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

ПРИНЯТО

на заседании педагогического совета
Протокол № 2
«26» 12 2023 г.

УТВЕРЖДАЮ

Директор СПб ГБПОУ «АУГСГиП»
_____ А.М.Кривоносов
«___» _____ 2023 г.

КОМПЛЕКТ КОНТРОЛЬНО-ОЦЕНОЧНЫХ СРЕДСТВ

по текущему контролю успеваемости
и промежуточной аттестации
по профессиональному модулю
ПМ.03 ЭКСПЛУАТАЦИЯ ОБЪЕКТОВ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

по специальности
09.02.06 Сетевое и системное администрирование

Квалификация
Системный администратор

Форма обучения
очная

Санкт-Петербург
2023 год

Комплект контрольно-оценочных средств по профессиональному модулю ПМ.03 Эксплуатация объектов сетевой инфраструктуры разработан на основе Федерального государственного образовательного стандарта по специальности 09.02.06 Сетевое и системное администрирование, утвержденного приказом Министерства Просвещения РФ от 10 июля 2023 г. № 519.

СОГЛАСОВАНО
ООО «ДЖИ-ТИ ИНВЕСТ»
Генеральный директор
_____ П.С. Тюганов
«26» 12 2023 г.

Комплект контрольно-оценочных средств по профессиональному модулю рассмотрен на заседании методического совета СПб ГБПОУ «АУГСГиП»
Протокол № 2 от «29» 11 2023 г.

Комплект контрольно-оценочных средств по профессиональному модулю рассмотрен на заседании цикловой комиссии общетехнических дисциплин и компьютерных технологий
Протокол № 4 от «21» 11 2023 г.

Председатель цикловой комиссии: Караченцева М.С. _____

СОДЕРЖАНИЕ

1. Паспорт комплекта оценочных средств

Результатом освоения профессионального модуля является готовность обучающегося к выполнению вида профессиональной деятельности Эксплуатация объектов сетевой инфраструктуры и составляющих его профессиональных компетенций, а также общих компетенций, формирующихся в процессе освоения ППССЗ в целом.

Комплект контрольно-оценочных средств позволяет оценивать:

1. Освоение профессиональных компетенций (ПК), соответствующих виду профессиональной деятельности, и общих компетенций (ОК):

Код	Наименование результата обучения
ПК 3.1	Осуществлять проектирование сетевой инфраструктуры
ПК 3.2	Обслуживать сетевые конфигурации программно-аппаратных средств
ПК 3.3.	Осуществлять защиту информации в сети с использованием программно-аппаратных средств
ПК 3.4.	Осуществлять устранение нетипичных неисправностей в работе сетевой инфраструктуры
ПК 3.5.	Модернизировать сетевые устройства информационно-коммуникационных систем
ПК.3.6	*Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов*
ПК 3.7	*Применять криптографические аппаратные средства защиты информации на защищаемых объектах*
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.

2. Приобретение в ходе освоения профессионального модуля практического опыта:

Освоение практического опыта

Владеть навыками	Виды работ на учебной и/ или производственной практике и требования к их выполнению
– проектировать архитектуру локальной сети в соответствии с поставленной задачей; – использовать специальное программное обеспечение для моделирования, проектирования и тестирования компьютерных сетей; – настраивать протоколы динамической маршрутизации; – определять влияния приложений на проект сети; – анализировать, проектировать и настраивать схемы потоков трафика в компьютерной сети; – устанавливать и настраивать сетевые протоколы и сетевое оборудование в соответствии с конкретной задачей; – выбирать технологии, инструментальные средства при организации процесса исследования объектов сетевой инфраструктуры; – создавать и настраивать одноранговую сеть, компьютерную сеть с помощью маршрутизатора, беспроводную сеть; – выполнять поиск и устранение проблем в компьютерных сетях; – отслеживать пакеты в сети и настраивать программно-аппаратные межсетевые экраны; – настраивать коммутацию в корпоративной сети; – обеспечивать целостность резервирования информации; – обеспечивать безопасное хранение и передачу информации в глобальных и локальных сетях;	Учебная практика: 1. Инструктаж по технике безопасности при работе на персональном компьютере. 2. Настройка работоспособности сети 3. Настройка удаленного администрирования 4. Настройка аппаратного обеспечения сетевой инфраструктуры 5. Настройка программного обеспечения сетевой инфраструктуры. 6. Выполнение профилактической работы на объекте сетевой инфраструктуры 7. Выполнение мониторинга и анализа работы локальной сети с помощью программно-аппаратных средств 8. Устранение выявленных неисправностей в результате мониторинга локальной сети 9. Выполнение операций резервного копирования и восстановления данных 10. Проведение инвентаризации технических средств сетевой инфраструктуры 11. Контроль оборудования после его ремонта 12. Наблюдение за трафиком локальной сети 13. Установка системы обнаружения вторжений 14. Настройка системы обнаружения вторжений 15. Выполнение мониторинга работы системы обнаружения вторжений 16. Устранение выявленных неисправностей в результате мониторинга работы системы обнаружения вторжений 17. Настройка правил работы системы обнаружения вторжений 18. Установка ОС Kali Linux для применения стеганографии 19. Применение стеганографии Производственная практива: 1. Ознакомление с сетевой инфраструктурой организации

Владеть навыками	Виды работ на учебной и/ или производственной практике и требования к их выполнению
– создавать и настраивать одноранговую сеть, компьютерную сеть с помощью маршрутизатора, беспроводную сеть; – выполнять поиск и устранение проблем в компьютерных сетях; – отслеживать пакеты в сети и настраивать программно-аппаратные межсетевые экраны; – фильтровать, контролировать и обеспечивать безопасность сетевого трафика; – определять влияние приложений на проект сети; – мониторинг производительности сервера и протоколирования системных и сетевых событий; – использовать специальное программное обеспечение для моделирования, проектирования и тестирования компьютерных сетей; – создавать и настраивать одноранговую сеть, компьютерную сеть с помощью маршрутизатора, беспроводную сеть; – создавать подсети и настраивать обмен данными; – выполнять поиск и устранение проблем в компьютерных сетях; – анализировать схемы потоков трафика в компьютерной сети; – оценивать качество и соответствие требованиям проекта сети; – оформлять техническую документацию; – определять влияние приложений на проект сети; – анализировать схемы потоков трафика в компьютерной сети; – оценивать качество и соответ-	2. Настройка аппаратного и программного обеспечения сетевой инфраструктуры 3. Эксплуатация технических средств сетевой инфраструктуры 4. Обслуживание сетевой инфраструктуры 5. Мониторинг обновлений программно-аппаратных средств сетевой инфраструктуры. 6. Поддержка пользователей сети 7. Составление план-графика профилактических работ сетевой инфраструктуры 8. Выполнение профилактических работ сетевой инфраструктуры 9. Организация бесперебойной работы системы по резервному копированию и восстановлению информации 10. Замена расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры 11. Проведение инвентаризации технических средств сетевой инфраструктуры 12. Контроль оборудования после его ремонта

Владеть навыками	Виды работ на учебной и/ или производственной практике и требования к их выполнению
ствие требованиям проекта сети	

3. Освоение умений и усвоение знаний:

№	Освоенные умения, усвоенные знания
З1	– общие принципы построения сетей;
З2	– сетевые топологии;
З3	– многослойную модель OSI;
З4	– требования к компьютерным сетям;
З5	– архитектуру протоколов;
З6	– стандартизацию сетей;
З7	– этапы проектирования сетевой инфраструктуры;
З8	– элементы теории массового обслуживания;
З9	– основные понятия теории графов;
З10	– алгоритмы поиска кратчайшего пути;
З11	– основные проблемы синтеза графов атак;
З12	– системы топологического анализа защищенности компьютерной сети;
З13	– основы проектирования локальных сетей, беспроводные локальные сети;
З14	– стандарты кабелей, основные виды коммуникационных устройств, термины, понятия, стандарты и типовые элементы

№	Освоенные умения, усвоенные знания
	структурированной кабельной системы: монтаж, тестирование;
315	– средства тестирования и анализа;
316	– базовые протоколы и технологии локальных сетей;
317	– общие принципы построения сетей;
318	– основные проблемы синтеза графов атак;
319	– системы топологического анализа защищенности компьютерной сети;
320	– архитектуру сканера безопасности;
321	– принципы построения высокоскоростных локальных сетей;
322	– требования к компьютерным сетям;
323	– требования к сетевой безопасности;
324	– элементы теории массового обслуживания;
325	– основные понятия теории графов;
326	– основные проблемы синтеза графов атак;
327	– системы топологического анализа защищенности компьютерной сети;
328	– этапы проектирования сетевой инфраструктуры;
329	– организацию работ по вводу в эксплуатацию объектов и сегментов компьютерных сетей;
330	– стандарты кабелей, основные виды коммуникационных устройств, термины, понятия, стандарты и типовые элементы структурированной кабельной системы: монтаж, тестирование;
331	– программно-аппаратные средства технического контроля;
332	– принципы и стандарты оформления технической документации
332	– принципы создания и оформления топологии сети;
333	– информационно-справочные системы для замены (поиска) технического оборудования
334	*системы обнаружения вторжения;*
335	*программно-аппаратные средства для создания защищённой сети;*

№	Освоенные умения, усвоенные знания
336	*DLP-системы для защиты от внутренних утечек информации*
337	*основные понятия, определения, основные алгоритмы шифрования с секретным ключом;*
338	*основные понятия, определения, модель передачи защищенных сообщений с открытым ключом шифрования;*
339	*основные понятия, определения и алгоритмы стеганографии;*
340	*основные принципы анализа криптографических систем*
У1	проектировать локальную сеть;
У2	выбирать сетевые топологии;
У3	рассчитывать основные параметры локальной сети;
У4	применять алгоритмы поиска кратчайшего пути;
У5	планировать структуру сети с помощью графа с оптимальным расположением узлов;
У6	использовать математический аппарат теории графов;
У7	настраивать стек протоколов TCP/IP и использовать встроенные утилиты операционной системы для диагностики работоспособности сети;
У8	выбирать сетевые топологии;
У9	рассчитывать основные параметры локальной сети;
У10	применять алгоритмы поиска кратчайшего пути;
У11	планировать структуру сети с помощью графа с оптимальным расположением узлов;
У12	использовать математический аппарат теории графов;
У13	использовать многофункциональные приборы и программные средства мониторинга;
У14	использовать программно-аппаратные средства технического контроля
У15	использовать программно-аппаратные средства технического контроля;
У16	читать техническую и проектную документацию по организации сегментов сети;
У17	контролировать соответствие разрабатываемого проекта нормативно-технической документации;
У18	использовать программно-аппаратные средства технического контроля;
У19	использовать техническую литературу и информационно-справочные системы для замены (поиска аналогов) устаревшего оборудования;
У20	читать техническую и проектную документацию по организации сегментов сети;
У21	контролировать соответствие разрабатываемого проекта нормативно-технической документации;
У22	использовать техническую литературу и информационно-справочные системы для замены (поиска аналогов) устаревшего оборудования;
У23	*устанавливать системы обнаружения и предотвращения вторжений;*
У24	*работать с системой обнаружения и предотвращения вторжений;*

№	Освоенные умения, усвоенные знания
У25	*создавать защищённую сеть;*
У26	*настраивать и модифицировать межсетевое взаимодействие;*
У27	*устанавливать DLP-систему;*
У28	*создавать правила и политики безопасности в DLP-системах;*
У29	*создавать отчёты по инцидентам в DLP-системах;*
У30	*применять на практике алгоритмы шифрования секретным ключом;*
У31	*проводить анализ криптостойкости алгоритмов и протоколов*
У32	*создавать программы, реализующие алгоритмы и протоколы защищенной передачи данных*
У32	*конструировать крипто-стойкие алгоритмы и протоколы*
У33	*проводить анализ данных на наличие скрытой информации*

Формой аттестации по профессиональному модулю является экзамен по профессиональному модулю. Итогом экзамена является однозначное решение: «вид профессиональной деятельности освоен/не освоен».

2. Система контроля и оценки освоения программы ПМ.03 Эксплуатация объектов сетевой инфраструктуры

2.1. Формы промежуточной аттестации по ППССЗ при освоении профессионального модуля

Элементы модуля, профессиональный модуль	Формы промежуточной аттестации
МДК.03.01 Эксплуатация объектов сетевой инфраструктуры	Комплексный экзамен
МДК.03.02 Технологии автоматизации технологических процессов	Дифференцированный зачёт
МДК.03.03 Безопасность компьютерных сетей	Комплексный экзамен
МДК 03.04 Защита от внутренних угроз информационной безопасности	Экзамен
МДК 03.05 Основы криптографической защиты данных	Дифференцированный зачёт
Производственная практика	Дифференцированный зачёт
ПМ.03	**Экзамен**

2.2. Организация контроля и оценки освоения программы ПМ

Итоговый контроль освоения вида профессиональной деятельности «Эксплуатация объектов сетевой инфраструктуры» осуществляется на экзамене. Условием допуска к экзамену является положительная аттестация по МДК, учебной и производственной практике.

Экзамен проводится в виде выполнения практического экзаменационного задания.

Условием положительной аттестации по ПМ.03 «Эксплуатация объектов сетевой инфраструктуры» (вид профессиональной деятельности освоен) на экзамене является положительная оценка освоения всех профессиональных компетенций по всем контролируемым показателям. При отрицательном заключении хотя бы по одной из профессиональных компетенций принимается решение «вид профессиональной деятельности не освоен».

Промежуточный контроль освоения профессионального модуля осуществляется при проведении экзаменов по МДК.03.01, МДК.03.03, МДК.03.04, дифференцированных зачётов по МДК.03.02, МДК.03.05 и производственной практике. Предметом оценки освоения МДК являются умения и знания. Экзамен по МДК проводится по заранее подготовленным и утвержденным экзаменационным вопросам. Условием положительной аттестации является получение обучающимся на экзамене оценки «удовлетворительно», «хорошо», «отлично».

Предметом оценки по учебной практике является освоение общих и профессиональных компетенций, умений. Контроль и оценка по учебной и (или) производственной практике проводится на основе Аттестационного листа обучающегося с места прохождения практики.

Текущий контроль по МДК осуществляется в форме выполнения практических заданий, устных зачетов.

3. Комплект материалов для освоения умений и усвоения знаний, оценки сформированности общих и профессиональных компетенций по виду профессиональной деятельности

3.1. Задания для оценки освоения теоретического курса профессионального модуля

3.1.1. Оценка освоения теоретического курса профессионального модуля по МДК.03.01

Дидактические единицы	Проверяемые ОК, ПК	Формы контроля (наименование контрольной точки)	
		Текущая аттестация	Промежуточная аттестация
Тема 1.1. Эксплуатация технических средств сетевой инфраструктуры	ОК 1-9 ПК 3.1, ПК 3.2. ПК 3.4, ПК 3.5	Устный зачет по теме 1.1.	Ответы на экзаменационные вопросы
	ОК 1-9 ПК 3.1, ПК 3.2. ПК 3.4, ПК 3.5	Практическая работа № 20 Эксплуатация объектов сетевой инфраструктуры	
Тема 1.2. Эксплуатация систем IP-телефонии	ОК 1-9 ПК 3.1, ПК 3.2. ПК 3.4, ПК 3.5	Устный зачет по теме 2.1.	
	ОК 1-9 ПК 3.1, ПК 3.2. ПК 3.4, ПК 3.5	Практическая работа № 37 Эксплуатация систем IP-телефонии	
Тема 1.3. Инвентаризация технических средств сетевой инфраструктуры , замена расходных материалов и мелкий ремонт периферийного оборудования	ОК 1-9 ПК 3.1, ПК 3.2. ПК 3.4, ПК 3.5	Практическая работа № 39 Замена расходных материалов и мелкий ремонт периферийного оборудования	

Устный зачет по теме 1.1.

Инструкция для обучающихся

Зачет сдается в рамках учебного занятия. Каждый студент отвечает в устной форме на предложенные преподавателем 5 случайных вопроса.

Выполнение задания: одному студенту на ответ выделяется 3 мин., группа сдает зачет за одно учебное занятие.

Перечень вопросов:

1. Физические аспекты эксплуатации. Физическое вмешательство в инфраструктуру сети.
2. Активное и пассивное сетевое оборудование: кабельные каналы, кабель, патч-панели, розетки.

3. Полоса пропускания, паразитная нагрузка.
4. Расширяемость сети. Масштабируемость сети. Добавление отдельных элементов сети (пользователей, компьютеров, приложений, служб).
5. Наращивание длины сегментов сети; замена существующей аппаратуры.
6. Увеличение количества узлов сети; увеличение протяженности связей между объектами сети.
7. Техническая и проектная документация. Паспорт технических устройств.
8. Физическая карта всей сети; логическая топология компьютерной сети.
9. Классификация регламентов технических осмотров, технические осмотры объектов сетевой инфраструктуры.
10. Проверка объектов сетевой инфраструктуры и профилактические работы
11. Проведение регулярного резервирования. Обслуживание физических компонентов; контроль состояния аппаратного обеспечения; организация удаленного оповещения о неполадках.
12. Программное обеспечение мониторинга компьютерных сетей и сетевых устройств.
13. . Протокол SNMP, его характеристики, формат сообщений, набор услуг.
14. Задачи управления: анализ производительности и надежности сети.
15. Оборудование для диагностики и сертификации кабельных систем. Сетевые мониторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры.

Эталоны ответов: приведены в учебном пособии по МДК.03.01 «Эксплуатация объектов сетевой инфраструктуры»

Практическая работа № 15 Настройка безопасного доступа к маршрутизатору

Инструкция для обучающихся

Внимательно прочитайте задание. Проведите установку и настройку контроллеров.

Время выполнения – 90 минут.

Задание

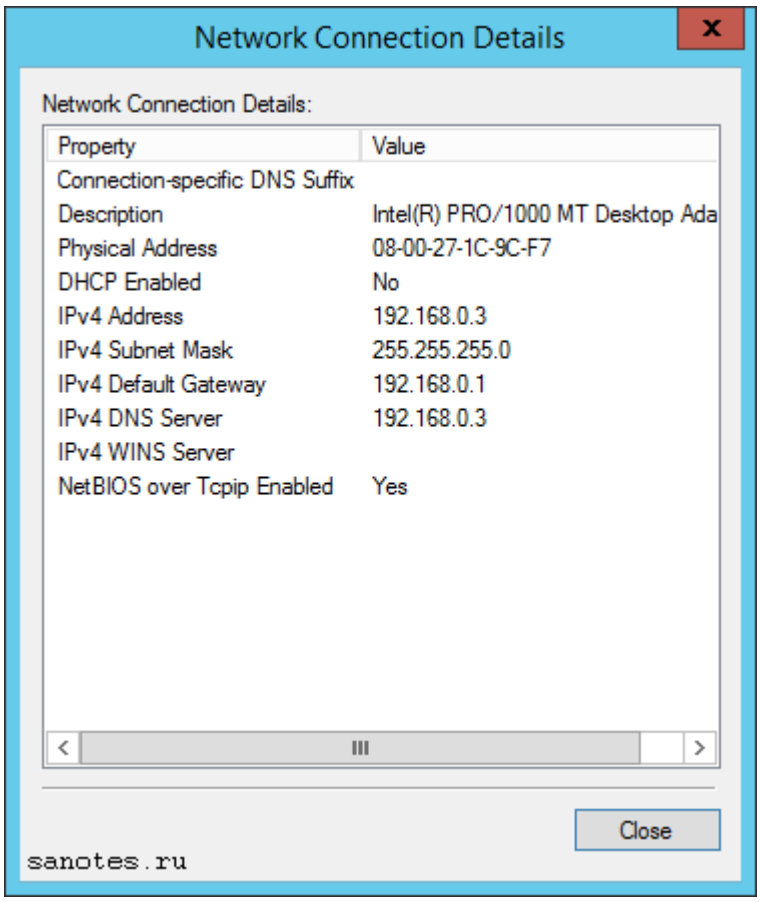
1) Основной контроллер домена, ОС — Windows Server 2016 R2 with GUI.

2) Дополнительный контроллер домена (на случай выхода из строя основного), ОС — Windows Server 2016 R2 Core.

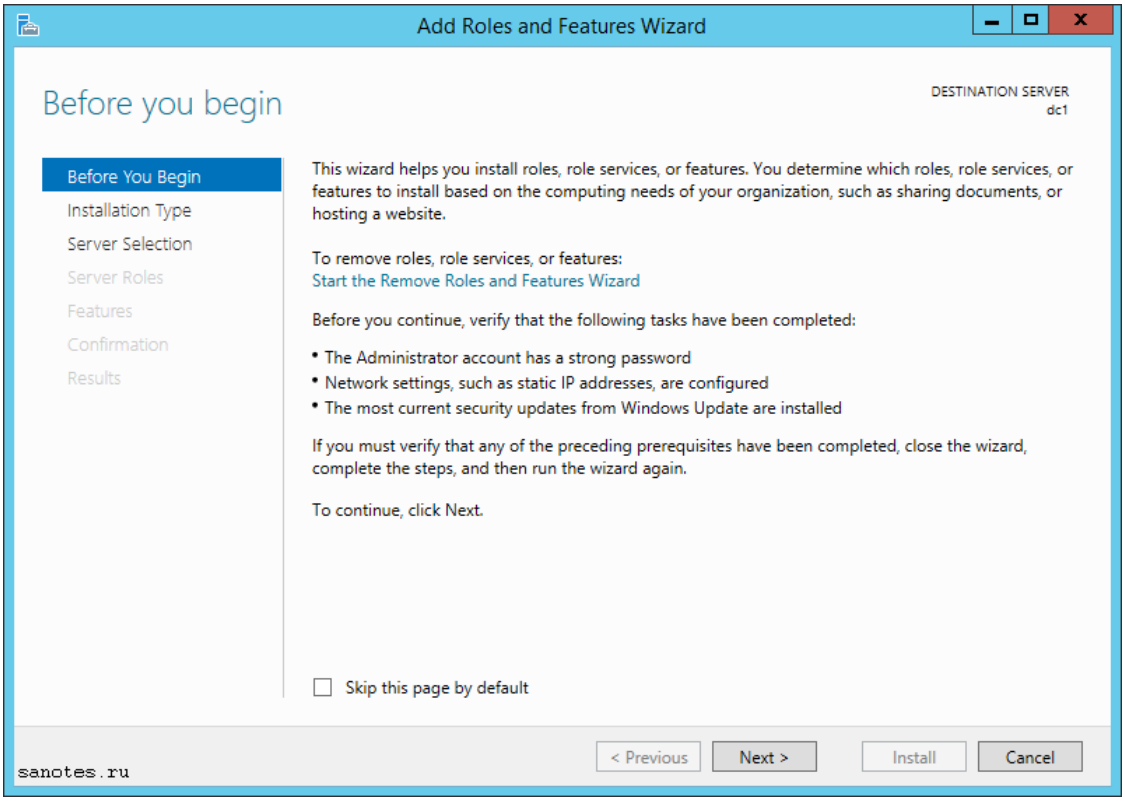
3) Контроллер домена только для чтения (RODC), находящийся в филиале компании за vpn-каналом, ОС — Windows Server 2012 R2 Core.

Шаг 1: Установка первого контроллера домена. Подготовка.

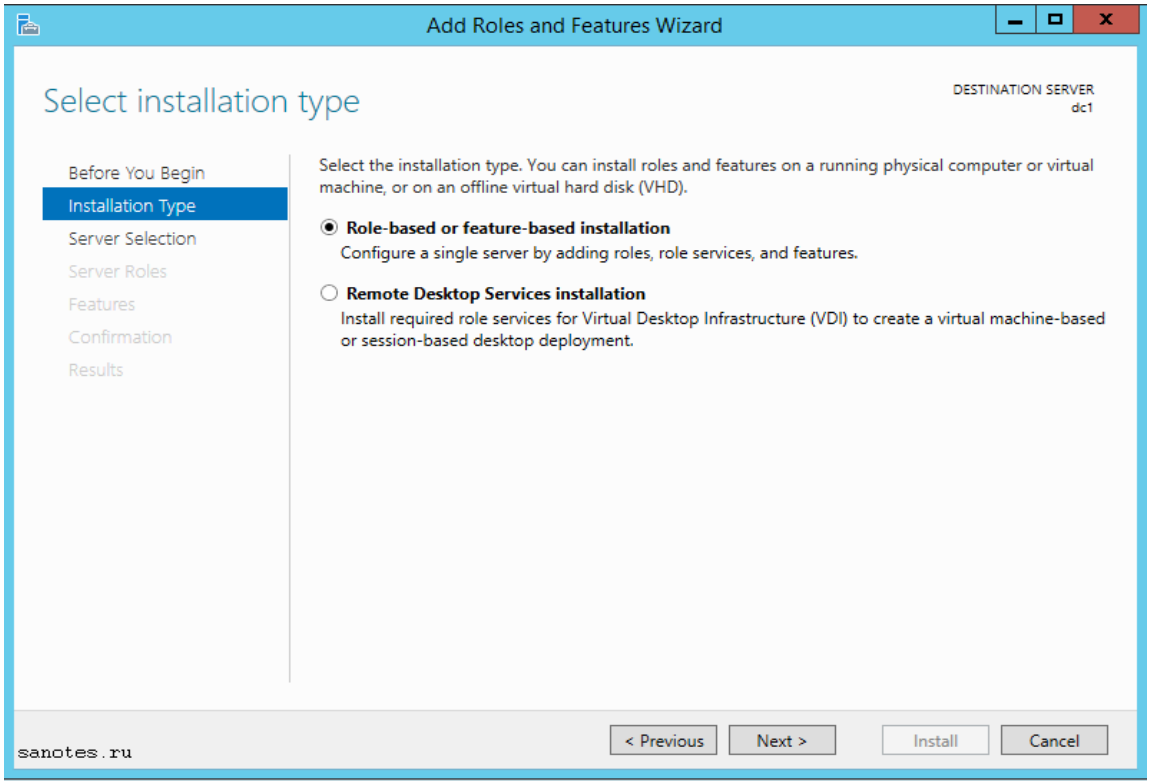
Перед запуском мастера ролей, серверу необходимо задать сетевое имя и настроить ip-адрес. Настройки TCP/IP укажем как на скриншоте ниже.



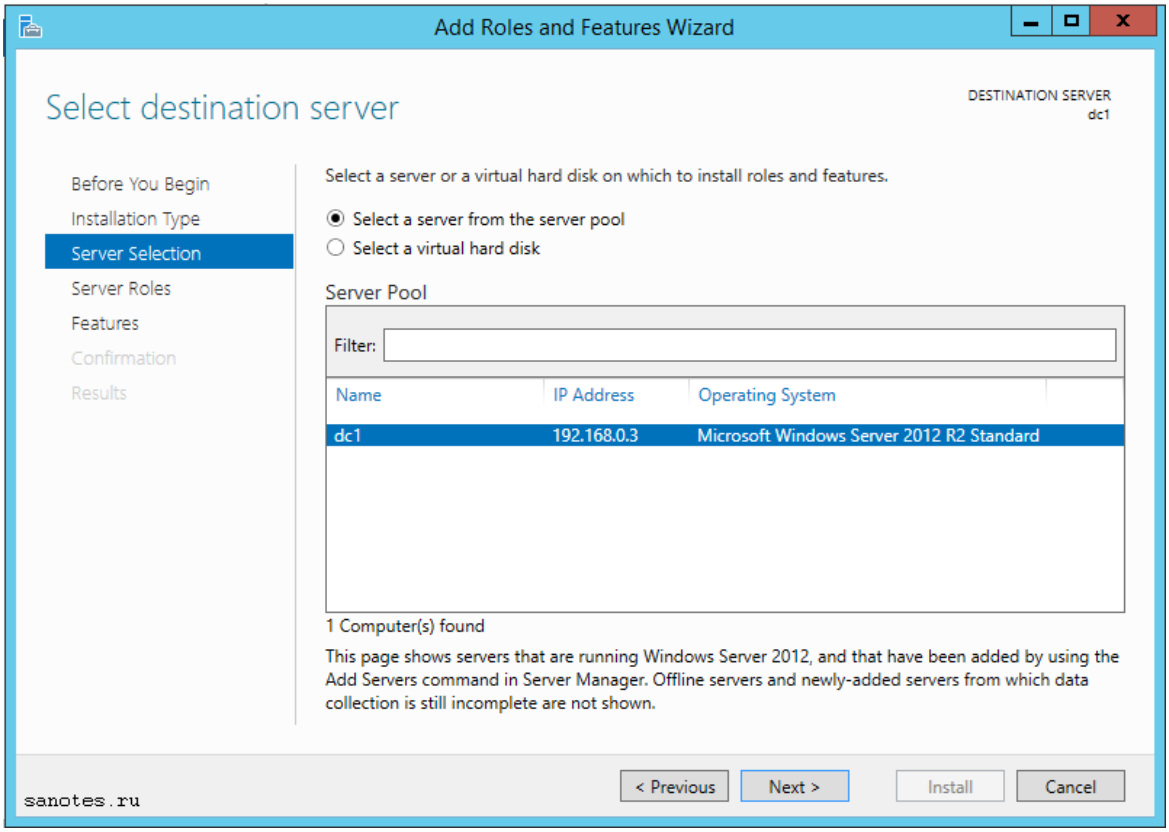
Запускаем диспетчер сервера — **Server Manager -> Dashboard -> Configure this local server -> Add Role and Features Wizard.** На первом экране мастер нам сообщает, что перед тем как продолжить, должен быть установлен сложный пароль администратора, в настройках сети указан статический ip-адрес, установлены последние обновления. Если все это сделано, то нажимаем Next.



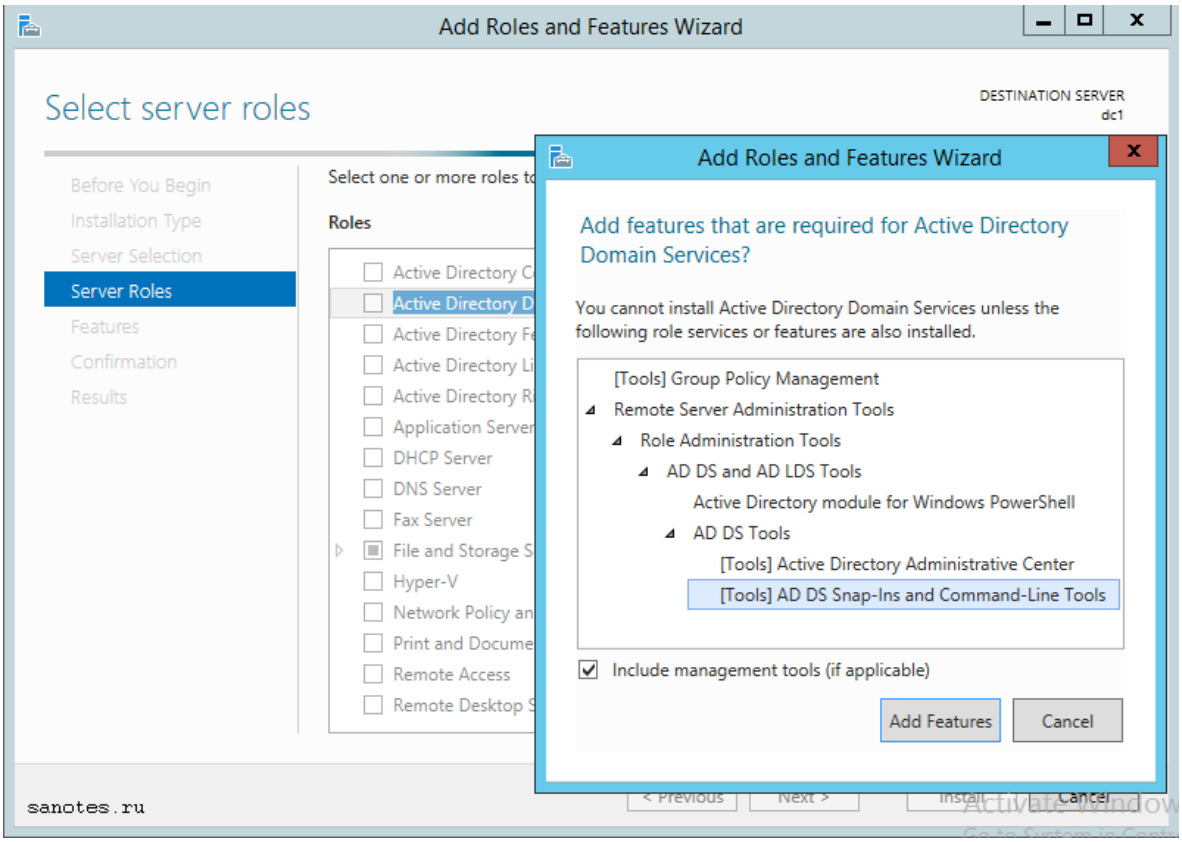
На следующем экране, выбираем первый пункт **Role-based or feature-based installation** (Базовая установка ролей и компонентов). Второй пункт **Remote Desktop Service installtion** предназначен исключительно для установки роли удаленных рабочих столов.



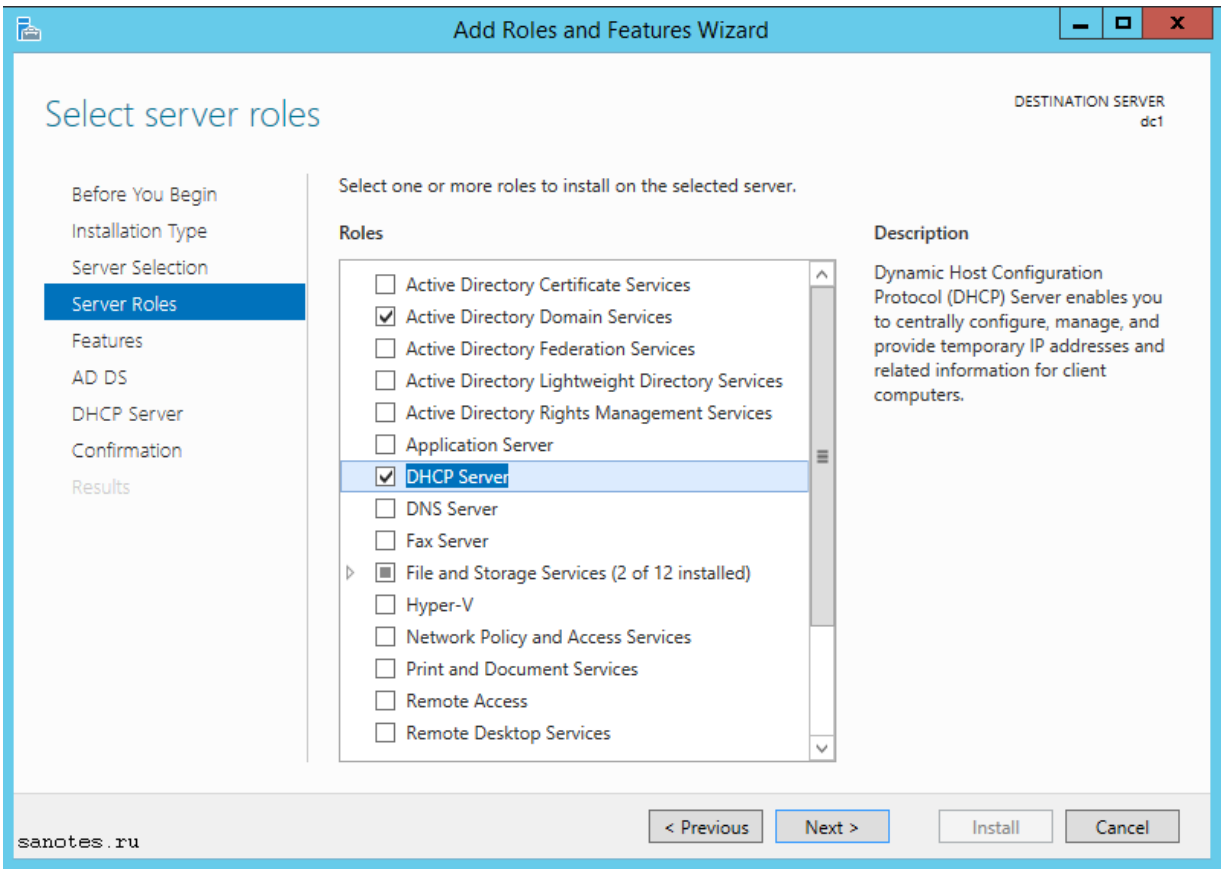
На экране **Select Destination server** диспетчер предлагает нам, выбрать сервер из пула или расположенный на VHD-диске. Поскольку у нас пока только один локальный сервер, то нажимаем Next.



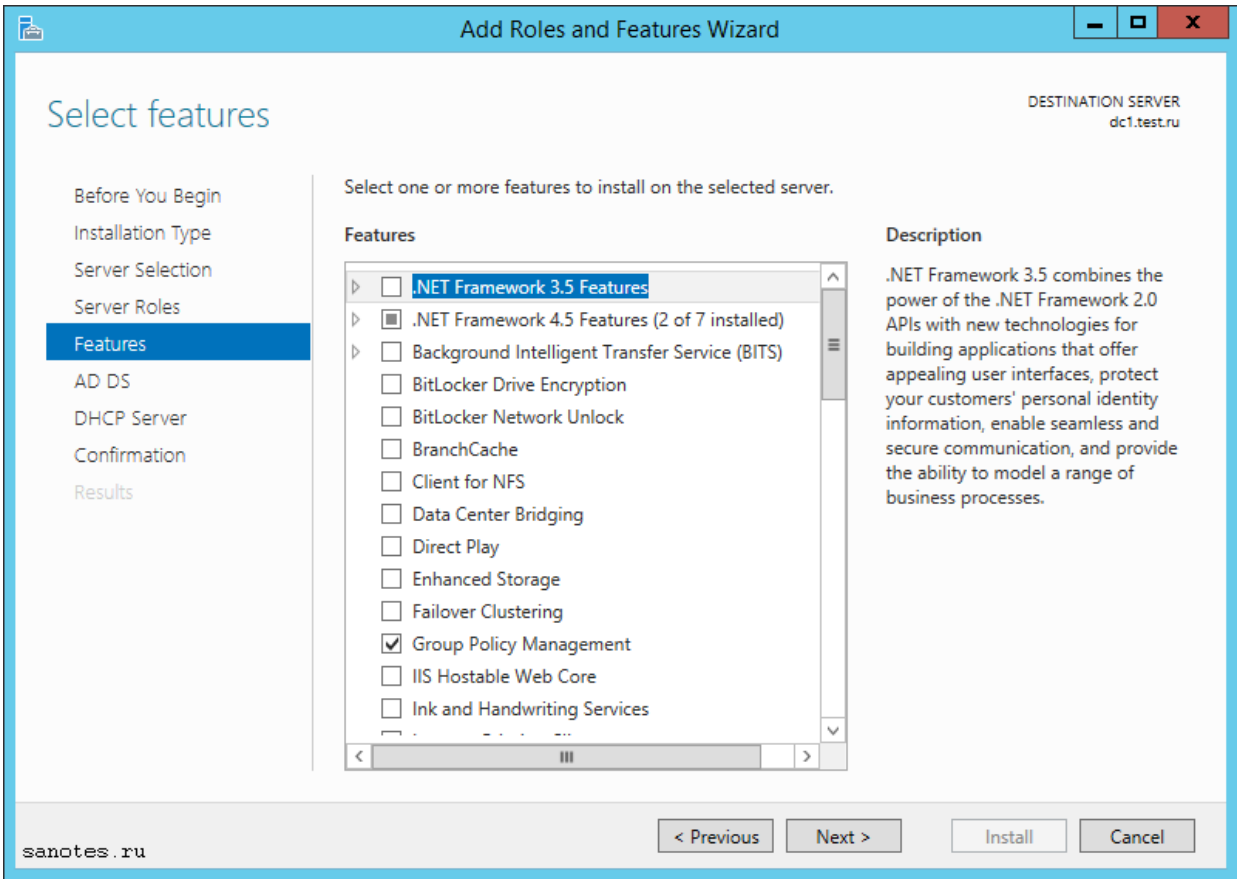
Выбираем **Active Directory Domain Services** (Доменные службы Active Directory), после чего появится окно с предложением добавить роли и компоненты, необходимые для установки роли AD. Нажимаем кнопку Add Features и затем Next.



Обычно, на серверах с AD DS имеет смысл, параллельно разворачивать DHCP Server, поэтому отмечаем его для установки так же. Соглашаемся с установкой компонент. Нажимаем Next.



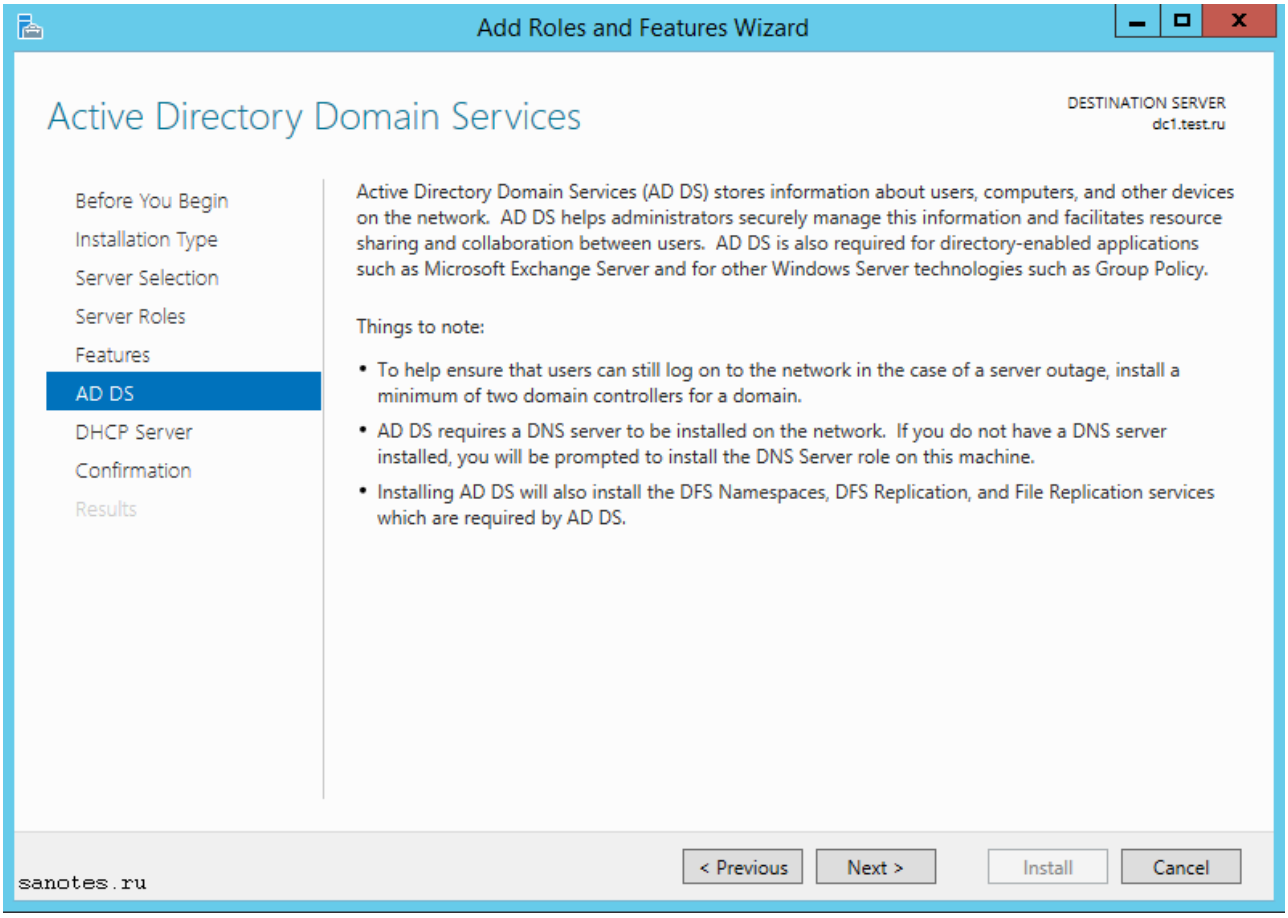
На экране **Features** предлагается выбрать дополнительные компоненты. На контроллере домена ничего экстраординарного обычно не требуется, поэтому нажимаем Next.



На завершающих этапах подготовки к установке, на вкладке AD DS, мастер даст нам некоторые пояснения, а именно, в случае, если основной контроллер будет не доступен, то рекомендуется в одном домене держать как минимум два контроллера.

Службы **Active Directory Domain Services** требуют установленного в сети DNS-сервера. В случае если он не установлен, то роль DNS Server будет предложена для установки.

Так же, службы **Active Directory Domain Services** требуют установки дополнительных служб пространства имен, файловой и DFS репликации **(DFS Namespace, DFS Replication, File Replication)**. Нажимаем Next.



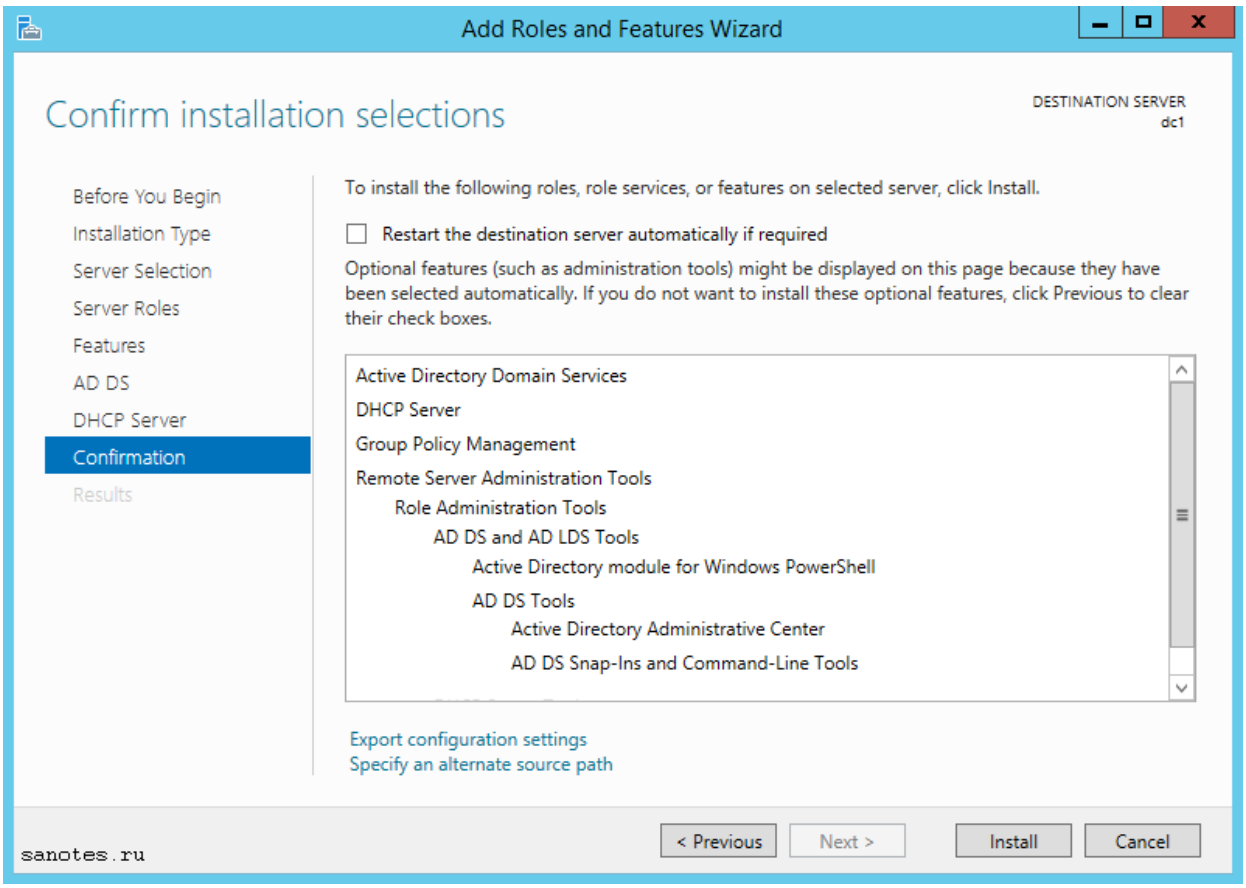
На последнем экране **Confirm installation selection** (Подтверждение устанавливаемых компонентов), можно экспортировать конфигурацию в xml-фаил, который поможет быстро установить еще один сервер с идентичными настройками. Для этого потребуется на новом сервере, используя PowerShell, ввести следующую команду:

```
Install-WindowsFeature –ConfigurationFilePath
D:\ConfigurationFiles\DeploymentConfigTemplate.xml
```

или если требуется задать новое имя серверу, набираем:

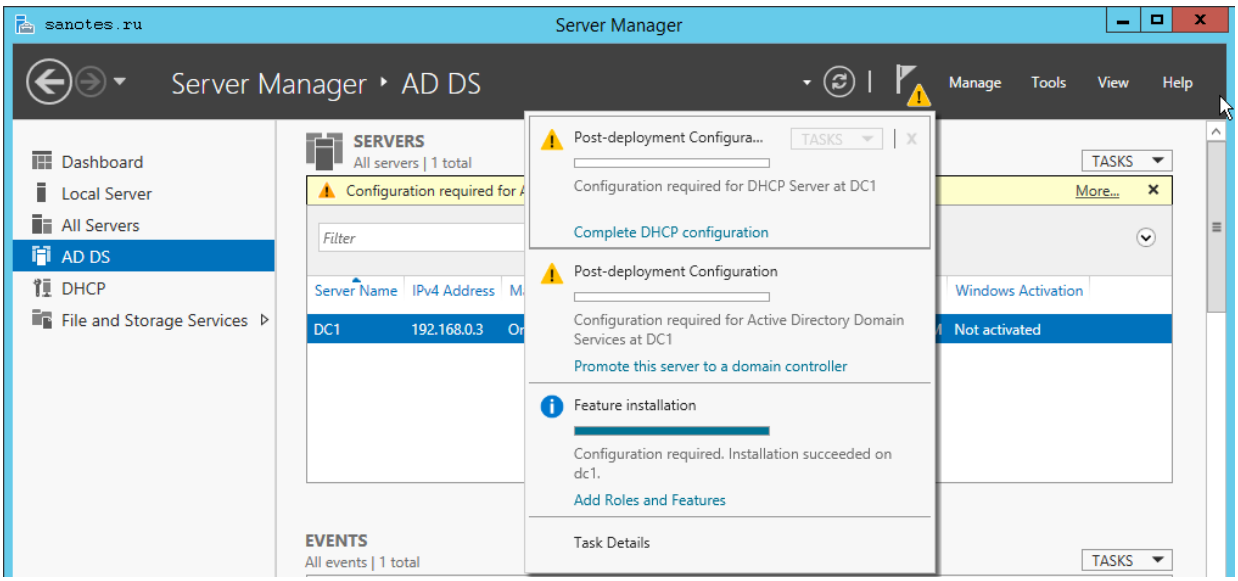
```
Install-WindowsFeature –ConfigurationFilePath
D:\ConfigurationFiles\ADCSConfigFile.xml -ComputerName $servername
```

В конце нажимаем Install. Дожидаемся окончания процесса установки.



Шаг 2: Установка первого контроллера домена. Настройка служб Active Directory, DNS, DHCP.

Теперь нажимаем на значок треугольника с восклицательным знаком и выбираем сначала **Promote this server to domain controller** (Повысить этот сервер до контроллера домена). Позже запустим процесс развертывания DHCP-сервера.



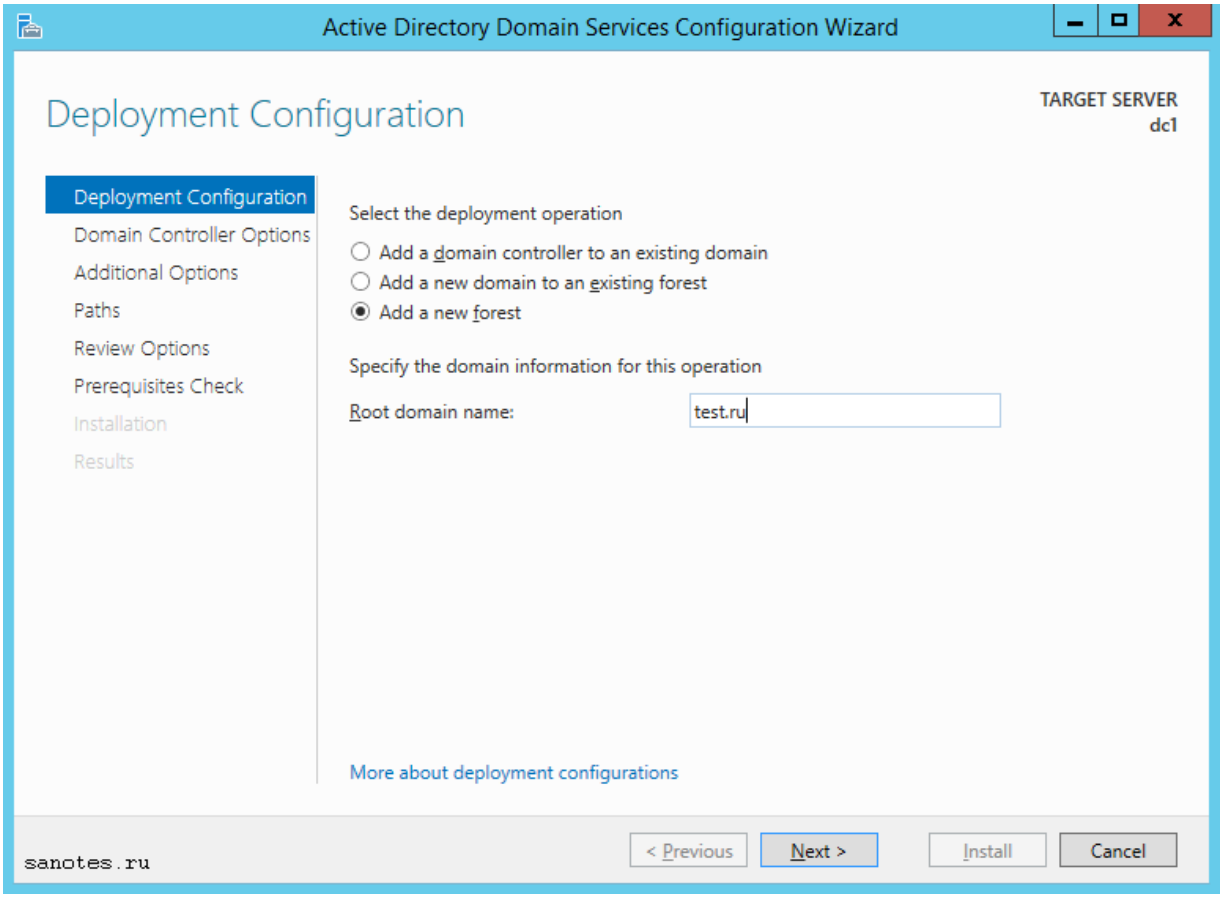
Запустится мастер **Active Directory Domain Services Configuration Wizard** (Мастер конфигурации доменных служб Active Directory). Доступно, три варианта развертывания, если:

Add New Forest — создать новый корневой домен в новом лесу. Используется для новой «чистой» установки Active Directory; (например 'test.ru')

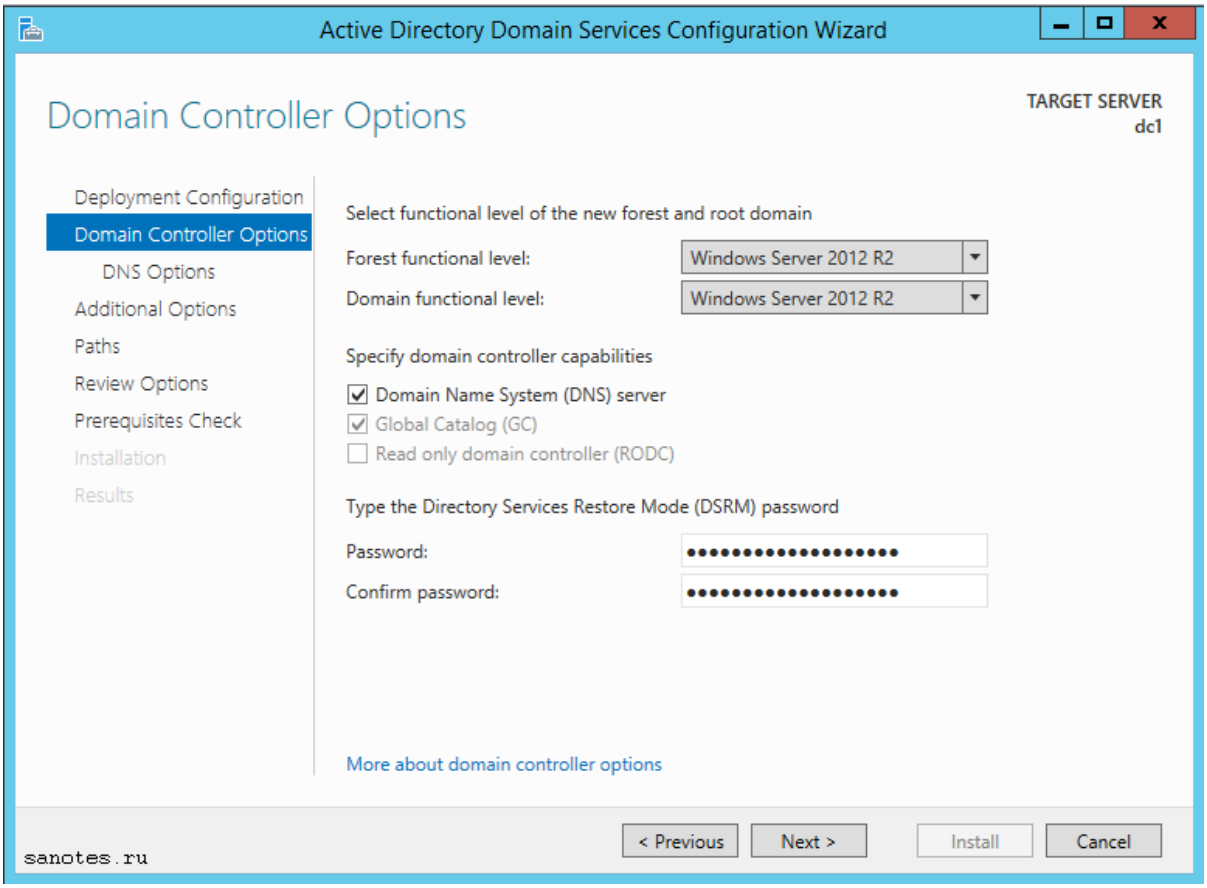
Add a new domain to an existing forest — добавить новый домен в существующем лесу, возможные варианты: *Tree Domain* - корневой домен нового дерева в существующем лесу (например 'test2.ru' параллельно с 'test.ru') или *Child Domain* — дочерний домен в существующем лесу (например 'corp.test.ru')

Add a domain controller to an existing domain — добавить дополнительный контроллер домена в существующем домене, используется для резервного или филиального домена.

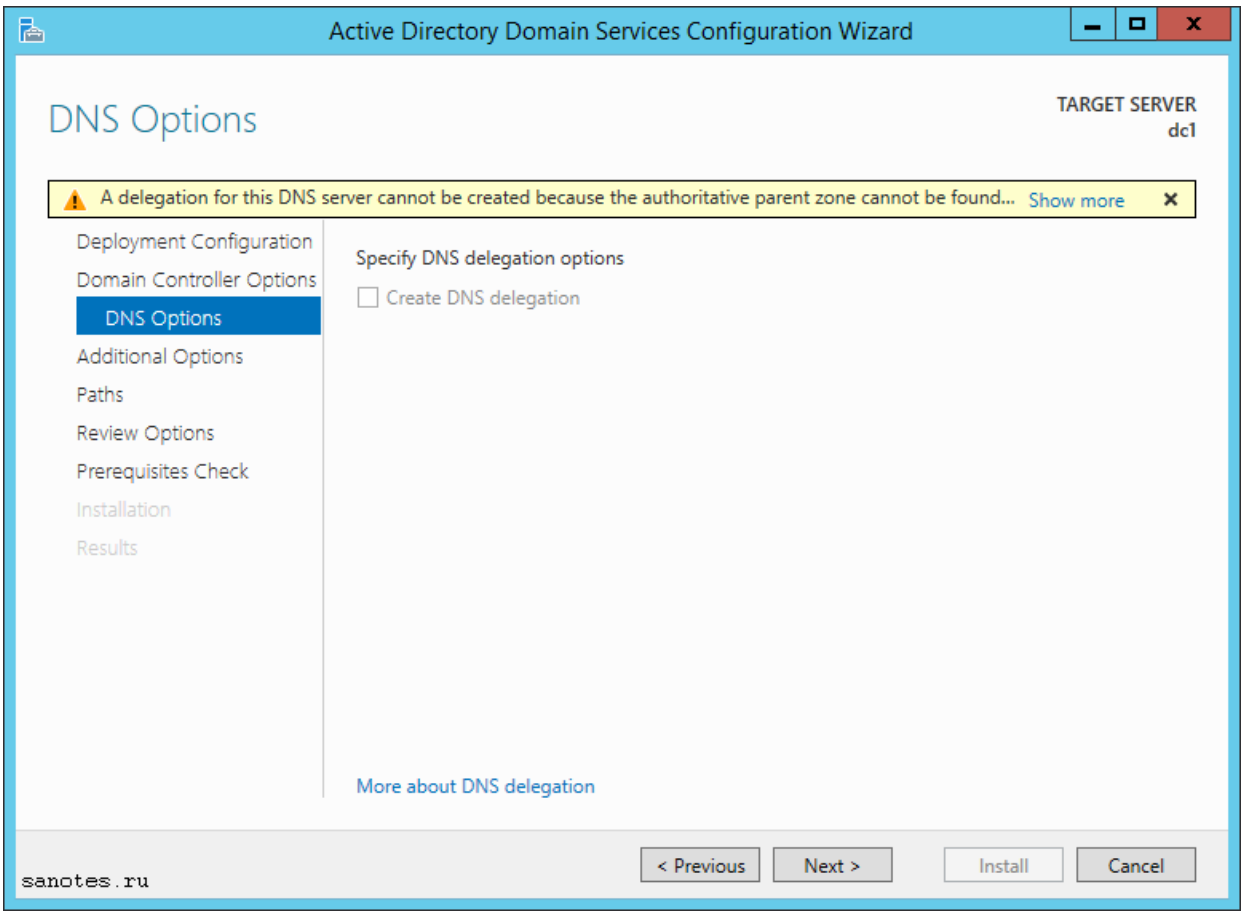
Выбираем вариант **Add New Forest**, задаем корневое имя домена, нажимаем Next.



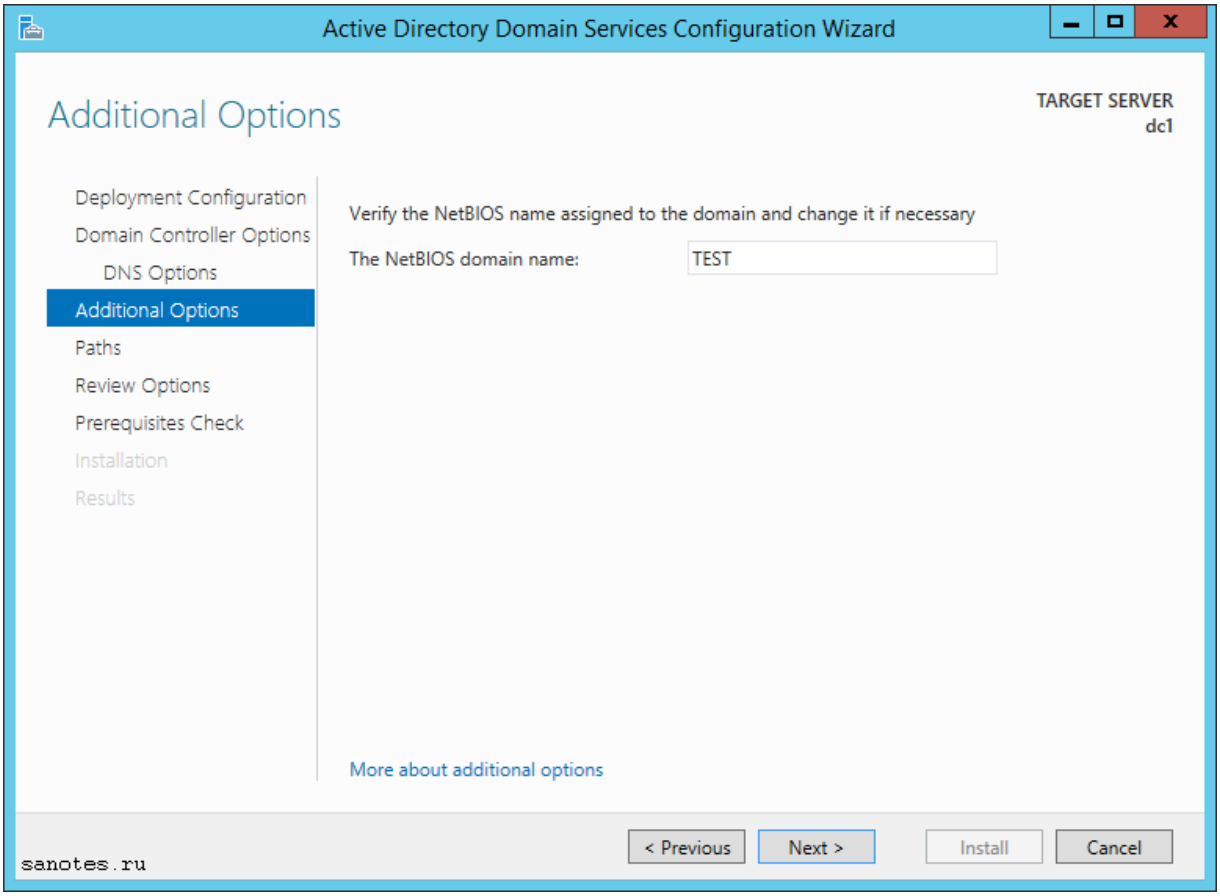
На следующей вкладке можно задать функциональный уровень домена и леса (по умолчанию 2016 R2), снять или отметить для установки DNS Server, и задать пароль для режима восстановления службы каталогов (DSRM). Укажем только пароль для DSRM и нажмем Далее.



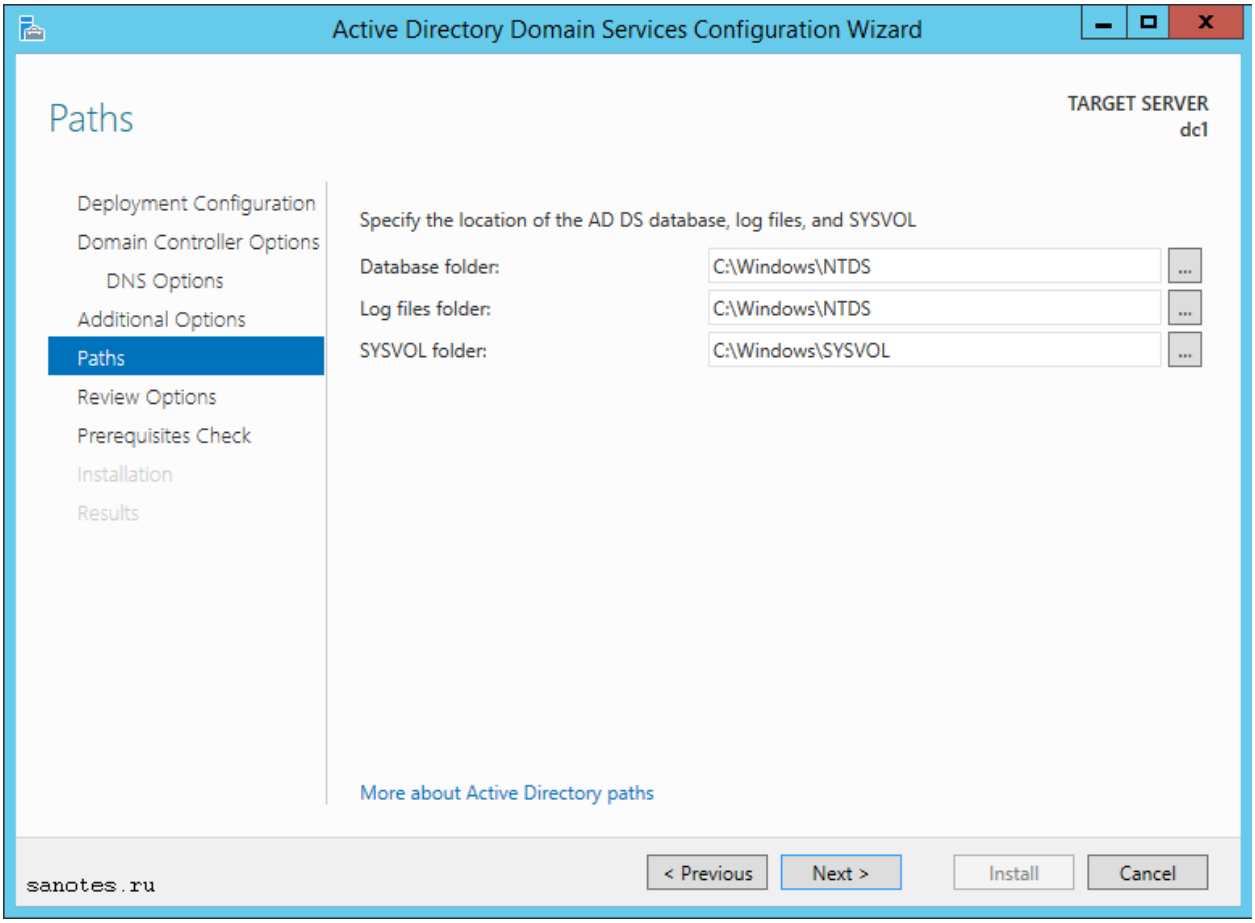
На следующем шаге **DNS Options** мастер ругнется, на то, что делегирование для этого DNS-сервера создано не было, потому что не найдена дочерняя зона или запущенный DNS-сервер. Что не удивительно, т.к. роль DNS Server у нас создается в процессе. Нажимаем Next.



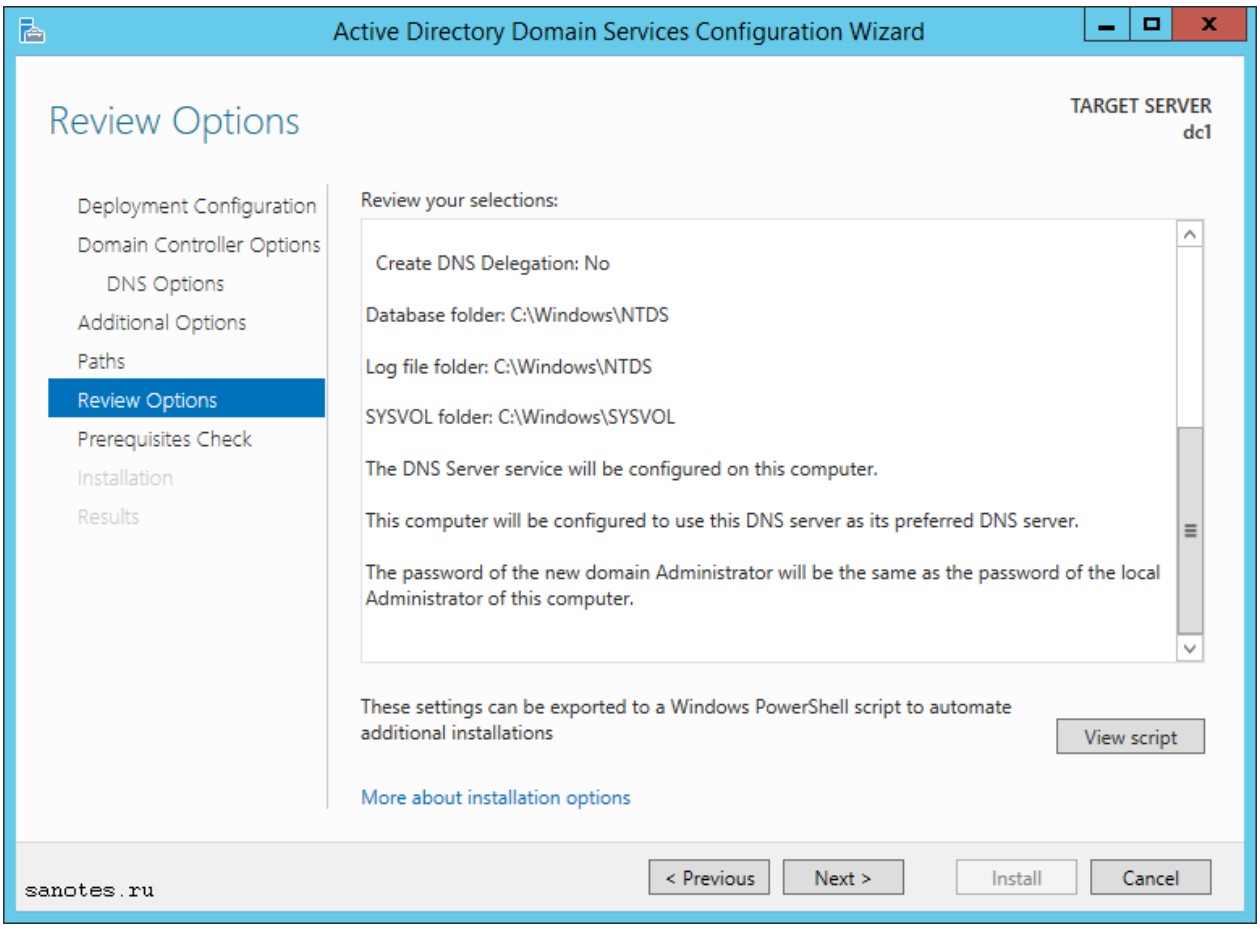
Далее в Addional Optional соглашаемся с NetBIOS именем, которое предлагает нам система, жмем Next.



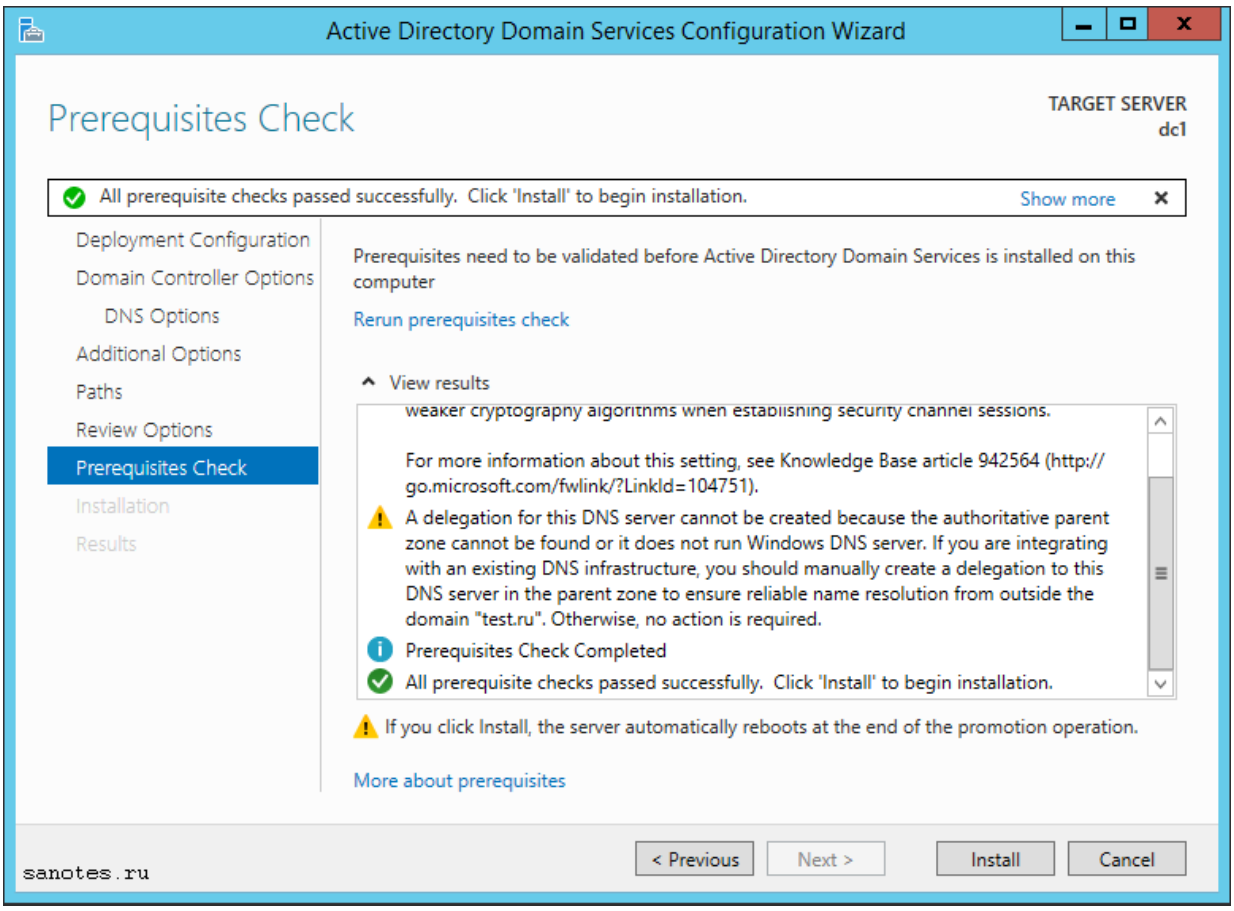
В разделе **Paths** можно изменить путь к каталогам баз данных, файлам журнала и к SYSVOL. Оставляем по умолчанию, нажимаем Next.



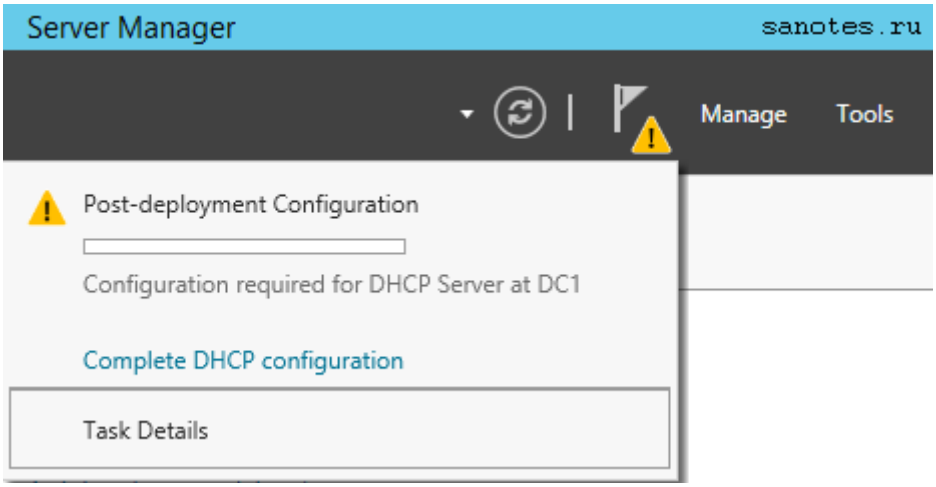
На следующем этапе **Review Options** отображается сводная информация по настройке. Кнопка **View Script**, позволяет посмотреть **Powershell** скрипт, при помощи которого, в будущем можно будет произвести настройку доменных служб **Active Directory**. Нажимаем Next.



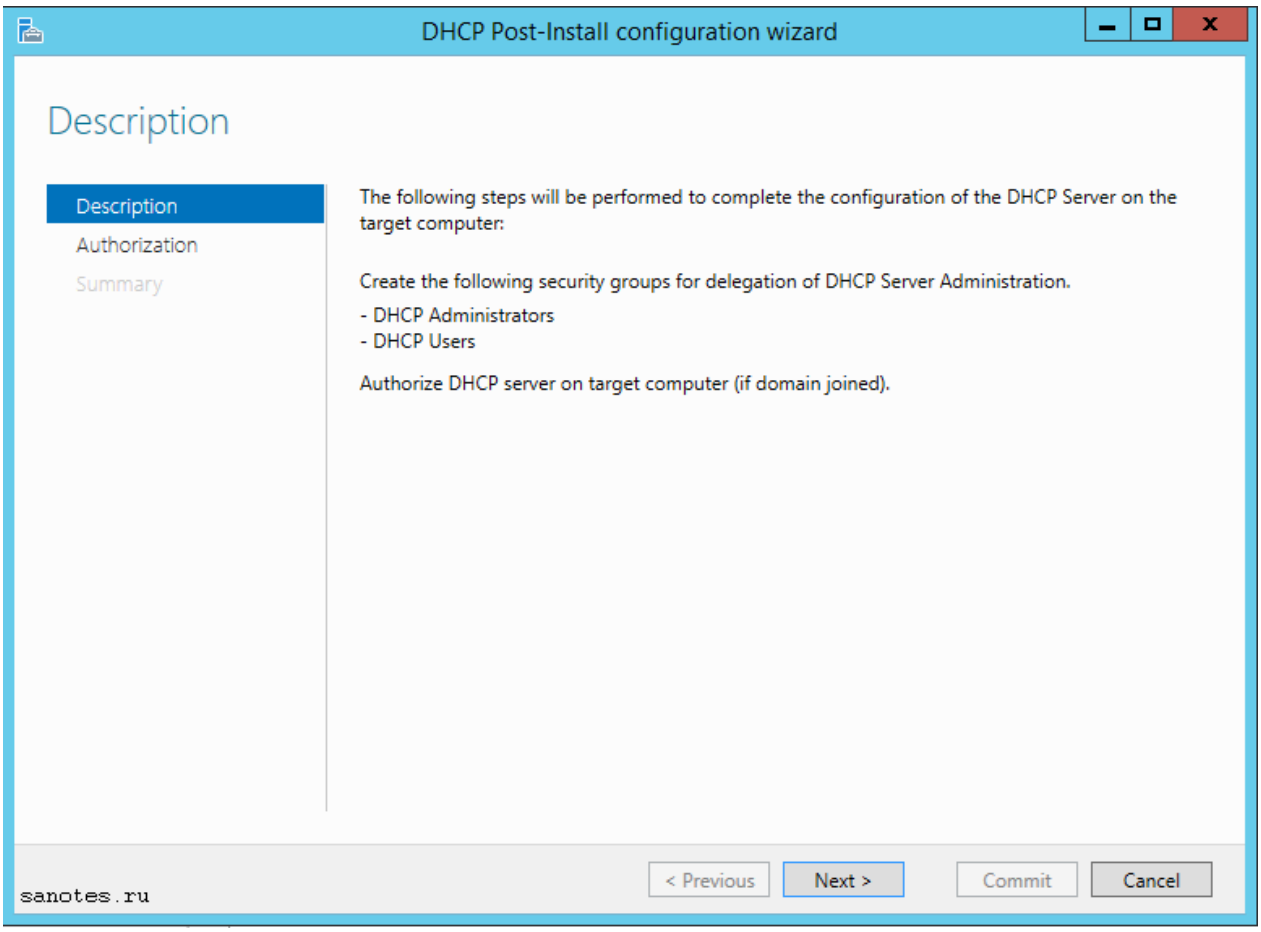
И наконец, на последнем этапе предварительных проверок, если видим надпись: *«All prerequisite checks are passed successfully. Click «install» to begin installation*.» (Все предварительные проверки пройдены успешно. Нажмите кнопку «установить», чтобы начать установку.), то нажимаем Install, дожидаемся окончания процесса установки.



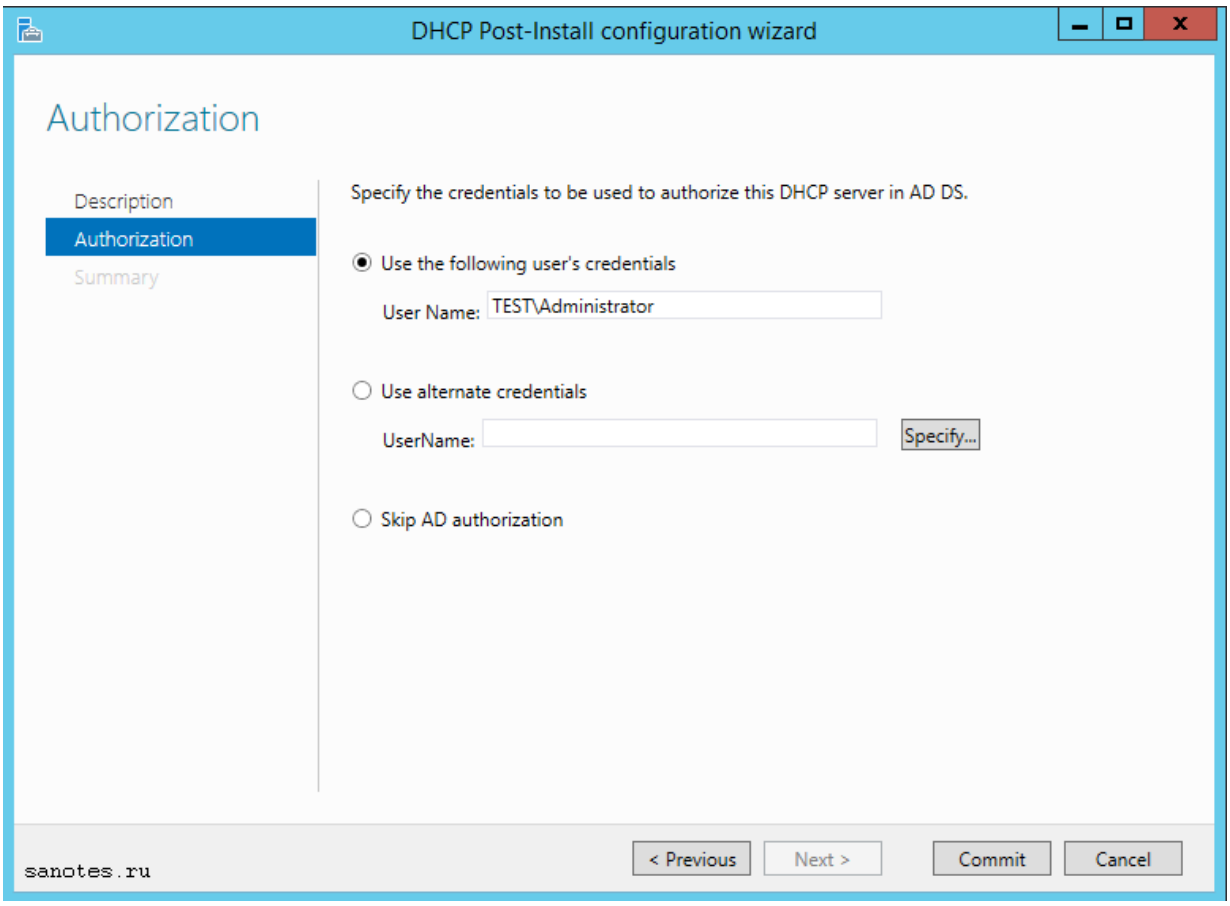
После перезагрузки, снова заходим в **Server Manager -> Dashboard** и запускаем пиктограмму треугольника с восклицательным знаком и выбираем там **Complete DHCP Configuration** (Завершение конфигурации DHCP).



Запустится мастер по конфигурированию DHCP, который нам сообщит, что будут созданы группы безопасности администратора и пользователя DHCP-сервера, и будет произведена авторизация в AD. Нажимаем Next.

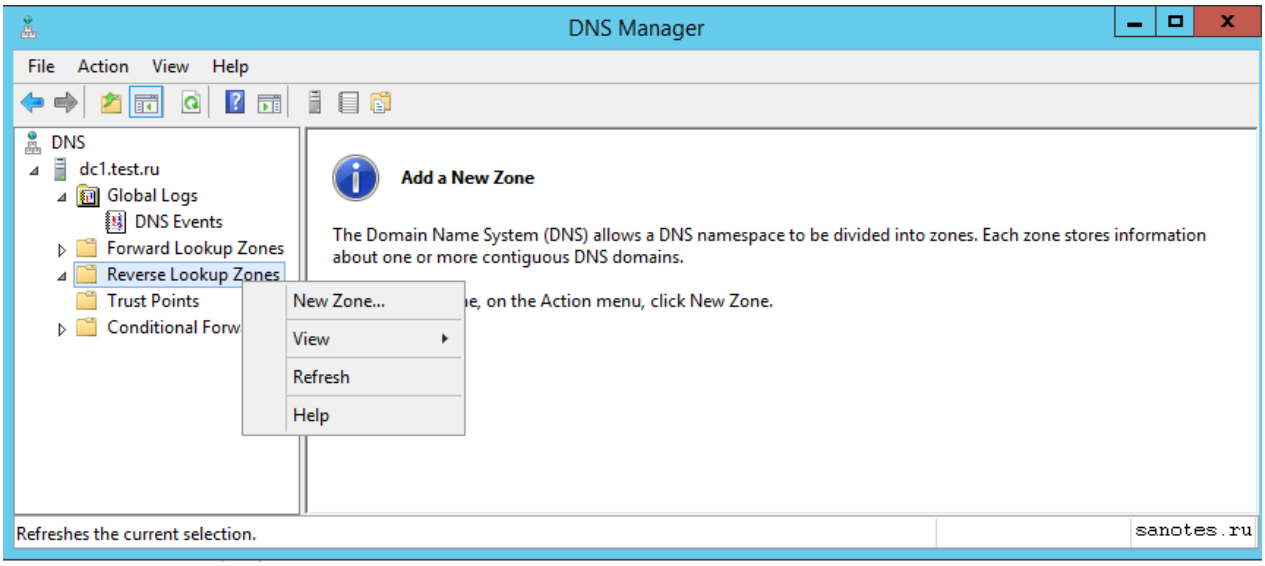


На следующем экране нажимаем Commit что бы завершить процесс авторизации в Active Directory.



Если видим, что *Create Security Group — Done* и *Authorizing DHCP Server — Done*, то процесс завершился успешно, нажимаем Close.

Теперь создадим обратную зону в DNS. Обратная зона, позволяет выполнить разрешение FQDN-имен хостов по их IP-адресам. В процессе добавления ролей AD и DNS по умолчанию не создаются, поскольку предполагается, что в сети может существовать другой DNS-сервер, контролирующий обратную зону. Поэтому создадим ее сами, для этого переходим в диспетчер DNS (DNS Manager), на вкладку Reverse Lookup Zones, кликаем правой кнопкой и выбираем New Zone.



Запустится мастер DNS-зоны. Соглашаемся с параметрами по умолчанию, а именно нам предлагается создать основную зону которая будет хранится на этом сервере (Primary

Zone) и будет интегрирована в Active Directory (Store the zone in Active Directory...). Нажимаем Next.

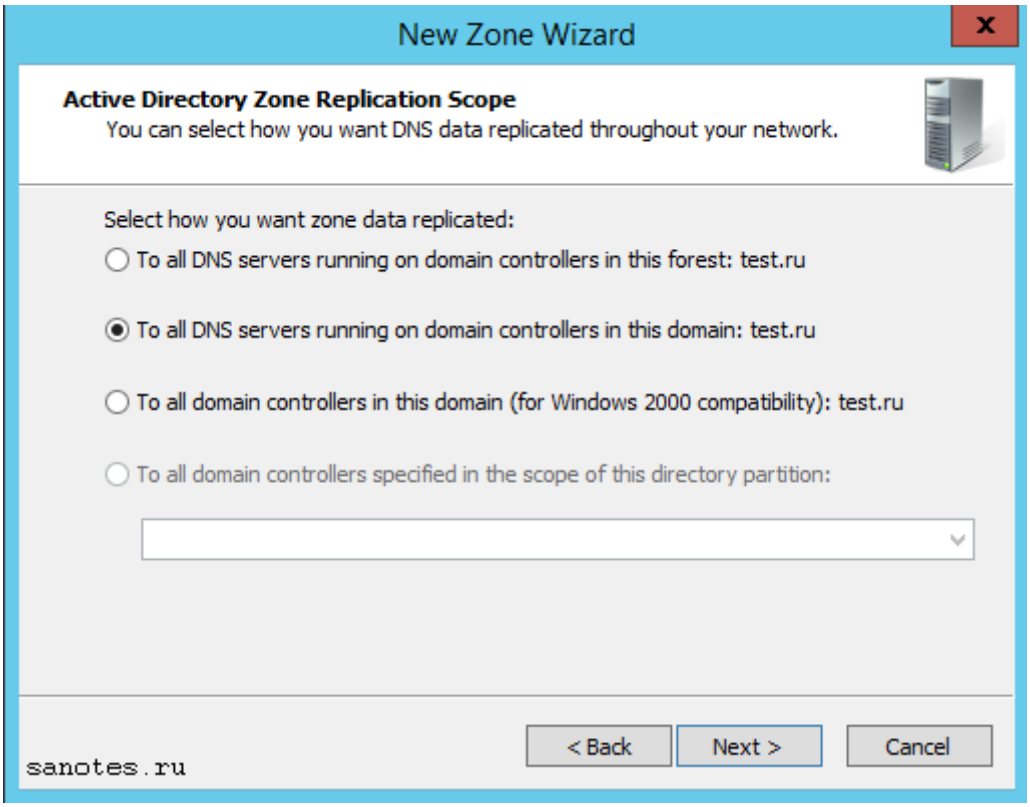
На следующем экране, предлагается выбрать как зона будет реплицироваться, обмениваться данными с другими зонами расположенными на контроллерах и DNS-серверах. Возможны следующие варианты:

Для всех DNS-серверов расположенных на контроллере домена в этом лесу (To all DNS servers running on domain controllers in this forest). Репликации во всем лесу Active Directory включая все деревья доменов.

Для всех DNS-серверов расположенных на контроллере домена в этом домене (To all DNS servers running on domain controllers in this domain). Репликация внутри текущего домена и его дочерних доменов.

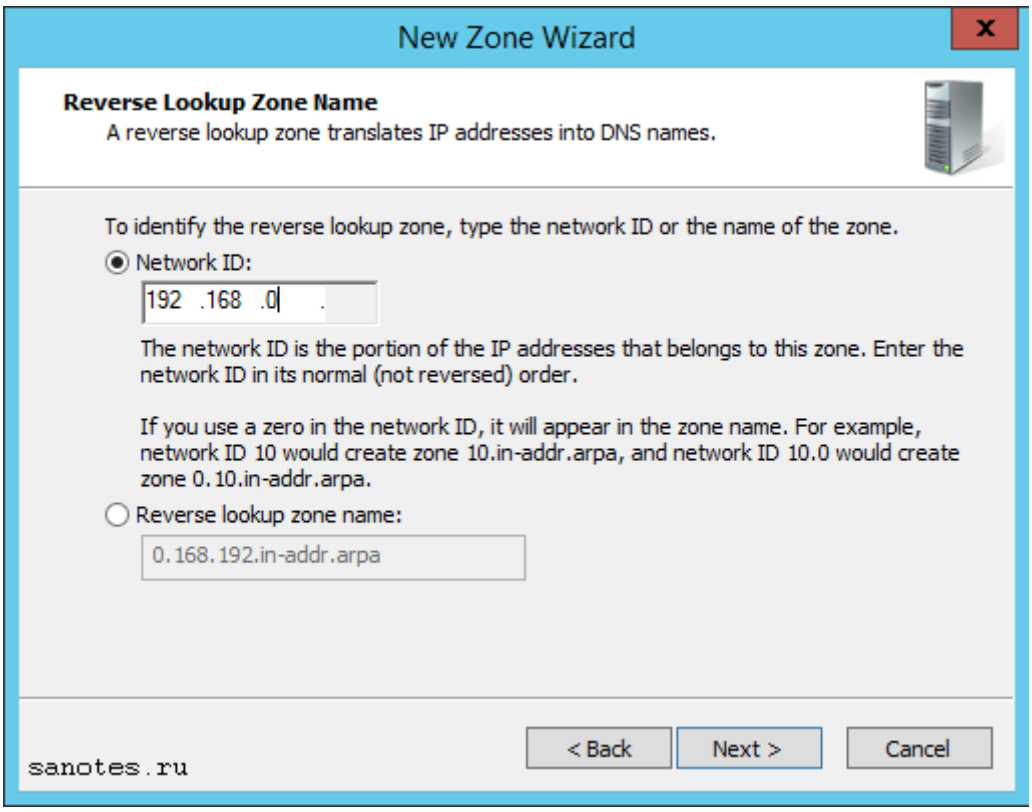
Для всех контроллеров домена в этом домене (To all domain controllers in this domain). Репликация на все контроллеры домена внутри текущего домена и его дочерних доменов.

На все контроллеры домена в указанном разделе каталога приложений (To all domain controllers specified in the scope of this directory partition). Репликация на все контроллеры домена, но DNS-зона располагается в специальном каталоге приложений. Поле будет доступно для выбора, после создания каталога.



Выбираем вариант по умолчанию, нажимаем Next. Затем выбираем протокол по умолчанию IPv4 и снова жмем Next.

На следующем экране зададим идентификатор сети (Network ID). В нашем случае 192.168.0. В поле Reverse Lookup Zone Name увидим как автоматически подставится адрес зоны обратного просмотра. Нажимаем Next.



На экране Dynamic Update (динамические обновления), выберем один из трех возможных вариантов динамического обновления.

