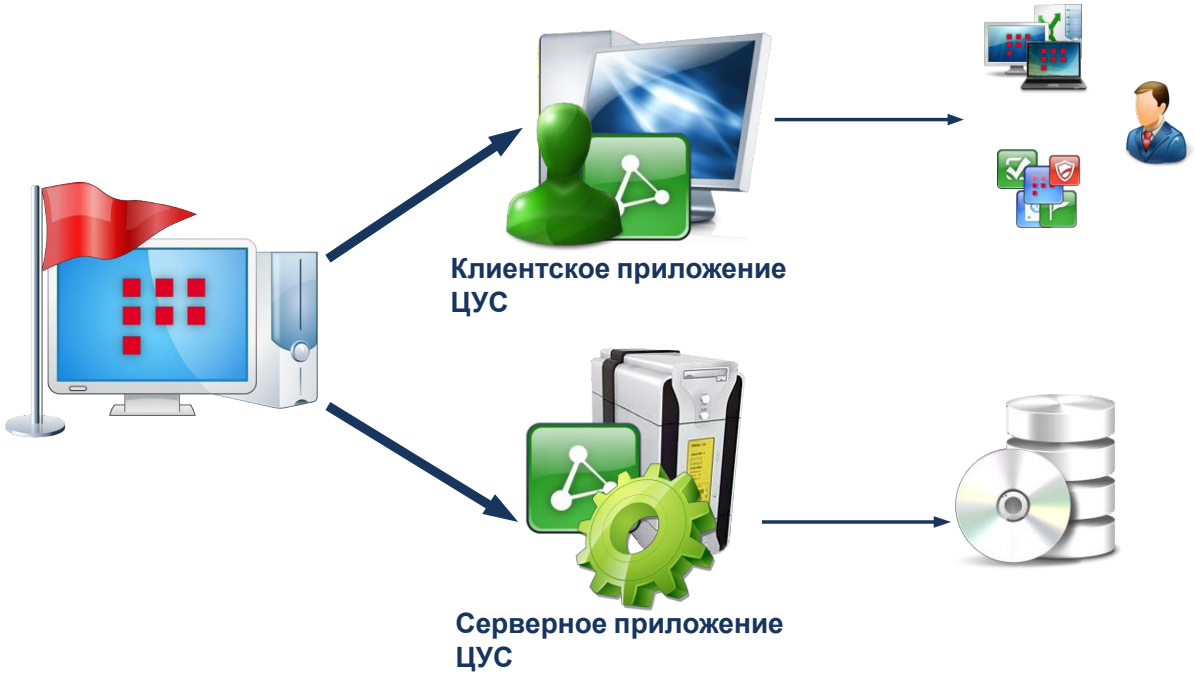
База данных SQL-сервера

При установке серверного приложения ЦУСа создаются:

- ✔ *база данных с именем **ViPNetAdministrator**, в которой хранится информация о структуре и настройках сети ViPNet*
- ✔ *база данных с именем **ViPNetJournals**, в которой хранятся журналы аудита программы ViPNet ЦУС*
- ✔ *учетная запись пользователя **CaUser**, под которыми осуществляется подключение УКЦ к базе данных*
- ✔ *учетная запись пользователя **NccUser**, под которыми осуществляется подключение ЦУС к базе данных*
- ✔ *учетная запись пользователя с правами администратора базы данных*

ViPNet Administrator 4.x

ViPNet Центр управления сетью



ViPNet Центр управления сетью предназначен для формирования и управления структурой сети ViPNet

ViPNet ЦУС состоит из двух компонент:

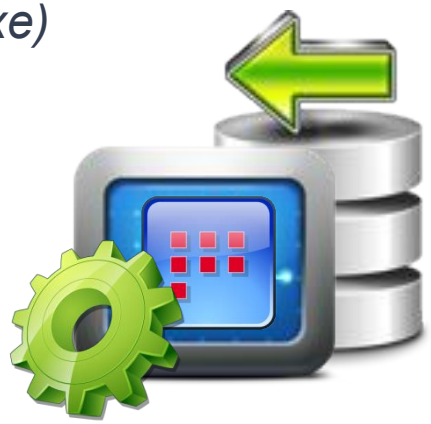
- ✔ *серверного приложения ЦУС*
- ✔ *клиентского приложения ЦУС*

