Администрирование системы защиты информации ViPNet версии 4.x

НОЧУ ДПО ЦПК «Учебный центр «ИнфоТеКС»
education@infotecs.ru

ОАО «ИнфоТеКС», Москва
(495) 737-61-92
www.infotecs.ru

Требования к первичным знаниям слушателя

Перед началом обучения на курсе «Администратор системы защиты информации ViPNet версии 4.x», слушатель должен знать:

- принципы работы IP-сетей;
- технологии, применяемые для защиты конфиденциальной информации;
- принципы работы защищенных виртуальных сетей (VPN).

Цель курса

После окончания курса администратор системы защиты информации ViPNet должен знать:

- порядок проектирования защищенных корпоративных сетей на базе технологии ViPNet;
- особенности криптосистемы и состав ключевой информации ViPNet;
- правила администрирования объектов защищенной сети ViPNet;
- основные характеристики, назначение и принципы работы базовых программных модулей ViPNet Network Security.

После окончания курса администратор системы защиты информации ViPNet должен уметь:

- проектировать и администрировать защищенные сети ViPNet;
- проектировать и внедрять системы защиты информации на базе технологии ViPNet;
- обеспечивать корректное взаимодействие объектов сети ViPNet;
- обеспечивать бесперебойную работу серверных модулей ViPNet;
- обеспечивать бесперебойную работу клиентских модулей ViPNet;
- консультировать пользователей по вопросам работы с ПО ViPNet;
- организовывать взаимодействие сетей ViPNet;
- использовать прикладные сервисы ViPNet.

ОАО «ИнфоТеКС»

открытое акционерное общество «Информационные технологии и коммуникационные системы»

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 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: https://www.infotecs.ru/about/sertificate/

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

СЕРТИФИКАТ СООТВЕТСТВИЯ

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

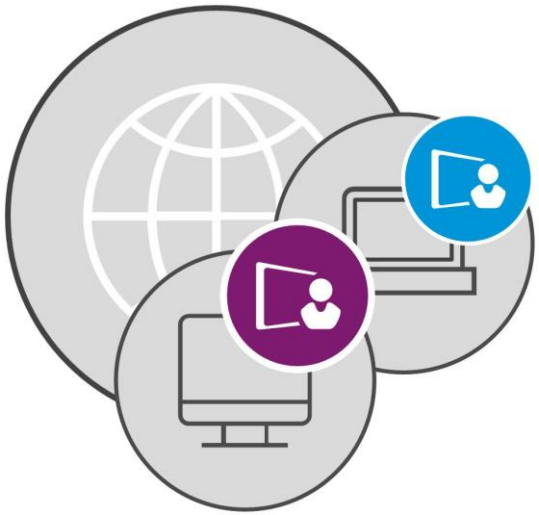
Настоящий сертификат зарегистрирован в государственном реестре сертификатов ФСБ России.

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)

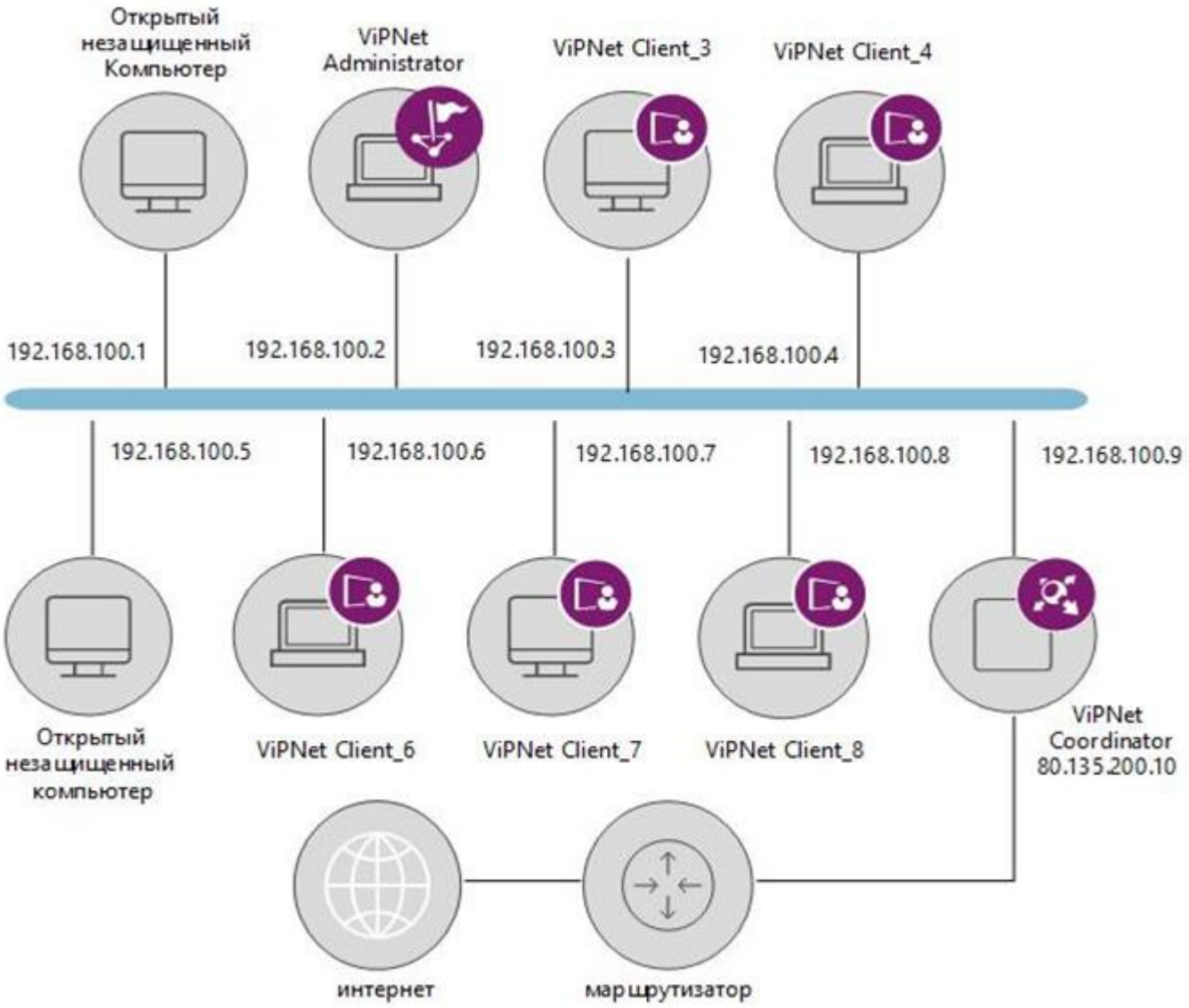
Архитектура VPN

Виртуальные защищенные сети (VPN)

VPN (Virtual Protected Network):

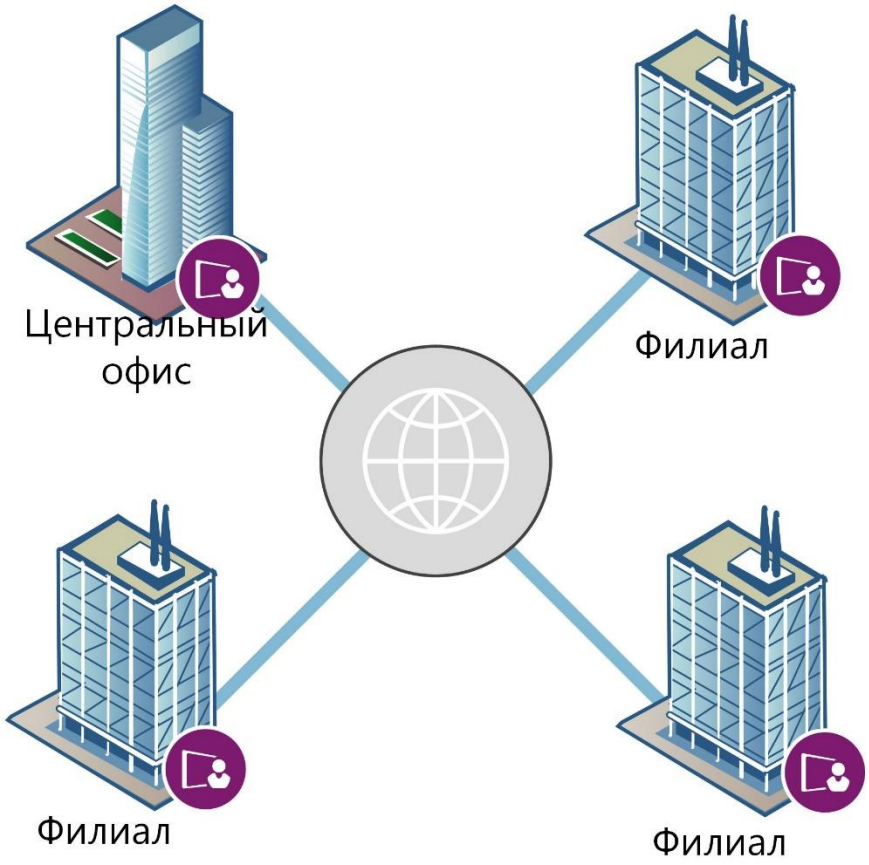
- это обобщённое название технологий, которые позволяют объединить в виртуальную защищенную сеть произвольное количество локальных сетей и отдельных компьютеров
- VPN-сеть строится поверх других сетей передачи данных (в том числе и сети Интернет)
- с помощью криптографических методов VPN-сеть позволяет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

Схема защиты информации средствами ViPNet в ЛВС



Архитектура VPN

Intranet VPN



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

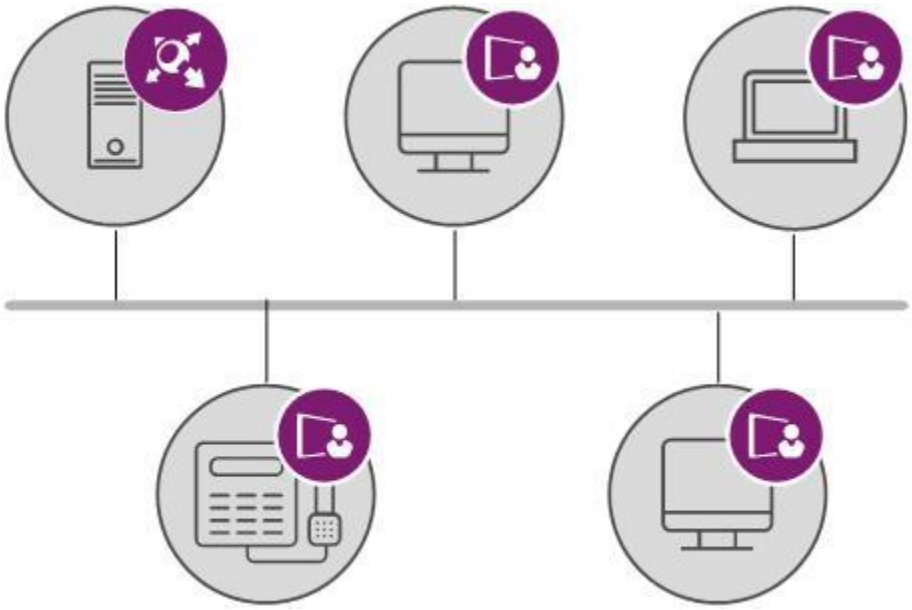
Архитектура VPN

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

Client-Server VPN



- обеспечивает защиту передаваемых данных между двумя узлами корпоративной сети.

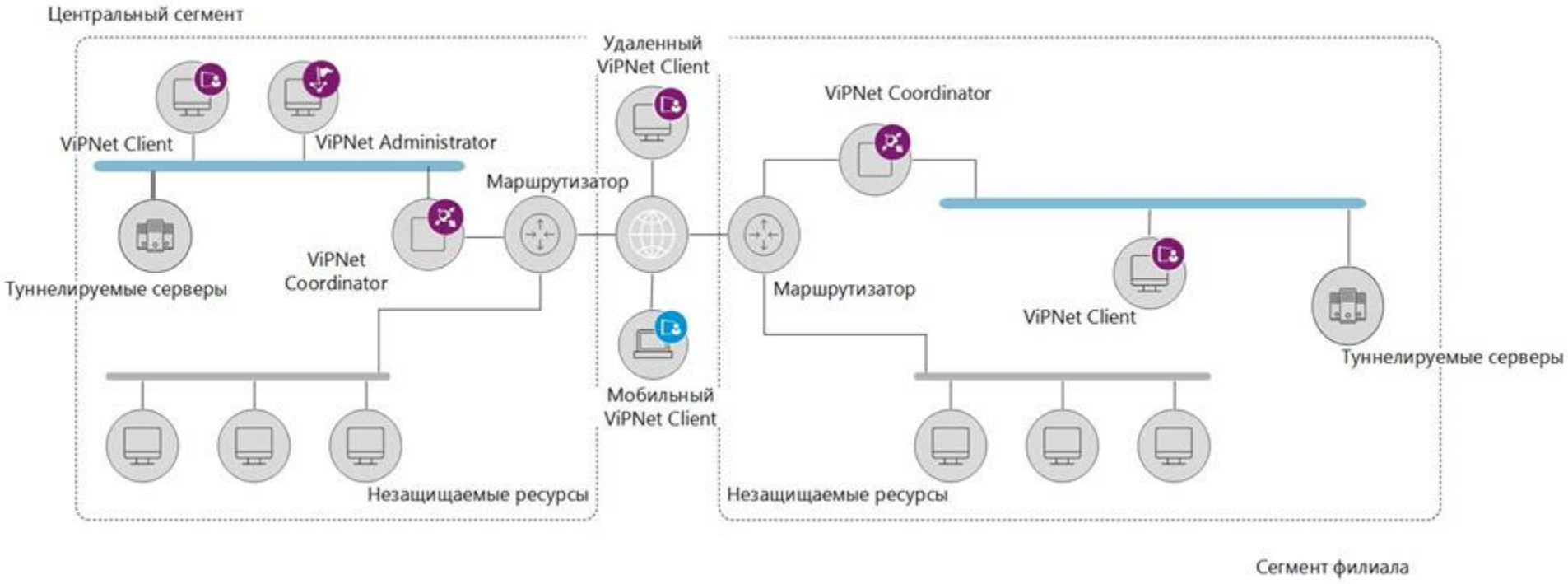
Архитектура VPN

Extranet VPN

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

Типичная схема организации защиты информации

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



Технология ViPNet

Туннелирование IP-трафика

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

Туннель создается с помощью технологий инкапсуляции и туннелирования

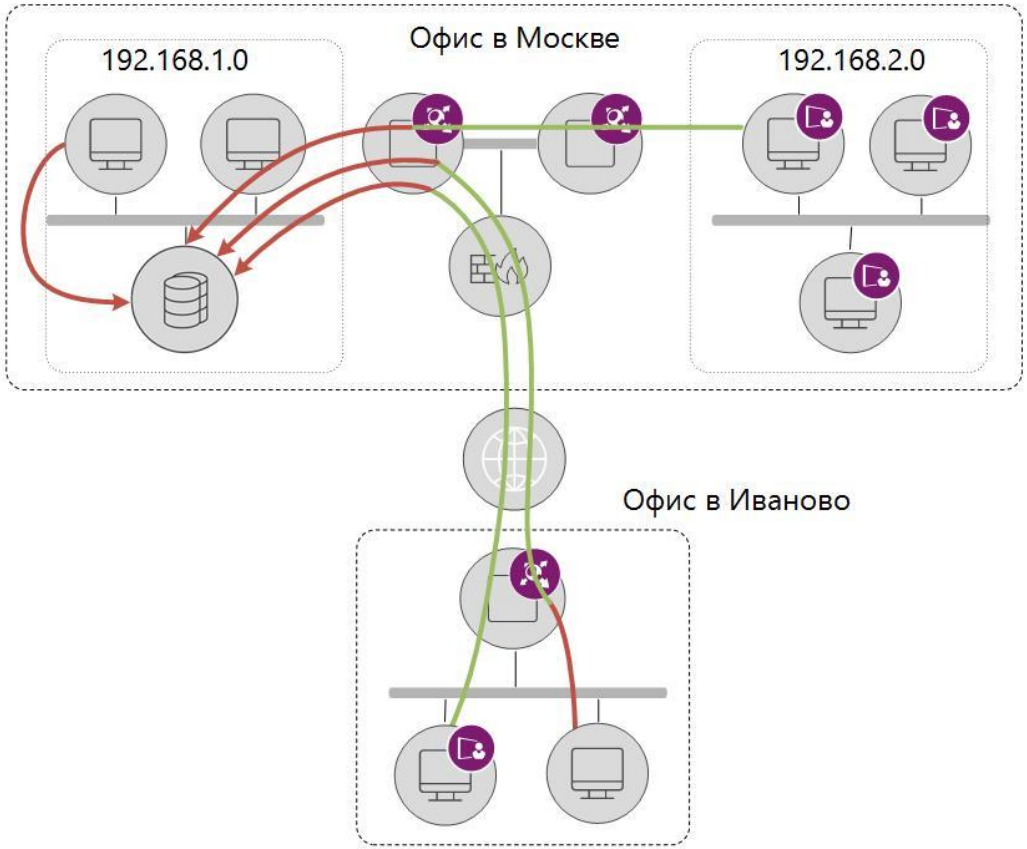
Туннель обладает свойствами защищенной выделенной линии

