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

УТВЕРЖДАЮ
Заместитель директора
по учебно-производственной работе
_____ О.В. Фомичева
«26» декабря 2023 г.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
по выполнению практических работ
по МДК.02.01 Программные и программно-аппаратные средства защиты информации
ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ

для специальности
10.02.05 Обеспечение информационной безопасности автоматизированных систем

Санкт-Петербург
2023 г.

Методические рекомендации рассмотрены на заседании методического совета СПб ГБПОУ «АУГСГиП»

Протокол № 2 от «29» ноября 2023 г.

Методические рекомендации одобрены на заседании цикловой комиссии общетехнических дисциплин и компьютерных технологий

Протокол № 4 от «21» ноября 2023 г.

Председатель цикловой комиссии: Караченцева М.С. _____

Разработчики: преподаватели СПб ГБПОУ «АУГСГиП»

С О Д Е Р Ж А Н И Е

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Рабочая тетрадь для выполнения практических работ предназначена для организации работы на практических занятиях по темам 1.1-1.10 МДК.02.01«Программные и программно-аппаратные средства защиты информации» ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами», являющегося важной составной частью в системе подготовки специалистов среднего профессионального образования по специальности ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами».

Практические занятия являются неотъемлемым этапом изучения тем 1.1-1.10 МДК.02.01«Программные и программно-аппаратные средства защиты информации» и проводятся с целью:

– формирования практических умений в соответствии с требованиями к уровню подготовки обучающихся, установленными рабочей программой учебной дисциплины;

– обобщения, систематизации, углубления, закрепления полученных теоретических знаний;

– готовности использовать теоретические знания на практике.

Практические занятия по темам 1.1-1.10 МДК.02.01«Программные и программно-аппаратные средства защиты информации» способствуют формированию следующих общих и профессиональных компетенций:

– ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

– ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

– ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

– ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

– ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

– ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.

– ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

– ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.

– ОК 09. Использовать информационные технологии в профессиональной деятельности.

– ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.
– ОК 11. Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.
– ПК 2.1. Применять программно-аппаратные средства обеспечения информационной безопасности в автоматизированных системах.
– ПК 2.2. Участвовать в эксплуатации программно - аппаратных средств обеспечения информационной безопасности, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности.
– ПК 2.3. Участвовать в мониторинге эффективности применяемых программно - аппаратных средств обеспечения информационной безопасности в автоматизированных системах.
– ПК 2.4. Участвовать в обеспечении учета, обработки, хранения и передачи конфиденциальной информации.
– ПК 2.5. Решать частные технические задачи, возникающие при проведении всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, программ, алгоритмов.
– ПК 2.6. Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности программно - аппаратными средствами.

В Рабочей тетради предлагаются к выполнению практические работы, предусмотренные рабочей программой ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами».

При разработке содержания практических работ учитывался уровень сложности освоения студентами соответствующей темы, общих и профессиональных компетенций, на формирование которых направлен ПМ.02.

Выполнение практических работ в рамках тем 1.1-1.10 МДК.02.01«Программные и программно-аппаратные средства защиты информации» ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами» позволяет освоить комплекс работ по выполнению настройки программных средств защиты информации в автоматизированных системах, обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами. В Рабочей тетради представлены примеры установки и настройки программных и программных-аппаратных средств защиты информации по темам 1.1-1.10 МДК.02.01«Программные и программно-аппаратные средства защиты информации».

Рабочая тетрадь для выполнения практических заданий по темам 1.1-1.10 МДК.02.01«Программные и программно-аппаратные средства защиты информации» ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами» имеет практическую направленность и значимость. Формируемые

в процессе их проведения умения могут быть использованы студентами в будущей профессиональной деятельности.

80-90 % заданий направлено на выполнение, моделирование обучающимися практических видов работ, связанных с будущей профессиональной деятельностью в условиях, приближенных к реальным производственным.

Рабочая тетрадь предназначена для студентов колледжа, изучающих темы 1.1-1.10 МДК.02.01«Программные и программно-аппаратные средства защиты информации», ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами» и может использоваться как на учебных занятиях, которые проводятся под руководством преподавателя, так и для самостоятельного выполнения практических работ, предусмотренных рабочей программой во внеаудиторное время.

Практические занятия проводятся в учебном кабинете, не менее двух академических часов, обязательным этапом является самостоятельная деятельность студентов.

Практические занятия в соответствии с требованием ФГОС включают такой обязательный элемент, как использование персонального компьютера.

Оценки за выполнение практических работ выставляются по пятибалльной системе. Оценки за практические работы являются обязательными текущими оценками по темам 1.1-1.10 МДК.02.01«Программные и программно-аппаратные средства защиты информации» ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами» и выставляются в журнале теоретического обучения.

1. ПЕРЕЧЕНЬ ПРАКТИЧЕСКИХ РАБОТ ПО ТЕМАМ 1.1-1.10 МДК.02.01 «ПРОГРАММНЫЕ И ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ» ПМ.02 «ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ»

№ раздела, темы	Освоение умений в процессе занятия	Формируемые ОК и ПК	Тема практического занятия	Кол-во часов
Тема 2.1	З1, З2,З3 У1-У5	ОК1-ОК11 ПК2.1-ПК2.6	Практическая работа № 1 «Сравнительный анализ продуктов SIEM»	2
Тема 2.4	З1, З2,З3 У1-У5	ОК1-ОК11 ПК2.1-ПК2.6	Практическая работа № 2 «Создание загрузочной флешки с антивирусной программой для быстрой проверки»	2
Тема 2.5.	З1, З2,З3 У1-У5	ОК1-ОК11 ПК2.1-ПК2.6	Практическая работа № 3 «Установка серверной версии Windows»	2
		ОК1-ОК11 ПК2.1-ПК2.6	Практическая работа № 4 «Установка домена Active Directory»	2
		ОК1-ОК11 ПК2.1-ПК2.6	Практическая работа № 5 «Создание и внесение пользователей и компьютеров в домен»	2
		ОК1-ОК11 ПК2.1-ПК2.6	Практическая работа № 6 «Создание и применение глобальных политик домена»	2
		ОК1-ОК11 ПК2.1-ПК2.6	Практическая работа № 7 «Создание и применение локальных политик домена»	2
		ОК1-ОК11 ПК2.1-ПК2.6	Практическая работа № 8 «Установка сервера безопасности Secret Net Studio»	2
		ОК1-ОК11 ПК2.1-	Практическая работа № 9 «Установка клиента и программы управления Secret Net Studio»	2

№ раздела, темы	Освоение умений в процессе занятия	Формируемые ОК и ПК	Тема практического занятия	Кол-во часов
		ПК2.6		
		ОК1-ОК11 ПК2.1-ПК2.6	Практическая работа № 10 «Настройка централизованной установки клиента Secret Net Studio»	2
		ОК1-ОК11 ПК2.1-ПК2.6	Практическая работа № 11 «Работа с действующими средствами локальной защиты с помощью Secret Net Studio»	2
		ОК1-ОК11 ПК2.1-ПК2.6	Практическая работа № 12 «Удаление всех компонентов Secret Net Studio»	2
		ОК1-ОК11 ПК2.1-ПК2.6	Практическая работа № 13 «Установка Dallas Lock»	2
		ОК1-ОК11 ПК2.1-ПК2.6	Практическая работа № 14 «Настройка средств администрирования в Dallas Lock»	2
		ОК1-ОК11 ПК2.1-ПК2.6	Практическая работа № 15 «Настройка подсистем управления доступом в Dallas Lock»	2
		ОК1-ОК11 ПК2.1-ПК2.6	Практическая работа № 16 «Разграничение доступа к объектам файловой системы в Dallas Lock»	2
		ОК1-ОК11 ПК2.1-ПК2.6	Практическая работа № 17 «Работа с подсистемой регистрации и учёта в Dallas Lock»	2
Тема 2.6.	З1, З2,З3 У1-У5	ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 18 Установка и настройка Traffic monitor	2

№ раздела, темы	Освоение умений в процессе занятия	Формируемые ОК и ПК	Тема практического занятия	Кол-во часов
		ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 19 Установка и настройка Device monitor	2
		ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 20 Установка клиента Device monitor	2
		ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 21 Установка и настройка Crawler	2
	З1, З2,З3 У1-У5	ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 22 Создание правил и проверка их работоспособности в Device monitor	2
		ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 23 Создание правил с использованием «белых» и «чёрных» списков в Device monitor	2
		ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 24 Работа с Задачами и Журналом в Device monitor	2
	З1, З2,З3 У1-У5	ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 25 Добавление ролей, редактирование ролей, удаление ролей в Traffic monitor	2
	З1, З2,З3 У1-У5	ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 26 Работа с терминами и списками в Traffic monitor	2
		ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 27 Работа с тегами и объектами в Traffic monitor	2

№ раздела, темы	Освоение умений в процессе занятия	Формируемые ОК и ПК	Тема практического занятия	Кол-во часов
		ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 28 Создание политик защиты данных в Traffic monitor	2
		ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 29 Создание политик защиты данных на агентах в Traffic monitor	1
		ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 30 Создание политик контроля персон в Traffic monitor	1
		ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 31 Создание политик с использованием правил передачи в Traffic monitor	1
		ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 32 Создание политик с использованием правил копирования в Traffic monitor	2
		ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 33 Создание политик с использованием правил хранения в Traffic monitor	2
		ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 34 Создание политик с использованием правил работы в приложениях в Traffic monitor	2
	З1, З2,З3 У1-У5	ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 35 Создание политик с использованием регулярных выражений в Traffic monitor	2
	З1, З2,З3 У1-У5	ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 36 Создание и изменение виджетов в Traffic Monitor	2
		ОК1-ОК11 ПК2.1-	Практическое занятие № 37 Создание и изменение отчётов в Traffic Monitor	2

№ раздела, темы	Освоение умений в процессе занятия	Формируемые ОК и ПК	Тема практического занятия	Кол-во часов
		ПК2.6		
Тема 2.7	З1, З2,З3 У1-У5	ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 38 Работа с требованиями и рекомендациями по технической защите конфиденциальной информации	1
		ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 39 Работа с нормативно-правовой документацией, регламентирующей порядок проведения аттестации объектов информатизации	1
Тема 2.8	З1, З2,З3 У1-У5	ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 40 Развёртывание защищённой сети ViPNet. Учет отказов в работе средств вычислительной техники.	2
		ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 41 Создание структуры защищённой сети ViPNet	2
		ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 42 Создание защищённой сети ViPNet	2
		ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 43 Развёртывание рабочего места помощника главного администратора защищённой сети ViPNet	2
	З1, З2,З3 У1-У5	ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 44 Модификация защищённой сети ViPNet	2
		ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 45 Компрометация ключей в защищённой сети ViPNet	2
		ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 46 Настройка политик безопасности в VipNet Policy Manager	2
		ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 47 Организация межсетевого взаимодействия	2

№ раздела, темы	Освоение умений в процессе занятия	Формируемые ОК и ПК	Тема практического занятия	Кол-во часов
		ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 48 Модификация межсетевого взаимодействия в защищённой сети ViPNet	2
Тема 2.9	З1, З2,З3 У1-У5	ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 49 Установка openssl в centos	2
		ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 50 Создание самоподписанного сертификата SSL	2
	З1, З2,З3 У1-У5	ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 51 Заполнение анкеты для сертификата	2
		ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 52 Применение сертификата	2
	З1, З2,З3 У1-У5	ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 53 Перемещение ssl-сертификата с сервера windows на сервер, отличный от window	
	З1, З2,З3 У1-У5	ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 54 Установка Nginx для последующей настройки прокси-сервера	2
		ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 55 Настройка прокси-сервера с помощью Nginx	2
		ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 56 Настройка правильной работы ssl при использовании Nginx	2
Тема 2.10	З1, З2,З3 У1-У5	ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 57 Установка серверной версии Ubuntu	2

№ раздела, темы	Освоение умений в процессе занятия	Формируемые ОК и ПК	Тема практического занятия	Кол-во часов
		ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 58 Установка Samba	2
		ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 59 Настройка Samba	2
		ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 60 Конфигурирование BIND9 на контроллере домена Ubuntu Server	2
	З1, З2,З3 У1-У5	ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 61 Установка системы обнаружения и предотвращения вторжения Snort	2
		ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 62 Настройка системы обнаружения и предотвращения вторжения Snort	2
		ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 63 Настройка записи предупреждений о вторжениях в базу данных	2
		ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 64 Установка пакетов для веб-интерфейса IDS Snort	2
		ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 65 Настройка веб-интерфейса для системы обнаружения и предотвращения вторжения Snort	1
		ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 66 Применение правил для IDS Snort	2
		ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 67 Проверка настроенных правил в IDS Snort с помощью сканирования портов	2

2. Описание порядка выполнения практических работ

2.1. Практическая работа № 1 «Сравнительный анализ продуктов SIEM»

Задание:

С помощью ресурсов Интернета составить сравнительную таблицу по продуктам SIEM.

Требования:

— выбрать три компании;

— функциональность продукта;

— отказоустойчивость и резервирование продукта;

— защищённость продукта;

— техническая поддержка и обновление продукта;

— лицензирование продукта.

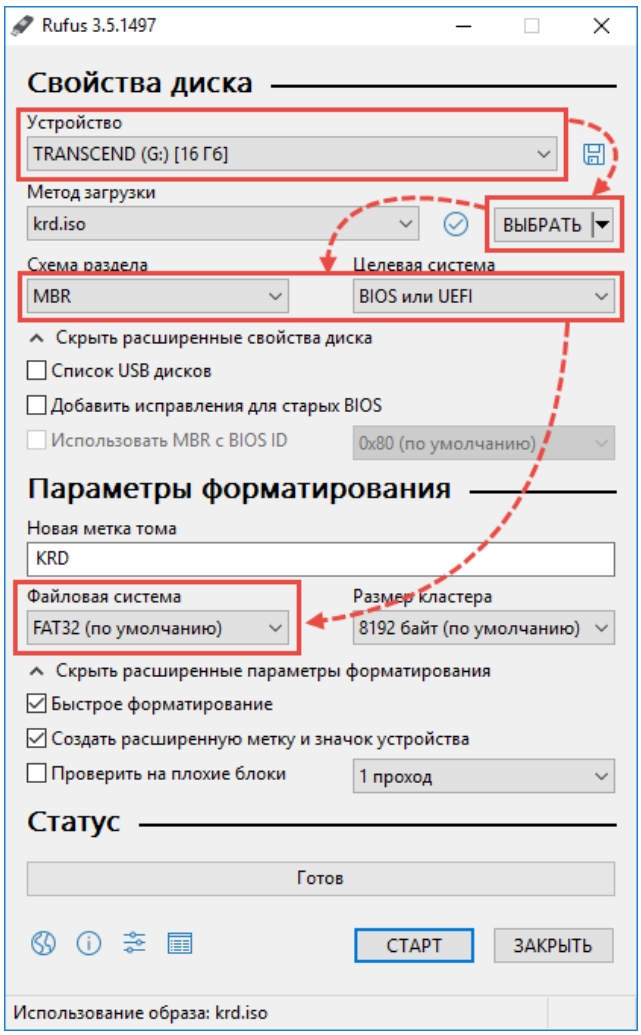
Сформируйте и оформите таблицу.

2.2. Практическая работа № 2 «Создание загрузочной флешки с антивирусной программой для быстрой проверки»

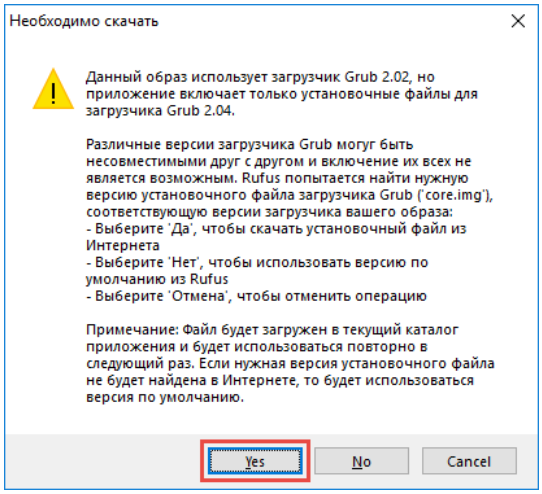
Задание:

Для задания вам нужен USB-носитель больше 1 ГБ

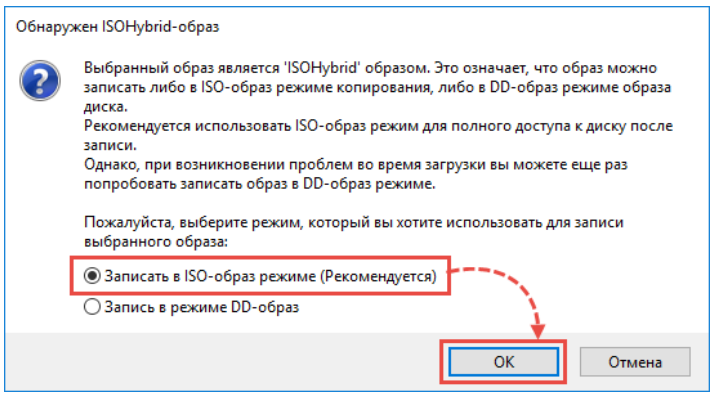
1. Скачать бесплатную программу Kaspersky Rescue Disk с официального сайта kaspersky.ru
2. Скачать бесплатную программу для записи образа в ISO-режиме Rufus
3. Откройте Rufus.
4. Выберите USB-носитель.
5. Нажмите Выбрать и выберите образ Kaspersky Rescue Disk.
6. Выберите схему раздела MBR и целевую систему BIOS или UEFI.
7. Выберите файловую систему FAT32.



6. Нажмите Старт.
7. Нажмите Yes.



8. Выберите Записать в ISO-образ режиме (Рекомендуется) и нажмите ОК.

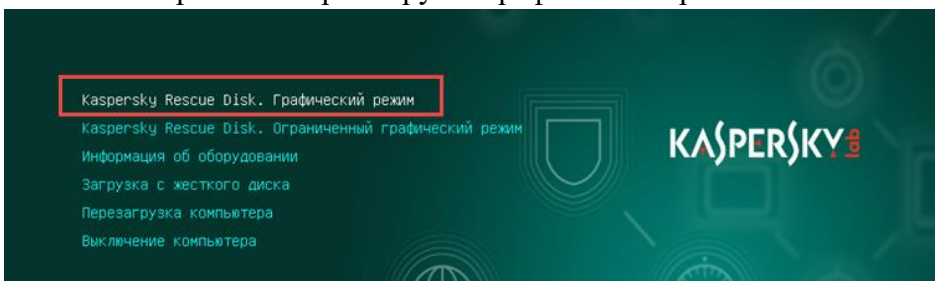


9. Сделайте скриншот во время записи образа и вставьте его в отчёт.

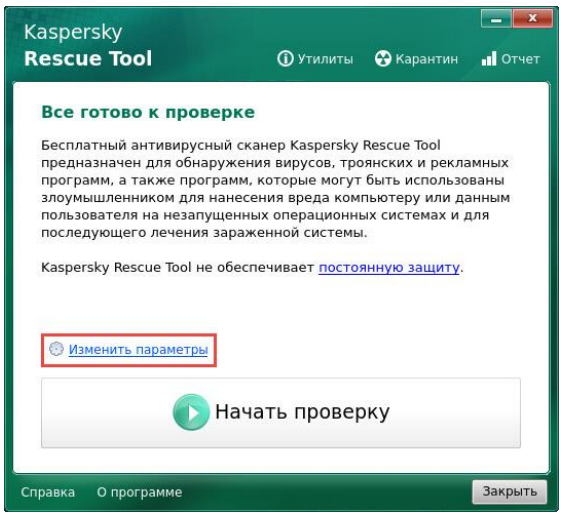
Загрузочная флешка с антивирусной программой готова.

10. Подключите USB-носитель к компьютеру.
11. Настройте компьютер для загрузки с USB-носителя.
12. Загрузите компьютер с Kaspersky Rescue Disk:
    - ✓ Нажмите на клавишу Esc, когда на экране появится сообщение с текстом «Press ESC to load Kaspersky Rescue Disk».
    - ✓ Выберите язык графического интерфейса и нажмите на клавишу Enter.

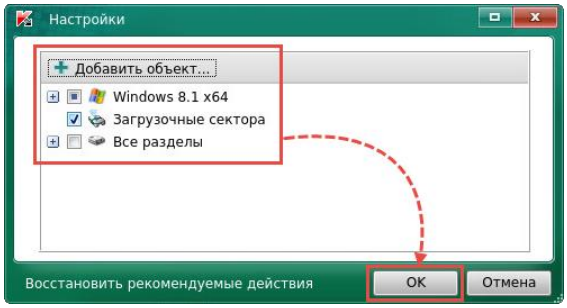
    - ✓ Выберите режим загрузки:
        - Kaspersky Rescue Disk. Графический режим — загружает графическую подсистему. Мы рекомендуем использовать этот режим.
        - Kaspersky Rescue Disk. Ограниченный графический режим — загружает графическую подсистему в упрощенном виде. Используйте, если возникли проблемы при загрузке графического режима.



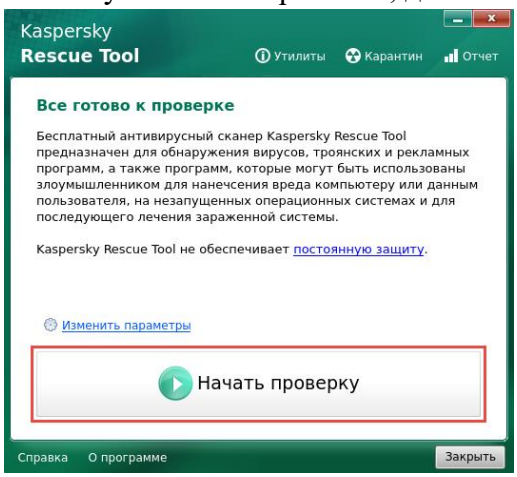
    - ✓ Нажмите на клавишу Enter и дождитесь загрузки системы.
13. Запустите проверку компьютера:
14. Примите Лицензионное соглашение.
15. При необходимости нажмите Изменить параметры.



16. Настройте параметры проверки и нажмите OK.



17. Запустите сканирование, для этого нажмите Начать проверку.



Проверка компьютера будет запущена.

Вставьте скриншот (фотографию) при проверке компьютера

2.3. Практическая работа № 3 «Установка серверной версии Windows»

Задание:

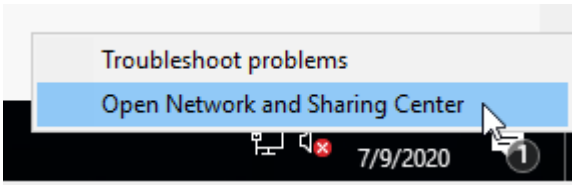
1. С помощью VirtualBox создайте новую виртуальную машину с названием WinServer16_фамилии. Для виртуальной машины выберете следующие параметры:ОЗУ 4048 Гб, диск vdi на 50 Гб, папка сохранения на диск D. Сохранить. вставить скриншот с созданной виртуальной машиной в VirtualBox.
2. Запустить созданную машину, выбрать iso-файл с Windows Server 2016. Запустить установку.
   Язык оставить English.
   установку выбрать Standard
   Тип установки выбрать Custom
   согласится с установкой на диск 0 в 50.0 GB
   Password придумать надёжный и записать его в отчёт.
   Вставить скриншот с рабочим столом установленной операционной системой Windows Server 2016.
3. С помощью ресурсов Интернета заполнить таблицу сравнительной характеристики по серверным версиям операционной системы Windows:

	Windows Sever 2016	Windows Sever 2019
Год выпуска первой версии		
Последняя версия		
Интерфейс администратора (вставить фото)		
Возможности Azure		
Реализованная безопасность		
Минимальные требования для установки		
Стоимость версий Standard		

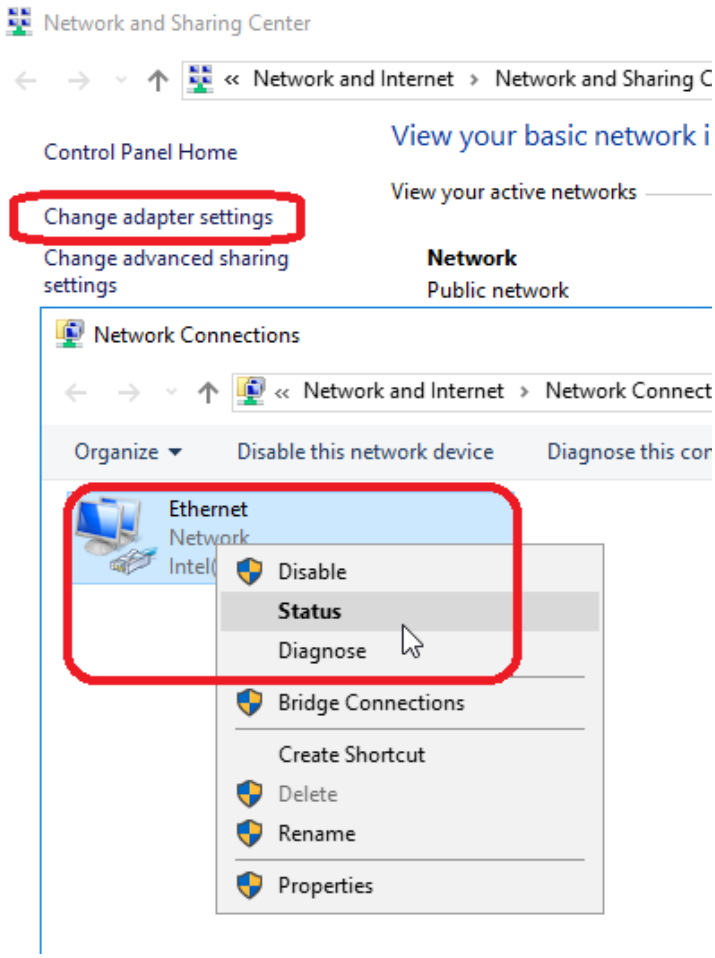
2.4. Практическая работа № 4 «Установка домена Active Directory»

Задание 1:

1. Присвоить статический IP-адрес компьютеру с установленным Windows Server. Для этого в системном трее выбрать Открыть Центр управления сетями и общим доступом:



Далее выбрать адаптер → Состояние → Свойства:

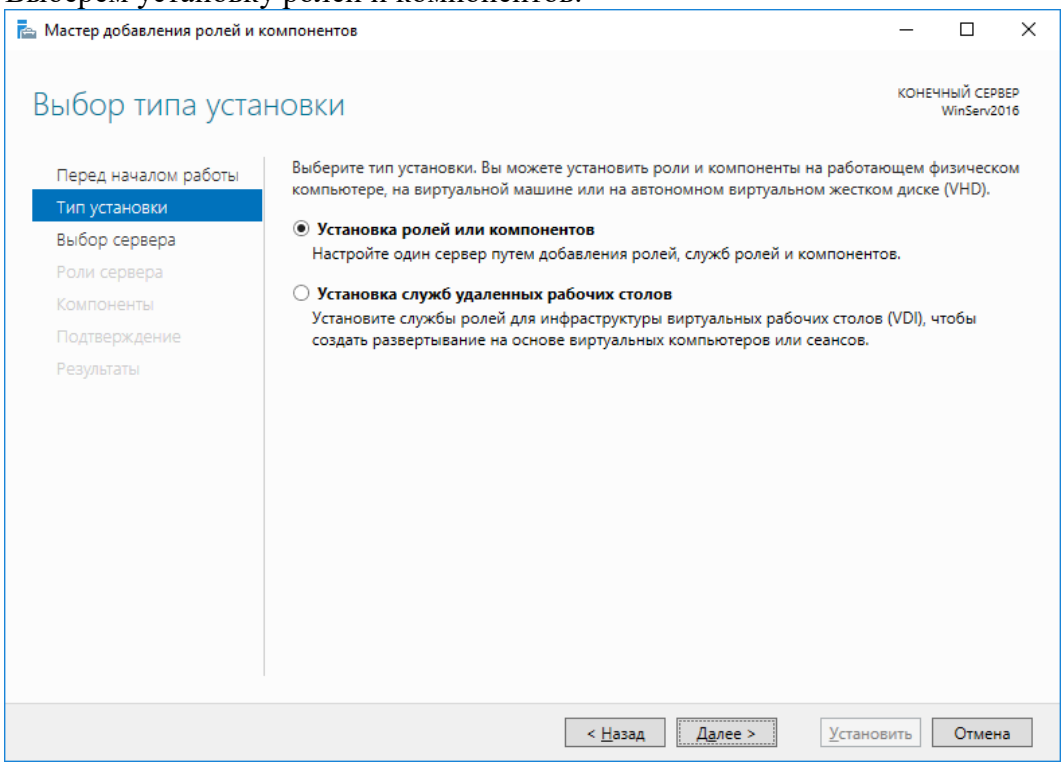


В открывшемся окне выбрать “Протокол Интернета версии 4” и снова кликнуть на “Свойства”.

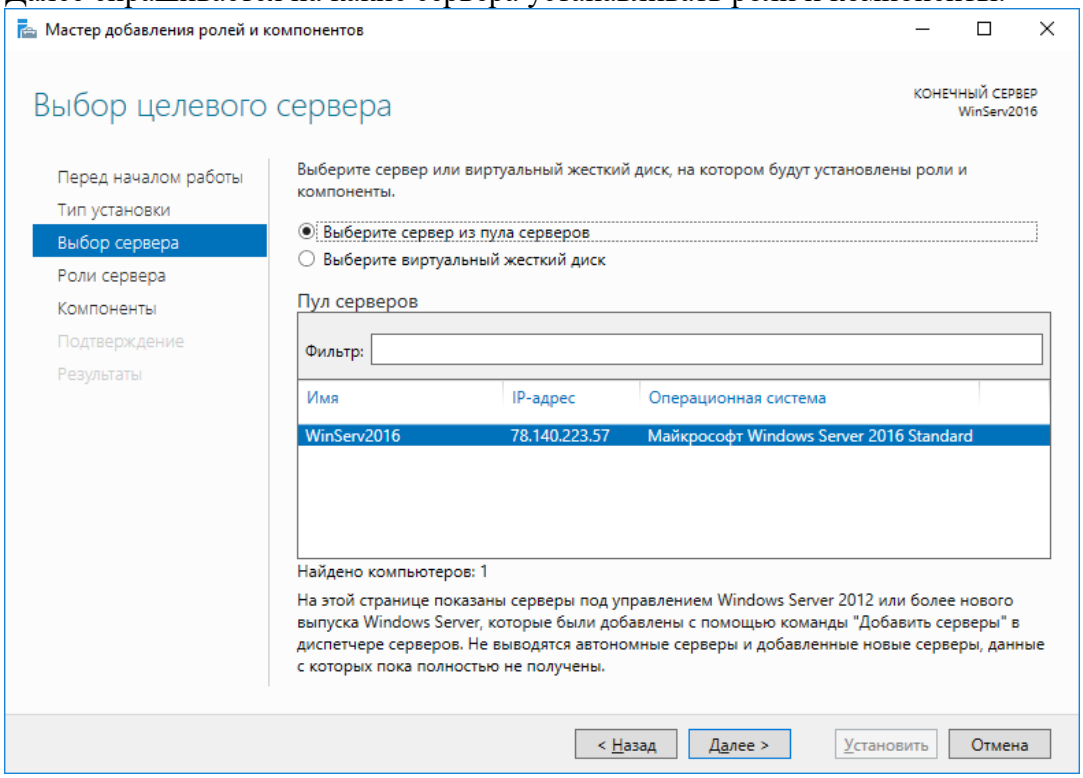
Заполнить поля следующим образом: IP-адрес – 192.168.1.5. DNS – 127.0.0.1.
Нажать на кнопку “ОК”.
Вставьте скриншот с вашими результатами.

2. Далее переходим в Диспетчер серверов, выбираем добавить роли и компоненты.

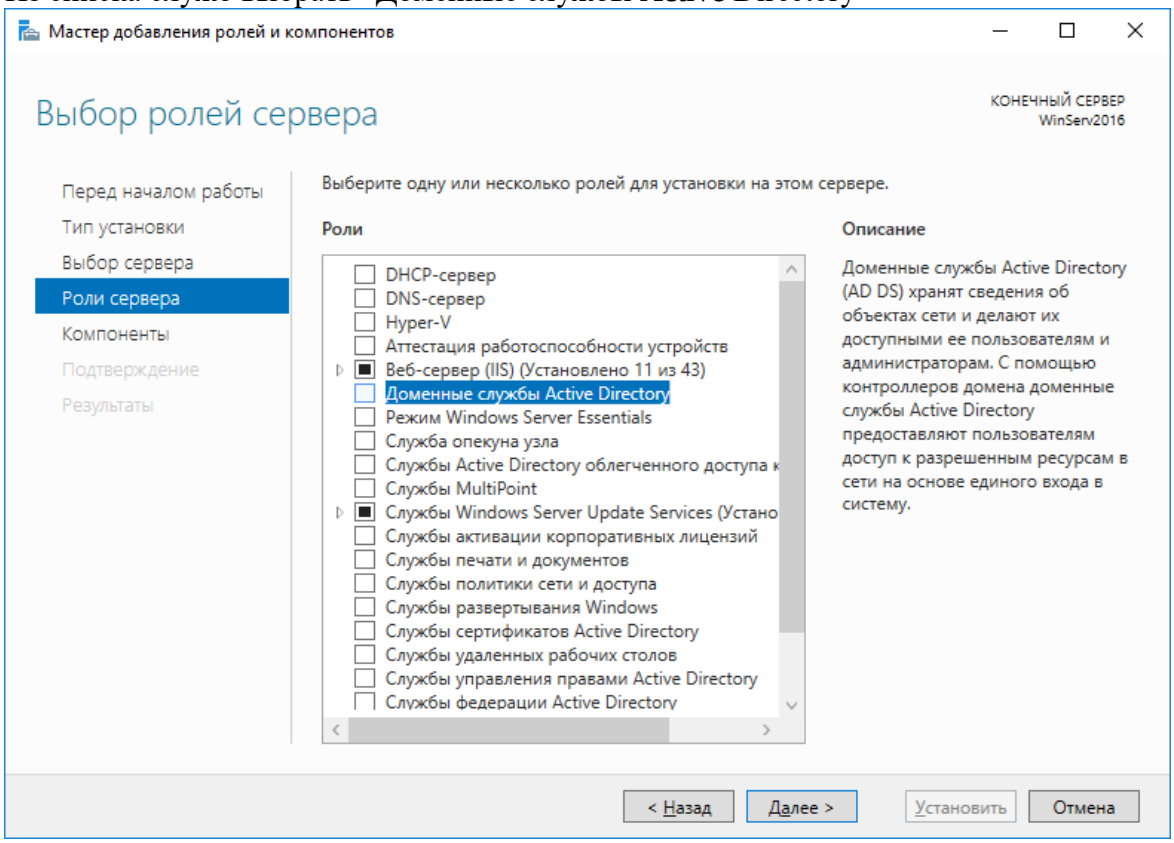
Выберем установку ролей и компонентов.



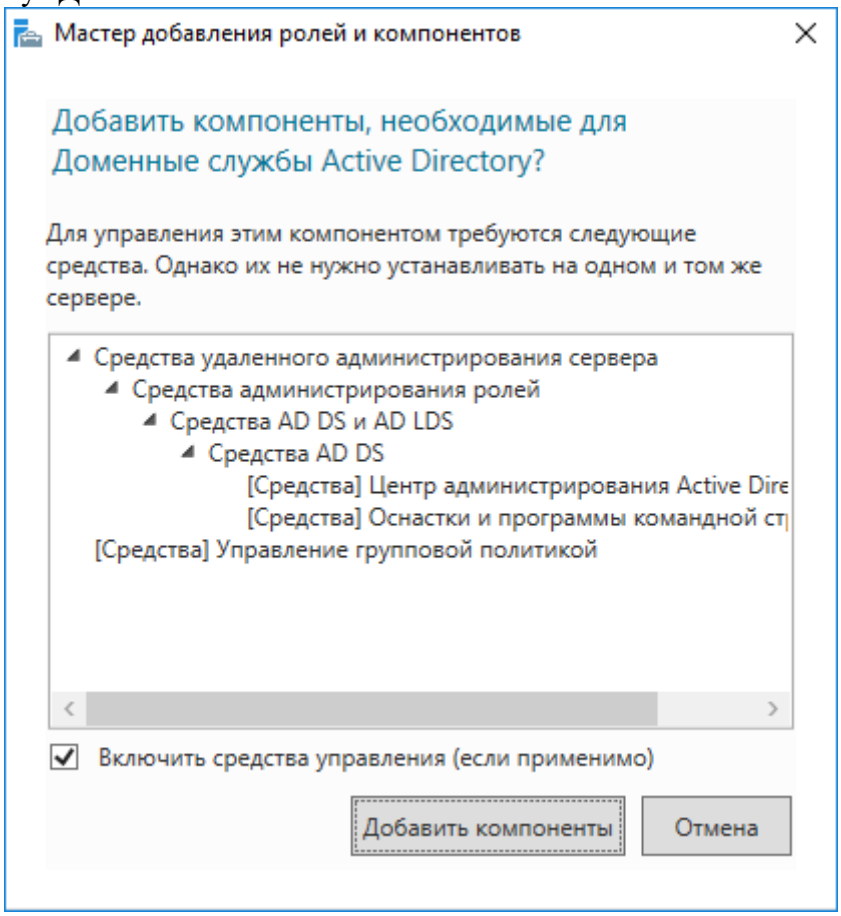
Далее спрашивается на какие сервера устанавливать роли и компоненты.



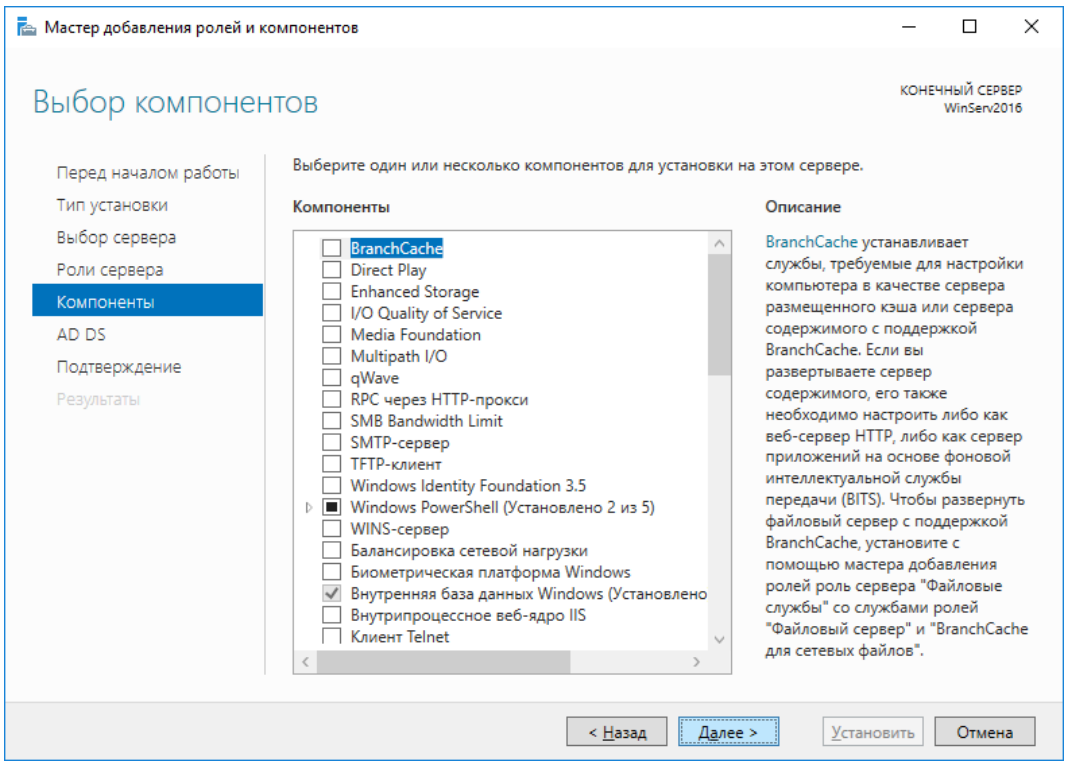
Из списка служб выбрать “Доменные службы Active Directory”



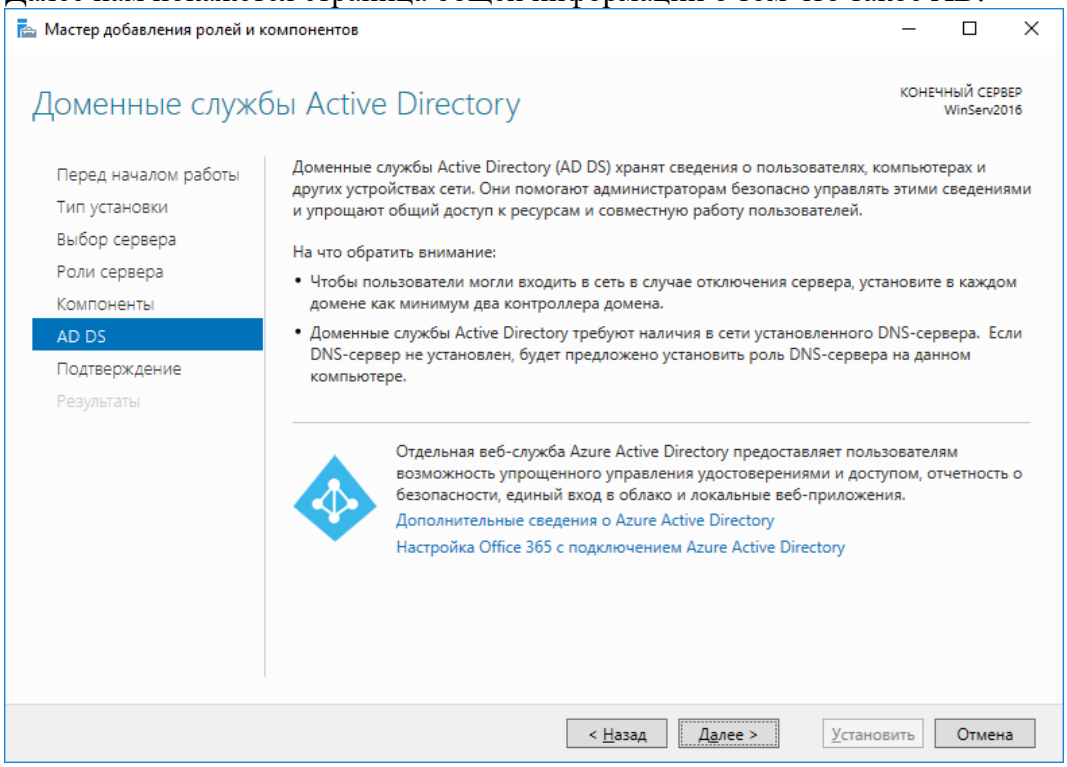
Система также попросит установить дополнительные компоненты. Согласимся, нажав кнопку “Добавить компоненты”.



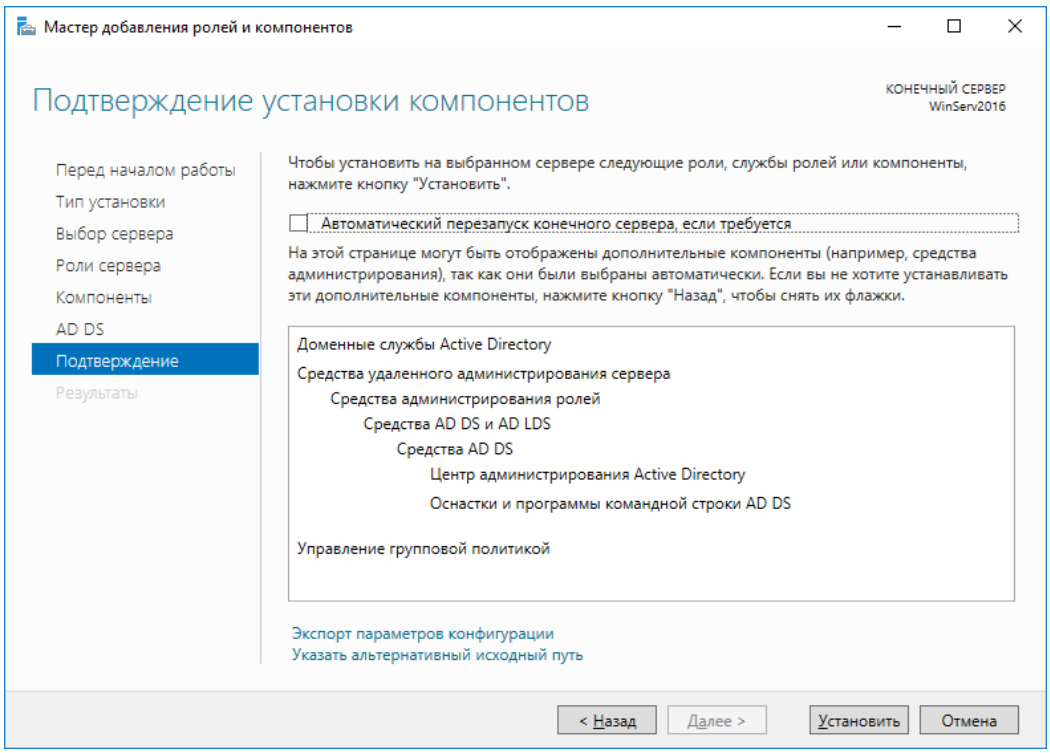
Следующий шаг пропускаем.



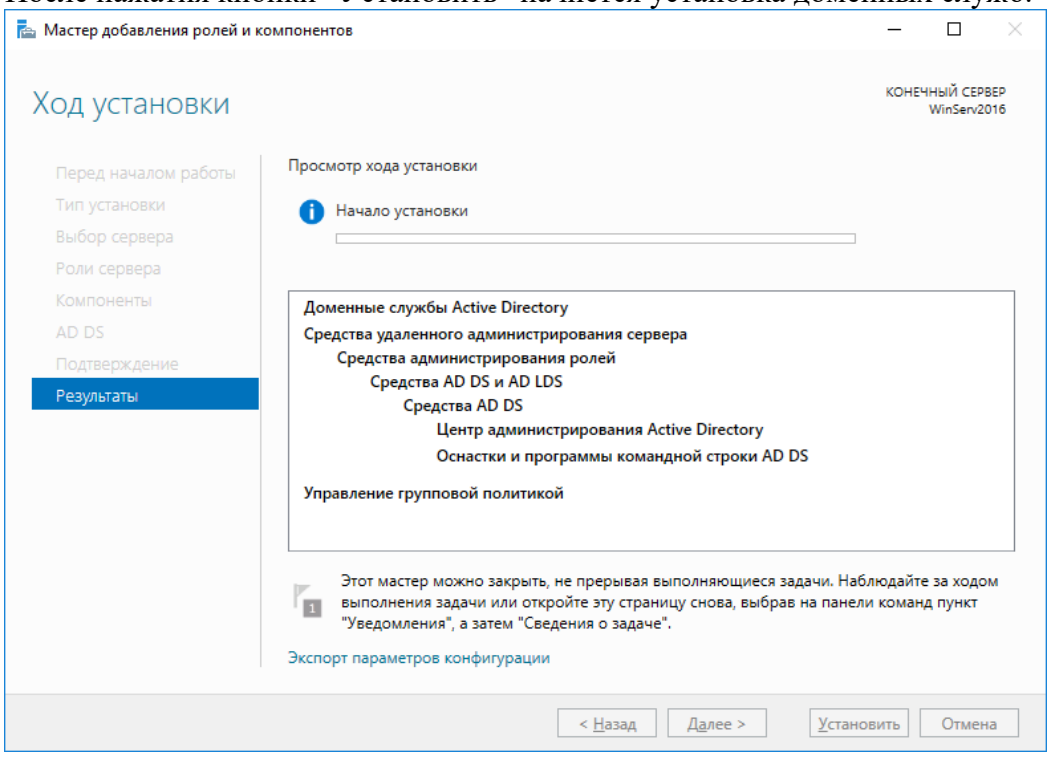
Далее нам покажется страница общей информации о том что такое AD.



После нажатия кнопки “Далее” выведется последняя страница где можно включить автоматическую перезагрузку сервера после установки.

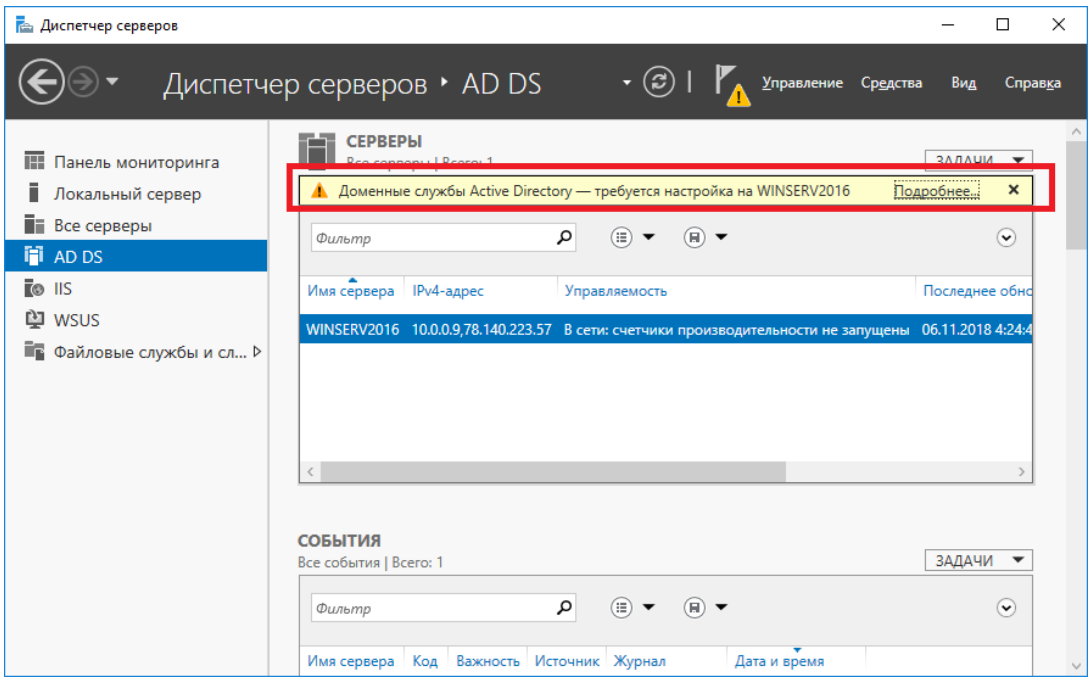


После нажатия кнопки “Установить” начнется установка доменных служб.