ViPNet Administrator 4.x

Серверное приложение ViPNet ЦУС

Серверное приложение ViPNet ЦУС:

- *осуществляет чтение и запись информации в базу данных SQL и обеспечивают взаимодействие с клиентским приложением*
- *представляет собой набор служб:*
  - ✔ *NccService (процесс Infotecs.WinNCC.Communication.Hosting.exe)*
  - ✔ *NccFilewatcherService (процесс Infotecs.WinNcc.FileWatcher.Service.exe)*
- *запускается автоматически после загрузки операционной системы*



ViPNet Administrator 4.x

Клиентское приложение ViPNet ЦУС

Клиентское приложение ViPNet ЦУС:

- *обеспечивает удобный графический интерфейс для управления структурой сети ViPNet и свойствами сетевых объектов*
- *может быть установлено:*
  - ✔ *на одном компьютере с серверным приложением*
  - ✔ *на удаленном компьютере*
  - ✔ *на нескольких компьютерах (при работе в многопользовательском режиме)*
- *в процессе работы взаимодействует с серверным приложением ЦУС*

ViPNet Administrator 4.x

Функции ViPNet ЦУС

управление структурой сети ViPNet

- ✔ *создание и удаление сетевых узлов*
- ✔ *создание и удаление пользователей*
- ✔ *определение связей между сетевыми узлами и пользователями*

настройка свойств объектов сети

- ✔ *добавление ролей на сетевые узлы*
- ✔ *настройка параметров доступа к сетевым узлам (IP-адреса, DNS-имена и т.д.)*
- ✔ *настройка способа подключения к внешней сети*
- ✔ *задание полномочий пользователей*
- ✔ *настройка туннелируемых ресурсов*

ViPNet Administrator 4.x

infotecs

Функции ViPNet ЦУС

организация межсетевого

- ✔ *организация защищенного соединения с другими сетями ViPNet*
- ✔ *управление связями между узлами своей сети и узлами доверенных сетей*
- ✔ *обмен межсетевой информацией*

