Санкт-Петербургское государственное бюджетное
профессиональное образовательное учреждение
«Академия управления городской средой, градостроительства и печати»

УТВЕРЖДАЮ
Заместитель директора
по учебно-производственной работе
О.В. Фомичева
«16» 12 2023 г.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
по выполнению практических работ
по МДК.03.04 Защита от внутренних угроз информационной безопасности
ПМ.03 ЭКСПЛУАТАЦИЯ ОБЪЕКТОВ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

для специальности

09.02.06 Сетевое и системное администрирование

Санкт-Петербург
2023 г.

Методические рекомендации рассмотрены на заседании методического совета СПб ГБПОУ «АУГСГиП»
Протокол № 2 от «29» 11 2023 г.

Методические рекомендации одобрены на заседании цикловой комиссии информационных технологий
Протокол № 4 от «21» 11 2023 г.

Председатель цикловой комиссии: Караченцева М.С. _____

Разработчики: преподаватели СПб ГБПОУ «АУГСГиП»

С О Д Е Р Ж А Н И Е

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Рабочая тетрадь для выполнения практических работ предназначена для организации работы на практических занятиях по МДК.03.04 «Защита от внутренних угроз информационной безопасности», являющегося важной составной частью в системе подготовки специалистов среднего профессионального образования по специальности 09.02.06 Сетевое и системное администрирование.

Практические занятия являются неотъемлемым этапом изучения тем МДК.03.04 «Защита от внутренних угроз информационной безопасности» и проводятся с целью:

- формирования практических умений в соответствии с требованиями к уровню подготовки обучающихся, установленными рабочей программой ПМ.03;
- обобщения, систематизации, углубления, закрепления полученных теоретических знаний;
- готовности использовать теоретические знания на практике.

Практические занятия по темам МДК.03.04 «Защита от внутренних угроз информационной безопасности» способствуют формированию следующих общих и профессиональных компетенций:

ПК 3.3. Осуществлять защиту информации в сети с использованием программно-аппаратных средств

ПК 3.6. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов

ОК 1. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам;

ОК 2. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности;

ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях;

ОК 4. Эффективно взаимодействовать и работать в коллективе и команде;

ОК 5. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста;

ОК 6. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения;

ОК 7. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях;

ОК 8. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности;

ОК 9. Пользоваться профессиональной документацией на государственном и иностранном языках.

В Рабочей тетради предлагаются к выполнению практические работы, предусмотренные рабочей программой ПМ.03 «Эксплуатация объектов сетевой инфраструктуры».

При разработке содержания практических работ учитывался уровень сложности освоения студентами соответствующей темы, общих и профессиональных компетенций, на формирование которых направлен ПМ.03 «Эксплуатация объектов сетевой инфраструктуры».

Выполнение практических работ в рамках тем МДК.03.04 «Защита от внутренних угроз информационной безопасности» ПМ.03 «Эксплуатация объектов сетевой инфраструктуры» позволяет освоить комплекс работ по защите информации с применением программно-аппаратных средств защиты. В Рабочей тетради представлены примеры применения программно-аппаратных средств защиты информации по МДК.03.04 «Защита от внутренних угроз информационной безопасности».

Рабочая тетрадь для выполнения практических заданий по темам МДК.03.04 «Защита от внутренних угроз информационной безопасности» ПМ.03 «Эксплуатация объектов сетевой инфраструктуры» имеет практическую направленность и значимость. Формируемые в процессе их проведения умения могут быть использованы студентами в будущей профессиональной деятельности.

Рабочая тетрадь предназначена для студентов колледжа, изучающих темы МДК.03.04 «Защита от внутренних угроз информационной безопасности» ПМ.03 «Эксплуатация объектов сетевой инфраструктуры».

Оценки за выполнение практических работ выставляются по пятибалльной системе. Оценки за практические работы являются обязательными текущими оценками по МДК.03.04 «Защита от внутренних угроз информационной безопасности» ПМ.03 «Эксплуатация объектов сетевой инфраструктуры» и выставляются в журнале теоретического обучения.

1. Перечень практических работ по темам МДК.03.04 «Защита от внутренних угроз информационной безопасности» ПМ.03 «Эксплуатация объектов сетевой инфраструктуры»

№ раздела, темы	Освоение умений в процессе занятия	Формируемые ОК и ПК	Тема практического занятия	Кол-во часов
Тема 5.1.	создавать защищённую сеть	ОК 1 – ОК 9 ПК 3.3, ПК 3.6	Практическая работа № 1 Развёртывание защищённой сети ViPNet: установка ЦУС	2
			Практическая работа № 2 Развёртывание защищённой сети ViPNet: установка УКЦ	2
			Практическая работа № 3 Развёртывание защищённой сети ViPNet: установка клиента ViPNet	2
			Практическая работа № 4 Создание структуры защищённой сети ViPNet	2
			Практическая работа № 5 Развёртывание рабочего места помощника главного администратора защищённой сети ViPNet	2
			Практическая работа № 6 Настройка рабочего места помощника главного администратора защищённой сети ViPNet	2
	Настраивать и модифицировать межсетевое взаимодействие	ОК 1 – ОК 9 ПК 3.3, ПК 3.6	Практическая работа № 7 Модификация защищённой сети ViPNet	2
			Практическая работа № 8 Компрометация ключей в защищённой сети ViPNet	2
			Практическая работа № 9 Поднятие защищённой сети ViPNet после компрометации	2
			Практическая работа № 10 Настройка политик безопасности в ViPNet Policy Manager	2
			Практическая работа № 11 Межсетевое взаимодействие	2
			Практическая работа № 12 Модификация межсетевого взаимодействия в защищённой сети ViPNet	2
			Практическая работа № 13 Составить сравнительную характеристику программно-аппаратных средств для создания защищённой сети	2
Тема 5.2	Устанавливать DLP-систему	ОК 1 – ОК 9 ПК 3.3, ПК 3.6	Практическая работа № 14 Установка и настройка Traffic monitor	2
			Практическая работа № 15 Настройка Traffic monitor	2
			Практическая работа № 16 Установка Device monitor	2

№ раздела, темы	Освоение умений в процессе занятия	Формируемые ОК и ПК	Тема практического занятия	Кол-во часов
			Практическая работа № 17 Настройка Device monitor	2
			Практическая работа № 18 Установка клиента Device monitor. Настройка периметра компании, добавление пользователей и компьютеров в домен	2
			Практическая работа № 19 Установка и настройка Crawler	2
	Создавать правила и политики безопасности в DLP-системах	ОК 1 – ОК 9 ПК 3.3, ПК 3.6	Практическая работа № 20 Создание простых правил и проверка их работоспособности в Device monitor	2
			Практическая работа № 21 Создание правил с использованием «белых» и «чёрных» списков в Device monitor	2
			Практическая работа № 22 Добавление ролей, редактирование ролей, удаление ролей в Traffic monitor	2
			Практическая работа № 23 Создание объектов защиты в Traffic monitor	2
			Практическая работа № 24 Изменение объектов защиты в Traffic monitor	2
			Практическая работа № 25 Добавление политик безопасности в Traffic monitor	2
			Практическая работа № 26 Создание политик с использованием перехвата фотографий в Traffic monitor	2
			Практическая работа № 27 Работа с терминами (добавление, настройка параметров, импорт из файла, редактирование, удаление, поиск, перемещение) в Traffic monitor	2
			Практическая работа № 28 Работа со списками (добавление элементов в список, редактирование, удаление) в Traffic monitor	2
			Практическая работа № 29 Работа с тегами (добавление группы тегов, редактирование параметров группы тегов, добавление тегов, редактирование тегов, удаление тегов) в Traffic monitor	2
			Практическая работа № 30 Создание политик безопасности	2
			Практическая работа № 31 Создание политик с использованием комбинированных объектов защиты	2
	Создавать отчёты	ОК 1 –	Практическая работа № 32	2

№ раздела, темы	Освоение умений в процессе занятия	Формируемые ОК и ПК	Тема практического занятия	Кол-во часов
	по инцидентам в DLP-системах	ОК 9 ПК 3.3, ПК 3.6	Создание виджетов в Traffic Monitor. Изменение виджетов в Traffic Monitor	
			Практическая работа № 33 Создание отчётов в Traffic Monitor. Изменение отчётов в Traffic Monitor	2

2. ОПИСАНИЕ ПОРЯДКА ВЫПОЛНЕНИЯ ПРАКТИЧЕСКИХ РАБОТ

Практическая работа № 1
Развёртывание защищённой сети ViPNet: установка ЦУС

Задание:

Установка ПК ViPNet Administrator 4:

VM_1:
ViPNet Administrator
ViPNet Client
ViPNet Policy Manager
VM_2:
ViPNet NCC Client
ViPNet Client
VM_1 = Win 7_1
VM_2 = Win7_2

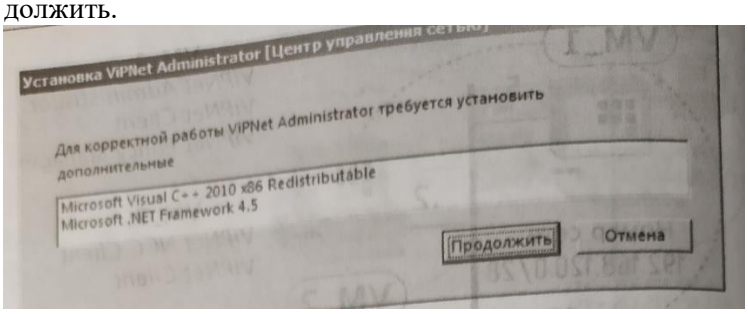
Формулировка задания

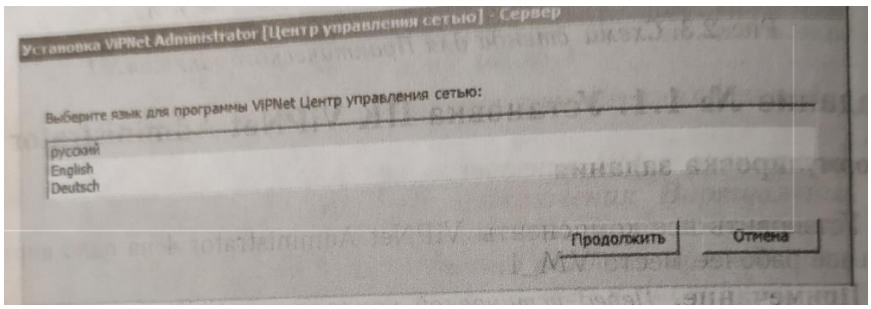
Установить все компоненты ViPNet Administrator 4 на одно виртуальное рабочее место VM_1.

Примечание. Перед установкой компонентов ViPNet необходимо убедиться в соответствии узла (персонального компьютера/сервера/виртуальной машины) системным требованиям. В случае если узел, на котором запланирована установка компонентов ViPNet, не соответствует системном требованиям, его необходимо переконфигурировать. В противном случае корректная работа и правильность выполнения практических заданий не гарантирована.

Установка серверного приложения ViPNet ЦУС

1. Для установки серверного приложенйя ViPNet Центр управления сетью откройте файл Setup.exe из каталога серверного приложения ViPNet Administrator.
2. В окне Установка ViPNet Administrator Центр управления сетью будет предложено установить дополнителъиде программное обеспечение. Список необходимого дополнительного ПО зависит от ранее установленных на компьютер программ. Чтобы начать установку, нажмите, кнопку Продолжить.
3. В появившемся окне выберите язык для программы Центр управления сетью и нажмите Продолжить.

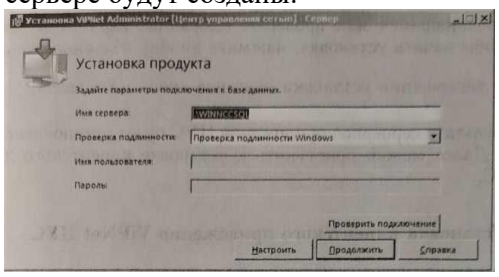




4. На странице Лицензионное соглашение ознакомьтесь с условиями лицензионного соглашения. В случае, Согласия установите соответствующий флажок. Затем нажмите кнопку Продолжить.

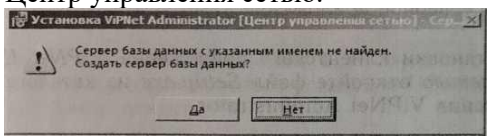
5. На странице Установка продукта задайте параметры подключения к базе данных. Если вы не укажете, имя существующего SQL-сервера, то на компьютере будет установлен SQL-сервер из комплекта поставки и создан именованный экземпляр с именем WINNCCSQL. При необходимости вы можете задать другое имя экземпляра. В рамках выполнения практического задания изменять параметры подключения не требуется. Нажмите кноп ку Продолжить и в следующем окне - Установить сейчас.

6. В появившемся окне о создании сервера базы данных нажмите кнопку Да. При этом на SQL-сервере будут созданы:



• База данных с именем ViPNetAdministrator.

• База данных с именем ViPNetJournals, в которой хранятся журналы аудита программы ViPNet Центр управления сетью.



• Учетная запись пользователя с правами администратора базы данных для пользователя, от имени которого был запущен файл установки серверного приложения ЦУС.

• Две учетные записи пользователей KcaUser и NccUser, под которыми осуществляется подключение УКЦ и серверного приложения ЦУС к базе данных соответственно.

7. После создания сервера базы данных требуется перезагрузка компьютера, программа выдаст соответствующее сообщение. Выполните перезагрузку.

После перезагрузки установка серверного приложения ЦУС будет продолжена автоматически. Если после перезагрузки установка серверного приложения не продолжилась автоматически, необходимо самостоятельно запустить Setup.exe из каталога серверного приложения ViPNet Administrator (это необходимо для завершения установки серверного приложения, так как до перезагрузки были установлены только дополнительные компоненты и SQL-сервер).

8. В появившемся окне выберите язык для программы Центр управления сетью и нажмите Продолжить.

9. На странице Установка продукта нажмите Продолжить.

10. В появившемся окне проверьте выбранные параметры установки. Чтобы начать установку, нажмите кнопку Установить сейчас.

11. По завершении установки нажмите кнопку Закрыть.

В результате серверное приложение ЦУС будет установлено на компьютер. Далее можно приступить к установке клиентского при ложения ЦУС.

вставить скриншот с установленным серверным приложением ЦУС.

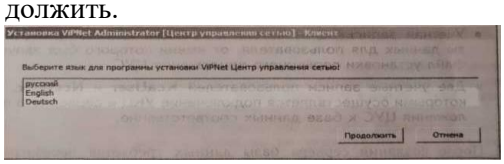
Практическая работа № 2
Развёртывание защищённой сети ViPNet: установка УКЦ

Задание:

Установка клиентского приложения ViPNet ЦУС

В рамках настоящего практического задания клиентское приложение ViPNet Центр управления сетью устанавливается на то же рабочее место, что и серверное приложение.

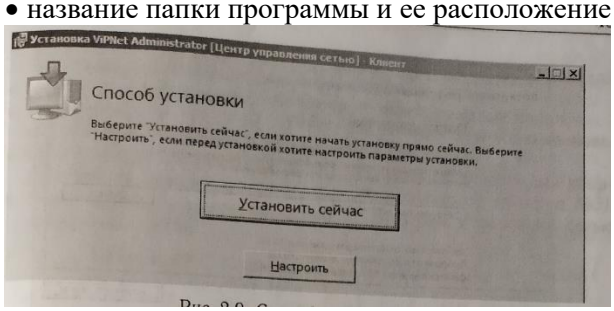
1. Для установки клиентского приложения ViPNet Центр управления сетью откройте файл Setup.exe из каталога клиентского приложения ViPNet Administrator.
2. В появившемся окне выберите язык для клиентского приложения ViPNet ЦУС и нажмите Продолжить.



3. На странице Лицензионное соглашение ознакомьтесь с условиями лицензионного соглашения. В случае согласия установите соответствующий флажок. Затем нажмите кнопку Продолжить.
4. На странице Способ установки нажмите Установить сейчас.

Если требуется настроить параметры установки, то нажмите кнопку Настроить на странице Способ установки и укажите:

- путь к папке установки программы на компьютере;
- имя пользователя и название организации;
- название папки программы и ее расположение в меню Пуск.



5. По завершении установки нажмите кнопку Закрыть.

В результате клиентское приложение ЦУС будет установлено на компьютер. Далее можно приступить к установке ПО ViPNet Удостоверяющий и ключевой центр.

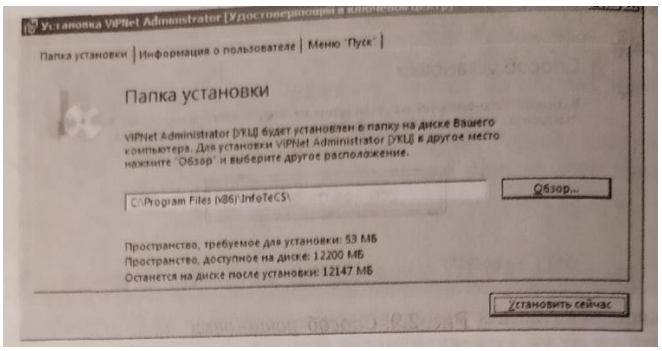
Вставить скриншот с установленным клиентским приложением ЦУС.

Установка ViPNet Удостоверяющий и ключевой центр

В рамках настоящего практического задания ViPNet Удостоверяющий и ключевой центр устанавливается на то же рабочее место, что и серверное приложение:

1. Для установки компонента ViPNet Удостоверяющий и ключевой центр откройте файл Setup.exe из каталога удостоверяющего и ключевого центра ViPNet Administrator.
2. Подождите, пока на компьютер будет автоматически установлено необходимое программное обеспечение, в том числе программа ViPNet CSP.
3. В окне Установка ViPNet Administrator [Удостоверяющий и ключевой центр] на странице Лицензионное соглашение ознакомьтесь с условиями лицензионного соглашения. В случае согласия установите соответствующий флажок. Затем нажмите кнопку Продолжить.
4. На странице Способ установки нажмите кнопку Установить сейчас.
5. Если потребуется настроить параметры установки, то нажмите кнопку Настроить на странице Способ установки и укажите:

- путь к папке установки программы на компьютере;
- имя пользователя и название организации;
- название папки программы и её расположение в меню Пуск.



6. По окончании установки нажмите кнопку Закрыть,

После установки УКЦ потребуется перезагрузка компьютера, программа выдаст соответствующее сообщение. Выполните перезагрузку.

Вставить скриншот с установленным УКЦ.

Задание 2:

Ответить на следующие вопросы:

✓ Из каких компонентов состоит программный комплекс ViPNet Administrator 4?
✓ Какие функции выполняет ЦУС?
✓ Какие функции выполняет УКЦ?
✓ Какие функции выполняет ViPNet Coordinator?
✓ Какие функции выполняет ViPNet Client?
✓ Назовите состав ЦУС
✓ Назовите рабочие каталоги ЦУС/УКЦ?

Ответы:

Практическая работа № 3
Развёртывание защищённой сети ViPNet: установка клиента ViPNet

Задание:

Создать структуру защищенной сети в соответствии с заданной схемой, настроить связи пользователей (в соответствии с матрицей связей в ЦУС и сформировать дистрибутивы Ключей для сетевых узлов В УКЦ.

Таблица. Пользователи и сетевые узлы (клиенты)

№	Название СУ	Имя пользователя на СУ
1	Главный администратор	Глав админ Петров
2	Помощник глав админа	Помощник глав админа Иванов
3	Сотрудник_1 Центр офис	Сотруд_1 Центр Кузнецов
4	Сотрудник_2 Филиал	Сотруд_2 Филиал Попов

В ЦУС предусмотрено автоматическое создание связей без возмож ности их удаления между некоторыми сетевыми узлами (в списке связей помечаются серым цветом, ЦУС → Свойства узла):

✓ Связь узла с Центром управления сетью.
✓ Между координатором и зарегистрированными на нем клиентами.
✓ Связи между координатором и клиентами, для которых данный координатор назначен сервером IP-адресов.
✓ Связь между сетевым узлом и координатором, выбранным для организации соединений с внешними узлами.
✓ Между координаторами, образующие межсерверный канал.
✓ Связь между узлом с ПО ViPNet Policy Manager и подчиненными ему СУ
✓ Связи шлюзовых координаторов своей сети со шлюзовыми координаторами доверенных сетей
✓ Связи Центра управления сетью с Центрами управления сетью доверенных сетей.

Связи пользователей	Координатор Центр офис	. Глав админ Петров	Помощник глав админа Иванов	Сотруд_1 Центр Кузнецов	Координатор Филиал	Сотруд_2 Филиал Попов
Координатор Центр офис		•	•	•	•	
Глав админ Петров	•		•			
Помощник глав админа Иванов	•	•				
Сотруд_1 Центр Кузнецов	•					•
Координатор Филиал	•					•
Сотруд_2 Филиал Попов				•	•	

Примечание. Связь узла с Центром управления сетью является технологической и используется только для обеспечения возможности рассылки справочников, ключей и обновлений программного обеспечения.

Рекомендуется устанавливать в первую очередь связи пользователей, так как в данном случае связи узлов будут установлены автоматически.

На каждом защищенном узле в программе ViPNet Монитор в разделе «Защищенная сеть» отображается список сетевых узлов, с которыми, связан данный узел. Однако для отображения в программе ViPNet Монитор узла с программой ViPNet ЦУС необходимо дополнительно создать связь между пользователями СУ и ЦУС.

Внимание! Если связь с Центром управления сетью должна оставаться скрытой, не следует создавать связи между пользователями сетевых узлов и пользователем Центра управления сетью.

Для начала работы с программой ViPNet ЦУС:

1. Выполните запуск программы с ярлыка на Рабочем столе или через меню Пуск (Пуск → Все программы → ViPNet ViPNen Administrator → Центр управления сетью).

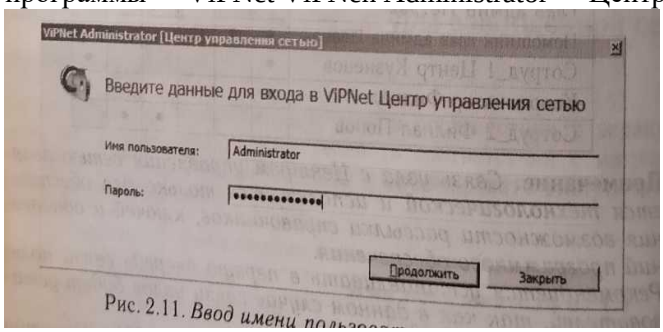
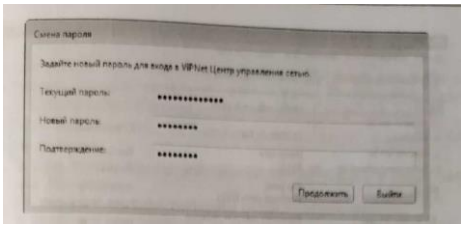
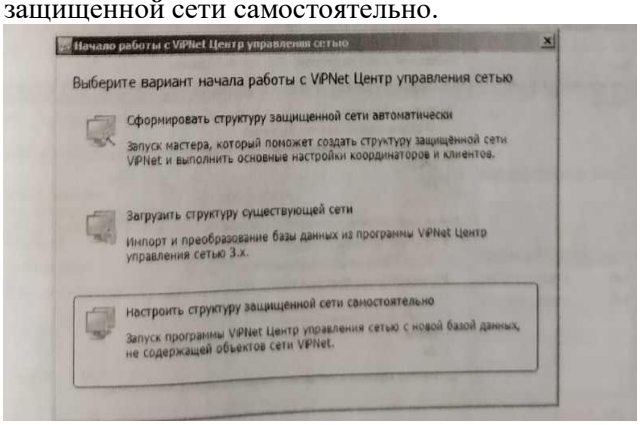


Рис. 2.11. *Ввод имени пользователя*

2. В появившемся окне введите имя и пароль - Administrator, нажмите кнопку Продолжить.
3. После загрузки программы будет предложено сменить пароль! Чтобы сменить пароль, введите текущий пароль (Administrator) новый пароль, а затем нажмите кнопку Продолжить. В рамках практического занятия задайте новый пароль - 11111111.
4. В окне Начало работы с ViPNet Центр, управления сетью с помощью кнопки Обзор укажите путь к. файлу лицензии на сеты ViPNet (*.itcslic или infotecs.reg) и нажмите кнопку Продолжить.



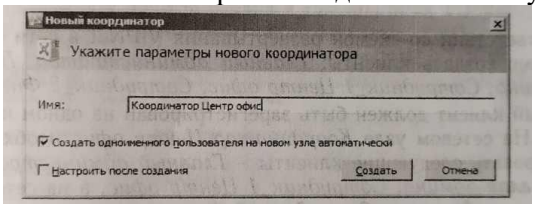
5. В появившемся окне с выбором возможных сценариев работы нажмите Настроить структуру защищенной сети самостоятельно.



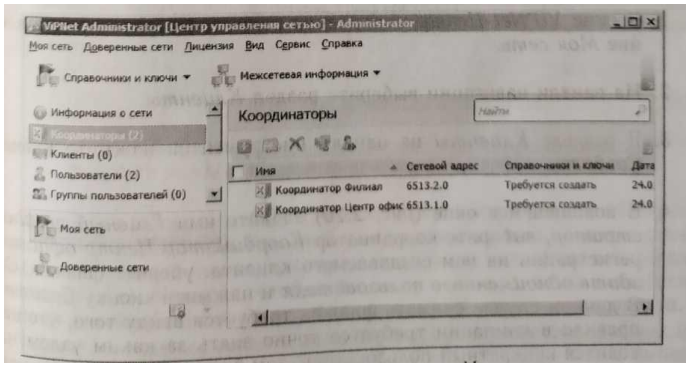
6. Откроется главное окно программы.
7. Проверьте первоначальные настройки программы ViPNet Центр управления сетью. Для этого выполните следующие действия:
✓ В меню Сервис выберите пункт Параметры;
✓ В открывшемся окне перейдите в раздел Роли;
✓ Затем, если обнаружите различия, задайте значения параметров в соответствии с рис.

Вставьте скриншот, подтверждающий выполнение задания

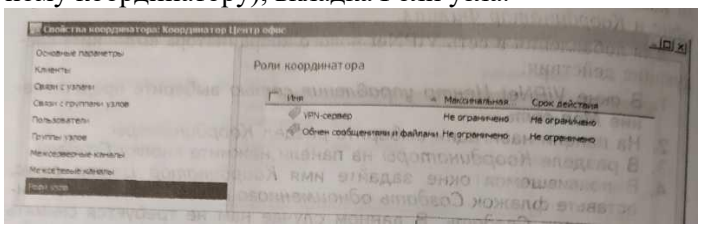
Примечание. В реальной сети рекомендуется задавать средний или минимальный уровень полномочий. Полномочия задаются при нажатии на подчеркнутые мелким пунктиром параметры, расположенные в скобочках.
Теперь можно приступить к созданию структуры защищённой сети.
Создание координаторов
В соответствии со схемой развертывания ViPNet в локальной сети компании необходимо создать сетевые узлы: Координатор Центр офис и Координатор Филиал.
✓ Для добавления в сеть ViPNet нового координатора выполните следующие действия:
✓ В окне ViPNet Центр управления сетью выберите представление Моя сеть.
✓ На панели навигации выберите раздел Координаторы.
✓ В разделе Координаторы на панели нажмите кнопку Создать.
✓ В появившемся окне задайте имя Координатор Центр офис, оставьте флажок Создать одноименного пользователя и нажмите кнопку Создать. В данном случае нам не требуется снимать флажок, так как имя узла и имя пользователя координатора, будут совпадать. Таким образом не придется совершать лишних действий (это ускорит процесс создания структуры сети).
Аналогичным образом создается сетевой узел Координатор Филиал.



После создания раздел Координаторы окна ViPNet Центр управления сетью представления Моя сеть будет иметь следующий вид:



Созданным координаторам автоматически назначаются роли VPN. сервер и Обмен сообщениями и файлами. Чтобы убедиться в этом, зайдите в свойства координатора (двойной щелчок по выбранному координатору), вкладка Роли узла.



Вставьте скриншот, подтверждающий выполнение задания

Практическая работа № 4
Создание структуры защищённой сети ViPNet

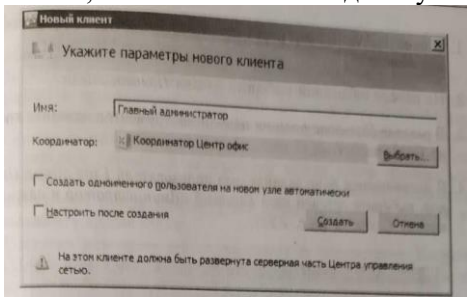
Задание:

Создание клиентов

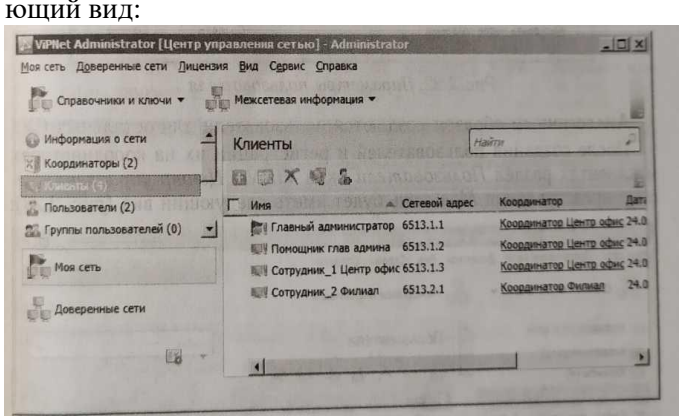
В соответствии со схемой развертывания ViPNet в сети компании необходимо создать клиенты: Главный администратор, Помощник глав админа, Сотрудник_1 Центр офис, Сотрудник_2 Филиал. Каждый клиент должен быть зарегистрирован на одном из координаторов. На сетевом узле Координатор Центр офис необходимо зарегистрировать следующие клиенты - Главный администратор, Помощник глав админа, Сотрудник.1 Центр офис, а на сетевом узле Координатор Филиал - Сотрудник_2 Филиал.

Чтобы добавить в сеть ViPNet нового клиента, выполните следующие действия:

1. В окне ViPNet Центр управления сетью выберите представление Моя сеть.
2. На панели навигации выберите раздел Клиенты.
3. В разделе Клиенты на панели инструментов нажмите кнопку Создать.
4. В появившемся окне задайте имя Главный администратор, выберите координатор Координатор Центр офис для регистрации на нем создаваемого клиента, уберите флажок Создать одноименного пользователя и нажмите кнопку Создать. В данном случае снимать флажок требуется ввиду того, что как правило в компании требуется точно знать за каким узлом находится конкретный пользователь, тем более если на одном узле их несколько.



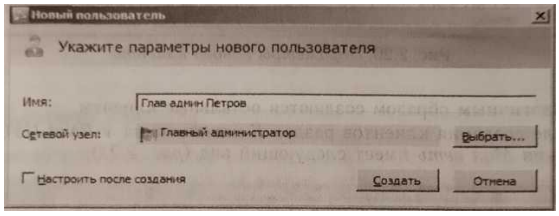
Аналогичным образом создаются остальные клиенты.
После создания клиентов раздел Клиенты окна ViPNet ЦУС представления Моя сеть имеет следующий вид:



Созданным клиентам автоматически назначаются роли – VPN-клиент, Business Mail и Обмен сообщениями и файлами, а для первого созданного клиента, дополнительно — системные роли Network Control Center и Policy Manager. Чтобы убедиться в этом, зайдите в свойства клиента (двойной щелчок по выбранному узлу), вкладка Роли узла.

Вставьте скриншот, подтверждающий выполнение задания

Теперь необходимо создать пользователей и зарегистрировать их на клиентах в соответствии с таблицей. Для этого выполните следующие действия:
1. В окне ViPNet Центр управления сетью выберите представление Моя сеть.
2. На панели навигации выберите раздел Клиенты.
3. В разделе Пользователи на панели инструментов нажмите кнопку Создать.
4. В появившемся окне задайте имя пользователя Глав админ Петров, выберите сетевой узел Главный администратор и нажмите кнопку Создать



Аналогичным образом создаются пользователи для остальных СУ.
После создания пользователей и регистрации их на координаторах и клиентах раздел Пользователи окна ViPNet Центр управления сетью представления Моя сеть будет иметь следующий вид:

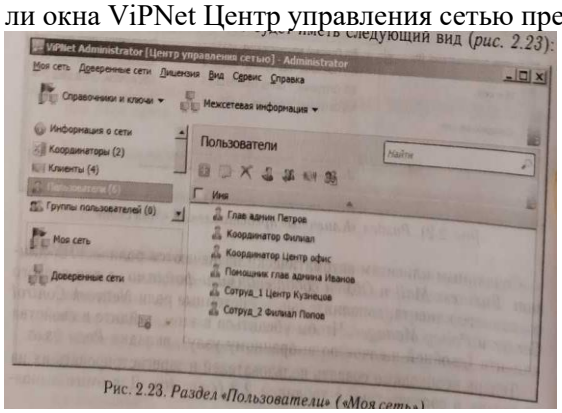


Рис. 2.23. Раздел «Пользователи» («Моя сеть»)

Вставьте скриншот, подтверждающий выполнение задания

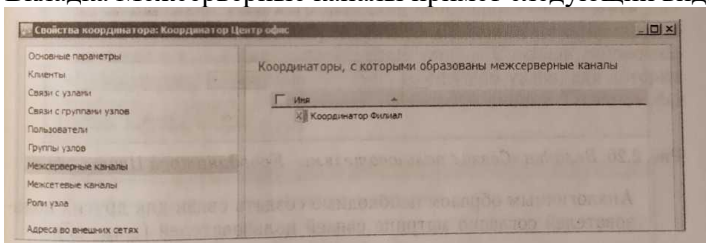
Создание межсерверных каналов и связей

Межсерверный канал связывает два координатора и позволяет им выполнять функцию сервера-маршрутизатора - обмениваться управляющими и прикладными транспортными конвертами. Необходимо, чтобы все координаторы были связаны между собой напрямую или через другие координаторы, то есть должен существовать хотя бы один путь передачи служебной информации между двумя любыми координаторами. Можно связать все координаторы с одним центральным координатором (схема «звезда»), все координаторы между собой или использовать другие схемы.

Построим межсерверный канал между координаторами Координатор Центр офис и Координатор Филиал. Для этого следует выполнить следующие действия:

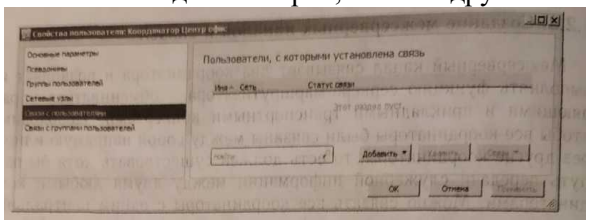
1. Перейдите в свойства СУ Координатор Центр офис (двойной щелчок по выбранному узлу).
2. На вкладке Межсерверные каналы нажмите кнопку Добавить.
3. В открывшемся окне выберите сетевой узел Координатор Филиал и нажмите кнопку Добавить.

Вкладка Межсерверные каналы примет следующий вид.

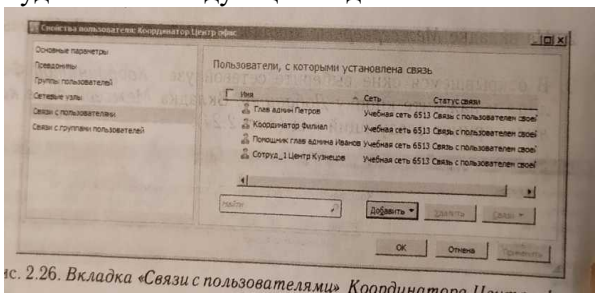


Теперь необходимо создать связи между пользователями в соответствии с матрицей связей пользователей защищенной сети

4. Перейдите в свойства пользователя Координатор Центр офис (двойной щелчок по выбранному узлу). Вкладка Связи с пользователями имеет следующий вид - на первоначальном этапе данный раздел пуст.
5. Добавьте связь пользователя Координатор Центр офис с пользователем Глав админ Петров. Для этого на вкладке Связи с пользователями нажмите кнопку Добавить и выберите из списка пользователя Глав админ Петров, а также других в соответствии с матрицей связей пользователей.



После связывания пользователей вкладка Связи с пользователями для Координатор Центр офис будет иметь следующий вид:



ис. 2.26. *Вкладка «Связи с пользователями» Координатора Центр офис*

Аналогичным образом необходимо создать связи для других пользователей согласно матрице связей пользователей.

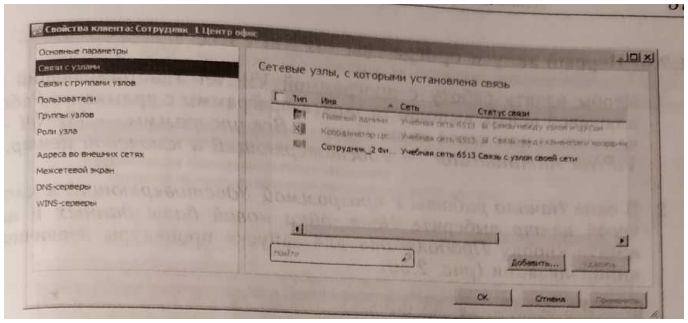
После этого автоматически будут созданы связи между узлами, к которым относятся связанные пользователи.

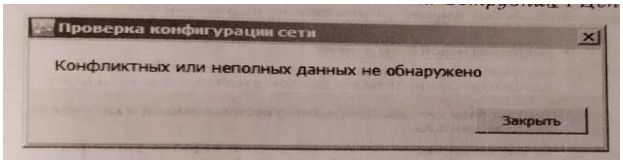
Примечание. Рекомендуется устанавливать в первую очередь связи между пользователями. Появиться возможность вести конфиденциальную переписку между конкретными пользователями, а не узлами.

6. Проверьте конфигурацию сети, выбрав в меню Моя сеть пункт Проверить конфигурацию сети...

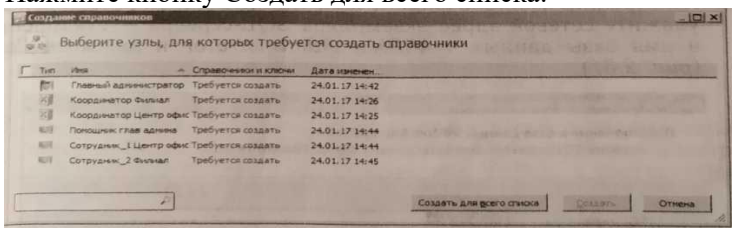
В случае, если сеть сконфигурирована верно, на экран будет выведено сообщение «Конфликтных или неполных данных не обнаружено».

Связи с пзяьзоваг...





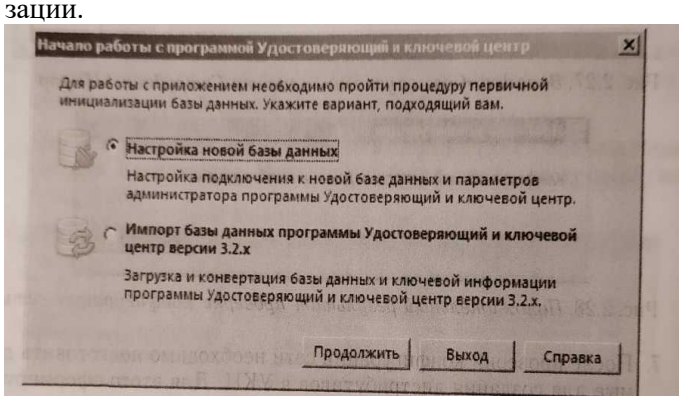
7. После проверки конфигурации сети необходимо подготовить данные для создания дистрибутивов в УКЦ. Для этого сформируйте справочники, выбрав в меню Моя сеть → Создать справочники. На экран будет выведено окно со списком узлов, для которых требуется создать справочники. Нажмите кнопку Создать для всего списка.