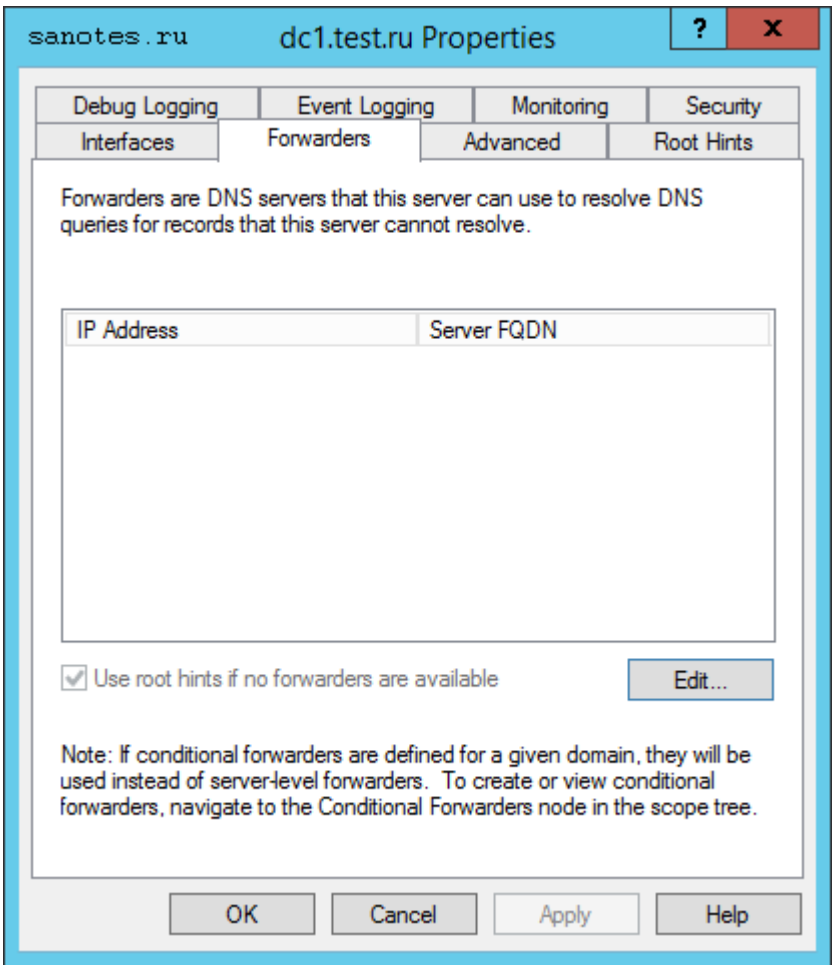
Разрешить только безопасные динамические обновления (Allow Only Secure Dynamic Updates). Это опция доступна, только если зона интегрирована в Active Directory.

Разрешить любые, безопасные и не безопасные динамические обновления (Allow Both Nonsecure And Secure Dynamic Updates). Данный переключатель, позволяет любому клиенту обновлять его записи ресурса в DNS при наличии изменений.

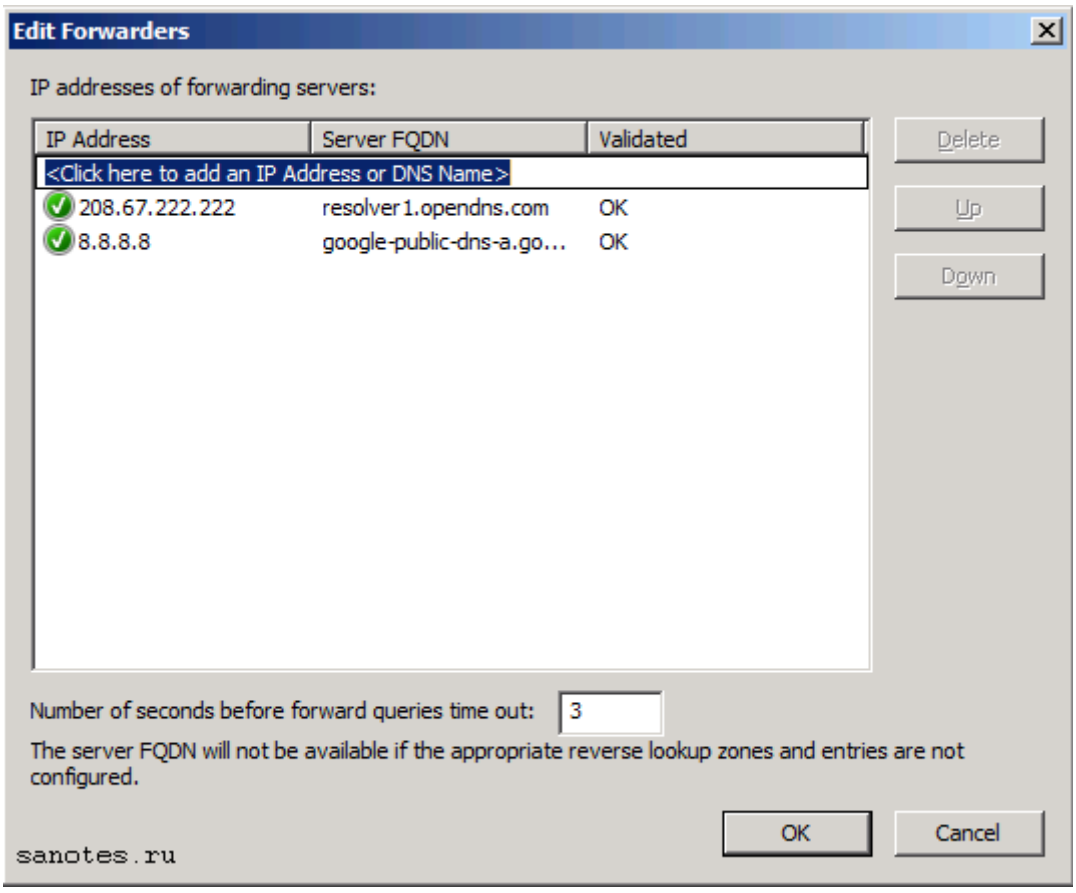
Запретить динамические обновления (Do Not Allow Dynamic Updates). Это опция отключает динамические обновления DNS. Ее следует использовать только при отсутствии интеграции зоны с Active Directory.

Выбираем первый вариант, нажимаем Next и завершаем настройку нажатием Finish.

Еще одна полезная опция, которая обычно настраивается в DNS — это серверы пересылки или Forwarders, основное предназначение которых кэшировать и перенаправлять DNS-запросы с локального DNS-сервера на внешний DNS-сервер в сети интернет, например тот что находится у провайдера. Например мы хотим, что бы локальные компьютеры в нашей доменной сети, в сетевых настройках у которых прописан DNS-сервер (192.168.0.3) смогли получить доступ в интернет, необходимо что бы наш локальный dns-сервер был настроен на разрешение dns-запросов вышестоящего сервера. Для настройки серверов пересылки (Forwarders) переходим в консоль менеджера DNS. Затем в свойствах сервера переходим на вкладку Forwarders и нажимаем там Edit.

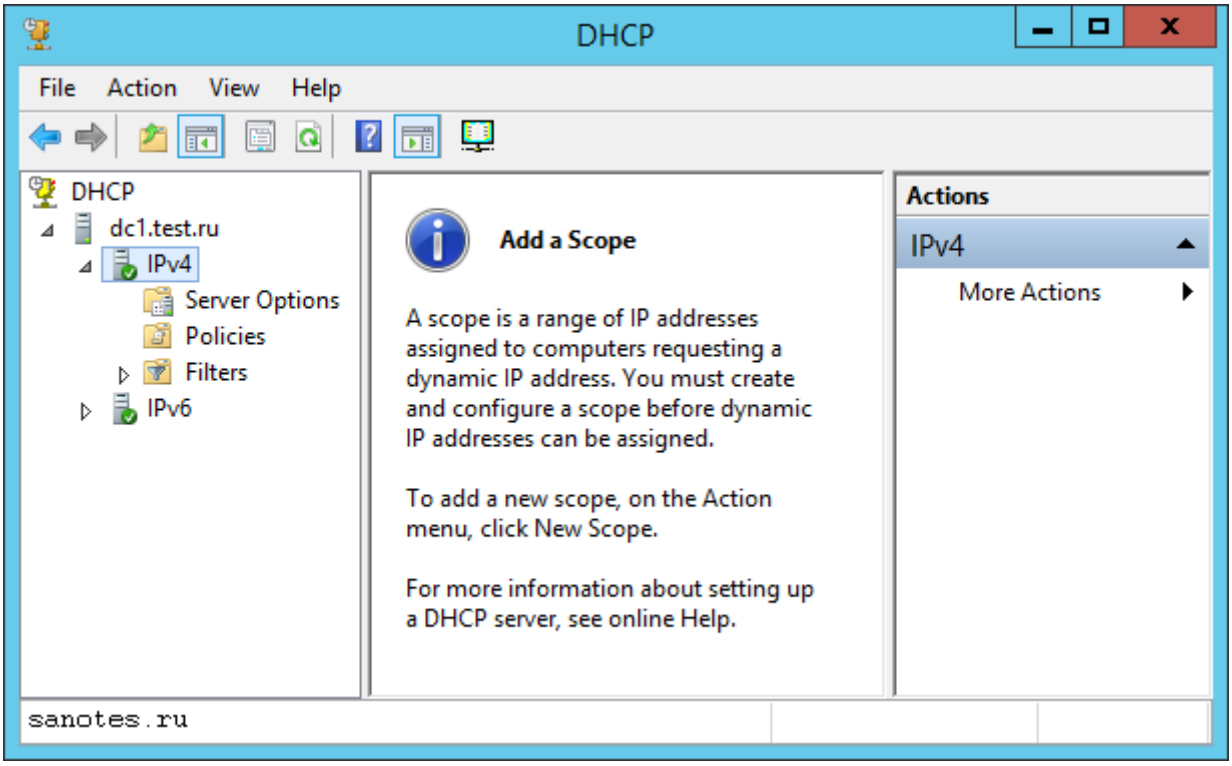


Укажем как минимум один IP-адрес. Желательно несколько. Нажимаем OK.

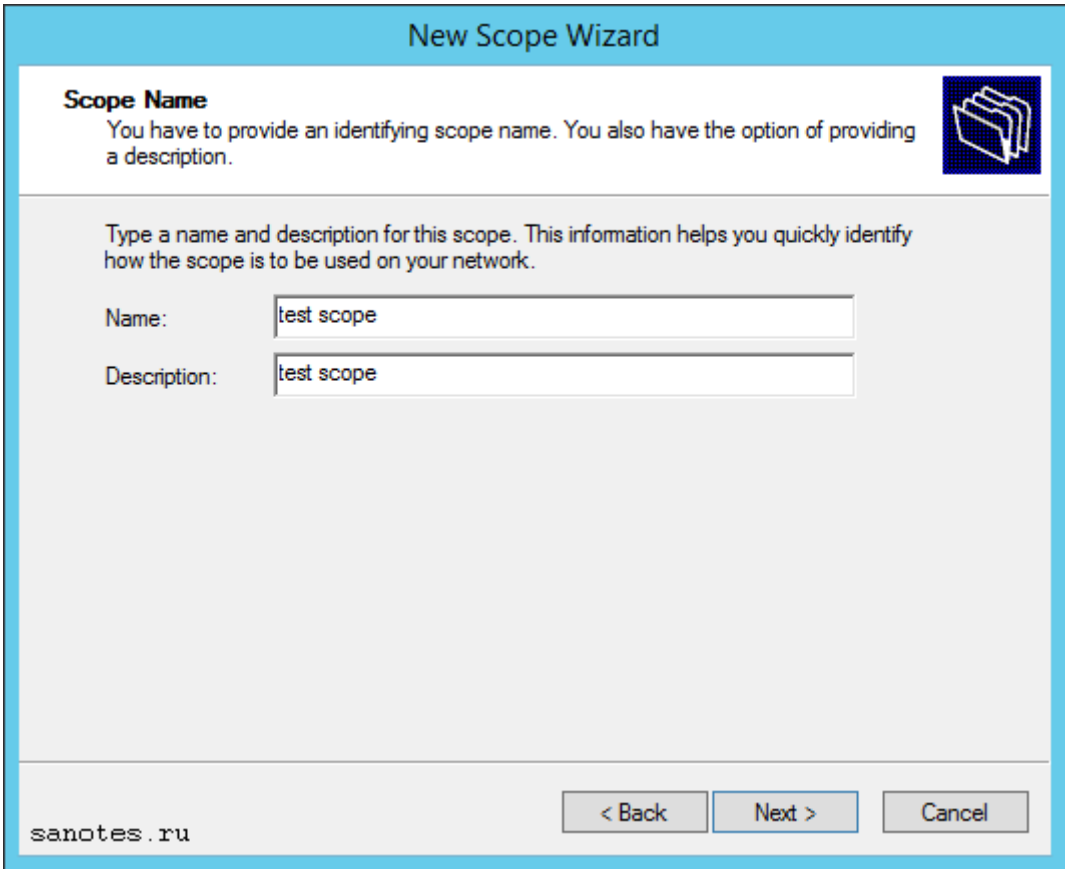


Настройка службы DHCP.

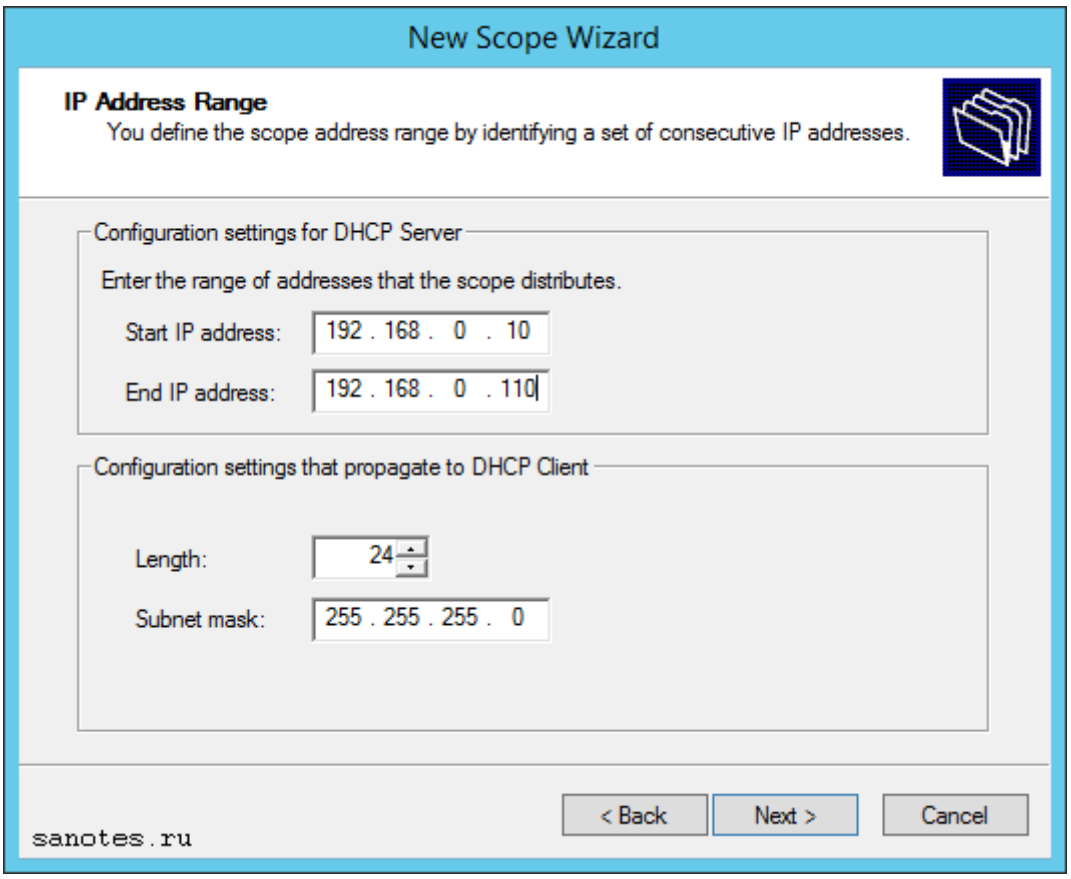
Запускаем оснастку DHCP.



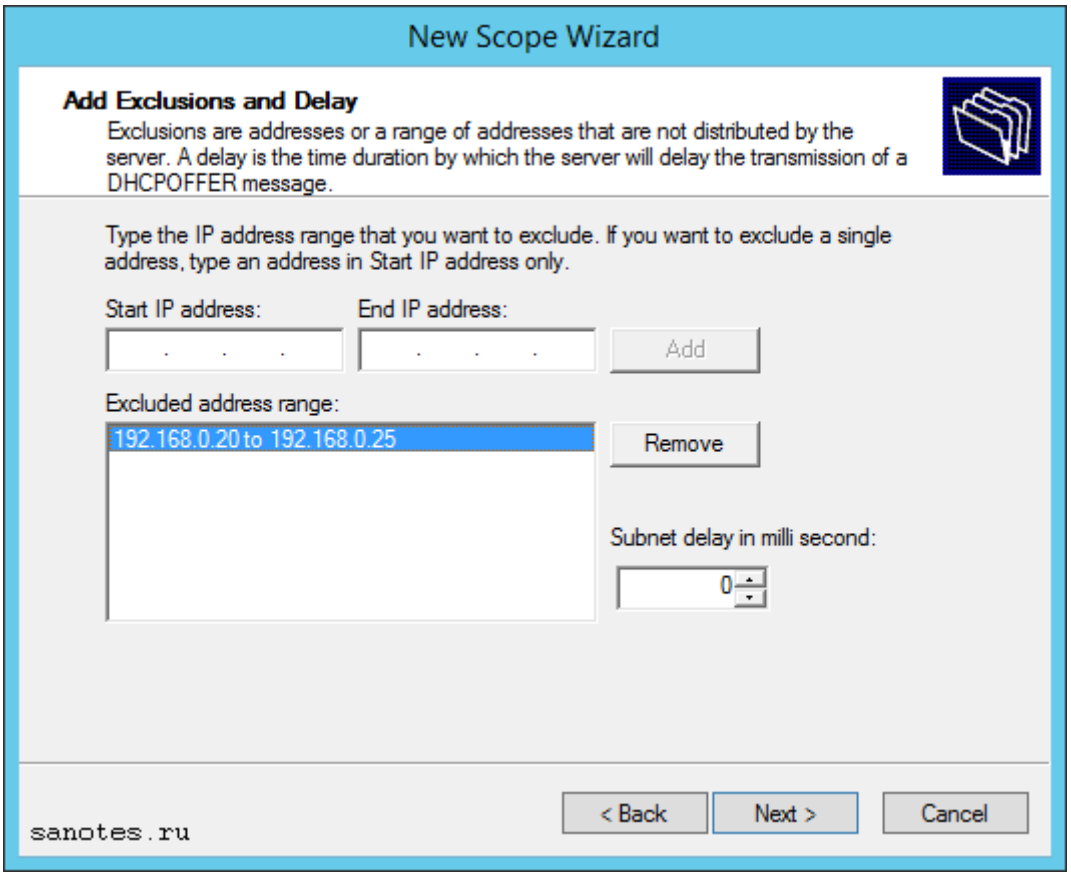
Сперва зададим полный рабочий диапазон адресов из которого будут браться адреса для выдачи клиентам. Выбираем Action\New Scope. Запустится мастер добавления области. Зададим имя области.



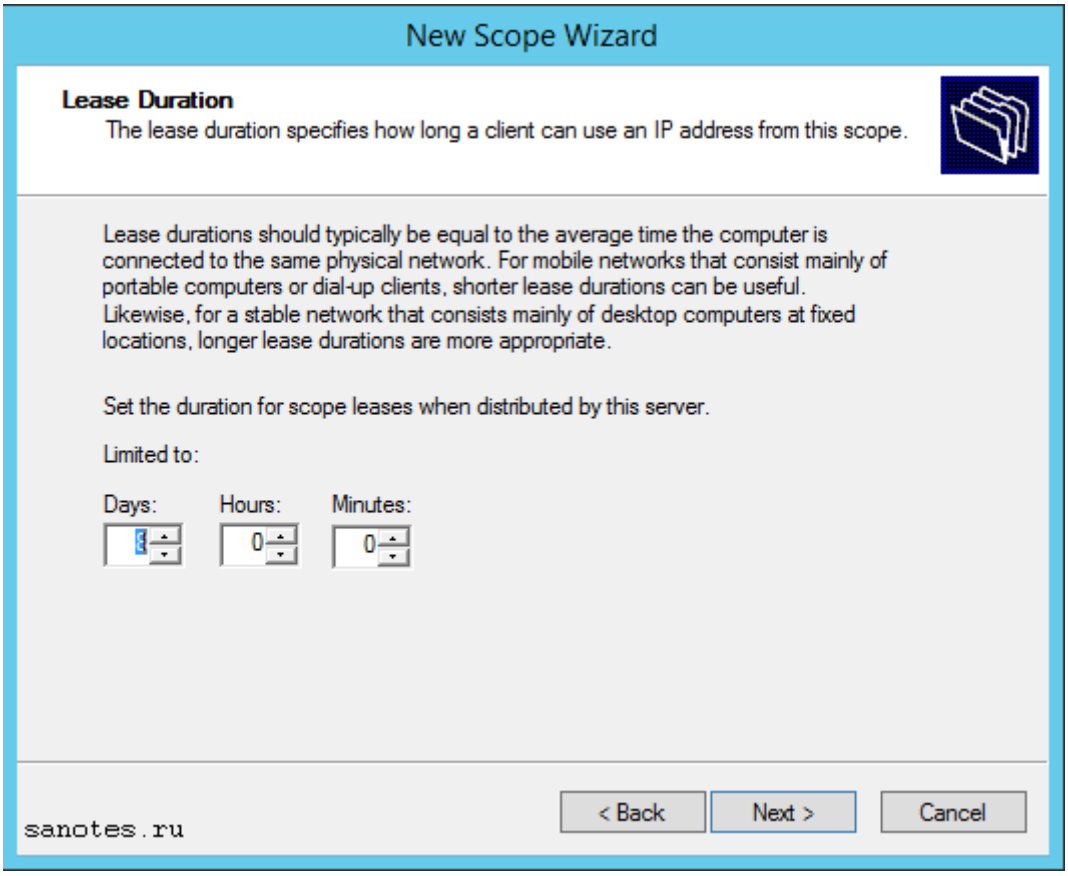
Далее укажем начальный и конечный адрес диапазона сети.



Далее добавим адреса которые мы хотим исключить из выдачи клиентам. Жмем Далее.

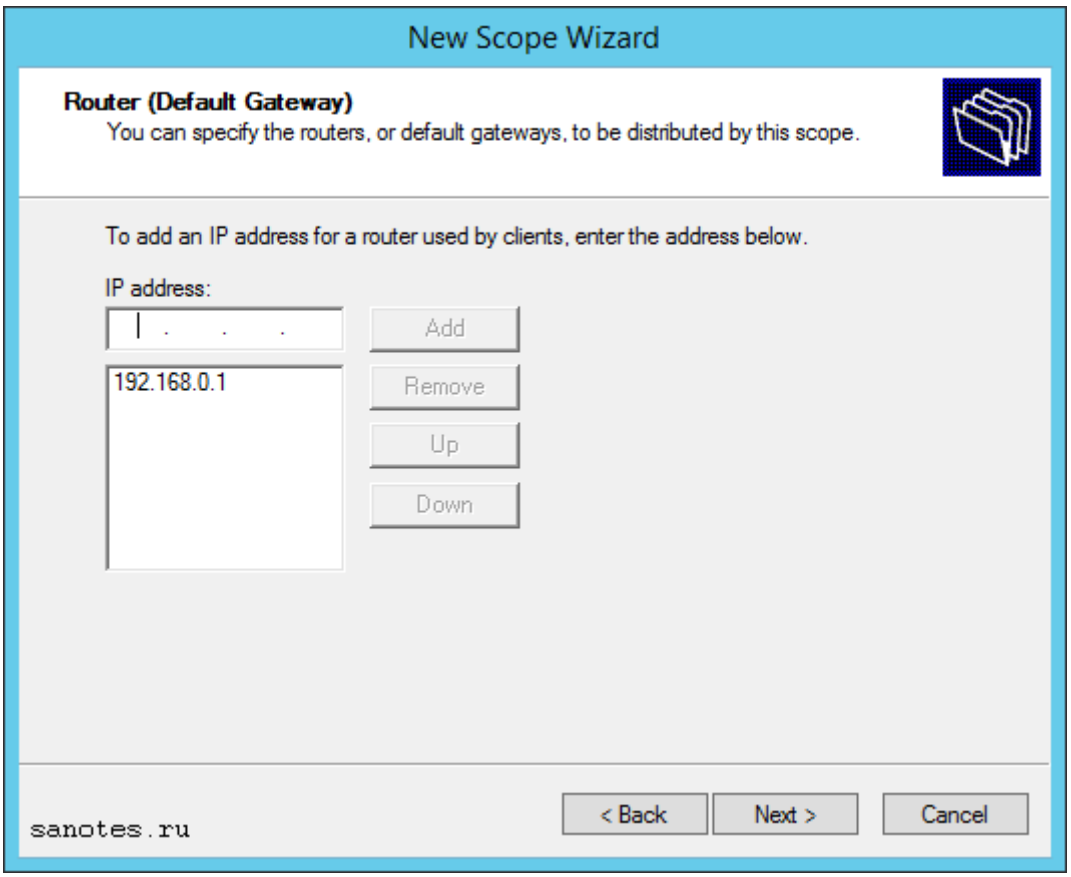


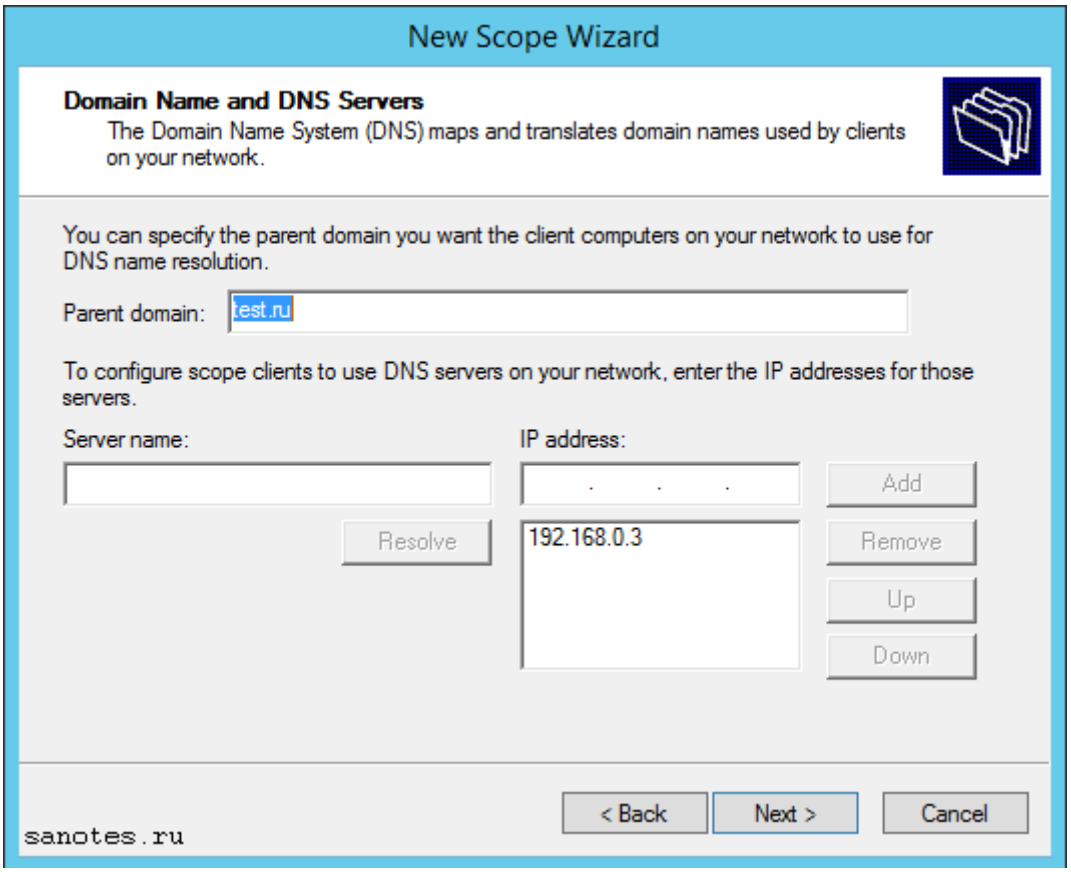
На экране Lease Duration укажем отличное от по умолчанию время аренды, если требуется. Жмем Далее.

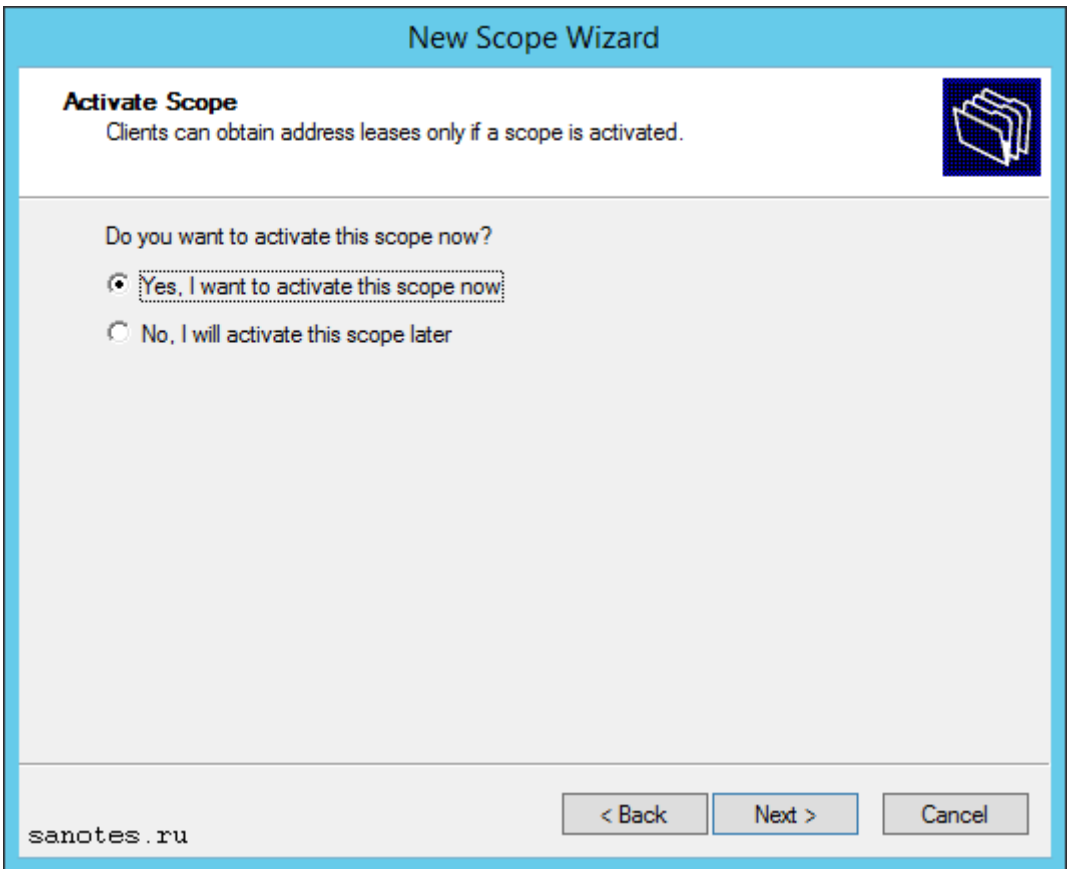


Затем согласимся, что хотим настроить опции DHCP: Yes, I want to configure these option now.

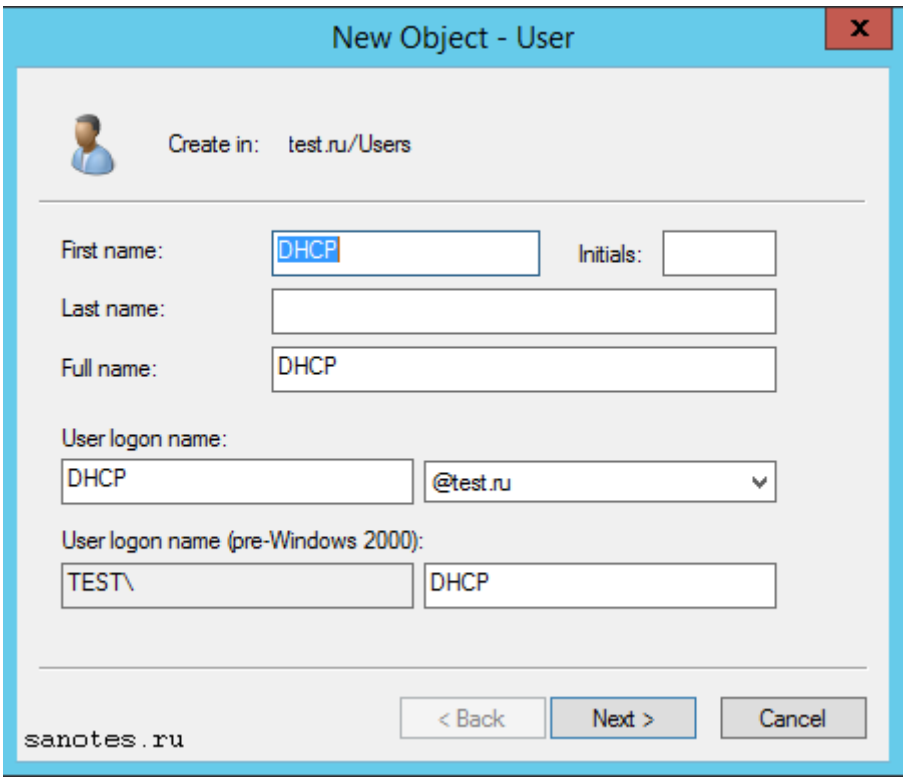
Последовательно укажем шлюз, доменное имя, адреса DNS, WINS пропускаем и в конце соглашаемся с активацией области нажатием: Yes, I want to activate this scope now. Finish.


New Scope Wizard
Router (Default Gateway)
You can specify the routers, or default gateways, to be distributed by this scope.
To add an IP address for a router used by clients, enter the address below.
IP address:
Add
192.168.0.1
Remove
Up
Down
sanotes.ru
< Back
Next >
Cancel

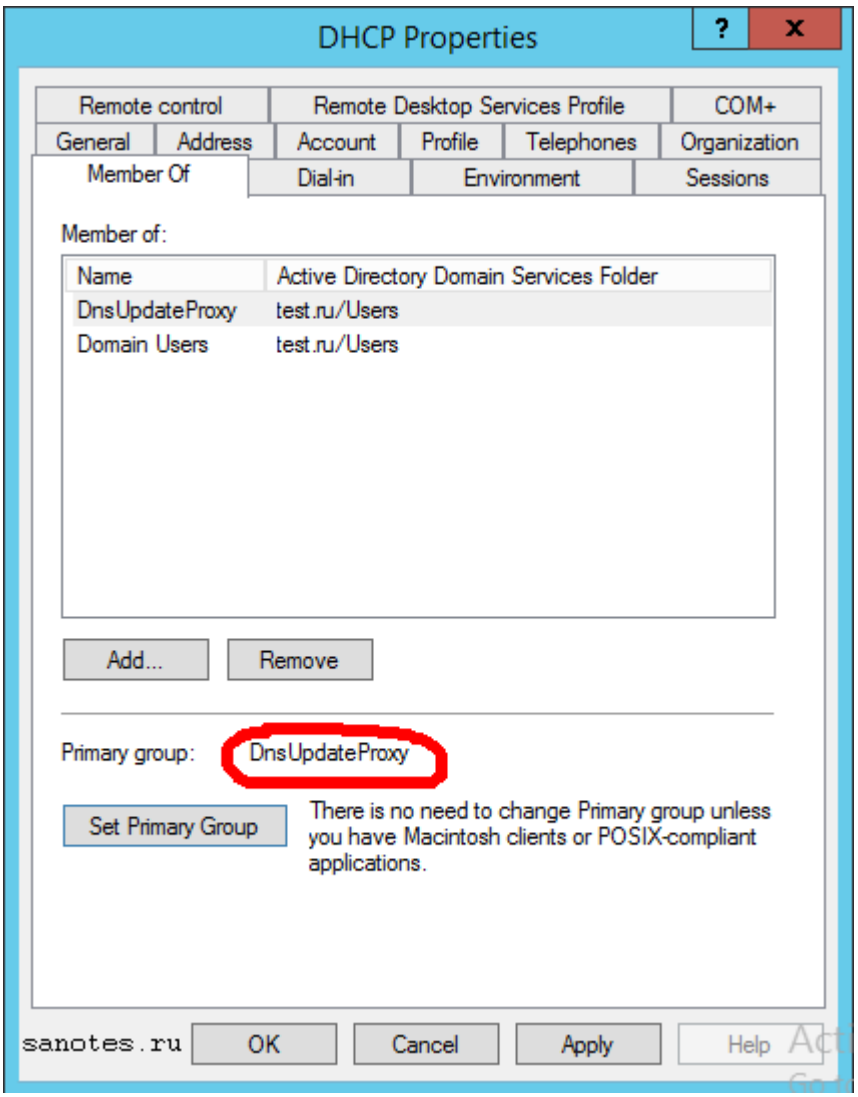

New Scope Wizard
Domain Name and DNS Servers
The Domain Name System (DNS) maps and translates domain names used by clients on your network.
You can specify the parent domain you want the client computers on your network to use for DNS name resolution.
Parent domain:
est.ru
To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.
Server name:
IP address:
Add
Resolve
192.168.0.3
Remove
Up
Down
sanotes.ru
< Back
Next >
Cancel



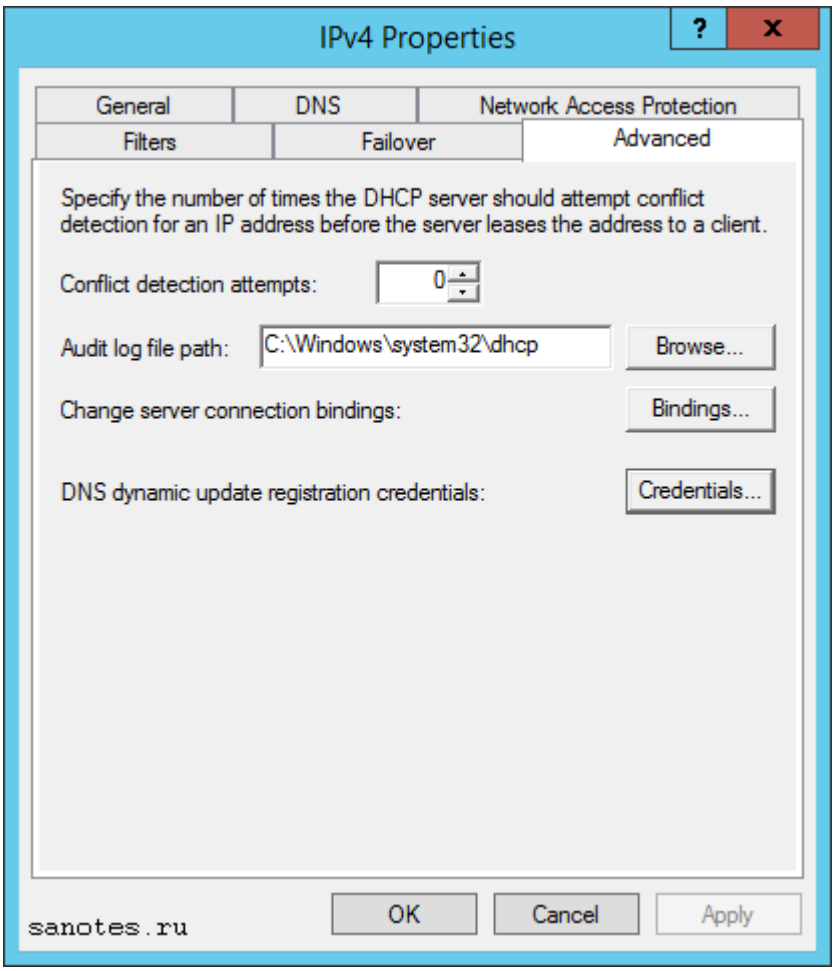
Для безопасной работы службы DHCP, требуется настроить специальную учетную запись для динамического обновления записей DNS. Это необходимо сделать, с одной стороны для того что бы предотвратить динамическую регистрацию клиентов в DNS при помощи административной учетной записи домена и возможного злоупотребления ею, с другой стороны в случае резервирования службы DHCP и сбоя основного сервера, можно будет перенести резервную копию зоны на второй сервер, а для этого потребуется учетная запись первого сервера. Для выполнения этих условий, в оснастке Active Directory Users and Computers создадим учетную запись с именем dhcp и назначим бессрочный пароль, выбрав параметр: Password Never Expires.



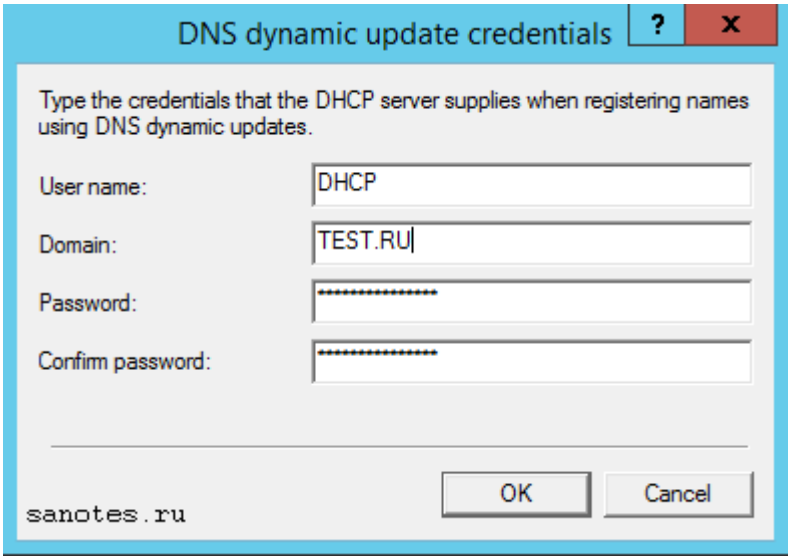
Назначим пользователю надежный пароль и добавим в группу DnsUpdateProxy. Затем удалим пользователя из группы Domain Users, предварительно назначив пользователю primary группу «DnsUpdateProxy». Данная учетная запись будет отвечать исключительно за динамическое обновление записей и не иметь доступа не каким другим ресурсам где достаточно базовых доменных прав.



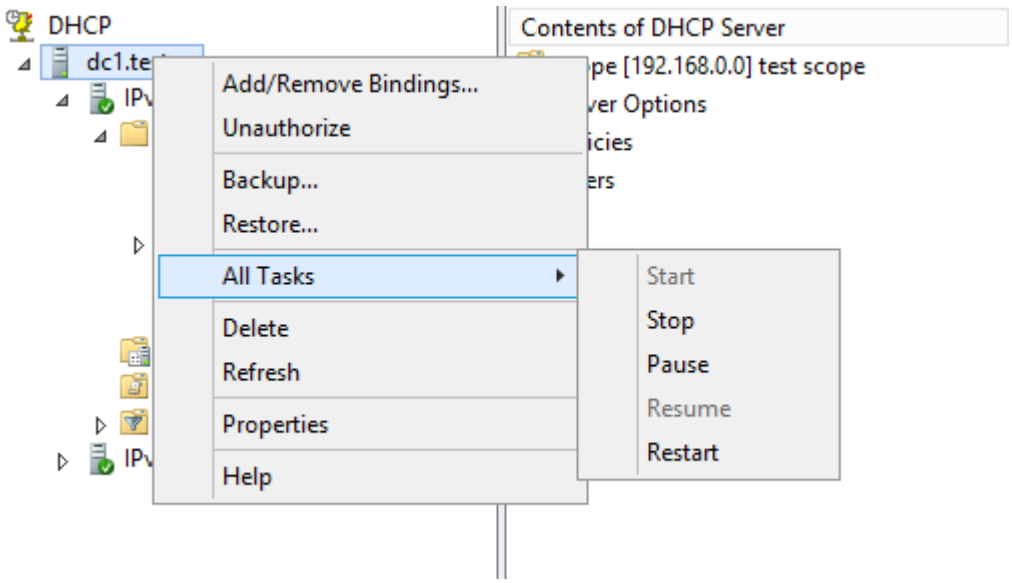
Нажимаем Apply и затем OK. Открываем снова консоль DHCP. Переходим в свойства протокола IPv4 на вкладку Advanced.



Нажимаем Credentials и указываем там нашего пользователя DHCP.

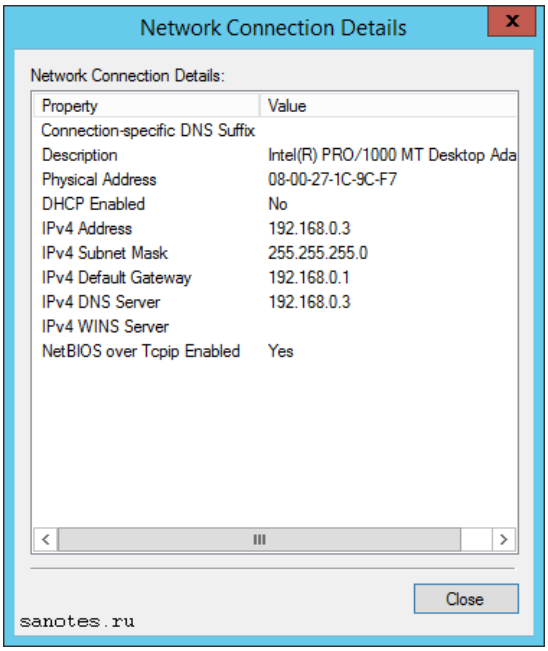


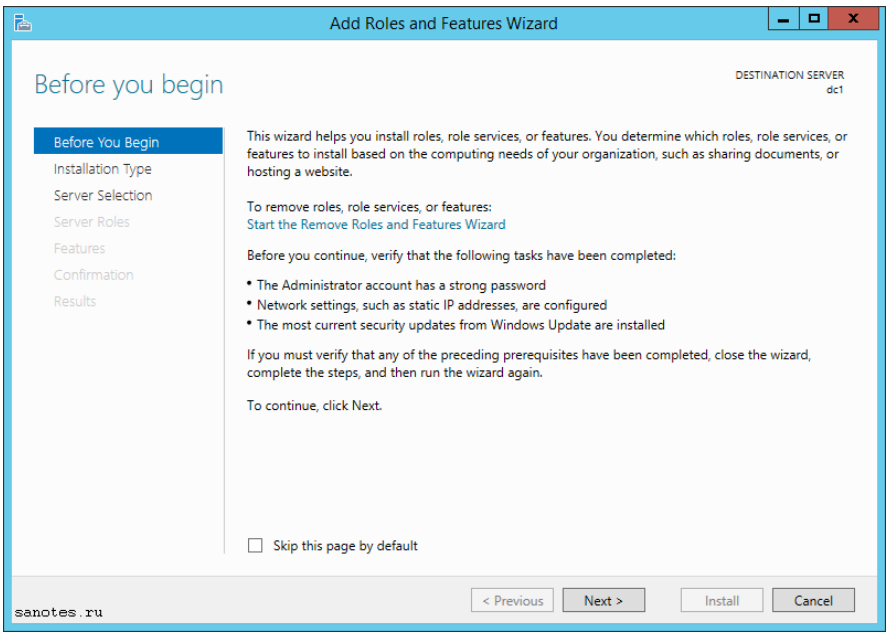
Нажимаем ОК, перезапускаем службу.

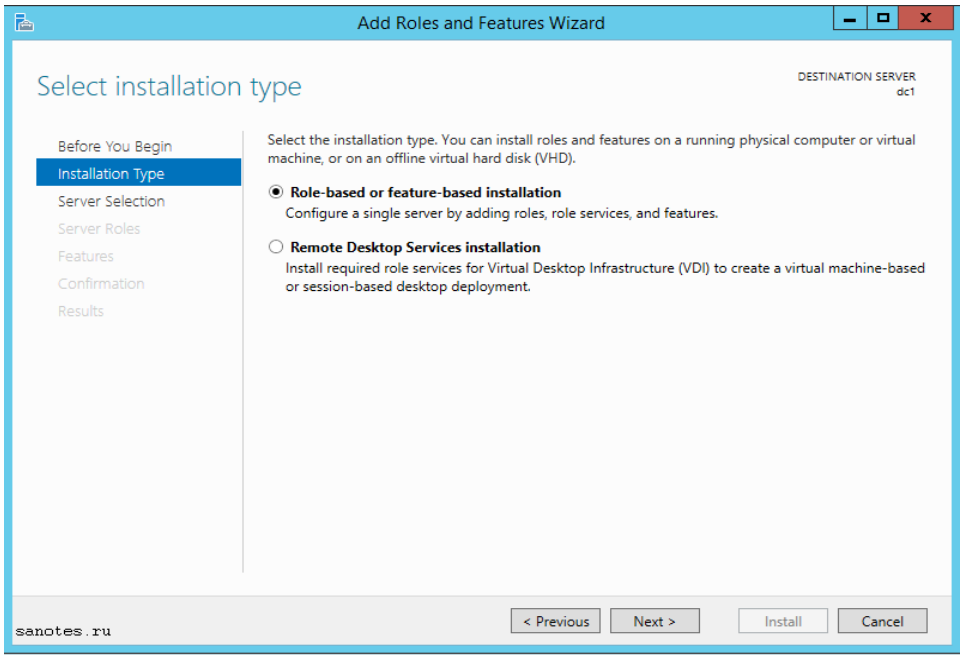


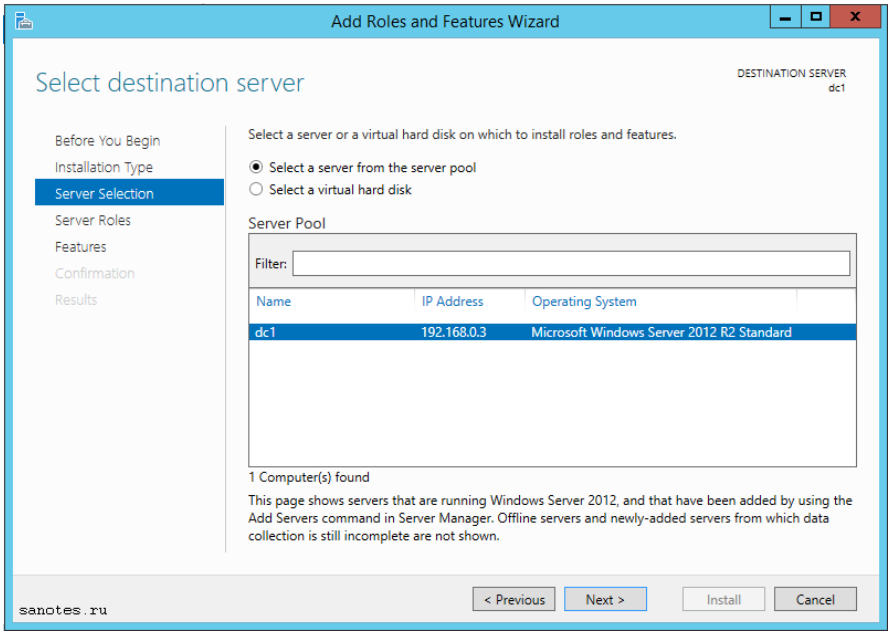
Позже мы еще вернемся к настройке DHCP, когда будем настраивать резервирование службы DHCP, но для этого нам надо поднять как минимум второй и последующий контроллеры домена.

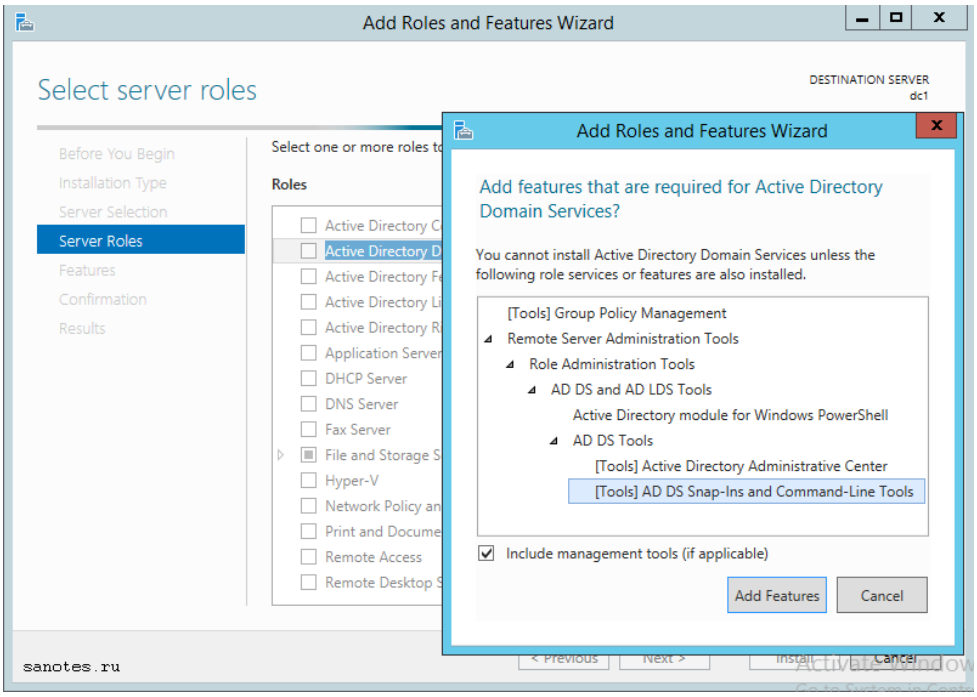
Эталон ответа:

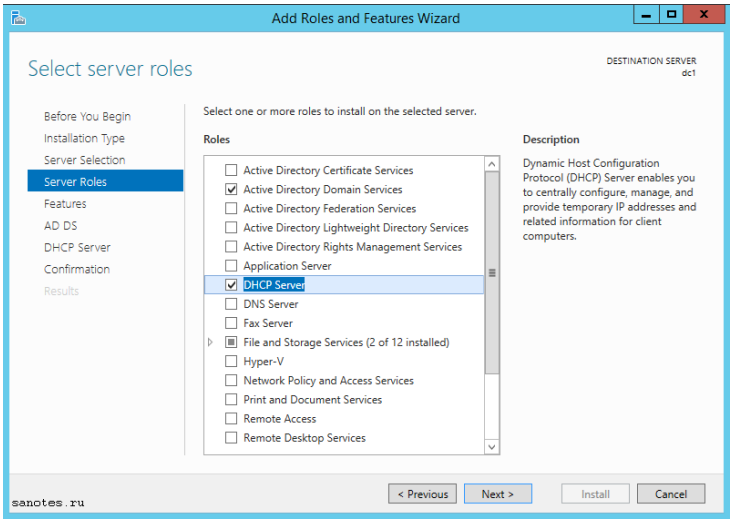


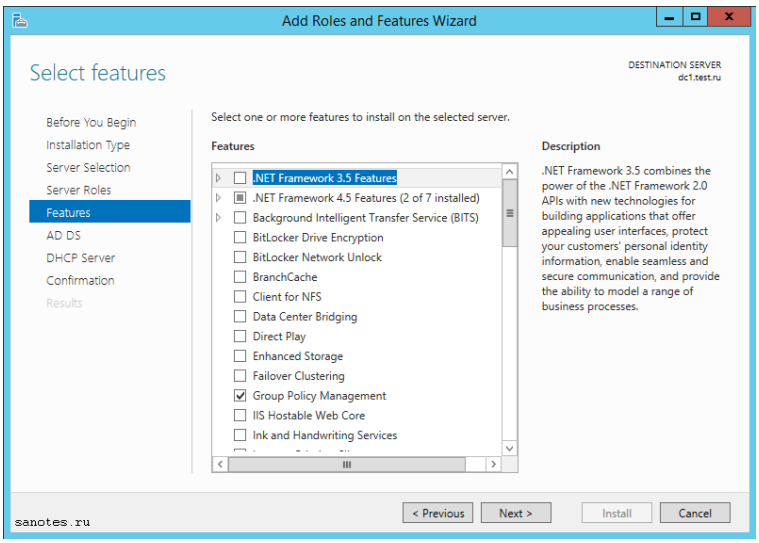

Add Roles and Features Wizard
Before you begin
DESTINATION SERVER
dc1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.
To remove roles, role services, or features:
Start the Remove Roles and Features Wizard
Before you continue, verify that the following tasks have been completed:
• The Administrator account has a strong password
• Network settings, such as static IP addresses, are configured
• The most current security updates from Windows Update are installed
If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.
To continue, click Next.
Skip this page by default
< Previous
Next >
Install
Cancel
sanotes.ru

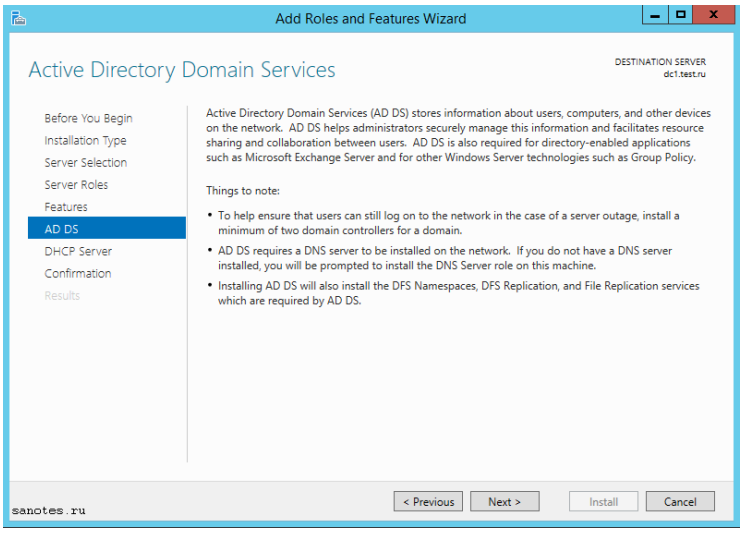

Add Roles and Features Wizard
Select installation type
DESTINATION SERVER
dc1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).
Role-based or feature-based installation
Configure a single server by adding roles, role services, and features.
Remote Desktop Services installation
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.
< Previous
Next >
Install
Cancel
sanotes.ru

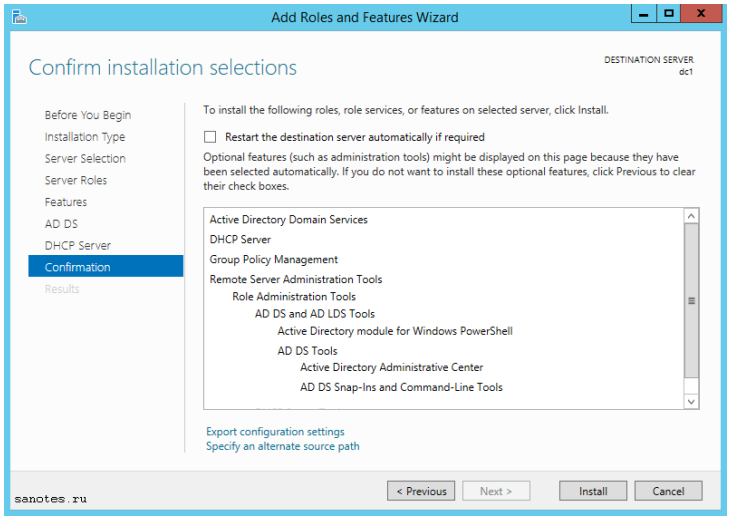

Add Roles and Features Wizard
Select destination server
DESTINATION SERVER
dc1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select a server or a virtual hard disk on which to install roles and features.
Select a server from the server pool
Select a virtual hard disk
Server Pool
Filter:
Name
IP Address
Operating System
dc1
192.168.0.3
Microsoft Windows Server 2012 R2 Standard
1 Computer(s) found
This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.
sanotes.ru
< Previous
Next >
Install
Cancel

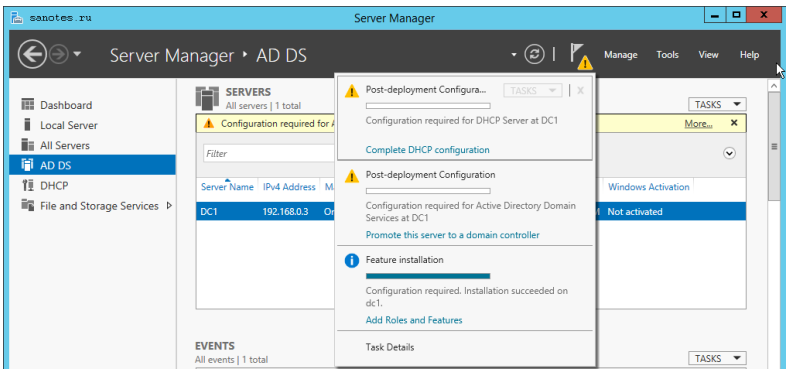

Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
dc1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Roles
Add Roles and Features Wizard
Add features that are required for Active Directory Domain Services?
You cannot install Active Directory Domain Services unless the following role services or features are also installed.
[Tools] Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
[Tools] Active Directory Administrative Center
[Tools] AD DS Snap-Ins and Command-Line Tools
Include management tools (if applicable)
Add Features
Cancel
sanotes.ru

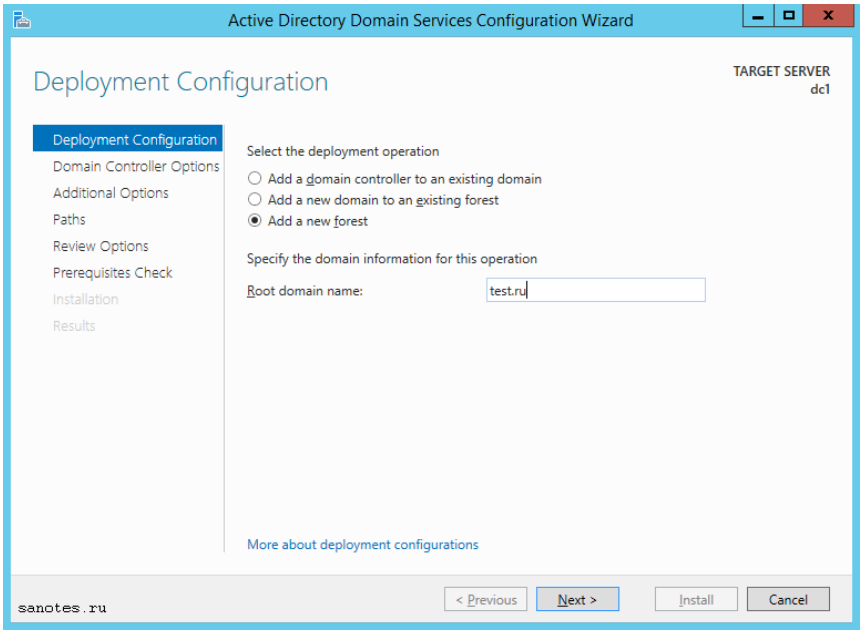

Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
dc1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
DHCP Server
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Description
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Application Server
DHCP Server
DNS Server
Fax Server
File and Storage Services (2 of 12 installed)
Hyper-V
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Dynamic Host Configuration Protocol (DHCP) Server enables you to centrally configure, manage, and provide temporary IP addresses and related information for client computers.
sanotes.ru
< Previous
Next >
Install
Cancel

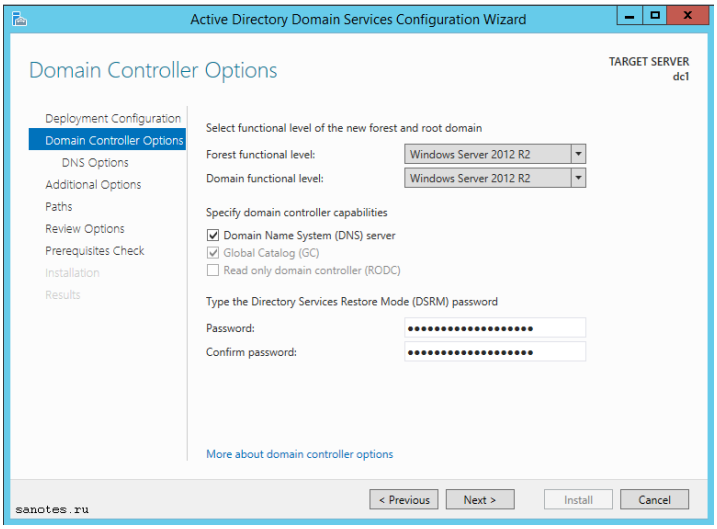

Add Roles and Features Wizard
Select features
DESTINATION SERVER
dc1.test.ru
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
DHCP Server
Confirmation
Results
Select one or more features to install on the selected server.
Features
.NET Framework 3.5 Features
.NET Framework 4.5 Features (2 of 7 installed)
Background Intelligent Transfer Service (BITS)
BitLocker Drive Encryption
BitLocker Network Unlock
BranchCache
Client for NFS
Data Center Bridging
Direct Play
Enhanced Storage
Failover Clustering
Group Policy Management
IIS Hostable Web Core
Ink and Handwriting Services
Description
.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
sanotes.ru
< Previous
Next >
Install
Cancel

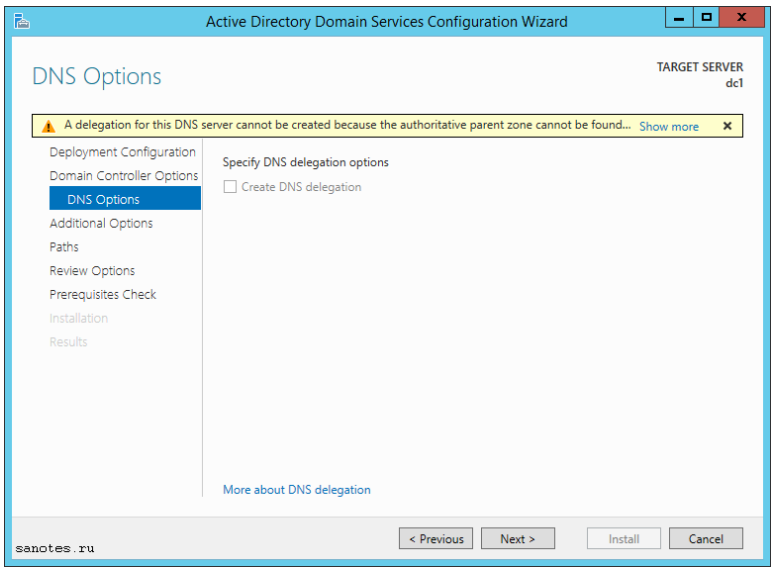

Add Roles and Features Wizard
Active Directory Domain Services
DESTINATION SERVER
dc1.test.ru
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
DHCP Server
Confirmation
Results
Active Directory Domain Services (AD DS) stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource sharing and collaboration between users. AD DS is also required for directory-enabled applications such as Microsoft Exchange Server and for other Windows Server technologies such as Group Policy.
Things to note:
To help ensure that users can still log on to the network in the case of a server outage, install a minimum of two domain controllers for a domain.
AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this machine.
Installing AD DS will also install the DFS Namespaces, DFS Replication, and File Replication services which are required by AD DS.
sanotes.ru
< Previous
Next >
Install
Cancel

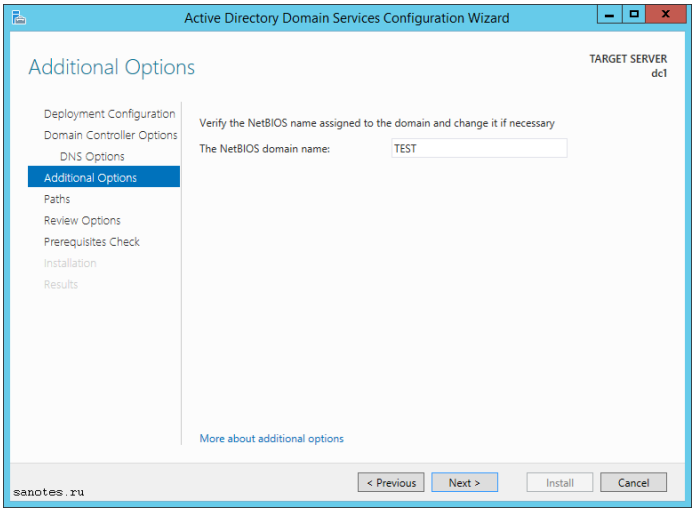

Add Roles and Features Wizard
Confirm installation selections
DESTINATION SERVER
dc1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
DHCP Server
Confirmation
Results
To install the following roles, role services, or features on selected server, click Install.
Restart the destination server automatically if required
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.
Active Directory Domain Services
DHCP Server
Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
Active Directory Administrative Center
AD DS Snap-Ins and Command-Line Tools
Export configuration settings
Specify an alternate source path
sanotes.ru
< Previous
Next >
Install
Cancel

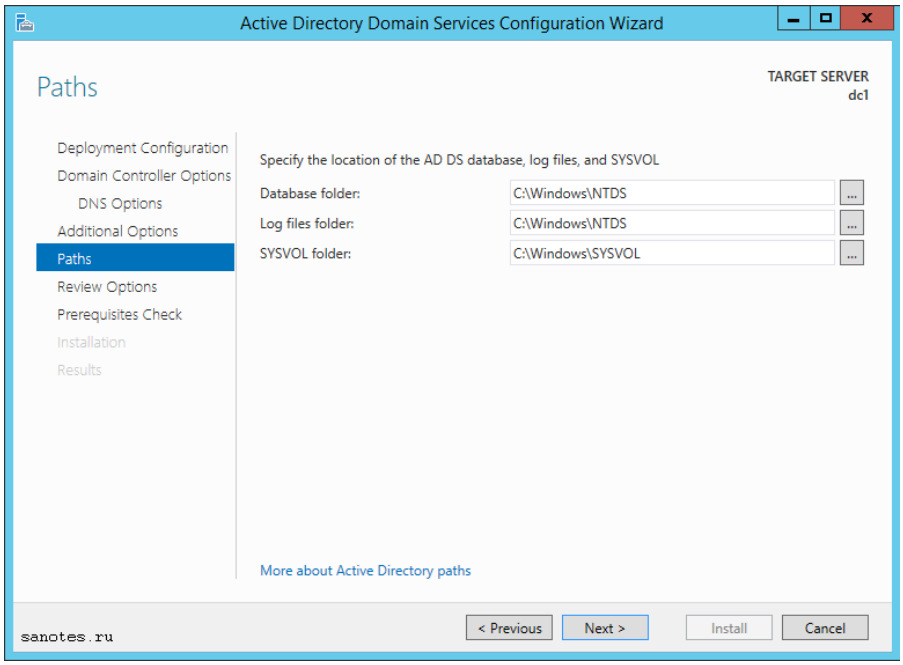

sanotes.ru
Server Manager
Server Manager ▸ AD DS
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DHCP
File and Storage Services
SERVERS
All servers | 1 total
Post-deployment Configura...
Configuration required for DHCP Server at DC1
Complete DHCP configuration
Post-deployment Configuration
Configuration required for Active Directory Domain Services at DC1
Promote this server to a domain controller
Feature installation
Configuration required. Installation succeeded on dc1.
Add Roles and Features
Task Details
Server Name
IPv4 Address
DC1
192.168.0.3
Windows Activation
Not activated
EVENTS
All events | 1 total
TASKS

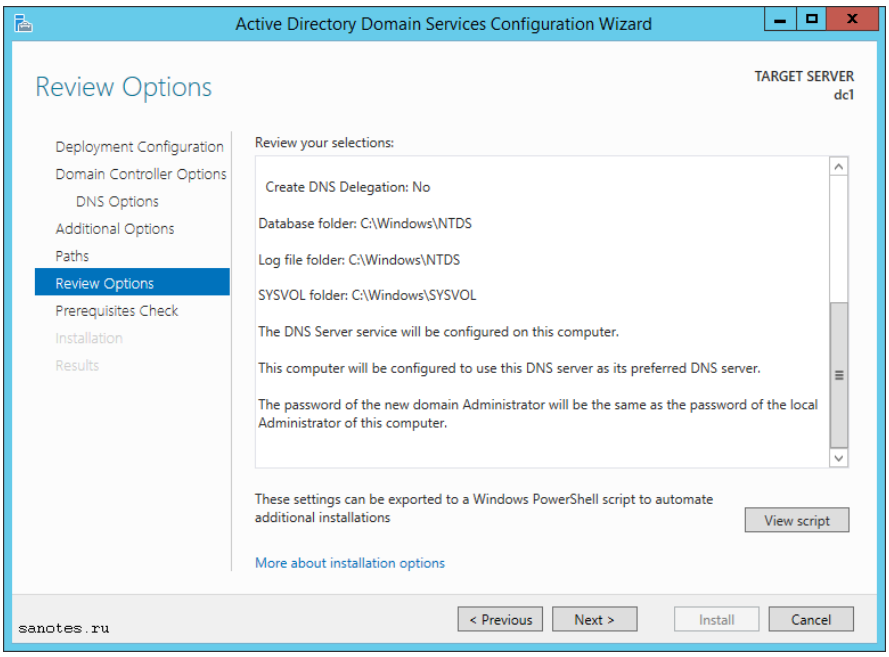

Active Directory Domain Services Configuration Wizard
Deployment Configuration
TARGET SERVER
dc1
Deployment Configuration
Domain Controller Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Select the deployment operation
Add a domain controller to an existing domain
Add a new domain to an existing forest
Add a new forest
Specify the domain information for this operation
Root domain name:
test.ru
More about deployment configurations
sanotes.ru
< Previous
Next >
Install
Cancel

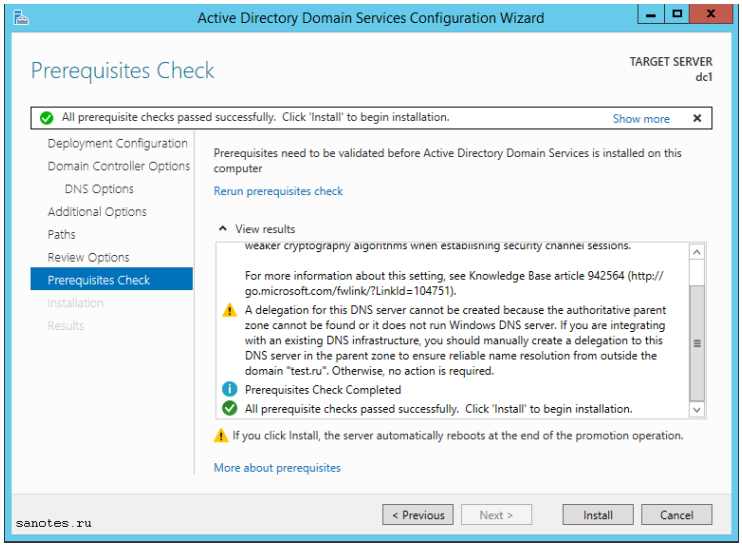

Active Directory Domain Services Configuration Wizard
Domain Controller Options
TARGET SERVER
dc1
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Select functional level of the new forest and root domain
Forest functional level:
Windows Server 2012 R2
Domain functional level:
Windows Server 2012 R2
Specify domain controller capabilities
Domain Name System (DNS) server
Global Catalog (GC)
Read only domain controller (RODC)
Type the Directory Services Restore Mode (DSRM) password
Password:
Confirm password:
More about domain controller options
sanotes.ru
< Previous
Next >
Install
Cancel

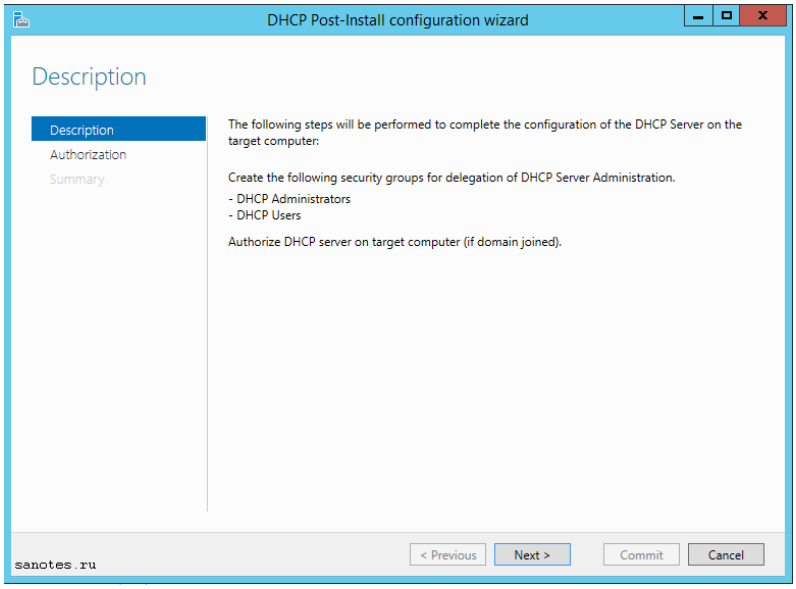

Active Directory Domain Services Configuration Wizard
DNS Options
TARGET SERVER
dc1
A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found...
Show more
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Specify DNS delegation options
Create DNS delegation
More about DNS delegation
sanotes.ru
< Previous
Next >
Install
Cancel

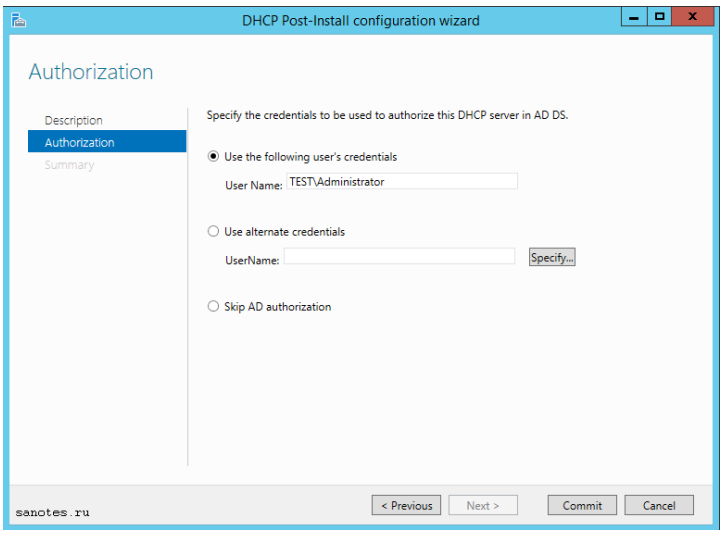

Active Directory Domain Services Configuration Wizard
Additional Options
TARGET SERVER
dc1
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Verify the NetBIOS name assigned to the domain and change it if necessary
The NetBIOS domain name:
TEST
More about additional options
sanotes.ru
< Previous
Next >
Install
Cancel

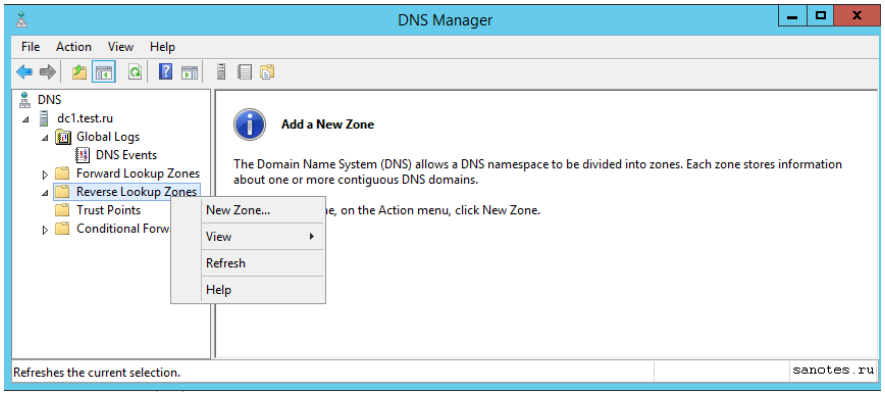

Active Directory Domain Services Configuration Wizard
Paths
TARGET SERVER
dc1
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Specify the location of the AD DS database, log files, and SYSVOL
Database folder:
C:\Windows\NTDS
Log files folder:
C:\Windows\NTDS
SYSVOL folder:
C:\Windows\SYSVOL
More about Active Directory paths
sanotes.ru
< Previous
Next >
Install
Cancel

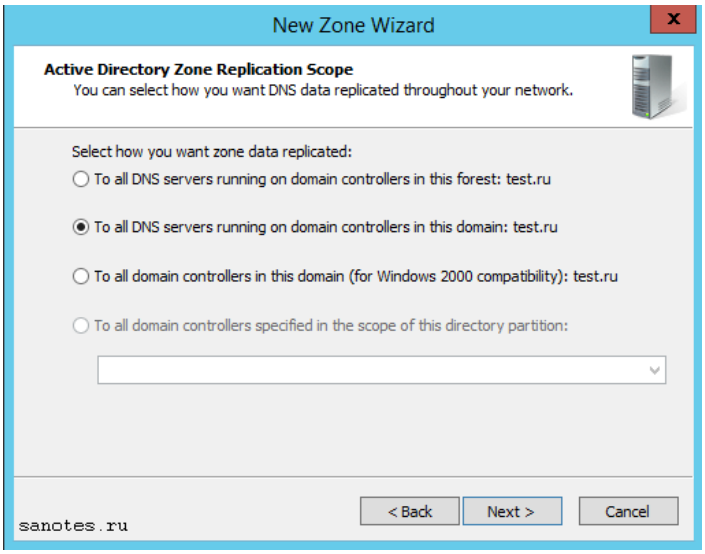

Active Directory Domain Services Configuration Wizard
Review Options
TARGET SERVER
dc1
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Review your selections:
Create DNS Delegation: No
Database folder: C:\Windows\NTDS
Log file folder: C:\Windows\NTDS
SYSVOL folder: C:\Windows\SYSVOL
The DNS Server service will be configured on this computer.
This computer will be configured to use this DNS server as its preferred DNS server.
The password of the new domain Administrator will be the same as the password of the local Administrator of this computer.
These settings can be exported to a Windows PowerShell script to automate additional installations
View script
More about installation options
sanotes.ru
< Previous
Next >
Install
Cancel

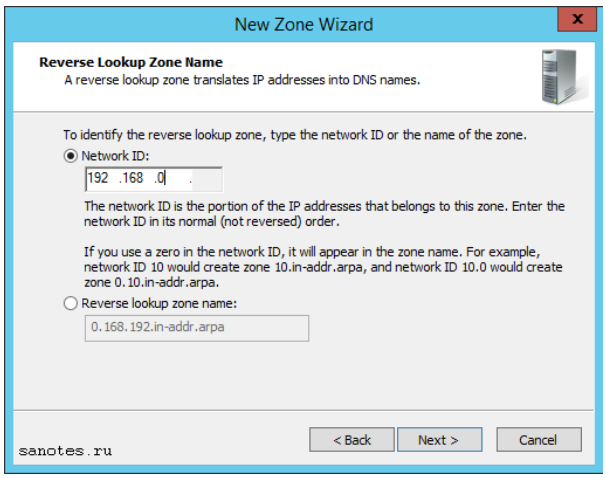

Active Directory Domain Services Configuration Wizard
Prerequisites Check
TARGET SERVER
dc1
All prerequisite checks passed successfully. Click 'Install' to begin installation.
Show more
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Prerequisites need to be validated before Active Directory Domain Services is installed on this computer
Rerun prerequisites check
View results
For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).
A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "test.ru". Otherwise, no action is required.
Prerequisites Check Completed
All prerequisite checks passed successfully. Click 'Install' to begin installation.
If you click Install, the server automatically reboots at the end of the promotion operation.
More about prerequisites
sanotes.ru
< Previous
Next >
Install
Cancel

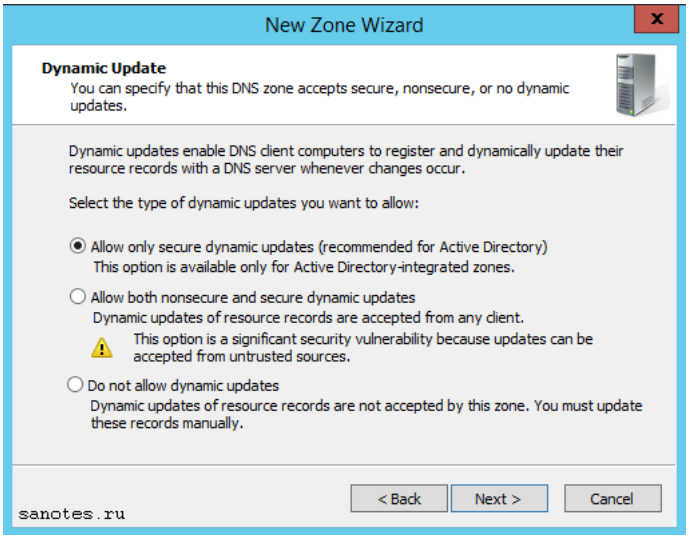

DHCP Post-Install configuration wizard
Description
Description
Authorization
Summary
The following steps will be performed to complete the configuration of the DHCP Server on the target computer:
Create the following security groups for delegation of DHCP Server Administration.
- DHCP Administrators
- DHCP Users
Authorize DHCP server on target computer (if domain joined).
sanotes.ru
< Previous
Next >
Commit
Cancel

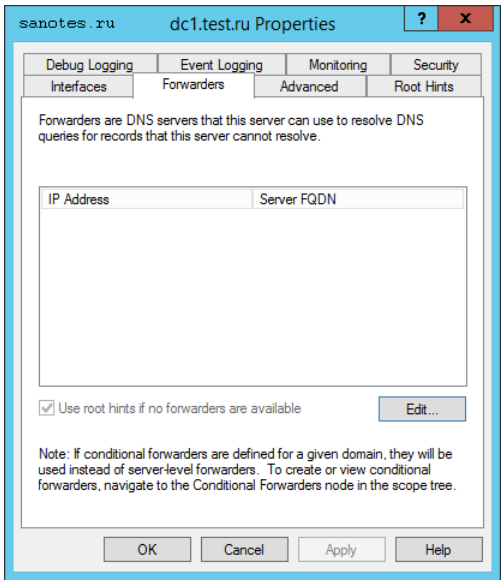

DHCP Post-Install configuration wizard
Authorization
Description
Authorization
Summary
Specify the credentials to be used to authorize this DHCP server in AD DS.
Use the following user's credentials
User Name: TEST\Administrator
Use alternate credentials
UserName:
Specify...
Skip AD authorization
sanotes.ru
< Previous
Next >
Commit
Cancel

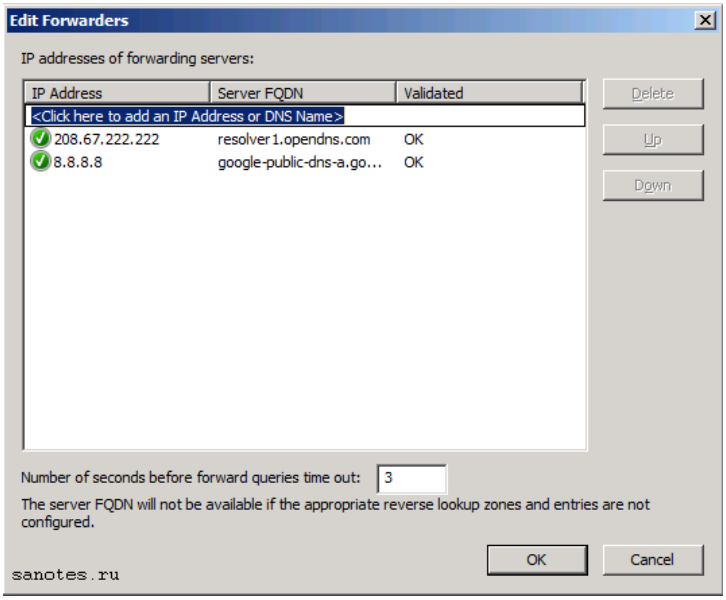

DNS Manager
File Action View Help
DNS
dc1.test.ru
Global Logs
DNS Events
Forward Lookup Zones
Reverse Lookup Zones
Trust Points
Conditional Forw
Add a New Zone
The Domain Name System (DNS) allows a DNS namespace to be divided into zones. Each zone stores information about one or more contiguous DNS domains.
e, on the Action menu, click New Zone.
New Zone...
View
Refresh
Help
Refreshes the current selection.
sanotes.ru

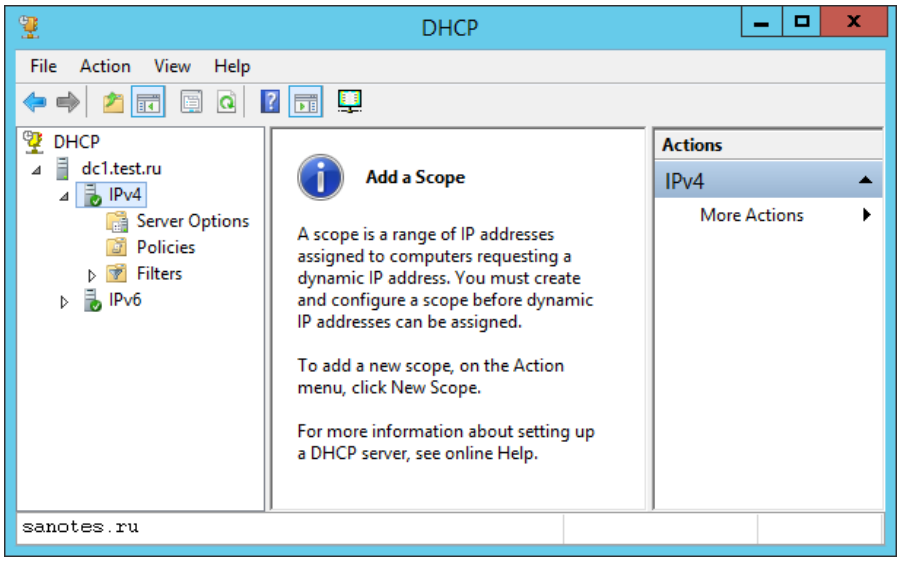

New Zone Wizard
Active Directory Zone Replication Scope
You can select how you want DNS data replicated throughout your network.
Select how you want zone data replicated:
To all DNS servers running on domain controllers in this forest: test.ru
To all DNS servers running on domain controllers in this domain: test.ru
To all domain controllers in this domain (for Windows 2000 compatibility): test.ru
To all domain controllers specified in the scope of this directory partition:
sanotes.ru
< Back
Next >
Cancel

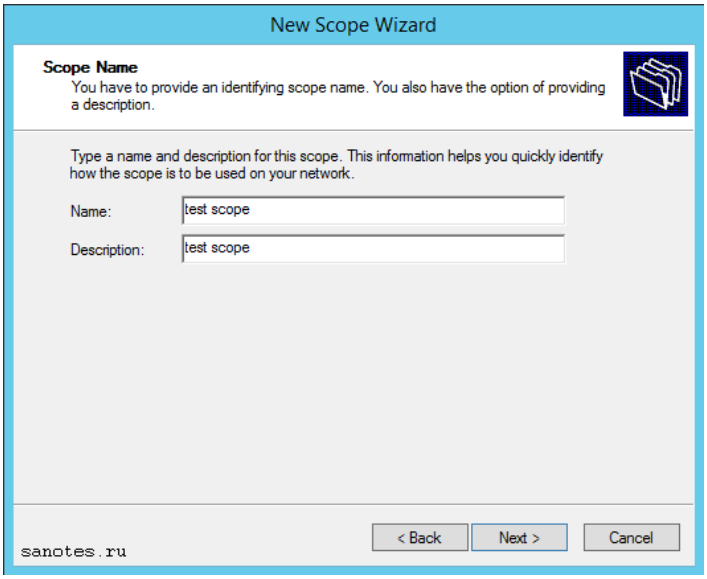

New Zone Wizard
Reverse Lookup Zone Name
A reverse lookup zone translates IP addresses into DNS names.
To identify the reverse lookup zone, type the network ID or the name of the zone.
Network ID:
192 .168 .0
The network ID is the portion of the IP addresses that belongs to this zone. Enter the network ID in its normal (not reversed) order.
If you use a zero in the network ID, it will appear in the zone name. For example, network ID 10 would create zone 10.in-addr.arpa, and network ID 10.0 would create zone 0.10.in-addr.arpa.
Reverse lookup zone name:
0.168.192.in-addr.arpa
sanotes.ru
< Back
Next >
Cancel

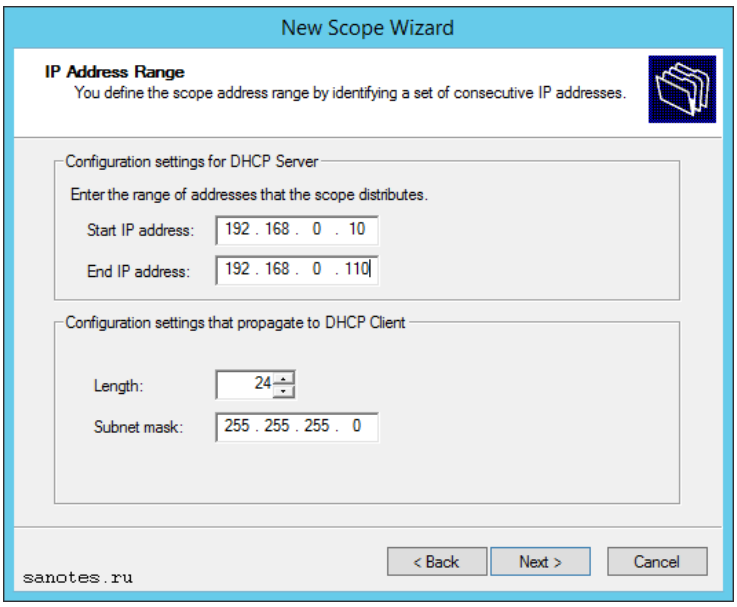

New Zone Wizard
Dynamic Update
You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.
Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.
Select the type of dynamic updates you want to allow:
Allow only secure dynamic updates (recommended for Active Directory)
This option is available only for Active Directory-integrated zones.
Allow both nonsecure and secure dynamic updates
Dynamic updates of resource records are accepted from any client.
This option is a significant security vulnerability because updates can be accepted from untrusted sources.
Do not allow dynamic updates
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.
sanotes.ru
< Back
Next >
Cancel

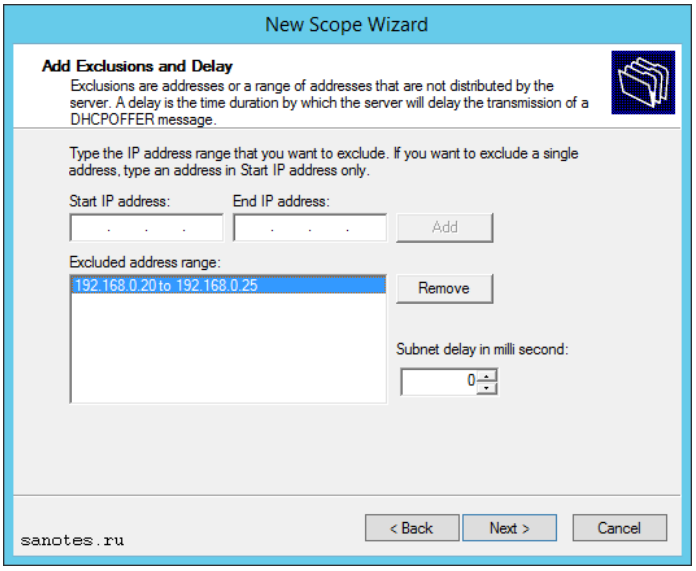

sanotes.ru
dc1.test.ru Properties
Debug Logging
Event Logging
Monitoring
Security
Interfaces
Forwarders
Advanced
Root Hints
Forwarders are DNS servers that this server can use to resolve DNS queries for records that this server cannot resolve.
IP Address
Server FQDN
Use root hints if no forwarders are available
Edit...
Note: If conditional forwarders are defined for a given domain, they will be used instead of server-level forwarders. To create or view conditional forwarders, navigate to the Conditional Forwarders node in the scope tree.
OK
Cancel
Apply
Help

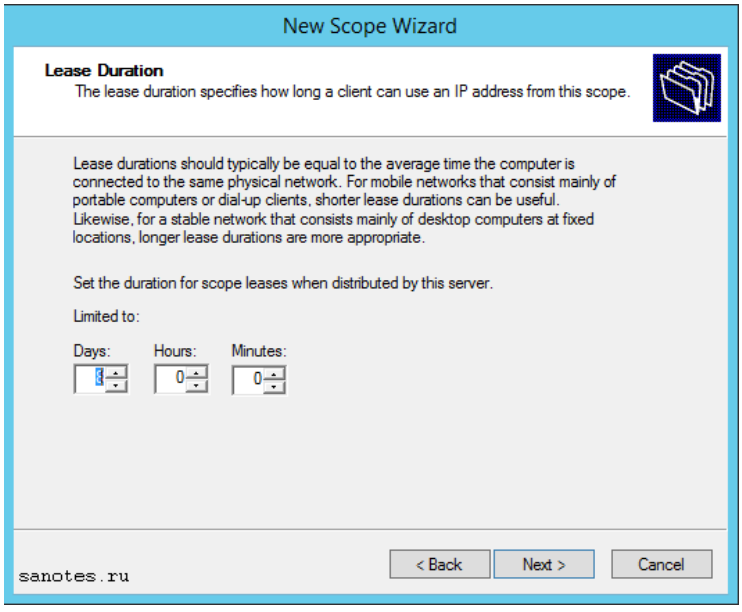

Edit Forwarders
IP addresses of forwarding servers:
IP Address
Server FQDN
Validated
<Click here to add an IP Address or DNS Name>
208.67.222.222
resolver1.opendns.com
OK
8.8.8.8
google-public-dns-a.go...
OK
Delete
Up
Down
Number of seconds before forward queries time out:
3
The server FQDN will not be available if the appropriate reverse lookup zones and entries are not configured.
OK
Cancel
sanotes.ru

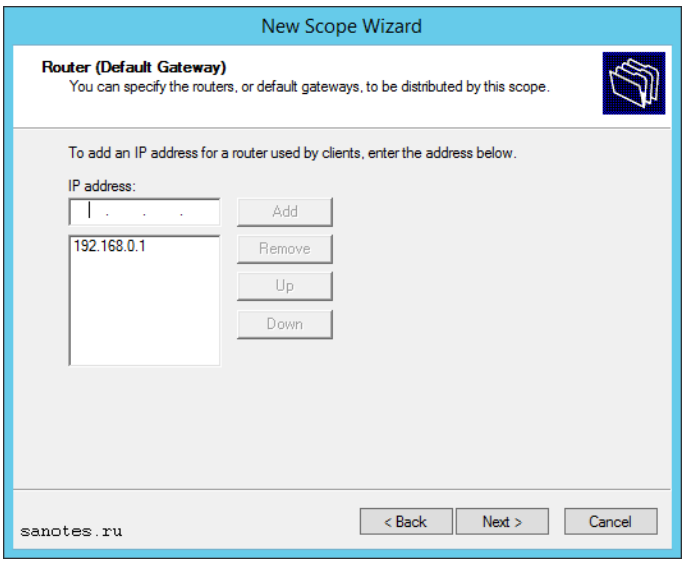

DHCP
File
Action
View
Help
DHCP
dc1.test.ru
IPv4
Server Options
Policies
Filters
IPv6
Add a Scope
A scope is a range of IP addresses assigned to computers requesting a dynamic IP address. You must create and configure a scope before dynamic IP addresses can be assigned.
To add a new scope, on the Action menu, click New Scope.
For more information about setting up a DHCP server, see online Help.
Actions
IPv4
More Actions
sanotes.ru

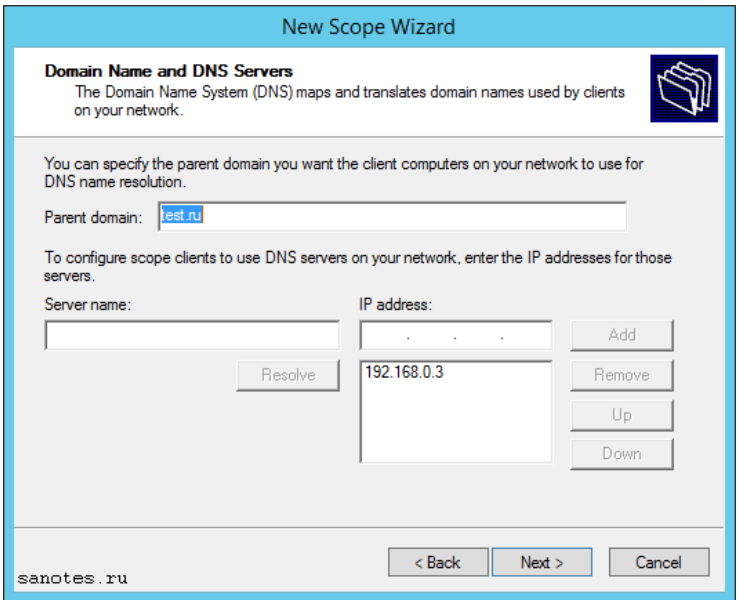

New Scope Wizard
Scope Name
You have to provide an identifying scope name. You also have the option of providing a description.
Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.
Name:
test scope
Description:
test scope
< Back
Next >
Cancel
sanotes.ru

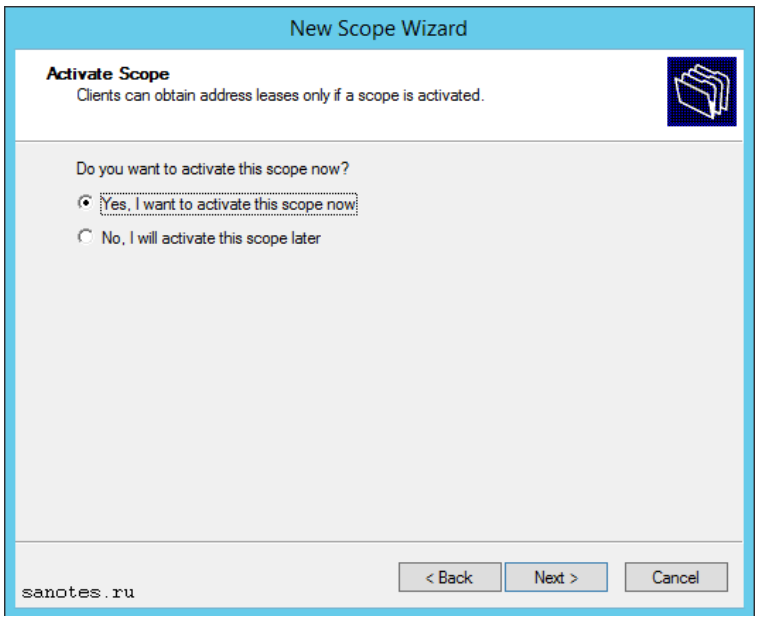

New Scope Wizard
IP Address Range
You define the scope address range by identifying a set of consecutive IP addresses.
Configuration settings for DHCP Server
Enter the range of addresses that the scope distributes.
Start IP address: 192 . 168 . 0 . 10
End IP address: 192 . 168 . 0 . 110
Configuration settings that propagate to DHCP Client
Length: 24
Subnet mask: 255 . 255 . 255 . 0
sanotes.ru
< Back
Next >
Cancel

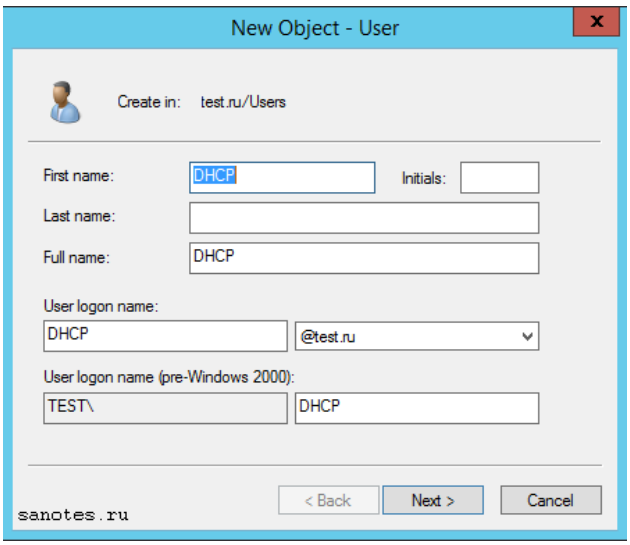

New Scope Wizard
Add Exclusions and Delay
Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCPOFFER message.
Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.
Start IP address:
End IP address:
Add
Excluded address range:
192.168.0.20 to 192.168.0.25
Remove
Subnet delay in milli second:
0
sanotes.ru
< Back
Next >
Cancel

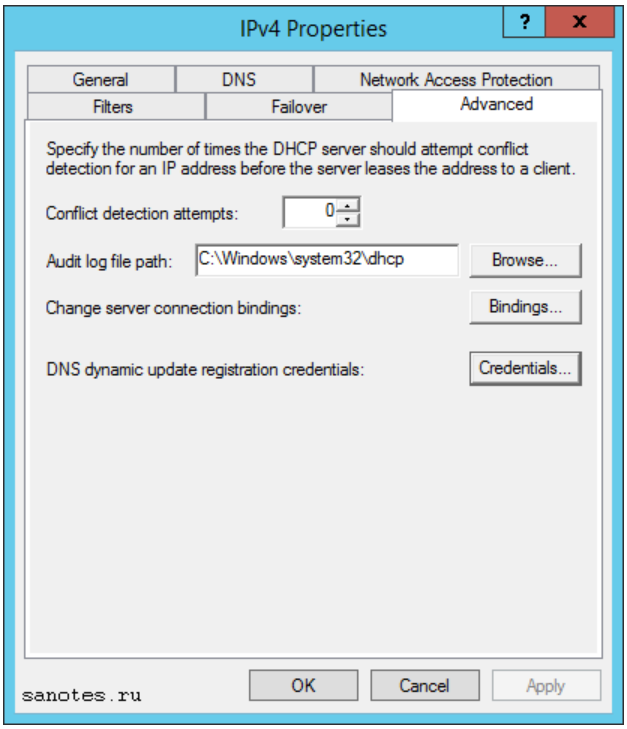

New Scope Wizard
Lease Duration
The lease duration specifies how long a client can use an IP address from this scope.
Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.
Set the duration for scope leases when distributed by this server.
Limited to:
Days:
Hours:
Minutes:
0
0
sanotes.ru
< Back
Next >
Cancel

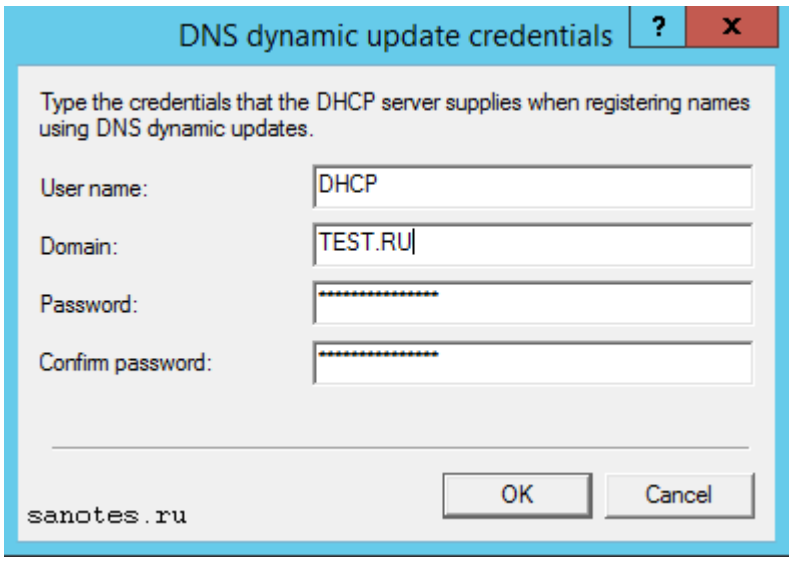

New Scope Wizard
Router (Default Gateway)
You can specify the routers, or default gateways, to be distributed by this scope.
To add an IP address for a router used by clients, enter the address below.
IP address:
Add
192.168.0.1
Remove
Up
Down
sanotes.ru
< Back
Next >
Cancel

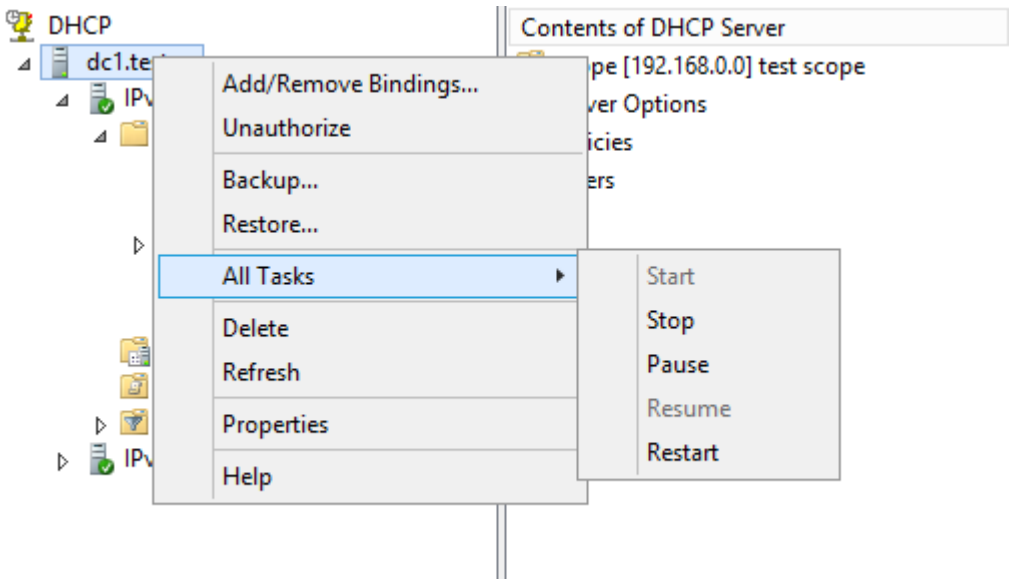

New Scope Wizard
Domain Name and DNS Servers
The Domain Name System (DNS) maps and translates domain names used by clients on your network.
You can specify the parent domain you want the client computers on your network to use for DNS name resolution.
Parent domain:
test.ru
To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.
Server name:
IP address:
Add
Resolve
192.168.0.3
Remove
Up
Down
sanotes.ru
< Back
Next >
Cancel


New Scope Wizard
Activate Scope
Clients can obtain address leases only if a scope is activated.
Do you want to activate this scope now?
Yes, I want to activate this scope now
No, I will activate this scope later
sanotes.ru
< Back
Next >
Cancel


New Object - User
Create in: test.ru/Users
First name: DHCP
Initials:
Last name:
Full name: DHCP
User logon name:
DHCP
@test.ru
User logon name (pre-Windows 2000):
TEST\
DHCP
< Back
Next >
Cancel
sanotes.ru


IPv4 Properties
General
DNS
Network Access Protection
Filters
Failover
Advanced
Specify the number of times the DHCP server should attempt conflict detection for an IP address before the server leases the address to a client.
Conflict detection attempts:
0
Audit log file path:
C:\Windows\system32\dhcp
Browse...
Change server connection bindings:
Bindings...
DNS dynamic update registration credentials:
Credentials...
OK
Cancel
Apply
sanotes.ru


DNS dynamic update credentials
Type the credentials that the DHCP server supplies when registering names using DNS dynamic updates.
User name:
DHCP
Domain:
TEST.RU
Password:
Confirm password:
OK
Cancel
sanotes.ru



Устный зачет по теме 2.1.