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



Инкапсуляция IP-трафика

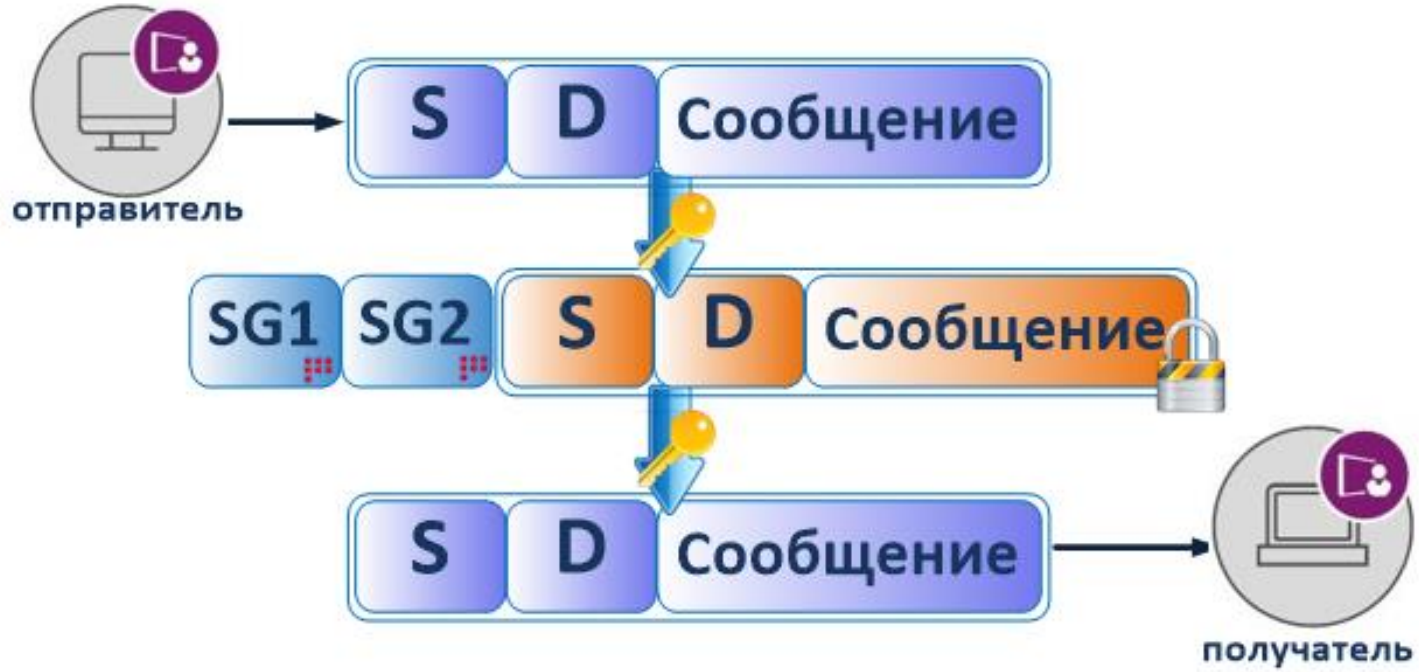
Инкапсуляция:

- 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



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

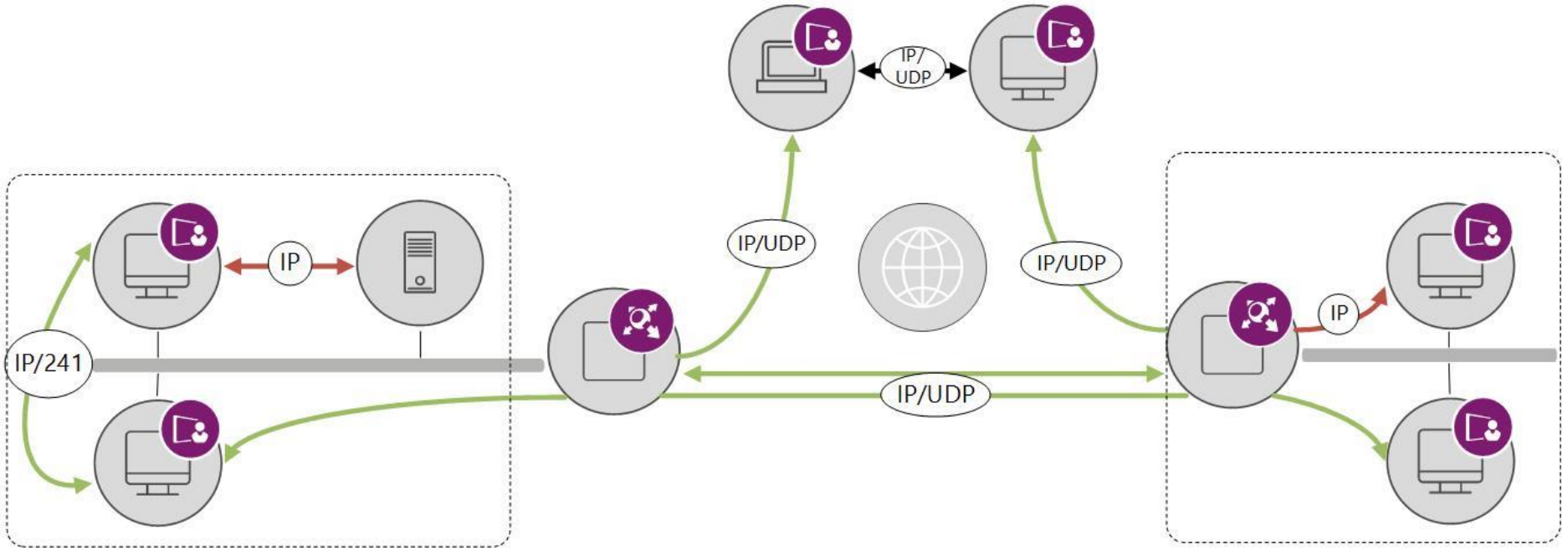
- если по пути следования пакета нет преобразования IP-адресов (узлы доступны по реальным IP-адресам);
- если узлы расположены в одном маршрутизируемом сегменте.

используется протокол IP/UDP (порт 55777)

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

Технология ViPNet

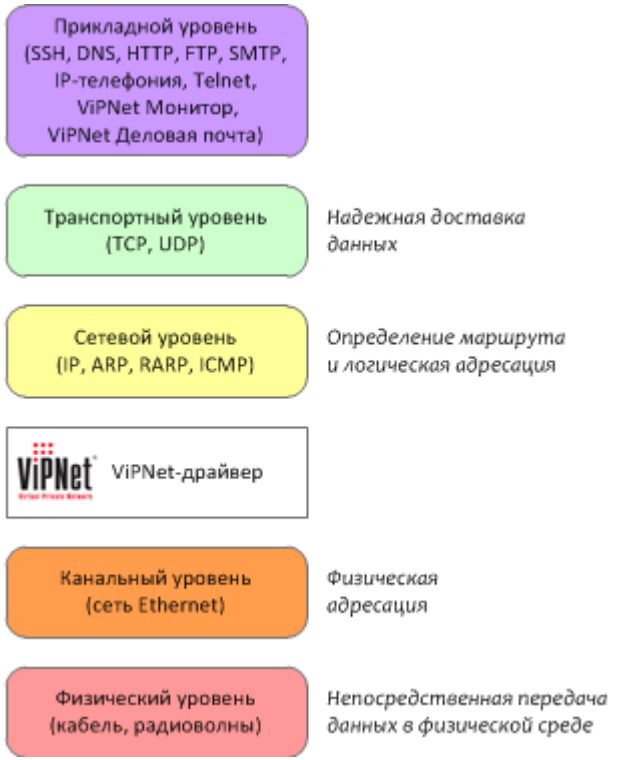
Инкапсуляция IP-трафика



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.



Примечание. На приведенной схеме модели OSI допущены следующие упрощения:

- Транспортный и сеансовый уровни объединены в транспортный уровень.
- Прикладной уровень и уровень представления объединены в прикладной уровень.

Технология ViPNet

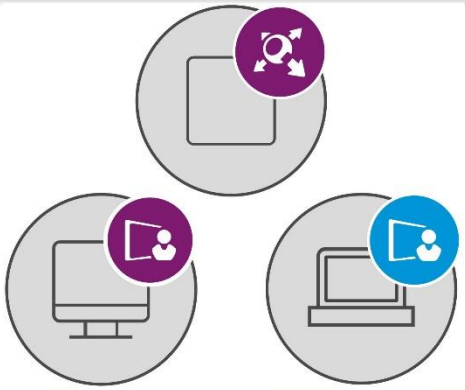
Модули защищенной сети ViPNet

ViPNet Network Security 4.x

Программно-аппаратный комплекс ViPNet

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



Назначение VPN ViPNet

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

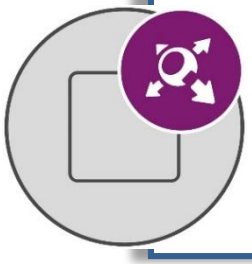
- создание защищенной среды передачи данных с использованием публичных и выделенных каналов связи путем организации сети VPN;
- развертывание инфраструктуры открытых ключей (PKI) и организация Удостоверяющего центра, что позволит использовать ЭП в прикладном ПО Заказчика (системах ЭДО, электронной почте,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

ViPNet Network Security 4.x

Базовые модули ViPNet 4.x

ViPNet Administrator

- предназначен для создания и управления защищенной сетью ViPNet



ViPNet Coordinator

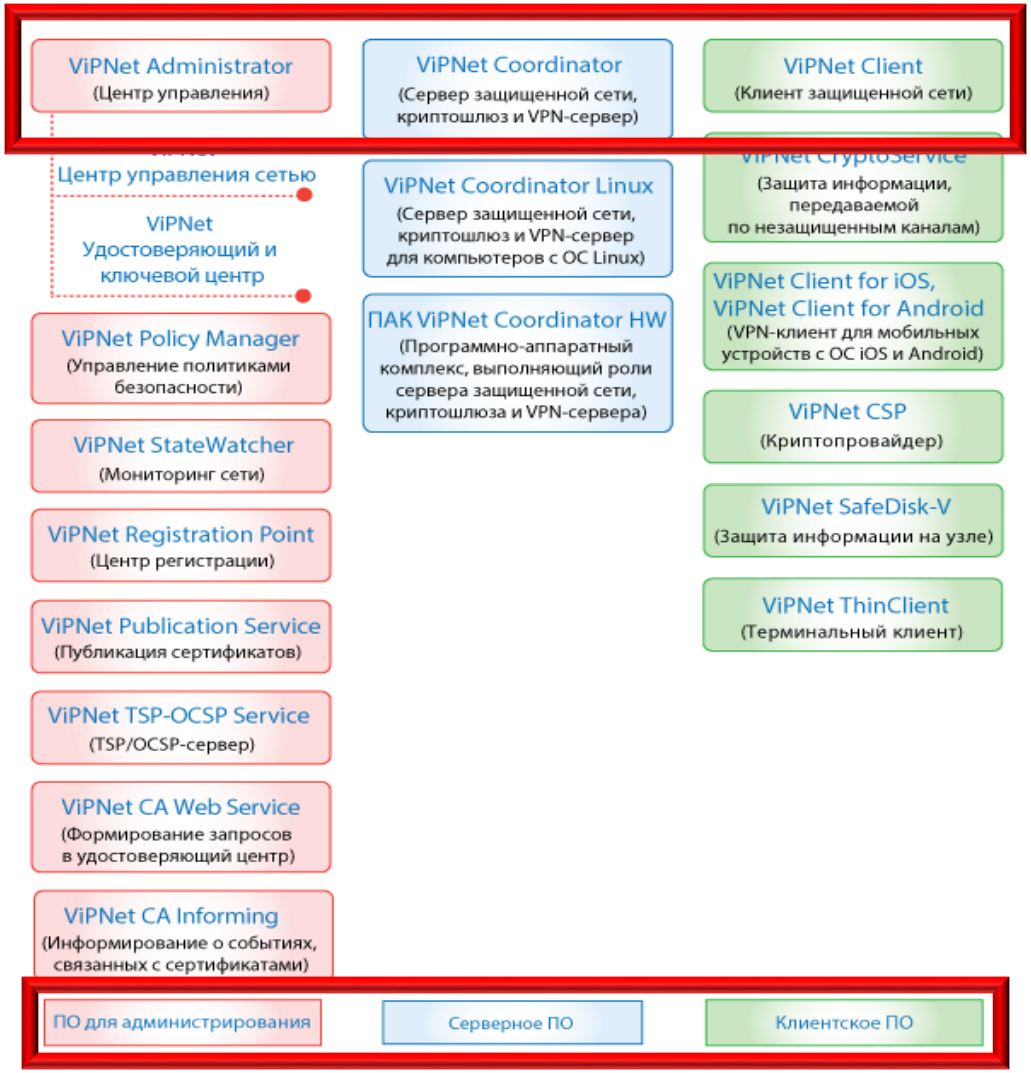
- предназначен для защиты сегментов IP-сетей, координации работы узлов защищенной сети

ViPNet Client

- предназначен для защиты отдельных компьютеров

ViPNet Network Security 4.x

Состав VPN ViPNet 4.x



ViPNet Network Security 4.x

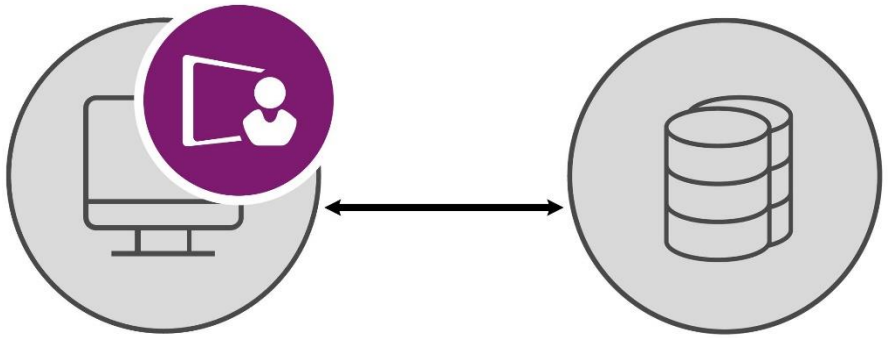
ViPNet Administrator

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.

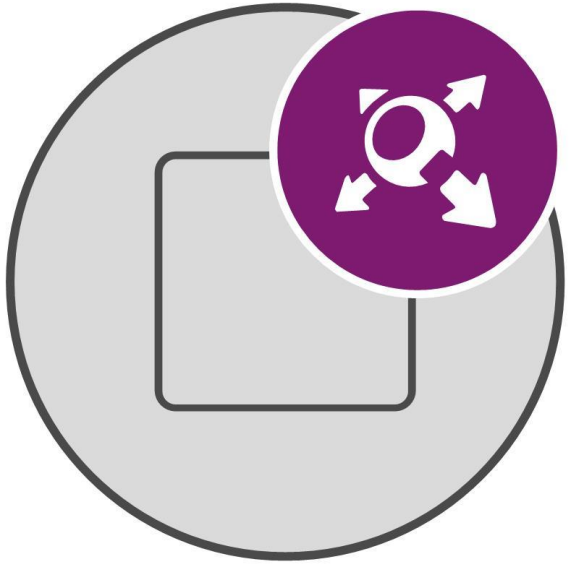
ViPNet Coordinator

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.
- …

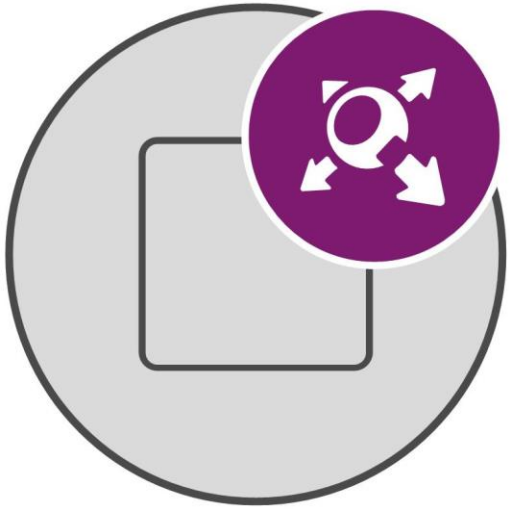


Функции ViPNet Coordinator

- 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.

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 Client

предназначен:

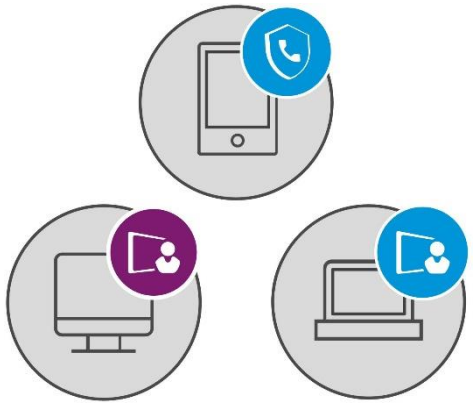
- для защиты рабочих компьютеров пользователей сети ViPNet.