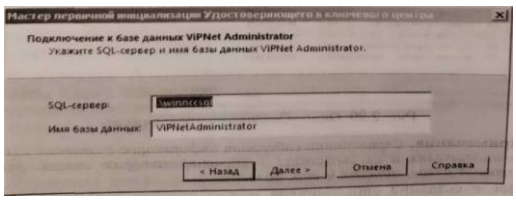
Примечание. Справочники содержат информацию о сетевых узлах, пользователях и их свойствах - идентификаторах, связях, ролях сетевых узлов, адресах и так далее.
После создания справочников можно перейти к первому запуску компонента ViPNet Удостоверяющий и ключевой центр.

Вставьте скриншот, подтверждающий выполнение задания

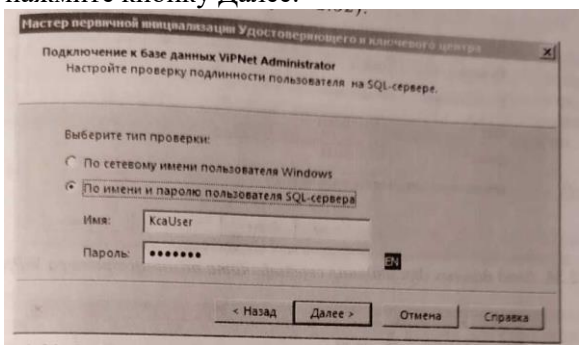
Первый запуск программы ViPNet УКЦ
1. Чтобы начать работу с программой ViPNet Удостоверяющий и ключевой центр, выполните запуск программы с ярлыка на Рабочем столе или через меню Пуск → Все программы → ViPNet →ViPNet Administrator → Удостоверяющий и ключевой центр.
2. В окне Начало работы с программой Удостоверяющий и ключевой центр выберите Настройка новой базы данных и нажмите кнопку Продолжить для запуска процедуры первичной инициализации.



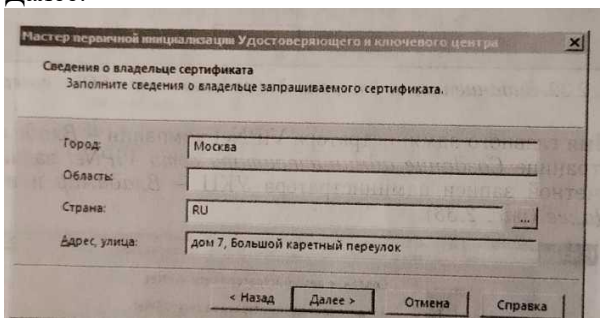
3. На первой странице мастера инициализации нажмите Далее.
4. На странице Подключение к базе данных ViPNet Administrator укажите сетевой адрес экземпляра SQL-сервера - .\winnccsql и имя базы данных - ViPNet Administrator и нажмите Далее.

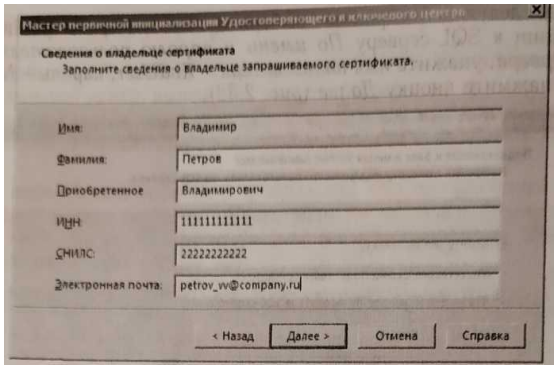


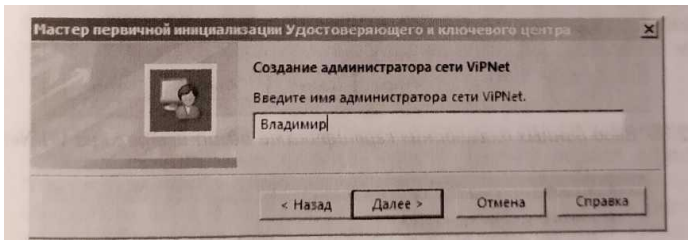
5. На следующей странице выберите тип проверки при подключении к SQL-серверу По имени и паролю пользователя SQL- сервера, укажите имя пользователя - KcaUser, пароль - Humbert и нажмите кнопку Далее:



6. Имя главного администратора ViPNet компании - Владимир. На странице Создание администратора сети ViPNet задайте имя учетной записи администратора УКЦ - Владимир и нажмите Далее:





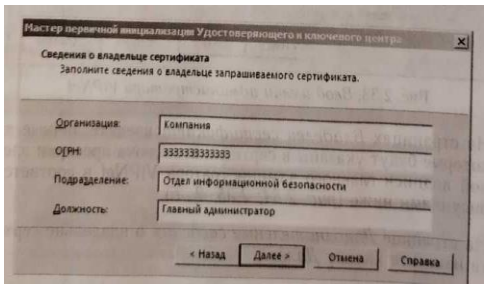


7. На страницах Владелец сертификата введите личные данные, которые будут указаны в сертификате ключа проверки электронной подписи главного администратора ViPNet в соответствии с рисунками ниже:
8. На странице Дополнительные сведения о владельце сертификата нажмите кнопку Далее.
9. На странице Параметры ключа электронной подписи оставьте значения ио умолчанию и нажмите кнопку Далее.
10. На странице Срок действия сертификата установите максимальное значение — 192 месяца с настоящего момента
11. На странице Программные средства, в случае, если планируется осуществлять создание и выдачу квалифицированных сертификатов ключей проверки электронных подписей указываются программные продукты, используемые в качестве средства электронной подписи издателя, средства электронной подписи владельцев сертификатов и средства удостоверяющего центра.
Внимание! В рамках настоящего практического задания функционирование продуктов ViPNet в качестве аккредитованного удостоверяющего центра не рассматривается, поэтому флаг «Функционировать в качестве аккредитованного удостоверяющего центра» устанавливать не нужно.
12. На странице Автоматический режим работы нажмите Далее.
13. На странице Место хранения контейнеров ключа подписи и ключа защиты УКЦ выберите место хранения контейнера ключей администратора - В файле.

Вставьте скриншот, подтверждающий выполнение задания

В зависимости от выбранного места хранения будет определен срок действия ключа ЭП. При хранении ключа электронной подписи в файле на компьютере либо на внешнем устройстве, которое не поддерживает алгоритм ГОСТ 34.10-2001, срок действия ключа ограничивается одним годом. Если ключ ЭП хранится на устройстве с поддержкой ГОСТ 34.10-2001 (был непосредственно сформирован на нем), то его срок действия составляет 3 года.

Под сроком действия понимается срок использования ключа электронной подписи для подписи издаваемых сертификатов пользователей. При этом список аннулированных сертификатов может быть подписан и по истечении срока действия ключа ЭП.
14. На странице Настройка паролей выберите тип создаваемого пароля - Собственный пароль, способ выдачи пароля пользователя - Сохранять пароль в файл XPS в папку (рекомендуется за-



помнить путь к данной папке или заменить на собственный, в дальнейшем его можно будет изменить на вкладке Сервис → Настройка... → Пароли), нажмите кнопку Далее. На появившейся странице задайте пароль администратора сети ViPNet - 11111111 (восемь единиц).
СОВЕТ. При выполнении практических занятий рекомендуется использовать, простые запоминающиеся пароли во всех программах (например, 11111111 - восемь единиц).
Примечание. В реальной ситуации, при настройке и формировании сети рекомендуется руководствоваться существующими правилами парольной безопасности или применять сгенерированные встроенными средствами ViPNet пароли, достаточной сложности.

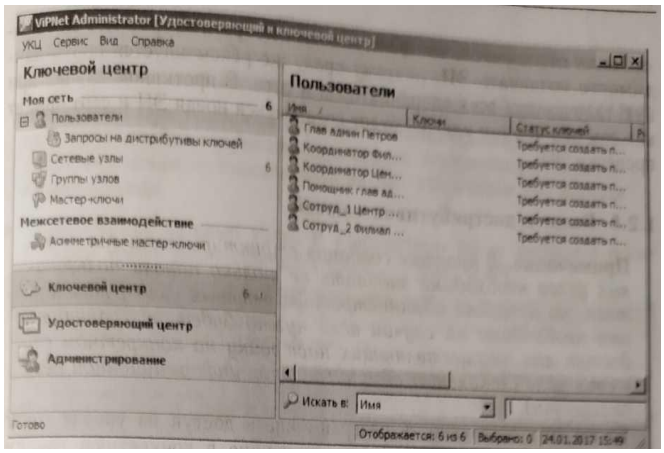
15. На странице готовности к завершению первичной инициализации убедитесь в правильности параметров, заданных на предыдущих страницах мастера. При изменении параметров вернитесь на нужную страницу с помощью кнопки Назад.

16. Для продолжения работы нажмите кнопку Далее. Поводите указателем в пределах окна Электронная рулетка и после успешного завершения инициализации нажмите Закрыть.

При успешном проведении первичной инициализации будет выполнены следующие операции:
✓ Создана учётная запись администратора УКЦ
✓ Создан ключ электронной подписи и издан сертификат администратора УКЦ
✓ Созданы мастер-ключи
✓ Установлено соединение с базой данных SQL и произведено её заполнение данными.

Вставьте скриншот, подтверждающий выполнение задания

В случае корректной инициализации появится главное окно программы.
Перед началом работы в УКЦ проверьте первоначальные настройки программы. В меню Сервис выберите пункт Настройка. В открывшемся окне в разделе Пароли установите тип пароля, который будет использоваться при создании новых паролей, - Собственный пароль, на вкладке Сертификаты снимите флажки Редактировать поля сертификатов при издании и Создавать ключи электронной подписи.
После проверки первоначальных настроек необходимо снять вручную флажок Создавать ключи электронной подписи в свойствах пользователей (УКЦ Моя сеть Пользователи, кликнуть правой кнопкой мыши на пользователя и выбрать пункт Ключи пользователя → Создавать ключи электронной подписи).
Теперь можно приступить к созданию дистрибутивов ключей.



Примечание. В разделе Сервис → Настройка... → Сертификаты, стоит обратить внимание на второй пункт Создавать ключи электронной подписи. В случае если в вашей сети для большинства узлов (клиентов) требуется выпуск электронной подписи и сертификата проверки электронной подписи (например, для обеспечения юридически значимого электронного документооборота), то рекомендуется оставить данный флажок включенным.
Но главное - не забывать снимать вручную данный флажок в свойствах конкретного пользователя, которому не нужно выпускать электронную подпись (УКЦ → Моя сеть → Пользователи, кликнуть правой кнопкой мыши на пользователя которому не нужно формировать ЭП выбрать пункт Ключи пользователя → Создавать ключи электронной подписи).
В ином случае, рекомендуется снять галочку в настройках УКЦ, тогда ключи электронной подписи не будут формироваться для всех новых узлов, добавляемых в сеть.

Также стоит учесть тот факт, что для координаторов нет необходимости создавать ЭП, поэтому сразу же рекомендуется снять данную галочку для всех координаторов в сети. В противном случае при каждом обновлении ключей будет создаваться новая ЭП и сертификат проверки ЭП.

Выдача дистрибутивов ключей

Примечание. В процессе создания структуры сети для сетевых узлов необходимо задавать не только пароли пользователя, но и пароли администратора сетевых узлов, так как это необходимо на случай если нужно будет разграничить доступ лиц, осуществляющих настройку на конкретном сетевом узле (локальный администратор информационной безопасности).

Также есть возможность разграничивать доступ на уровне групп узлов, в данном случае все узлы, входящие в конкретную группу, могут запускаться в режиме администратора с Использованием пароля администратора данной группы.

При создании сети ViPNet в ЦУСе автоматически создается группа «Вся сеть», в которую входят все узлы данной сети ViPNet. При первом запуске УКЦ в обязательном порядке задается пароль администратора сетевых узлов группы «Вся сеть». Данную группу нельзя удалить, а пароль присвоенный данной группе может быть. использован для запуска ПО ViPNet на любом узле в режиме администраторе

Внимание! Пароли администратора (группы или узла) нельзя передавать или каким-либо образом сообщать пользователю узла. Данный тип паролей предназначен исключительно для администрирования конкретного узла или группы узлов и может быть сообщен только лицу ответственному за настройку и контроль работоспособности средств криптографической защиты информации (например, локальному администратору по информационной безопасности, назначенному внутренним приказом по организации).

Дистрибутивы ключей необходимы для активации программных продуктов ViPNet (ViPNet Client, ViPNet Coordinator, ViPNet Policy 1 Manager и т. д.) на сетевых узлах защищенной сети.

Если на сетевом узле зарегистрировано несколько пользователей, то для каждого из них будет сформирован свой дистрибутив.

Для выдачи дистрибутивов ключей выполните следующие действия:

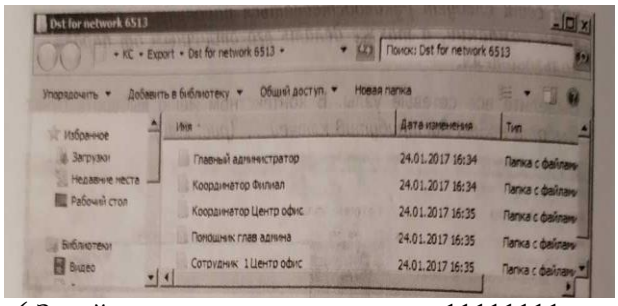
✓ В окне программы ViPNet Удостоверяющий и ключевой центр на панели навигации выберите представление Ключевой центр и перейдите в раздел Моя сеть → Сетевые узлы.

✓ Задайте пароль администратора для всех созданных сетевых узлов.

Для этого двойным щелчком откройте Свойства сетевого узла, перейдите на вкладку Пароль администратора, нажмите кнопку Создать пароль... → Тип пароля: Собственный → Пароль: 11111111

Внимание! При создании паролей администраторов в реальной сети следует руководствоваться парольными политиками компании, а также делать его отличным от пароля пользователя.

✓ Выделите все сетевые узлы. В контекстном меню выберите пункт Выдать новый дистрибутив ключей...



✓ Задайте пароль пользователя — 11111111 по очереди для каждого пользователя защищенной сети.

После окончания выдачи дистрибутива откроется окно проводника с папкой, содержащей подкаталоги сетевых узлов с готовыми дистрибутивами. Запомните путь до этой папки или измените папку, используемую по умолчанию для сохранения дистрибутивов на собственную (Сервис → Настройка… → Дистрибутивы ключей). Путь до папки с дистрибутивами ключей понадобиться в дальнейшем для установки и активации VipNet.

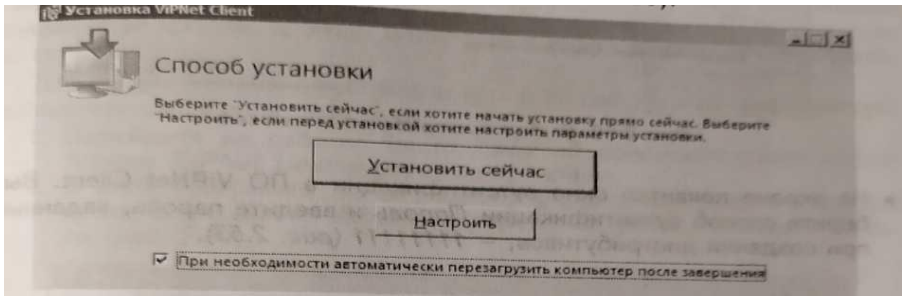
Администратор УКЦ должен доверенным путем (например, с помощью спец- или фельдъегерской связи, отправки на существующий сетевой узел с помощью программы ViPNet Client или лично в руки по доверенности) передать пользователю следующее:

✓ Дистрибутив ключей (dst-файл).
✓ Пароль пользователя.
Вставьте скриншот, подтверждающий выполнение задания

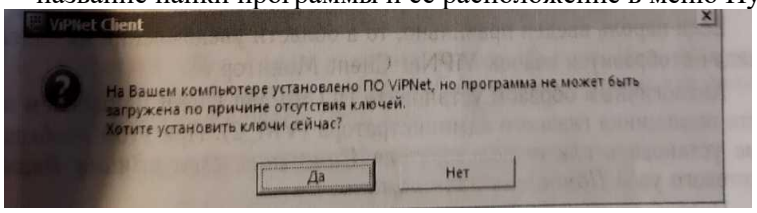
Практическая работа № 5
Развёртывание рабочего места помощника главного администратора защищённой сети ViPNet

Задание:

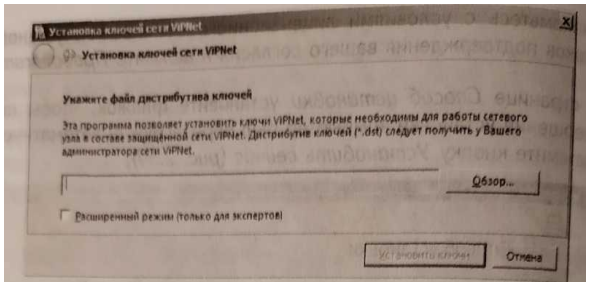
1. На виртуальной машине (VM_1 - рабочее место главного администратора сети), где уже установлен ЦУС и УКЦ, доустановить ViPNet Client и активировать его с помощью dst-файла, выпущенного для СУ Главный администратор.
2. Развернуть на виртуальной машине (VM_2 - рабочее место помощника главного администратора) необходимое ПО - клиентскую часть ViPNet Administrator ЦУС и ViPNet Client, который необходимо активировать с помощью dst-файла, выпущенного для СУ *Помощник глав админа.*
Установка ViPNet Client
Программное обеспечение VipNet Client необходимо установить на VM_1 и VM_2. Для этого выполните следующие действия:
1. На рабочем месте главного администратора сети (VM_1) запустите установочный файл <имя_файла>.exe. Дождитесь завершения подготовки к установке VipNet Client.
2. Ознакомьтесь с условиями лицензионного соглашения, установите флажок подтверждения вашего согласия и нажмите Продолжить.



На странице Способ установки установите флажок, чтобы после завершения установки компьютер был перезагружен автоматически, и нажмите кнопку Установить сейчас.
3. Если потребуется настроить параметры установки, то на странице Способ установки нажмите кнопку Настроить и укажите:
✓ путь к папке установки программы на компьютере;
✓ имя пользователя и название организации;
✓ название папки программы и ее расположение в меню Пуск.

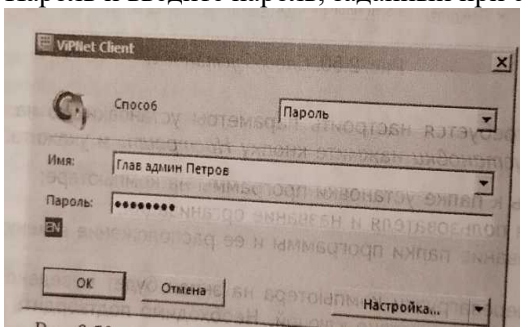


4. После перезагрузки компьютера на экран будет выведено диалоговое окно об отсутствие ключей. Необходимо подтвердить установку ключей.
5. На странице Установка ключей сети VipNet укажите файл дистрибутива ключей *.dst для пользователя Глав админ Петров сетевого узла Главный администратор и нажмите кнопку Установить ключи. Дистрибутивы ключей были созданы при выполнении предыдущих заданий.



По завершении процедуры установки ключей нажмите Закрыть.

6. На экране появится окно аутентификации в ПО ViPNet Client. Выберите способ аутентификации Пароль и введите пароль, заданный при создании дистрибутивов, - 11111111



Вставьте скриншот, подтверждающий выполнение задания

Если пароль введен правильно, то в области уведомлений на панели задач отобразится значок VipNet Client Монитор.

Аналогичным образом установите ПО VippNet Client на рабочем месте помощника главного администратора (VM_2). При этом необходимо установить ключи пользователя Помощник глав администратора Иванов сетевого узла Помощник глав администратора.

Проверьте связанность узлов для этого на рабочем месте помощника главного администратора (VM_2) необходимо войти в VipNet Client Монитор и в разделе Защищённая сеть выделить узел Главный администратор и нажать F5 — узел должен иметь статус Доступен.

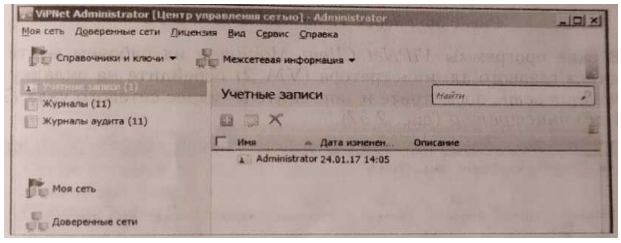
Примечание. После установки и успешной аутентификации в VipNet Client, появиться диалоговое окно Установка корневого сертификата. Это связано с тем, что при формировании dst-файла для данного пользователя была создана ЭП, так как в настройках для созданных узлов по умолчанию устанавливается флажок Создавать ключи электронной подписи.

Установка и настройка клиентского приложения ЦУС на рабочем месте помощника главного администратора сети

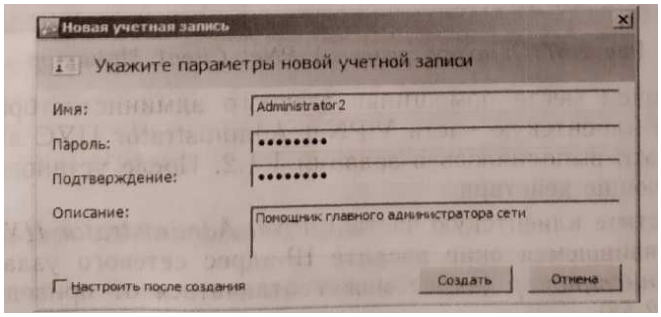
Для того чтобы дать возможность помощнику главного администратора управлять через дополнительное рабочее место ЦУС конфигурацией защищённой сети, необходимо создать учётную запись помощника главного администратора в ЦУС (на VM_1) и установить клиентского приложение ЦУС на рабочем месте помощника главного администратора сети (VM_2).

Для создания учетной записи помощника главного администратора, выполните следующие действия:

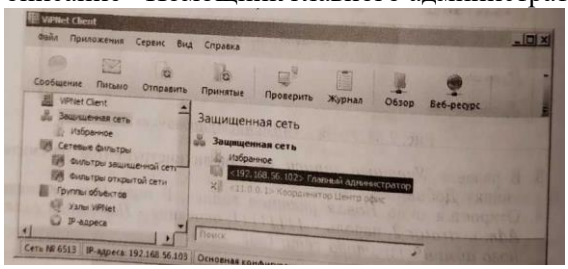
1. Перейдите на рабочее место Главный администратор в программе VipNet Центр управления сетью.



2. В окне программы VipNet Центр управления сетью выберите пункт меню Вид → Администрирование, раздел Учётные записи.



3. В разделе Учетные записи на панели инструментов нажмите кнопку Добавить.
4. Откроется окно Новая учетная запись. В поле Имя укажите Administrator 2, пароль - 11111111, описание - Помощник главного администратора сети.

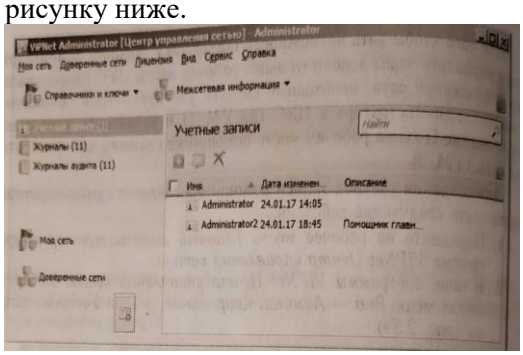


Вставьте скриншот, подтверждающий выполнение задания

Практическая работа № 6
Настройка рабочего места помощника главного администратора защищённой сети ViPNet

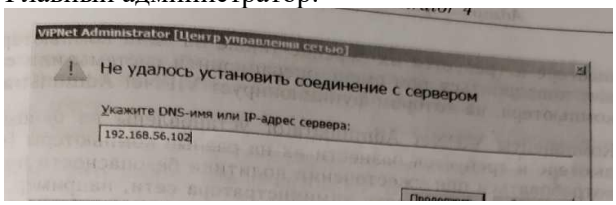
Задание:

После создания помощника главного администратора раздел Учётные записи примет вид согласно рисунку ниже.



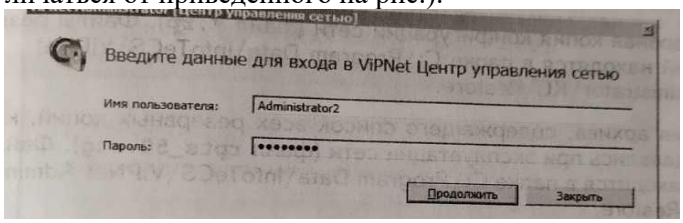
Вставьте скриншот, подтверждающий выполнение задания

В окне программы VipNet Client Монитор на рабочем месте помощника главного администратора (VM_2) перейдите на вкладку Защищённая сеть, посмотрите и запомните IP-адрес сетевого узла Главный администратор.



На рабочем месте помощника главного администратора (VM_2) установите клиентскую часть VipNet Administrator ЦУС аналогично тому, как это выполнялось в предыдущих заданиях. После установки выполните следующие действия:
1. Запустите клиентскую часть VipNet Administrator ЦУС.

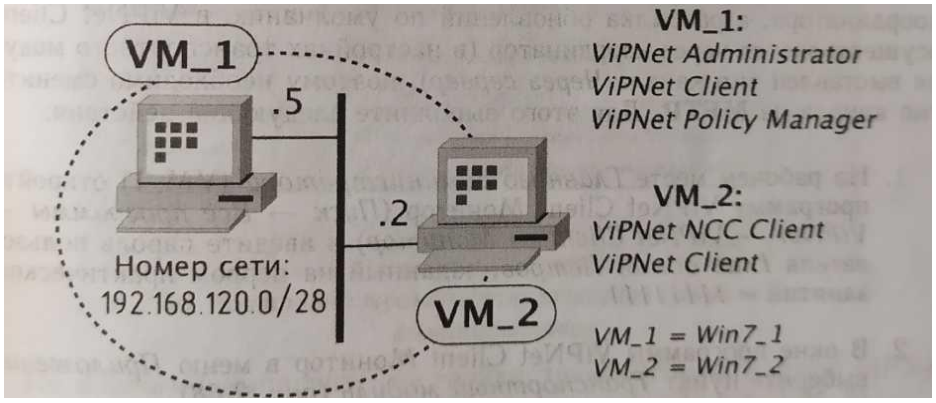
2. В появившемся окне введите IP-адрес сетевого узла Главный администратор (адрес может отличаться от приведенного на рис.).



3. Если связь с сервером установилась, то появится окно для ввода имени пользователя и пароля для входа. Введите имя пользователя — Administrator2, пароль — 11111111.
4. После успешного подключения клиентской части ЦУС, расположенной на рабочем месте помощника главного администратора будет выведено диалоговое окно, в котором необходимо задать новый пароль. Введите старый пароль 11111111, новый пароль - 11111111.
Таким образом, теперь управлять защищенной сетью ViPNet можно двух рабочих мест.
Вставьте скриншот, подтверждающий выполнение задания

Практическая работа № 7
Модификация защищённой сети ViPNet

Задание:



Для выполнения практического задания потребуется две виртуальные машины VM_1 (Главный администратор) и VM 2 (Помощник главного администратора). В предыдущем практическом занятии они были уже настроены, но лучше еще раз убедитесь в корректности сетевых настроек, а также ПО ViPNet.
Настройка программного обеспечения ViPNet
Для обеспечения более быстрого прохождения обновлений на клиентах при выполнений настоящего практического задания необходимо настроить *Транспортный модуль,* обеспечивающий обмен служебными конвертами. Так как на данном этапе в сети нет развернутого координатора, а рассылка обновлений по умолчанию в ViPNet Client осуществляется через координатор (в настройках транспортного модуля выставлен тип канала *Через сервер)*, поэтому необходимо сменить тип канала на MFTP. Для этого выполните следующие действия:
На рабочем месте Главного администратора (VM_1) откройте программу ViPNet Client Монитор (Пуск → Все программы → VipNet → ViPNet Client → Монитор) и введите пароль пользователя Глав админ Петров, заданный на первом практическом занятии — 11111111.
В окне программы ViPNet Client Монитор в меню Приложения выберите пункт Транспортный модуль.

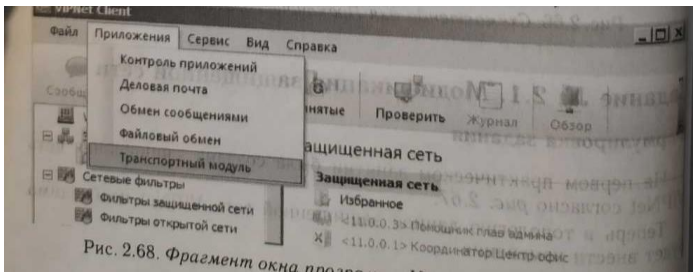
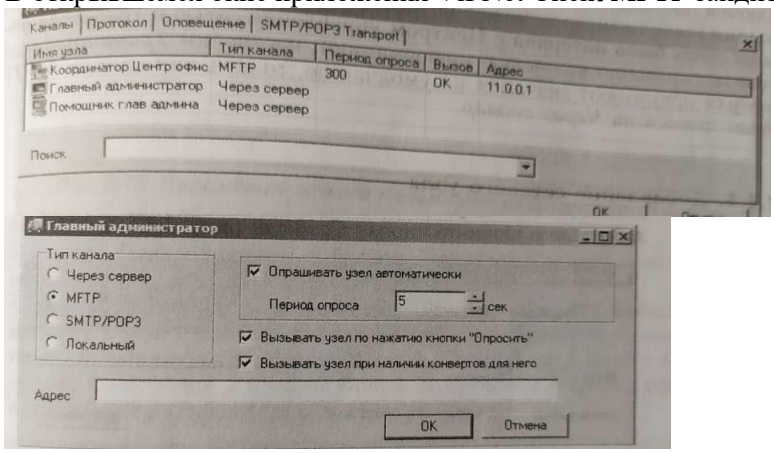


Рис. 2.68. *Фрагмент окна продукта*

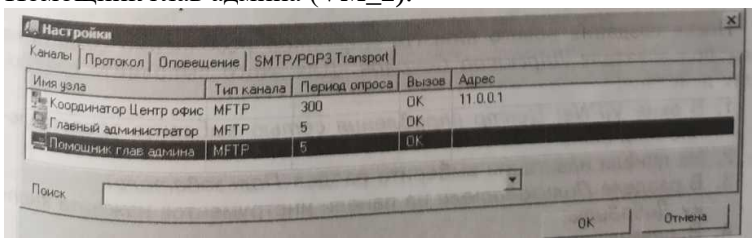
В открывшемся окне приложения ViPNet Client MFTP зайдите в пункт меню Настройки



Дважды щелкните левой кнопкой мыши сперва на узел Главный администратор, выберите тип канала MFTP, установите период опроса равным 5 секунд, установите флажок напротив строки Вызывать узел по нажатию кнопки «Опросить» и нажмите кнопку ОК. Затем отройте свойства узла Помощник глав админа и выставьте такие же настройки.

Вставьте скриншот, подтверждающий выполнение задания

По аналогии выполните настройки транспортного модуля VipNet Client MFTP на рабочем месте Помощник глав админа (VM_2).



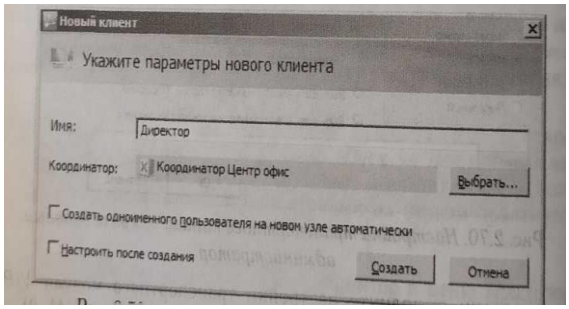
Стоит обратить внимание, на то что после повторной установки ключей посредством мастера установки ключей локально на каждой из машин (такое действие может потребоваться при выполнении задания, если связь была потеряна с Центром управления сетью и требуется обновить справочно-ключевую информацию), настройки Транспортного модуля принимают значения по умолчанию, то есть тип канала MFTP будет сменён на Через сервер.

Вставьте скриншот, подтверждающий выполнение задания

Добавление сетевого узла

Для добавления нового клиента Директор перейдите на рабочее место Главный администратор и выполните следующие действия:

1. В окне ViPNet Центр управления сетью выберите представление Моя сеть.
2. На панели навигации выберите раздел Клиенты.
3. В разделе Клиенты на панели инструментов нажмите Добавить,

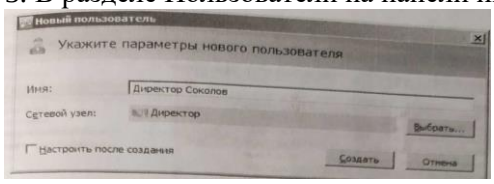


4. В появившемся окне задайте имя Директор, выберите координатор Координатор Центр офис для регистрации на нем создаваемого клиента, уберите флажок Создать одноименного пользователя и нажмите кнопку Создать.

Вставьте скриншот, подтверждающий выполнение задания

После создания нового клиента Директор необходимо создать на нём пользователя Директор Соколов. Для этого выполните следующие действия:

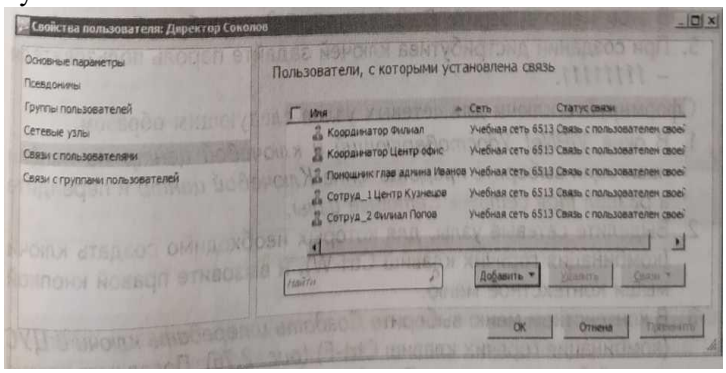
1. В окне ViPNet Центр управления сетью выберите представление Моя сеть.
2. На панели навигации выберите раздел Пользователи.
3. В разделе Пользователи на панели инструментов нажмите кнопку Добавить.



4. В появившемся окне задайте имя пользователя Директор Соколов, выберите сетевой узел Директор и нажмите кнопку Создать.

Установите связи пользователя Директор Соколов с пользователями Помощник глав админа Иванов, Сотрудник_1 Центр Кузнецов, Сотрудник_2 Филиал Попов, Координатор Центр офис, Координатор Филиал (связь между пользователями обеспечивает возможность ведения конфиденциальной переписки в программе VipNet Client Деловая почта между этими пользователями). Для этого:

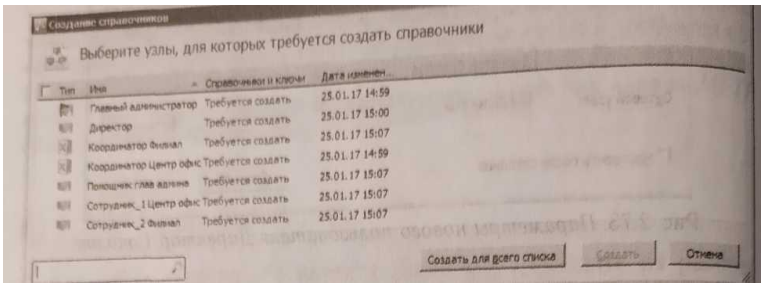
1. В окне ViPNet Центр управления сетью выберите представление Моя сеть.
2. На панели навигации выберите раздел Пользователи.
3. В списке Пользователей выберите Директор Соколов и на панели инструментов нажмите кнопку Свойства.



В окне Свойства пользователя: Директор Соколов выберите вкладку Связи с пользователями и добавьте связи с пользователями Помощник глав админа Иванов, Сотрудник Центр Кузнецов, Сотрудник_2 Филиал Попов, Координатор Центр офис, Координатор Филиал.

Сформируйте справочники следующим образом:

В окне VipNet Центр управления сетью нажмите кнопку Справочники и ключи → Создать справочники… и в открывшемся окне нажмите кнопку Создать для всего списка

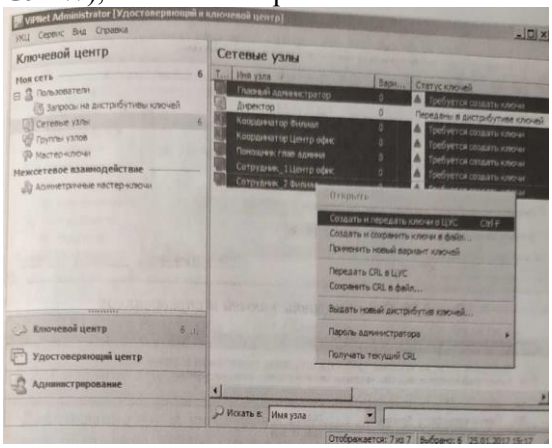


После формирования справочников в программе ViPNet УКЦ необходимо выдать дистрибутив ключей для сетевого узла Директор и ключи для сетевых узлов, которых коснулись изменения в ЦУС: Главный администратор, Помощник глав админа Иванов, Сотрудник_1 Центр Кузнецов, Сотру дник_2 Филиал Попов, Координатор Центр офис, Координатор Филиал.

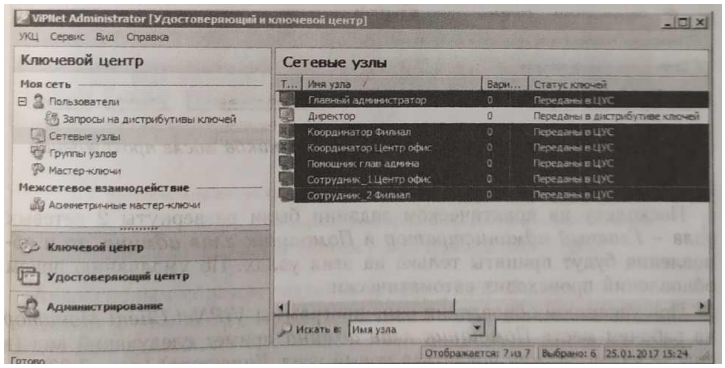
Вставьте скриншот, подтверждающий выполнение задания

Выдайте дистрибутив ключей для пользователя Директор Соколов следующим образом:
1. В окне ViPNet Удостоверяющий и ключевой центр на панели навигации выберите представление Ключевой центр и перейдите в раздел Моя сеть Сетевые узлы.
2. Задайте пароль администратора для сетевого узла Директор.
3. Выделите сетевой узел Директор и вызовите правой кнопкой мыши контекстное меню.
4. В этом меню выберите Выдать новый дистрибутив ключей.
5. При создании дистрибутива ключей задайте пароль пользователя — 11111111.
Вставьте скриншот, подтверждающий выполнение задания

Сформируйте ключи для сетевых узлов следующим образом:
1. В окне VipNet Удостоверяющий и ключевой центр на панели навигации выберите представление Ключевой центр и перейдите в раздел Моя сеть → Сетевые узлы.
2. Выделите сетевые узлы, для которых необходимо создать ключи (комбинация горячих клавиш Ctrl-W), и вызовите правой кнопкой мыши контекстное меню.