Инструкция для обучающихся

Зачет сдается в рамках учебного занятия. Каждый студент отвечает в устной форме на предложенные преподавателем 5 случайных вопроса.

Выполнение задания: одному студенту на ответ выделяется 3 мин., группа сдает зачет за одно учебное занятие.

Перечень вопросов:

1. Настройка H.323. Описание H.323 и общие рекомендации.
2. Функциональные компоненты H.323.Установка и поддержка соединения H.323. Соединения без и с использованием GateKeeper. Соединения с использованием нескольких GateKeeper.
3. Многопользовательские конференции. Обеспечение отказоустойчивости.
4. Настройка SIP. Описание и общие рекомендации. Технология SIP и связанные с ней стандарты.
5. Функциональные компоненты SIP. Сообщения SIP. Адресация SIP.
6. Модель установления соединения. Планирование отказоустойчивости.
7. Установка и инсталляция программного коммутатора. Монтажные процедуры.
8. Процедуры инсталляции. Управление аппаратными средствами и портами. Протоколы управления MGCP, H.248.
9. Управление программным коммутатором. Маршрутизация. Группы соединительных линий. Подключение станций с TDM (абонентский доступ TDM).
10. Сигнализация SIP, SIP-T, H.323 и SIGTRAN. IP -абоненты. Группы абонентов. Дополнительные абонентские услуги.
11. Организация эксплуатации систем IP-телефонии
12. Техническое обслуживание, плановый текущий ремонт, плановый капитальный ремонт, внеплановый ремонт
13. Восстановление работы сети после аварии
14. Схемы послеаварийного восстановления работоспособности сети, техническая и проектная документация, способы резервного копирования данных, принципы работы хранилищ данных

Эталоны ответов: приведены в учебном пособии по МДК.03.01 «Эксплуатация объектов сетевой инфраструктуры»

Практическая работа № 37 Эксплуатация систем IP-телефонии

Ознакомление с протоколом SIP, его роль при передаче голосых сигналов.

7.2 Рабочее задание

7.2.1 Соберите схему с использованием шлюзов VRX-1010-E1, коммутатора второго уровня D-Link DES-1024, ПК с прикладным процессом
3CX Phone.
7.2.2 Присвоить ПК IP-адрес и маску подсети.
7.2.3 Осуществите подключение сетевого шнура на консольный порт шлюза VRX-1010-E1 через SSH-клиент.
7.2.4 Ознакомиться с выполнением различных процедур и команд.
7.2.5 Подключить мультимедийные приставки в ПК.
7.2.6 На ПК запустите программу 3CX Phone и осуществите ее настройку для подключения к шлюзу.
7.2.6 Осуществите тестовые звонки между ПК с помощью сигнального протокола по соединительной линии связи на основе интерфейса PRI.
7.2.7 Составьте отчет о результатах выполнения работы.

7.3 Методические указания по выполнению работы

7.3.1 Соберите схему согласно рисунку 7.1.
7.3.2 Проведите настройки согласно лабораторной работе 5 для каждого шлюза VRX-1010-E1.
7.3.3 Добавьте в файл /etc/asterisk/sip.conf следующие строки:
[<X>] type=peer dtmfmode=rfc2833 host=<remoteIP> secret=<pass> context=office Здесь <X> - имя удаленного шлюза в соответствии с вариантом,
<remoteIP> - IP-адрес удаленного шлюза, <pass> - общий с удаленным шлюзом пароль.

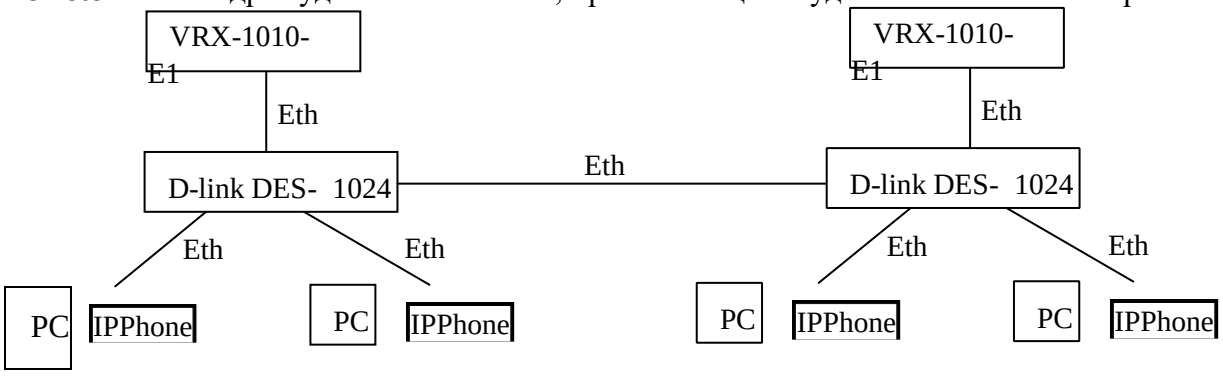


Рисунок 7.1 – Схема сети

7.3.4 Добавьте в файл /etc/asterisk/extensions.conf следующие строки
exten => _0X.,1,Dial(SIP/<X>/{EXTEN:1}) same => n,HangUp()

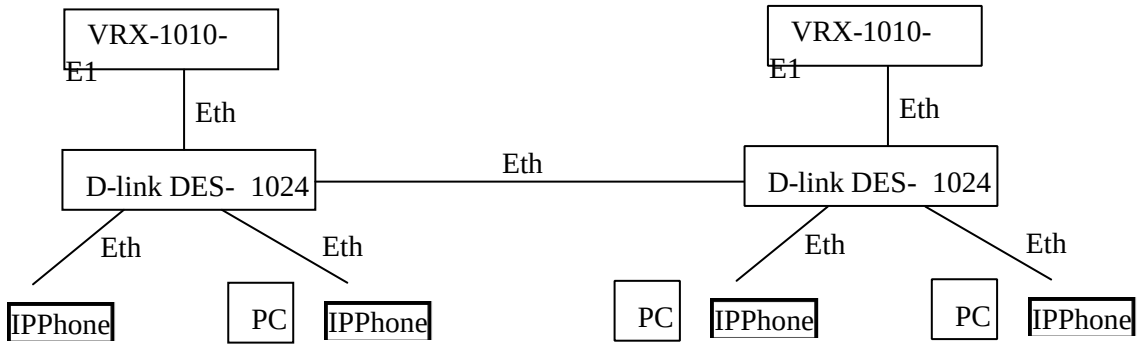
Здесь <X> - имя удаленного шлюза в соответствии с вариантом.
7.3.5 В консоли введите следующую команду service asterisk restart

7.3.6 Выполните тестовые вызовы между ПК на разных шлюзах через префикс 0 (таблица 6.1).
7.3.7 Составьте отчет о результатах выполнения работы.

Таблица 7.1 – Исходные данные

№	SIP-адреса	№	SIP-адреса	№	SIP-адреса
1	1000 GW1	8	1007 GW2	15	1014 GW1
2	1001 GW2	9	1008 GW1	16	1015 GW2
3	1002 GW1	10	1009 GW2	17	1016 GW1
4	1003 GW2	11	1010 GW1	18	1017 GW2
5	1004 GW1	12	1011 GW2	19	1018 GW1
6	1005 GW2	13	1012 GW1	20	1019 GW2
7	1006 GW1	14	1013 GW2		

Эталон ответа



Практическая работа № 39 Замена расходных материалов и мелкий ремонт периферийного оборудования

Инструкция для обучающихся

Внимательно прочитайте задание. Проведите замену расходных материалов.

Время выполнения – 90 минут.

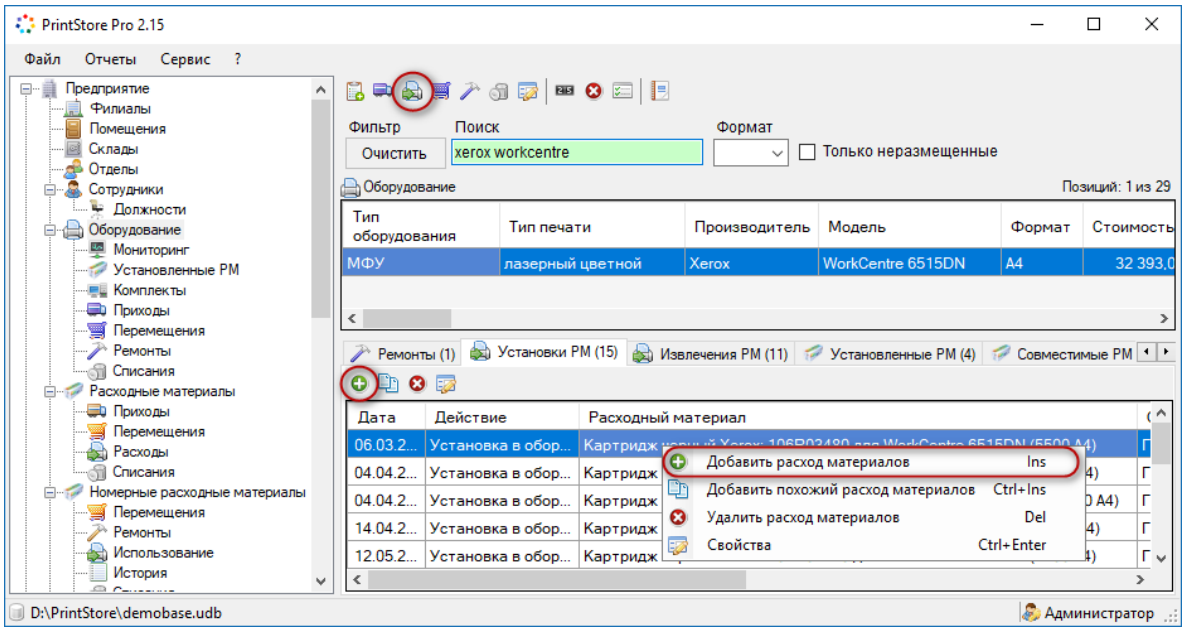
Задание

Ознакомиться с специализированным ПО по учету и контролю расходных материалов.

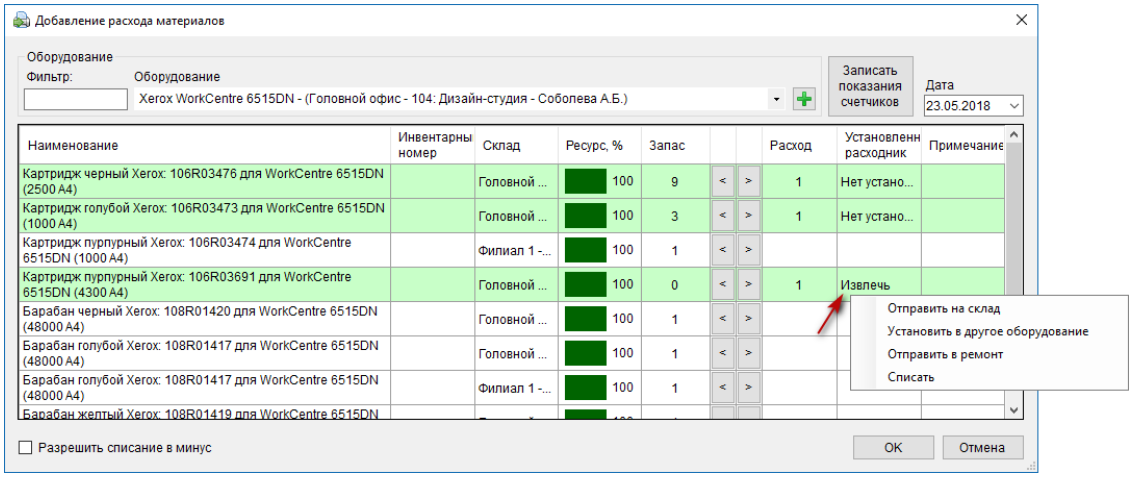
Установка расходных материалов в оборудование

В PrintStore необходимо фиксировать все действия по замене расходных материалов в оборудовании. Важно, чтобы данные об установленных в печатных устройствах расходниках соответствовали действительности. В этом случае программа сможет отображать актуальную информацию о материалах, используемых в оборудовании на текущий момент, и корректно рассчитывать остаток ресурса в них, например, запас чернил (тонера) в каждом картридже.

Запись об установке расходного материала в оборудование можно добавить в нескольких разделах программы: «Оборудование», «Расходные материалы», «Номерные расходные материалы», а также на соответствующих закладках. Удобнее всего оформлять установку расходника в конкретное устройство через раздел «Оборудование» и на закладке «Установки РМ» данного раздела. Для этого следует выделить в таблице нужное устройство (принтер, МФУ и т.п.) и выбрать кнопку / команду «Добавить расход материалов».



Установка в оборудование учитывается, как расход, использование материала. Соответствующий диалог показан на изображении ниже.



Программа автоматически учитывает совместимость расходных материалов с моделью и слотами выбранного устройства и предлагает для установки перечень подходящих ему картриджей и других расходников из имеющихся в наличии. В столбце «Запас» представлена информация об остатках РМ на складах на выбранную дату.

Номерные расходные материалы (НРМ) указаны отдельно в конце списка, у них присутствуют серийные / инвентарные номера. По каждому НРМ отображается текущий остаток ресурса (краски, тонера и т.п.) на выбранную дату. У обычных материалов (не номерных) остаток ресурса всегда равен 100%, т.к. предполагается, что со склада в оборудование всегда устанавливают новые картриджи, а возможность возвращать на склад частично использованные материалы доступна только для НРМ.

Для того чтобы установить расходник в оборудование, необходимо нажать кнопку > напротив соответствующего материала. При установке картриджа в пустой слот в столбце «Установленный расходник» появится подсказка об отсутствии в данном слоте предыдущего РМ — «Нет установленных расходников». В случае замены картриджей **старый расходник должен быть обязательно извлечен из оборудования** следующим образом: в столбце «Установленный расходник» появится кнопка «Извлечь» (отмечена стрелкой на изображении выше), нажав на которую следует выбрать требуемое действие с извлекаемым РМ. Как правило, это списание. Номерной материал также может быть отправлен на склад, установлен в другое устройство или отправлен на перезаправку (в ремонт).

Кнопка «Записать показания счетчиков» позволяет внести в программу текущие значения счетчиков печати у оборудования при замене расходных материалов, например, количество отпечатанных страниц.

По умолчанию установка расходных материалов оформляется на текущую дату. В случае изменения даты соответствующим образом изменятся и значения в столбце «Расход». В нем будет показан расход материалов за выбранный день. При необходимости расход может быть отредактирован «задним числом». Опция «Разрешить списание в минус» позволяет добавлять записи расхода «задним числом» независимо от текущего остатка на складах. Однако следует помнить, что при подобном ведении учета возможны ошибки. Вовремя их обнаружить и исправить помогает процедура верификации.

Обратите внимание, что в программе существует ограничение на одно однотипное действие в день. Т.е. установить картридж в один и тот же слот принтера можно только 1 раз за сутки.

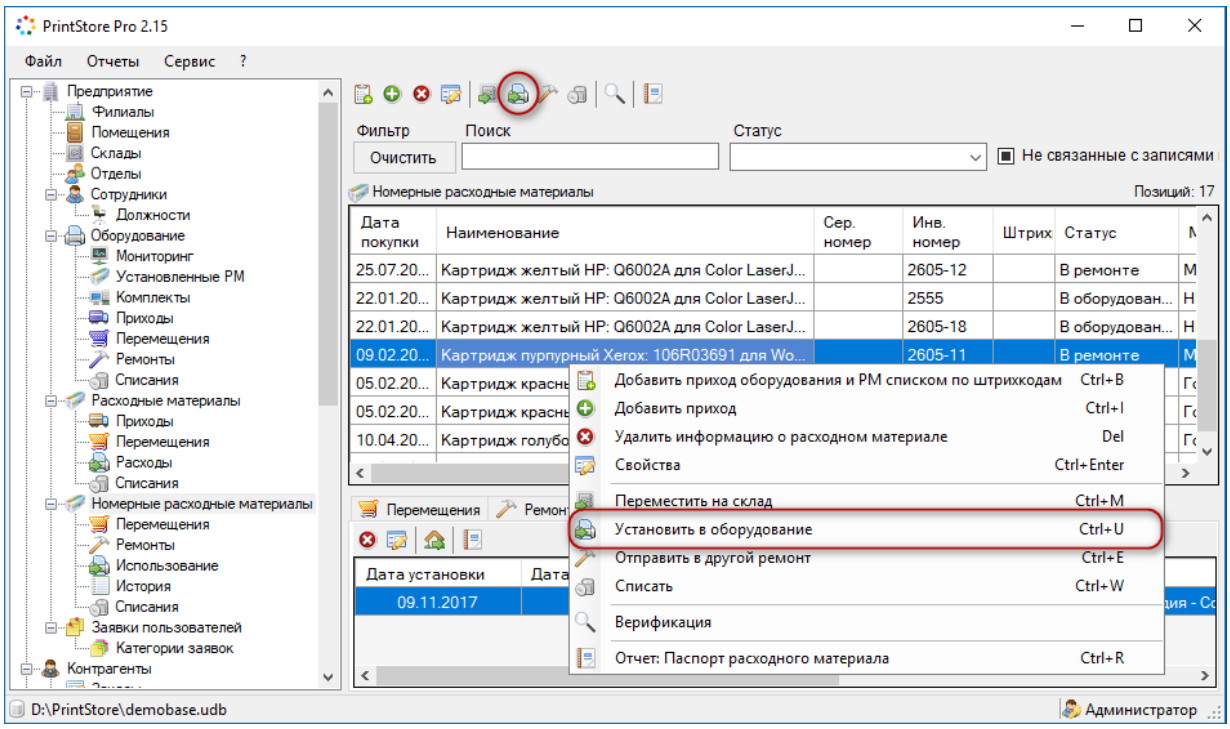
Автоматическое определение замены расходных материалов

Программа может автоматически обнаружить замену расходного материала у оборудования, находящегося в мониторинге, при изменении ресурса установленного РМ в бОльшую сторону. Например, остаток тонера в картридже был 0%, а стал 100%. Для этого должны быть соблюдены несколько условий, которые подробно описаны здесь.

При обнаружении замены РМ в подраздел «Расходные материалы — Расходы» автоматически будет добавлена соответствующая запись о расходе РМ со склада, сопоставленного с данным оборудованием. Сопоставление можно настроить по филиалам, отделам, помещениям и т.д. Например, чтобы при замене РМ в принтерах из бухгалтерии, расход этих РМ автоматически оформлялся с основного склада. Настройка сопоставлений производится в диалоге свойств склада на закладке «Автоматическое списание РМ» (раздел «Склады»).

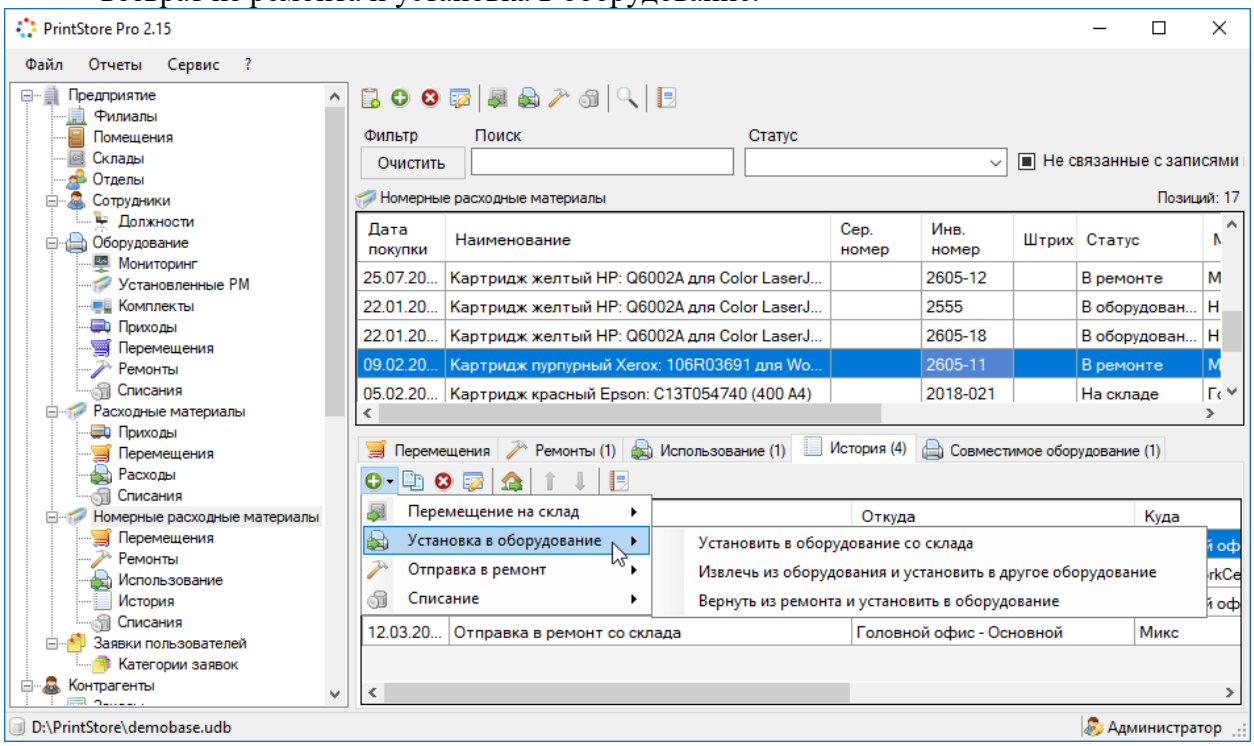
Установка в оборудование номерных материалов

Рассмотренный выше способ установки материалов в оборудование применим как к обычным, так и к номерным расходникам (они представлены в одном диалоге). Однако НРМ может быть установлен в печатное устройство не только со склада, но и после извлечения из другого оборудования или возврата из сервиса. Оформить запись о расходе НРМ можно в разделе «Номерные расходные материалы» с помощью кнопки / команды  «Установить в оборудование» (Ctrl+U).



Создать запись о расходе номерного материала также возможно на закладке «История» данного раздела с помощью кнопки / команды «Добавить действие...». Возможные варианты:

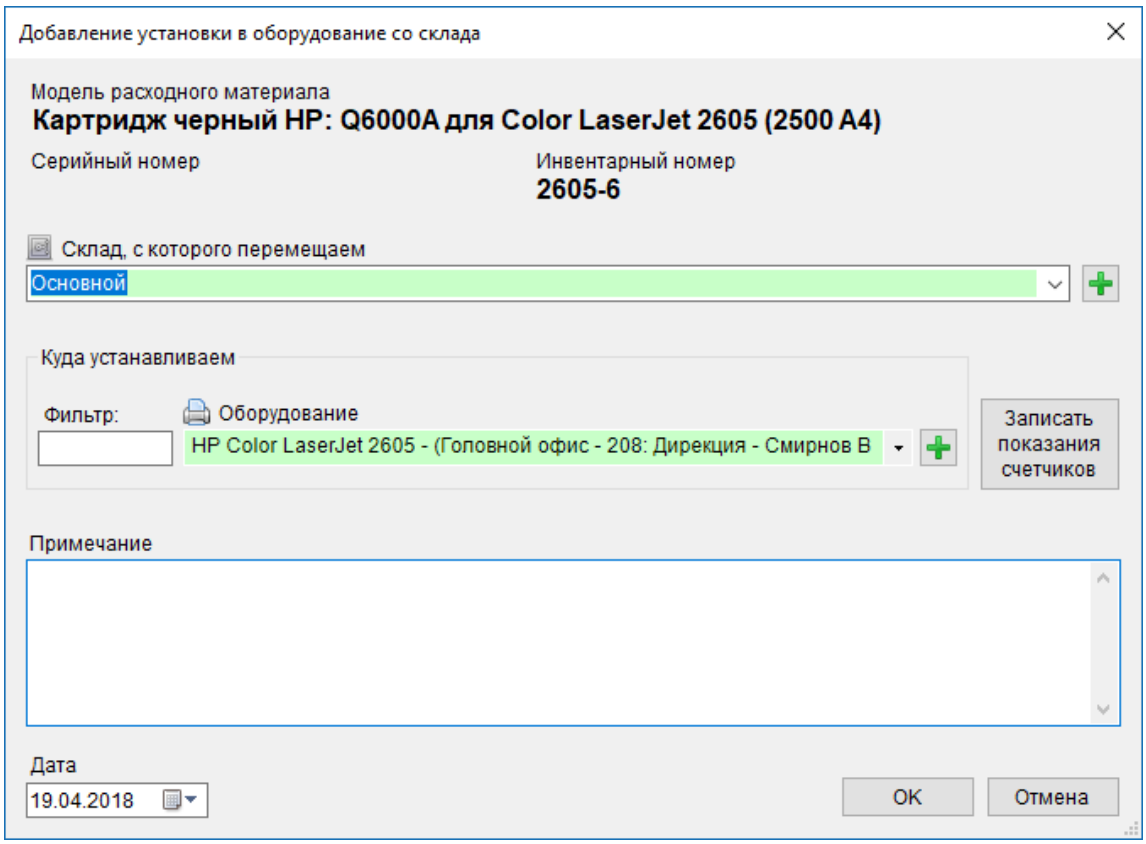
- установка в оборудование со склада;
- извлечение из одного оборудования и установка в другое;
- возврат из ремонта и установка в оборудование.



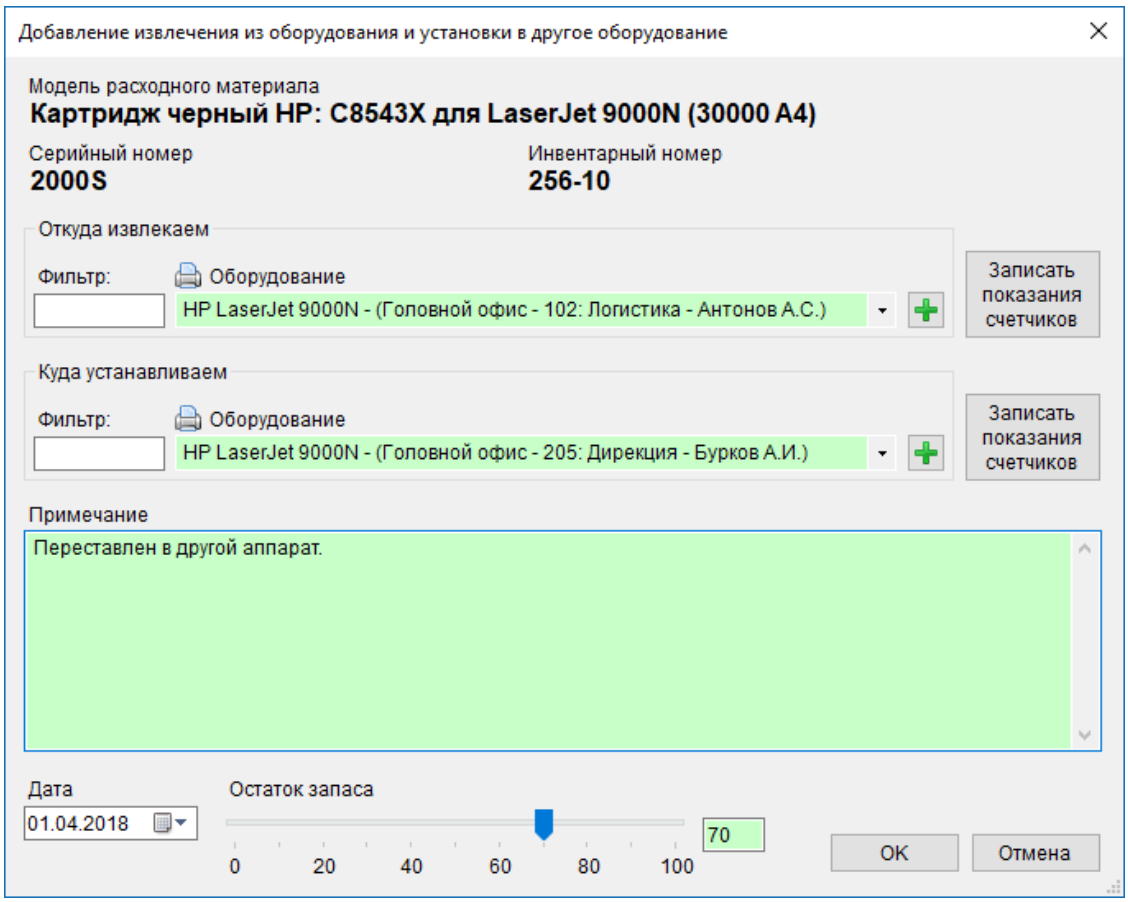
В каждом случае откроется соответствующий диалог, в котором следует выбрать совместимое оборудование для установки расходного материала. По умолчанию установка оформляется текущей датой, которую при необходимости можно изменить. Кнопка «Записать показания счетчиков» в каждом диалоге позволяет внести показания счетчиков пе-

чати у оборудования на момент замены расходника, например, текущее количество отпечатанных страниц.

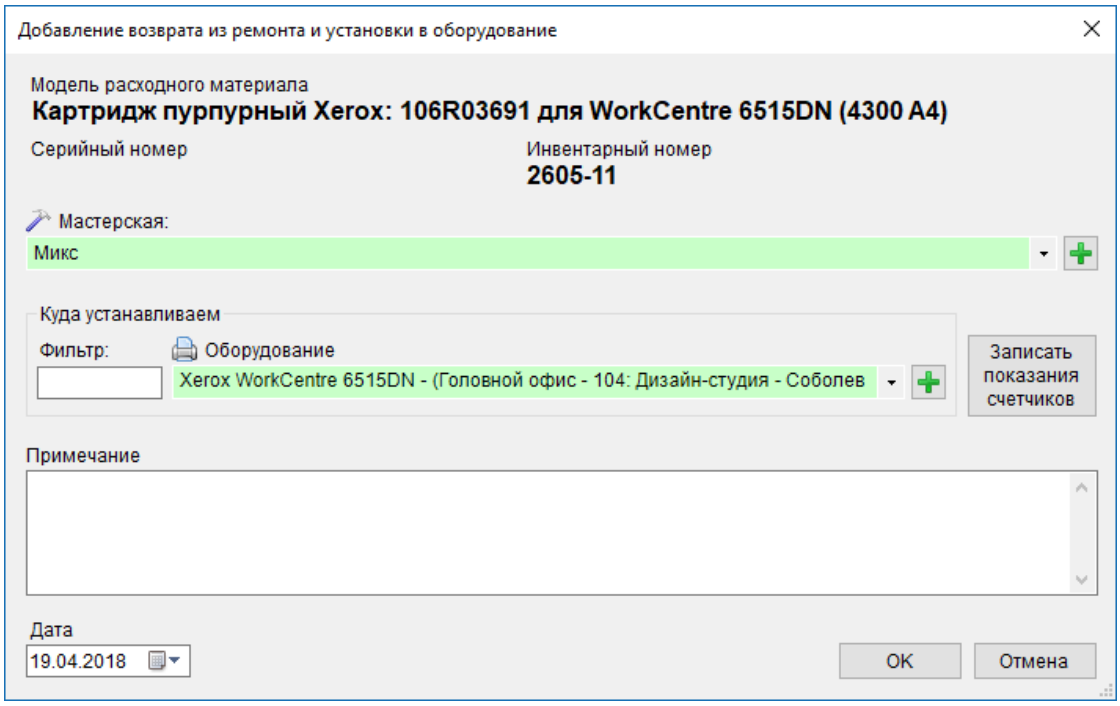
Диалог установки номерного расходного материала со склада.



Диалог извлечения номерного расходного материала из одного оборудования и установки в другое. Имеется возможность указать запас ресурса в НРМ на момент перестановки, например, остаток тонера (чернил) в процентах.



Диалог возврата номерного расходного материала из ремонта и установки в оборудование.

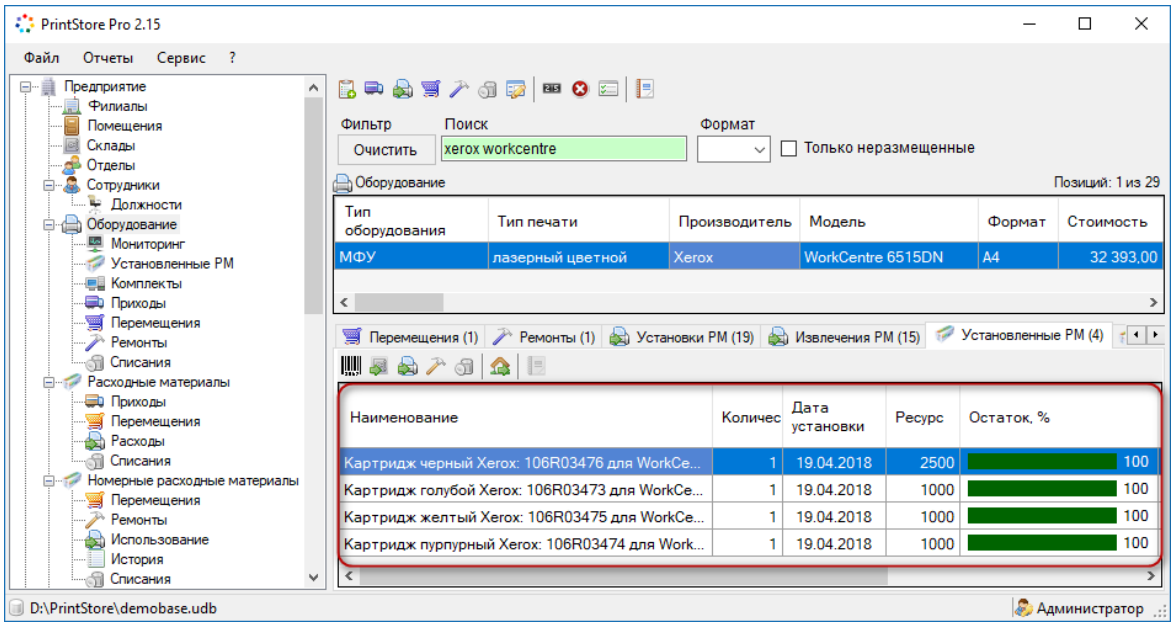


Просмотр установленных материалов

Установленные в конкретное устройство расходные материалы отображаются в разделе «Оборудование» на закладке «Установленные РМ». Расходные материалы

у находящегося в мониторинге оборудования можно просмотреть в подразделе «Оборудование — Мониторинг». Перечень всех расходных материалов, установленных в оборудовании предприятия на данный момент, представлен в подразделе «Оборудование — Установленные РМ». По каждому материалу отслеживается скорость расхода и текущий остаток ресурса, например, тонера или чернил.

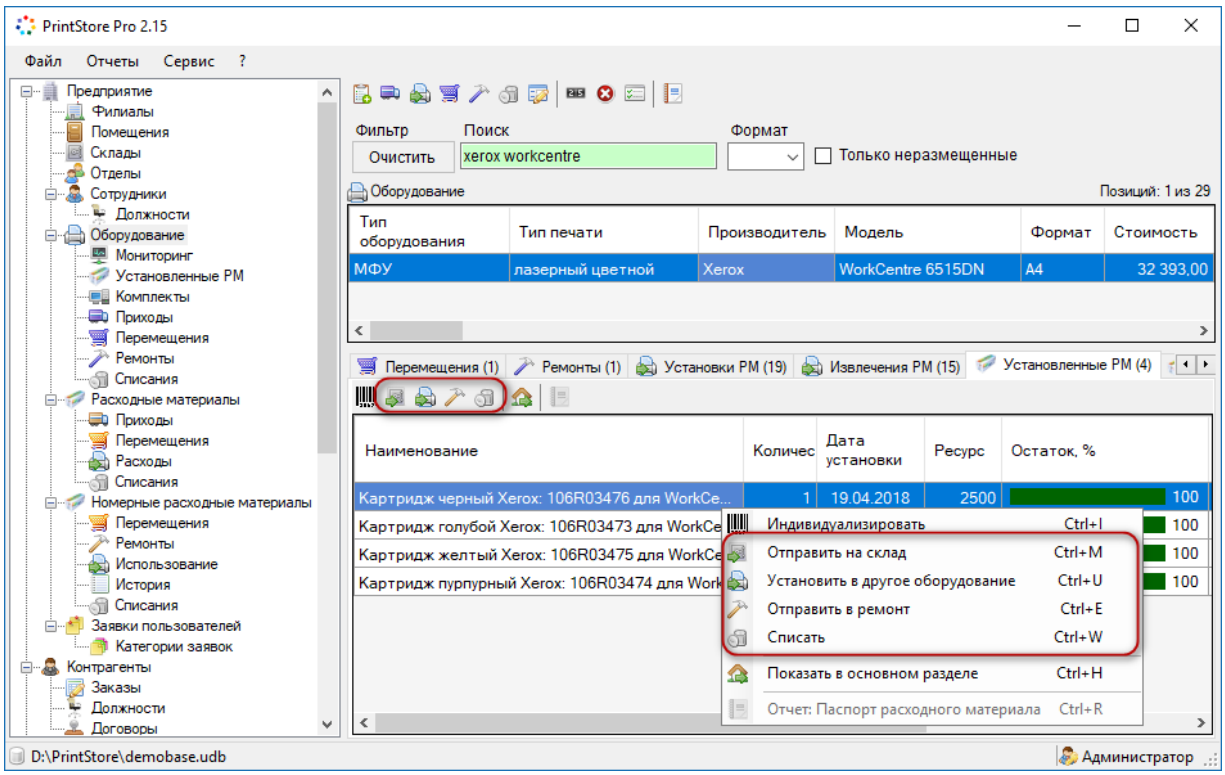
Обратите внимание, что количество установленных расходных материалов должно соответствовать количеству слотов в данном устройстве. Например, если в принтере 4 слота — для черного, желтого, пурпурного и голубого картриджей, то на закладке «Установленные РМ» по этому устройству должно отображаться 4 картриджа. Если их больше, это означает, что при установке какого-либо картриджа старый не был извлечен. В этом случае лишние картриджи необходимо списать.



Извлечение материалов из оборудования

Установленный в оборудовании материал обычно извлекают при замене расходников.

На закладке «Установленные РМ» и в одноименном подразделе раздела «Оборудование» также имеется возможность извлечь расходный материал из оборудования при помощи соответствующих кнопок на панели инструментов и команд контекстного меню. Извлеченный расходник может быть списан, а номерной материал дополнительно отправлен на склад, в сервис или переставлен в другое устройство.



История установок РМ и отчеты

Программа хранит историю установок и извлечений расходных материалов по каждому устройству, которая доступна на закладках «Установки РМ» и «Извлечения РМ» раздела «Оборудование».

История установок по всем расходникам представлена в подразделе «Расходные материалы — Расходы», по номерным материалам — «Номерные расходные материалы — Использование». Статистику использования в оборудовании материалов конкретной модели можно просмотреть на закладке «Расходы материалов» в разделе «Расходные материалы». История установок и извлечений отдельного номерного материала представлена на закладках «Использование» и «История» раздела «Номерные расходные материалы».

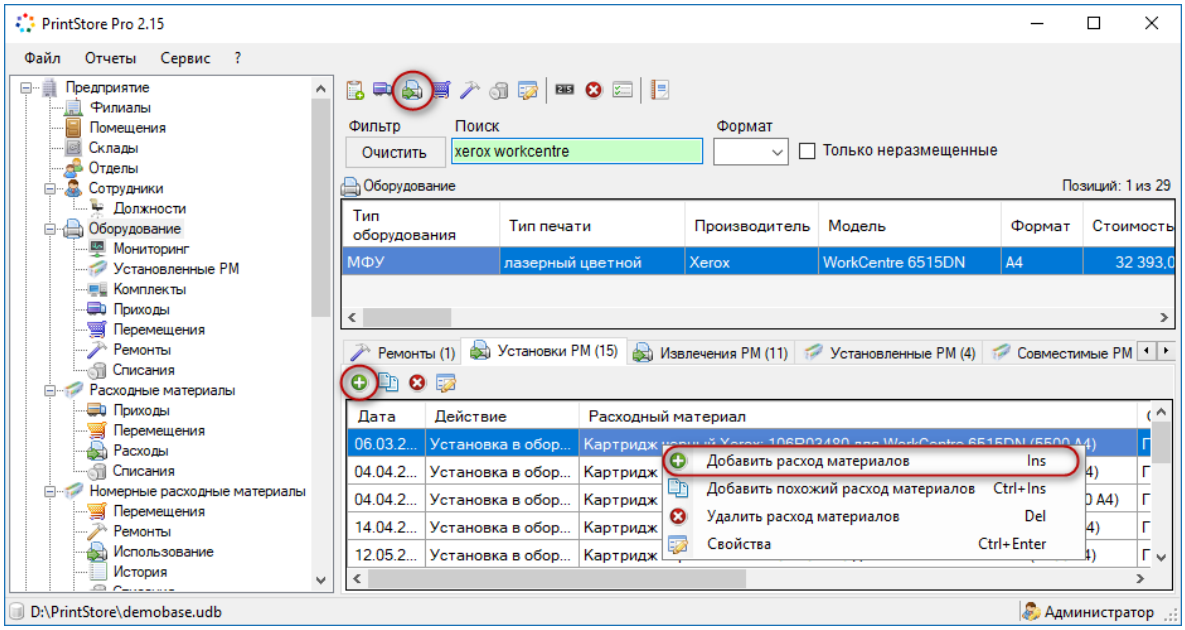
При необходимости можно отредактировать или удалить отдельную запись об установке или извлечении материала. В случае удаления записи, установка / извлечение будет отменено.

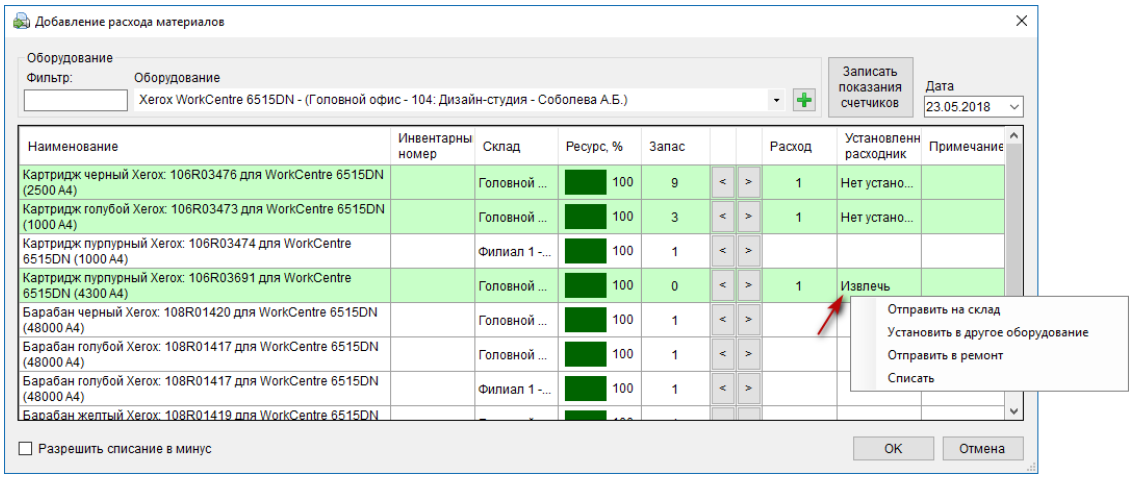
В программе доступен ряд отчетов по материалам, находящимся в оборудовании. Отчет «Расход материалов» позволяет просмотреть информацию об использовании расходных материалов в оборудовании за указанный период времени. Отчет «Номерные расходные материалы в оборудовании» содержит перечень НРМ, которые на текущий момент установлены в оборудовании. Наконец, в отчете «Использование номерных расходных материалов» представлена история установок и извлечений номерных материалов за выбранный период времени.

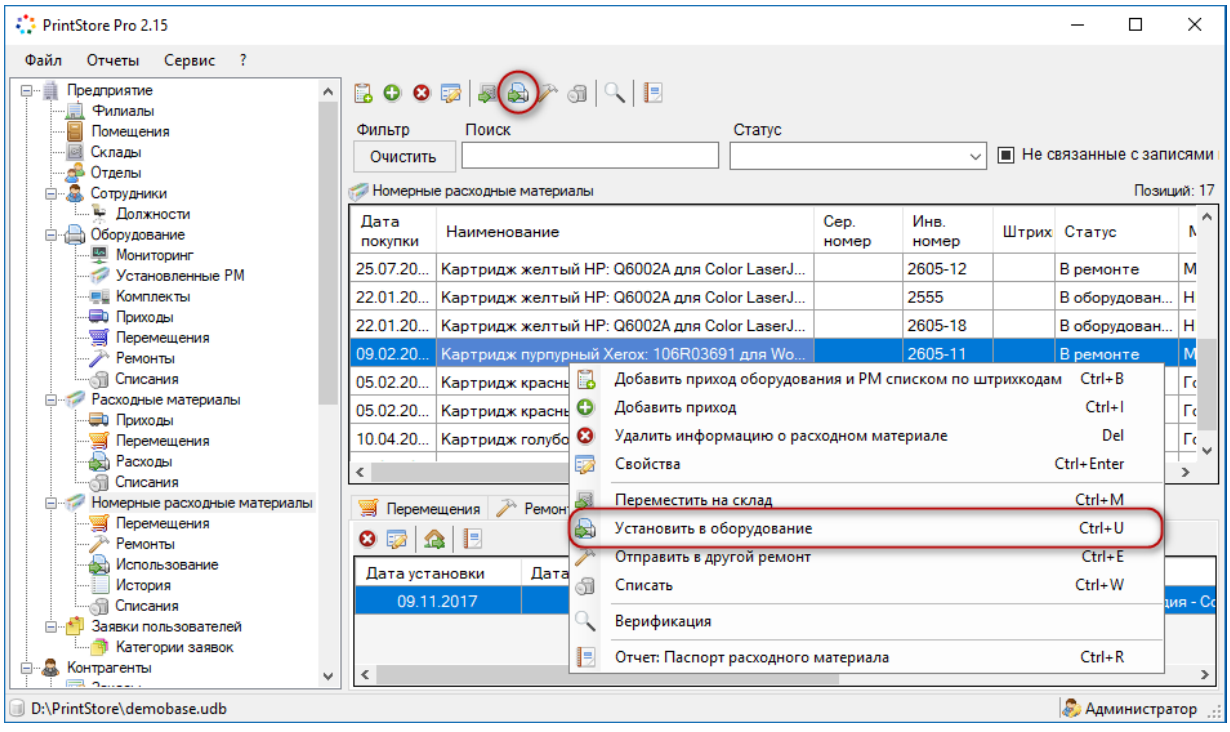
При просмотре записей об использовании материалов и отчетов действуют настройки доступа текущего пользователя программы. Если пользователю ограничен просмотр информации отдельных филиалов, то эта информация не отображается.

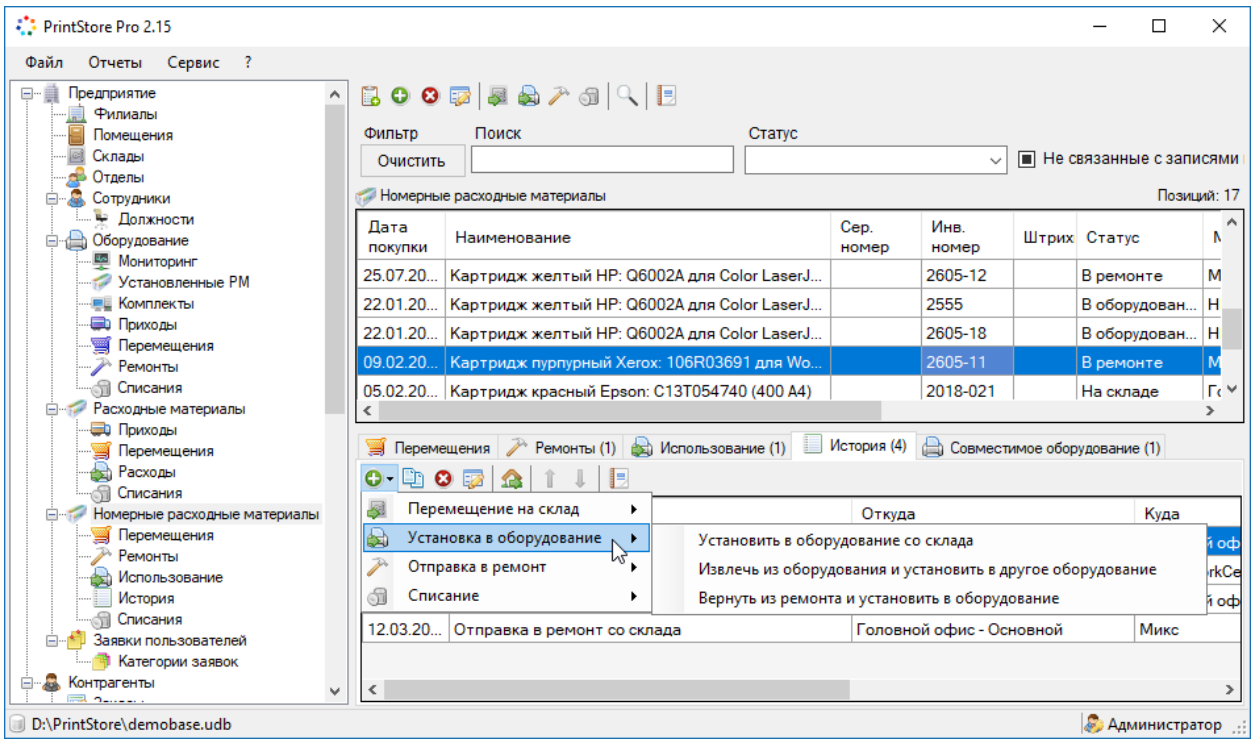
Эталон ответа:

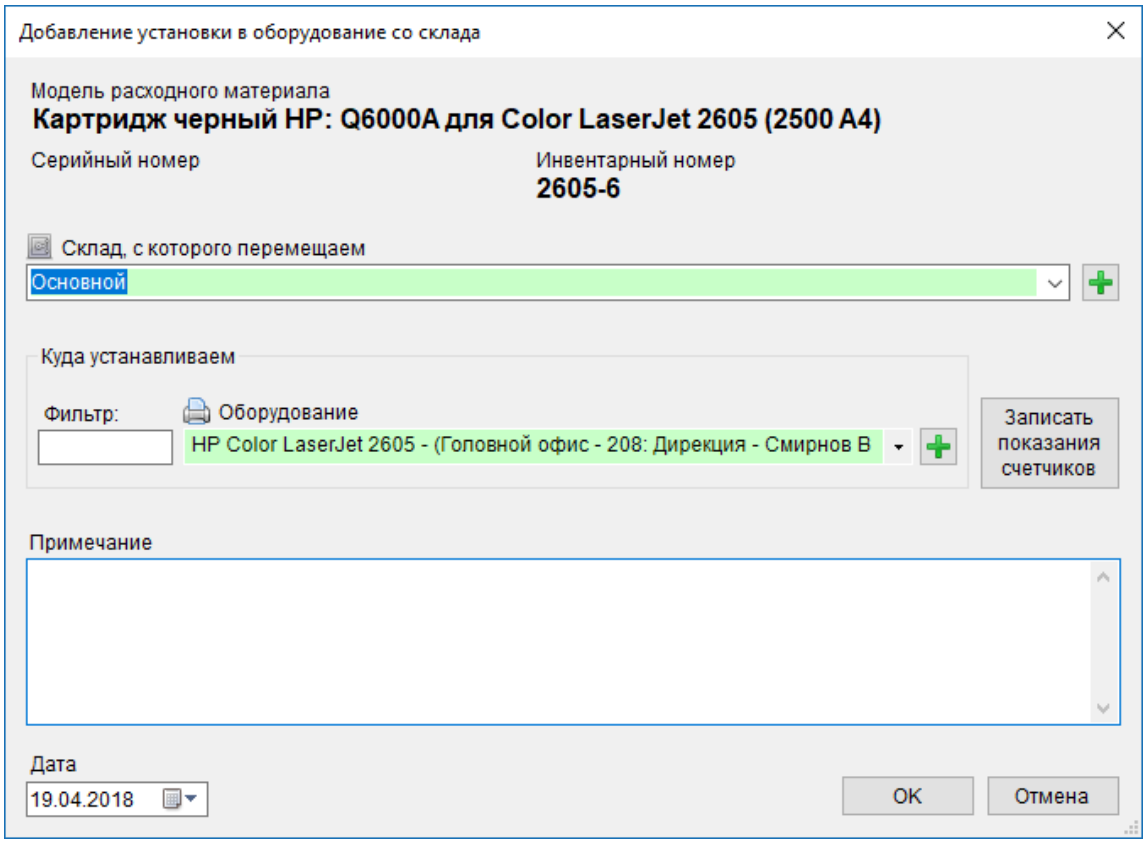
Ознакомиться с специализированным ПО по учету и контролю расходных материалов.

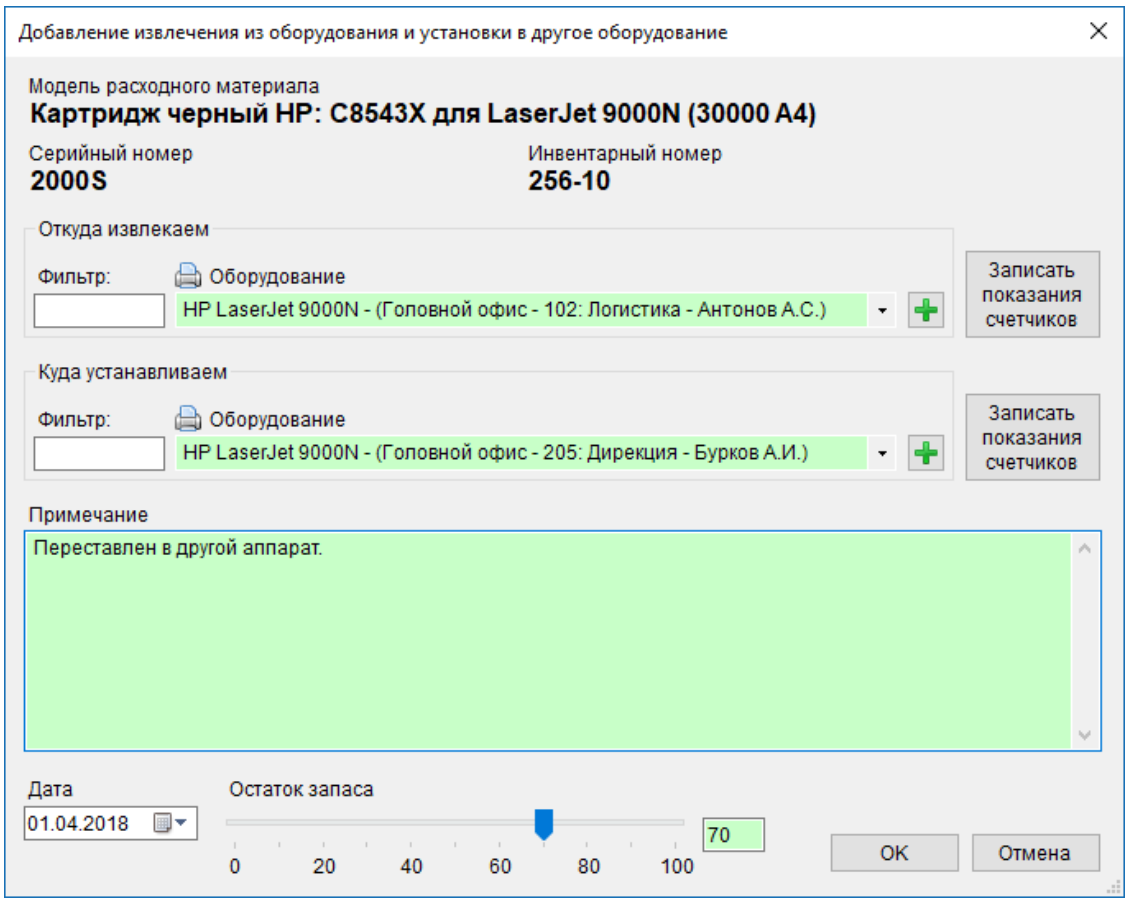


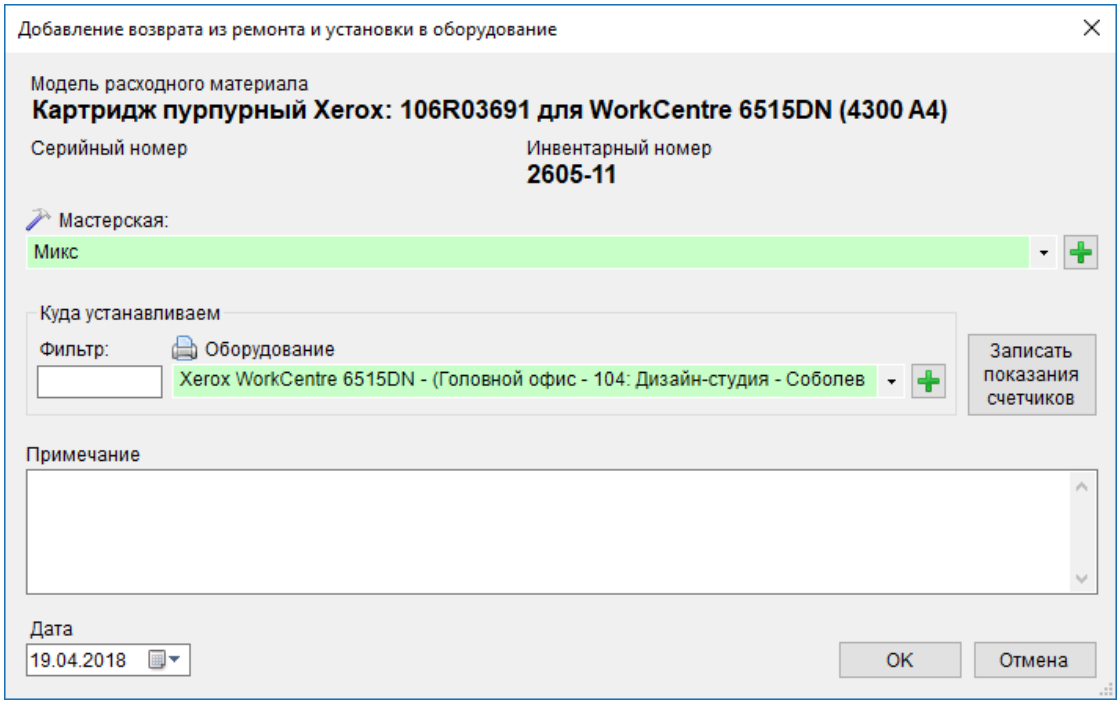


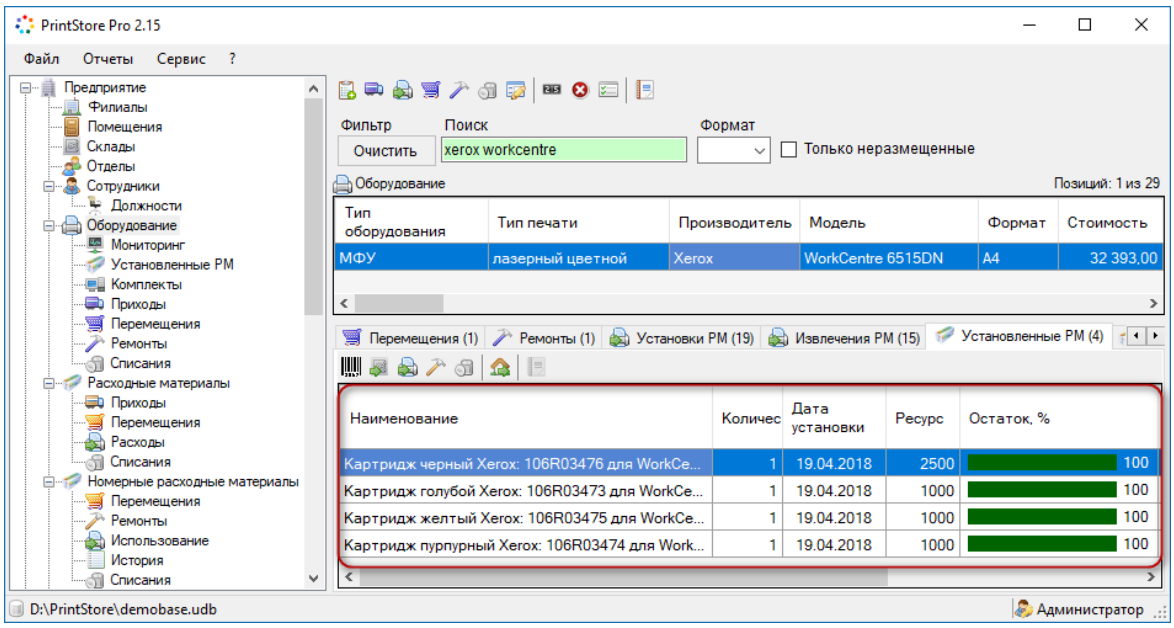


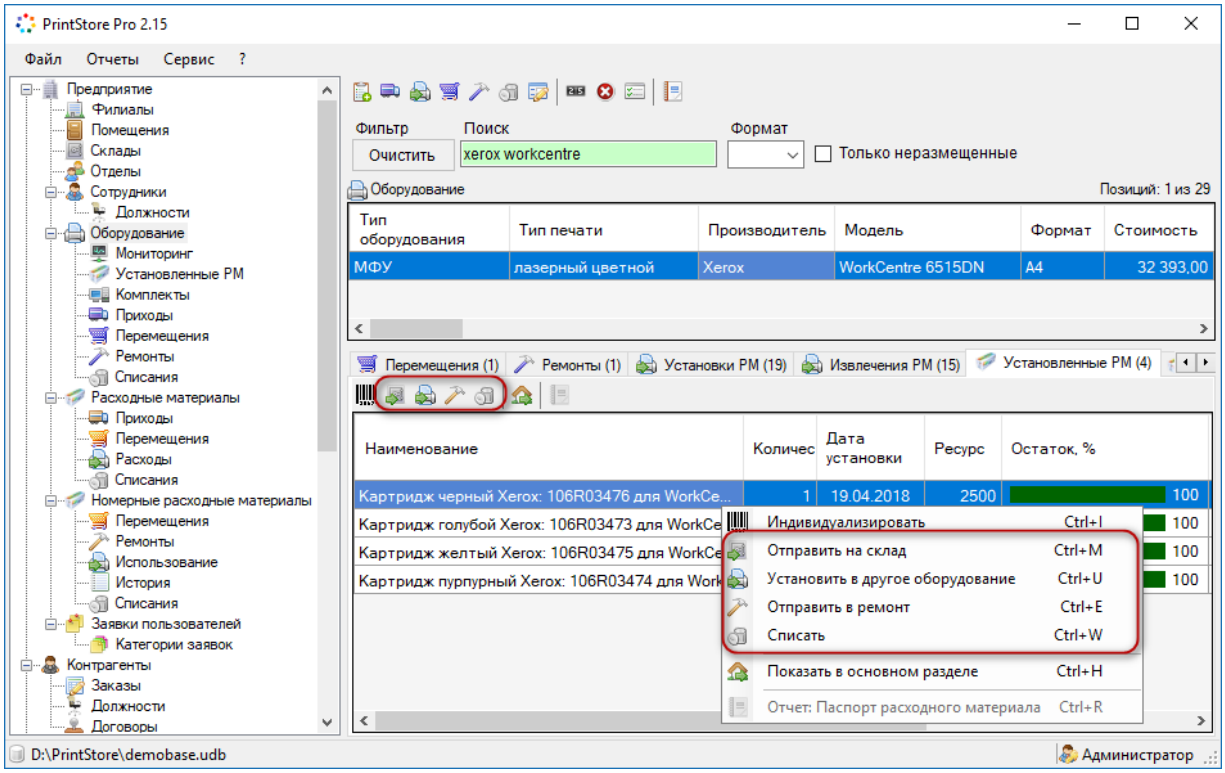

PrintStore Pro 2.15
Файл
Отчеты
Сервис
?
Предприятие
Филиалы
Помещения
Склады
Отделы
Сотрудники
Должности
Оборудование
Мониторинг
Установленные РМ
Комплекты
Приходы
Перемещения
Ремонты
Списания
Расходные материалы
Приходы
Перемещения
Расходы
Списания
Номерные расходные материалы
Перемещения
Ремонты
Использование
История
Списания
Заявки пользователей
Категории заявок
Контрагенты
Фильтр
Поиск
Статус
Очистить
Не связанные с записями
Номерные расходные материалы
Позиций: 17
Дата покупки
Наименование
Сер. номер
Инв. номер
Штрих
Статус
25.07.20...
Картридж желтый HP: Q6002A для Color LaserJ...
2605-12
В ремонте
22.01.20...
Картридж желтый HP: Q6002A для Color LaserJ...
2555
В оборудован...
22.01.20...
Картридж желтый HP: Q6002A для Color LaserJ...
2605-18
В оборудован...
09.02.20...
Картридж пурпурный Xerox: 106R03691 для Wo...
2605-11
В ремонте
05.02.20...
Картридж красный Epson: C13T054740 (400 A4)
2018-021
На складе
Перемещения
Ремонты (1)
Использование (1)
История (4)
Совместимое оборудование (1)
Перемещение на склад
Установка в оборудование
Отправка в ремонт
Списание
Установить в оборудование со склада
Извлечь из оборудования и установить в другое оборудование
Вернуть из ремонта и установить в оборудование
Откуда
Куда
12.03.20...
Отправка в ремонт со склада
Головной офис - Основной
Микс
D:\PrintStore\demobase.udb
Администратор


Добавление установки в оборудование со склада
Модель расходного материала
Картридж черный HP: Q6000A для Color LaserJet 2605 (2500 A4)
Серийный номер
Инвентарный номер
2605-6
Склад, с которого перемещаем
Основной
Куда устанавливаем
Фильтр:
Оборудование
HP Color LaserJet 2605 - (Головной офис - 208: Дирекция - Смирнов В
Записать показания счетчиков
Примечание
Дата
19.04.2018
OK
Отмена


Добавление извлечения из оборудования и установки в другое оборудование
Модель расходного материала
Картридж черный HP: C8543X для LaserJet 9000N (30000 A4)
Серийный номер
2000S
Инвентарный номер
256-10
Откуда извлекаем
Фильтр:
Оборудование
HP LaserJet 9000N - (Головной офис - 102: Логистика - Антонов А.С.)
Записать показания счетчиков
Куда устанавливаем
Фильтр:
Оборудование
HP LaserJet 9000N - (Головной офис - 205: Дирекция - Бурков А.И.)
Записать показания счетчиков
Примечание
Переставлен в другой аппарат.
Дата
01.04.2018
Остаток запаса
0
20
40
60
80
100
70
OK
Отмена


Добавление возврата из ремонта и установки в оборудование
Модель расходного материала
Картридж пурпурный Xerox: 106R03691 для WorkCentre 6515DN (4300 A4)
Серийный номер
Инвентарный номер
2605-11
Мастерская:
Микс
Куда устанавливаем
Фильтр:
Оборудование
Xerox WorkCentre 6515DN - (Головной офис - 104: Дизайн-студия - Соболев
Записать показания счетчиков
Примечание
Дата
19.04.2018
OK
Отмена


PrintStore Pro 2.15
Файл
Отчеты
Сервис
?
Предприятие
Филиалы
Помещения
Склады
Отделы
Сотрудники
Должности
Оборудование
Мониторинг
Установленные РМ
Комплекты
Приходы
Перемещения
Ремонты
Списания
Расходные материалы
Приходы
Перемещения
Расходы
Списания
Номерные расходные материалы
Перемещения
Ремонты
Использование
История
Списания
Фильтр
Очистить
Поиск
xerox workcentre
Формат
Только неразмещенные
Оборудование
Позиций: 1 из 29
Тип оборудования
Тип печати
Производитель
Модель
Формат
Стоимость
МФУ
лазерный цветной
Xerox
WorkCentre 6515DN
A4
32 393,00
Перемещения (1)
Ремонты (1)
Установки РМ (19)
Извлечения РМ (15)
Установленные РМ (4)
Наименование
Количес
Дата установки
Ресурс
Остаток, %
Картридж черный Xerox: 106R03476 для WorkCe...
1
19.04.2018
2500
100
Картридж голубой Xerox: 106R03473 для WorkCe...
1
19.04.2018
1000
100
Картридж желтый Xerox: 106R03475 для WorkCe...
1
19.04.2018
1000
100
Картридж пурпурный Xerox: 106R03474 для Work...
1
19.04.2018
1000
100
D:\PrintStore\demobase.udb
Администратор


PrintStore Pro 2.15
Файл
Отчеты
Сервис
?
Предприятие
Филиалы
Помещения
Склады
Отделы
Сотрудники
Должности
Оборудование
Мониторинг
Установленные РМ
Комплекты
Приходы
Перемещения
Ремонты
Списания
Расходные материалы
Приходы
Перемещения
Расходы
Списания
Номерные расходные материалы
Перемещения
Ремонты
Использование
История
Списания
Заявки пользователей
Категории заявок
Контрагенты
Заказы
Должности
Договоры
Фильтр
Очистить
Поиск
xerox workcentre
Формат
Только неразмещенные
Оборудование
Позиций: 1 из 29
Тип оборудования
Тип печати
Производитель
Модель
Формат
Стоимость
МФУ
лазерный цветной
Xerox
WorkCentre 6515DN
A4
32 393,00
Перемещения (1)
Ремонты (1)
Установки РМ (19)
Извлечения РМ (15)
Установленные РМ (4)
Наименование
Количес
Дата установки
Ресурс
Остаток, %
Картридж черный Xerox: 106R03476 для WorkCe...
1
19.04.2018
2500
100
Картридж голубой Xerox: 106R03473 для WorkCe
Картридж желтый Xerox: 106R03475 для WorkCe
Картридж пурпурный Xerox: 106R03474 для Work
Индивидуализировать
Ctrl+I
Отправить на склад
Ctrl+M
Установить в другое оборудование
Ctrl+U
Отправить в ремонт
Ctrl+E
Списать
Ctrl+W
Показать в основном разделе
Ctrl+H
Отчет: Паспорт расходного материала
Ctrl+R
D:\PrintStore\demobase.udb
Администратор

3.1.2. Оценка освоения теоретического курса профессионального модуля по МДК.03.02

Дидактические единицы	Проверяемые ОК, ПК	Формы контроля (наименование контрольной точки)	
		Текущая аттестация	Промежуточная аттестация
Тема 2.1. Автоматизированные системы управления технологическими процессами	ОК 1-9 ПК 3.1, ПК 3.2. ПК 3.4, ПК 3.5	Устный зачет по теме 2.1	Устный ответ на дифференцированном зачете
	ОК 1-9 ПК 3.1, ПК 3.2. ПК 3.4, ПК 3.5	Практическая работа № 2 Классификация технологических объектов управления на примере производственного предприятия	
		Практическая работа № 4 Изучение принципов работы АСУТП и САУ на примере реальных систем управления	
Тема 2.2. Промышленные сетевые технологии и протоколы в АСУ ТП	ОК 1-9 ПК 3.1, ПК 3.2. ПК 3.4, ПК 3.5	Устный зачет по теме 2.2	

Устный зачет по теме 2.1

Инструкция для обучающихся

Зачет сдается в рамках учебного занятия. Каждый студент отвечает в устной форме на предложенные преподавателем 5 случайных вопроса.

Выполнение задания: одному студенту на ответ выделяется 3 мин., группа сдает зачет за одно учебное занятие.

Перечень вопросов:

1. Понятие объекта управления.
2. Классификации технологических объектов управления
3. Основные функции АСУТП
4. Основные функции САУ.
5. Техническое, программное и информационное обеспечение АСУТП
6. Состав АСУ ТП
7. Основные понятия автоматизированной обработки информации
8. Простая модель технологического процесса

Эталоны ответов: приведены в учебном пособии по МДК.03.02 «Технологии автоматизации технологических процессов»

Устный зачет по теме 2.2

Инструкция для обучающихся

Зачет сдается в рамках учебного занятия. Каждый студент отвечает в устной форме на предложенные преподавателем 5 случайных вопроса.

Выполнение задания: одному студенту на ответ выделяется 3 мин., группа сдает зачет за одно учебное занятие.

Перечень вопросов:

1. Требования к промышленным сетям.
2. Протокол MODBUS
3. Беспроводные локальные сети для промышленного применения
4. Типовые промышленные проводные и кабельные сетевые протоколы

Эталоны ответов: приведены в учебном пособии по МДК.03.02 «Технологии автоматизации технологических процессов»

Практическая работа № 3 Анализ и сравнение систем управления технологическими объектами на примере различных отраслей промышленности

Задание:

1. Ознакомьтесь с материалом о системах управления технологическими объектами объектов управления.
2. Приведите пример АСУТП в газовой промышленности.
3. Приведите пример АСУТП в Электроэнергетике.
4. Приведите примеры АСУТП в химической промышленности.
5. Приведите примеры АСУТП в металлургии.
6. Сравните системы между собой.

Оформите в виде отчета.
Эталон ответа:

1. Приведите пример АСУТП в газовой промышленности.
«Интегрированная многоуровневая АСУ предприятия “Пермтрансгаз”» [ПС5/2002-1] рассматриваются история создания, структура, функции и особенности системы автоматизации крупного регионального газотранспортного предприятия (в его состав входит 15 многоцеховых компрессорных станций (КС), более 9 тыс. км магистральных газопроводов (МГ), свыше 100 газораспределительных станций (ГРС)). Созданная система отличается применением комплексного подхода: в рамках единых диспетчерских комплексов объединяются управление линейной частью МГ, контроль параметров КС, решение задач учета реализации газа, расчетов с потребителями, другие диспетчерские задачи. Эскизный проект ИАСУ «Пермтрансгаз» предусматривает реализацию системы, построенной по трехуровневой схеме и включающей в себя уровни ЦДП, ДП ЛПУМГ и низовых систем. Структура ЦДП включает в себя сервер АСУТП, рабочие места диспетчеров для решения задач управления в реальном времени, сервер реляционной БД для автоматизации учета реализации газа и решения других диспетчерских задач, а также средства информационных обменов и вычислительная сеть аппарата управления предприятия. Основными функциями ЦДП являются: сбор в реальном времени информации о состоянии линейной части, ГРС и газокомпрессорных станций, отображение информации

на графических мониторах специалистов, диагностика нештатных и аварийных ситуаций, ведение оперативного и глубокого архивов событий и значений измеряемых параметров, отображение графиков процессов, подготовка отчетов. ЦДП также осуществляет сбор информации о подаче газа потребителям, планирование реализации газа и решает другие связанные с этим задачи. Системы уровня ЛПУМГ имеют унифицированную структуру и состоят из сервера АСУТП, рабочих мест диспетчера и инженера КИПиА и других специалистов, средств подключения к диспетчерскому пункту систем цеховой автоматики и линейной телемеханики, автоматики ГРС, средств информационных обменов с ЦДП. ДП ЛПУМГ осуществляет в режиме реального времени сбор информации и выдачу команд управления от всех компонентов АСУТП, также обеспечивается контроль узла подключения КС, основных параметров работы КЦ и газоперекачивающих агрегатов, реализуются возможности аварийных остановов. На низовом уровне в систему входят АСУТП линейной части (СЛТМ), АСУ ГРС и КЦ. В систему также включены рабочие места операторов ГРС и сменных инженеров КЦ. При создании АСУТП нового поколения или такой ее части, как диспетчерского пункта, часто ставится задача сохранения инвестиций заказчика, сделанных в ранее установленные низовые средства контроля и управления: контроллеры линейной части, цеховых систем. В статье «Интегрированное решение для системы управления объектами ООО “Волгоградтрансгаз”» [ПС5/2002-2] рассматривается именно такой случай: замена ЦДП и части ДП ЛПУМГ с необходимостью сохранения получения данных от различных подсистем. Была поставлена задача интегрировать на уровне ЦДП в единую информационную базу реального времени данные от систем телемеханики «Магистраль-2», Serck-Controls, MMG, «Компас», а также данные от современных ДП ЛПУМГ. При этом на уровне ЦДП потребителями информации являются система отображения (множество АРМ специалистов и большой экран), программы расчета запаса газа и проч., для которых требуется генерация файлов данных специальных форматов. Общая структура системы управления, с выделенной коммуникационной системой, приведена на рис. 15.1. Особенностью данного проекта, которую можно экстраполировать на многие системы распределенного диспетчерского управления, является низкое качество каналов связи, требующее разработки специальных алгоритмов передачи данных при синхронизации баз данных локальных и центрального диспетчерских пунктов.

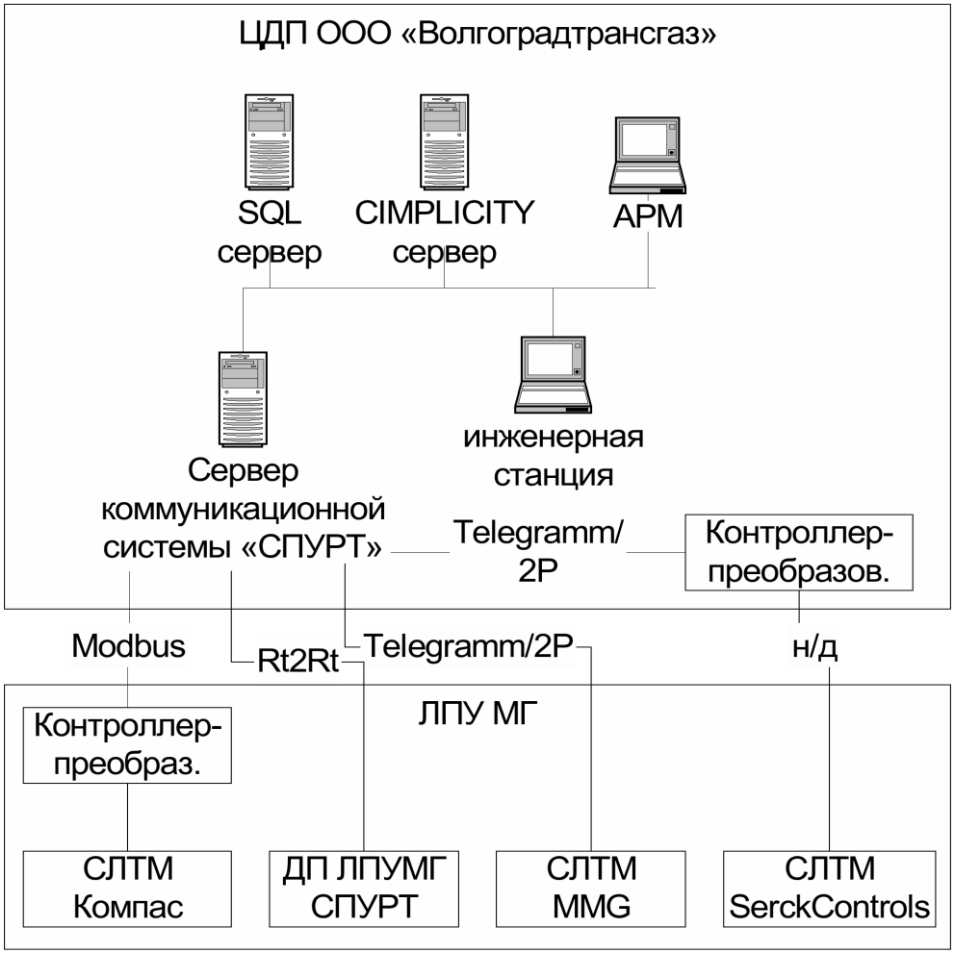
2. Приведите пример АСУТП в Электроэнергетике.

   «АСУТП Нижневартовской ГРЭС» [СТА3/1999] описываются опыт разработки, структура и программное обеспечение АСУТП первого блока Нижневартовской ГРЭС. Верхний уровень АСУТП содержит следующие компоненты:

   - Оперативные и неоперативные рабочие места, оперативная и архивная базы данных.
   - Мнемощит – блок из 4-х проекционных экранов.
   - Пульты аварийного и резервного управления котлом и турбиной.

   Нижний уровень – это контроллеры (применяется резервирование). Каждый контроллер состоит из набора плат. Монтируемых на общее шасси (крейт) и содержит в своем составе процессорную плату, сетевую плату, плату дискретного ввода/вывода, плату аналогового ввода. Через эти платы осуществляется

управление и обмен информацией с устройствами сопряжения с объектом



В составе АСУТП реализованы следующие основные технологические подсистемы:

- Сбор и первичная обработка информации – обеспечивает сбор, первичную обработку и контроль достоверности входной информации.
- Отображение информации в виде экранных мнемосхем, меню, мнемограмм, графиков, гистограмм, таблиц. Также ведется протокол событий, в котором отображаются все изменения дискретных параметров и модулей управления за последние 12 часов.
- Технологические защиты, включая регистрацию и анализ аварийных ситуаций;
- Дистанционное управление, осуществляется с функциональной клавиатуры или мышью; объектами ДУ являются задвижки, регулирующие клапаны, двигатели. Помимо собственно управления путем подачи команд оператор имеет возможность переводить режим работы аппаратуры на автоматическое управление.
- Автоматическое регулирование предназначено для автоматической стабилизации или изменений по заданным законам технологических параметров или их соотношений во всех режимах эксплуатации энергоблока.
- Технологическая сигнализация. Вывод сигналов и сообщений технологической сигнализации осуществляется тремя способами: часть сигналов выводится на индивидуальные сигнальные табло; вся ТС выводится на сигнализационные дисплеи, каждое появление сигнала сопровождается миганием и звуком; аварийные сообщения появляются в строке сообщений дисплеев оперативных рабочих мест.

- Протоколирование и документирование. Подсистема предназначена для формирования ведомостей, журналов и т.п., а также для протоколирования действий оператора-технолога, автоматики, защит и блокировок во время работы энергоблока.
- Диагностика программно-технического комплекса. Подсистема обеспечивает

А также:

- Контроль состояния технологического оборудования.
- Расчет, анализ и отображение технико-экономических показателей.
- Метрологический контроль.
- Справочно-обучающая система.

3. Приведите примеры АСУТП в химической промышленности.

В первых же строках статьи «АСУТП получения 1,2-дихлорэтана на Стерлитамакском АО “Каустик”» [СТА4/1997] указывается, что процесс получения 1,2-дихлорэтана (ДХЭ) реализован по непрерывной технологической схеме. Технологический процесс является пожаро- и взрывоопасным. АСУ ТП-ДХЭ представляет собой иерархическую двухуровневую распределенную систему. Нижний уровень АСУ ТП-ДХЭ включает три подсистемы:

- подсистему контроля и регистрации параметров технологического процесса;
- подсистему автоматического регулирования параметров;
- подсистему сигнализации и противоаварийной защиты процесса при отклонении параметров за допустимые границы.

На верхнем уровне системы АСУ ТП-ДХЭ на базе персональных компьютеров организуются автоматизированные рабочие места аппаратчиков, с которых в реальном времени должны выполняться функции контроля и управления стадий синтеза и ректификации ДХЭ, а также функции архивации текущей информации и ее обработки за отчетные периоды времени. В общем виде реализуемые на АРМ верхнего уровня АСУ ТП-ДХЭ функции можно разделить на три подкласса:

- индикация параметров ТП и сигнализация нарушений режима;
- управление из кадра (с экрана) технологическим процессом;
- управление переходом по экранам (кадрам).

Информация о нарушениях технологического режима подлежит автоматической распечатке на принтерах ПК АРМ с одновременным сохранением ее в специальном файле-отчете тревог. На мониторах ПК АРМ возможность сигнализации отклонений от уставок обеспечена для всех контролируемых параметров. Кроме сигналов от датчиков и преобразователей, на экранах ПК АРМ осуществляется контроль и индикация переменных, коэффициентов и констант на входах и выходах алгоблоков в алгоритмической структуре подсистемы автоматического регулирования и обеспечивается возможность их изменения в реальном времени.