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 (32/64-разрядная)	Windows Server 2012 (64-разрядная)
Windows Server 2008 R2 (64-разрядная)	Windows Server 2008 R2 (64-разрядная)	
Windows 7 (32/64-разрядная)	Windows 7 (32/64-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

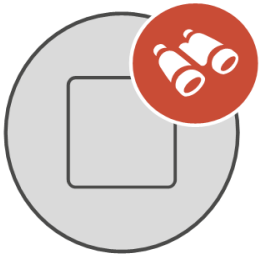
Дополнительные модули ViPNet Network Security 4.x

ViPNet xFirewall

- шлюз безопасности, межсетевой экран, предназначенный для фильтрации трафика на всех уровнях и создания гранулированной политики безопасности на основе учетных записей пользователей и списка приложений

ViPNet CSP

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



ViPNet IDS

- программно-аппаратный комплекс для обнаружения вторжений в информационные системы, функционирующий на основе динамического анализа сетевого и прикладного трафика стека протоколов TCP/IP

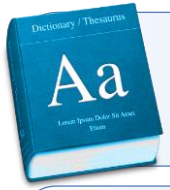
ViPNet Network Security 4.x

Новые возможности ViPNet Network Security 4.x

клиент-серверная архитектура ViPNet ЦУС

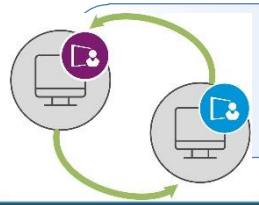
возможность многопользовательского режима работы с ViPNet ЦУС

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



изменение в терминологии ViPNet

назначение права подписи и выбор узлов для рассылки СОС 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

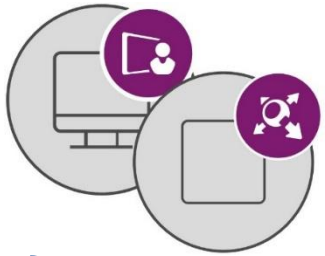
Объекты защищенной сети ViPNet

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:

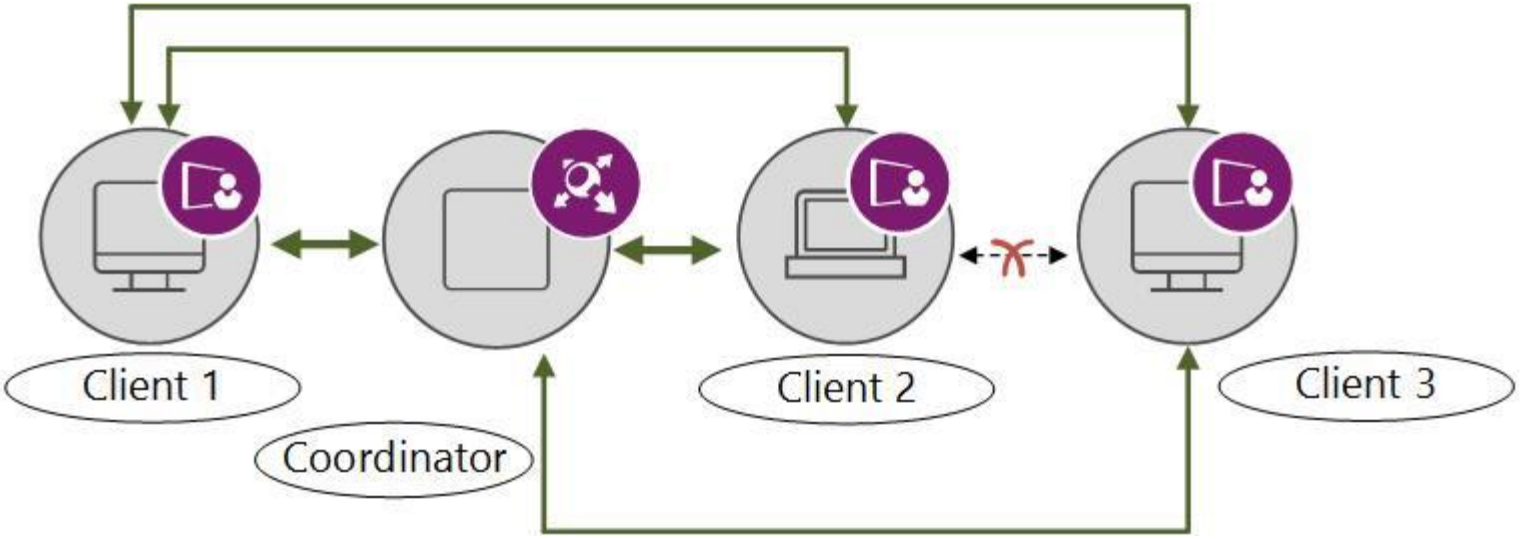
компьютер, на который установлено ПО ViPNet Coordinator или специальный программно-аппаратный комплекс

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 администратором

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:

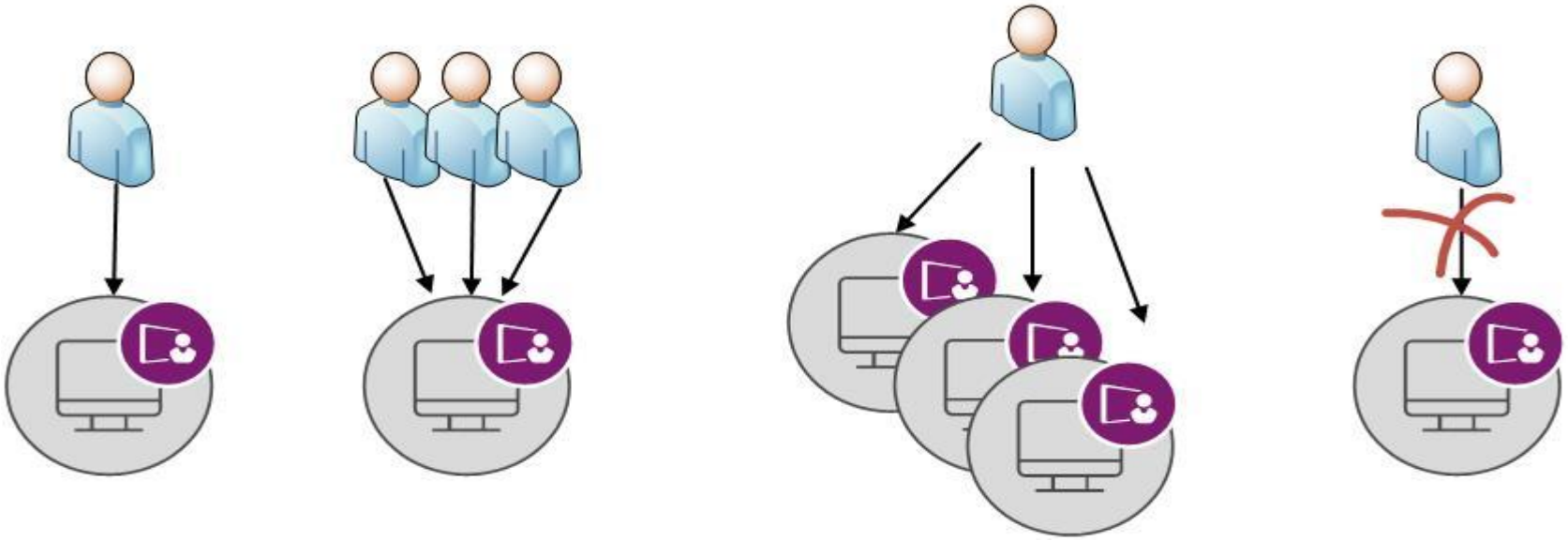
- владелец ключевой информации для доступа в защищенную сеть;
- параметры пользователя настраиваются администратором ViPNet в клиентском приложении ЦУС.

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



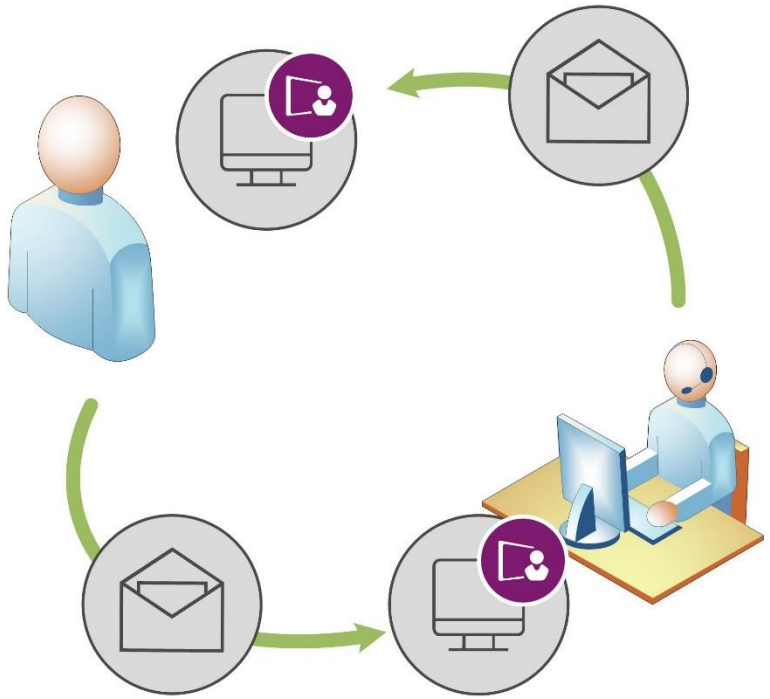
Внимание! Если пользователь зарегистрирован на нескольких сетевых узлах, его ключевая информация может быть отправлена только на первый узел, на который он был добавлен

Пользователь ViPNet

Связи между пользователями ViPNet

Связи между пользователями:

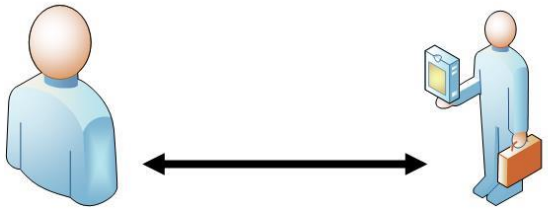
- позволяют пользователям обмениваться друг с другом персональными зашифрованными сообщениями в программе ViPNet Деловая почта. Сообщение сможет прочесть только тот пользователь, которому оно адресовано.



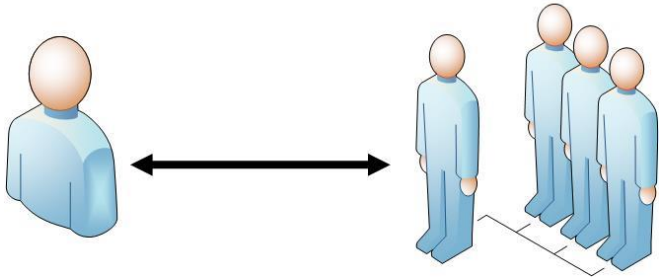
Пользователь ViPNet

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.

Роли сетевых узлов

Примеры ролей сетевых узлов

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 на клиент или координатор (для назначения уровня полномочий пользователя)

0018 "VPN-сервер"

- позволяет использовать на сетевом узле программное обеспечение ViPNet Coordinator (Win или Lin). Может быть добавлена только на координатор

0000 “Business Mail"

- позволяет использовать на клиенте программу ViPNet Деловая почта

Роли сетевых узлов

Примеры ролей сетевых узлов

001E "SafeDisk"

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

0020 "CryptoService"

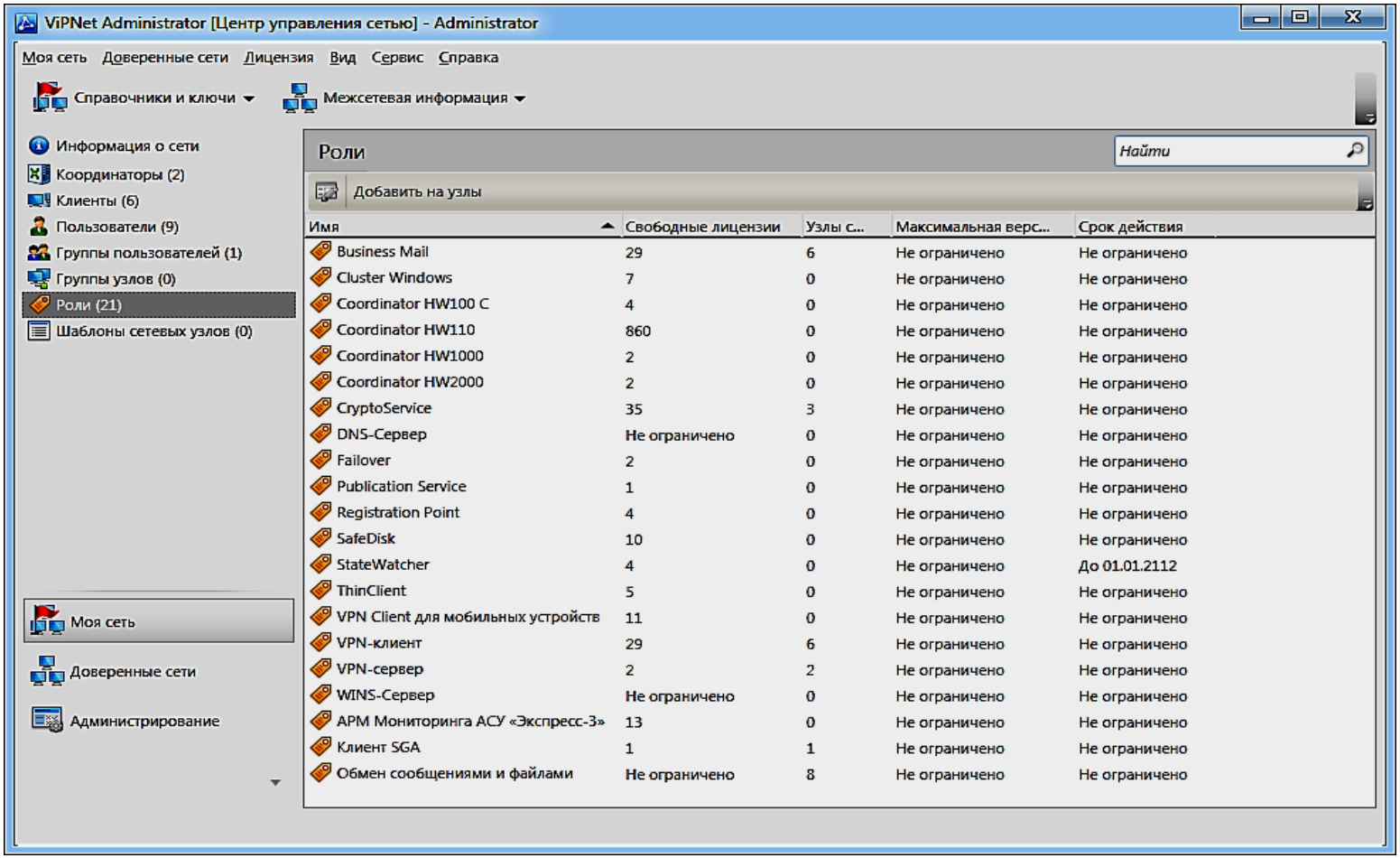
- позволяет использовать на сетевом узле программу ViPNet CryptoService. Может быть добавлена на клиент или координатор

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.

Роли сетевых узлов

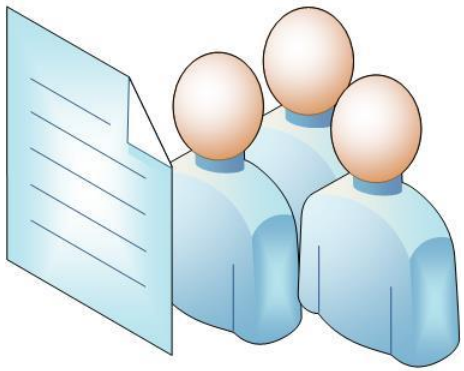
Примеры ролей сетевых узлов



Полномочия пользователей

Полномочия пользователя ViPNet :

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



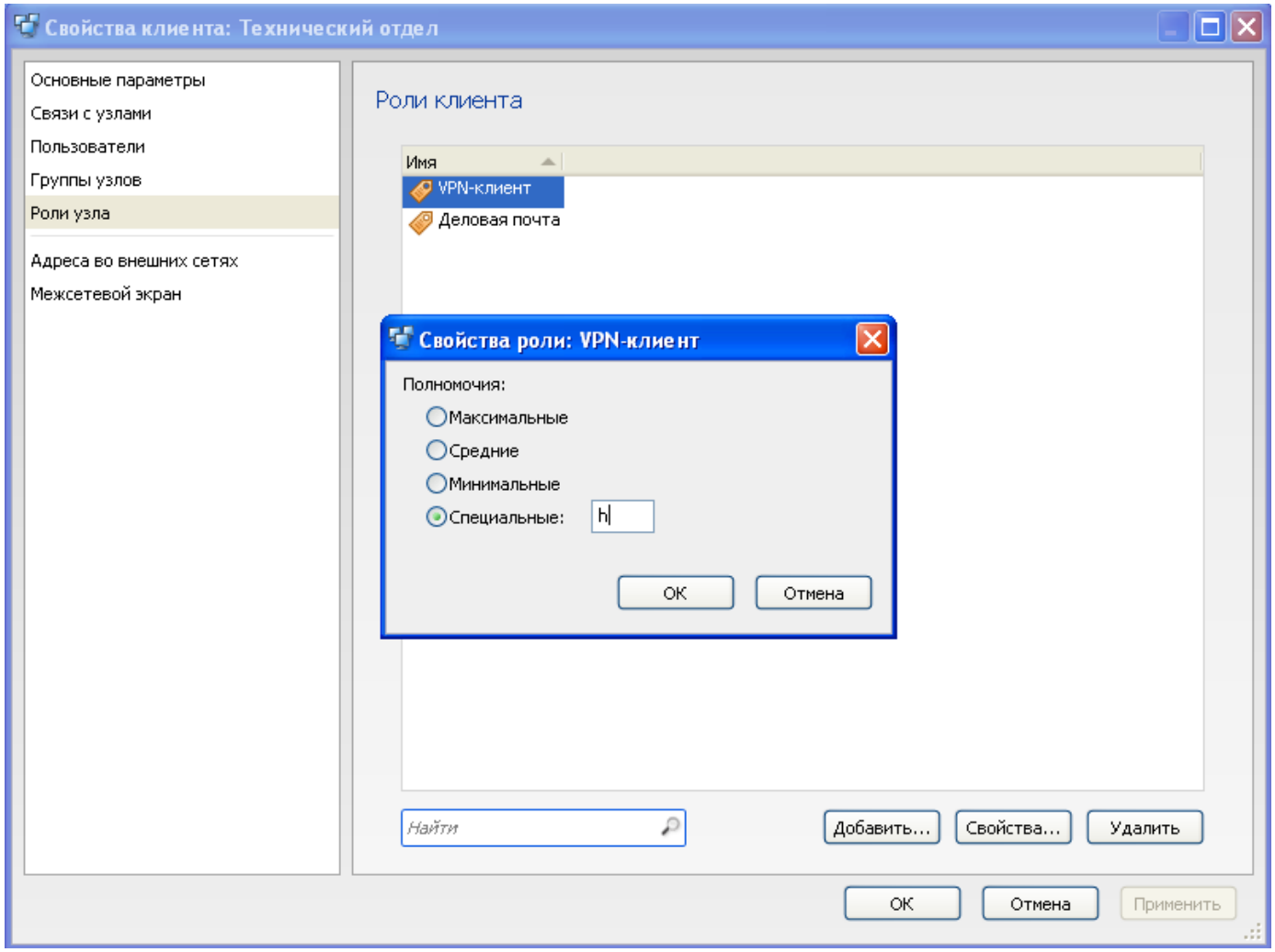
Полномочия пользователей

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

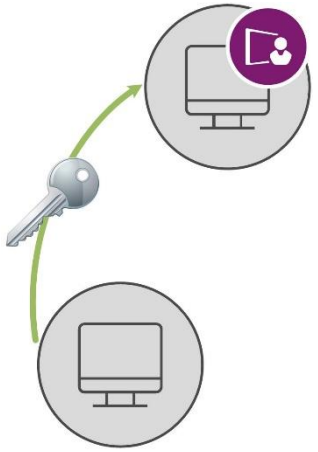


Лицензирование сети ViPNet

Файл лицензии

Файл лицензии:

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



Лицензирование сети ViPNet

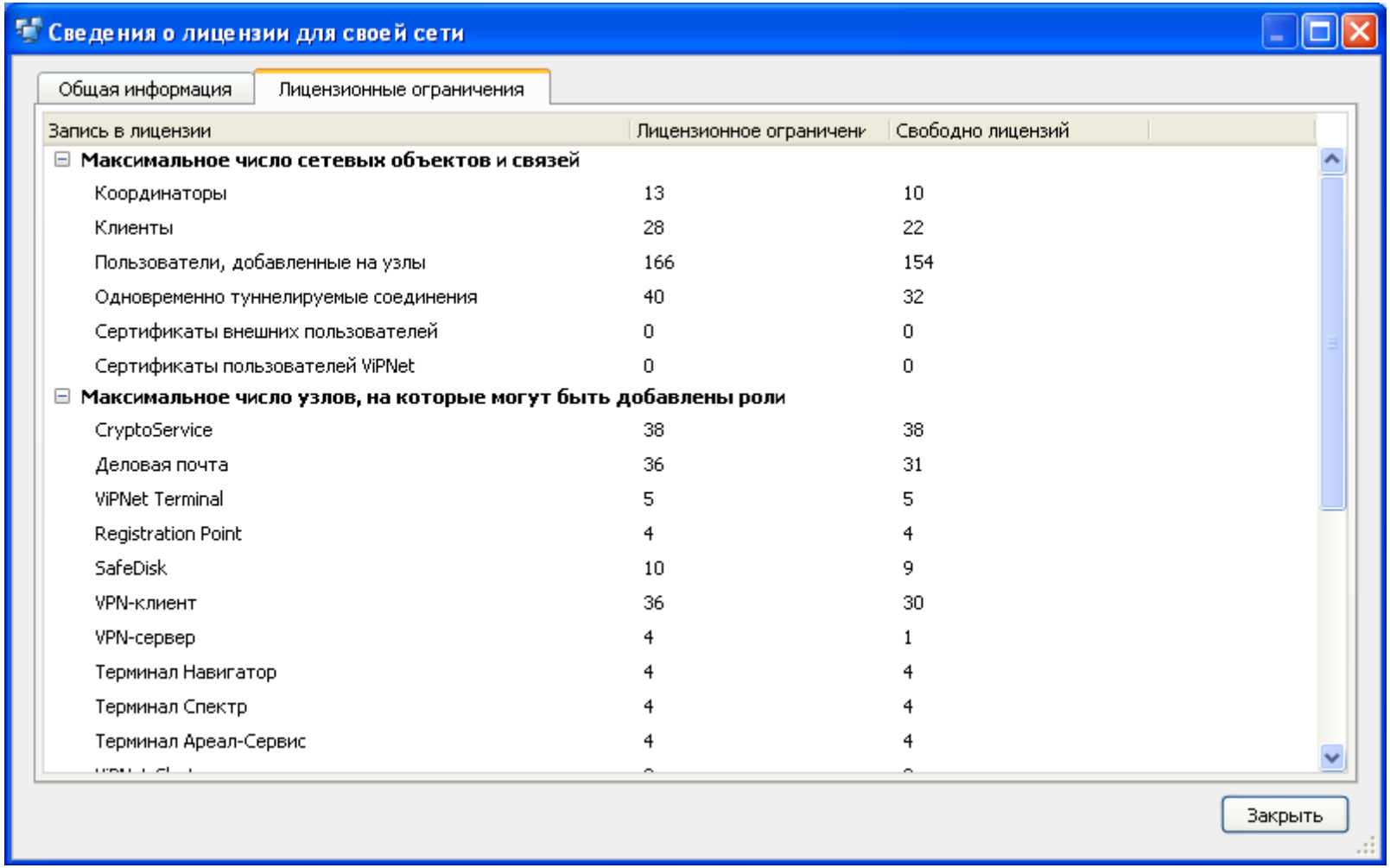
Состав файла лицензии

Файл лицензии содержит:

- номер сети ViPNet;
- информацию о владельце сети ViPNet;
- информацию о подчиненных сетях;
- ограничение на версию ПО ViPNet Administrator;
- максимальное число сетевых объектов и связей;
- список ролей;
- максимальное число узлов, на которые могут быть добавлены роли;
- параметры добавления ролей;
- срок действия лицензии.

Лицензирование сети ViPNet

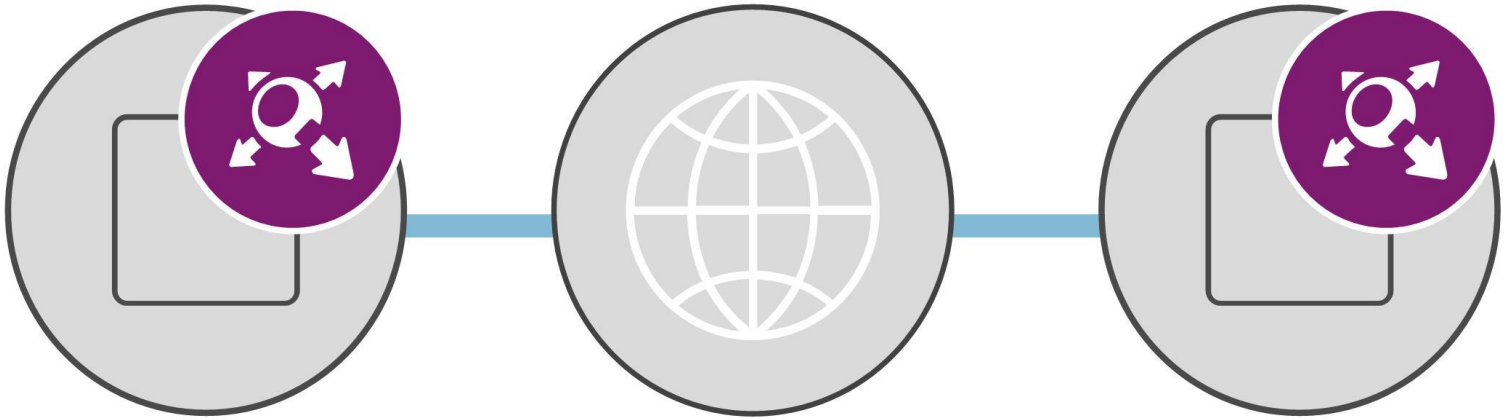
Просмотр файла лицензии



Межсерверные каналы

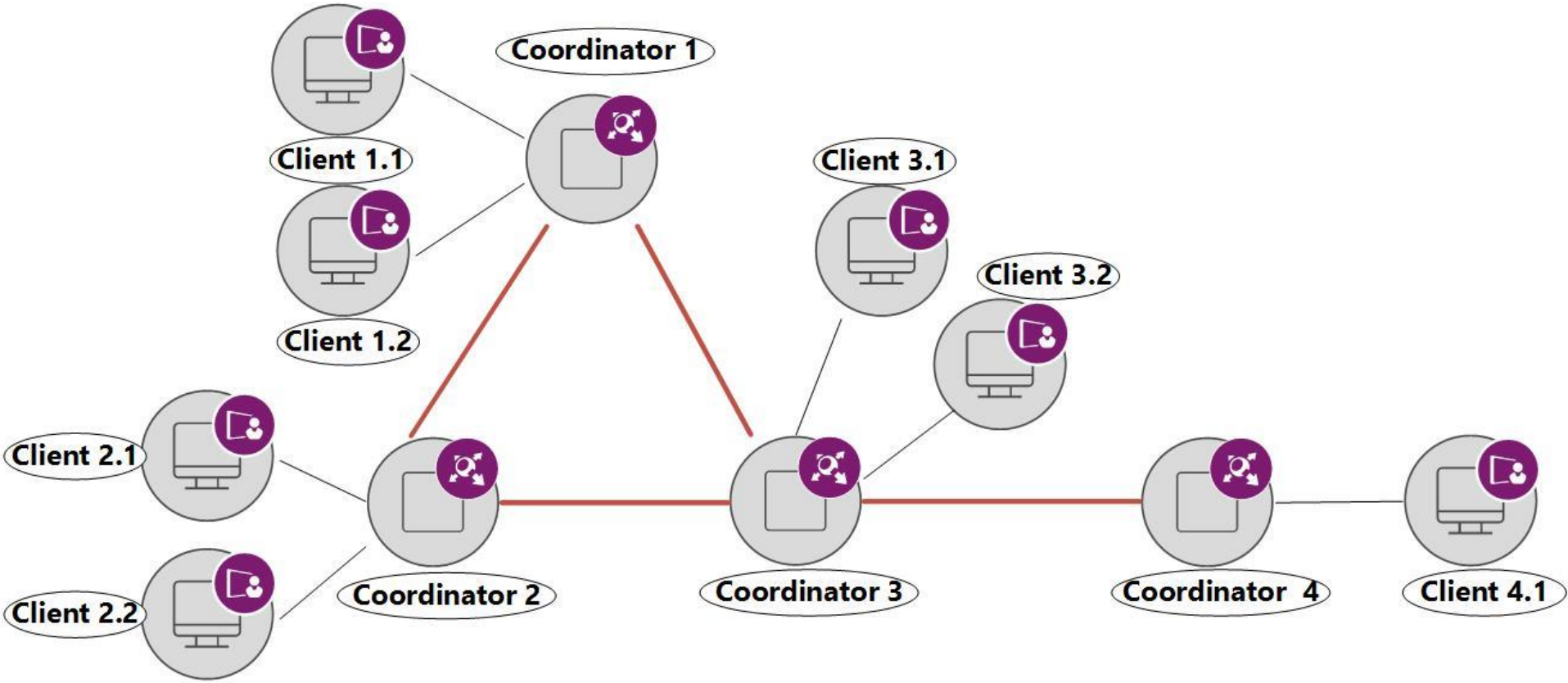
Межсерверные каналы

- 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.



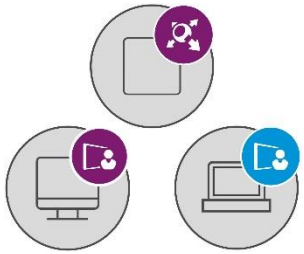
Межсерверные **каналы**

Межсерверные каналы



Идентификаторы объектов

Идентификаторы объектов сети ViPNet



Сеть ViPNet
1A0F

уникальный 4-символьный шестнадцатеричный идентификатор (номер сети ViPNet)

Сетевой Узел
1A0F0012

уникальный 8-символьный шестнадцатеричный идентификатор: 1A0F – номер сети, 0012 – номер СУ

Пользователь
1A0F00D

уникальный 8-символьный шестнадцатеричный идентификатор: 1A0E – номер сети, 000D – номер пользователя

Роль
001D

уникальный 4-символьный шестнадцатеричный идентификатор

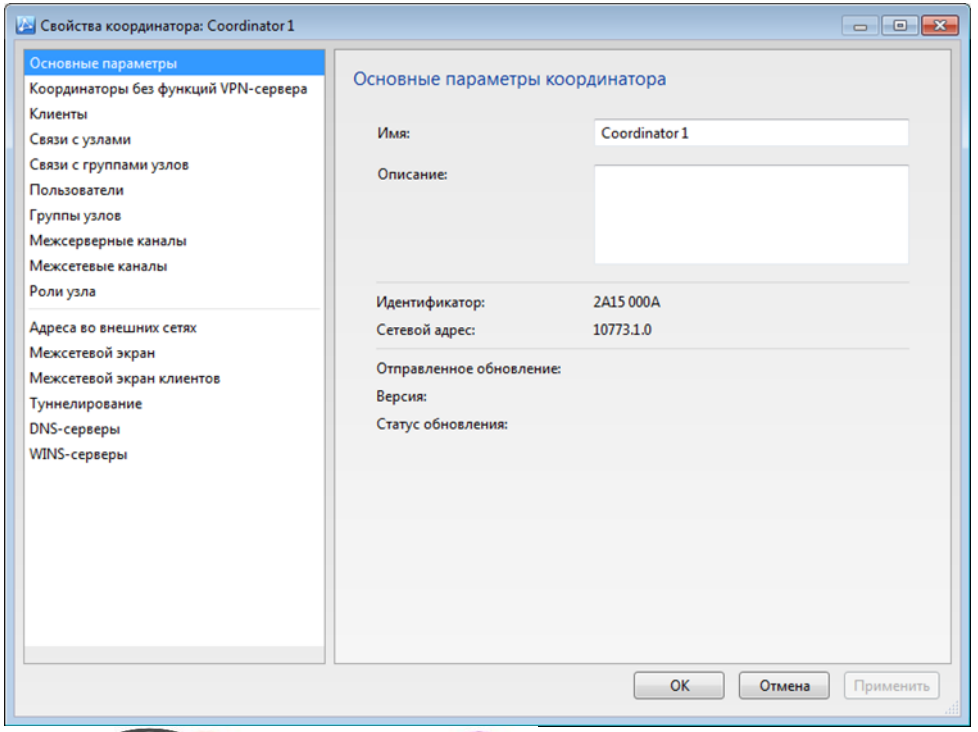
Сетевой адрес

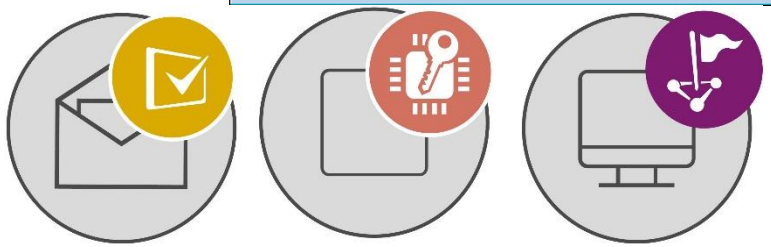
Сетевой адрес

Сетевой адрес состоит:

- ✓ **для координатора**: из номера сети ViPNet, номера координатора
- ✓ **для клиента**: из номера сети, номера координаторд и номера клиента на координаторе;

На основе сетевого адреса осуществляется маршрутизация пакетов в сети ViPNet.