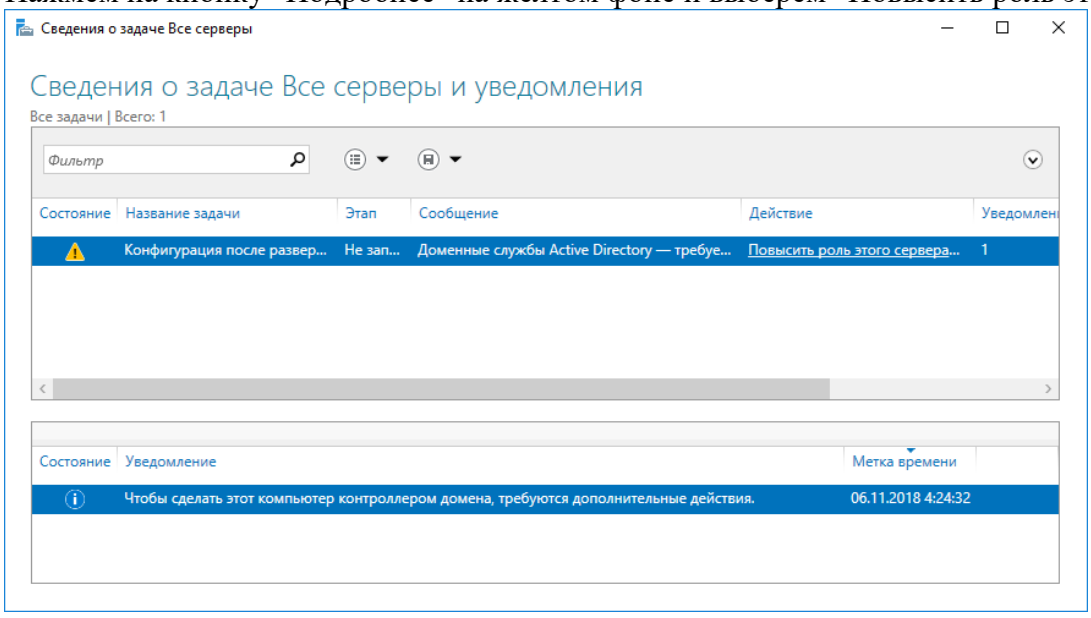


Вставьте один скриншот во время установки доменных служб.

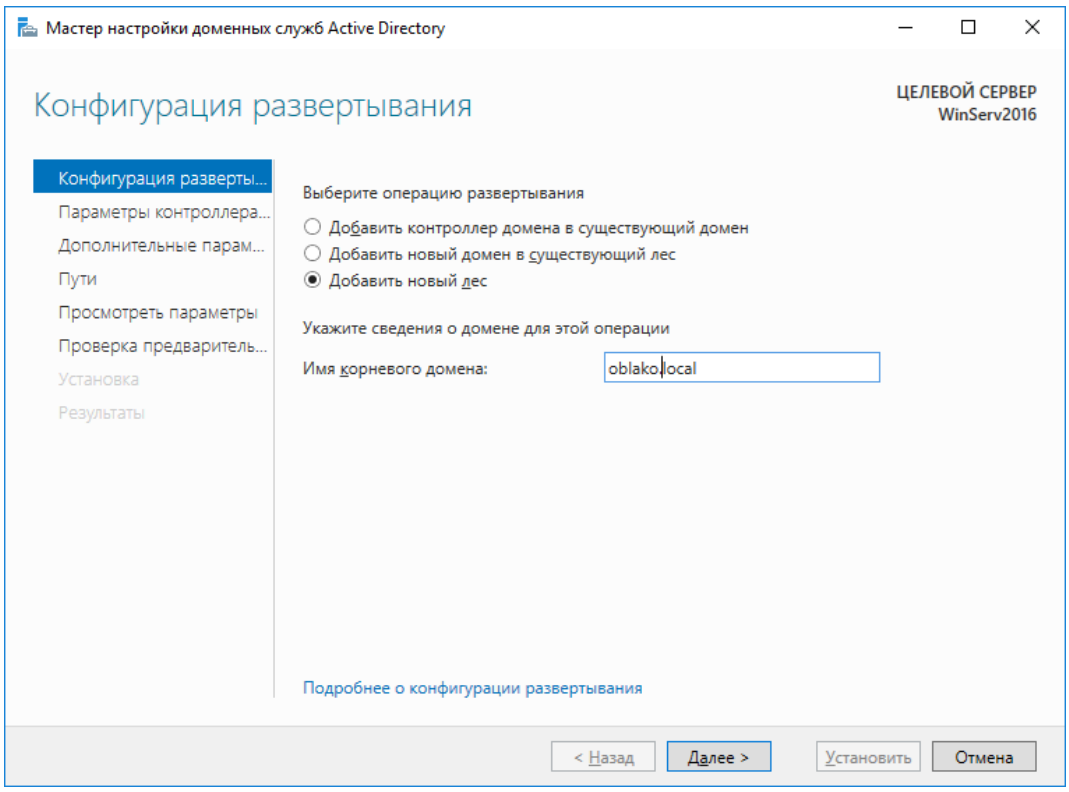
Теперь можно приступать к развертыванию AD. Для этого вернемся в диспетчер сервера и перейдем на вкладку AD DS (Active Directory Domain Service - Доменные Службы Active Directory). На ней нас сразу предупредят, что требуется настройка служб AD.



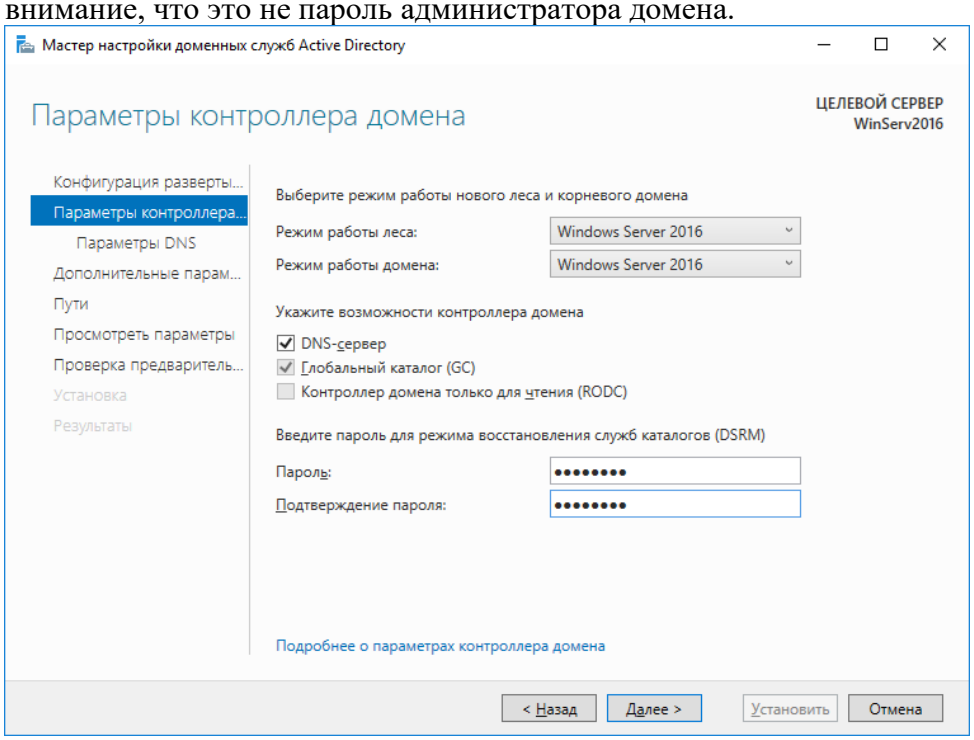
Нажмем на кнопку “Подробнее” на желтом фоне и выберем “Повысить роль этого сервера”.



Запустится мастер настройки AD. На первом шаге необходимо определить существует ли у нас инфраструктура AD или Мы будем создавать ее с нуля.
Доменом называется основная административная единица в сетевой инфраструктуре предприятия, в которую входят все сетевые объекты, такие как пользователи, компьютеры, принтеры, общие ресурсы и т.д.
Несколько доменов, связанных между собой, называется лесом. Связи между доменами называются отношениями доверия или иерархией.
Мы будем создавать новый лес, так как мы делаем новую инфраструктуру.
Также необходимо ввести имя домена. Не желательно задавать имя внешнего домена. Для внутренних доменов рекомендуется зона local.

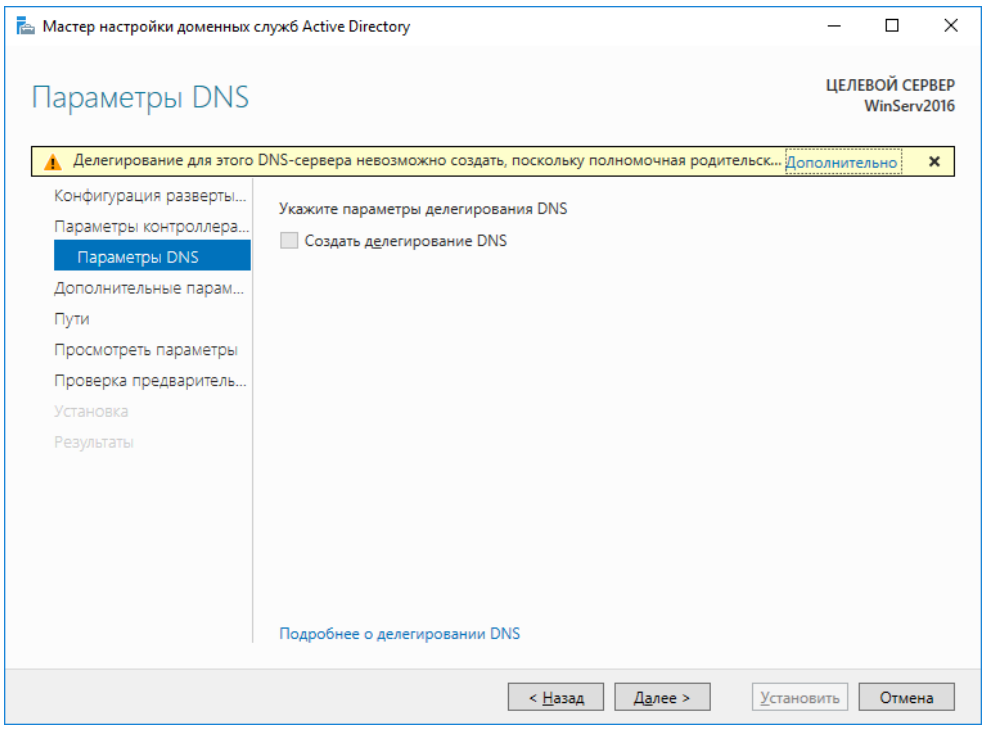


Следующим шагом необходимо выбрать режим работы домена и леса. Чем выше уровень тем больше возможностей поддерживается, но и тем более новая клиентская ОС должна использоваться на компьютерах. Также рекомендуется указать что данный сервер будет являться сервером DNS. Обязательно введите пароль для службы восстановления AD. обратите внимание, что это не пароль администратора домена.

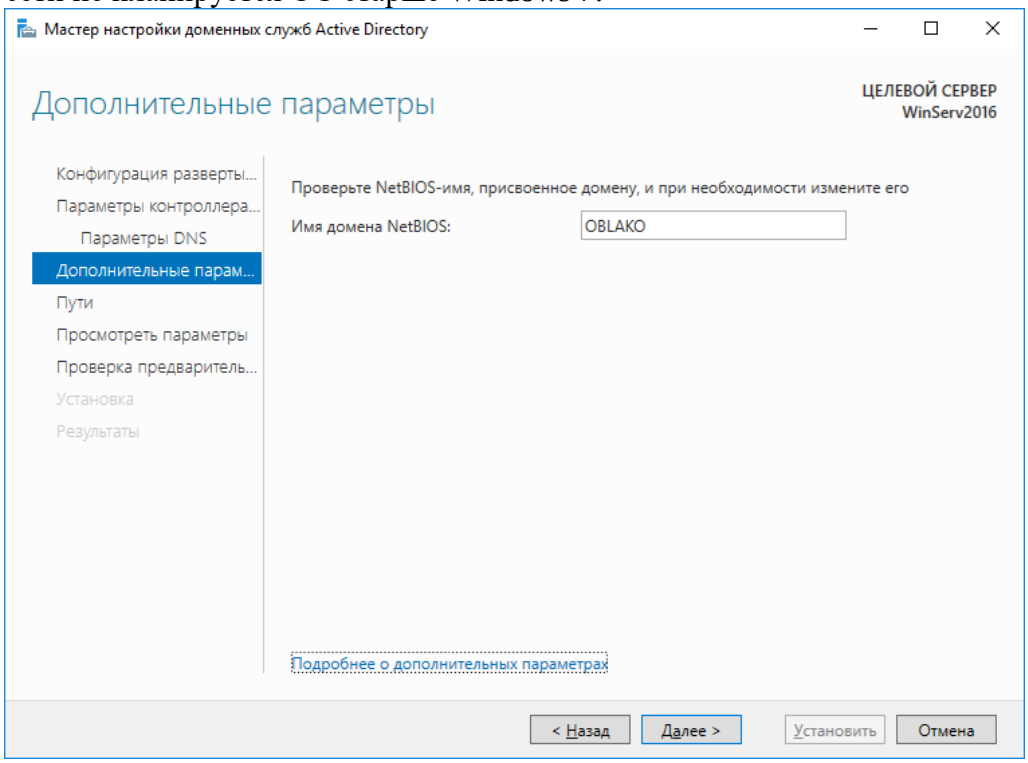


Придумайте новый пароль и впишите его ниже

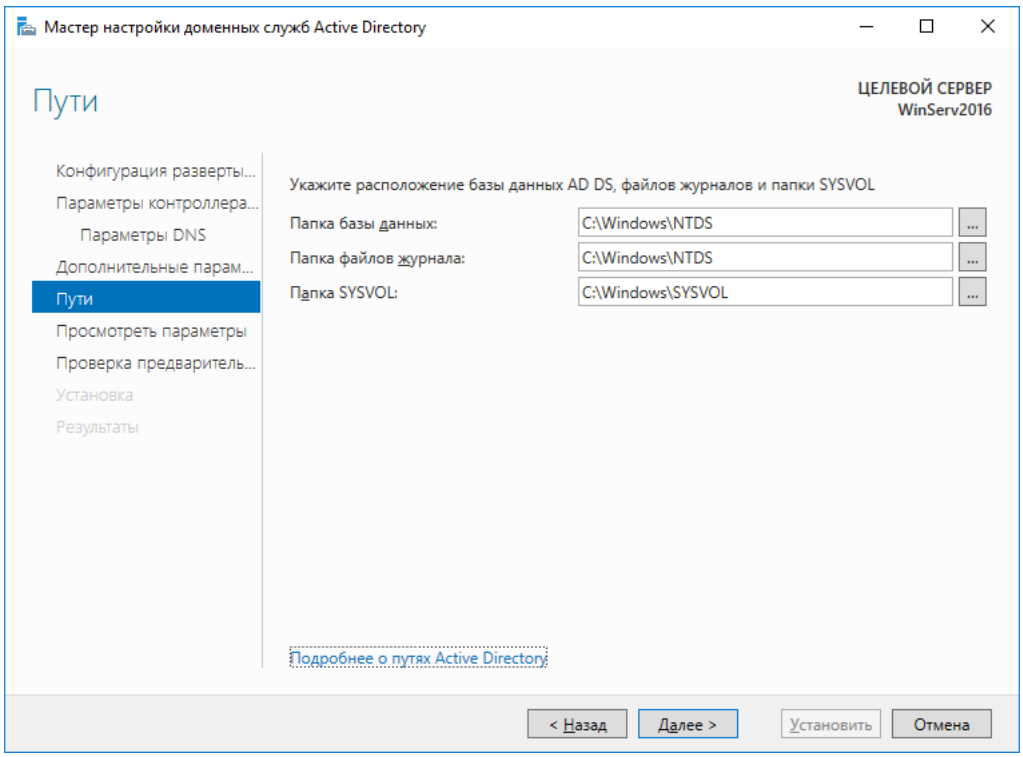
После нажатия “Далее” перейдем к настройке DNS. Этот шаг можно пропустить.



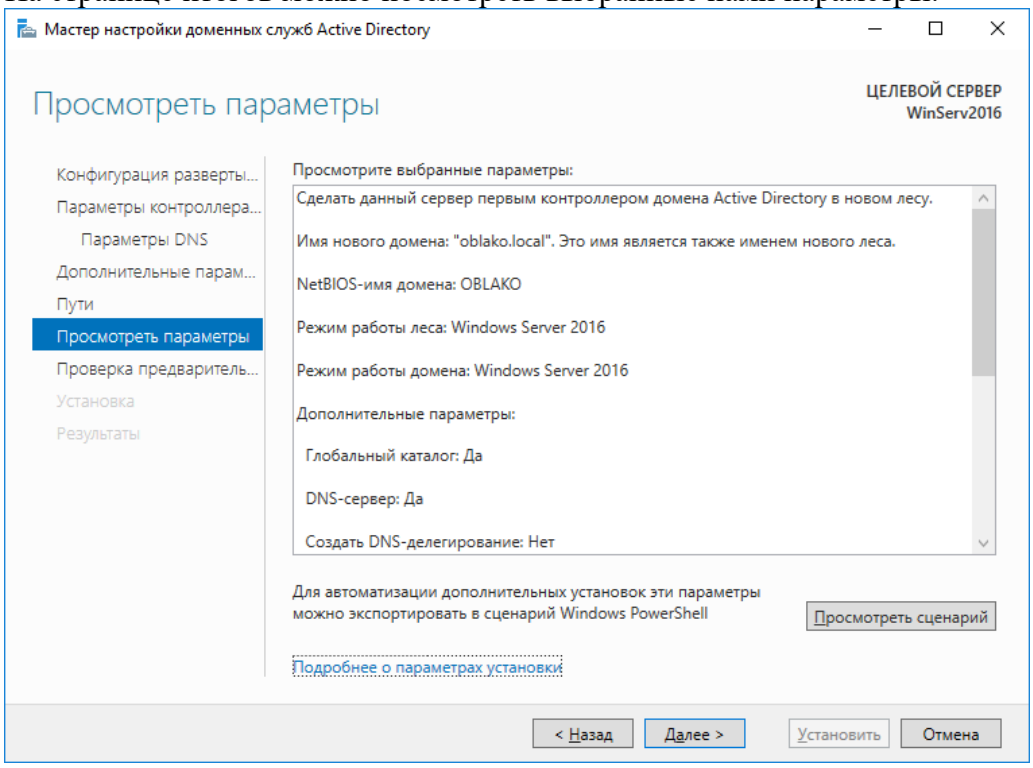
Проверим NetBIOS имя (используется для старых ОС). тоже можно пропустить, если у вас в сети не планируется ОС старше Windows 7.



Указываем расположение системных папок AD. Оставим назначение по умолчанию.

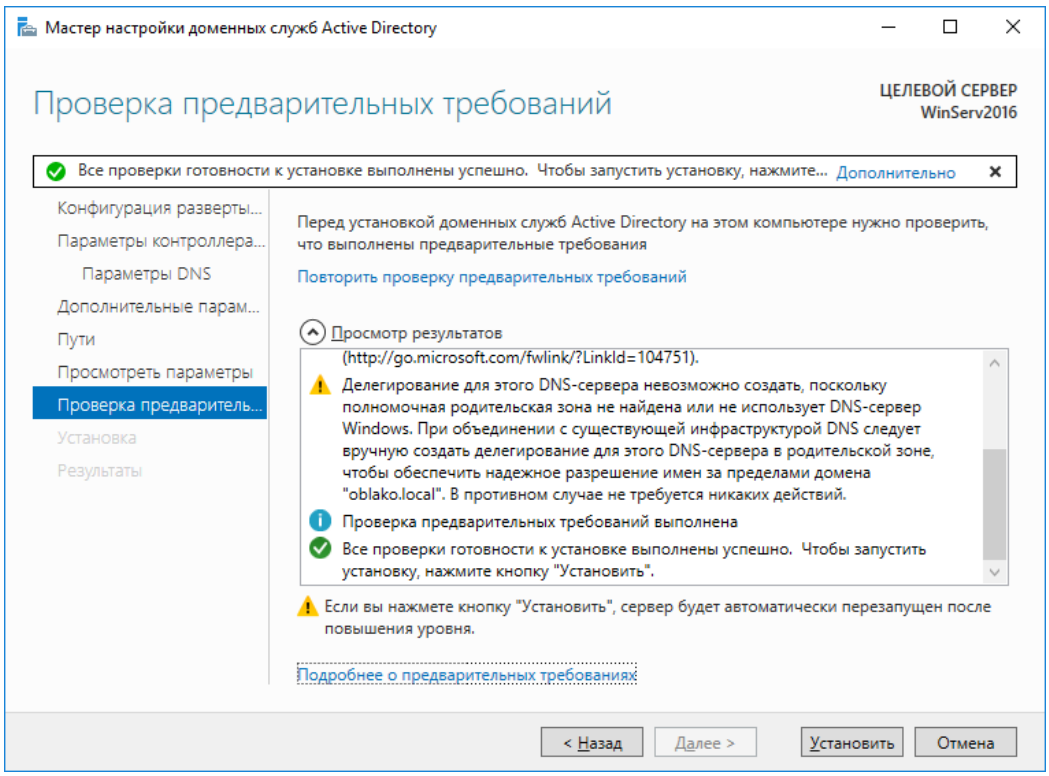


На странице итогов можно посмотреть выбранные нами параметры.

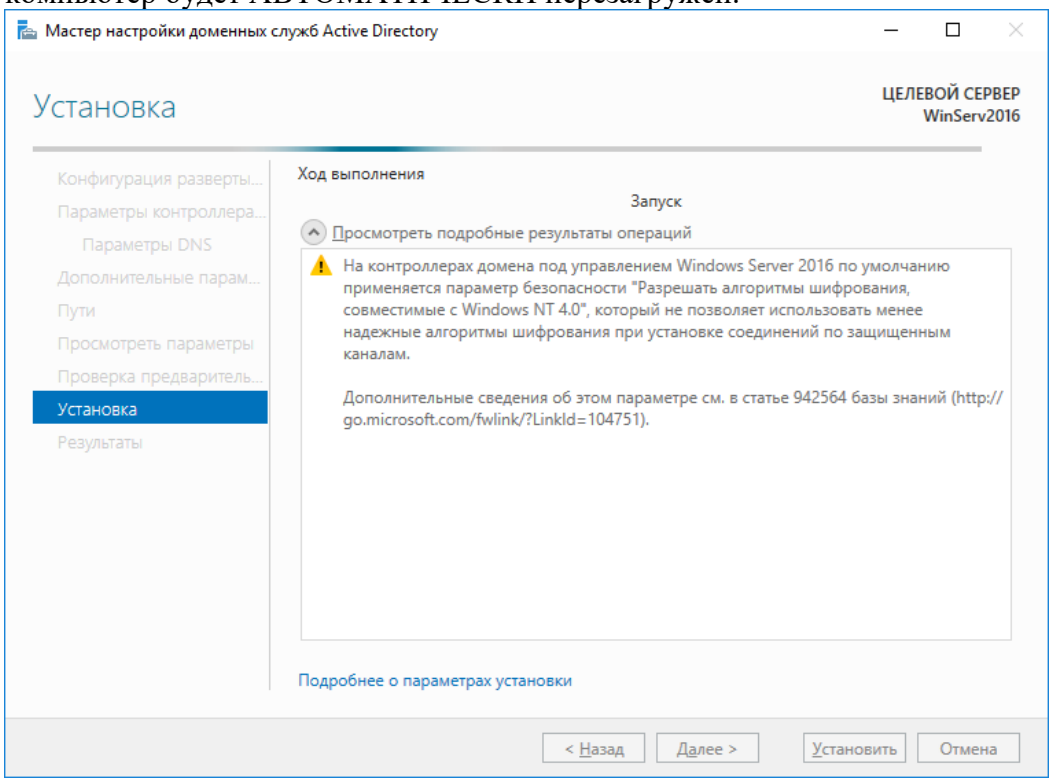


Вставьте скриншот с окном выбранных параметров.

После нажатия “Далее” запуститься проверка соответствия настройкам. После проведения анализа она покажет ошибки, которые нужно исправить или предупреждения, которые в, большинстве случаев, можно игнорировать.



После нажатия кнопки “Установить” будут произведены действия по развертыванию AD и компьютер будет АВТОМАТИЧЕСКИ перезагружен.



После перезагрузки сделайте скриншоты, доказывающие, что у вас на сервере подняты роли AD и DNS.

Задание 2:

С помощью ресурсов Интернета ответить на следующие вопросы:
1. Что значит возможность установки — Контроллер домена только для чтения (RODC) ?

2. Зачем вместе с AD принято поднимать сразу DNS-сервер?

3. Есть ли отличия поднятия AD на Windows server 2019 от 2016?

4. Что такое делегирование DNS?

5. Для чего нужно короткое имя NetBIOS при установке AD?

Ответы:

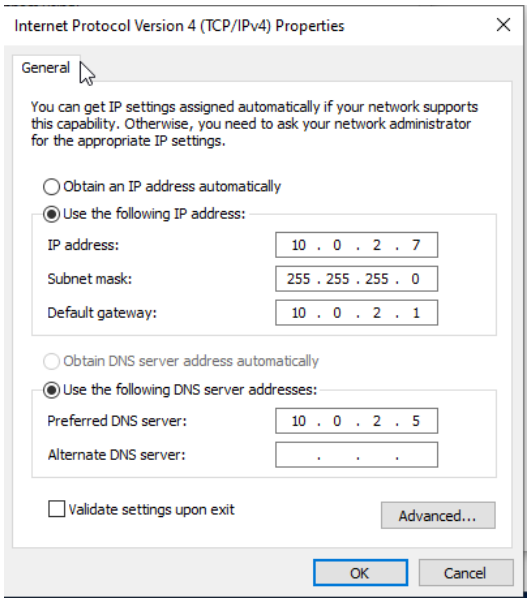
2.5. Практическая работа № 5 «Создание и внесение пользователей и компьютеров в домен»

Задание 1:

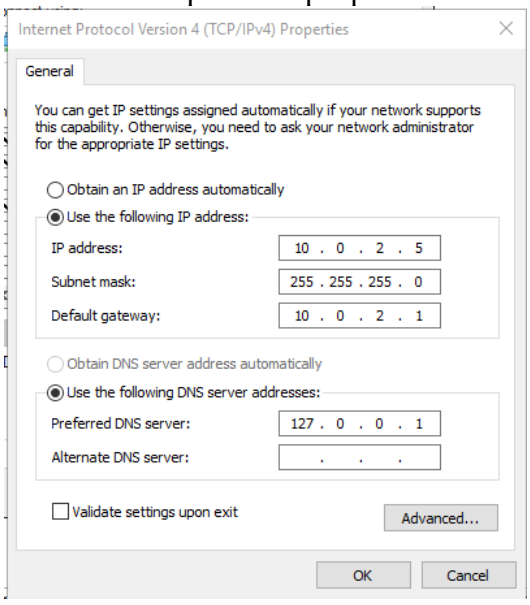
1. Запустить виртуальную машину с сервером и компьютер, который нужно добавить в домен.

2. Изменить сетевые настройки в соответствии со следующими параметрами:

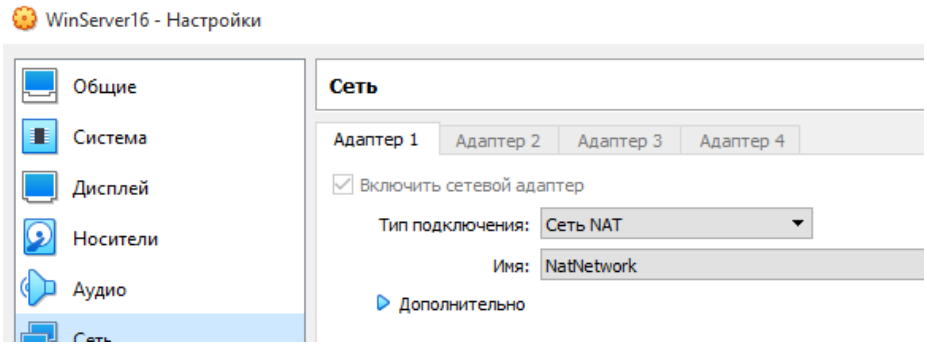
Сетевые настройки рабочей станции:



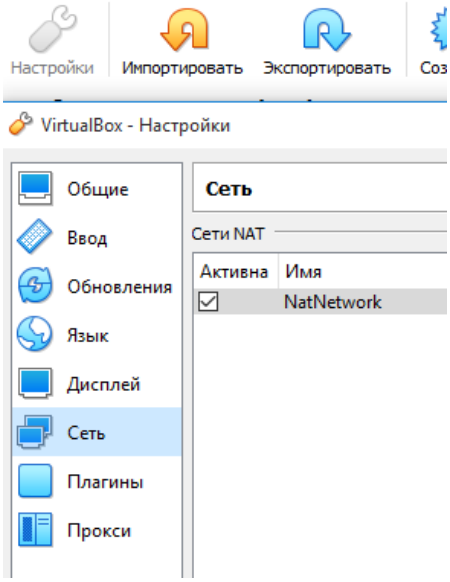
Сетевые настройки сервера:



Настройки VirtualBox для сервера и рабочей станции:



Общие настройки для сети VirtualBox:



На рабочей станции отключить Firewall.

Вставить информацию с ping с сервера на рабочую станцию и с рабочей станции на сервер.

3. Для добавления рабочей станции в домен необходимо сделать следующее:

Settings → Accounts → Access work or school → Connect → Join this device to a local Active Directory domain. Далее пишем название домена, затем Администратора домена, его пароль. Далее аккаунт и тип Администратор.

Перезагрузить рабочую станцию.

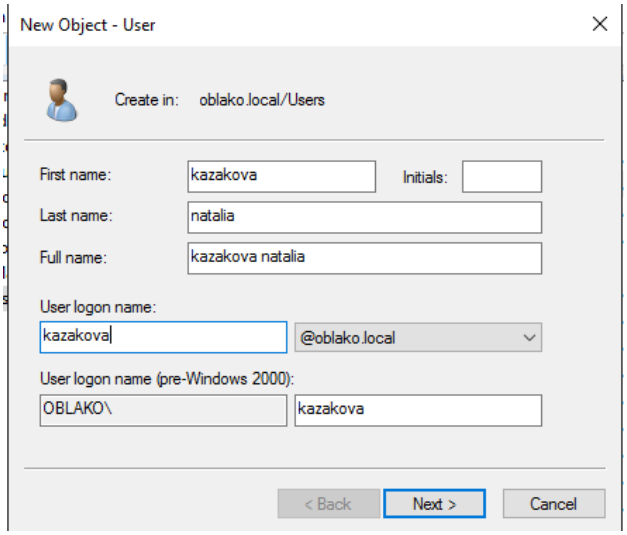
Вставить скриншот стартового окна рабочей станции с информацией о домене.

4. Переходим к добавлению пользователей в домен. Для этого заходим на сервер.Для работы с пользователями и компьютерами в AD нужно открыть оснастку Active Directory – пользователи и компьютеры. Для этого необходимо в меню Пуск выбрать Администрирование и далее Active Directory – пользователи и компьютеры.

5. В появившейся оснастке нужно открыть ваш домен oblaco.local → Пользователи. Вам необходимо создать Новую группу глобальных пользователей. Создайте группы Бухгалтерия, Администрация, отдел IT, отдел ИБ, Инженеры, Менеджеры.

6. Далее создайте новых глобальных пользователей.

Пример:



Необходимо создать для Бухгалтерии 3 пользователя, для Администрации 6 пользователей, для отдела IT 5 пользователей, для отдела ИБ – 3 пользователя, для отдела Инженеры 5 пользователей, для отдела Менеджеры - 2 пользователя.

При создании пользователя запретить изменять пароли и поставить неограниченный срок на пароль.

После создания пользователя открыть его свойства. Добавить мобильный номер, должность.

Когда все пользователи созданы внести их в соответствующие группы пользователей.

Записать в виде таблицы всех созданных пользователей, их должности, пароли.

7. Под каждым созданным пользователем зайти на рабочую станцию и вставить скриншоты, подтверждающие заход в систему.

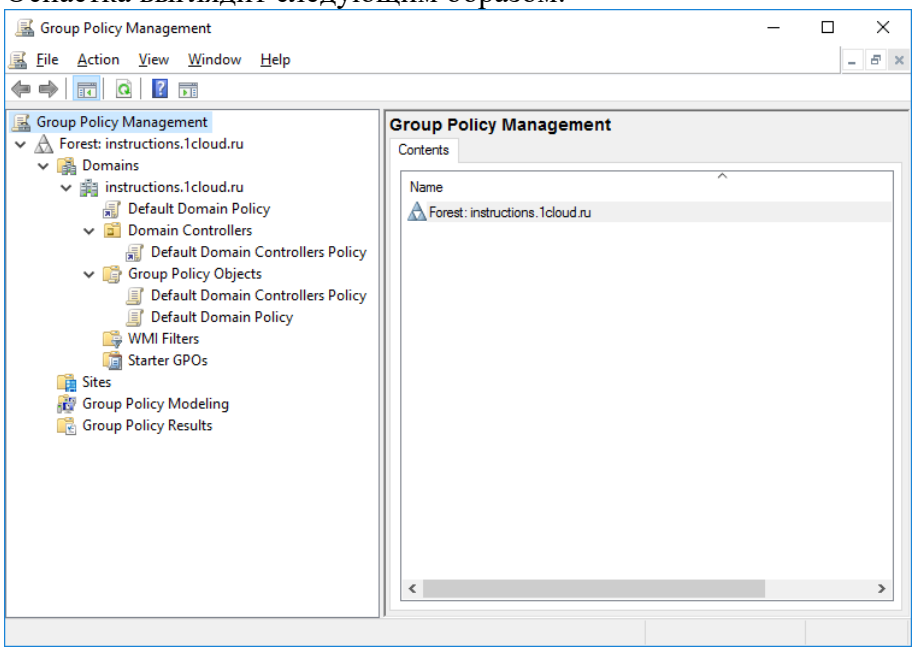
Задание 2:

Ответить на следующие вопросы:
Чем отличается внесение пользователей в домен от внесения компьютеров в домен?
Ответ:

2.6. Практическая работа № 6 «Создание и применение глобальных политик домена»

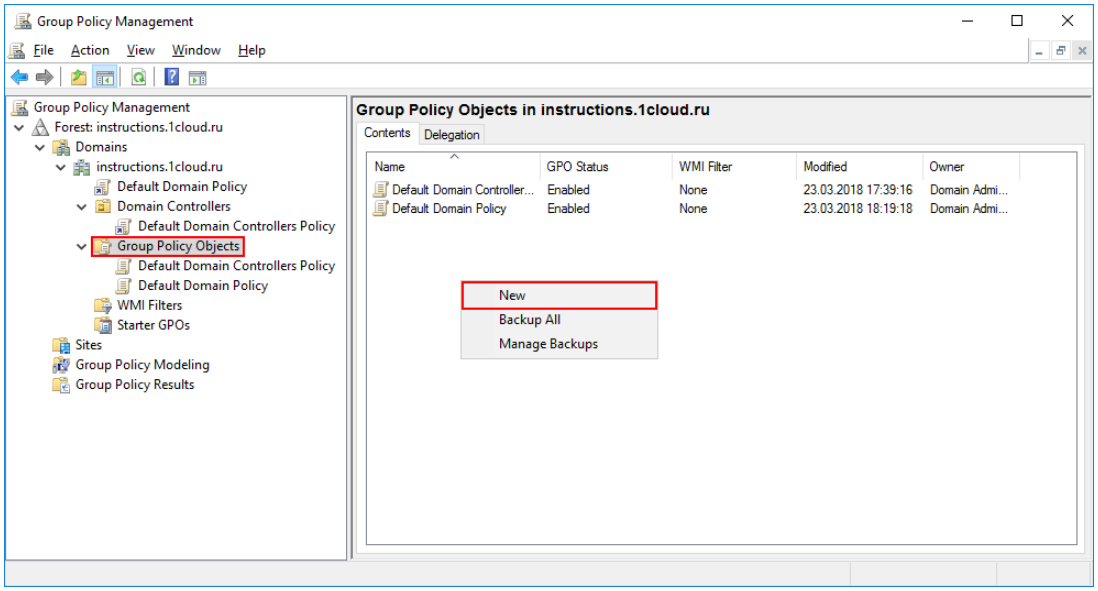
Задание 1:

Для создания политик необходимо запустить оснастку Group Policy Management. Оснастка выглядит следующим образом:

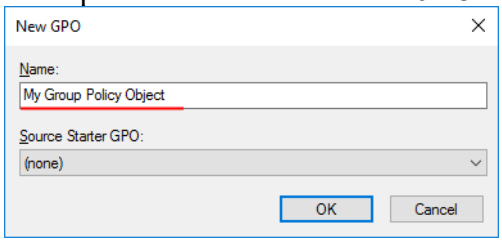


Создание объектов групповой политики

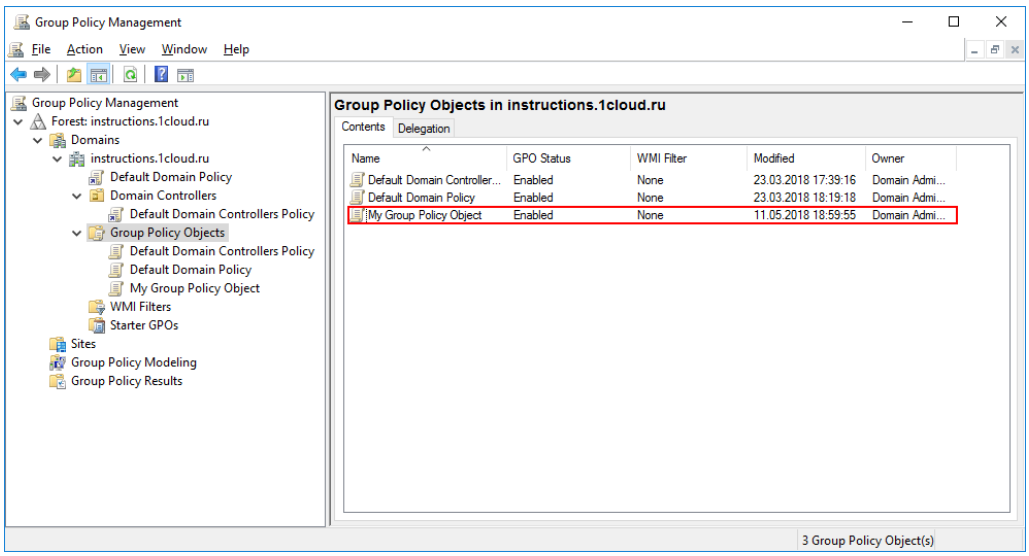
Для создания объекта групповой политики перейдите во вкладку Forest → Domains → Ваш домен → Group Policy Objects. С помощью правой кнопки мыши откройте меню и выберете New.



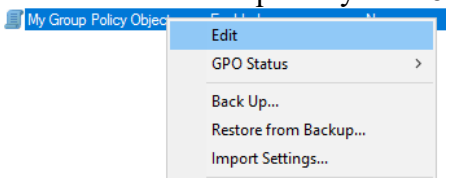
В открывшемся окне в поле Name введите удобное для вас имя групповой политики.



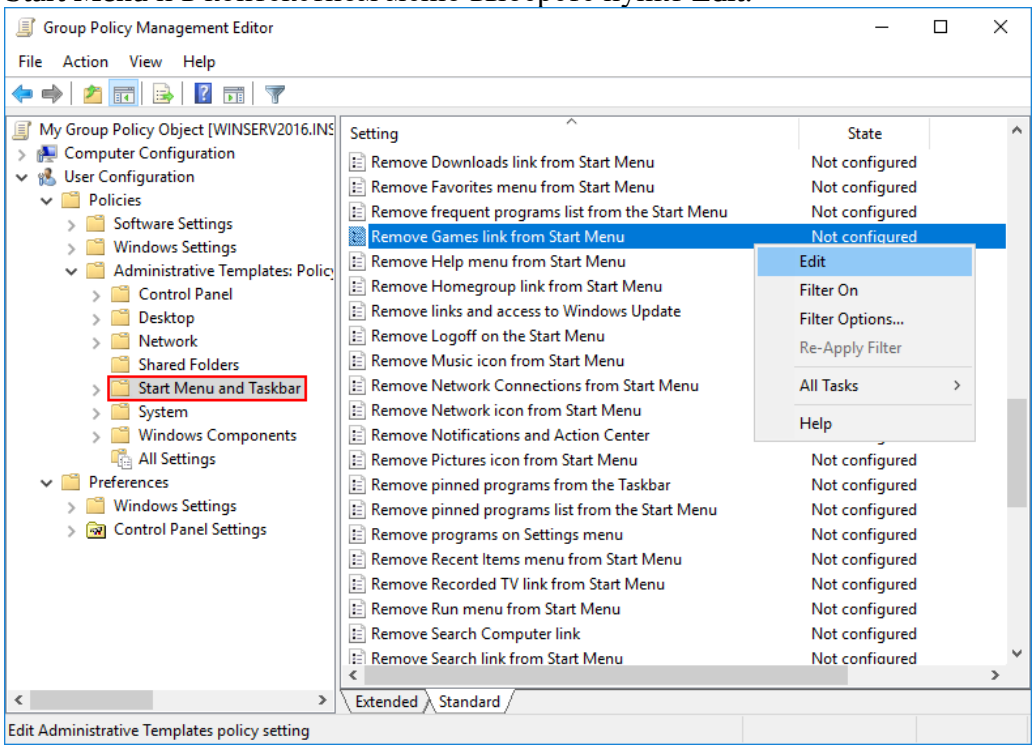
После этого вы увидите созданный объект в списке.



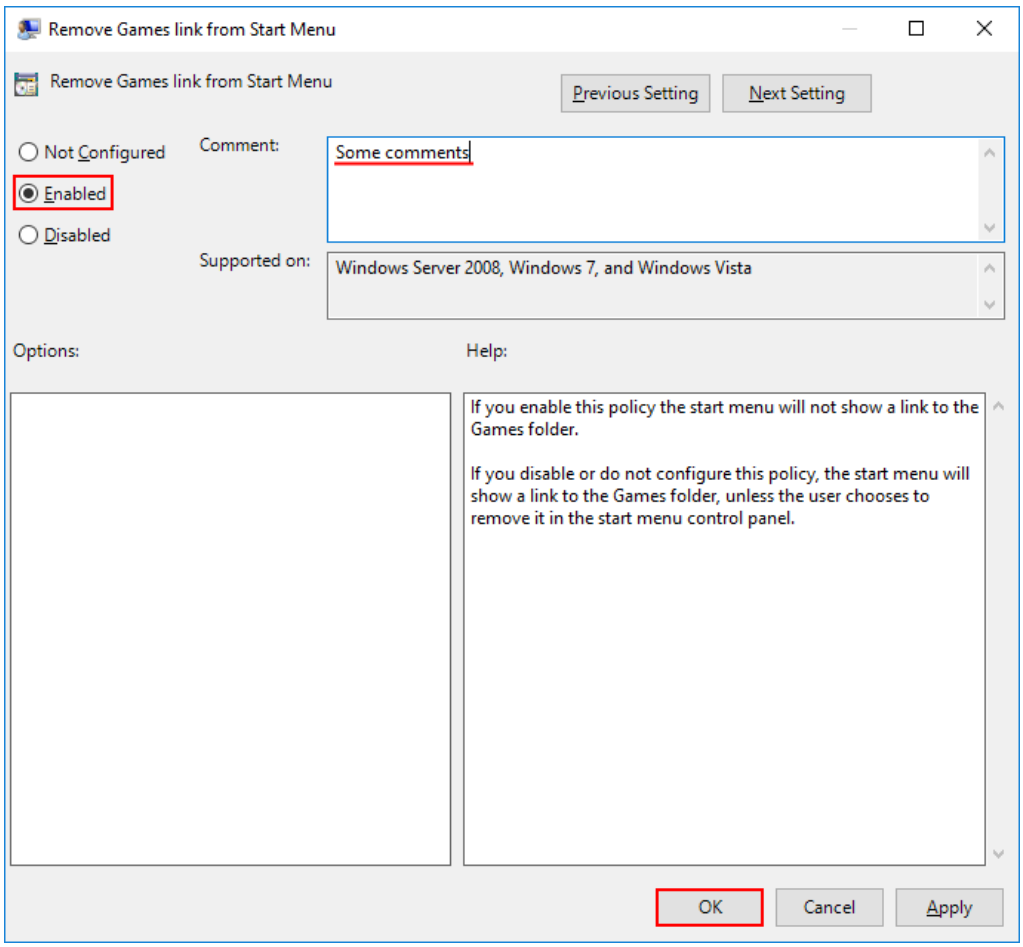
Теперь необходимо настроить созданный объект под конкретные задачи. в качестве примера удалим ссылку Games из меню Start. Для это с помощью правой кнопки мыши откройте меню объекта и выберете пункт Edit.



В редакторе групповых политик перейдите по иерархии User Configuration → Policies → Administrative Templates → Start Menu and Taskbar. Найдите опцию Remove Games link from Start Menu и в контекстном меню выберете пункт Edit.



В открывшемся окне отметьте Enable для включения правила и при необходимости напишите комментарий. Нажмите OK для сохранения изменений.



На этом создание объекта групповой политики закончено.
Вставить скриншот с созданной политикой.

Задание 2

В этот же объект групповой политики добавить определённую картинку на рабочий стол (User Configuration → Policies → Administrative … → Desktop → Desktop Wallpaper → Edit → Enabled → написать путь к картинке → Apply).
Вставить скриншот с окном политики и затем скриншот с рабочим столом рабочей станции.

Задание 3

В этот же объект групповой политики добавить запрет на добавление и удаление программ (в Control Panel).
Вставить скриншот с окном политики и затем скриншот с попыткой удаления/установки программ на рабочей станции.

Задание 4

В этот же объект групповой политики включить лимит на профиль пользователя в 30 000 Кб (System → User Profiles)
Вставить скриншот с окном политики.

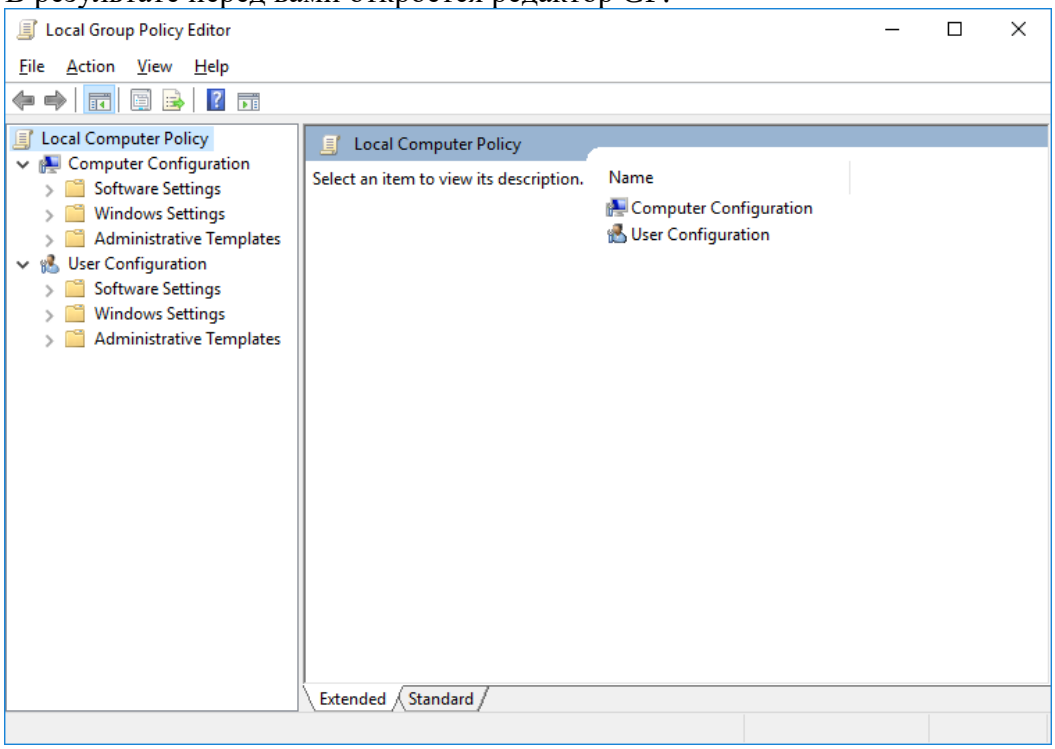
Задание 5

В этом же объекте групповой политики создать 2 любые политики,
Поясните, что вы сделали и скриншоты, подтверждающие выполнение.