отправка обновлений на сетевые узлы

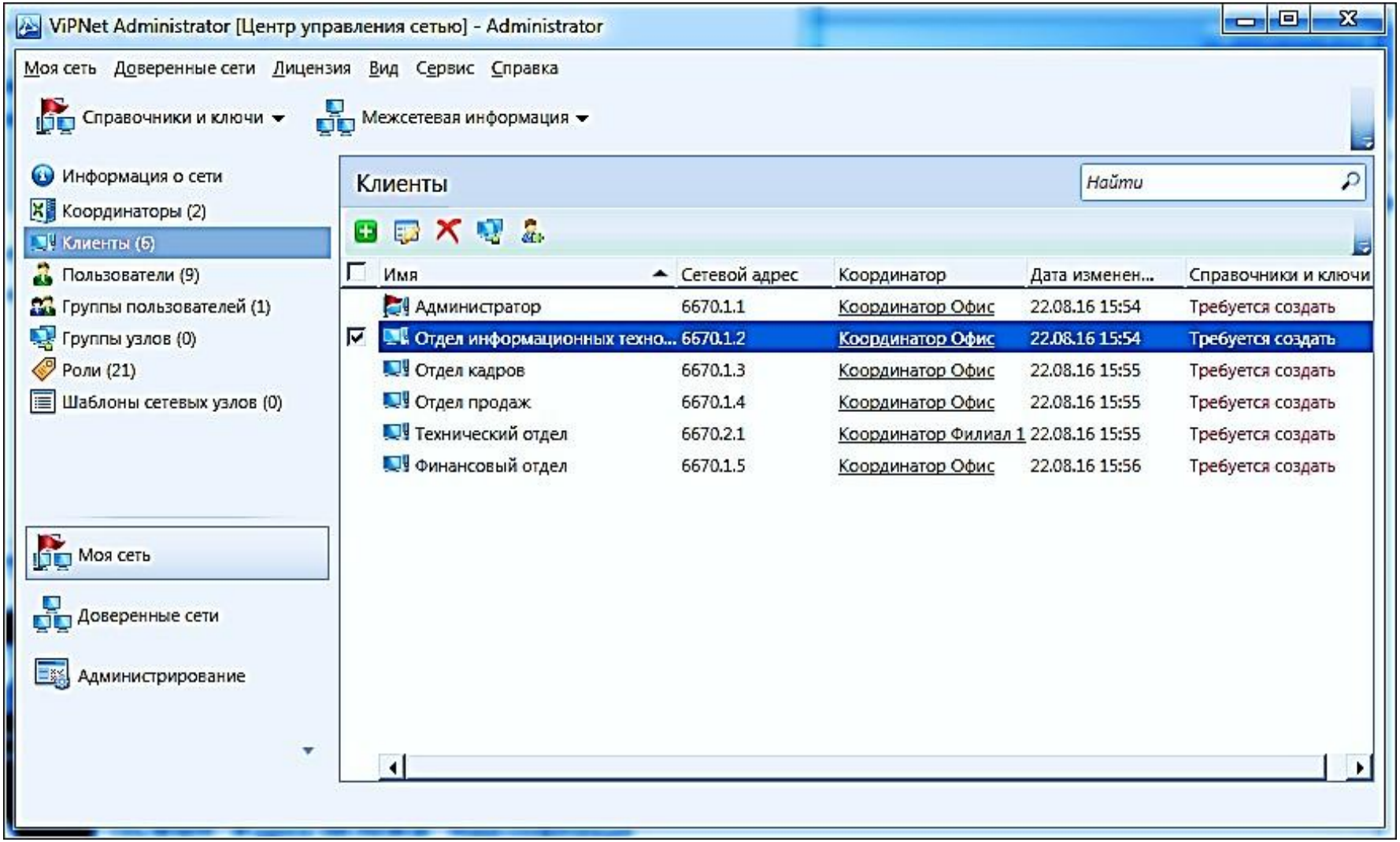
- ✔ *удаленное обновление на сетевых узлах ключей*
- ✔ *удаленное обновление на сетевых узлах справочников*
- ✔ *удаленное обновление на сетевых узлах программного обеспечения ViPNet*

административные

- ✔ *создание и удаление учетных записей администраторов ViPNet ЦУС*
- ✔ *просмотр журналов аудита системных событий ViPNet ЦУС*
- ✔ *просмотр журналовобмена транспортными конвертами между ЦУС узлами и ViPNet*
- ✔ *резервное копирование и восстановление данных*
- ✔ *обновление лицензии на сеть ViPNet*

ViPNet Administrator 4.x

Интерфейс клиентского приложения ЦУС



ViPNet Administrator 4.x

ViPNet Удостоверяющий и ключевой центр

ViPNet Удостоверяющий и ключевой центр предназначен для формирования ключей шифрования и электронной подписи и управления инфраструктурой PKI

ViPNet УКЦ состоит из двух компонент:

- ✔ *ключевого центра*
- ✔ *удостоверяющего центра*

ViPNet Administrator 4.x

Задачи ключевого центра

- *формирование мастер-ключей своей сети*
- *формирование межсетевых мастер-ключей, необходимых для установления взаимодействия с доверенными сетями*
- *создание ключей для объектов сети ViPNet*
- *обновление ключевой информации сети ViPNet*
- *формирование паролей*
- *генерация ключей подписи Уполномоченных лиц Удостоверяющего центра*
- *генерация ключей подписи пользователей*