Сетевой адрес

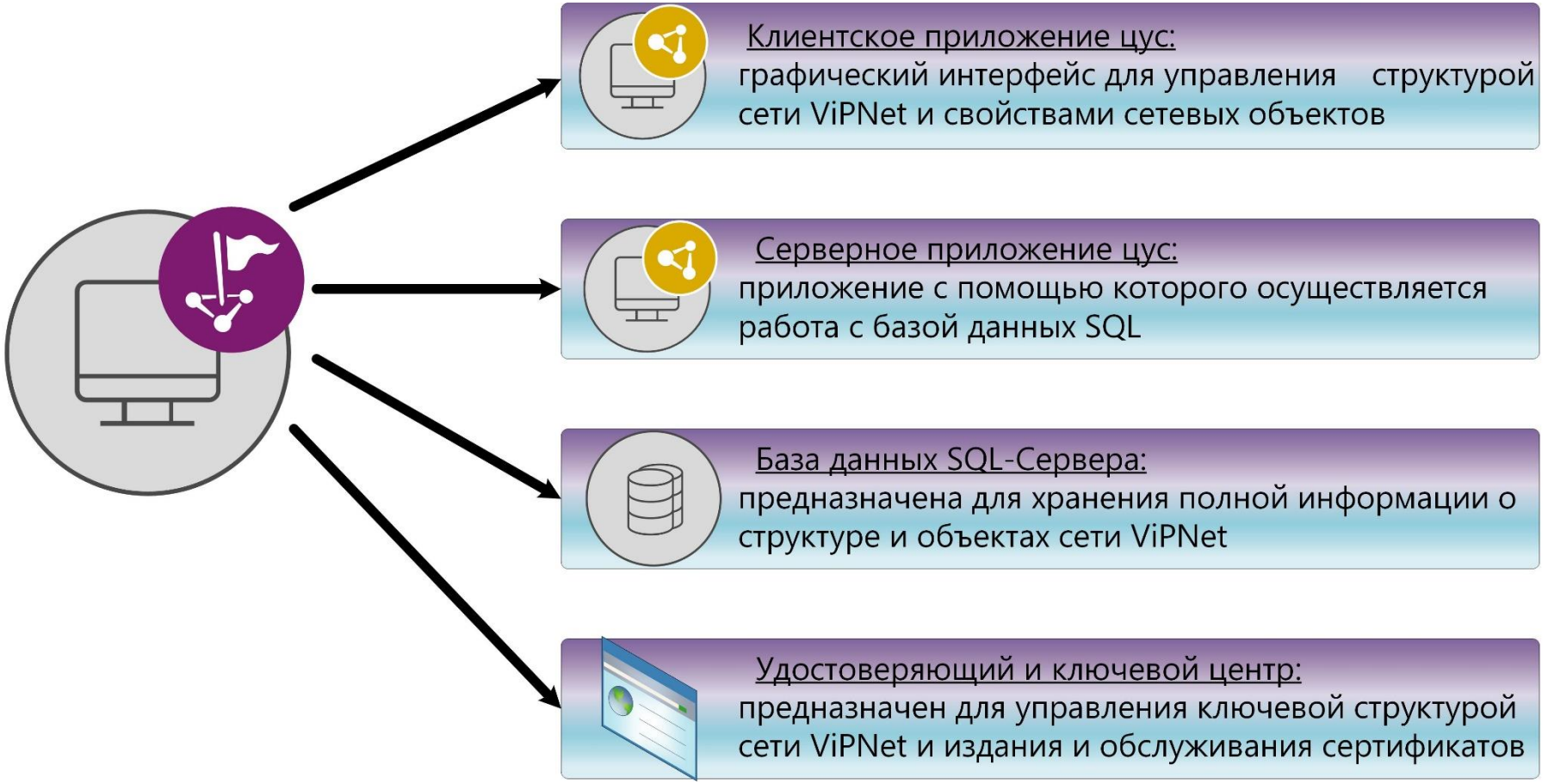
Сетевой адрес

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.

ViPNet Administrator 4.x

ViPNet Administrator 4.x

Состав ViPNet Administrator



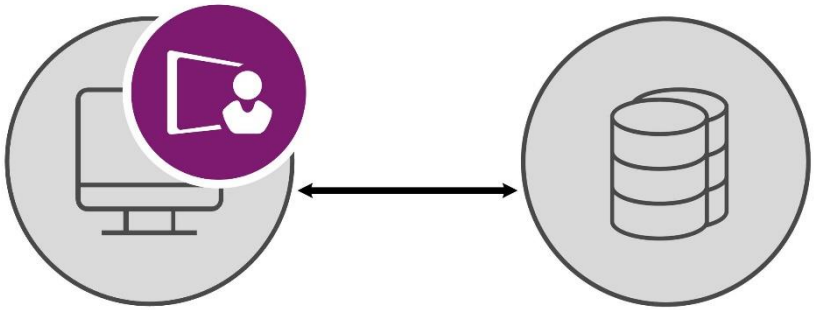
База данных SQL-сервера

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

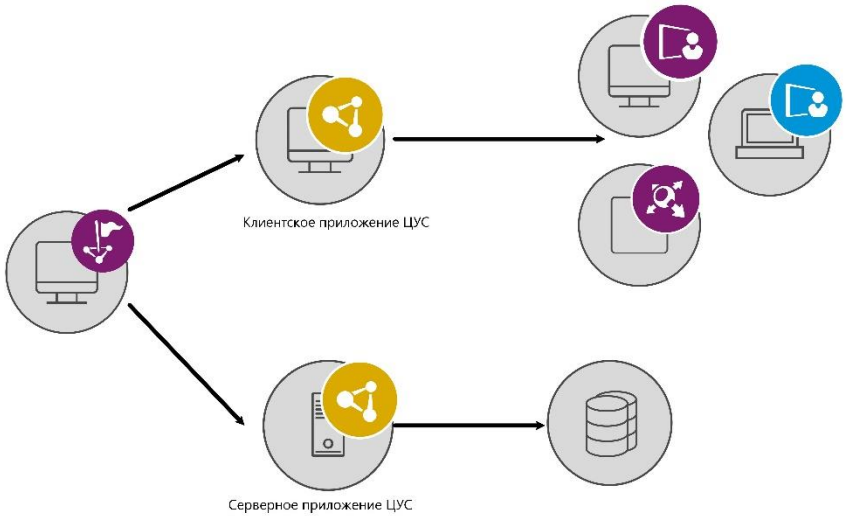
Внимание! По умолчанию устанавливается Microsoft SQL Server 2014 Express и создается именованный экземпляр SQL-сервера WINNCCSQL

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 Центр управления сетью



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

ViPNet ЦУС состоит из двух компонент:

- серверное приложение ЦУС;
- клиентское приложение ЦУС.

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.

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

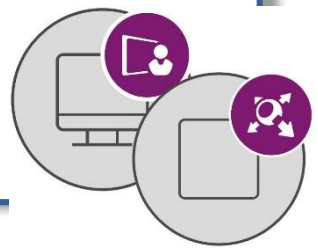
Функции ViPNet ЦУС

управление структурой сети ViPNet

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

настройка свойств объектов сети ViPNet

- *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

Функции ViPNet ЦУС

организация межсетевого взаимодействия

- 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 ViPNet

- удаленное обновление на сетевых узлах ключей;
- удаленное обновление на сетевых узлах справочников;
- удаленное обновление на сетевых узлах программного обеспечения ViPNet;

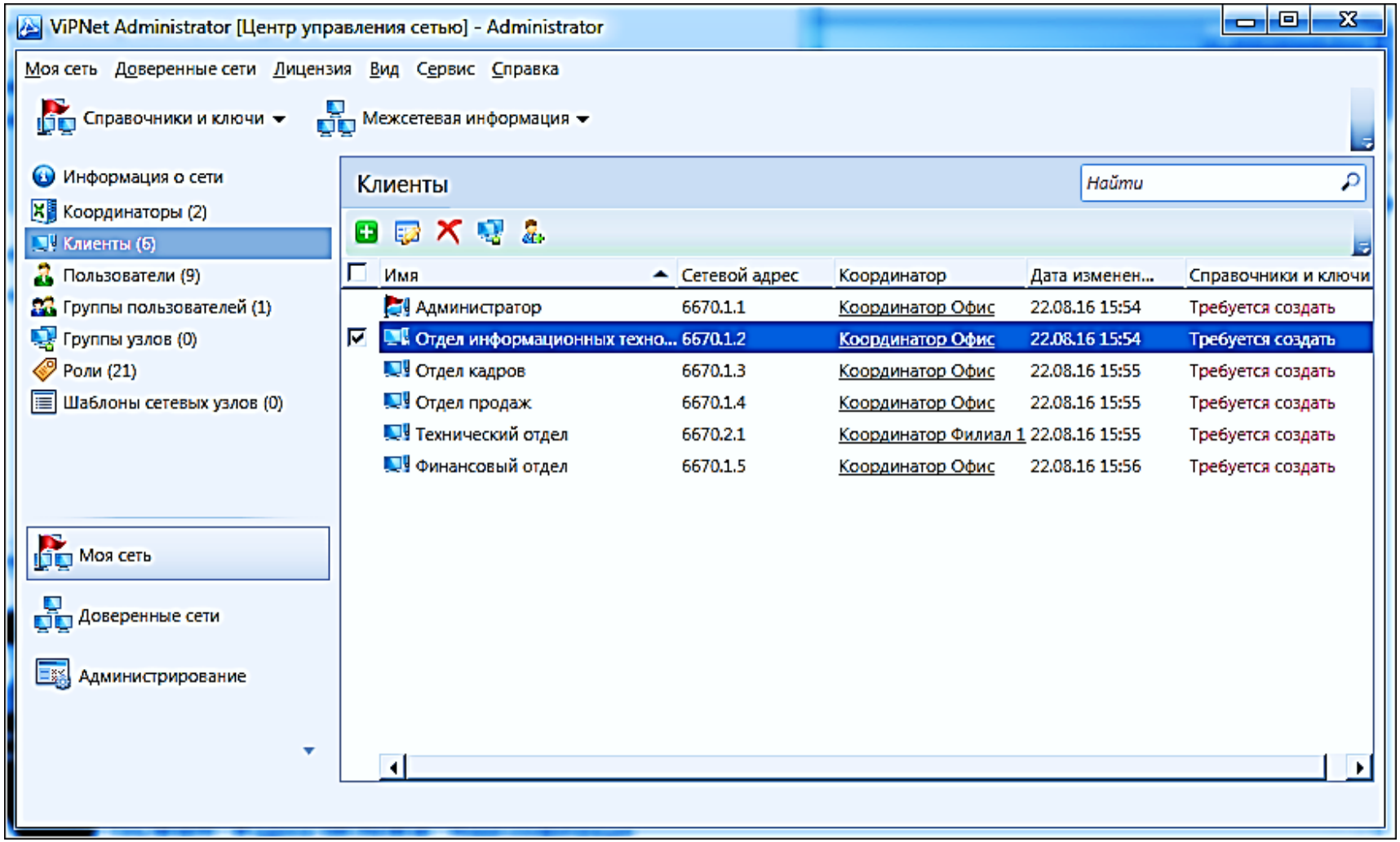
Функции ViPNet ЦУС

административные функции

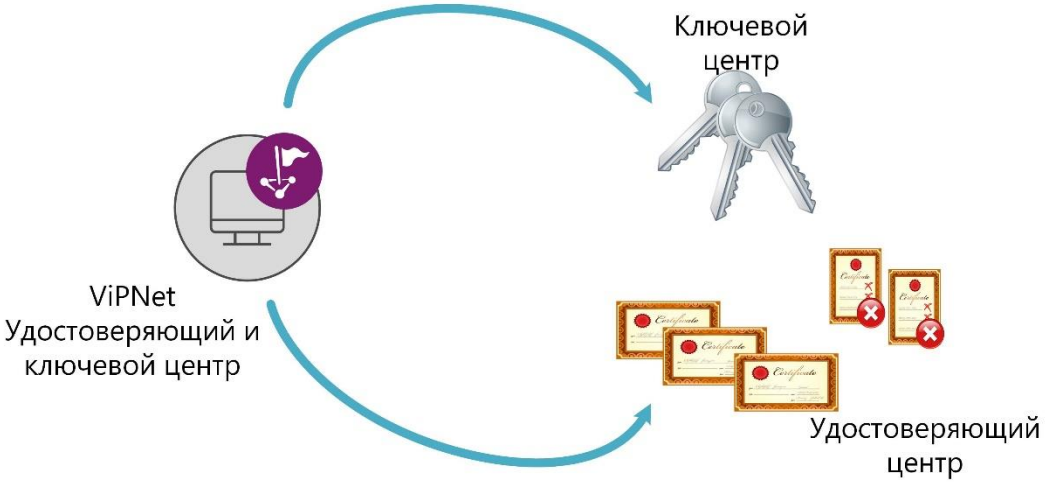
- создание и удаление учетных записей администраторов ViPNet ЦУС;
- просмотр журналов аудита системных событий ViPNet ЦУС;
- просмотр журналов обмена транспортными конвертами между ЦУС и узлами ViPNet;
- резервное копирование и восстановление данных ;
- обновление лицензии на сеть ViPNet.

ViPNet Administrator 4.x

Интерфейс клиентского приложения ЦУС



ViPNet Удостоверяющий и ключевой центр



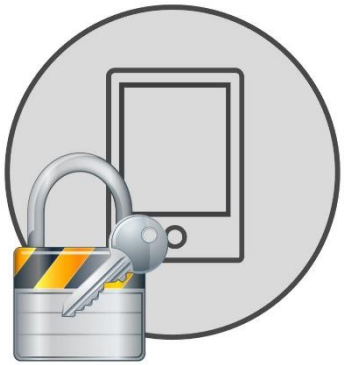
ViPNet Удостоверяющий и ключевой центр предназначен для формирования ключей шифрования и электронной подписи и управления инфраструктурой PKI

ViPNet УКЦ состоит из двух компонент:

- ✓ ключевой центр;
- ✓ удостоверяющий центр.

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.

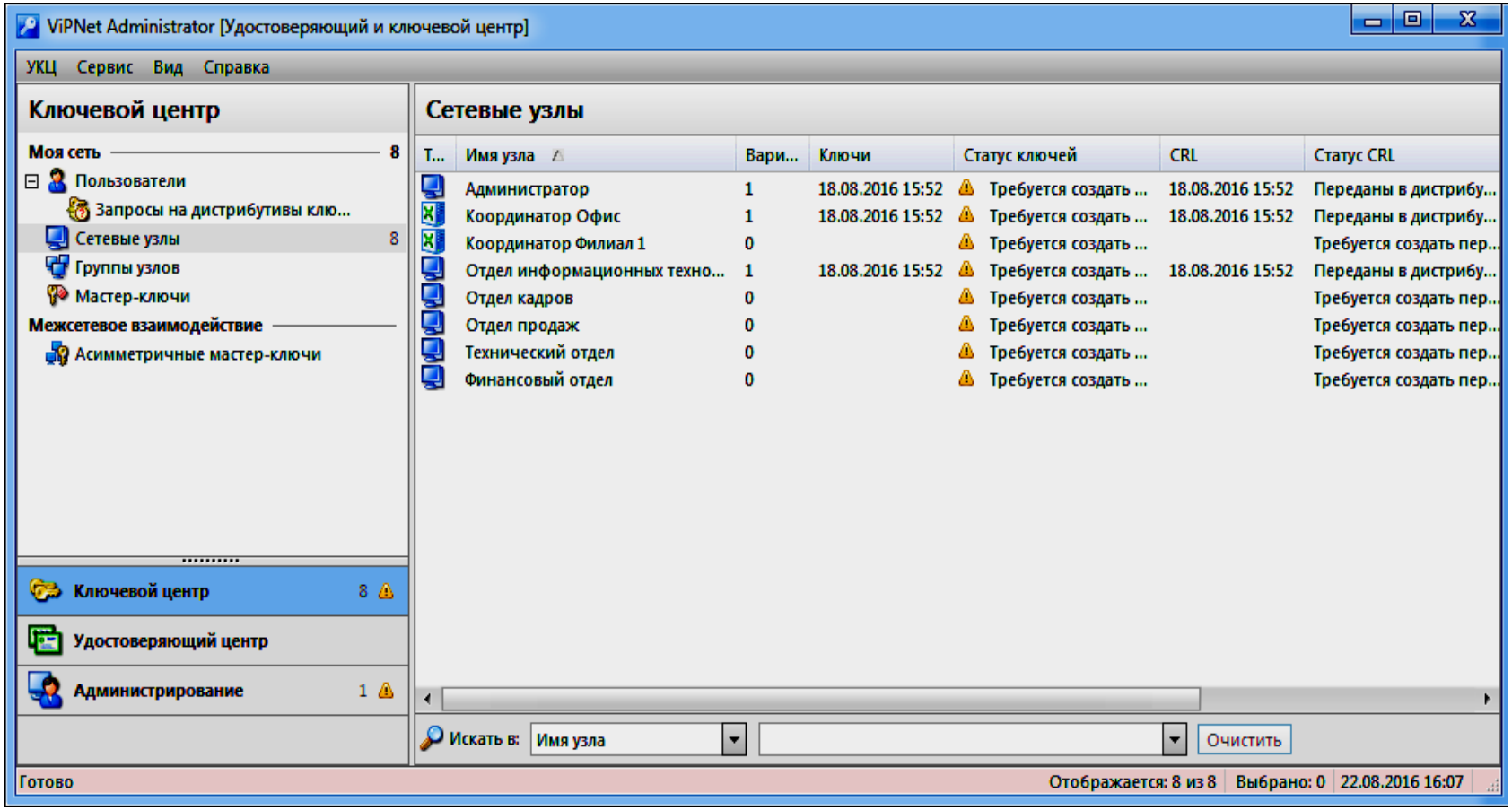


Задачи удостоверяющего центра

- 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 СОС 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