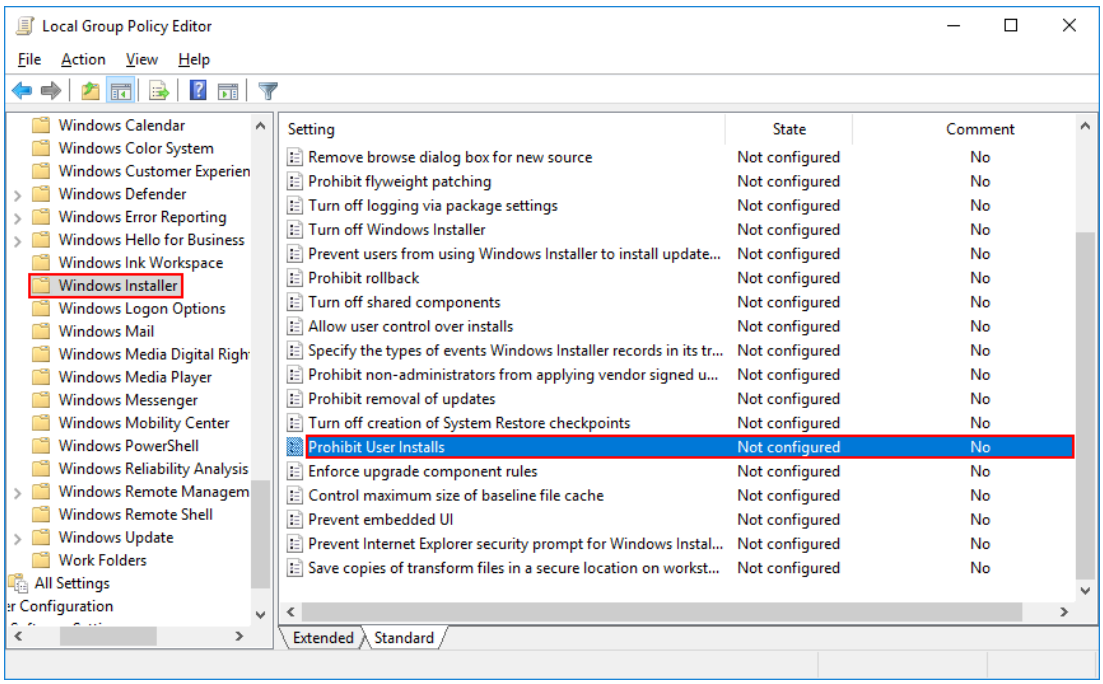
2.7. Практическая работа № 7 «Создание и применение локальных политик домена»

Задание 1:

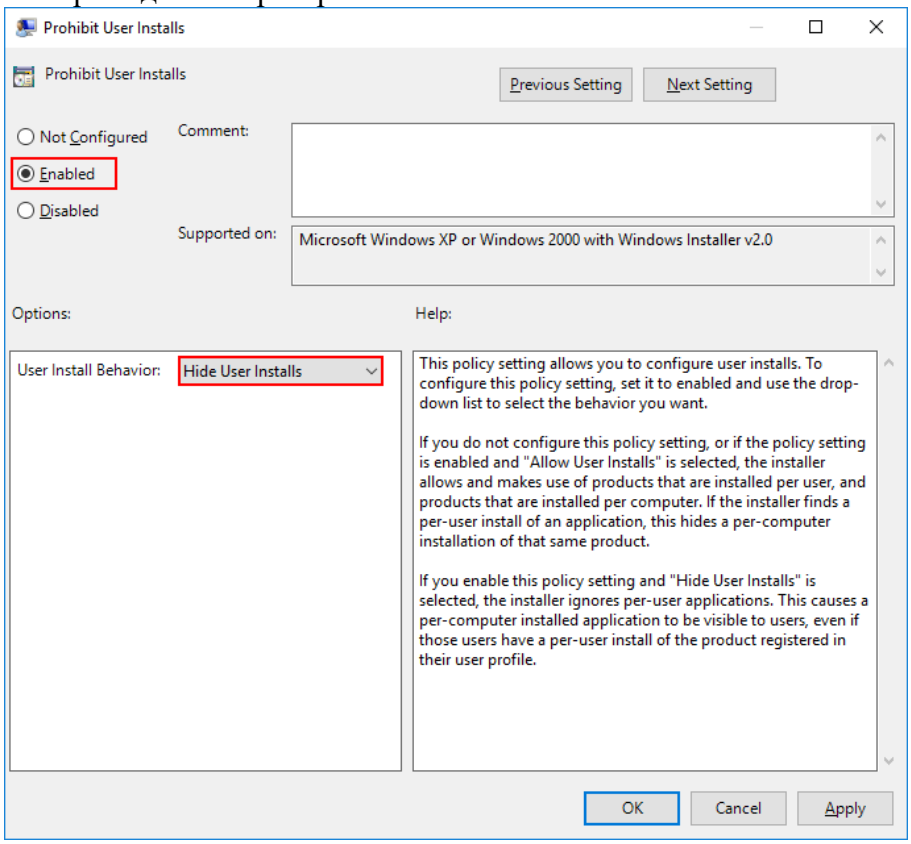
Для создания локальных политик домена запустить оснастку Local Security Policy.
(в Поиске набрать gpedit.msc)
В результате перед вами откроется редактор GP.



Настройка запрета установки программ для пользователей
Откройте редактор GPO, в древовидной структур найдите Computer Configuration → Administrative Templates → Windows Components → Windows Installer. В правой части окна выберете Prohibit User Installs. С помощью двойного щелчка мыши откройте настройки.

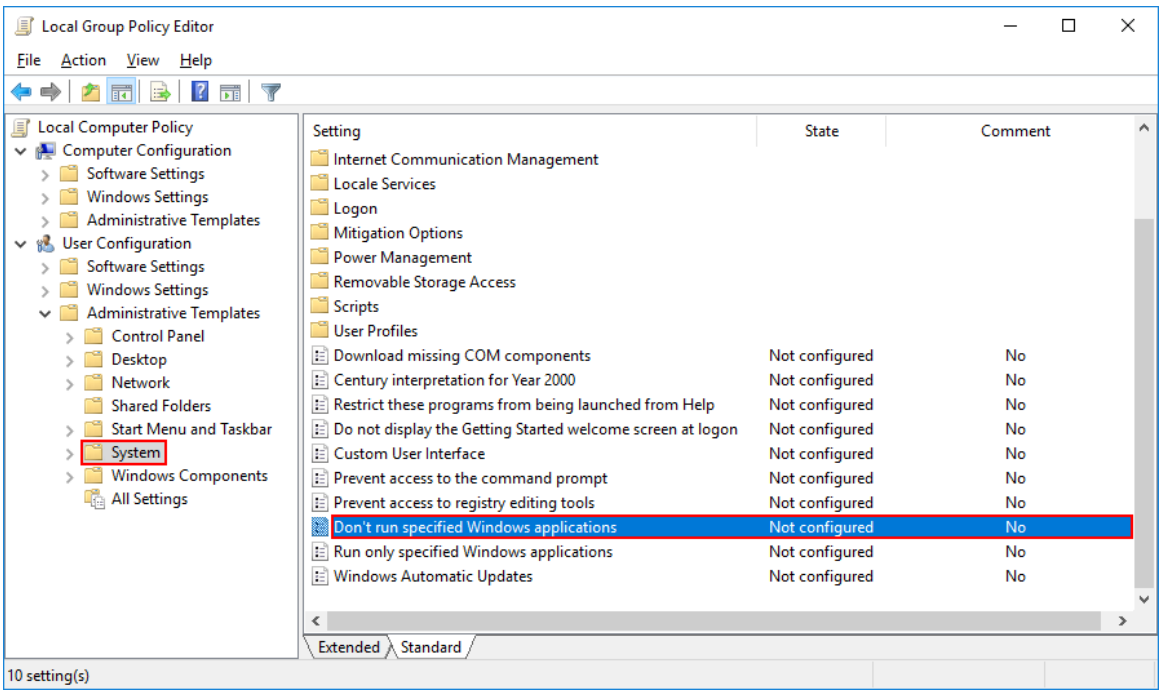


В открывшемся окне выберете опцию Enabled, а в выпадающем списке Hide User Installs. В результате пользователей сервера пропадет возможность установки приложений и программ без прав администратора.

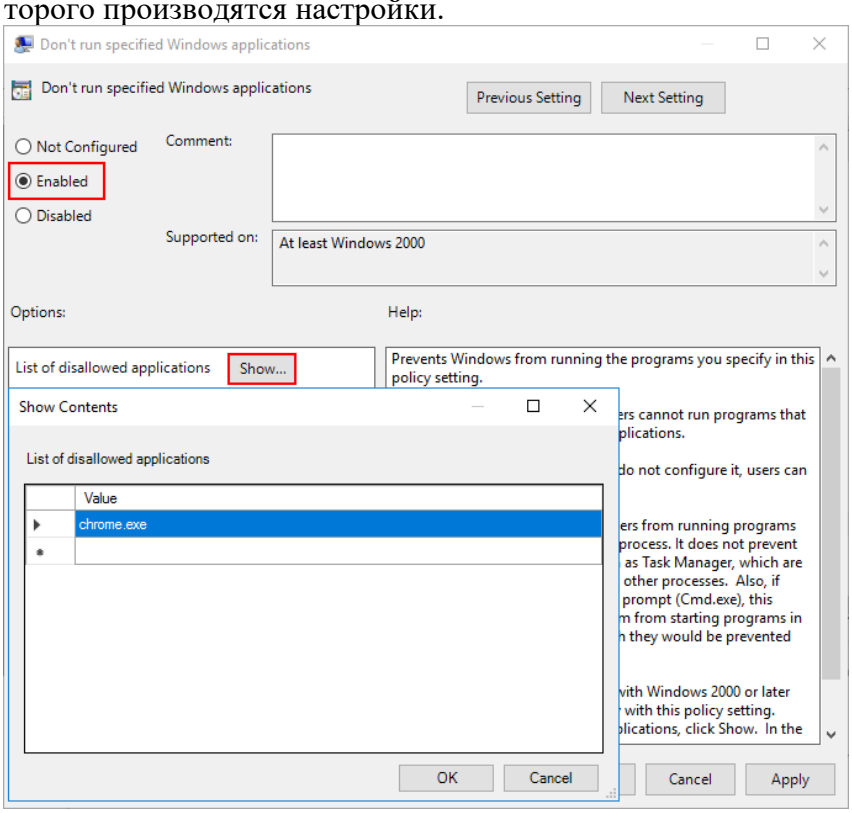


Настройка запрета запуска программ для пользователей

Откройте редактор GP, в древовидной структур найдите User Configuration → Administrative Templates → System. В правой части окна выберете Don’t run spicified Windows Applications. С помощью двойного щелчка мыши откройте настройки политики.



В открывшемся окне выберете опцию Enabled, а и нажмите кнопку Show. В открывшийся список введите приложения, запуск которых будет запрещен для пользователя от имени которого производятся настройки.



Задание 2:

1. Открыть в Локальных политиках «Конфигурация компьютера» (Computer Configuration) → «Конфигурация Windows» (Windows Settings) → «Параметры безопасности» (Security Settings) → «Политики учетных записей» (Account Policies) → «Политика паролей» (Password Policy).

2. Просмотреть информацию по политикам пароля, вставить скриншот с информацией.
3. Изменить политику паролей и вставить скриншот с изменённой информацией.

Задание 3:

Измените Политику блокировки учетных записей (Account Lockout Policy) в случае неверного ввода паролей. Изменить продолжительность блокировки учётной записи, изменить пороговое значение блокировки.
Вставить скриншот с изменённой политикой.

Задание 4:

С помощью ресурсов Интернета ответить на следующие вопросы:

- ✓ Где физически хранятся доменные групповые политики?
- ✓ Чем отличаются локальные политики домена от групповых политик домена?
- ✓ Что такое GPO?

Ответы:

2.8. Практическая работа № 8 «Установка сервера безопасности Secret Net Studio»

Задание 1:

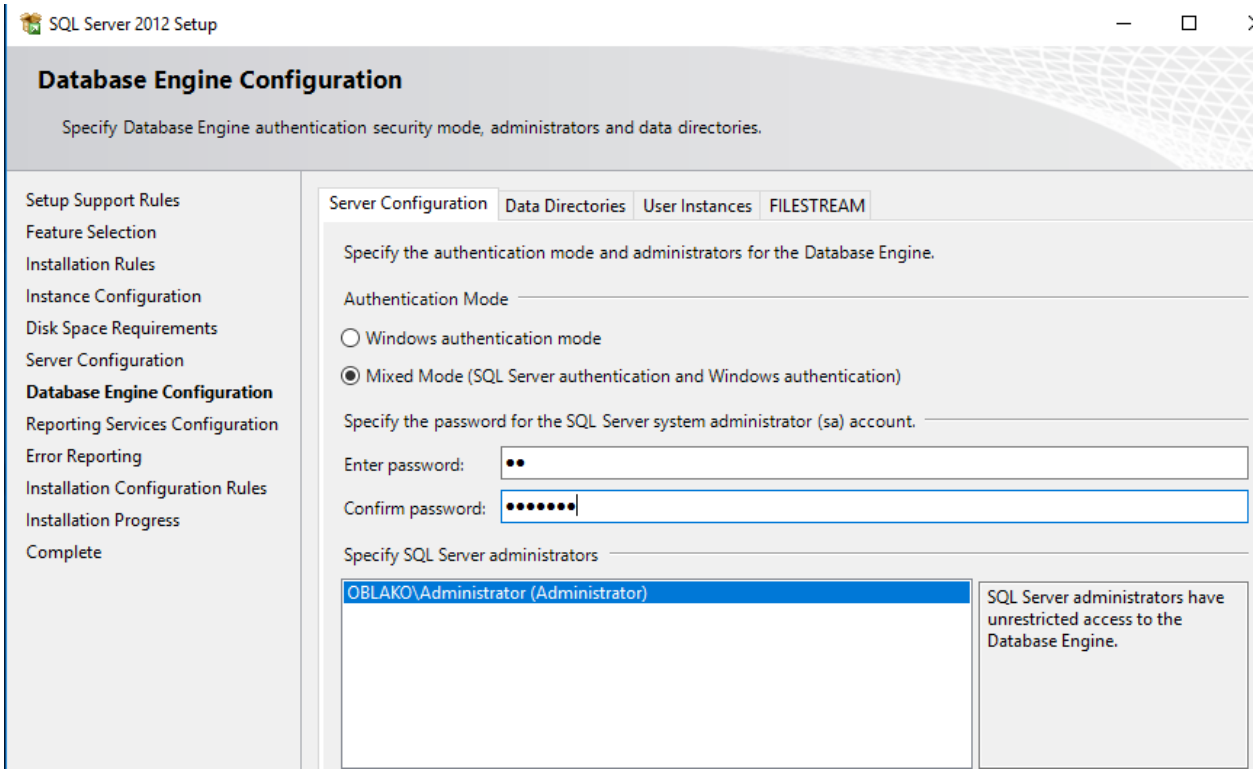
1. Для установки сервера безопасности Secret Net Studio необходимо запустить ваш сервер на Windows, скопировать на него или открыть доступ для дистрибутивов:

Каталог	Содержимое
\Setup\Server\	Дистрибутив сервера безопасности
\Setup\Console\	Дистрибутивы программы управления
\Setup\Client\	Дистрибутивы клиента
\Setup\SnCard\	Файлы установки драйвера средства аппаратной поддержки
\Documentation\	Комплект документации
\Tools\	Вспомогательные утилиты, файлы для установки и настройки ПО

Запустить необходимый дистрибутив для установки и следовать инструкции (Admin Guide – Install). Обратите внимание на необходимый для установки сервера дополнительный софт.

При установке MS SQL Server выберете правильную версию (RU/EU), перед этим установите другой дополнительный софт. При установке MS SQL Server выберете Установить всё.

Далее при установке выбрать следующий вид аутентификации:



Обратите внимание, что пользователь – локальный системный администратор имеет название sa.

Придумайте и запишите пароль.

Возможно потребуется перезагрузка при установке MS SQL Server.

Вставьте скриншот с именем сервера СУБД. Обратите внимание, что вам в названии сервера СУБД нужен путь даже при установке локально (нужно имя вашего компьютера с сервером).

При установке Secret Net Studio стр.15 -16 инструкции по установке прочитать внимательно. Вставьте скриншот с окном Настройки СУБД, записать логины и пароли.

Далее придумать название организации и отдел, который будет защищать данное программное обеспечение.

Вставить скриншот с данными организации

Записать все проблемы, которые возникли при установке и как вы их решили.

Задание 2:

С помощью ресурсов Интернета ответить на следующие вопросы:

- ✓ Чем отличается MS SQL Server Express от MS SQL Server? Почему первый бесплатный, а второй нет? Стоимость MS SQL Server.
- ✓ Стоимость программного обеспечения Secret Net Studio.

Ответы:

2.9. Практическая работа № 9 «Установка программы управления Secret Net Studio»

Задание 1:

1. Для установки сервера безопасности Secret Net Studio необходимо запустить ваш сервер на Windows, рабочую станцию, находящуюся в домене.

Скопировать на сервер и рабочую станцию или открыть доступ для дистрибутивов:

Каталог	Содержимое
\Setup\Server\	Дистрибутив сервера безопасности
\Setup\Console\	Дистрибутивы программы управления
\Setup\Client\	Дистрибутивы клиента
\Setup\SnCard\	Файлы установки драйвера средства аппаратной поддержки
\Documentation\	Комплект документации
\Tools\	Вспомогательные утилиты, файлы для установки и настройки ПО

2. Программу управления необходимо установить на сервер.

3. После установки программы управления необходимо в обязательном порядке установить пакет обновлений 8.5.5329.40, находящийся на установочном диске системы Secret Net Studio в каталоге \Tools\SecurityCode\ManualPatches\8_ 5_ 5329_ 40_ Inc76262_ Build27. Без этого обновления невозможна корректная работа с паролем (PIN) сервисного режима в механизме самозащиты Secret Net Studio и недоступно управление новой функцией контроля административных привилегий.

Вставить скриншот с установленной программой управления Secret Net Studio.

4. Запустить Программу управления Secret Net Studio → Обновить → Connect. Может быть потребуется раза два нажать прежде чем откроется Программу управления. Выбрать Рабочий режим. вставить скриншот с запущенной программой.

записать все проблемы, которые возникли при установке и как вы их решили.

Задание 2:

С помощью ресурсов Интернета и/или инструкции по установке Secret Net Studio ответить на следующие вопросы:

- ✓ В каком случае нужно ставить клиента Secret Net Studio локально?
- ✓ Какие компоненты можно установить на клиента Secret Net Studio?
- ✓ Для чего нужен драйвер средств аппаратной поддержки в Secret Net Studio?

Ответы:

2.10. Практическая работа № 10 «Настройка централизованной установки клиента Secret Net Studio»

Задание 1:

1. Установить централизованно клиент Secret Net Studio, используя инструкцию со страницы 23 (имя файла: Admin Guide – Install):

Вставить скриншот панели «Развёртывания» с вкладкой «Репозиторий».

Опишите, как создать задания для централизованной установки клиента Secret Net Studio.

2. В случае невозможности централизованной установки клиента Secret Net Studio установить его локально на рабочую станцию, находящуюся в домене.

Вставить скриншот с окном Установки со всеми галочками успешной установки.

3. Перезагрузите рабочую станцию с установленным клиентом Secret Net Studio.

Вставьте скриншот с изменениями загрузки операционной системы на рабочей станции.

4. Найдите в меню Пуск все установленные компоненты клиента Secret Net Studio. Закрепите все компоненты на панели задач.

Вставьте скриншот с выполненным заданием.

Задание 2:

С помощью ресурсов Интернета и/или документации по Secret Net Studio ответить на следующие вопросы:

- ✓ Чем отличается вход в систему при установленном программно-аппаратном комплексе «Соболь»?
- ✓ Какие бывают режимы входа в систему при различных режимах идентификации пользователей?
- ✓ Можно ли на одной рабочей станции установить разные режимы входа?
- ✓ Как выглядит на экране запрос персонального идентификатора при использовании комплекса «Соболь»?

Ответы:

2.11. Практическая работа № 11 «Работа с действующими средствами локальной защиты с помощью Secret Net Studio»

Задание 1:

Запустите управление параметрами безопасности пользователей. Откройте свойства вашего пользователя → Параметры безопасности → Доступ. Установите уровень допуска Конфиденциально.

Вставьте скриншот с выполненным заданием.

Добавьте нового пользователя из AD (не создавать нового). Должна появиться надпись после добавления Доменный пользователь. вставьте скриншот с добавленным пользователем.

Запустите Локальный центр управления Secret Net Studio — Настройки. Смените максимальный период неактивности до блокировки экрана.

Вставьте скриншот с выполненным заданием.

В базовой защите на вход в систему установите количество неудачных попыток аутентификации на 1 попытку.

Вставьте скриншот с выполненным заданием.

Установите в базовой защите в журнале не затирать события.

Вставьте скриншот с выполненным заданием.

Перейдите в Локальную защиту → Замкнутая программная среда → Удалите возможность у пользователей создавать криптоконтейнеры.

Вставьте скриншот с выполненным заданием.

Перейдите в Сетевую защиту → Обнаружение вторжений → измените время блокировки атакующего хоста. Внесите в белый список любой IP-адрес.

Вставьте скриншот с выполненным заданием.

Перейдите в Регистрации событий → Дискреционное управление доступом → включите регистрацию доступа к файлам и каталогам.

Вставьте скриншот с выполненным заданием.

Выйдите с вкладки Настройки, перейдите на вкладку Журналы. Создайте журнал по событиям Secret Net Studio. Получите журнал и экспортируйте.

Вставьте скриншот с выполненным заданием.

Перейдите на вкладку Отчёты → Ресурсы АРМ→ выберете несколько пунктов для будущего отчёта → нажмите Построить → Просмотреть.

Вставьте скриншот с выполненным заданием.

Закройте данный программный компонент. Откройте Контроль программ и данных. Просмотрите структуру Субъектов управления.

Вставьте скриншот и ответьте на вопрос: Для чего предназначен компонент Контроль программ и данных?

Закройте все компоненты Secret Net Studio. На Рабочем столе создайте новую папку. Откройте контекстное меню папки.

Вставьте скриншот и ответьте на вопрос: что появилось в контекстном меню от Secret Net Studio и что это означает?

Откройте Свойства новой созданной папки, перейдите на вкладку Secret Net Studio. Измените на Категорию Конфиденциально.

Вставьте скриншот с выполненным заданием.

Задание 2:

С помощью ресурсов Интернета и/или документации по Secret Net Studio ответить на следующие вопросы:

- ✓ Что такое теневое копирование?
- ✓ Для чего предназначено Затирание данных в Центре управления Secret Net Studio?

- ✓ По каким принципам работает Обнаружение вторжений в Центре управления Secret Net Studio?
- ✓ По каким принципам работает Персональный межсетевой экран в Центре управления Secret Net Studio?
- ✓ По каким принципам работает Доверенная среда в Центре управления Secret Net Studio?

Ответы:

2.12. Практическая работа № 12 «Удаление всех компонентов Secret Net Studio»

Задание 1:

Удалить все компоненты Secret Net Studio с использованием инструкции (со стр. 41).
Вставить скриншоты с удаленными программами управления, сервера, клиента.

Задание 2:

С помощью ресурсов Интернета и/или документации по Secret Net Studio ответить на следующие вопросы:

- ✓ Почему перед удалением компонентов Secret Net Studio необходимо сохранить конфиденциальную информацию?
- ✓ В каком порядке необходимо удалять компоненты Secret Net Studio?
- ✓ Как удалить клиента Secret Net Studio в интерактивном режиме?
- ✓ На какие особенности нужно обратить внимание при удалении сервера безопасности Secret Net Studio?

Ответы:

2.13. Практическая работа № 13 «Установка Dallas Lock»

Задание 1:

1. Прочитать все начальные требования по установке Dallas Lock в Руководстве по эксплуатации СЗИ НСД Dallas Lock.
2. Запустить сервер с контроллером домена и создать пользователя, добавить его в группу администраторов и администраторов домена для установки и работы с Dallas Lock.

Записать Логин и пароль

3. Запустить виртуальную рабочую станцию, входящую в домен Oblako под новым пользователем. Следую инструкциям по установке запустить и установить Dallas Lock.

4. Записать логин и пароль для суперпользователя DalasLock. Он отличается от нового администратора.

5. вставить скриншот с успешной установкой DalasLock. Перезагрузить компьютер.

6. Вставить скриншот входа в систему после перезагрузки.

7. Войти в систему, сделать скриншот с ярлыком на DalasLock Рабочем столе.

Задание 2:

С помощью ресурсов Интернета и/или документации по Dallas Lock ответить на следующие вопросы:

- ✓ Является ли поле «код технической поддержки» при установке Dallas Lock обязательным? Для чего оно нужно?
- ✓ Что такое Домен безопасности (ДБ) и зачем вводить клиента в ДБ?
- ✓ Можно ли компьютер с ролью Контроллер домена вводить в Домен безопасности?
- ✓ В какую папку всегда устанавливается DallasLock?
- ✓ Какие варианты входа в систему могут быть при установленном DallasLock?

Ответы:

2.14. Практическая работа № 14 «Настройка средств администрирования в Dallas Lock»

Задание 1:

1. Включить рабочую станцию с установленным Dallas Lock и запустить Администрирование.

2. Перейти на вкладку Параметры безопасности. Настроить Категорию «Вход» в соответствии с классом защищённости 1Б по следующим рекомендациям:

Таблица №1. Политики безопасности вкладки «Параметры безопасности»

Параметры	Классы защищенности АС/Значения параметров		
	1Б, 1В, 1Г, 1Д	2А, 2Б	3А, 3Б
Категория «Вход»	**Значения параметров**		
Вход: запрет смены пользователя без перезагрузки	1Б: Вкл. (реком.) 1В, 1Г, 1Д: Выкл. (АИБ)	2А: Вкл. (реком.) 2Б: Выкл. (АИБ)	Выкл. (АИБ)
Вход: отображать имя последнего пользователя	Да (реком.)	Да (реком.)	Да (реком.)
Вход: максимальное кол-во ошибок ввода пароля	5 (реком.)	5 (реком.)	5 (реком.)
Вход: время блокировки учетной записи в случае ввода неправильных паролей	15 мин. (реком.)	15 мин. (реком.)	15 мин. (реком.)
Вход: отображать информацию о последнем успешном входе	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)

Параметры	Классы защищенности АС/Значения параметров		
	1Б, 1В, 1Г, 1Д	2А, 2Б	3А, 3Б
Вход: запрет одновременной работы пользователей с различными уровнями или метками мандатного доступа	1Б, 1В: Выкл. (АИБ) 1Г, 1Д: «-»	2А: Выкл. (АИБ) 2Б: «-»	«-»
Вход: выбор мандатной метки при входе в ОС	1Б, 1В: Выкл. (АИБ) 1Г, 1Д: «-»	2А: Выкл. (АИБ) 2Б: «-»	«-»
Вход: разрешить использование смарт-карт	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Вход: запретить использование парольного интерфейса входа	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Вход: автоматический выбор аппаратного идентификатора при авторизации	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Пароли: максимальный срок действия пароля	42 дн. (реком.)	42 дн. (реком.)	42 дн. (реком.)
Пароли: минимальный срок действия пароля	Не используется (АИБ)	Не используется (АИБ)	Не используется (АИБ)
Пароли: напоминать о смене пароля за	14 дн. (реком.)	14 дн. (реком.)	14 дн. (реком.)
Пароли: минимальная длина	1Б: не менее 8 симв. (обяз.) 1В, 1Г, 1Д: не менее 6 симв. (обяз.)	не менее 6 симв. (обяз.)	не менее 6 симв. (обяз.)
Пароли: необходимо наличие цифр	Да (обяз.)	Да (обяз.)	Да (обяз.)
Пароли: необходимо наличие спец. символов	1Б: Да (реком.) 1В, 1Г, 1Д: Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Пароли: необходимо наличие строчных и прописных букв	1Б: Да (реком.) 1В, 1Г, 1Д: Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Пароли: необходимо отсутствие цифр в первом и последнем символе	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Пароли: необходимо изменение пароля не меньше чем	Не используется (АИБ)	Не используется (АИБ)	Не используется (АИБ)
Домен безопасности	Не задан (АИБ)	Не задан (АИБ)	Не задан (АИБ)
Сеть: Ключ удаленного доступа	АИБ	АИБ	АИБ
Сеть: Время хранения сетевого кэша	30 мин (АИБ)	30 мин (АИБ)	30 мин (АИБ)
Сеть: список незащищенных серверов	АИБ	АИБ	АИБ
Настройка считывателей аппаратных идентификаторов	АИБ	АИБ	АИБ
Блокировать компьютер при отключении аппаратного идентификатора	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Блокировать файл-диски при отключении аппаратного идентификатора	Да (АИБ)	Да (АИБ)	Да (АИБ)
Текс сообщения при входе	АИБ	АИБ	АИБ
Использовать авторизационную информацию от СДЗ Dallas Lock	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)

Вставить скриншоты выполненной работы.

3. Настроить Категорию «Аудит» в соответствии с классом защищённости 1Б по следующим рекомендациям:

Категория «Аудит»	Значения параметров		
Журнал входов в систему	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (обяз.)
Журнал ресурсов	1Д: Вкл. (реком.) 1Г, 1В, 1Б: Вкл. (обяз.)	2А: Вкл. (обяз.) 2Б: Вкл. (реком.)	Вкл. (реком.)
Журнал управления политиками безопасности	1Д, 1Г: Вкл. (реком.) 1В, 1Б: Вкл. (обяз.)	Вкл. (реком.)	Вкл. (реком.)

Параметры	Классы защищенности АС/Значения параметров		
	1Б, 1В, 1Г, 1Д	2А, 2Б	3А, 3Б
Журнал управления учетными записями	1Д, 1Г: Вкл. (реком.) 1В, 1Б: Вкл. (обяз.)	Вкл. (реком.)	Вкл. (реком.)
Журнал печати	1Д: Выкл. (АИБ) 1Г, 1В, 1Б: Вкл. (обяз.)	2А: Вкл. (обяз.) 2Б: Выкл. (АИБ)	3А: Вкл. (обяз.) 3Б: Выкл. (АИБ)
Журнал запуска/завершения процессов	1Д: Вкл. (реком.) 1Г, 1В, 1Б: Вкл. (обяз.)	2А: Вкл. (обяз.) 2Б: Вкл. (реком.)	Вкл. (реком.)
Служебный журнал МЭ	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Журнал пакетов МЭ	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Журнал соединений МЭ	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Журнал трафика фильтрации МЭ	Вкл. (АИБ)	Вкл. (АИБ)	Вкл. (АИБ)
Журнал событий ОС	Вкл. (обяз.)	Вкл. (обяз.)	Вкл. (обяз.)
Журнал трафика СОВ	Вкл. (АИБ)	Вкл. (АИБ)	Вкл. (АИБ)
Журнал контроля приложений СОВ	Вкл. (АИБ)	Вкл. (АИБ)	Вкл. (АИБ)
Фиксировать в журнале входов неправильные пароли	1Д: Нет (АИБ) 1Г, 1В, 1Б:Да (обяз.)	Нет (АИБ)	Нет (АИБ)
Заносить в журнал исходящие попытки входа на удаленные компьютеры	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Заносить в журнал события запуска и остановки ОС	Да (обяз.)	Да (обяз.)	Да (обяз.)
Заносить в журнал события запуска и остановки модулей администрирования DL	1Д: Да (реком.) 1Г, 1В, 1Д: Да (обяз.)	2А: Вкл. (обяз.) 2Б: Вкл. (реком.)	Вкл. (реком.)
Аудит устройств	1Д: Вкл. (реком.) 1Г, 1В, 1Д: Вкл. (обяз.)	2А: Вкл. (обяз.) 2Б: Вкл. (реком.)	3А: Вкл. (обяз.) 3Б: Вкл. (реком.)
Аудит событий зачистки	1Д: Вкл. (реком.) 1Г, 1В, 1Д: Вкл. (обяз.)	2А: Вкл. (обяз.) 2Б: Вкл. (реком.)	3А: Вкл. (обяз.) 3Б: Вкл. (реком.)
Аудит доступа: Заносить в журналы ошибки ОС	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Аудит доступа/запуска: Вести аудит системных пользователей	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Печатать/редактировать штамп	1Д, 1Г: Нет (АИБ) 1В, 1Б: Да (обяз.)	2А: Да (обяз.) 2Б: Нет (АИБ)	3А: Да (обяз.) 3Б: Нет (АИБ)
Создавать теневые копии распечатываемых документов	Нет (АИБ)	Нет (АИБ)	Нет (АИБ)
Разрешать печатать из-под уровней доступа	1Д, 1Г: «-» 1В, 1Б: Все уровни (реком.)	2А: Все уровни (реком.) 2Б: «-»	«-»
Добавлять штамп при печати под уровнями	1Д, 1Г: «-» 1В, 1Б: Все уровни (реком.)	2А: Все уровни (реком.) 2Б: «-»	«-»
Выгрузка журналов	Выкл. (АИБ)	Выкл. (АИБ)	Выкл. (АИБ)
Максимальное кол-во записей в журналах	2 000 (АИБ)	2 000 (АИБ)	2 000 (АИБ)
Периодическая архивация журналов	Не используется (АИБ)	Не используется (АИБ)	Не используется (АИБ)

вставить скриншоты выполненной работы.

Задание 2:

С помощью ресурсов Интернета и/или документации по Dallas Lock ответить на следующие вопросы:

- ✓ Поясните класс защищённости 1Б, 1В, 1Г, 1Д.
- ✓ Что такое мандатная метка при входе в ОС?
- ✓ Что такое контроль приложений СОВ?
- ✓ Что такое теневые копии распечатываемых документов?

Ответы:

2.15. Практическая работа № 15 «Настройка подсистем управления доступом в Dallas Lock»

Задание 1:

1. Включить рабочую станцию с установленным Dallas Lock и запустить Администрирование.
2. Перейти на вкладку Учётные записи. Создать пользователя user1. Придумать любое полное имя, описание. В Параметрах выставить Отключена, запретить смену пароля пользователя. сгенерировать пароль и записать.

Вставить скриншот с созданным пользователем на вкладке Учётные записи.

3. Перейти на вкладку Контроль ресурсов → Устройства. Любым двум устройствам разрешить дискреционный доступ.

Вставить скриншот с разрешением и пояснением выбора устройств для дискреционного доступа.

4. Любым двум устройствам разрешить мандатный доступ. вставить скриншот с разрешением и пояснением выбора устройств для мандатного доступа.
5. Любому одному из выше выбранных устройств включить аудит успеха.
6. Любому одному из выше выбранных устройств включить аудит отказа.

Задание 2:

С помощью ресурсов Интернета и/или документации по Dallas Lock ответить на следующие вопросы:

- ✓ Для чего в Dallas Lock нужен пользователь secServer?
- ✓ Для чего в Dallas Lock нужен пользователь anonymous?
- ✓ Понятие дискреционного доступа
- ✓ Понятие мандатного доступа
- ✓ Для чего нужен аудит доступа? Что показывает аудит успеха? Что показывает аудит Отказа?

Ответы

2.16. Практическая работа № 16 «Разграничение доступа к объектам файловой системы в Dallas Lock»

Задание 1:

1. Включить рабочую станцию с установленным Dallas Lock и запустить Администрирование.

2. Перейти на вкладку Параметры безопасности → Очистка остаточной информации. Выставить следующие параметры:

Категория «Очистка остаточной информации»	
Очищать освобождаемое дисковое пространство	Да (реком.)
Очищать файл подкачки виртуальной памяти	Да (реком.)
Очищать данные в конфиденциальных сеансах доступа	Да (реком.)
Проверять очистку информации	Нет (АИБ)
Количество циклов затирания	От 1 (АИБ)
Затирающая последовательность	Значение выставляется АИБ

Вставить скриншот с выставленными параметрами.

3. На вкладке Контроль целостности выставить следующие параметры:

Категория «Контроль целостности»	
Подкатегория «Политики»	
Проверять целостность ФС при загрузке ОС	Вкл. (обяз.)
Периодический контроль ФС	Вкл. (обяз.)
Контроль ФС по расписанию	Данный параметр можно включить или не использовать, определяется АИБ
Проверять целостность прогр. апп. среды при загрузке ОС	Вкл. (обяз.)
Периодический контроль прогр. апп. среды	Вкл. (обяз.)
Контроль прогр.апп. среды по расписанию	Данный параметр можно включить или не использовать, определяется АИБ
Проверять целостность реестра при загрузке ОС	Вкл. (обяз.)
Периодический контроль реестра	Вкл. (обяз.)
Контроль реестра по расписанию	Данный параметр можно включить или не использовать, определяется АИБ
Изменение файлов с назначенным контролем целостности	Разрешать (АИБ)

скриншот с выставленными параметрами.

4. Перейти на вкладку Контроль ресурсов → Глобальные. Установить на Параметры реестра дискреционный доступ одному из пользователей.

Вставить скриншот с результатом.

5. Установить дискреционный доступ на Параметры сети для того же пользователя, а также включить Аудит доступа на открытие объекта Успех.

Вставить скриншоты с результатами.

Задание 2:

С помощью ресурсов Интернета и/или документации по Dallas Lock ответить на следующие вопросы:

- ✓ Что означает алгоритм CRC32 контроля целостности?
- ✓ Понятие дескриптора объекта.

Ответы:

2.17. Практическая работа № 17 «Работа с подсистемой регистрации и учёта в Dallas Lock»

Задание 1:

1. Включить рабочую станцию с установленным Dallas Lock и запустить Администрирование. Перейти на вкладку Журналы.
2. На вкладке Журнал входов просмотрите информацию за сегодняшнюю дату. Выпишите пользователя с успешным входом и выпишите пользователя с запрещённым доступом.

вставьте информацию о запрещённом Пользователе ОС – кто/что это.

3. На вкладке Журнал упр.уч.записями просмотрите какие были операции с учётными записями.

вставьте скриншот из этого журнала и ответ на вопрос: Есть ли операции заблокированные? Если есть, то как вы думаете, почему?

4. На вкладке Журнал ресурсов просмотрите информацию.

Запишите какие объекты доступа менялись и везде ли результат положительный.

5. На вкладке Журнал упр.политиками просмотрите информацию за сегодняшний день.

вставьте скриншот с информацией за сегодняшний день.

6. На вкладке Журнал процессов просмотрите информацию за сегодняшний день.

напишите ответ на вопрос: Что показывает журнал процессов? Чем он отличается от диспетчера задач?

7. К Журналу процессов примените фильтр с сегодняшней датой, с операцией запуска и результатом успеха.

вставить скриншот настроек фильтра и скриншот с результатом фильтра.

вставить скриншот настроек фильтра и скриншот с результатом фильтра.

8. На Рабочем столе создаёте текстовый файл с любым текстом. Сохраните. Закройте.Зайдите в Администрированием Dallas Lock → Журналы.

Вставьте скриншот из журнала, в котором отображается информация о ваших действиях.

Задание 2:

С помощью ресурсов Интернета и/или документации по Dallas Lock ответить на следующие вопросы:

- ✓ Для чего нужен Журнал?
- ✓ Для чего в Журнале предусмотрены фильтры?
- ✓ Для чего Журнал может понадобиться экспортировать?

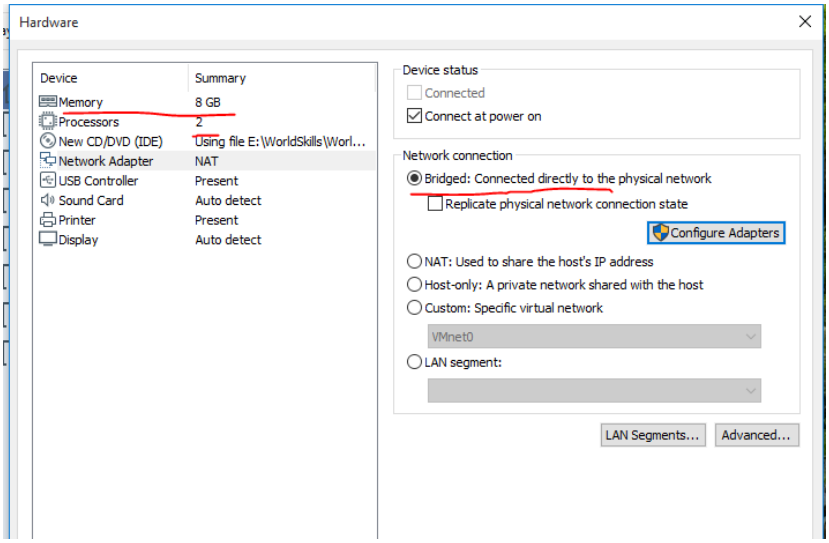
Ответы:

2.18. Практическая работа № 18 «Установка Infowach Trafic Monitor»

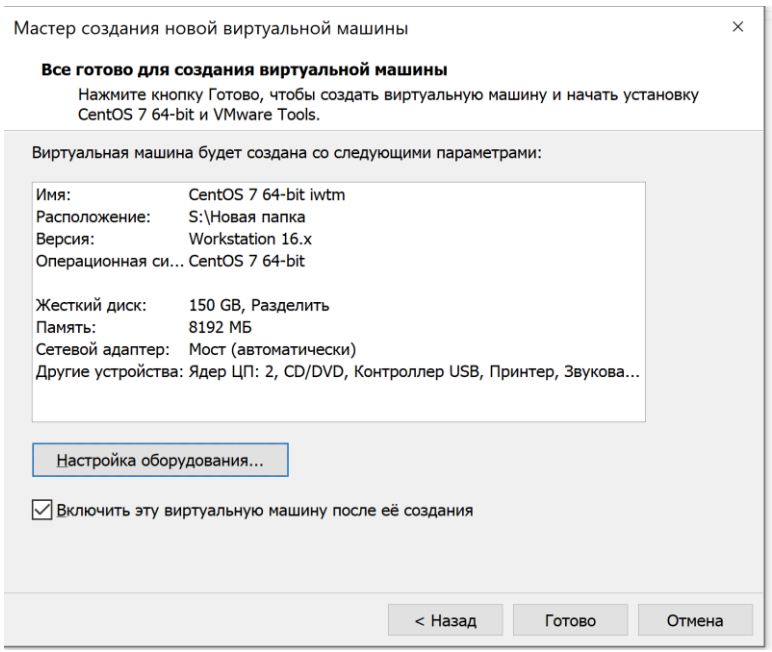
Задание 1:

1. Установить CentOS 7, дать минимум 100 гб на диске, 8 гб ram, 2 потока ЦП. Сетевой адаптер: мост:

— в английской версии VMware:

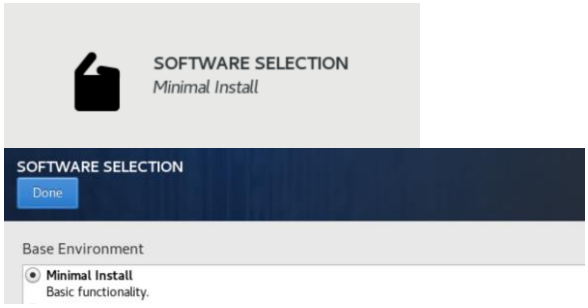


— в русской версии VMware:

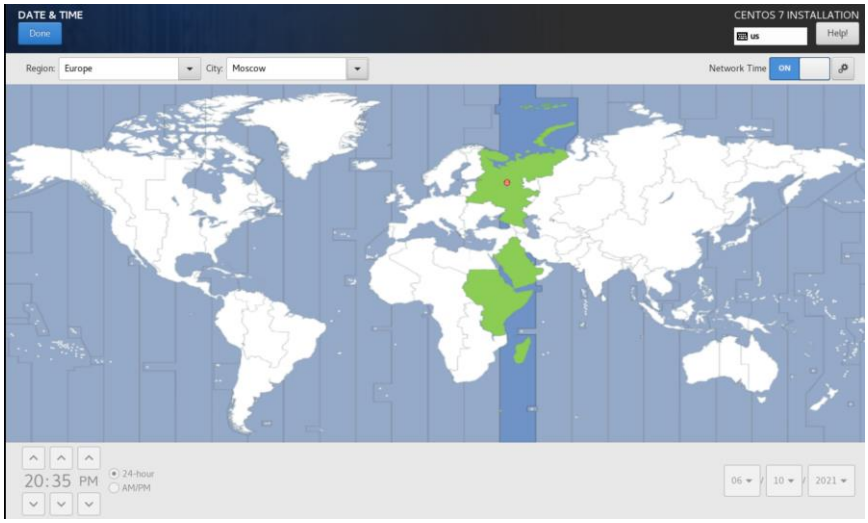


2. После запуска процесса установки выбрать:

— выбор программ – минимальная установка;

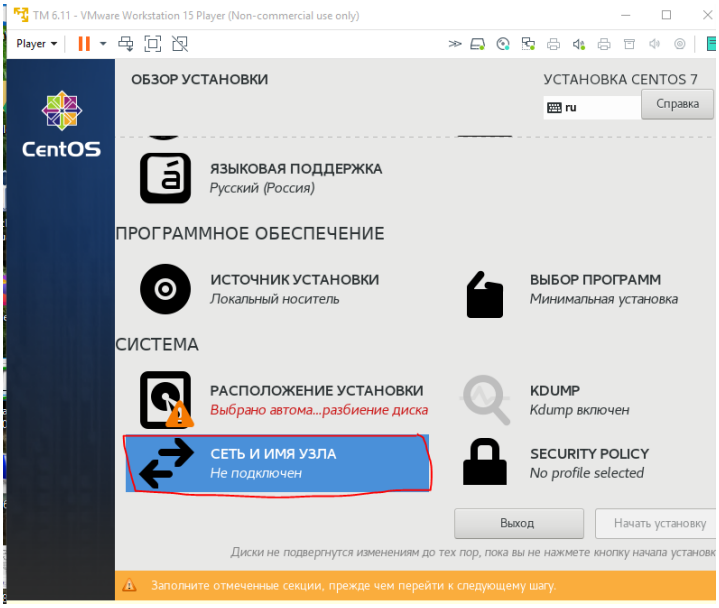


— задать время:

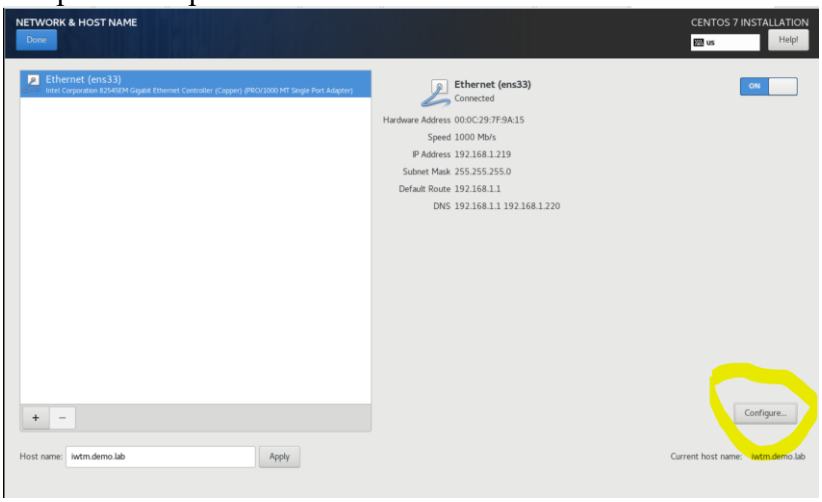


— настроить сеть:

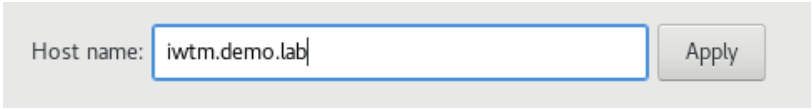
выбрать пункт в меню:



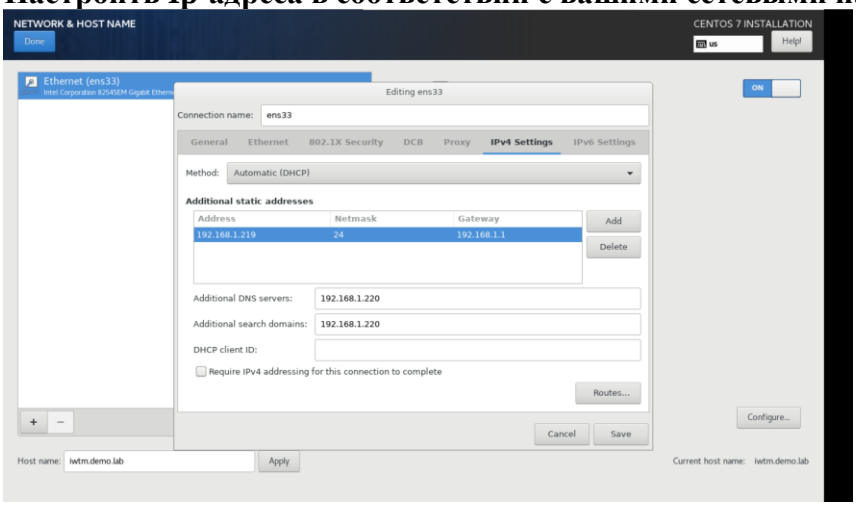
выбрать Настроить:



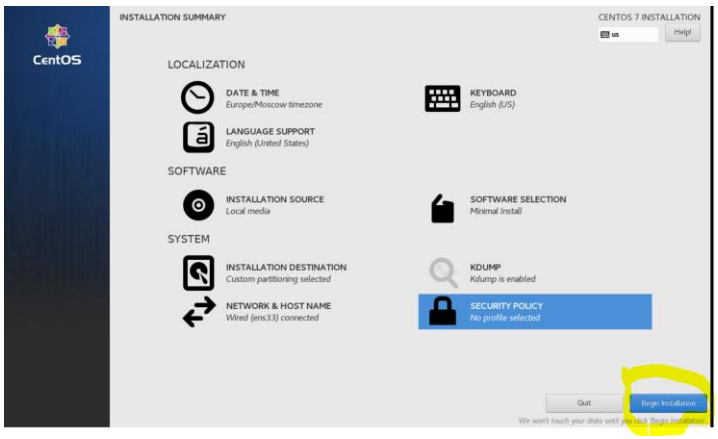
iwtm – обязательное имя машины.
demo.lab – имя вашего домена.



Далее выбрать Параметры IPv4:
Настроить Ip-адреса в соответствии с вашими сетевыми настройками!