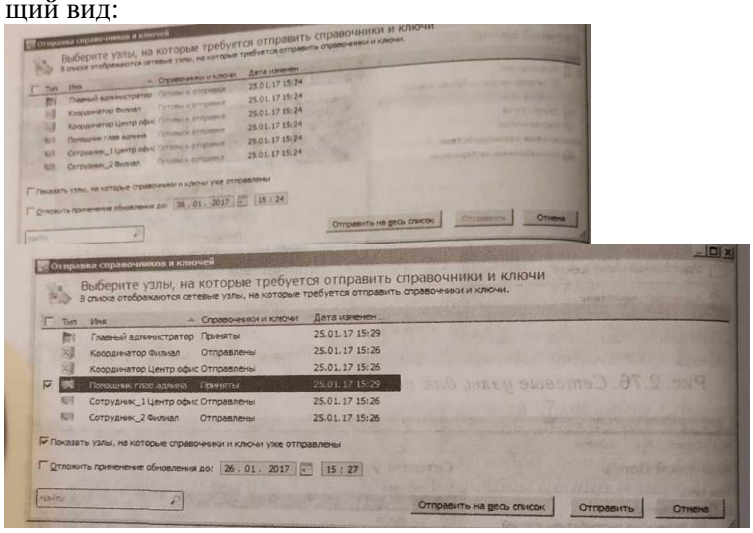
3. В контекстном меню выберите Создать и передать ключи в ЦУС (комбинация горячих клавиш Ctrl-F). после чего статус ключей будет сменён на Переданы в ЦУС



Для отправки ключей на узлы в окне VipNet Центр управления сетью нажмите кнопку Справочники и ключи → Отправить справочники и ключи… и в открывшемся окне нажмите кнопку Отправить на весь список.

Чтобы проверить процесс прохождения обновлений в окне ViPNet Центр управления сетью нажмите кнопку Справочники и ключи → Отправить справочники и ключи. ..и в открывшемся окне установите флажок Показать узлы, на которые справочники и ключи уже отправлены (из данного меню можно повторно отправлять).

Пои успешном прохождении обновлений окно Отправка справочников и ключей примет следующий вид:



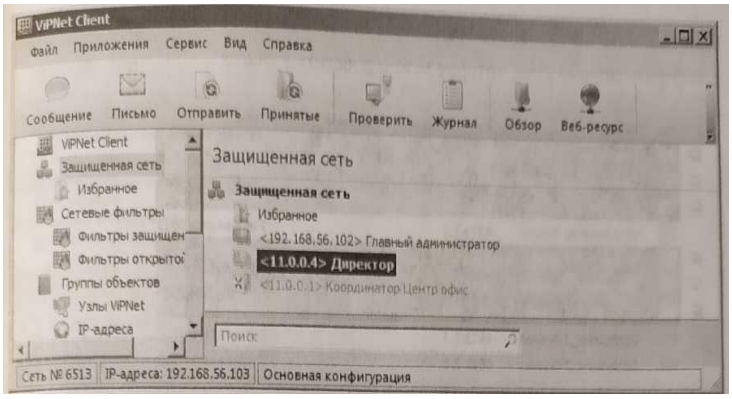
Поскольку на практическом задании были развернуты 2 сетевых узла — Главный администратор и Помощник глав админа, то и обновления будут приняты только на этих узлах. По умолчанию прием обновлений происходит автоматически.

При успешном обновлении окна программы VipNet Client Монитор на рабочем месте Помощник глав админа примет следующий вид (в списке узлов должен появиться новый узел Директор).

Далее необходимо создать ещё пару новых сетевых узлов — клиент Бухгалтер с пользователем Бухгалтер Прохорова (для данного пользователя также потребуется установить связь с пользователями Директор Соколов, Помощник глав админа и Сотрудник_1 Центр Кузнецов) в центральном офисе компании, клиент Сотрудник_3 Филиал с пользователем Сотруд_3 Филиал Горохов (для данного пользователя также потребуется установить связь с пользователем Сотрудник_2 Филиал Попов) в филиале компании.

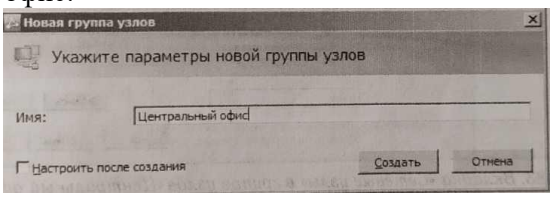
Сформировать справочники и ключи, разослать их на узлы.

Вставьте скриншот, подтверждающий выполнение задания



Создание групп узлов

Для создания групп узлов Центральный офис и Филиал в разделе Группы узлов окна ViPNet Центр управления сетью нажмите кнопку Создать новую группу узлов и задайте имя Центральный офис.



Аналогичным образом создайте группу узлов Филиал.

Добавьте узлы в группу Центральный офис. Для этого выполните следующие действия:

В разделе Группы узлов окна VipNet Центр управления сетью выделите группу узлов Центральный офис и нажмите кнопку Свойства группы узлов.

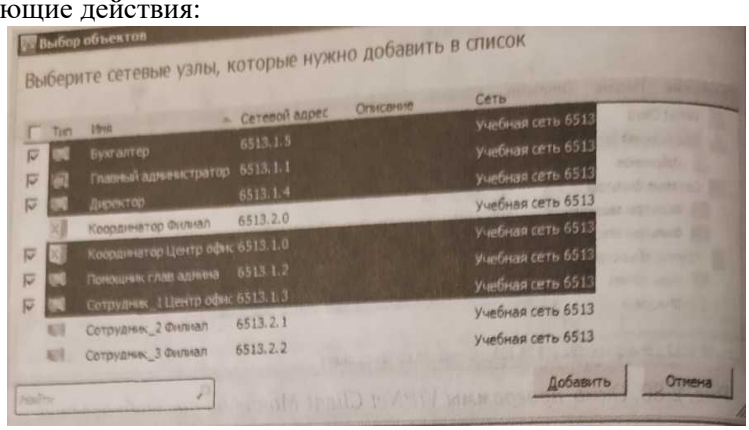
Перейдите на вкладку Сетевые узлы и добавьте узлы Координатор Центр офис, Директор, Главный администратор, Помощник глав админа, Сотрудник_1 Центр офис, Бухгалтер

В результате вкладка Сетевые узлы примет вид:

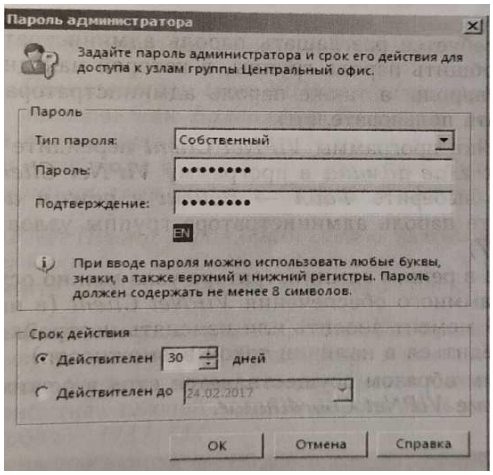
Вставьте скриншот, подтверждающий выполнение задания

Аналогичным образом добавьте узлы Координатор Филиал, Сотрудник_2 Филиал, Сотрудник_3 Филиал в группу узлов Филиал.

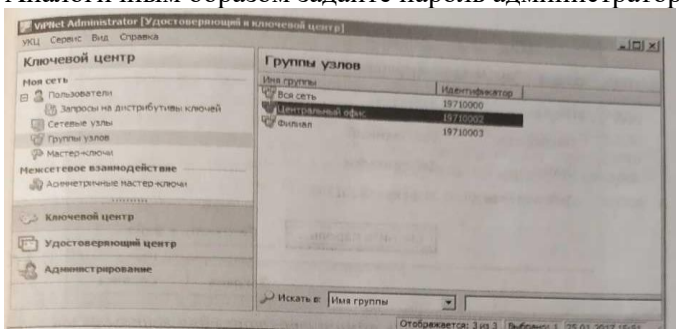
Задайте пароль администратора для группы узлов Центральный офис. Для этого выполните следующие действия:



1. Перейдите в раздел Группы узлов окна VipNet Удостоверяющий и ключевой центр.
2. Дважды щелкните группу Центральный офис.
3. В открывшемся окне перейдите на вкладку Пароль администратора и нажмите кнопку Создать.
4. Задайте пароль — 22222222 и нажмите ОК.



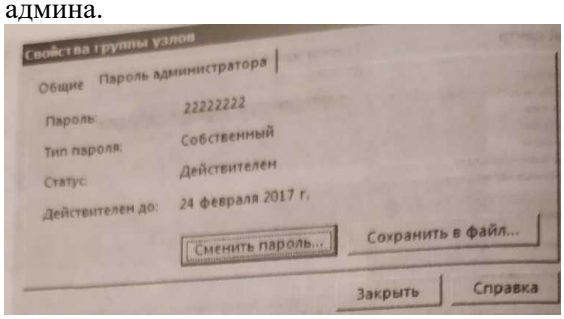
Созданный пароль отобразится на вкладке Пароль администратора.
Аналогичным образом задайте пароль администратора для группы узлов Филиал — 33333333.



Отправьте обновления ключей на узлы следующим образом:

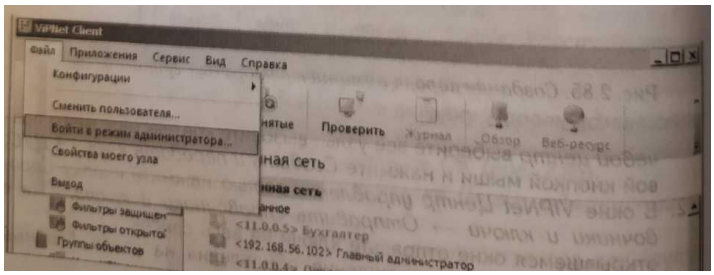
Вставьте скриншот, подтверждающий выполнение задания

1. В разделе Сетевые узлы окна VipNet Удостоверяющий и ключевой центр выберите все узлы, вызовите контекстном меню правой кнопкой мыши и нажмите Создать и предать ключи в ЦУС.
2. В окне VipNet Центр управления сетью нажмите кнопку Справочники и ключи → Отправить спровчники и ключи… и в открывшемся окне отправьте ключи на веь список.
3. Проконтролируйте прохождение обновления на узлах Главный адмнистратор, Помощник глав админа.



Теперь для выполнения настроек узлов Центрального офиса и Филиала не потребуется разглашать пароль администратора всей сети, достаточно сообщить пароль группы, в которой находится требуемый узел (данный пароль, а также пароль администратора сетевого узла нельзя сообщать пользователям).
Для настройки программы ViPNet Client перейдите на рабочее м сто Помощник глав админа в программу ViPNet Client Монитор. В верхнем меню выберите Файл → Войти в режим администратора... и введите пароль администратора группы узлов Центральный офис.
После входа в режим администратора узла можно осуществлять настройку программного обеспечения ViPNet Client (в настоящем задании на данный момент вносить или изменять настройки не требуется, достаточно убедиться в наличии такой возможности).

Аналогичным образом осуществляется вход в режиме администратора в программе VipNet Coordinator.



Примечание. В случае если по установленным в организации правилам нельзя разглашать пароль администратора группы и нет возможности администратору группы присутствоавать в удаленных офисах, но требуется обеспечить возможность производить настройки программы VipNet Client/Coordinator, нужно задать пароль администратора для каждого сетевого узла. Для этого необходимо кликнуть на узел и задать пароль на вкладке Пароль администратора.

Вставьте скриншот, подтверждающий выполнение задания

Добавление нового пользователя

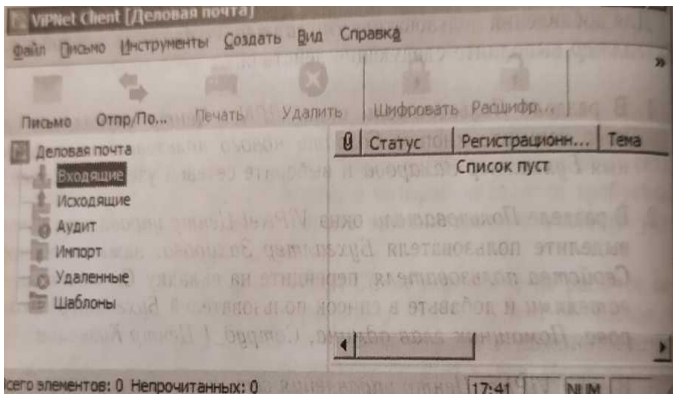
Для добавлений пользователя Бухгалтер Захарова на сетевой узел Бухгалтер выполните следующие действия:

1. В разделе Пользователи окна ViPNet Центр управления сетью нажмите кнопку Создать нового пользователя, задайте имя Бухгалтер Захарова и выберите сетевой узел Бухгалтер.
2. В разделе Пользователи окна ViPNet Центр управления сетью выделите пользователя Бухгалтер Захарова, нажмите кнопку Свойства пользователя, перейдите на вкладку Связи с пользователями и добавьте в список пользователей Бухгалтер Прохорова, Помощник глав админа, Сотруд_1 Центр Кузнецов.
3. В окне ViPNet Центр управления сетью нажмите кнопку Справочники и ключи → Создать справочники... и в открывшемся окне нажмите кнопку Создать для всего списка.
4. В разделе Сетевые узлы окна ViPNet Удостоверяющий и ключевой центр выделите узел Бухгалтер, в контекстном меню выберите пункт Выдать новый дистрибутив ключей. При создании дистрибутива ключей задайте пароль пользователя Бухгалтер Захарова - 11111111
5. Передайте доверенным способом дистрибутив ключей и пароль пользователю Бухгалтер Захарова (в рамках настоящего задания передавать дистрибутив ключей никуда не нужно).
6. В разделе Сетевые узлы окна ViPNet Удостоверяющий и ключевой центр выберите узлы, для которых требуется создать ключи, в контекстном меню выберите пункт Создать и передать ключи в ЦУС.
7. В окне ViPNet Центр управления сетью нажмите кнопку Справочники и ключи → Отправить справочники и ключи... и в открывшемся окне отправьте ключи на весь список.
8. Проконтролируйте прохождение обновления на узлах Главный администратор, Помощник глав админа.

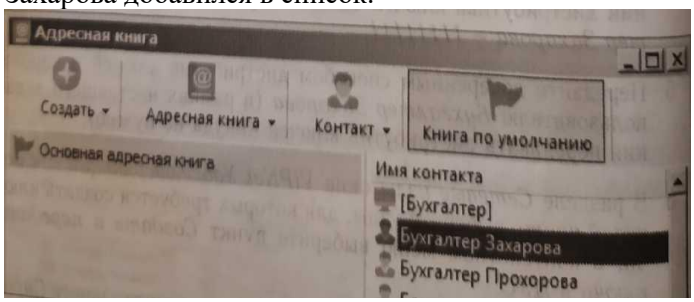
Вставьте скриншот, подтверждающий выполнение задания

В результате правильного выполнения задания в списке адресатов в программе VipNet Client Деловая почта на рабочем месте Помощник глав админа будет добавлен пользователь Бухгалтер Захарова. Чтобы это проверить, выполните следующие действия:

Откройте программу VipNet Client Деловая почта на рабочем месте Помощник глав админа (Пуск → Все программы → VipNet → VipNet Client → Деловая почта).



В меню Инструменты выберите пункт Адресная книга… и убедитесь, что пользователь Бухгалтер Захарова добавился в список.



Вставьте скриншот, подтверждающий выполнение задания

Удаление связей пользователей

Для удаления связи пользователей Бухгалтер Захарова и Помощник глав админа Иванов выполните следующие действия:

1. . В разделе Пользователи Окна ViPNet Центр управления сетью выделите пользователя Бухгалтер Захарова, нажмите кнопку Свойства пользователя.
2. Перейдите на вкладку Связи с пользователями, в списке пользователей отметьте Помощник глав админа Иванов и нажмите кнопку Удалить.
3. В окне ViPNet Центр управления сетью нажмите кнопку Справочники и ключи → Создать справочники…и в открывшемся окне нажмите кнопку Создать для всего списка.
4. В разделе Сетевые узлы окна ViPNet Удостоверяющий и ключевой центр выберите узлы, для которых требуется создать ключи, в контекстном меню выберите пункт Создать и передать ключи в ЦУС.
5. В окне ViPNet Центр управления сетью нажмите кнопку Справочники и ключи → Отправить справочники и ключи... и в открывшемся окне отправьте ключи на весь список.
6. Проконтролируйте прохождение обновления на узле Помощник глав админа.

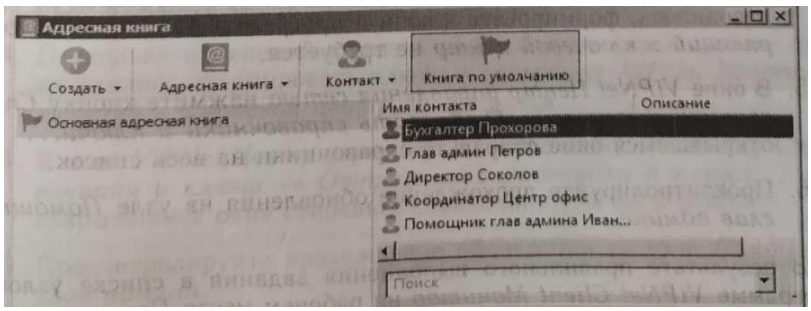
Если задание выполнено правильно, то из списка адресатов в программе ViPNet Client Деловая почта с рабочего места Помощник глав админа будет удален пользователь Бухгалтер Захарова.

Вставьте скриншот, подтверждающий выполнение задания

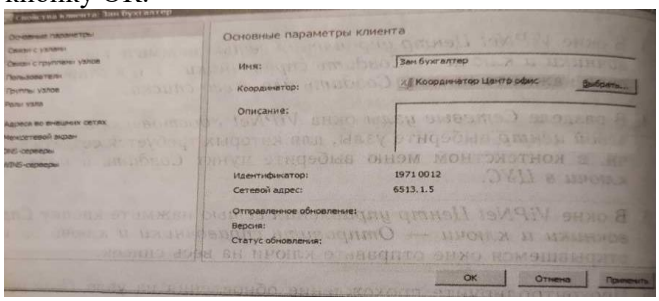
Изменение названия сетевого узла

Для изменения названия сетевого узла Бухгалтер на Зам бухгалтера выполните следующие действия:

В окне VipNet Центр управления сетью выберите раздел Клиенты, выделите узел Бухгалтер и нажмите кнопку Свойства клиента.



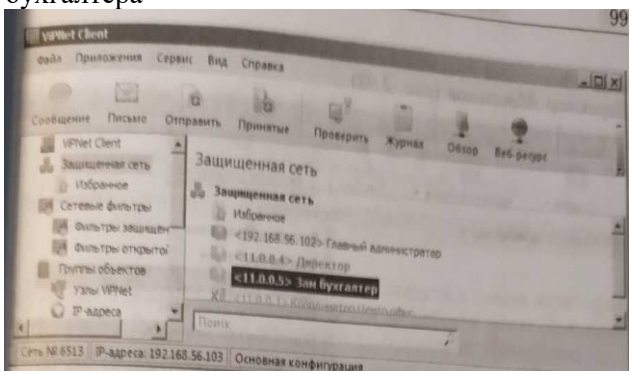
В свойствах клиента Бухглатер измените название сетевого узла на Зам бухгалтера и нажмите кнопку ОК.



В окне VipNet Центр управления сетью нажмите кнопку Справочники и ключи → Создать справочники… и в открывшемся окне нажмите кнопку Создать для всего списка.
Поскольку изменений в связях узлов или пользователей не производилось, формировать ключи в программе VipNet Удостоверяющий и ключевой центр не требуется.

В окне VipNet Центр управления сетью нажмите кнопку Справочники и ключи → Отправить справочники и ключи… и в открывшемся окне отправьте справочники на весь список.
Проконтролируйте прохождение обновления на узле Помощник глав администратора.
Вставьте скриншот, подтверждающий выполнение задания

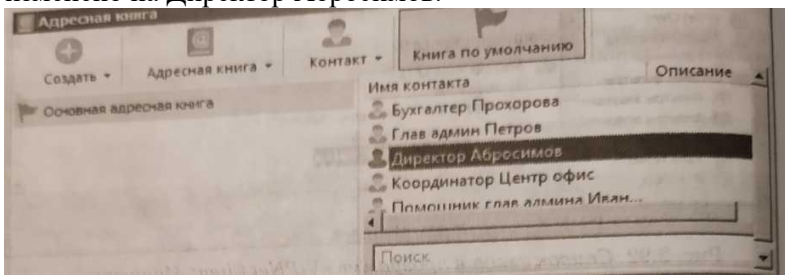
В результате правильного выполнения задания в списке узлов в программе VipNet Client Монитор на рабочем месте Помощник глав администратора название сетевого узла Бухгалтер будет изменено на Зам бухгалтера



Вставьте скриншот, подтверждающий выполнение задания

Изменение имени пользователя
Для изменения имени пользователя Директор Соколов на Директор Абросимов выполните следующие действия:
1. В окне ViPNet Центр управления сетью выберите раздел Пользователи, выделите пользователя Директор Соколов и нажмите кнопку Свойства пользователя.
2. В свойствах пользователя Директор Соколов измените имя на Директор Абросимов и нажмите кнопку ОК. Появится диалоговое окно, в котором будет сообщаться, что данный пользователь единственный на данном узле и вам нужно выбрать переименовывать узел или нет. В данной ситуации переименование узла не требуется, поэтому нажмите кнопку Нет.
3. В окне ViPNet Центр управления сетью нажмите кнопку Справочники и ключи → Создать справочники… и в открывшемся к окне нажмите кнопку Создать для всего списка.

4. Поскольку изменений в связях узлов или пользователей не производилось, формировать ключи в программе ViPNet Удостоверяющий и ключевой центр не требуется.
5. В окне ViPNet Центр управления сетью нажмите кнопку Справочники и ключи → Отправить справочники и ключи… и в открывшемся окне отправьте справочники на весь список.
6. Проконтролируйте прохождение обновления на узле Помощник глав админа.
В результате правильного выполнения задания в адресной книге в программе ViPNet Client Деловая почта на рабочем месте Помощник глав админа имя пользователя Директор Соколов будет изменено на Директор Абросимов.

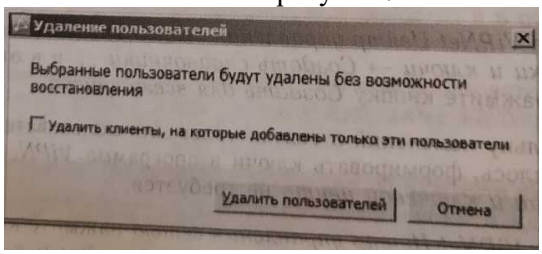


Вставьте скриншот, подтверждающий выполнение задания

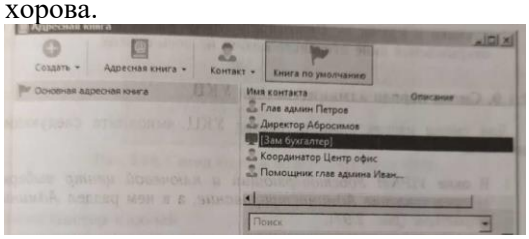
Аналогичным образом переименуйте пользователя Бухгалтер Захарова в Зам бухгалтера Захарова, так как в предыдущем задании имя ее узла было изменено.

Вставьте скриншот, подтверждающий выполнение задания

Удаление пользователя
Для удаления пользователя *Бухгалтер Прохорова* выполните следующие действия:
1. В разделе *Пользователи* окна *ViPNet Центр управления сетью* выберите пользователя *Бухгалтер Прохорова* и нажмите кнопку *Удалить.* При этом удалять клиента, на котором зарегистрирован пользователь не требуется.



2. В окне VipNet Центр управления сетью нажмите кнопку Справочники и ключи → Создать справочники … и в открывшемся окне нажмите кнопку Создать для всего списка.
3. В разделе Сетевые узлы окна VipNet Удостоверяющий и ключевой центр выберите узлы, для которых требуется создать ключи, в контекстном меню выберите пункт Создать и передать ключи в ЦУС.
4. В окне VipNet Центр управления сетью нажмите кнопку Справочники и ключи → Отправить справочники и ключи… и в открывшемся окне отправьте ключи на весь список.
5. Проконтролируйте прохождение обновления на узле Помощник глав админа.
В результате правильного выполнения задания в списке адресатов в программе VipNet Client Деловая почта на рабочем месте Помощник глав админа будет удалён пользователь Бухгалтер Прохорова.



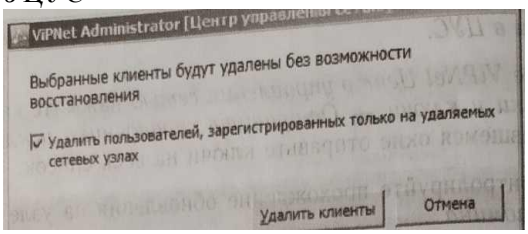
Вставьте скриншот, подтверждающий выполнение задания

Удаление сетевого узла
Для удаления сетевого узла *Сотрудник_3 Филиал* выполните следующие действия:

1. В разделе *Клиенты* окна *ViPNet Центр управления сетью* выделите сетевой узел *Сотрудник_3 Филиал,* нажмите кнопку *Удалить* и установите флажок *Удалить пользователей, зарегистрированных только на удаляемых сетевых узлах* в диалоговом окне

2. В окне *ViPNet Центр управления сетью* нажмите кнопку *Справочники и ключи → Создать справочники,..* и создайте справочники для всех узлов, которые были связаны с клиентом *Сотрудник_3 Филиал.*

3. В разделе *Сетевые узлы* окна *ViPNet Удостоверяющий и ключевой центр* выберите узлы, для которых требуется создать ключи в контекстном меню выберите пункт *Создать и передать ключи в ЦУС*



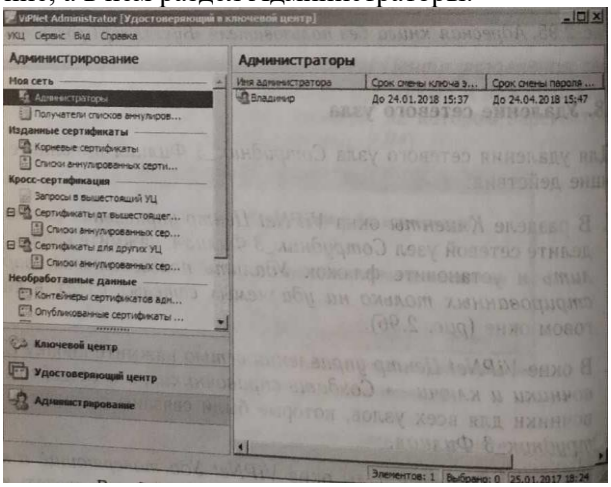
4. В окне ViPNet Центр управления сетью нажмите кнопку Справочники и ключи → Отправить справочники и ключи... и в открывшемся окне отправьте ключи на весь список.

Вставьте скриншот, подтверждающий выполнение задания

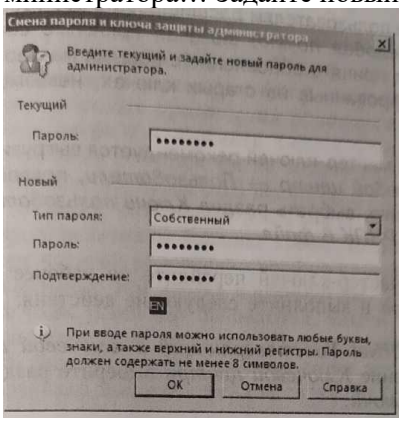
Смена пароля администратора УКЦ

Для смены пароля администратора УКЦ, выполните следующие действия:

1. В окне ViPNet Удостоверяющий и ключевой центр выберите представление Администрирование, а в нем раздел Администраторы.



2. Выделите администратора Владимир, в контекстном меню выберите пункт Сменить пароль администратора… Задайте новый пароль — 55555555.



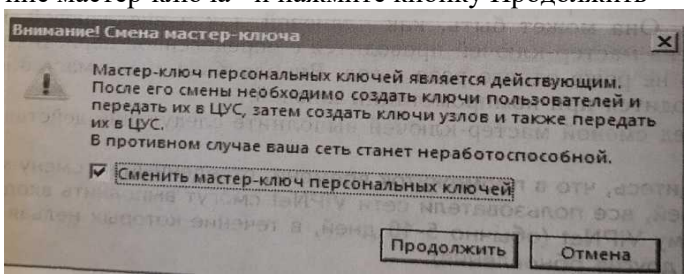
Вставьте скриншот, подтверждающий выполнение задания

Смена мастер-ключей

Смена мастер-ключей влечет за собой смену всех ключей в сети ViPNet. Она может быть, как плановой, так и внеплановой. Плановая смена мастер-ключей проводится с определенной периодич-

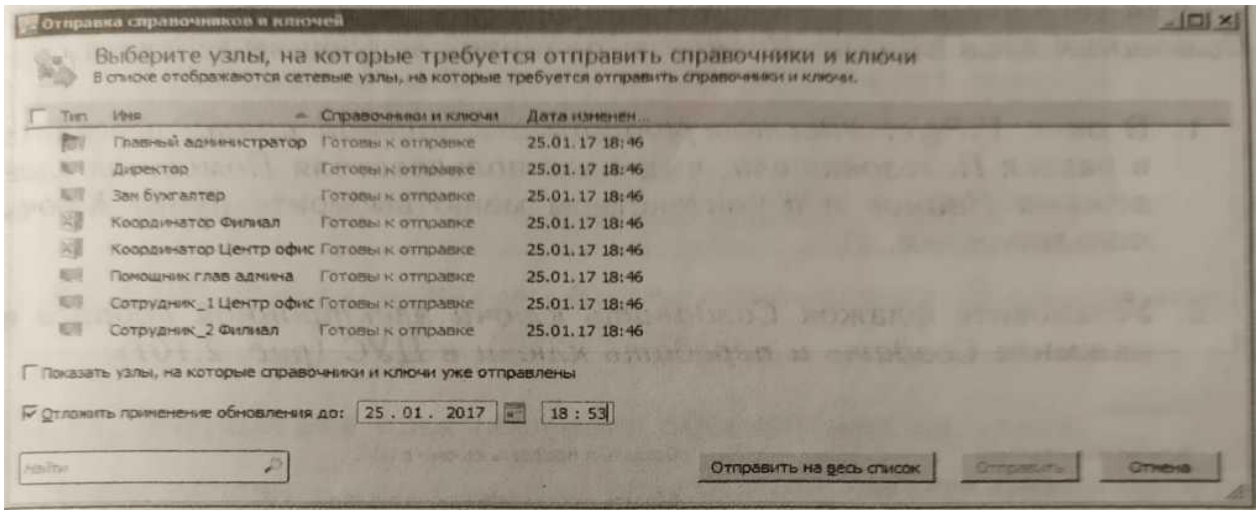
ностью, обычно не реже одного раза в год. Внеплановая смена мастер-ключей производится при компрометации ключей.
Перед сменой мастер-ключей выполните следующие действия:
✓ Убедитесь, что в промежуток времени, отведенный на смену ключей, все пользователи сети ViPNet смогут выполнить вход в программу ViPNet (обычно 5-10 дней, в течение которых нельзя проводить другие обновления).
✓ Убедитесь, что у каждого пользователя на узле имеется резервный набор персональных ключей. Если пользователь зарегистрирован на нескольких узлах, то его резервный набор ключей должен присутствовать на каждом из узлов. Без резервного набора новые ключи на узлах не вступят в действие. Резервный набор перс по умолчанию сохраняется в папке установки ViPNet.
Пример:
C:\Program Files (x 86) \InfoTeCS\ViPNet Client\user_<****>\key_disk\dom*.pk, где **** — идентификатор узла.
✓ Проинформируйте всех пользователей и администраторов сети ViPNet о планируемом обновлении ключей и сроках его проведения.
✓ Рекомендуйте пользователям расшифровать все сообщения программы ViPNet Деловая почта, включая архивные сообщения. После того как будет принято обновление с новыми мастер-ключами, сообщения, зашифрованные на старых ключах, невозможно будет прочитать.
✓ Перед сменой мастер-ключей рекомендуется выгрузить РНПК в файл: УКЦ → Ключевой центр → Пользователи, правой кнопкой мыши по пользователю, выбрать раздел Ключи пользователя → Создать и сохранить РНПК в файл... .
Вставьте скриншот, подтверждающий выполнение задания

Для смены мастер-ключей перейдите на рабочее место Главного администратора и выполните следующие действия:
1. В окне ViPNet Удостоверяющий и ключевой центр выберите представление Ключевой центра выберите раздел Моя сеть → Мастер-ключи.
2. Поочередно в контекстном меню каждого из трех мастер-ключей выберите пункт Сменить.
3. В появившемся окне с сообщением о смене мастер-ключа уста новите флажок Сменить <название мастер-ключа> и нажмите кнопку Продолжить



4. В окне ViPNet Удостоверяющий и Ключевой центр перейдите в раздел Пользователи, выделите всех пользователей, в контекстном меню выберите пункт Ключи пользователя → Создать к передать ключи в ЦУС.
5. В разделе Сетевые узлы, окна ViPNet Удостоверяющий и ключевой центр выберите всё узлы, в контекстном меню выберите пункт Создать и передать ключи в ЦУС.
6. В окне ViPNet Центр управления сетью нажмите кнопку Справочники и ключи → Отправить справочники и ключи...
7. В открывшемся окне, установите флажок Отложить применение обновления до, установите дату и время таким образом, чтобы обновление было применено через 5 минут от текущей даты и времени (обратите внимание, на дату, по умолчанию при активации отложенного применения обновления дата сдвинута на 1 день вперед) и нажмите кнопку Отправить на весь список (в реальной сети при смене мастер-ключей необходимо применять обновлений через 5-10 дней после их отправки, стоит учитывать тот факт; что сетевые узлы могут быть выключены, и если они будут неактивны большее время, то может возникнуть ситуация при которой обновления вообще не дойдут до сетевого узла. Это связано с тем что на координаторе, за которым находятся такие узлы установит обновления, ключи изменяться и те сетевые узлы станут не доступны. Поэтому рекомендуется распланировать рассылку обновлений при смене мастер-ключей так, чтобы не возникло вышеизложенной ситуации.

8. Проконтролируйте доставку обновлений на узлы Главный администратор, Помощник глав администратора.

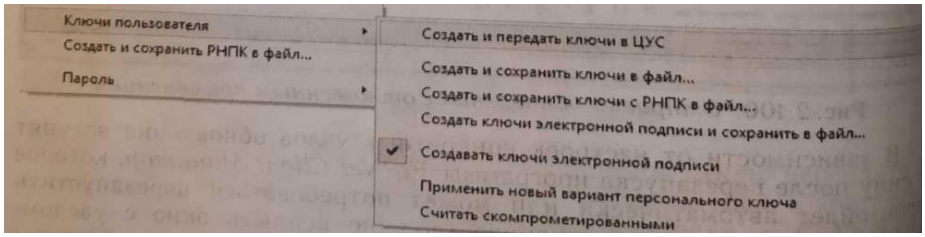


Вставьте скриншот, подтверждающий выполнение задания

В зависимости от настроек конкретных узлов обновления вступят в силу после перезапуска программы *ViPNet Client Монитор,* которое произойдет автоматически или может потребоваться перезапустить *ViPNet Client Монитор* вручную (должно всплыть окно с уведомление о необходимости перезапуска). Во втором случае необходимо будет выполнить следующие действия:
1. На рабочем месте Главного администратора в области уведомлений на панели задач Windows щелкните значок программы ViPNet Client Монитор и в открывшемся окне нажмите Файл → Выход.
2. Теперь откройте программу ViPNet Client Монитор - меню Пуск → Все программы ViPNet → ViPNet Client → Монитор.
Аналогично перезапустить ViPNet Client Монитор на рабочем месте Помощник глав администратора.
После перезагрузки на экран будет выведено сообщение о необходимости указать путь до места расположения резервного набора персональных ключей. Указываете путь до файла резервного набора персональных ключей и вводите пароль пользователя.
После корректного обновления загрузится ViPNet Client Монитор.

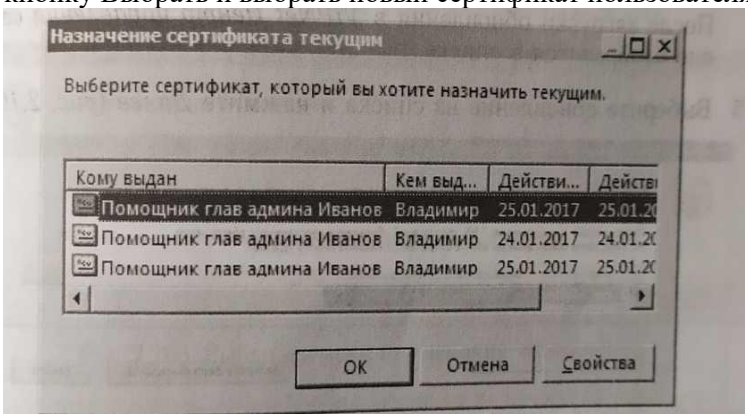
Вставьте скриншот, подтверждающий выполнение задания

Формирование нового сертификата ключа проверки электронной подписи
Если пользователь на сетевом узле по каким-то причинам не смог сделать запрос на сертификат ключа проверки электронной подписи самостоятельно (например, срок действия сертификата закончился), то сформировать новый сертификат и ключ электронной подписи возможно в программе ViPNet *Удостоверяющий и ключевой центр* в промессе создания ключей пользователя.
Для того чтобы сформировать новый сертификат для пользователя Помощник глав администратора Иванов выполните следующие действия:
1. В окне ViPNet Удостоверяющий и ключевой центр перейдите в раздел Пользователи, выделите пользователя Помощник глав администратора Иванов и в контекстном меню выберите пункт Ключи пользователя.



2. Установите флажок Создавать ключи электронной подписи и нажмите Создать и передать ключи в ЦУС.

3. 3. В окне ViPNet Центр управления сетью нажмите кнопку Справочники и ключи → Отправить справочники и ключи…
4. В открывшемся нажмите кнопку Отправить на весь список.
5. Аналогичным образом создать и отправить на весь список ключи узлов.
6. Проконтролируйте применение обновлений на узле Помощник глав админа.
7. На рабочем месте Помощник глав админа в области уведомлений на панели задач Windows щелкните по значку программы ViPNet Client Монитор и в открывшемся окне в меню Сервис выберите пункт Настройка параметров безопасности.
8. В окне Настройка параметров безопасности перейти на вкладку Электронная подпись, нажать кнопку Выбрать и выбрать новый сертификат пользователя Помощник глав админа Иванов.