4. **^ Пищевая промышленность. АСУТП мукомольного завода**

В статье «Объектно-структурированная АСУ ТП мукомольного завода» [СТА3/2000] описана объектно-ориентированная информационная структура АСУТП мукомольного завода, позволяющая упростить тиражирование и модернизацию аналогичных систем управления. Целью управления мукомольным заводом является максимальное увеличение выработки высоких сортов муки. Оценка потенциала роста выручки от внедрения современной АСУ ТП,

проведенная на основании статистики эффективности работы однотипных заводов (так называемый типовой проект производительностью 250 тонн зерна в сутки) составляет около 120 тыс. долларов США в год. На территории России находится около ста таких заводов. Основные задачи управления на мукомольном производстве: стабилизация технологических показателей подаваемого в размол зерна; оперативный контроль процесса размола; сокращение времени простоев за счет быстрого пуска оборудования и предупреждения аварий технологических машин. Также специфика мукомольного производства – довольно медленные (десятки секунд) переходные процессы, а автоматическое управление пока ограничивается стабилизацией физико-технологических показателей зерна, поступающего в размол. В основе системы лежит набор объектов, иерархия которых определяется порядком получения и обработки сигналов. Основных информационные слоев (уровней) АСУ ТП мукомольного завода три:

- Уровень аппаратных сигналов. На этом уровне производится сбор информации от технических средств контроля и управления. Информационный интерфейс этого уровня не зависит от типа примененного устройства связи с объектом управления (УСО). (Было выбрано УСО фирмы Advantech ADAM-5000 с интерфейсом RS-485). Три сети контроллеров ADAM-5000 обслуживаются одинаковыми программными серверами, которые осуществляют первичную обработку и отображение информации. Необходимость использования нескольких сетей была обусловлена топологией предприятия и повышенными требованиями к динамике контуров аналогового регулирования.
- Уровень инженерных сигналов. Этот уровень представлен программными серверами аналоговых регуляторов, весов и дискретных дозаторов и сервером сменного времени. Эти серверы получают информацию от интерфейса серверов ADAM-5000, производят обработку и фильтрацию сигналов, вырабатывают управляющие и сигнализирующие воздействия, которые поступают на исполнительные устройства. Интерфейсы серверов этого уровня поставляют пользовательским программам информацию в размерности контролируемых параметров (расход в единицу времени, суммарная выработка и т.п.). Эти же серверы осуществляют регистрацию событий с записью их в текстовые файлы и базу данных, а также накопление информации для ее последующей статистической обработки. Сервер сменного времени необходим для привязки событий ко времени работы отдельных смен. Кроме того, он вырабатывает сообщения для инициализации периодических действий персонала: отбора проб, проведения анализов, формирования отчетов и т.п. Сервер аналоговых регуляторов производит фильтрацию поступающего аналогового сигнала от сервера ADAM дискретным фильтром первого порядка, визуально и аппаратно сигнализирует о выходе параметра за заданные пределы и осуществляет управление контролируемым параметром по ПИ-закону регулирования.
- Уровень технологических объектов управления Он представлен программным сервером технологических машин завода и пользовательскими программами, осуществляющими связь оператора с процессом. Интерфейс сервера машин представляет информацию о состоянии машины, принимает команды от клиентской программы на включение и отключение отдельных машин, а получая информацию от сервера ADAM и сервера регуляторов, он определяет состояние машин и передает данные о случившихся с машиной событиях своим клиентам. Кроме того, он самостоятельно отключает

при аварии отдельной машины необходимый набор технологического оборудования завода. Сервер производит регистрацию событий.

При проектировании визуального интерфейса пользовательских программ применялся принцип выдачи оператору только того минимума информации, который достаточен для принятия решений при управлении процессом. Однако это не значит, что оператор ограничен в получении более подробных данных. Для этого ему необходимо обратиться к серверу, который снабжает прикладную программу информацией, и получить от него нужные данные. Очевидным преимуществом выбранной трехслойной информационной структуры, по мнению авторов, является независимость задач каждого информационного уровня от конкретной реализации сервера и аппаратных средств. Недостатком является пока еще низкое быстродействие, особенно при применении технологии DCOM.

4. Приведите примеры АСУТП в металлургии.

Статья «Система контроля технологии и управления скоростными режимами прокатного стана» [СТА1/2001] посвящена вопросу создания АСУ скоростными режимами прокатки на обжимном стане Донецкого металлургического завода. Рассматриваются структура, аппаратное и программное обеспечение системы. Основным назначением разрабатываемой автоматизированной системы являлось повышение эксплуатационной надежности оборудования прокатных клетей 950 и 900 за счет строгого соблюдения технологии прокатки и предотвращения возникновения и развития неустойчивых и аварийных режимов. В соответствии с поставленной задачей система управления скоростными режимами должна обеспечивать:

- … задачи, специфические для управления прокатным станом, а также:
- отслеживание предельных значений обжатий и запрет на работу оборудования при грубых ошибках операторов с выдачей соответствующих сообщений;
- индикацию режимов работы главных приводов и выдачу сообщений дежурному по машинному залу и оператору;
- протоколирование событий, накопление статистических данных.

Подсистема контроля аварийных режимов должна функционировать автономно от системы регулирования и обеспечивать постоянную регистрацию параметров работы приводов и переключений в системе управления для сохранения предыстории развития аварийных процессов. Исходя из особенностей объекта автоматизации и функций системы, в качестве аппаратной базы были выбраны IBM PC совместимые промышленные контроллеры. Их достоинствами являются открытость архитектуры, удобство построения вычислительной сети, возможность применения гибких разветвленных алгоритмов, удобство визуализации и протоколирования данных, большие объемы доступного программного обеспечения. В качестве операционной системы была выбрана ОС РВ QNX. Т.к. в функции системы входит управление быстротекущим процессом изменения скорости приводов при одновременном анализе большого количества технологических параметров и протоколирование событий, то только использование ОС с заданным временем отклика могло обеспечить нормальную работу. Более подробно задачи АСУТП можно представить, рассмотрев основные задачи ПО:

1. Опрос состояния аналоговых и дискретных датчиков объекта управления.

2. Цифровая обработка аналоговых сигналов, контроль достоверности сигналов, привязка к физическим величинам.
3. Определение параметров, непосредственное измерение которых невозможно, по измеряемым параметрам на основе «наблюдателя состояния».
4. Контроль отклонения сигналов за заданные границы (уставки) с выдачей сообщений оперативному персоналу.
5. Пуск регистратора аварийных процессов в случае аварийных и предаварийных ситуаций с выдачей оперативному персоналу соответствующего сообщения.
6. Расчет управляющих воздействий для рабочей и резервной систем управления.
7. Анализ состояния силовой схемы электроприводов с автоматическим переключением на резерв.
8. Ограничение скоростных режимов работы клетей.
9. Контроль за соблюдением технологии операторами с необходимыми блокировками.
10. Технологическая сигнализация положения органов управления.
11. Ведение протокола работы системы (информация об аварийных ситуациях, изменении параметров положения органов управления, о работе защит и технических средств комплекса и т.д.) с последующей архивацией.
12. Отображение в режиме реального времени выбранных параметров электроприводов.
13. Оперативное изменение параметров настройки системы с блокировками «от дурака» и контролем доступа.
14. Оперативный ввод и изменение схем скоростных и технологических режимов прокатки в виде таблиц с помощью специального редактора, с контролем доступа.
15. Сброс блокировок (квитирование) аварийных ситуаций дежурным по машинному залу.

Все основные задачи системы, связанные с реализацией функций установки и контроля скоростных и технологических режимов работы блюминга, обеспечиваются путем настройки и конфигурирования системы с помощью вспомогательных программных средств и не требуют от обслуживающего персонала знаний в области применения языков программирования. В результате, созданная система управления скоростными режимами и контроля технологии прокатки позволяет повысить надежность работы оборудования обжимного стана, улучшить обеспечение обслуживающего персонала информацией о технологических и электрических эксплуатационных параметрах, увеличить оперативность устранения аварийных ситуаций в электрических цепях главных приводов (уменьшить время простоев).

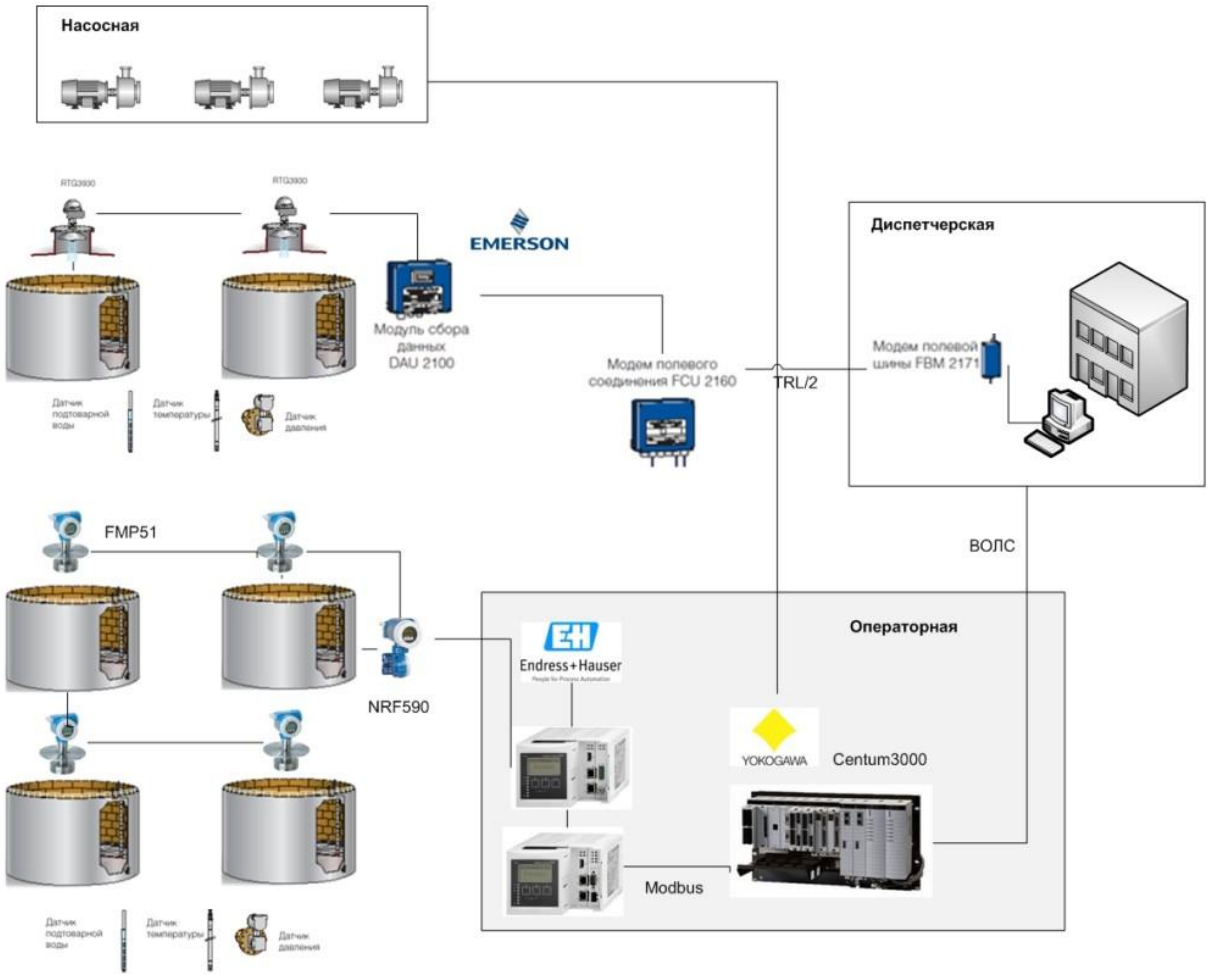
Практическая работа № 4 Изучение принципов работы АСУТП и САУ на примере реальных систем управления

Задание:

1. Ознакомьтесь с материалом о системе диспетчеризации производства Атырауского НПЗ
   https://iiot.kz/projects/asu-tp-paz-i-rsu
2. Нарисуйте структурную схему АСУ ТП.
3. Опишите подсистемы АСУ ТП.
4. Опишите принцип работы АСУ ТП.

Эталон ответа:

1. Нарисуйте структурную схему АСУ ТП.
   Структурная схема АСУ ТП ПАЗ РСУ «Резервуарный парк N1" АНПЗ



2. Опишите подсистемы АСУ ТП.

   - Установка ДИЗТОПЛИВО;
   - Установка ОЧИСТКА ВОДОРОДА;
   - Установка ПРОИЗВОДСТВО ВОДОРОДА;
   - Установка ПРОИЗВОДСТВО СЕРЫ;
   - Установка ГРАДИРНЯ;
   - Изомеризация;
   - Установка ГИДРООЧИСТКА БЕНЗИНА;
   - Установка АМИНОВАЯ ОЧИСТКА ГАЗОВ;
   - МАТЕРИАЛЬНЫЕ БАЛАНСЫ ВЫПУСК ПРОДУКЦИ

3. Опишите принцип работы АСУ ТП.

Данные из TRACE MODE записываются в СУБД ORACLE – одну из самых мощных и распространенных СУБД в промышленности. Новая АСДУ Атырауского НПЗ под управлением SCADA TRACE MODE в режиме реального времени делает десятки SQL-запросов к СУБД, на основе данных о характеристиках различных нефтепродуктов из базы центральной лаборатории завода, производит перерасчет для фактической температуры и формирует материальные потоки для восьми установок с целью создания общего материального баланса завода.

3.1.2. Оценка освоения теоретического курса профессионального модуля по МДК.03.03

Дидактические единицы	Проверяемые ОК, ПК	Формы контроля (наименование контрольной точки)	
		Текущая аттестация	Промежуточная аттестация
Тема 3.1. Безопасность компьютерных сетей	ОК 1- 9 ПК 3.3, ПК 3.6	Устный зачет по темам 3.1.1-3.1.7	Устный ответ на экзамене
		Устный зачет по темам 3.1.8-3.1.15	
		Устный зачет по темам 2.1.16. – 2.1.21	
	ОК 1- 9 ПК 3.3, ПК 3.6	Практическая работа № 2 Основные этапы допуска к ресурсам вычислительной системы.	
		Практическая работа № 16 Монитор вторжений Threat Detection шлюза безопасности ASA	
Тема 3.2. Системы обнаружения вторжения	ОК 1- 9 ПК 3.3, ПК 3.6	Практическая работа № 21 Установка системы обнаружения и предотвращения вторжения Snort	
		Практическая работа № 26 Настройка веб-интерфейса для системы обнаружения и предотвращения вторжения Snort	

Устный зачет по темам 3.1.1-3.1.7

Инструкция для обучающихся

Зачет сдается в рамках учебного занятия. Каждый студент отвечает в устной форме на предложенные преподавателем 5 случайных вопроса.

Выполнение задания: одному студенту на ответ выделяется 3 мин., группа сдает зачет за одно учебное занятие.

Перечень вопросов:

1. Фундаментальные принципы безопасной сети
2. Современные угрозы сетевой безопасности.
3. Вирусы, черви и троянские кони.
4. Методы атак.
5. Безопасность Сетевых устройств OSI

6. Безопасный доступ к устройствам.
7. Назначение административных ролей.
8. Мониторинг и управление устройствами.
9. Использование функция автоматизированной настройки безопасности.
10. Авторизация, аутентификация и учет доступа (AAA)

Эталоны ответов: приведены в учебном пособии по МДК.03.03 «Безопасность компьютерных сетей»

Устный зачет по теме 3.1.8. – 3.1.15

Инструкция для обучающихся

Зачет сдается в рамках учебного занятия. Каждый студент отвечает в устной форме на предложенные преподавателем 5 случайных вопроса.

Выполнение задания: одному студенту на ответ выделяется 3 мин., группа сдает зачет за одно учебное занятие.

Перечень вопросов:

1. Свойства AAA.
2. Локальная AAA аутентификация.
3. Server-based AAA
4. Реализация технологий брандмауэра
5. ACL. Технология брандмауэра
6. Контекстный контроль доступа (CBAC).
7. Политики брандмауэра основанные на зонах.
8. Реализация технологий предотвращения вторжения
9. IPS технологии.
10. IPS сигнатуры.

Эталоны ответов: приведены в учебном пособии по МДК.03.03 «Безопасность компьютерных сетей»

Устный зачет по теме 3.1.16. – 3.1.21

Инструкция для обучающихся

Зачет сдается в рамках учебного занятия. Каждый студент отвечает в устной форме на предложенные преподавателем 5 случайных вопроса.

Выполнение задания: одному студенту на ответ выделяется 3 мин., группа сдает зачет за одно учебное занятие.

Перечень вопросов:

1. Реализация IPS.
2. Проверка и мониторинг IPS
3. Безопасность локальной сети
4. Обеспечение безопасности пользовательских компьютеров.
5. Соображения по безопасности второго уровня (Layer-2).

6. Конфигурация безопасности второго уровня.
7. Безопасность беспроводных сетей, VoIP и SAN
8. Криптографические системы
9. Реализация технологий VPN
10. GRE VPN.
11. Компоненты и функционирование IPSec VPN.

Эталоны ответов: приведены в учебном пособии по МДК.03.03 «Безопасность компьютерных сетей»

Практическая работа № 15 Монитор вторжений Threat Detection шлюза безопасности ASA

Инструкция для обучающихся

Внимательно прочитайте задание. Проведите установку и настройку контроллеров.

Время выполнения – 90 минут.

Задание

Задание:

Топология

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.1.1	255.255.255.0	Недоступно
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
ПК-А	Сетевой адаптер	192.168.1.3	255.255.255.0	192.168.1.1

Задачи

Часть 1. Настройка основных параметров устройства
Часть 2. Настройка маршрутизатора для доступа по протоколу SSH
Часть 3. Проверка сеанса связи по протоколу Telnet с помощью программы Wireshark
Часть 4. Проверка сеанса связи по протоколу SSH с помощью программы Wireshark
Часть 5. Настройка коммутатора для доступа по протоколу SSH
Часть 6. Настройка протокола SSH в интерфейсе командной строки коммутатора

Исходные данные/сценарий

Раньше для удалённой настройки сетевых устройств в основном применялся протокол Telnet. При этом протоколы типа Telnet не включают проверку подлинности и шифрова-

ние информации, передаваемой между клиентом и сервером, что позволяет сетевым средствам слежения перехватывать пароли и данные конфигурации.
Secure Shell(SSH)— это сетевой протокол, устанавливающий безопасное подключение эмулятора терминала к маршрутизатору или иному сетевому устройству. Протокол SSH шифрует все сведения, которые поступают по сетевому каналу, и предусматривает аутентификацию удалённого компьютера. Протокол SSH всё больше заменяет Telnet — именно его выбирают сетевые специалисты в качестве средства удалённого входа в систему. Чаще всего протокол SSH применяется для входа на удалённое устройство и выполнения команд, но может также передавать файлы по связанным протоколам SFTP или SCP.
Чтобы протокол SSH работал, на взаимодействующих сетевых устройствах должна быть настроена его поддержка. В ходе лабораторной работы вы активируете на маршрутизаторе SSH-сервер и подключитесь к маршрутизатору, используя ПК с клиентом SSH. В локальной сети подключение обычно устанавливается с помощью Ethernet и IP-адреса. Кроме того, в ходе лабораторной работы вы настроите маршрутизатор для приёма подключений по протоколу SSH и воспользуетесь программой Wireshark для перехвата и просмотра сеансов Telnet и SSH. Это покажет, какую важную роль играет шифрование данных, осуществляемое протоколом SSH. И, наконец, вам придётся самостоятельно настроить коммутатор для подключения по протоколу SSH.
Примечание. Маршрутизаторы, используемые на практических занятиях CCNA: маршрутизаторы с интеграцией сервисов серии Cisco 1941 (ISR) установленной версии Cisco IOS 15.2(4) M3 (образ universalk9). Используемые коммутаторы: семейство коммутаторов Cisco Catalyst 2960 версии CISCO IOS 15.0(2) (образ lanbasek9). Можно использовать другие маршрутизаторы, коммутаторы и версии CISCO IOS. В зависимости от модели и версии Cisco IOS выполняемые доступные команды и выводы могут отличаться от данных, полученных в ходе лабораторных работ. Точные идентификаторы интерфейса см. в таблице сводной информации об интерфейсах маршрутизаторов в конце данной лабораторной работы.
Примечание. Убедитесь, что информация, имеющаяся на маршрутизаторе и коммутаторе, удалена и они не содержат файлов загрузочной конфигурации. Если вы не уверены, что сможете это сделать, обратитесь к инструктору.
Необходимые ресурсы

- 1 маршрутизатор (Cisco 1941 с универсальным образом M3 версии CISCO IOS 15.2(4) или аналогичным)
- 1 коммутатор (серия Cisco 2960, с программным обеспечением Cisco IOS версии 15.0(2), образ lanbasek9 или аналогичный)
- Один ПК (Windows 7, Vista или XP с эмулятором терминала, например Tera Term, и установленной программой Wireshark)
- Консольные кабели для настройки устройств CISCO IOS через консольные порты
- Кабели Ethernet в соответствии с топологией

Часть 1: Основные настройки устройства
В части 1 потребуется настройка топологии сети и основных параметров, таких как IP-адреса интерфейсов, доступ к устройствам и пароли на маршрутизаторе.
Шаг 1: Создайте сеть в соответствии с изображенной на схеме топологией.
Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.
Шаг 3: Настройте маршрутизатор.

a. Подключите консоль к маршрутизатору и активируйте привилегированный режим.
b. Войдите в режим конфигурации.

c. Отключите поиск в DNS, чтобы предотвратить попытки маршрутизатора преобразовывать неверно введённые команды таким образом, как будто они являются именами узлов.

d. Назначьте **class** в качестве пароля привилегированного режима.

e. Назначьте **cisco** в качестве пароля консоли и включите вход по паролю.

f. Назначьте **cisco** в качестве пароля виртуального терминала и включите вход по паролю. g. Зашифруйте пароли.

h. Создайте баннер, который предупреждает о запрете несанкционированного доступа.

i. Настройте и активируйте интерфейс маршрутизатора G0/1 с помощью сведений, содержащихся в таблице адресации.

j. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Шаг 4: Настройте ПК-A.

a. Настройте на ПК-A IP-адрес и маску подсети.

b. Настройте на ПК-A шлюз по умолчанию.

Шаг 5: Проверьте подключение к сети.

Отправьте эхо-запрос с помощью команды ping с ПК-A на маршрутизатор R1. Если эхо-запрос с помощью команды ping не проходит, найдите и устраните неполадки подключения.

Часть 2: Настройка маршрутизатора для доступа по протоколу SSH

Подключение к сетевым устройствам по протоколу Telnet сопряжено с риском для безопасности, поскольку вся информация передаётся в виде открытого текста. Протокол SSH шифрует данные сессии и требует аутентификации устройств, поэтому для удалённых подключений рекомендуется использовать именно его. В части 2 вам нужно настроить маршрутизатор для приёма соединений по протоколу SSH по линиям VTY.

Шаг 1: Настройте аутентификацию устройств.

При генерации ключа шифрования используются имя устройства и домен. Это значит, что эти имена необходимо указать перед вводом команды **crypto key**.

a. Укажите имя устройства.

Router(config)# **hostname R1**

b. Укажите домен для устройства.

R1(config)# **ip domain-name ccna-lab.com**

Шаг 2: Создайте ключ шифрования с указанием его длины.

R1(config)# **crypto key generate rsa modulus 1024**

The name for the keys will be: R1.ccna-lab.com

% The key modulus size is 1024 bits % Generating 1024 bit RSA keys, keys will be non-exportable...

[OK] (elapsed time was 1 seconds)

R1(config)#

*Jan 28 21:09:29.867: %SSH-5-ENABLED: SSH 1.99 has been enabled

Шаг 3: Создайте имя пользователя в локальной базе учётных записей.

R1(config)# **username admin privilege 15 secret adminpass**

R1(config)#

*Feb 6 23:24:43.971: End->Password:QHjxdsVkjtoP7VxKIcPsLdTiMIvyLkyjT1HbmYxZigc

R1(config)#

Примечание. Пятнадцатый уровень привилегий предоставляет пользователю права администратора.

Шаг 4: Активируйте протокол SSH на линиях VTY.

a. Активируйте протоколы Telnet и SSH на входящих линиях VTY с помощью команды **transport input**.

R1(config)# **line vty 0 4**
R1(config-line)# **transport input telnet ssh**

b. Измените способ входа в систему — выберите проверку пользователей по локальной базе учётных записей.

R1(config-line)# **login local**
R1(config-line)# **end** R1#

Шаг 5: Сохраните текущую конфигурацию в файл загрузочной конфигурации.

R1# **copy running-config startup-config**
Destination filename [startup-config]?
Building configuration...
[OK]
R1#

Часть 3: Проверка сеанса связи по протоколу Telnet с помощью программы Wireshark

В части 3 вы воспользуетесь программой Wireshark для перехвата и просмотра данных, передаваемых во время сеанса связи маршрутизатора по протоколу Telnet. С помощью программы Tera Term вы подключитесь к маршрутизатору R1 по протоколу Telnet, войдёте в систему и запустите на маршрутизаторе команду show run.

Примечание. Если на вашем компьютере нет программного обеспечения клиента Telnet/SSH, его необходимо установить. Чаще всего для работы с протоколами Telnet и SSH используются программы Tera Term (http://download.cnet.com/Tera-Term/3000-20432_4-75766675.html) и PuTTy (www.putty.org).

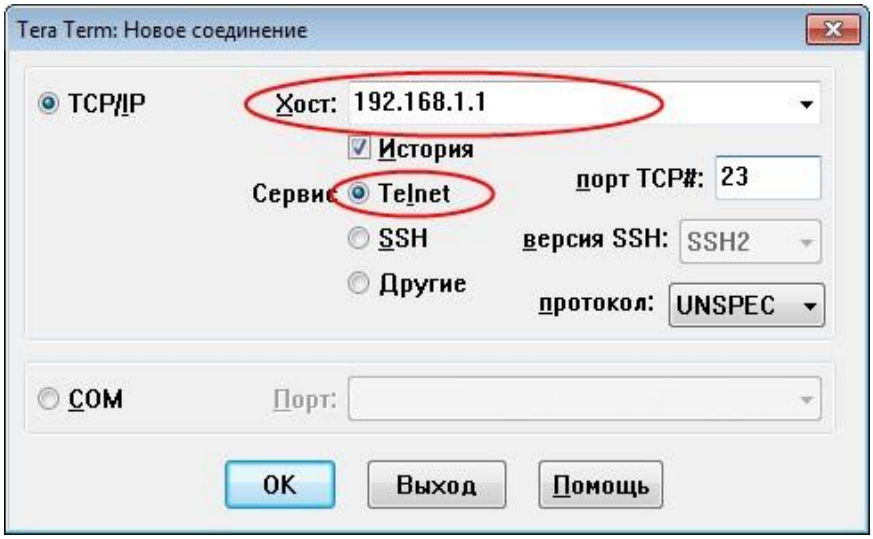
Примечание. По умолчанию доступ к Telnet из командной строки вWindows 7 отключён. Чтобы
активировать подключение по протоколу Telnet из окна командной строки, нажмите кнопку
Пуск >Панель управления>Программы>Программы и компоненты>Включение или отключение компонентов Windows. Установите флажок рядом с компонентом **Клиент Telnet** и нажмите кнопку **OK**.

Шаг 1: Откройте Wireshark и начните сбор данных в интерфейсе локальной сети.

Примечание. Если перехват данных в интерфейсе локальной сети запустить не удаётся, попробуйте открыть программу Wireshark с помощью параметра **Запуск от имени администратора**.

Шаг 2: Начните сеанс подключения к маршрутизатору по протоколу Telnet.

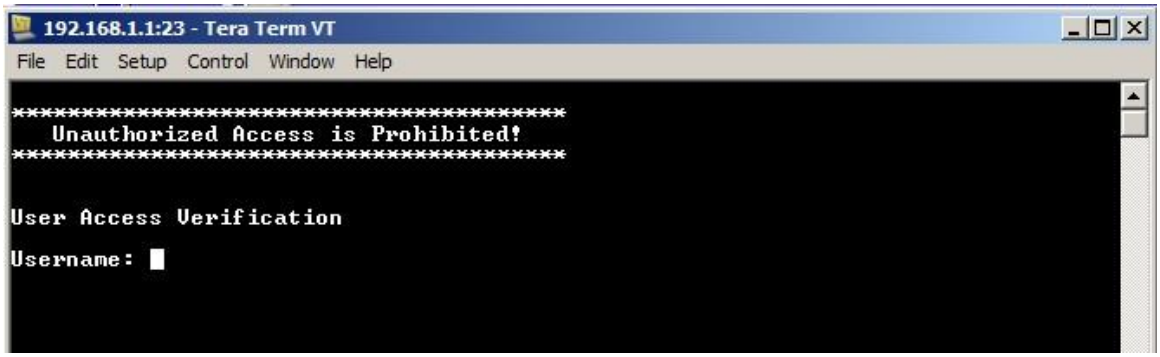
a. Запустите программу Tera Term, установите переключатель сервиса **Telnet**, а в поле «Host» введите **192.168.1.1**.



Какой порт TCP используется для сеансов Telnet по умолчанию?

_____

a. В окне командной строки после приглашения Username: (Имя пользователя) введите **admin**, а после Password: (Пароль) — **adminpass**. Эти запросы появляются потому, что командой **login local** вы настроили линии VTY на использование локальной базы учётных записей.



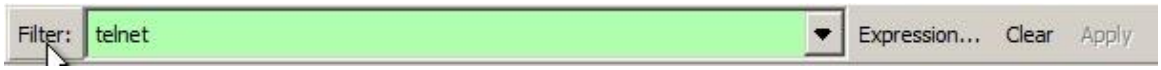
c. Введите команду **show run**.

R1# **show run**

d. Введите команду **exit**, чтобы завершить сеанс работы с протоколом Telnet и выйти из программы Tera Term.
R1# **exit**

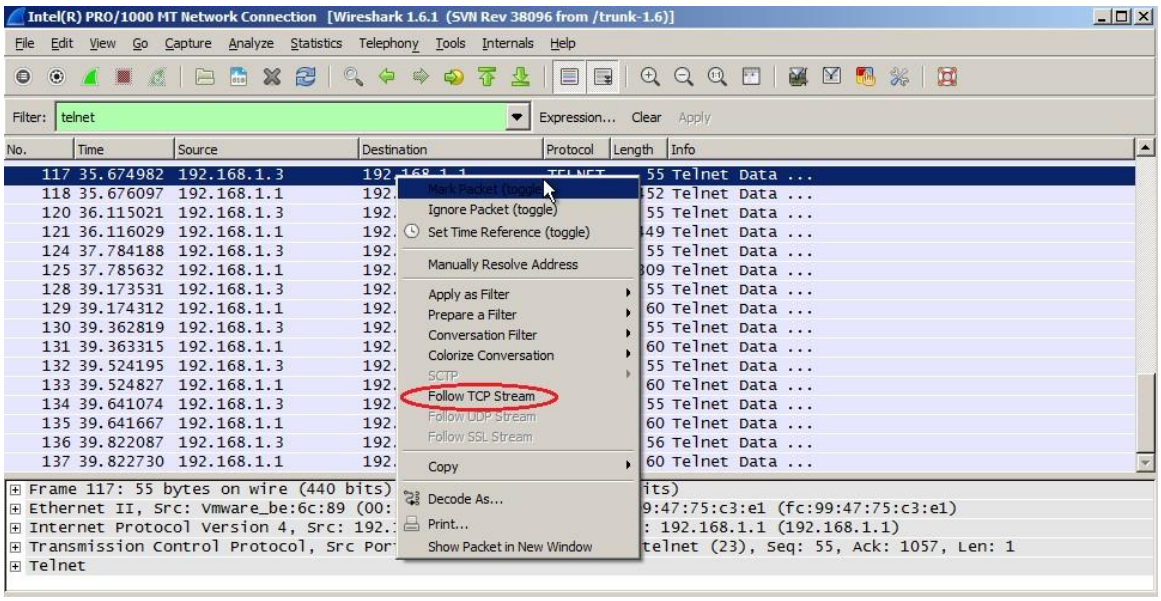
Шаг 3: Остановите сбор данных программой Wireshark.

Шаг 4: Примените один из фильтров Telnet для данных, собираемых программой Wireshark.



Шаг 5: Используйте функцию TCP в Wireshark для просмотра сеанса Telnet.

a. Нажмите правой кнопкой мыши на одну из строк **Telnet** в разделе **Packet list** (Список пакетов) программы Wireshark и выберите в раскрывающемся списке пункт **Follow TCP Stream** (Следить за TCP-потоком).



b. В окне Follow TCP Stream (Следить за TCP-потоком) отображаются данные о текущем сеансе подключения к маршрутизатору по протоколу Telnet. Весь сеанс связи (включая пароль) отображается открытым текстом. Обратите внимание на то, что введённые имя пользователя и команда **show run** отображаются с повторяющимися символами. Это связано с настройкой отображения в Telnet, которая позволяет выводить на экран символы, набираемые на клавиатуре.

Эталон ответа

Задание:

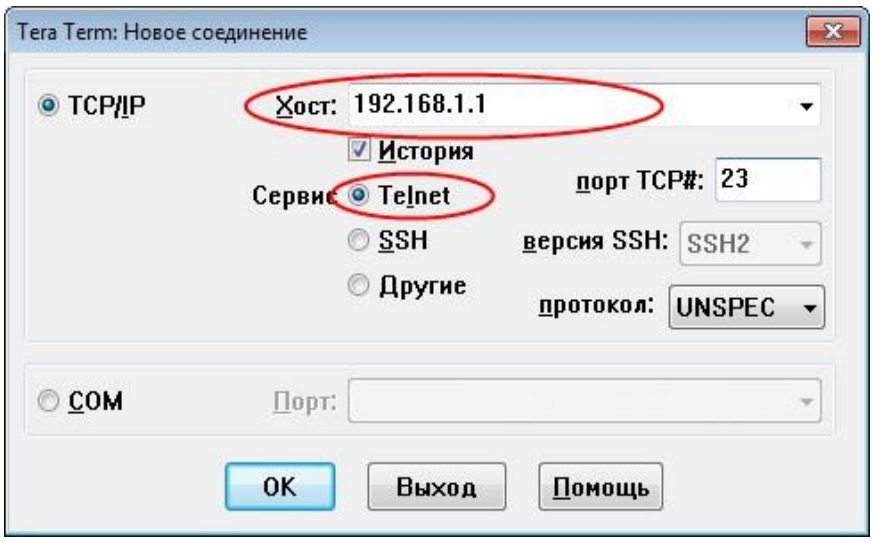
Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.1.1	255.255.255.0	Недоступно
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
ПК-A	Сетевой адаптер	192.168.1.3	255.255.255.0	192.168.1.1

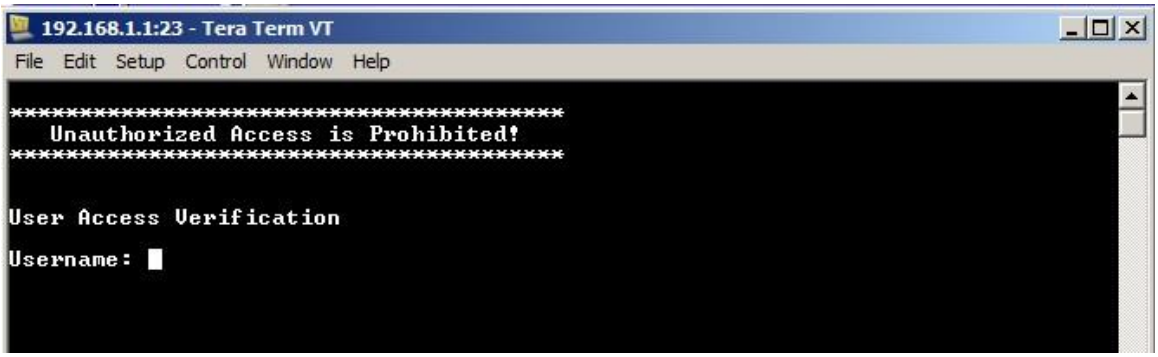
R1(config)# **username admin privilege 15 secret adminpass**

R1(config)#

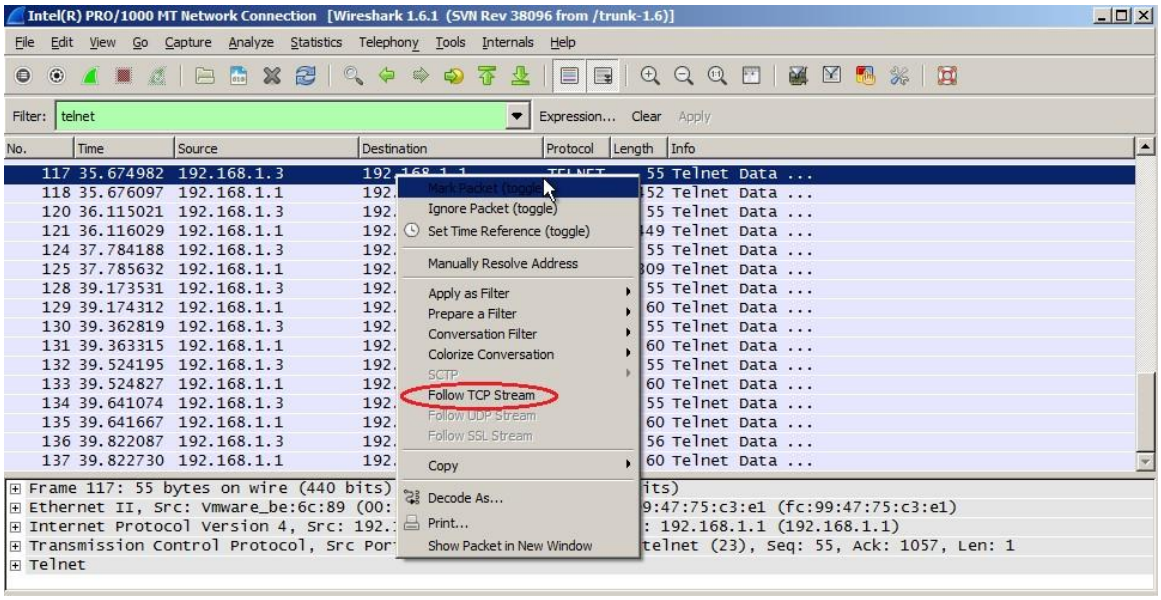
*Feb 6 23:24:43.971: End->Password:QHjxdsVkjtoP7VxKIcPsLdTiMIvyLkyjT1HbmYxZigc

R1(config)#





с. Введите команду **show run**.



Практическая работа № 45 Настройка безопасного доступа к маршрутизатору

Инструкция для обучающихся

Внимательно прочитайте задание. Проведите установку и настройку контроллеров.

Время выполнения – 90 минут.

Задание

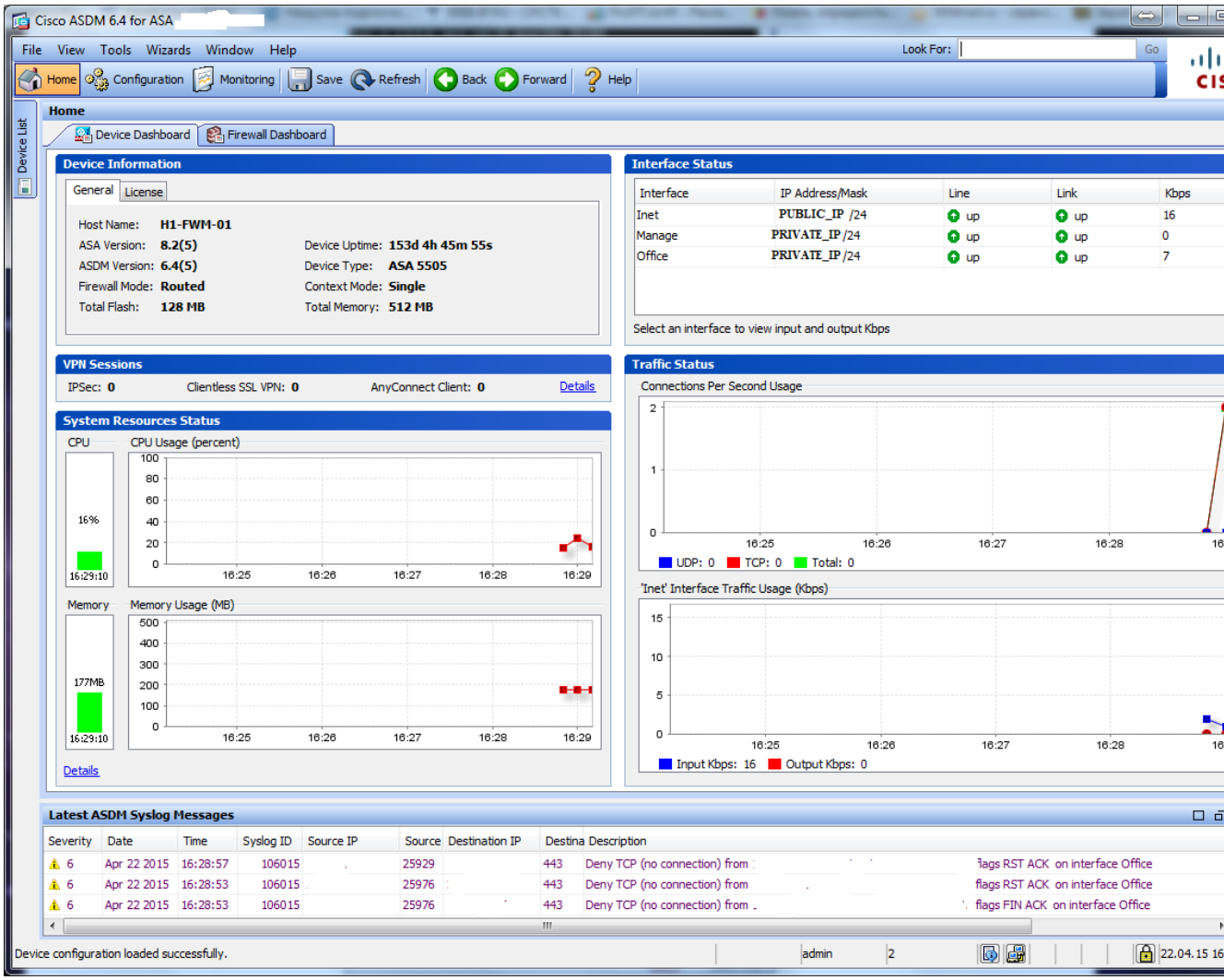
Задание:

Удаленный клиент при подключении через браузер непосредственно к cisco, скачивает специальное клиентское приложение Cisco AnyConnect Client на свой компьютер.

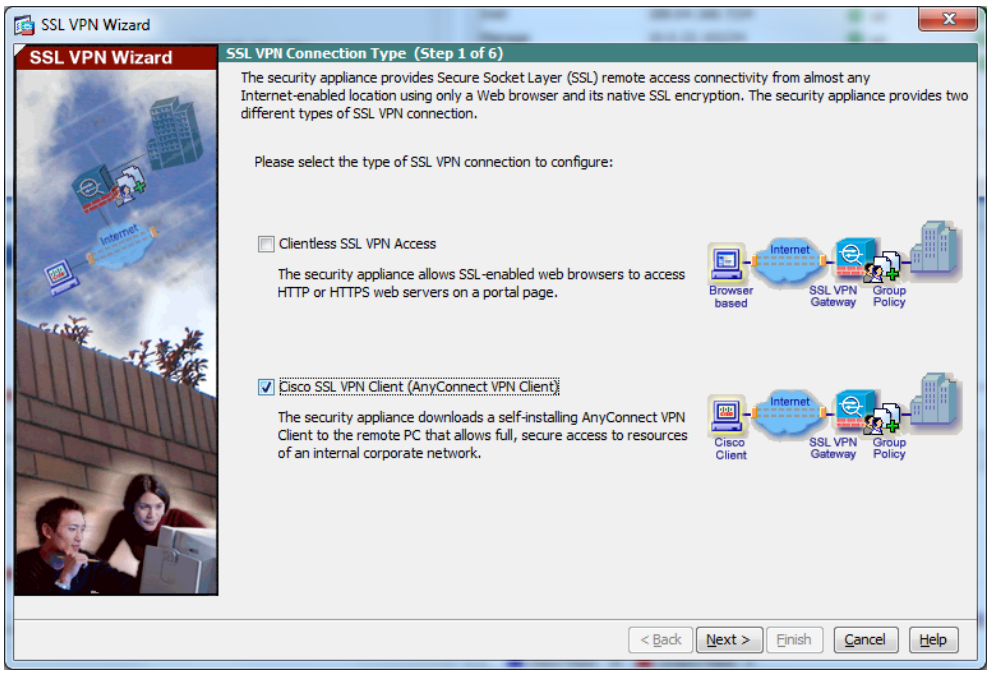
Будем рассматривать настройку SSL VPN параллельно 2-мя способами через графический интерфейс Cisco ASDM и через консоль CLI.
Используемое оборудование Cisco ASA-5505 (Security Appliance Software Version 9.1(6)6)

Настройка с помощью ASDM

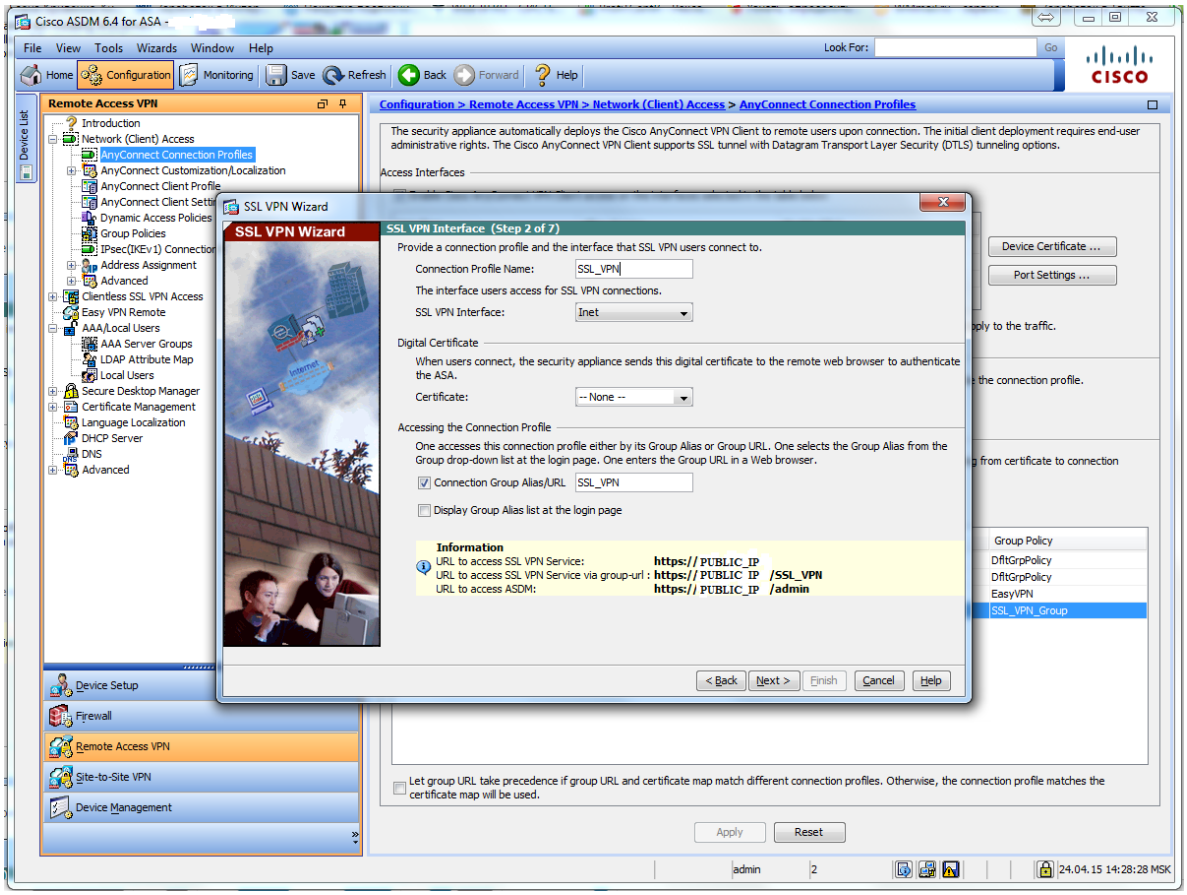
Запускаем Cisco ASDM, откроется основной экран



Здесь выбираем «Wizard»---«SSL VPN Wizard».



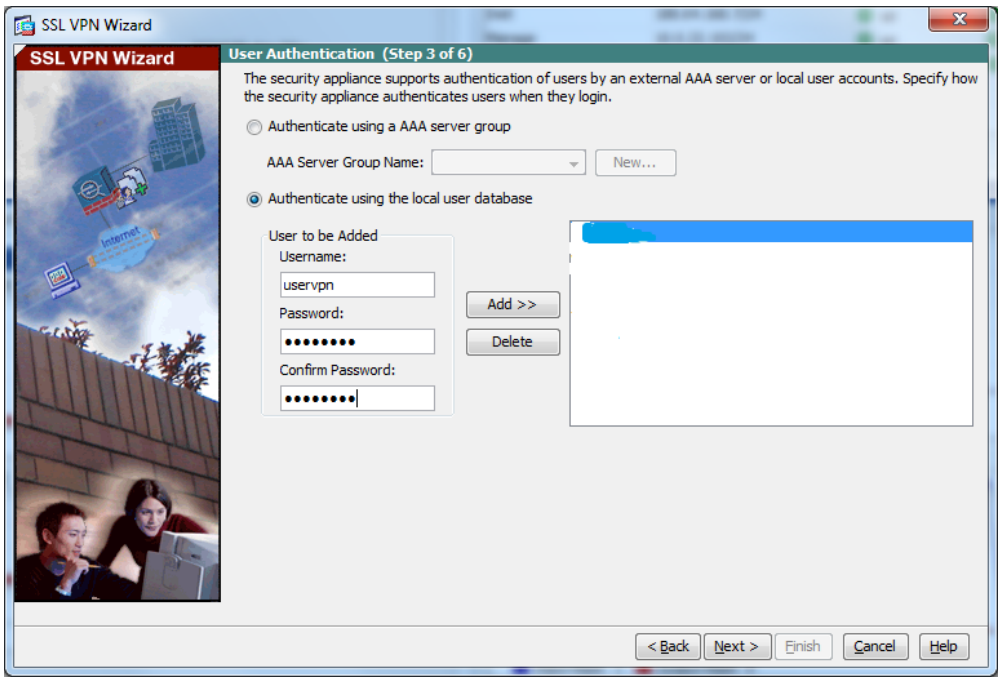
В открывшемся окне выбираем пункт «Cisco SSL VPN Client (AnyConnect VPN Client)» и нажимаем «Next»:



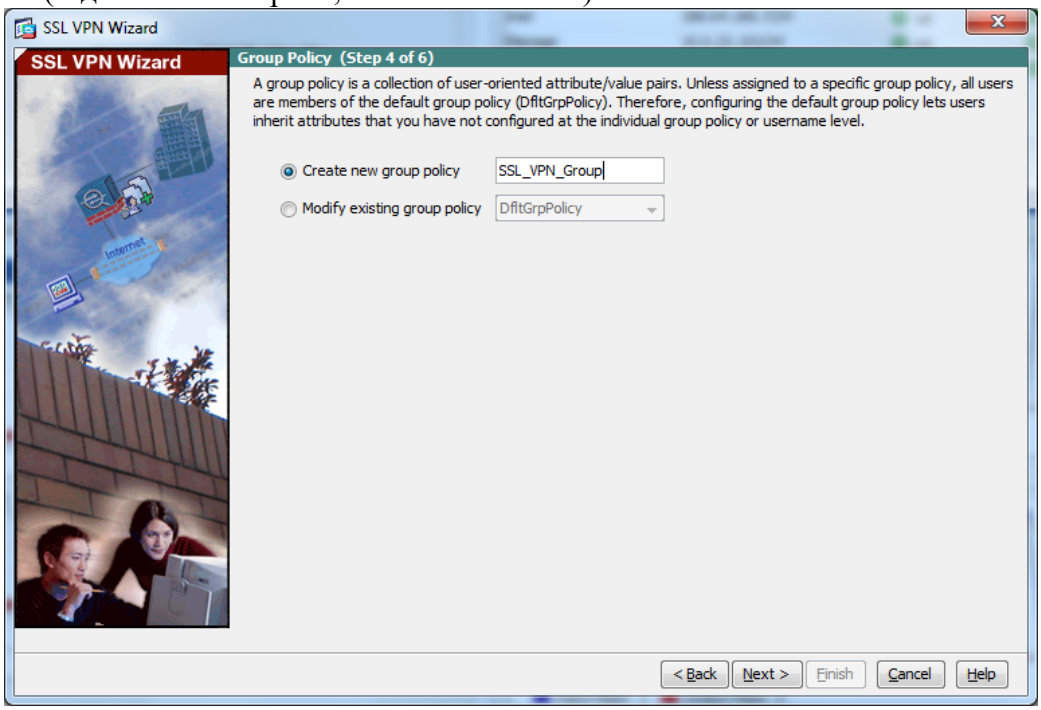
Здесь вводим имя нашего профайла, проверяем, что стоит имя нашего внешнего интерфейса (в данном случае Inet).

Если на cisco настроено несколько vpn подключений, то также указываем имя алиаса. Запоминаем доступы к SSL VPN Service и ASDM.

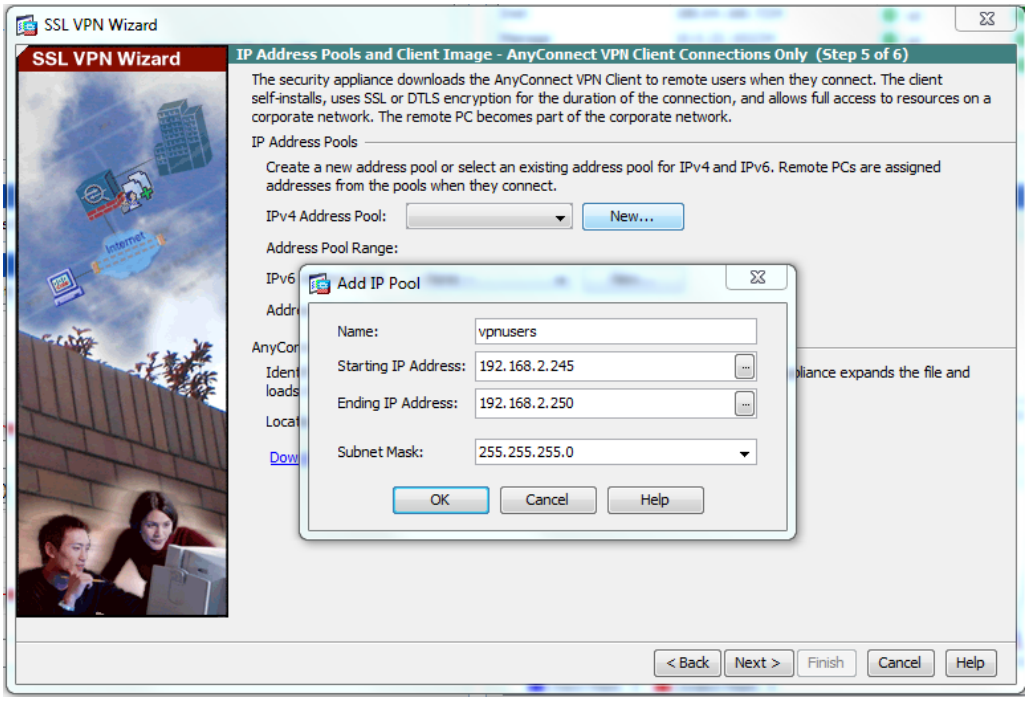
Затем нажимаем «Next»:



Ставим аутентификацию с использованием локальной базы и создаем нового пользователя (задаем имя и пароль, нажимаем «Add»). Затем нажимаем «Next»:

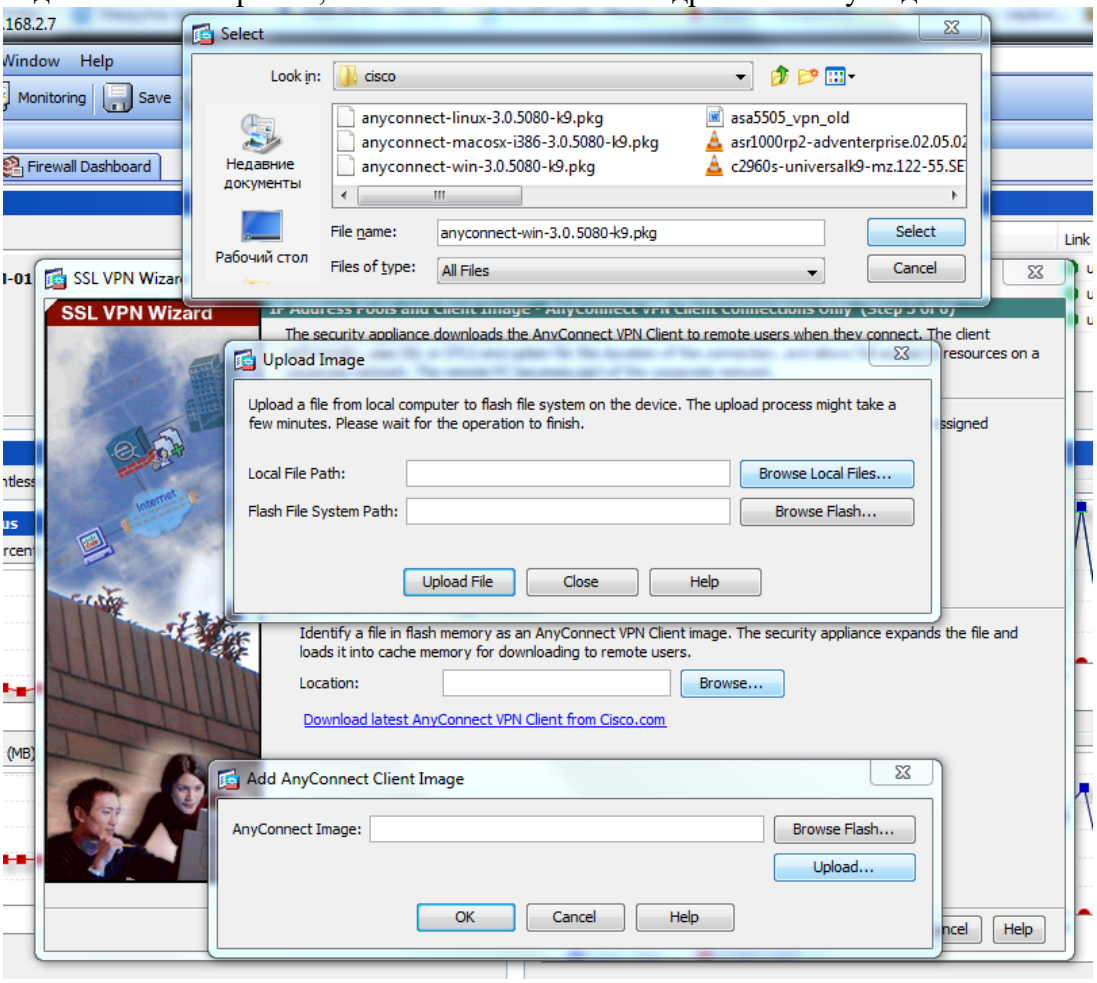


Здесь указываем имя отдельной групповой политики для SSL клиентов и нажимаем «Next»:



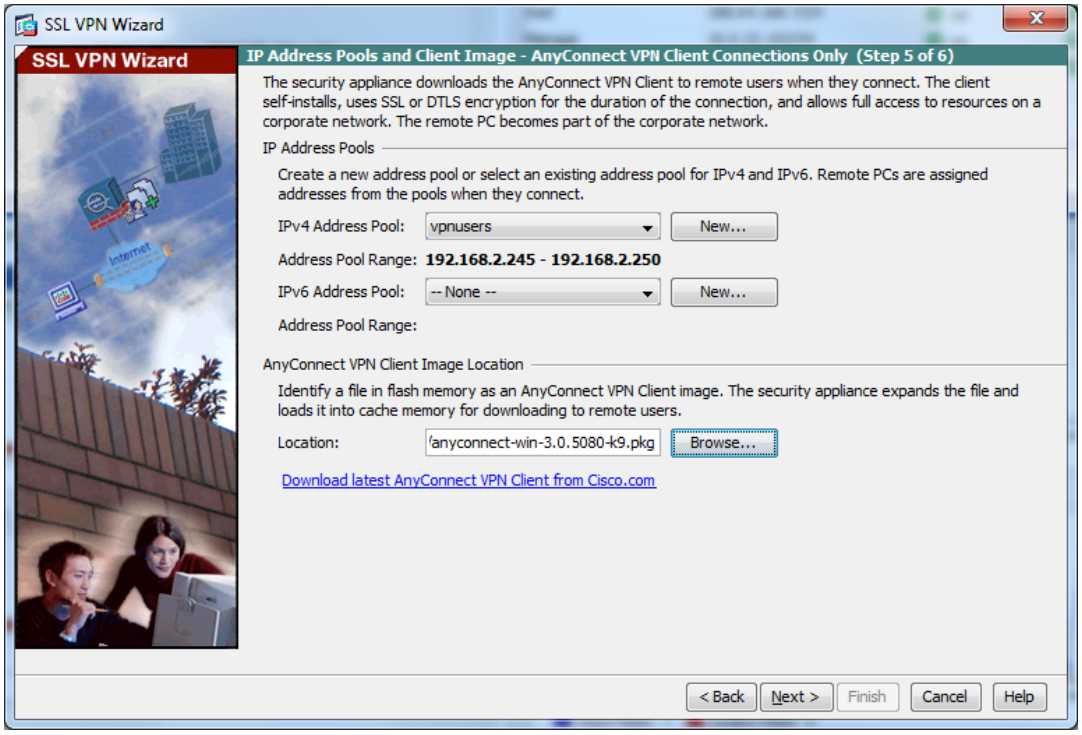
Здесь сначала создаем пул ip адресов, из которого будут выдаваться ip адреса для SSL VPN клиентов.

Задаем название pool-a, начальный и конечный адреса и маску подсети. Нажимаем «OK».

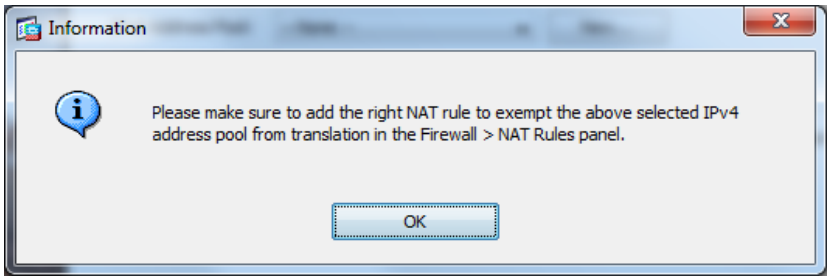


На этой же странице загружаем образ клиента Cisco AnyConnect под Windows.

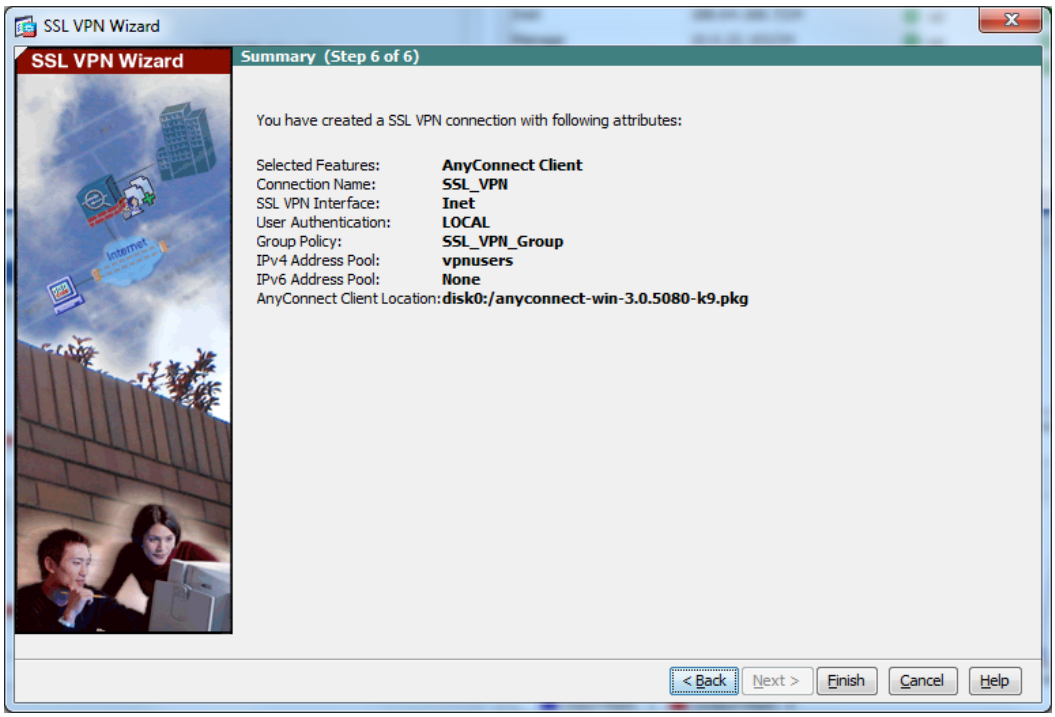
Для того чтобы его загрузить во flash cisco ASA, необходимо нажать в соответствующем пункте «Browse», в следующем появившемся окошке «Upload»,
затем в следующем окошке «Browse local files» и указать нужный файл из списка. Далее нажимаем по порядку «Select»---«Upload File»---«OK»
(после нажатий будут всплывать информационные окошки об успешном выполнении). В итоге, получиться вот такое окно:



Нажимаем «Next»:

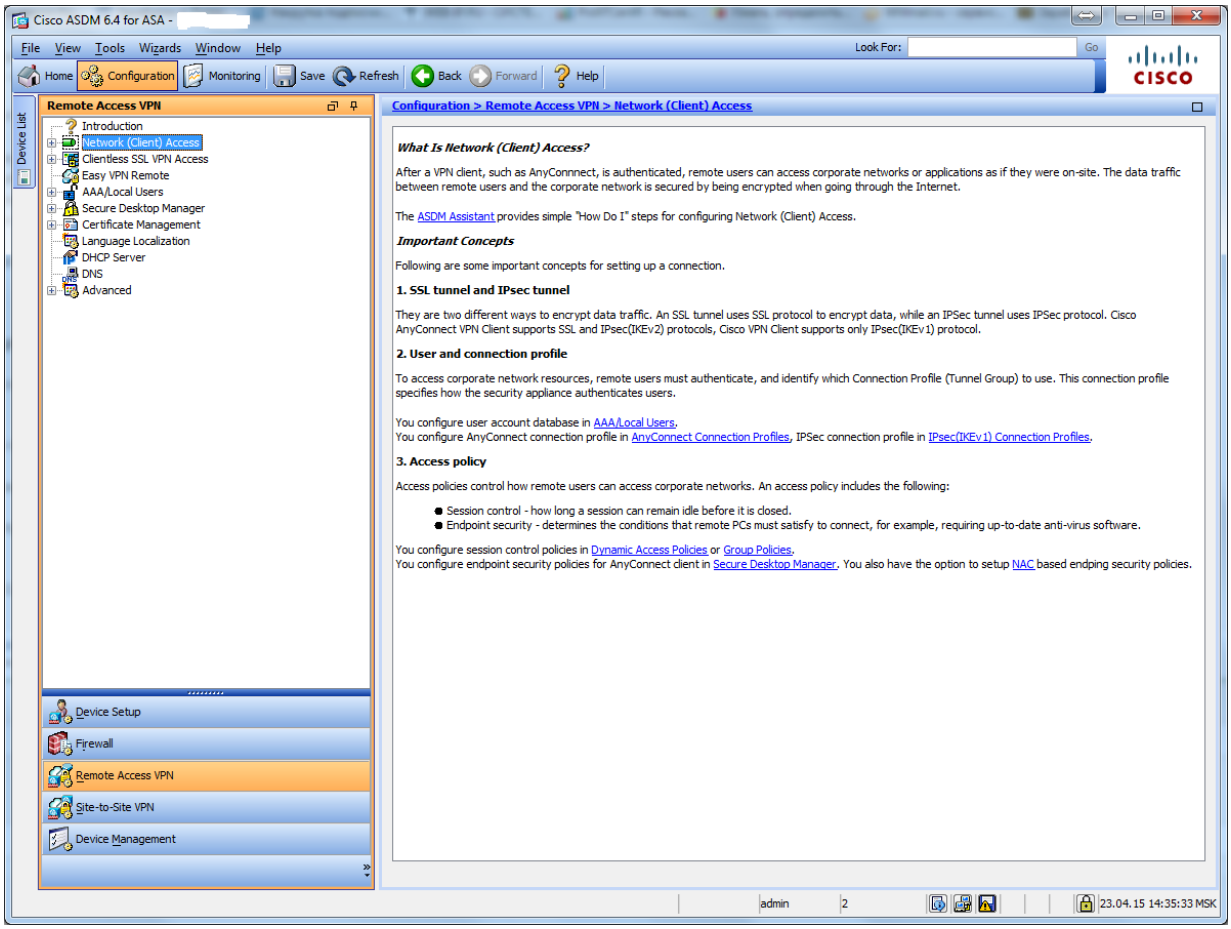


Это окно напоминает, что адреса, которые используются в пуле не должны попадать под политики NAT, если он настроен на cisco.
Нажимаем «OK».



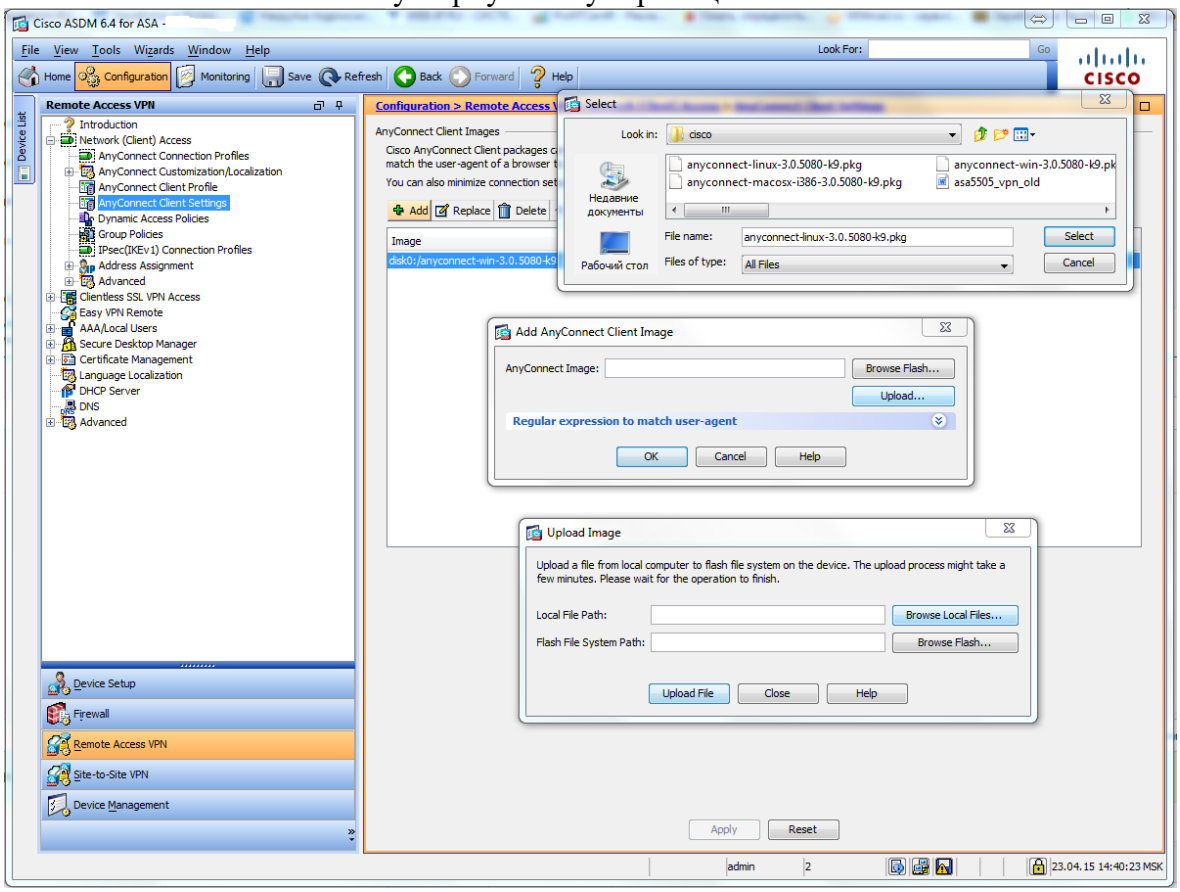
Здесь показаны все наши настройки, которые будут сконфигурированы. Нажимаем «Finish».

Более точные настройки (не через Wizard) можно посмотреть в разделе Configuration - Remote Access VPN

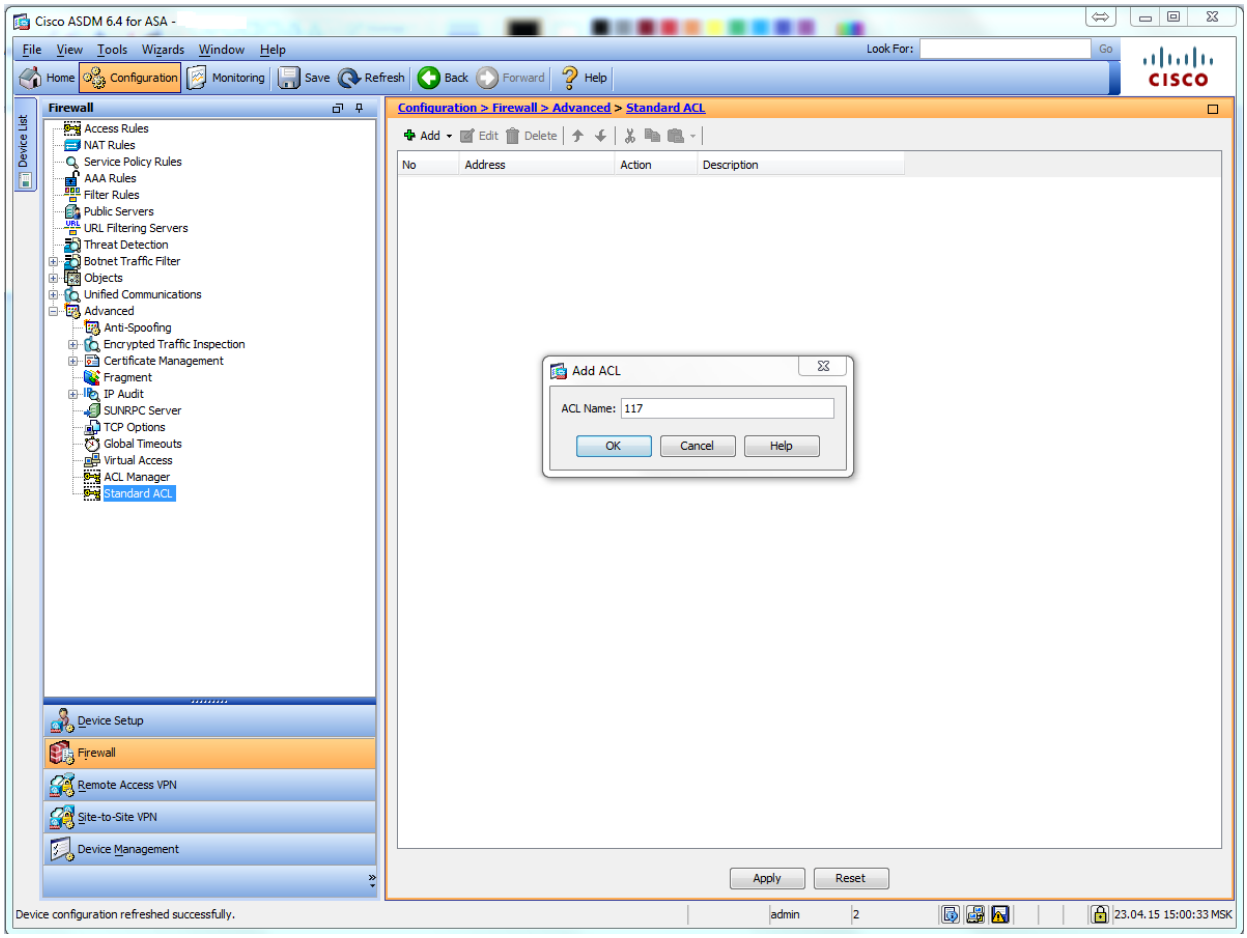


Нам необходимо добавить образы клиента под Mac и Linux, для этого заходим в раздел

Network (Client) Access - AnyConnect Client Settings,
Здесь мы увидим уже загруженный образ клиента под Windows, нажимаем кнопку с зеленым плюсиком Add, и по аналогии как в Wizard добавляем образы под Linux и Mac.
После чего нажимаем кнопку "Aplly" внизу страницы.

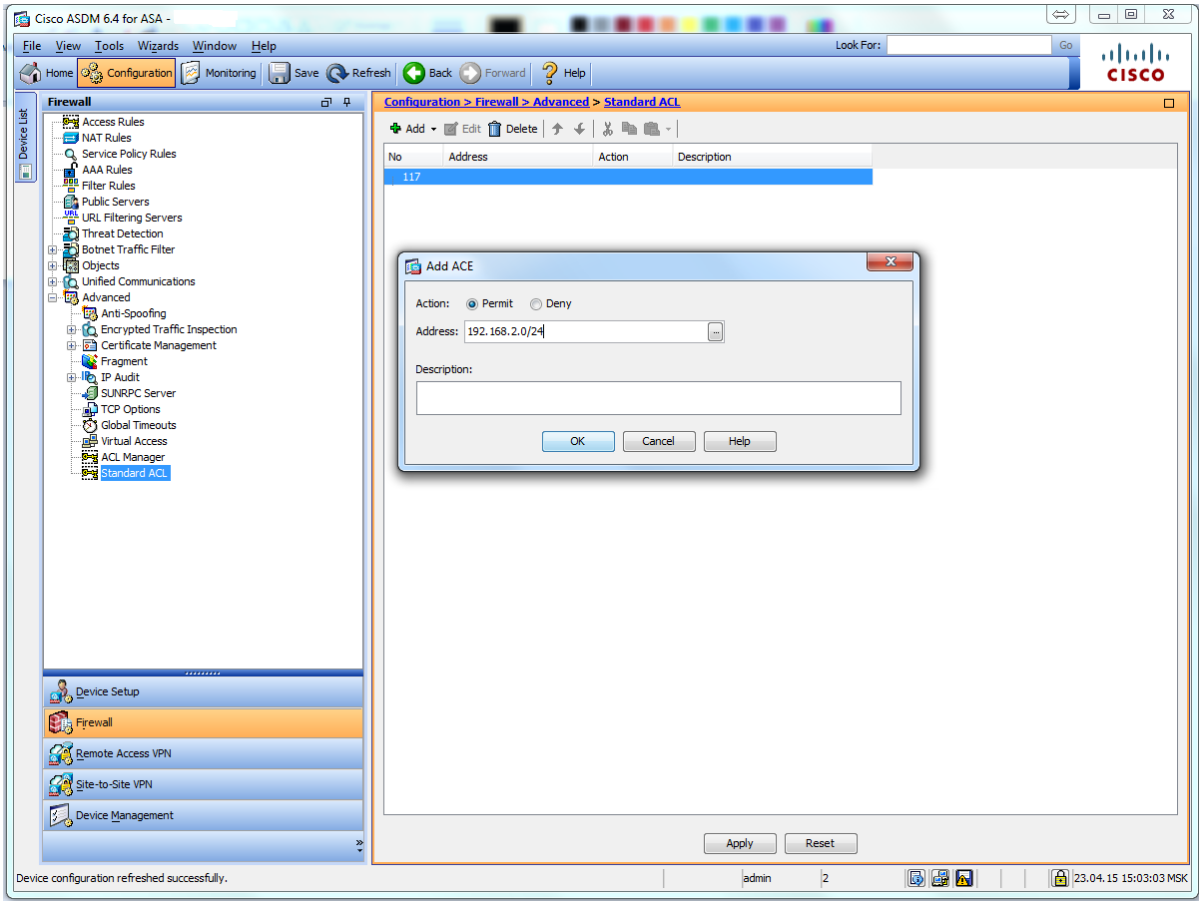


По умолчанию весь трафик клиента попадает в туннель, так как эта настройка наследуется из политики по умолчанию.
Для того чтобы указать какой трафик должен попадать в туннель, необходимо создать ACL, который будет его описывать и изменить политику туннелирования.
Эта функция называется split tunneling.
Для групповой политики SSL_VPN в туннель будет попадать только трафик, который идет в сеть 192.168.2.0/24.
Сначала создадим access-list, под который будет попадать трафик 192.168.2.0/24.
Для этого заходим в раздел Configuration - Firewall - Advanced - Standart ACL, нажимаем кнопку с зеленым плюсиком Add, в выпадающем списке выбираем Add ACL.
В появившемся окне вводим номер ACL и нажимаем OK.



Теперь нужно добавить содержимое для этого листа, это будет одна строка, встаем на наш аксесс лист 117, нажимаем кнопку с зеленым плюсиком Add, в выпадающем списке выбираем Add ACL.
Появится окно для ввода содержимого, Action оставляем Permit, в строку address вводим 192.168.2.0/24. Нажимаем OK и Aplly внизу страницы.

Аксесс-лист готов.



Теперь настраиваем split tunneling. Для этого нужно зайти в настройки самой групповой политики.

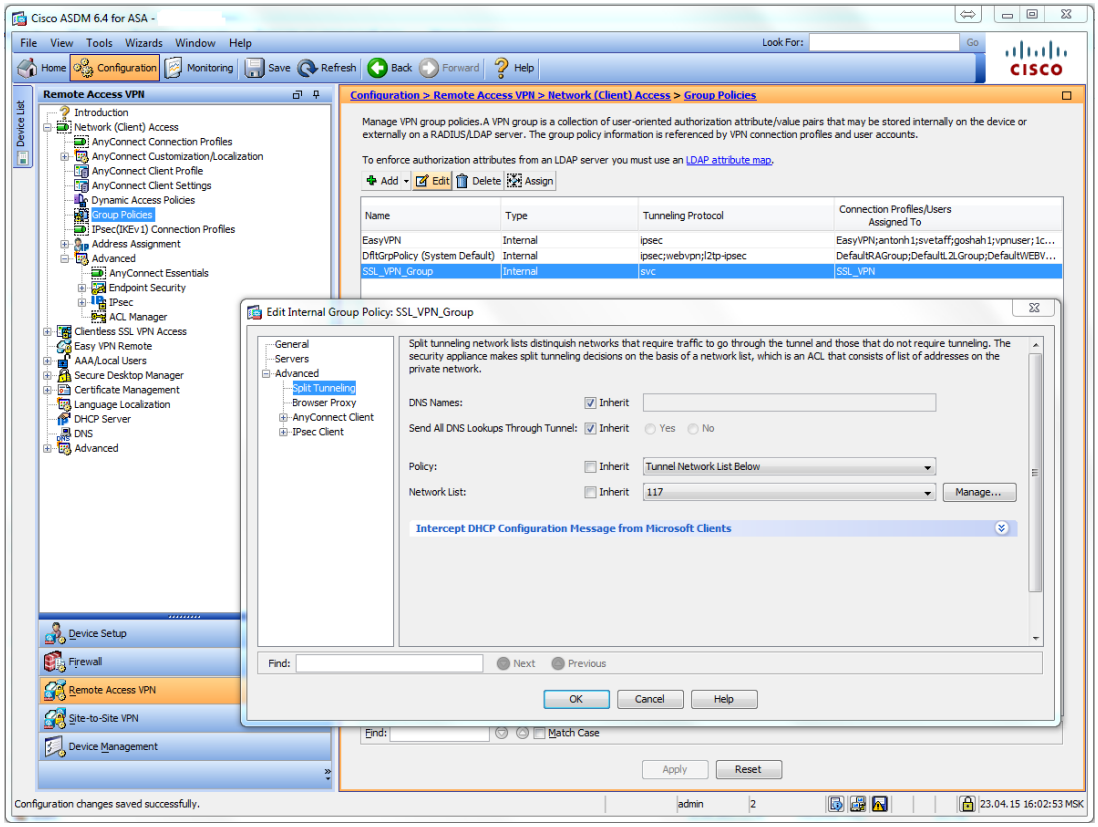
Идем Configuration - Remote Access VPN - Network (Client) Access - Group Policies.

В открывшемся окне в списке политик находим нашу SSL_VPN_Group. Встаем на нее, нажимаем кнопку Edit.

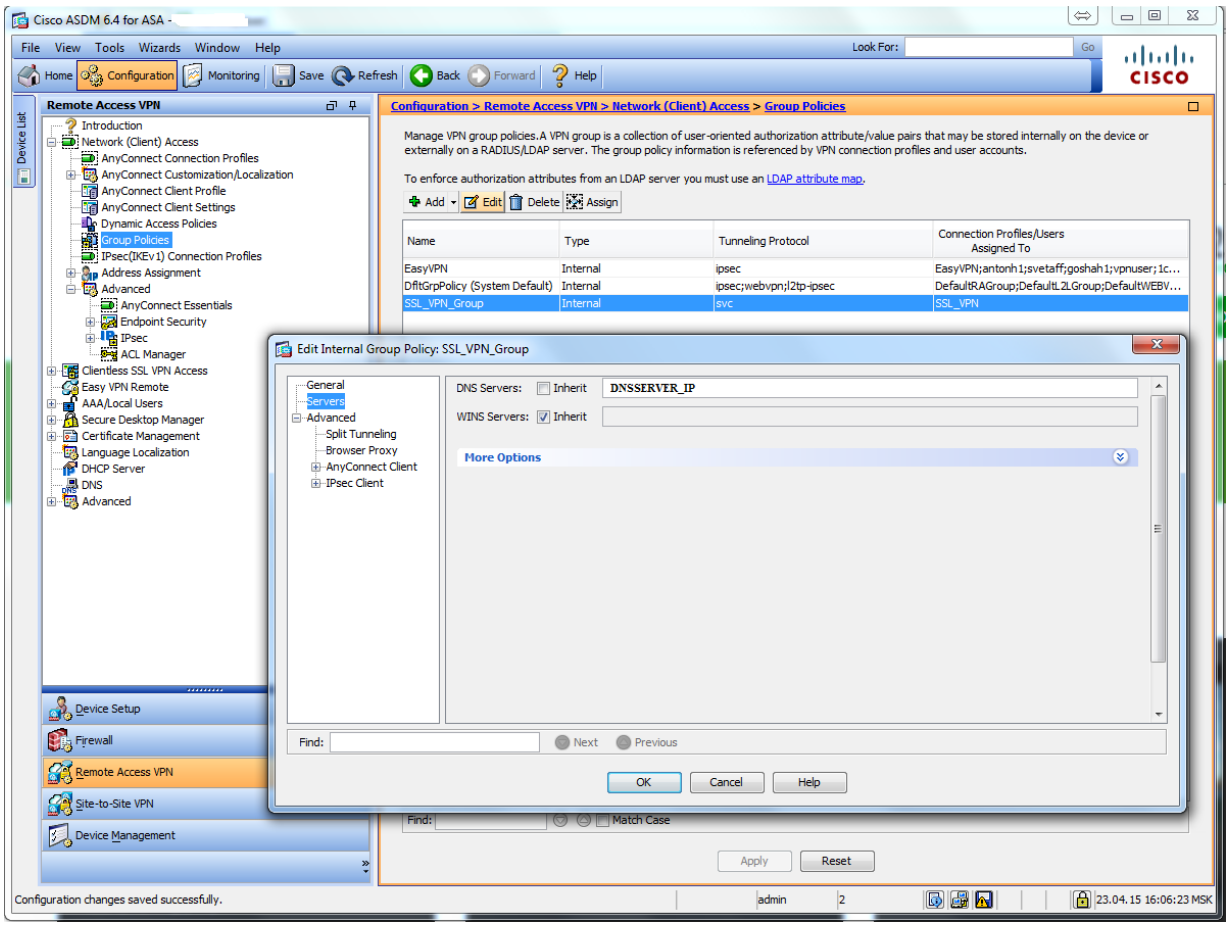
Откроется окно настроек групповой политики. Слева разворачиваем вкладку Advanced, выбираем Split Tunneling.

Напротив записи Policy убираем галку Inherit, и в выпадающем списке выбираем Tunnel Network List Bellow.

Напротив записи Network List убираем галку Inherit, и в выпадающем списке выбираем аксесс-лист 117. Нажимаем OK и Aplly внизу страницы.



Если имеется локальный DNS сервер также нужно прописать его в групповой политике. Идем туда же в настройки групповой политики. Слева выбираем Servers. Напротив строки DNS servers убираем галку Inherit и вписываем адрес локального DNS сервера. Нажимаем OK и Aplly внизу страницы.



Настройка с помощью CLI

Теперь посмотрим какие настройки появились у нас в CLI.

Акксесс-лист для опции Split Tunneling.

access-list 117 standard permit 192.168.2.0 255.255.255.0
Пул для ip адресов

ip local pool vpnusers 192.168.2.245-192.168.2.250 mask 255.255.255.0

Настройки webvpn. Включение svc. Интерфейс Inet. Пути к образам клиентов.
webvpn
 enable Inet
 anyconnect-essentials
 svc image disk0:/anyconnect-win-3.0.5080-k9.pkg 1
 svc image disk0:/anyconnect-linux-3.0.5080-k9.pkg 2
 svc image disk0:/anyconnect-macosx-i386-3.0.5080-k9.pkg 3
 svc enable
 tunnel-group-list enable

Настройки профайла.
tunnel-group SSL_VPN type remote-access
tunnel-group SSL_VPN general-attributes
 address-pool vpnusers
 default-group-policy SSL_VPN_Group

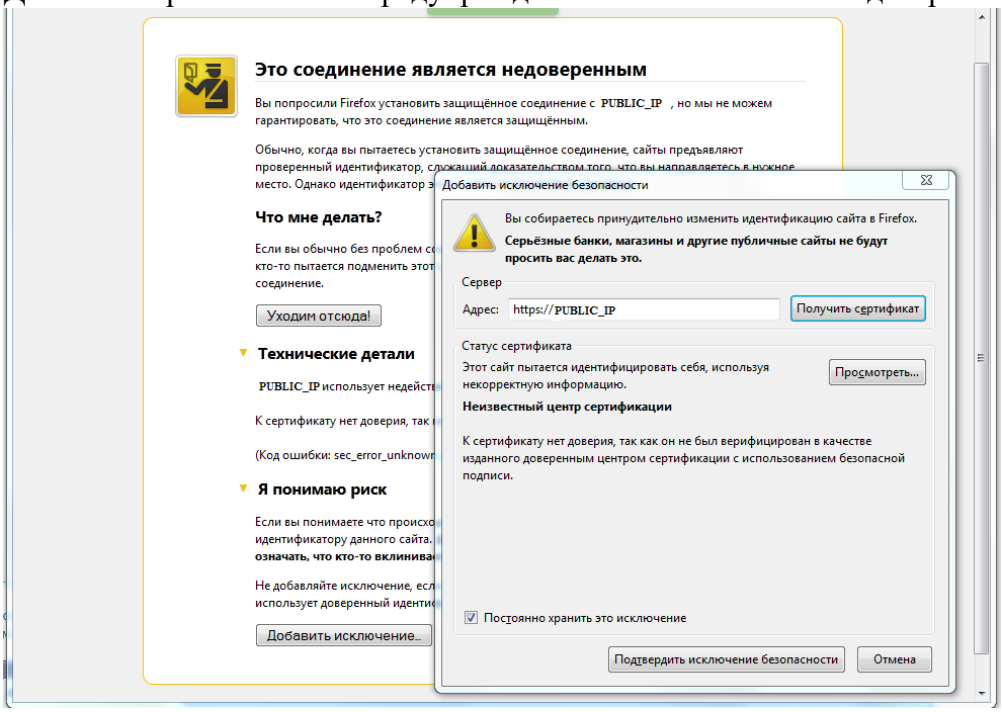
```
tunnel-group SSL_VPN webvpn-attributes
 group-alias SSL_VPN enable
```

Настройки групповой политики. DNS сервер. Опция split-tunnel.

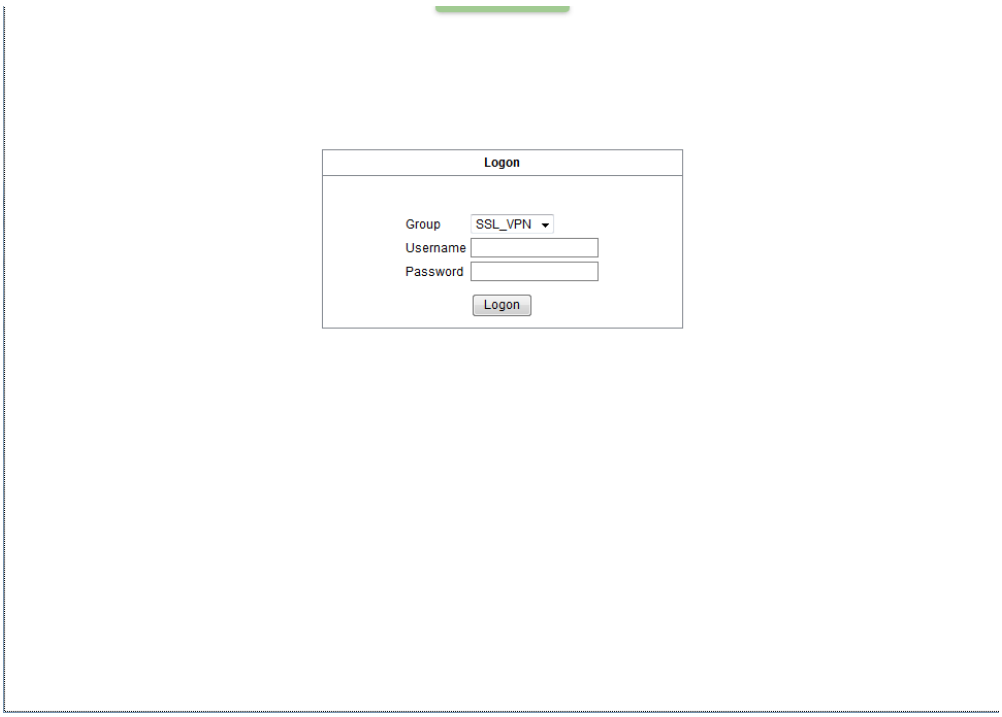
```
group-policy SSL_VPN_Group internal
group-policy SSL_VPN_Group attributes
 dns-server value DNSSERVER_IP
 vpn-tunnel-protocol svc
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value 117
 default-domain none
```

Установка клиента

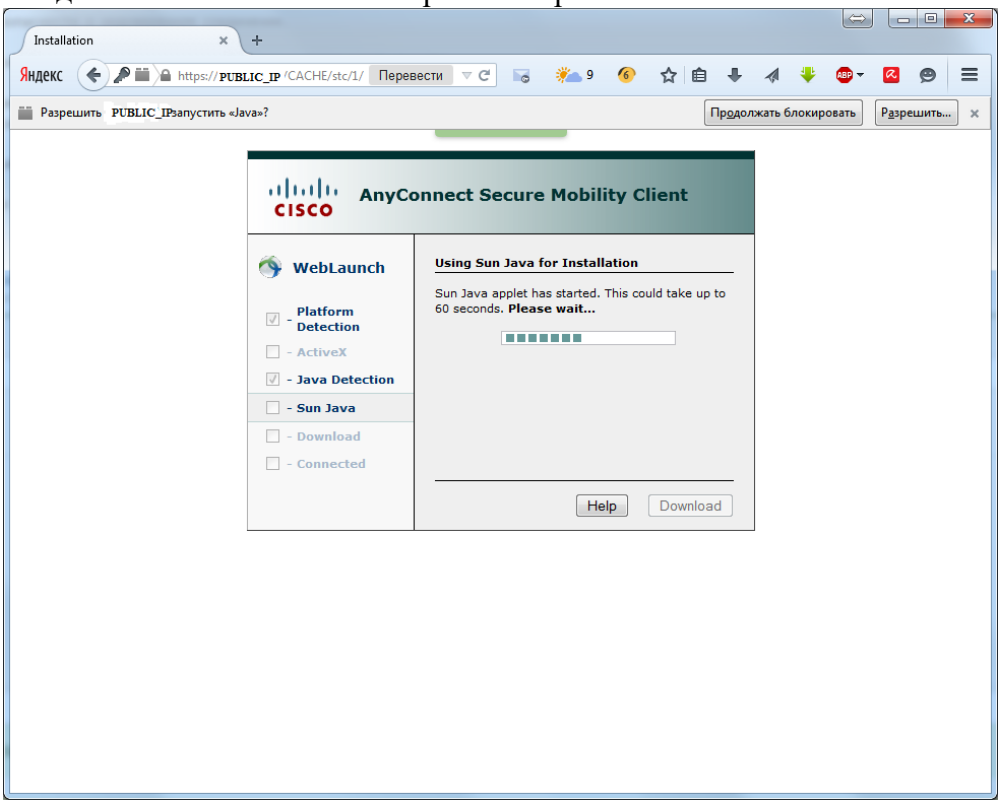
Заходим в браузер. В адресной строке набираем https://PUBLIC_IP
Должно открыться окно с предупреждением безопасности о недоверенном соединении.