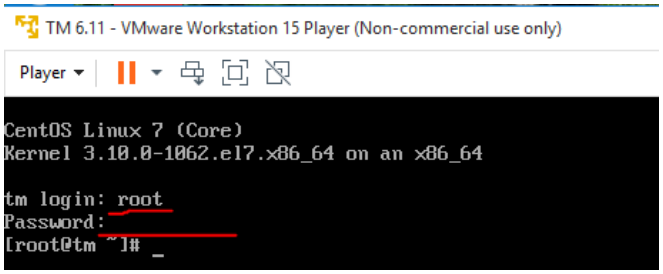
3. Запустить установку



4. Установить пароль для root в соответствии с требованиями, например 1q2w3e4r
5. Имя узла указать iwtm.

6. После установки перезагрузить установленную машину.

7. Далее при запросе login к вашей машине вводим root. Далее вводим пароль (ОБРАТИТЕ ВНИМАНИЕ: в Linux пароль при наборе не показывает никакие знаки!):



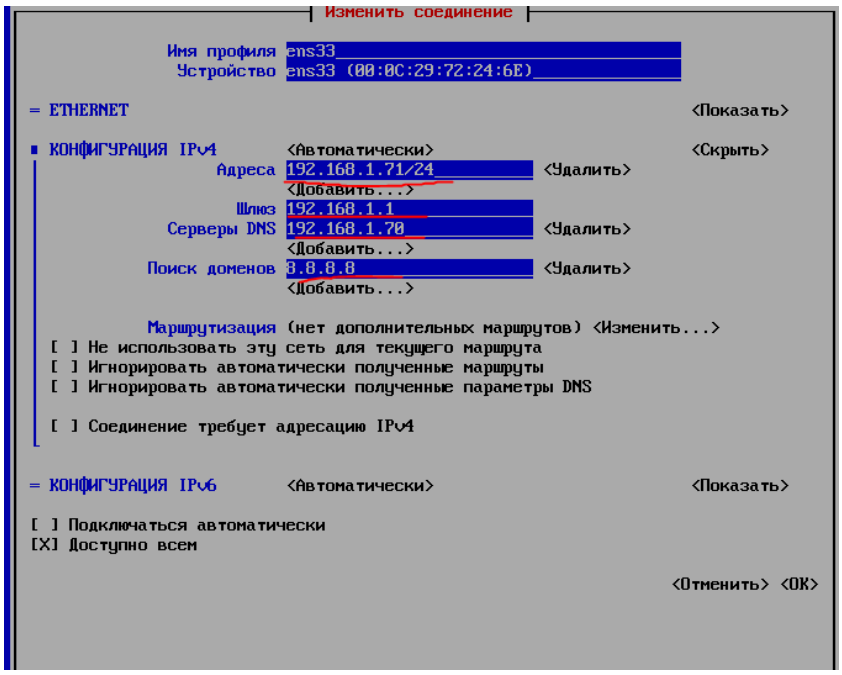
Убедиться, что вы вошли и у вас на экране [root@**iwtm**~]#

Если имя узла не iwtm, то на следующем шаге при запуске nmtui изменить (пункт — Измените имя узла).

<u>В отчёт вставить скриншот, показывающий установленную машину с успешным входом в систему.</u>

8. Далее для проверки сетевых настроек набрать следующую команду:

Убедиться что у вас заполнены следующие поля:



Если у вас всё настроено, то менять ничего не нужно!

В отчёт вставить скриншот с вашими сетевыми настройками.

Далее с помощью клавиш Tab, Стрелок и Enter выйти из nmtui ничего не изменяя.

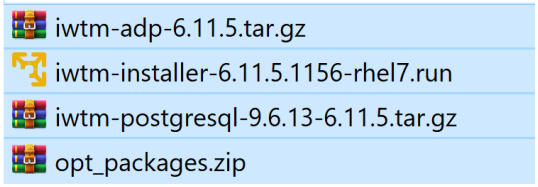
9. Выполнить проверку соединения Centos с доменом:

— выполнить ping домена на Centos;

— выполнить ping Centos на домене.

В отчёт вставить скриншот с удачными версиями ping. (Если на Centos сеть недоступна, то запускаем nmtui и включаем сетевой адаптер!)

10. Для установки iwtm потребуется перенести на виртуальную машину с Centos следующие файлы:

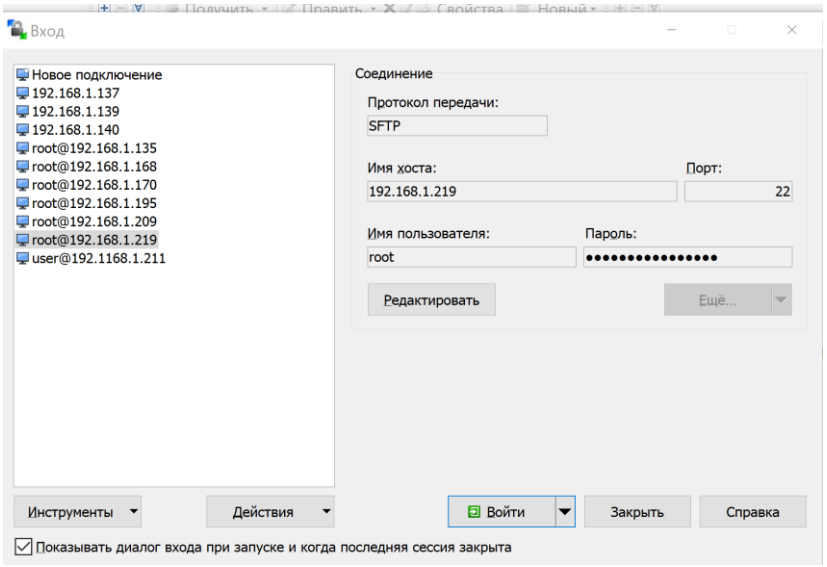


Для этого на машину с доменом установите WinSCP, а также скопируйте необходимые файлы.

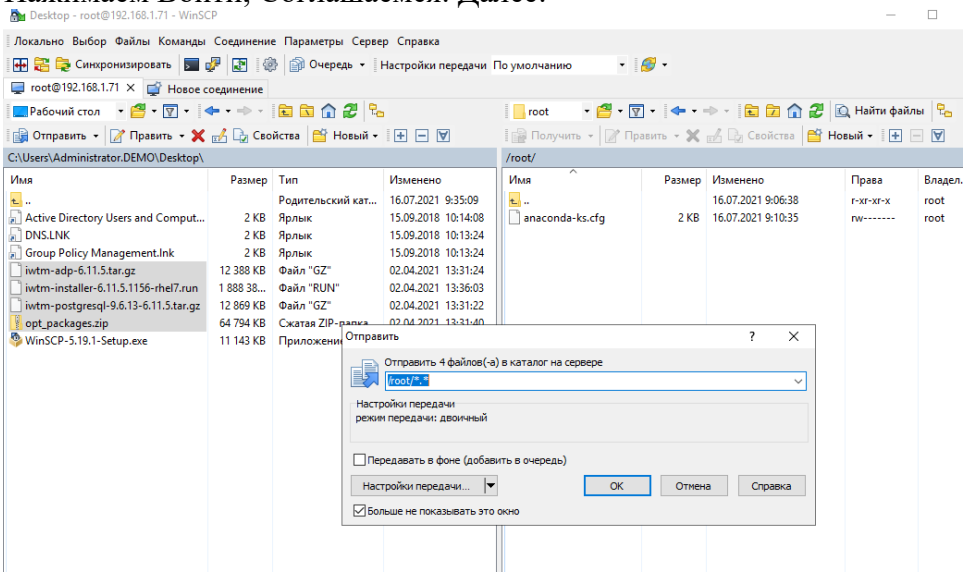
11. Запустить WinSCP и задать параметры подключения:

Имя хоста – Ip-адрес вашей машины с Centos;

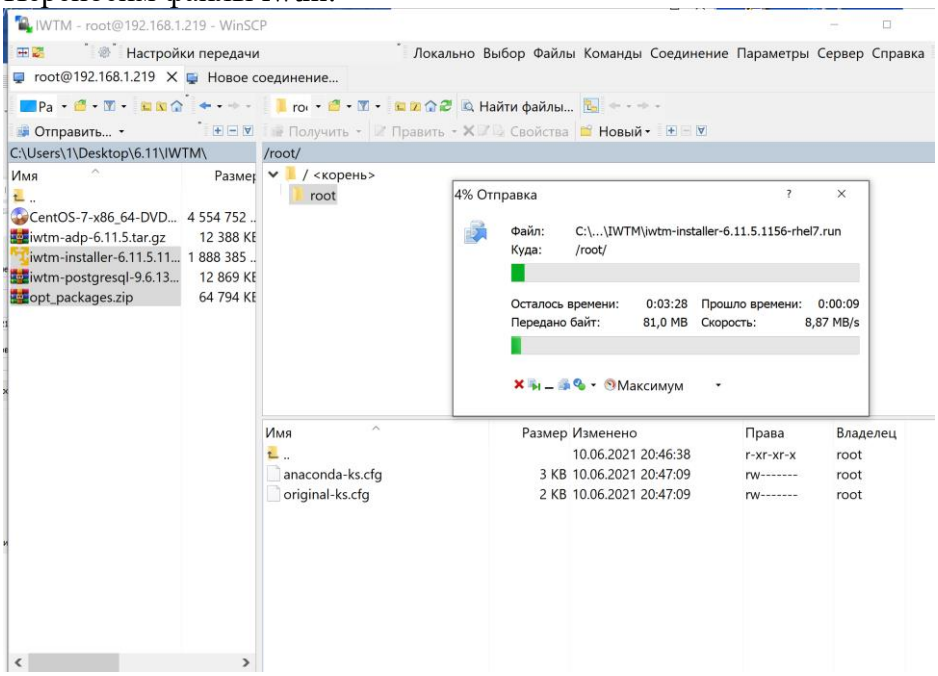
Пароль – пароль root на вашей машине с Centos.



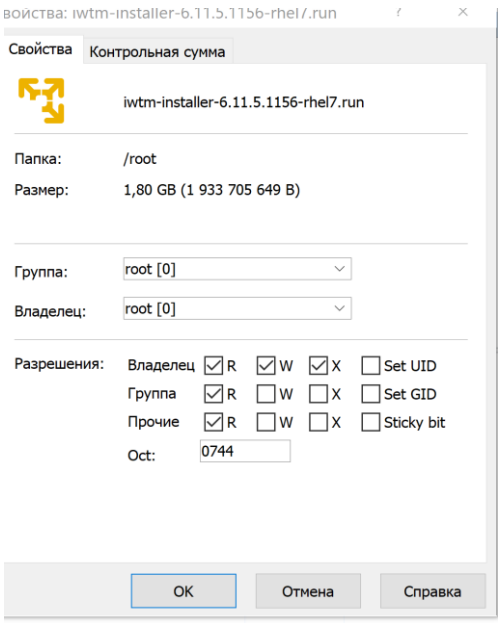
Нажимаем Войти, Соглашаемся. Далее:



Переносим файлы iwtm:



12. Необходимо изменить права файла iwtm-installer-6.11.5.1156-rhel7.run (добавить исполнение). Можно сделать через свойства файла или команда chmode



или

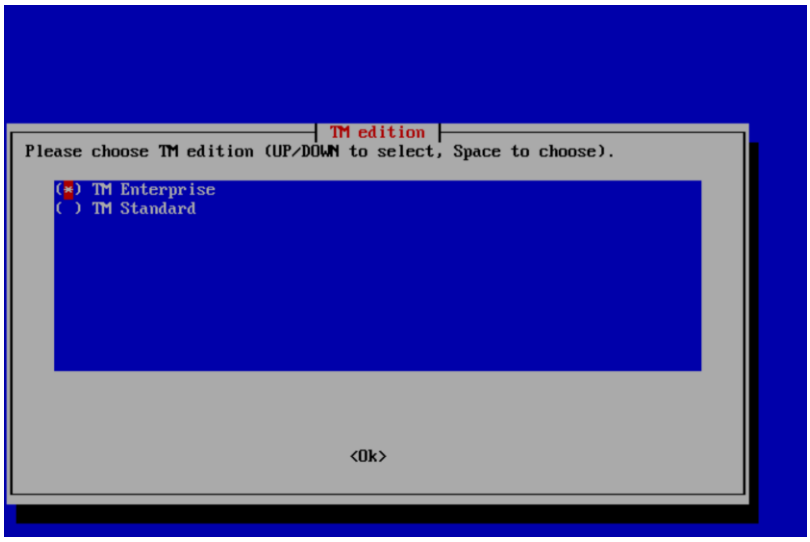
```
[root@iwtm ~]# chmod +x iwtm-installer-6.11.5.1156-rhel7.run
```

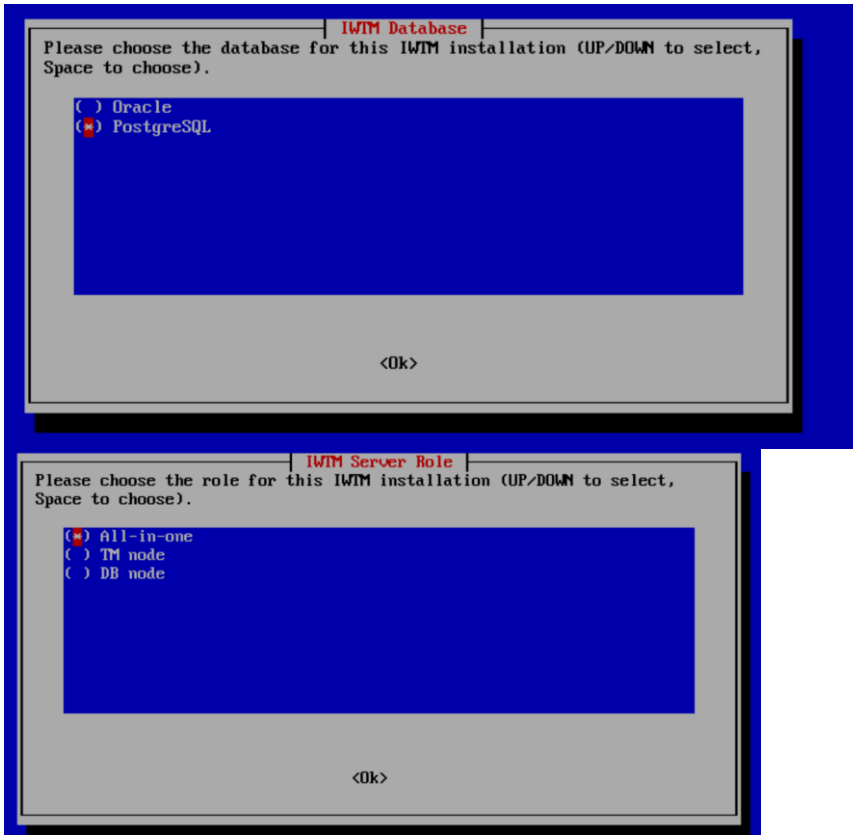
13. Запускаем установку:

```
anaconda-ks.cfg  iwtm-adp-6.11.5.tar.gz  iwtm-installer-6.11.5.1156-rhel7.run
[root@iwtm ~]# ./iwtm-installer-6.11.5.1156-rhel7.run
Verifying archive integrity...
```

Для запуска установки достаточно набрать ./iw а далее нажать клавишу Tab. Таким образом выберется нужный вам файл.

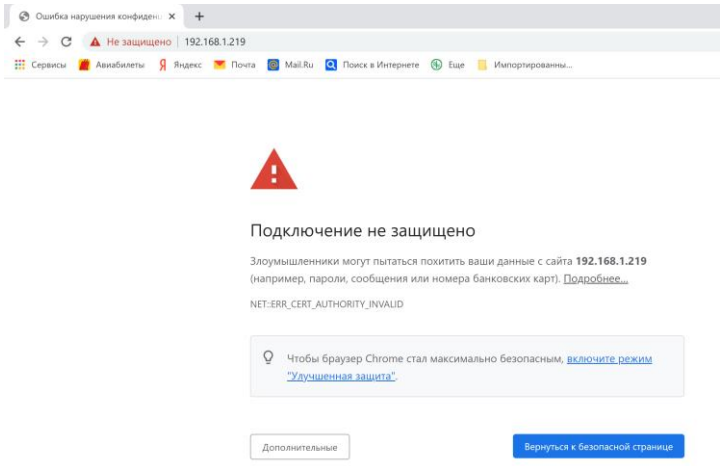
14. Выбираем:





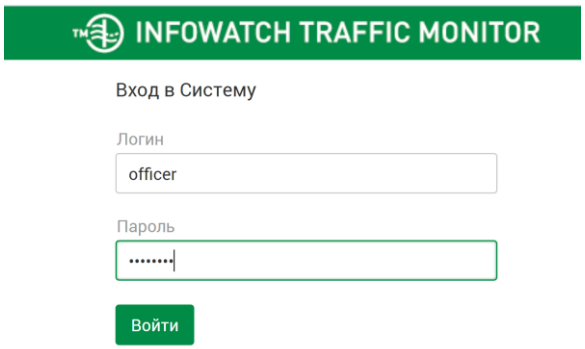
Далее все по умолчанию.

15. После установки в браузере пишем ip адрес iwtm



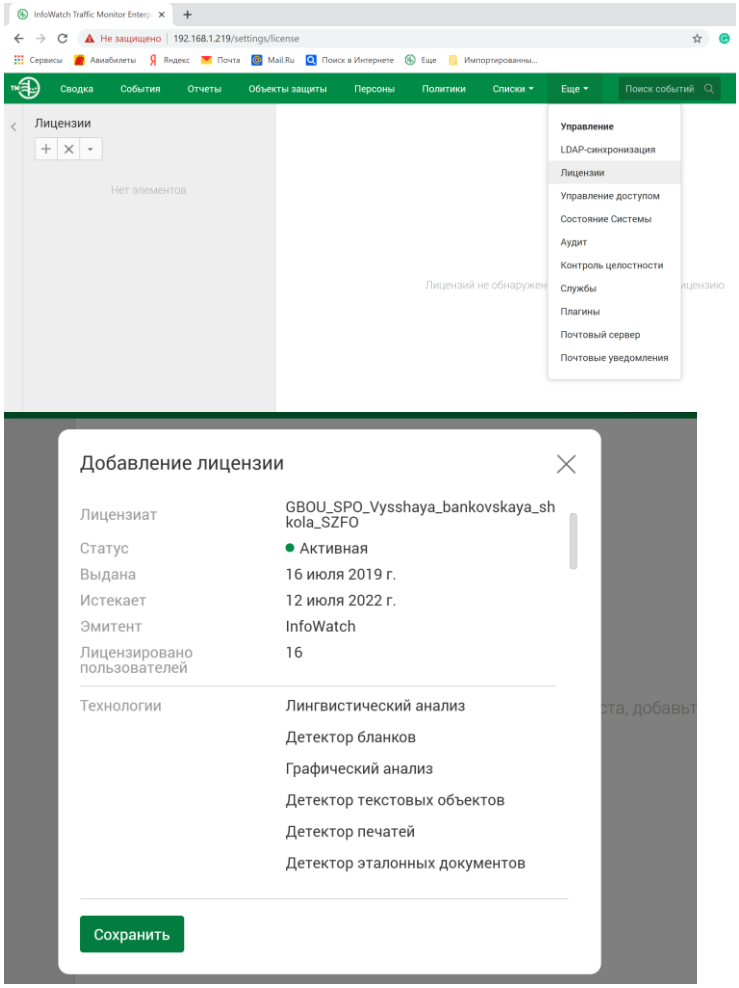
Нажимаем дополнительно далее выбираем перейти

16. Логин officer Пароль xxXX1234



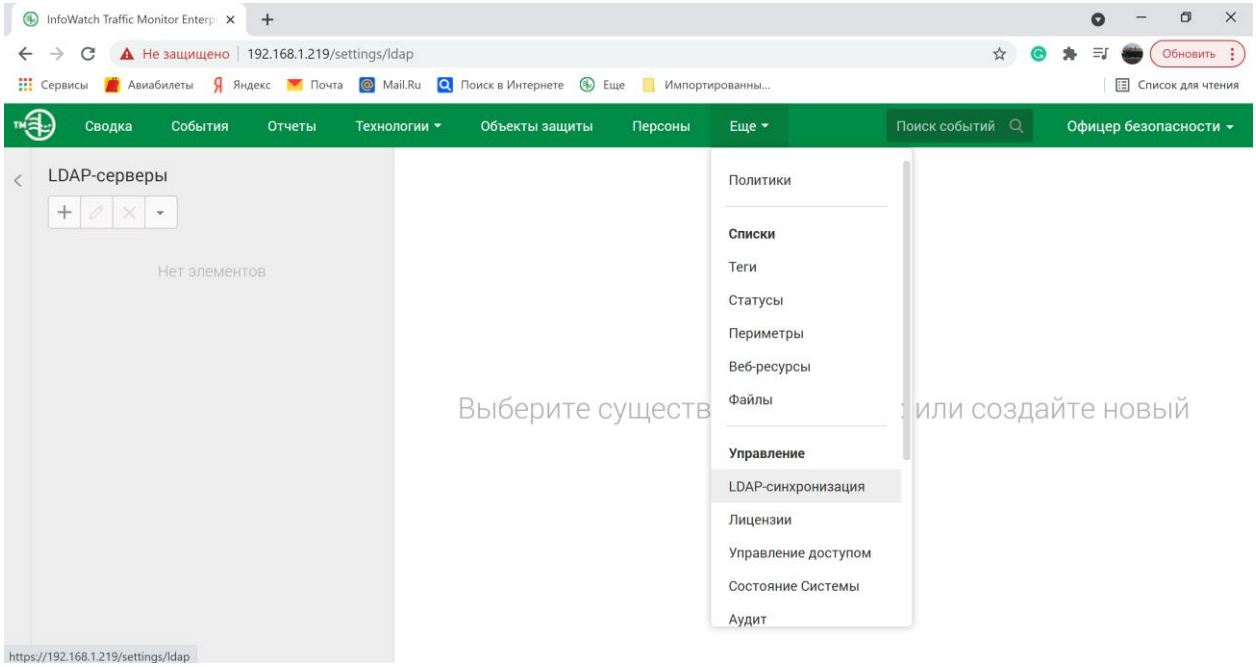
В отчёт вставить скриншот с удачным входом.

17. Далее нужно добавить лицензию. Нажать плюс и выбрать файл с лицензией



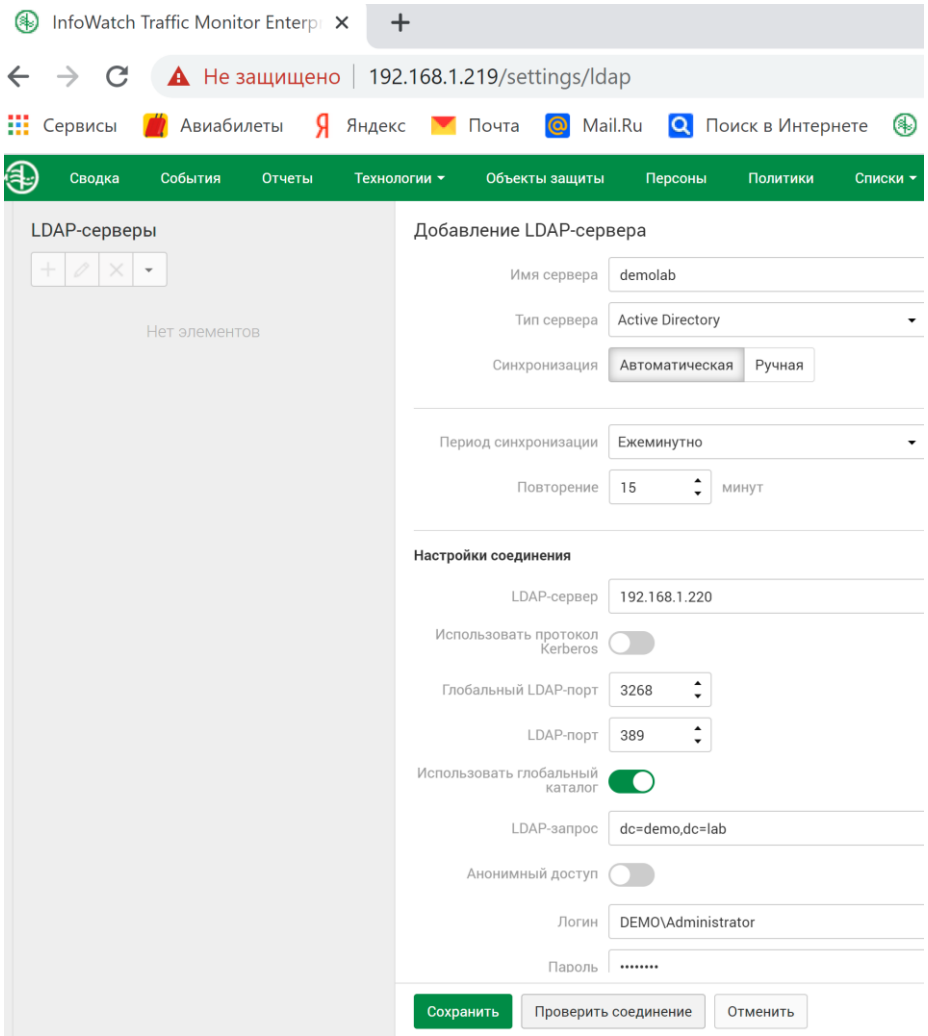
В отчёт вставить скриншот с присоединенной лицензией.

18. Для настройки необходимо выполнить LDAP-синхронизацию. Для этого заходим в Ещё→LDAP-синхронизация:



Нажимаем плюс

19. Заполняем поля для подключения к AD по умолчанию пароль xxXX1234



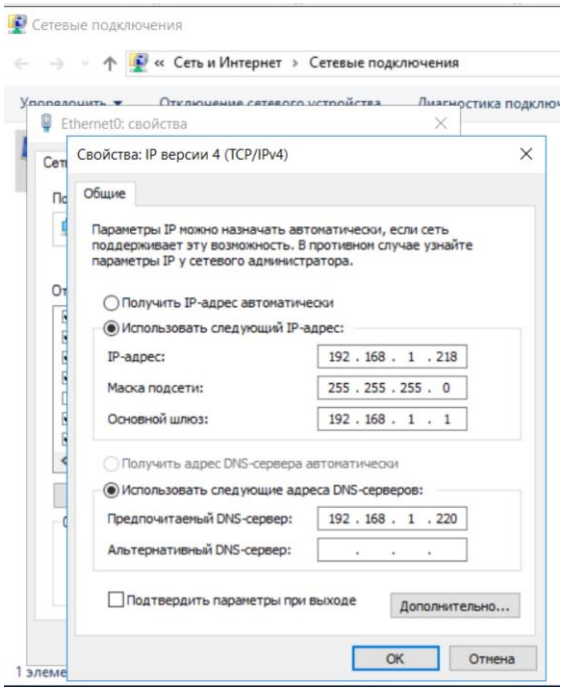
Нажимаем проверить соединение. Если успешно то сохранить.

<u>В отчёт вставить скриншот, подтверждающий удачную синхронизацию.</u>

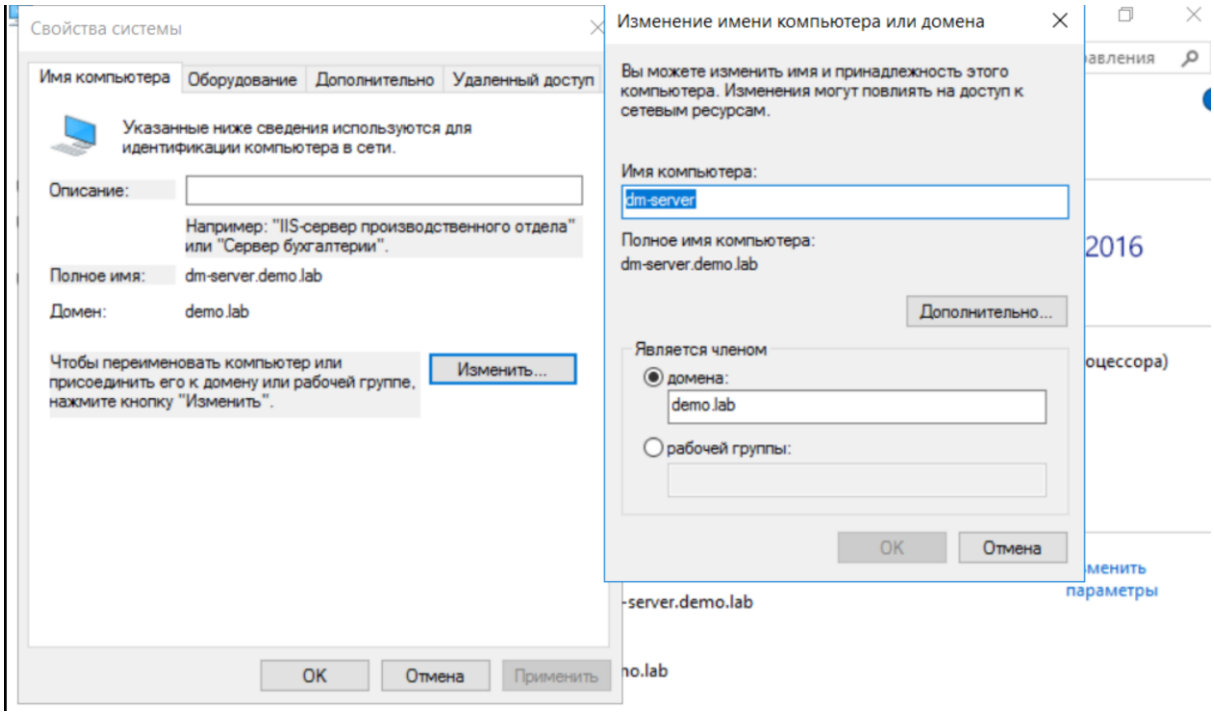
2.19. Практическая работа № 19 «Установка Infowach Device Monitor»

Задание:

1. Установить windows server 2016
2. Настроить сеть. Указать в качестве DNS-сервера адрес вашего домена.

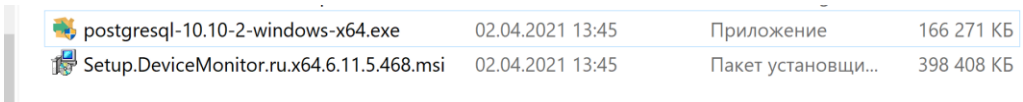


3. Добавить сервер в домен

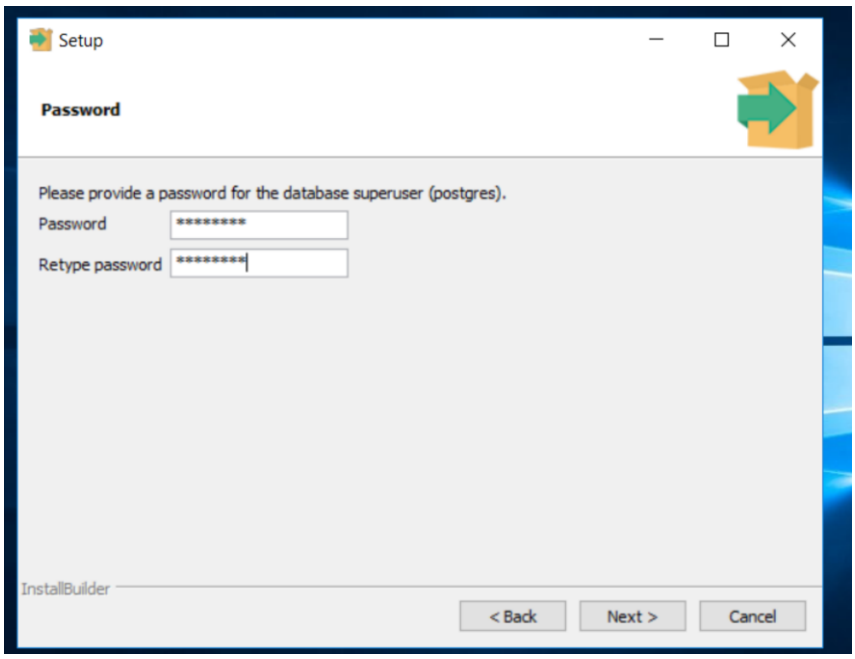


Выполнить перезагрузку системы. Войти под доменным пользователем.

4. Скопировать следующие файлы на вашу машину:



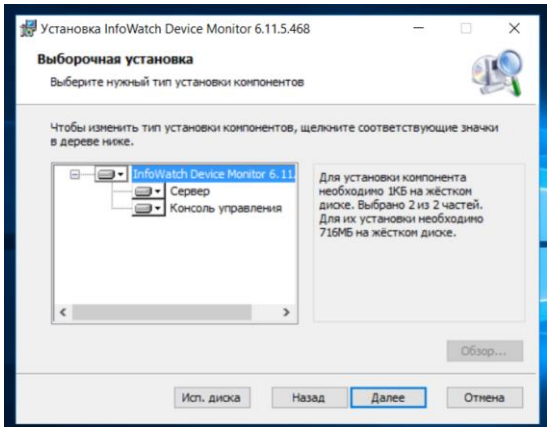
5. Установить базу данных



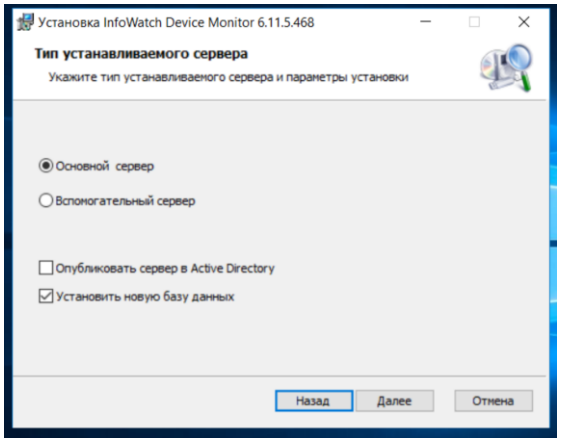
Запомнить пароль.

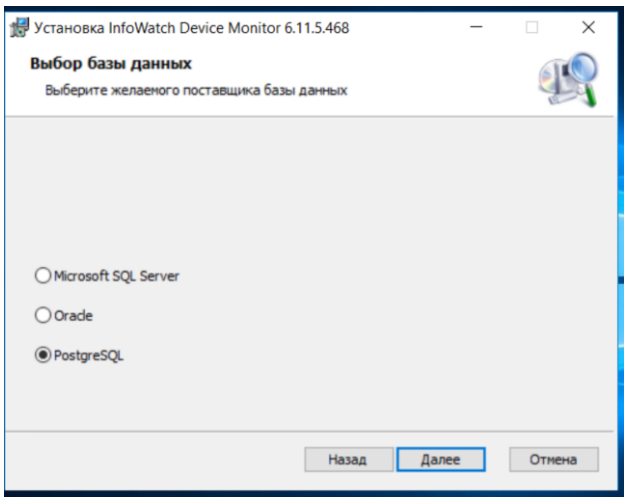
6. Запустить: 

7. Выбрать далее

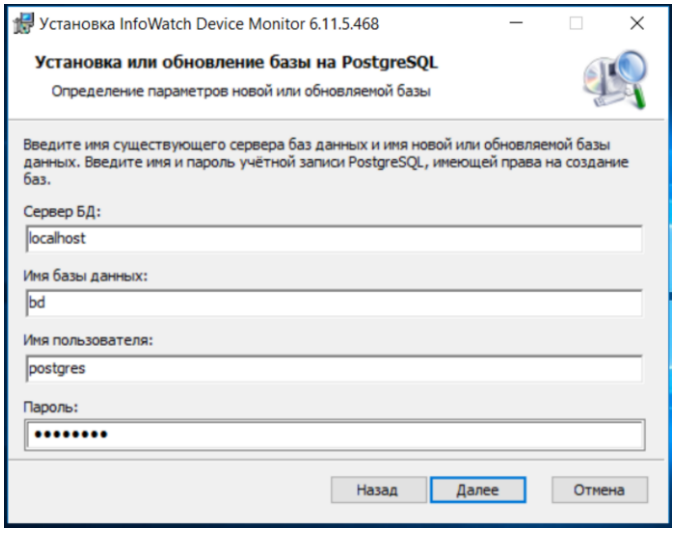


8. Выбрать

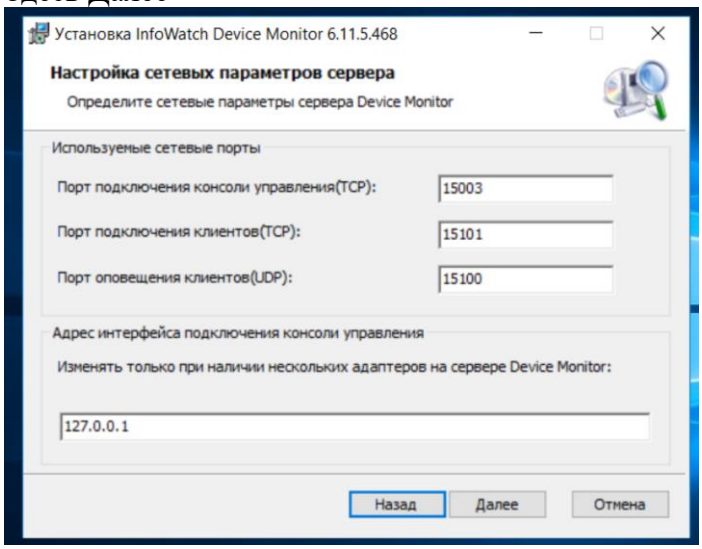




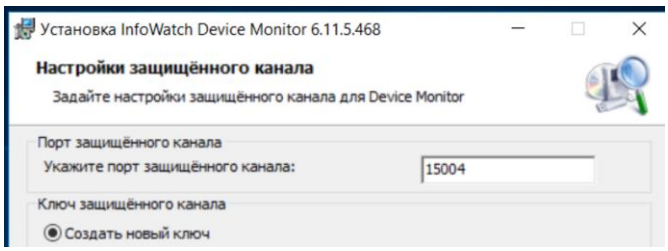
9. Задать данные для соединения с базой данных (пароль из пункта 5)



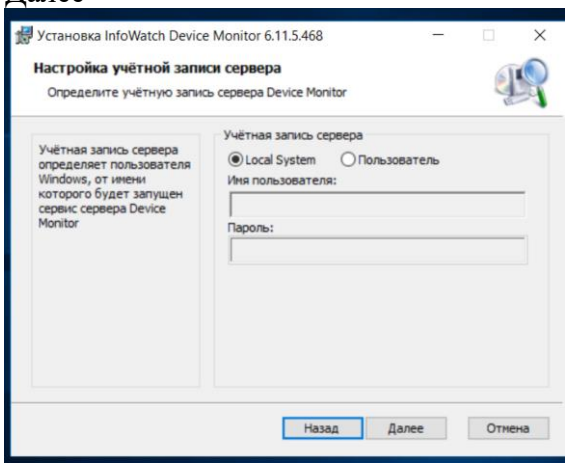
Здесь Далее



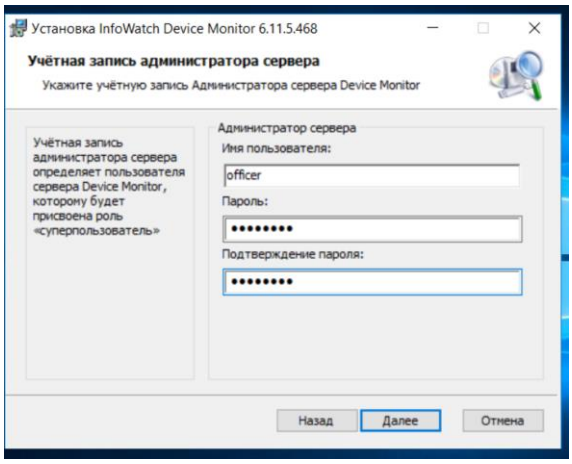
10. Создать ключ и сохранить



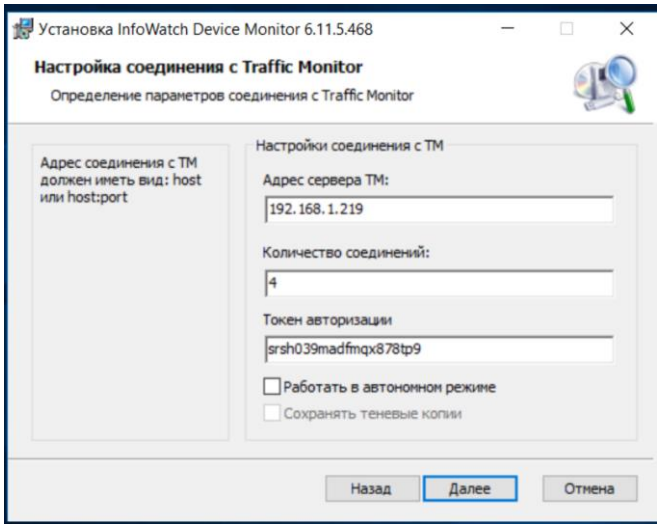
Далее



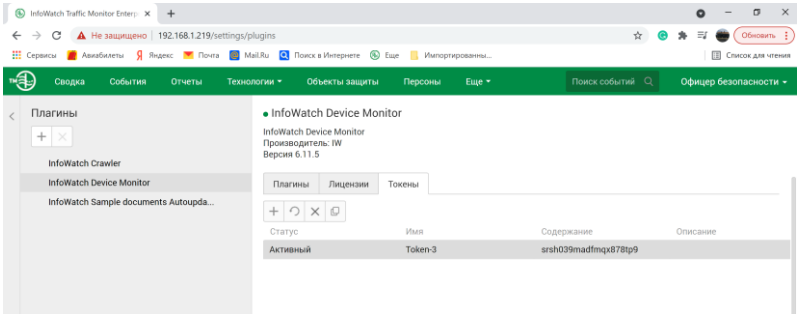
11. Задать пользователя и пароль



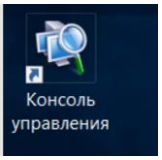
12. Задать адрес и токен:



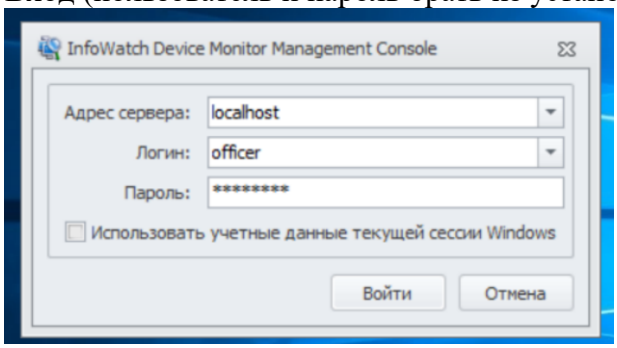
Токен находиться в веб интерфейсе iwtm Вкладка плагины:



Далее устанавливаем.

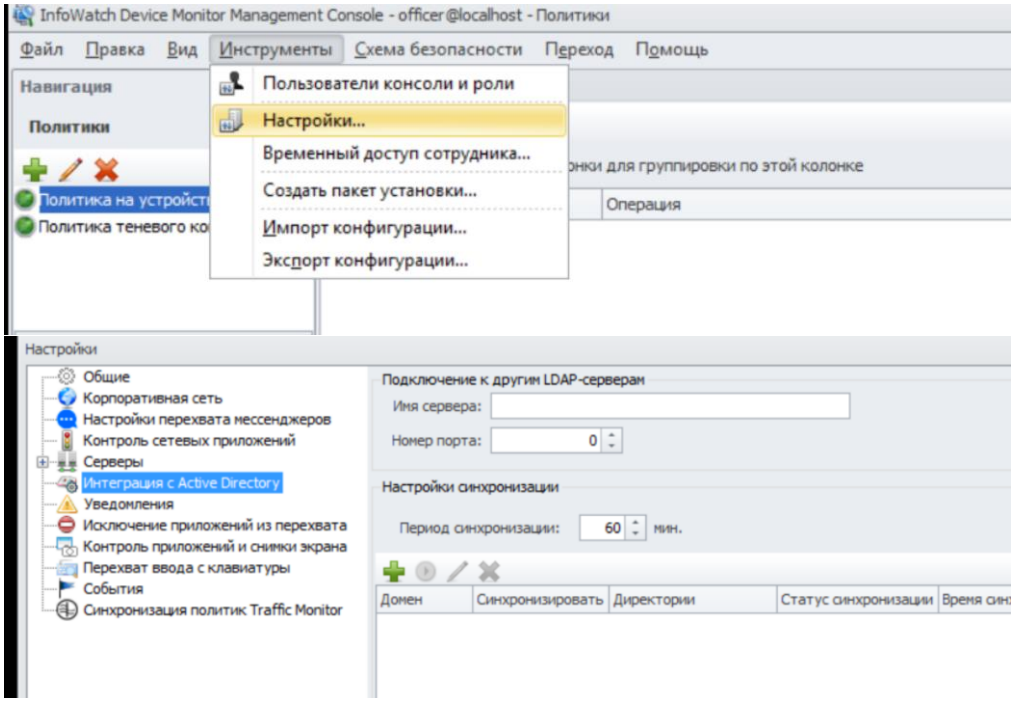
13. После установки заходим в Консоль управления. 

Вход (пользователь и пароль брать из установки iwdm):

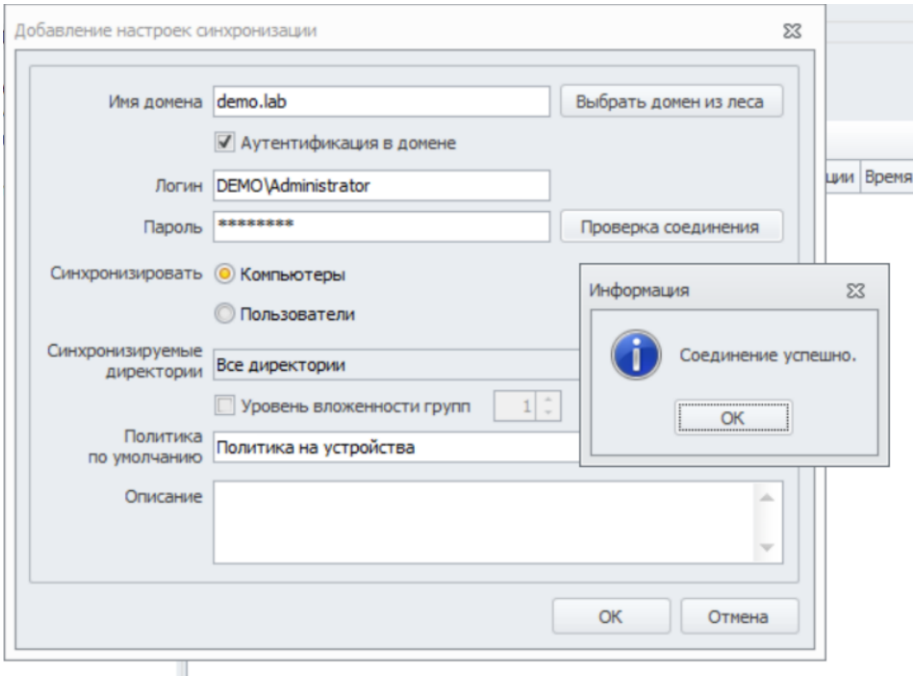


Вставляем в отчёт скриншот Консоли управления с удачным входом в неё.

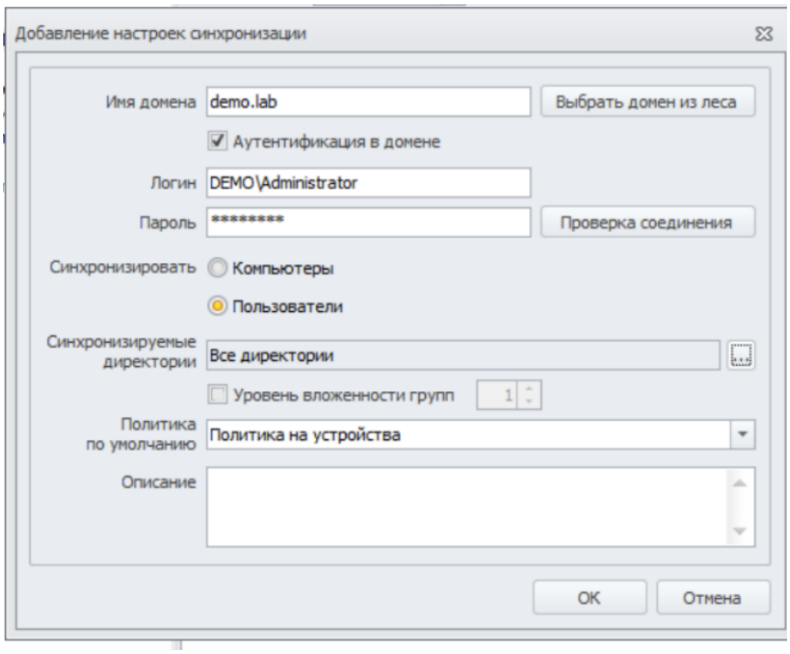
14. Далее требуется настроить консоль управления. Инструменты → Настройки:



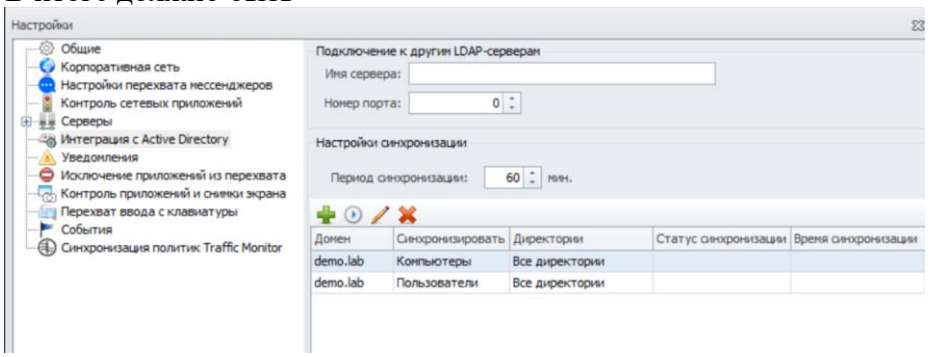
15. Задаем параметры соединения с AD



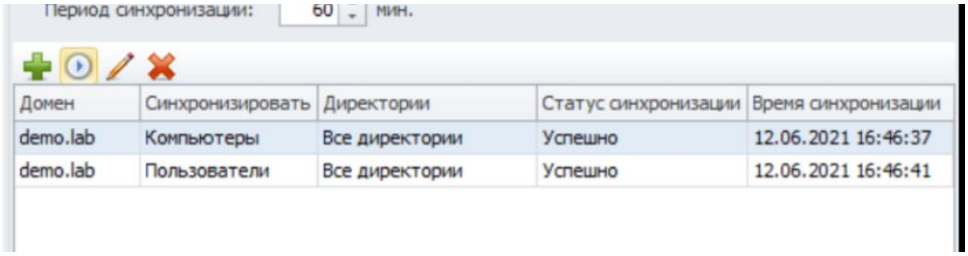
16. Создать синхронизацию пользователей



В итоге должно быть



17. Сохранить и выполнить синхронизацию

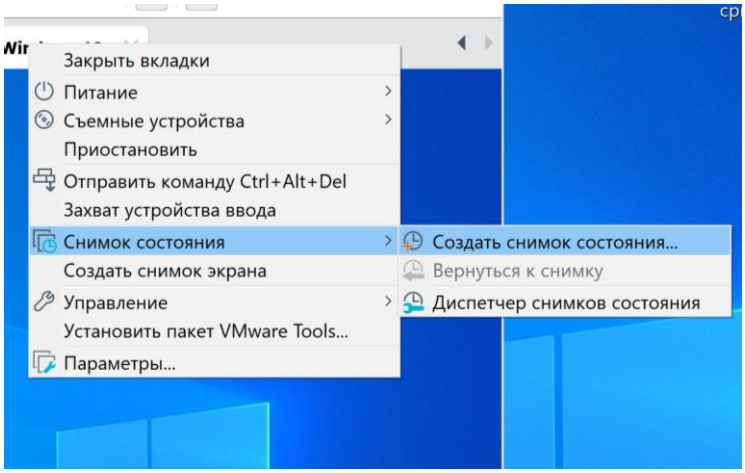


В отчёт вставить скриншоты с выполненной синхронизацией.
Проверить синхронизацию политик ТМ. Вставить скриншот с удачной синхронизацией.