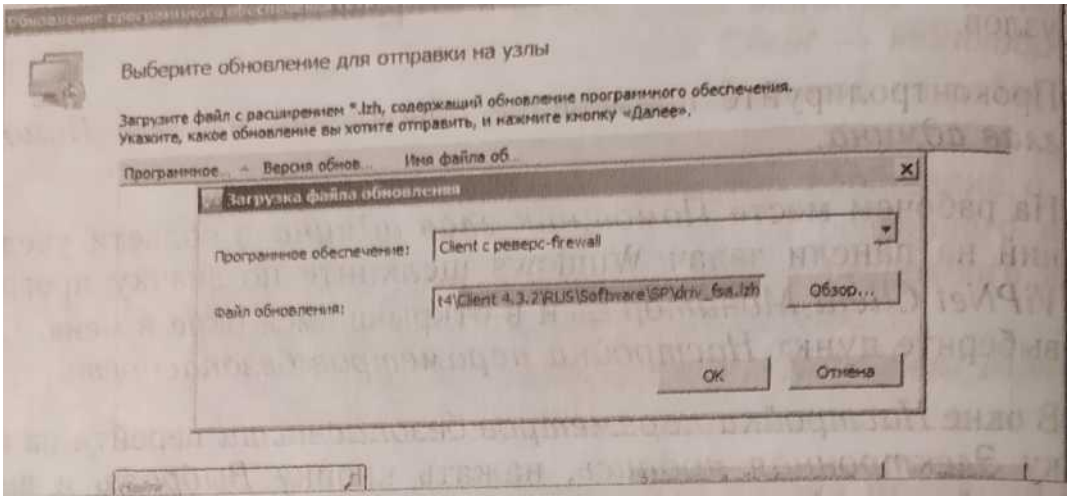


Вставьте скриншот, подтверждающий выполнение задания

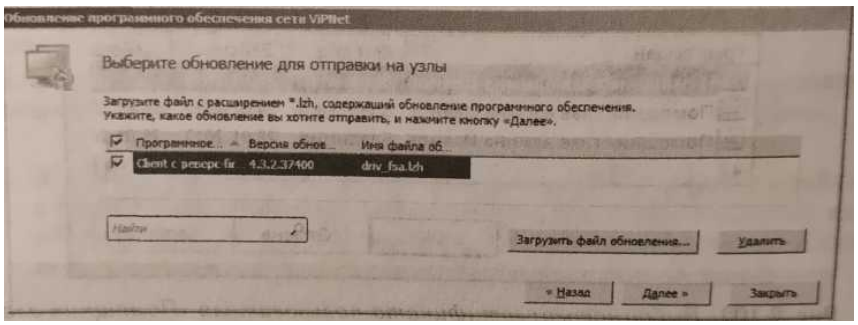
Обновление программного обеспечения на узлах

Чтобы обновить программное обеспечение VipNet Client на узле Помощник глав админа выполните следующие действия:

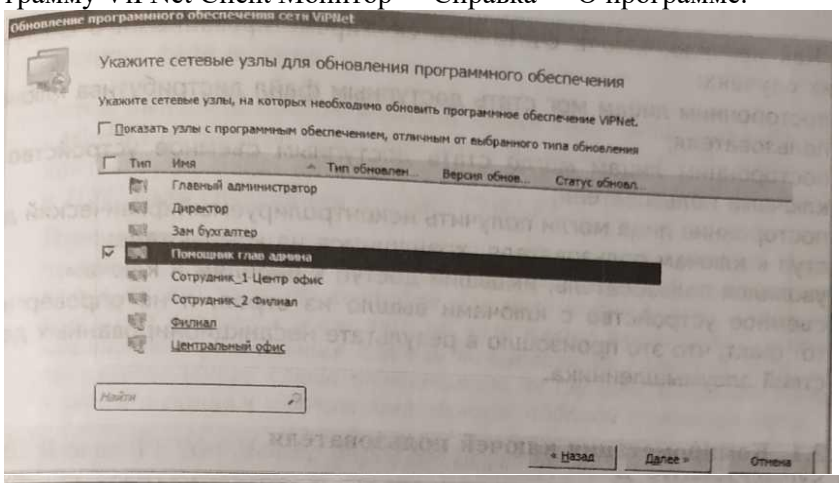
1. В окне VipNet Центр управления сетью в меню Моя сеть выберите пункт Обновить программное обеспечение на узлах.
2. В появившемся окне нажмите кнопку Далее.
3. Нажмите кнопку Загрузить файл обновления → Обзор и выберите файл с обновлением *.lzh. (файл с обновлением в рамках данного практического занятия находится в папке дистрибутивом… \VipNet4\Client|RUS\Software\SP).
4. Нажмите кнопку ОК.После загрузки обновления в *ViPNet Центр управления сетью* оно отобразится в списке.

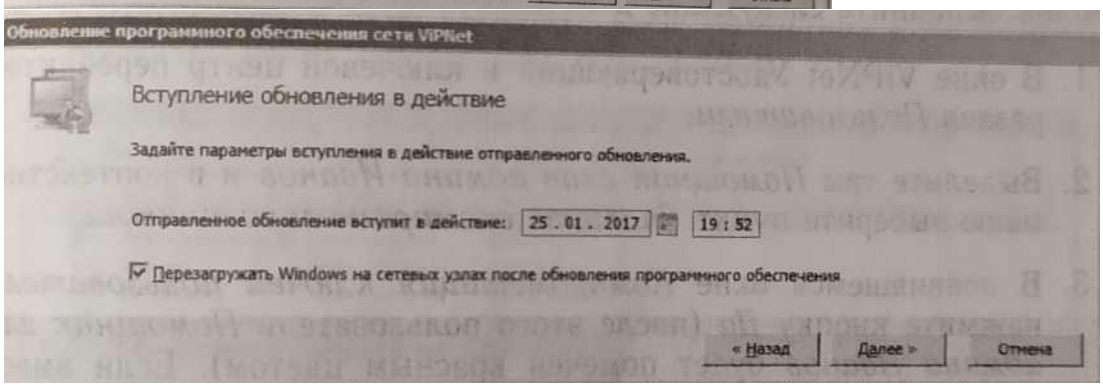


5. Выберите обновление из списка и нажмите *Далее.*



6. На следующем шаге укажите сетевой узел Помощник глав админа.
7. Теперь задайте время применения обновления - текущее время и установите флажок Перезагружать Windows на сетевых узлах после обновления программного обеспечения.
8. Следуйте указаниям мастера, нажимая кнопку Далее. На заключительном шаге дождитесь окончания отправки обновления и перезагрузки операционной системы.
9. Для проверки версии программного обеспечения на узле Помощник глав админа зайдите в программу ViPNet Client Монитор → Справка → О программе.





В рамках данного практического занятия явных изменений в версии не будет, так как был использован файл обновления той же версии *ViPNet Client,* но этого достаточно чтобы изучить процедуру обновления ПО.

Вставьте скриншот, подтверждающий выполнение задания

Практическая работа № 8
Компрометация ключей в защищённой сети ViPNet

Задание:

В настоящем задании необходимо скомпрометировать ключи пользователя Помощник глав администратора Иванов.

О компрометации

Компрометация может происходить с удалением или без удаления сетевого узла, пользователя. Как правило, ключи считаются скомпрометированными в следующих случаях:

✓ посторонним лицам мог стать доступным файл дистрибутива ключей пользователя;

✓ посторонним лицам могло стать доступным съемное устройство с ключами пользователя;

✓ посторонние лица могли получить неконтролируемый физический доступ к ключам пользователя, хранящимся на компьютере;

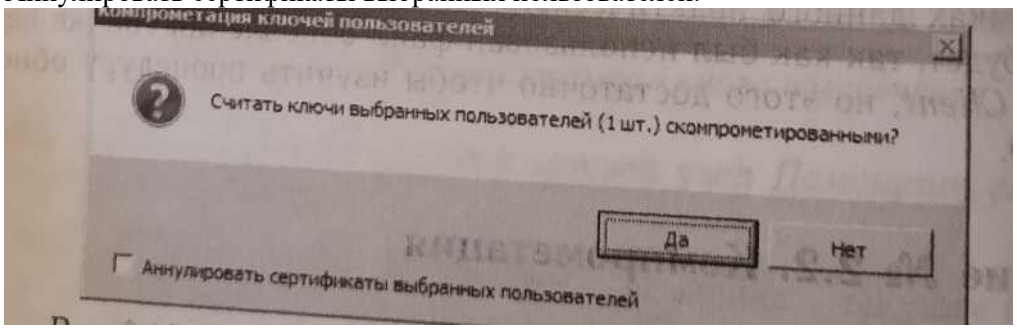
✓ уволился пользователь, имевший доступ к паролям и ключам;

✓ съемное устройство с ключами вышло из строя, и не опровергнут тот факт, что это произошло в результате несанкционированных действий злоумышленника.

Компрометация ключей пользователя

Для компрометации ключей пользователя Помощник глав админа Иванов выполните следующие действия:

1. В окне ViPNet Удостоверяющий и ключевой центр перейдите в раздел Пользователи,
2. Выделите там Помощник глав админа Иванов и в контекстном меню выберите пункт Считать скомпрометированными.
3. В появившемся окне Компрометация ключей пользователей нажмите кнопку Да (после этого пользователь Помощник глав админа Иванов будет помечен красным цветом). Если вместе с ключами пользователя были скомпрометированы его ключи электронной подписи, установите флажок Аннулировать сертификаты выбранных пользователей.



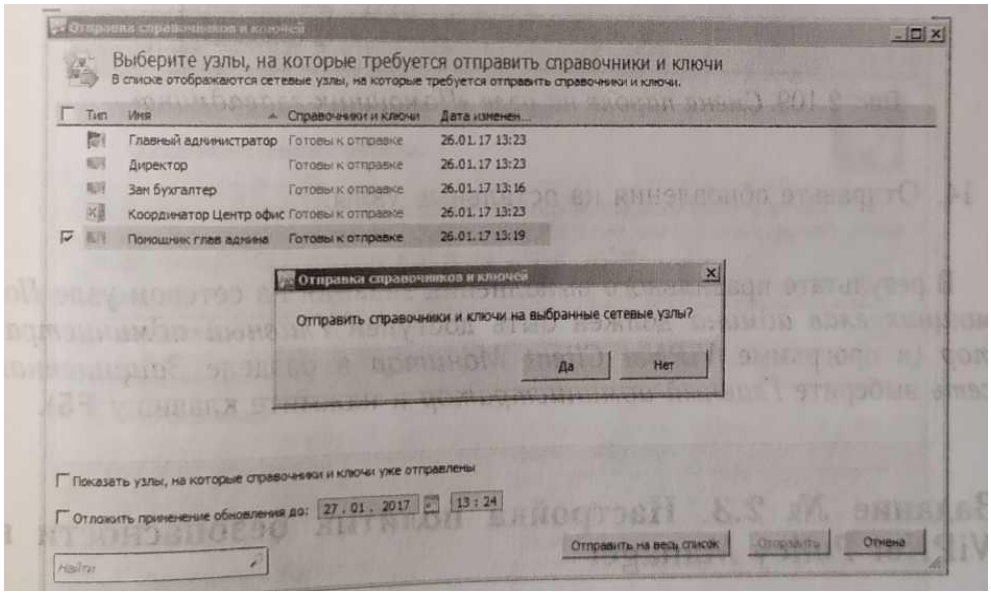
4. Повторно вызовите нажатием «правой, кнопки мыши на пользователя Помощник глав админа Иванов контекстное меню и выберите пункт Ключи пользователя Создать и передать ключи в ЦУС.
5. В окне ViPNet Удостоверяющий - ключевой центр перейдите в раздел Сетевые узлы.
6. После этого создайте и передайте в ЦУС ключи для узла Помощник глав админа.
7. Затем выделите правой кнопкой мыши (или сочетанием клавиш Ctrl+W) остальные узлы, для которых нужно создать ключи и в контекстном меню выберите пункт Создать и передать ключи в ЦУС (или сочетанием клавиш Ctrl+F).

Вставьте скриншот, подтверждающий выполнение задания

Практическая работа № 9
Поднятие защищённой сети ViPNet после компрометации

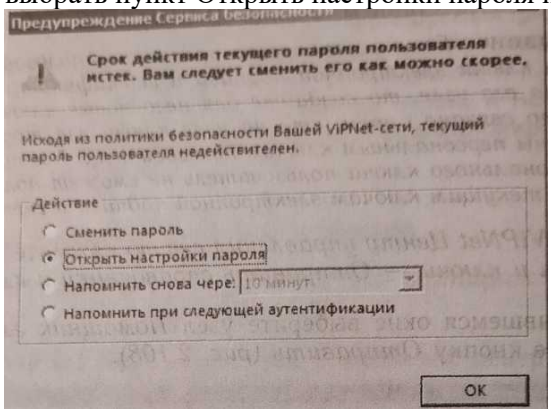
Задание:

8. В окне ViPNet Центр управления сетью нажмите кнопку Справочники и ключи → Отправить справочники и ключи...
9. В открывшемся окне выберите узел Помощник глав админа и нажмите кнопку Отправить.



Вставьте скриншот, подтверждающий выполнение задания

10. Проконтролируйте доставку обновления на узел Помощник глав админа.
11. Проконтролируйте применение обновления на скомпрометированном узле Помощник глав администратора.
12. После перезапуска ПО ViPNet Client, появиться диалоговое окно, в котором необходимо будет указать путь до РНПК и ввести пароль пользователя.
13. После успешного обновления на узле Помощник глав администратора появиться диалоговое окно с информацией о том, что текущий пароль истек и его следует сменить. Для смены пароля необходимо выбрать пункт Открыть настройки пароля и установит новый пароль - 11111111



14. Отправьте обновления на остальные узлы.
В результате правильного выполнения задания на сетевом узле Помощник глав администратора должен быть доступен Главный администратор (в программе ViPNet Client Монитор в разделе Защищенная сеть выберите Главный администратор и нажмите клавишу F5).

Вставьте скриншот, подтверждающий выполнение задания

Практическая работа № 10
Настройка политик безопасности в VipNet Policy Manager

Задание:

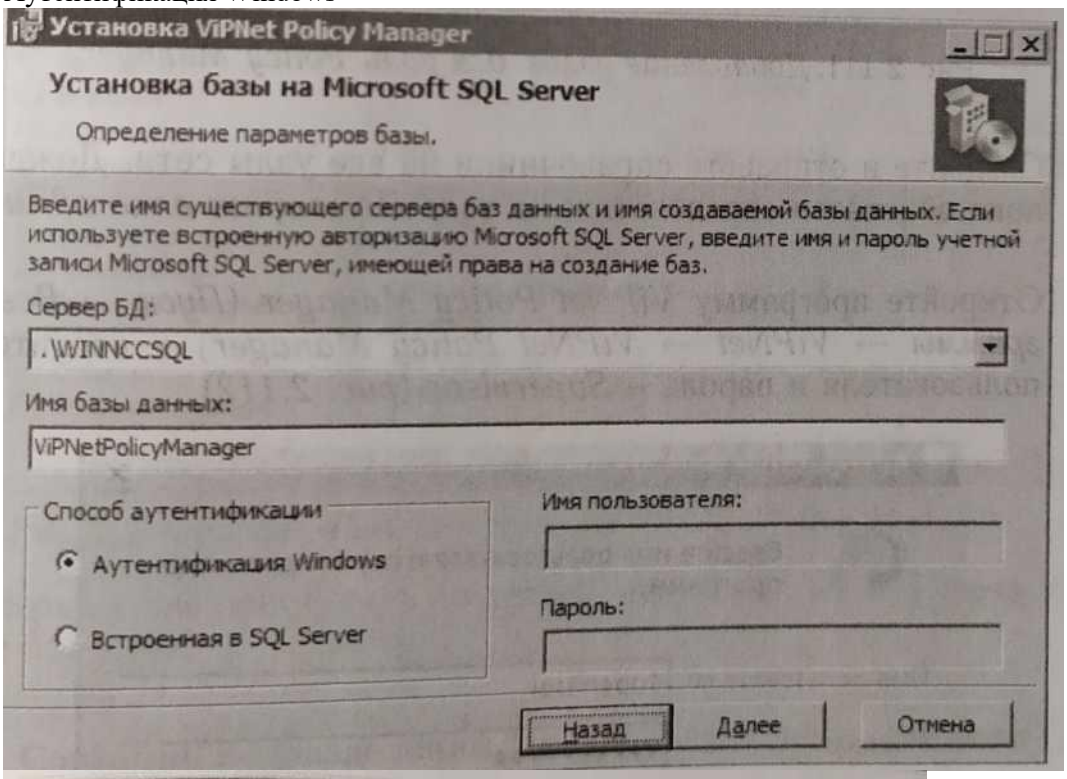
В настоящем заданий необходимо:

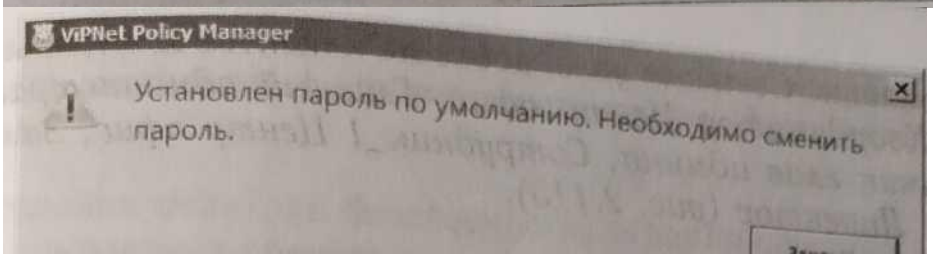
1. Установить ViPNet Policy Manager.
2. Создать подразделения Центральный офис, Филиал.
3. Создать политики безопасности, ограничивающей доступ работников компании к социальным сетям Вконтакте и Одноклассники.
4. Создать политики безопасности, блокирующей весь открытый трафик на рабочем месте Помощник глав админа.

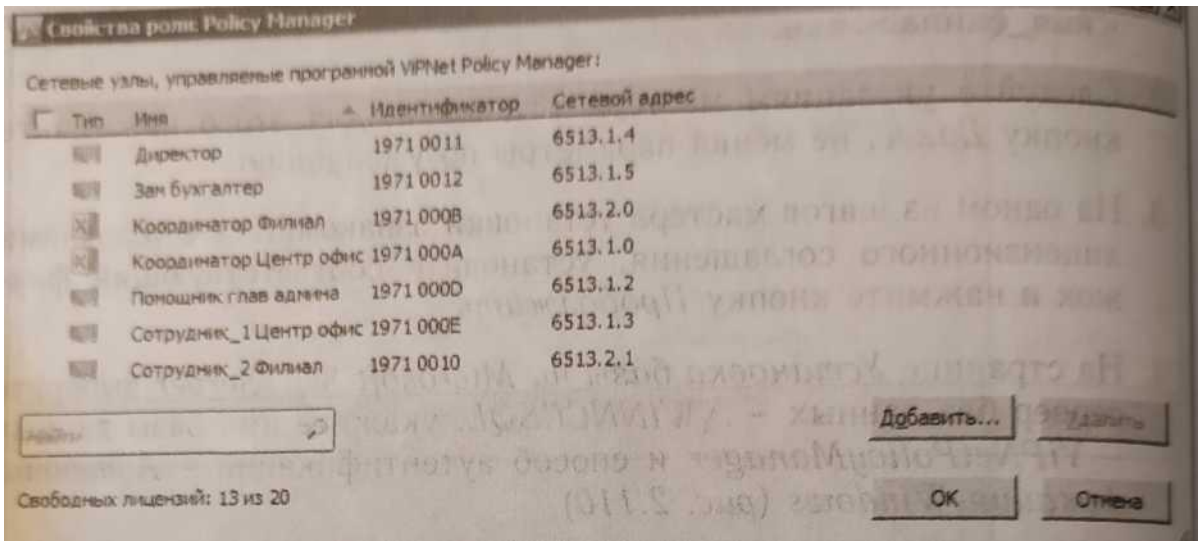
Установка ViPNet Policy Manager

ПО ViPNet Policy Manager допускается развертывать только на клиенте с ролью Network Control Center, поэтому клиенту Главный администратор была автоматически назначена роль Policy Manager.

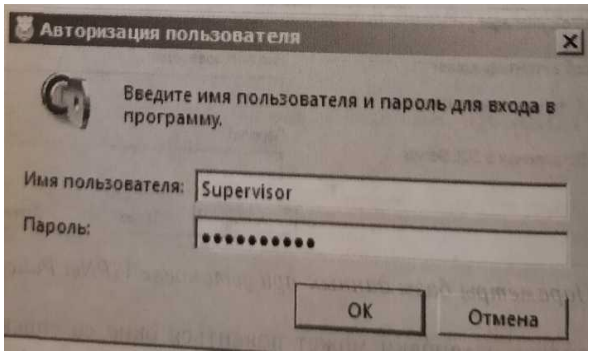
1. На рабочем месте Главный администратор запустите установочный файл программного обеспечения ViPNet Policy Manager <имя_файла>. exe.
2. Следуйте указаниям мастера установки, для этого нажимайте кнопку Далее, не меняя параметры по умолчанию.
3. На одном из шагов мастера установки ознакомьтесь с условиями лицензионного соглашения, установите соответствующий флажок и нажмите кнопку Продолжить.
4. На странице Установка базы на Microsoft SQL Server выберите сервер баз данных - .\WINNCCSQL, укажите имя базы данных - ViPNetPolicyManager и способ аутентификации - Аутентификация Windows







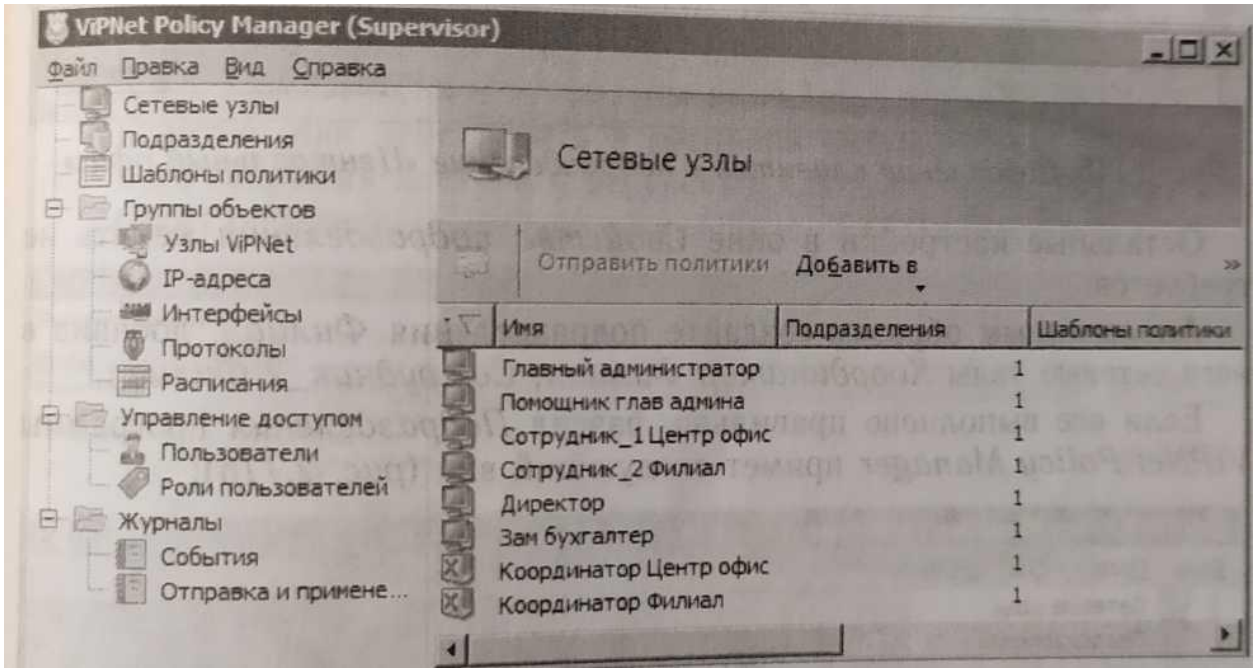
5. В процессе установки может появиться окно со списком приложений которые требуется закрыть. Выберите Закрыть приложения и попытаться перезапустить их и нажмите ОК.
Для обеспечения нормальной работы продукта VipNet Policy Manager выполните следующие действия:
1. В окне VipNet Центр управления сетью перейдите в раздел Клиенты.
2. В свойствах клиента Главный администратор выберите Роли узла → Policy Manager → Свойства и добавьте в список все узлы сети
3. Создайте и отправьте справочники на все узлы сети. Дождитесь пока обновятся справочники на узле Помощник глав админа.



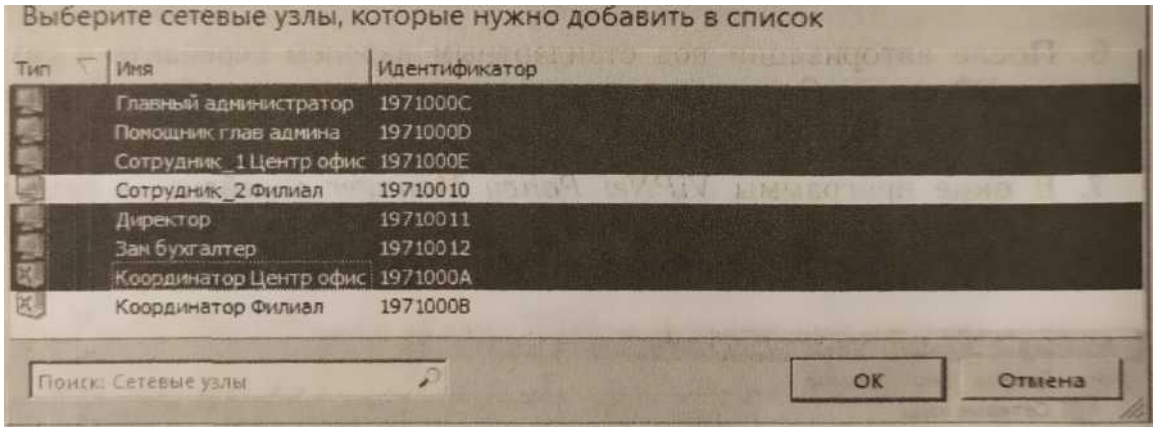
4. Откройте программу ViPNet Policy Manager (Пуск → Все программы → ViPNet →ViPNet Policy Manager) и введите им пользователя и пароль – Supervisor.
5. На экран будет выведено предупреждение о необходимости смены пароля пользователя Supervisor.
6. После авторизации под стандартным паролем перейдите в раздел Файл → Сменить пароль пользователя и задайте пароль — 11111111 (восемь единиц).
7. В окне программы VipNet Policy Manager перейдите в раздел Сетевые узлы. Если предыдущие шаги выполнены верно, то в списке будут отображены все узлы сети VipNet.

Вставьте скриншот, подтверждающий выполнение задания

Теперь можно приступить к управлению узлами ViPNet через ViPNet Policy Manager.
Создание подразделений Центральный офис, Филиал
Для создания подразделений Центральный офис, Филиал выполните следующие действия:
1. В окне программы VipNet Policy Manager перейдите в раздел Подразделения и нажмите кнопку Создать.
2. В открывшемся окне Свойства подразделения на вкладке Основные параметры задайте имя Центральный офис.



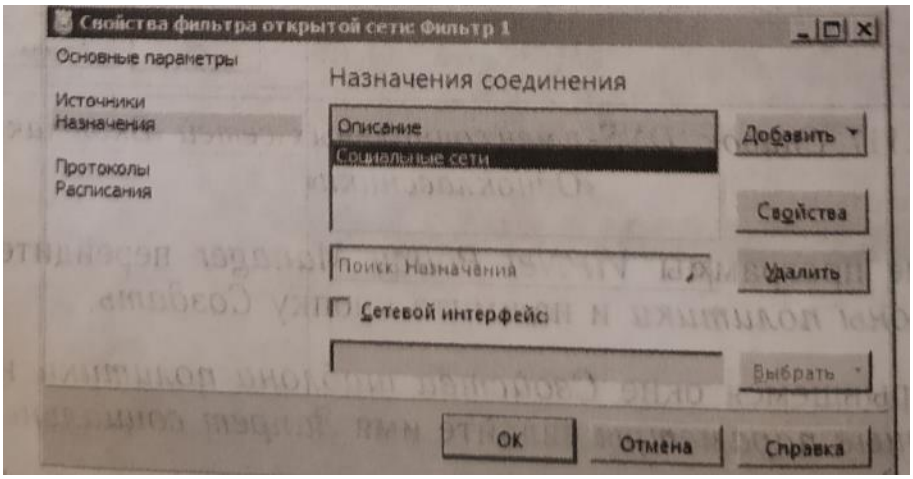
3. На вкладке Сетевые узлы добавьте клиентов Центрального офиса: Координатор Центр офис, Главный администратор, Помощник глав админа, Сотрудник_1 Центр офис, Зам бухгалтер, Директор.

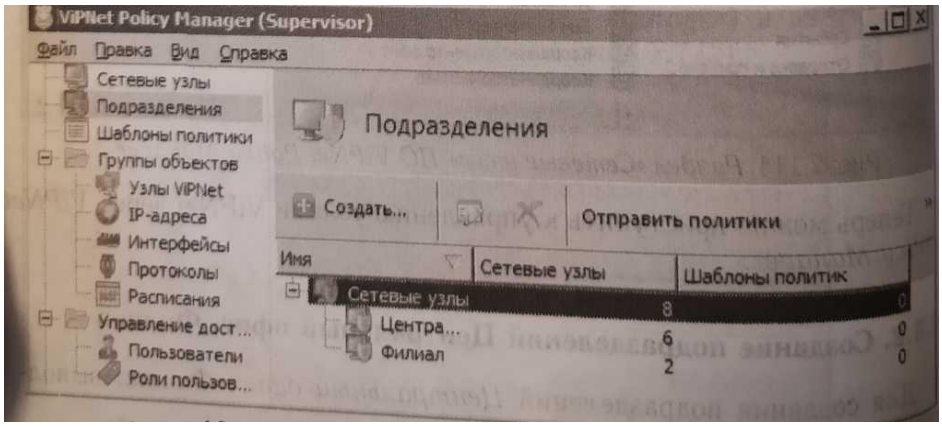


Остальные настройки в окне Свойства подразделения менять не требуется.
Аналогичным образом создайте подразделения Филиал, добавив в него сетевые узлы Координатор Филиал, Сотрудник_2 Филиал.
Если все выполнено правильно, раздел Подразделения программы ViPNet Policy Manager примет следующий вид

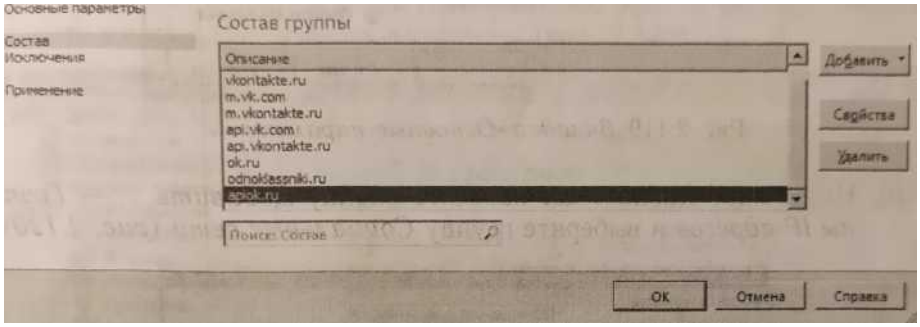
Вставьте скриншот, подтверждающий выполнение задания

Создание политики безопасности, ограничивающей доступ работников компании к социальным сетям Вконтакте и Одноклассники
Для создания политики безопасности, ограничивающей доступ работников компании к социальным сетям Вконтакте и Одноклассники, выполните следующие действия:
1. В окне программы ViPNet Policy Manager перейдите в раздел Группы объектов —* IP-адреса и нажмите кнопку Создать.
2. В открывшемся окне Свойства группы IP-адресов на вкладке Основные параметры затаите имя Социальные сети.
3. На вкладке Состав нажмите кнопку Добавить → DNS-имя... и добавьте имя vk.com.



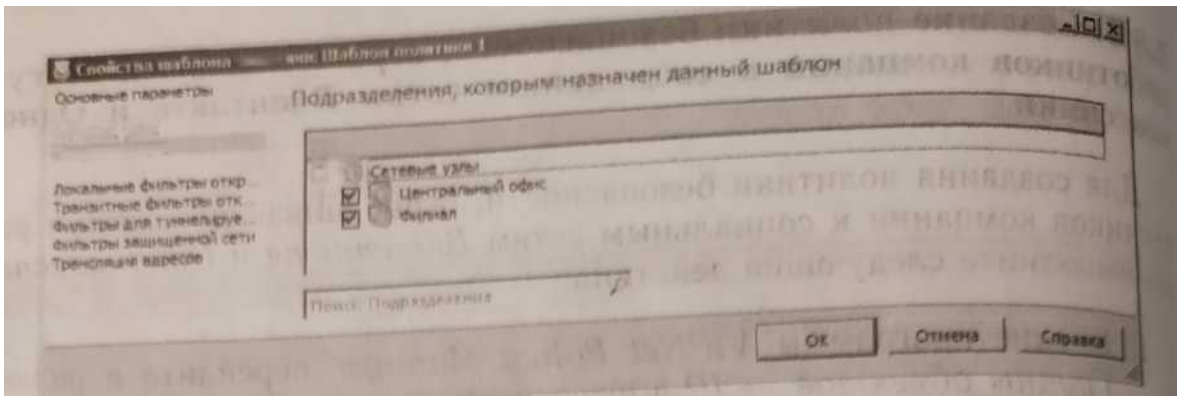


Аналогичным образом добавьте DNS-имена согласно рисунку ниже (в рамках практического занятия не обязательно вбивать все DNS-имена, они приведены в качестве примера, чтобы было понятно, как действовать в реальной ситуации, для эффективного закрытия доступа к ресурсам). Соответствующие IP-адреса будут определены автоматически.

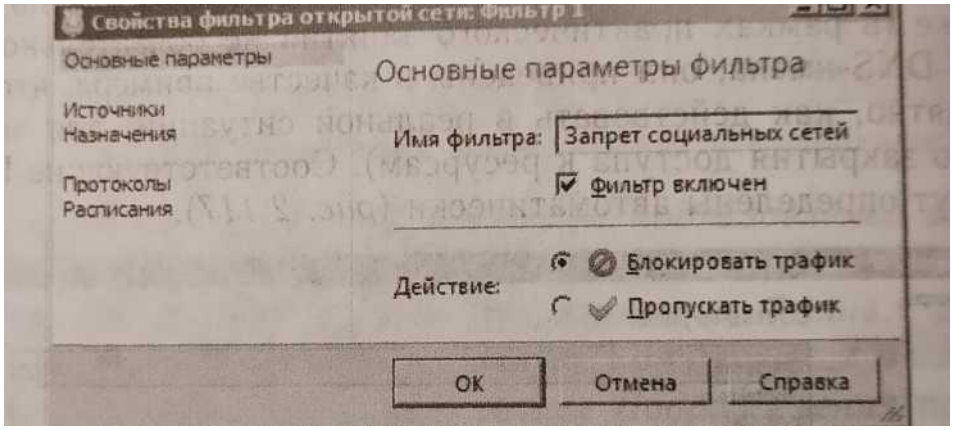


4. В окне программы ViPNet Policy Manager перейдите в раздел Шаблоны политики и нажмите кнопку Создать.
5. В открывшемся окне Свойства шаблона политики на вкладке Основные параметры задайте имя Запрет социальных сетей.
6. На вкладке Подразделения отметьте подразделения Центральный офис и Филиал На вкладке Локальные фильтры открытой сети нажмите кнопку Создать...

7. В открывшемся окне Свойства фильтра открытой сети на вкладке Основные параметры задайте имя фильтра Запрет социальных сетей и установите переключатель в положение Блокировать трафик

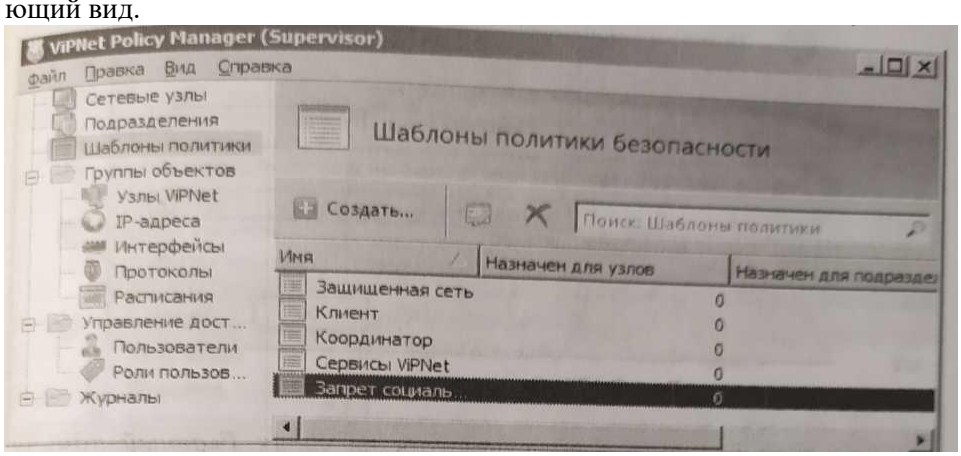


8. На вкладке Назначения нажмите кнопку Добавить... р пы IP-адресов и выберите группу Социальные сети.

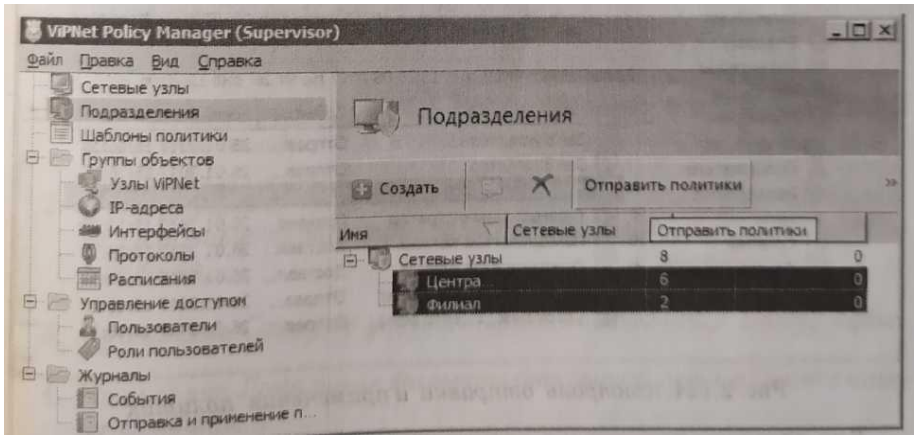


Вставьте скриншот, подтверждающий выполнение задания

9. Остальные параметры окна Свойства фильтра открытой сети и Свойства шаблона политики менять не требуется.
10. После создания политики Запрет социальных сетей раздел Шаблоны политики примет следующий вид.

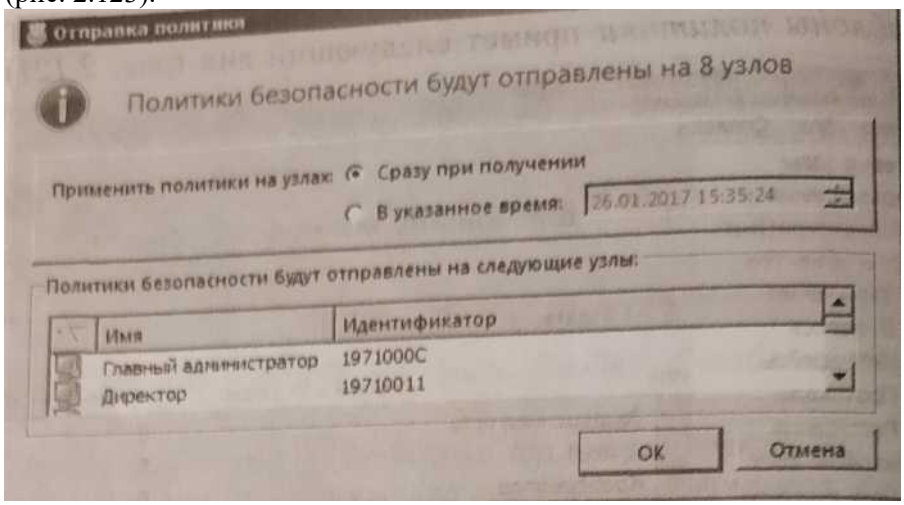


11. Отправьте политики на узлы. Для этого в окне программы ViPNet Policy Manager перейдите в раздел Подразделения.
12. Выделите подразделения Центральный офис и Филиал, нажмите кнопку Отправить политики.