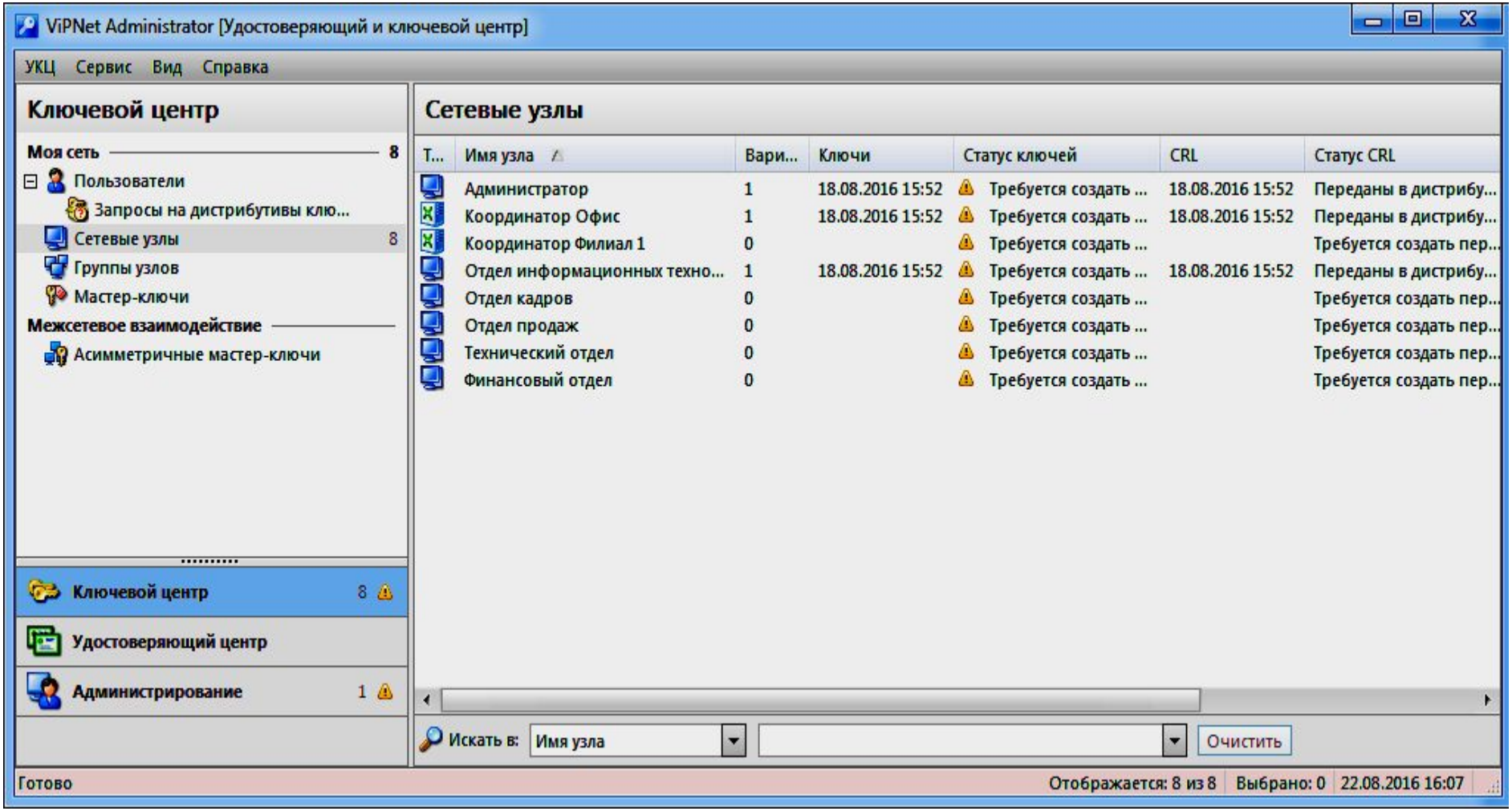
ViPNet Administrator 4.x

Задачи удостоверяющего центра

- *издание сертификатов открытого ключа подписи*
- *управление жизненным циклом сертификатов*
- *формирование корневых сертификатов администраторов, списков отозванных сертификатов, запросов на проведение кросс-сертификации*
- *импорт корневых сертификатов и CAC из доверенных сетей ViPNet и других удостоверяющих центров*
- *разбор конфликтных ситуаций и экспертиза правомочности и подлинности электронных документов*
- *сервисные функции (оповещение, автоматическое формирование архивов)*