Со всем соглашаемся (устанавливаем (получаем) сертификат и добавляем источник в исключения).
Нажимаем на «Подтвердить исключение безопасности» и у вас откроется следующее окно:

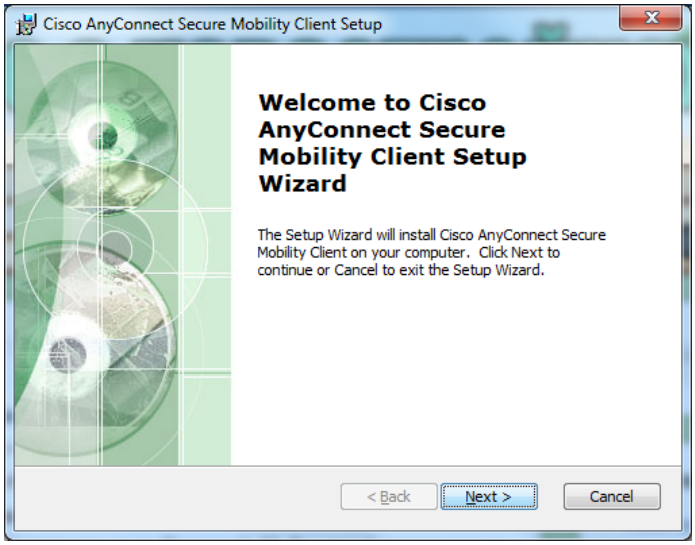


Вводим имя пользователя и пароль. Откроется такое окно:



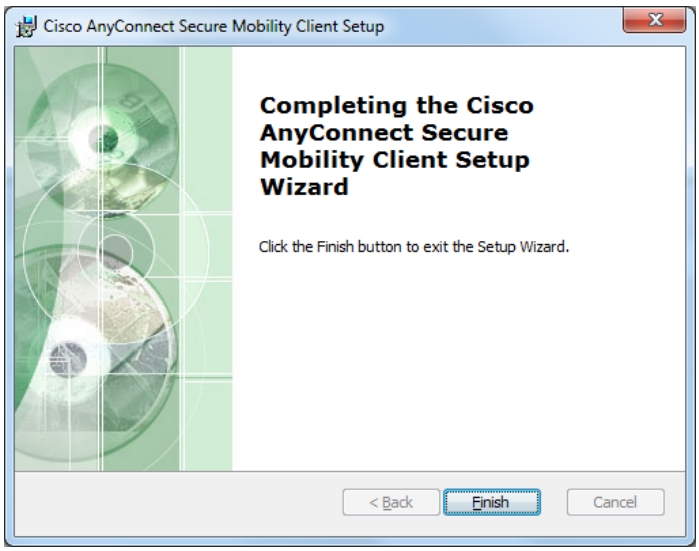
Программа установки пытается определить установленную ОС, для того чтобы запустить установку Cisco AnyConnect Client.
В результате программа предложить скачать подходящий под ОС образ:

Скачиваем образ и запускаем программу установки:



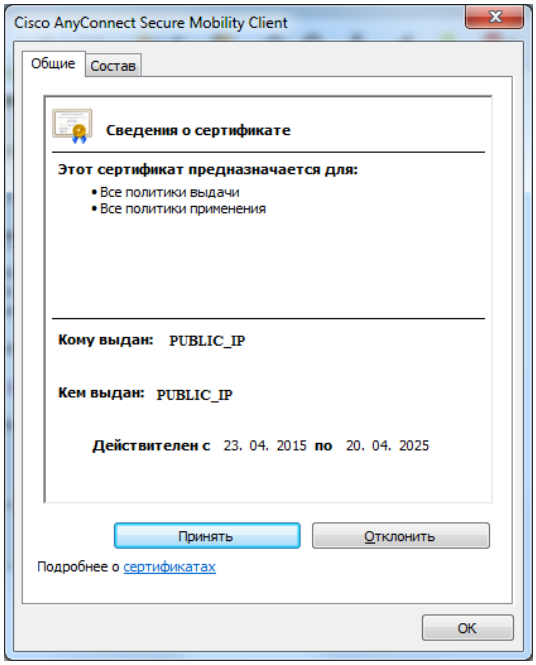
Нажимаем Next, принимаем лицензионное соглашение, Next, Install. Начнется установка.

Нажимаем Finish. Установка завершена.



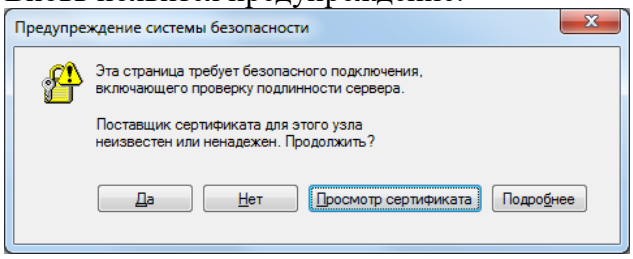
Запускаем программу. Справа внизу появится окошко.

Вводим ip-адрес для подключения, нажимаем Connect.
Появится окно с информацией о сертификате.



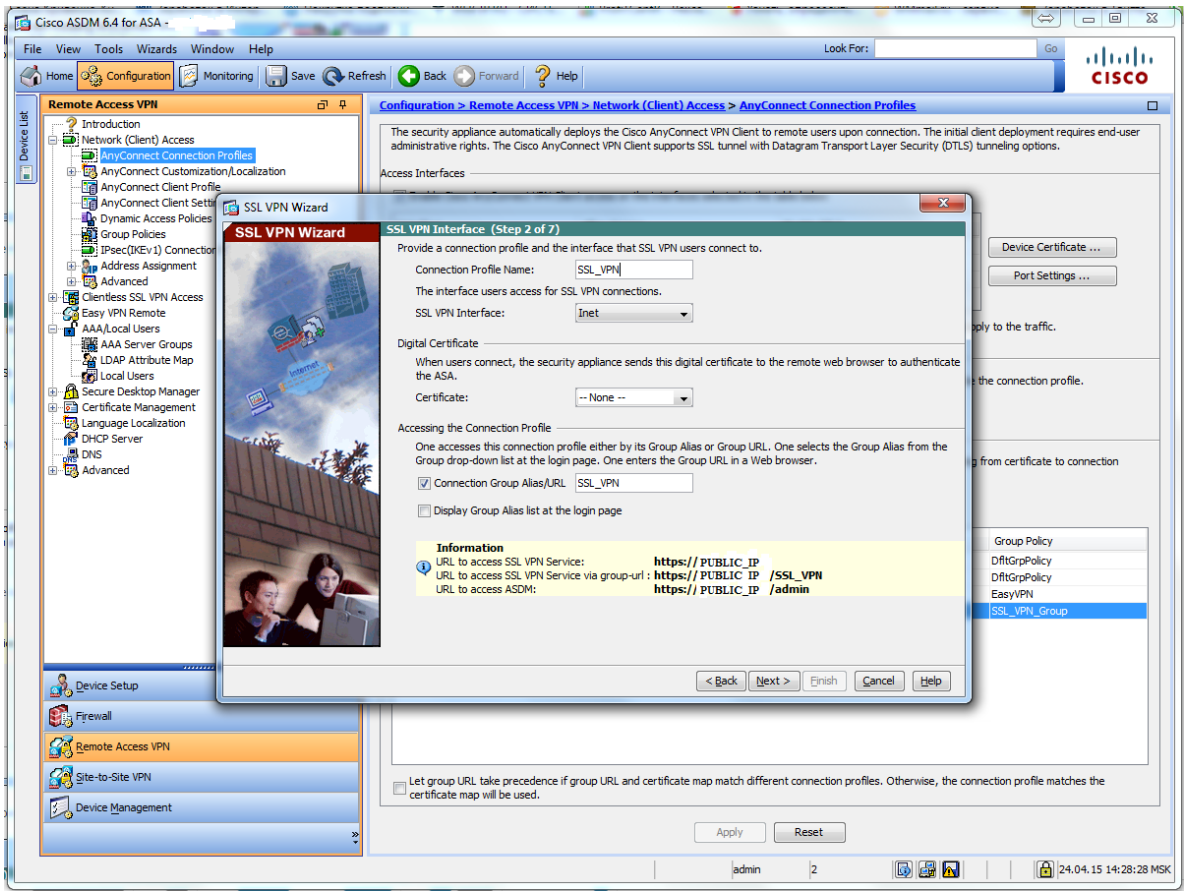
Нажимаем "Принять". Появится окно с запросом логина и пароля.

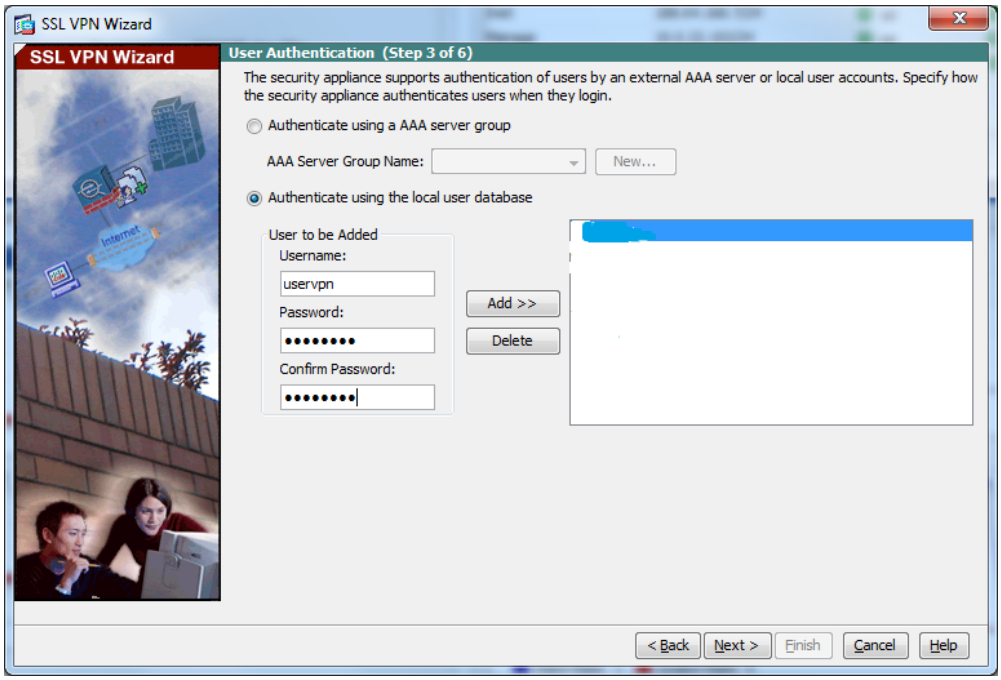
Вновь появится предупреждение:

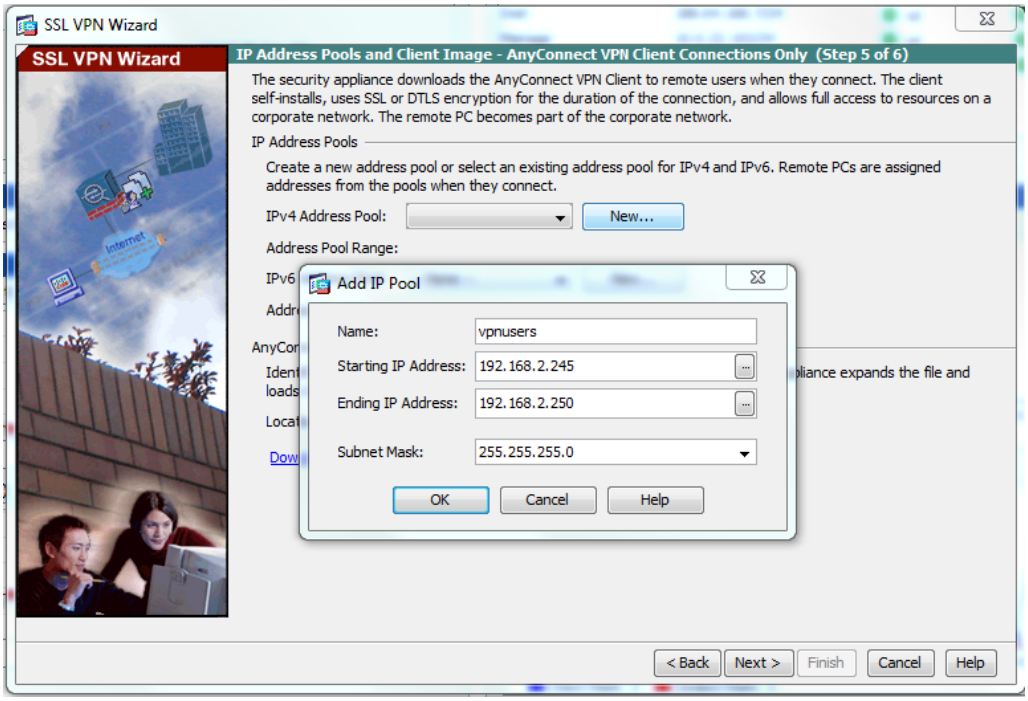


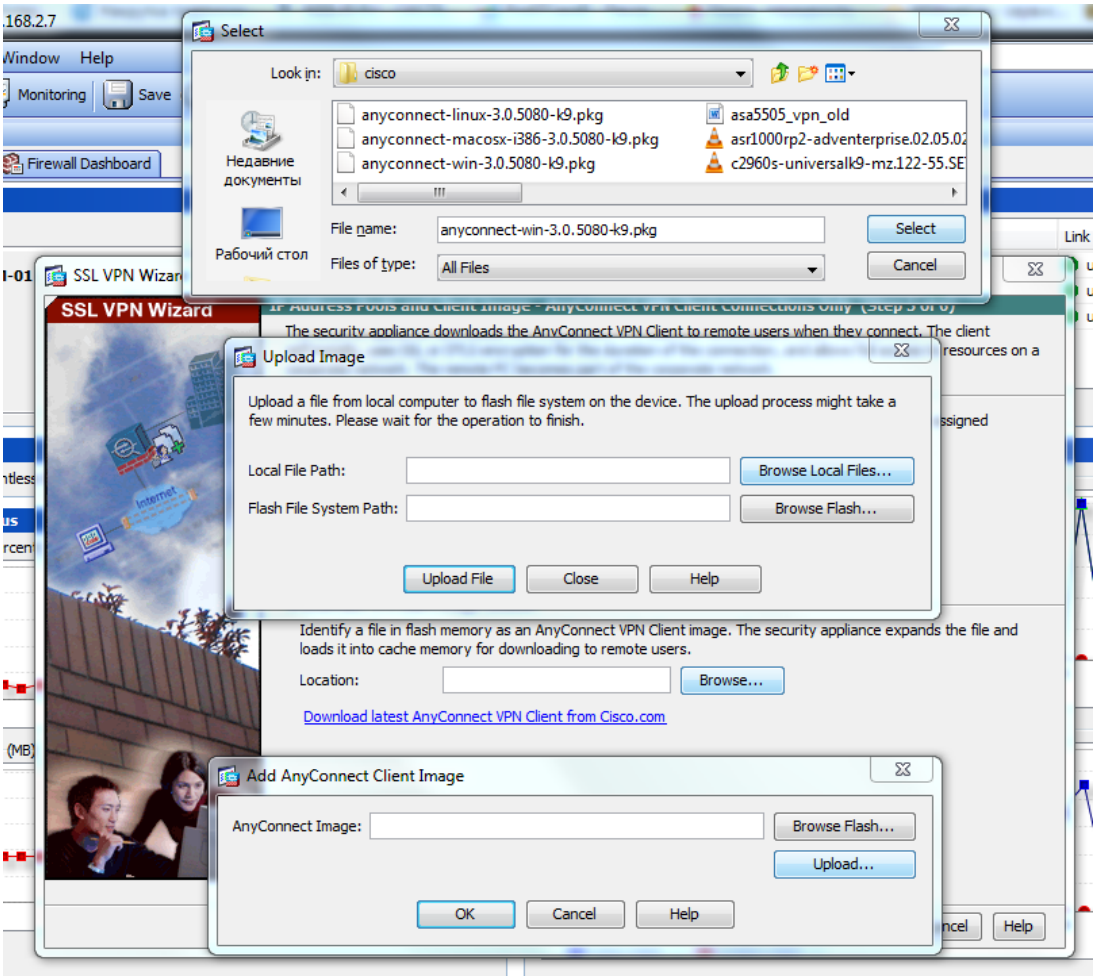
Нажимаем Принять, начнется подключение. В результате окно справа внизу примет вид. VPN подключен.

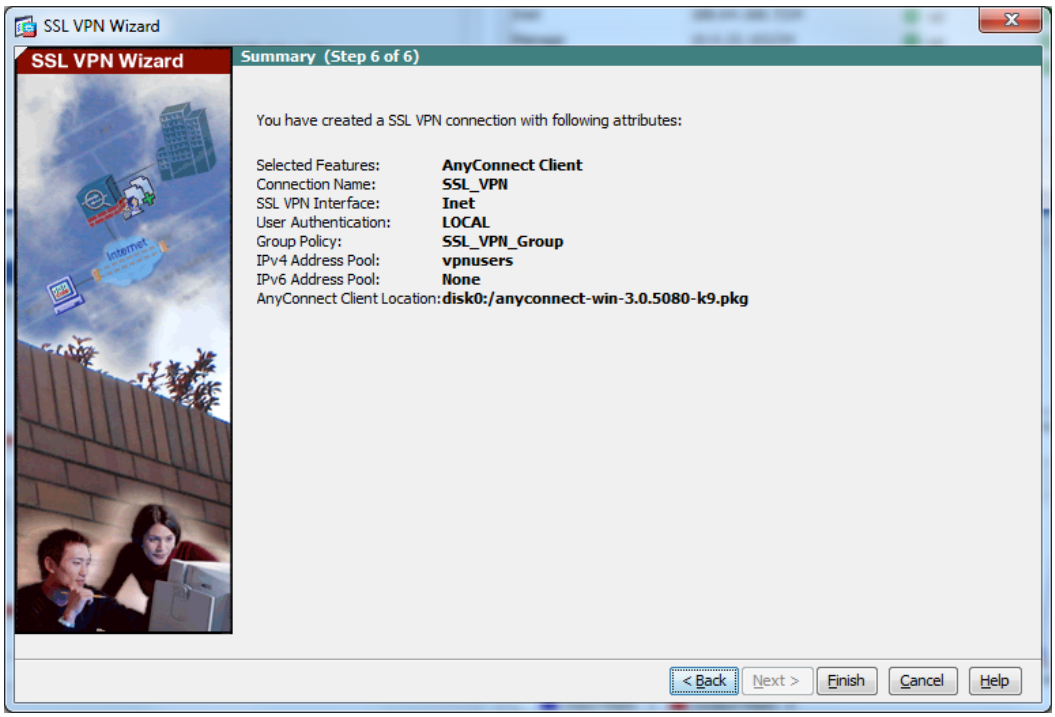
Эталон ответа:

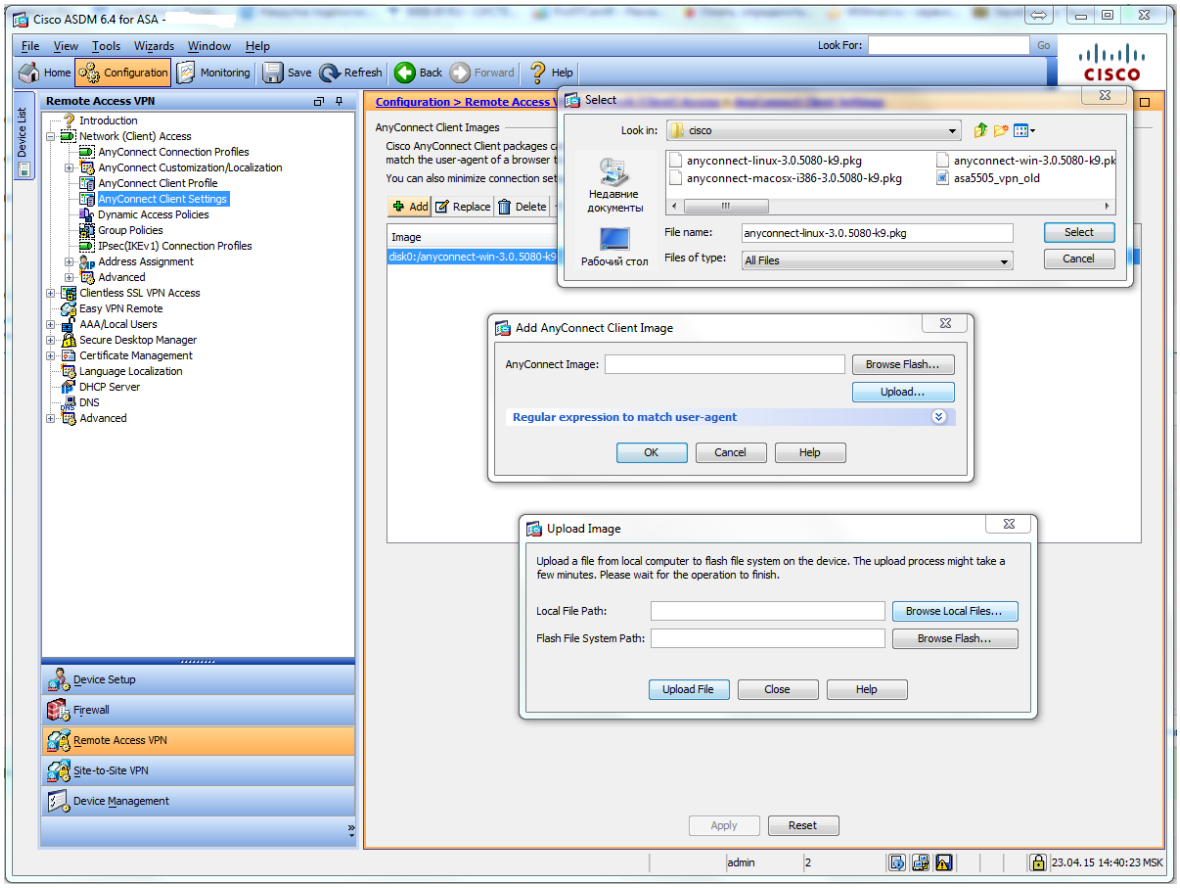

Cisco ASDM 6.4 for ASA -
File View Tools Wizards Window Help
Look For:
Home Configuration Monitoring Save Refresh Back Forward Help
Remote Access VPN
Introduction
Network (Client) Access
AnyConnect Connection Profiles
AnyConnect Customization/Localization
AnyConnect Client Profile
AnyConnect Client Sett
Dynamic Access Policies
Group Policies
IPsec(IKEv1) Connectio
Address Assignment
Advanced
Clientless SSL VPN Access
Easy VPN Remote
AAA/Local Users
AAA Server Groups
LDAP Attribute Map
Local Users
Secure Desktop Manager
Certificate Management
Language Localization
DHCP Server
DNS
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles
The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.
Access Interfaces
Device Certificate ...
Port Settings ...
Group Policy
DfltGrpPolicy
DfltGrpPolicy
EasyVPN
SSL_VPN_Group
Let group URL take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile matches the certificate map will be used.
Apply
Reset
admin
2
24.04.15 14:28:28 MSK
SSL VPN Wizard
SSL VPN Wizard
SSL VPN Interface (Step 2 of 7)
Provide a connection profile and the interface that SSL VPN users connect to.
Connection Profile Name:
SSL_VPN
The interface users access for SSL VPN connections.
SSL VPN Interface:
Inet
Digital Certificate
When users connect, the security appliance sends this digital certificate to the remote web browser to authenticate the ASA.
Certificate:
-- None --
Accessing the Connection Profile
One accesses this connection profile either by its Group Alias or Group URL. One selects the Group Alias from the Group drop-down list at the login page. One enters the Group URL in a Web browser.
Connection Group Alias/URL
SSL_VPN
Display Group Alias list at the login page
Information
URL to access SSL VPN Service: https:// PUBLIC_IP
URL to access SSL VPN Service via group-url : https:// PUBLIC_IP /SSL_VPN
URL to access ASDM: https:// PUBLIC_IP /admin
< Back
Next >
Finish
Cancel
Help

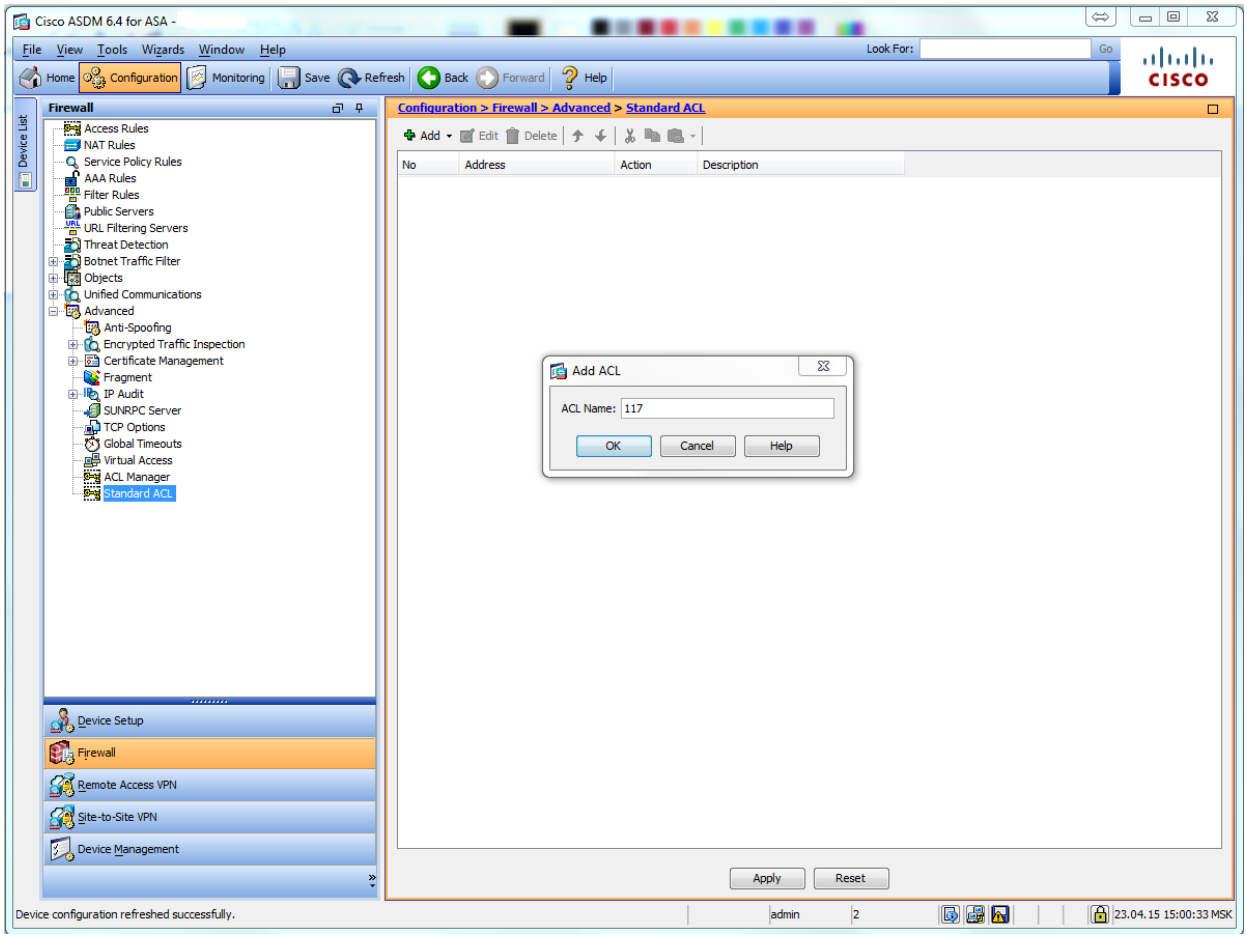

SSL VPN Wizard
SSL VPN Wizard
User Authentication (Step 3 of 6)
The security appliance supports authentication of users by an external AAA server or local user accounts. Specify how the security appliance authenticates users when they login.
Authenticate using a AAA server group
AAA Server Group Name:
New...
Authenticate using the local user database
User to be Added
Username:
uservpn
Password:
Confirm Password:
Add >>
Delete
< Back
Next >
Finish
Cancel
Help

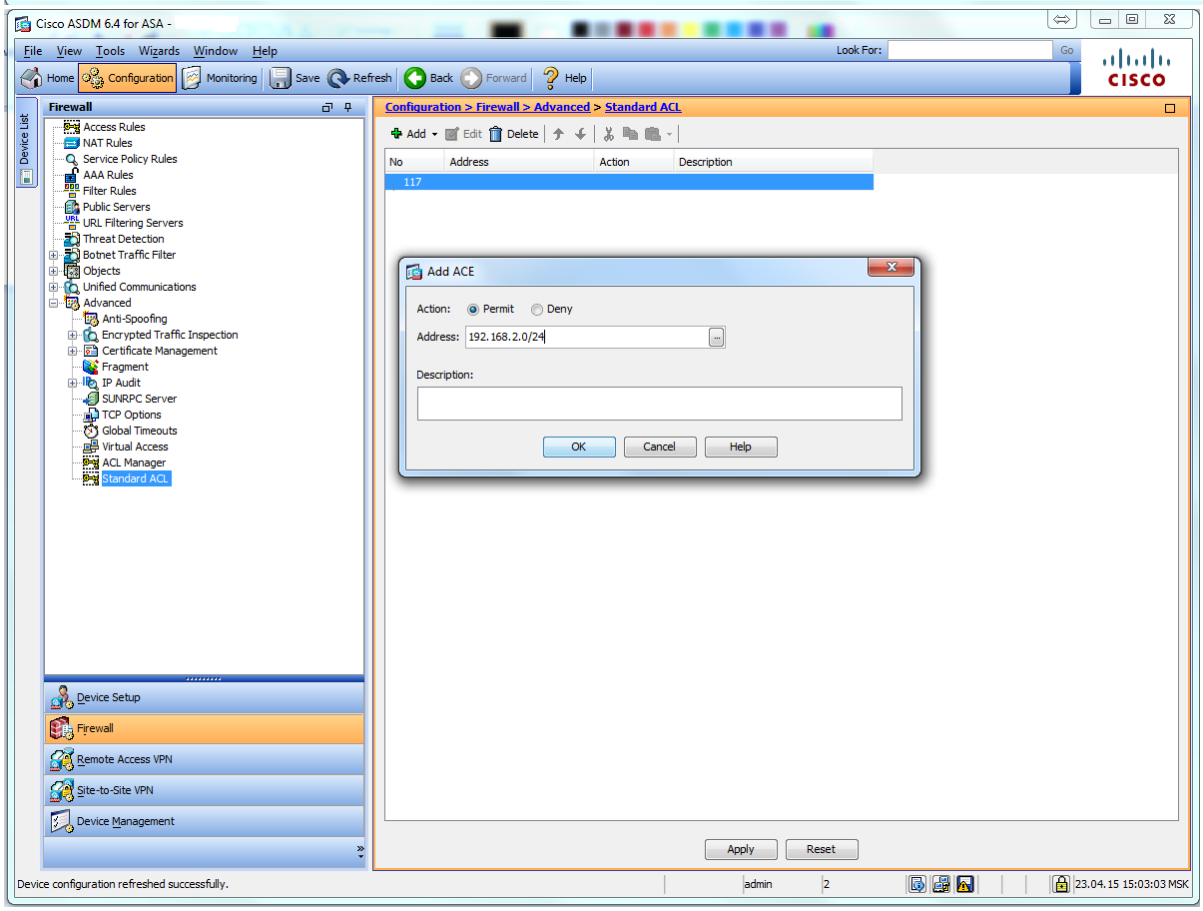

SSL VPN Wizard
SSL VPN Wizard
IP Address Pools and Client Image - AnyConnect VPN Client Connections Only (Step 5 of 6)
The security appliance downloads the AnyConnect VPN Client to remote users when they connect. The client self-installs, uses SSL or DTLS encryption for the duration of the connection, and allows full access to resources on a corporate network. The remote PC becomes part of the corporate network.
IP Address Pools
Create a new address pool or select an existing address pool for IPv4 and IPv6. Remote PCs are assigned addresses from the pools when they connect.
IPv4 Address Pool:
New...
Address Pool Range:
Add IP Pool
Name:
vpnusers
Starting IP Address:
192.168.2.245
Ending IP Address:
192.168.2.250
Subnet Mask:
255.255.255.0
OK
Cancel
Help
< Back
Next >
Finish
Cancel
Help

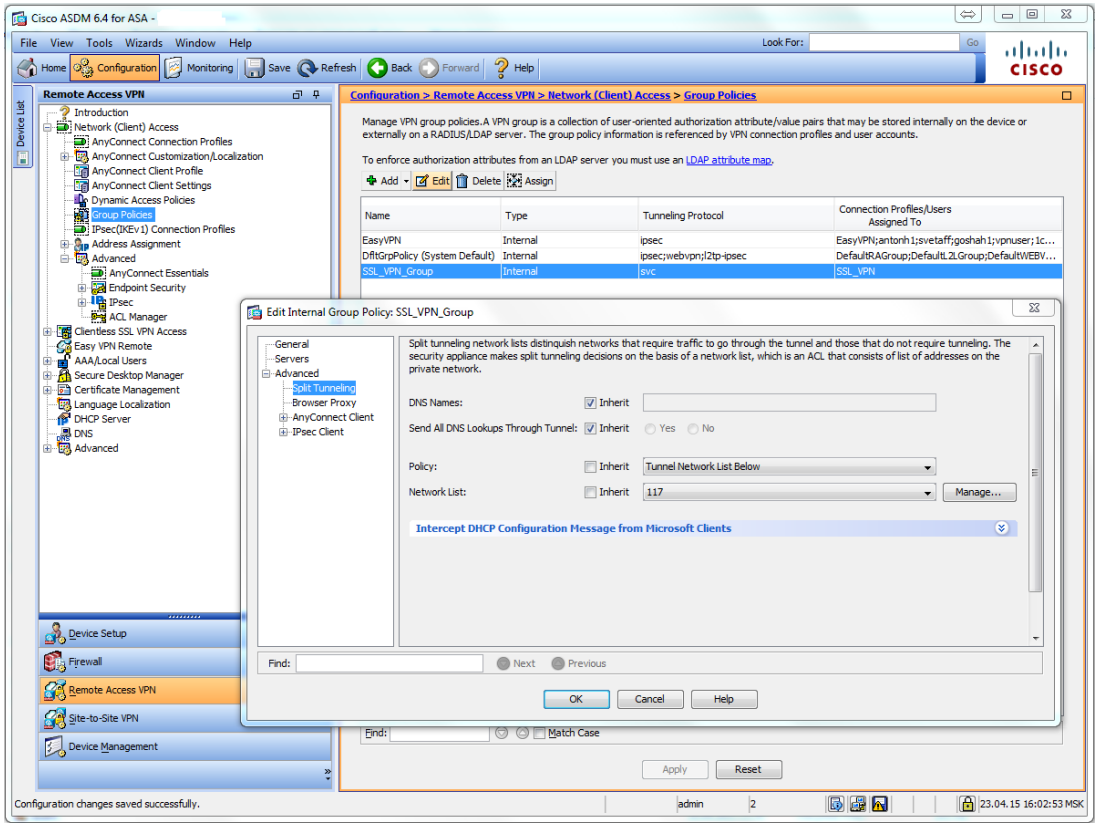

Select
Look in:
cisco
anyconnect-linux-3.0.5080-k9.pkg
anyconnect-macosx-i386-3.0.5080-k9.pkg
anyconnect-win-3.0.5080-k9.pkg
asa5505_vpn_old
asr1000rp2-adventerprise.02.05.02
c2960s-universalk9-mz.122-55.SE
Недавние документы
Рабочий стол
File name:
anyconnect-win-3.0.5080-k9.pkg
Files of type:
All Files
Select
Cancel
SSL VPN Wizard
Upload Image
Upload a file from local computer to flash file system on the device. The upload process might take a few minutes. Please wait for the operation to finish.
Local File Path:
Browse Local Files...
Flash File System Path:
Browse Flash...
Upload File
Close
Help
Identify a file in flash memory as an AnyConnect VPN Client image. The security appliance expands the file and loads it into cache memory for downloading to remote users.
Location:
Browse...
Download latest AnyConnect VPN Client from Cisco.com
Add AnyConnect Client Image
AnyConnect Image:
Browse Flash...
Upload...
OK
Cancel
Help

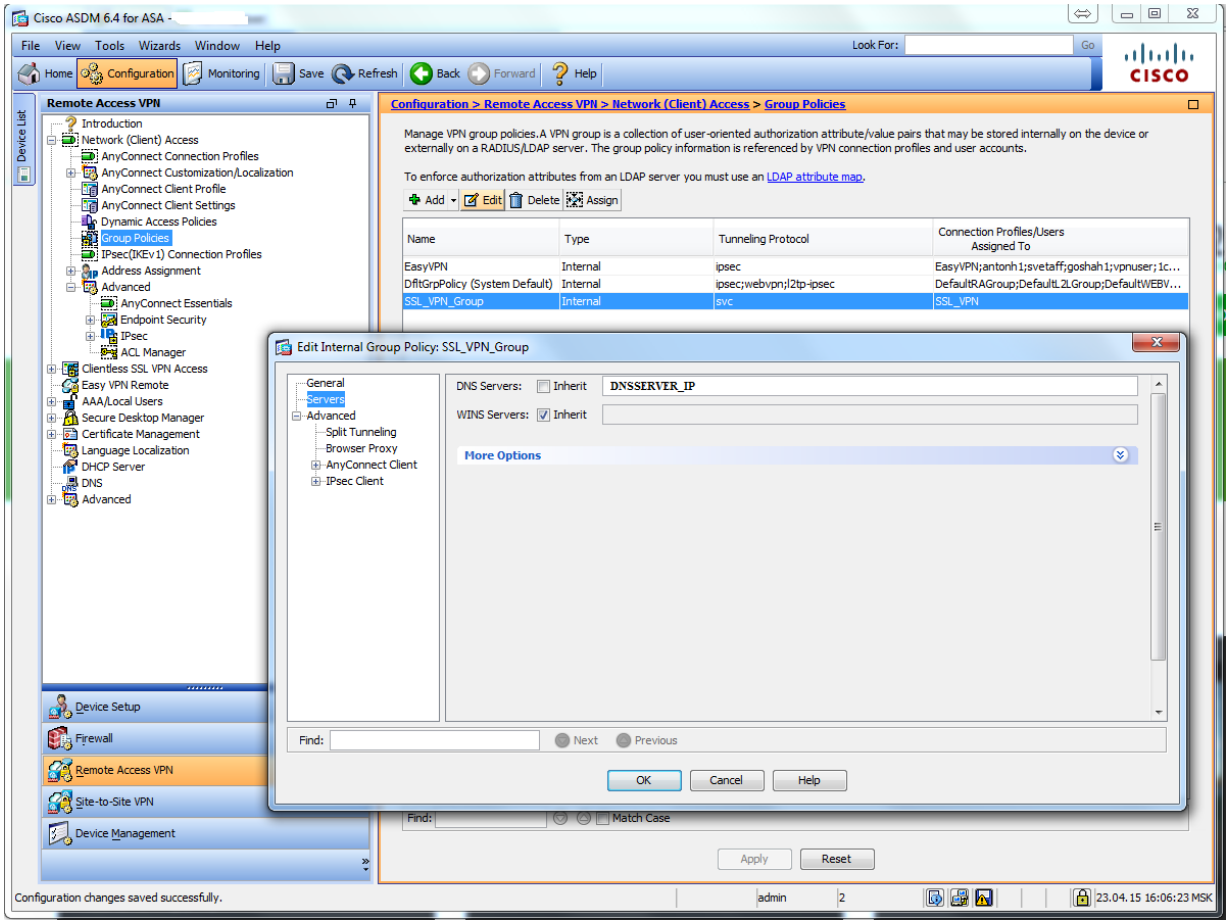

SSL VPN Wizard
SSL VPN Wizard
Summary (Step 6 of 6)
You have created a SSL VPN connection with following attributes:
Selected Features: AnyConnect Client
Connection Name: SSL_VPN
SSL VPN Interface: Inet
User Authentication: LOCAL
Group Policy: SSL_VPN_Group
IPv4 Address Pool: vpnusers
IPv6 Address Pool: None
AnyConnect Client Location: disk0:/anyconnect-win-3.0.5080-k9.pkg
< Back
Next >
Finish
Cancel
Help

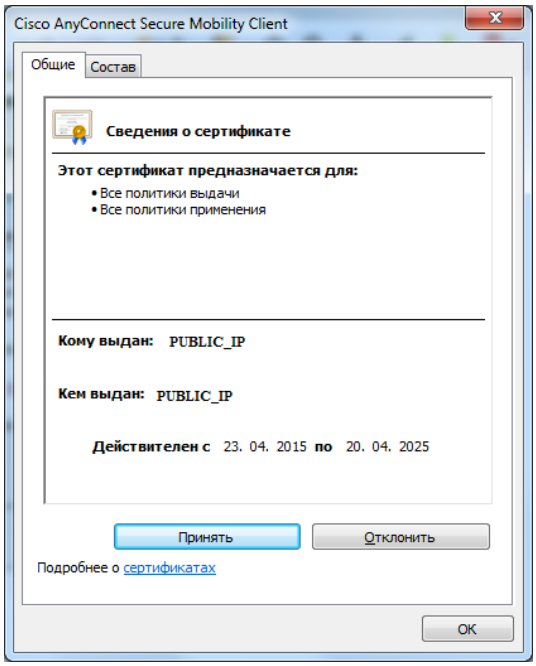

Cisco ASDM 6.4 for ASA -
File View Tools Wizards Window Help
Look For:
Home Configuration Monitoring Save Refresh Back Forward Help
Remote Access VPN
Introduction
Network (Client) Access
AnyConnect Connection Profiles
AnyConnect Customization/Localization
AnyConnect Client Profile
AnyConnect Client Settings
Dynamic Access Policies
Group Policies
IPsec(IKEv1) Connection Profiles
Address Assignment
Advanced
Clientless SSL VPN Access
Easy VPN Remote
AAA/Local Users
Secure Desktop Manager
Certificate Management
Language Localization
DHCP Server
DNS
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Configuration > Remote Access
AnyConnect Client Images
Add Replace Delete
Image
Select
Look in: cisco
anyconnect-linux-3.0.5080-k9.pkg
anyconnect-macosx-i386-3.0.5080-k9.pkg
anyconnect-win-3.0.5080-k9.pk
asa5505_vpn_old
File name: anyconnect-linux-3.0.5080-k9.pkg
Files of type: All Files
Select
Cancel
Add AnyConnect Client Image
AnyConnect Image:
Browse Flash...
Upload...
Regular expression to match user-agent
OK
Cancel
Help
Upload Image
Upload a file from local computer to flash file system on the device. The upload process might take a few minutes. Please wait for the operation to finish.
Local File Path:
Browse Local Files...
Flash File System Path:
Browse Flash...
Upload File
Close
Help
Apply
Reset
admin
2
23.04.15 14:40:23 MSK

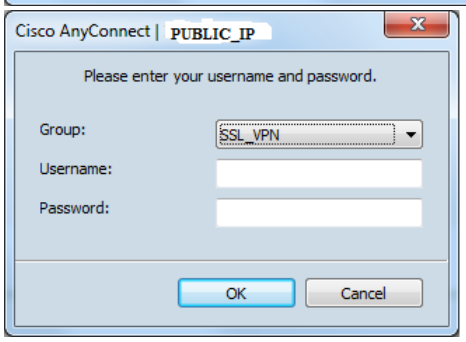

Cisco ASDM 6.4 for ASA -
File View Tools Wizards Window Help
Look For:
Home Configuration Monitoring Save Refresh Back Forward Help
Firewall
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Botnet Traffic Filter
Objects
Unified Communications
Advanced
Anti-Spoofing
Encrypted Traffic Inspection
Certificate Management
Fragment
IP Audit
SUNRPC Server
TCP Options
Global Timeouts
Virtual Access
ACL Manager
Standard ACL
Configuration > Firewall > Advanced > Standard ACL
Add Edit Delete
No Address Action Description
Add ACL
ACL Name: 117
OK Cancel Help
Apply Reset
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Device configuration refreshed successfully.
admin
23.04.15 15:00:33 MSK


Cisco ASDM 6.4 for ASA -
File View Tools Wizards Window Help
Look For:
Home Configuration Monitoring Save Refresh Back Forward Help
Firewall
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Botnet Traffic Filter
Objects
Unified Communications
Advanced
Anti-Spoofing
Encrypted Traffic Inspection
Certificate Management
Fragment
IP Audit
SUNRPC Server
TCP Options
Global Timeouts
Virtual Access
ACL Manager
Standard ACL
Configuration > Firewall > Advanced > Standard ACL
Add Edit Delete
No Address Action Description
117
Add ACE
Action: Permit Deny
Address: 192.168.2.0/24
Description:
OK Cancel Help
Apply Reset
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Device configuration refreshed successfully.
admin
23.04.15 15:03:03 MSK


Cisco ASDM 6.4 for ASA -
File View Tools Wizards Window Help
Look For:
Home Configuration Monitoring Save Refresh Back Forward Help
Remote Access VPN
Introduction
Network (Client) Access
AnyConnect Connection Profiles
AnyConnect Customization/Localization
AnyConnect Client Profile
AnyConnect Client Settings
Dynamic Access Policies
Group Policies
IPsec(IKEv1) Connection Profiles
Address Assignment
Advanced
AnyConnect Essentials
Endpoint Security
IPsec
ACL Manager
Clientless SSL VPN Access
Easy VPN Remote
AAA/Local Users
Secure Desktop Manager
Certificate Management
Language Localization
DHCP Server
DNS
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Configuration > Remote Access VPN > Network (Client) Access > Group Policies
Manage VPN group policies.A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts.
To enforce authorization attributes from an LDAP server you must use an LDAP attribute map.
Add Edit Delete Assign
Name
Type
Tunneling Protocol
Connection Profiles/Users Assigned To
EasyVPN
Internal
ipsec
EasyVPN;antonh1;svetaff;goshah1;vpnuser;1c...
DfltGrpPolicy (System Default)
Internal
ipsec;webvpn;l2tp-ipsec
DefaultRAGroup;DefaultL2LGroup;DefaultWEBV...
SSL_VPN_Group
Internal
svc
SSL_VPN
Edit Internal Group Policy: SSL_VPN_Group
General
Servers
Advanced
Split Tunneling
Browser Proxy
AnyConnect Client
IPsec Client
Split tunneling network lists distinguish networks that require traffic to go through the tunnel and those that do not require tunneling. The security appliance makes split tunneling decisions on the basis of a network list, which is an ACL that consists of list of addresses on the private network.
DNS Names: Inherit
Send All DNS Lookups Through Tunnel: Inherit Yes No
Policy: Inherit Tunnel Network List Below
Network List: Inherit 117 Manage...
Intercept DHCP Configuration Message from Microsoft Clients
Find: Next Previous
OK Cancel Help
Find: Match Case
Apply Reset
Configuration changes saved successfully.
admin 2
23.04.15 16:02:53 MSK


Cisco ASDM 6.4 for ASA -
File View Tools Wizards Window Help
Look For:
Home Configuration Monitoring Save Refresh Back Forward Help
Remote Access VPN
Introduction
Network (Client) Access
AnyConnect Connection Profiles
AnyConnect Customization/Localization
AnyConnect Client Profile
AnyConnect Client Settings
Dynamic Access Policies
Group Policies
IPsec(IKEv1) Connection Profiles
Address Assignment
Advanced
AnyConnect Essentials
Endpoint Security
IPsec
ACL Manager
Clientless SSL VPN Access
Easy VPN Remote
AAA/Local Users
Secure Desktop Manager
Certificate Management
Language Localization
DHCP Server
DNS
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Configuration > Remote Access VPN > Network (Client) Access > Group Policies
Manage VPN group policies.A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts.
To enforce authorization attributes from an LDAP server you must use an LDAP attribute map.
Add Edit Delete Assign
Name
Type
Tunneling Protocol
Connection Profiles/Users Assigned To
EasyVPN
Internal
ipsec
EasyVPN;antonh1;svetaff;goshah1;vpnuser;1c...
DfltGrpPolicy (System Default)
Internal
ipsec;webvpn;l2tp-ipsec
DefaultRAGroup;DefaultL2LGroup;DefaultWEBV...
SSL_VPN_Group
Internal
svc
SSL_VPN
Edit Internal Group Policy: SSL_VPN_Group
General
Servers
Advanced
Split Tunneling
Browser Proxy
AnyConnect Client
IPsec Client
DNS Servers: Inherit DNSSERVER_IP
WINS Servers: Inherit
More Options
Find: Next Previous
OK Cancel Help
Find: Match Case
Apply Reset
Configuration changes saved successfully.
admin 2
23.04.15 16:06:23 MSK





Практическая работа № 21 «Установка системы обнаружения и предотвращения вторжения Snort»

Задание 1:

1. Сначала необходимо установить всё необходимое программное обеспечение, чтобы облачный сервер был готов:

   sudo apt install -y gcc libpcre3-dev zlib1g-dev libluajit-5.1-dev \
   libpcap-dev openssl libssl-dev libnghttp2-dev libdumbnet-dev \
   bison flex libdnet autoconf libtool

   В отчёт вставить скриншот с результатом.

2. Установка состоит из нескольких шагов:

Загрузка кода, его настройка, компиляция кода, установка его в соответствующих каталог и настройка правил обнаружения.

Создадим временную папку для загрузки:
mkdir ~/snort_src && cd ~/snort_src

3. Snort использует библиотеку сбора данных DAQ. Загрузите последний пакет с веб-сайта с помощью команды wget:

   wget https://www.snort.org/downloads/snort/daq-2.0.7.tar.gz

4. Загрузка займёт несколько секунд. По завершении исходный код нужно извлечь из архива и перейти в новый каталог:

   tar -xvzf daq-2.0.7.tar.gz
   cd daq-2.0.7

   В отчёт вставить скриншот с результатом.

5. Последняя версия требует дополнительного шага для автоматической перенастройки DAQ перед запуском конфигурации:

   autoreconf -f -i

6. После этого запустите скрипт конфигурации и скомпилируйте программу с помощью команды:

   ./configure && make && sudo make install

7. С установленным DAQ можно начинатать работать и вернуться в папку загрузки:

   cd ~/snort_src

   В отчёт вставить скриншот с результатом.

8. Далее загрузите исходный код Snort с помощью wget. Перед этим зайдите на сайт, в случае наличия более поздней версии замените версию в команде загрузки:

   wget https://www.snort.org/downloads/snort/snort-2.9.16.tar.gz

9. После завершения загрузки извлеките исходный код и перейдите в каталог:

tar -xvzf snort-2.9.16.tar.gz
cd snort-2.9.16

В отчёт вставить скриншот с результатом.

10. Затем настройте установку с включённым sourcefire:

    ./configure --enable-sourcefire && make && sudo make install

11. Далее необходимо настроить Snort для системы. Для этого нужно отредактировать некоторые файлы конфигурации, загрузку правил и пробный запуск. Начнём с обновления общих библиотек:
    sudo ldconfig
12. Snort устанавливается в /usr/local/bin/snort директорию, рекомендуется создать ссылку на /usr/sbin/snort.

    sudo ln -s /usr/local/bin/snort /usr/sbin/snort

    В отчёт вставить скриншот с результатом.

13. Для безопасного запуска Snort без доступа root нужно создать нового непривилегированного пользователя и новую группу пользователей для запуска демона

    sudo groupadd snort
    sudo useradd snort -r -s /sbin/nologin -c SNORT_IDS -g snort

14. Затем создайте папки для размещения конфигураций Snort:

    sudo mkdir -p /etc/snort/rules
    sudo mkdir /var/log/snort
    sudo mkdir /usr/local/lib/snort_dynamicrules

15. Установите разрешения для новых папок:

    sudo chmod -R 5775 /etc/snort
    sudo chmod -R 5775 /var/log/snort
    sudo chmod -R 5775 /usr/local/lib/snort_dynamicrules
    sudo chown -R snort:snort /etc/snort
    sudo chown -R snort:snort /var/log/snort
    sudo chown -R snort:snort /usr/local/lib/snort_dynamicrules

16. Создайте новые файлы для белых и чёрных списков и локальные правила:

    sudo touch /etc/snort/rules/white_list.rules
    sudo touch /etc/snort/rules/black_list.rules
    sudo touch /etc/snort/rules/local.rules

17. Затем скопируйте конфигурационный файл из папки загрузки:

    sudo cp ~/snort_src/snort-2.9.16/etc/*.conf* /etc/snort
    sudo cp ~/snort_src/snort-2.9.16/etc/*.map /etc/snort

    В отчёт вставить скриншот с результатом.

Затем нужно загрузить правила обнаружения, которыми Snort будет следовать для выявления потенциальных угроз. Snort предоставляет три уровня набора правил:

- ✓ Community rules are freely available although slightly limited.
- ✓ By registering for free on their website you get access to your Oink code, which lets you download the registered users rule sets.
- ✓ Lastly, subscriber rules are just that, available to users with an active subscription to Snort services.

18. Для быстрого тестирования Snort можно скачать правила:

    wget https://www.snort.org/rules/community -O ~/community.tar.gz

19. Извлекаем правила и копируем в конфигурационную папку:

    sudo tar -xvf ~/community.tar.gz -C ~/
    sudo cp ~/community-rules/* /etc/snort/rules

    В отчёт вставить скриншот с результатом.

20. По умолчанию Snort ожидает некоторые правила, которые не включены в файл правил. С помощью следующей команды можно закомментировать ненужные строки в файле правил:

    sudo sed -i 's/include \$RULE_PATH/#include \$RULE_PATH/' /etc/snort/snort.conf

21. Далее вам нужно зарегистрироваться на сайте Snort, зайти на него под своим аккаунтом, открыть данные своего аккаунта, перейти в Oinkcode, скопировать данный код и в следующую команду его вставить:

    wget https://www.snort.org/rules/snortrules-snapshot-29160.tar.gz?oinkcode=oinkcode -O ~/registered.tar.gz

    В отчёт вставить скриншот с результатом.

22. Регистрация нужна для загрузки правил. Далее распаковываем в папку:

    sudo tar -xvf ~/registered.tar.gz -C /etc/snort

23. После установки отредактируем конфигурационный файл:

    sudo nano /etc/snort/snort.conf

24. Найдите разделы, которые указаны ниже и измените параметры по образцу:

```
# Setup the network addresses you are protecting
ipvar HOME_NET 10.0.2.15/24
# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET !$HOME_NET
# Path to your rules files (this can be a relative path)
var RULE_PATH /etc/snort/rules
var SO_RULE_PATH /etc/snort/so_rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules
# Set the absolute path appropriately
var WHITE_LIST_PATH /etc/snort/rules
```

```
var BLACK_LIST_PATH /etc/snort/rules
```

25. В шестом разделе измените следующее:
    # unified2
    # Recommended for most installs
    output unified2: filename snort.log, limit 128

    В отчёт вставить скриншот с результатом.

26. Далее найдите список включённых наборов правил. Раскомментируйте следующую строку для возможности загружать пользовательские правила:

    include $RULE_PATH/local.rules

27. Также можно добавить строку:

    include $RULE_PATH/community.rules

28. Сохраните и выйдите.

    В отчёт вставить скриншот с результатом.

29. Проверьте конфигурацию:

    sudo snort -T -c /etc/snort/snort.conf

30. После запуска проверки должен появиться текст похожий на:

```
--== Initialization Complete ==--

,,_     -*> Snort! <*-
o"  )~   Version 2.9.16 GRE (Build 118)
""    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2020 Cisco and/or its affiliates. All rights reserved.

Copyright (C) 1998-2013 Sourcefire, Inc., et al.

Using libpcap version 1.8.1

Using PCRE version: 8.39 2016-06-14

Using ZLIB version: 1.2.11

Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.1

Preprocessor Object: SF_DCERPC2  Version 1.0

Preprocessor Object: SF_SSH  Version 1.1

Preprocessor Object: SF_FTPTELNET  Version 1.2

Preprocessor Object: SF_SDF  Version 1.1

Preprocessor Object: SF_DNP3  Version 1.1

Preprocessor Object: SF_REPUTATION  Version 1.1

Preprocessor Object: SF_IMAP  Version 1.0

Preprocessor Object: SF_SMTP  Version 1.1
```

```
Preprocessor Object: SF_GTP  Version 1.1
Preprocessor Object: appid  Version 1.1
Preprocessor Object: SF_MODBUS  Version 1.1
Preprocessor Object: SF_POP  Version 1.0
Preprocessor Object: SF_DNS  Version 1.1
Preprocessor Object: SF_SSLPP  Version 1.1
Preprocessor Object: SF_SIP  Version 1.1
```

В случае возникновения ошибок читаем ошибки, ищем где и исправляем. Чаще всего это отсутствие папок/файлов.

В отчёт вставить скриншот с результатом.

31. Для проверки Snort на регистрацию предупреждений добавьте предупреждение:

    sudo nano /etc/snort/rules/local.rules

32. Следующую строку в файл:

    alert icmp any any -> $HOME_NET any (msg:"ICMP test"; sid:10000001; rev:001;)

    В отчёт вставить скриншот с результатом.

33. Правило состоит из следующих частей:
    - ✓ action for traffic matching the rule, alert in this case
    - ✓ traffic protocol like TCP, UDP or ICMP like here
    - ✓ the source address and port, simply marked as any to include all addresses and ports
    - ✓ the destination address and port, $HOME_NET as declared in the configuration and any for port
    - ✓ some additional bits
    - ✓ log message
    - ✓ unique rule identifier (sid) which for local rules needs to be 1000001 or higher
    - ✓ rule version number.

    Сохраните, выйдите.

34. Запустите Snort с опциями печати предупреждений. Нужно будет правильно выбрать сетевой интерфейс.

    sudo snort -A console -i eth0 -u snort -g snort -c /etc/snort/snort.conf

    Для проверки интерфейса можно воспользоваться командой:

    ip addr

    С включённым Snort при пинге вашего сервера вы должны увидеть уведомление для каждого ICMP-вызова в терминале.

07/12-11:20:33.501624 [**] [1:10000001:1] ICMP test [**] [Priority: 0] {ICMP} 83.136.252.119 -> 80.69.173.202

После появления предупреждений вы можете остановить их Ctrl+C. Все предупреждения записываются в журнал /var/log/snort/snort.log.timestamp.

35. Прочитать логи можно с помощью команды внизу:

    snort -r /var/log/snort/snort.log.

    В отчёт вставить скриншот с результатом.

36. Для запуска snort в фоновом режиме в качестве службы нужно отредактировать следующий файл:

```
sudo nano /lib/systemd/system/snort.service
Введите следующее:
[Unit]
Description=Snort NIDS Daemon
After=syslog.target network.target


[Service]
Type=simple
ExecStart=/usr/local/bin/snort -q -u snort -g snort -c /etc/snort/snort.conf -i eth0


[Install]
WantedBy=multi-user.target
```

    Следующей командой перезагрузите демон systemctl:
    sudo systemctl daemon-reload

37. Затем выполните старт snort:
    sudo systemctl start snort
38. Увидеть статус можно следующей командой:

    sudo systemctl status snort
    В отчёт вставить скриншот с результатом.
    Система обнаружения вторжений установлена и протестирована.

Эталон ответа:

Задание 1:

1. Сначала необходимо установить всё необходимое программное обеспечение, чтобы облачный сервер был готов:

   sudo apt install -y gcc libpcre3-dev zlib1g-dev libluajit-5.1-dev \
   libpcap-dev openssl libssl-dev libnghttp2-dev libdumbnet-dev \
   bison flex libdnet autoconf libtool

   В отчёт вставить скриншот с результатом.

2. Установка состоит из нескольких шагов:

Загрузка кода, его настройка, компиляция кода, установка его в соответствующих каталог и настройка правил обнаружения.

Создадим временную папку для загрузки:
mkdir ~/snort_src && cd ~/snort_src

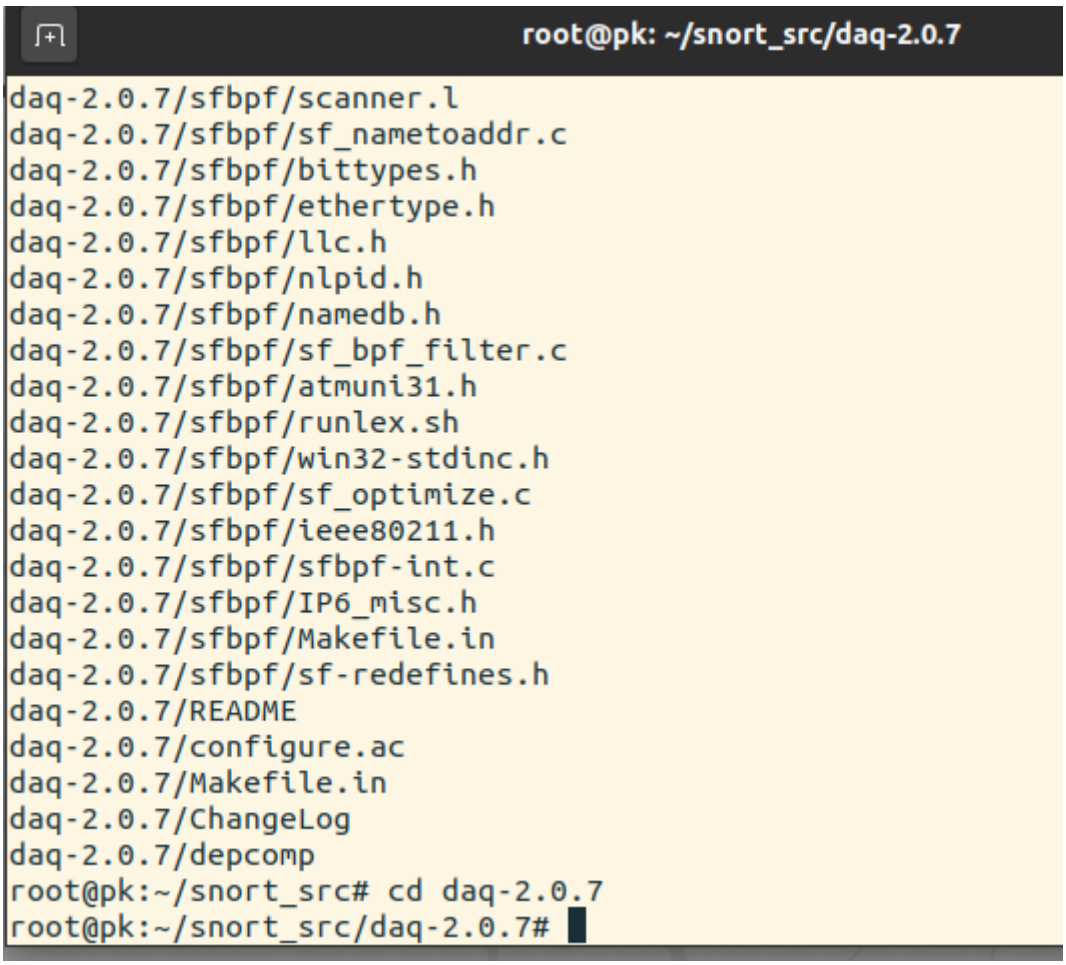
3. Snort использует библиотеку сбора данных DAQ. Загрузите последний пакет с веб-сайта с помощью команды wget:

   wget https://www.snort.org/downloads/snort/daq-2.0.7.tar.gz

4. Загрузка займёт несколько секунд. По завершении исходный код нужно извлечь из архива и перейти в новый каталог:

   tar -xvzf daq-2.0.7.tar.gz
   cd daq-2.0.7

   В отчёт вставить скриншот с результатом.



5. Последняя версия требует дополнительного шага для автоматической перенастройки DAQ перед запуском конфигурации:

   autoreconf -f -i

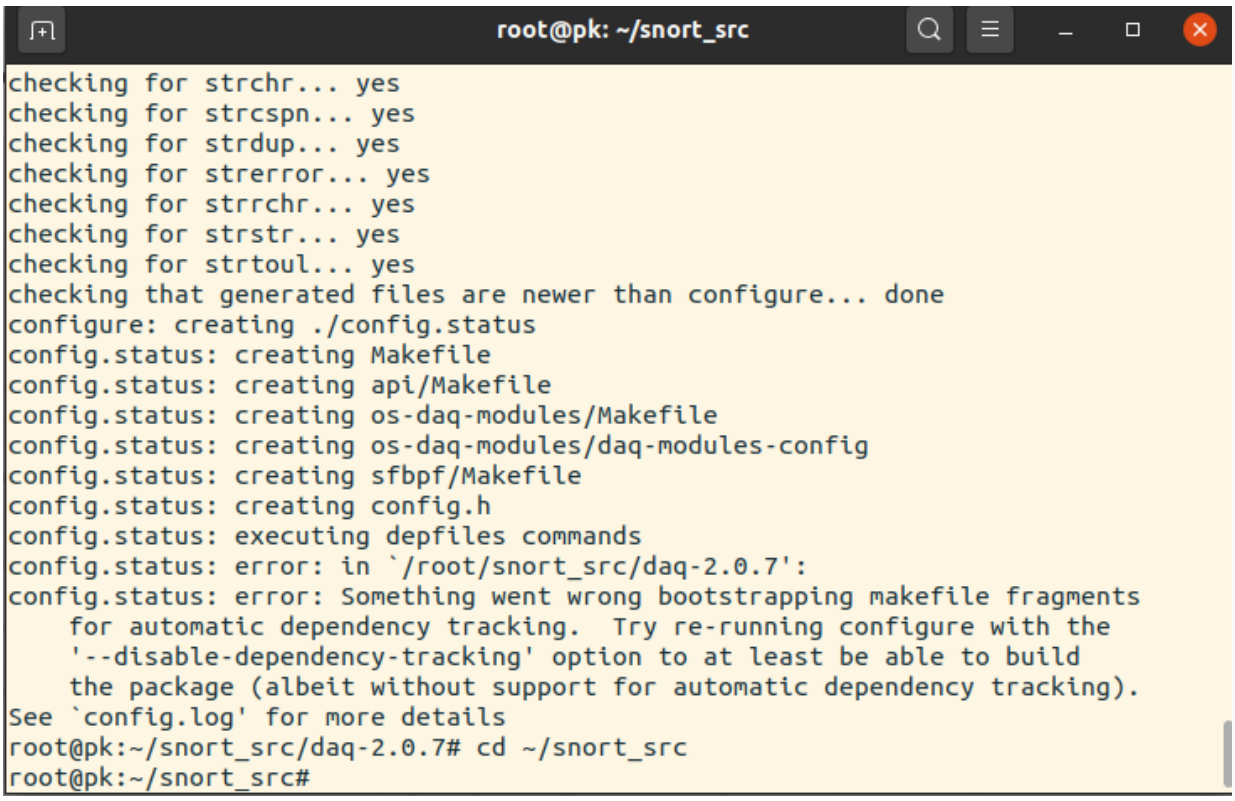
6. После этого запустите скрипт конфигурации и скомпилируйте программу с помощью команды:

   ./configure && make && sudo make install

7. С установленным DAQ можно начинатать работать и вернуться в папку загрузки:

   cd ~/snort_src

   В отчёт вставить скриншот с результатом.



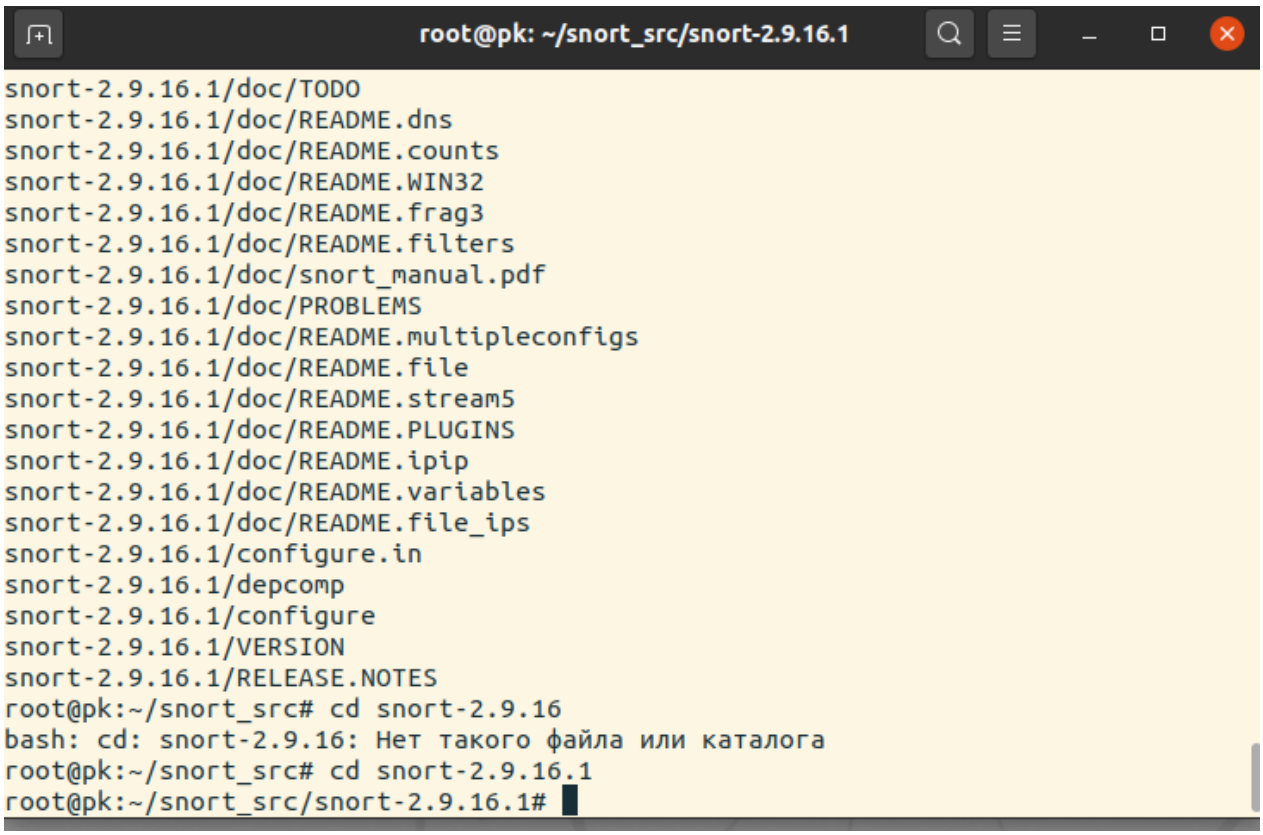
8. Далее загрузите исходный код Snort с помощью wget. Перед этим зайдите на сайт, в случае наличия более поздней версии замените версию в команде загрузки:

   wget https://www.snort.org/downloads/snort/snort-2.9.16.1.tar.gz

9. После завершения загрузки извлеките исходный код и перейдите в каталог:

   tar -xvzf snort-2.9.16.1.tar.gz
   cd snort-2.9.16.1

   В отчёт вставить скриншот с результатом.



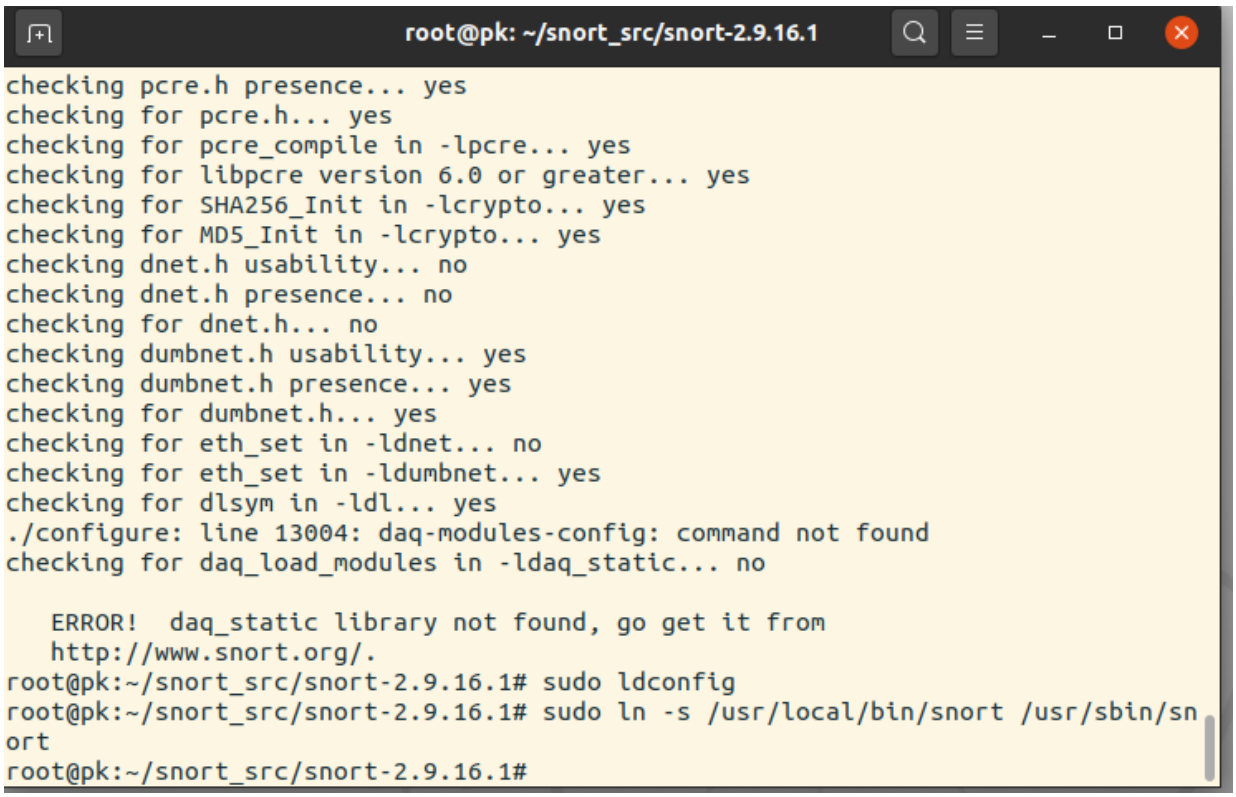
10. Затем настройте установку с включённым sourcefire:

    ./configure --enable-sourcefire && make && sudo make install

11. Далее необходимо настроить Snort для системы. Для этого нужно отредактировать некоторые файлы конфигурации, загрузку правил и пробный запуск. Начнём с обновления общих библиотек:
    sudo ldconfig
12. Snort устанавливается в /usr/local/bin/snort директорию, рекомендуется создать ссылку на /usr/sbin/snort.

    sudo ln -s /usr/local/bin/snort /usr/sbin/snort

    В отчёт вставить скриншот с результатом.



13. Для безопасного запуска Snort без доступа root нужно создать нового непривилегированного пользователя и новую группу пользователей для запуска демона

    sudo groupadd snort
    sudo useradd snort -r -s /sbin/nologin -c SNORT_IDS -g snort

14. Затем создайте папки для размещения конфигураций Snort:

    sudo mkdir -p /etc/snort/rules
    sudo mkdir /var/log/snort
    sudo mkdir /usr/local/lib/snort_dynamicrules

15. Установите разрешения для новых папок:

    sudo chmod -R 5775 /etc/snort
    sudo chmod -R 5775 /var/log/snort
    sudo chmod -R 5775 /usr/local/lib/snort_dynamicrules
    sudo chown -R snort:snort /etc/snort
    sudo chown -R snort:snort /var/log/snort
    sudo chown -R snort:snort /usr/local/lib/snort_dynamicrules

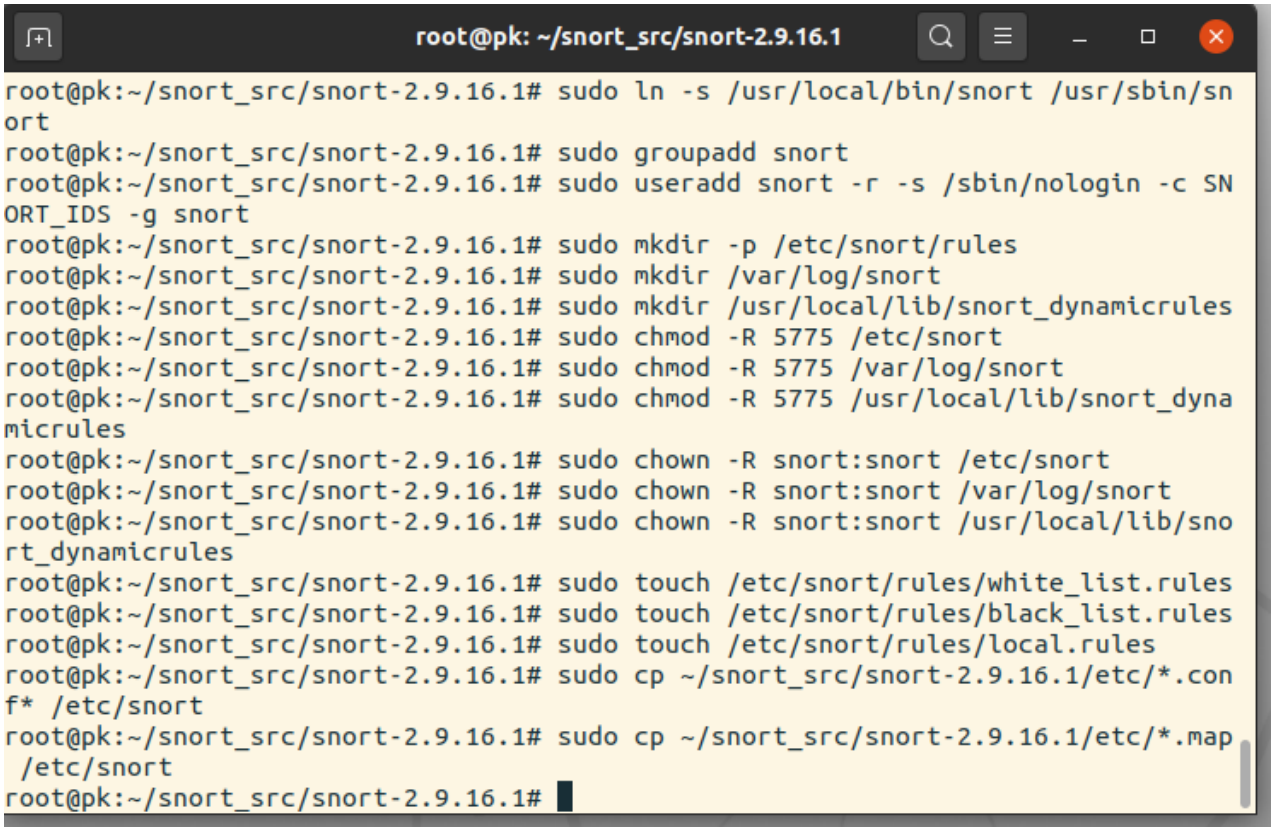
16. Создайте новые файлы для белых и чёрных списков и локальные правила:

    sudo touch /etc/snort/rules/white_list.rules
    sudo touch /etc/snort/rules/black_list.rules
    sudo touch /etc/snort/rules/local.rules

17. Затем скопируйте конфигурационный файл из папки загрузки:

    sudo cp ~/snort_src/snort-2.9.16.1/etc/*.conf* /etc/snort
    sudo cp ~/snort_src/snort-2.9.16.1/etc/*.map /etc/snort

В отчёт вставить скриншот с результатом.



Затем нужно загрузить правила обнаружения, которыми Snort будет следовать для выявления потенциальных угроз. Snort предоставляет три уровня набора правил:

- ✓ Community rules are freely available although slightly limited.
- ✓ By registering for free on their website you get access to your Oink code, which lets you download the registered users rule sets.
- ✓ Lastly, subscriber rules are just that, available to users with an active subscription to Snort services.

18. Для быстрого тестирования Snort можно скачать правила:

    wget https://www.snort.org/rules/community -O ~/community.tar.gz

19. Извлекаем правила и копируем в конфигурационную папку:

    sudo tar -xvf ~/community.tar.gz -C ~/
    sudo cp ~/community-rules/* /etc/snort/rules

    В отчёт вставить скриншот с результатом.

20. По умолчанию Snort ожидает некоторые правила, которые не включены в файл правил. С помощью следующей команды можно закомментировать ненужные строки в файле правил:

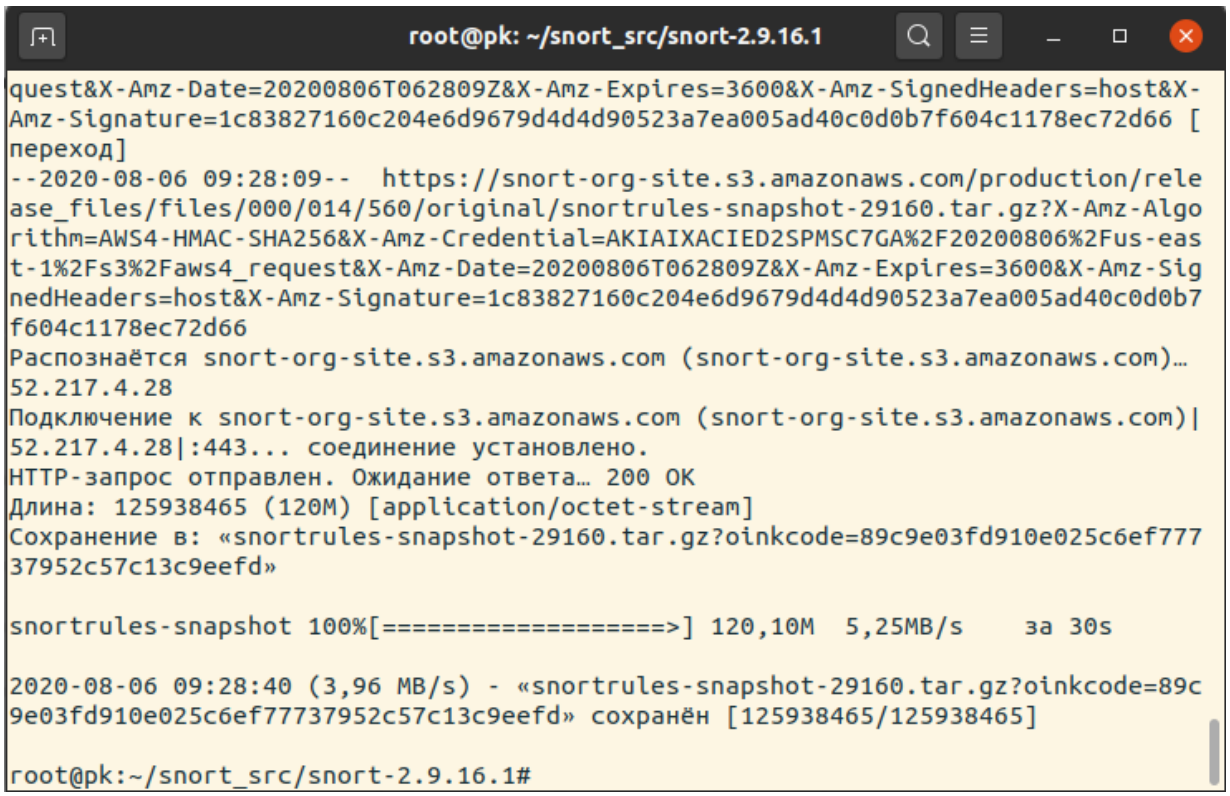
    sudo sed -i 's/include \$RULE_PATH/#include \$RULE_PATH/' /etc/snort/snort.conf

21. Далее вам нужно зарегистрироваться на сайте Snort, зайти на него под своим аккаунтом, открыть данные своего аккаунта, перейти в Oinkcode, скопировать данный код и в следующую команду его вставить:

wget https://www.snort.org/rules/snortrules-snapshot-29160.tar.gz?oinkcode=
89c9e03fd910e025c6ef77737952c57c13c9eefd

https://www.snort.org/rules/snortrules-snapshot-29160.tar.gz?oinkcode=89c9e03fd910e025c6ef77737952c57c13c9eefd

В отчёт вставить скриншот с результатом.



22. Регистрация нужна для загрузки правил. Далее распаковываем в папку:

    sudo tar -xvf ~/registered.tar.gz -C /etc/snort

    sudo tar -xvf snortrules-snapshot-29160.tar.gz?oinkcode=89c9e03fd910e025c6ef77737952c57c13c9eefd.1

    Через sudo nautilus всё было скопировано в /etc/snort

23. После установки отредактируем конфигурационный файл:

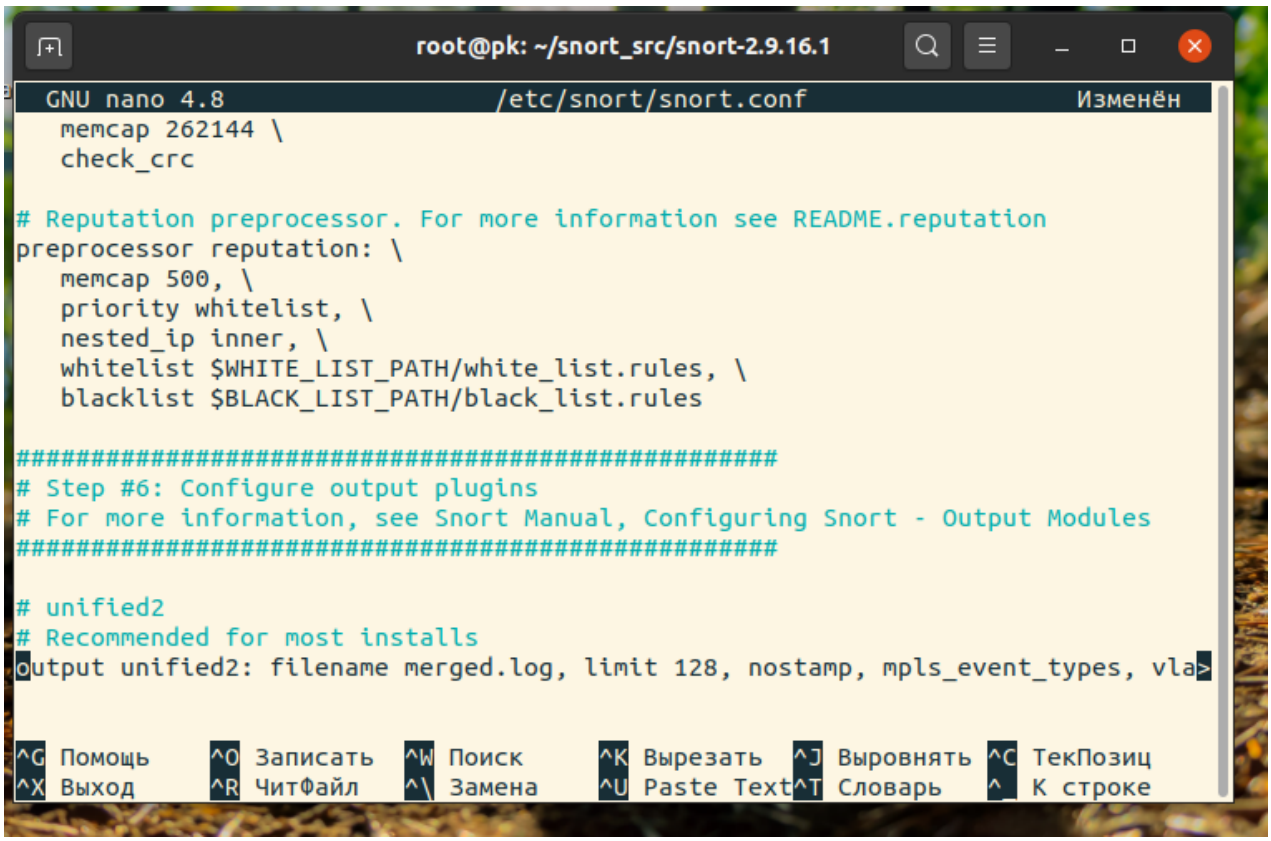
    sudo nano /etc/snort/snort.conf

24. Найдите разделы, которые указаны ниже и измените параметры по образцу:

```
# Setup the network addresses you are protecting
ipvar HOME_NET 10.0.2.14/24
# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET !$HOME_NET
# Path to your rules files (this can be a relative path)
var RULE_PATH /etc/snort/rules
var SO_RULE_PATH /etc/snort/so_rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules
# Set the absolute path appropriately
var WHITE_LIST_PATH /etc/snort/rules
var BLACK_LIST_PATH /etc/snort/rules
```

25. В шестом разделе измените следующее:
    # unified2
    # Recommended for most installs
    output unified2: filename snort.log, limit 128

    В отчёт вставить скриншот с результатом.



26. Далее найдите список включённых наборов правил. Раскомментируйте следующую строку для возможности загружать пользовательские правила:

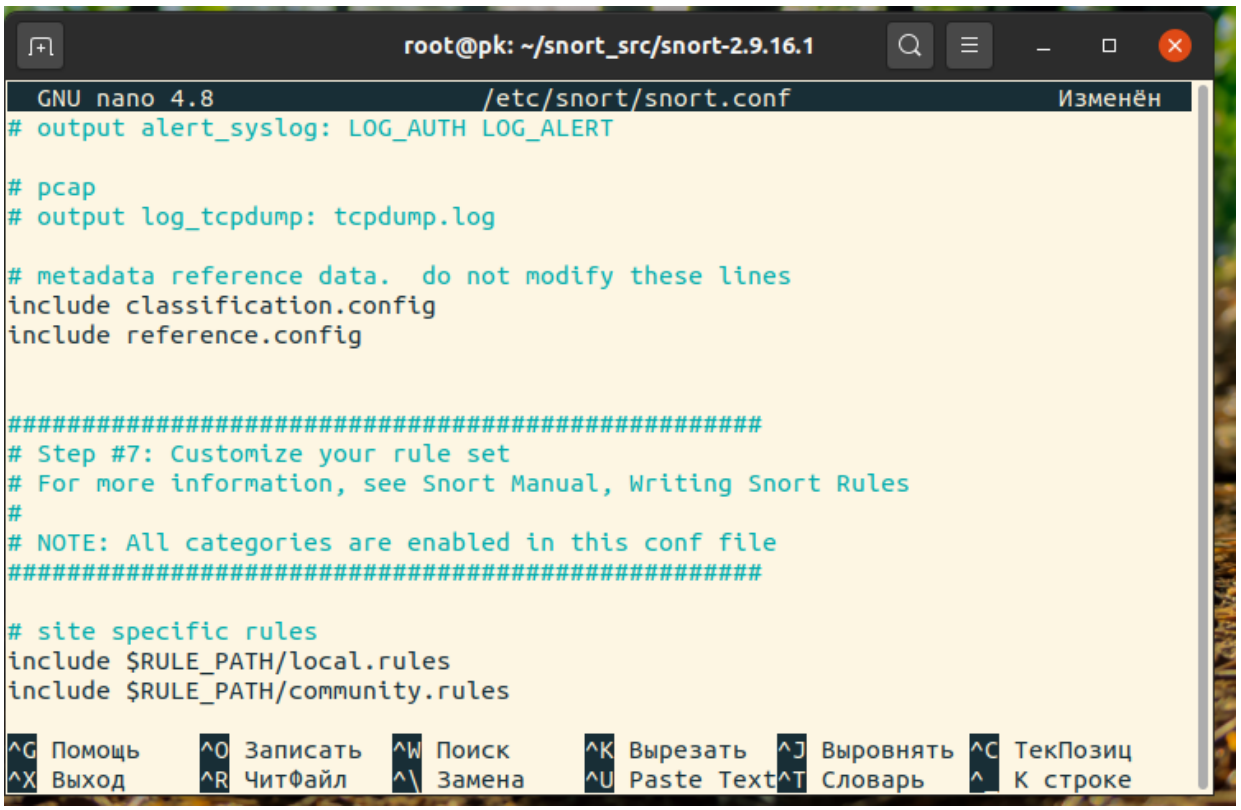
    include $RULE_PATH/local.rules

27. Также можно добавить строку:

    include $RULE_PATH/community.rules

28. Сохраните и выйдите.

    В отчёт вставить скриншот с результатом.



29. Проверьте конфигурацию:

    sudo snort -T -c /etc/snort/snort.conf

30. После запуска проверки должен появиться текст похожий на:

```
--== Initialization Complete ==--
```

```
,,_     -*> Snort! <*-
o"  )~   Version 2.9.16 GRE (Build 118)
""    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2020 Cisco and/or its affiliates. All rights reserved.

Copyright (C) 1998-2013 Sourcefire, Inc., et al.

Using libpcap version 1.8.1

Using PCRE version: 8.39 2016-06-14

Using ZLIB version: 1.2.11

Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.1

Preprocessor Object: SF_DCERPC2  Version 1.0

Preprocessor Object: SF_SSH  Version 1.1

Preprocessor Object: SF_FTPTELNET  Version 1.2

Preprocessor Object: SF_SDF  Version 1.1

Preprocessor Object: SF_DNP3  Version 1.1

Preprocessor Object: SF_REPUTATION  Version 1.1
```

```
Preprocessor Object: SF_IMAP  Version 1.0
Preprocessor Object: SF_SMTP  Version 1.1
Preprocessor Object: SF_GTP  Version 1.1
Preprocessor Object: appid  Version 1.1
Preprocessor Object: SF_MODBUS  Version 1.1
Preprocessor Object: SF_POP  Version 1.0
Preprocessor Object: SF_DNS  Version 1.1
Preprocessor Object: SF_SSLPP  Version 1.1
Preprocessor Object: SF_SIP  Version 1.1
```

В случае возникновения ошибок читаем ошибки, ищем где и исправляем. Чаще всего это отсутствие папок/файлов.

В отчёт вставить скриншот с результатом.

```
tasha@pk:~/snort_src/snort3/build$ /usr/local/bin/snort -V

   ,,_     -*> Snort++ <*-
  o"  )~   Version 3.0.2 (Build 2)
   ''''    By Martin Roesch & The Snort Team
           http://snort.org/contact#team
           Copyright (C) 2014-2020 Cisco and/or its affiliates. All rights reserved
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using DAQ version 3.0.0
           Using LuaJIT version 2.1.0-beta3
           Using OpenSSL 1.1.1f  31 Mar 2020
           Using libpcap version 1.9.1 (with TPACKET_V3)
           Using PCRE version 8.43 2019-02-23
           Using ZLIB version 1.2.11
           Using FlatBuffers 1.12.0
           Using Hyperscan version 5.2.1 2020-08-06
           Using LZMA version 5.2.4
```

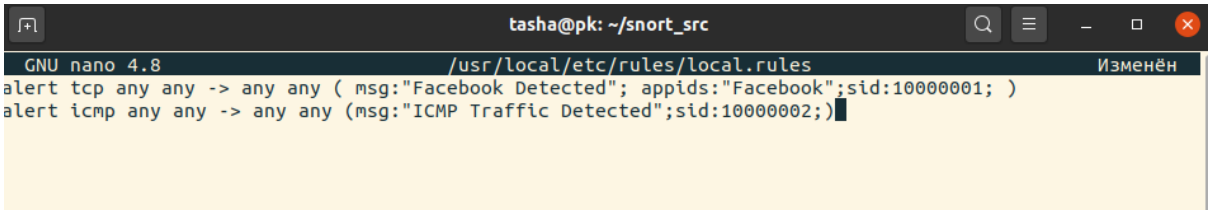
31. Для проверки Snort на регистрацию предупреждений добавьте предупреждение:

    sudo nano /etc/snort/rules/local.rules

32. Следующую строку в файл:

    alert icmp any any -> $HOME_NET any (msg:"ICMP test"; sid:10000001; rev:001;)

    В отчёт вставить скриншот с результатом.



33. Правило состоит из следующих частей:
    - ✓ action for traffic matching the rule, alert in this case
    - ✓ traffic protocol like TCP, UDP or ICMP like here
    - ✓ the source address and port, simply marked as any to include all addresses and ports
    - ✓ the destination address and port, $HOME_NET as declared in the configuration and any for port
    - ✓ some additional bits
    - ✓ log message
    - ✓ unique rule identifier (sid) which for local rules needs to be 1000001 or higher
    - ✓ rule version number.

    Сохраните, выйдите.

34. Запустите Snort с опциями печати предупреждений. Нужно будет правильно выбрать сетевой интерфейс.

    sudo snort -A consolecd -i **eth0** -u snort -g snort -c /etc/snort/snort.conf

    Для проверки интерфейса можно воспользоваться командой:

    ip addr

    С включённым Snort при пинге вашего сервера вы должны увидеть уведомление для каждого ICMP-вызова в терминале.

    07/12-11:20:33.501624 [**] [1:10000001:1] ICMP test [**] [Priority: 0] {ICMP} 83.136.252.119 -> 80.69.173.202

    После появления предупреждений вы можете остановить их Ctrl+C. Все предупреждения записываются в журнал /var/log/snort/snort.log.timestamp.

35. Прочитать логи можно с помощью команды внизу:

    snort -r /var/log/snort/snort.log.