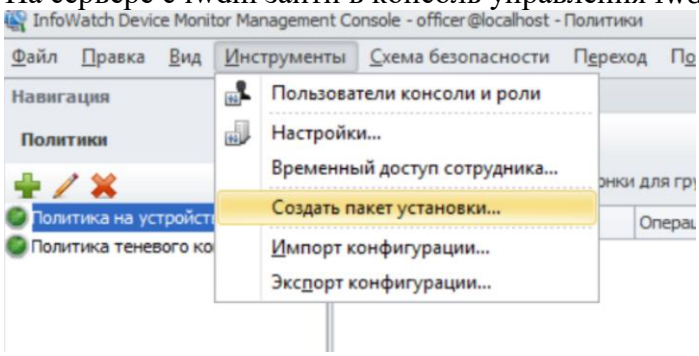
Практическая работа № 20 «Установка клиента Infowach Device Monitor»

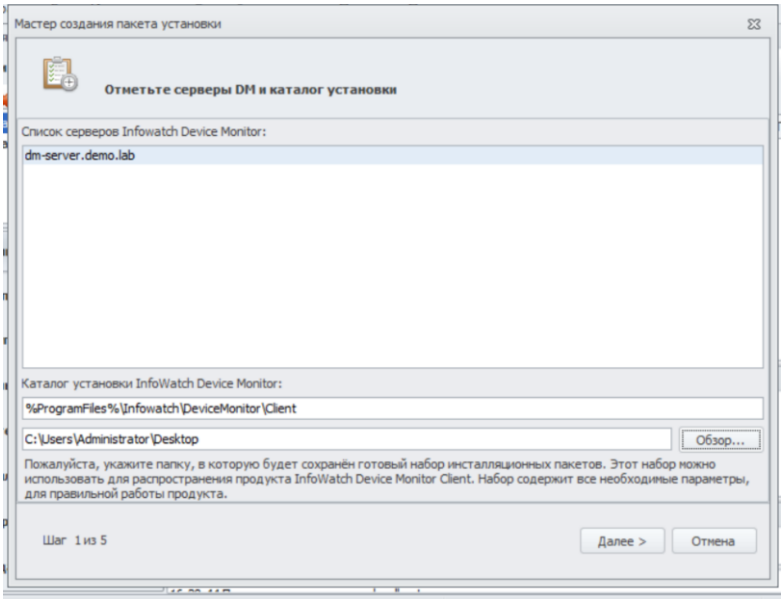
Задание:

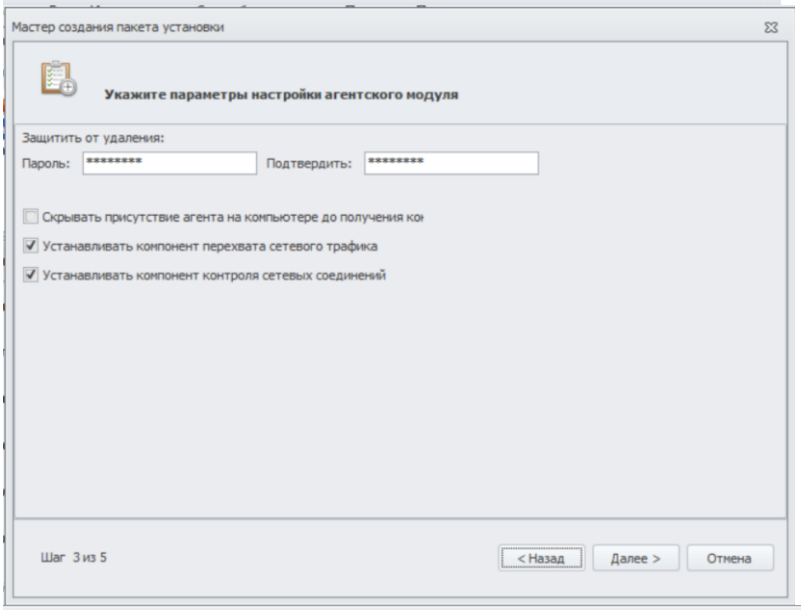
1. Предварительно должен быть установлен windows 10 с настроенной сетью и добавлен в домен
2. Сделать снимок состояния машины средствами гипервизора.

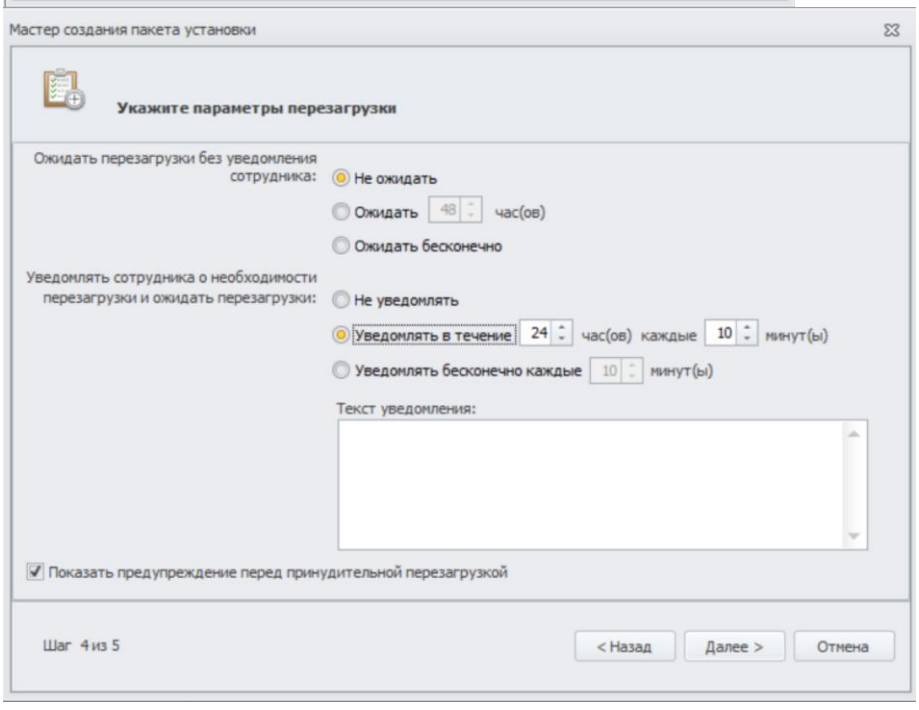


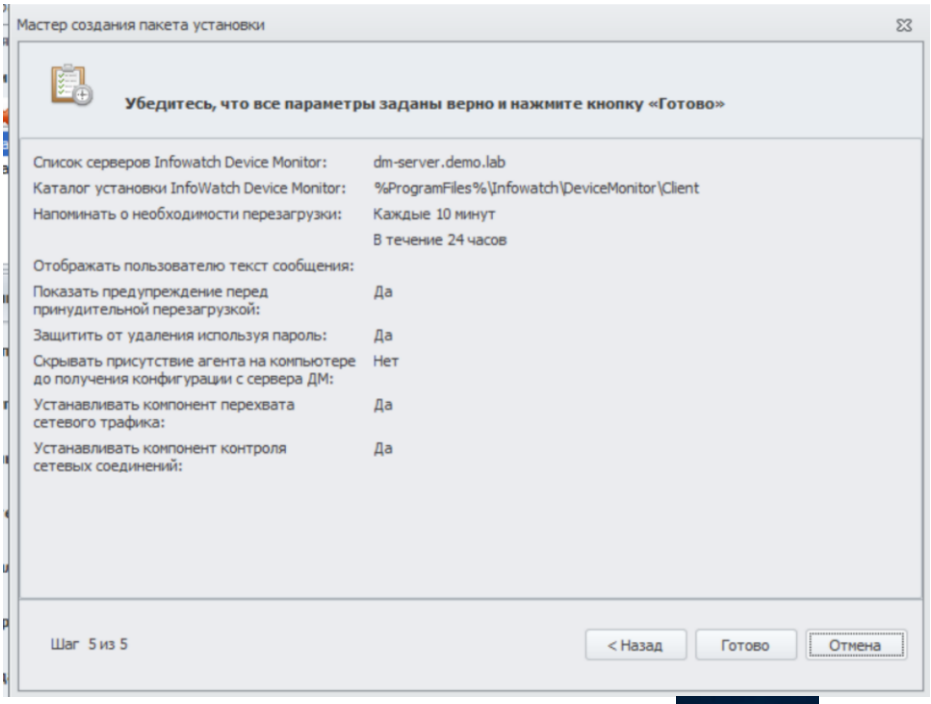
Установить клиент можно тремя способами.
Предпочтительный способ — установка через групповые политики (в отчёте должны быть скриншоты, подтверждающие подобное выполнение).
Второй по значимости способ — установка через задачу первичного распространения (в отчёте должны быть скриншоты, подтверждающие подобное выполнение).
Самый простой способ — установка с помощью пакета установки с последующим переносом его на машину потенциального нарушителя и установки.
Способ 1 (самый простой и в реальных боевых условиях неправильный) с помощью пакета установки
На сервере с iwdm зайти в консоль управления iwdm

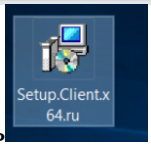



Мастер создания пакета установки
Отметьте серверы DM и каталог установки
Список серверов Infowatch Device Monitor:
dm-server.demo.lab
Каталог установки InfoWatch Device Monitor:
%ProgramFiles%\Infowatch\DeviceMonitor\Client
C:\Users\Administrator\Desktop
Обзор...
Пожалуйста, укажите папку, в которую будет сохранён готовый набор инсталляционных пакетов. Этот набор можно использовать для распространения продукта InfoWatch Device Monitor Client. Набор содержит все необходимые параметры, для правильной работы продукта.
Шаг 1 из 5
Далее >
Отмена

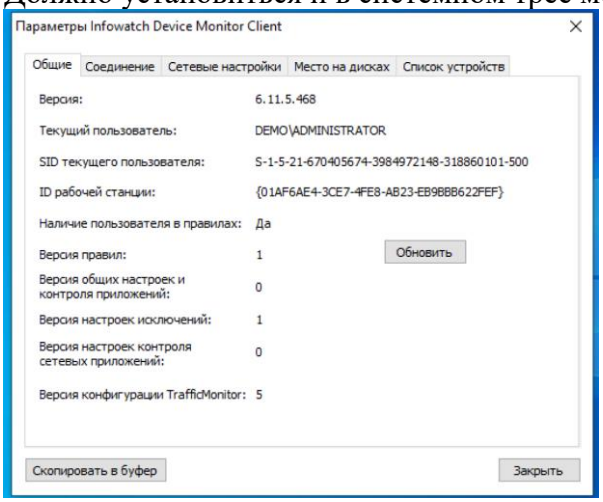

Мастер создания пакета установки
Укажите параметры настройки агентского модуля
Защитить от удаления:
Пароль:
****
Подтвердить:
****
Скрывать присутствие агента на компьютере до получения ко
Устанавливать компонент перехвата сетевого трафика
Устанавливать компонент контроля сетевых соединений
Шаг 3 из 5
< Назад
Далее >
Отмена


Мастер создания пакета установки
Укажите параметры перезагрузки
Ожидать перезагрузки без уведомления сотрудника:
Не ожидать
Ожидать
48
час(ов)
Ожидать бесконечно
Уведомлять сотрудника о необходимости перезагрузки и ожидать перезагрузки:
Не уведомлять
Уведомлять в течение
24
час(ов) каждые
10
минут(ы)
Уведомлять бесконечно каждые
10
минут(ы)
Текст уведомления:
Показать предупреждение перед принудительной перезагрузкой
Шаг 4 из 5
< Назад
Далее >
Отмена



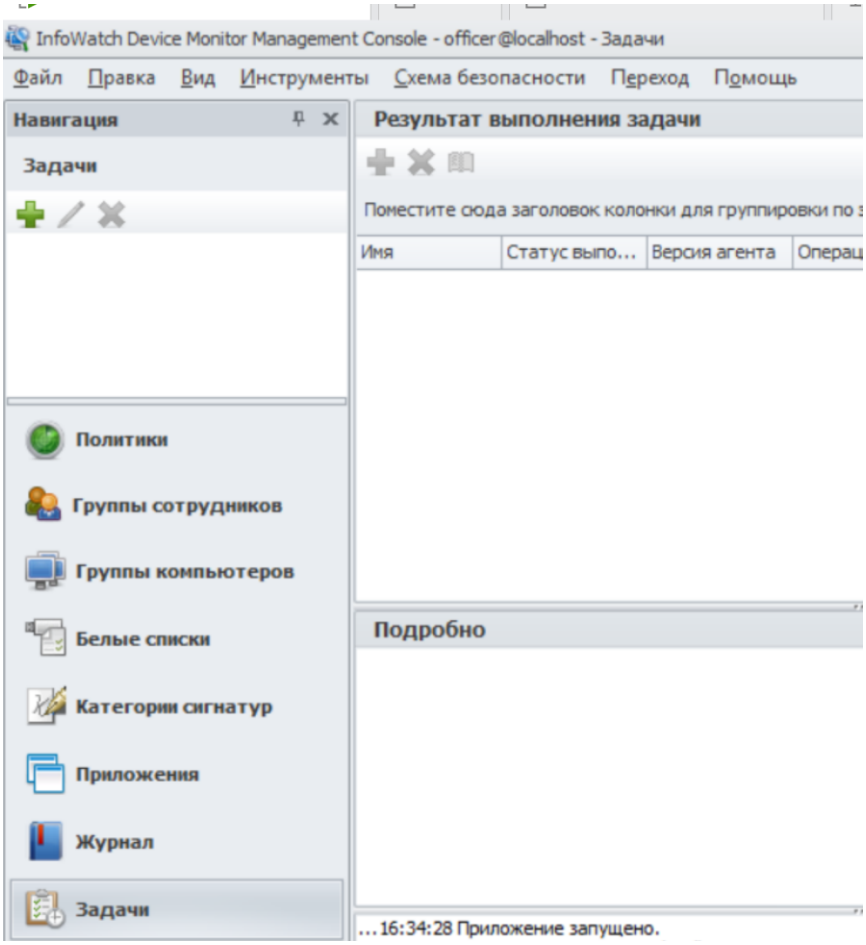
Скопировать на машину нарушитель и запустить 

Должно установиться и в системном трее можете увидеть:

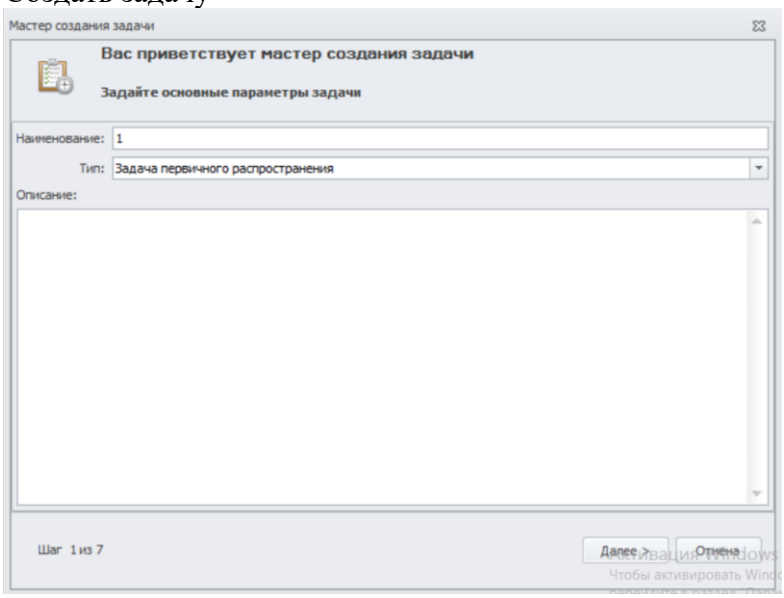


Способ 2 — установка через задачу первичного распространения

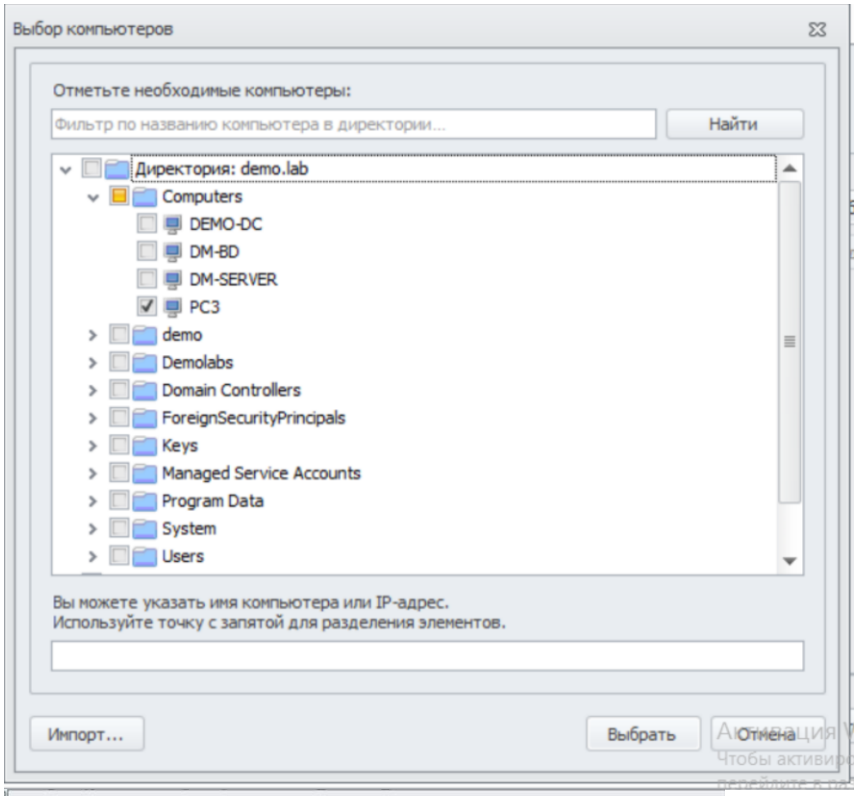
В консоле управления iwdm выбрать Задачи:

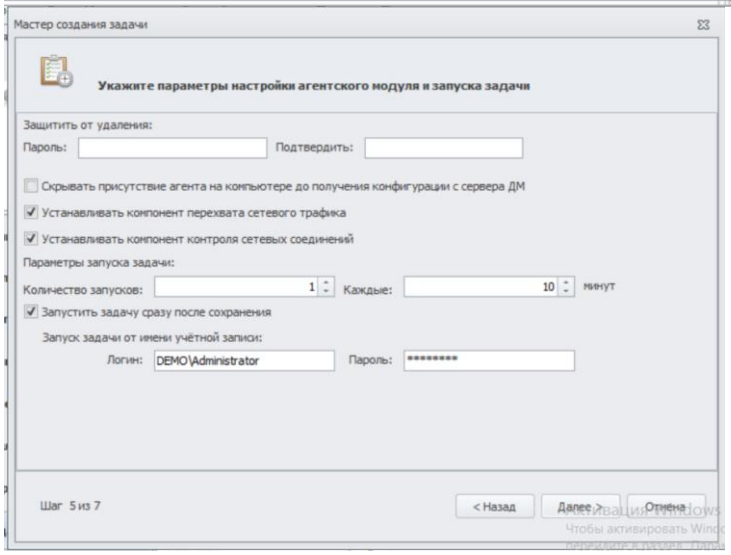


Создать задачу

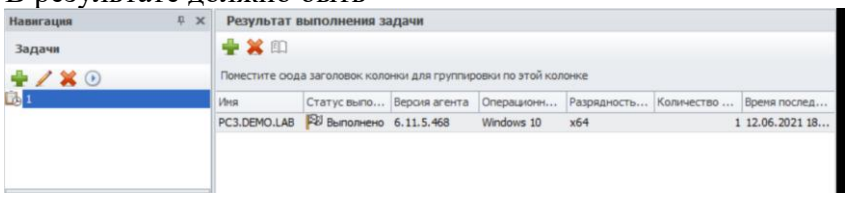


Добавить нужный пк

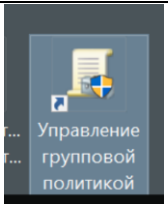




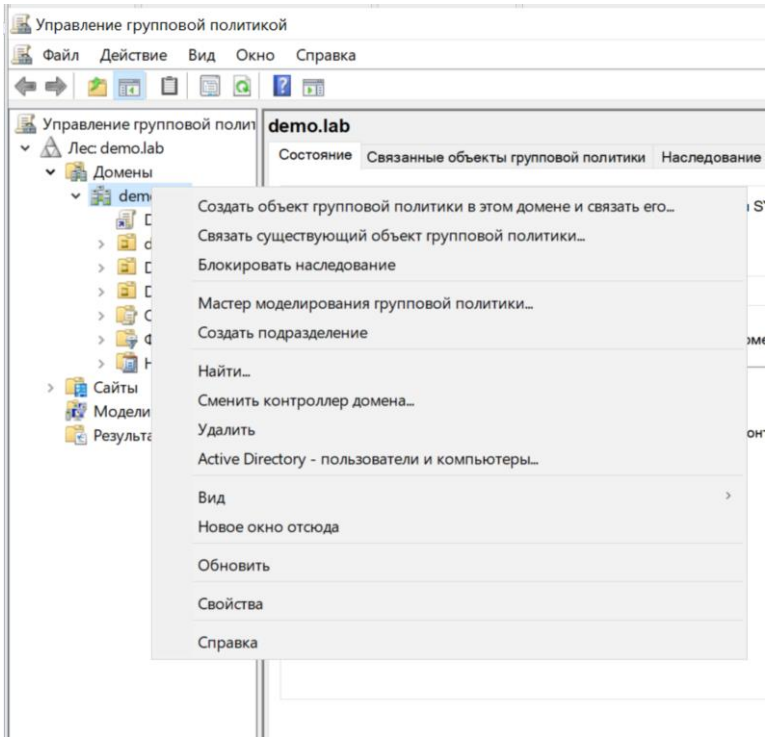
В результате должно быть



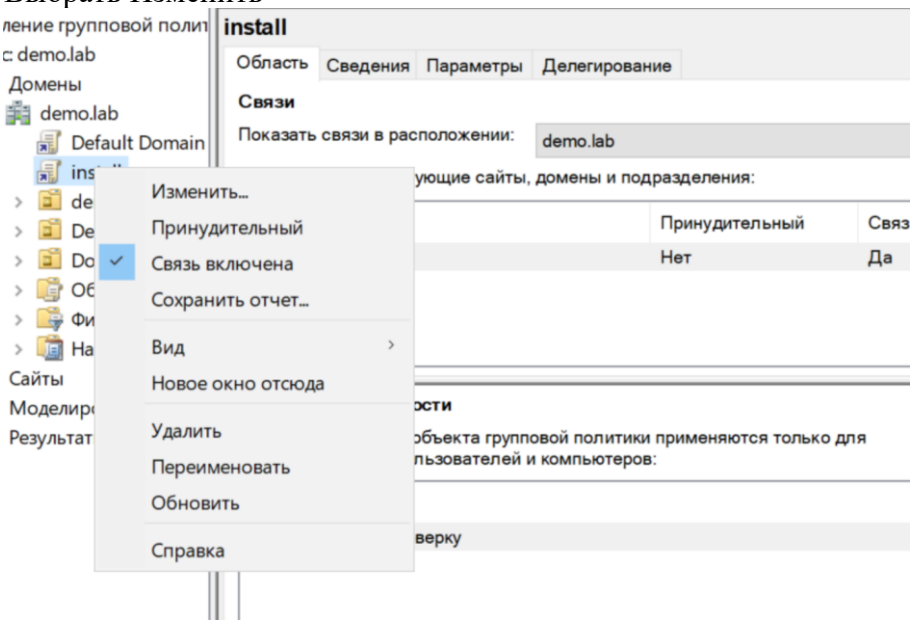
Способ 3 установка через политики AD

На сервере с AD Зайти в 

Выбрать Создать объект групповой политики в этом домене и связать его:

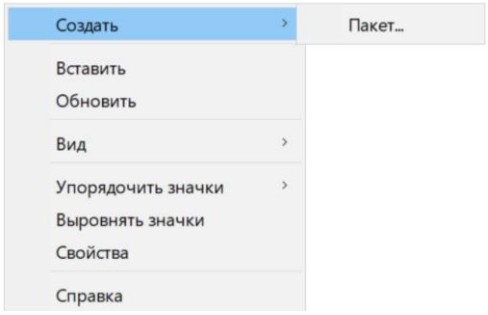


Выбрать Изменить

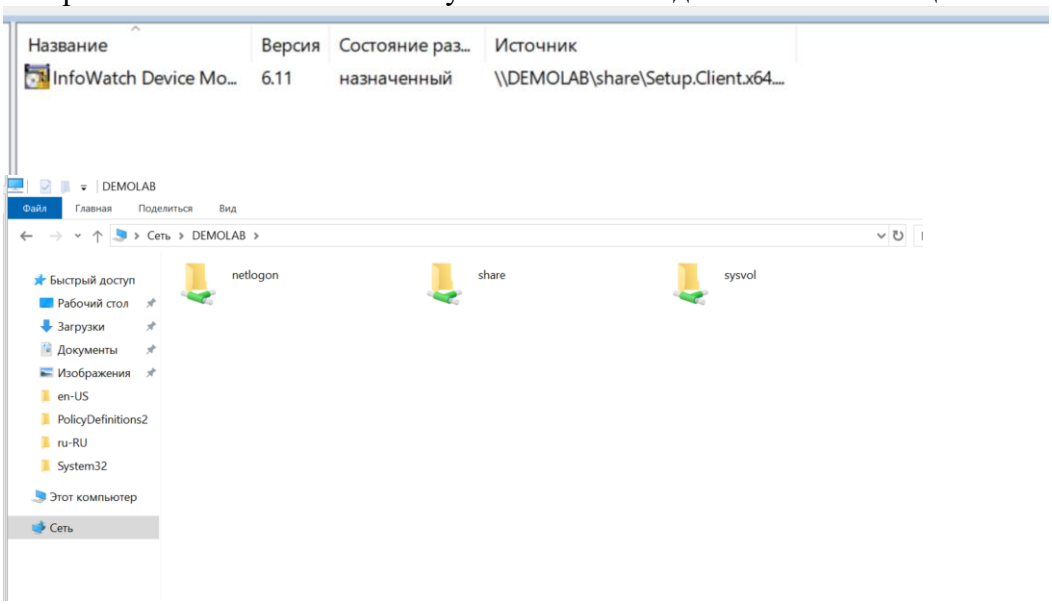


Перейти в

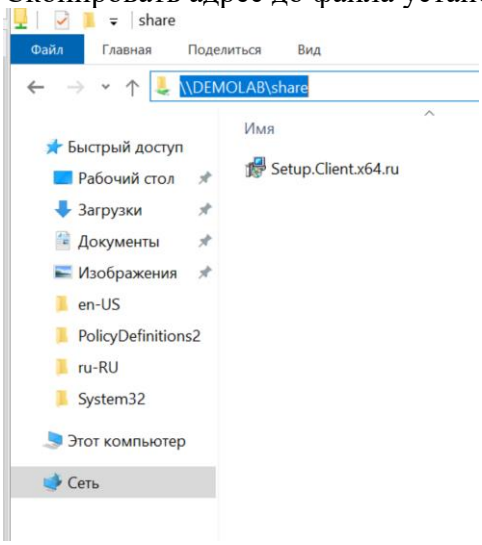
Создать пакет



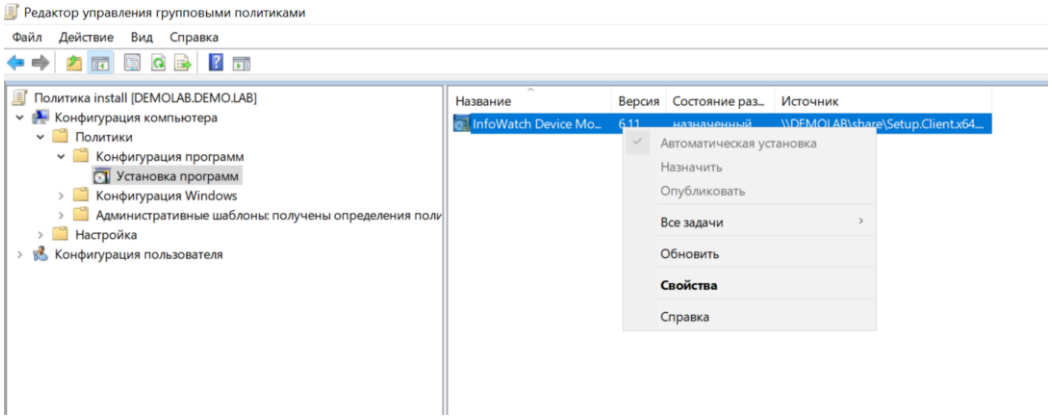
Выбрать msi пакет из 1 способа установки Файл должен быть в общей папке



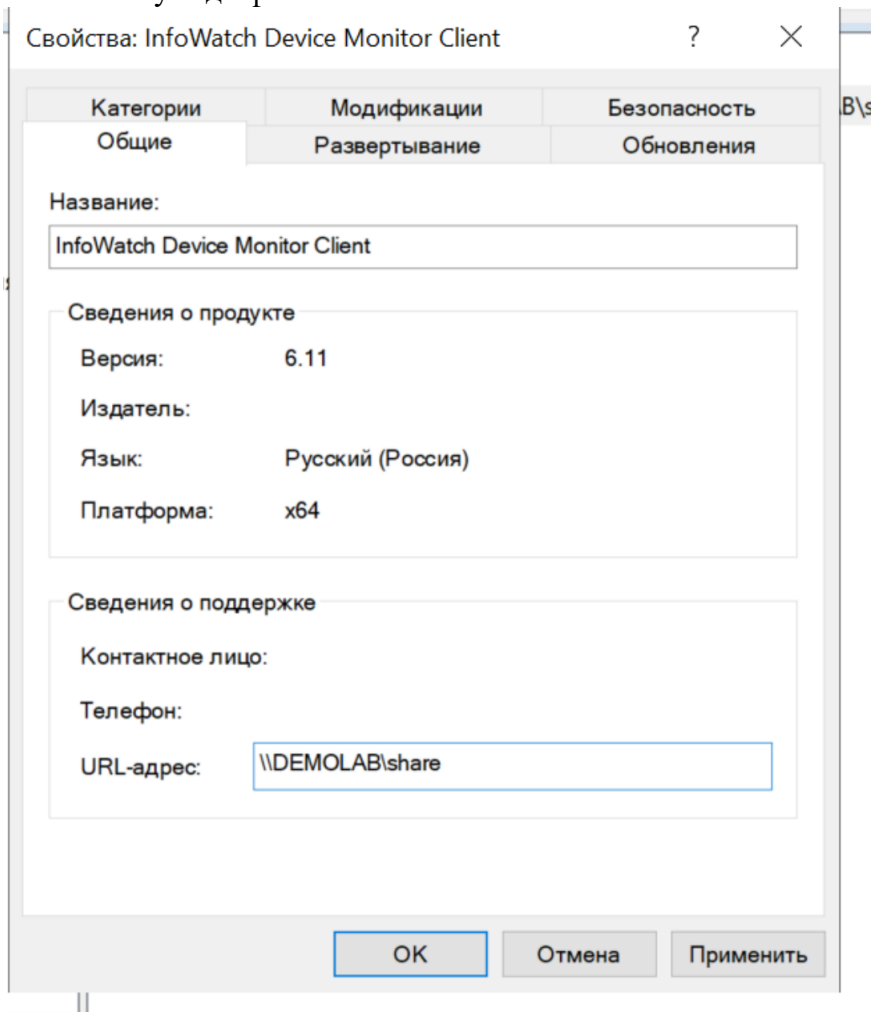
Скопировать адрес до файла установки



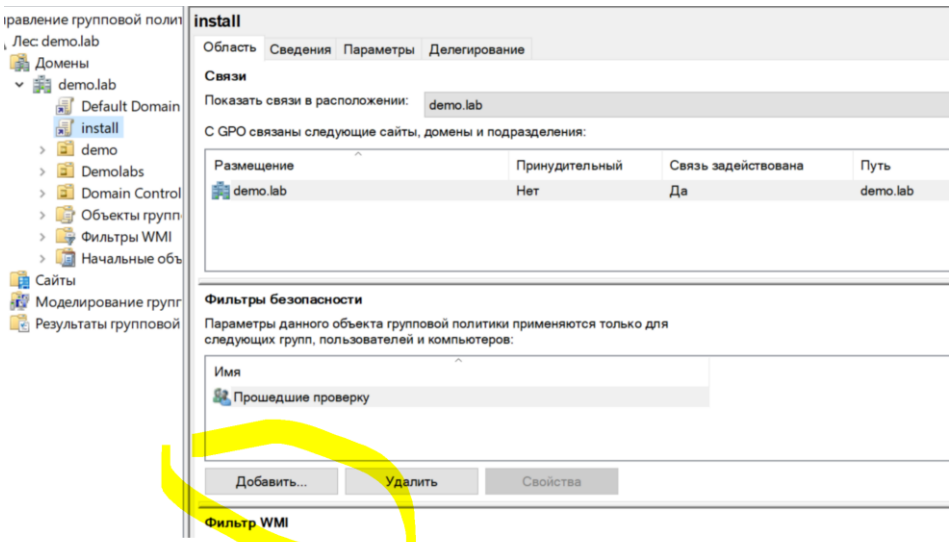
Зайти в свойства пакета

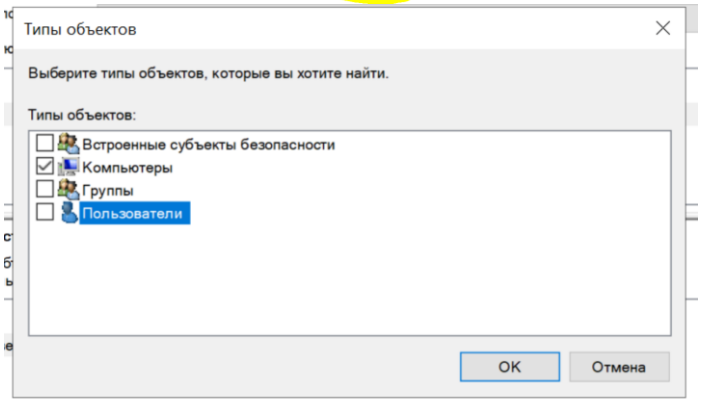


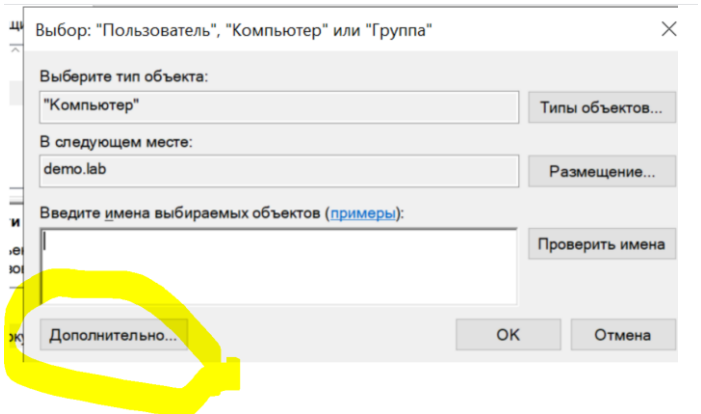
Вставить путь до файла

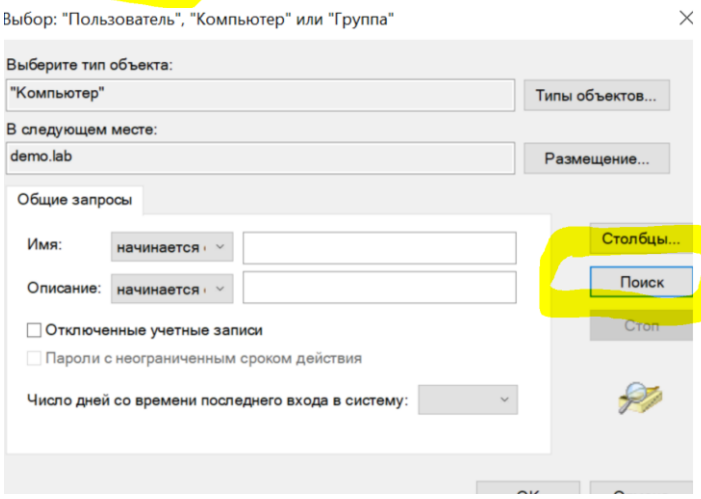


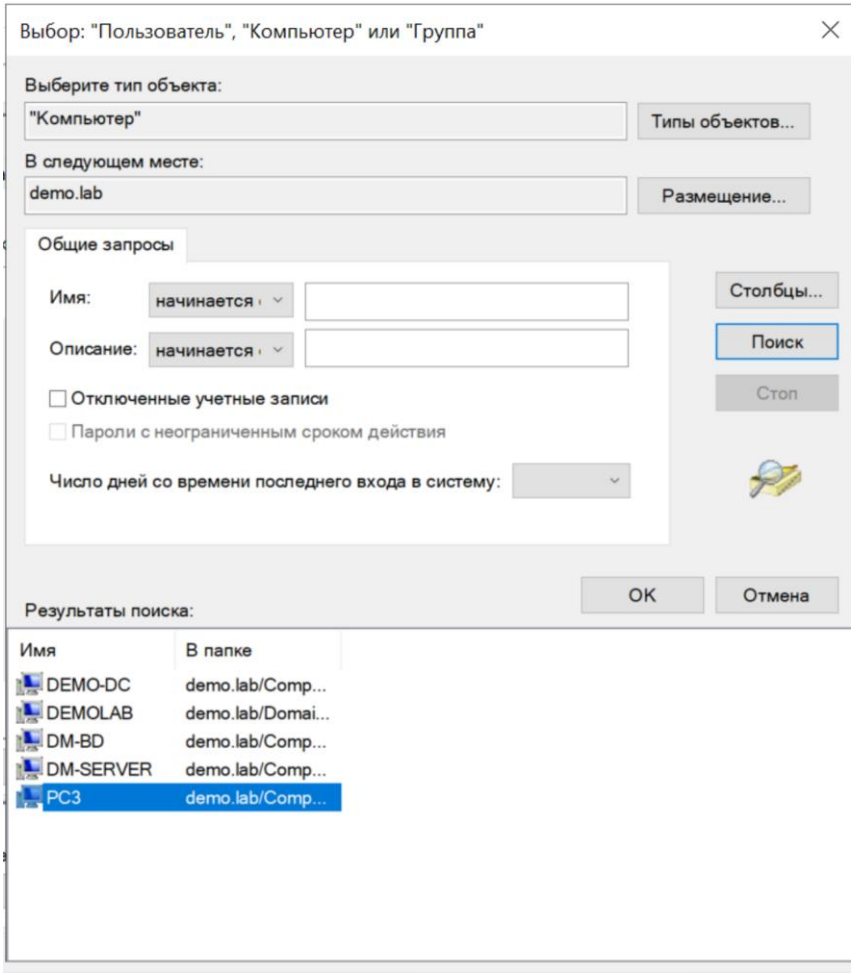
Выйти из редактирования политики, добавить компьютер, на который будет распространять-ся политика

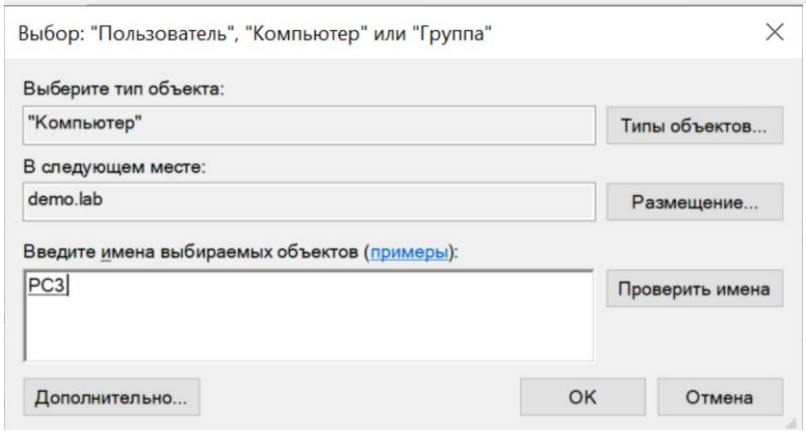

install
Область
Сведения
Параметры
Делегирование
Связи
Показать связи в расположении:
demo.lab
С GPO связаны следующие сайты, домены и подразделения:
Размещение
Принудительный
Связь задействована
Путь
demo.lab
Нет
Да
demo.lab
Фильтры безопасности
Параметры данного объекта групповой политики применяются только для следующих групп, пользователей и компьютеров:
Имя
Прошедшие проверку
Добавить...
Удалить
Свойства
Фильтр WMI


Типы объектов
Выберите типы объектов, которые вы хотите найти.
Типы объектов:
Встроенные субъекты безопасности
Компьютеры
Группы
Пользователи
OK
Отмена

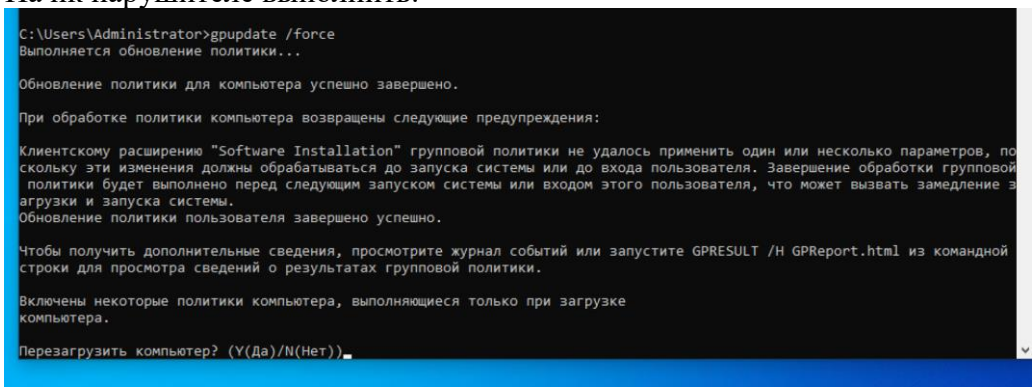

Выбор: "Пользователь", "Компьютер" или "Группа"
Выберите тип объекта:
"Компьютер"
Типы объектов...
В следующем месте:
demo.lab
Размещение...
Введите имена выбираемых объектов (примеры):
Проверить имена
Дополнительно...
OK
Отмена


Выбор: "Пользователь", "Компьютер" или "Группа"
Выберите тип объекта:
"Компьютер"
Типы объектов...
В следующем месте:
demo.lab
Размещение...
Общие запросы
Имя:
начинается
Описание:
начинается
Столбцы...
Поиск
Стоп
Отключенные учетные записи
Пароли с неограниченным сроком действия
Число дней со времени последнего входа в систему:

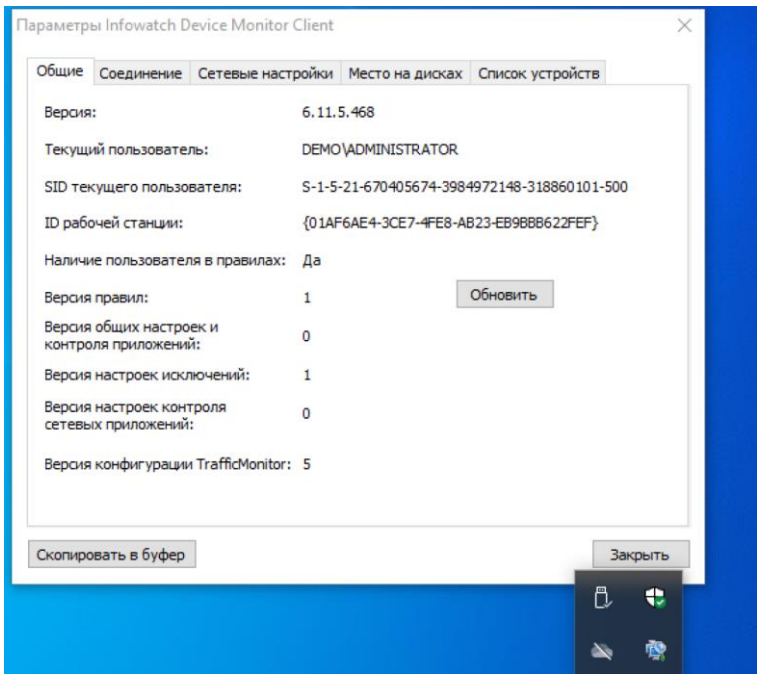




На пк нарушителе выполнить:



Итогом будет

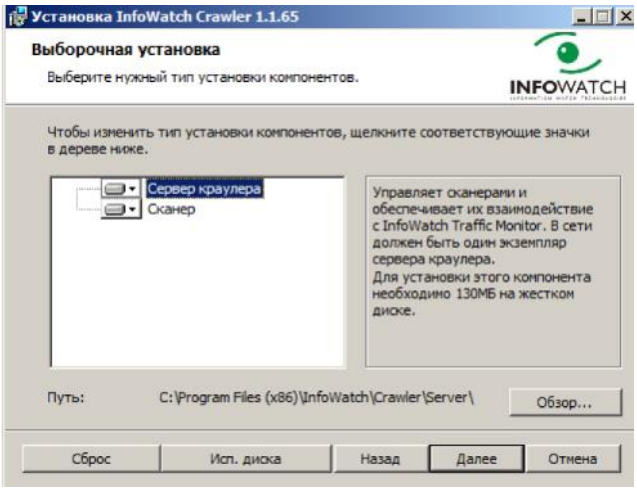


В отчёт вставить скриншоты, подтверждающие выбранный вами способ установки, а также скриншоты, подтверждающие успешную установку клиента DM.

Практическая работа № 21 «Установка и настройка Crawler»

Задание:

Установить InfoWatch.Crawler на компьютер с Консолью управления Device Monitor.
Пояснение:
Перехватчик Краулер реализован в виде двух служб Windows:
✓ InfoWatch.Crawler.Scanner – выполняет сканирование сетевых папок и файловых хранилищ согласно заданным пользователем параметрам;
✓ InfoWatch.Crawler.Server – управляет службой сканирования и обеспечивает связь с Консолью управления Traffic Monitor;
Порядок выполнения работы:
1. Чтобы установить Краулер:
Запустите установочный пакет Crawler_vx.x.xxx.msi, где x.x.xxx – номер версии.



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

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

выполните команду service iwtm restart kicker.

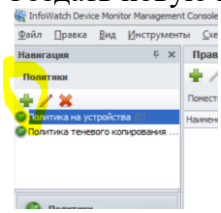
Настройте Crawler на автоматическое ежедневное сканирование только ранее созданного каталога вашего Windows Server и зафиксируйте выполнение задания скриншотом настройки crawler в web-консоли IWTM.

В отчёт вставить скриншот с удачной установкой Краулера.
В отчёт вставить скриншот, подтверждающий настройку Краулера.
В отчет вставить скриншот, подтверждающий работоспособность краулера.