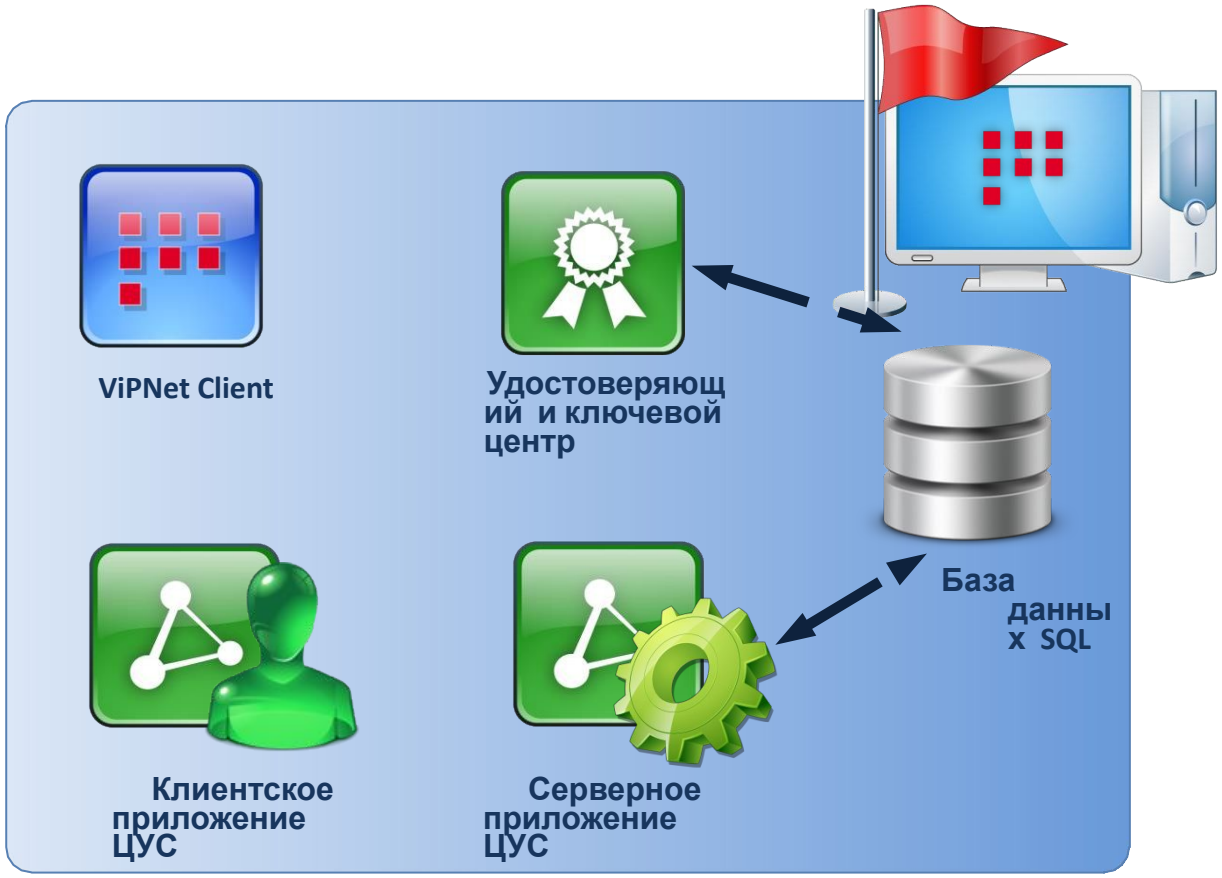
ViPNet Administrator 4.x

Интерфейс удостоверяющего и ключевого центра