    <u>В отчёт вставить скриншот с результатом.</u>

```
--------------------------------------------------
rule counts
       total rules loaded: 2
               text rules: 2
             option chains: 2
             chain headers: 2
--------------------------------------------------
port rule counts
             tcp     udp    icmp      ip
     any       1       0       1       0
   total       1       0       1       0
--------------------------------------------------
ips policies rule stats
              id  loaded  shared enabled    file
               0       2       0       2    /usr/local/etc/snort/snort.lua
--------------------------------------------------
pcap DAQ configured to passive.
Commencing packet processing
++ [0] enp0s3
```

```
08/06-17:38:05.321637 [**] [1:10000001:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP}
10.0.2.14:41492 -> 157.240.203.35:443
08/06-17:38:05.321634 [**] [1:10000001:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP}
157.240.203.35:443 -> 10.0.2.14:41492
08/06-17:38:05.321646 [**] [1:10000001:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP}
157.240.203.35:443 -> 10.0.2.14:41492
08/06-17:38:05.321853 [**] [1:10000001:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP}
10.0.2.14:41492 -> 157.240.203.35:443
08/06-17:38:05.321850 [**] [1:10000001:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP}
157.240.203.35:443 -> 10.0.2.14:41492
08/06-17:38:05.321862 [**] [1:10000001:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP}
157.240.203.35:443 -> 10.0.2.14:41492
08/06-17:38:05.322028 [**] [1:10000001:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP}
10.0.2.14:41492 -> 157.240.203.35:443
08/06-17:38:05.322025 [**] [1:10000001:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP}
157.240.203.35:443 -> 10.0.2.14:41492
08/06-17:38:05.322174 [**] [1:10000001:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP}
10.0.2.14:41492 -> 157.240.203.35:443
08/06-17:38:05.322162 [**] [1:10000001:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP}
157.240.203.35:443 -> 10.0.2.14:41492
08/06-17:38:05.322887 [**] [1:10000001:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP}
10.0.2.14:41492 -> 157.240.203.35:443
08/06-17:38:05.323005 [**] [1:10000001:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP}
157.240.203.35:443 -> 10.0.2.14:41492
08/06-17:38:05.329119 [**] [1:10000001:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP}
157.240.203.35:443 -> 10.0.2.14:41492
08/06-17:38:05.329147 [**] [1:10000001:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP}
10.0.2.14:41492 -> 157.240.203.35:443
```

```
tasha@pk:~/snort_src$ sudo chmod a+r /var/log/snort/appid_stats.log
tasha@pk:~/snort_src$ cat /var/log/snort/appid_stats.log
1596724669,DNS,362,450
1596724669,Facebook,4783,128541
1596724669,HTTPS,4783,128541
1596724669,SSL client,4783,128541
1596724717,DNS,196,240
1596724717,Facebook,4837,138717
1596724717,HTTPS,4837,138717
1596724717,SSL client,4837,138717
tasha@pk:~/snort_src$
```

36. Для запуска snort в фоновом режиме в качестве службы нужно отредактировать следующий файл:

sudo nano /lib/systemd/system/snort.service
Введите следующее:

```
[Unit]
Description=Snort NIDS Daemon
After=syslog.target network.target


[Service]
Type=simple
ExecStart=/usr/local/bin/snort -q -u snort -g snort -c /etc/snort/snort.conf -i eth0


[Install]
WantedBy=multi-user.target
```

Следующей командой перезагрузите демон systemctl:
sudo systemctl daemon-reload

37. Затем выполните старт snort:
sudo systemctl start snort
38. Увидеть статус можно следующей командой:

sudo systemctl status snort
В отчёт вставить скриншот с результатом.
Система обнаружения вторжений установлена и протестирована.

2. Практическая работа № 29 «Настройка виртуальной машины для эмуляции угроз ИБ»

Задание:

Запускаем рабочую станцию на Kali Linux.

1. Пробуем провести DoS-атаку на наш Apache. Так как BASE работает по HTTP, легкий способ его «положить» — это атака Slowloris. Поэтому скачиваем на Kali соответствующий скрипт и запускаем атаку:
sudo pip3 install slowloris
slowloris example.com
git clone https://github.com/gkbrk/slowloris.git
cd slowloris
python3 slowloris.py example.com

```
root@kali:~/x# git clone https://github.com/gkbrk/slowloris.git
Клонирование в «slowloris»…
remote: Enumerating objects: 6, done.
remote: Counting objects: 100% (6/6), done.
remote: Compressing objects: 100% (6/6), done.
remote: Total 78 (delta 0), reused 3 (delta 0), pack-reused 72
Распаковка объектов: 100% (78/78), готово.
root@kali:~/x# cd slowloris/
root@kali:~/x/slowloris# python3 slowloris.py 192.168.1.20
[02-11-2018 22:06:26] Attacking 192.168.1.20 with 150 sockets.
[02-11-2018 22:06:26] Creating sockets...
[02-11-2018 22:06:30] Sending keep-alive headers... Socket count: 150
[02-11-2018 22:06:45] Sending keep-alive headers... Socket count: 150
[02-11-2018 22:07:00] Sending keep-alive headers... Socket count: 150
^C
Stopping Slowloris...
```

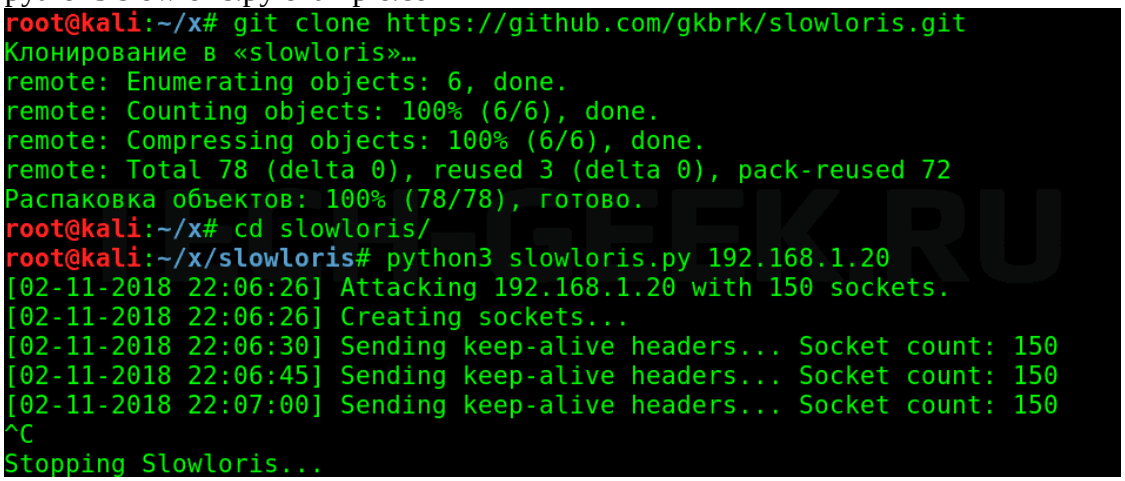
В отчёт вставить скриншоты с установленным скриптом и запуском атаки на Apache, лог из Snort.

2. Запустим sql-инъекцию с kali на машину с установленным snort:(http://sqlmap.org/)
Команда для скачивания: git clone --depth 1 https://github.com/sqlmapproject/sqlmap.git sqlmap-dev
Запустите sqlmap на BASE по запросу http://ip-адрес snort/base/base_stat_alerts.php?sensor=1
Результатов не будет, потому что snort не настроен для обнаружения данной атаки.
В отчёт вставьте скриншот.
Создайте следующее правило:
alert tcp any any -> any any (msg: "SQL Injection"; content: "GET"; http_method; uricontent: "and 1=1"; nocase; sid:3000001; rev:1;)
Снова запустите атаку и посмотрите результаты.
В отчёт вставьте скриншот с результатами.

Эталон ответа:

Запускаем рабочую станцию на Kali Linux.

1. Пробуем провести DoS-атаку на наш Apache. Так как BASE работает по HTTP, легкий способ его «положить» — это атака Slowloris. Поэтому скачиваем на Kali соответствующий скрипт и запускаем атаку:
sudo pip3 install slowloris
slowloris example.com
git clone https://github.com/gkbrk/slowloris.git
cd slowloris
python3 slowloris.py example.com



В отчёт вставить скриншоты с установленным скриптом и запуском атаки на Apache, лог из Snort.

```
Хотите продолжить? [Д/н] y
Пол:1 http://mirror-1.truenetwork.ru/kali kali-rolling/main amd64 python-pi
p-whl all 20.0.2-5kali1 [1842 kB]
Пол:2 http://mirror-1.truenetwork.ru/kali kali-rolling/main amd64 python3-w
heel all 0.34.2-1 [24,0 kB]
Пол:3 http://mirror-1.truenetwork.ru/kali kali-rolling/main amd64 python3-p
ip all 20.0.2-5kali1 [211 kB]
Получено 2078 kB за 2с (1360 kB/s)
Выбор ранее не выбранного пакета python-pip-whl.
(Чтение базы данных … на данный момент установлено 307711 файлов и каталого
в.)
Подготовка к распаковке …/python-pip-whl_20.0.2-5kali1_all.deb …
Распаковывается python-pip-whl (20.0.2-5kali1) …
Выбор ранее не выбранного пакета python3-wheel.
Подготовка к распаковке …/python3-wheel_0.34.2-1_all.deb …
Распаковывается python3-wheel (0.34.2-1) …
Выбор ранее не выбранного пакета python3-pip.
Подготовка к распаковке …/python3-pip_20.0.2-5kali1_all.deb …
Распаковывается python3-pip (20.0.2-5kali1) …
Настраивается пакет python3-wheel (0.34.2-1) …
Настраивается пакет python-pip-whl (20.0.2-5kali1) …
Настраивается пакет python3-pip (20.0.2-5kali1) …
Обрабатываются триггеры для man-db (2.9.3-2) …
Обрабатываются триггеры для kali-menu (2020.3.2) …
tasha@pk2:~$ sudo pip3 install slowloris
Collecting slowloris
  Downloading Slowloris-0.2.1.tar.gz (4.2 kB)
Building wheels for collected packages: slowloris
  Building wheel for slowloris (setup.py) ... done
  Created wheel for slowloris: filename=Slowloris-0.2.1-py3-none-any.whl si
ze=4280 sha256=ecc704f5e103810d376e7f3a706eaee7dff0845ab262a6782e0cfc77d701
fd11
  Stored in directory: /root/.cache/pip/wheels/d6/a3/a6/7bc2e68303a0a117e9f
b9718ecedba6268822497ad0c6b8212
Successfully built slowloris
Installing collected packages: slowloris
Successfully installed slowloris-0.2.1
tasha@pk2:~$ slowloris example.com
[11-08-2020 10:43:05] Attacking example.com with 150 sockets.
[11-08-2020 10:43:05] Creating sockets...
[11-08-2020 10:43:26] Sending keep-alive headers... Socket count: 127
[11-08-2020 10:43:45] Sending keep-alive headers... Socket count: 127
[11-08-2020 10:44:06] Sending keep-alive headers... Socket count: 150
[11-08-2020 10:44:25] Sending keep-alive headers... Socket count: 150
[11-08-2020 10:44:54] Sending keep-alive headers... Socket count: 149
[11-08-2020 10:45:12] Sending keep-alive headers... Socket count: 150
[11-08-2020 10:45:31] Sending keep-alive headers... Socket count: 150
```

15	11.369943000	fa:16:3e:2f:aa:a3	fa:16:3e:39:9c:e7	ARP	42 192.168.50.4 is at fa:16:3e
16	26.663252000	192.168.50.4	192.168.50.5	Syslog	205 AUTHPRIV.NOTICE: Oct 17 10:6
17	26.668978000	192.168.50.4	192.168.50.5	Syslog	147 AUTHPRIV.INFO: Oct 17 10:01:
18	32.769092000	192.168.50.66	192.168.50.5	ICMP	98 Echo (ping) request id=0x0f
19	32.770025000	192.168.50.5	192.168.50.66	ICMP	98 Echo (ping) reply id=0x0f
20	32.769041000	192.168.50.66	192.168.50.5	ICMP	98 Echo (ping) request id=0x0f
21	32.770036000	192.168.50.5	192.168.50.66	ICMP	98 Echo (ping) reply id=0x0f
22	33.769879000	192.168.50.66	192.168.50.5	ICMP	98 Echo (ping) request id=0x0f
23	33.770349000	192.168.50.5	192.168.50.66	ICMP	98 Echo (ping) reply id=0x0f
24	33.769921000	192.168.50.66	192.168.50.5	ICMP	98 Echo (ping) request id=0x0f
25	33.770338000	192.168.50.5	192.168.50.66	ICMP	98 Echo (ping) reply id=0x0f
26	38.991066000	192.168.50.4	192.168.50.5	Syslog	130 AUTHPRIV.INFO: Oct 17 10:02:
27	419.531043000	192.168.50.4	192.168.50.5	Syslog	176 AUTHPRIV.NOTICE: Oct 17 10:6

Запустим sql-инъекцию с kali на машину с установленным snort:(http://sqlmap.org/)
Команда для скачивания: git clone --depth 1 https://github.com/sqlmapproject/sqlmap.git sqlmap-dev
Запустите sqlmap на BASE по запросу http://ip-адрес snort/base/base_stat_alerts.php?sensor=1
Результатов не будет, потому что snort не настроен для обнаружения данной атаки.
В отчёт вставьте скриншот.
Создайте следующее правило:
alert tcp any any -> any any (msg: "SQL Injection"; content: "GET"; http_method; uricontent: "and 1=1"; nocase; sid:3000001; rev:1;)
Снова запустите атаку и посмотрите результаты.
В отчёт вставьте скриншот с результатами.

```
tasha@pk2:~$ git clone --depth 1 https://github.com/sqlmapproject/sqlmap.git sqlmap-dev
Клонирование в «sqlmap-dev»…
remote: Enumerating objects: 694, done.
remote: Counting objects: 100% (694/694), done.
remote: Compressing objects: 100% (627/627), done.
remote: Total 694 (delta 217), reused 222 (delta 56), pack-reused 0
Получение объектов: 100% (694/694), 6.56 MiB | 7.27 MiB/s, готово.
Определение изменений: 100% (217/217), готово.
tasha@pk2:~$
```

```
10/17-11:43:07.077920  [**] [1:2013929:1] ET POLICY HTTP traffic on port 443 (OPTIONS) [**] [Classification: Potentially
 Bad Traffic] [Priority: 2] {TCP} 192.168.1.129:49709 -> 192.168.1.250:443
10/17-11:43:13.534251  [**] [1:2009358:5] ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine) [**]
 [Classification: Web Application Attack] [Priority: 1] {TCP} 192.168.1.129:58976 -> 192.168.1.250:80
10/17-11:43:13.534337  [**] [1:2009358:5] ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine) [**]
 [Classification: Web Application Attack] [Priority: 1] {TCP} 192.168.1.129:58977 -> 192.168.1.250:80
10/17-11:43:13.685675  [**] [1:2003068:6] ET SCAN Potential SSH Scan OUTBOUND [**] [Classification: Attempted Informatio
n Leak] [Priority: 2] {TCP} 192.168.1.129:34981 -> 192.168.1.250:22
10/17-11:43:13.685675  [**] [1:2001219:18] ET SCAN Potential SSH Scan [**] [Classification: Attempted Information Leak]
[Priority: 2] {TCP} 192.168.1.129:34981 -> 192.168.1.250:22
10/17-11:43:13.735278  [**] [1:2009358:5] ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine) [**]
 [Classification: Web Application Attack] [Priority: 1] {TCP} 192.168.1.129:58982 -> 192.168.1.250:80
```

3.1.3. Оценка освоения теоретического курса профессионального модуля по МДК.03.04

Дидактические единицы	Проверяемые ОК, ПК	Формы контроля (наименование контрольной точки)	
		Текущая аттестация	Промежуточная аттестация
Тема 4.1. Использование программно-аппаратных средств для создания защищённой сети	ОК 1- 9 ПК 3.3, ПК 3.6	Практическая работа № 4 Создание структуры защищённой сети ViPNet	Устный ответ на экзамене
		Практическая работа № 10 Настройка политик безопасности в VipNet Policy Manager	

Дидактические единицы	Проверяемые ОК, ПК	Формы контроля (наименование контрольной точки)	
		Текущая аттестация	Промежуточная аттестация
		Практическая работа № 11 «Межсетевое взаимодействие»	
Тема 4.2 Использование DLP-системы Infowatch для защиты от внутренних утечек информации	ОК 1- 9 ПК 3.3, ПК 3.6	Практическая работа № 14 «Установка и настройка Traffic monitor»	
		Практическая работа № 25 «Добавление политик безопасности в Traffic monitor»	
		Практическая работа № 26 «Создание политик с использованием перехвата фотографий в Traffic monitor»	
		Практическая работа № 33 «Создание и изменение отчётов в Traffic Monitor»	
	ОК 1- 9 ПК 3.3, ПК 3.6	Устный зачёт по темам 3.1. – 3.2.	

3. Практическая работа № 4 «Создание структуры защищённой сети ViPNet»

Задание:

Создание клиентов

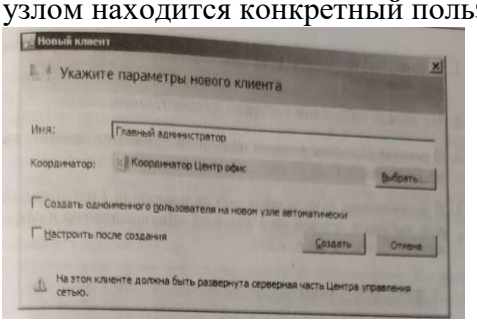
В соответствии со схемой развертывания ViPNet в сети компании необходимо создать клиенты: Главный администратор, Помощник глав админа, Сотрудник_1 Центр офис, Сотрудник_2 Филиал.

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:

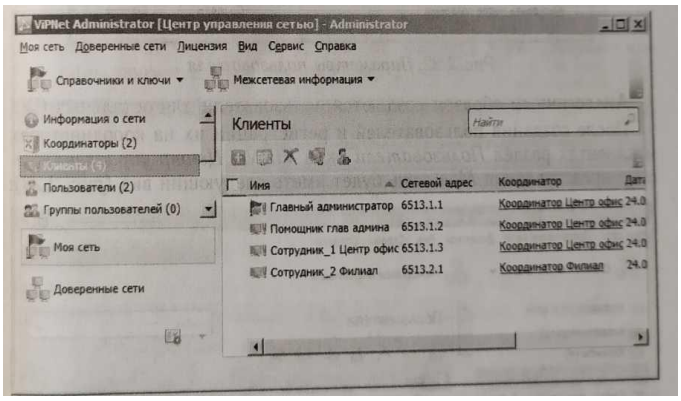
1. В окне ViPNet Центр управления сетью выберите представление Моя сеть.
2. На панели навигации выберите раздел Клиенты.
3. В разделе Клиенты на панели инструментов нажмите кнопку Создать.
4. В появившемся окне задайте имя Главный администратор, выберите координатор Координатор Центр офис для регистрации 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:

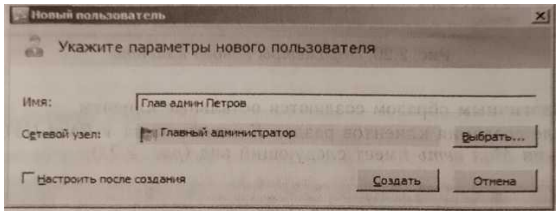


Созданным клиентам автоматически назначаются роли – VPN-клиент, Business Mail и Обмен сообщениями и файлами, а для первого созданного клиента, дополнительно — системные роли Network Control Center и Policy Manager. Чтобы убедиться в этом, зайдите в свойства клиента (двойной щелчок по выбранному узлу),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

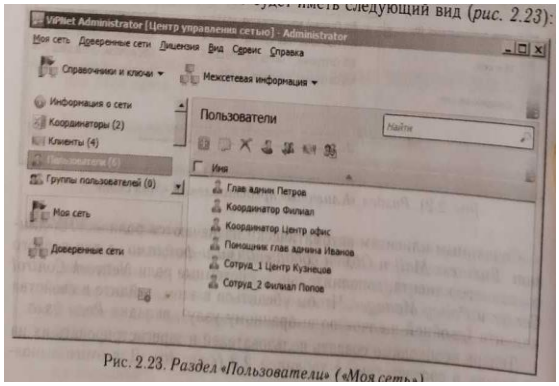


Рис. 2.23. Раздел «Пользователи» («Моя сеть»)

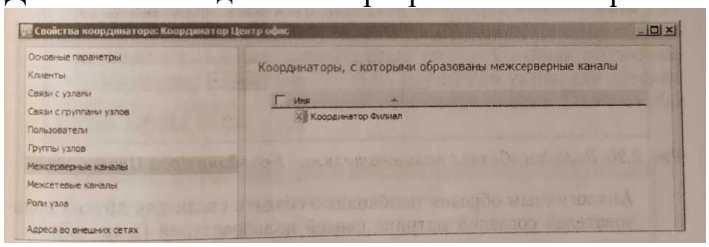
Вставьте скриншот, подтверждающий выполнение задания

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:

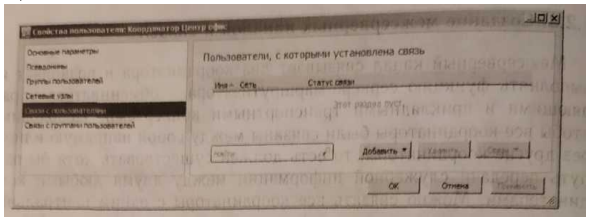
1. Перейдите в свойства СУ Координатор Центр офис (двойной щелчок по выбранному узлу).
2. На вкладке Межсерверные каналы нажмите кнопку Добавить.
3. В открывшемся окне выберите сетевой узел Координатор Филиал и нажмите кнопку Добавить. Вкладка Межсерверные каналы примет следующий вид.



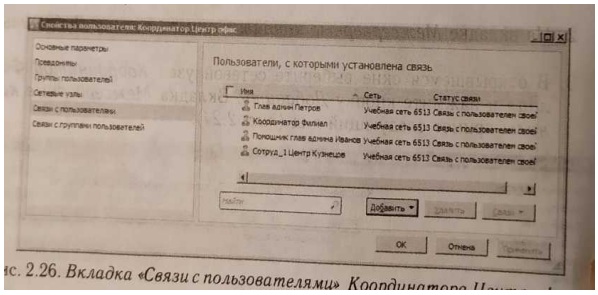
Теперь необходимо создать связи между пользователями в соответствии с матрицей связей пользователей защищенной сети

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:



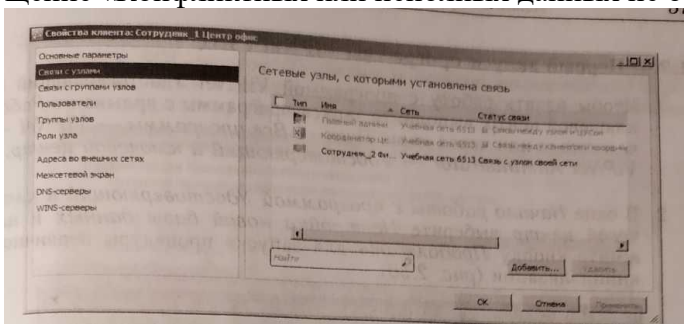
ис. 2.26. *Вкладка «Связи с пользователями» Координатора Центр*

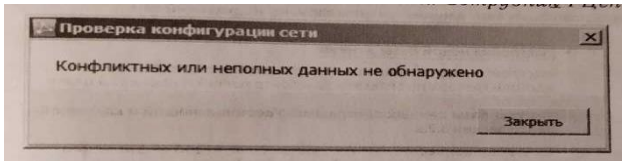
Аналогичным образом необходимо создать связи для других пользователей согласно матрице связей пользователей.

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

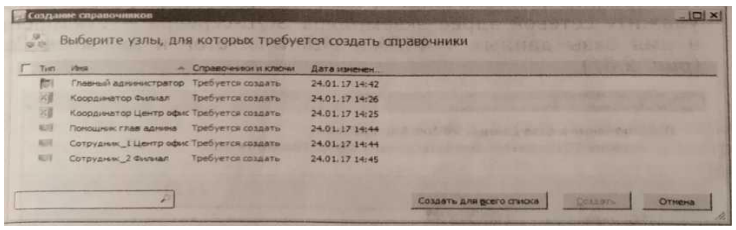
Примечание. Рекомендуется устанавливать в первую очередь связи между пользователями. Появиться возможность вести конфиденциальную переписку между конкретными пользователями, а не узлами.

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».





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.



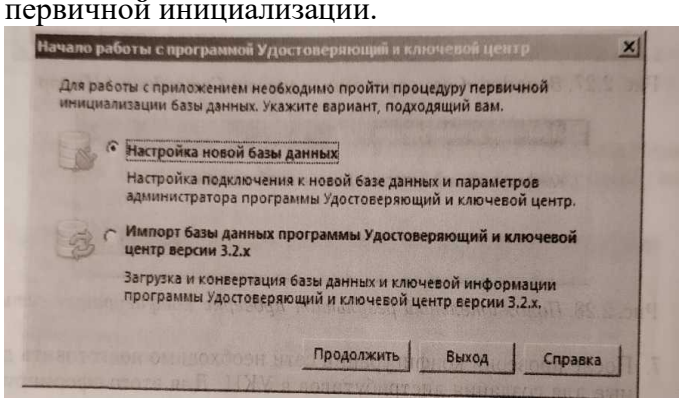
Примечание. Справочники содержат информацию о сетевых узлах, пользователях и их свойствах - идентификаторах, связях, ролях сетевых узлов, адресах и так далее.

После создания справочников можно перейти к первому запуску компонента ViPNet Удостоверяющий и ключевой центр.

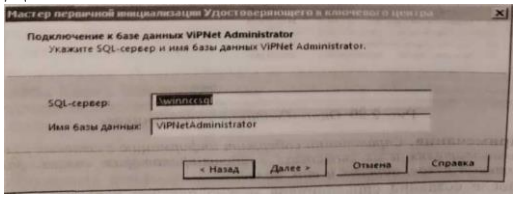
Вставьте скриншот, подтверждающий выполнение задания

Первый запуск программы ViPNet УКЦ

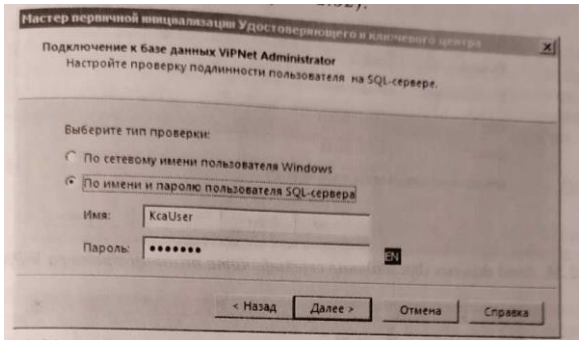
1. Чтобы начать работу с программой ViPNet Удостоверяющий и ключевой центр, выполните запуск программы с ярлыка на Рабочем столе или через меню Пуск → Все программы → ViPNet →ViPNet Administrator → Удостоверяющий и ключевой центр.
2. В окне Начало работы с программой Удостоверяющий и ключевой центр выберите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



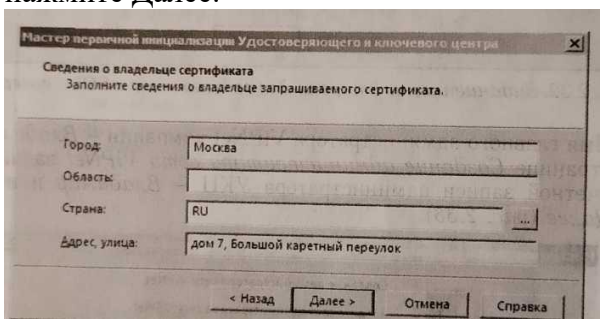
3. На первой странице мастера инициализации нажмите Далее.
4. На странице Подключение к базе данных ViPNet Administrator укажите сетевой адрес экземпляра SQL-сервера - .\winnccsql и имя базы данных - ViPNet Administrator и нажмите Далее.

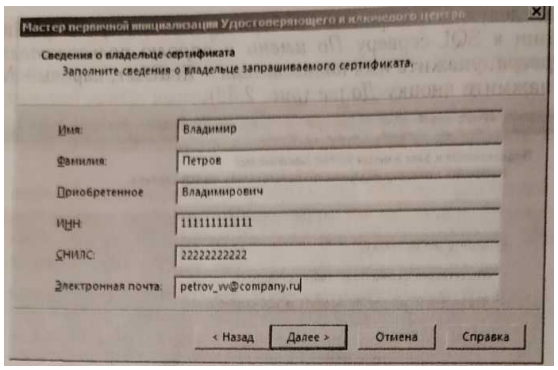


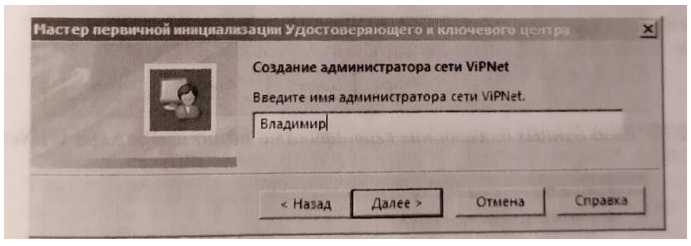
5. На следующей странице выберите тип проверки при подключении к SQL-серверу По имени и паролю пользователя SQL- сервера, укажите имя пользователя - KcaUser, пароль - Humbert и нажмите кнопку Далее:



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





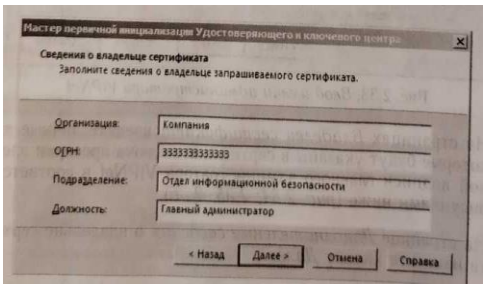


7. На страницах Владелец сертификата введите личные данные, которые будут указаны в сертификате ключа проверки электронной подписи главного администратора ViPNet в соответствии с рисунками ниже:
8. На странице Дополнительные сведения о владельце сертификата нажмите кнопку Далее.
9. На странице Параметры 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 запомнить 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

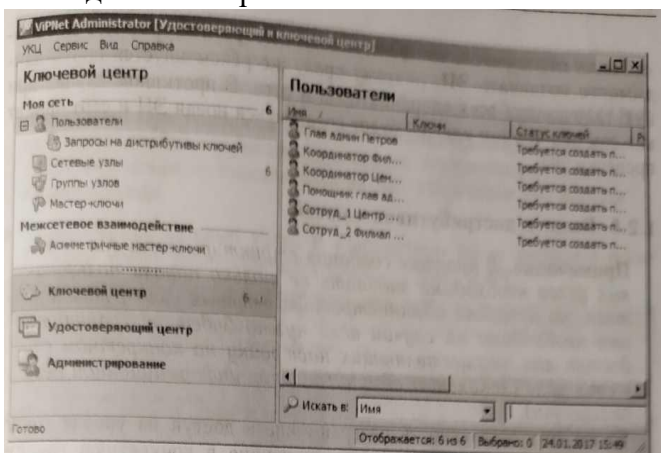
(восемь единиц).
СОВЕТ. При выполнении практических занятий рекомендуется использовать, простые запоминающиеся пароли во всех программах (например, 11111111 - восемь единиц).

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 па-

роль, 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

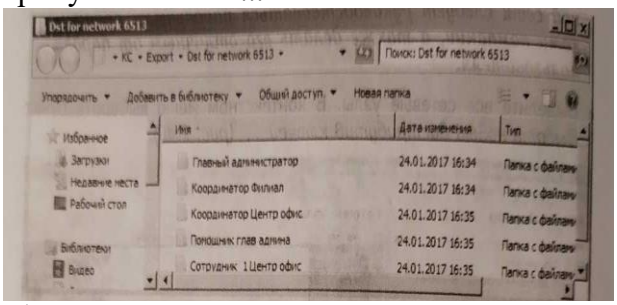
Внимание! Пароли администратора (группы или узла) нельзя передавать или каким-либо образом сообщать пользователю узла. Данный тип паролей предназначен исключительно для администрирования конкретного узла или группы узлов и может быть сообщен только лицу ответственному за настройку и контроль работоспособности 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...



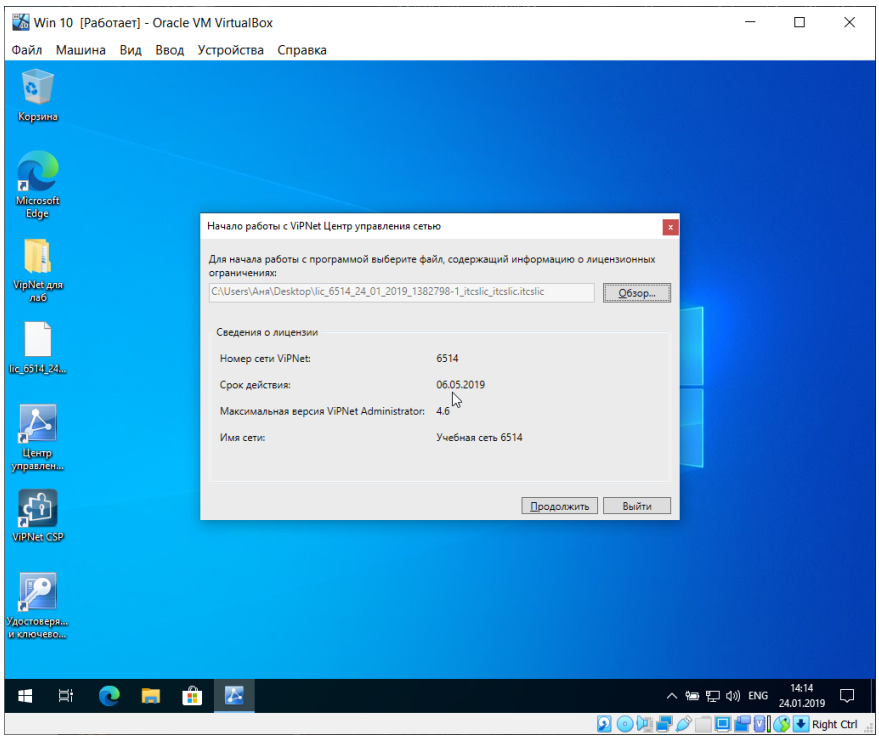
✓ Задайте пароль пользователя — 11111111 по очереди для каждого пользователя защищенной сети.
После окончания выдачи дистрибутива откроется окно проводника с папкой, содержащей подкаталоги сетевых узлов с готовыми дистрибутивами. Запомните путь до этой папки или измените папку, используемую по умолчанию 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:

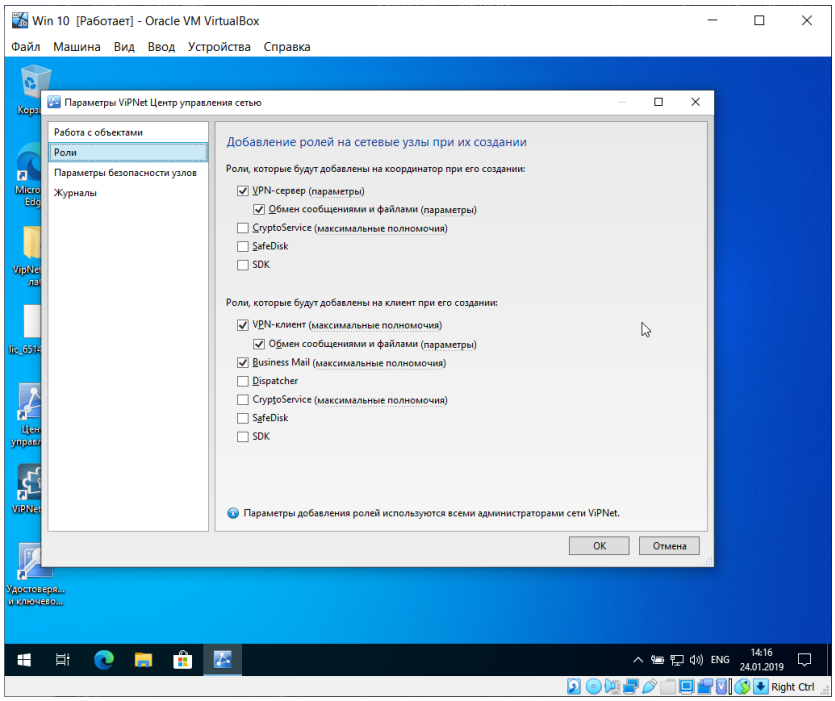
✓ Дистрибутив ключей (dst-файл).
✓ Пароль пользователя.
Вставьте скриншот, подтверждающий выполнение задания

Эталон ответа:

1. 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).



2. В появившемся окне с выбором возможных сценариев работы нажмите Настроить структуру защищенной сети самостоятельно
3. Откроется главное окно программы
4. 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 п ров в соответствии

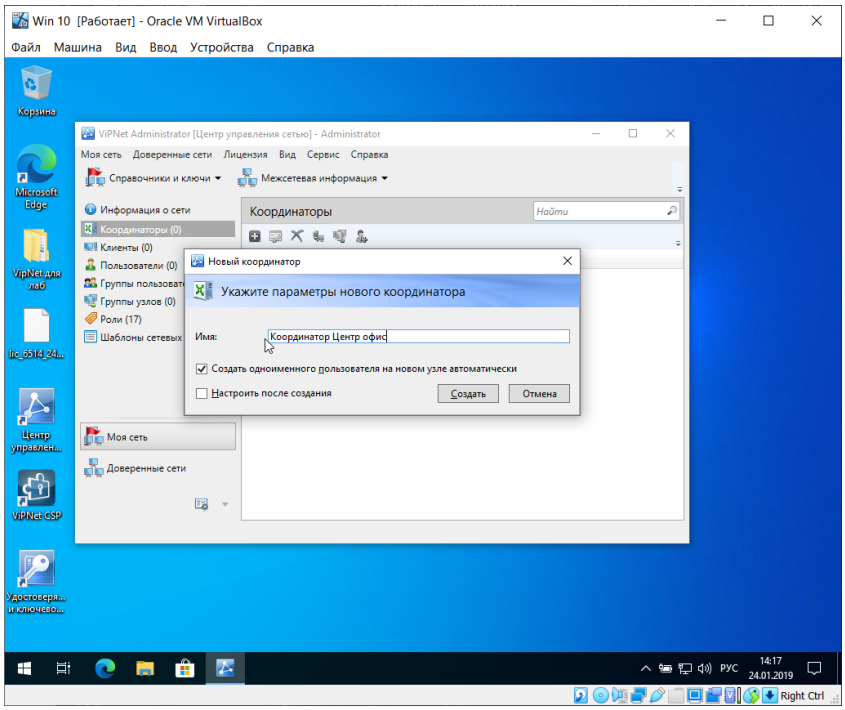


Теперь можно приступить к созданию структуры защищённой сети.

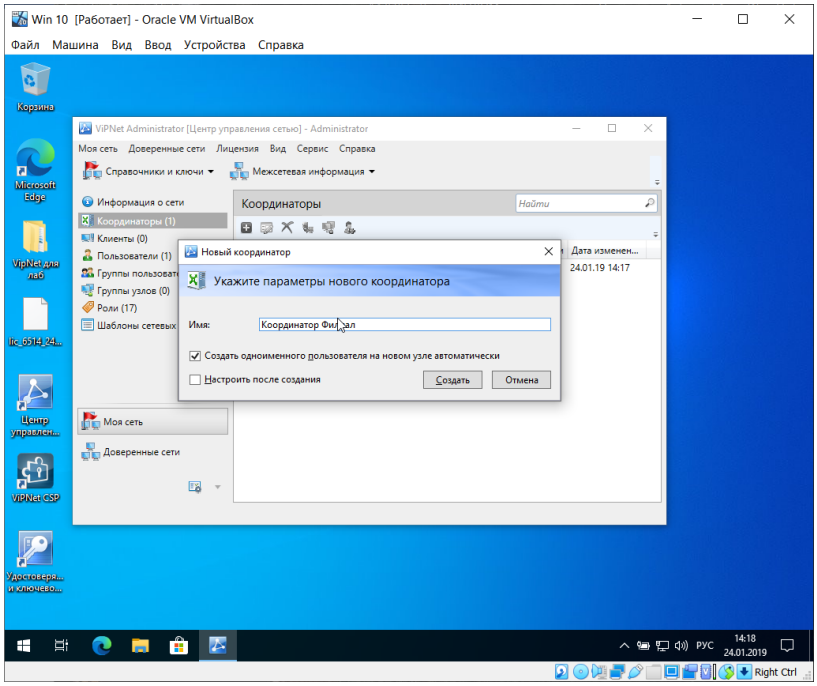
Создание координаторов

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).

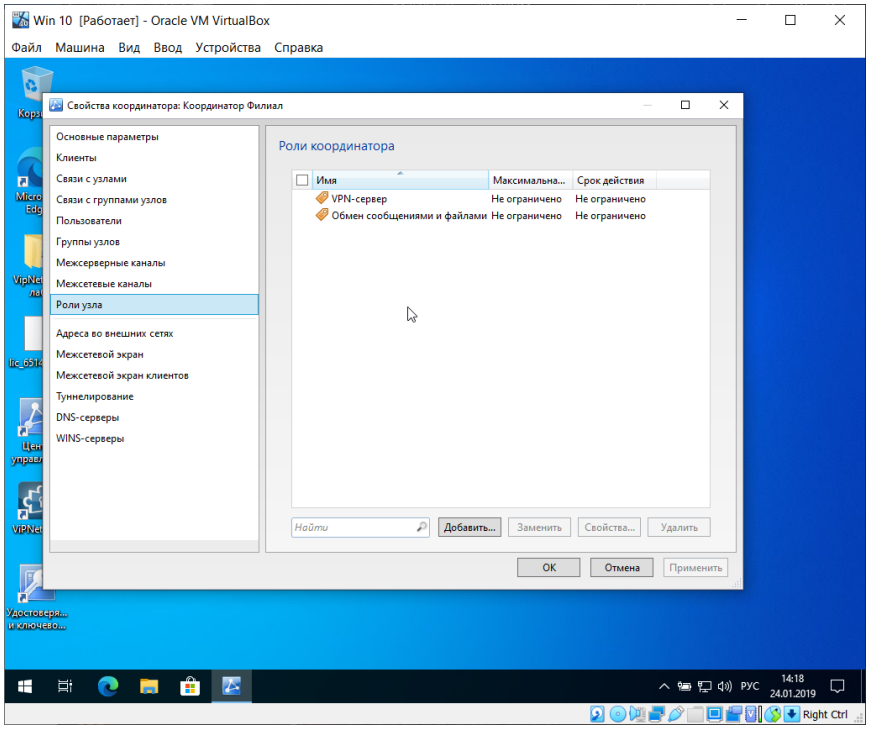


Аналогичным образом создается сетевой узел Координатор Филиал.

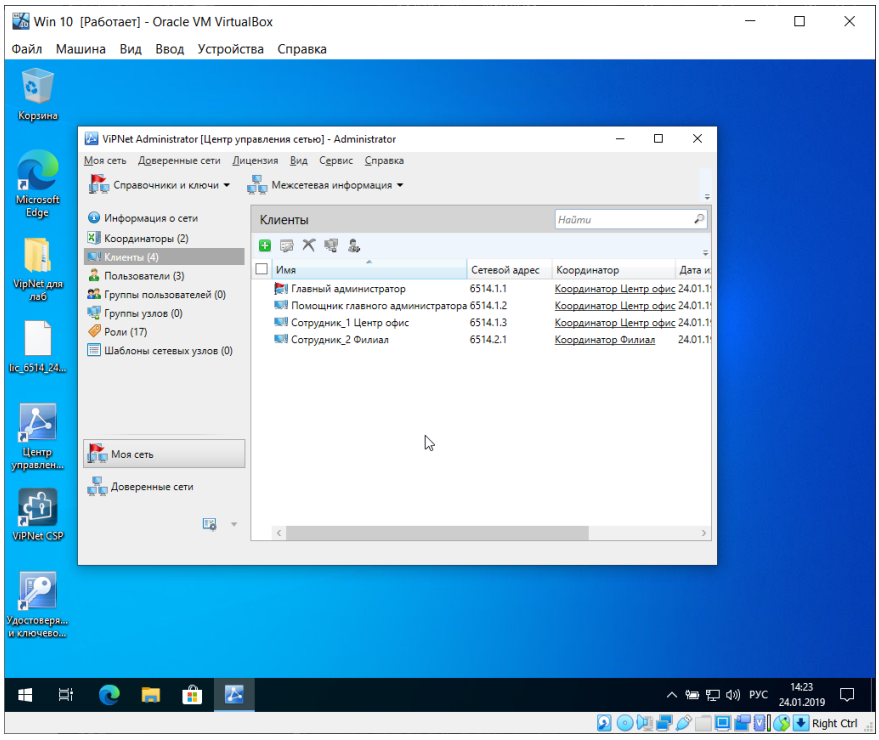


После создания раздел Координаторы окна ViPNet Центр управления сетью представления Моя сеть будет иметь следующий вид:

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



Создание клиентов

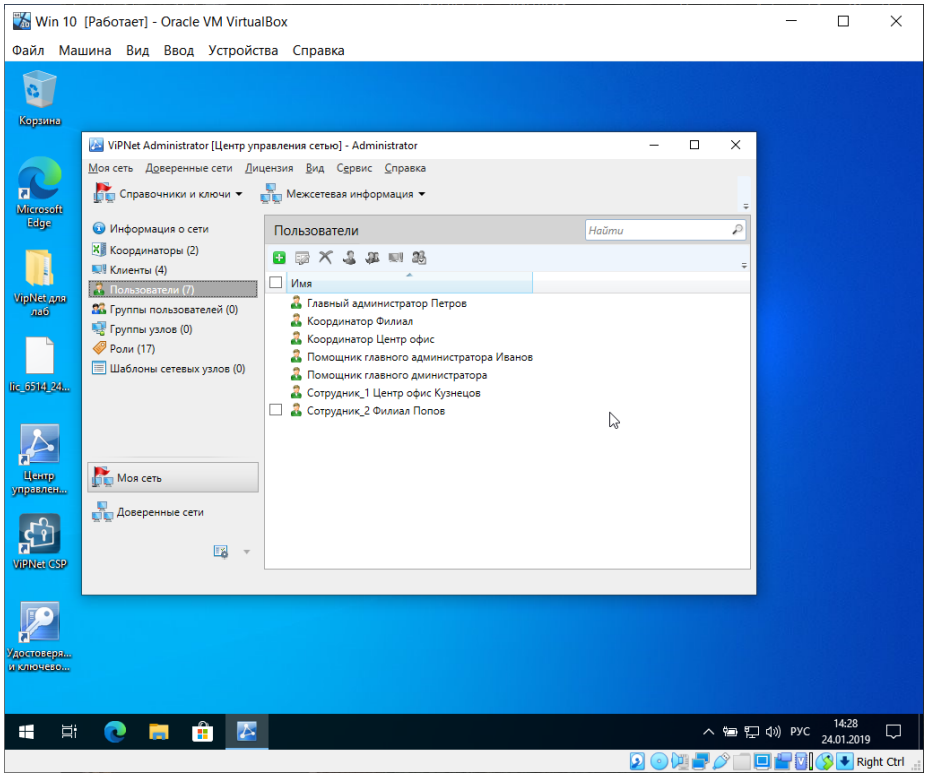


Созданным клиентам автоматически назначаются роли – VPN-клиент, Business Mail и Обмен сообщениями и файлами, а для первого созданного клиента, дополнительно — си-

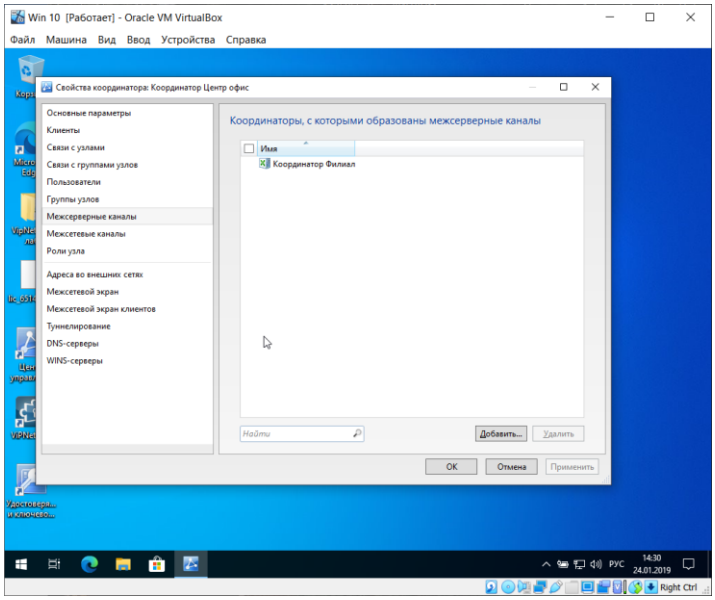
стемные роли Network Control Center и Policy Manager. Чтобы убедиться в этом, зайдите в свойства клиента (двойной щелчок по выбранному узлу), вкладка Роли узла.

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



Создание межсерверных каналов и связей



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

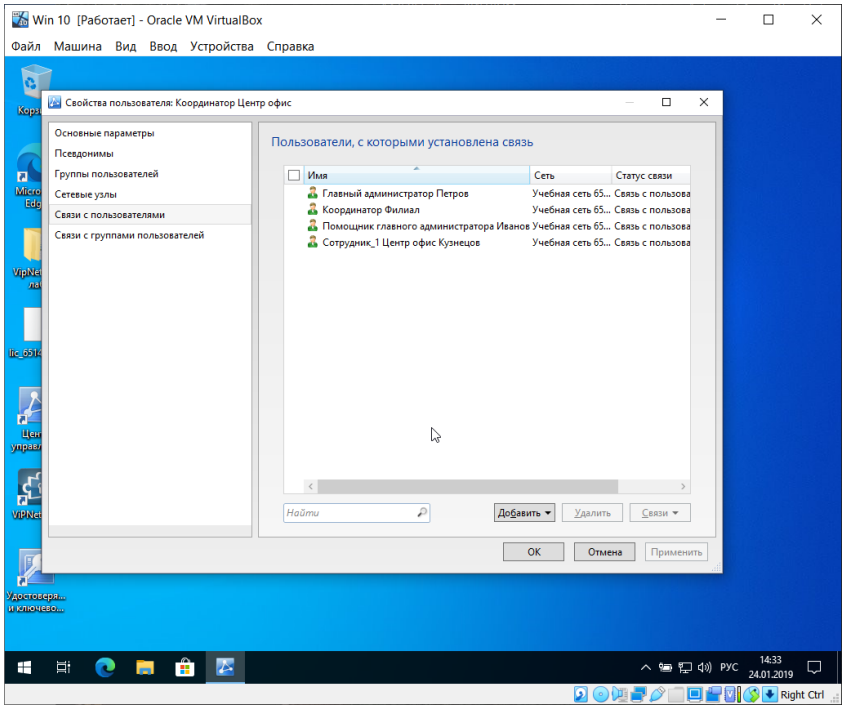
8. Перейдите в свойства пользователя Координатор Центр офис (двойной щелчок по вы-

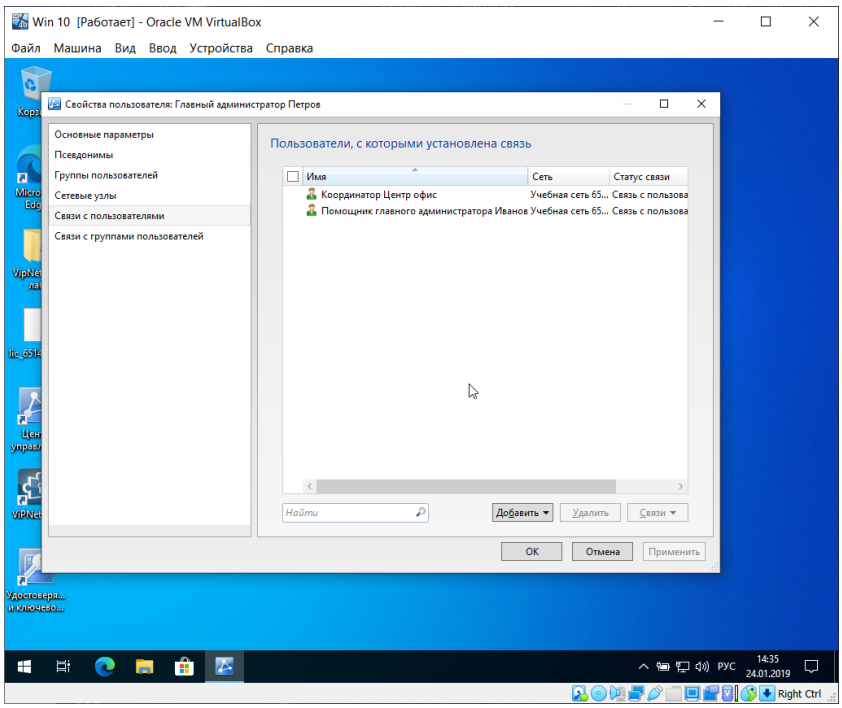
бранному узлу). Вкладка Связи с пользователями имеет следующий вид - на первоначальном этапе данный раздел пуст

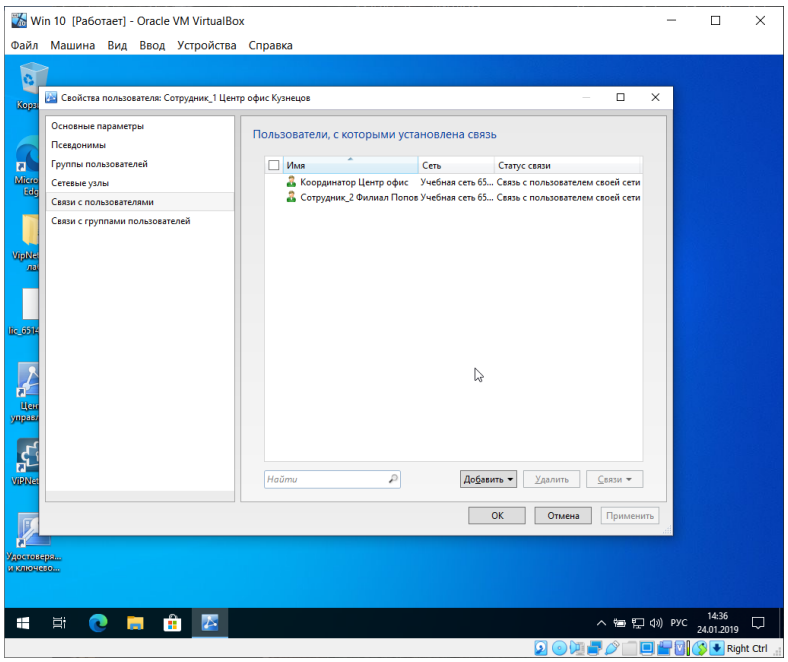
9. Добавьте связь пользователя Координатор Центр офис с пользователем Глав админ Петров. Для этого на вкладке Связи с пользователями нажмите кнопку Добавить и выберите из списка пользователя Глав админ Петров, а также других в соответствии с матрицей связей пользователей.

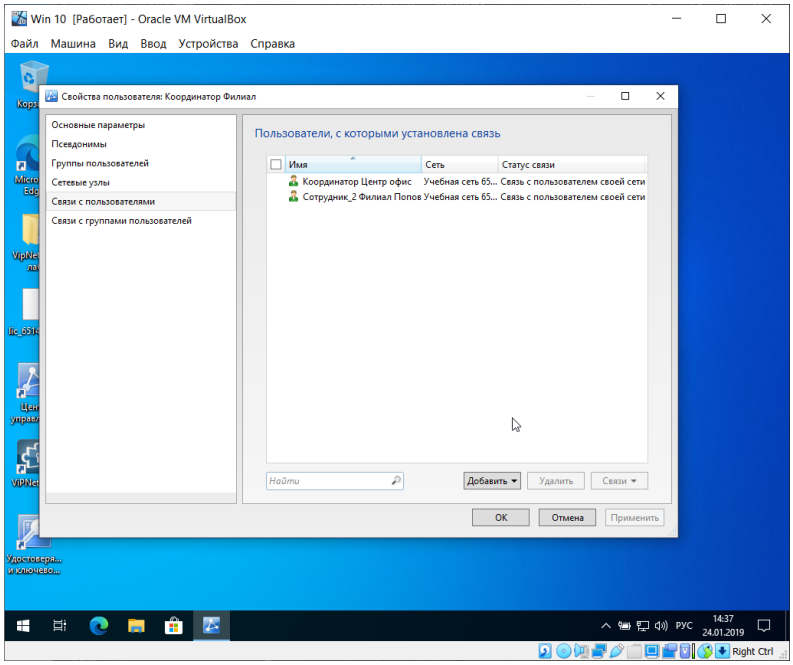
После связывания пользователей вкладка Связи с пользователями для Координатор Центр офис будет иметь следующий вид

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





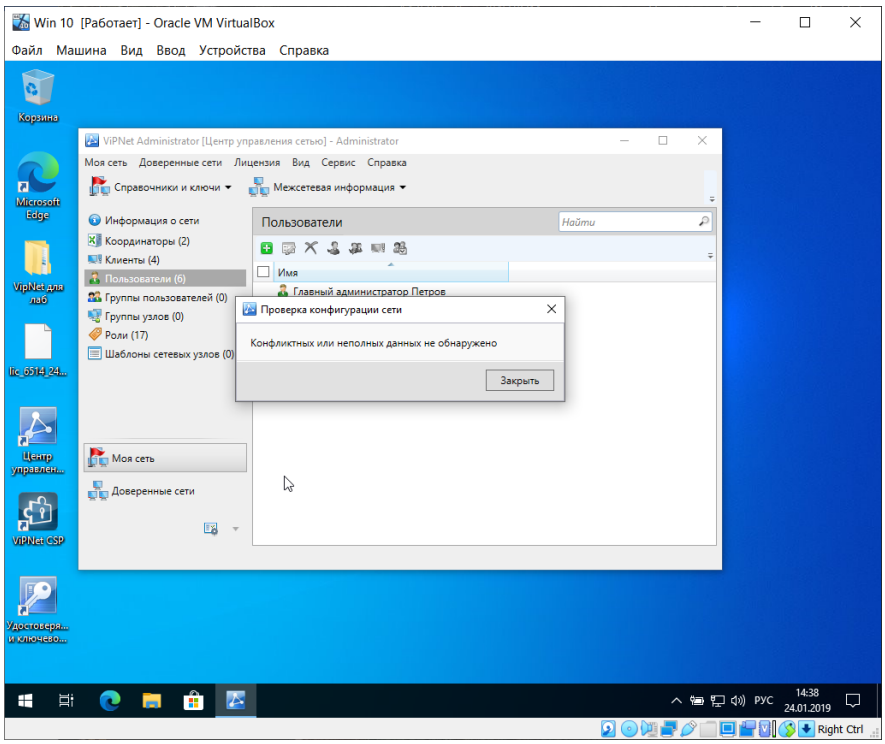




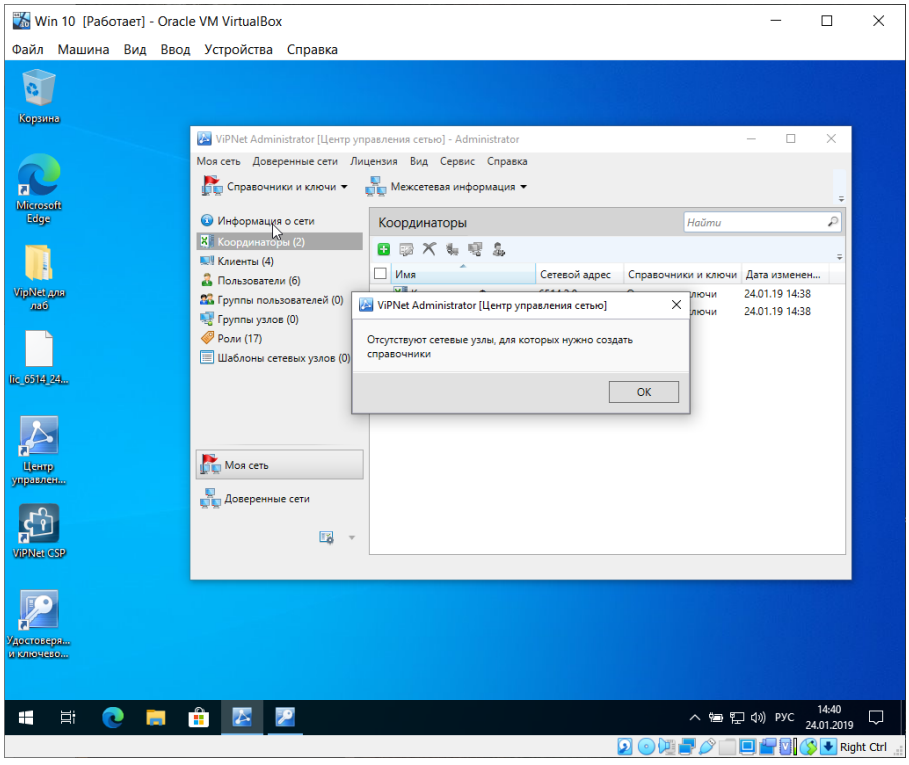
После этого автоматически будут созданы связи между узлами, к которым относятся связанные пользователи

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

10. 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»



11. 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.

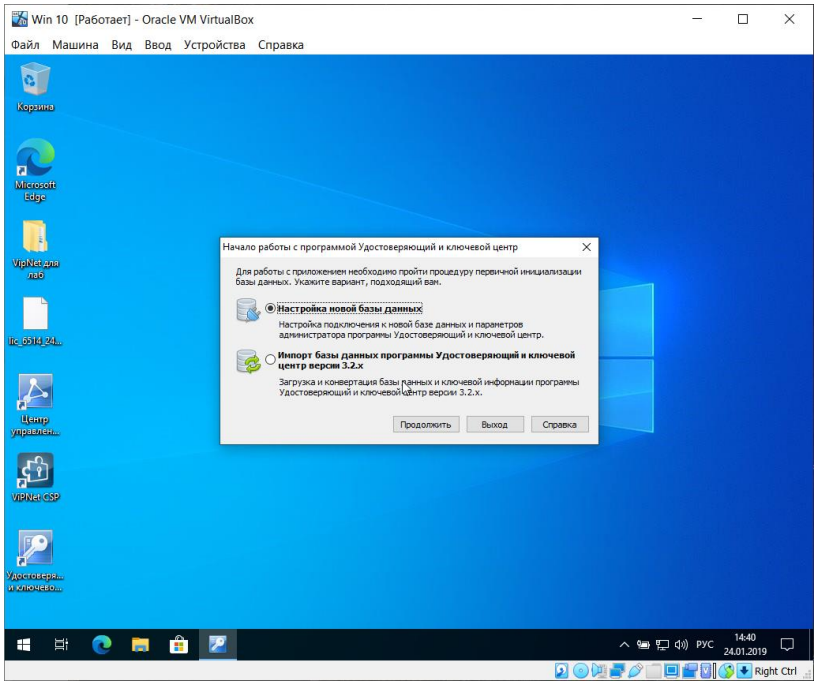


Создали.

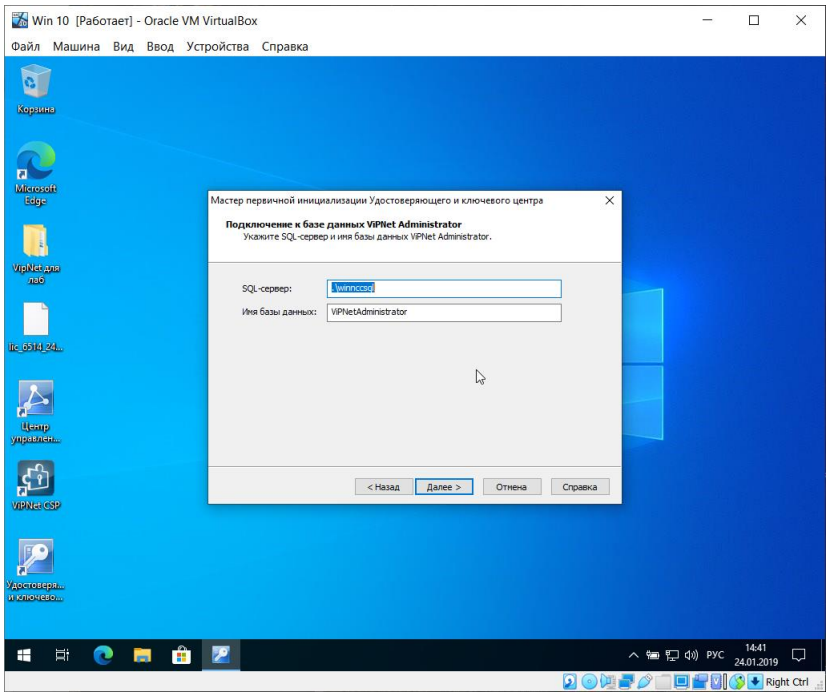
После создания справочников можно перейти к первому запуску компонента ViPNet Удостоверяющий и ключевой центр.

Первый запуск программы ViPNet УКЦ

17. 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.
18. В окне Начало работы с программой Удостоверяющий и ключевой центр выберите Настройка новой базы данных и нажмите кнопку Продолжить для запуска процедуры первичной инициализации



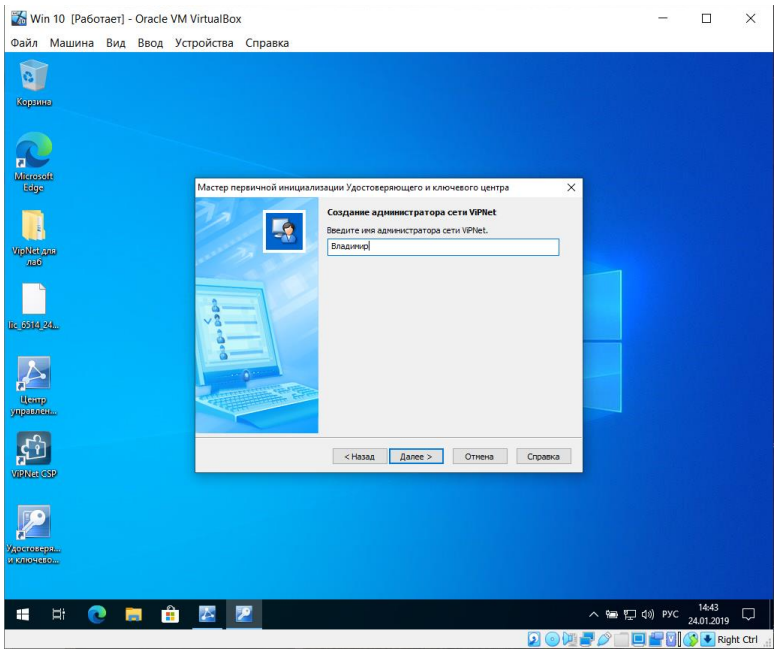
19. На первой странице мастера инициализации нажмите Далее.
20. На странице Подключение к базе данных ViPNet Administrator укажите сетевой адрес экземпляра SQL-сервера - .\winnccsql и имя базы данных - ViPNet Administrator и нажмите Далее



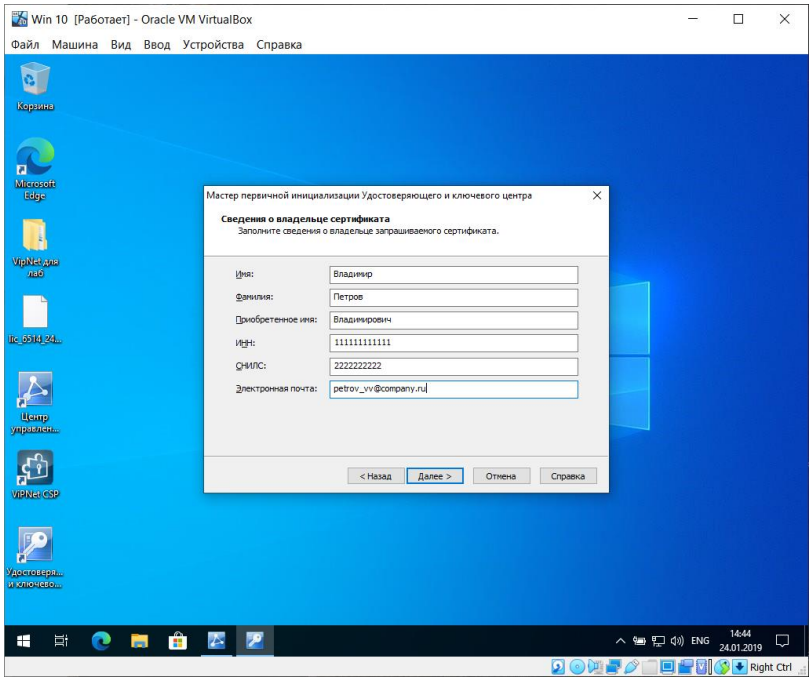
21. На следующей странице выберите тип проверки при подключении к SQL-серверу По

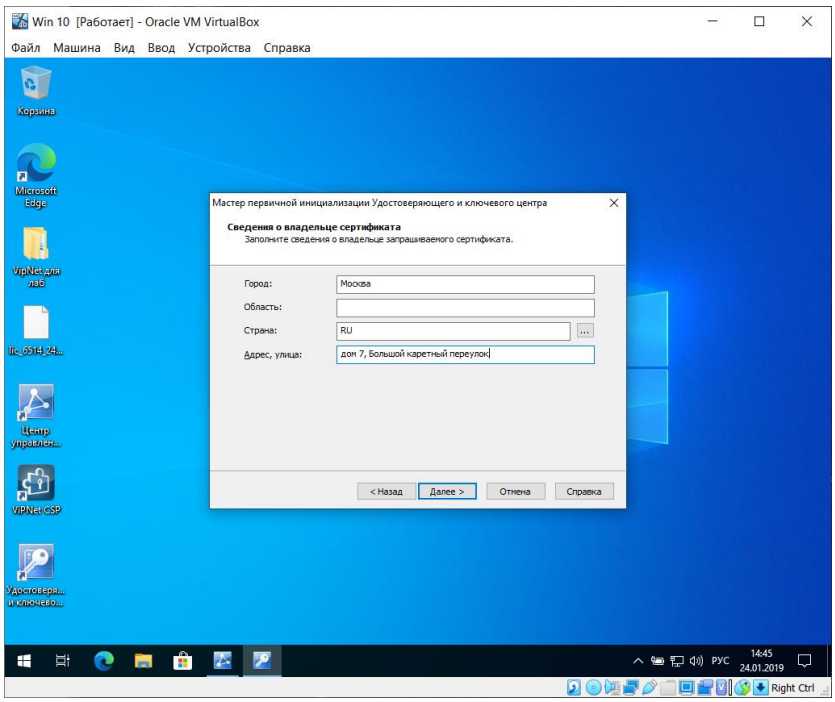
имени и паролю пользователя SQL- сервера, укажите имя пользователя - KcaUser, пароль - Humbert и нажмите кнопку Далее

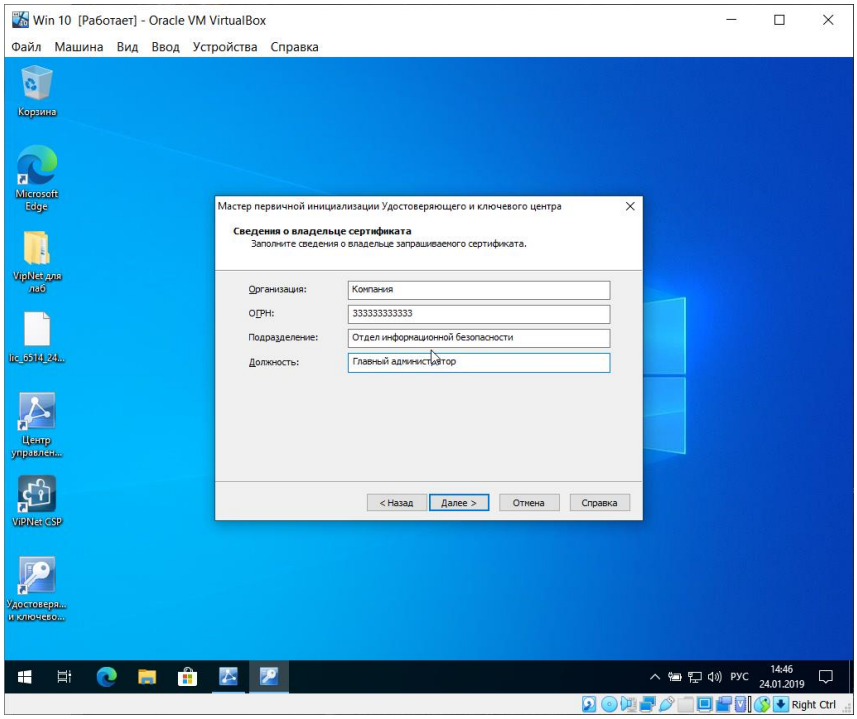
22. Имя главного администратора ViPNet компании - Владимир. На странице Создание администратора сети ViPNet задайте имя учетной записи администратора УКЦ - Владимир и нажмите Далее



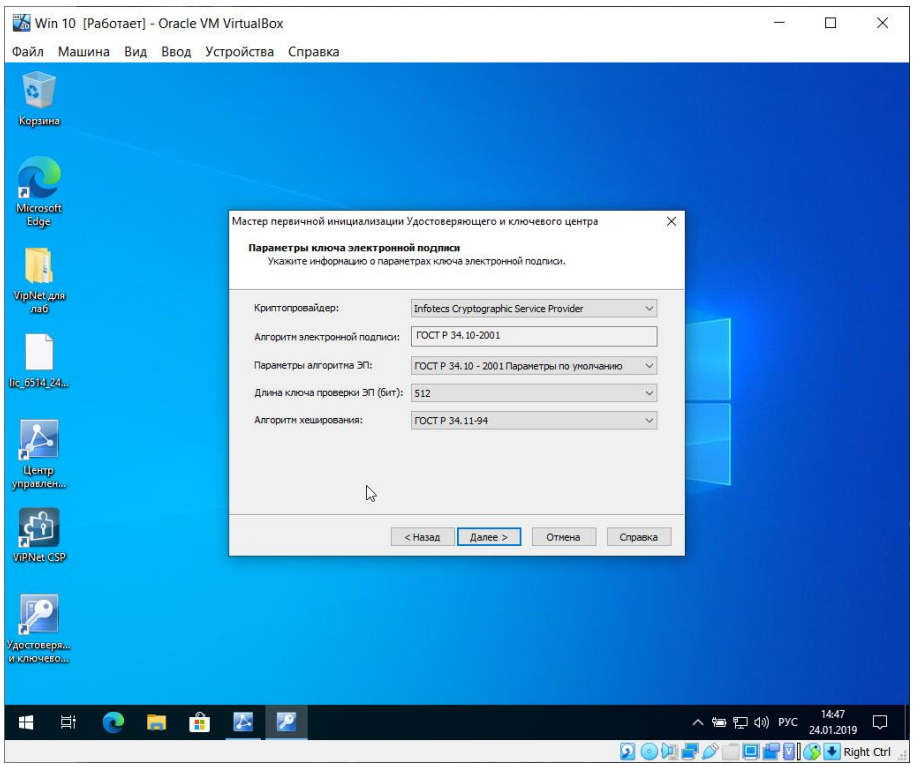
23. На страницах Владелец сертификата введите личные данные, которые будут указаны в сертификате ключа проверки электронной подписи главного администратора ViPNet в соответствии с рисунками ниже (рис. 2.34, 2.35, 2.36).



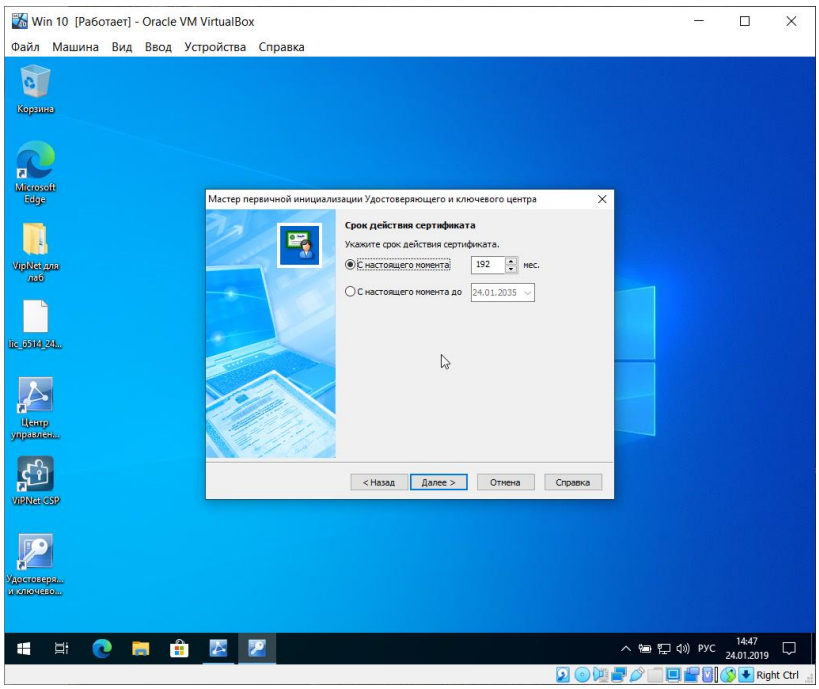




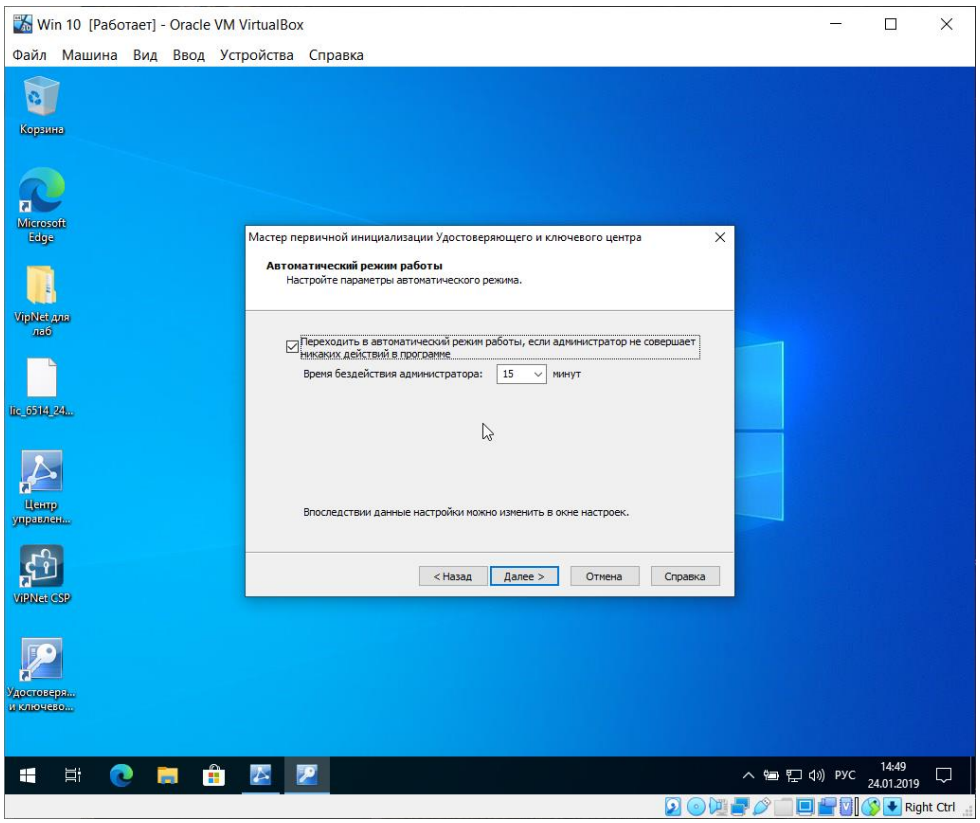
24. На странице Дополнительные сведения о владельце сертификата нажмите кнопку Далее.
25. На странице Параметры ключа электронной подписи оставьте значения ио умолчанию и нажмите кнопку Далее.



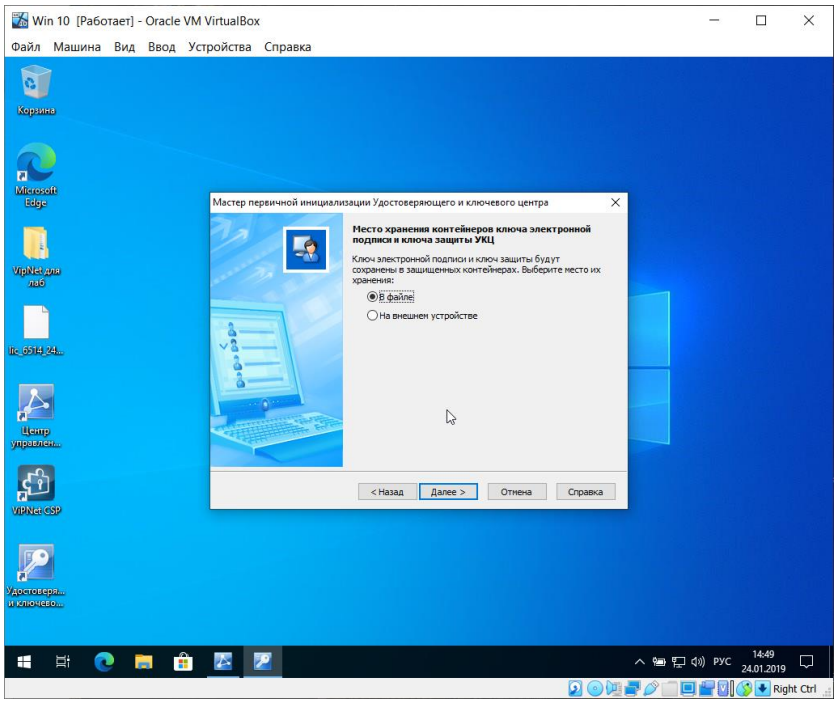
26. На странице Срок действия сертификата установите максимальное значение — 192 месяца с настоящего момента



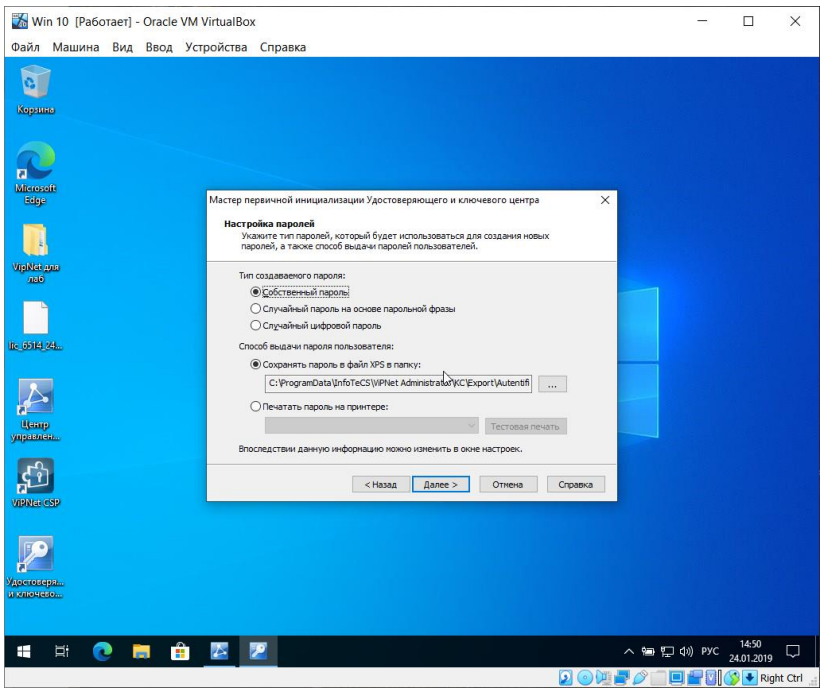
27. На странице Программные средства, в случае, если планируется осуществлять создание и выдачу квалифицированных сертификатов ключей проверки электронных подписей указываются программные продукты, используемые в качестве средства электронной подписи издателя, средства электронной подписи владельцев сертификатов и средства удостоверяющего центра.
28. На странице Автоматический режим работы нажмите Далее.

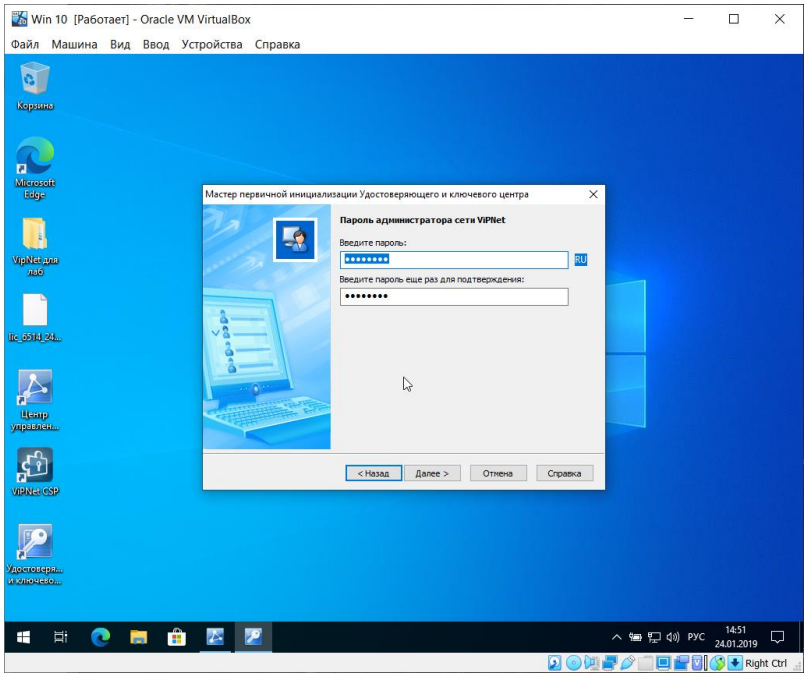


29. На странице Место хранения контейнеров ключа подписи и ключа защиты УКЦ выберите место хранения контейнера ключей администратора - В файле.

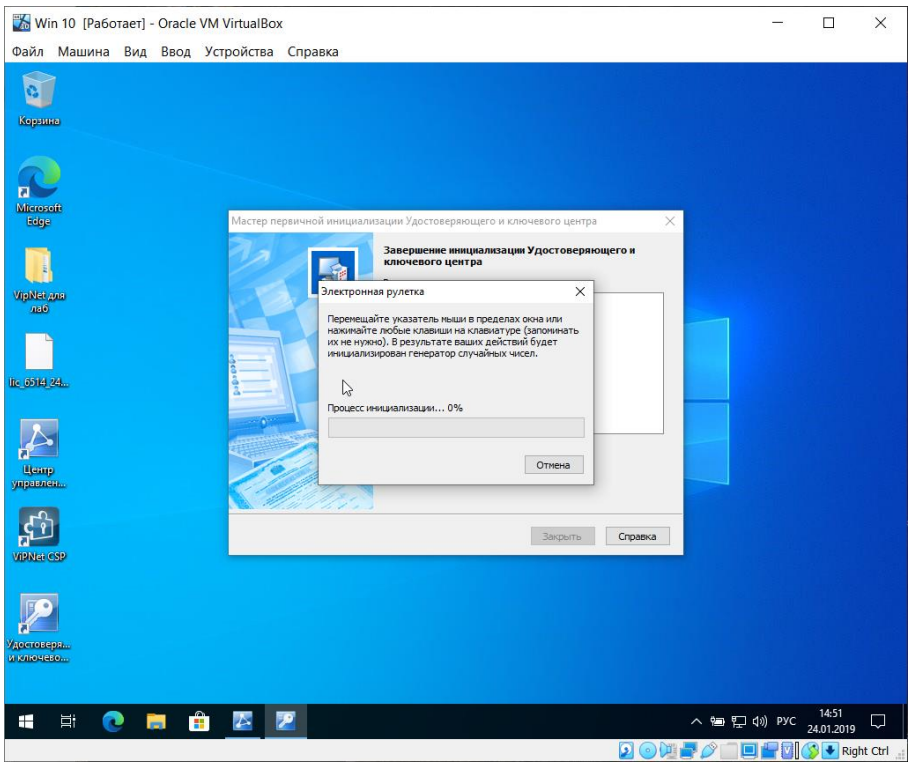


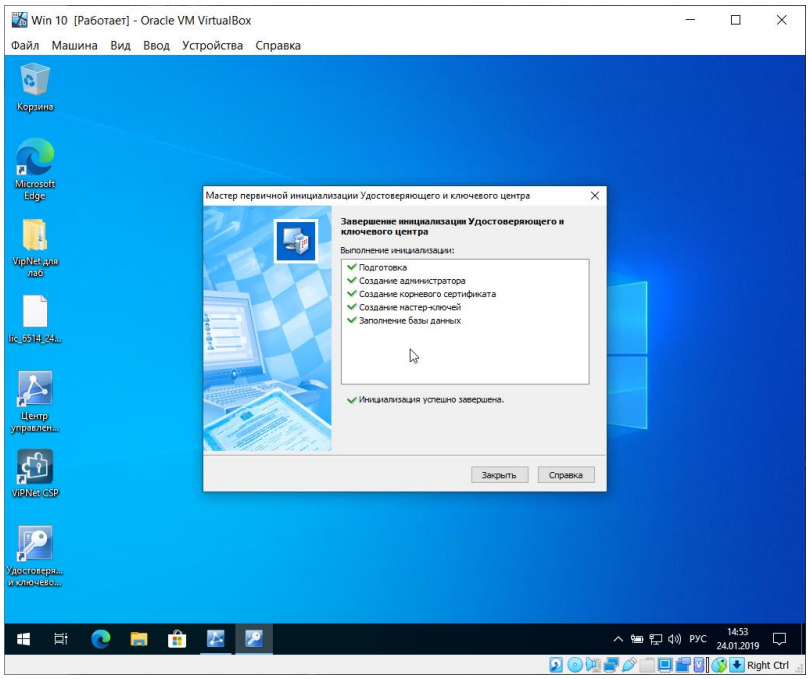
30. На странице Настройка паролей выберите тип создаваемого пароля - Собственный пароль, способ выдачи пароля пользователя - Сохранять пароль в файл XPS в папку (рекомендуется запомнить путь к данной папке или заменить на собственный, в дальнейшем его можно будет изменить на вкладке Сервис → Настройка... → Пароли), нажмите кнопку Далее. На появившейся странице задайте пароль администратора сети ViPNet - 11111111 (восемь единиц





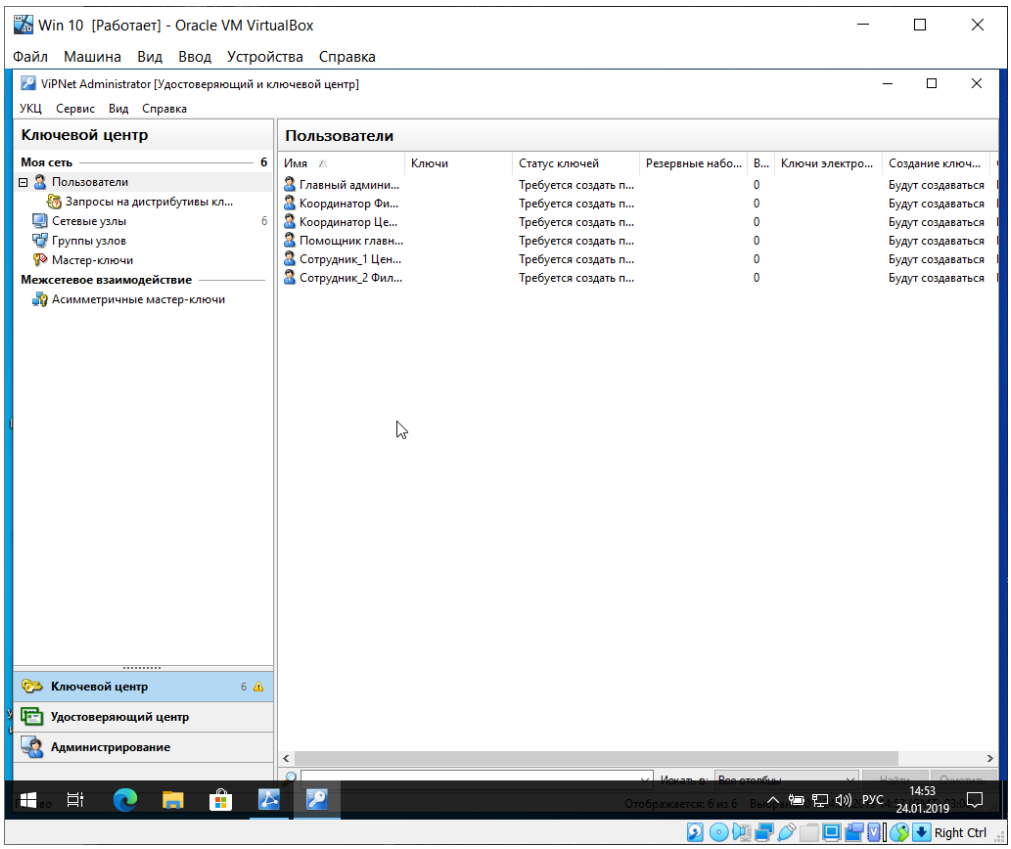
31. На странице готовности к завершению первичной инициализации убедитесь в правильности параметров, заданных на предыдущих страницах мастера. При изменении параметров вернитесь на нужную страницу с помощью кнопки Назад.
32. Для продолжения работы нажмите кнопку Далее. Поводите указателем в пределах окна Электронная рулетка и после успешного завершения инициализации нажмите Закрыть.



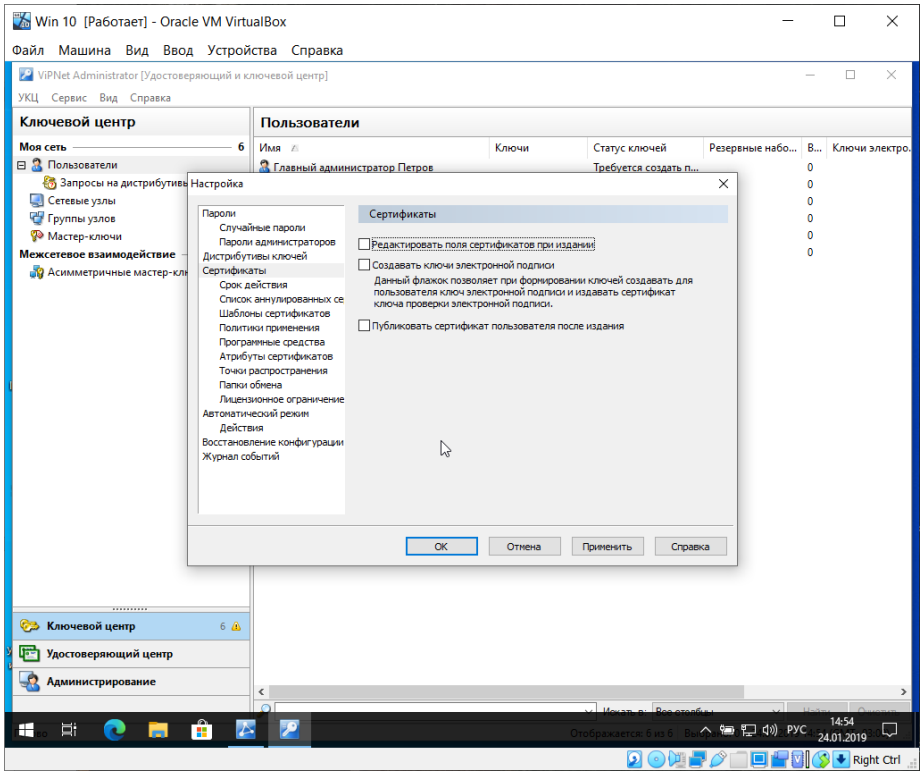


При успешном проведении первичной инициализации будет выполнены следующие операции:

✓ 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.

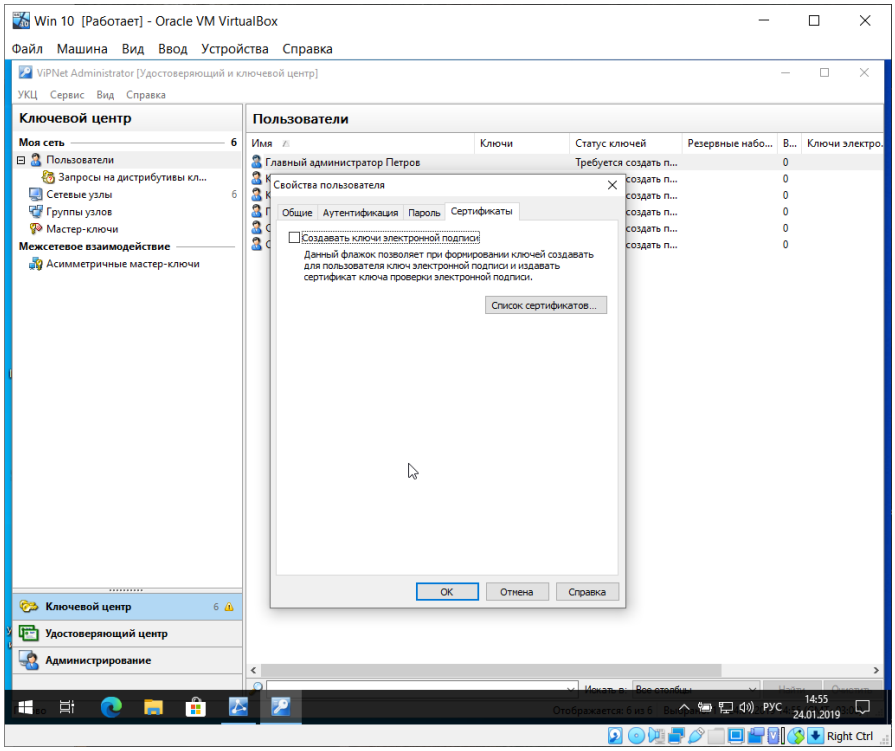


Перед началом работы в УКЦ проверьте первоначальные настройки программы. В меню Сервис выберите пункт Настройка. В открывшемся окне в разделе Пароли установите тип пароля, который будет использоваться при создании новых паролей, - Собственный пароль, на вкладке Сертификаты снимите флажки Редактировать поля сертификатов при издании и Создавать ключи электронной подписи.