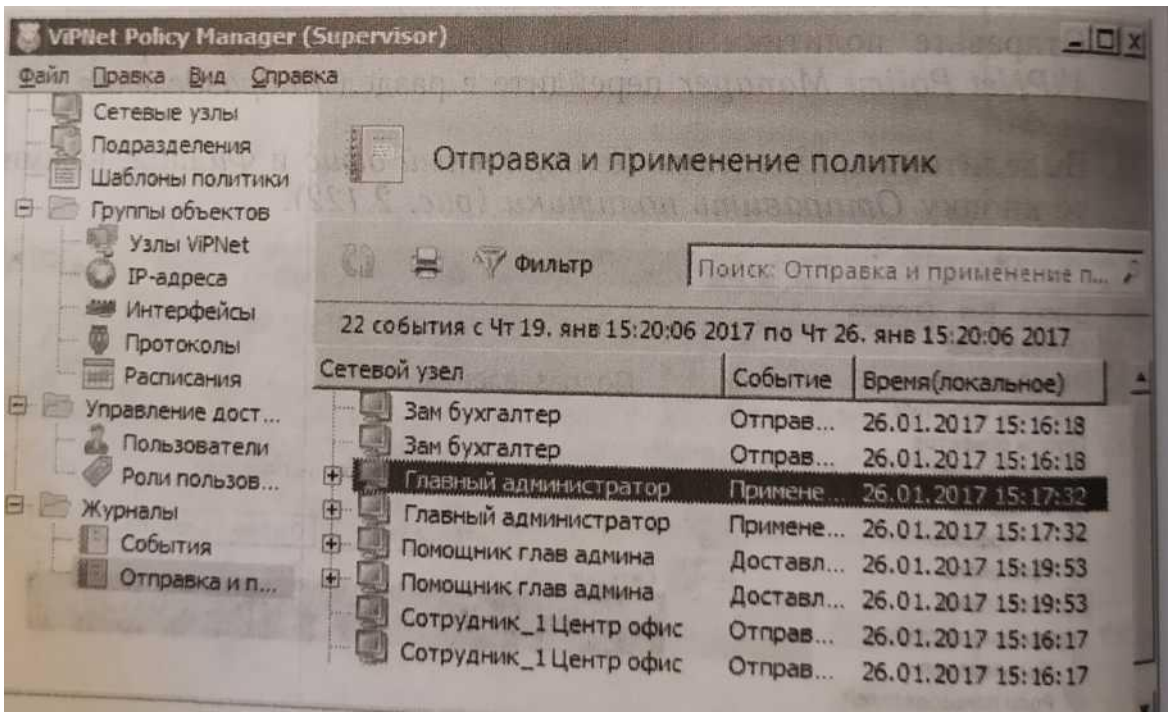


Вставьте скриншот, подтверждающий выполнение задания

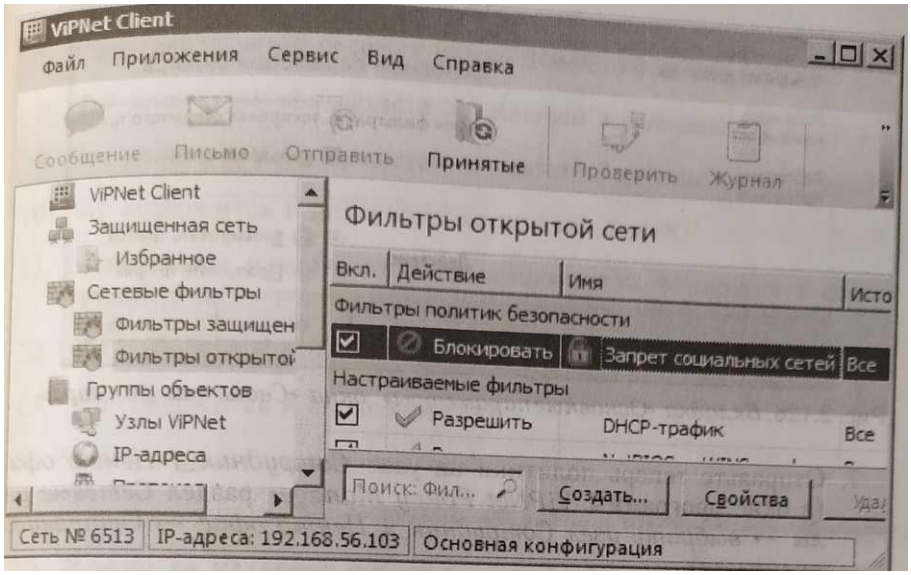
13. На экран будет выведено окно Отправка политики. Не меняя параметров, нажмите кнопку ОК (рис. 2.123).



Для контроля за ходом отправки политик на узлы в окне программы *ViPNet Policy Manager* перейдите в раздел Журналы → Отправка и применение политик. Статус политик на узлах Главный администратор и Помощник глав админа должен измениться на Применена.



Для проверки применения политик на рабочих местах Главный администратор и Помощник глав администратора зайдите в программу ViPNet Client Монитор Сетевые фильтры → Фильтры открытой сети. Убедитесь, что добавлен новый фильтр Запрет социальных сетей.



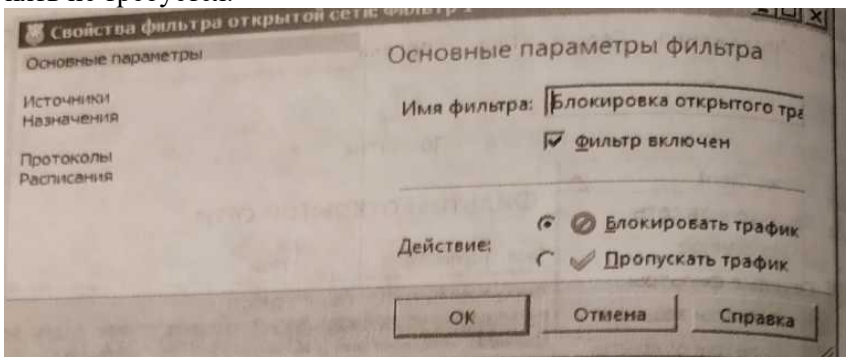
Вставьте скриншот, подтверждающий выполнение задания

Создание политики безопасности, блокирующей весь открытый трафик на рабочем месте Сотрудник_1 Центр офис

Для создания политики безопасности, блокирующей весь открытый трафик на рабочем месте Сотрудник_1 Центр офис, выполните следующие действия:

1. В окне программы ViPNet Policy Manager перейдите в раздел Шаблоны политики и нажмите кнопку Создать.
2. В открывшемся окне Свойства шаблона политики на вкладке Основные параметры задайте имя Блокировка открытого трафика.
3. На вкладке Сетевые узлы добавьте Сотрудник_1 Центр офис.
4. На вкладке Локальные фильтры открытой сети нажмите кнопку Создать…

5. В открывшемся окне Свойства фильтра открытой сети на вкладке Основные параметры задайте имя фильтра Блокировка открытого трафика, установите переключатель в положение Блокировать трафик и нажмите ОК.
6. Остальные параметры окна Свойства фильтра открытой сети и Свойства шаблона политики менять не требуется.



Отправьте теперь политики на узел Сотрудник_1 Центр офис (в окне программы ViPNet Policy Manager раздел Сетевые узлы → выбрать узел Сотрудник_1 Центр офис → Отправить политики). Проверить были ли приняты политики или нет в данном случае» получится, так как данный узел не был развернут.

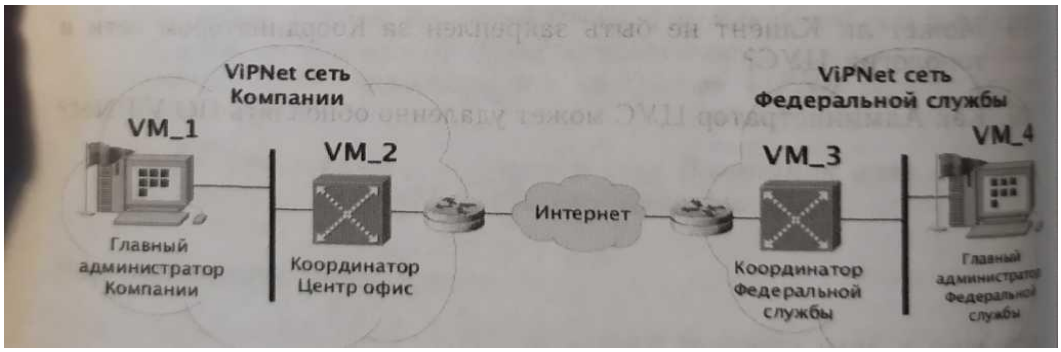
Вставьте скриншот, подтверждающий выполнение задания

Практическая работа № 11
Межсетевое взаимодействие

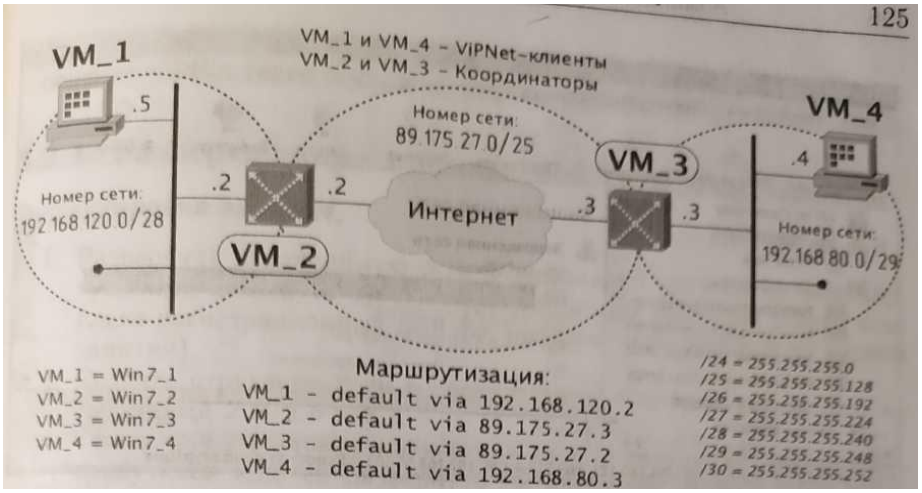
Задание:

1. Установка ViPNet Coordinator в качестве межсетевого шлюза
2. Первоначальная настройка межсетевого взаимодействия
3. Модификация межсетевого взаимодействия

В рамках практического занятия необходимо смоделировать ситуацию, в которой компания с уже имеющейся сетью ViPNet решила организовать межсетевое взаимодействие с сетью ViPNet Федеральной службы для организации юридически значимого электронного документооборота посредством ПО ViPNet Деловая почта.
При организации межсетевого взаимодействия, как и при любой модификации сети, тем более реальной, стоит заранее продумывал все этапы запланированного мероприятия от начала до конца. Поэтому из уже имеющейся сети и сети Федеральной службы выделим только те сетевые узлы, которые нам понадобиться связать, и представим их в виде схемы



В реальной ситуации количество узлов, которые потребуется связать, может оказаться гораздо больше, и поэтому вовсе не обязательно их отражать на схеме, однако общую модель и план действия лучше составить, а остальные связи узлов проработать в виде таблицы.



Примечание. Стенд для данной практической работы рекомендуется разворачивать в соответствии с проработанной схемой. Так как в предыдущих заданиях был развернут не только узел с ViPNet Administrator (VM_1), но и рабочее место помощника главного администратора с ViPNet Client (VM_2), то лучше сделать откат системы на второй виртуальной машине к исходному состоянию, чтобы установить на нее ViPNet Coordinator.

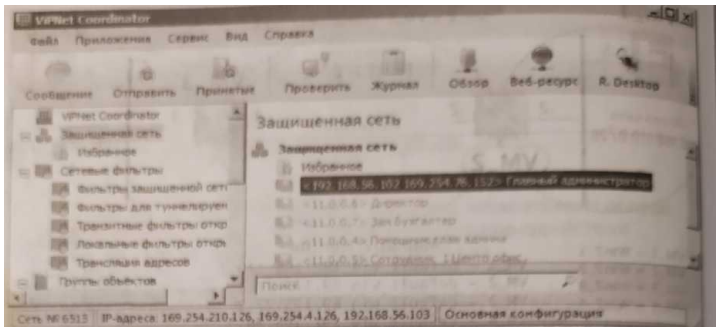
Внимание! Не забудьте создать обновленный dst-файл для координатор! Это необходимо, так как в предыдущих практических заданиях вносилось много изменений в структуру сети и неоднократно изменялись ключи, поэтому выпущенный в самом начале dst-файл не подойдет.

Установка ViPNet Coordinator в качестве межсетевого шлюза

В первую очередь развернем Координатор Центр офис для ранее созданной сети. Запустите установочный файл ViPNet Coordinator <имя_файла>. exe. Прочесе установки аналогичен установке ViPNet Client. При этом необходимо установись ключи пользователя Координатор Центр офис.

Проверка доступности узлов в защищенной сети

На рабочем месте Координатор Центр офис в области, уведомлений на панели задач щелкните 2 раза значок ViPNet Coordinator Монитор. На экран будет выведено окно программы.



Во вкладке Защищенная сеть отображаются сетевые узлы, с которыми есть связи.

Проверьте доступность сетевых узлов. Для этого щелкните правой кнопкой мыши узел Главный администратор и выберите пункт Проверить соединение.

Если все настроено правильно, то в окне Главный администратор — Проверка соединения отобразится статус Доступен.

Вставьте скриншот, подтверждающий выполнение задания

Первоначальная настройка межсетевого взаимодействия

В настоящем задании необходимо:

1. Развернуть защищенную сеть Федеральной службы.
2. Настроить межсетевое взаимодействие с использованием индивидуального симметричного межсетевого мастер-ключа.

Предварительные настройки:

✓ Для подготовки к заданию выполните следующие действия:

✓ Проверьте, что на виртуальной машине VM_1 установлено ПО VipNet Administrator, VipNet Policy Manager и VipNet Client.
✓ Проверьте, что на виртуальной машине VM_2 установлено программное обеспечение VipNet Coordinator с установленными ключами пользователя Координатор Центр офис.
✓ На виртуальных машинах VM_3 и VM_4 удалите программное обеспечение VipNet (если оно было установлено ранее).

Развертывание защищенной сети Фед. Службы

1. Развернуть защищенную сеть Федеральной службы на базе виртуальных машин VM_3 и VM_4 (используя при этом второй комплект регистрационных файлов, которые были выданы на первом занятии).
2. Создать структуру сети в соответствии с предложенными ниже таблицами 2.5, 2.6 и 2.7.
3. Сформировать справочники и ключи и на основе созданных дистрибутивов ключей развернуть на виртуальных машинах Координатор Федеральной службы и Администратор ViPNet Федеральной службы.

Пояснение к заданию

На виртуальной машине VM_4 необходимо установить программное обеспечение ViPNet Administrator и ViPNet Client, а на виртуальной машине VM_3 - ViPNet Coordinator.
Защищенная сеть Федеральной службы состоит из 3 узлов - 1 координатор и 2 клиента (табл.).

Таблица .— Состав защищенной сети Федеральной службы

	Тип	Название	Расположение	Комментарии 1
1	Координатор	Координатор Федеральной службы	Федеральная служба	Для развертывания ПК ViPNet Coordinator
2	Клиент	Администратор ViPNet Федеральной службы		Для развертывания ПК ViPNet Administrator
3		Специалист по приёму отчётности		Рабочее место специалиста по приему отчетности

Матрица связей узлов защищённой сети Федеральной службы представлена в таблице.
На каждом узле защищенной сети присутствует по одному пользователю (табл.).
Связи между пользователями не установлены.
Не забудьте отключить у пользователей создание ЭП.

Таблица — Матрица связей узлов в сети Федеральной службы

Федеральная служба	Координатор Федеральной службы	Администратор ViPNet Фед. службы	Специалист по отчетности
Координатор Федерала ной службы		•	•

Администратор ViPNet Фед. службы	•		•
Специалист по отчетности	•	•	

Таблица — Определение пользователей

№	Название СУ	Имя пользователя на СУ
1	Координатор Федеральной службы	Координатор Федеральной службы
2	Администратор ViPNet Федеральной службы	Админ ФедСлужбы Новиков
3	Специалист по отчетности	Спец отчетности Морозов

Порядок выполнения задания:

Развертывание программного обеспечения ViPNet Центр управления сетью, ViPNet Удостоверяющий и ключевой центр, ViPNet Client и ViPNet Coordinator осуществляется в том же порядке, что и в предыдущих практических занятиях.

При настройке программ ViPNet задайте пароли:

✓ 11111111 — для входа в программы VipNet Центр управления сетью и VipNet Удостоверяющий и ключевой центр (пароль администратора сети VipNet);

✓ 11111111 — для пользователей защищённой сети.

Имя администратора VipNet Федеральной службы — Константин.

Настройка межсетевого взаимодействия с использованием индивидуального симметричного ММК

Настроить взаимодействие защищённой сети Компании и защищенной сети Федеральной службы таким образом, чтобы узлы Координатор Центр офис и Координатор. Федеральной службы могли взаимодействовать друг с другом по шифрованному каналу.

Проверка взаимодействия осуществляется в окне программы ViPNet Coordinator Монитор → Защищенная сеть → в контекстном меню узла выбрать Проверить соединение. На узле Координатор Федеральной службы должен быть доступен узел Координатор Центр офис и наоборот.

Пояснение к заданию

Если требуется организовать канал для защищенного обмена информацией между двумя разными сетями ViPNet, то между этими сетями следует установить межсетевое взаимодействие. Сети ViPNet, с которыми в вашей сети установлено межсетевое взаимодействие, называются доверенными сетями.

Для каждой доверенной сети в Удостоверяющем и ключевом центре создается межсетевой мастер-ключ, на основе которого формируются ключи для защищенного обмена информацией с данной доверенной сетью.

Также для каждой доверенной сети назначается шлюзовой координатор. Шлюзовой координатор своей сети связан с аналогичным координатором доверенной сети, и через эти координаторы направляются все транспортные конверты, передаваемые между двумя сетями.

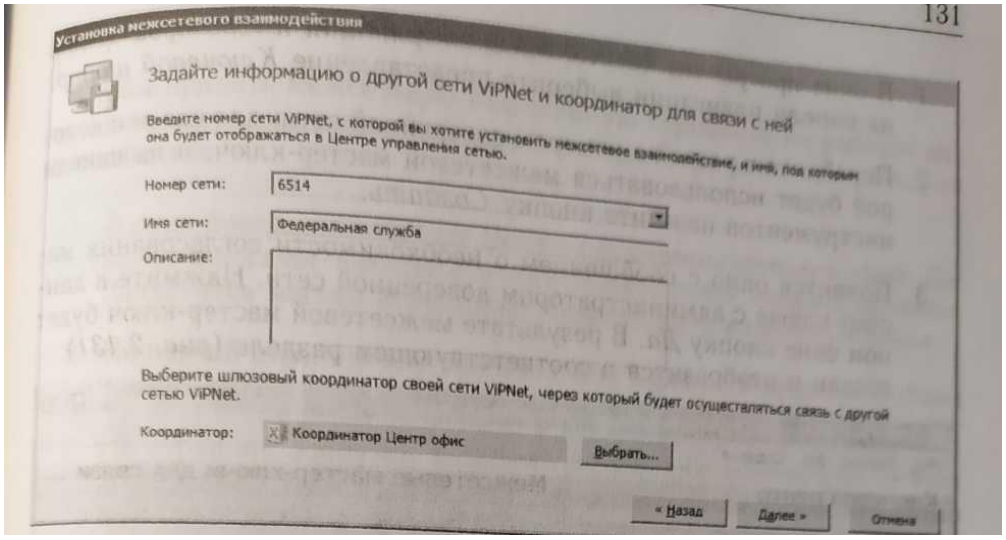
Чтобы обеспечить возможность защищенного соединения между сетевыми узлами вашей и доверенной сетей, обмена письмами в программе ViPNet Деловая почта, файлами и так далее, следует создать связи между объектами вашей сети ViPNet и объектами доверенной сети.

Организация межсетевого взаимодействия между сетями ViPNet состоит из следующих этапов:

1. Администратор первой сети ViPNet, инициирующий межсетевое взаимодействие, создает в Центре управления сетью файл мел сетевой информации, а в Удостоверяющем и ключевом центре

межсетевой мастер-ключ. Затем по доверенным каналам связи он передает файл межсетевой информации и межсетевой маете ключ администратору второй сети ViPNet.
2. Администратор второй сети ViPNet принимает межсетевую информацию, затем создает файл с ответной межсетевой информацией и передает его администратору первой сети.
3. Администратор второй сети импортирует переданный ему межсетевой мастер-ключ.
4. Администратор первой сети завершает организацию межсетевого взаимодействия приемом ответной межсетевой информации.
5. Администратор каждой сети создаёт новые справочники и ключи и отправляет их на узлы своей сети.
После этого узлы доверенных сетей, участвующие в межсетевом взаимодействии, смогут обмениваться информацией друг с другом.
Внимание! Необходимо учитывать, что при организации межсетевого взаимодействия в реальной сети, пользователя Главный администратор не рекомендуется включать в межсетевую информацию и связывать его с другими пользователями доверенной сети из соображений безопасности.
Также следует обратить внимание, что в Фильтрах защищенной сети по умолчанию разрешено подключение по RDP (на клиентах и координаторах), поэтому при организации межсетевого взаимодействия, необходимо будет запретить подключение по RDP из доверенной сети, а также проверить настройки удалённого доступа в ОС.

Порядок выполнения задания
Инициация межсетевого взаимодействия
Чтобы инициировать межсетевое взаимодействие с сетью ViPNet Федеральной службы, выполните следующие действия на рабочем месте Главный администратор сети Компании:
1. В окне ViPNet Центр управления сетью в меню Доверенные сети выберите пункт Установить взаимодействие. Будет запущен мастер Установка межсетевого взаимодействия.
2. На первой странице мастера выберите вариант Я инициатор межсетевого взаимодействия и нажмите кнопку Далее.
3. На странице Задайте информацию о другой сети ViPNet и координатор для связи с ней (необходимо правильно указать номер доверенной сети, с которой вы устанавливаете межсетевое взаимодействие, в противном случае могут возникнуть проблемы), впишите имя сети - Федеральная служба, которое будет отображаться в программе ViPNet Центр управления сетью, и выберите шлюзовой координатор своей сети - Координатор Центр офис. Затем нажмите Далее.
4. На странице Укажите сетевые узлы своей сети ViPNet для связывания выберите узлы сети, которые будут участвовать во взаимодействии с узлами сети Федеральной службы — Главный администратор и Координатор Центр.

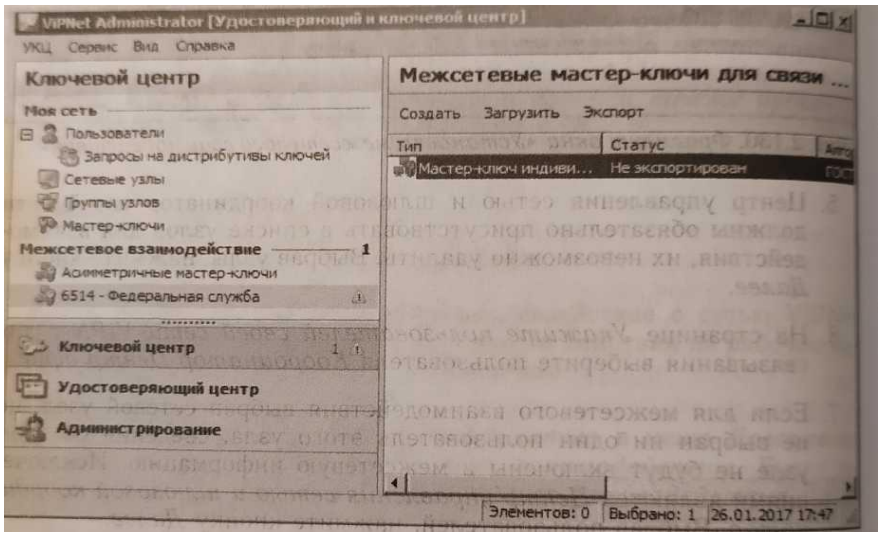


5. Центр управления сетью и шлюзовой координатор своей сети должны обязательно присутствовать в списке узлов для взаимодействия, их невозможно удалить. Выбрав узлы, нажмите кнопку Далее.

6. На странице Укажите пользователей своей сети ViPNet для связывания выберите пользователя Координатор Центр офис.
7. Если для межсетевого взаимодействия выбран сетевой узел, но не выбран ни один пользователь этого узла, сведения об этом узле не будут включены в межсетевую информацию. Исключениями являются Центр управления сетью и шлюзовой координатор. Выбрав пользователей, нажмите кнопку Далее.
8. На открывшейся странице Подготовка к сохранению межсетевой информации завершена при необходимости укажите комментарий для администратора сети Федеральной службы и нажмите кнопку Далее.
9. На странице Укажите файл для сохранения межсетевой информации нажмите кнопку Обзор и укажите каталог для сохранения файла межсетевой информации - Рабочий стол. Затем нажмите кнопку Далее.
10. На странице Сохранение межсетевой информации после завершения записи файла нажмите кнопку Далее, на следующей странице нажмите кнопку Готово.

Вставьте скриншот, подтверждающий выполнение задания

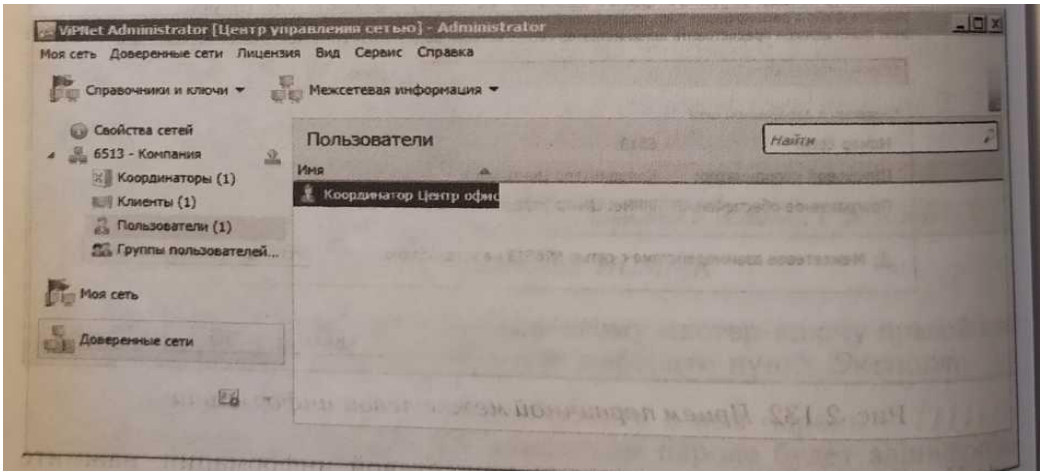
Чтобы создать индивидуальный симметричный межсетевой мастер ключ, выполните следующие действия:
1. В окне программы ViPNet Удостоверяющий и ключевой центр на панели навигации выберите представление Ключевой центр
2. Перейдите в раздел с номером доверенной сети, для связи с которой будет использоваться межсетевой мастер-ключ, и на панели инструментов нажмите кнопку Создать.
3. Появится окно с сообщением о необходимости согласования мастер-ключа с администратором доверенной сети. Нажмите в данном окне кнопку Да. В результате межсетевой мастер-ключ будет создан и отобразится в соответствующем разделе:



4. Щелкните по созданному межсетевой мастер-ключу правой кноп кой мыши и в контекстном меню выберите пункт Экспорт.
5. Появится окно ввода пароля. Укажите в нем пароль - 11111111 и нажмите кнопку ОК. На указанном пароле будет зашифрован экспортируемый ключ.
6. В появившемся окне укажите каталог, в который будет сохранен межсетевой мастер-ключ - Рабочий стал, затем нажмите кнопку ОК.
7. Передайте доверенным способом файл межсетевой информации с расширением*. lzh, межсетевой мастер-ключ «net ****.key» и пароль, на котором зашифрован межсетевой мастер-ключ - 11111111, администратору сети Федеральной службы.

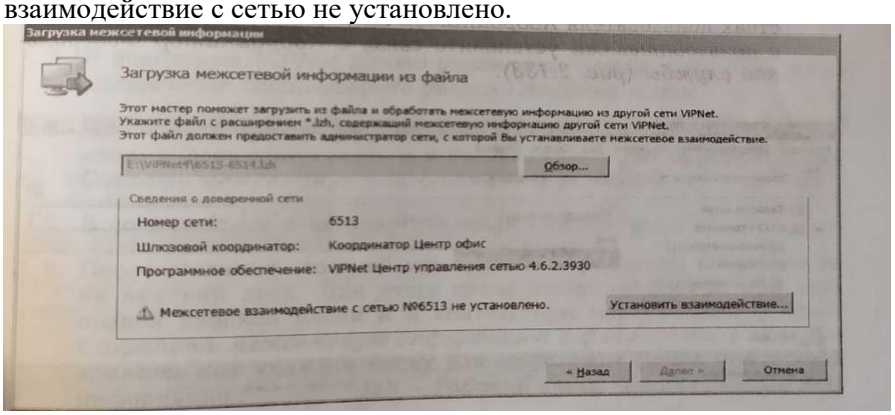
Вставьте скриншот, подтверждающий выполнение задания

Прием первичной межсетевой информации



Чтобы принять межсетевую информацию перейдите на рабочее место администратора сети Федеральной службы и выполните следующие действия:

1. В окне программы ViPNet Центр управления сетью в меню Доверенные сети выберите пункт Установить взаимодействие. Запустится мастер Установка межсетевого взаимодействия.
2. На первой странице мастера выберите вариант Я принимаю файл с межсетевой информацией и нажмите кнопку Далее.
3. На странице Загрузка межсетевой информации из файла укажите файл с межсетевой информацией, полученный от Главного администратора сети ViPNet Компании, который инициировал межсетевое взаимодействие. После указания файла в окне мастера появится предупреждение, что взаимодействие с сетью не установлено.

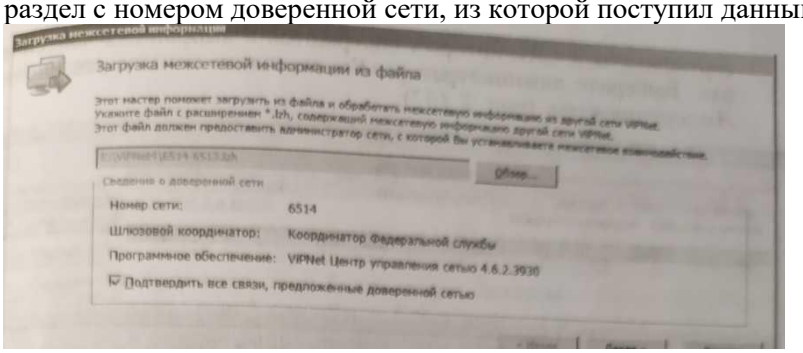


4. Чтобы продолжить загрузку межсетевой информации, нажмите кнопку Установить взаимодействие.
5. На странице Задайте информацию о другой сети ViPNet и координатор для связи с ней выберите шлюзовой координатор - Координатор Федеральной службы, затем нажмите Далее.
6. На странице Изменения в межсетевой информации ознакомьтесь со списком узлов и пользователей, которые были выбраны для межсетевого взаимодействия Главным администратором сети VipNet Компании, который инициировал межсетевое взаимодействие. Затем нажмите кнопку Далее.
7. Если файл межсетевой информации содержит ошибки, откроется страница Проверка межсетевой информации со списком обнаруженных конфликтных или неполных данных. При обнаружении конфликтных данных загрузка межсетевой информации будет невозможна. В этом случае обратитесь к администратору доверенной сети для устранения конфликтов.
8. Чтобы продолжить обработку межсетевой информации, нажмите кнопку Далее.
9. На странице Загрузка межсетевой информации после завершения обработки информации нажмите кнопку Готово.
10. В представлении Доверенные сети выберите Сеть №**** (вместо звездочек будет номер сети, инициировавшей межсетевое взаимодействие) и перейдите на вкладку Пользователи. В свойствах пользователя Координатор Центр офис на вкладке Связи с пользователями установите связь с Координатор Федеральной службы.

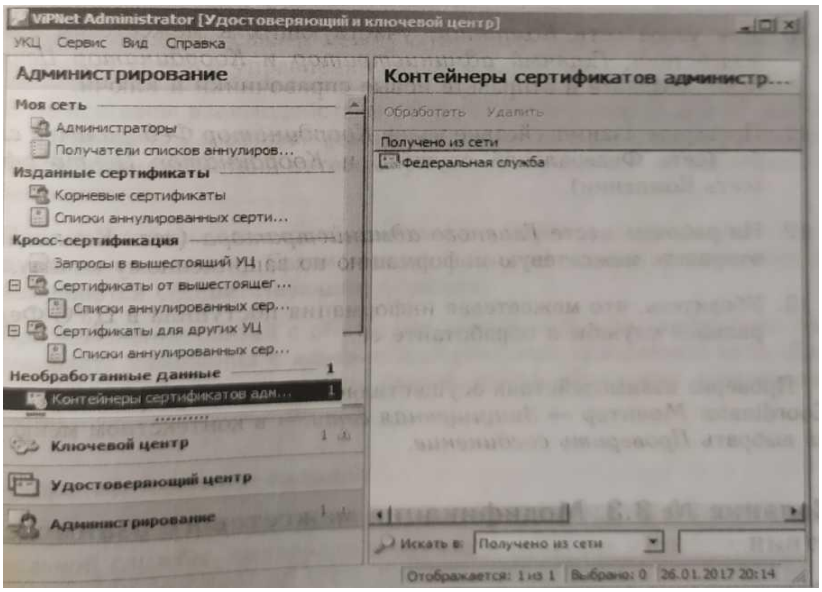
Вставьте скриншот, подтверждающий выполнение задания

После приема первичной межсетевой информации в ПО VipNet УКЦ импортируйте переданный Главным администратором Компании межсетевой мастер-ключ:

1. В окне программы на панели навигации выберите представление Ключевой центр и прейдите в раздел с номером доверенной сети, из которой поступил данный мастер-ключ.



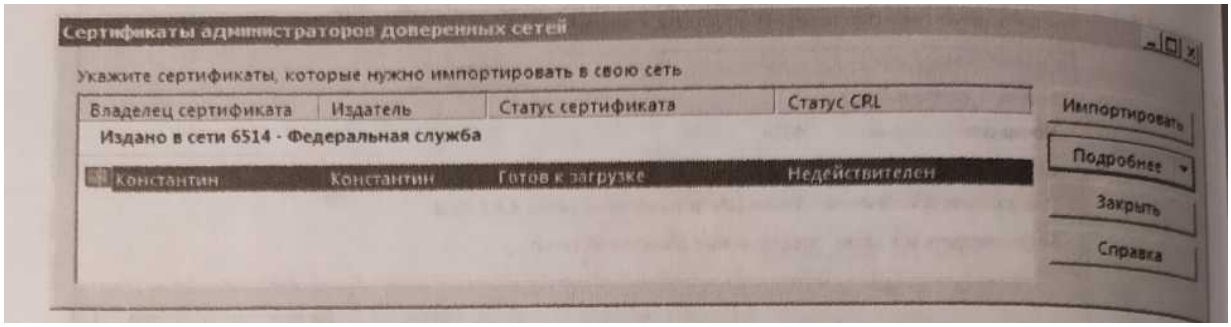
2. На панели инструментов нажмите кнопку Загрузить.
3. При импорте ИСММК «net ****.key» появится окно ввода пароля. Введите пароль, на котором был зашифрован данный ключ - 11111111. При правильном вводе пароля мастер-ключ будет импортирован.
Импортированный мастер-ключ будет сразу добавлен в список межсетевых мастер-ключей выбранного раздела.
После того, как ключ будет импортирован, в УКЦ необходимо зайти в раздел Межсетевое взаимодействие выбрать строку с ИСММК, щелкнуть по строке правой кнопкой мыши и выбрать пункт Использовать.



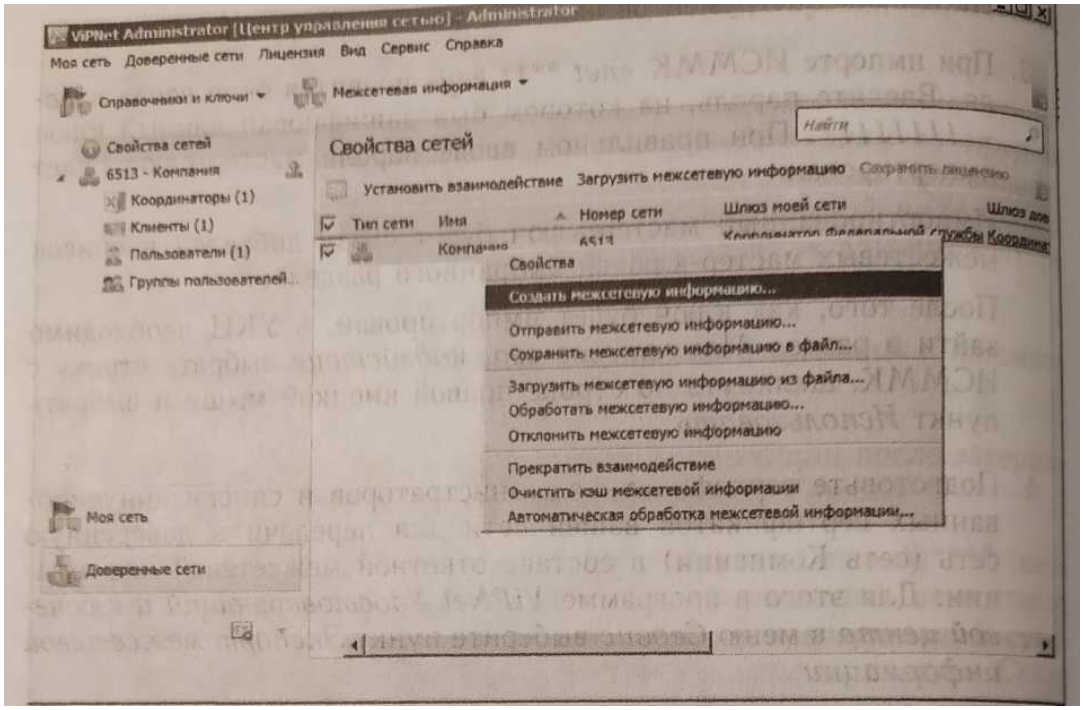
4. Подготовьте сертификаты администраторов и списки аннулированных сертификатов вашей сети для передачи в доверенную сеть (сеть Компании) в составе ответной межсетевой информации. Для этого в программе ViPNet Удостоверяющий и ключевой центр в меню Сервис выберите пункт Экспорт межсетевой информации.
5. В программе ViPNet Центр управления сетью в представлении Доверенные сети выберите раздел Свойства сетей.
6. На панели просмотра щелкните правой кнопкой мыши добавленную доверенную сеть и в контекстном меню выберите пункт Создать межсетевую информацию. В появившемся окне нажмите кнопку Создать.
7. После создания ответной межсетевой информации сохраните ее на жесткий диск. Для этого снова щелкните доверенную сеть правой кнопкой мыши и в контекстном меню выберите пункт Сохранить межсетевую информацию в файл, затем в окне Сохранить как укажите папку для сохранения файла межсетевой информации *****-****.lzh — Рабочий стол.
8. Создайте новые справочники и ключи для узлов сети Федеральной службы, участвующих в межсетевом взаимодействии - Администратор ViPNet Федеральной службы и Координатор Федеральной службы, и отправьте их на узлы.
9. Передайте администратору сети Компании созданный файл межсетевой информации *****-****.lzh

Вставьте скриншот, подтверждающий выполнение задания

Завершение организации межсетевого взаимодействия
Чтобы принять ответную межсетевую информацию и завершить организацию взаимодействия, выполните следующие действия на рабочем месте Главный администратор (сеть Компании):
1. Получите у администратора доверенной сети ViPNet Федеральной службы файл, содержащий ответную межсетевую информацию ****-****.lzh.
2. В окне программы ViPNet Центр управления сётью в меню Доверенные сети выберите пункт Загрузить межсетевую информацию из файла.
3. В окне Загрузка межсетевой информации укажите файл межсетевой информации, полученной от администратора другой сети ViPNet, и следуйте мастеру, нажимая кнопку Далее, а на заключительном шаге — Готово.
4. Примите ответную межсетевую информацию с помощью мастера Обработка межсетевой информации.