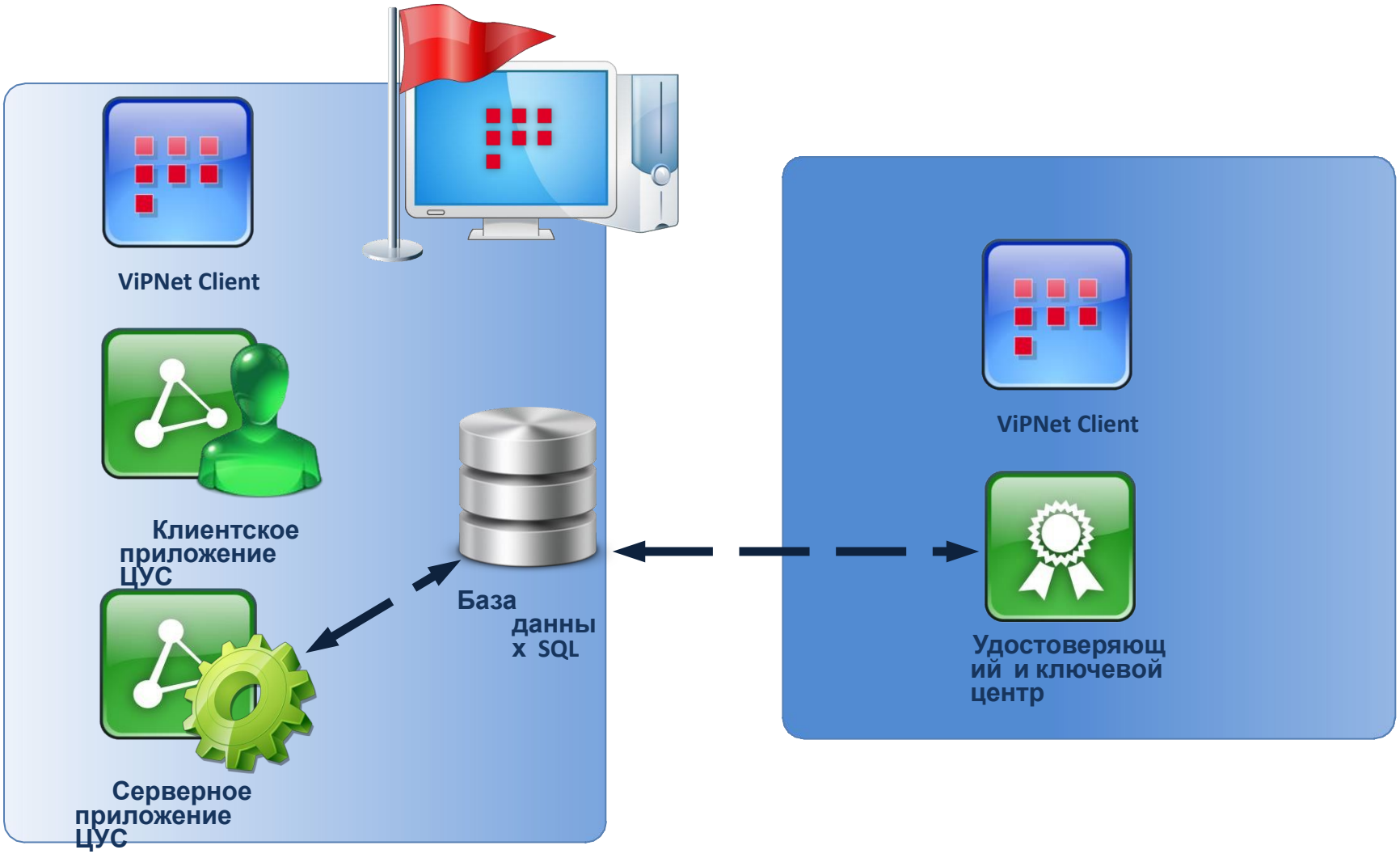
ViPNet Administrator 4.x

Схемы размещения компонентов ViPNet Administrator