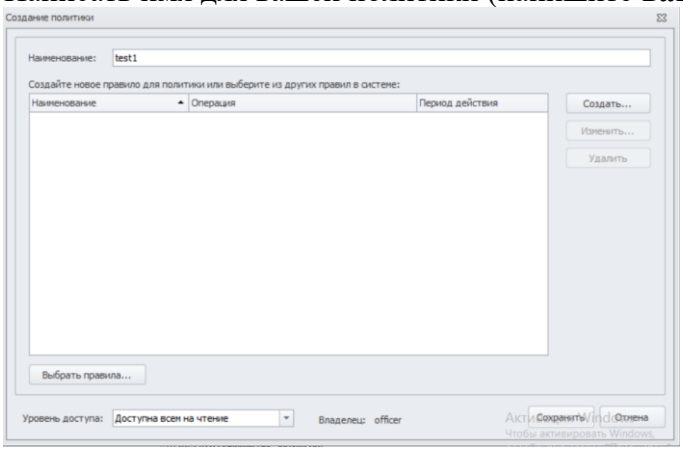
Практическая работа № 22 «Создание простых правил и проверка их работоспособности в Device monitor»

Задание:

Создать новую группу политик, нажав на знак «+»:

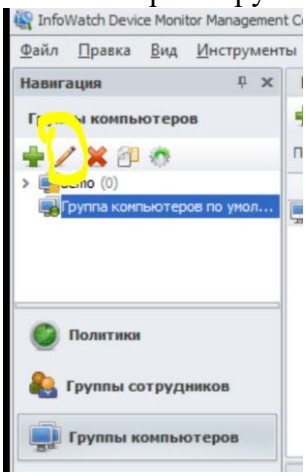


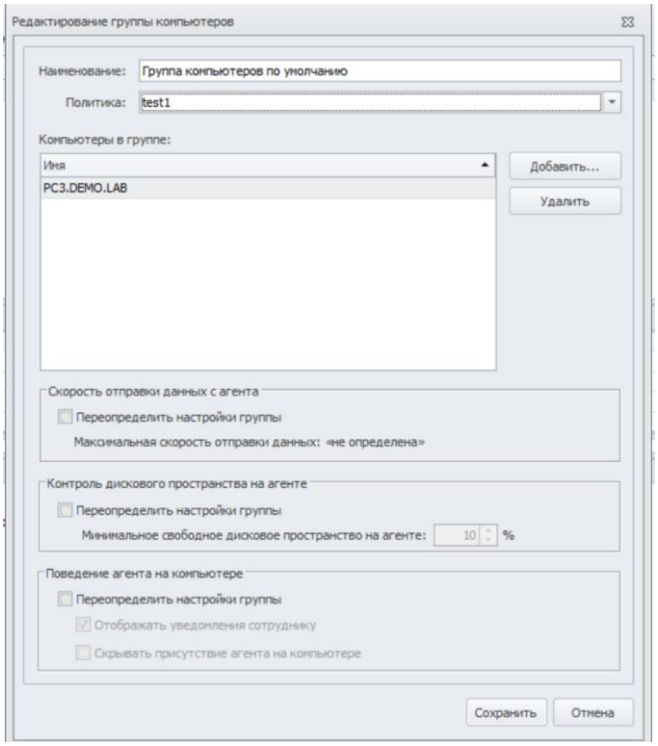
Написать имя для вашей политики (напишите **вашу фамилию**):



Далее Сохранить.

Затем Выбрать Группы компьютеров → Изменить группу компьютеров:





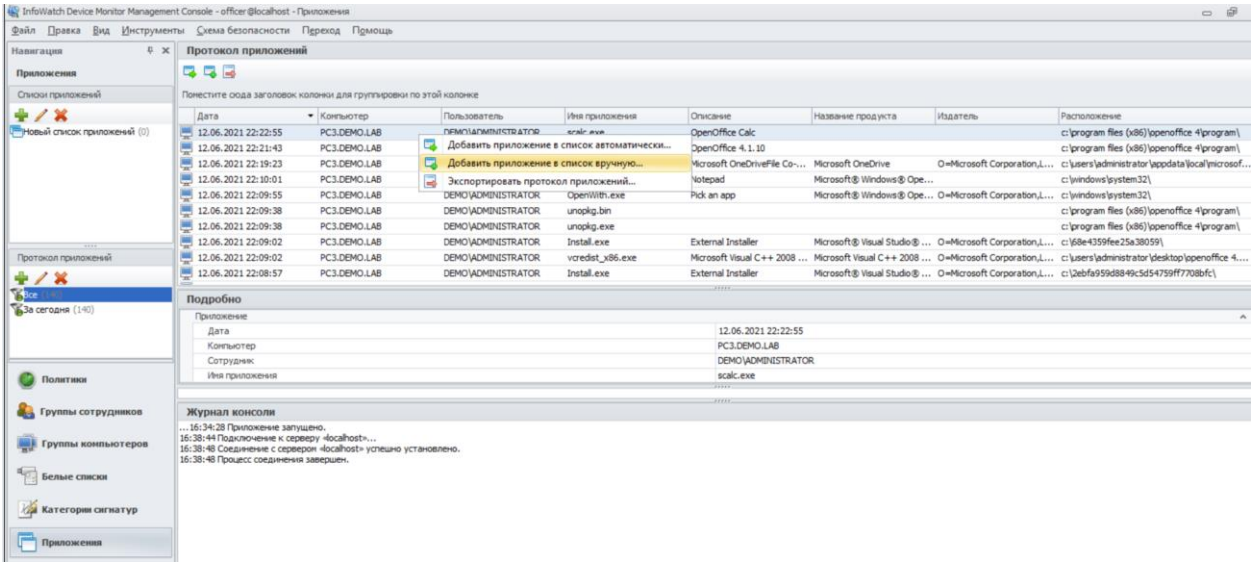
Здесь должна отображаться ваша новая политика, а также машина потенциального нарушителя.

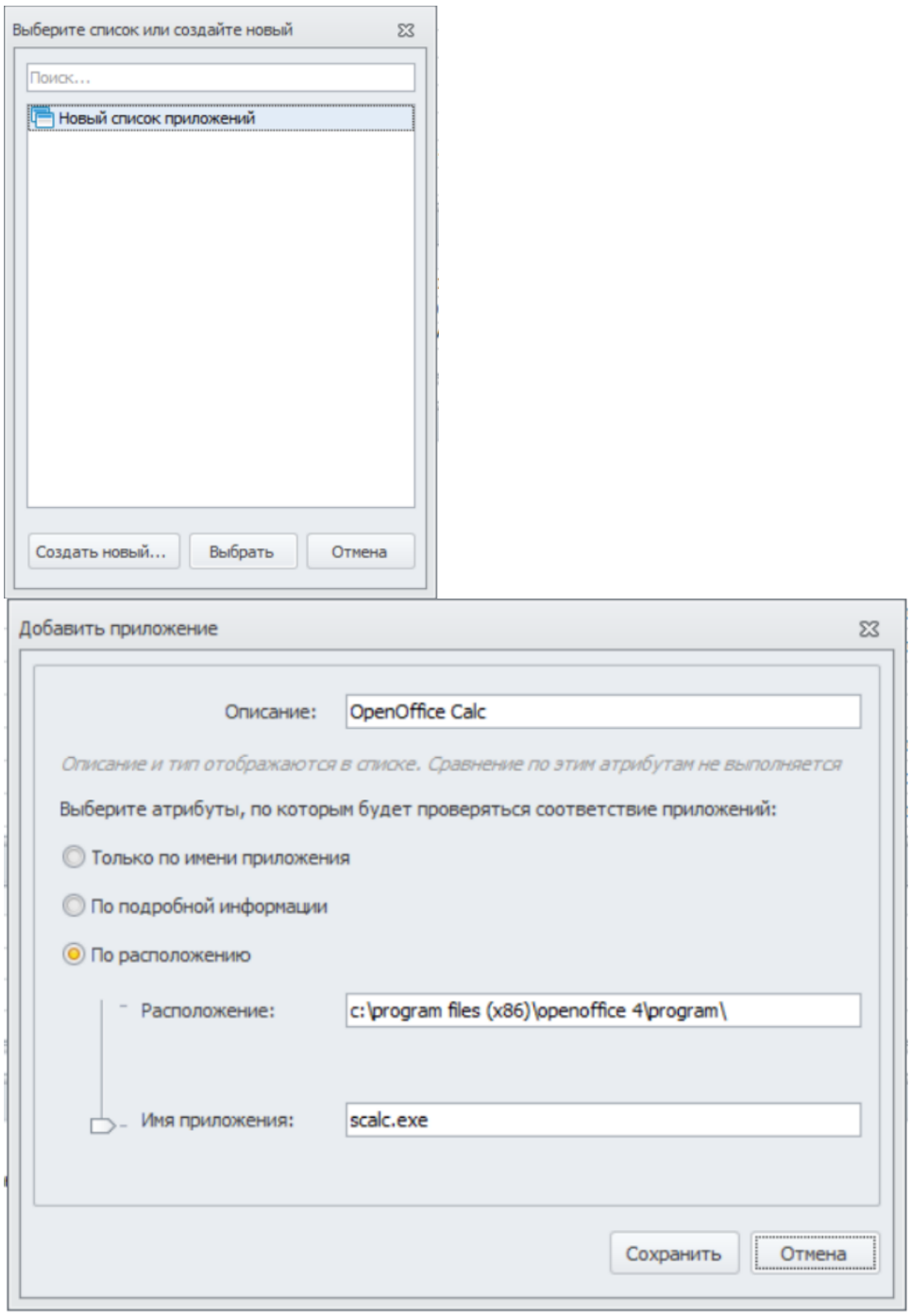
<u>В отчёт вставить скриншот, подтверждающий выполнение этого задания.</u>

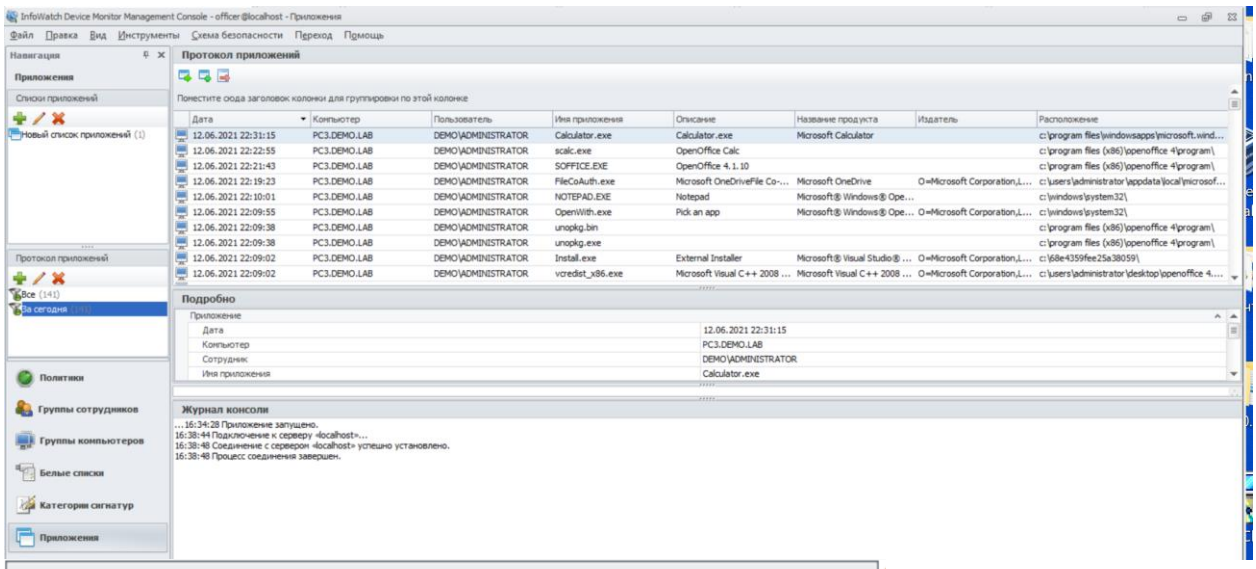
Переходим к созданию Правил.

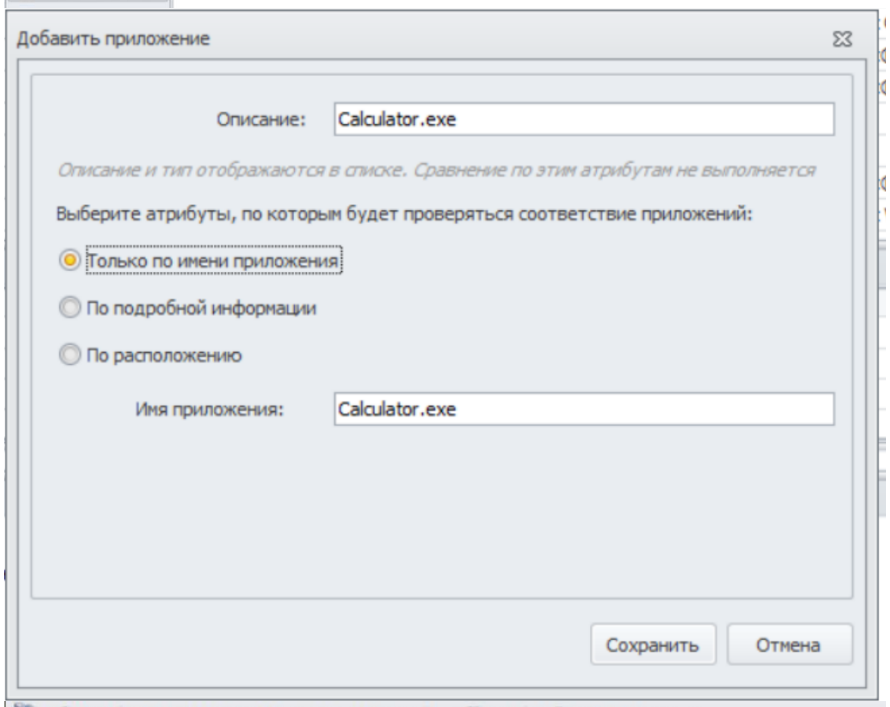
Правило 1. Необходимо запретить создание снимков экрана в табличных процессорах (Excel или OpenOffice Calc) и калькуляторе для предотвращения утечки секретных расчетов и баз данных. Проверить работоспособность и зафиксировать выполнение скриншотом.

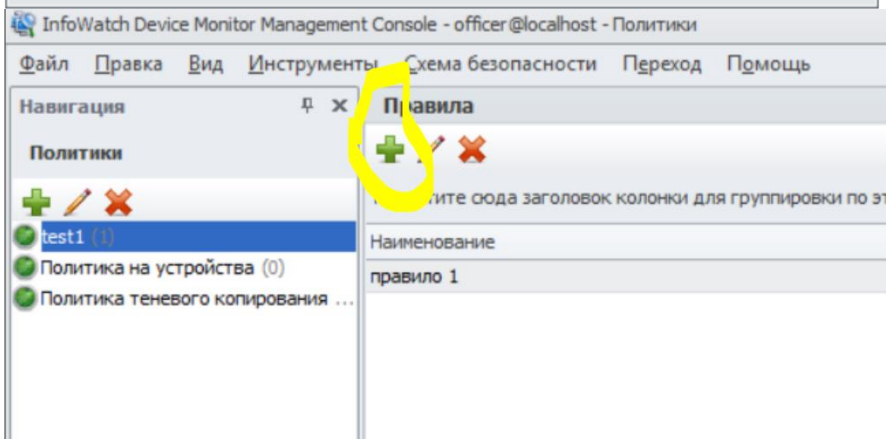
Необходимо запустить приложение на пк с агентом или вручную указать имя приложения (.exe) для того, чтобы в списке Приложений отобразились необходимые для правила приложения:

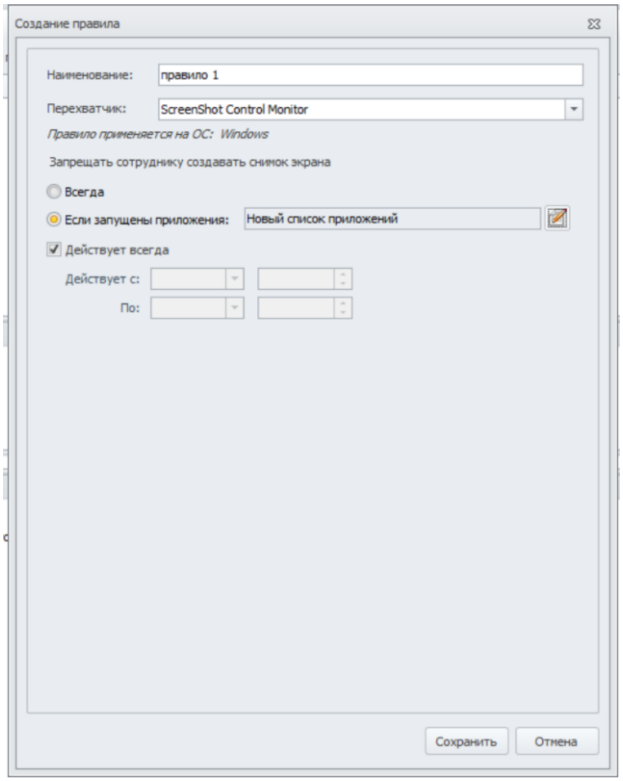



Выберите список или создайте новый
Поиск...
Новый список приложений
Создать новый...
Выбрать
Отмена
Добавить приложение
Описание:
OpenOffice Calc
Описание и тип отображаются в списке. Сравнение по этим атрибутам не выполняется
Выберите атрибуты, по которым будет проверяться соответствие приложений:
Только по имени приложения
По подробной информации
По расположению
Расположение:
c:\program files (x86)\openoffice 4\program\
Имя приложения:
scalc.exe
Сохранить
Отмена

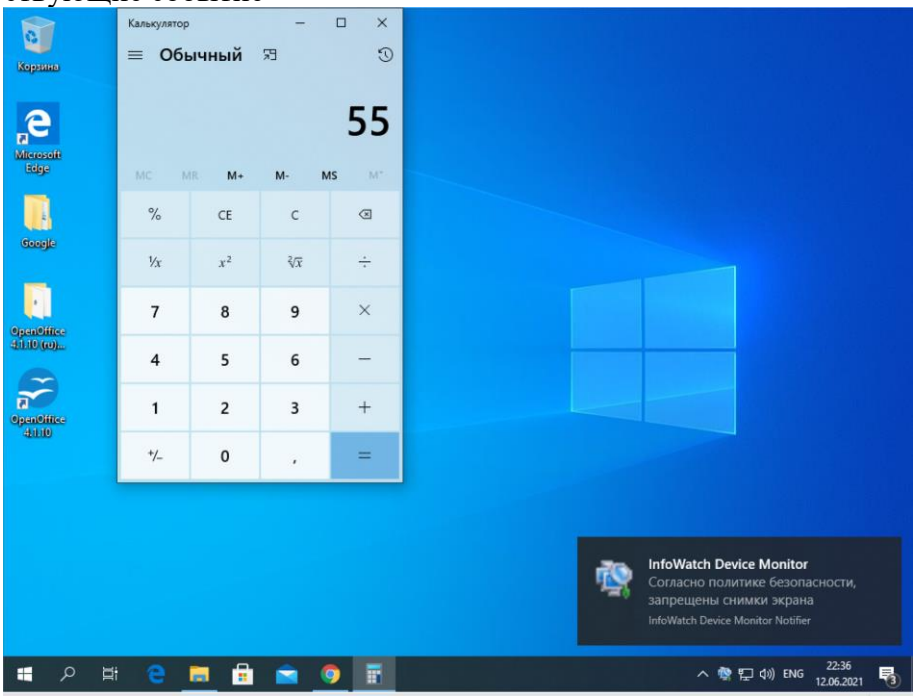

InfoWatch Device Monitor Management Console - officer@localhost - Приложения
Файл Правка Вид Инструменты Схема безопасности Переход Помощь
Навигация
Приложения
Списки приложений
Новый список приложений (1)
Протокол приложений
Все (141)
За сегодня (141)
Политики
Группы сотрудников
Группы компьютеров
Белые списки
Категории сигнатур
Приложения
Протокол приложений
Поместите сюда заголовок колонки для группировки по этой колонке
Дата
Компьютер
Пользователь
Имя приложения
Описание
Название продукта
Издатель
Расположение
12.06.2021 22:31:15 PC3.DEMO.LAB DEMO\ADMINISTRATOR Calculator.exe Calculator.exe Microsoft Calculator
12.06.2021 22:22:55 PC3.DEMO.LAB DEMO\ADMINISTRATOR scalc.exe OpenOffice Calc
12.06.2021 22:21:43 PC3.DEMO.LAB DEMO\ADMINISTRATOR SOFFICE.EXE OpenOffice 4.1.10
12.06.2021 22:19:23 PC3.DEMO.LAB DEMO\ADMINISTRATOR FileCoAuth.exe Microsoft OneDriveFile Co-... Microsoft OneDrive O=Microsoft Corporation,L...
12.06.2021 22:10:01 PC3.DEMO.LAB DEMO\ADMINISTRATOR NOTEPAD.EXE Notepad Microsoft® Windows® Ope...
12.06.2021 22:09:55 PC3.DEMO.LAB DEMO\ADMINISTRATOR OpenWith.exe Pick an app Microsoft® Windows® Ope... O=Microsoft Corporation,L...
12.06.2021 22:09:38 PC3.DEMO.LAB DEMO\ADMINISTRATOR unopkg.bin
12.06.2021 22:09:38 PC3.DEMO.LAB DEMO\ADMINISTRATOR unopkg.exe
12.06.2021 22:09:02 PC3.DEMO.LAB DEMO\ADMINISTRATOR Install.exe External Installer Microsoft® Visual Studio® ... O=Microsoft Corporation,L...
12.06.2021 22:09:02 PC3.DEMO.LAB DEMO\ADMINISTRATOR vcredist_x86.exe Microsoft Visual C++ 2008 ... Microsoft Visual C++ 2008 ... O=Microsoft Corporation,L...
Подробно
Приложение
Дата 12.06.2021 22:31:15
Компьютер PC3.DEMO.LAB
Сотрудник DEMO\ADMINISTRATOR
Имя приложения Calculator.exe
Журнал консоли
16:34:28 Приложение запущено.
16:38:44 Подключение к серверу «localhost»...
16:38:48 Соединение с сервером «localhost» успешно установлено.
16:38:48 Процесс соединения завершен.


Добавить приложение
Описание: Calculator.exe
Описание и тип отображаются в списке. Сравнение по этим атрибутам не выполняется
Выберите атрибуты, по которым будет проверяться соответствие приложений:
Только по имени приложения
По подробной информации
По расположению
Имя приложения: Calculator.exe
Сохранить
Отмена


InfoWatch Device Monitor Management Console - officer@localhost - Политики
Файл Правка Вид Инструменты Схема безопасности Переход Помощь
Навигация
Политики
test1 (1)
Политика на устройства (0)
Политика теневого копирования
Правила
Наименование
правило 1

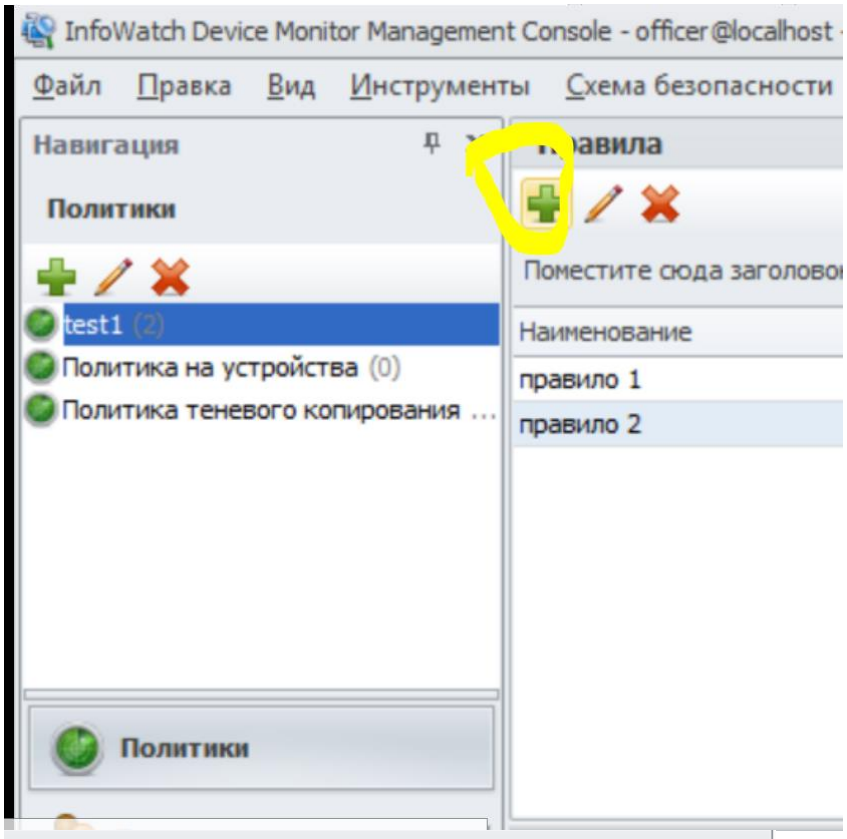


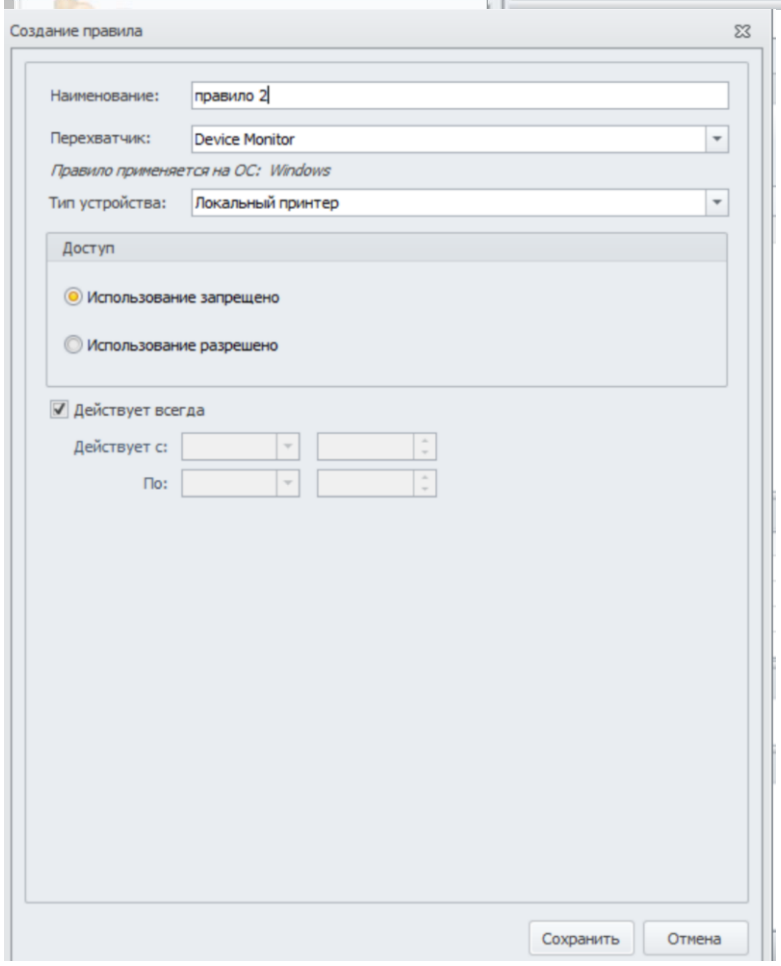
В итоге при попытке сделать скриншот должно выдать уведомление и появиться соответствующие событие



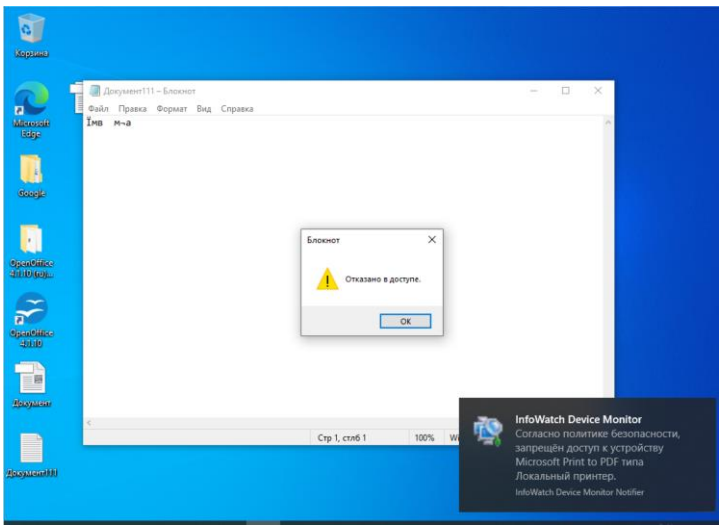
В отчёт вставить скриншоты, подтверждающие создание данного правила, а также скриншот, подтверждающий работоспособность созданного правила.

Правило 2. Необходимо запретить печать на локальных принтерах, но при этом оставить возможность печати на сетевых принтерах. Зафиксировать создание политики скриншотом.





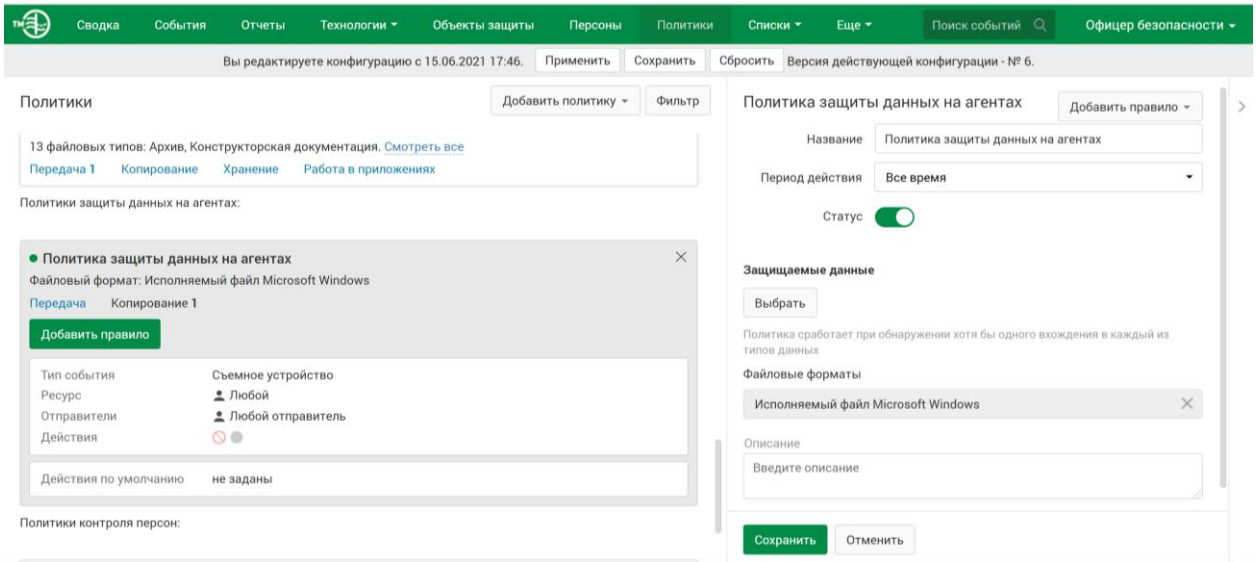
В итоге должно быть.
Проверить с помощью виртуального принтера

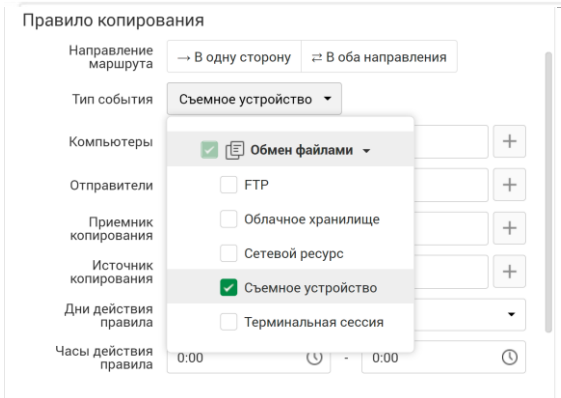


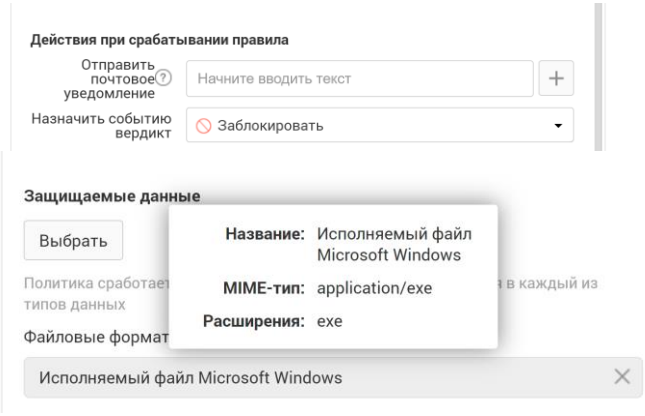
В отчёт вставить скриншоты, подтверждающие создание данного правила, а также скриншот, подтверждающий работоспособность созданного правила.

Правило 3. Создать политику по блокировке копирования исполняемых exe-файлов на USB накопители. Проверить работоспособность и зафиксировать выполнение (зафиксировать результаты в виде скриншотов). Проверить работоспособность и зафиксировать выполнение скриншотом.

Данное задание выполняется с помощью веб-консоли ТМ. Запускаем веб-консоль → Политики → Добавить политику → Политика защиты данных на агентах:

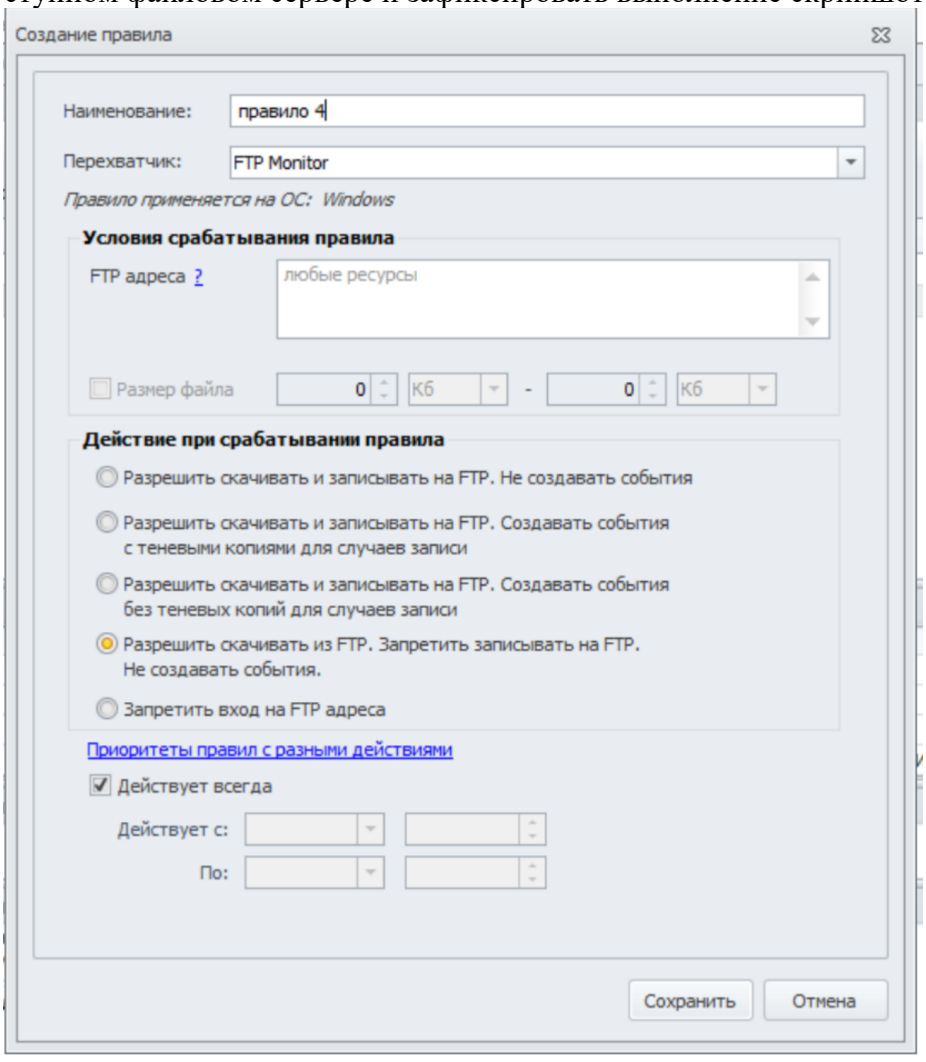






В отчёт вставить скриншоты, подтверждающие создание данного правила, а также скриншот, подтверждающий работоспособность созданного правила.

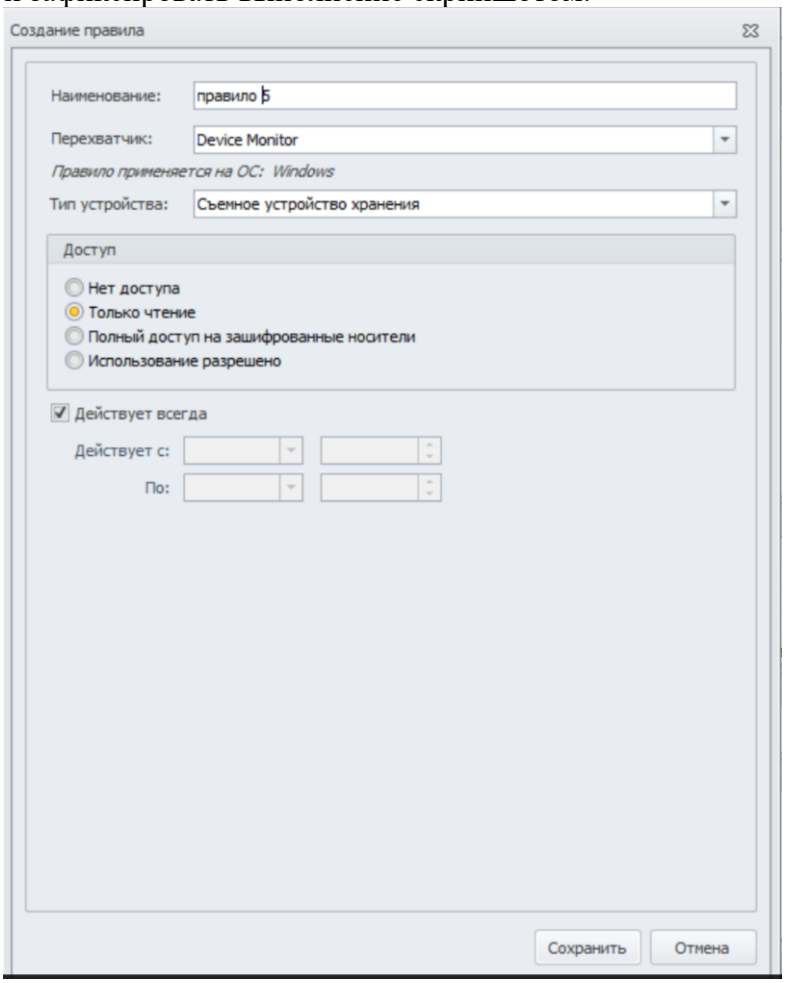
Правило 4. В связи с небезопасностью ftp-серверов разрешить только скачивание по протоколу ftp, загрузку файлов на сервер запретить. Проверить работоспособность на любом доступном файловом сервере и зафиксировать выполнение скриншотом.



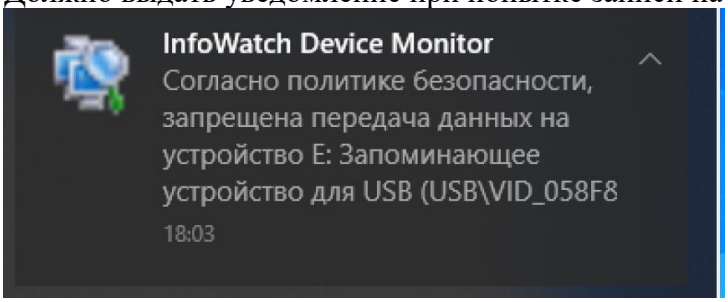
Самостоятельно проверить с помощью dlptest.com

В отчёт вставить скриншоты, подтверждающие создание данного правила, а также скриншот, подтверждающий работоспособность созданного правила.

Правило 5. Необходимо запретить запись файлов на все съемные носители информации (флешки), оставив возможность чтения и копирования с них. Проверить работоспособность и зафиксировать выполнение скриншотом.



Должно выдать уведомление при попытке записи на устройство

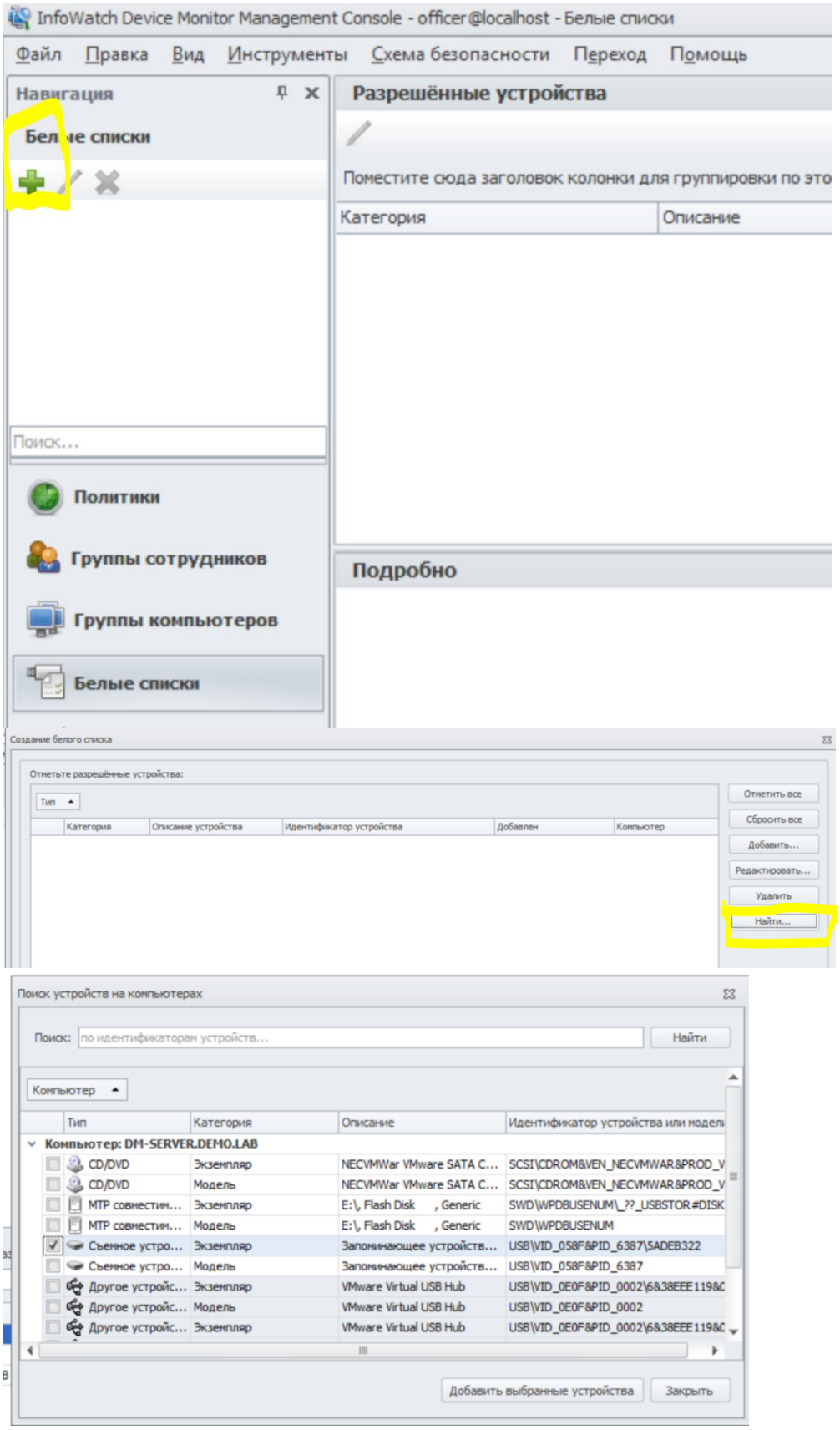


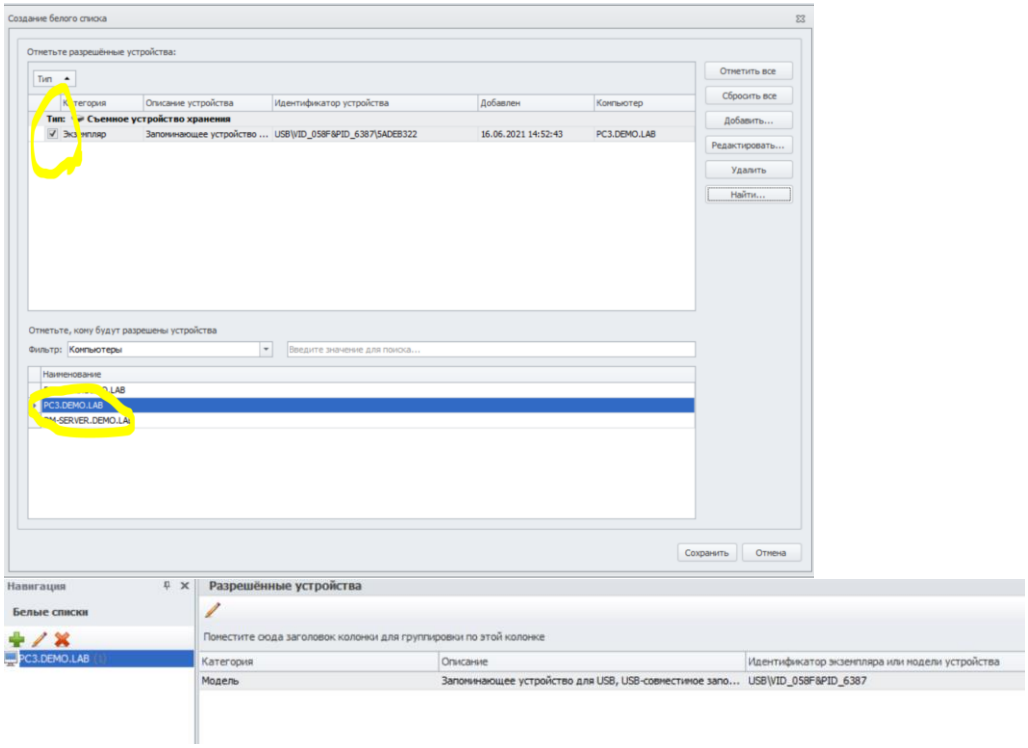
В отчёт вставить скриншоты, подтверждающие создание данного правила, а также скриншот, подтверждающий работоспособность созданного правила.

Практическая работа № 23 «Создание правил с использованием «черных» и «белых» списков в Device monitor»

Задание:

Правило 6. С учетом ранее созданной политики необходимо разрешить запись файлов на доверенный носитель. Запрет на запись на остальные носители оставить в силе. Проверить работоспособность и зафиксировать настройку и выполнение скриншотами.