5. В окне программы ViPNet Удостоверяющий и ключевой центр перейдите в представление Администрирование и на панели навигации выберите раздел Необработанные данные → Контейнеры сертификатов администраторов сетей VipNet.
6. На панели просмотра выберите контейнер *Федеральная служба* и на панели инструментов нажмите *Обработать.*



7. В появившемся окне будет представлен список администраторов, сертификаты и CRL которых содержатся в выбранных контейнерах Выберите администратора Константин и нажмите кнопку Импортировать.

8. В окне программы ViPNet Удостоверяющий и ключевой центр в представлении Ключевой центр выберите раздел Межсетевое взаимодействие Федеральная служба.
9. Выберите межсетевой мастер-ключ и щелкните по нему правой кнопкой мыши. В контекстном меню выберите команду Текущий для ввода межсетевого мастер-ключа в действие.
10. Для узлов сети Компании, участвующих в межсетевом взаимодействии, Главный администратор и Координатор Центр офис, создайте и отправьте новые справочники и ключи.
11. Проверьте взаимодействие узлов Координатор Федеральной службы (сеть Федеральной службы) и Координатор Центр офис (сеть Компании).
12. На рабочем месте Главного администратора (сеть Компании) отправьте межсетевую информацию по защищенному каналу.
13. Убедитесь, что межсетевая информация поступила в ЦУС Федеральной службы и обработайте ее.

Проверка взаимодействия осуществляется в окне программы ViPNet Coordinator Монитор → Защищенная сеть → в контекстном меню узла выбрать Проверить соединение.

Вставьте скриншот, подтверждающий выполнение задания

Практическая работа № 12
Модификация межсетевого взаимодействия в защищённой сети ViPNet

Задание:

В настоящем задании необходимо:
1. Установить связи между пользователями доверенных сетей.
2. Удалить связи между пользователями доверенных сетей.
3. Прекращение межсетевого взаимодействия

Установление связей между пользователями доверенных се гей

Формулировка задания

Установить связи между пользователями сети компании – Сотрудник_1 Центр Кузнецов, Зам бухгалтера Захарова, Директор Абросимов и сети Федеральной службы - Координатор Федеральной службы.

При этом в списке защищенной сети узла Координатор Федеральной службы должны появиться клиенты Сотрудник_1 Центр офис, Зам бухгалтера, Директор

Пояснение к заданию

Связи сетевых узлов и пользователей вашей сети с сетевыми узлами и пользователями доверенной сети обеспечивают возможность взаимодействия этих объектов между собой так же, как связи между объектами одной сети ViPNet.

Однако создание связей между объектами вашей сети и объектам доверенных сетей и управление связями имеет ряд особенностей:

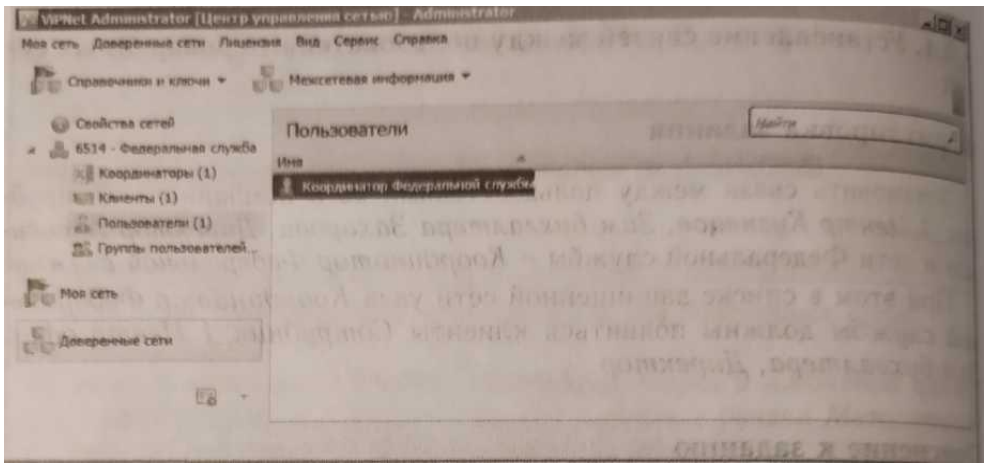
В межсетевом взаимодействии обязательно участвует пара объектов - пользователь и сетевой узел этого пользователя. Участие в межсетевом взаимодействии сетевого узла и пользователя по отдельности невозможно.

При межсетевом взаимодействии можно изменить только связи между пользователями. Связи между сетевыми узлами автоматически изменяются соответствующим образом.

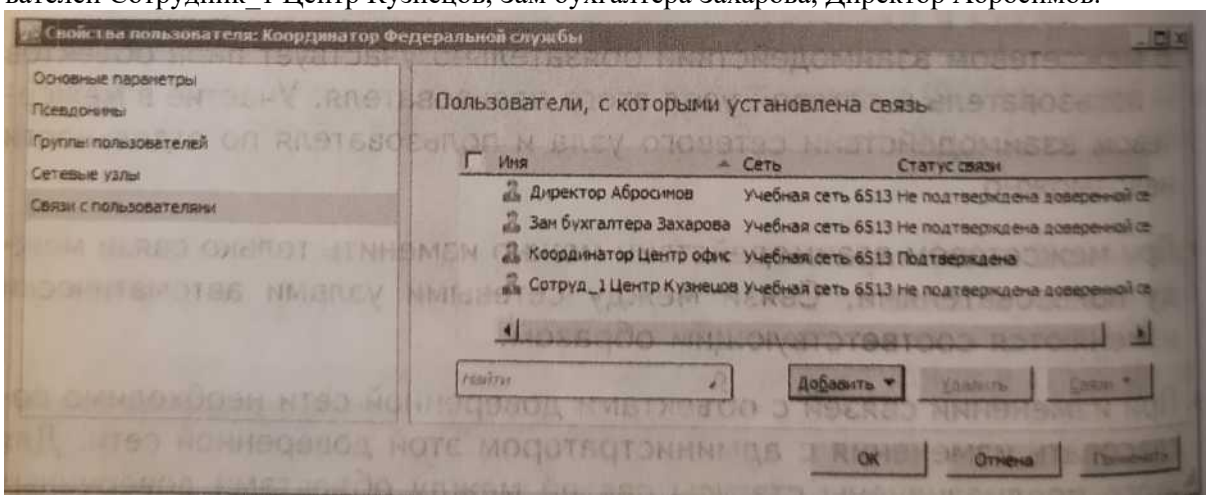
При изменении связей с объектами доверенной сети необходимо согласовать изменения с администратором этой доверенной сети этого предназначены статусы связей между объектами доверенных сетей.

Порядок выполнения задания

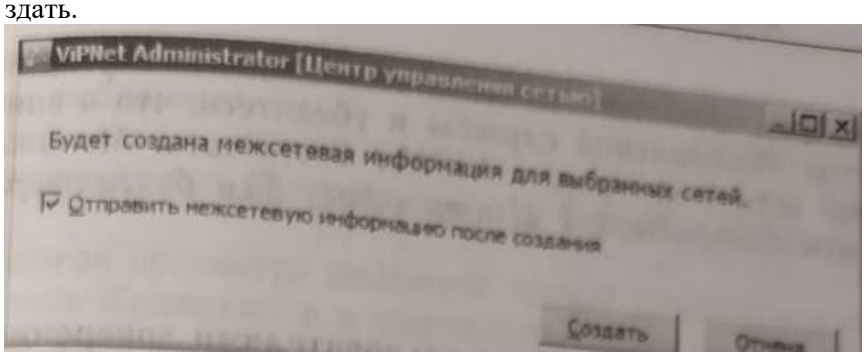
Чтобы добавить связи пользователей сети ViPNet Компании и Федеральной службы, выполните следующие действия на рабочем месте Главный администратор (сеть Компании):
1. В окне программы ViPNet Центр управления сетью в представлении Доверенные сети выберите сеть Федеральная служба и перейдите на вкладку Пользователи.
2. Зайдите в свойства пользователя Координатор Федеральной службы.



3. В открывшемся окне перейдите на вкладку Связи с пользователями и добавьте в список пользователей Сотрудник_1 Центр Кузнецов, Зам бухгалтера Захарова, Директор Абросимов.



4. В представлении Доверенные сети выберите раздел Свойства сетей.
5. На панели просмотра щелкните правой кнопкой мыши на доверенную сеть Федеральная служба и в контекстном меню выберите пункт Создать межсетевую информацию. В открывшемся окне установите флажок Отправить межсетевую информацию после создания и нажмите кнопку Создать.



Вставьте скриншот, подтверждающий выполнение задания

Чтобы принять межсетевую информацию из сети Компании, перейдите на рабочее место администратора сети Федеральной службы и выполните следующие действия:
1. В окне программы ViPNet Центр управления сетью в меню Доверенные сети выберите пункт Обработать межсетевую информацию.
2. В открывшемся окне выберите сеть Компании и нажмите кнопку Обработать выбранные.
3. В представлении Доверенные сети выберите раздел Свойства сетей.
4. На панели просмотра щелкните правой кнопкой мыши доверенную сеть Компании и в контекстном меню выберите пункт Создать межсетевую информацию.
5. В открывшемся окне установите флажок Отправить межсетевую информацию после создания и нажмите кнопку Создать.

6. Создайте и отправьте новые справочники и ключи для узла Координатор Федеральной службы.
Чтобы принять ответную межсетевую информацию от сети Федеральной службы, перейдите на рабочее место Главный администратор сети Компании и выполните следующие действия:
1. В окне программы ViPNet Центр управления сетью в меню Доверенные сети выберите пункт Обработать межсетевую информацию.
2. В открывшемся окне выберите сеть Федеральная служба и нажмите кнопку Обработать выбранные.
3. Создайте и отправьте новые справочники и ключи для узлов Сотрудник_1 Центр офис, Зам бухгалтера, Директор.
Для проверки правильности выполнения задания перейдите на узел Координатор Федеральной службы и убедитесь, что в списке узлов защищенной сети в программе ViPNet Coordinator Монитор появились клиенты Сотрудник_1 Центр офис, Зам бухгалтера, Директор.

Вставьте скриншот, подтверждающий выполнение задания

Удаление связей между пользователями доверенных сетей
Формулировка задания
Удалить связи между пользователями сети Компании Директор Абросимов и сети Федеральной службы Координатор Федеральной службы. При этом из списка защищенной сети узла Координатор Федеральной службы будет исключен клиент Директор.
Порядок выполнения задания
Чтобы удалить связи пользователей сети ViPNet Компании и Федеральной службы, выполните следующие действия на рабочем месте Главный администратор (сеть Компании):
1. В окне программы ViPNet Центр управления сетью в представлении Доверенные сети выберите сеть Федеральная служба и перейдите на вкладку пользователи.
2. Зайти в свойства пользователя Координатор Фед. службы.
3. В открывшемся окне перейдите на вкладку Связи с пользователями и удалите из списка пользователей Директор Абросимов.
4. В представлении Доверенные сети выберите Свойства сетей.
5. На панели просмотра щелкните правой кнопкой мыши доверенную сеть Федеральная служба и в контекстном меню выверите пункт Создать межсетевую информацию.
6. В открывшемся окне установите флажок Отправить межсетевую информацию после создания и нажмите кнопку Создать.
Вставьте скриншот, подтверждающий выполнение задания

Чтобы принять межсетевую информацию от сети Компании, перейдите на рабочее место администратора сети Федеральной службы и выполните следующие действия:
1. В окне программы ViPNet Центр управления сетью в меню Доверенные сети выберите пункт Обработать межсетевую информацию.
2. В открывшемся окне выберите сеть и нажмите кнопку Обработать выбранные.
3. В представлении Доверенные сети выберите Свойства сетей.
4. На панели просмотра щелкните правой кнопкой мыши доверенную сеть Компании и в контекстном меню выберите пункт Создать межсетевую информацию.
5. В открывшемся окне установите флажок Отправить межсетевую информацию после создания и нажмите кнопку Создать.
6. Создайте и отправьте новые справочники и ключи для узла Координатор Федеральной службы.

Вставьте скриншот, подтверждающий выполнение задания
Чтобы принять ответную межсетевую информацию от сети Федеральной службы, перейдите на рабочее место Главный администратор (сеть Компании) и выполните следующие действия:
1. В окне программы ViPNet Центр управления сетью в меню Доверенные сети выберите пункт Обработать межсетевую информацию.
2. В открывшемся окне выберите сеть Федеральной службы и нажмите кнопку Обработать выбранные.
3. Создайте и отправьте новые справочники и ключи для узла Директор.

Для проверки правильности выполнения задания перейдите узел Координатор Федеральной службы и убедитесь, что в списке узлов защищенной сети в программе ViPNet Coordinator Монитор отсутствует клиент Директор.

Вставьте скриншот, подтверждающий выполнение задания

Прекращение межсетевого взаимодействии

Формулировка задания

Прекратить межсетевое взаимодействия Компании и Федеральной службы.

Проверка правильности выполнения задания осуществляется в программе ViPNet Coordinator Монитор на узлах Координатор Центр офис и Координатор федеральной службы. В списке узлов защищенной сети на узлах должны отсутствовать клиенты и координаторы из других сетей.

Порядок выполнения задания

Чтобы прекратить межсетевое взаимодействие Компании и Федеральной службы, выполните следующие действия на рабочем месте Главный администратор (сеть Компании):

1. В окне программы ViPNet Центр управления сетью выберите представление Доверенные сети.
2. На панели навигации выберите раздел Свойства сетей.
3. На панели просмотра щелкните правой кнопкой мыши доверенную сеть Федеральная служба, межсетевое взаимодействие с которой требуется прекратить, и в контекстном меню выберите пункт Прекратить взаимодействие.
4. В окне подтверждения установите флажок Прекратить взаимодействие, затем нажмите кнопку Прекратить взаимодействие.

Вставьте скриншот, подтверждающий выполнение задания

В открывшемся окне Прекращение взаимодействия с выбранными сетями будет отображен процесс удаления данных об объектах доверенной сети и их связях с объектами вашей сети. Также информация о доверенной сети будет удалена в программе ViPNet Удостоверяющий и ключевой центр.

5. Создайте и отправьте новые справочники и ключи для узлов, которые были задействованы в межсетевом взаимодействии.

Аналогичные действия проделайте на рабочем месте Администратор сети ViPNet Федеральной службы.

Убедитесь, что связи между узлами Координатор Центр офис и Координатор Федеральной службы больше нет.

Вставьте скриншот, подтверждающий выполнение задания

Практическая работа № 13
Составить сравнительную характеристику программно-аппаратных средств для создания защищённой сети

Задание:

С помощью учебного пособия, конспекта, опыта выполнения практических работ и ресурсов Интернета заполнить следующую таблицу по программно-аппаратным решениям для создания защищённой сети

Продукт	Поддерживаемые операционные системы	Дата последнего обновления и последняя версия	Стоимость продукта	Протоколы, с которыми работает продукт	Достоинства	Недостатки
VipNet						
Крипто-						

Про						
Cisco VPN Solutions						
Traffic Inspector Next Generation						
Продукт на выбор						

Практическая работа № 14
Установка и настройка Traffic monitor

Задание:

Для работы с Инфовоч необходимо четыре виртуальные машины:

1. Машина с вашим доменом, например на WindowsServer2016. Поднять DNS и AD, настроить сетевые настройки
2. Машина с установленным ТМ на RedHut. Установка по описанию ниже.
3. Машина с установленным WindowsSever2016 для последующей установки DeviceMonitor
4. Машина с установленным Win10 для установки агента DeviceMonitor

Необходима настройка сетевых адаптеров.

Установить на всех 4-х компьютерах Сетевой мост.

Порядок установки:

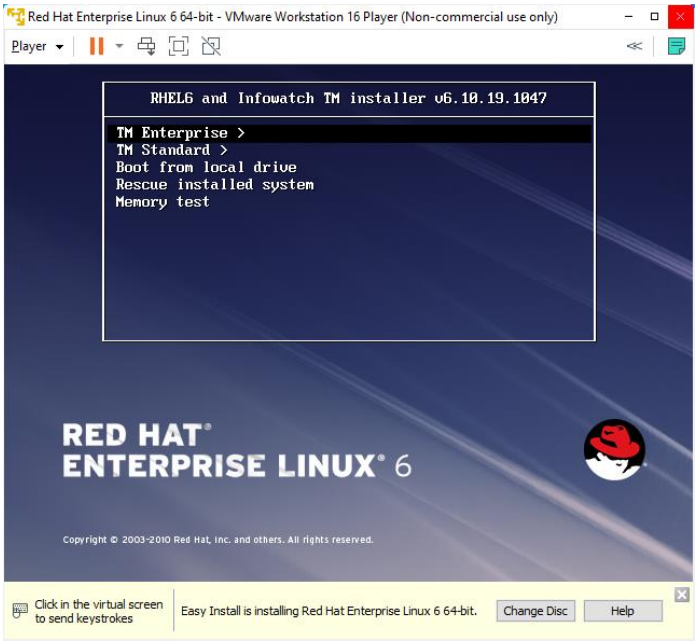
1. Установить WinServer2016 для домена установить, настроить сетевой адаптер, поднять роль DNS-сервера и AD, добавить несколько пользователей, перезапустить домен и оставить включенным
2. Установить WinServer2016 для DM. Настроить сетевой адаптер. Добавить в домен.
3. Используя дальше порядок установки установить RedHut с ТМ. Для данной виртуальной машины необходимо 8 Гб ОЗУ, 2 процессора, 100 Гб места на диске, сетевой адаптер – сетевой мост. Во время установки ввод сетевых настроек обязателен.

Пример сетевых настроек на всех 4-х виртуальных машинах:

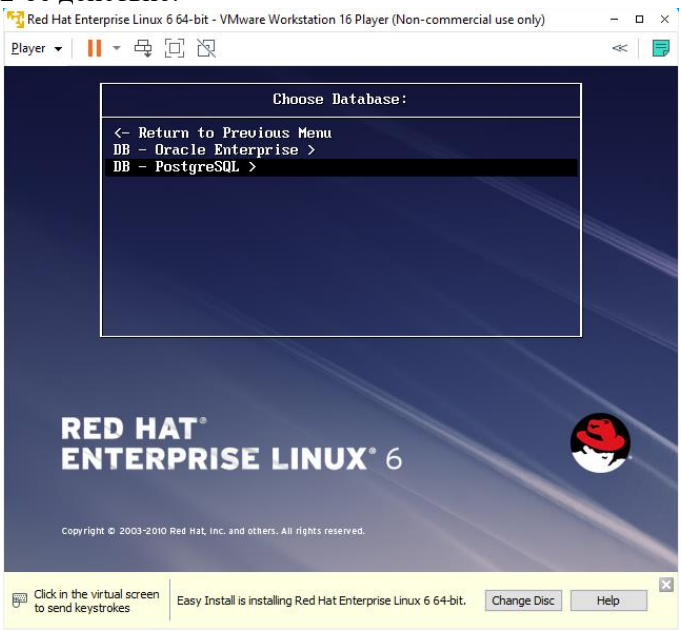
Физический ПК1	Физический ПК2
Домен Ip-адрес: 192.168.6.60 Маска: 255.255.255.0 Шлюз: 192.168.6.1. DNS1: 192.168.2.51 DNS2: 8.8.8.8	WinServer2016 для DM Ip-адрес: 192.168.6.62 Маска: 255.255.255.0 Шлюз: 192.168.6.1. DNS1: 192.168.6.60
Win10 Ip-адрес: 192.168.6.61 Маска: 255.255.255.0 Шлюз: 192.168.6.1. DNS1: 192.168.6.60	RedHut с ТМ Ip-адрес: 192.168.6.63 Маска: 255.255.255.0 Шлюз: 192.168.6.1. DNS1: 192.168.6.60

Установить InfoWatch Traffic Monitor Enterprise:

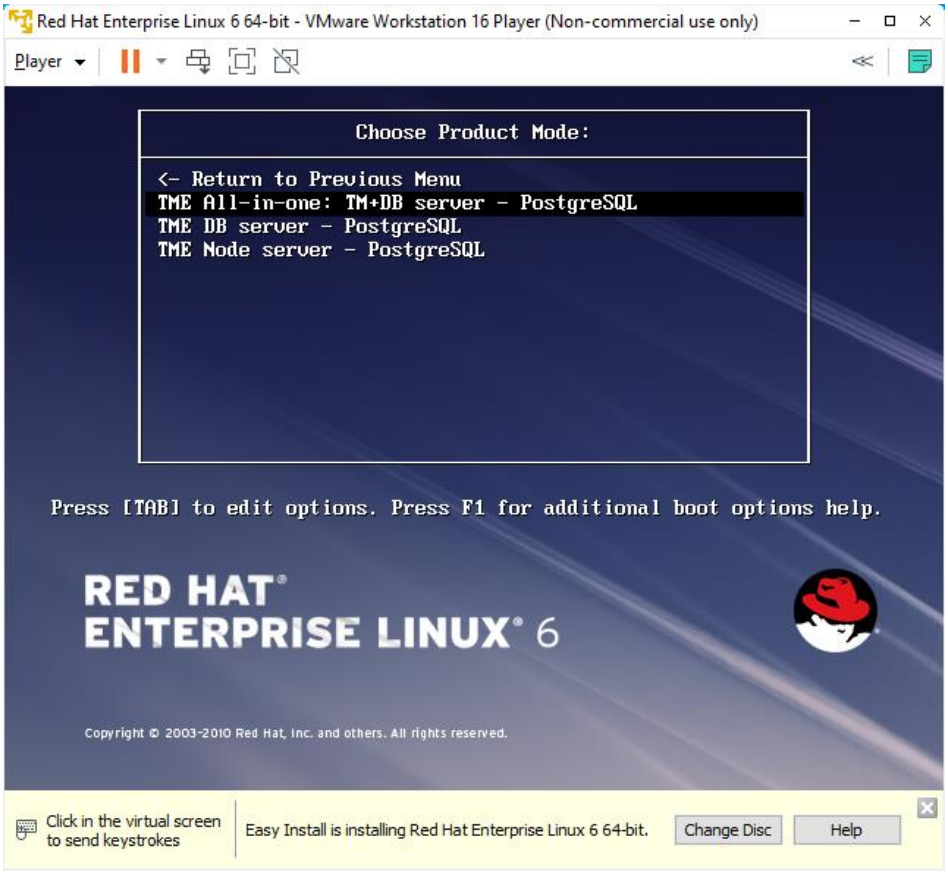
1-ое действие:



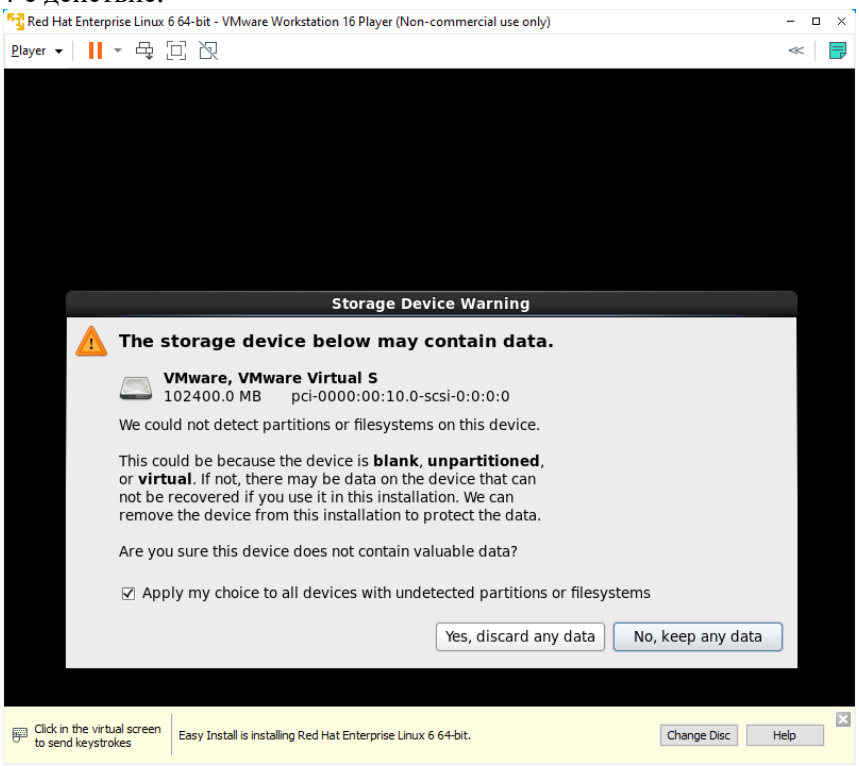
2-ое действие:



3-е действие:

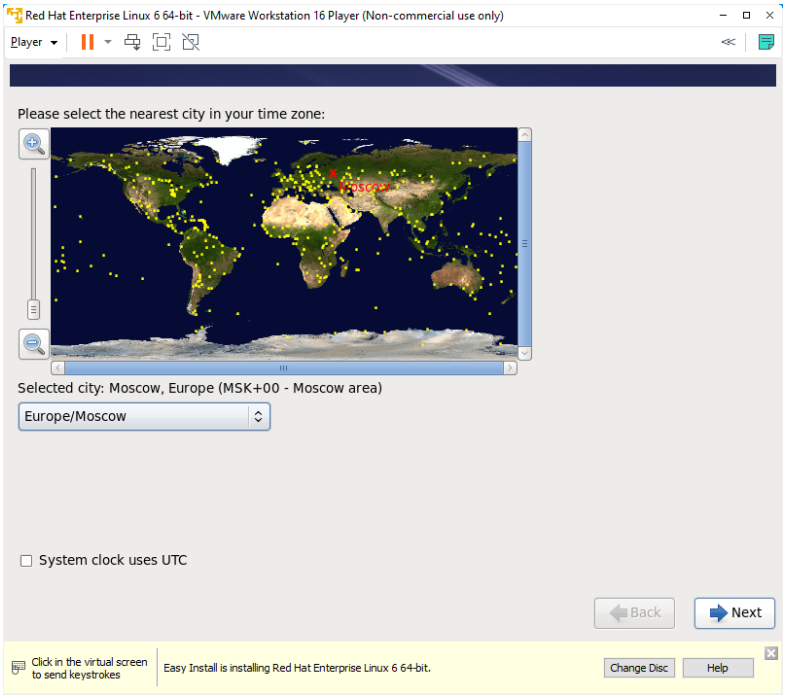


4-е действие:

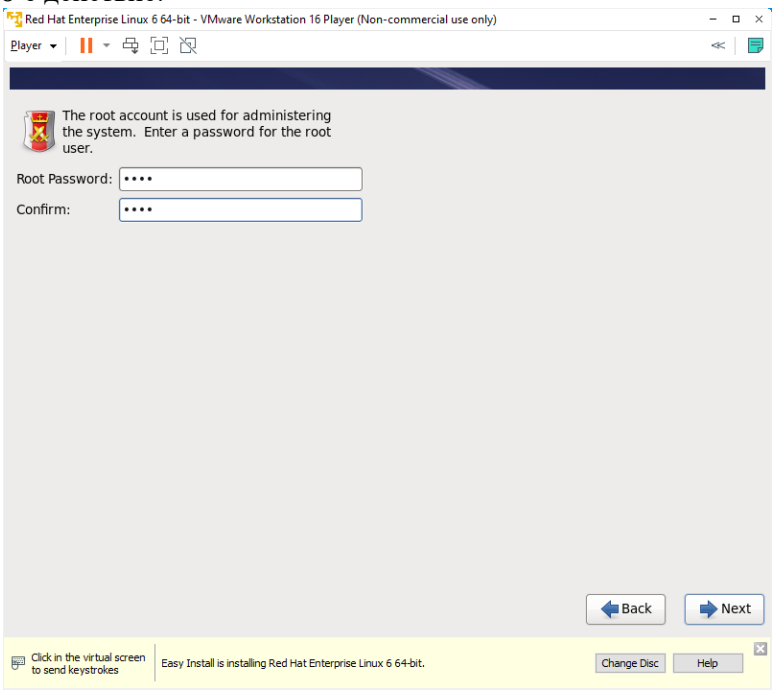


ВЫБИРАЕМ “Yes, discard any data”

5-е действие:

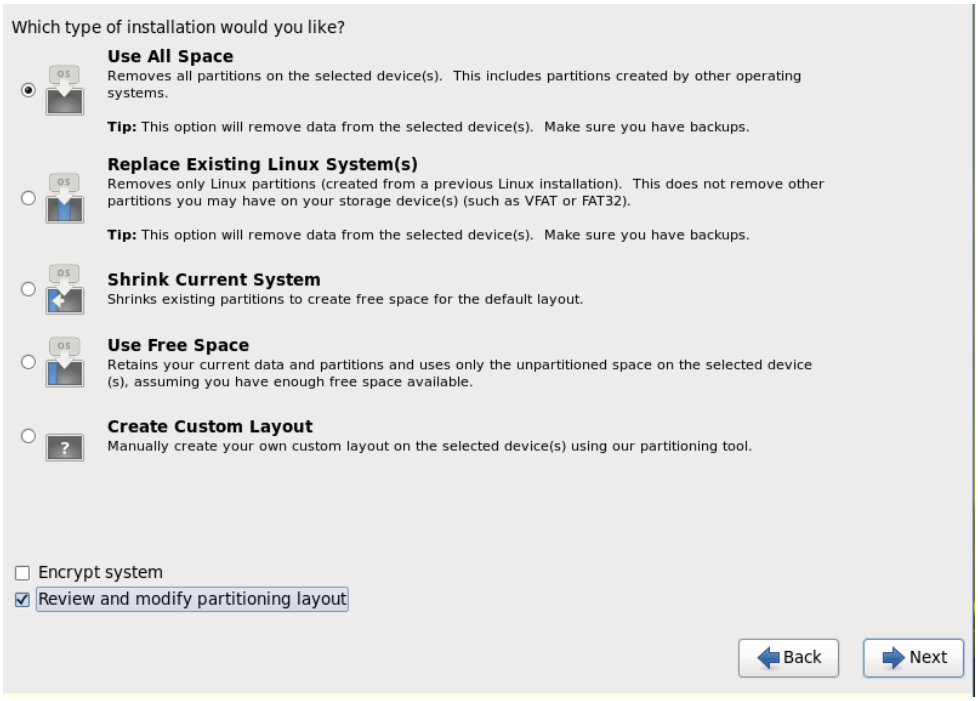


6-е действие:

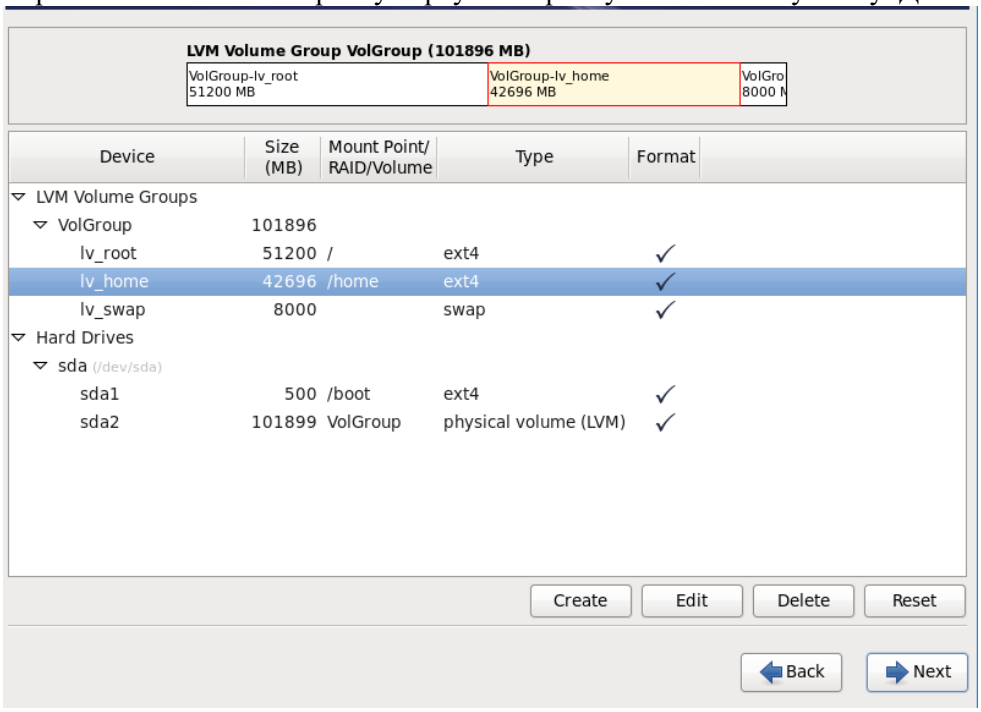


Не забываем написанный пароль. Пароль не менее 8-ми символов

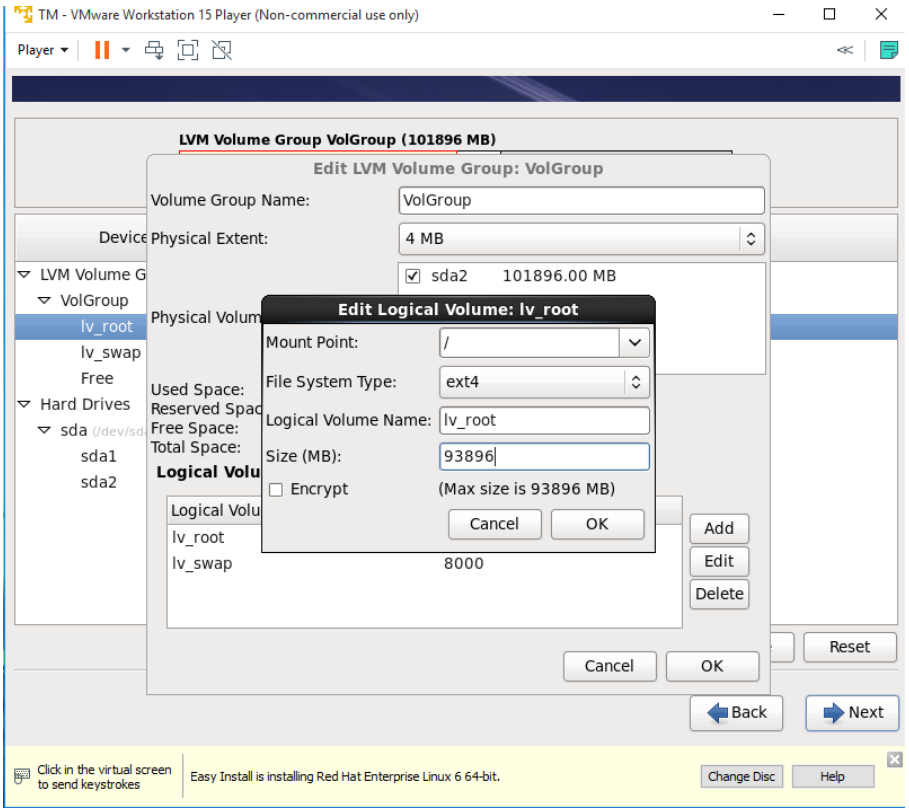
7-е действие:



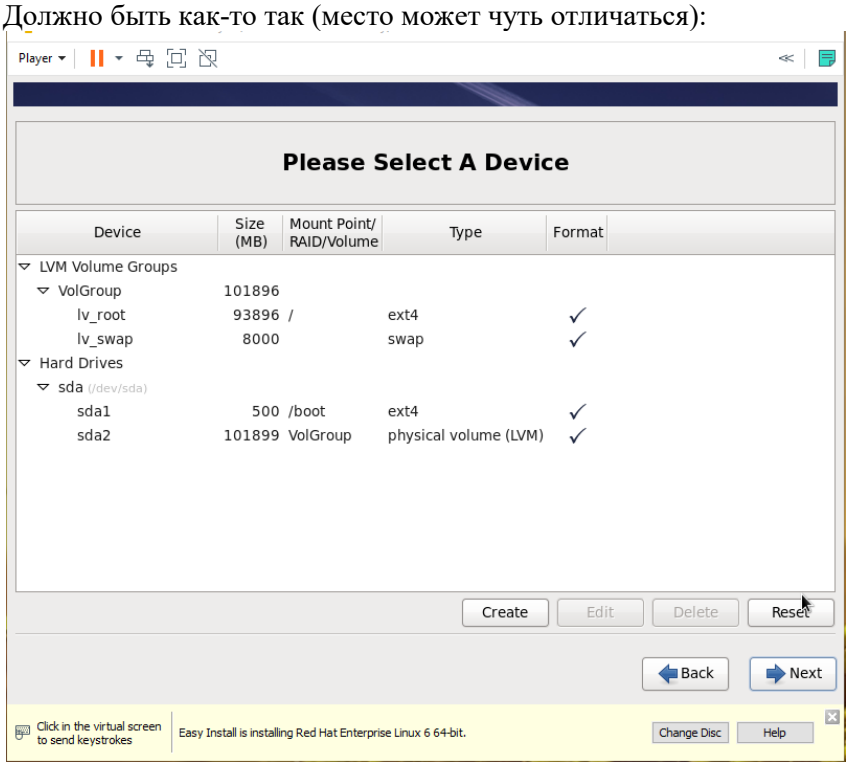
Обратите внимание на строчку первую выбранную и на галочку внизу. Далее



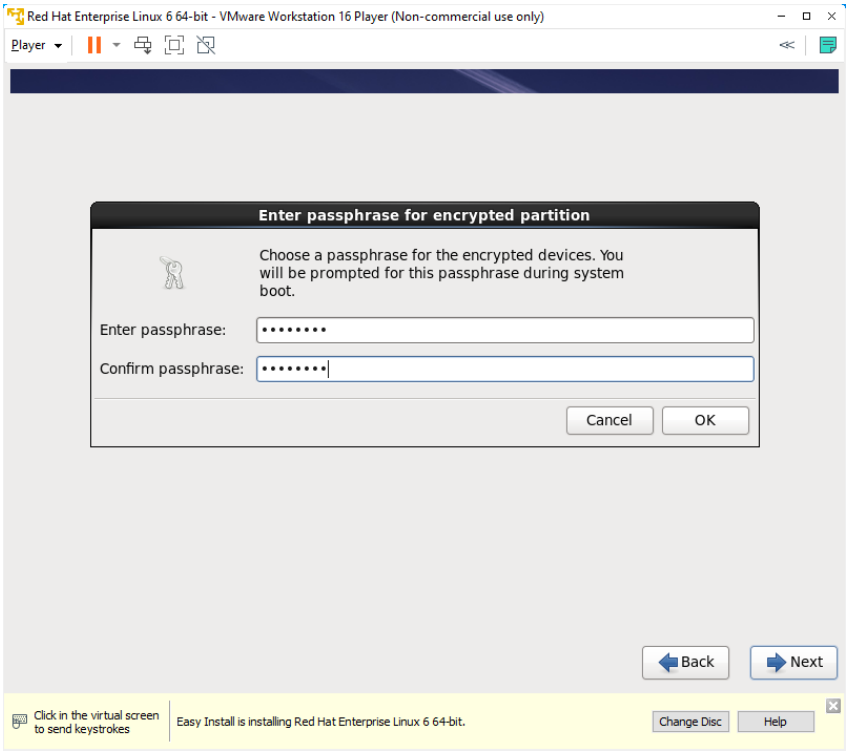
Раздел домашний удалить, а рутовскому разделу с помощью Правки отдать всё место:



Должно быть как-то так (место может чуть отличаться):



8-е действие:

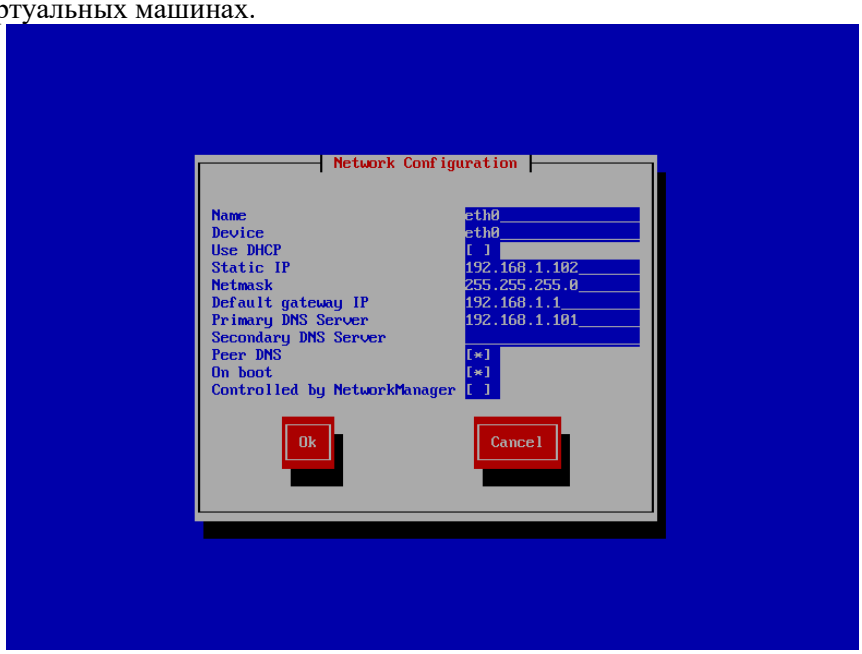


Пишем кодовую фразу, не менее 8-ми символов (12345678)

Далее согласиться с форматированием и смотреть на процесс установки ☺

9-е действие:

настраиваем сетевые настройки, используя пример выше, но учитывая ваши настройки на других виртуальных машинах.