Схемы размещения компонентов ViPNet Administrator

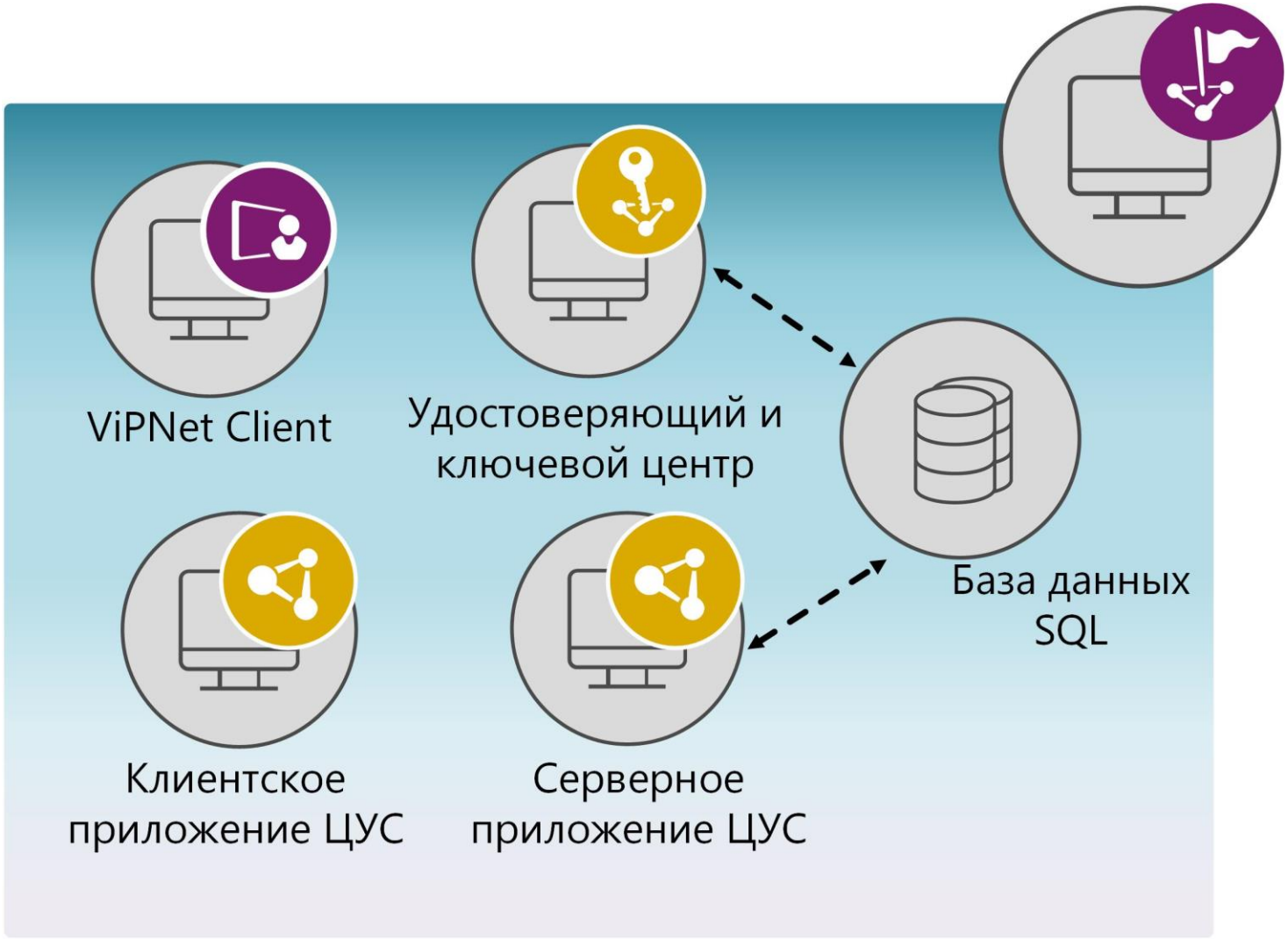
Существует две основных схемы размещения компонентов ViPNet Administrator:

1. Установка всех компонентов ViPNet Administrator на одном компьютере.

2. Установка компонентов ViPNet Administrator на разных компьютерах.

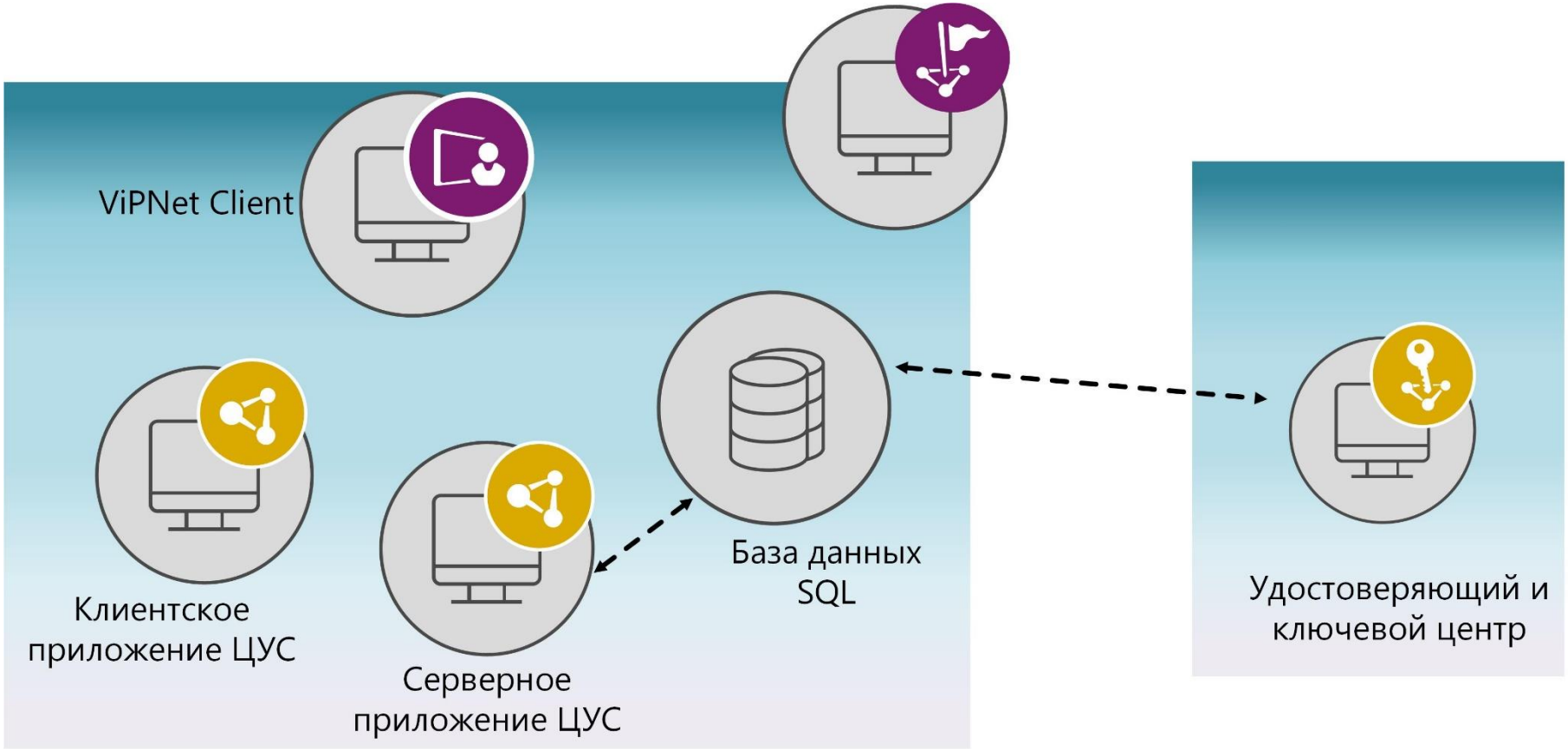
ViPNet Administrator 4.x

Схемы размещения компонентов ViPNet Administrator



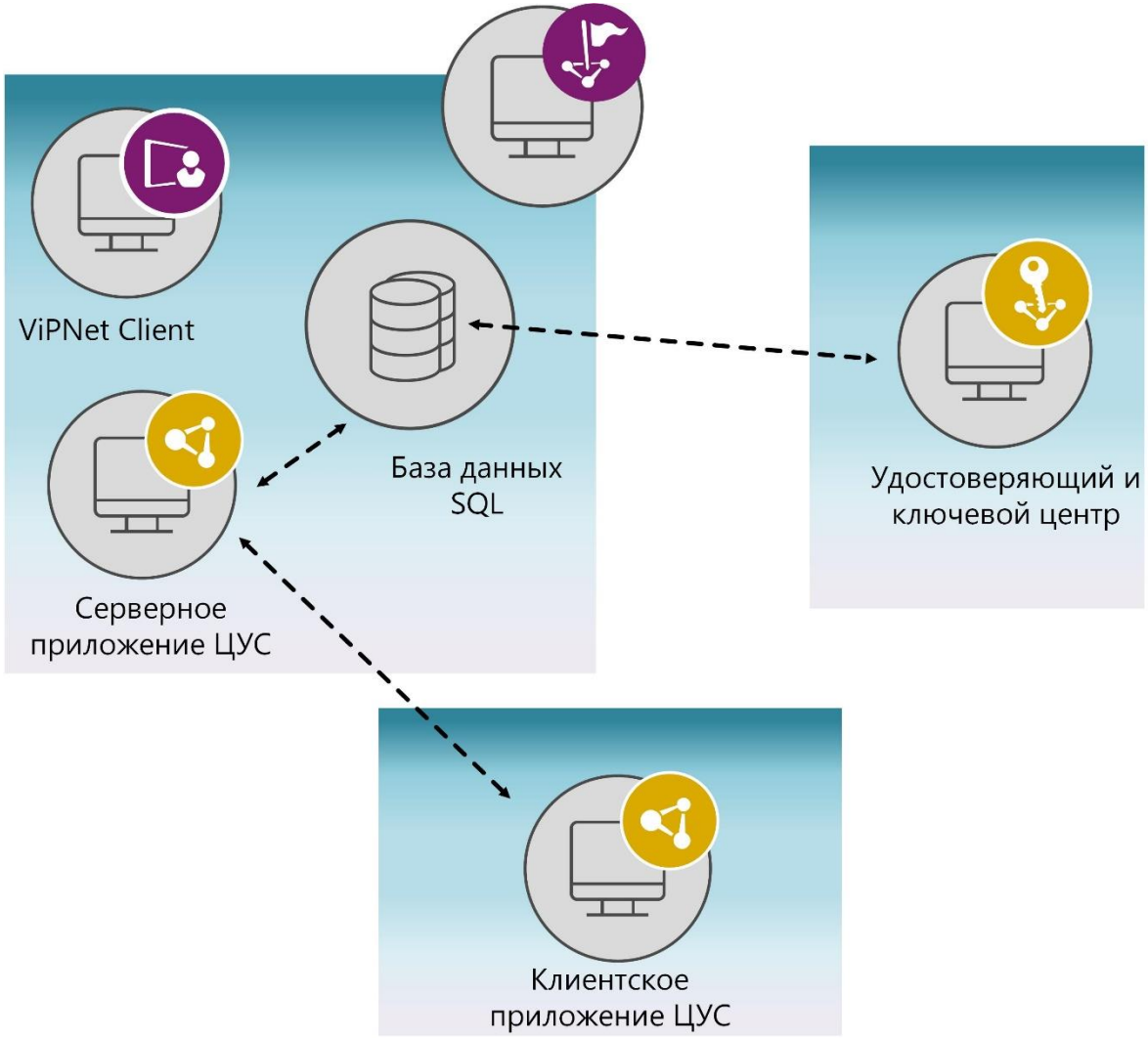
ViPNet Administrator 4.x

Схемы размещения компонентов ViPNet Administrator



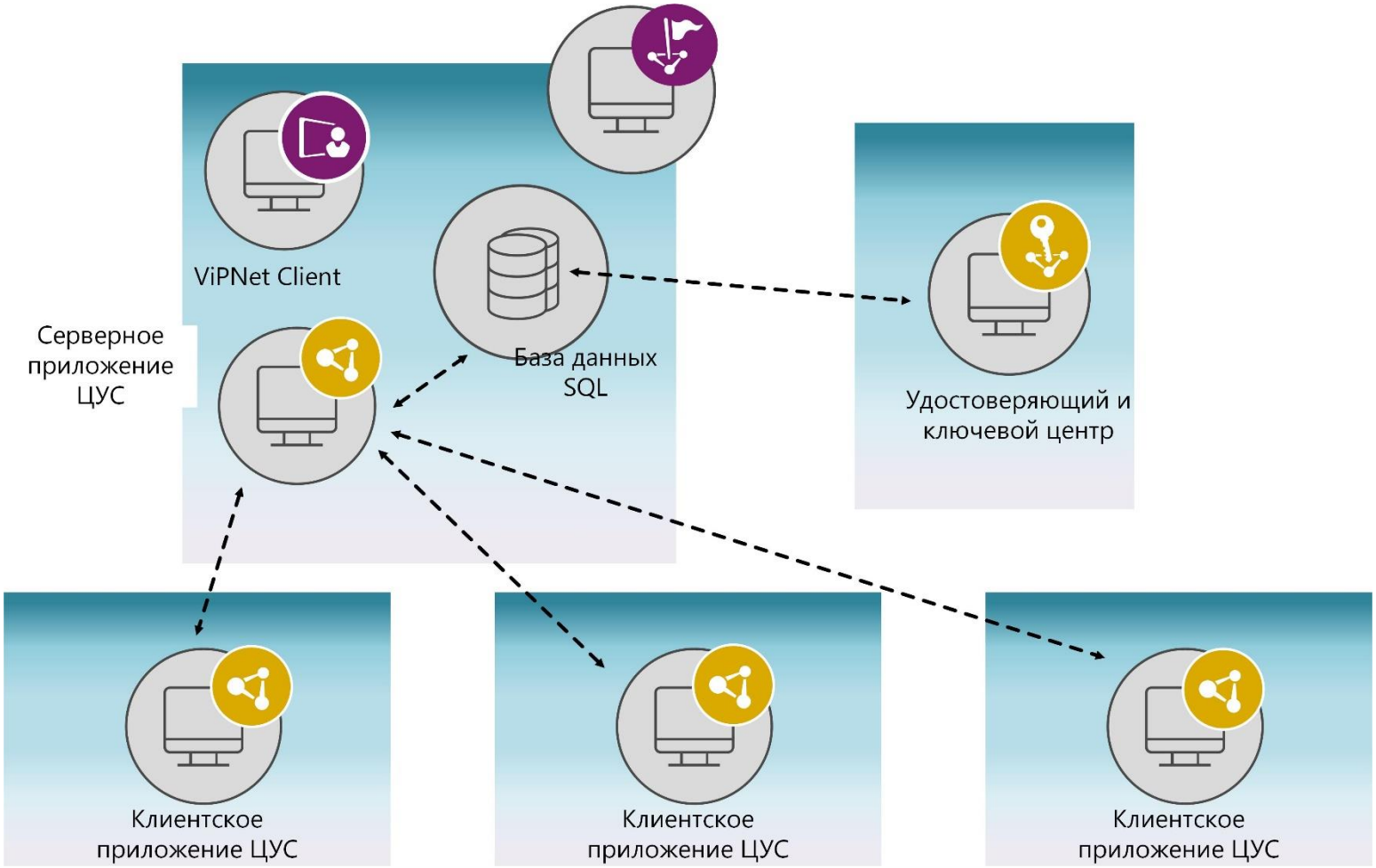
ViPNet Administrator 4.x

Схемы размещения компонентов ViPNet Administrator



ViPNet Administrator 4.x

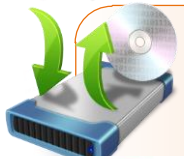
Схемы размещения компонентов ViPNet Administrator



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 сети

ViPNet Policy Manager

ViPNet Policy Manager

Определение ViPNet Policy Manager

ViPNet Policy Manager:

- предназначен для централизованного управления политиками безопасности узлов защищенной сети ViPNet;
- позволяет задавать различные политики безопасности для отдельных сетевых узлов и групп узлов и централизованно рассылать их на сетевые узлы.

Внимание! ViPNet Policy Manager 4.2 можно устанавливать только на сетевом узле, который является Центром управления сетью.

ViPNet Policy Manager

Функции ViPNet Policy Manager

объединение сетевых узлов в группы ("подразделения")

- сетевые узлы, к которым должна применяться одинаковая политика безопасности можно объединять в группы;
- политики безопасности назначаются не отдельным узлам, а всему подразделению, что упрощает управление политиками безопасности;

назначение шаблонов политики безопасности

- шаблон политики безопасности можно назначить отдельным узлам или подразделениям;
- шаблон, назначенный подразделению, распространяется на все узлы, входящие в состав этого подразделения;
- от порядка следования шаблонов зависит приоритет применения на узле параметров безопасности, заданных в шаблонах;

ViPNet Policy Manager

Функции ViPNet Policy Manager

управление шаблонами политики безопасности

- шаблон политики безопасности можно создать, настроить (изменить) или удалить;

рассылка результирующей политики на сетевые узлы

- формируется автоматически при отправке политики безопасности на узел;
- позволяет учесть приоритет шаблонов и исключить повторы одного и того же шаблона;
- политики безопасности можно рассылать на отдельные узлы или на группы узлов;

контроль за отправкой и применением политик безопасности

- все события, связанные с применением политик безопасности, записываются в журнал;

Функции ViPNet Policy Manager

управление учетными записями пользователей

- учетная запись содержит имя, пароль, персональные данные и роли пользователя;
- учетную запись можно создать, изменить или удалить;

управление ролями пользователей

- роли используются для разграничения полномочий пользователей;
- в ViPNet Policy Manager можно использовать предустановленные роли или создавать свои;

аудит действий пользователей

- действия пользователей в ViPNet Policy Manager регистрируются в журнале событий.

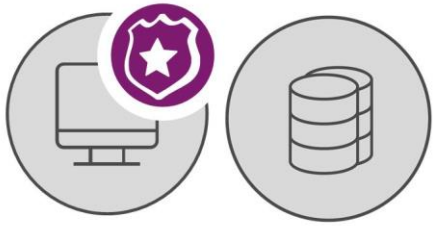
База данных ViPNet Policy Manager

База данных ViPNet Policy Manager:

- предназначена для хранения информации об управляемых сетевых узлах, учетных записях пользователей, политик безопасности, другой необходимой информации;
- создается автоматически при установке ViPNet Policy Manager.

Для размещения базы данных можно использовать:

- существующий развернутый SQL-сервер, который установлен на компьютер с ViPNet Policy Manager или удаленный компьютер.