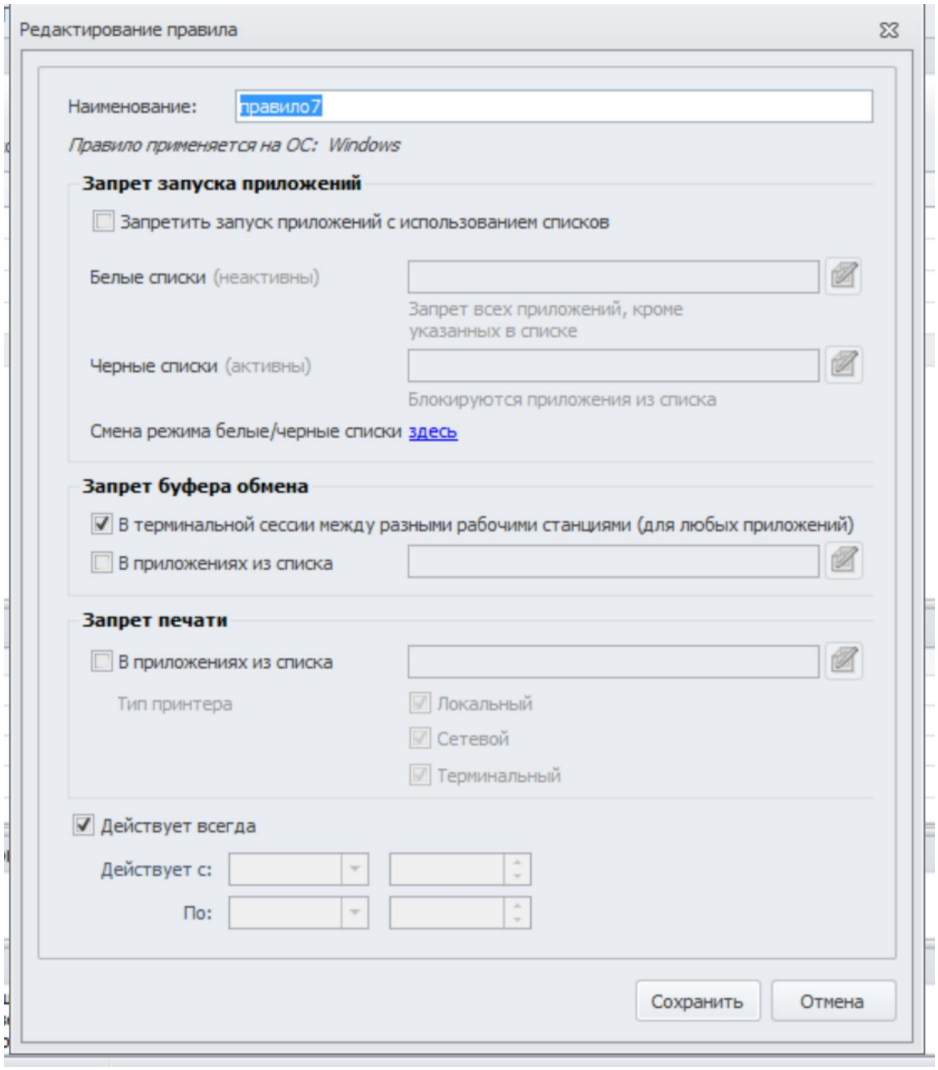

InfoWatch Device Monitor Management Console - officer@localhost - Белые списки
Файл Правка Вид Инструменты Схема безопасности Переход Помощь
Навигация
Белые списки
Разрешённые устройства
Поместите сюда заголовок колонки для группировки по это
Категория
Описание
Поиск...
Политики
Группы сотрудников
Группы компьютеров
Белые списки
Подробно
Создание белого списка
Отметьте разрешённые устройства:
Тип
Категория
Описание устройства
Идентификатор устройства
Добавлен
Компьютер
Отметить все
Сбросить все
Добавить...
Редактировать...
Удалить
Найти...
Поиск устройств на компьютерах
Поиск:
по идентификаторам устройств...
Найти
Компьютер
Тип
Категория
Описание
Идентификатор устройства или модели
Компьютер: DM-SERVER.DEMO.LAB
CD/DVD Экземпляр NECVMWar VMware SATA C... SCSI\CDROM&VEN_NECVMWAR&PROD_V
CD/DVD Модель NECVMWar VMware SATA C... SCSI\CDROM&VEN_NECVMWAR&PROD_V
MTP совместим... Экземпляр E:\, Flash Disk , Generic SWD\WPDBUSENUM_??_USBSTOR#DISK
MTP совместим... Модель E:\, Flash Disk , Generic SWD\WPDBUSENUM
Съемное устро... Экземпляр Запоминающее устройств... USB\VID_058F&PID_6387\5ADEB322
Съемное устро... Модель Запоминающее устройств... USB\VID_058F&PID_6387
Другое устройс... Экземпляр VMware Virtual USB Hub USB\VID_0E0F&PID_0002\6&38EEE119&
Другое устройс... Модель VMware Virtual USB Hub USB\VID_0E0F&PID_0002
Другое устройс... Экземпляр VMware Virtual USB Hub USB\VID_0E0F&PID_0002\6&38EEE119&
Добавить выбранные устройства
Закрыть



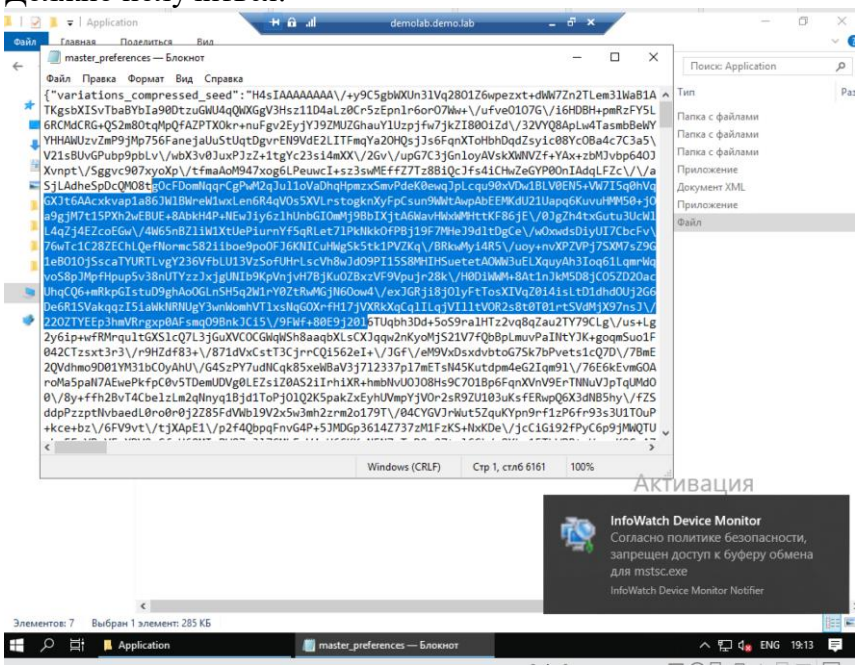
Убедиться в возможности записи на устройство файла.

В отчёт вставить скриншоты, подтверждающие создание данного правила, а также скриншот, подтверждающий работоспособность созданного правила.

Правило 7. На виртуальной машине необходимо запретить использование буфера обмена при подключении к удаленным машинам по протоколу RDP, а в группе компьютеров по умолчанию необходимо контролировать буфер обмена при копировании из/в терминальных сессий. Проверить работоспособность попыткой копирования текста из сеанса RDP и зафиксировать выполнение скриншотом как блокировки, так и контроля. Для работы RDP может потребоваться дополнительная настройка.

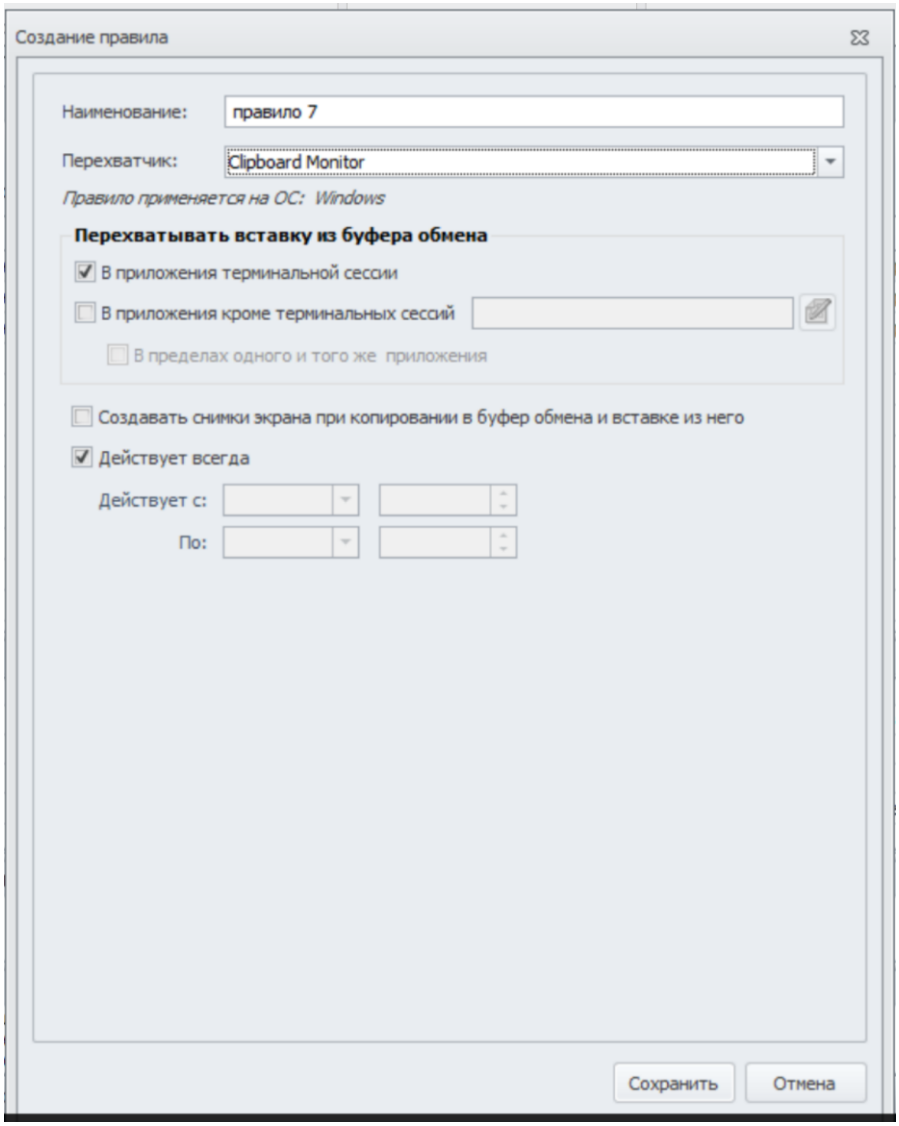


Должно получиться:

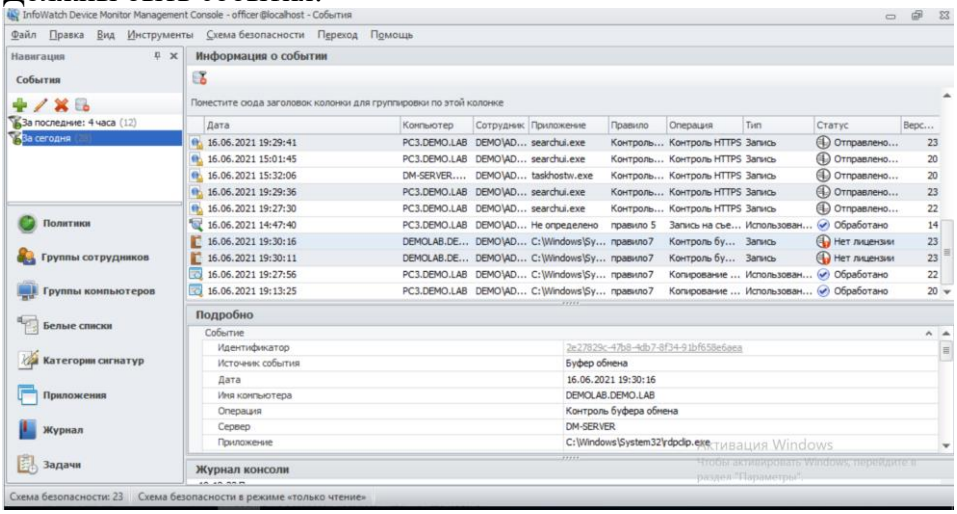


В отчёт вставить скриншоты, подтверждающие создание данного правила, а также скриншот, подтверждающий работоспособность созданного правила.

Удалить правило 7 для выполнения 2 части задания.

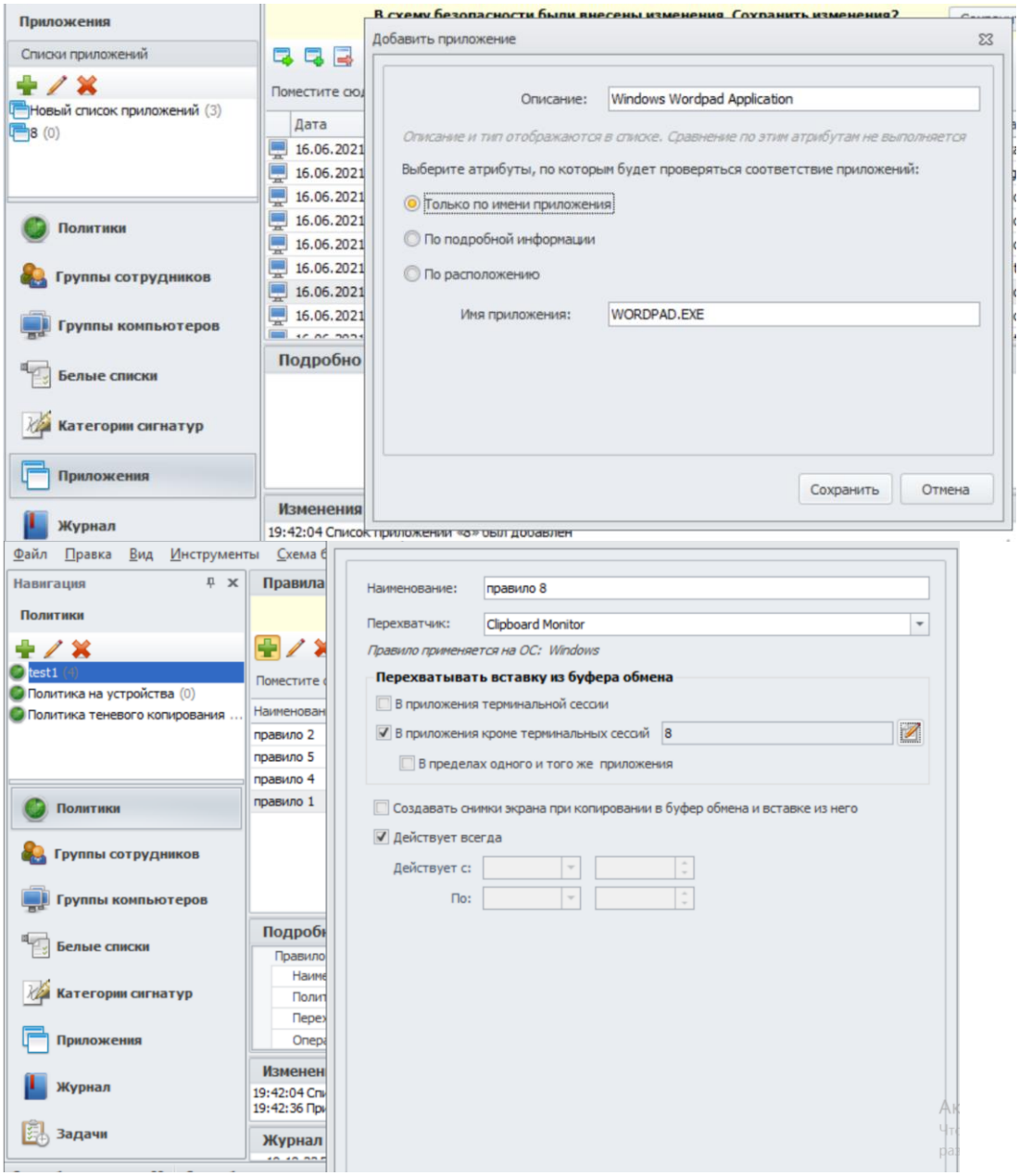


Должны быть события:



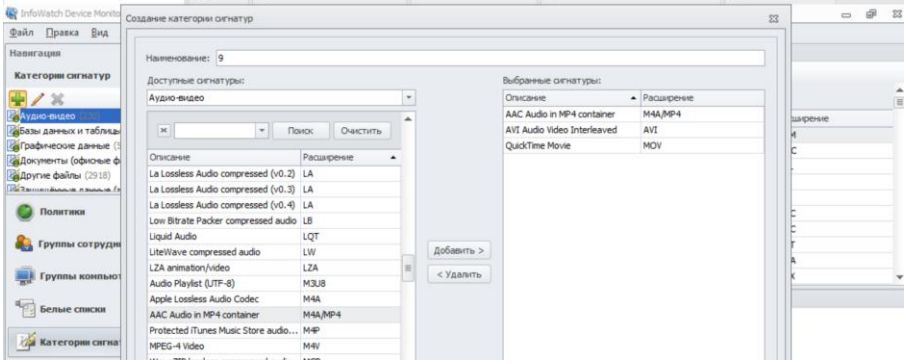
<u>В отчёт вставить скриншоты, подтверждающие создание данного правила, а также скриншот, подтверждающий работоспособность созданного правила.</u>

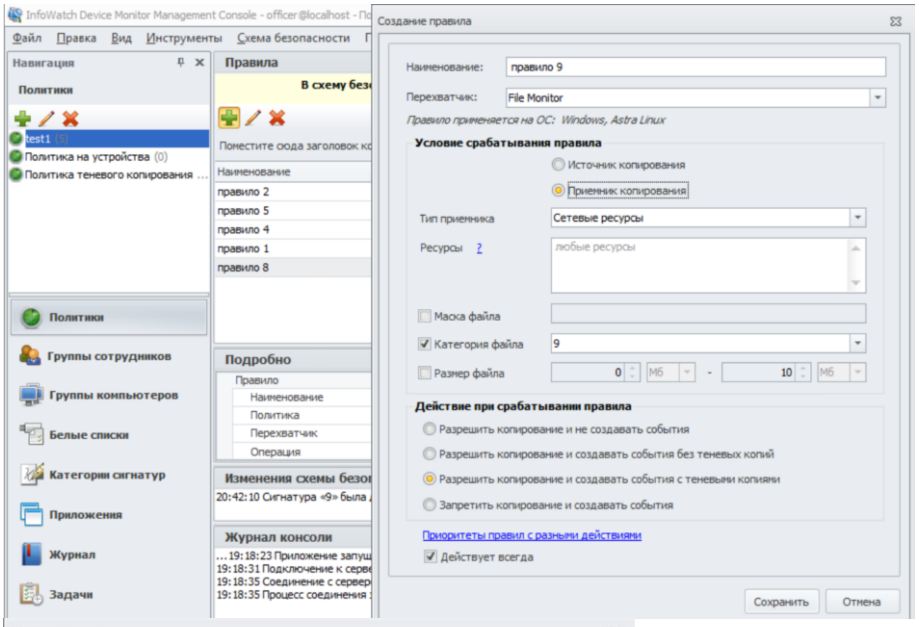
Правило 8. Необходимо поставить на контроль буфер обмена в текстовых процессорах (Word или Writer или Wordpad). Проверить работоспособность и зафиксировать выполнение занесением пары событий в IWTM на любые политики.

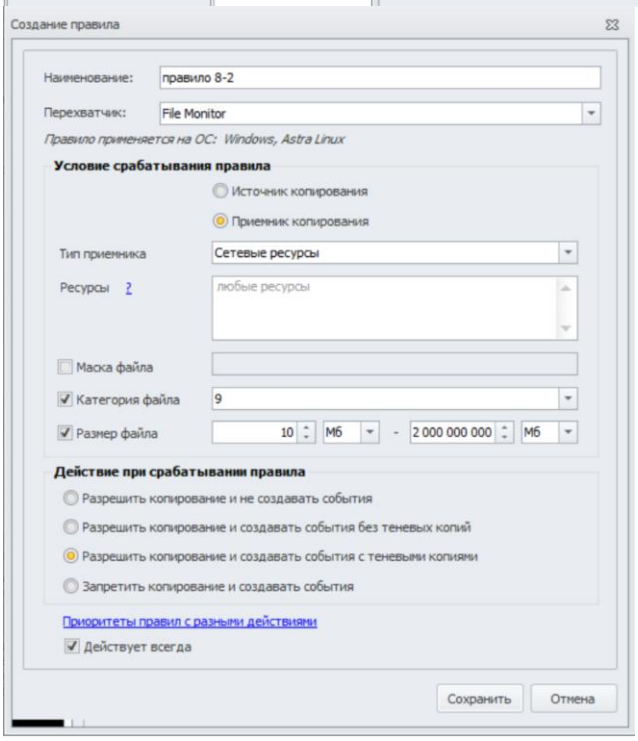


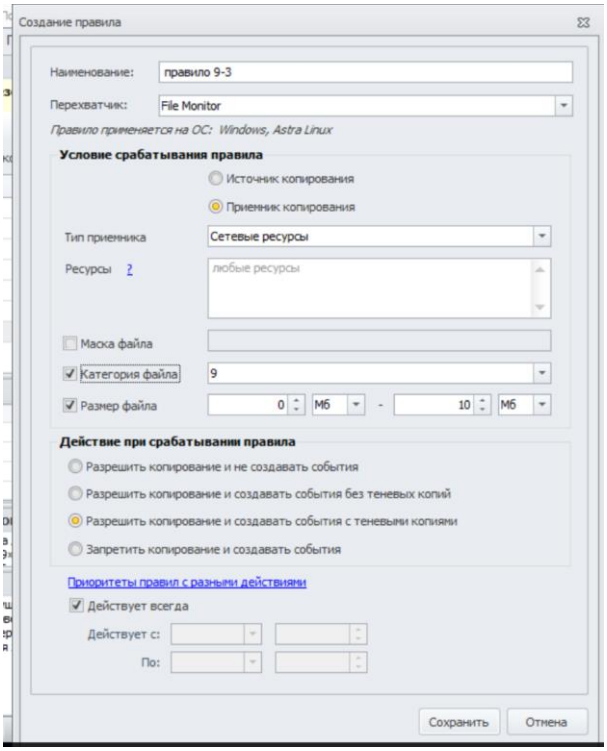
В отчёт вставить скриншоты, подтверждающие создание данного правила, а также скриншот, подтверждающий работоспособность созданного правила.

Правило 9. Для предотвращения неэффективного расхода рабочего времени сотрудников отслеживать движение видео контента (*.avi, *.mov, *.mp4) в общих папках компании. Отдельно контролировать файлы больше 10 Мбайт и меньше 10 Мбайт. (1 Мбайт = 1024 Кбайт) Проверить работоспособность и зафиксировать выполнение скриншотом




InfoWatch Device Monitor Management Console - officer@localhost
Файл Правка Вид Инструменты Схема безопасности
Навигация
Политики
test1 (5)
Политика на устройства (0)
Политика теневого копирования
Правила
Наименование
правило 2
правило 5
правило 4
правило 1
правило 8
Подробно
Правило
Наименование
Политика
Перехватчик
Операция
Изменения схемы безоп
Журнал консоли
Политики
Группы сотрудников
Группы компьютеров
Белые списки
Категории сигнатур
Приложения
Журнал
Задачи
Создание правила
Наименование: правило 9
Перехватчик: File Monitor
Правило применяется на ОС: Windows, Astra Linux
Условие срабатывания правила
Источник копирования
Приемник копирования
Тип приемника Сетевые ресурсы
Ресурсы ?
любые ресурсы
Маска файла
Категория файла 9
Размер файла 0 Мб - 10 Мб
Действие при срабатывании правила
Разрешить копирование и не создавать события
Разрешить копирование и создавать события без теневых копий
Разрешить копирование и создавать события с теневыми копиями
Запретить копирование и создавать события
Приоритеты правил с разными действиями
Действует всегда
Сохранить
Отмена


Создание правила
Наименование: правило 8-2
Перехватчик: File Monitor
Правило применяется на ОС: Windows, Astra Linux
Условие срабатывания правила
Источник копирования
Приемник копирования
Тип приемника Сетевые ресурсы
Ресурсы ?
любые ресурсы
Маска файла
Категория файла 9
Размер файла 10 Мб - 2 000 000 000 Мб
Действие при срабатывании правила
Разрешить копирование и не создавать события
Разрешить копирование и создавать события без теневых копий
Разрешить копирование и создавать события с теневыми копиями
Запретить копирование и создавать события
Приоритеты правил с разными действиями
Действует всегда
Сохранить
Отмена



В отчёт вставить скриншоты, подтверждающие создание данного правила, а также скриншот, подтверждающий работоспособность созданного правила.

Практическая работа № 24 «Работа с Задачами и Журналом в Device monitor»

Задание:

1. Создать пользователя с Привилегией Просмотра событий группы.
   В отчёт вставить скриншот, подтверждающий выполнение задания.
2. Выполните просмотр журнала аудита. Сделайте самостоятельно три фильтра (фильтр на период дат; фильтры на Объект и дейтвие).
   В отчёт вставьте информацию по фильтрам и результат просмотра журнала.
3. Выполните Экспорт журнала в MS Excel.
   В отчёт вставить скриншот из MS Excel с журналом.
4. В разделе Задачи создать задачу обновления для агента.
   В отчёт вставить скриншот, подтверждающий выполнение задания.
5. В разделе Задачи установить пароль для удаления Device Monitor Agent всех виртуальных машин нарушителей с помощью средств DeviceMonitor Server (удаленно). Пароль: *1q2w3e4r*.
   В отчёт вставить скриншот, подтверждающий выполнение задания.

Практическая работа № 25 «Добавление ролей, редактирование ролей, удаление ролей в Traffic Monitor»

Задание:

1. Создайте локальную группу пользователей «Подозрительные» в Traffic Monitor. Добавьте в нее пользователя домена ноутбука и виртуальной клиентской машины.
   Подтвердите выполнение задания скриншотами.
2. Необходимо создать пользователя системы с правами доступа только на чтение и выполнение отчетов, сводок и событий, а также на просмотр каталога локальных и доменных пользователей .
   Логин: userevents, пароль: XxXx4321
   Подтвердите выполнение задания скриншотами.
3. Внешние эксперты привлекаются компанией для оценки эффективности работы её службы безопасности в части создания политик DLP-системы.
   Создайте пользователя Auditor (Аудитор), пароль xxXX1122, который может только просматривать только политики, без просмотра событий и пользователей.
   Подтвердите выполнение задания скриншотами.
4. 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.

5. *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.
6. Наделите импортированного пользователя из Active Directory новой созданной ролью
   Подтвердите выполнение задания скриншотами.
7. Откройте Руководство администратора → Области видимости. В отчёте ответьте на вопрос: Что такое область видимость и зачем она нужна?
8. Создайте область видимости, добавьте нового импортированного пользователя.
   Подтвердите выполнение задания скриншотами.

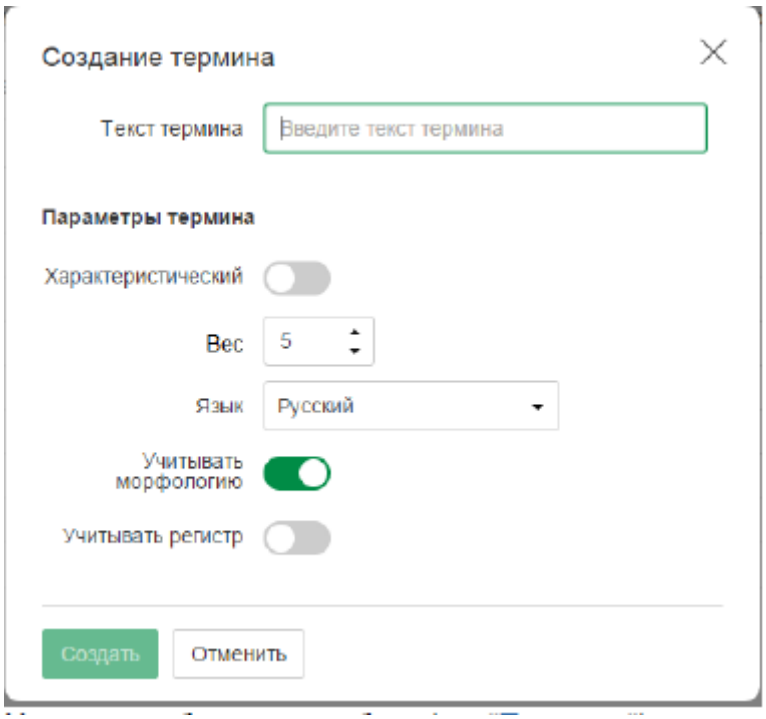
Практическая работа № 26 «Работа с терминами и списками в Traffic monitor»

Задание:

Работа с терминами

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

- ✓ Перейдите в раздел Технологии → Категории и термины



- ✓ Выберите целевую категорию.
- ✓ Добавьте в нее термин *Дата выдачи ИНН*.
- ✓ Включите настройку Характеристический.

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

2. Добавить термин Утечка кода программы
Требуется, чтобы при наличии в трафике фрагментов программного кода, Система помечала объект перехвата как утечку кода программы. Для этого:

- ✓ Создайте категорию *Утечка кода программы*.
- ✓ Добавьте в нее термины: Procedure, Result.

В результате анализа переданных данных, среди которых обнаруживаются указанные термины, Система присваивает объекту перехвата категорию *Утечка кода программы*

3. Создайте политику с низким уровнем угрозы, демонстрирующую работу термина Дата выдачи ИНН.
В отчёт скриншот с созданной политикой.
Проверьте работоспособность политики и вставьте скриншот с результатом проверки политики.

4. Создайте политику с низким уровнем угрозы, демонстрирующую работу термина Утечка кода программы.
В отчёт скриншот с созданной политикой.
Проверьте работоспособность политики и вставьте скриншот с результатом проверки политики.

Работа со списками

1. Работа со списком статусов:
Перейдите в раздел «Списки» → Статусы → Создать статус. Название *Под присмотром*, вы-

берите цвет.
Добавьте 3-м персонам данный статус.
В отчёт вставьте скриншот.
Удалите статус Подозрительные (он по умолчанию есть). В отчёт вставьте скриншот.

2. Работа со списком веб-ресурсов:
Перейдите в раздел «Списки» → Веб-ресурсы → Создание списка ресурсов. Название списка «Сайты партнеров». Внесите веб-ресурсы: worldskills.moscow, dlptest.com, dlp.demo.lab, worldskills.ru**.**
В отчёт вставьте скриншот.

3. Перейдите в периметры.
Нужно исключить из перехвата почту генерального директора.
В отчёт скриншот исключения.
Проверьте работоспособность исключения из перехвата. В отчёт скриншот с результатом.

4. Создайте политику, детектирующую передачу любой информации от «Под присмотром». Уровень угрозы низкий, детектировать, название политики «Под присмотром».
В отчёт скриншот созданной политики.
Проверьте работоспособность. В отчёт скриншот с результатом.

5. Создайте локальную группу пользователей «Злостные прогульщики», а также группу «Ленивые тюленьчики». Добавьте в каждую из них любых 3-х пользователей из разных отделов. Подтвердите выполнение задания скриншотами.

Практическая работа № 27 «Работа с тегами и объектами в Traffic monitor»

Задание 1:

1. Перейдите в раздел Списки → Теги → Создать тег. Создайте тег «Бюрократы». Примените его с политике:

Ввести политику, детектирующую передачу любой информации от бухгалтерии за пределы компании. Уровень угрозы низкий, детектировать, тег «Бюрократы».
В отчёт вставьте скриншоты, подтверждающие выполнение задания.

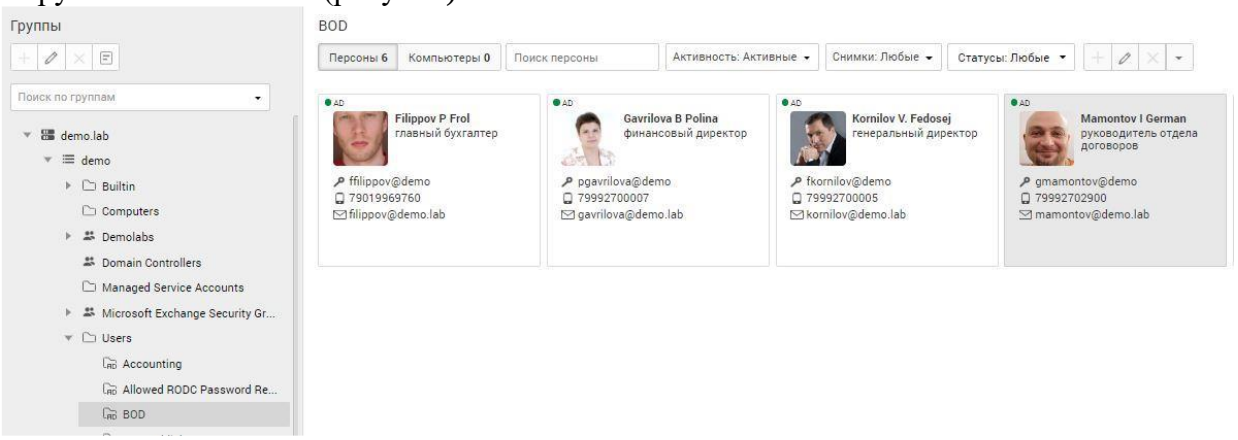
2. Создайте тег Архивариусы и примените его к политике:

Ввести политику, детектирующую передачу любой информации от отдела кадров за пределы компании.
В отчёт вставьте скриншоты, подтверждающие выполнение задания.

Задание 2:

Для работы с Объектом защиты создадим следующую Политику:
Формулировка задания 1: Компания планирует финансировать выдвижение начальника отдела договоров компании (господин Мамонтов) в качестве депутата в законодательное собрание региона. В связи с этим необходимо блокировать распространение потенциально компрометирующих данных по начальнику отдела договоров со стороны сотрудников компании. Необходимо блокировать передачу данных за пределы компании, в которых упоминаются имя и/или фамилия начальника совета директоров (в т.ч. в переписке с иностранным заказчиком). Информацию о персонах можно найти в каталоге пользователей. Уровень угрозы средний, блокировать, тег «Заксобрание».
Выбор персоны

Перед созданием политики проверим, кто является руководителем отдела договоров. Для этого переходим в раздел «Персоны», раскрываем группы персон и компьютеров домена (левая часть рабочей области на Рисунке). Просмотреть карточку требуемой персоны можно в группе Users → BOD (рисунок).



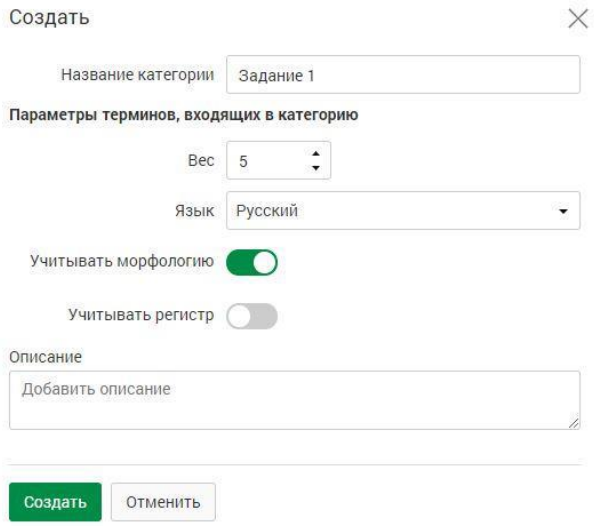
В карточке указаны имя и фамилия, по которым будет срабатывать блокировка передачи данных. Перед созданием политики добавим термины и объект защиты.

<u>В отчёт вставить скриншот, подтверждающий выполнение данного задания</u>

<u>Создание терминов</u>

В разделе «Технологии» выбираем пункт «Категории и термины».

1. Создание категории

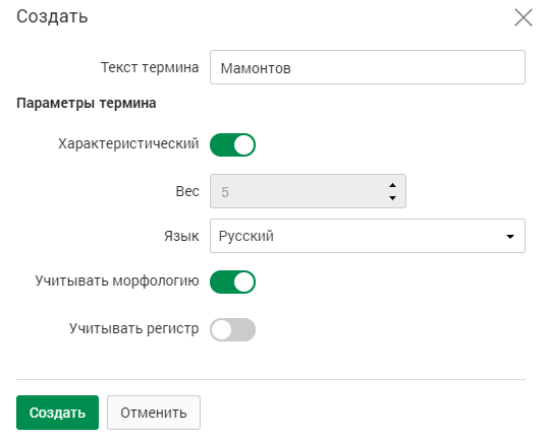


−Ввести название категории, например «Задание 1»

−Указать или оставь по умолчанию вес, язык, учёт морфологии и регистра для терминов, входящих в категорию

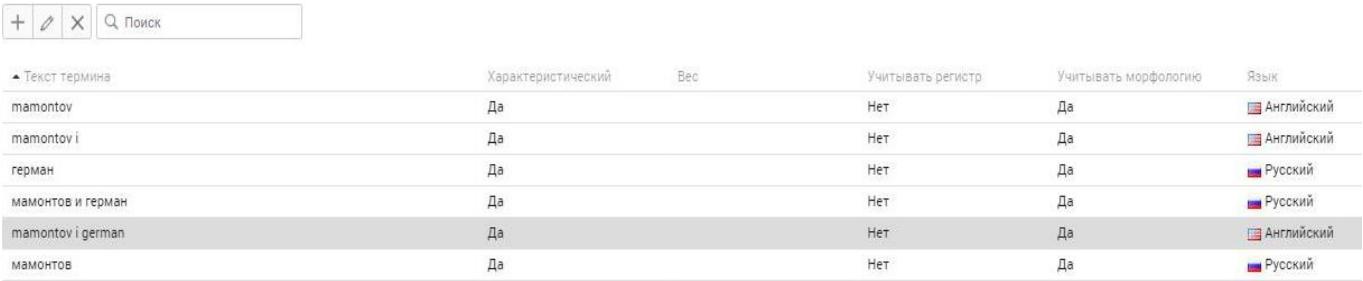
−При необходимости добавить описание

2. Добавление термина



–Нажать + в созданной категории
–Ввести текст термина
–Выбрать поле «Характеристический». Если этот атрибут включен, то нахождение термина в трафике обязательно присваивает объекту категорию, содержащую термин.
–Указать вес, означающий значимость термина. Если выбран пункт «Характеристический», то вес не указывается.
–Указать язык термина
–При необходимости выбрать пункт учитывать морфологию
–При необходимости выбрать пункт учитывать регистр
–Нажать «Создать»

Аналогично добавить другие термины, соответствуя заданию. Учитывать язык написания и варианты с латиницей или/и кириллицей. В результате выполнения задания страница с терминами может выглядеть, как представлено на:



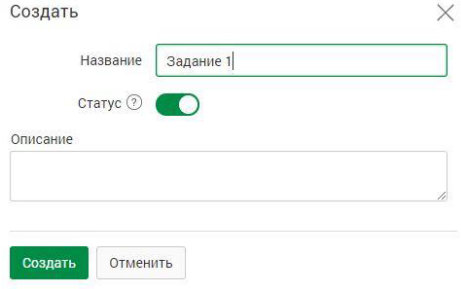
В данном задании необходимо учесть вариант, когда имя персоны задаётся с использование латинских и русских букв.

В отчёт вставить скриншот, подтверждающий выполнение данного задания

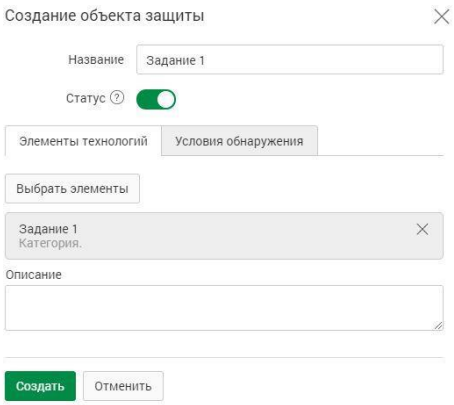
Создание объекта защиты

Для создания объекта защиты необходимо перейти в раздел «Объект защиты».

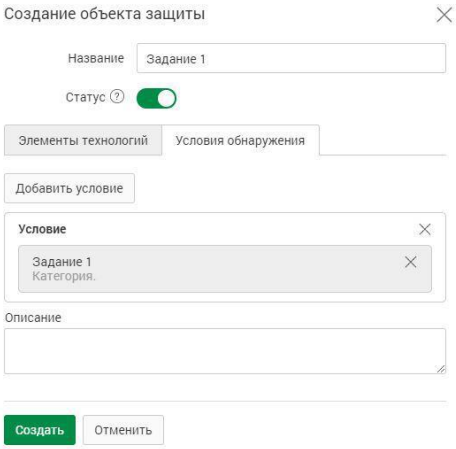
1. Создать каталог объектов защиты



−Выбрать знак «+», после появится окно создание каталога
−Ввести название, например «Задание 1»
−Выбрать статус
−При необходимости дать описание
−Нажать «Создать»
2. Для создания объекта защиты требуется выбрать созданный каталог и нажать знак «+», в появившемся окне:
−В пункте «Категория» выбрать «Задание 1»
−Нажать «Создать»
−Ввести название, например «Задание 1»
−Выбрать статус
−Проверь, что в «Элементы технологий» выбрана нужная категория



−В пункте «Условия обнаружения», в качестве условия выбрано «Задание 1»



−Нажать «Создать»

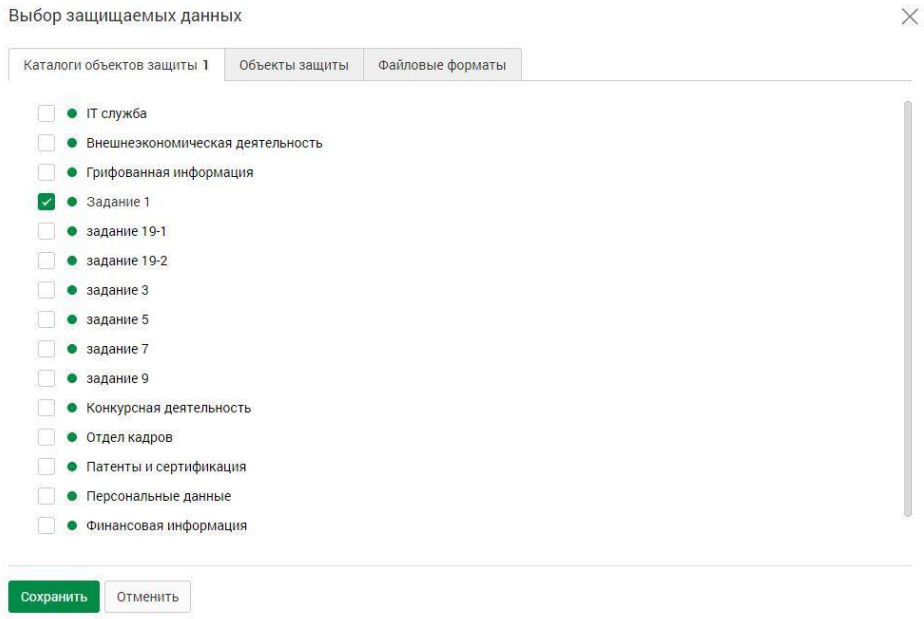
<u>В отчёт вставить скриншот, подтверждающий выполнение данного задания</u>

<u>Создание политики</u>

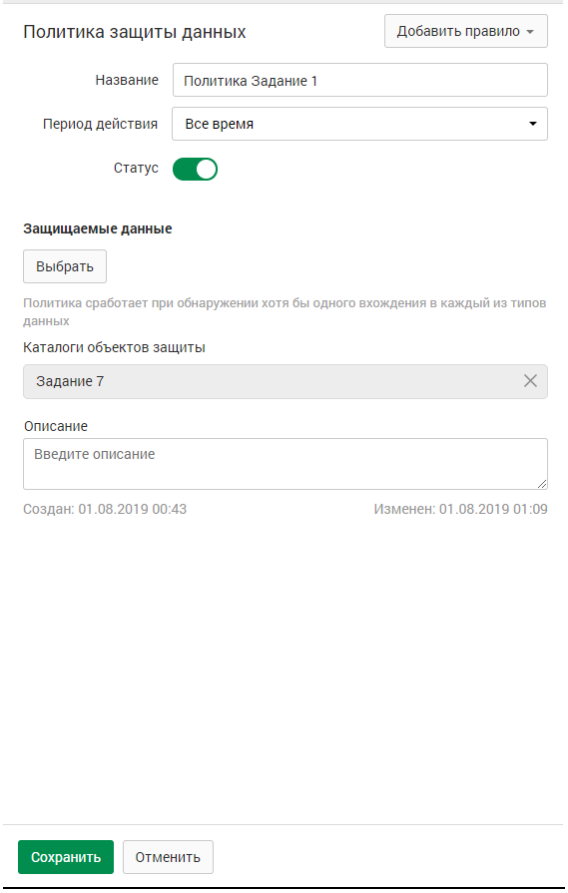
Примечание: При работе созданных политик могут отрабатывать стандартные политики (по умолчанию включены), рекомендуется их отключить/удалить или модифицировать.
Перейти в раздел «Политики» и выполнить следующие операции:
1. Нажать кнопку «Добавить политику» → «Политика защиты данных»

2. Ввести название, например «Политика Задание 1»

3. Выбрать защищаемые данные (Объект защиты), Задание 1



4. Нажать «Сохранить»



В отчёт вставить скриншот, подтверждающий выполнение данного задания

Добавление правила передачи

Для добавления правила нужно нажать кнопку «Добавить правило» → «Передачи», после чего откроется панель добавления нового правила, в которой требуется выполнить следующие операции:

1. Выбрать «+» в пункте «Отправители» → вкладка «Группы» → поставить галочку «demo.lab»

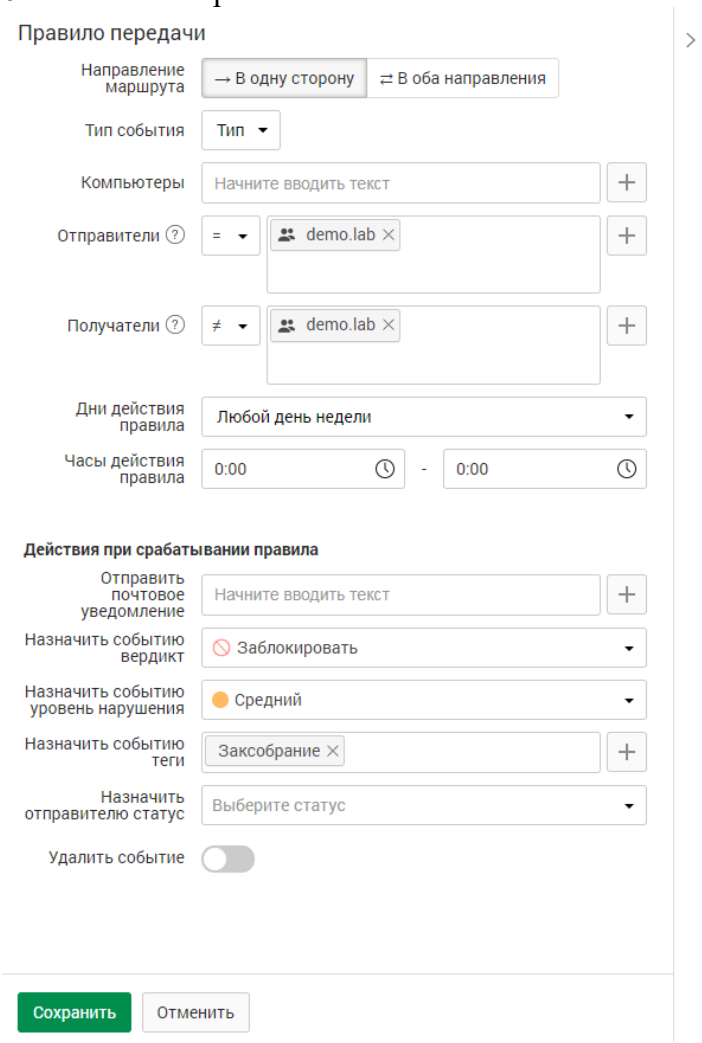
2. Выбрать «+» в пункте «Получатели» и указать оператор ≠. Аналогично прошлому пункту вкладка «Группы» → поставить галочку «demo.lab»

3. Назначить событию вердикт «Заблокировать»

4. Назначить событию уровень нарушения «Средний»

5. Назначить тег «Заксобрание» (см Добавить тег)

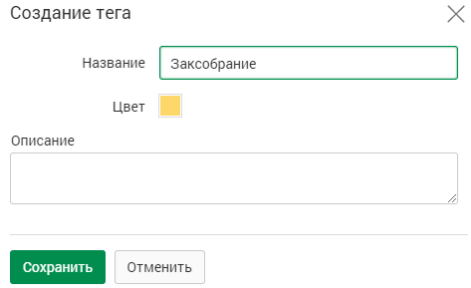
6. Нажать «Сохранить»



<u>В отчёт вставить скриншот, подтверждающий выполнение данного задания</u>

Добавить тег

Перейти в раздел «Списки» → «Теги», откроется страница управления тегами. Для добавления нового требуется нажать знак «+» и указать



1. Название тега

2. Цвет

3. При необходимости дать описание

4. Нажать «Сохранить»

В отчёт вставить скриншот, подтверждающий выполнение данного задания

Выполнить проверку работоспособности созданной политики и вставить скриншот, подтверждающий выполнение данного задания.

Практическая работа № 28 «Политики защиты данных на Traffic monitor»

Задание:

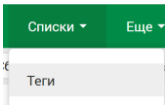
Политика 1

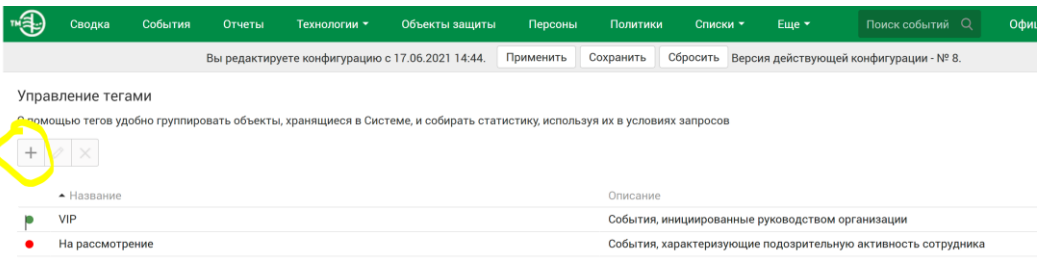
У генерального директора компании недавно появился котик и его фото утекло всеть компании. Теперь сотрудники обмениваются смешными картинками с подписями и масками внутри компании и выкладывают их в социальные сети. Директор решил, что его котик вызвал снижение качества работы сотрудников из-за повышенной милоты картинок и хочет запретить обмен фотографией котика. Необходимо запретить обмен фотографией и немного измененной фотографиейкотика (до ≈50%) как внутри компании, так и за ее пределы. Фотография котика есть в дополнительных данных.