Клавиша ПРОБЕЛ использовать для установки статического адреса, далее когда настройки все установлены клавишей Tab двигаться до ОК

10-е действие:

На след.окне просто Соглашаться и Сохранять.

На всех след. Окнах соглашаться и Сохранять.

Далее будет установка. Сидим и ждём.

Когда машина установится появится приветственная строка в ожидании вашего логина

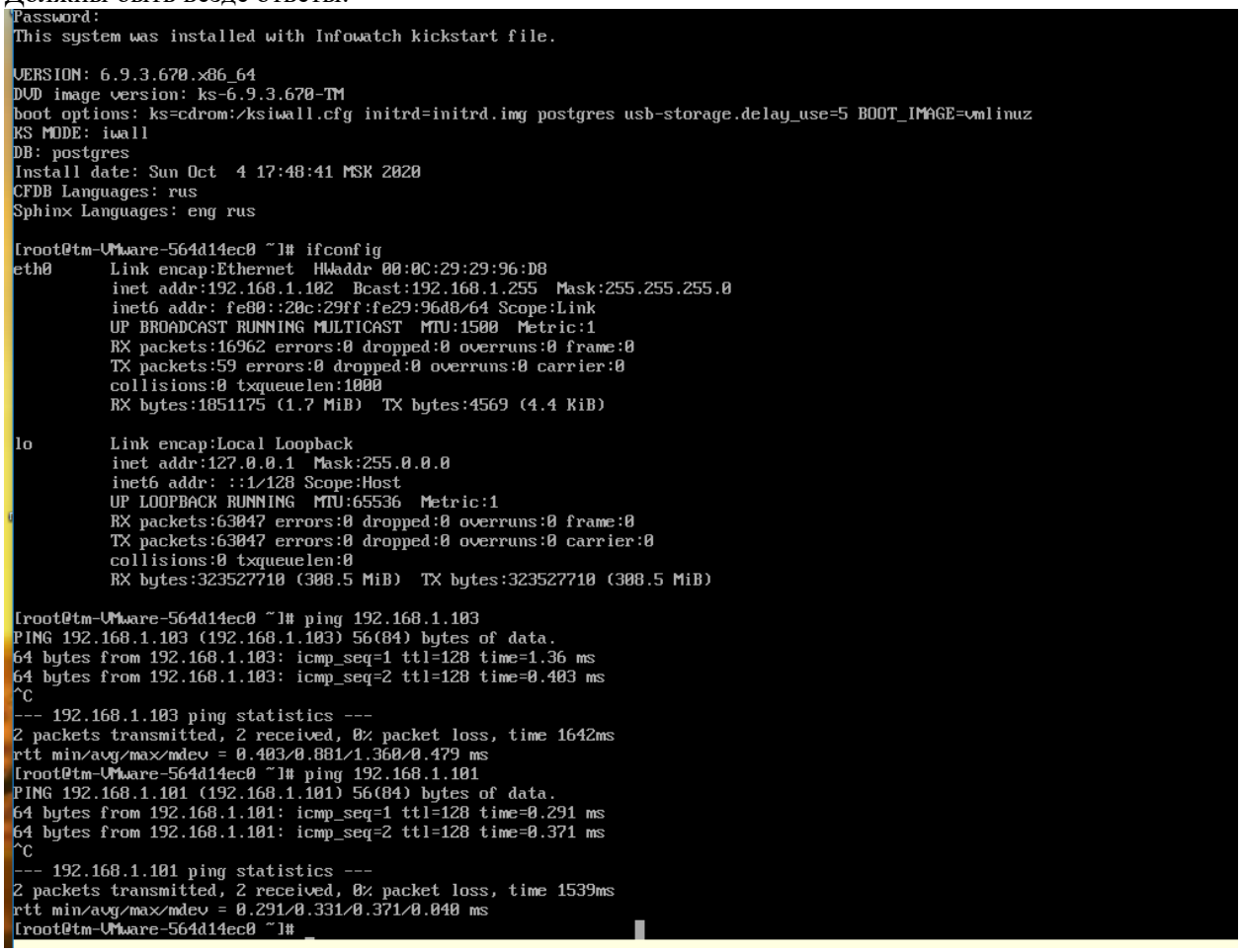
Пишем root и ваш пароль

Нажимаем Enter.

После этого вы должны увидеть строку ожидающую команд.

Проверьте командой ifconfig сетевые настройки, затем выполните ping машины вашего домена и машины для DM.

Должны быть везде ответы:



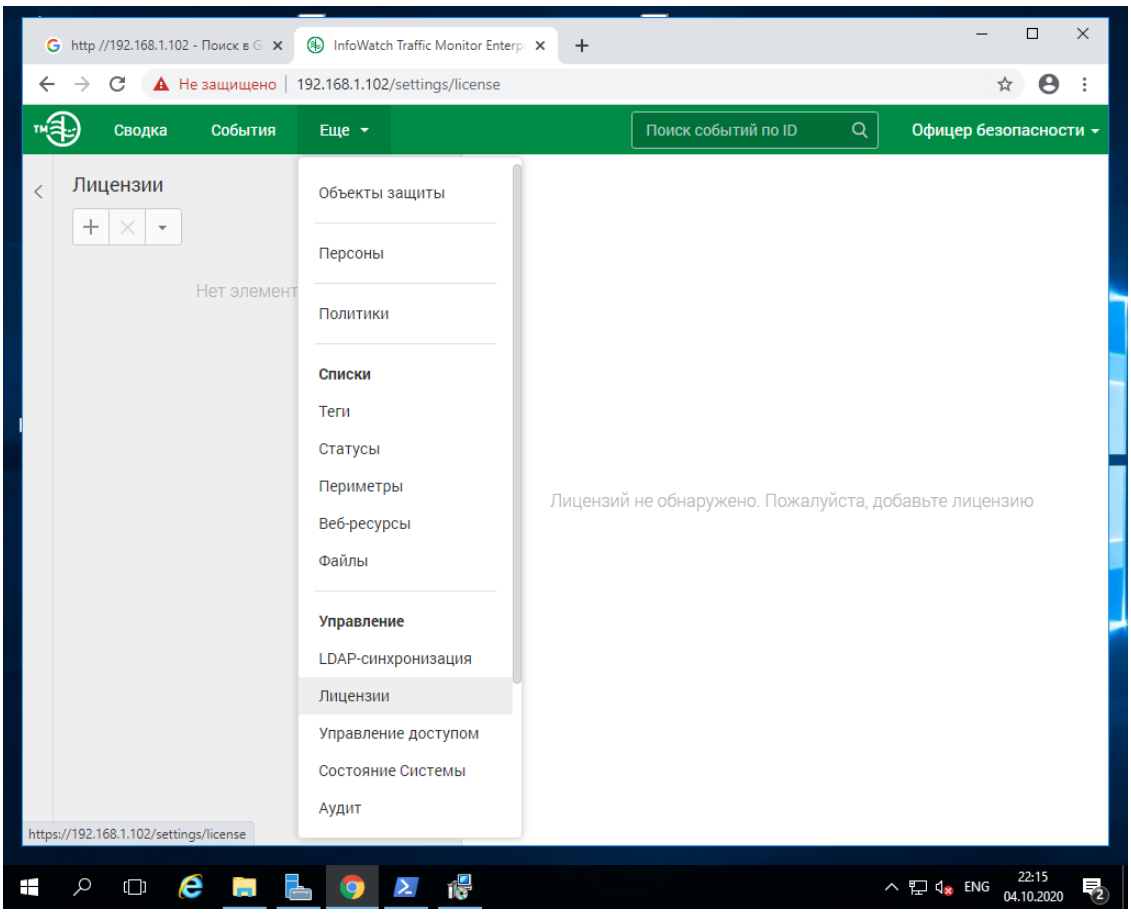
Практическая работа № 15
Настройка Traffic monitor

Задание:

Установите 

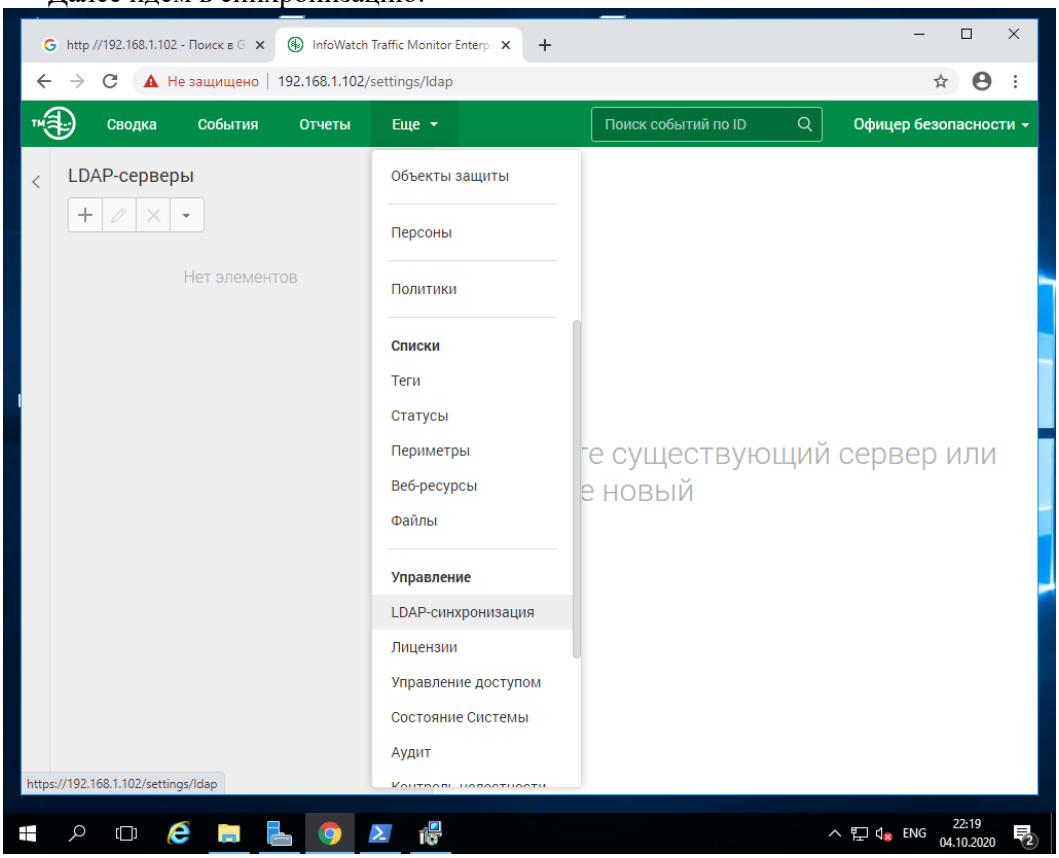
на машину для DM

- Далее в хроме напишите айпи-адрес машины ТМ: например: http:\\192.168.1.102\
- Далее ДОПОЛНИТЕЛЬНО
- Далее ВСЁ РАВНО ПЕРЕЙТИ
- Перед вами должно появиться зелёное окно с ТМ
- Далее идём ставить лицензию:

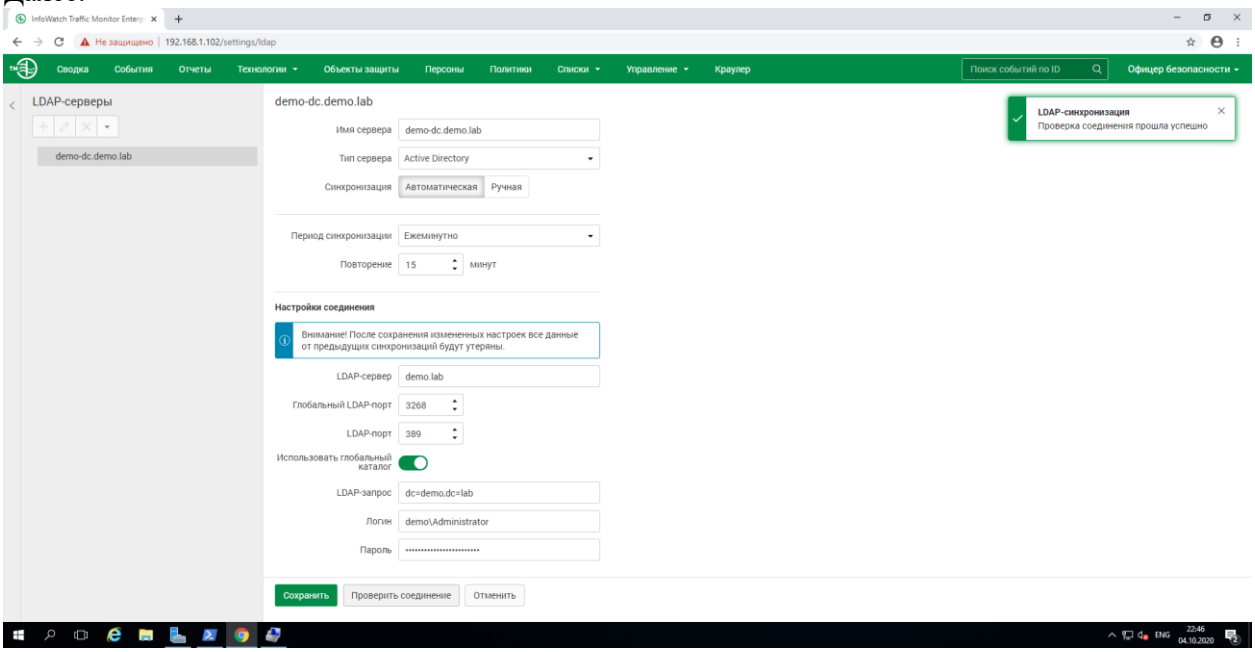


— Нажимаем Плюс
— Выбираем файл лицензии
— Листаем в самый низ когда лицензия загрузилась и нажимаем Сохранить.
— Справа в лицензиях должна появиться лицензия, далее страница сама перезагрузится.

Далее идем в синхронизацию:



Далее:



Обратите внимание на все поля!!!!! Заполнить их в соответствии с настройками вашего домена.
Имя сервера – это меня машины ПК домена, LDAP-сервер — это имя домена, иногда работает при айпи-адресе вместо имени домена.
Далее проверить и Сохранить при успешной синхронизации
<u>В отчёте необходимы следующие скриншоты:</u>

- Настроенного домена
- Установленной машины с DM, входящей в домен
- Пинги с ответами на всех компьютерах
- Установленная лицензия на TM
- Выполненная синхронизация на TM

Задание 2:
С помощью документации ответить на следующие вопросы:

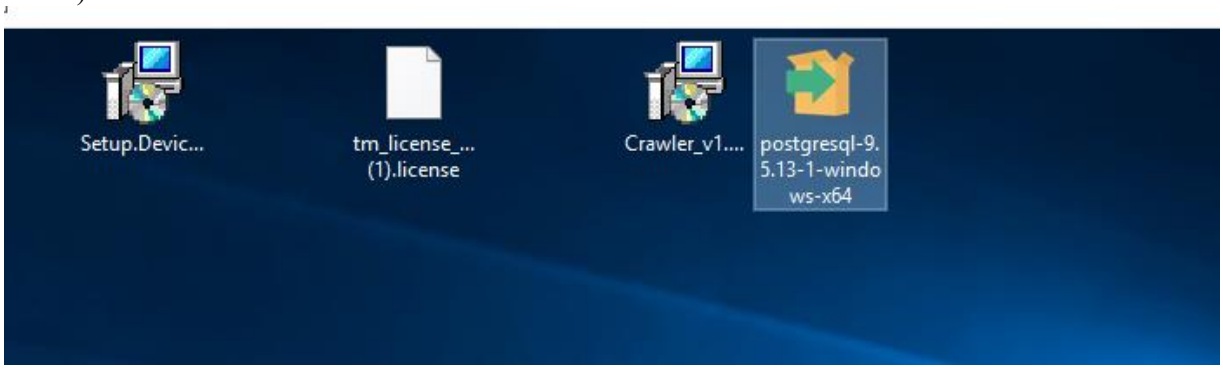
- ✓ Перечислите отличия IW TM 6 Enterprice от IW TM 6 Standart.
- ✓ В каких случаях рекомендуется отдельная установка сервера TM и сервера базы данных?
- ✓ К какому внутреннему формату приводятся объекты в системе IW TM 6?
- ✓ Какие СУБД поддерживаются системой IW TM 6?
- ✓ За прием каких данных отвечают компоненты sniffer и proxy?
- ✓ Какая компонента системы IW TM 6 извлекает текст из полученного объекта?
- ✓ Какая компонента системы IW TM 6 отвечает за запуск технологий анализа?
- ✓ В какой файл прописываются политики информационной безопасности?
- ✓ Для чего в системе используется формат 2liro?
- ✓ Для чего используется связка компонент системы SMTPD и Deliverd?

Ответы:
…

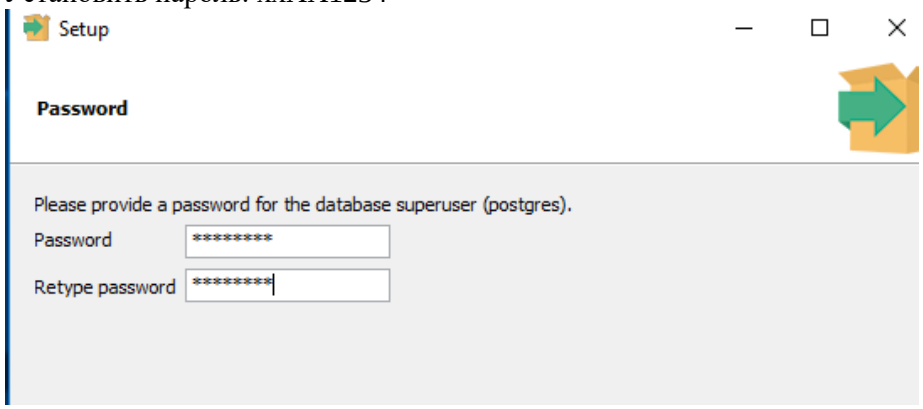
Практическая работа № 16
Установка Device monitor

Задание:

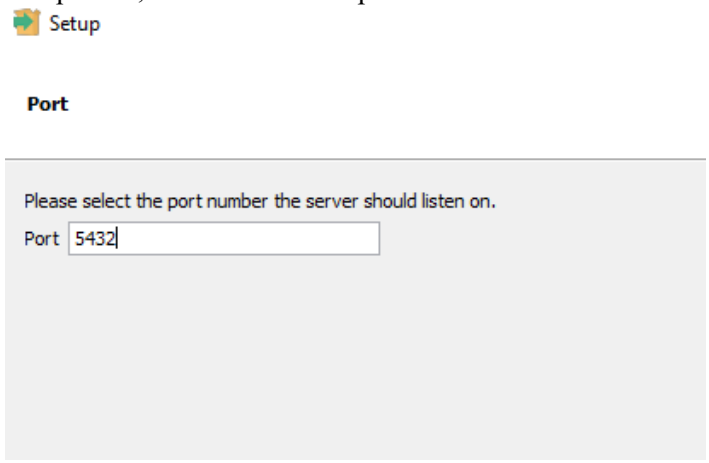
Установка серверной части InfoWatch Device Monitor.
В состав серверной части входят следующие компоненты:
✓ база данных,
✓ сервер InfoWatch Device Monitor,
✓ консоль управления InfoWatch Device Monitor.
Серверная часть InfoWatch Device Monitor устанавливается при помощи универсальной программы установки.
Для управления базой данных будем использовать СУБД PostgreSQL.
Запустить машину с сервером 2016 для DM.
Скопировать из сети на Рабочий стол машины DM следующий софт (у вас более новые версии в папке):



Далее запустить установку Postgresql
Установить пароль: xxXX1234

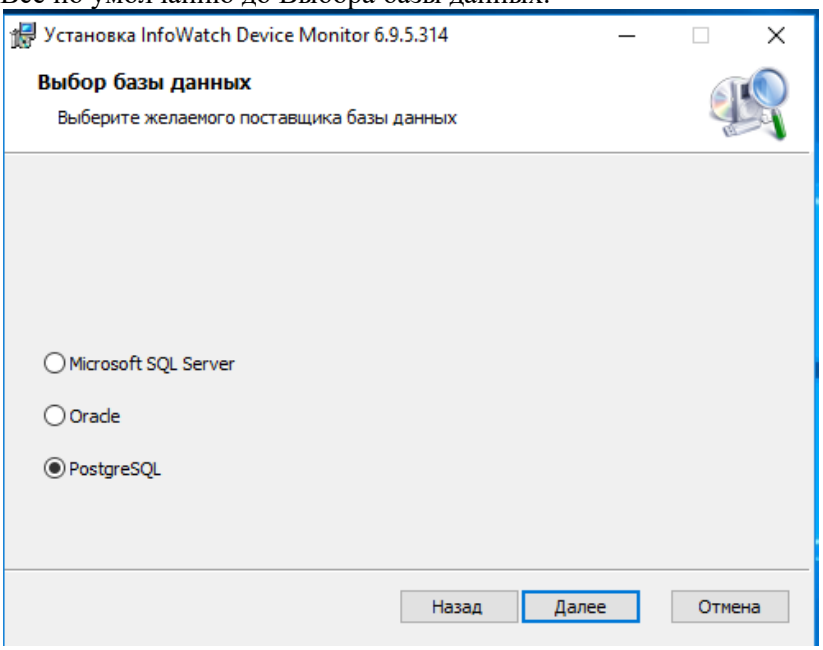


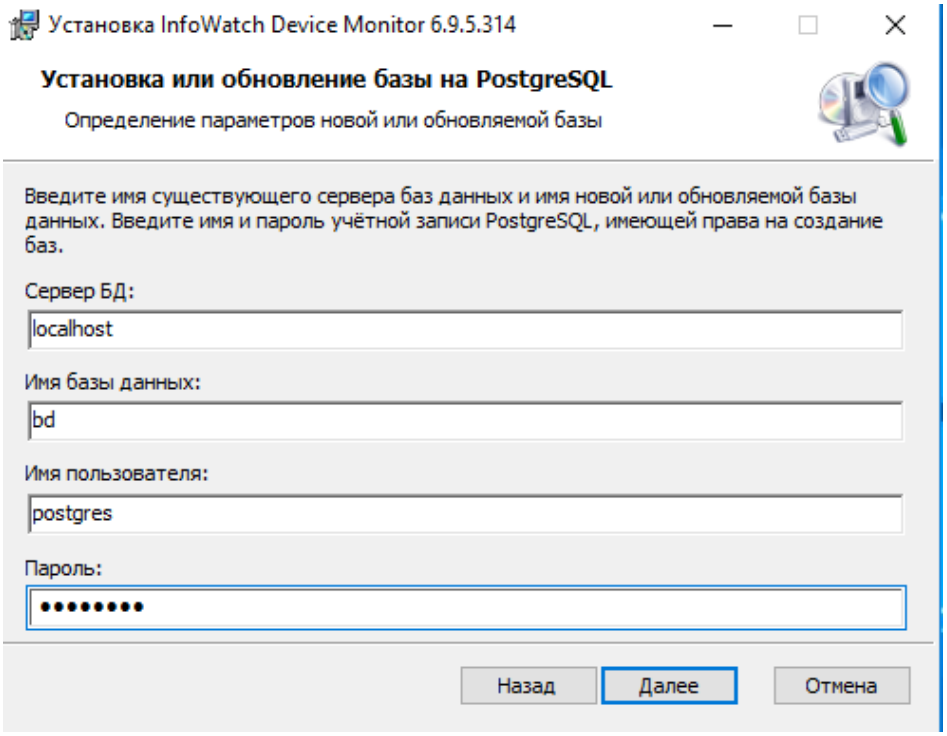
Не трогать, но запомнить порт:



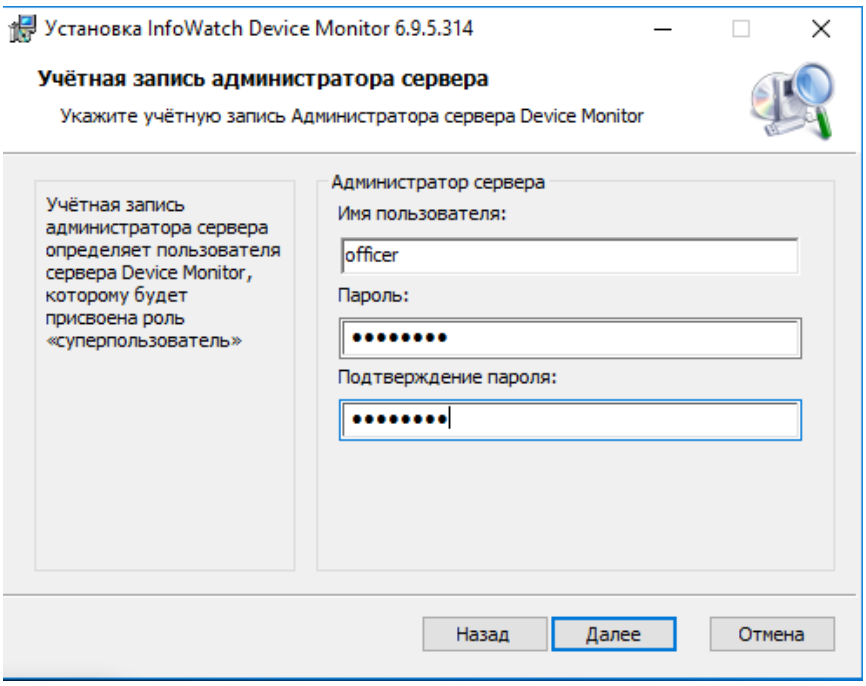
Далее по умолчанию.

Далее устанавливаем DeviceMonitor
Всё по умолчанию до Выбора базы данных:



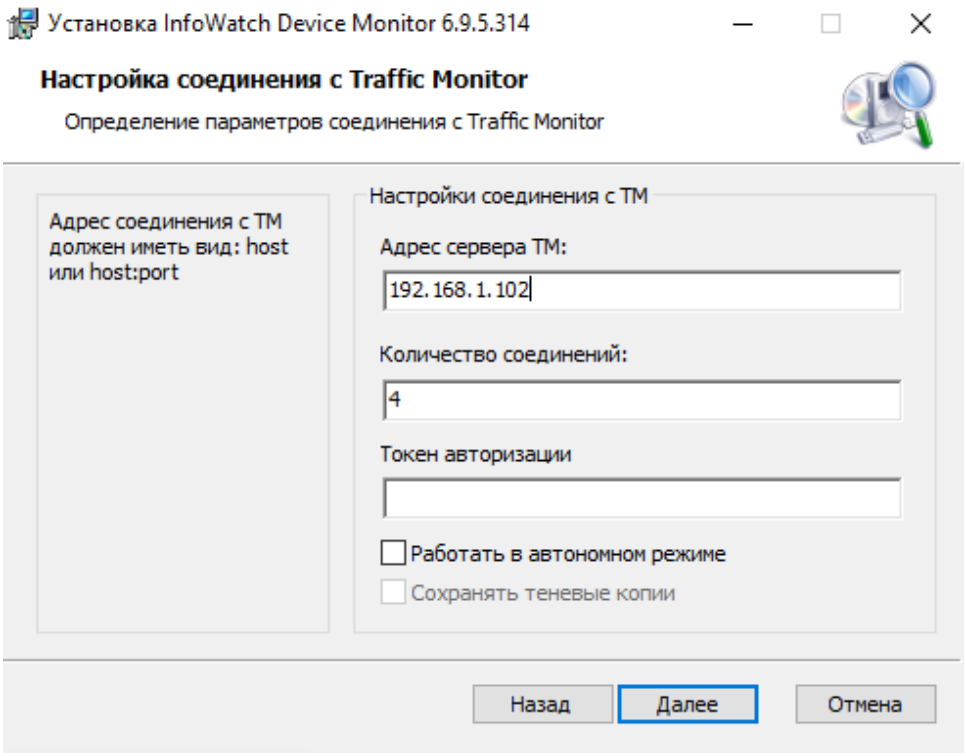


Пароль: xxXX1234
Далее по умолчанию.
Ключ можно сохранить на Рабочем столе.
Далее:



Пароль xxXX1234

Далее:

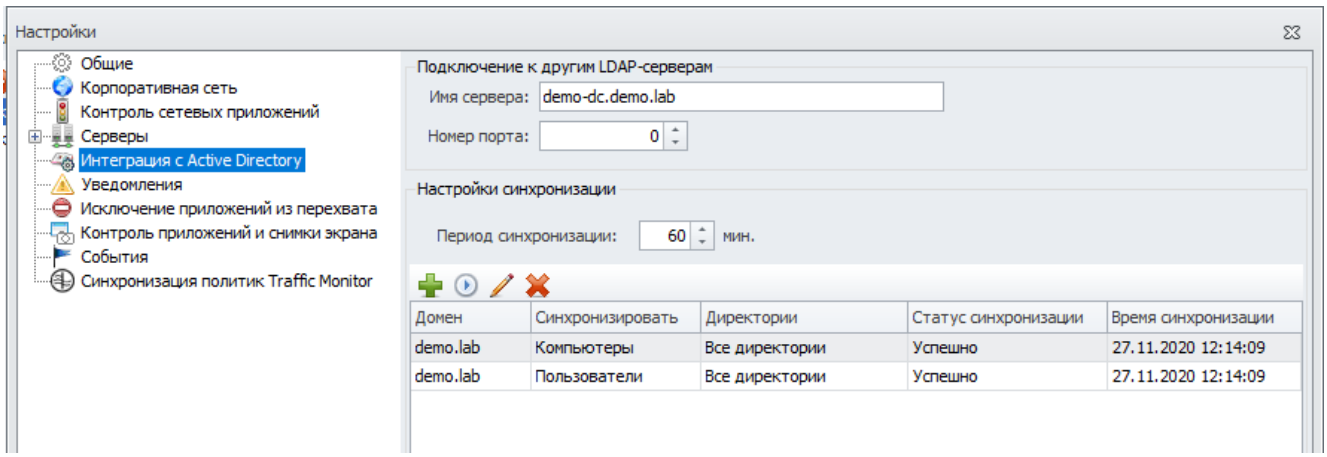


Токен авторизации можно скопировать с ТМ: Ещё → Управление → Плагины → Токен.

Практическая работа № 17
Настройка Device monitor

Задание 1:

Запустить установившуюся консоль, войти в неё.
Настроить синхронизацию для компьютеров и пользователей с вашим доменом, а также проверить синхронизацию с ТМ: (Настройки –Серверы, Интеграция и Синхронизация политик ТМ)



В отчёте должны быть следующие скриншоты:
— Установленной консоли
— Запущенной работающей консоли
— Успешной синхронизации с компьютерами и пользователями
— Успешной синхронизации с политиками ТМ

Практическая работа № 18
Установка клиента Device monitor

Задание:

Установку Агента может выполнять пользователь, имеющий права локального администратора на том компьютере, на который выполняется установка.
Запуск мастера установки
Откройте каталог Client. В данном каталоге найдите и запустите файл установки для требуемой платформы.
В результате на экран будет выведено окно приветствия мастера установки InfoWatch Device Monitor Client. Нажмите на кнопку Далее, чтобы перейти к следующему окну мастера установки.
Настройка параметров
Укажите параметры соединения с Сервером InfoWatch Device Monitor:
Сервер. Имя сервера InfoWatch Device Monitor.
Порт. Номер порта, используемого для соединения между Агентом и Сервером InfoWatch Device Monitor (по умолчанию задан порт 15101).
Нажмите кнопку Далее.
Завершение установки
После перехода к окну Подтверждение установки, нажмите кнопку Далее, чтобы начать установку Агента. Следуйте дальнейшим указаниям мастера для завершения установки.
По окончании установки перезагрузите компьютер.

Вставьте скриншот, подтверждающий выполнение задания

Практическая работа № 19
Установка и настройка Crawler

Задание:

Установить InfoWatch.Crawler.Scanner.

Пояснение:

Перехватчик Краулер реализован в виде двух служб Windows:

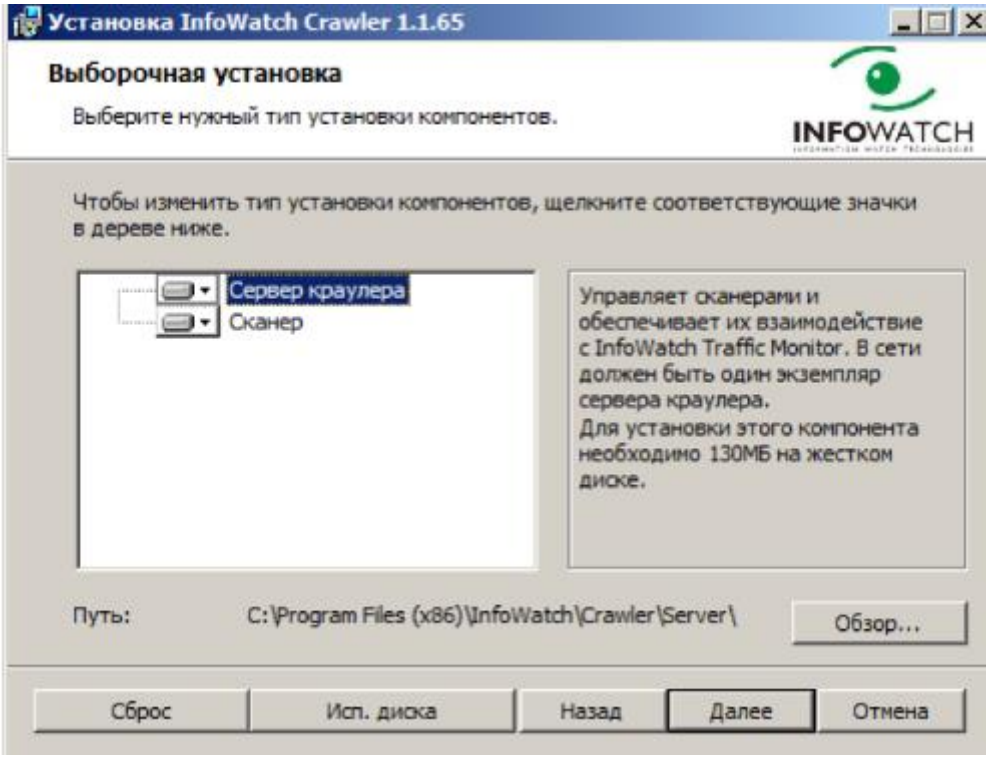
✓ InfoWatch.Crawler.Scanner – выполняет сканирование сетевых папок и файловых хранилищ согласно заданным пользователем параметрам;

✓ InfoWatch.Crawler.Server – управляет службой сканирования и обеспечивает связь с Консолью управления Traffic Monitor;

Порядок выполнения работы:

1. Чтобы установить Краулер:

Запустите установочный пакет Crawler_vx.x.xxx.msi, где x.x.xxx – номер версии.



2. После установки компонента Сервер запустите его, выполнив следующие действия:
подключитесь к серверу, на котором установлен пакет iwtm-webgui;

в файле web.conf, расположенном в директории /opt/iw/tm5/etc, измените значение параметра enabled секции crawler с "0" на "1";

выполните команду service iwtm restart kicker.

Вставьте скриншот, подтверждающий выполнение задания

Практическая работа № 20
Создание простых правил и проверка их работоспособности в Device monitor

Задание 1:

При работе с Консолью управления требуется постоянное соединение с Сервером InfoWatch Device Monitor. Для этого необходимо выполнить авторизацию, в процессе которой определяются права пользователя на запуск Консоли управления.

При первом запуске Консоли управления используются данные (имя пользователя и пароль) учетной записи, которой назначена роль Суперпользователь (учетная запись Суперпользователя создается в процессе установки Сервера.

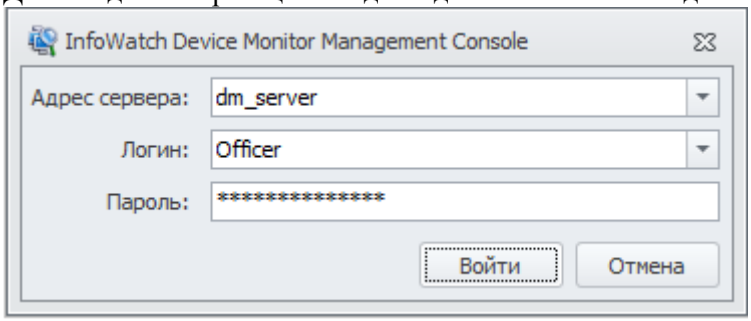
Чтобы начать работу с Консолью управления:

Запустите Консоль управления (DM). Для этого в меню Пуск выберите пункт Программы → InfoWatch → Device Monitor → Консоль управления либо используйте ярлык на рабочем столе (создается по умолчанию при установке).