ViPNet Administrator 4.x

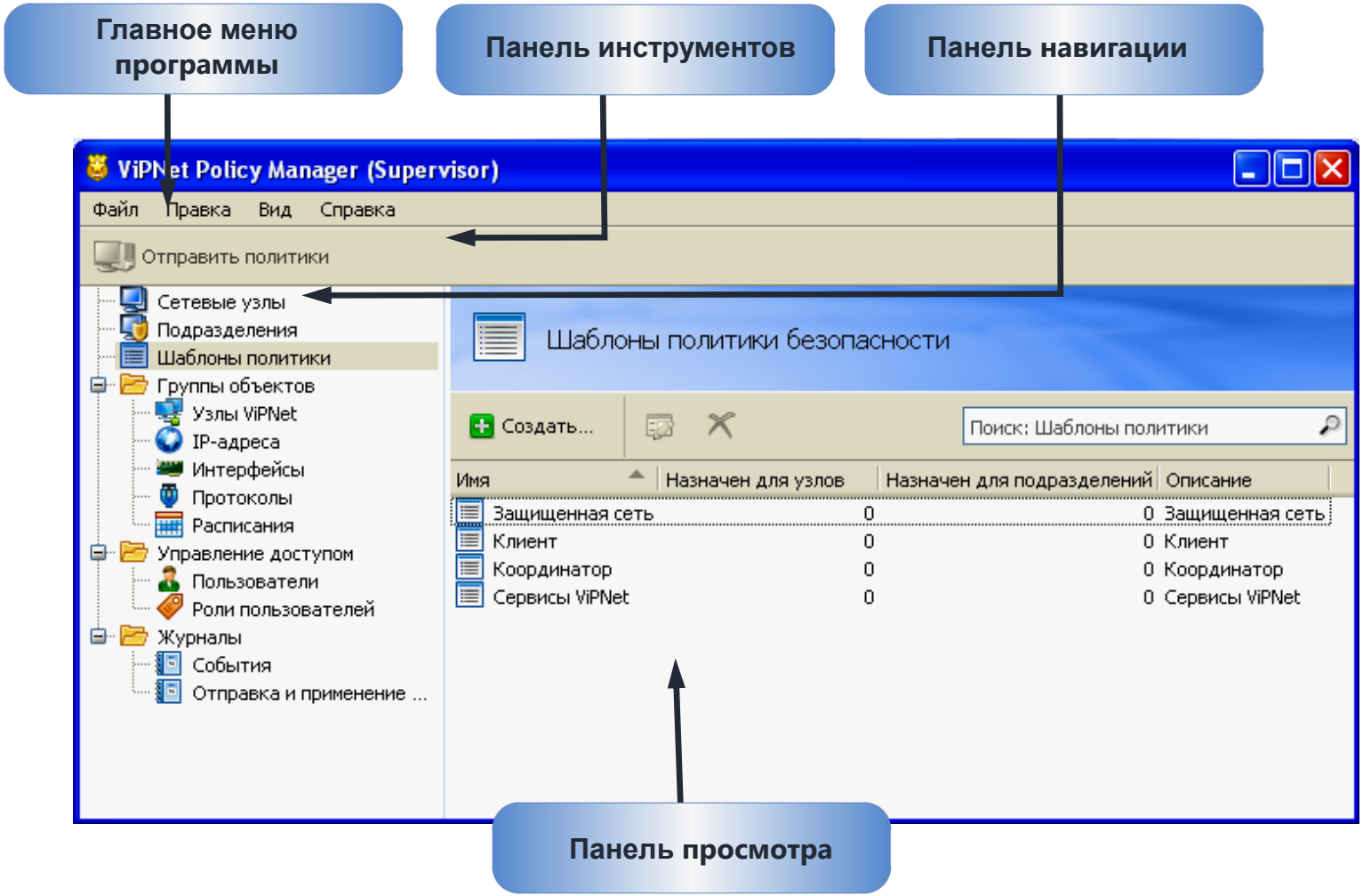
Поддерживаемые версии СУБД

- ✓ Microsoft SQL Server 2005
- ✓ Microsoft SQL Server 2008
- ✓ Microsoft SQL Server 2008 R2
- ✓ Microsoft SQL Server 2014 Express

Внимание! При установке ViPNet Policy Manager по умолчанию используется экземпляр SQL-сервера: **.\SQLEXPRESS** и создается база данных с именем **ViPNetPolicyManager**

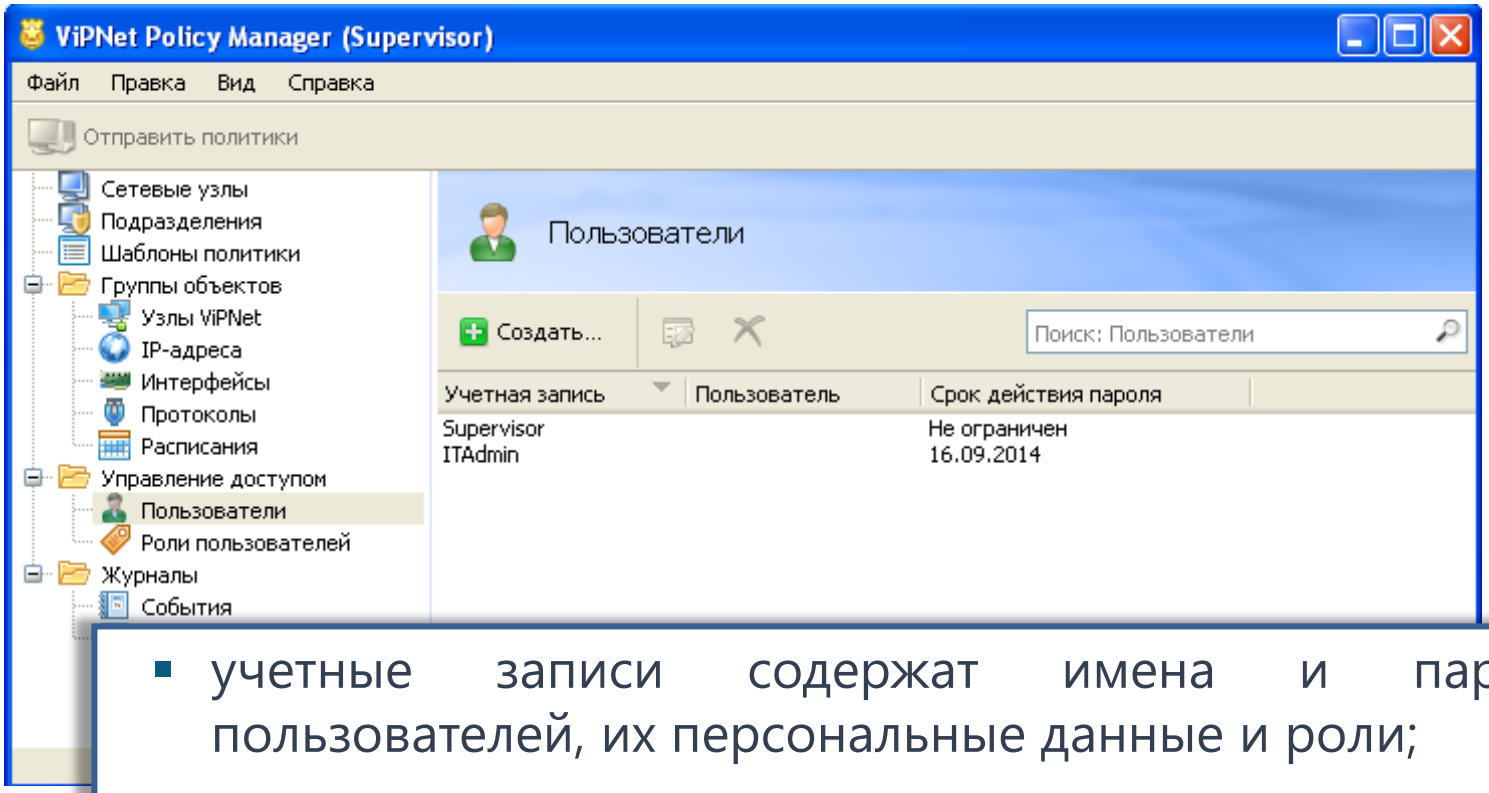
ViPNet Policy Manager

Интерфейс ViPNet Policy Manager



ViPNet Policy Manager

Разграничение доступа в ViPNet Policy Manager

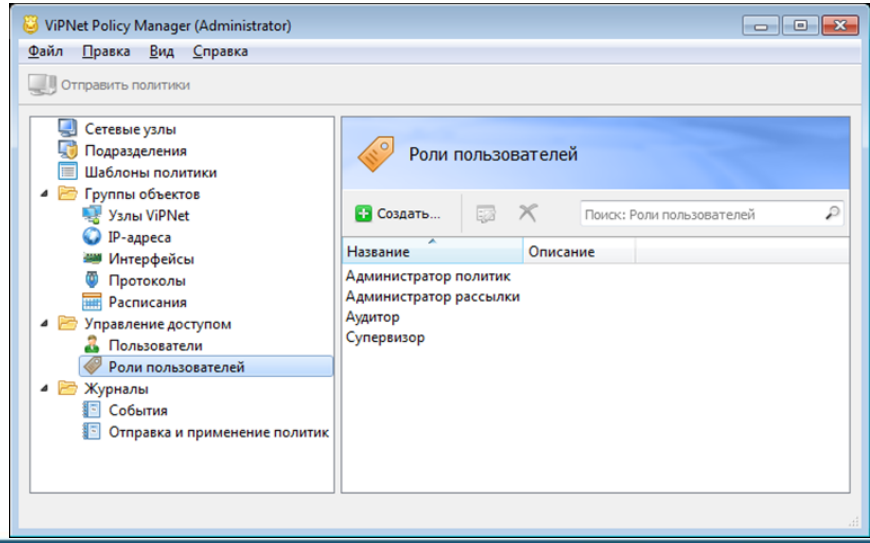


- учетные записи содержат имена и пароли пользователей, их персональные данные и роли;
- при установке создается учетная запись с именем **Supervisor** и паролем **Supervisor**. Встроенную учетную запись нельзя удалить.

Роли пользователей в ViPNet Policy Manager

Роли пользователей:

- используются для разграничения полномочий пользователей при работе с программой ViPNet Policy Manager;
- определяют действия, которые разрешено выполнять пользователю в программе;
- состоят из одного или нескольких допустимых полномочий (набором разрешенных действий);
- каждому пользователю может быть назначена одна или несколько ролей.



Роли пользователей в ViPNet Policy Manager

предустановленные роли пользователей

- супервизор — имеет все полномочия;
- аудитор — имеет полномочие Аудит;
- администратор рассылки — имеет полномочия Назначение шаблонов и Отправка политик;
- администратор политик — имеет полномочия Управление подразделениями, Управление шаблонами и Назначение шаблонов.

роли, созданные администратором ViPNet Policy Manager

ViPNet Policy Manager

Полномочия пользователей в ViPNet Policy Manager

- ✓ управление пользователями — создание, настройка и удаление учетных записей;

- ✓ управление ролями — создание, настройка и удаление ролей пользователей;

- ✓ управление подразделениями — создание, настройка и удаление подразделений;

- ✓ управление шаблонами — создание, настройка и удаление шаблонов политики безопасности и групп объектов;

ViPNet Policy Manager

Полномочия пользователей в ViPNet Policy Manager

- назначение шаблонов — назначение шаблонов политики безопасности сетевым узлам и подразделениям;

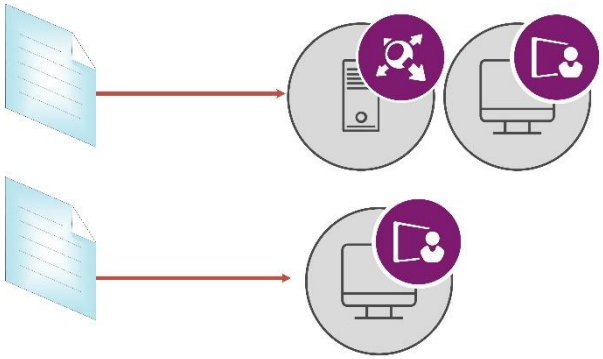
- *отправка политик — рассылка результирующих политик безопасности;*

- *аудит — просмотр подразделений, шаблонов, групп объектов, результирующих политик безопасности и журналов.*

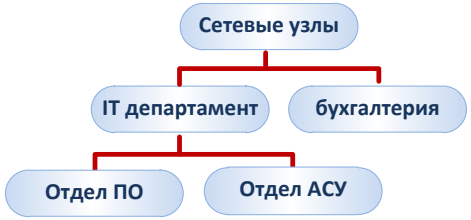
Подразделения

- группа сетевых узлов, объединенных под одним именем, к которым можно применить единую политику безопасности;

Отдел кадров



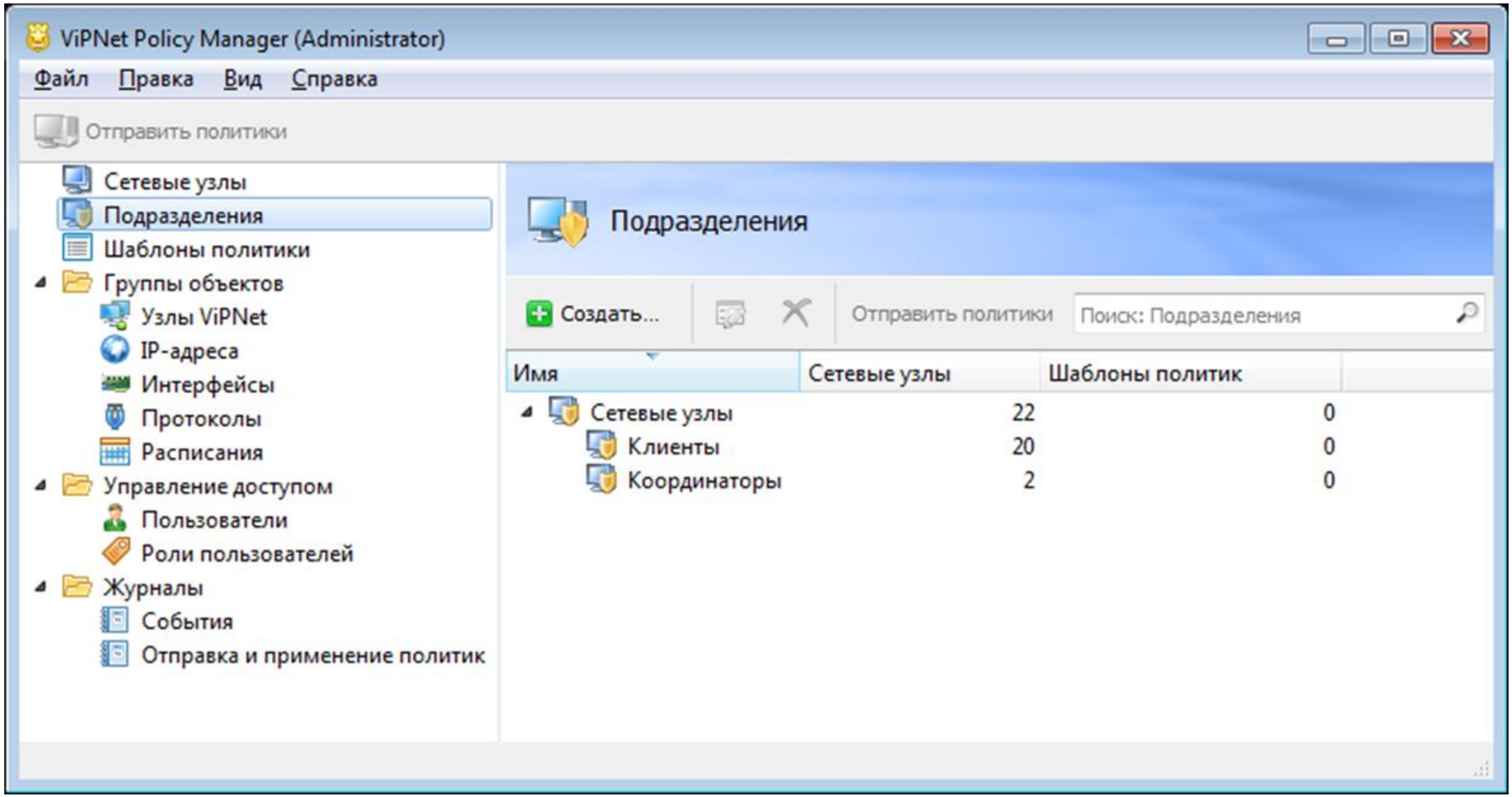
- рассылка политики безопасности может производиться как на отдельные узлы подразделения, так и сразу на все;



- подразделения можно выстроить иерархически, размещая одно подразделение в другом.