ViPNet Administrator 4.x

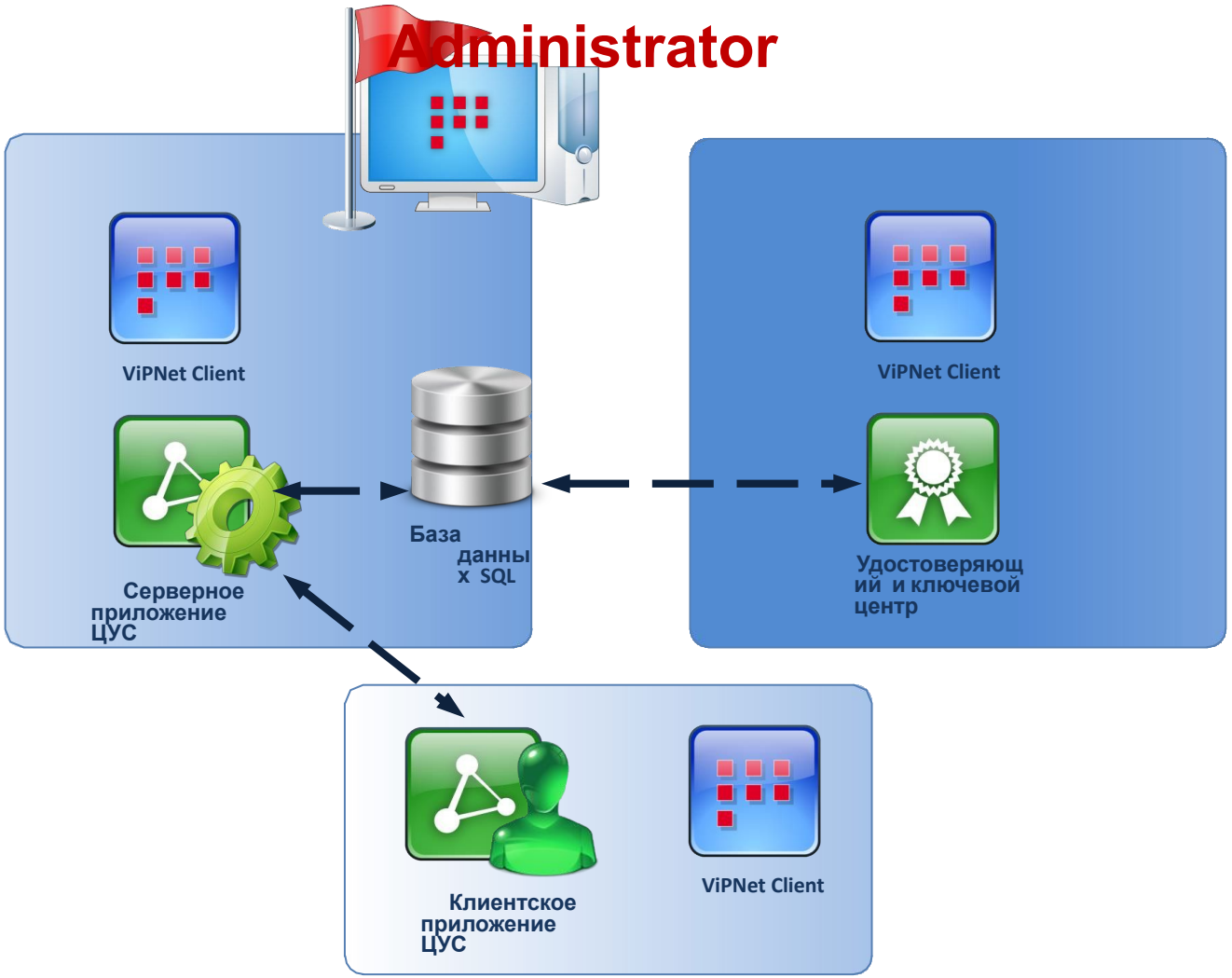
Схемы размещения компонентов ViPNet Administrator