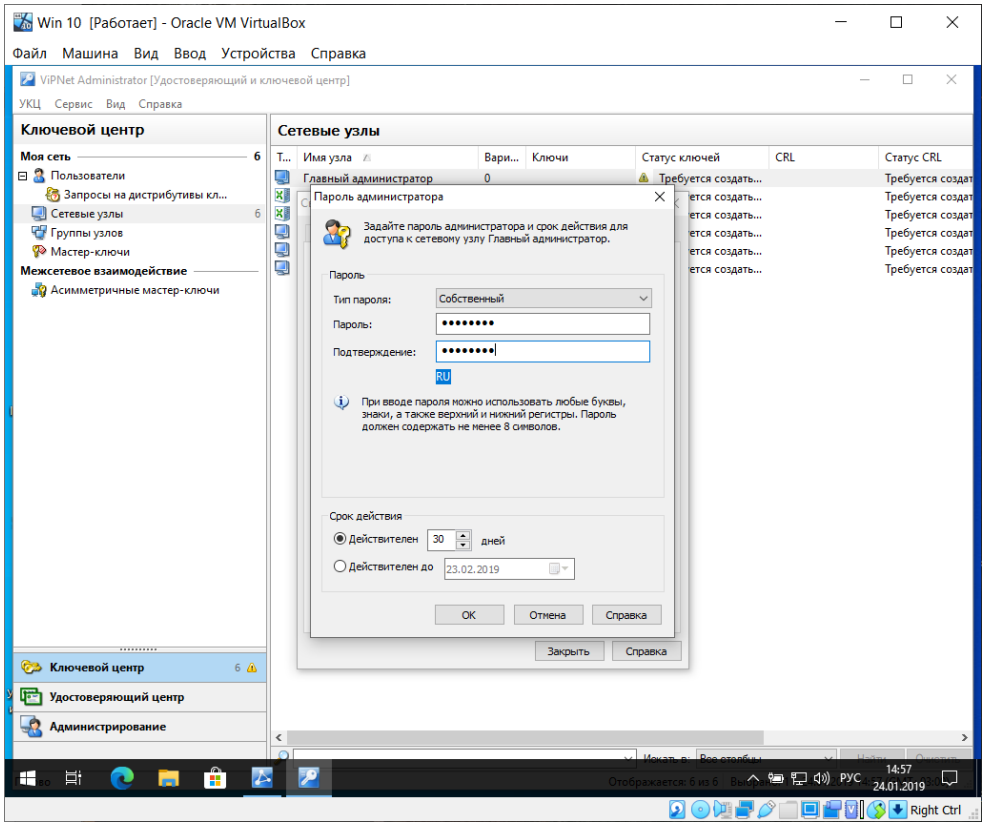
После проверки первоначальных настроек необходимо снять вручную флажок Создавать ключи электронной подписи в свойствах пользователей (УКЦ Моя сеть Пользователи,

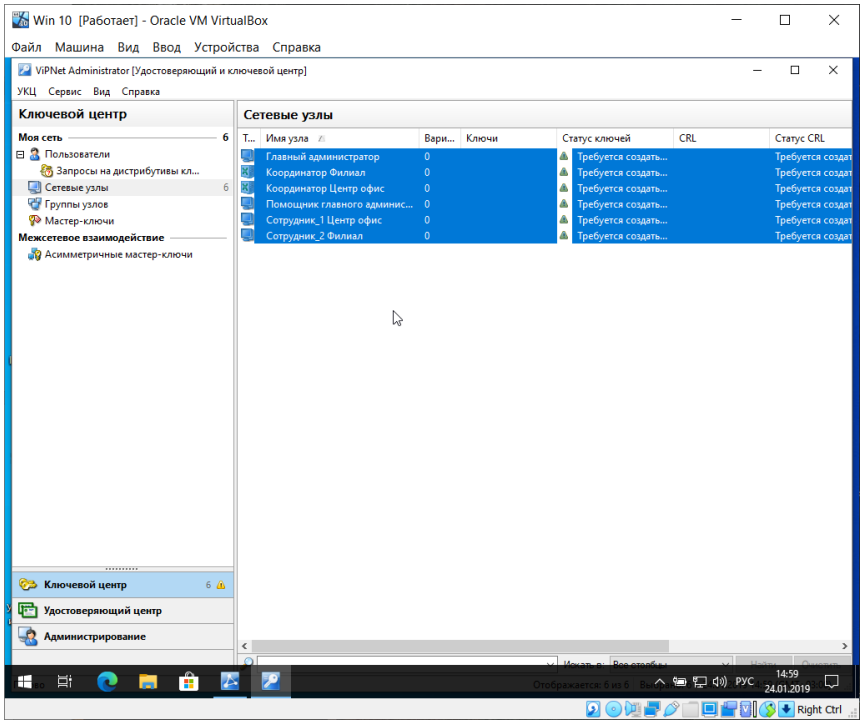
кликнуть правой кнопкой мыши на пользователя и выбрать пункт Ключи пользователя → Создавать ключи электронной подписи).



Теперь можно приступить к созданию дистрибутивов ключей.

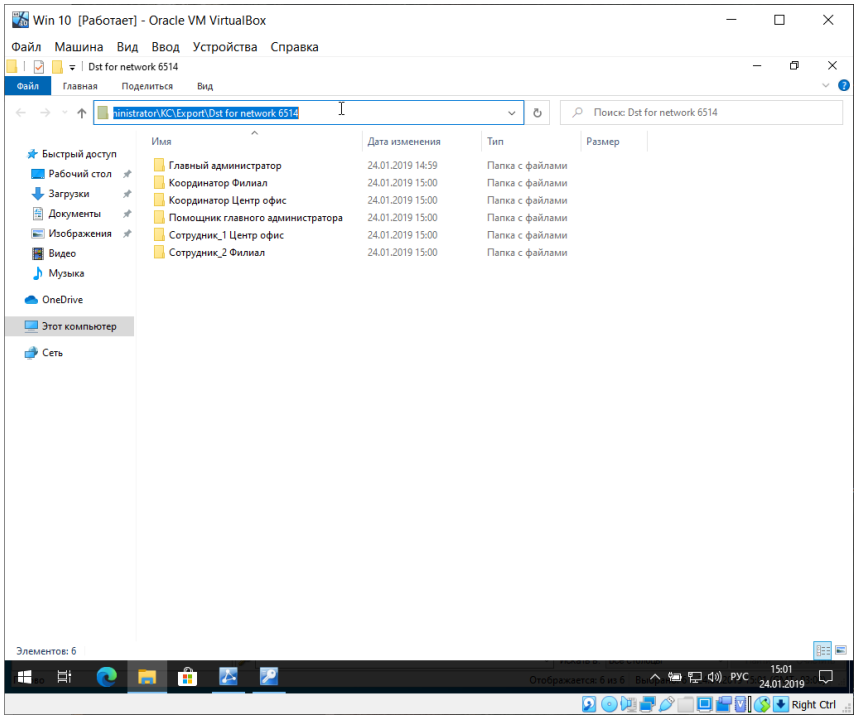
Для этого двойным щелчком откройте Свойства сетевого узла, перейдите на вкладку Пароль администратора, нажмите кнопку Создать пароль... → Тип пароля: Собственный





✓ 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.



4. Практическая работа № 10 «Настройка политик безопасности в защищённой сети VipNet Policy Manager»

Задание:

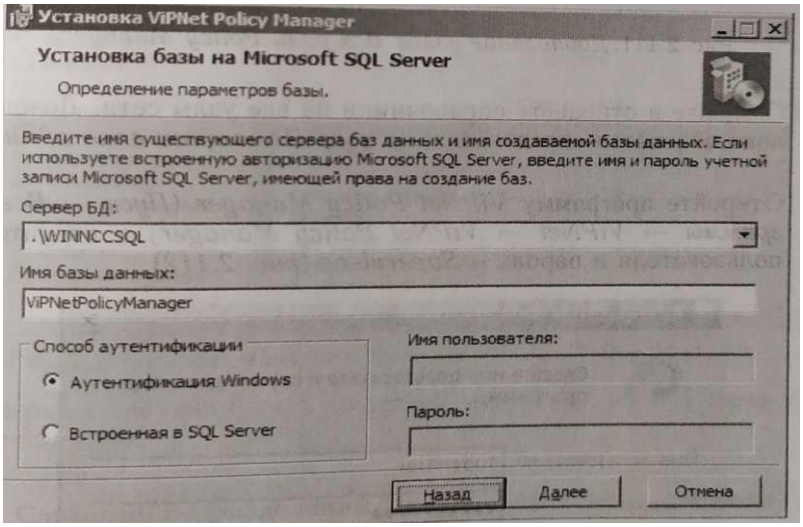
В настоящем заданий необходимо:

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 аутентифика-

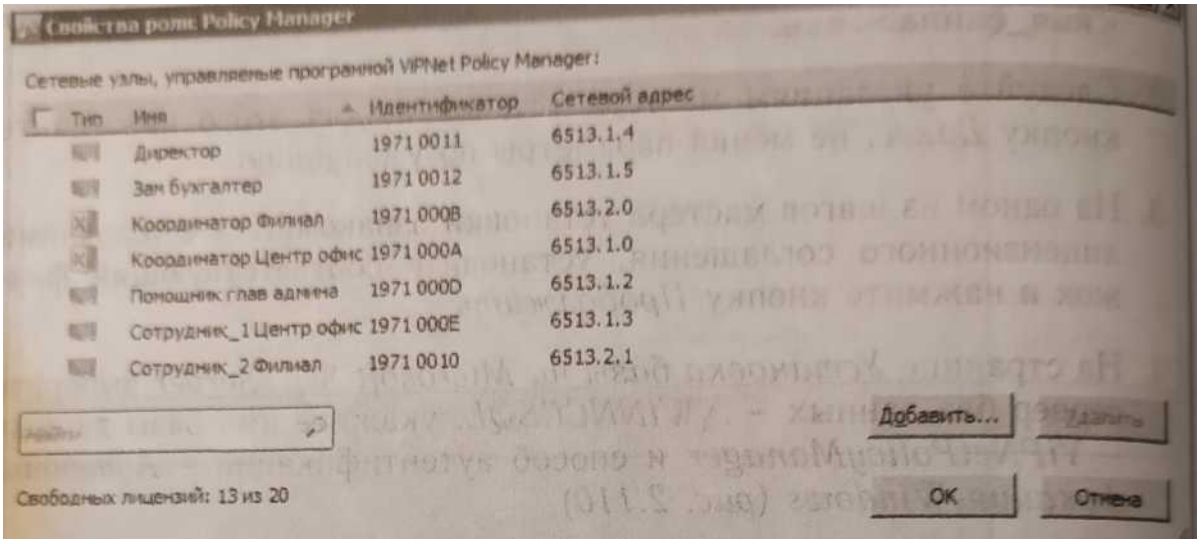


ции - Аутентификация Windows
5. В процессе установки может появиться окно со списком приложений которые требуется закрыть. Выберите Закрыть приложения и попытаться перезапустить их и нажмите ОК.

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
6. После авторизации под стандартным паролем перейдите в раздел Файл → Сменить па-



роль 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 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

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. 3 На вкладке Состав нажмите кнопку Добавить → DNS-имя... и добавьте имя vk.com.
4. 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
5. В окне программы ViPNet Policy Manager перейдите в раздел Шаблоны политики и нажмите кнопку Создать.
6. В открывшемся окне Свойства шаблона политики на вкладке Основные параметры задайте имя Запрет социальных сетей.
7. На вкладке Подразделения отметьте подразделения Центральный офис и Филиал На вкладке Локальные фильтры открытой сети нажмите кнопку Создать...
8. В открывшемся окне Свойства фильтра открытой сети на вкладке Основные параметры задайте имя фильтра Запрет социальных сетей и установите переключатель в положение Блокировать трафик
9. На вкладке Назначения нажмите кнопку Добавить... р пы IP-адресов и выберите группу Социальные сети
10. Остальные параметры окна Свойства фильтра открытой сети и Свойства шаблона политики менять не требуется.

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

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 админа зайдите в программу ViPNet Client Монитор Сетевые фильтры → Фильтры открытой сети. Убедитесь, что добавлен новый фильтр Запрет социальных сетей

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.

Эталон ответа:

Установка ViPNet Policy Manager

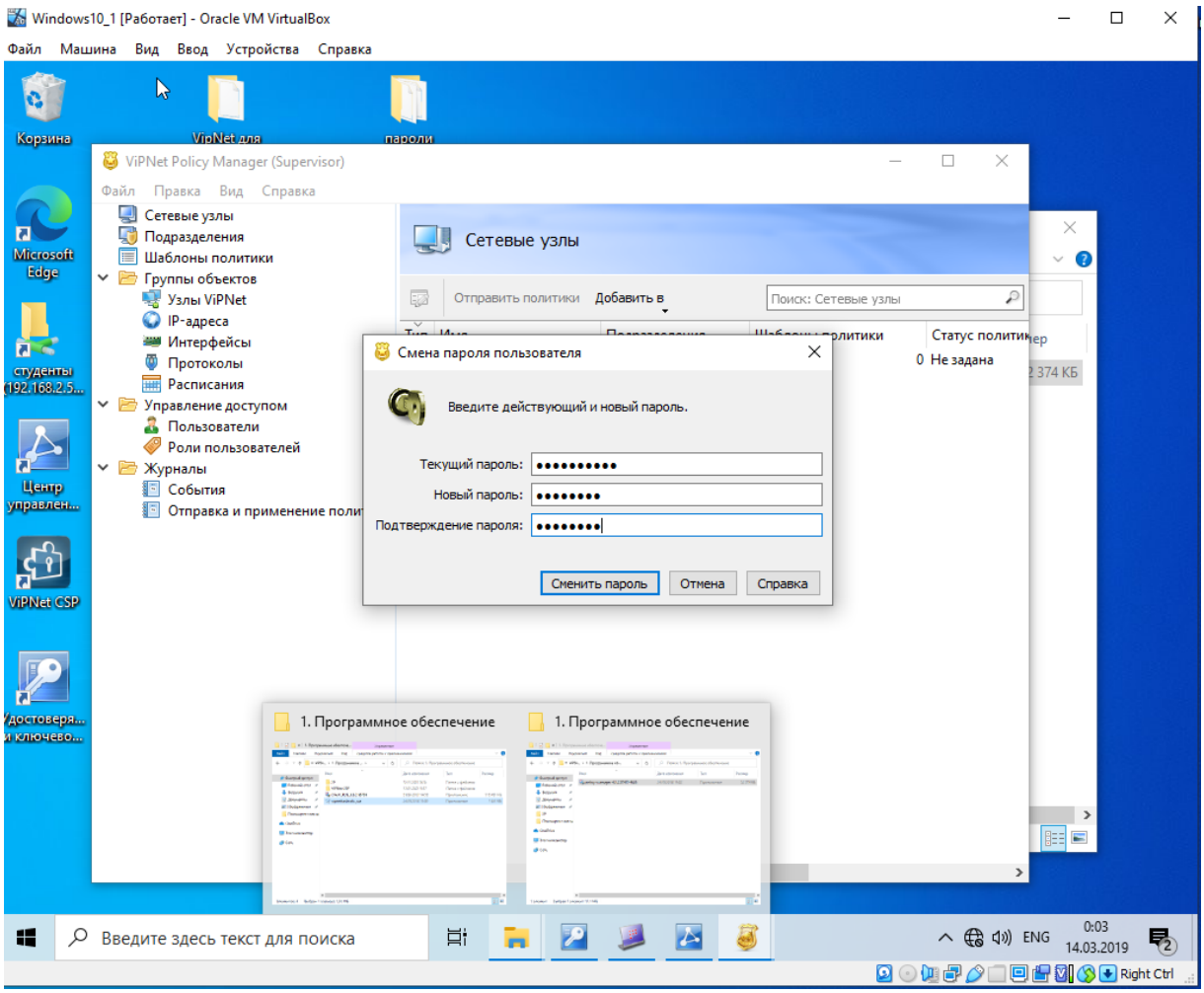
ПО ViPNet Policy Manager допускается развертывать только на клиенте с ролью Network Control Center, поэтому клиенту Главный администратор была автоматически назначена роль Policy Manager.

6. На рабочем месте Главный администратор запустите установочный файл программного обеспечения ViPNet Policy Manager <имя_файла>. exe.
7. Следуйте указаниям мастера установки, для этого нажимайте кнопку Далее, не меняя параметры по умолчанию.
8. На одном из шагов мастера установки ознакомьтесь с условиями лицензионного соглашения, установите соответствующий флажок и нажмите кнопку Продолжить.
9. На странице Установка базы на Microsoft SQL Server выберите сервер баз данных - .\WINNCCSQL, укажите имя базы данных - ViPNetPolicyManager и способ аутентификации - Аутентификация Windows
10. 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:

8. В окне VipNet Центр управления сетью перейдите в раздел Клиенты.
9. В свойствах клиента Главный администратор выберите Роли узла → Policy Manager → Свойства и добавьте в список все узлы сети
10. Создайте и отправьте справочники на все узлы сети. Дождитесь пока обновятся справочники на узле Помощник глав админа.
11. Откройте программу ViPNet Policy Manager (Пуск → Все программы → ViPNet →ViPNet Policy Manager) и введите им пользователя и пароль - Supervisor
12. На экран будет выведено предупреждение о необходимости смены пароля пользователя Supervisor
13. После авторизации под стандартным паролем перейдите в раздел Файл → Сменить пароль пользователя и задайте пароль — 11111111 (восемь единиц).
14. 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

Теперь можно приступить к управлению узлами ViPNet через ViPNet Policy Manager.



Создание подразделений Центральный офис, Филиал

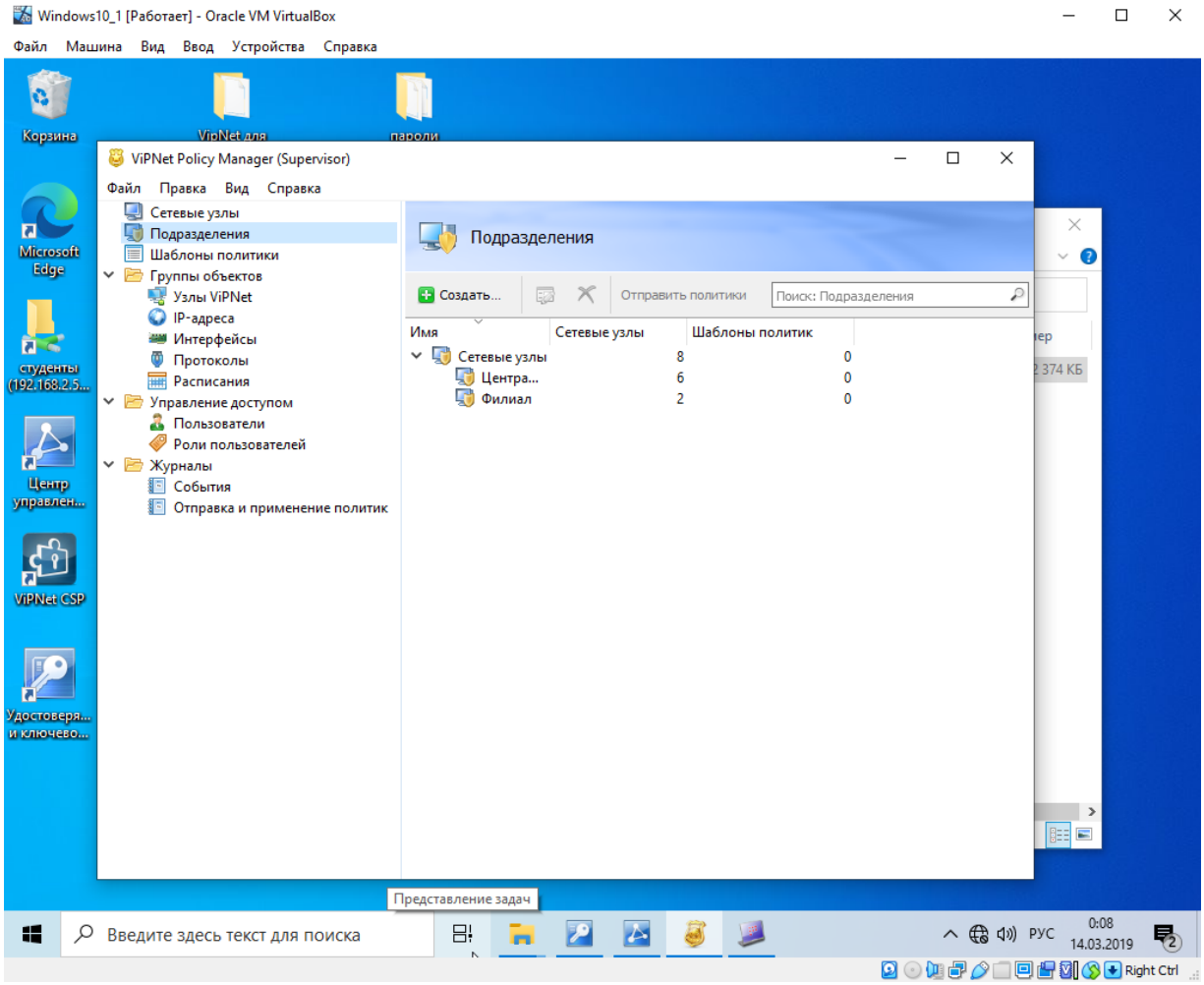
Для создания подразделений Центральный офис, Филиал выполните следующие действия:

4. В окне программы VipNet Policy Manager перейдите в раздел Подразделения и нажмите кнопку Создать.
5. В открывшемся окне Свойства подразделения на вкладке Основные параметры задайте имя Центральный офис.
6. На вкладке Сетевые узлы добавьте клиентов Центрального офиса: Координатор Центр офис, Главный администратор, Помощник глав администратора, 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



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:

14. В окне программы ViPNet Policy Manager перейдите в раздел Группы объектов —* IP-адреса и нажмите кнопку Создать.
15. В открывшемся окне Свойства группы IP-адресов на вкладке Основные параметры затаите имя Социальные сети.
16. 3 На вкладке Состав нажмите кнопку Добавить → DNS-имя... и добавьте имя vk.com.
17. 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
18. В окне программы ViPNet Policy Manager перейдите в раздел Шаблоны политики и нажмите кнопку Создать.
19. В открывшемся окне Свойства шаблона политики на вкладке Основные параметры задайте имя Запрет социальных сетей.
20. На вкладке Подразделения отметьте подразделения Центральный офис и Филиал
21. На вкладке Локальные фильтры открытой сети нажмите кнопку Создать...
22. В открывшемся окне Свойства фильтра открытой сети на вкладке Основные параметры задайте имя фильтра Запрет социальных сетей и установите переключатель в положение Блокировать трафик

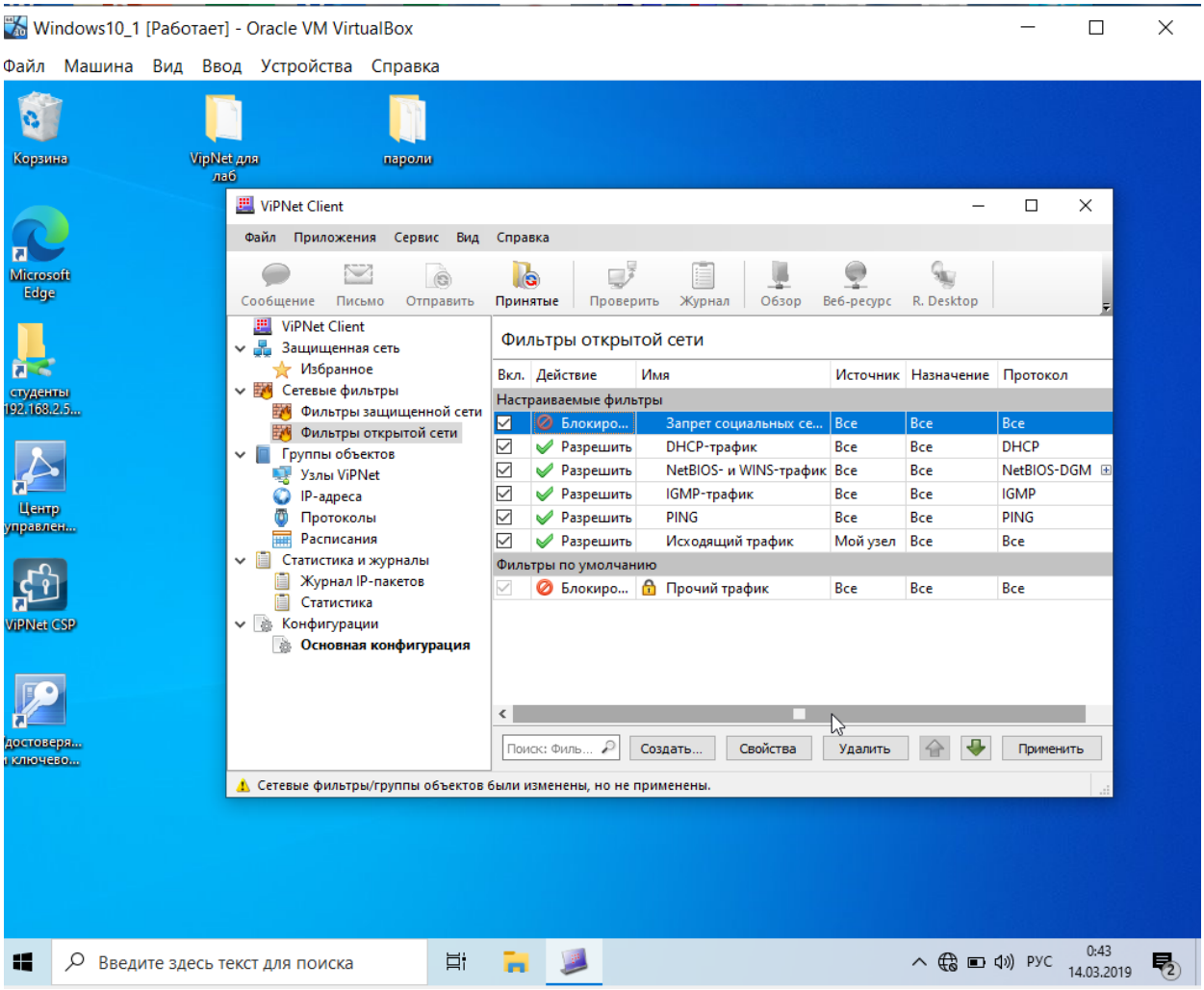
23. На вкладке Назначения нажмите кнопку Добавить... р пы IP-адресов и выберите группу Социальные сети
24. Остальные параметры окна Свойства фильтра открытой сети и Свойства шаблона политики менять не требуется.

После создания политики Запрет социальных сетей раздел Шаблоны политики примет следующий вид

25. Отправьте политики на узлы. Для этого в окне программы ViPNet Policy Manager перейдите в раздел Подразделения.
26. Выделите подразделения Центральный офис и Филиал, нажмите кнопку Отправить политики
27. На экран будет выведено окно Отправка политики. Не меняя параметров, нажмите кнопку ОК

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 админа зайдите в программу ViPNet Client Монитор Сетевые фильтры → Фильтры открытой сети. Убедитесь, что добавлен новый фильтр Запрет социальных сетей



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:

7. В окне программы ViPNet Policy Manager перейдите в раздел Шаблоны политики и нажмите кнопку Создать.
8. В открывшемся окне Свойства шаблона политики на вкладке Основные параметры задайте имя Блокировка открытого трафика.
9. На вкладке Сетевые узлы добавьте Сотрудник_1 Центр офис.
10. На вкладке Локальные фильтры открытой сети нажмите кнопку Создать…
11. 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
12. 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.

5. Практическая работа № 11 «Межсетевое взаимодействие»

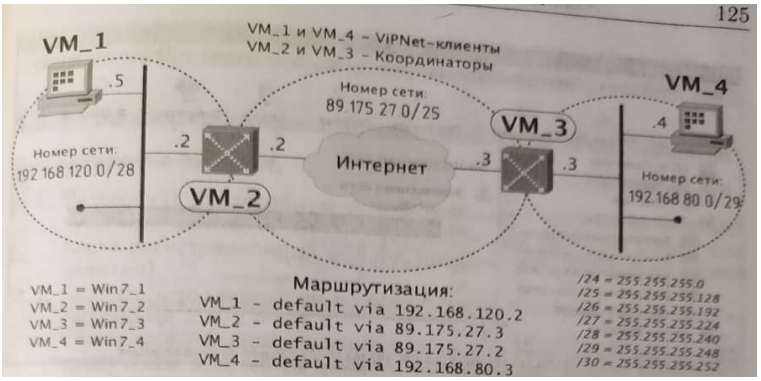
Задание:

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.



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.

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

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

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.

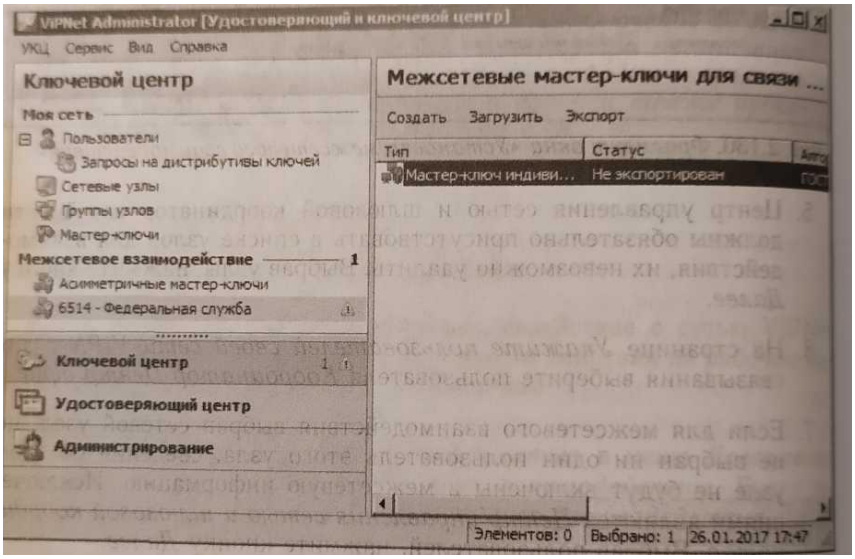
Для каждой доверенной сети в Удостоверяющем и ключевом центре создается межсетевой мастер-ключ, на основе которого формируются ключи для защищенного обмена информацией с данной доверенной сетью.

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.

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.

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.

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

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
7. В появившемся окне нажмите кнопку Создать.

8. 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.
9. 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.
10. Передайте администратору сети Компании созданный файл межсетевой информации *****-****.lzh

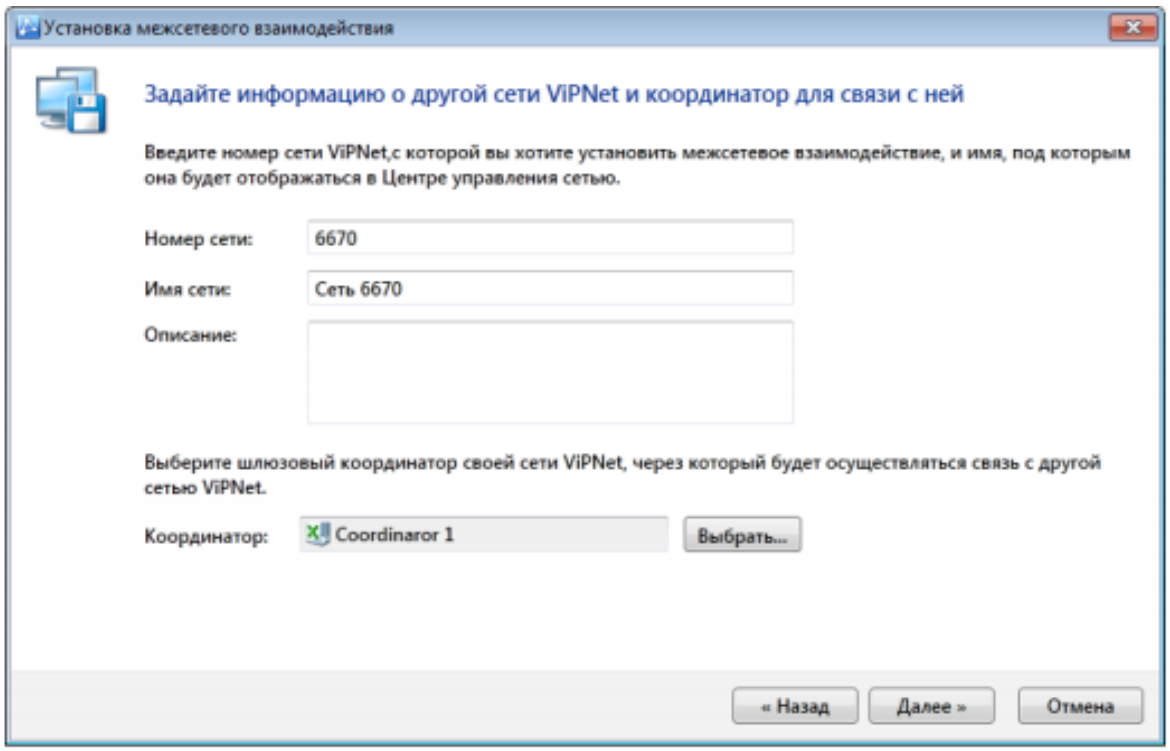
Завершение организации межсетевого взаимодействия

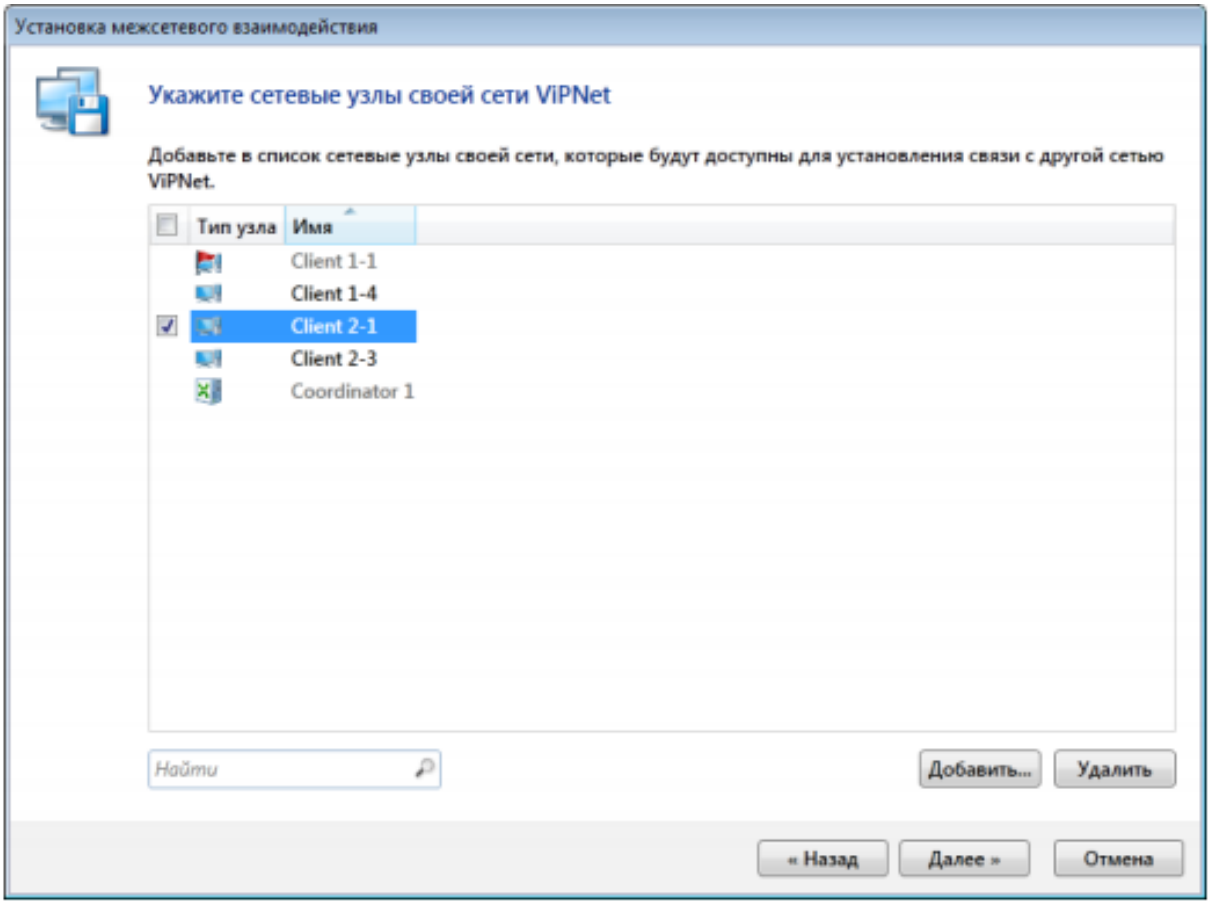
Чтобы принять ответную межсетевую информацию и завершить организацию взаимодействия, выполните следующие действия на рабочем месте Главный администратор (сеть Компании):

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.

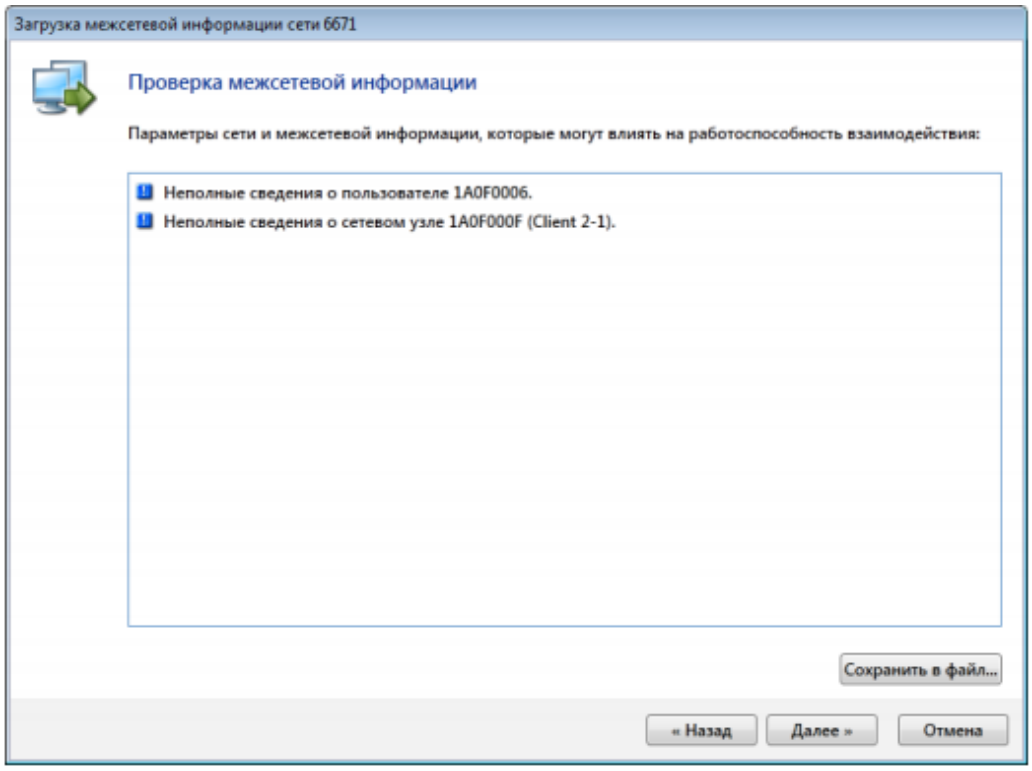
Эталон ответа:





11. Центр управления сетью и шлюзовой координатор своей сети должны обязательно присутствовать в списке узлов для взаимодействия, их невозможно удалить. Выбрав узлы, нажмите кнопку Далее.
12. На странице Укажите пользователей своей сети ViPNet для связывания выберите пользователя Координатор Центр офис.

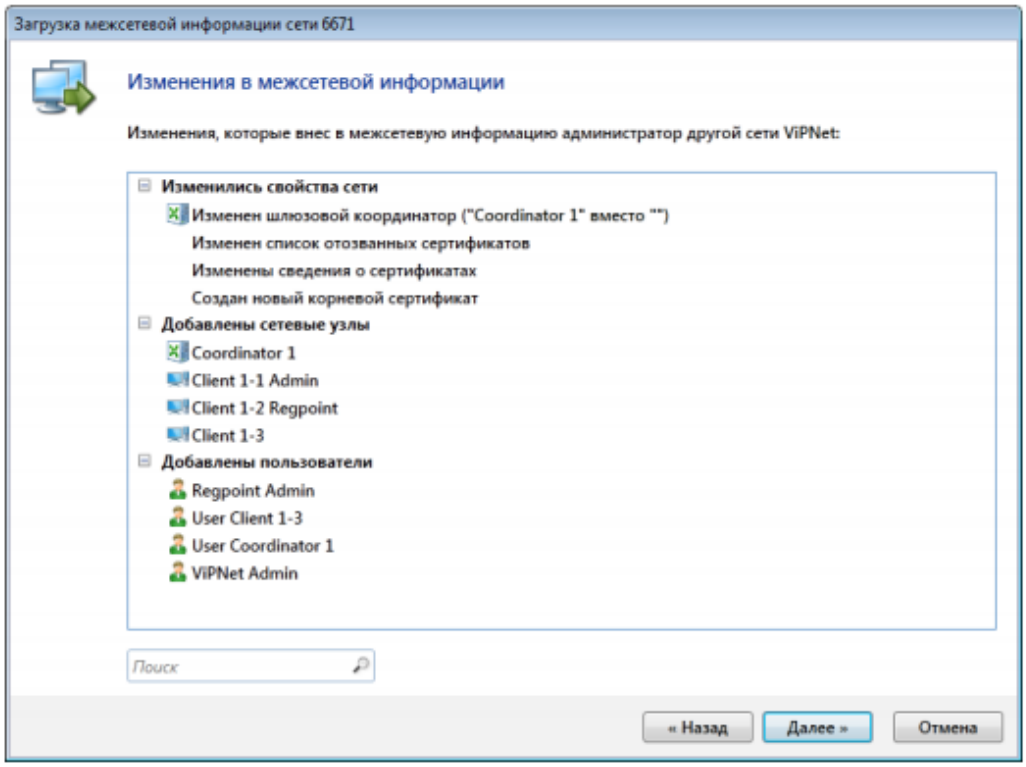
13. Если для межсетевого взаимодействия выбран сетевой узел, но не выбран ни один пользователь этого узла, сведения об этом узле не будут включены в межсетевую информацию. Исключениями являются Центр управления сетью и шлюзовой координатор. Выбрав пользователей, нажмите кнопку Далее.
14. На открывшейся странице Подготовка к сохранению межсетевой информации завершена при необходимости укажите комментарий для администратора сети Федеральной службы и нажмите кнопку Далее.
15. 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.



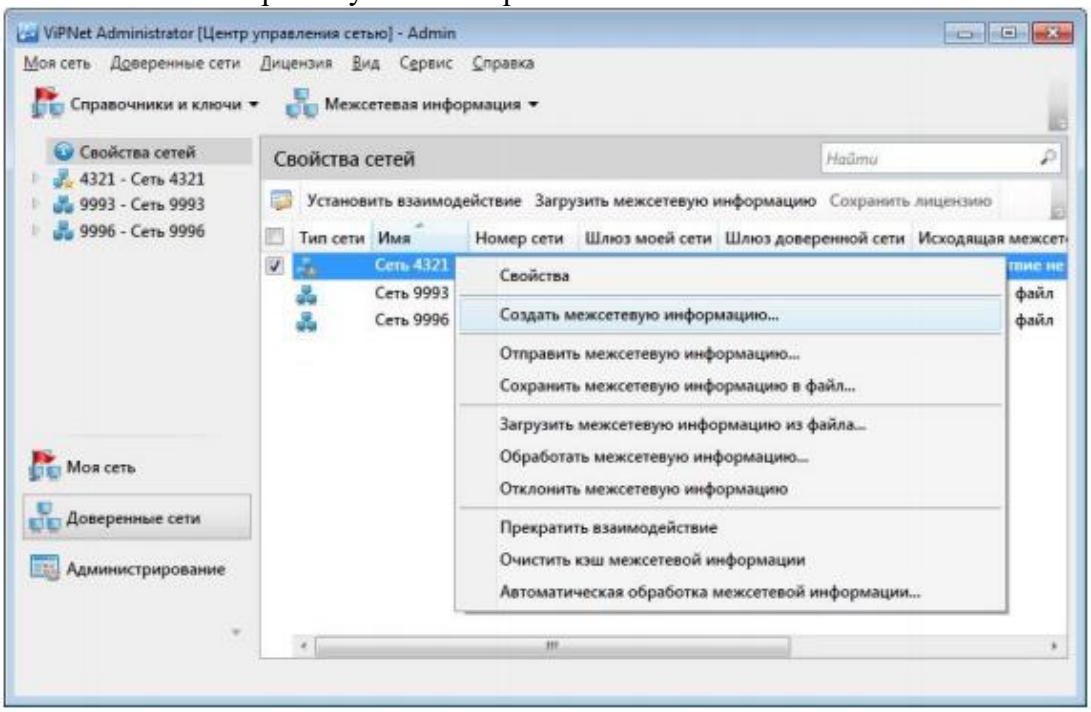
16. На странице Сохранение межсетевой информации после завершения записи файла нажмите кнопку Далее, на следующей странице нажмите кнопку Готово.

Чтобы создать индивидуальный симметричный межсетевой мастер ключ, выполните следующие действия:

8. В окне программы ViPNet Удостоверяющий и ключевой центр на панели навигации выберите представление Ключевой центр
9. Перейдите в раздел с номером доверенной сети, для связи с которой будет использоваться межсетевой мастер-ключ, и на панели инструментов нажмите кнопку Создать.
10. 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



Щелкните по созданному межсетевой мастер-ключу правой кноп кой мыши и в контекстном меню выберите пункт Экспорт.

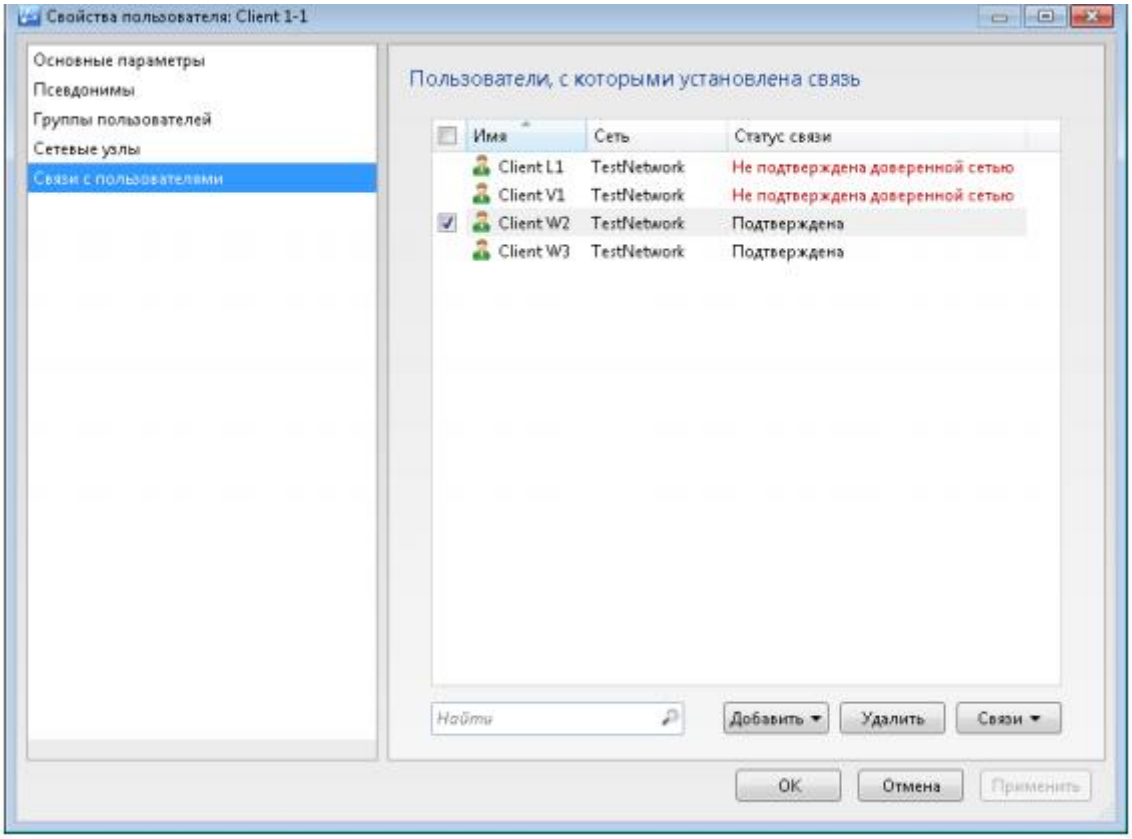


11. Появится окно ввода пароля. Укажите в нем пароль - 11111111 и нажмите кнопку ОК. На указанном пароле будет зашифрован экспортируемый ключ.
12. В появившемся окне укажите каталог, в который будет сохранен межсетевой мастер-ключ - Рабочий стал, затем нажмите кнопку ОК.
13. Передайте доверенным способом файл межсетевой информации с расширением*. lzh, межсетевой мастер-ключ «net ****.key» и пароль, на котором зашифрован межсетевой мастер-ключ - 11111111, администратору сети Федеральной службы.

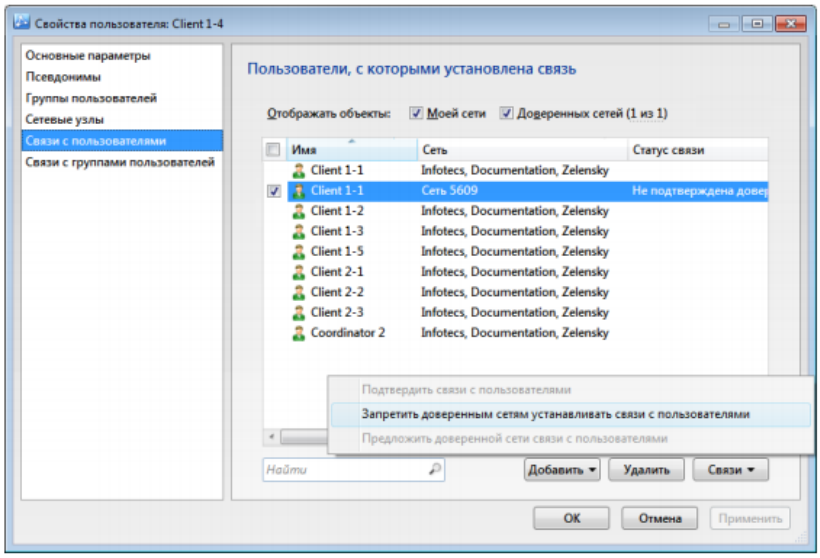
Завершение организации межсетевого взаимодействия

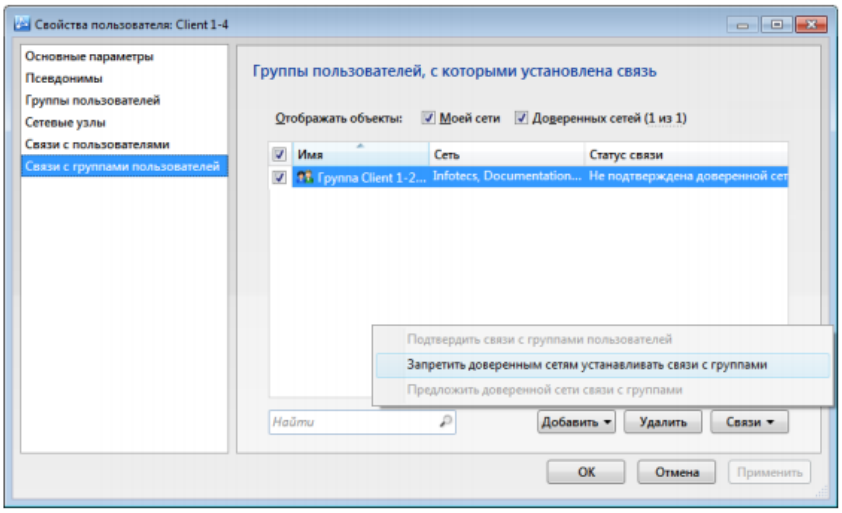
Чтобы принять ответную межсетевую информацию и завершить организацию взаимодействия, выполните следующие действия на рабочем месте Главный администратор (сеть Компании):

14. Получите у администратора доверенной сети ViPNet Федеральной службы файл, содержащий ответную межсетевую информацию ****-****.lzh.
15. В окне программы ViPNet Центр управления сётью в меню Доверенные сети выберите пункт Загрузить межсетевую информацию из файла.
16. 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.
17. Примите ответную межсетевую информацию с помощью мастера Обработка межсетевой информации
18. 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.



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





6. Практическая работа № 14 «Установка и настройка Traffic monitor»

Задание 1:

1. Установить InfoWatch Traffic Monitor Enterprise:

Тип установки: Все-в-одном Enterprise – все компоненты Системы (с СУБД Oracle Enterprise или PostgreSQL) устанавливаются на один сервер. Такая установка используется, если с учетом предполагаемой нагрузки на сервере будет обеспечен ресурс как для СУБД, так и для сервисов Traffic Monitor.

2. Установка системы Red Hat Enterprise Linux (IW TM 6 Enterprice в режиме «все в одном»):

✓ Выбор базы данных;
✓ выбор режима установки;
✓ выбор часового пояса;
✓ установка пароля суперпользователя Системы;
✓ выбор способа разбиения дискового пространства;

- ✓ настройка сети;
- ✓ настройка синхронизации времени (NTP-server);
- ✓ настройка локализации;
- ✓ настройка автоматического удаления событий из БД;
- ✓ завершение установки.

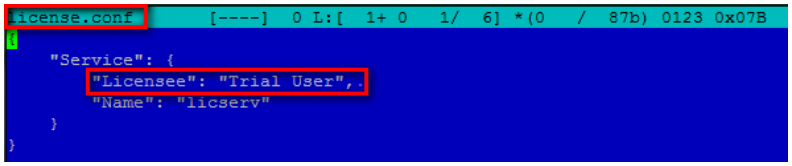
Задание 2 Настройка InfoWatch Traffic Monitor:

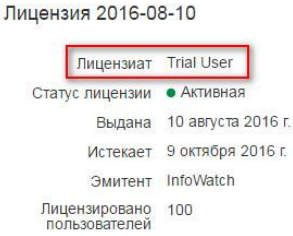
- ✓ Откройте интернет-браузер (рекомендуется использовать браузер Google Chrome.
- ✓ В адресной строке введите адрес сервера InfoWatch Traffic Monitor.
- ✓ В поле Логин укажите имя пользователя.
- ✓ В поле Пароль укажите пароль.
- ✓ Нажмите Войти.

Загрузите файл лицензии через консоль управления Traffic Monitor, раздел Управление→Лицензии.

Войдите в интерпретатор командной строки сервера Traffic Monitor.

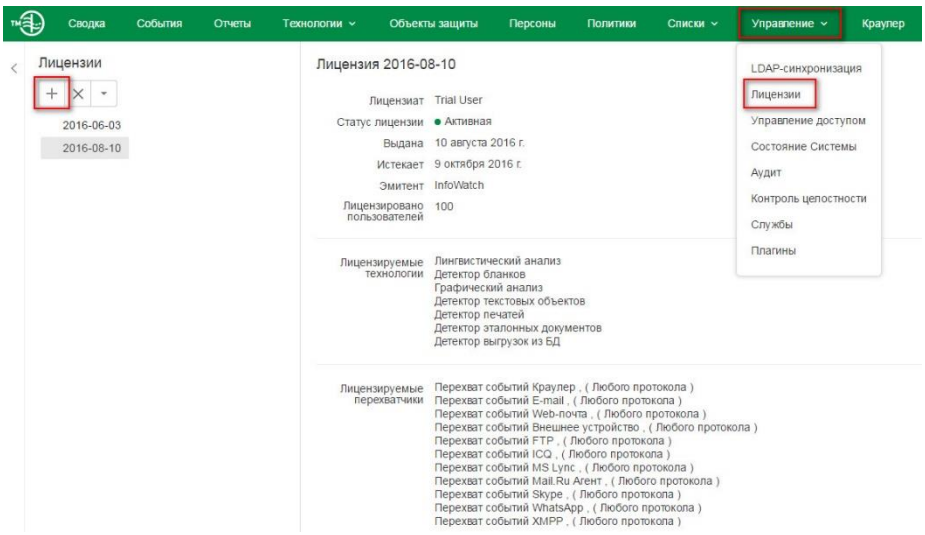
убедитесь, что параметр лицензиат, отображаемый в консоли, соответствует параметру Licensee в файле /opt/iw/tm5/etc/license.conf





перезапустите сервер Traffic Monitor следующей командой:

service iwtm restart



Задание 3:

С помощью базы знаний https://kb.infowatch.com/pages/viewpage.action?pageId=125533217 ответить на следующие вопросы:

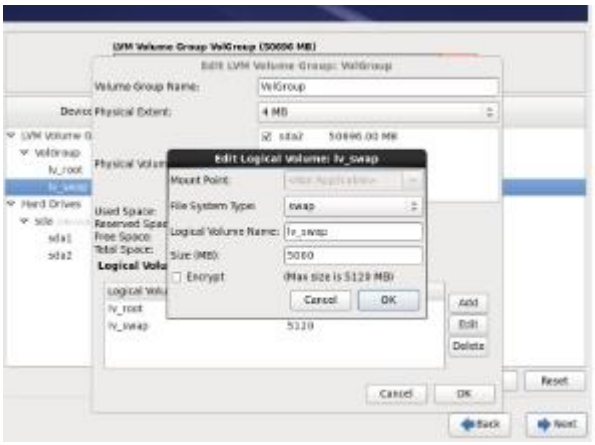
Перечислите отличия IW TM 6 Enterprice от IW TM 6 Standart.

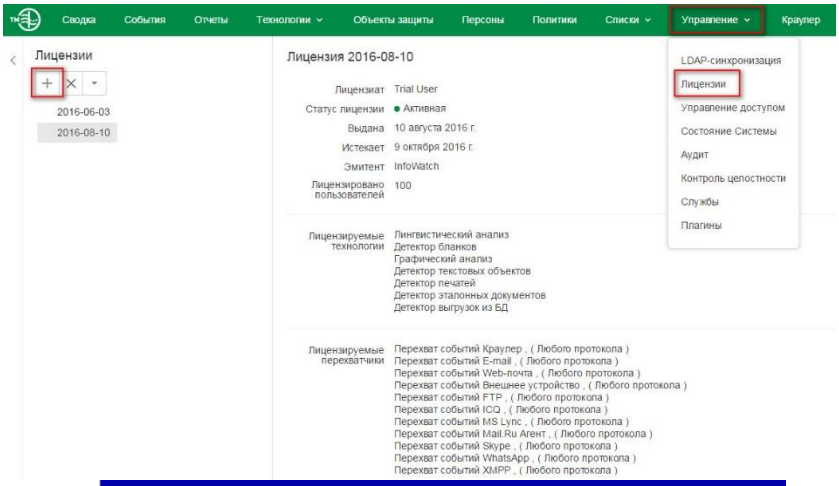
- ✓ В каких случаях рекомендуется отдельная установка сервера ТМ и сервера базы данных?
- ✓ К какому внутреннему формату приводятся объекты в системе IW TM 6?
- ✓ Какие СУБД поддерживаются системой IW TM 6?
- ✓ За прием каких данных отвечают компоненты sniffer и proxy?
- ✓ Какая компонента системы IW 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?

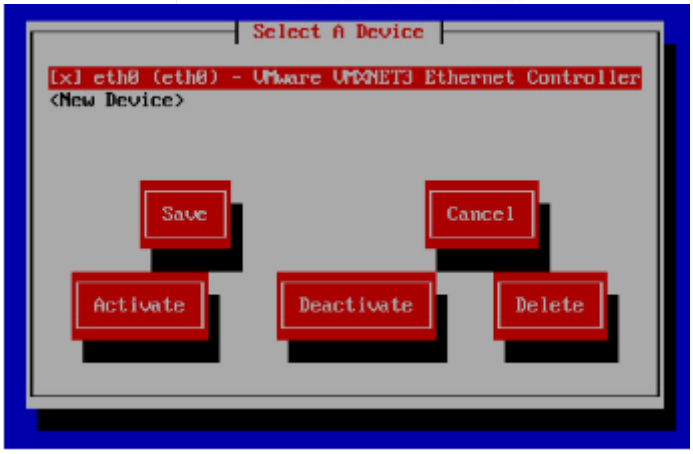
Эталон ответа:

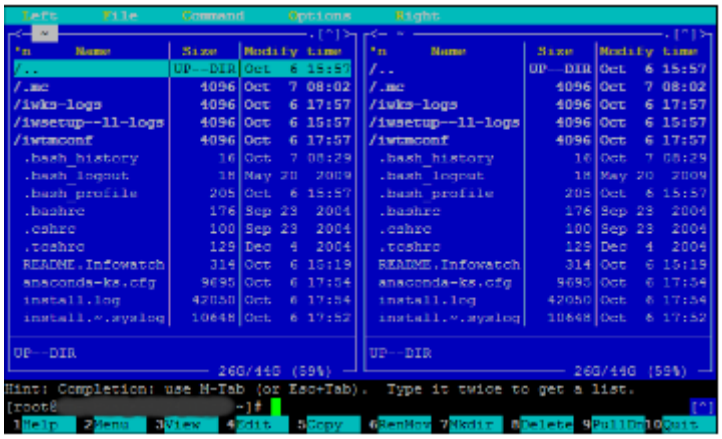
Задание 1:

1. Установить InfoWatch Traffic Monitor Enterprise:









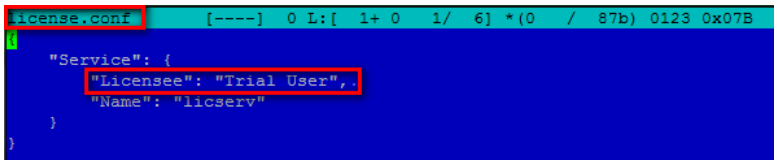
Задание 2 Настройка InfoWatch Traffic Monitor:

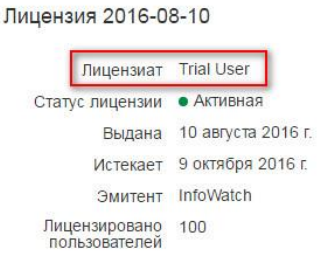
- ✓ Откройте интернет-браузер (рекомендуется использовать браузер Google Chrome.
- ✓ В адресной строке введите адрес сервера InfoWatch Traffic Monitor.
- ✓ В поле Логин укажите имя пользователя.
- ✓ В поле Пароль укажите пароль.
- ✓ Нажмите Войти.

Загрузите файл лицензии через консоль управления Traffic Monitor, раздел Управление→Лицензии.

Войдите в интерпретатор командной строки сервера Traffic Monitor.

убедитесь, что параметр лицензиат, отображаемый в консоли, соответствует параметру Licensee в файле /opt/iw/tm5/etc/license.conf



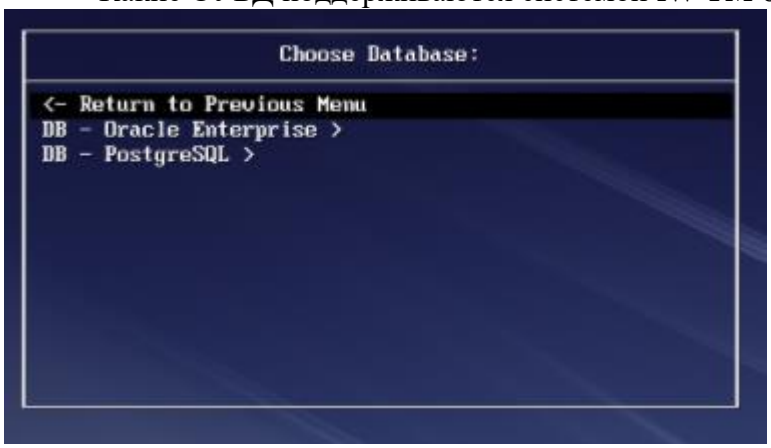


Задание 3:

С помощью базы знаний https://kb.infowatch.com/pages/viewpage.action?pageId=125533217 ответить на следующие вопросы:

- ✓ Перечислите отличия IW TM 6 Enterprice от IW TM 6 Standart.
  При установке редакции TM Standard, в качестве базы данных доступна только PostgreSQL.
- ✓ В каких случаях рекомендуется отдельная установка сервера TM и сервера базы данных?
  Такая установка используется, если с учетом предполагаемой нагрузки сервисы Traffic Monitor и СУБД не смогут производительно работать на одном компьютере.
- ✓ 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?

Сохраняют перехваченные пакеты, распределенные по сессиям.

- ✓ Какая компонента системы IW TM 6 извлекает текст из полученного объекта?

Подсистема анализа

- ✓ Какая компонента системы IW TM 6 отвечает за запуск технологий анализа?

Подсистема применения политик

- ✓ Для чего используется связка компонент системы SMTPD и Deliverd?

Процесс iw_deliverd, выполняющий доставку SMTP-писем адресатам при интеграции с почтовым relay-сервером

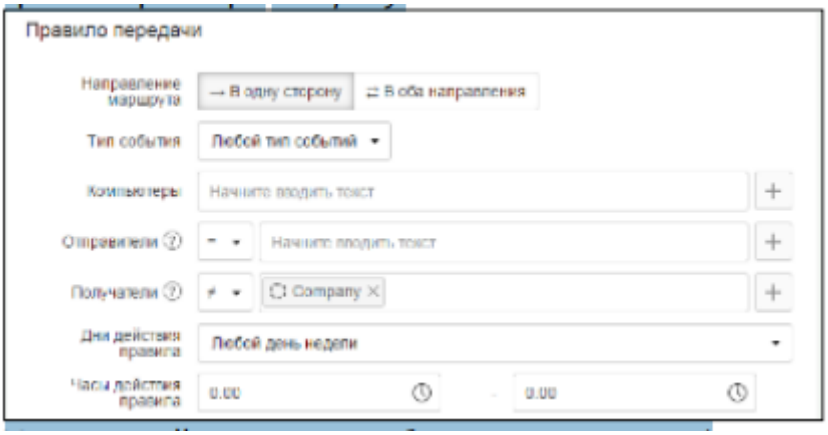
7. Практическая работа № 25«Добавление политик безопасности в Traffic monitor»

Задание:

1. Настройте перехват по всем перечисленным каналам:

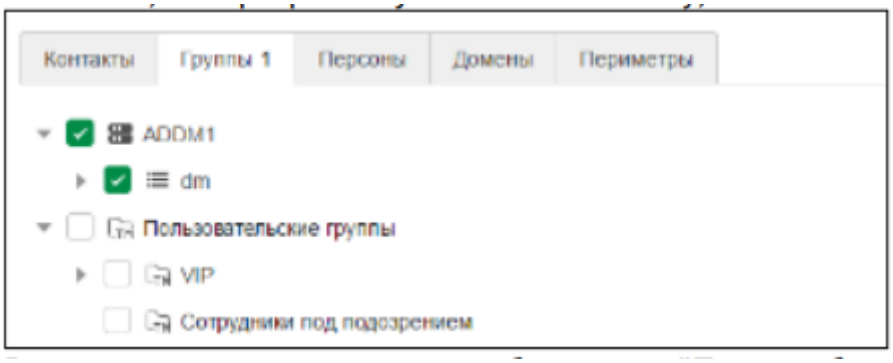
   - ✓ Сохраните скриншот демонстрирующий перехват по протоколу SMTP
   - ✓ Сохраните скриншот демонстрирующий перехват web-почты.
   - ✓ Сохраните скриншот, демонстрирующий результат работы OCR.
   - ✓ Сохраните скриншот демонстрирующий перехват по протоколу XMPP (Jabber)
   - ✓ Сохраните скриншот, демонстрирующий перехват событий печати.
   - ✓ Сохраните изображения, демонстрирующие перехват данных из буфера обмена.
   - ✓ Сохраните скриншот демонстрирующий перехват данных, копируемых на внешнее устройство хранения.
2. 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).

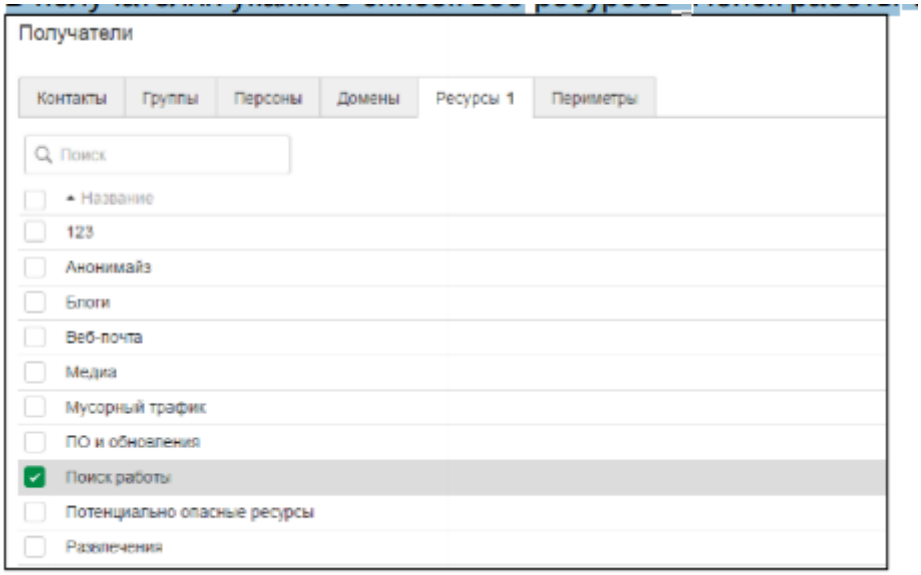


3. Требуется выявить сотрудников, посещающих сайты по поиску работы. Для этого:

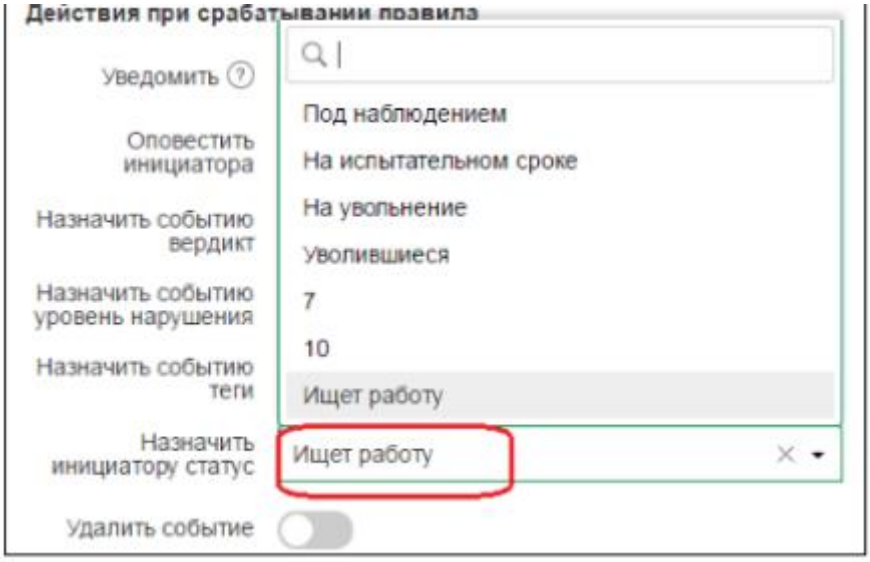
   - ✓ Создайте политику защиты данных "Выявление нелояльных сотрудников"
   - ✓ Добавьте правило передачи и укажите в качестве отправителей группу сотрудников компании, импортированную из Active Directory.



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



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

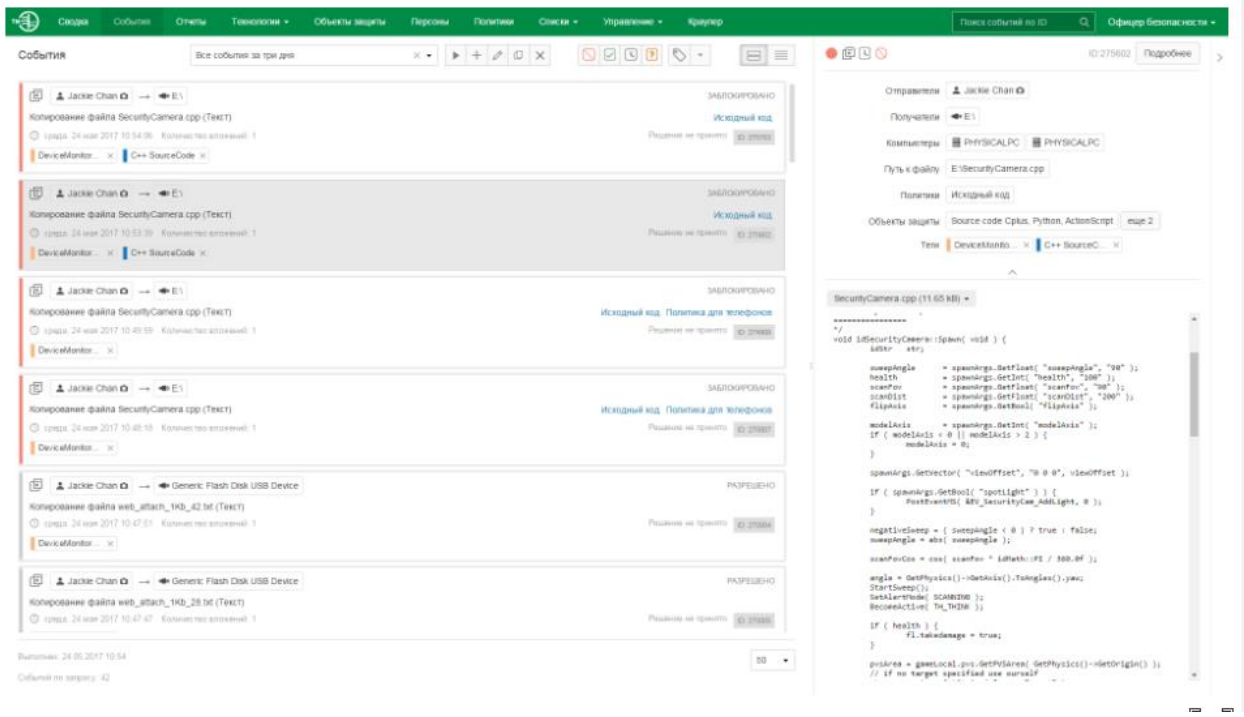


Сохраните правило и примените изменения конфигурации.

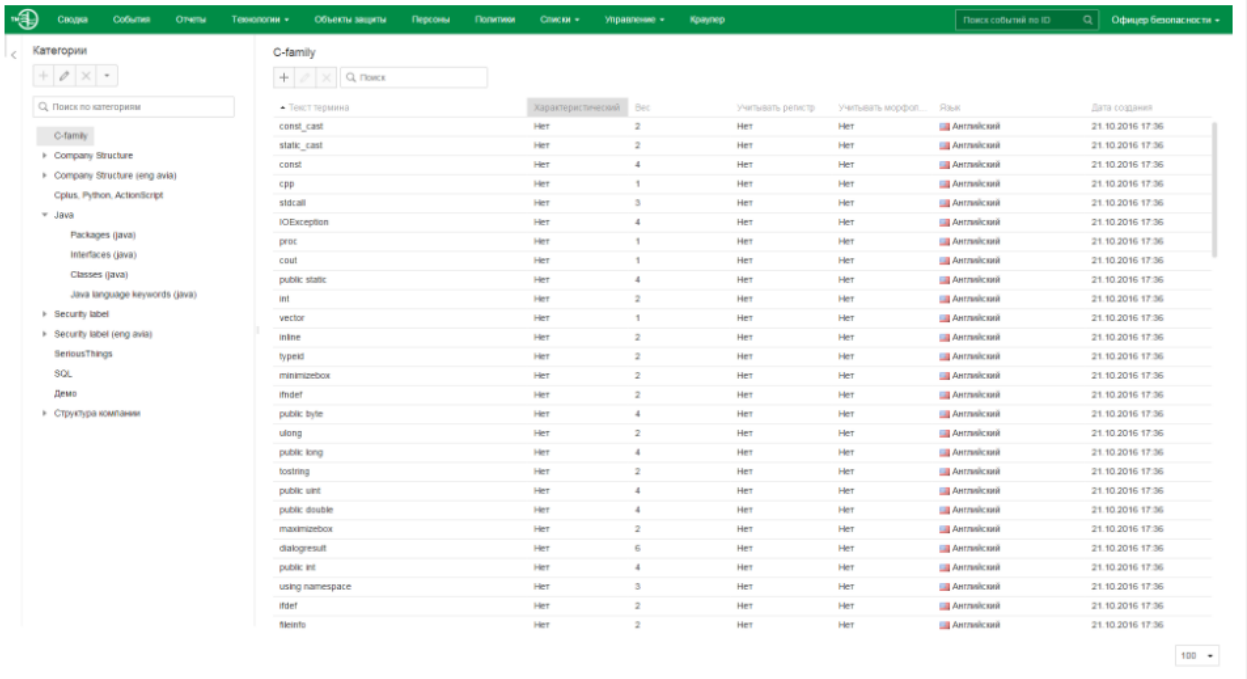
Эталон ответа:

Задание:

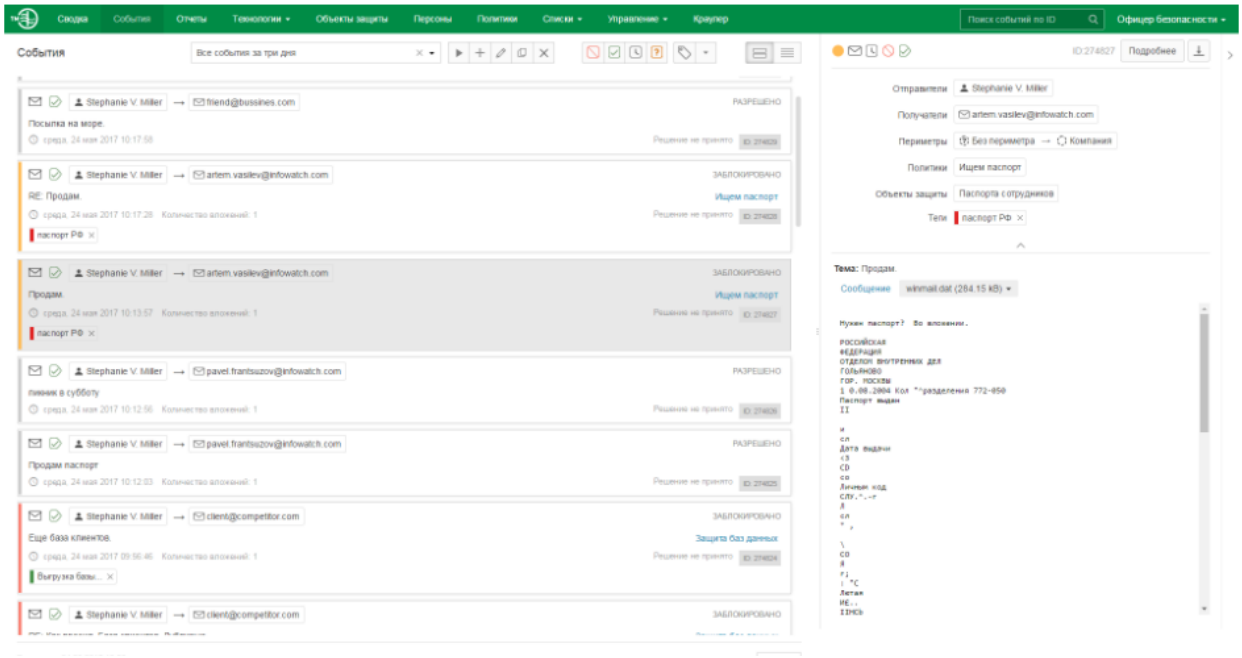
1. Настройте перехват по всем перечисленным каналам:
   - ✓ Сохраните скриншот демонстрирующий перехват по протоколу SMTP



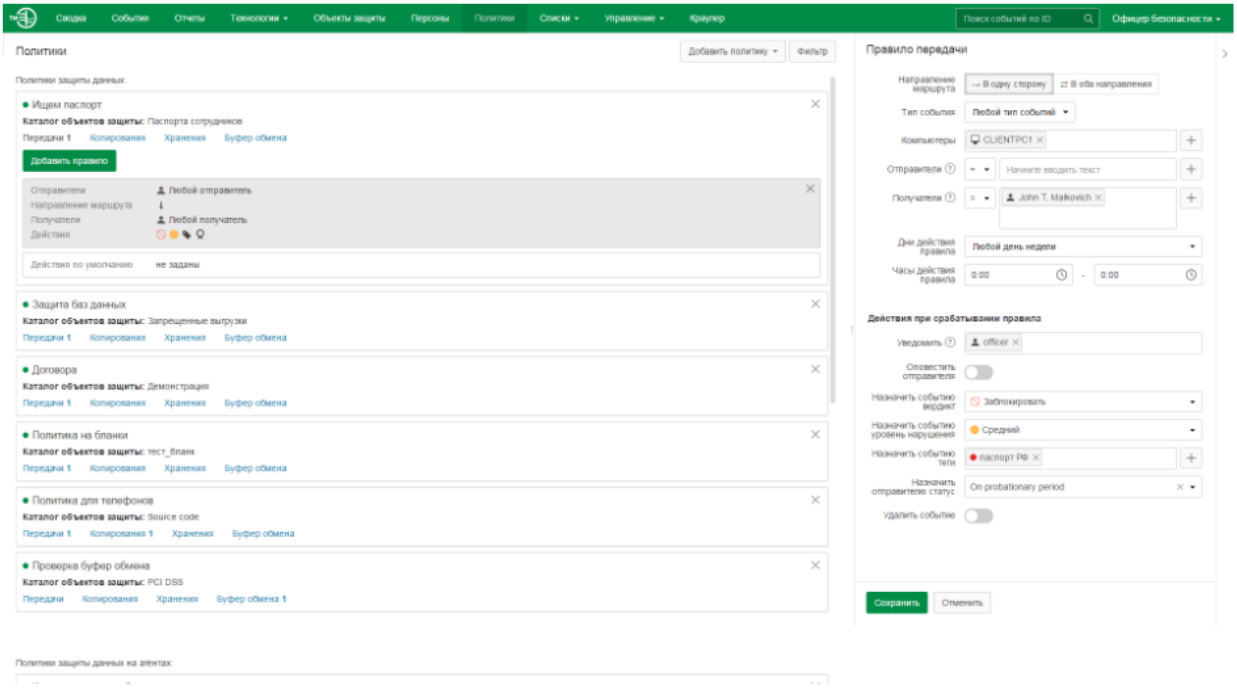
   - ✓ Сохраните скриншот демонстрирующий перехват web-почты.



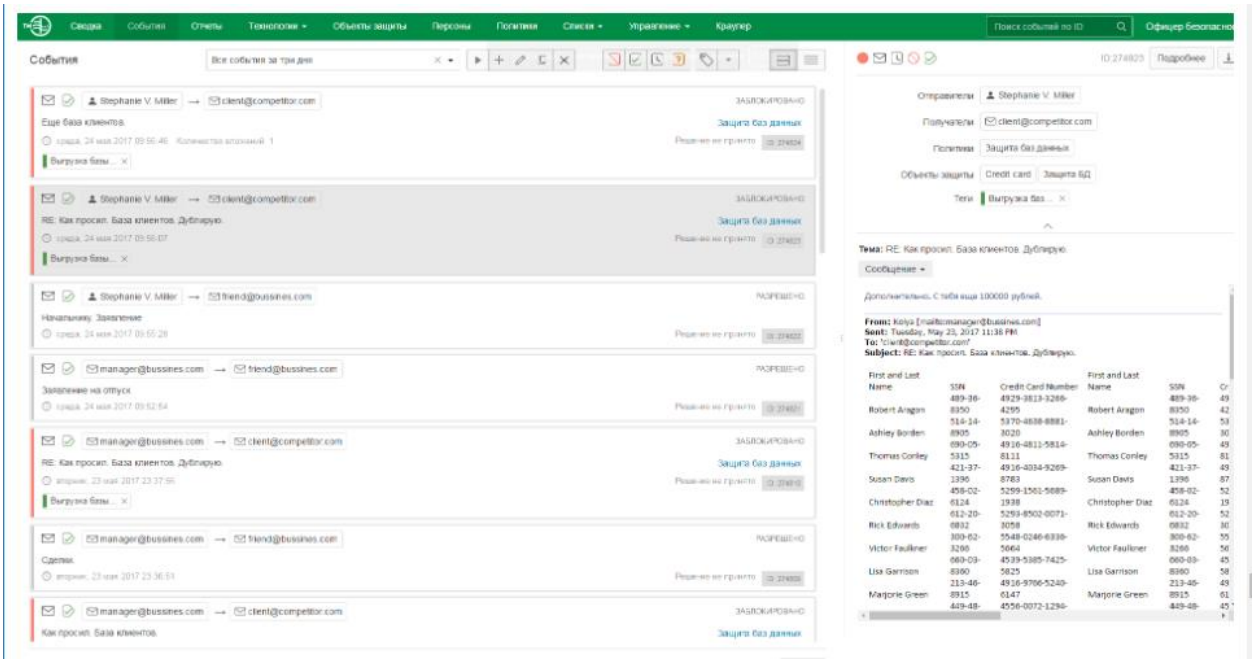
   - ✓ Сохраните скриншот, демонстрирующий результат работы OCR.



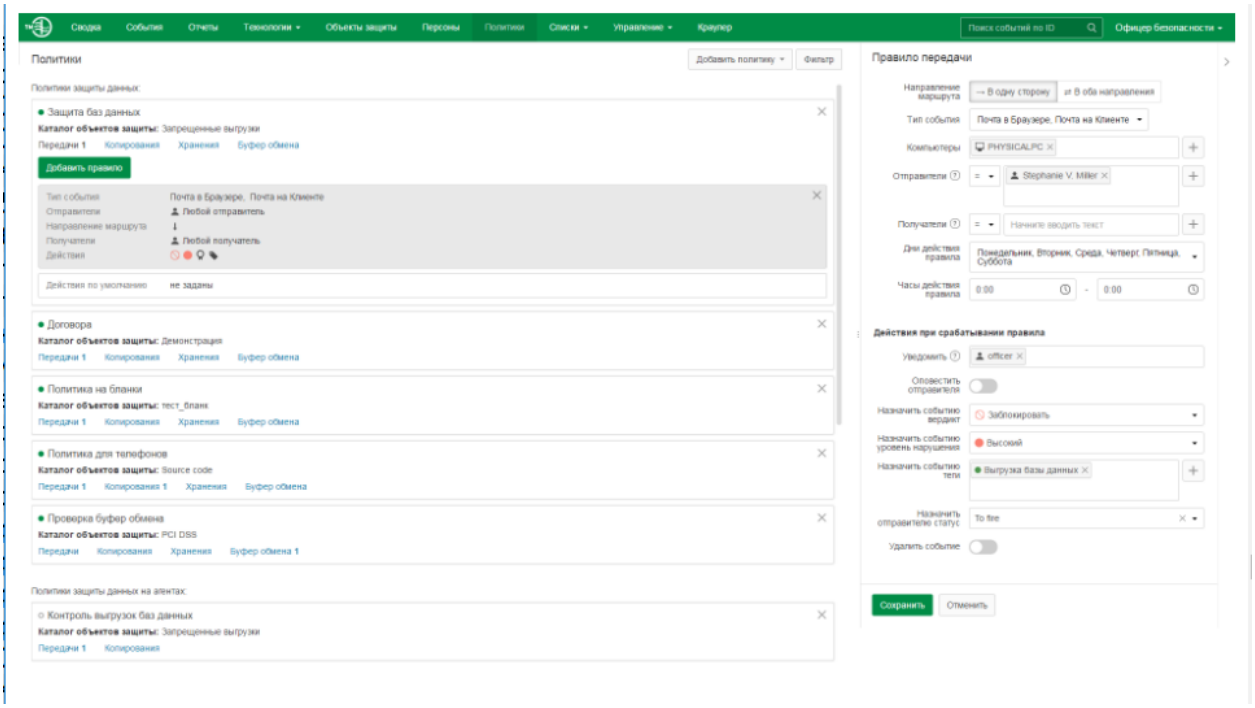
✓ Сохраните скриншот демонстрирующий перехват по протоколу XMPP (Jabber)



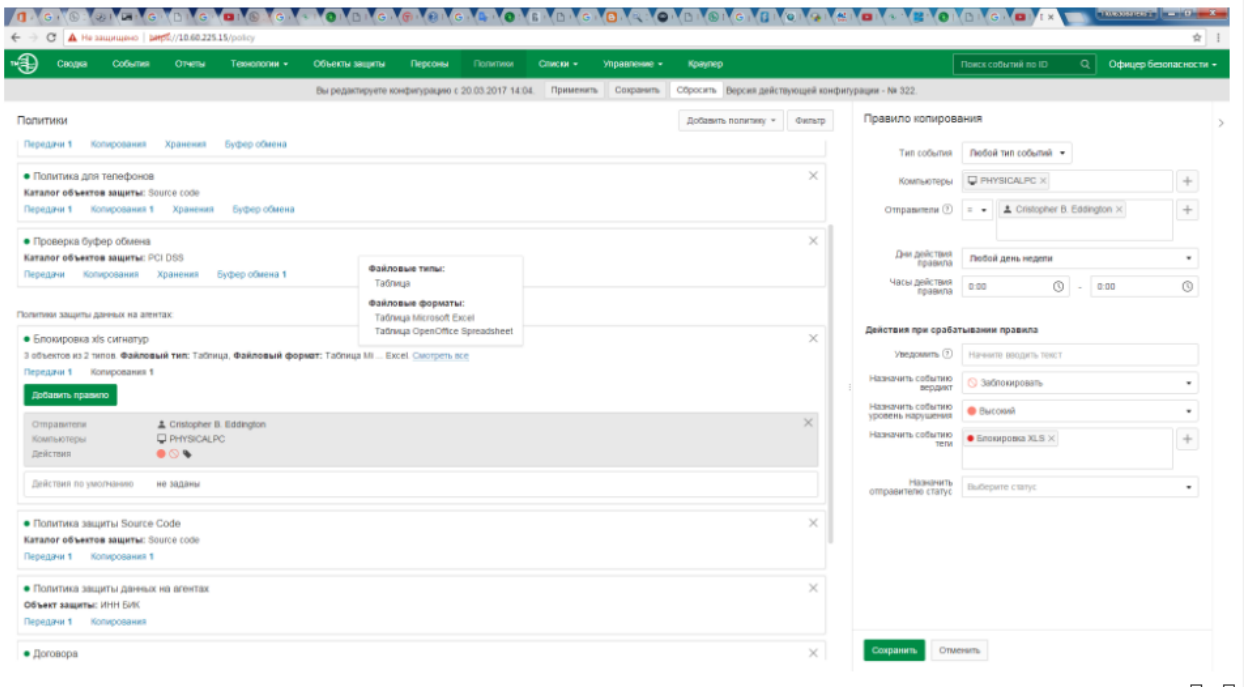
✓ Сохраните скриншот, демонстрирующий перехват событий печати.



✓ Сохраните изображения, демонстрирующие перехват данных из буфера обмена.

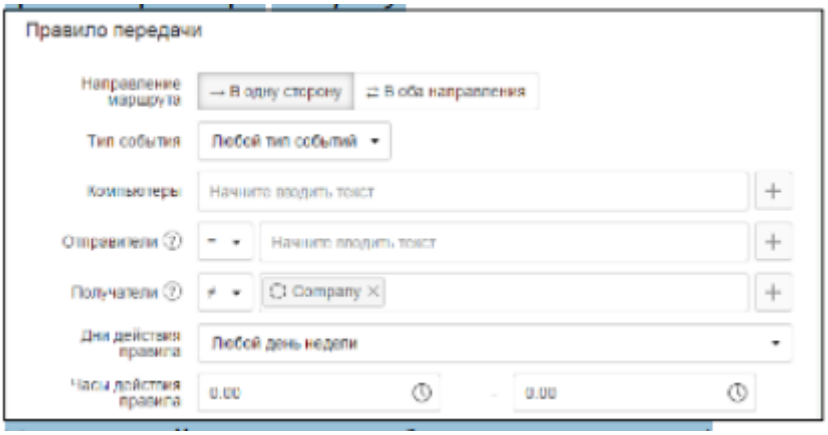


✓ Сохраните скриншот демонстрирующий перехват данных, копируемых на внешнее устройство хранения.



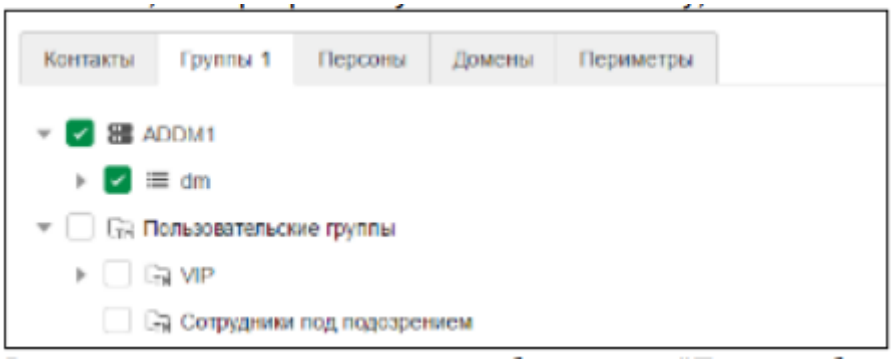
4. Требуется контролировать передачу устава компании за пределы компании, в том числе отправку документа по электронной почте и копирование на съемные носители. Для этого:

   - ✓ 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).

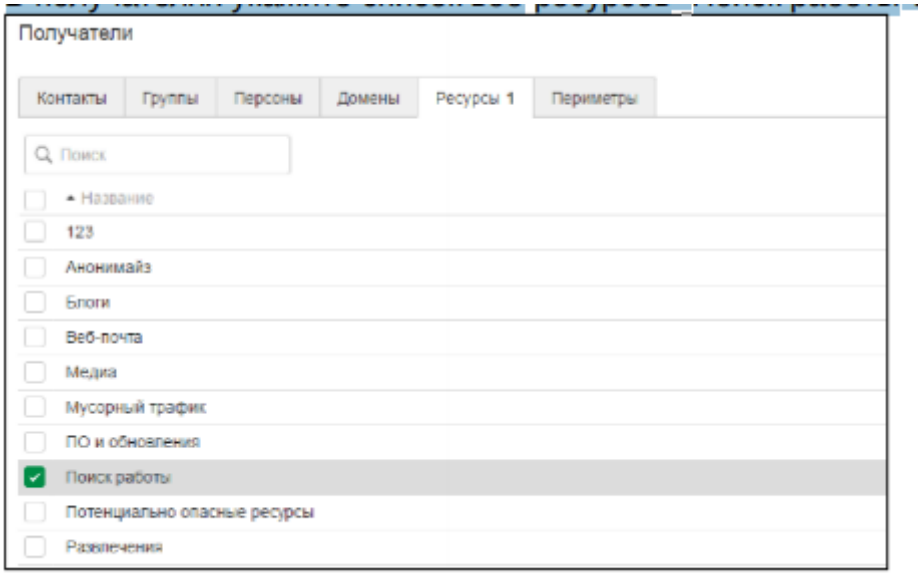


5. Требуется выявить сотрудников, посещающих сайты по поиску работы. Для этого:

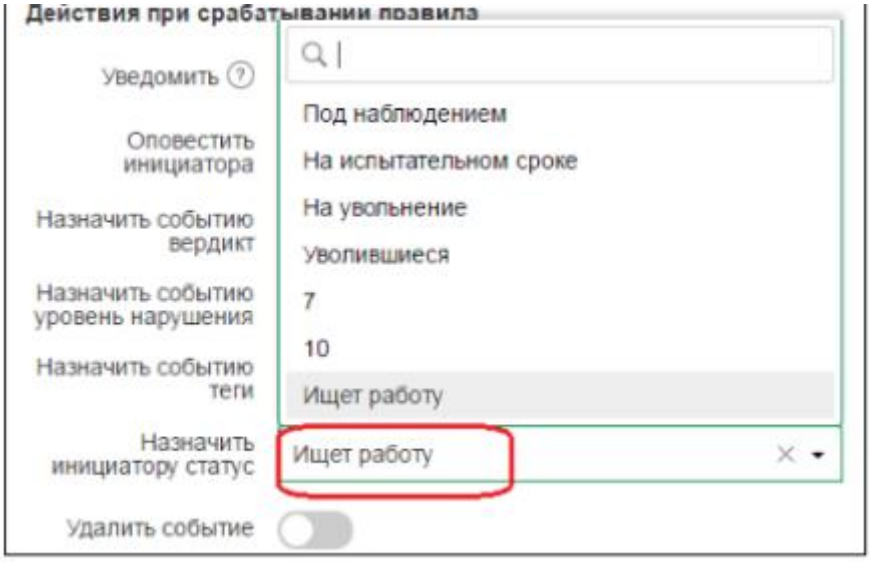
   - ✓ Создайте политику защиты данных "Выявление нелояльных сотрудников"
   - ✓ Добавьте правило передачи и укажите в качестве отправителей группу сотрудников компании, импортированную из Active Directory.