ViPNet Policy Manager

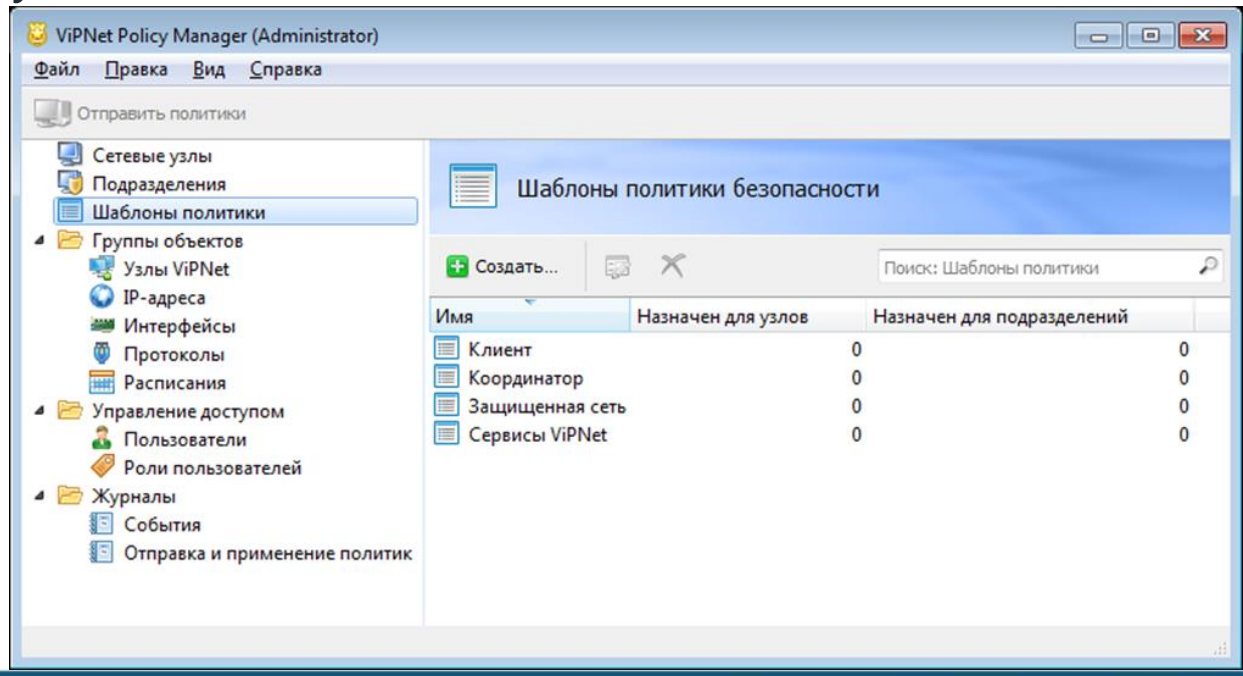
Иерархическое выстраивание подразделений



Шаблоны политики безопасности

Шаблон политики безопасности:

- набор сетевых фильтров и правил трансляции IP-адресов, предназначенный для реализации определенной политики безопасности;
- шаблоны политики безопасности можно назначить подразделениям и отдельным сетевым узлам;
- на основании шаблонов создаются результирующие политики безопасности, которые рассылаются на узлы ViPNet.



Состав шаблона политики безопасности

ШАБЛОН ПОЛИТИКИ БЕЗОПАСНОСТИ

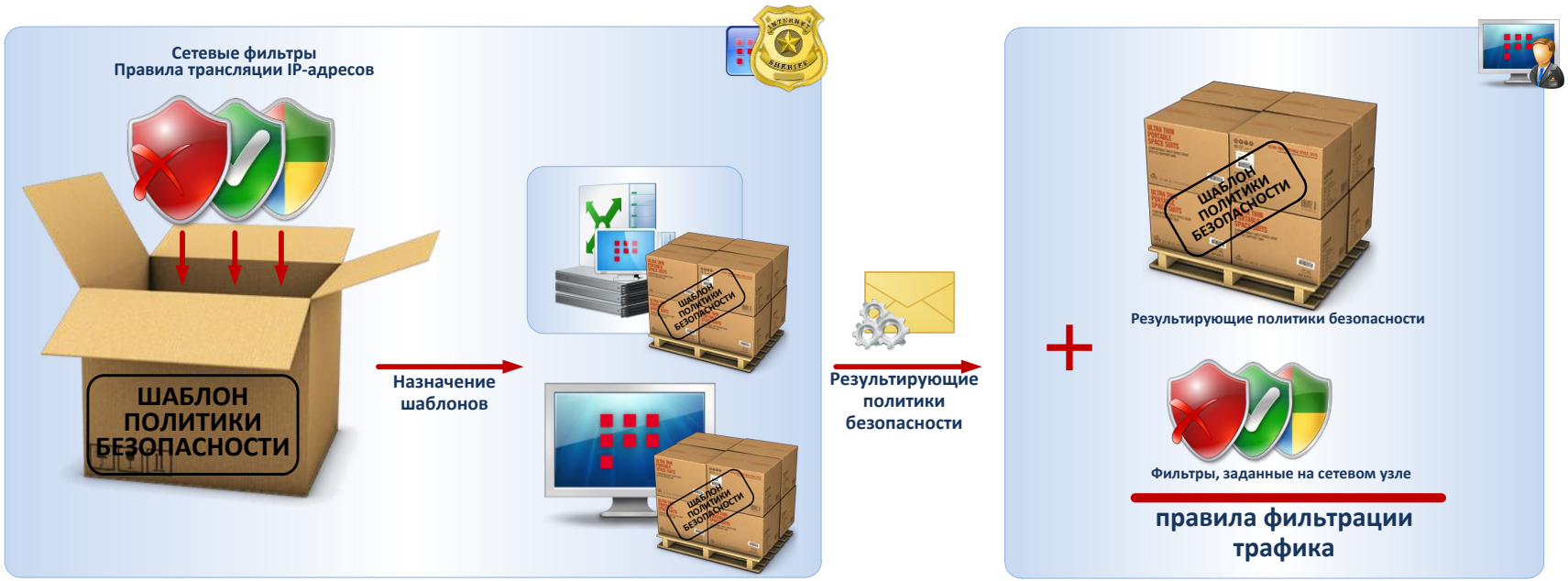
- шаблоны, созданные администратором;
- типовые шаблоны, поставляемые в составе Policy Manager.

Сетевые фильтры

- локальные фильтры открытой сети;
- транзитные фильтры открытой сети;
- фильтры для туннелируемых узлов;
- фильтры защищенной сети.

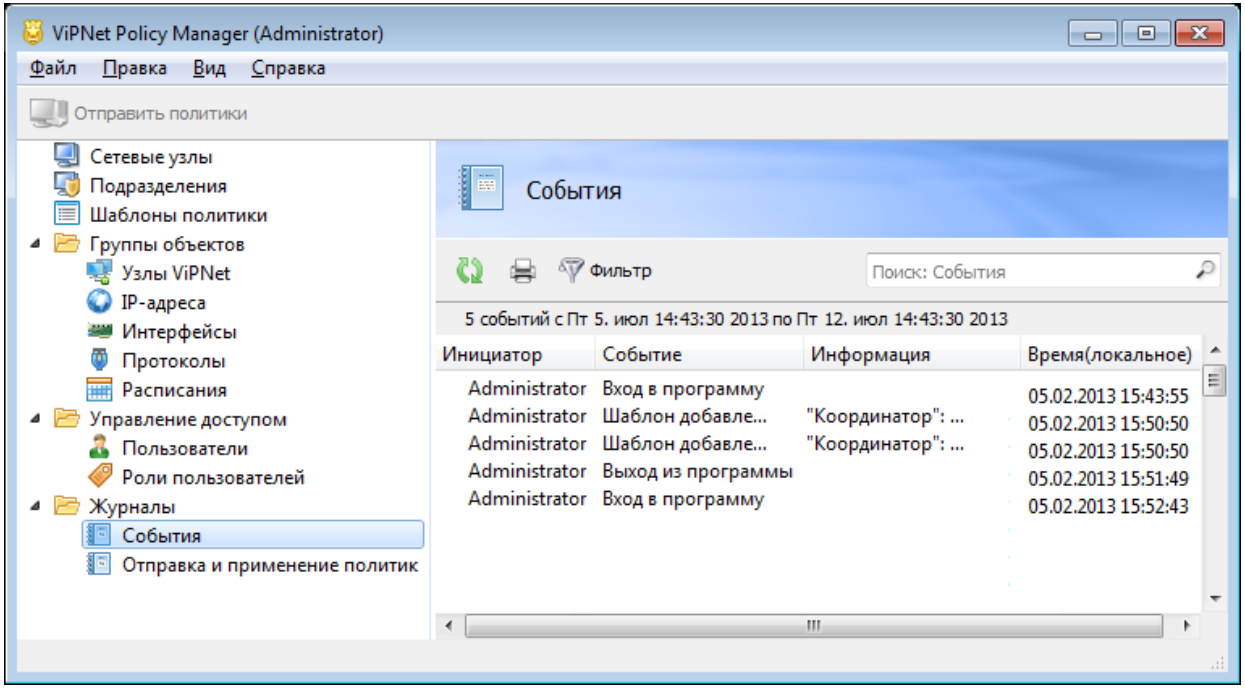
Правила трансляции IP-адресов

Формирование итоговых правил фильтрации трафика



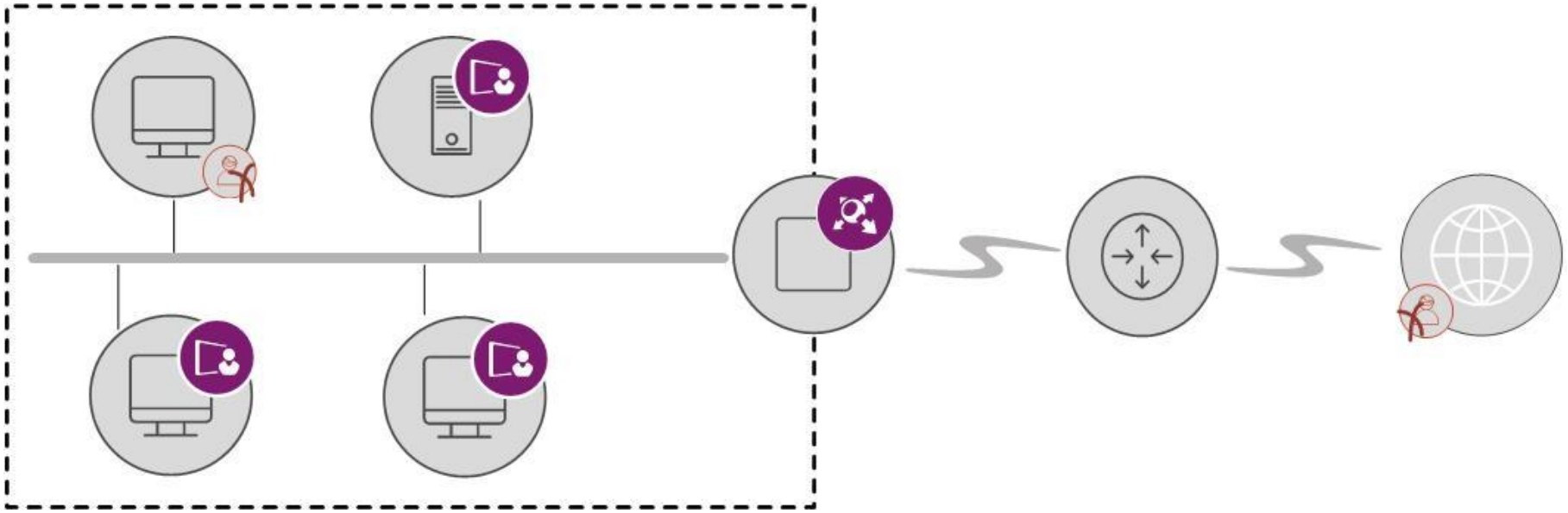
Формирование итоговых правил фильтрации трафика

События, связанные с отправкой политик безопасности на сетевые узлы и их применением на узлах, записываются в журнал, который отображается в подразделе **Отправка и применение политик** раздела **Журналы**.

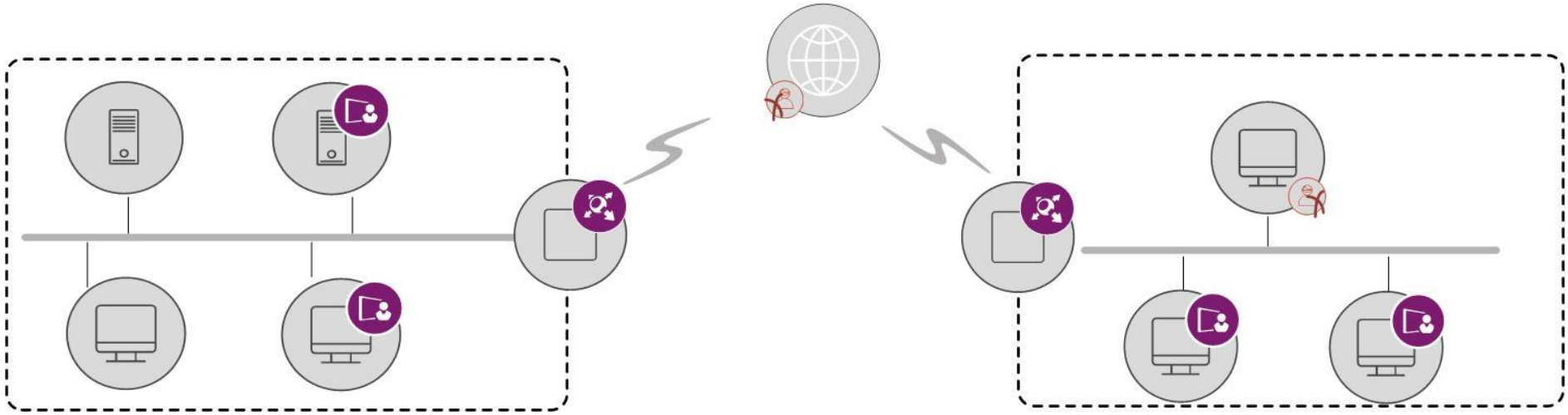


Раздел **Журналы** будет присутствовать на панели навигации только в случае, если текущий пользователь программы имеет полномочие **Аудит**.

Схемы защищенной сети ViPNet

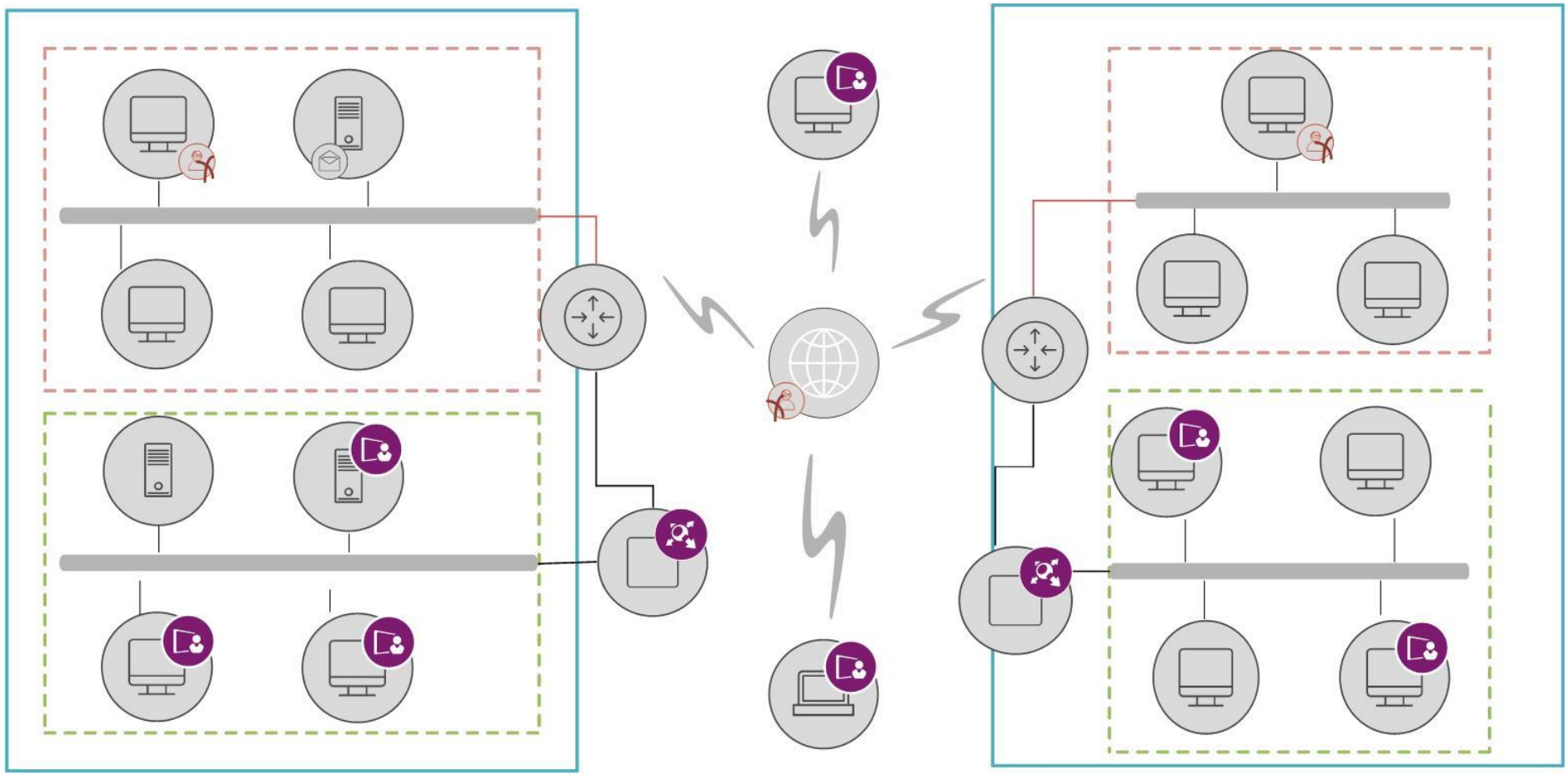


Схемы защищенной сети ViPNet



ViPNet Network Security 4.x

Схемы защищенной сети ViPNet



infotecs

Спасибо за внимание!

Вопросы?

НОЧУ ДПО ЦПК «Учебный центр «ИнфоТеКС»
education@infotecs.ru

ОАО «ИнфоТеКС», Москва
(495) 737-61-92
www.infotecs.ru