ViPNet Administrator 4.x

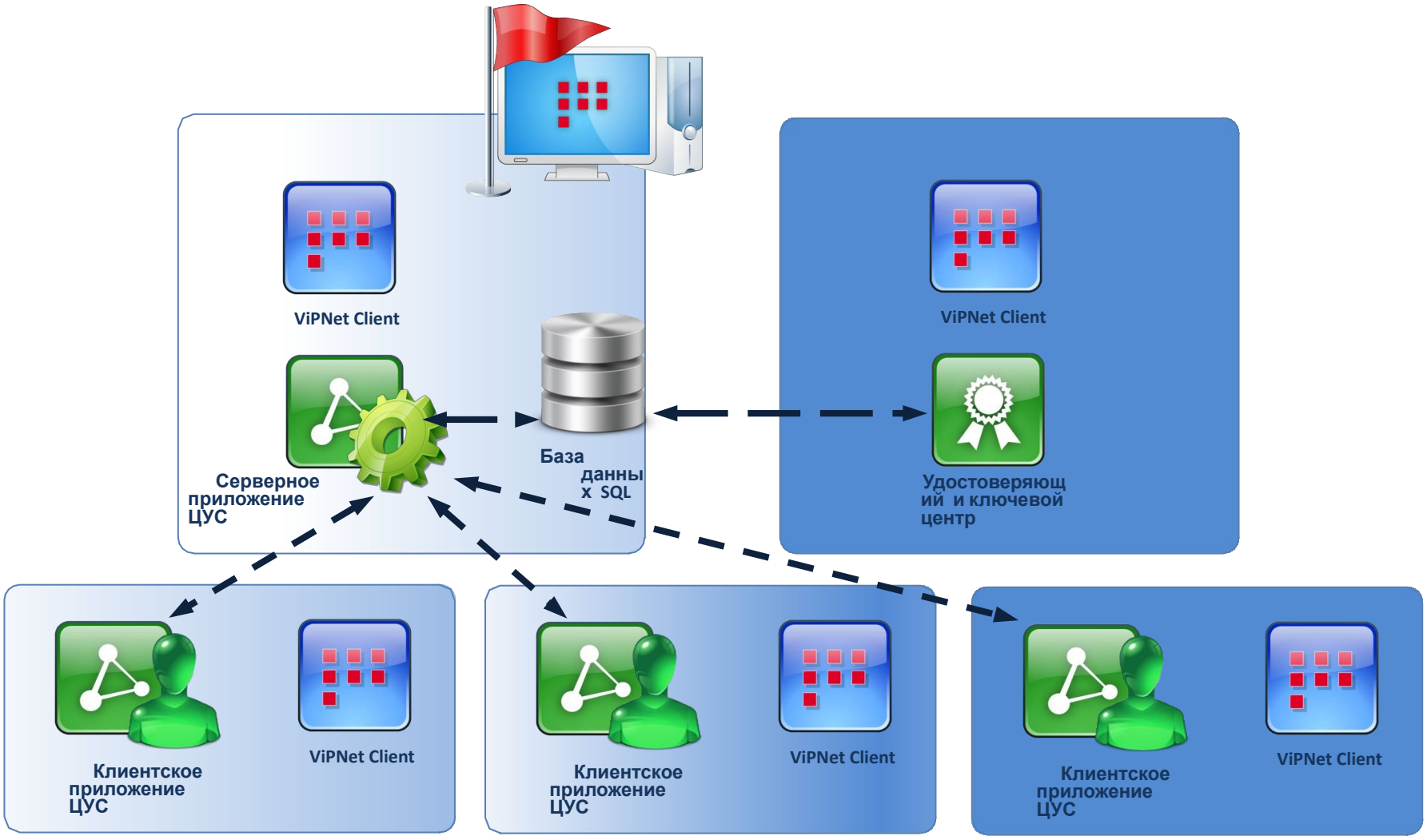
infotecs

Схемы размещения компонентов ViPNet Administrator



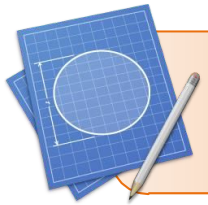
ViPNet Administrator 4.x

Схемы размещения компонентов ViPNet Administrator



ViPNet Administrator 4.x

Порядок создания сети ViPNet



1. разработка структуры защищенной сети

2. установка ПО ViPNet Administrator

3. создание и настройка сетевых узлов

4. создание и настройка пользователей

5. первичная инициализация УКЦ
   формирование dst-файлов

6. установка и настройка ПО ViPNet на компьютерах корпоративной