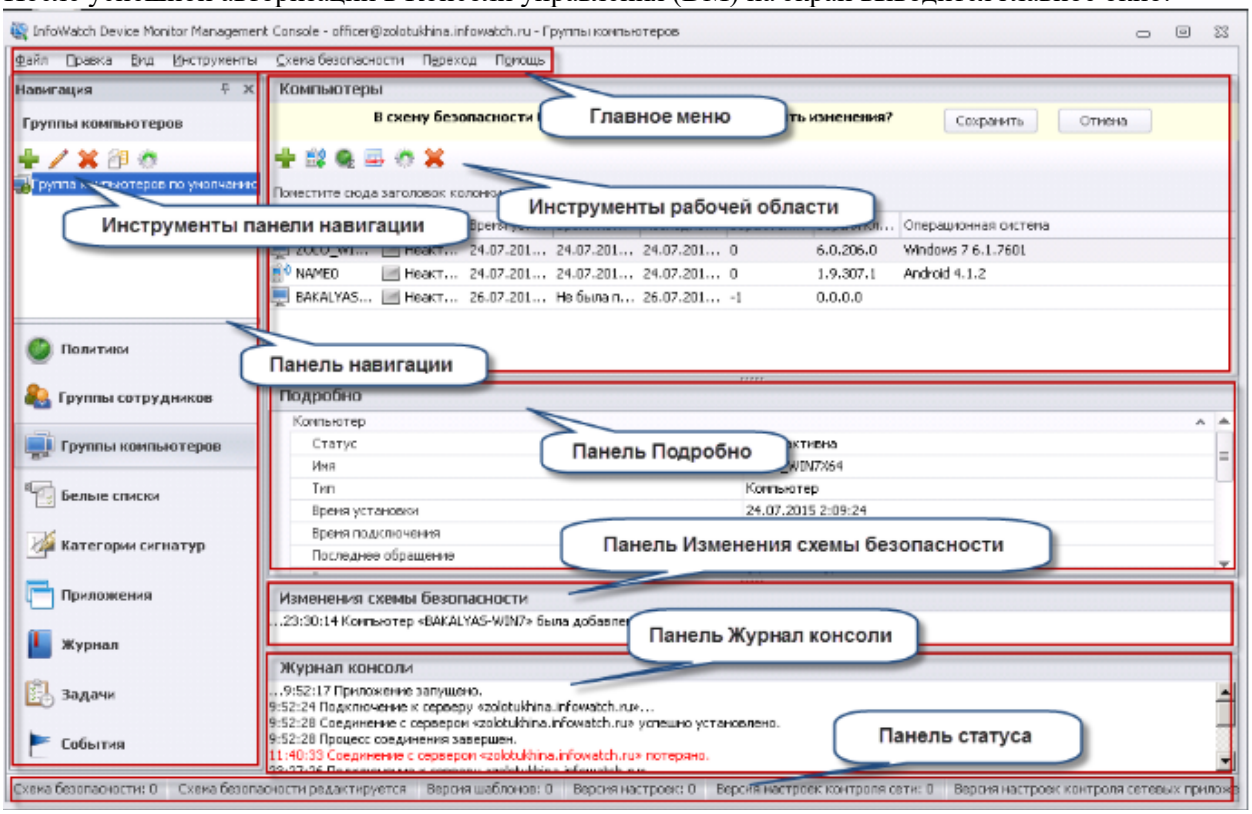
Выполните процедуру авторизации, как описано ниже.
Успешное прохождение авторизации возможно только при выполнении следующих условий:

- ✓ в базе данных существует учетная запись с указанными параметрами;
- ✓ учетной записи назначена роль;
- ✓ учетная запись является активной (не удалена);
- ✓ учетная запись не заблокирована.

Данные для авторизации вводят в диалоговом окне подключения.



После успешной авторизации в Консоли управления (DM) на экран выводится главное окно:



Вставьте скриншот, подтверждающий выполнение задания

Задание 2. Создание правил в Консоли управления (DM):

1. Необходимо создать новую политику (кроме политики на устройства по умолчанию), назвав ее «Чемпионат», применить ее к группе компьютеров по умолчанию. Последующие правила по заданиям должны быть добавлены в эту политику.
   Зафиксировать выполнение скриншотом.
2. Необходимо запретить пользоваться Microsoft Paint, а также Paint 3D (при наличии), так как участились случаи подделки печатей компании.
   Проверить работоспособность и зафиксировать выполнение скриншотом.

3. Необходимо запретить создание снимков экрана в табличных процессорах (Excel) и калькуляторе для предотвращения утечки секретных расчетов и баз данных.
   Проверить работоспособность и зафиксировать выполнение скриншотом.
4. Необходимо запретить печать на сетевых принтерах, но при этом оставить возможность печати на локальных принтерах.
   Зафиксировать создание политики скриншотом.

Практическая работа № 21
Создание правил с использованием «белых» и «чёрных» списков в Device monitor

Задание:

Создать следующие правила:

1. Необходимо запретить запись файлов на все съемные носители информации (флешки), оставив возможность чтения и копирования с них.
   Проверить работоспособность и зафиксировать выполнение скриншотом.
2. С учетом ранее созданной политики необходимо разрешить запись файлов на доверенный носитель. Запрет на запись на остальные носители оставить в силе.
   Проверить работоспособность и зафиксировать настройку и выполнение скриншотами.
3. Создать политику по блокировке копирования исполняемых exe-файлов на USB-накопители. Проверить работоспособность и зафиксировать выполнение (зафиксировать результаты в виде скриншотов). Удалить (или отключить) созданную политику, так как она может мешать выполнения следующих заданий.
   Проверить работоспособность и зафиксировать выполнение скриншотом.
4. Необходимо установить контроль за компьютером потенциального нарушителя в случае использования браузера Google Chrome путем создания снимков экрана каждые 15 секунд или при переходе на другую страницу.
   Проверить работоспособность и зафиксировать выполнение: продемонстрировать, что снимки экрана из задания появляются в консоли IWTM. Подтвердить выполнение задания скриншотами.
5. Заблокируйте доступ к CD/DVD, MTP-устройствам и дискетам на клиентском компьютере (виртуальной машине).
   Проверить работоспособность и зафиксировать выполнение скриншотом.
6. Осуществить выдачу временного доступа (30 минут) клиенту до заблокированного CD привода.
   Зафиксировать скриншотами факт выдачи доступа и необходимые действия в IWDM.
7. На виртуальной машине необходимо запретить использование буфера обмена при подключении к удаленным машинам по протоколу RDP, а в группе компьютеров по умолчанию необходимо контролировать буфер обмена при копировании из/в терминальных сессий.
   Проверить работоспособность и зафиксировать выполнение скриншотом как блокировки, так и контроля.
8. Необходимо установить (сменить) пароль для удаления Device Monitor Agent виртуальной машины-нарушителя с помощью средств DeviceMonitor Server (удаленно).
   Проверить работоспособность и зафиксировать выполнение скриншотом

Практическая работа № 20
Создание объектов защиты в Traffic monitor

Задание:

Установить InfoWatch.Crawler.Scanner.

Пояснение:

Перехватчик Краулер реализован в виде двух служб Windows:

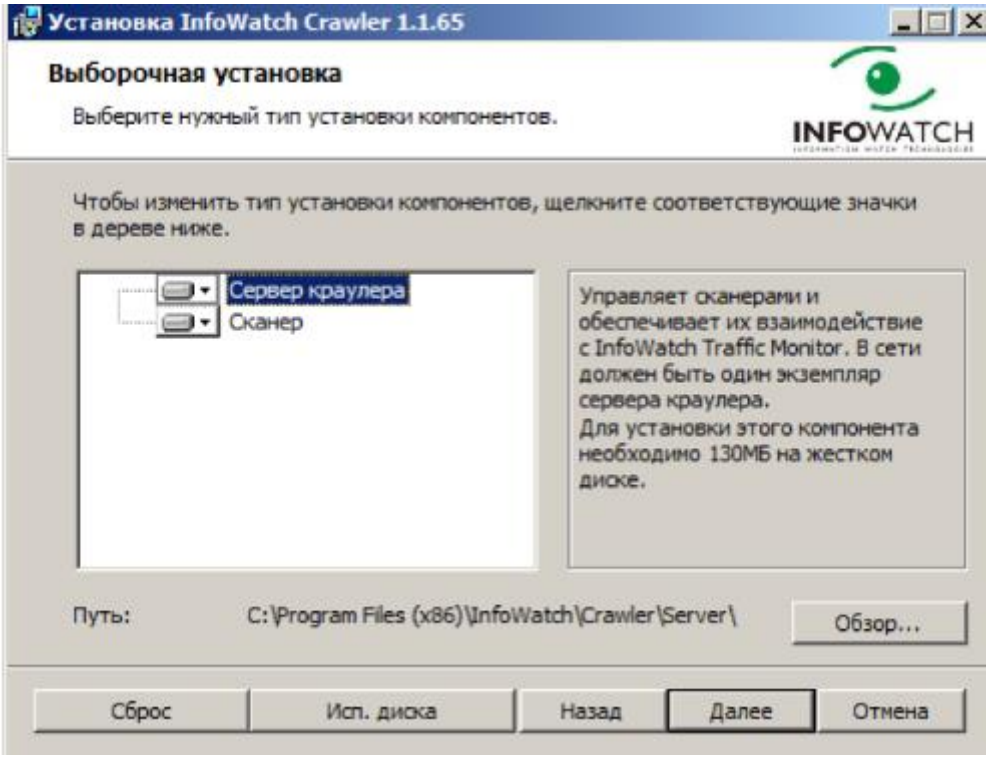
✓ InfoWatch.Crawler.Scanner – выполняет сканирование сетевых папок и файловых хранилищ согласно заданным пользователем параметрам;

✓ InfoWatch.Crawler.Server – управляет службой сканирования и обеспечивает связь с Консолью управления Traffic Monitor;

Порядок выполнения работы:

3. Чтобы установить Краулер:

Запустите установочный пакет Crawler_vx.x.xxx.msi, где x.x.xxx – номер версии.



4. После установки компонента Сервер запустите его, выполнив следующие действия:
подключитесь к серверу, на котором установлен пакет iwtm-webgui;

в файле web.conf, расположенном в директории /opt/iw/tm5/etc, измените значение параметра enabled секции crawler с "0" на "1";

выполните команду service iwtm restart kicker.

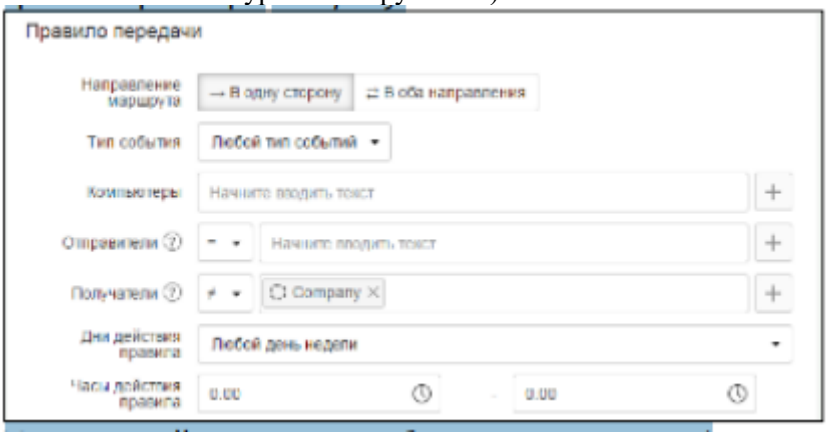
Вставьте скриншот, подтверждающий выполнение задания

Практическая работа № 21
Изменение объектов защиты в Traffic monitor

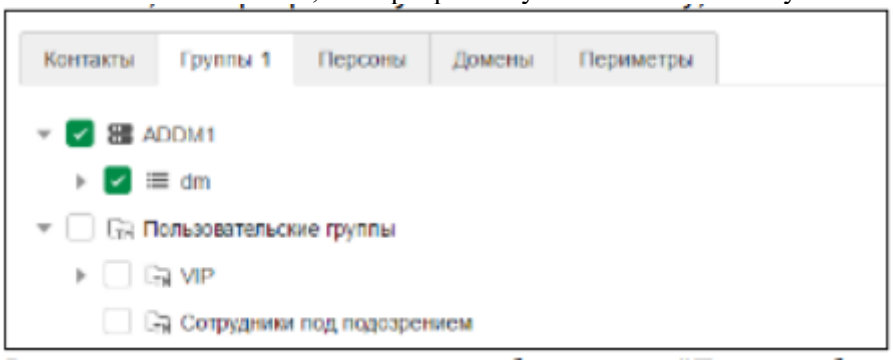
Задание:

1. Требуется контролировать передачу устава компании за пределы компании, в том числе отправку документа по электронной почте и копирование на съемные носители. Для этого:
   - ✓ Создайте политику защиты данных "Защита передачи устава организации".
   - ✓ В качестве защищаемых данных укажите объект защиты "Устав организации".
   - ✓ Добавьте правило передачи, контролирующее передачу данных любым получателям, кроме периметра Company.

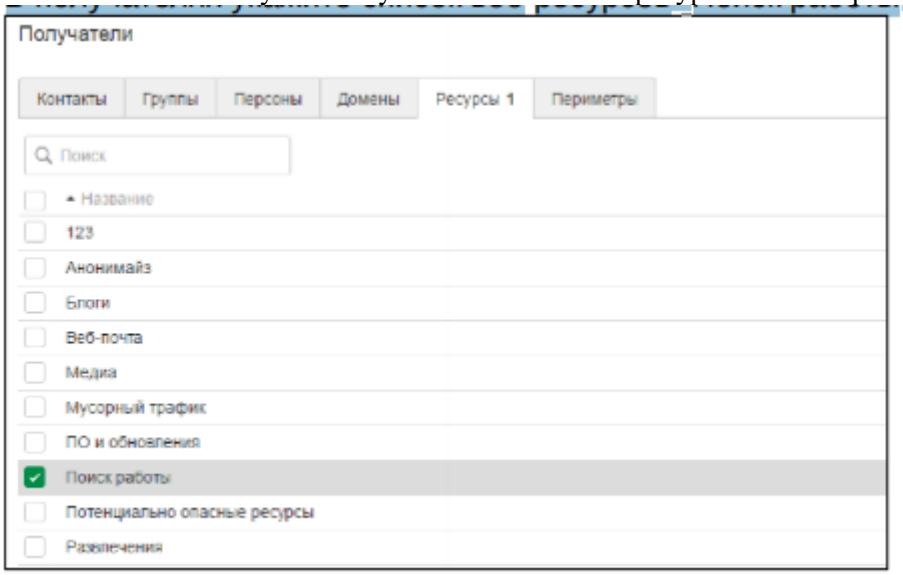
- ✓ Укажите действия при срабатывании правила (например, назначить событию низкий уровень нарушения).



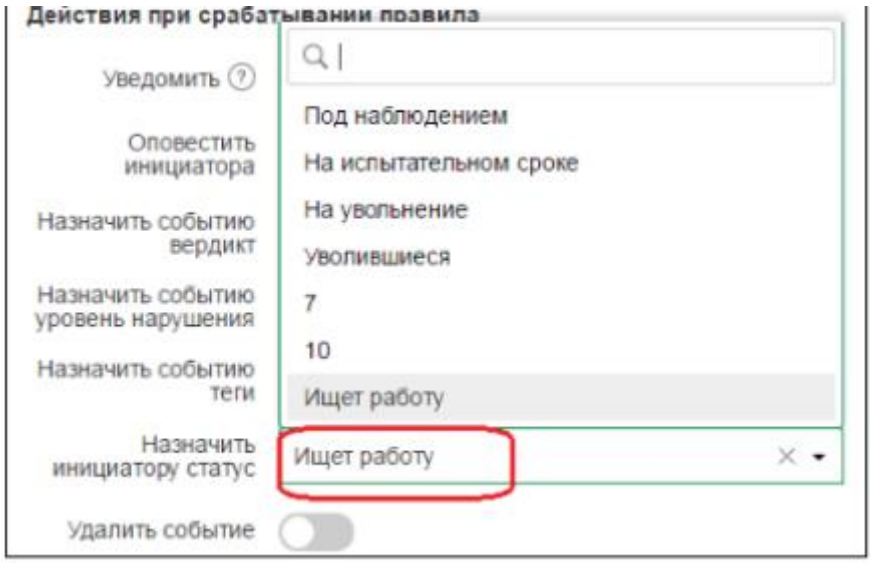
2. Требуется выявить сотрудников, посещающих сайты по поиску работы. Для этого:
   - ✓ Создайте политику защиты данных "Выявление нелояльных сотрудников"
   - ✓ Добавьте правило передачи и укажите в качестве отправителей группу сотрудников компании, импортированную из Active Directory.



   - ✓ В получателях укажите список веб-ресурсов "Поиск работы".



   - ✓ Укажите действия при срабатывании правила. Например, вы можете назначать отправителю определенный статус.



✓ Сохраните правило и примените изменения конфигурации.

Практическая работа № 22
Добавление ролей, редактирование ролей, удаление ролей в Traffic monitor

Задание:

1. Создайте локальную группу пользователей «Подозрительные» в Traffic Monitor. Добавьте в нее пользователя домена ноутбука и виртуальной клиентской машины.
   Подтвердите выполнение задания скриншотами.
2. Необходимо создать пользователя системы с правами доступа только на чтение и выполнение отчетов, сводок и событий, а также на просмотр каталога локальных и доменных пользователей .
   Логин: userevents, пароль: XxXx4321
   Подтвердите выполнение задания скриншотами.
3. Необходимо импортировать пользователя из Active Directory.
   Чтобы импортировать учетную запись:

   ✓ Перейдите в раздел Управление → Управление доступом.
   ✓ Перейдите на вкладку Пользователи.
   ✓ На панели инструментов нажмите  Добавить пользователя из LDAP.
   ✓ Установите флажок для требуемых пользователей.
   Подтвердите выполнение задания скриншотами.

4. *Создайте новую роль. Для этого перейдите в раздел Управление* → Управление доступом. Затем вкладку роли. Далее «+» Создать роль. Установите для новой роли возможность работы только с отчётами. Сохраните.
   Подтвердите выполнение задания скриншотами.
5. Наделите импортированного пользователя из Active Directory новой созданной ролью
   Подтвердите выполнение задания скриншотами.
6. Откройте Руководство администратора → Области видимости. В отчёте ответьте на вопрос: Что такое область видимость и зачем она нужна?
7. Создайте область видимости, добавьте нового импортированного пользователя.
   Подтвердите выполнение задания скриншотами.

Практическая работа № 23
Создание объектов защиты в Traffic monitor

Задание:

Настройте перехват по всем перечисленным каналам:
✓ Сохраните скриншот демонстрирующий перехват по протоколу SMTP
✓ Сохраните скриншот демонстрирующий перехват web-почты.
✓ Сохраните скриншот, демонстрирующий результат работы OCR.
✓ Сохраните скриншот демонстрирующий перехват по протоколу XMPP (Jabber)
✓ Сохраните скриншот, демонстрирующий перехват событий печати.
✓ Сохраните изображения, демонстрирующие перехват данных из буфера обмена.
✓ Сохраните скриншот демонстрирующий перехват данных, копируемых на внешнее устройство хранения.

Практическая работа № 24
Изменение объектов защиты в Traffic monitor

Задание:

Настройте перехват по всем перечисленным каналам:
✓ Сохраните скриншот демонстрирующий перехват по протоколу SMTP
✓ Сохраните скриншот демонстрирующий перехват web-почты.
✓ Сохраните скриншот, демонстрирующий результат работы OCR.
✓ Сохраните скриншот демонстрирующий перехват по протоколу XMPP (Jabber)
✓ Сохраните скриншот, демонстрирующий перехват событий печати.
✓ Сохраните изображения, демонстрирующие перехват данных из буфера обмена.
✓ Сохраните скриншот демонстрирующий перехват данных, копируемых на внешнее устройство хранения.

Практическая работа № 25
Добавление политик безопасности в Traffic monitor

Задание:

Настройте перехват по всем перечисленным каналам:
✓ Сохраните скриншот демонстрирующий перехват по протоколу SMTP
✓ Сохраните скриншот демонстрирующий перехват web-почты.
✓ Сохраните скриншот, демонстрирующий результат работы OCR.
✓ Сохраните скриншот демонстрирующий перехват по протоколу XMPP (Jabber)
✓ Сохраните скриншот, демонстрирующий перехват событий печати.
✓ Сохраните изображения, демонстрирующие перехват данных из буфера обмена.
✓ Сохраните скриншот демонстрирующий перехват данных, копируемых на внешнее устройство хранения.

Практическая работа № 26
Создание политик с использованием перехвата фотографий в Traffic monitor

Задание:

1. Используя Руководство пользователя по Infowatch написать политику:

- ✓ Необходимо создать объект защиты Фото и внести все возможные форматы фотографий. вставить скриншот с созданным объектом защиты.
- ✓ Создать политику *Передача фото*, запрещающую передавать Фото из компании. Уровень угрозы поставить высокий. вставить скриншот с созданной политикой.
- ✓ Проверить работоспособность политики. вставить скриншот с результатом.
- ✓ Внести следующие изменения в политику: разрешить отделу кадров отправлять фотографии из организации.
- ✓ Проверить работоспособность политики. вставить скриншот с результатом.

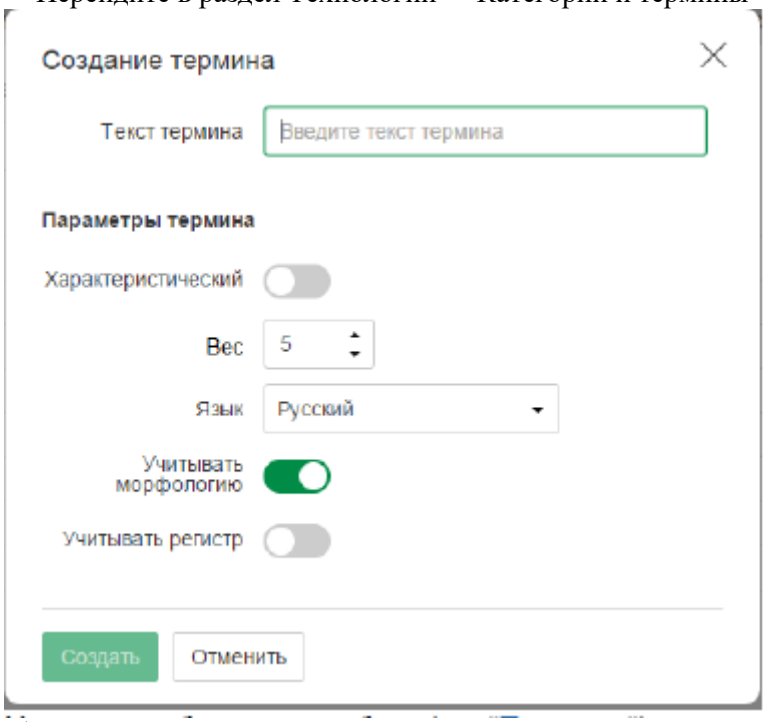
2. Создать политику Котик, с тегом Кот по следующему описанию:
   У генерального директора компании недавно появился котик и его фото утекло в сеть компании. Теперь сотрудники обмениваются смешными картинками с подписями и масками внутри компании и выкладывают их в социальные сети. Директор решил, что его котик вызвал снижение качества работы сотрудников из-за повышенной милоты картинок и хочет запретить обмен фотографией котика. Необходимо запретить обмен фотографией и немного измененной фотографией котика (до 50%) как внутри компании, так и за ее пределы, установить низкий уровень угрозы, тег «Кот».
   Выбрать в Интернете любую фотографию котика для работы.
   Проверить работоспособность на различные варианты, в том числе менее 50% и более 50% изменений фотографии котика.
   скриншоты с созданной политикой, с результатом работы политики.

Практическая работа № 27
Работа с терминами (добавление, настройка параметров, импорт из файла, редактирование, удаление, поиск, перемещение) в Traffic monitor

Задание:

1. Добавить термин Дата выдачи ИНН:
Требуется, чтобы при наличии в трафике хотя бы одного словосочетания "Дата выдачи ИНН", Система помечала объект перехвата как *Дата выдачи ИНН*. Для этого:

✓ Перейдите в раздел Технологии → Категории и термины



✓ Выберите целевую категорию.
✓ Добавьте в нее термин *Дата выдачи ИНН*.

✓ Включите настройку Характеристический.
При передаче данных, среди которых обнаруживается указанное словосочетание, Система присваивает объекту перехвата категорию *Дата выдачи ИНН*.

Вставьте скриншот, подтверждающий выполнение задания

2. Добавить термин Утечка кода программы
Требуется, чтобы при наличии в трафике фрагментов программного кода, Система помечала объект перехвата как утечку кода программы. Для этого:
✓ Создайте категорию *Утечка кода программы*.
✓ Добавьте в нее термины: Procedure, Result.
В результате анализа переданных данных, среди которых обнаруживаются указанные термины, Система присваивает объекту перехвата категорию *Утечка кода программы*

Вставьте скриншот, подтверждающий выполнение задания
5. Создайте политику с низким уровнем угрозы, демонстрирующую работу термина Дата выдачи ИНН.
скриншот с созданной политикой.
Проверьте работоспособность политики и Вставьте скриншот с результатом проверки политики.
6. Создайте политику с низким уровнем угрозы, демонстрирующую работу термина Утечка кода программы.
скриншот с созданной политикой.
Проверьте работоспособность политики и Вставьте скриншот с результатом проверки политики.

Практическая работа № 28
Работа со списками (добавление элементов в список, редактирование, удаление) в Traffic monitor

Задание:

1. Работа со списком статусов:

   Перейдите в раздел «Списки» → Статусы → Создать статус. Название *Под присмотром*, выберите цвет.

   Добавьте 3-м персонам данный статус. вставьте скриншот.

   Удалите статус Подозрительные (он по умолчанию есть). Вставьте скриншот.
2. Работа со списком веб-ресурсов:

   Перейдите в раздел «Списки» → Веб-ресурсы → Создание списка ресурсов. Название списка «Сайты партнеров». Внесите веб-ресурсы: worldskills.moscow, dlptest.com, dlp.demo.lab, worldskills.ru. Вставьте скриншот.
3. Перейдите в периметры.
   Нужно исключить из перехвата почту генерального директора.
   скриншот исключения.
   Проверьте работоспособность исключения из перехвата. скриншот с результатом.
4. Создайте политику, детектирующую передачу любой информации от «Под присмотром». Уровень угрозы низкий, детектировать, название политики «Под присмотром».
   скриншот созданной политики.
   Проверьте работоспособность. Скриншот с результатом.
5. Создайте локальную группу пользователей «Злостные прогульщики», а также группу «Ленивые тюленьчики». Добавьте в каждую из них любых 3-х пользователей из разных отделов. Подтвердите выполнение задания скриншотами.

Практическая работа № 29
Работа с тегами (добавление группы тегов, редактирование параметров группы тегов, добавление тегов, редактирование тегов, удаление тегов) в Traffic monitor

Задание:

1. Перейдите в раздел Списки → Теги → Создать тег. Создайте тег «Бюрократы». Примените его с политике:
Ввести политику, детектирующую передачу любой информации от бухгалтерии за пределы компании.
Уровень угрозы низкий, детектировать, тег «Бюрократы».
2. Создайте тег Архивариусы и примените его к политике:
Ввести политику, детектирующую передачу любой информации от отдела кадров за пределы компании

Задание 2:
Создать политику:
Необходимо поставить на контроль буфер обмена в офисных приложениях (MSWord/WordPad, Excel, PowerPoint).
Проверить работоспособность и зафиксировать выполнение занесением пары событий в IWTM на любые политики Traffic Monitor.
Также подтвердить выполнение скриншотом.

Задание 3:
Внешние эксперты привлекаются компанией для оценки эффективности работы её службы безопасности в части создания политик DLP-системы.
Создайте пользователя Auditor (Аудитор), пароль xxXX1122, который может только просматривать только политики, без просмотра событий и пользователей.
Подтвердите выполнение задания скриншотами.

Практическая работа № 30
Создание политик безопасности

Задание:

1. Создать каталог эталонных документов:
- Перейдите в раздел Технологии → Эталонные документы.
- В левой части рабочей области на панели инструментов нажмите Создать
- каталог эталонных документов.
- В открывшемся окне укажите параметры нового каталога.
- Нажмите Создать.
- Назовите каталог ДОКУМЕНТЫ КОМПАНИИ
  Вставьте скриншот.
2. Создать эталонный документ:
- Перейдите в раздел Технологии → Эталонные документы.
- В левой части рабочей области щелчком левой кнопки мыши выделите каталог, внутри которого будет создан эталонный документ.
- В правой части рабочей области на панели инструментов эталонных документов нажмите Добавить.
- В открывшемся диалоговом окне выберите тип данных, которые могут содержаться в документе: Текстовые или Все типы (могут содержать текст, изображения и бинарные данные).
- Нажмите Выбрать файлы и в открывшемся окне укажите документ, с которого требуется снять цифровой отпечаток. Нажмите Открыть.
- Выберите для загрузки текстовый файл, изображение или архив в соответствии с типом данных, указанным на шаге d. При этом действуют следующие правила:

    - Если формат выбранного файла не поддерживается Системой, то цифровой отпечаток будет загружен как бинарные данные.
    - Если для загрузки выбран архив, то в качестве эталонных документов будут добавлены содержащиеся в архиве файлы.
- После окончания загрузки эталонный документ будет добавлен в каталог. Все обязательные атрибуты присваиваются созданному эталонному документу по умолчанию
  Вставьте скриншот с эталонными документами.

Создать политики:

Политика 1:
Требуется, чтобы Система отслеживала передачу документа "Внутренний регламент компании" при наличии в трафике хотя бы 30% текста документа. Для этого:
- Выберите каталог эталонных документов или создайте новый каталог.
- Внутри выбранного каталога добавьте новый документ и укажите для него тип данных: Текстовые (так как документ не содержит изображения и графики).
- Загрузите документ "Внутренний регламент компании" в качестве эталонного документа.
- Укажите название эталонного документа, например, ВНУТРЕННИЙ_РЕГЛАМЕНТ_КОМПАНИИ.
- Установите для атрибута Порог цитируемости текстовых данных значение 30.
- Передачу документа отслеживать и внутри, и наружу. Уровень «средний». Детектировать.
  Скриншот ,подтверждающий создание политики и её работоспособность.

Политика 2:
Требуется, чтобы Система отслеживала передачу исполняемого файла "Setup.exe" при наличии в трафике хотя бы 10% бинарного содержимого файла "Setup.exe". Для этого:
- Выберите каталог эталонных документов или создайте новый каталог.
- Внутри выбранного каталога добавьте новый документ и укажите для него тип данных: Все типы.
- Загрузите файл "Setup.exe" в качестве эталонного документа.
- Укажите название эталонного документа, например, SETUP_EXE.
- Установите для атрибута Порог цитируемости бинарных данных значение 10.
- Для того чтобы Система отслеживала наличие в трафике указанных эталонных документов, их нужно включить в объекты защиты.
- Передачу документа отслеживать и внутри, и наружу. Уровень «средний». Детектировать.
  Скриншот ,подтверждающий создание политики и её работоспособность.

Практическая работа № 31
Создание политик с использованием комбинированных объектов защиты

Задание:

Создать политики по следующему описанию:

Политика 1. В связи с постоянными проблемами при организации очередного чемпионата WorldSkills (Региональный Чемпионат), совет директоров решил контролировать передачу информации о WorldSkills и Региональном Чемпионате за пределы компании. В связи с этим необходимо создать политику в InfoWatch Traffic Monitor на правило передачи текстовых данных за пределы компании (на адрес вне домена), содержащих слова «ВорлдСкиллз», «WorldSkills», «Межвуз» и «MezhVuz».
Необходимо учесть, что в словах могут содержаться комбинации латиницы и кириллицы, а также стоять пробел между словами, например: «Mezh Вуз». Ложных срабатываний быть не должно (например, просто на Меж или Skills).
*Разрешить передачу, но установить средний уровень угрозы. Тег «*WorldSkills*».*

Проверить работоспособность.
Вставить скриншот с работающей политикой и скриншот с работоспособностью.

Политика 2. Для контроля за движением официальных документов необходимо вести наблюдение за передачей как пустых, так и заполненных шаблонов документа (шаблон — «Договор компании.doc») за пределы компании. Стоит учесть, что содержимое документа может изменяться в пределах 25%.
Уровень угрозы низкий, не блокировать, тег «Договор».
В случае, если в документе присутствует фамилия генерального директора, выставить уровень угрозы средний, не блокировать, тег «Договор».
В случае, если в документе присутствует фамилия генерального директора, а также печать компании, выставить уровень угрозы высокий, блокировать для всех, тег «Договор».
Проверить работоспособность.
Вставить скриншот с работающей политикой и скриншот с работоспособностью.

Политика 3. Для мониторинга движения анкет необходимо вести наблюдение за анкетами с печатью компании за пределы компании, запрещая любую внешнюю передачу документов, содержащих печать компании в пустых и заполненных бланках «анкета участника.docx», при этом бланки без печати или просто печать контролировать не нужно. Генеральный директор и совет директоров могут обмениваться данной информацией совершенно свободно.
Печать + бланк: Уровень угрозы средний, блокировать, тег «Политика 3».
Проверить работоспособность.
Вставить скриншот с работающей политикой и скриншот с работоспособностью.

Политика 4. В честь юбилея компании была запущена акция с промокодами на скидку в 50% на перевозки для постоянных клиентов. По условиям акции промокод выдается только по запросу постоянного клиента. Есть вероятность утечки промокодов, в связи с этим необходимо контролировать защитить учечку текстового документа, содержащего промокоды («промокоды.docx»). Стоит учесть, что сотрудники могут воспользоваться жестким диском или флеш-накопителем, для того чтобы завладеть акционными купонами, а также слить не весь файл, а один или несколько купонов.
Запретить передачу данных, содержащих информацию об этих купонах, а также отслеживать со средним уровнем угрозы копирование этой информации на внешние носители, тег «Политика 4». При этом отдел продаж может пересылать данную информацию совершенно свободно.
Проверить работоспособность.
Вставить скриншот с работающей политикой и скриншот с работоспособностью.

Политика 5. В связи с постоянными заказами на транспортировку больших грузов, сотрудники компании подрабатывают в тайне от начальства, занимаясь попутной перевозкой других грузов, а также пассажиров. В связи с этим необходимо отслеживать в почтовых сообщениях упоминания об автостопе, халтуре, подработке, грузовом такси. Стоит учесть морфологию и различные варианты написания этих ключевых слов.
Уровень угрозы средний, не блокировать, тег «Политика 5».
Проверить работоспособность.
Вставить скриншот с работающей политикой и скриншот с работоспособностью.

Политика 6. Сотрудники отдела ИТ заподозрены в сливе баз данных клиентов. Необходимо настроить мониторинг выгрузок из БД для контроля движения данных из базы данных страховых компаний только при отправке из отдела информатизации. Критичными дан-

ными в выгрузке являются телефоны, ИНН, ОКПО, ОКФС, ОКОГУ и ОКОПФ и в 1 документе присутствует более 3 компаний. Для настройки используйте файл stock_members_details_catch.csv.
Уровень угрозы средний, блокировать, тег «Политика 6».
Проверить работоспособность.
Вставить скриншот с работающей политикой и скриншот с работоспособностью.

Политика 7. Было замечено, что сотрудники компании стали получать множество рекламных сообщений электронной почты, из-за чего возникла необходимость отследить потенциальную утечку баз email адресов сотрудников. В связи с этим необходимо детектировать сообщения, содержащие адреса электронной почты.
Стоит учесть, что в связи с импортозамещением данные адреса могут находиться и на кириллических доменах, а также содержать другие допустимые символы email адресов. Детектирование только частей адресов (например @mail.ru) недопустимо.
Пример формата адресов: e-mail@domain.com , mail+tag@mail.com , мой.меил@почта.ru , элепочта@компания.рф и т. п.
Уровень угрозы средний, не блокировать, тег «Политика 7».
Проверить работоспособность.
Вставить скриншот с работающей политикой и скриншот с работоспособностью.

Практическая работа № 32
Создание виджетов в Traffic Monitor. Изменение виджетов в Traffic Monitor

Задание 1:

Создайте новую вкладку сводки в разделе «Сводка» под названием «Чемпионат» и создайте в ней 4 виджета:

- Динамика активности по событиям за последнюю неделю
- Статистика по политикам за последние 3 дня
- По типу событий: необработанные нарушения за день
- По топ-нарушителям.

Вставьте скриншот, подтверждающий выполнение задания

Задание 2
Необходимо создать виджет, отображающий события с уровнем угрозы от низкого до высокого на правила копирования (внешние носители, печать) за последние 7 дней.
Вставьте скриншот, подтверждающий выполнение задания

Задание 3
Необходимо создать виджет для отображения нарушений только от компьютера нарушителя (виртуальная машина) со средним и высоким уровнем угрозы за последние 3 дня.
Вставьте скриншот, подтверждающий выполнение задания

Задание 4

Сделайте выборку (запрос), в котором будет отображено только по одному событию каждого типа: передачи, копирования, буфера обмена и хранения.

Вставьте скриншот, подтверждающий выполнение задания

Создайте в сводке «Чемпионат» дополнительные два виджета:

• Выборка по событиям краулера за последнюю неделю

• Выборка по политикам с технологиями: графические объекты, печати за последние 3 дня

Корректно выполненным заданием является наличие событий в системе и наличие скриншотов событий.

Практическая работа № 33
Создание отчётов в Traffic Monitor. Изменение отчётов в Traffic Monitor.

Задание 1:

Необходимо создать пользователя системы с правами доступа только на чтение и выполнение отчетов, сводок и событий.

- ✓ Логин: userevents, пароль: XxXx1122

Вставьте скриншот, подтверждающий выполнение задания

Задание 2: Создание отчета

Необходимо создать новый отчет в разделе «Отчеты», назвав его «Отчет ДемоЭкзамен».

Добавить 4 виджета в отчет:

- ✓ Динамика активности по событиям за последние 3 дня
- ✓ Статистика по политикам за последние 3 дня
- ✓ По типу событий: необработанные нарушения за 7 дней
- ✓ Вычислить топ-нарушителей и вывести отчет по нарушениям по данному отправителю.

Вставьте скриншот, подтверждающий выполнение задания

Задание 3:

Создайте отчет в разделе «Отчеты», назвав его «Отчёт2» и добавьте 2 виджета:

• Отобразить всех пользователей, занимающихся не относящейся к работе деятельностью (по тегам или другим критериям из задания на политики)

• Вычислить топ-нарушителей среди всех сотрудников компании и вывести отчет по нарушениям только по самому активному отправителю.

Вставьте скриншот, подтверждающий выполнение задания

Задание 4: Создание сводки по устройствам

Необходимо создать новую панель сводки в разделе «Сводка» и назвать ее «Сводка устройства».

- ✓ Добавить виджет, выводящий информацию по событиям Crawler за последние 3 дня со средним и высоким уровнем угрозы.

- ✓ Добавить виджет, выводящий информацию по событиям только с компьютера нарушителя за последние три дня, которые имеют один любой из ранее созданных тегов.
- ✓ Добавить виджет, выводящий информацию по событиям только с компьютера нарушителя за последние три дня, которые имеют уровень угрозы от низкого до высокого.

По каждому заданию вставить скриншоты.