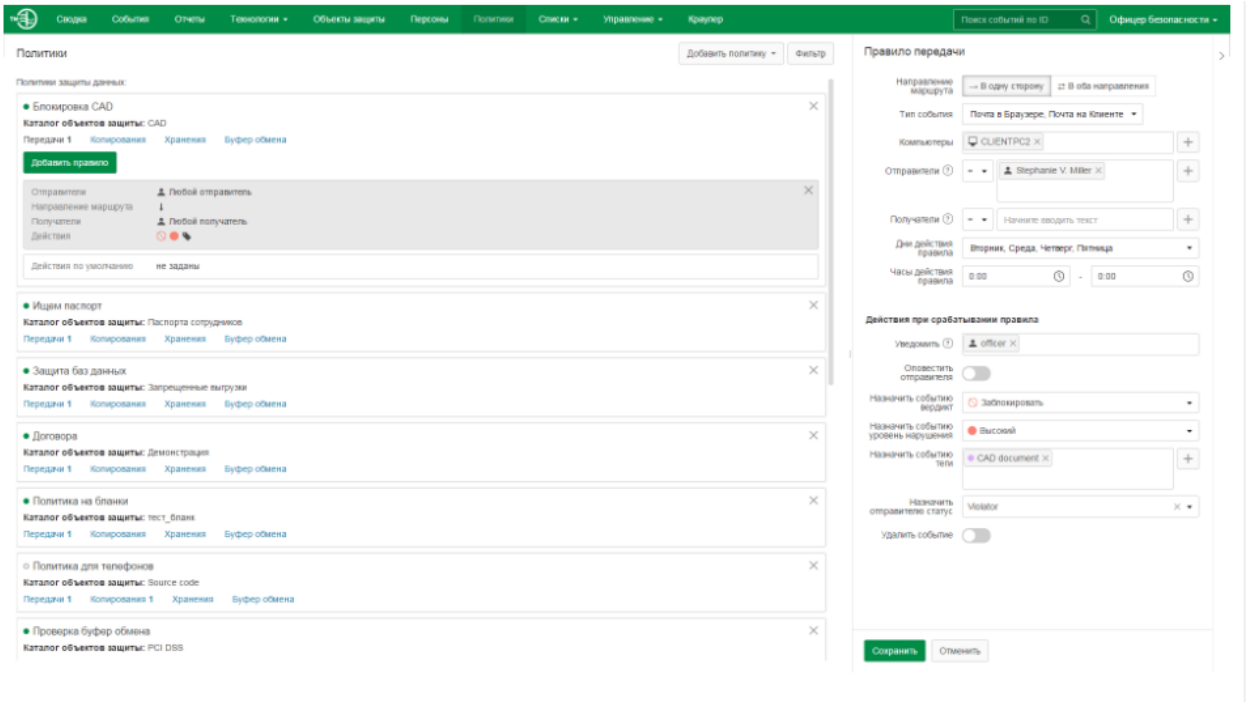
- ✓ В получателях укажите список веб-ресурсов "Поиск работы".

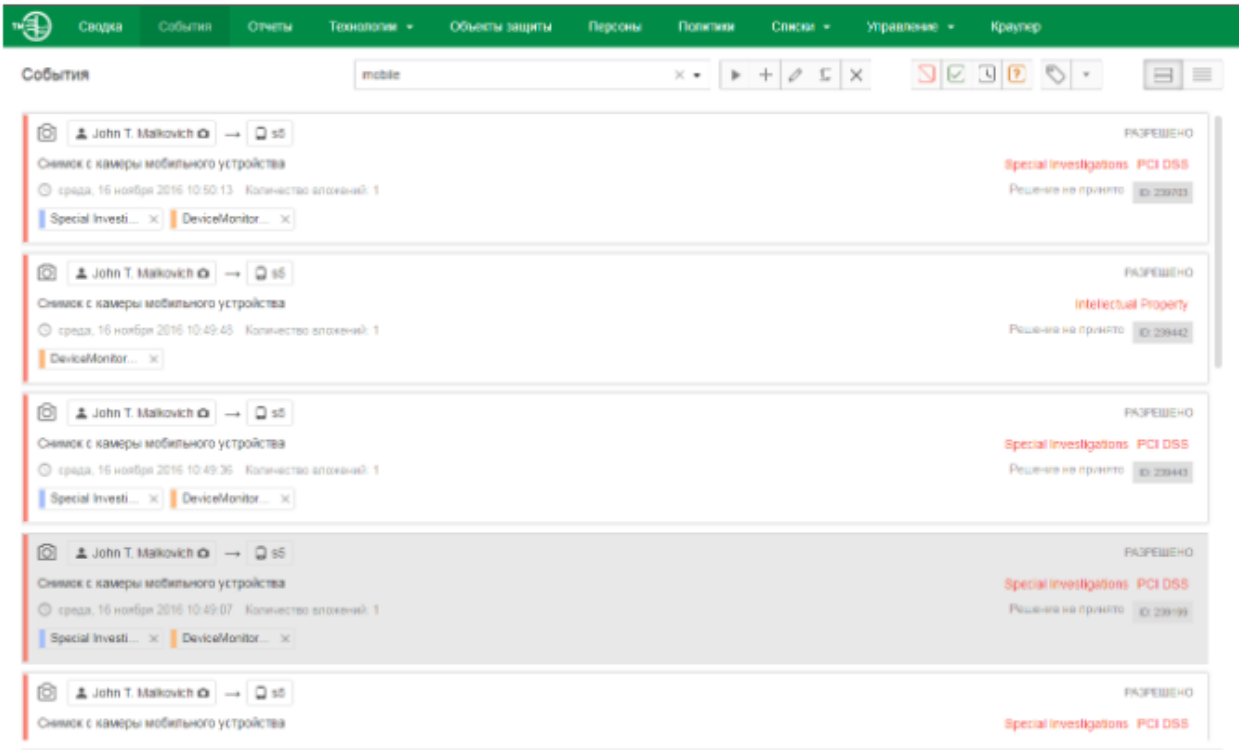


- ✓ Укажите действия при срабатывании правила. Например, вы можете назначать отправителю определенный статус.



Сохраните правило и примените изменения конфигурации.





8. Практическая работа № 26 «Создание политик с использованием перехвата фотографий 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.

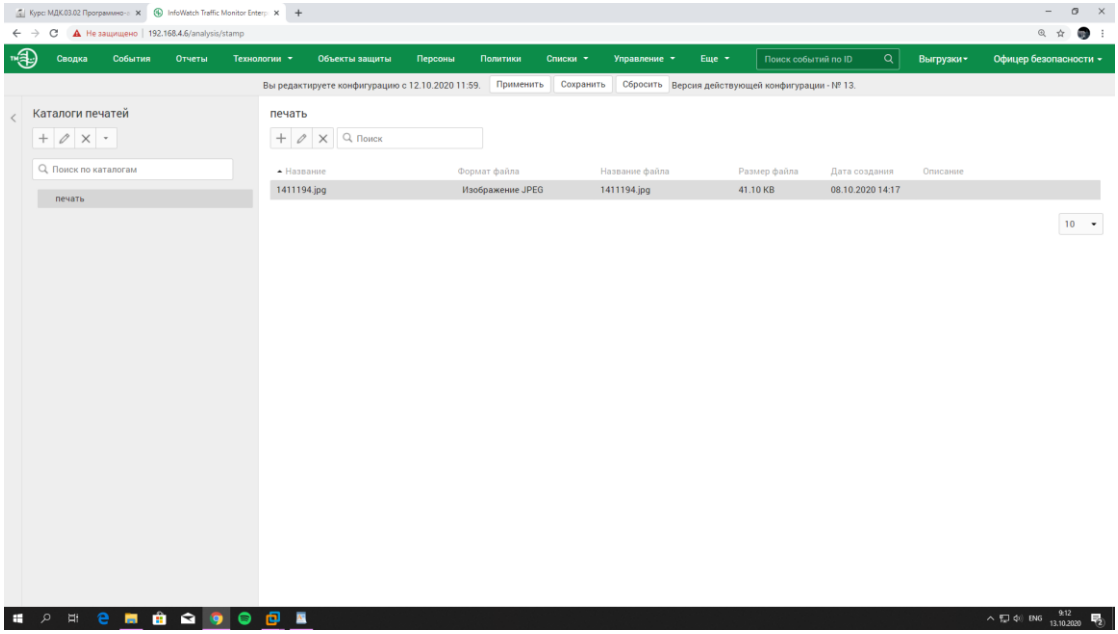
4. *Создайте новую роль. Для этого перейдите в раздел Управление* → Управление доступом. Затем вкладку роли. Далее «+» Создать роль. Установите для новой роли возможность работы только с отчётами. Сохраните.
   Подтвердите выполнение задания скриншотами.
5. Наделите импортированного пользователя из Active 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?

Создайте область видимости, добавьте нового импортированного пользователя.

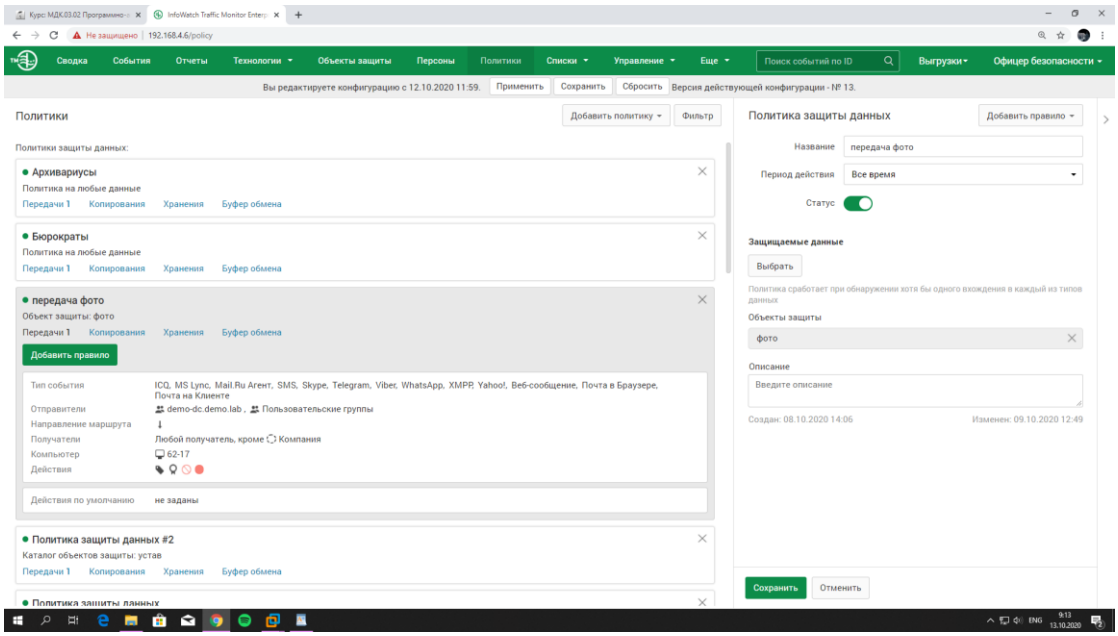
Эталон ответа:

Задание:

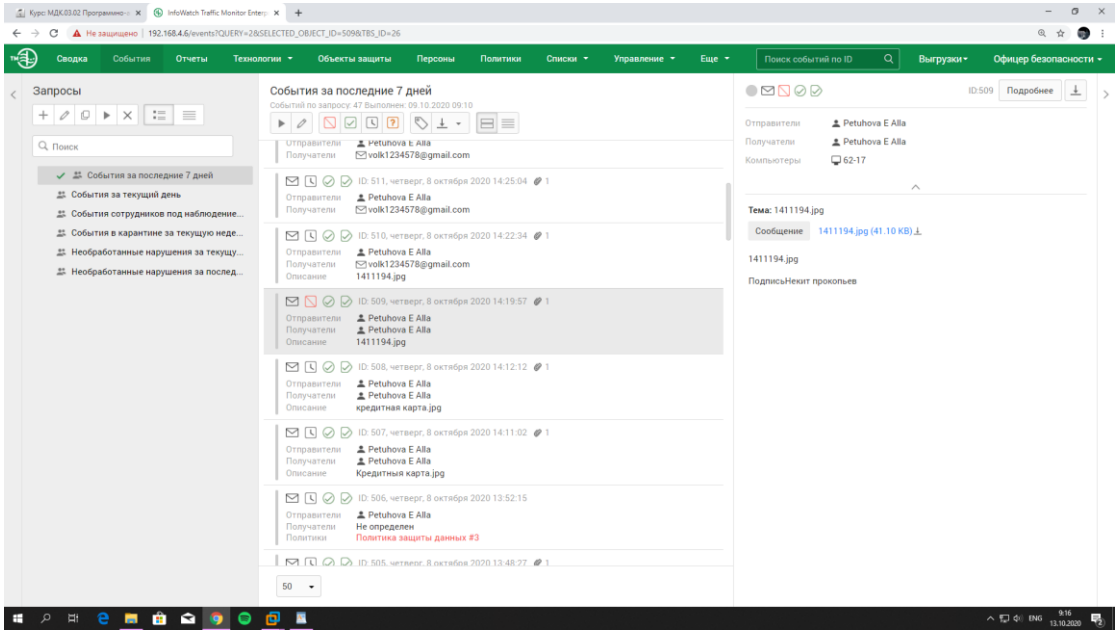
- Используя Руководство пользователя по Infowatch написать политику:
- Необходимо создать объект защиты Фото и внести все возможные форматы фотографий. В отчёт вставить скриншот с созданным объектом защиты.



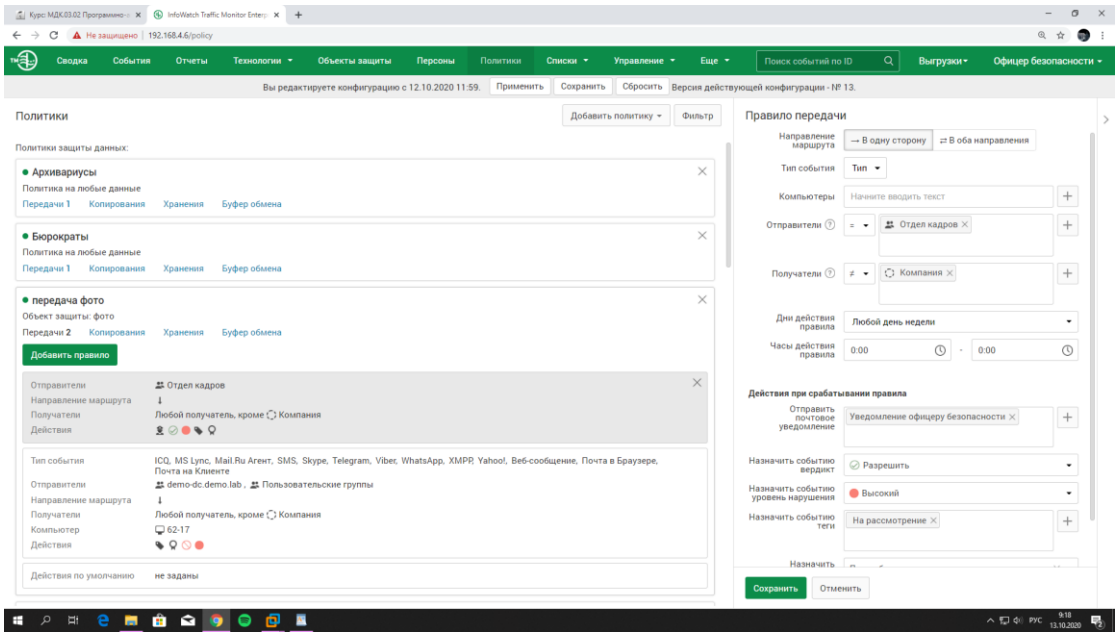
- Создать политику *Передача фото*, запрещающую передавать Фото из компании. Уровень угрозы поставить высокий. В отчёт вставить скриншот с созданной политикой.



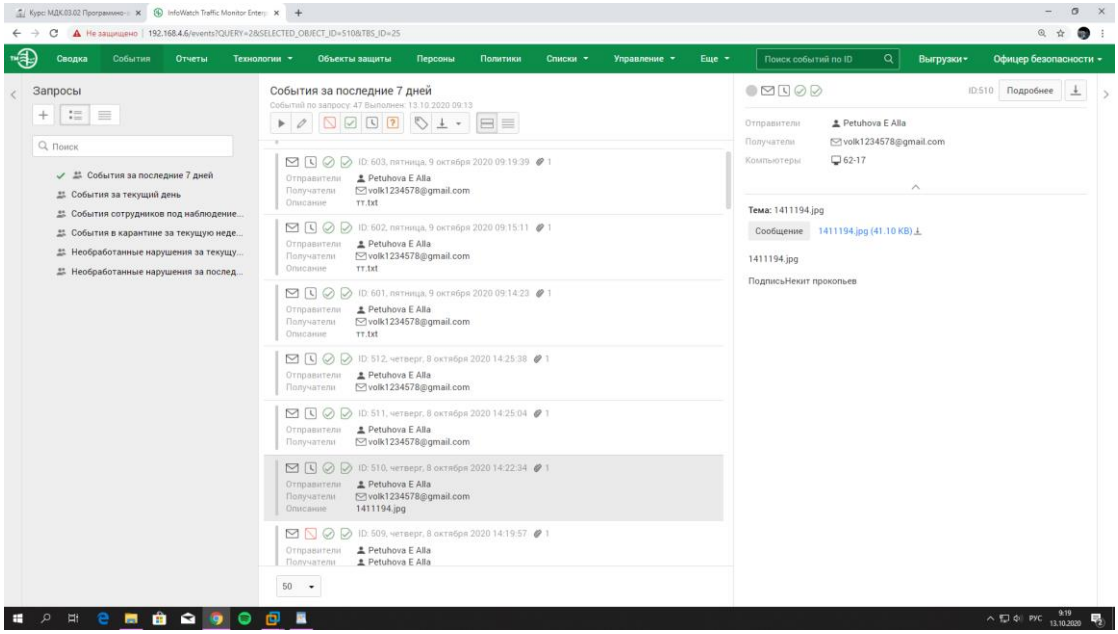
- Проверить работоспособность политики. В отчёт вставить скриншот с результатом.



- Внести следующие изменения в политику: разрешить отделу кадров отправлять фотографии из организации.

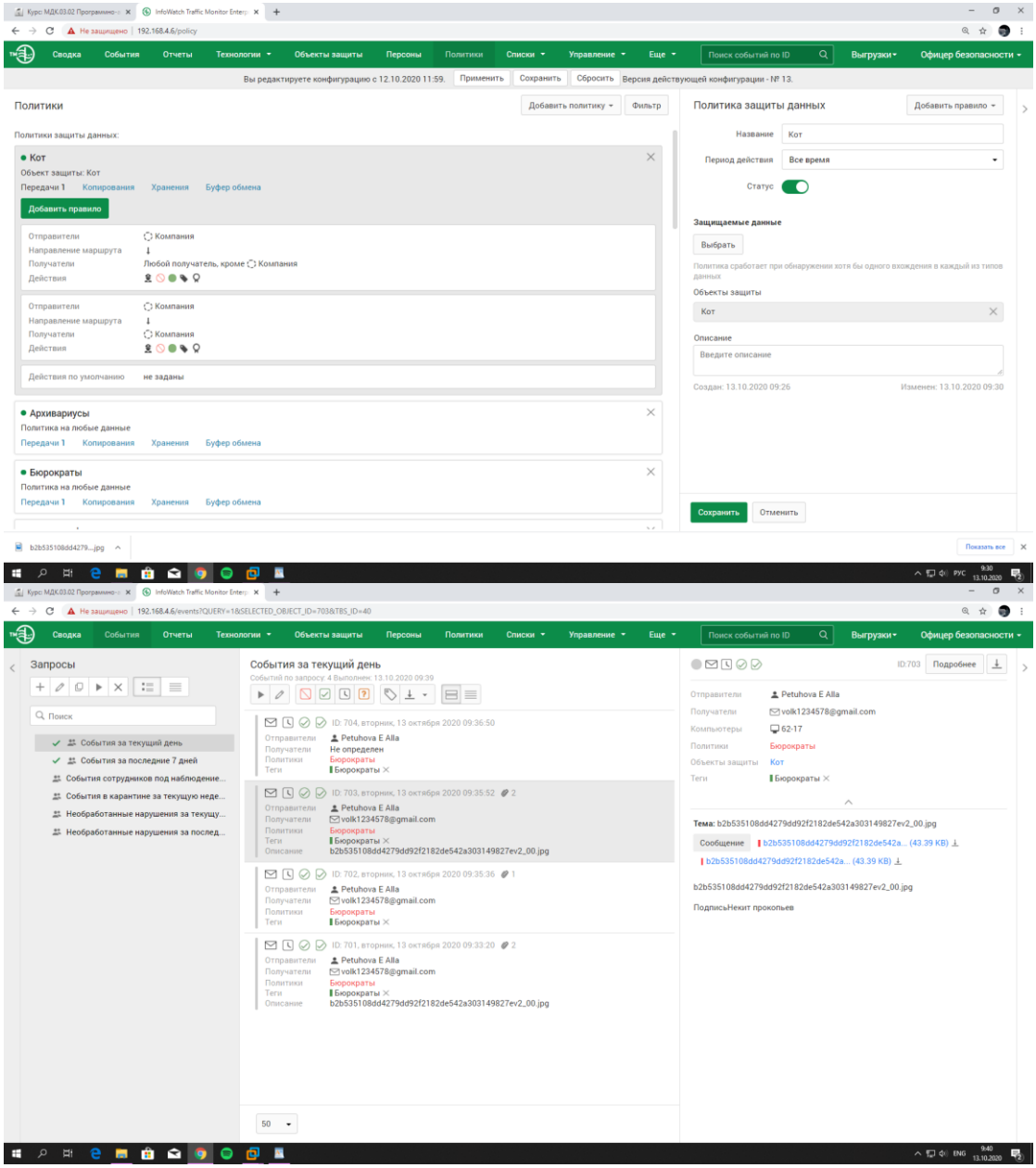


- Проверить работоспособность политики. В отчёт вставить скриншот с результатом.



- 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.
В отчёт скриншоты с созданной политикой, с результатом работы политики.



9. Практическая работа № 33 «Создание и 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

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.

Задание 3: Создание сводки

Необходимо удалить стандартную и создать новую панель сводки в разделе «Сводка», назвав ее «Сводка Демо».

Добавить 4 виджета на панель сводки:

- ✓ Динамика нарушений за последние три дня
- ✓ Статистика по политикам за последние три дня
- ✓ Количество нарушений за последние три дня
- ✓ Топ-нарушителей за последние три дня

Задание 4: Создание сводки по устройствам

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

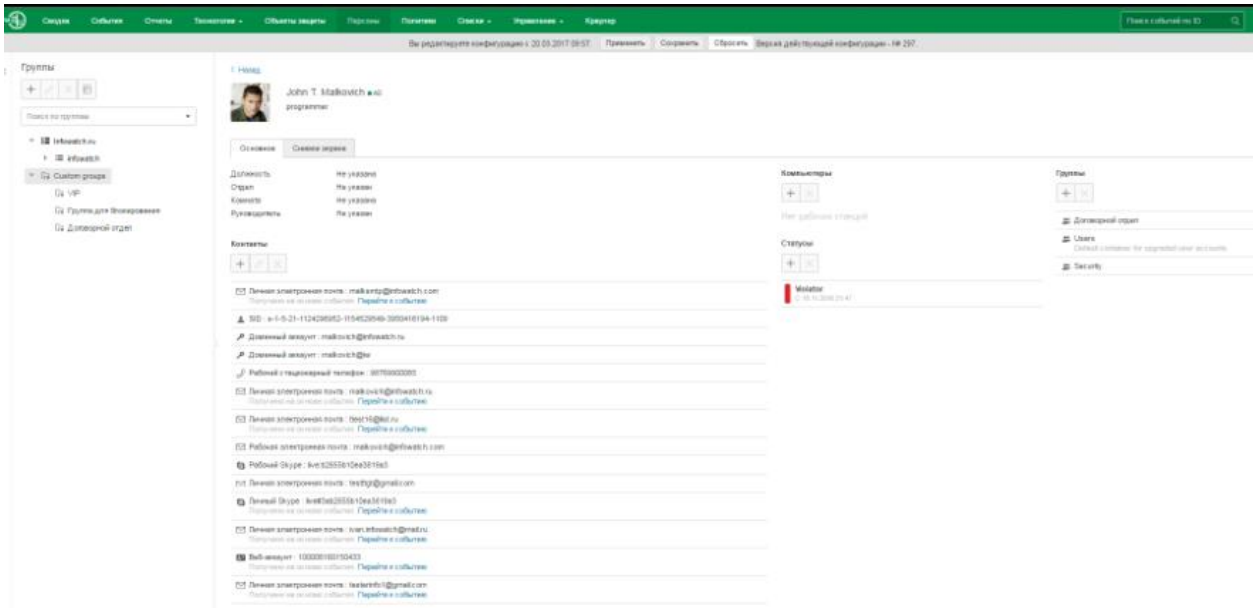
- ✓ Добавить виджет, выводящий информацию по событиям Crawler за последние 3 дня со средним и высоким уровнем угрозы.
- ✓ Добавить виджет, выводящий информацию по событиям только с компьютера нарушителя за последние три дня, которые имеют один любой из ранее созданных тегов.
- ✓ Добавить виджет, выводящий информацию по событиям только с компьютера нарушителя за последние три дня, которые имеют уровень угрозы от низкого до высокого.

По каждому заданию в отчёт вставить скриншоты.

Эталон ответа:

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

- ✓ Логин: userevents, пароль: XxXx1122

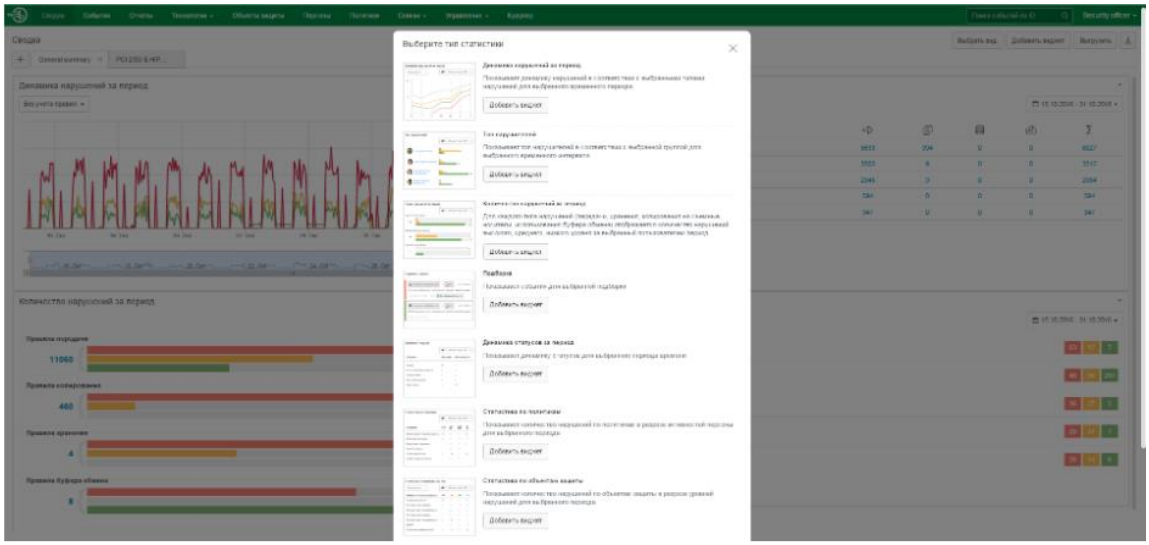


Задание 2: Создание отчета

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.

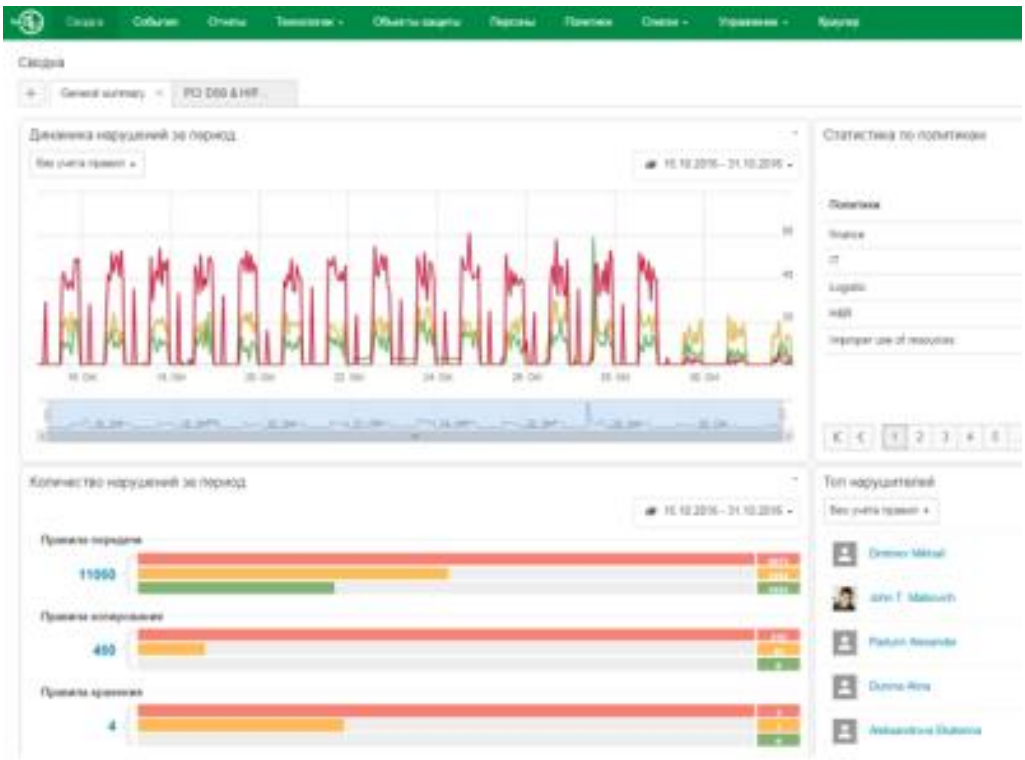


Задание 3: Создание сводки

Необходимо удалить стандартную и создать новую панель сводки в разделе «Сводка», назвав ее «Сводка Демо».

Добавить 4 виджета на панель сводки:

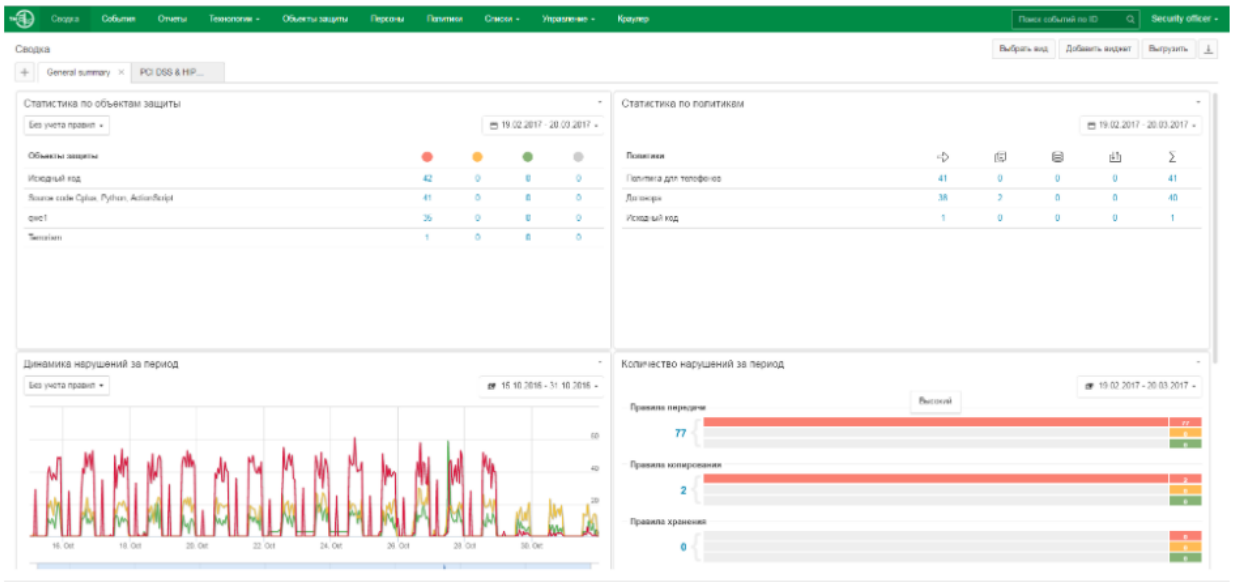
- ✓ Динамика нарушений за последние три дня
- ✓ Статистика по политикам за последние три дня
- ✓ Количество нарушений за последние три дня
- ✓ Топ-нарушителей за последние три дня



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.



10.Устный зачет по темам 3.1 – 3.3.

Инструкция для обучающихся: Зачет проводится в учебное время. Каждый студент отвечает на 2 вопроса по выбору преподавателя. С перечнем вопросов студенты ознакомлены заранее (за неделю). Время ответа 3 минуты. Время проведения зачета для группы – одно учебное занятие.

Перечень вопросов:

1. Общая характеристика и принципцы функционирования системы вторжений Snort
2. Синтаксис правил системы вторжений Snort
3. Общая характеристика и принципы функционирования VipNet
4. Порядок установки и настройки виртуальной защищённой сети
5. Общая характеристика и принципы функционирования dlp-системы Infowatch
6. Виды политик, способы их создания в Traffic monitor
7. Принципы построения регулярных выражений для создания политик
8. Виды правил и способы создания правил в Device monitor
9. Причины ложных срабатываний политик
10. Принципы мониторинга событий информационной безопасности в DLP-системе Infowatch

Эталоны ответов: приведены в Учебном пособии по МДК.03.03 «Защита от внутренних угроз информационной безопасности»

3.1.4. Оценка освоения теоретического курса профессионального модуля по МДК.03.05

Дидактические единицы	**Проверяемые ОК, ПК**	**Формы контроля (наименование контрольной точки)**		
		Текущая аттестация		**Промежуточная аттестация**
Тема 5.2. Классификация шифров	ОК1-ОК9 ПК 3.7	Практическая работа № 2 Алгоритмизация шифра Цезаря	Устный зачет по теме 5.2	Теоретические вопросы на дифференцированном зачёте
		Практическая работа № 5 Применение шифров гаммирования		
Тема 5.3. Криптографические протоколы		Практическая работа № 7 Метод шифрования с открытым ключом RSA	Устный зачет по теме 5.3	
Тема 5.4. Основы криптоанализа		Практическая работа № 13 Изучение частотного метода криптоанализа симметричных криптосистем	Устный зачет по теме 5.4	
Тема 5.5. Сетевые информационные службы		Практическая работа № 23 Анализ графических изображений на наличие скрытой информации.	Устный зачет по теме 5.5	

Устный зачет по теме 1

Инструкция для обучающихся

Зачет сдается в рамках учебного занятия. Каждый студент отвечает в устной форме на предложенные преподавателем 4 мини-вопросов.

Выполнение задания: одному студенту на ответ выделяется 3 мин., группа сдает зачет за одно учебное занятие.

Перечень вопросов:

1. Дайте определение понятиям «шифр», «ключ», «дешифрование».
2. Перечислите основные требования, предъявляемые к криптосистемам.
3. Дайте классификацию шифров по особенностям процедур преобразования сообщения.
4. Дайте классификацию шифров по стойкости шифра.

Эталоны ответов: **приведены в учебном пособии по МДК.03.05 «Основы криптографической защиты данных».**

Практическая работа № 2 «Алгоритмизация шифра Цезаря»

Инструкция для обучающихся

Внимательно прочитайте задание. Выполните опрессовку кабеля и розеток.

Время выполнения – 90 минут.

Задание

1. Ознакомьтесь с теоретической частью практической работы.
2. Загрузите программу Microsoft Excel.
3. На первом листе электронной книги запишите в столбец А буквы русского алфавита. В столбце В – номер букв, в столбце С – опять буквы (такая запись будет необходима для использования функции ВПР).
4. Переименуйте лист1 в Алфавит.
5. На втором листе электронной книги запишите название работы, ключ и название столбцов таблицы (S – исходные символы, X – числа исходных символов, Y – пересчитанные по формуле значения, S1 – символы закрытого текста). Значение ключа можно взять любым и обязательно его значение записать в отдельную ячейку (B5). В столбец S, начиная с 8 строки, впишите фамилию и имя, каждую букву в отдельной ячейке.

Вставьте фотографию выполненной работы

6. В столбце X должны быть числовые значения символов из столбца S. Эти значения хранятся на листе Алфавит. Чтобы получить их, можно воспользоваться функцией **ВПР** (категория – ссылки и массивы).

Встаем в ячейку B8 и вызываем функцию ВПР. Заполняем ее окно следующим образом:

Вставьте фотографию выполненной работы

7. Растянуть формулу вниз до конца таблицы.
8. В ячейку C8 (столбец Y) записывается формула для шифрования. Исходная формула метода Цезаря имеет вид: $y_i = (x_i + k) \mathrm{mod} n$. Операции mod в Excel со-

ответствует функция **ОСТАТ(число; делитель)**. В нашем случае **число** – это (x_i+k), а **делитель** – 32.

Т.е. функция **ОСТАТ** будет иметь вид **=ОСТАТ((B8+$B$5);32)**.

9. Эту формулу необходимо растянуть вниз до конца таблицы.
10. В ячейку D8 (столбец S1) опять записываем функцию **ВПР**, которая по числу Y найдет букву. Эта функция будет выглядеть следующим образом:

Вставьте фотографию выполненной работы

11. Окончательно таблица должна выглядеть следующим образом:

Вставьте фотографию выполненной работы

12. Рядом приготовьте место для дешифрования информации. Получите у преподавателя карточку с закрытым текстом и впишите его в столбец S1 новой таблицы.

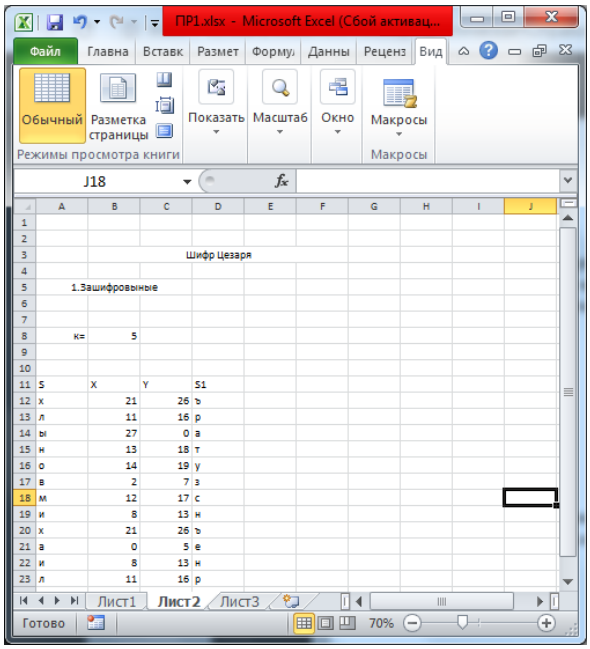
Вставьте фотографию выполненной работы

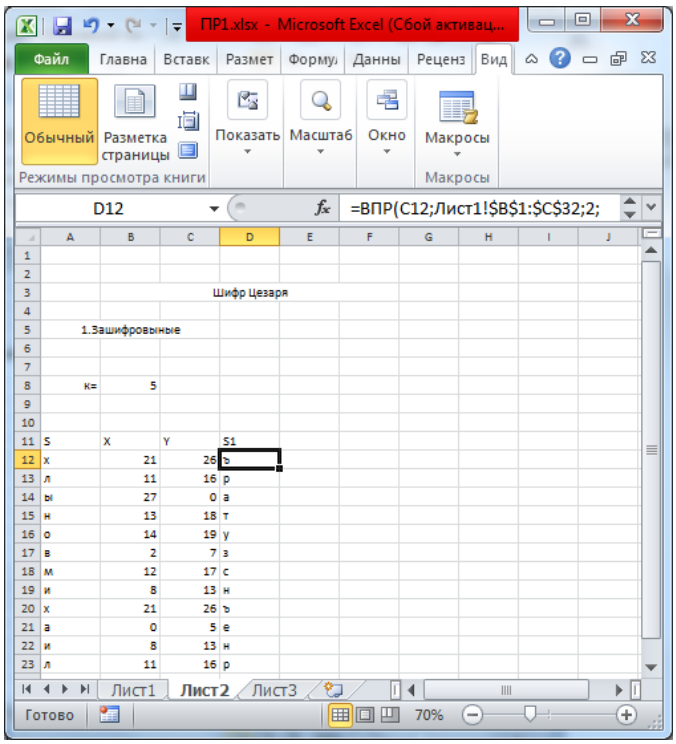
13. Проведите дешифрования текста по аналогии с зашифровыванием. Для расшифровывания (столбца X) используйте формулу $x_i = (y_i + (32-k)) \bmod 32$.

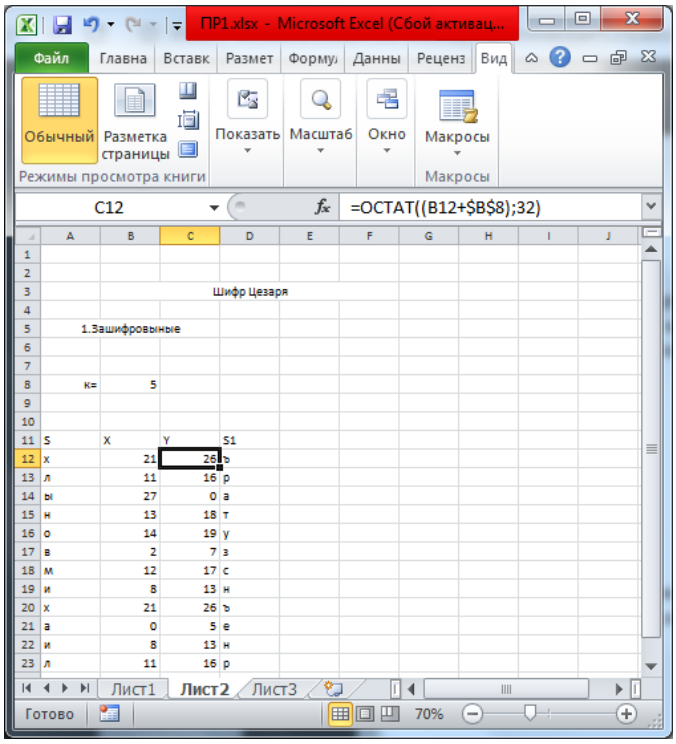
Вставьте фотографию выполненной работы

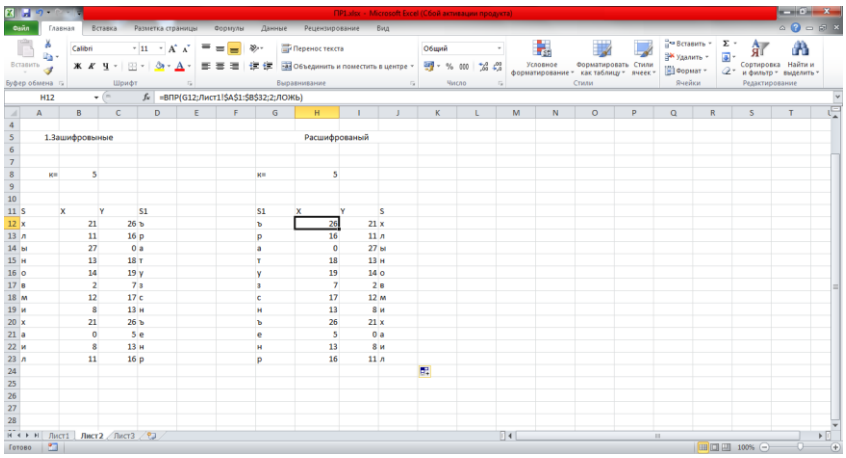
14. Запишите полученную фразу.

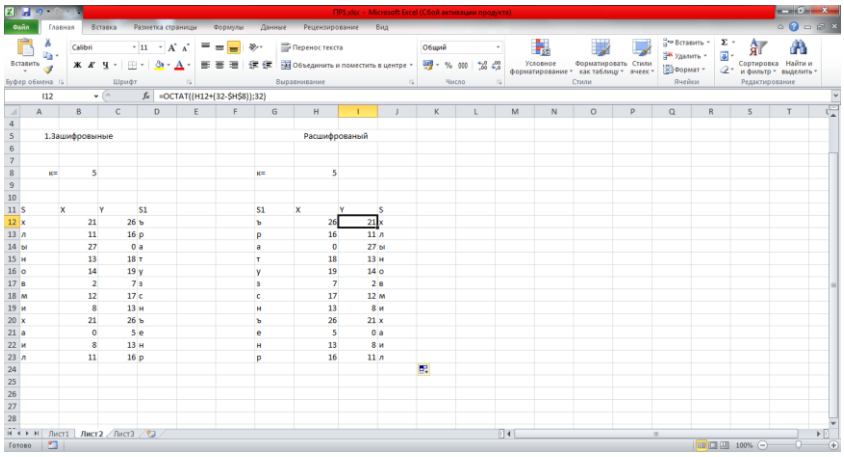
Эталон ответа:

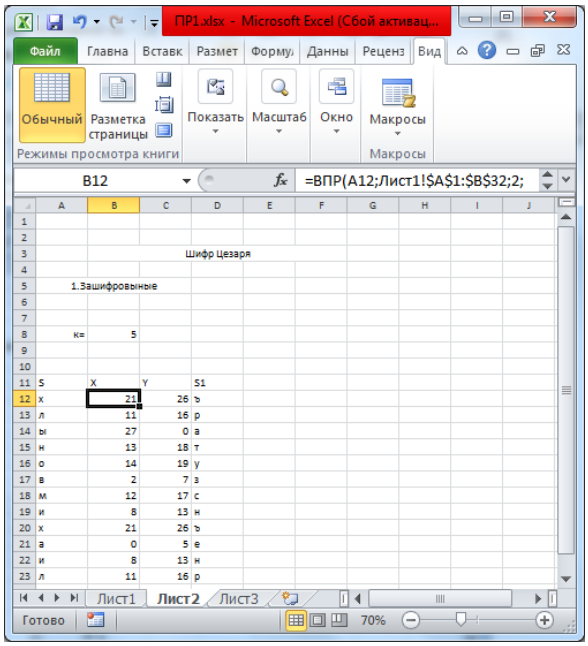


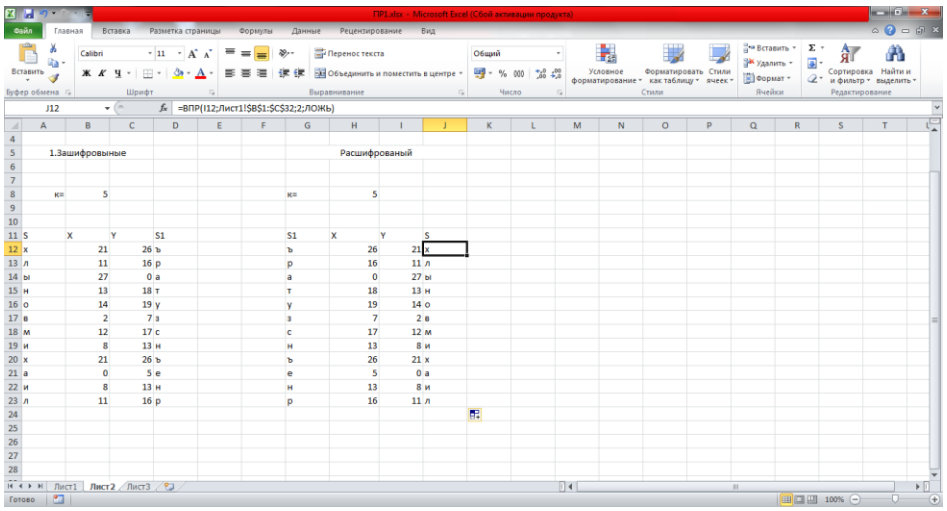

ПР1.xlsx - Microsoft Excel (Сбой активац...
Файл
Главна
Вставк
Размет
Форму
Данны
Реценз
Вид
Обычный
Разметка страницы
Показать
Масштаб
Окно
Макросы
Режимы просмотра книги
Макросы
D12
=ВПР(C12;Лист1!$B$1:$C$32;2;
Шифр Цезаря
1.Зашифровыные
к= 5
S X Y S1
х 21 26 ъ
л 11 16 р
ы 27 0 а
н 13 18 т
о 14 19 у
в 2 7 з
м 12 17 с
и 8 13 н
х 21 26 ъ
а 0 5 е
и 8 13 н
л 11 16 р
Лист1
Лист2
Лист3
Готово
70%

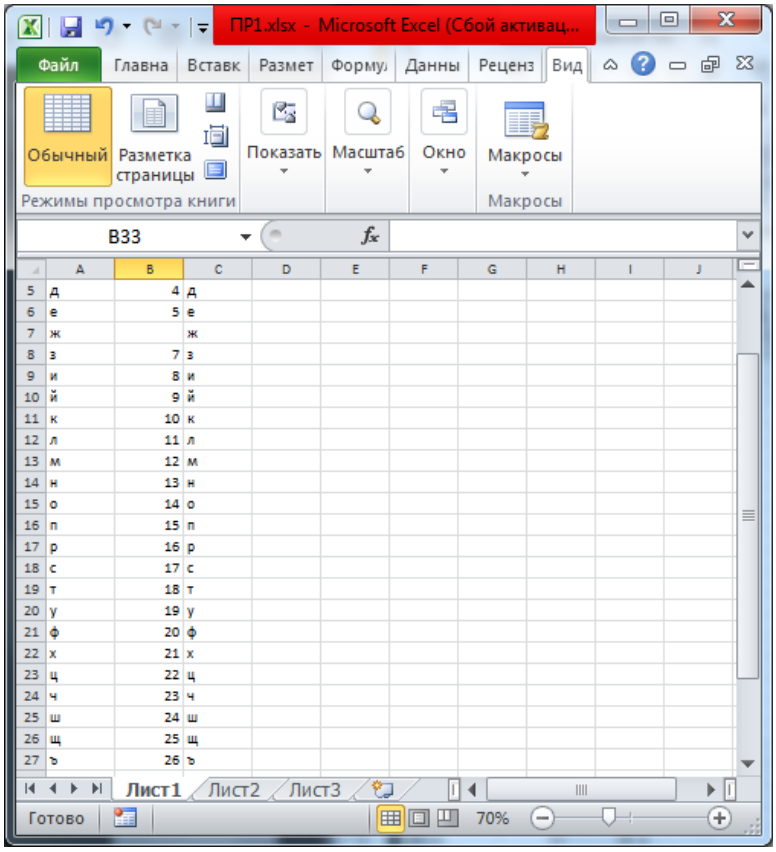

ПР1.xlsx - Microsoft Excel (Сбой активац...
Файл
Главна
Вставк
Размет
Форму
Данны
Реценз
Вид
Обычный
Разметка страницы
Показать
Масштаб
Окно
Макросы
Режимы просмотра книги
Макросы
C12
=ОСТАТ((B12+$B$8);32)
Шифр Цезаря
1.Зашифровыные
к= 5
S X Y S1
х 21 26 ъ
л 11 16 р
ы 27 0 а
н 13 18 т
о 14 19 у
в 2 7 з
м 12 17 с
и 8 13 н
х 21 26 ъ
а 0 5 е
и 8 13 н
л 11 16 р
Лист1
Лист2
Лист3
Готово
70%


ПР1.xlsx - Microsoft Excel (Сбой активации продукта)
=ВПР(G12;Лист1!$A$1:$B$32;2;ЛОЖЬ)
1.Зашифровыные
Расшифрованый
к=
5
S
X
Y
S1


ПР1.xlsx - Microsoft Excel (Сбой активации продукта)
=ОСТАТ((H12+(32-$H$8));32)
1.Зашифровыные
Расшифрованый
к=
5
S
X
Y
S1


ПР1.xlsx - Microsoft Excel (Сбой активац...
Файл
Главна
Вставк
Размет
Форму
Данны
Реценз
Вид
Обычный
Разметка страницы
Показать
Масштаб
Окно
Макросы
Режимы просмотра книги
Макросы
B12
=ВПР(A12;Лист1!$A$1:$B$32;2;
Шифр Цезаря
1.Зашифровыные
к=
5
S
X
Y
S1
Лист1
Лист2
Лист3
Готово
70%





Практическая работа № 5 «Применение шифров гаммирования»

Инструкция для обучающихся

Внимательно прочитайте задание. Примените шифр гаммирования.

Время выполнения – 90 минут.

Задание

- зашифровать свою фамилию с помощью шифров гаммирования по модулю N и модулю 2. При оформлении отчета необходимо привести исходное сообщение (фамилию), гамму и таблицы зашифрования/дешифрования;

- сгенерировать гамму с помощью регистра сдвига с линейной обратной связью (принять полином $x^8 + x^4 + x^3 + x^2 + 1$) и алгоритма Блюм - Блюм - Шуба. При оформлении отчета необходимо привести расчет исходного значения и таблицы генерации гамм для 10 итераций. Исходное значение определить сложением по модулю 2 всех букв фамилии в соответствии с кодировкой Windows 1251. Например, для фамилии "АБРАМОВ" расчет исходного значения для генераторов гамм будет выглядеть следующим образом.

1100 0000 А
1100 0001 Б
1101 0000 Р
1100 0000 А
1100 1100 М
1100 1110 О
1100 0010 В

11 :
01 0001 209_{10}

Эталон ответа:

	3		
S	X	Y	S1
Б	1	4	Д
А	0	3	Г
Й	9	12	М
Т	18	21	Х
Ы	27	30	Ю
С	17	20	Ф
О	14	17	С
Х	21	24	Ш
Р	16	19	У
А	0	3	Г
Н	13	16	Р
Я	31	2	В
Ю	30	1	Б
Т	18	21	Х
С	17	20	Ф
Я	31	2	В
В	2	5	Е
В	2	5	Е
И	8	11	Л
Д	4	7	З
Е	5	8	И
Ф	20	23	Ч
А	0	3	Г
Й	9	12	М
Л	11	14	О
О	14	17	С
В	2	5	Е

	3		
S	X	Y	S1
Б	1	4	Д
Е	5	8	И
Л	11	14	О
А	0	3	Г
Н	13	16	Р
К	10	13	Н
О	14	17	С
В	2	5	Е
А	0	3	Г
Л	11	14	О
Ь	28	31	Я
Б	1	4	Д
Е	5	8	И
Р	16	19	У
Т	18	21	Х
А	0	3	Г
Л	11	14	О
Е	5	8	И
К	10	13	Н
С	17	20	Ф
А	0	3	Г
Н	13	16	Р
Д	4	7	З
Р	16	19	У
О	14	17	С
В	2	5	Е
И	8	11	Л
Ч	23	26	Ъ

Практическая работа № 7 «Метод шифрования с открытым ключом RSA»

Инструкция для обучающихся

Внимательно прочитайте задание. Примените метод шифрования с открытым ключом RSA.

Время выполнения – 90 минут.

Задание

Задание 1. Известны значения модуля шифрования N, открытого ключа e и открытого текста. Закодировать символы сообщения с помощью табл. 1 (буквы «е» и «ё» не различаются), а затем зашифровать сообщение по алгоритму RSA с помощью открытого ключа (N, e).

Таблица 1

Таблица кодирования символов открытого текста

Символ	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п
Код	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Символ	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я
Код	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42

1. Выбрать параметры шифра и открытый текст из табл. 2 в соответствии с номером варианта (от 1 до 5). Выполнить кодирование, разбиение на блоки и шифрование блоков текста аналогично рассмотренному ниже примеру.

Таблица 2

Варианты задания

Номер варианта	N	e	Открытый текст	Криптограмма У
1	2279	281	сон	18221993
2	2773	113	лес	13081874
3	1643	127	вид	381131
4	1517	193	сто	367712
5	1711	235	гол	18384

Пример 1

N= 1739, e = 653, требуется зашифровать по алгоритму RSA текст «май».

2. Подготовить открытый текст к шифрованию, закодировав его с помощью табл. 3.7: м — 23, а — 11, й - 20.

Получили открытое сообщение X = 231120.

3. Разбить открытый текст X на блоки $x_к$, такие, что $x_к$<N. В рассматриваемом примере N= 1739, поэтому сообщение X можно разбить на два блока — x_1= 231, x_2 = 120.

4. Теперь можно зашифровать блоки x_1 используя формулу $y_к = x_к \bmod N$. Для вычислений можно воспользоваться табличным процессором MSExcel. Подготовить реализацию алгоритма для быстрого вычисления степени по модулю последовательным возведением в квадрат с хранением промежуточных результатов:

- перевести значение степени e в двоичное представление. В среде MS Excel для этих целей можно воспользоваться функцией ДЕС.В.ДВ группы Инженерные.

Данная функция осуществляет перевод значений только в диапазоне от 512 до 511.

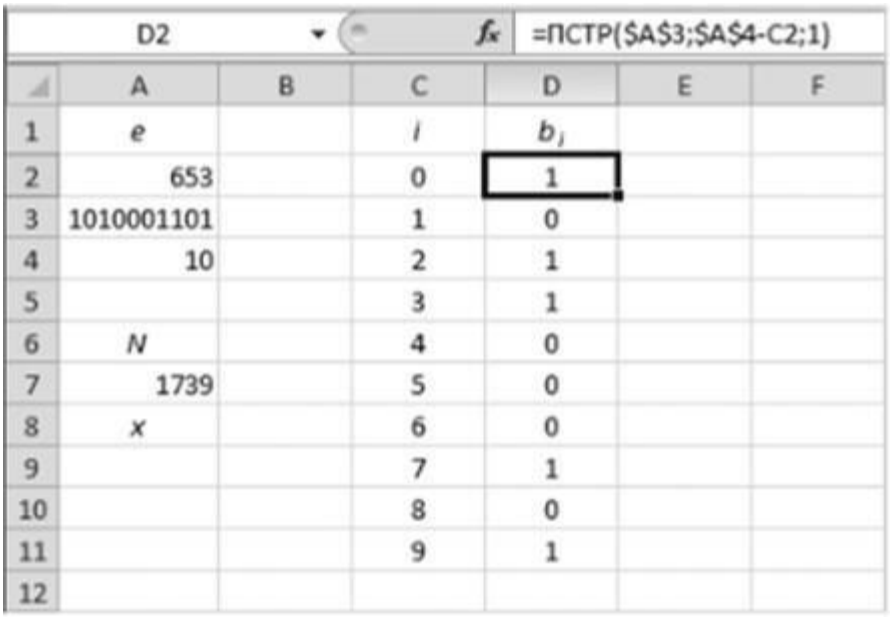
Если число e выходит за рамки указанного диапазона, следует воспользоваться стандартным приложением MS Windows Калькулятор, режим (вид) Программист. В этом случае следует установить переключатель системы счисления в позицию Dec (десятичная), ввести число e, а затем установить переключатель в позицию Bin (двоичная). Число будет переведено в двоичную систему счисления.

В примере e = 653 > 511, поэтому перевод в двоичную систему счисления осуществлен с помощью приложения Калькулятор: $e = 1010001101_2$.

Занести значение e в десятеричной и двоичной системах счисления на лист MS Excel;

- определить p — число разрядов двоичного представления числа e. В среде MS Excel для этих целей можно воспользоваться функцией ДЛСТР группы Текстовые. Пусть значение e в двоичной системе счисления занесено в ячейку A3. Тогда в ячейку A4 следует занести формулу =ДЛСТР(A3);
- теперь следует сформировать таблицу для вычисления степени e по модулю N. В ячейки столбца C занести значения от 0 до p - 1 (в примере - от 0 до 9), задав заголовок столбца — i;
- в соответствующие ячейки столбца D занести значения двоичных разрядов b_i (начиная с младшего разряда), для чего воспользоваться функцией ПСТР группы Текстовые. Если двоичное значение e находится

в ячейке A3, число разрядов h занесено в ячейку A4, а значения i содержатся в ячейках C2:C11, формула в ячейке D2 примет вид: =ПСТР($A$3;$A$4-C2;1). Ссылки на значения e и r должны быть абсолютными (преобразовать ссылку щелкнув на ней мышью, а затем нажав кнопку F4). Скопировать сформированную формулу в диапазон ячеек столбца D (D3:D11 в примере) рис. 1;



D2 | =ПСТР($A$3;$A$4-C2;1)

	A	B	C	D	E	F
1	*e*		*i*	b_j		
2	653		0	1		
3	1010001101		1	0		
4	10		2	1		
5			3	1		
6	*N*		4	0		
7	1739		5	0		
8	*x*		6	0		
9			7	1		
10			8	0		
11			9	1		
12						

Рис. 1. Занесение на лист MS Excel разрядов числа e

- занести в первый столбец значение N (в примере — 1739). Пусть значение 1739 занесено в ячейку A7, ячейка A6 содержит соответствующую подпись. Тогда в ячейку A8 занести подпись x, значения блоков для шифрования будут заноситься в дальнейшем в ячейку A9;
- в ячейках столбца E вычислить значения ряда x_2 задав заголовок столбца X_j — в ячейку E2 занести формулу =A9, в ячейку E3 — формулу =ОСТАТ(E2^2;$A$7), ссылка на значение N должна быть абсолютной. Скопировать формулу на оставшийся диапазон ячеек столбца E (E4:E11 в примере);
- в ячейки столбца F занести значение «1», если соответствующее значение бита = 0 (находится в столбце D), или значением E2 (из столбца E), если $b_i = 1$. Для этих целей следует воспользоваться функцией ЕСЛИ группы Логические. Формула в ячейке F2 имеет вид: =ЕСЛИ(D2=“0”;1;E2). Значение бита является текстовым, поэтому заключается в двойные кавычки. Скопировать формулу на диапазон ячеек столбца F (F3:F11 в примере);
- в столбце G подсчитать произведение значений из столбца F по модулю. Для этого в ячейку G2 ввести формулу =F2, в ячейку G3 — формулу =ОСТАТ(G2*F3;$A$7). Ссылка на значение N должна быть абсолютной.

Скопировать формулу на оставшийся диапазон ячеек столбца G (G4:G11 в примере);

- последняя заполненная ячейка столбца G (G11 в примере) содержит результат вычисления степени по модулю. Подписать эту ячейку как y.

5. Получить значения блоков шифротекста y_k, последовательно занося значения блоков $x_к$ в подготовленную для этого ячейку A9.

G11 | =ОСТАТ(G10*F11;$A$7)

	A	B	C	D	E	F	G	H
1	*e*		*i*	b_i	x_i			
2	653		0	1	120	120	120	
3	1010001101		1	0	488	1	120	
4	10		2	1	1640	1640	293	
5			3	1	1106	1106	604	
6	*N*		4	0	719	1	604	
7	1739		5	0	478	1	604	
8	*x*		6	0	675	1	604	
9	120		7	1	7	7	750	
10			8	0	49	1	750	
11			9	1	662	662	885	
12	*xk*	*yk*					*y*	
13	231	774						
14	120	885						
15		774885	Y					
16								

Рис. 2. Вычисление блоков шифротекста

Значения блоков $x_к$ и полученные $y_к$ с подписями занести на лист (например, в диапазон ячеек A12:B14) - рис. 2.

Значения блоков шифротекста: $y_1 = 774$, $y_2 = 885$.

Ниже сформированных блоков шифротекста получить полное значение У, использовав операцию конкатенации &. В примере в ячейку B15 следует занести формулу =B13&B14 и подписать эту ячейку как У. Получена криптограмма У = 774885.

Задание 2. Криптограмма У получена RSA шифрованием на известном открытом ключе (N, e). Определить секретный ключ d и получить открытый текст, если кодирование символов сообщения осуществлялось с помощью табл. 1.

Выбрать значения открытого ключа (N, e) и криптограммы У из табл. 2 в соответствии с номером варианта (от 1 до 5). Выполнить дешифрование криптограммы по аналогии с рассмотренным ниже примером.

Эталон ответа:

Задание №1.

142522	гол								
142	x1			i	b1	xi			
522	x2			0	1	522	522	522	
1711	n			1	0	435	1	522	
281	e			2	0	1015	1	522	
xк mod N		242962		3	1	203	203	1595	
				4	1	145	145	290	
e2	100011001			5	0	493	1	290	
p		9		6	0	87	1	290	
				7	0	725	1	290	
				8	1	348	348	1682	
								y	
x	Y					xi			
522	1682					142	142	142	
142	780					1343	1	142	
	7801682					255	1	142	
						7	7	994	
						49	49	798	
						690	1	798	
						442	1	798	
						310	1	798	
						284	284	780	
								Y	

Задание №2.

29	59		1624	1	0		i	bi	yi		
n	1711		281	0	1		0	1	384	384	384
ф(н)			219	1	-5	5	1	0	310	1	384
1624			62	-1	6	1	2	0	284	1	384
			33	4	-23	3	3	1	239	239	1093
d			29	-5	29	1	4	0	658	1	1093
393			4	9	-52	1	5	0	81	1	1093
110001001			1	-68	393	7	6	0	1428	1	1093
9			0	281	-1624	4	7	1	1383	1383	806
y							8	1	1502	1502	935
											x
18384											
	384										
	18										
x											
1236	935										
гжас											
бщ											

Практическая работа № 13 «Изучение частотного метода криптоанализа симметричных криптосистем»

Инструкция для обучающихся

Внимательно прочитайте задание. Примените частотный метод криптоанализа симметричных криптосистем.

Время выполнения – 90 минут.

Задание

Криптосистема Цезаря определяется выражением:

$$yi = (xi + k) \bmod m,\ i = \overline{1,n},$$

где y_i - буква криптограммы, x_i - буква открытого сообщения, k - ключ

шифра, n - длина криптограммы (открытого текста), m - мощность алфавита. Выражения для расшифрования имеет вид:

$$x_i = (y_i - k) \bmod m.$$

Метод частотного криптоанализа базируется на реализации методов теории статистических решений, а именно, на методе максимального правдоподобия [4]. В соответствии с этим методом оценкой ключа шифра k^* является такое его значение, которое доставляет максимальное значение логарифму функции правдоподобия $l(k)$. Для криптосистемы Цезаря оценка формируется в соответствии с выражением:

$$k^* = \arg\max_k l(k), \quad l(k) = \sum_{j=0}^{m-1} \nu_{(j+k) \bmod m} \log p_1(j), \qquad (1)$$

где $p_1(j)$ - оценка вероятности встречаемости j -й буквы алфавита мощности m в открытых текстах, ν_j - частость встречаемости j -й буквы в криптограмме.

Выражение (1) справедливо, если источник открытых сообщений представляет собой стационарный источник дискретных сообщений без памяти. В случае, когда источник открытых сообщений представляет собой однородную цепь Маркова, оценка ключа будет определяться в соответствии с выражением:

$$k^* = \arg\max_k \left\{ \sum_{j=0}^{m-1} \delta_{y_1,(j+k) \bmod m} + \sum_{j,s=0}^{m-1} \nu_{js} \log p_1(j) \right\}$$

2 Порядок выполнения работы

2.1 При подготовке к лабораторной работе

На этапе подготовки к лабораторной работе студенты должны, используя литературу [1,2,3,4] и материалы лекций углубить свои знания по криптосистеме Цезаря и частотному методу криптоанализа простейших шифров.

Студенты на предстоящее лабораторное занятие готовят русский и английский алфавиты со значениями вероятностей встречаемости букв.

2.2 Во время проведения занятия.

Преподаватель перед проведением занятия проводит контрольный опрос студентов и определяет степень их готовности к лабораторной работе. Затем преподаватель разбивает группу студентов на несколько подгрупп по два студента в каждой.

Каждая подгруппа получает от преподавателя индивидуальный вариант задания на лабораторную работу, который представляет собой криптограмму, зашифрованную с помощью криптосистемы Цезаря.

Студенты должны:

1. Определить частотные характеристики криптограммы, для чего рассчитать значение частоты встречаемости символов $j \in A_m$ в криптограмме.
2. Определить вероятностные характеристики алфавита, для чего вычислить значение логарифма вероятности встречаемости символа $\log p_1(j)$ для заданного алфавита.
3. Полученные значения свести в таблицу 1.

Таблица 1.

Буква	А	Б	…	Ю	Я
$j \in A_m$					
$\log p_1(j)$					
$\nu_j(Y)$					

4. В соответствии с выражением (1) определить значение логарифма функции правдоподобия $l(K)$ и построить соответствующую графическую зависимость.

5. Определить в соответствии с выражением (1) оценку ключа k^*. 6. Дешифровать заданную криптограмму, используя оценку ключа k^*. При получении осмысленного текста подготовить отчет и представить его преподавателю.

4 Содержание отчета

Отчет должен включать в себя следующие пункты:

1. Задание на выполнение лабораторной работы (исходную криптограмму).
2. Основные расчетные соотношения.
3. Результаты расчетов, сведенные в табл. 1.
4. Графическую зависимость $l(k)$ и значение оценки ключа k^*.
5. Полученный дешифрованием открытый текст.

Эталон ответа:

Выполняется совместно двумя студентами. Произвести расчет ключа.

1. Прочитайте конспект по данной теме в рабочей тетради.
2. Совместно с удалённой стороной устанавливать открытые параметры p и g (обычно значения p и g генерируются на одной стороне и передаются другой), где p является случайным простым числом (p-1)/2 также должно быть случайным простым числом (для повышения безопасности) g является первообразным корнем по модулю p.

p=7

(p-1)/2 =3

|P| = kor(g)

g=9

3. Вычислить открытый ключ A, используя преобразование над закрытым ключом

$A = g^a \bmod p$ для каждого студента.

a=2

$A=9^a \bmod 3 = 78$

4. Обменяться открытыми ключами с удалённой стороной.
5. Вычислить общий секретный ключ K, используя открытый ключ удаленной стороны B и свой закрытый ключ a

$K = B^a \bmod p$

$K=14^2 \bmod 3 =193$

K получается равным с обеих сторон, потому что:

$B^a \bmod p = (g^b \bmod p)a \bmod p = g^{ab} \bmod p = (g^a \bmod p)b \bmod p = A^b \bmod p$

6. Сравнить общие ключи. Абонент 2

P=5

(5-1)\2=2

G=4

b=2

$B=4^2 \bmod 2 = 14$

$Y=78^2 \bmod 2 = 193$

Практическая работа № 23 «Анализ графических изображений на наличие скрытой информации»

Инструкция для обучающихся

Внимательно прочитайте задание. Примените на практике анализ графических изображений на наличие скрытой информации.

Время выполнения – 90 минут.

Задание

Приступая к работе скачайте и распакуйте архив PR5.zip, программа и тестовое изображение в нем. В ходе выполнения работы можно указывать программе, в какие компоненты JPEG изображения внедрить больше информации, а в какие меньше. Суммарное количество информации при этом остается прежним и меняется только ее распределение между компонентами изображения.

После любых изменений в настройках нажимайте на надпись: «Изображение с внедренным сообщением» и тогда на экран будет выведено это изображение, а справа от

него будет выводиться количественная оценка его качества в дБ (PSNR - пиковое соотношение сигнал/шум). Для выполнения лабораторной работы необходимо, чтобы качество было больше 43 дБ.

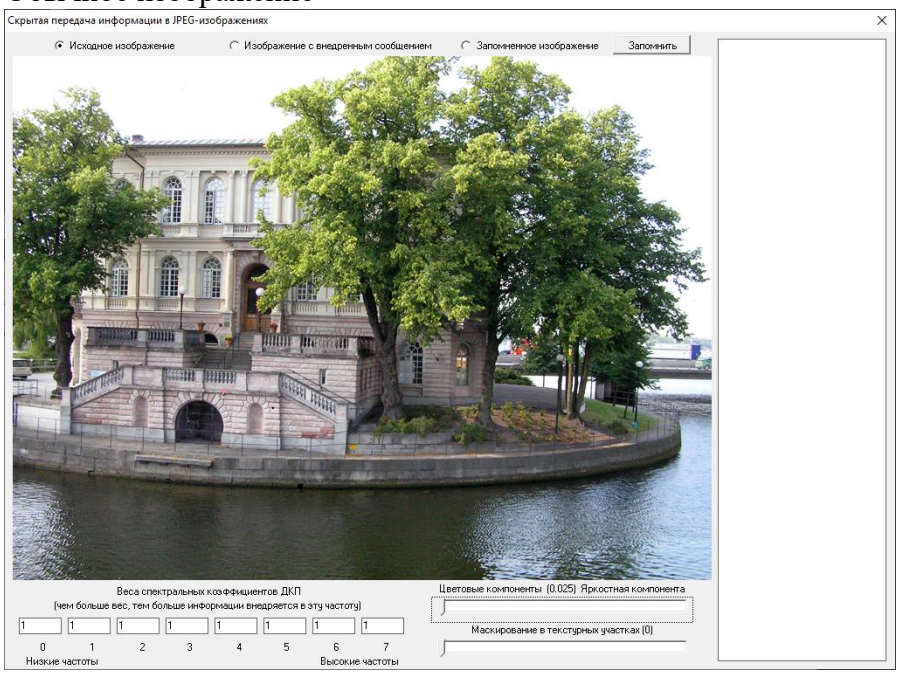
С помощью ползунка можно выбирать баланс распределения информации между цветовой и яркостной компонентой. Определите, в какой из компонент искажения заметнее?

С помощью ползунка «Маскирование в текстурных участках» можно перераспределять информацию между однородными (небо) участками изображения и текстурными (листья, рябь на воде).

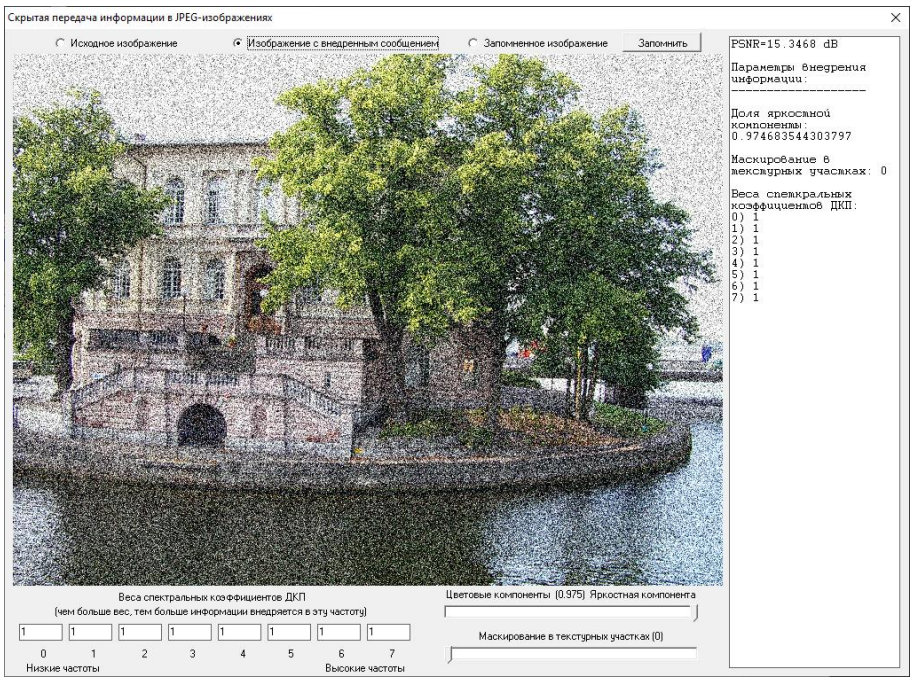
В восьми строках ввода можно для каждого коэффициента ДКП (при JPEG сжатии выполняется дискретное косинусное преобразование в блоках 8x8 пикселей и для каждого блока осуществляется квантование) отдельно задать долю внедрения туда информации. Эти коэффициенты должны быть положительными числами, большими, чем ноль. 0-й коэффициент соответствует самой низкой частоте, а 9-й - самой высокой. Чем больший коэффициент будет задан, тем больше информации будет внедрено в соответствующие частоты изображения. Определите, в каких частотах человеческий глаз лучше замечает искажения?

Эталон ответа

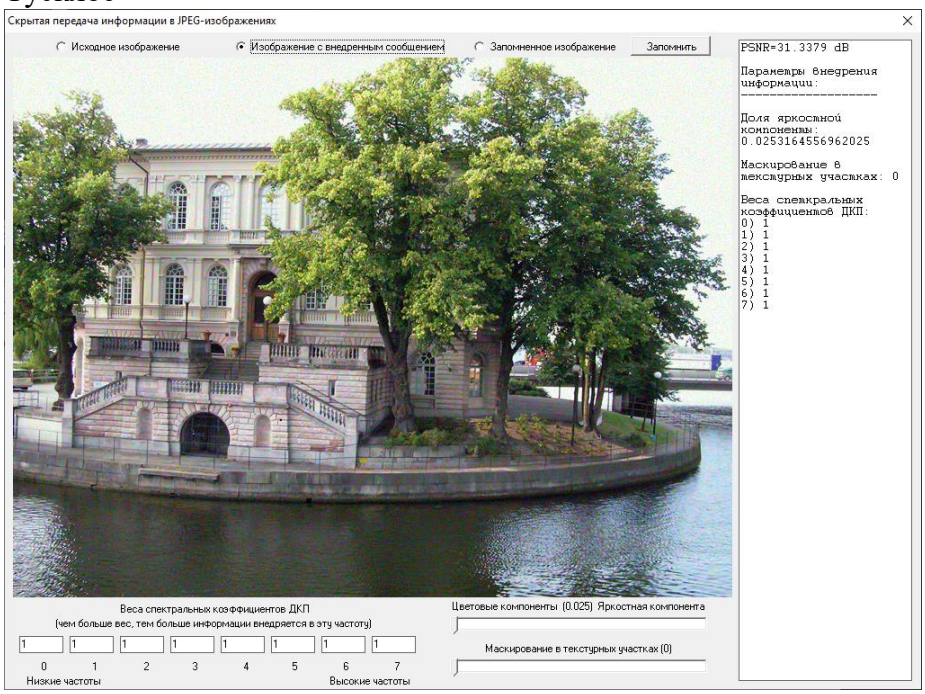
Обычное изображение



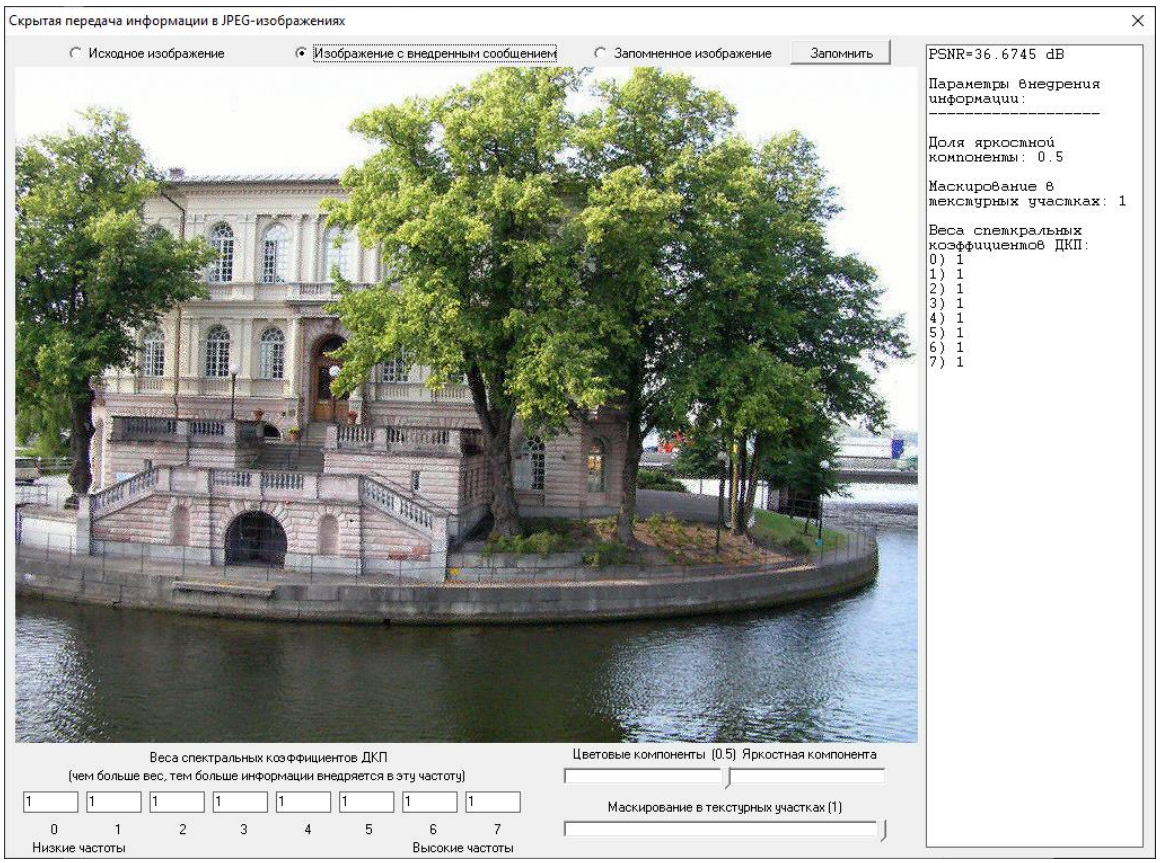
Яркое



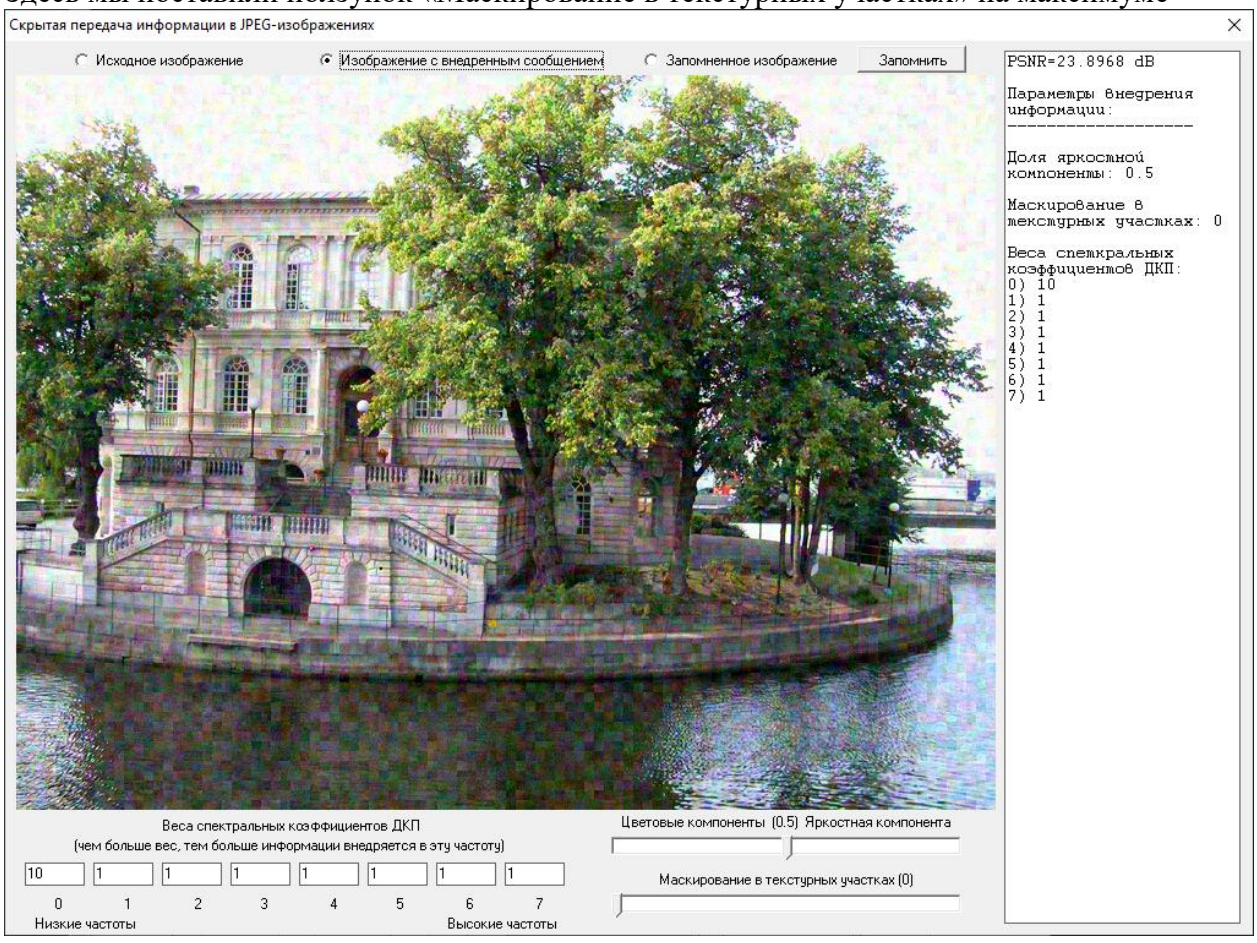
Тусклое



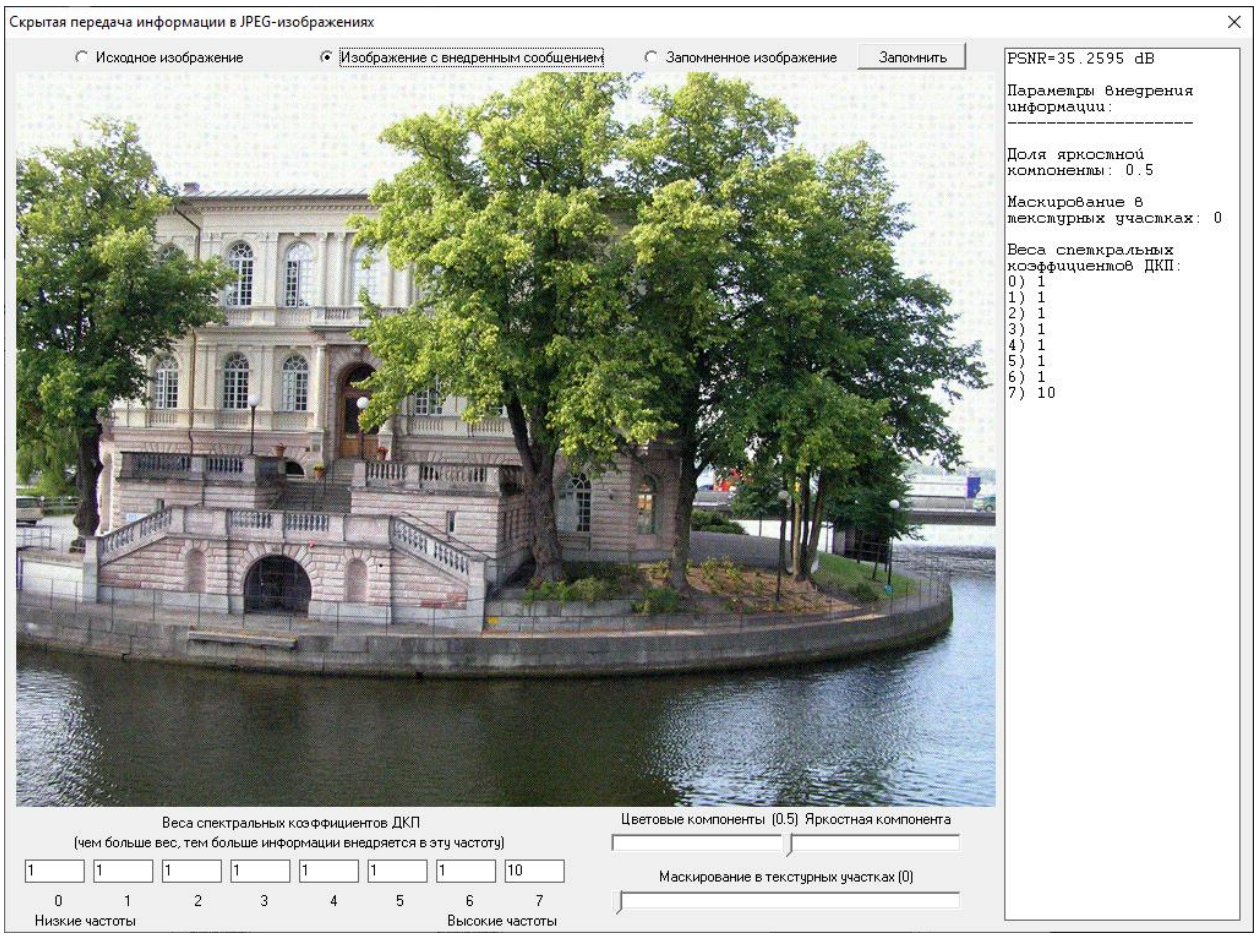
Видно, что более искаженное изображение, если оно будет яркое



Здесь мы поставили ползунок «Маскирование в текстурных участках» на максимуме



Искажения на низких частотах



Искажение на высоких частотах

Здесь видим, что человеческий глаз лучше замечает искажения на низких частотах

3.2. Оценка сформированности умений и знаний, общих компетенций при выполнении курсовой работы

Основные требования к структуре, содержанию и оформлению курсовой работы представлены в Методических рекомендациях для студентов по выполнению курсовой работы.

Курсовая работа выполняется по единой теме по индивидуальным вариантам: «Эксплуатация объектов сетевой инфраструктуры» и носит практический характер.

Проверяемые результаты обучения:

Показатели оценки работы

Проверяемые освоенные умения и усвоенные знания	Общие и профессиональные компетенции, формируемые в процессе выполнения роботы	Этап выполнения курсовой работы
У1-У5 З1-З3	ОК 1- 9 ПК 3.1, ПК 3.2 ПК 3.4, ПК 3.5	Выдача тем курсовых работ. Знакомство с Методическими указаниями по выполнению и оформлению курсовых работ
У6-У16 З1-З19	ОК 1- 9 ПК 3.1, ПК 3.2 ПК 3.4, ПК 3.5	Знакомство с источниками информации, подбор информации в соответствии с планом курсовой работы
У6-У16 З1-З19	ОК 1- 9 ПК 3.1, ПК 3.2 ПК 3.4, ПК 3.5	Выполнение Введения к курсовой работе
У6-У16 З1-З19	ОК 1- 9 ПК 3.1, ПК 3.2 ПК 3.4, ПК 3.5	Работа над теоретической частью курсовой работы
У6-У16 З1-З19	ОК 1- 9 ПК 3.1, ПК 3.2 ПК 3.4, ПК 3.5	Работа над практической частью курсовой работы
У6-У16 З1-З19	ОК 1- 9 ПК 3.1, ПК 3.2 ПК 3.4, ПК 3.5	Работа над составлением Заключения к работе
У6-У16 З1-З19	ОК 1- 9 ПК 3.1, ПК 3.2 ПК 3.4, ПК 3.5	Разработка презентации и доклада
У6-У16 З1-З19	ОК 1- 9 ПК 3.1, ПК 3.2 ПК 3.4, ПК 3.5	Подготовка к защите КР

3.3. Контрольно-оценочные материалы для промежуточной аттестации

Формой промежуточной аттестации по МДК.03.01 и МДК 03.03 является **комплексный экзамен.**

1. Перечень экзаменационных вопросов:
2. Физические аспекты эксплуатации. Физическое вмешательство в инфраструктуру сети.
3. Активное и пассивное сетевое оборудование: кабельные каналы, кабель, патч-панели, розетки.
4. Полоса пропускания, паразитная нагрузка.
5. Расширяемость сети. Масштабируемость сети. Добавление отдельных элементов сети (пользователей, компьютеров, приложений, служб).
6. Наращивание длины сегментов сети; замена существующей аппаратуры.
7. Увеличение количества узлов сети; увеличение протяженности связей между объектами сети.
8. Техническая и проектная документация. Паспорт технических устройств.
9. Физическая карта всей сети; логическая топология компьютерной сети.
10. Классификация регламентов технических осмотров, технические осмотры объектов сетевой инфраструктуры.
11. Проверка объектов сетевой инфраструктуры и профилактические работы
12. Проведение регулярного резервирования. Обслуживание физических компонентов; контроль состояния аппаратного обеспечения; организация удаленного оповещения о неполадках.
13. Программное обеспечение мониторинга компьютерных сетей и сетевых устройств.
14. Протокол SNMP, его характеристики, формат сообщений, набор услуг.
15. Задачи управления: анализ производительности и надежности сети.
16. Оборудование для диагностики и сертификации кабельных систем. Сетевые мониторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры.
17. Настройка H.323. Описание H.323 и общие рекомендации. Функциональные компоненты H.323.Установка и поддержка соединения H.323. Соединения без и с использованием GateKeeper. Соединения с использованием нескольких GateKeeper. Многопользовательские конференции. Обеспечение отказоустойчивости.
18. Настройка SIP. Описание и общие рекомендации. Технология SIP и связанные с ней стандарты. Функциональные компоненты SIP. Сообщения SIP. Адресация SIP. Модель установления соединения. Планирование отказоустойчивости.
19. Установка и инсталляция программного коммутатора. Монтажные процедуры. Процедуры инсталляции. Управление аппаратными средствами и портами. Протоколы управления MGCP, H.248. Создание аналоговых абонентов. Внутристанционная маршрутизация.
20. Управление программным коммутатором. Маршрутизация. Группы соединительных линий. Подключение станций с TDM (абонентский доступ TDM). Сигнализация SIP, SIP-T, H.323 и SIGTRAN. IP -абоненты. Группы абонентов. Дополнительные абонентские услуги.
21. Организация эксплуатации систем IP-телефонии.
22. ехническое обслуживание, плановый текущий ремонт, плановый капитальный ремонт, внеплановый ремонт.
23. Восстановление работы сети после аварии.
24. Схемы послеаварийного восстановления работоспособности сети, техническая и проектная документация, способы резервного копирования данных, принципы работы хранилищ данных
25. Системы инвентаризации сетевых ресурсов

26. Аудит сетевой инфраструктуры
27. Современные угрозы сетевой безопасности.
28. Методы атак.
29. Безопасность Сетевых устройств OSI
30. Безопасный доступ к устройствам.
31. Мониторинг и управление устройствами.
32. Авторизация, аутентификация и учет доступа (AAA)
33. ACL. Технология брандмауэра
34. Контекстный контроль доступа (CBAC).
35. Политики брандмауэра основанные на зонах.
36. Реализация технологий предотвращения вторжения
37. Безопасность локальной сети
38. Обеспечение безопасности пользовательских компьютеров.
39. Безопасность беспроводных сетей, VoIP и SAN
40. Криптографические системы
41. Реализация технологий VPN
42. Управление безопасной сетью
43. Принципы безопасности сетевого дизайна. Безопасная архитектура. Управление процессами и безопасность
44. Тестирование сети на уязвимости. Непрерывность бизнеса, планирование восстановления аварийных ситуаций
45. Жизненный цикл сети и планирование. Разработка регламентов компании и политик безопасности.
46. Cisco ASA. Введение в Адаптивное устройство безопасности ASA.
47. Использование систем обнаружения вторжения

Условия выполнения

1. Количество билетов для экзаменующегося: 1
2. Время подготовки к ответу: 30 минут
3. Требования к устным ответам:
   Полное овладение содержанием учебного материала, в котором обучающийся легко ориентируется, владение понятийным аппаратом.
4. Оборудование: учебная аудитория, стол, стул, пишущая ручка, бумага.

Результаты промежуточной аттестации фиксируются в протоколе.

Формой промежуточной аттестации по МДК.03.02 является **дифференцированный зачет.**

Перечень экзаменационных вопросов:

5. Понятие объекта управления.
6. Классификации технологических объектов управления
7. Основные функции АСУТП
8. Основные функции САУ.
9. Техническое, программное и информационное обеспечение АСУТП
10. Состав АСУ ТП
11. Основные понятия автоматизированной обработки информации

12. Простая модель технологического процесса
13. Требования к промышленным сетям.
14. Протокол MODBUS
15. Беспроводные локальные сети для промышленного применения
16. Типовые промышленные проводные и кабельные сетевые протоколы

Формой промежуточной аттестации по МДК.03.03 является **экзамен.**

Перечень экзаменационных вопросов:

1. Виды политик, способы их создания в Traffic monitor
2. Виды правил и способы создания правил в Device monitor
3. Виды программно-аппаратных средств защиты информации
4. Защита информации в VPN-сетях
5. Мониторинг событий информационной безопасности в DLP-системе Infowatch
6. Общая характеристика и принципы функционирования dlp-системы Infowatch
7. Общая характеристика продуктов ViPNet для создания защищённой сети
8. Понятие построения виртуальной защищённой сети, межсетевой взаимодействие защищённых сетей
9. Средства защиты в вычислительных сетях

Условия выполнения

1. Количество билетов для экзаменующегося: 1
2. Время подготовки к ответу: 30 минут
3. Требования к устным ответам:
   Полное овладение содержанием учебного материала, в котором обучающийся легко ориентируется, владение понятийным аппаратом.
4. Оборудование: учебная аудитория, стол, стул, пишущая ручка, бумага.

Результаты промежуточной аттестации фиксируются в протоколе.

Формой промежуточной аттестации по МДК.03.04 является **дифференцированный зачет.**

Перечень вопросов:

1. Шифры замены. Основы шифрования. Шифры однозначной замены.
2. Шифры перестановки. Шифры гаммирования.
3. Шифры одинарной перестановки. Шифры множественной перестановки
4. Шифрование с открытым ключом. Алгоритм RSA.
5. Алгоритм шифрования Эль-Гамаля
6. Протоколы обмена ключами.
7. Алгоритм Диффи-Хеллмана-Меркла
8. Протоколы аутентификации.
9. Хеш-функции. MD5.
10. Основные характеристики звуковой информации
11. Протоколы электронной цифровой подписи

12. Протокол на базе алгоритма RSA
13. Алгоритм цифровой подписи ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012.
14. Угрозы безопасности при использовании криптографии.
15. Методы криптоанализа. Частотный анализ.
16. Компьютерная стеганография.

Критерии оценки устных ответов

В системе оценки знаний и умений используются **следующие критерии**:

«Отлично» – за глубокое и полное овладение содержанием учебного материала, в котором обучающийся легко ориентируется, владение понятийным аппаратом за умение связывать теорию с практикой, решать практические задачи, высказывать и обосновывать свои суждения. Отличная отметка предполагает грамотное, логичное изложение ответа (как в устной, так и в письменной форме), качественное внешнее оформление.

«Хорошо» – если обучающийся полно освоил учебный материал, владеет понятийным аппаратом, ориентируется в изученном материале, грамотно излагает ответ, но содержание и форма ответа имеют некоторые неточности.

«Удовлетворительно» – если обучающийся обнаруживает знание и понимание основных положений учебного материала, но излагает его неполно, непоследовательно, допускает неточности в определение понятий, не умеет доказательно обосновать свои суждения.

«Неудовлетворительно» – если обучающийся имеет разрозненные, бессистемные знания, не умеет выделять главное и второстепенное, допускает ошибки в определение понятий, искажает их смысл, беспорядочно и неуверенно излагает материал, за полное незнание и непонимание учебного материала или отказ отвечать.