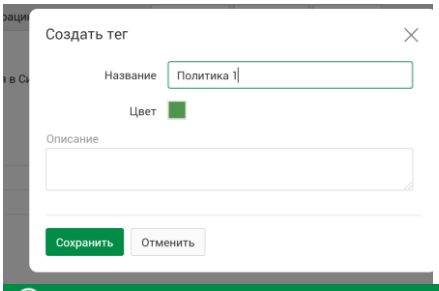
Вердикт: Заблокировать ×

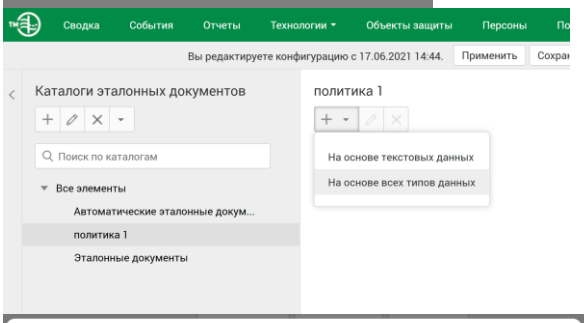
Уровень нарушения: низкий •

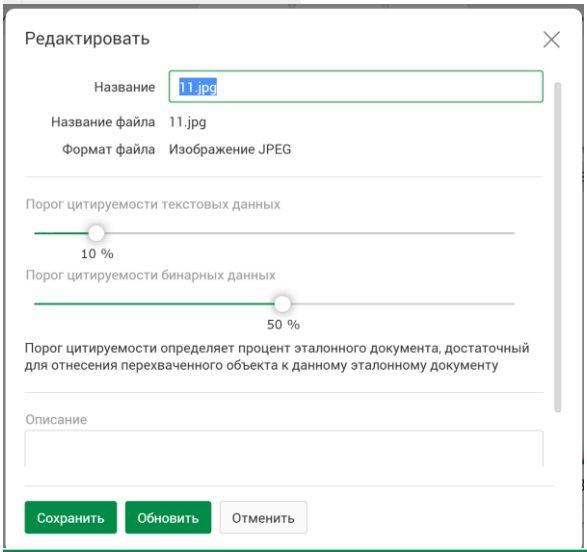
Тег: Политика 1

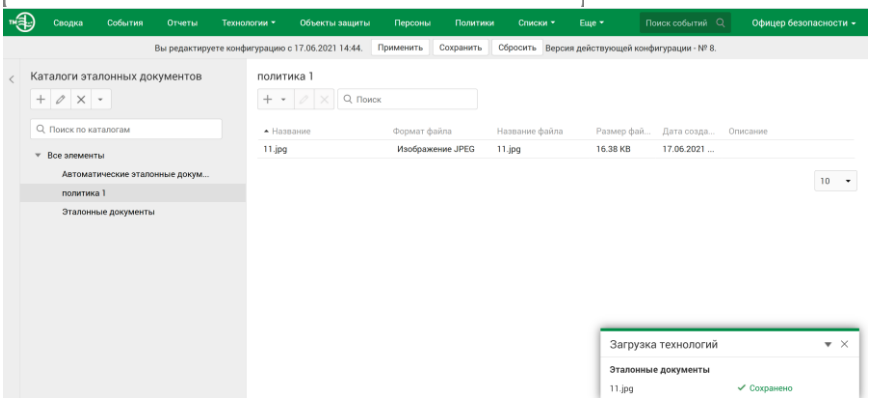


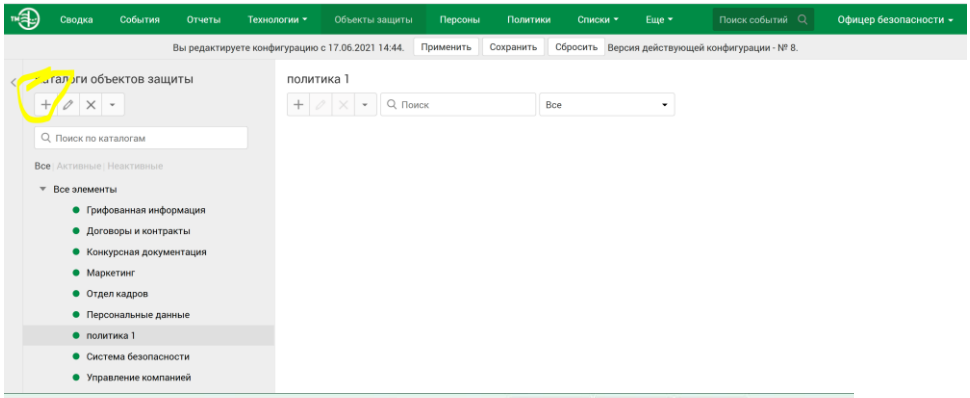

Сводка
События
Отчеты
Технологии
Объекты защиты
Персоны
Политики
Списки
Еще
Поиск событий
Вы редактируете конфигурацию с 17.06.2021 14:44.
Применить
Сохранить
Сбросить
Версия действующей конфигурации - № 8.
Управление тегами
Название
Описание
VIP
События, инициированные руководством организации
На рассмотрение
События, характеризующие подозрительную активность сотрудника

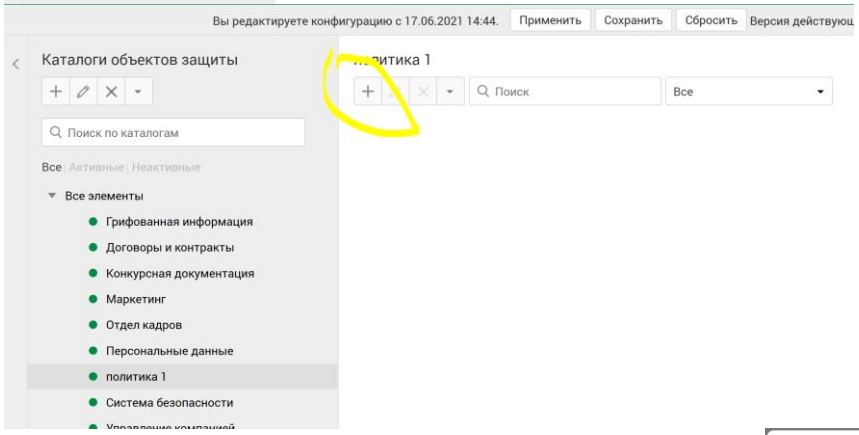

Создать тег
Название
Политика 1
Цвет
Описание
Сохранить
Отменить

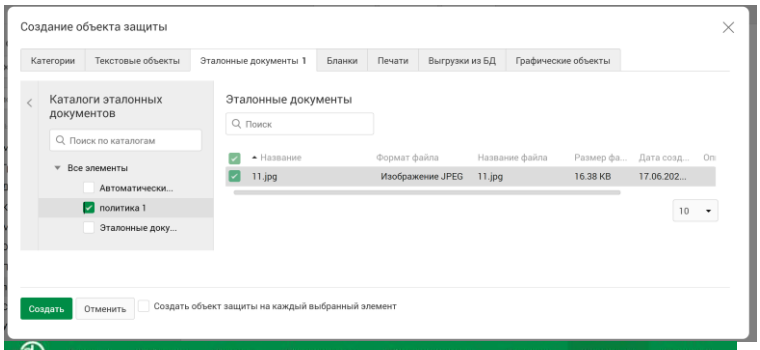

Сводка
События
Отчеты
Технологии
Объекты защиты
Персоны
Вы редактируете конфигурацию с 17.06.2021 14:44.
Применить
Каталоги эталонных документов
Поиск по каталогам
Все элементы
Автоматические эталонные докум...
политика 1
Эталонные документы
политика 1
На основе текстовых данных
На основе всех типов данных

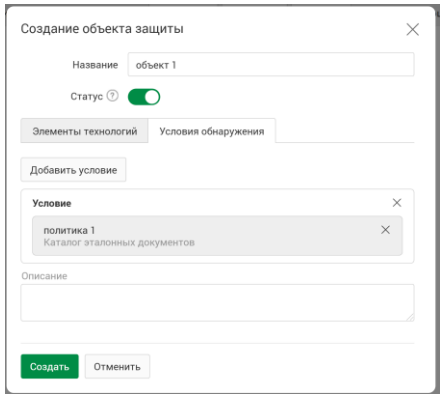

Редактировать
Название
11.jpg
Название файла
11.jpg
Формат файла
Изображение JPEG
Порог цитируемости текстовых данных
10 %
Порог цитируемости бинарных данных
50 %
Порог цитируемости определяет процент эталонного документа, достаточный для отнесения перехваченного объекта к данному эталонному документу
Описание
Сохранить
Обновить
Отменить

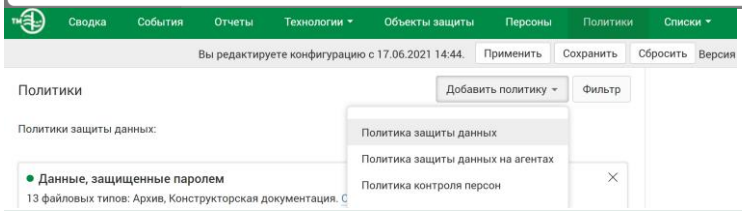

Сводка
События
Отчеты
Технологии
Объекты защиты
Персоны
Политики
Списки
Еще
Поиск событий
Офицер безопасности
Вы редактируете конфигурацию с 17.06.2021 14:44.
Применить
Сохранить
Сбросить
Версия действующей конфигурации - № 8.
Каталоги эталонных документов
Поиск по каталогам
Все элементы
Автоматические эталонные докум...
политика 1
Эталонные документы
политика 1
Поиск
Название
Формат файла
Название файла
Размер фай...
Дата созда...
Описание
11.jpg
Изображение JPEG
11.jpg
16.38 KB
17.06.2021 ...
10
Загрузка технологий
Эталонные документы
11.jpg
Сохранено

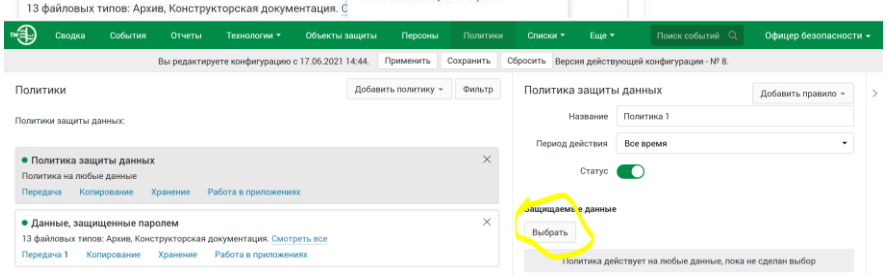

Сводка
События
Отчеты
Технологии
Объекты защиты
Персоны
Политики
Списки
Еще
Поиск событий
Офицер безопасности
Вы редактируете конфигурацию с 17.06.2021 14:44.
Применить
Сохранить
Сбросить
Версия действующей конфигурации - № 8.
Каталоги объектов защиты
Поиск по каталогам
Все | Активные | Неактивные
Все элементы
Грифованная информация
Договоры и контракты
Конкурсная документация
Маркетинг
Отдел кадров
Персональные данные
политика 1
Система безопасности
Управление компанией
политика 1
Поиск
Все

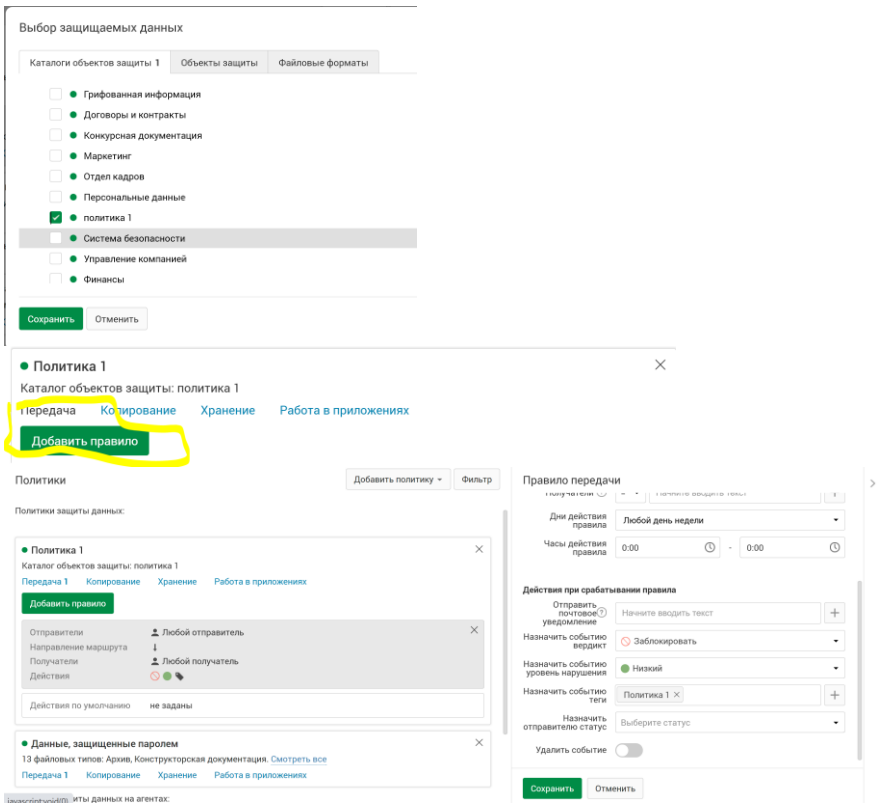

Вы редактируете конфигурацию с 17.06.2021 14:44.
Применить
Сохранить
Сбросить
Каталоги объектов защиты
Поиск по каталогам
Все | Активные | Неактивные
Все элементы
Грифованная информация
Договоры и контракты
Конкурсная документация
Маркетинг
Отдел кадров
Персональные данные
политика 1
Система безопасности
Поиск
Все


Создание объекта защиты
Категории
Текстовые объекты
Эталонные документы 1
Бланки
Печати
Выгрузки из БД
Графические объекты
Каталоги эталонных документов
Поиск по каталогам
Все элементы
политика 1
Эталонные документы
Поиск
Название
Формат файла
Название файла
Размер фа...
Дата созд...
11.jpg
Изображение JPEG
11.jpg
16.38 KB
17.06.202...
Создать
Отменить
Создать объект защиты на каждый выбранный элемент


Создание объекта защиты
Название
объект 1
Статус
Элементы технологий
Условия обнаружения
Добавить условие
Условие
политика 1
Каталог эталонных документов
Описание
Создать
Отменить

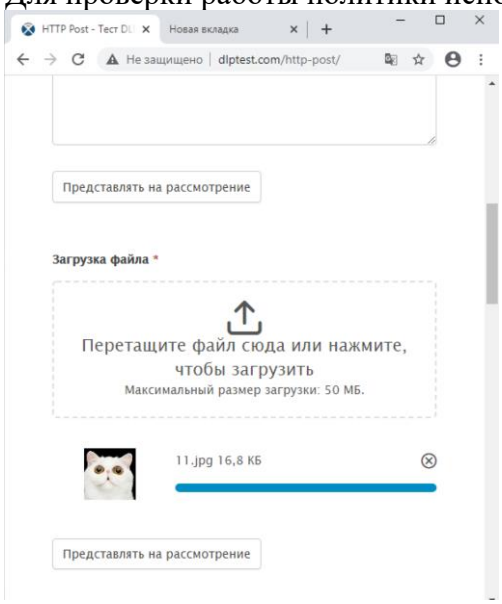

Сводка
События
Отчеты
Технологии
Объекты защиты
Персоны
Политики
Списки
Вы редактируете конфигурацию с 17.06.2021 14:44.
Применить
Сохранить
Сбросить
Политики
Добавить политику
Фильтр
Политики защиты данных:
Политика защиты данных
Политика защиты данных на агентах
Политика контроля персон
Данные, защищенные паролем
13 файловых типов: Архив, Конструкторская документация.


Сводка
События
Отчеты
Технологии
Объекты защиты
Персоны
Политики
Списки
Еще
Поиск событий
Офицер безопасности
Вы редактируете конфигурацию с 17.06.2021 14:44.
Применить
Сохранить
Сбросить
Версия действующей конфигурации - № 8.
Политики
Добавить политику
Фильтр
Политики защиты данных:
Политика защиты данных
Политика на любые данные
Передача
Копирование
Хранение
Работа в приложениях
Данные, защищенные паролем
13 файловых типов: Архив, Конструкторская документация.
Смотреть все
Передача 1
Копирование
Хранение
Работа в приложениях
Политика защиты данных
Добавить правило
Название
Политика 1
Период действия
Все время
Статус
Выбрать
Политика действует на любые данные, пока не сделан выбор

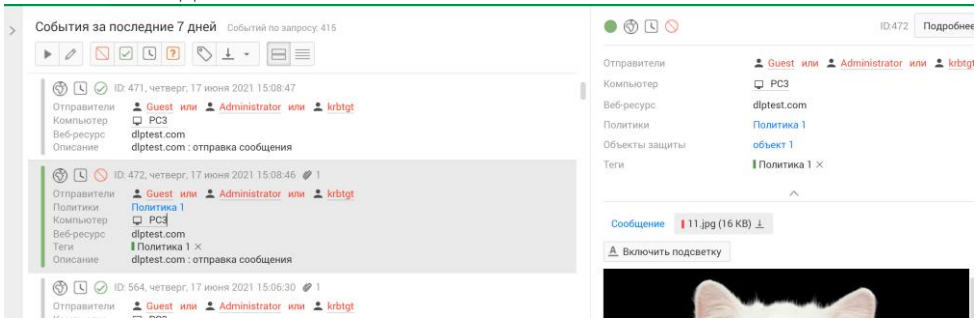


В отчёт вставьте скриншоты с созданной политикой.

Для проверки работы политики использовать dlptest.com:



В Событиях должно появиться:



В отчёт вставить скриншот из событий с отработанной политикой.

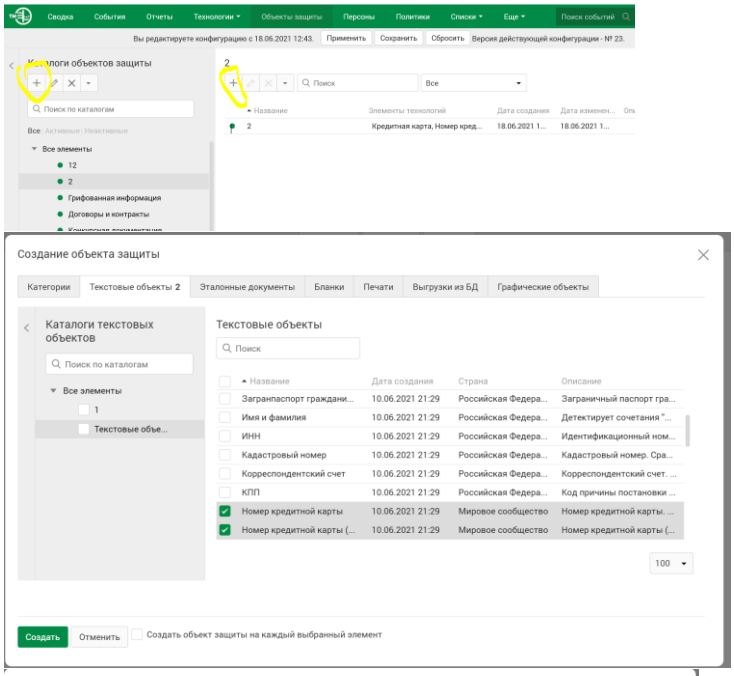
Политика 2

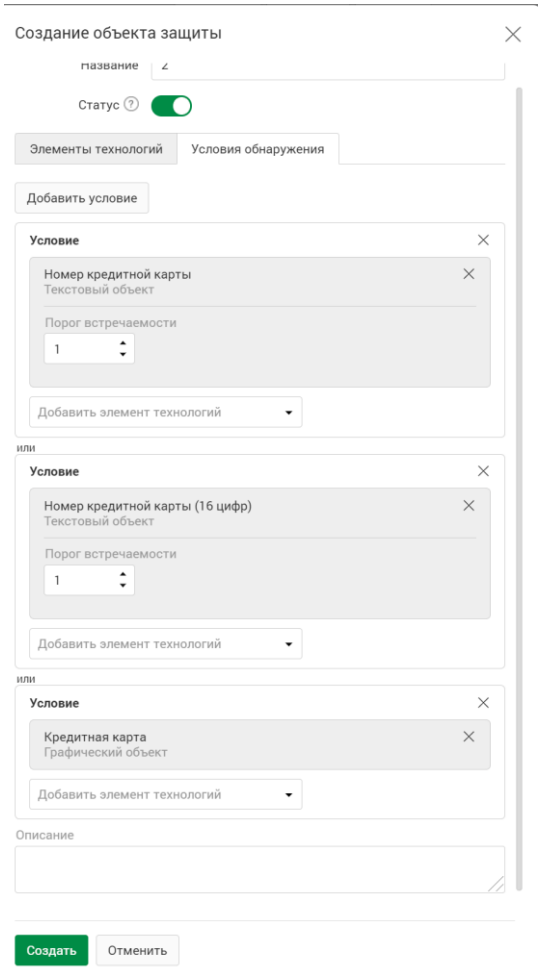
В последнее время бюджет компании стал резко падать. Подозрения пали наглавного бухгалтера, директор подозревает его в проведении денежных средств «мимо кассы». В связи с этим необходимо отслеживать передачу всех номеров исканов кредитных карт, отправляемых из отдела Бухгалтерии

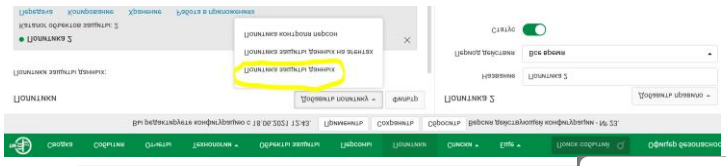
Вердикт: Заблокировать ×

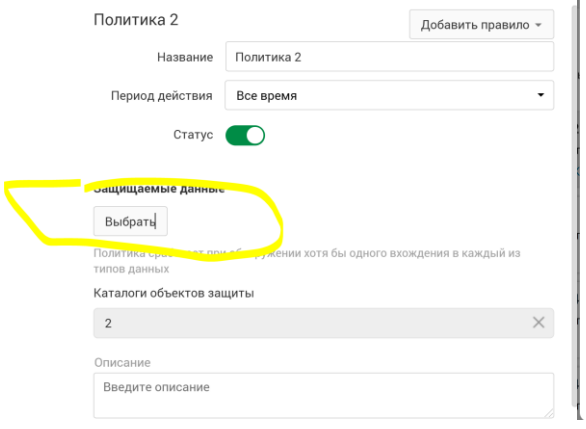
Уровень нарушения: высокий •

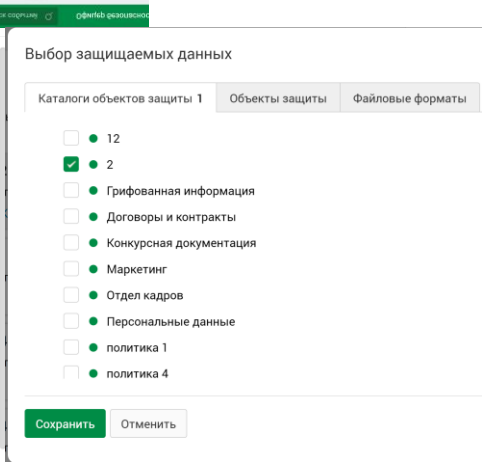
Тег: Политика 2

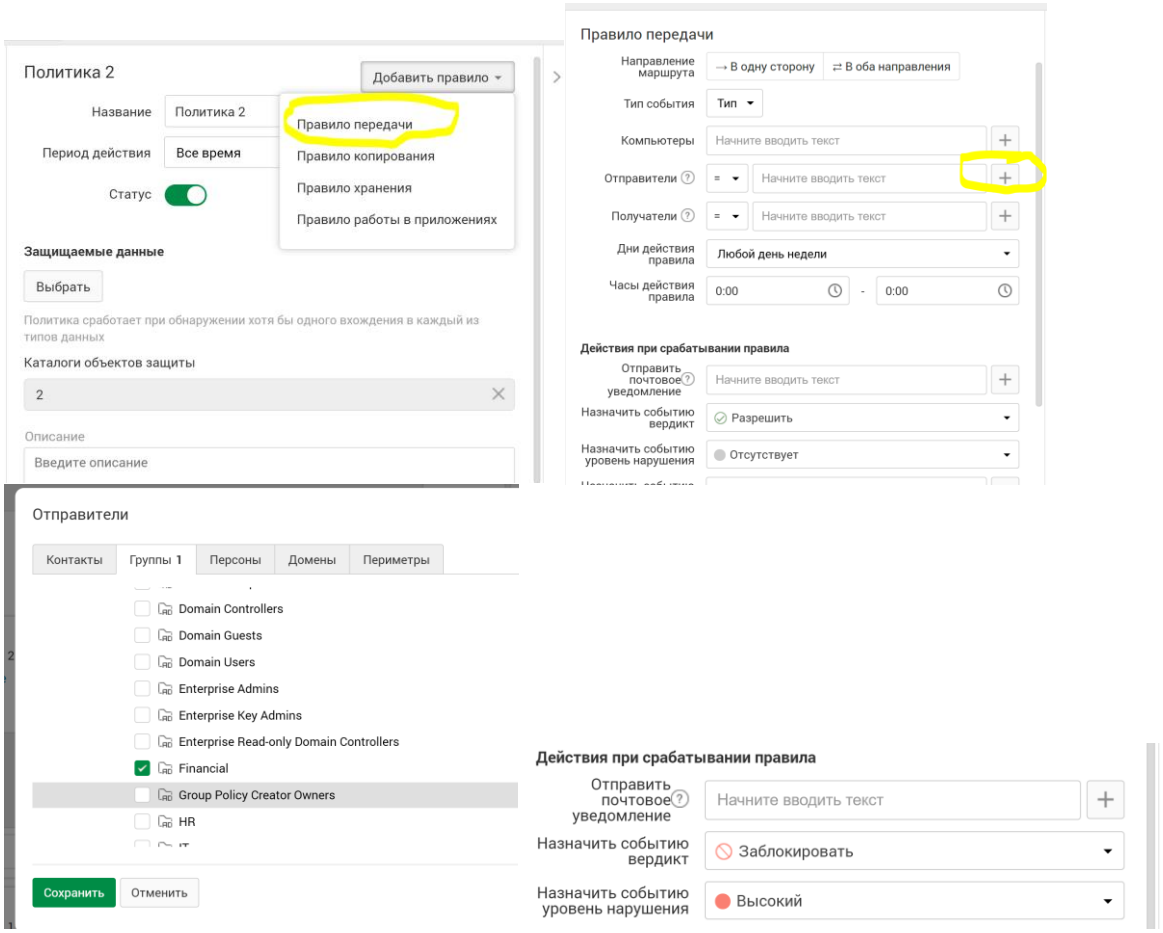



Создание объекта защиты
Название
Статус
Элементы технологий
Условия обнаружения
Добавить условие
Условие
Номер кредитной карты
Текстовый объект
Порог встречаемости
1
Добавить элемент технологий
или
Условие
Номер кредитной карты (16 цифр)
Текстовый объект
Порог встречаемости
1
Добавить элемент технологий
или
Условие
Кредитная карта
Графический объект
Добавить элемент технологий
Описание
Создать
Отменить




Политика 2
Добавить правило
Название
Политика 2
Период действия
Все время
Статус
Защищаемые данные
Выбрать
Каталоги объектов защиты
2
Описание
Введите описание


Выбор защищаемых данных
Каталоги объектов защиты 1
Объекты защиты
Файловые форматы
12
2
Грифованная информация
Договоры и контракты
Конкурсная документация
Маркетинг
Отдел кадров
Персональные данные
политика 1
политика 4
Сохранить
Отменить



В отчёт вставить скриншоты с настроенной политикой.
Проверить работоспособность политики и вставить скриншот из событий, подтверждающий работоспособность политики.

Практическая работа № 29 «Политики защиты данных на агентах в Traffic monitor»

Задание:

Политика V:
Требуется, чтобы Система отслеживала передачу исполняемого файла "Setup.exe" при наличии в трафике хотя бы 10% бинарного содержимого файла "Setup.exe". Для этого:

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

Политика М:
Требуется, чтобы Система отслеживала передачу документа "Внутренний регламент компании" при наличии в трафике хотя бы 30% текста документа. Для этого:

- ✓ Выберите каталог эталонных документов или создайте новый каталог.
- ✓ Внутри выбранного каталога добавьте новый документ и укажите для него тип данных:
  Текстовые (так как документ не содержит изображения и графики).
- ✓ Загрузите документ "Внутренний регламент компании" в качестве эталонного документа.
- ✓ Укажите название эталонного документа, например, ВНУТРЕННИЙ_РЕГЛАМЕНТ_КОМПАНИИ.
- ✓ Установите для атрибута Порог цитируемости текстовых данных значение 30.
- ✓ Передачу документа отслеживать и внутри, и наружу. Уровень «средний». Детектировать.
  Скриншот ,подтверждающий создание политики и её работоспособность.

Практическая работа № 30 «Создание политик контроля персон в Traffic monitor»

Задание:

Политика С
Необходимо вести контроль за Отделом кадров на предмет передачи персональных данных сотрудников за пределы компании.
Вердикт: разрешить
Уровень нарушения: средний;
Тег: Политика С

В отчет вставить скриншот создания политики.
В отчет вставить скриншоты, подтверждающие работоспособность политики.

Политика 10
В последнее время сотрудники стали чаще обсуждать популярные сериалы в мессенджерах и социальных сетях, из-за чего упала общая производительностьна 5%. Было решено отследить, кто больше всего занимается не рабочей
деятельностью, для чего необходимо создать политику для отслеживания 5(пяти) популярных на данный момент сериалов при передаче через веб- сообщения и почту.

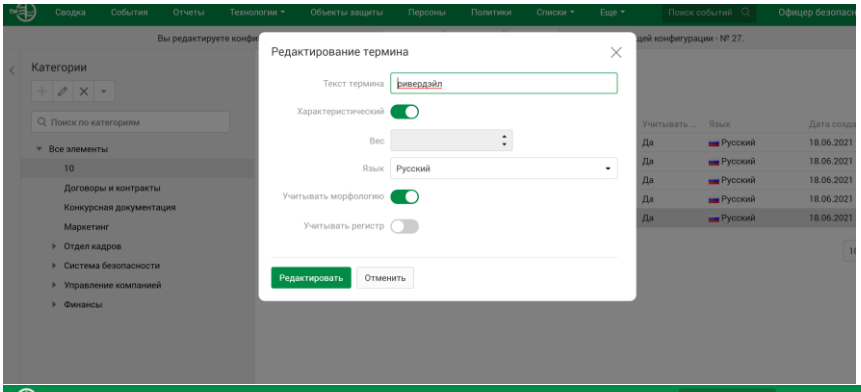
Список сериалов:

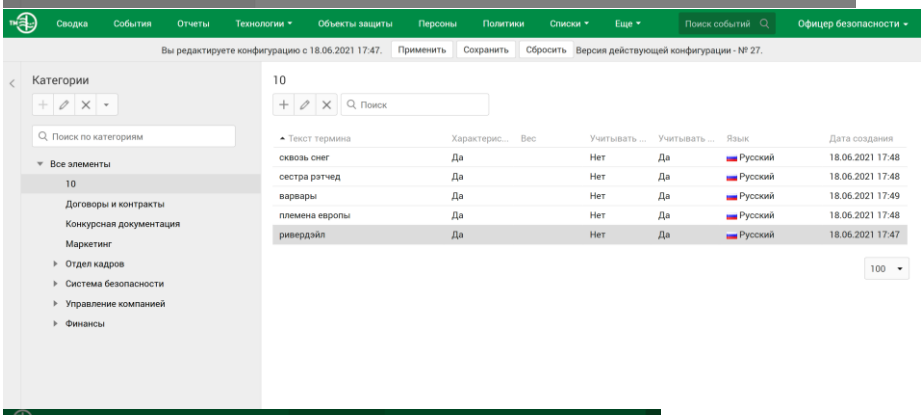
Ривердэйл, Сестра Рэтчед, Племена Европы, Сквозь снег, Варвары

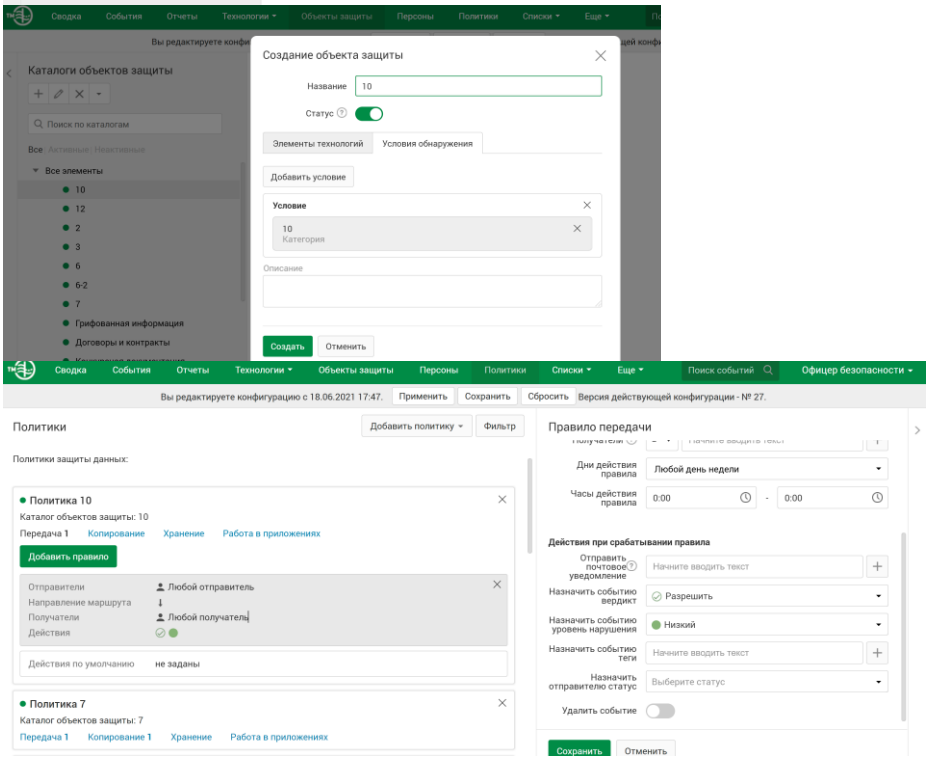
Вердикт: разрешить √

Уровень нарушения: низкий •

Тег: Политика 10







В отчет вставить скриншот создания политики.
В отчет вставить скриншоты, подтверждающие работоспособность политики.

Практическая работа № 31 «Создание политик с использованием правил передачи в Traffic monitor»

Задание:

Политика А

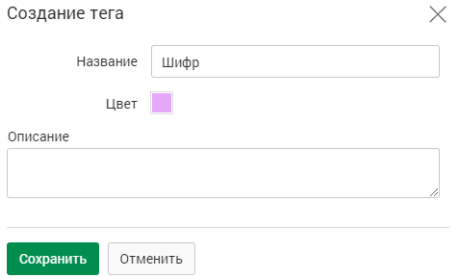
Необходимо поставить на мониторинг все зашифрованные и запароленные данные, т.к. попытки передачи таких данных несут потенциальную опасность утечки.
Уровень угрозы низкий, не блокировать, тег «Шифр».

Мониторинг данных

Выполнение данного задания сразу можно начать с создания политики, но предварительно создать тег «Шифр».

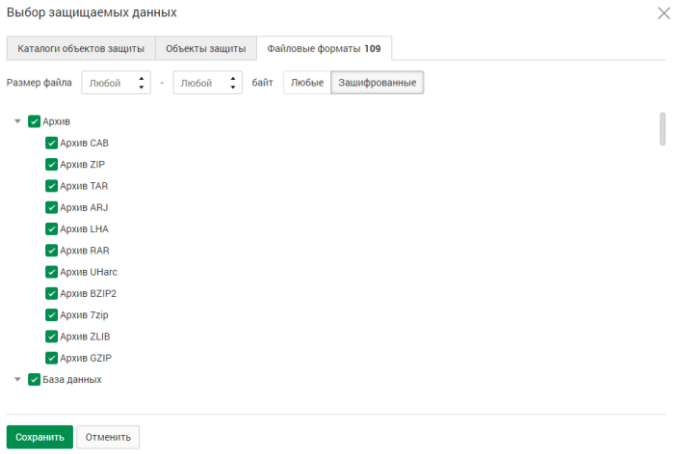
Добавление тега

Перейти в раздел «Списки» → «Теги», откроется страница управления тегами. Нажать знак «+», указать название тега «Шифр» и цвет

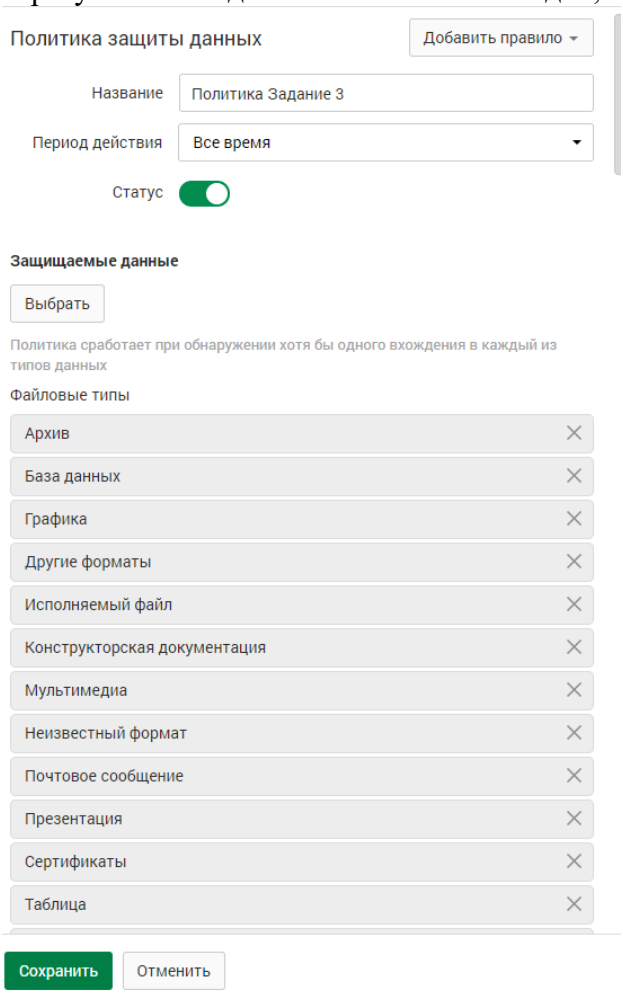


Создание политики

В панели добавления политики защиты данных выбираем объект защиты, переходим на вкладку «Файловые форматы» и активируем кнопку «Зашифрованные». Из списка выбираем все форматы файлов

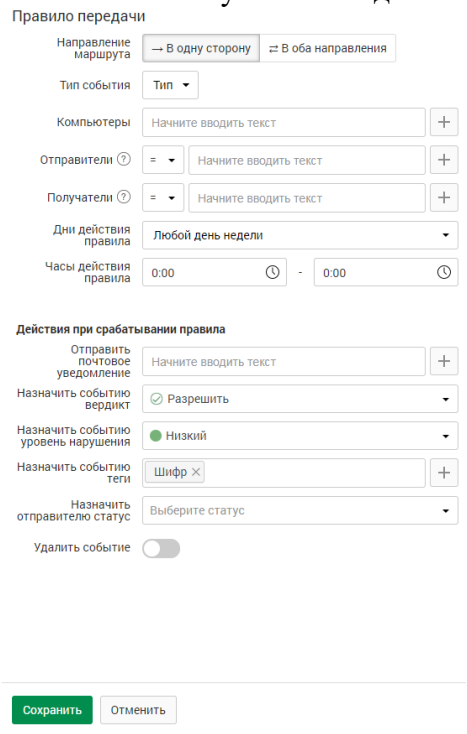


В результате созданная политика выглядит, как представлено:



Добавление правила передачи

В соответствии условию задания выставляем следующие параметры



–Поля «Получатели» и «Отправители» оставить по умолчанию, что будет означать любого отправителя и получателя

–Назначить событию вердикт «Разрешить», так как по условию требуется вести мониторинг данных

–Назначить событию уровень «Низкий»

–Нажать «Сохранить»

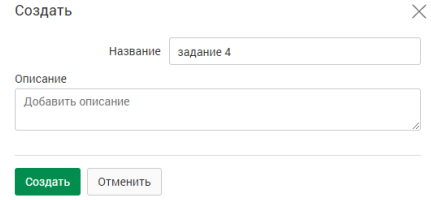
В отчёт вставить скриншот, подтверждающий создание политики.
В отчет вставить скриншот, подтверждающий работоспособность политики.

Политика В

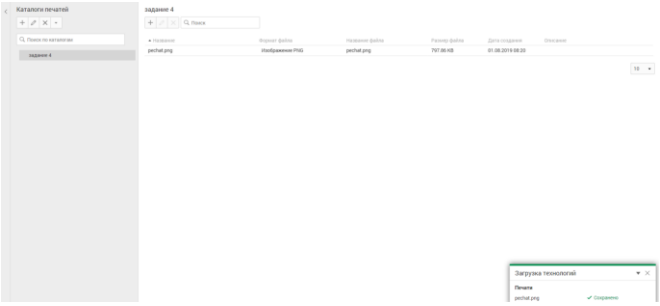
Для контроля за движением официальных документов необходимо вести наблюдение за передачей любых документов с печатями за пределы компании.
Уровень угрозы низкий, не блокировать, тег «Печать».
Для выполнения задания используется файл pechat.png.

Контроль документов с печатями

В разделе «Технологии» выбираем пункт «Печати» и нажимаем знак «+». Появится окно



Создания каталога, в котором вводим название и нажимаем «Создать». Затем в самом каталоге снова нажать «+» и выбрать файл с печатью. После этот файл будет загружен в систему и добавлен в каталог



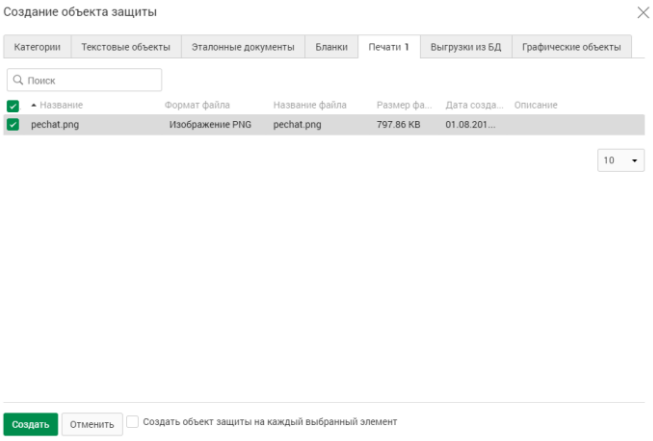
Добавление тега

Перейти в раздел «Списки» → «Теги», нажать знак «+», указать название тега «Печать» и цвет

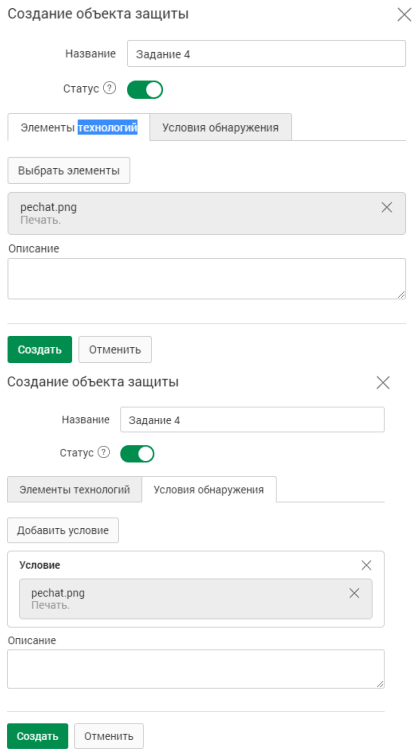
Создание объекта защиты

Для создания объекта защиты необходимо перейти в раздел «Объект защиты».
Создать каталог объектов защиты с названием «Задание 4».
Для создания объекта защиты требуется выбрать созданный каталог и нажать знак «+», в появившемся окне:

–В пункте «Печати» выбрать «pechat.png»

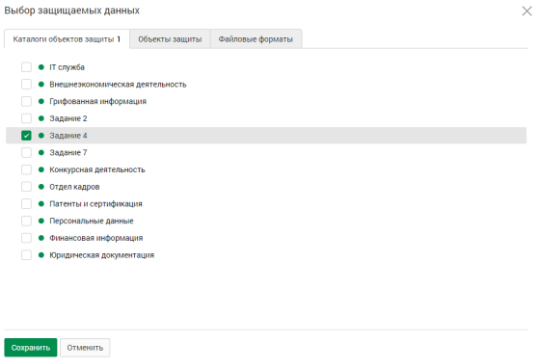


–Нажать «Создать»

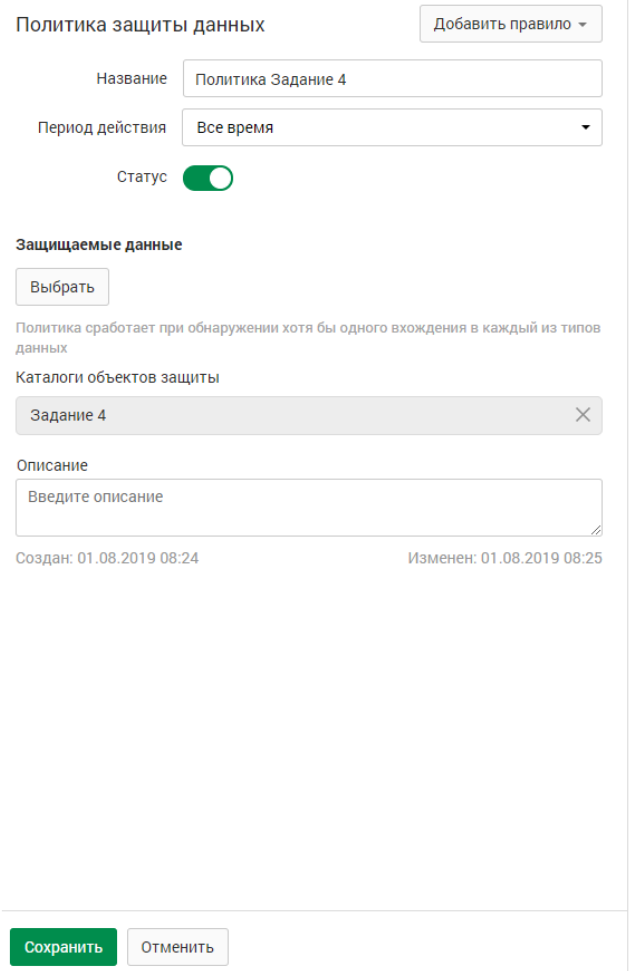


Создание политики

В панели добавления политики защиты данных выбираем объект защиты «Задание 4» из пункта «Каталоги объектов защиты»

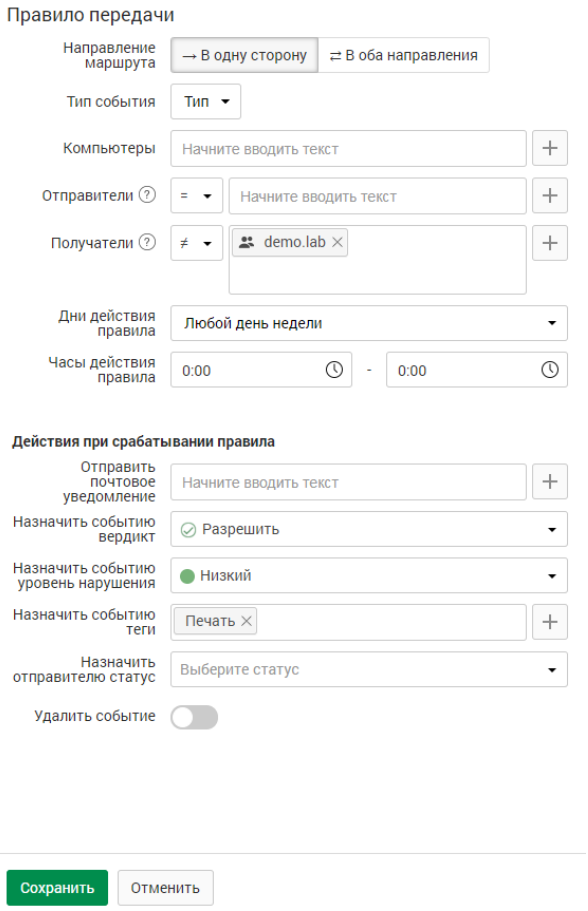


В результате создаваемая политика выглядит, как представлено:



Добавление правила передачи

В соответствии условию задания выставляем следующие параметры:



–В поле «Получатели» выбираем операцию ≠, затем знак «+» → вкладка «Группы» → поставить галочку «demo.lab»

–Назначить событию вердикт «Разрешить»

–Назначить событию уровень «Низкий»

–Тег «Печать»

–Нажать «Сохранить»

В отчёт вставить скриншот, подтверждающий создание политики.
В отчет вставить скриншот, подтверждающий работоспособность политики.

Практическая работа № 32 «Создание политик с использованием правил копирования в Traffic monitor»

Задание:

Политика D
Необходимо контролировать копирование документов, содержащих печать компании на облачные хранилища, на флешки и на сетевые ресурсы.
Вердикт: разрешить
Уровень угрозы: средний
тег: Политика D.
В отчёт вставить скриншот, подтверждающий создание политики.
В отчёт вставить скриншот, подтверждающий работоспособность политики.

Политика E
Необходимо контролировать копирование на флешки и облачные хранилища информацию, содержащую пароли организации (политика паролей: 8 знаков, прописные и строчные буквы, использование цифр) для сотрудников IT-отдела.
Вердикт: запретить
Уровень угрозы: высокий
тег: Политика E.
В отчёт вставить скриншот, подтверждающий создание политики.
В отчёт вставить скриншот, подтверждающий работоспособность политики.

Практическая работа № 33 «Создание политик с использованием правил хранения в Traffic monitor»

Задание:

Политика I
Запретить хранение документов, содержащих персональную информацию на общих сетевых ресурсах.
Вердикт: запретить
Уровень угрозы: высокий
Тег: политика I
В отчёт вставить скриншот с работающей политикой и скриншот с работоспособностью.

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

Практическая работа № 34 «Создание политик с использованием правил работы в приложениях в Traffic monitor»

Задание:

Политика Z
Поставить на контроль использование буфера обмена в документах приложения MS Excel для сотрудников отдела кадров.
Вердикт: разрешить

Уровень угрозы: низкий
Тег: Политика Z
В отчёт вставить скриншот созданной политики.
В отчёт вставить скриншот проверки работоспособности политики.

Политика Y
Контролировать использование MS Word сотрудниками IT-отдела по выходным дням.
Вердикт: разрешить
Уровень угрозы: низкий
Тег: Политика Z
В отчёт вставить скриншот созданной политики.
В отчёт вставить скриншот проверки работоспособности политики.

Практическая работа № 35 «Создание политик с использованием регулярных выражений в Traffic monitor»

Задание:
Политика 6

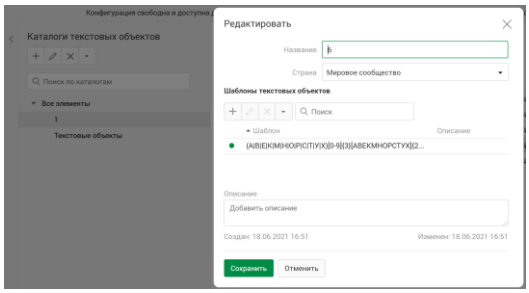
Стало известно, что сотрудники охраны (Security) ООО «Повозка» за определенную сумму пропускают автомобили из близлежащих домов наслужебную парковку. В связи с ужесточением корпоративной политики в компании, правом въезда на территорию обладает только генеральный директор.

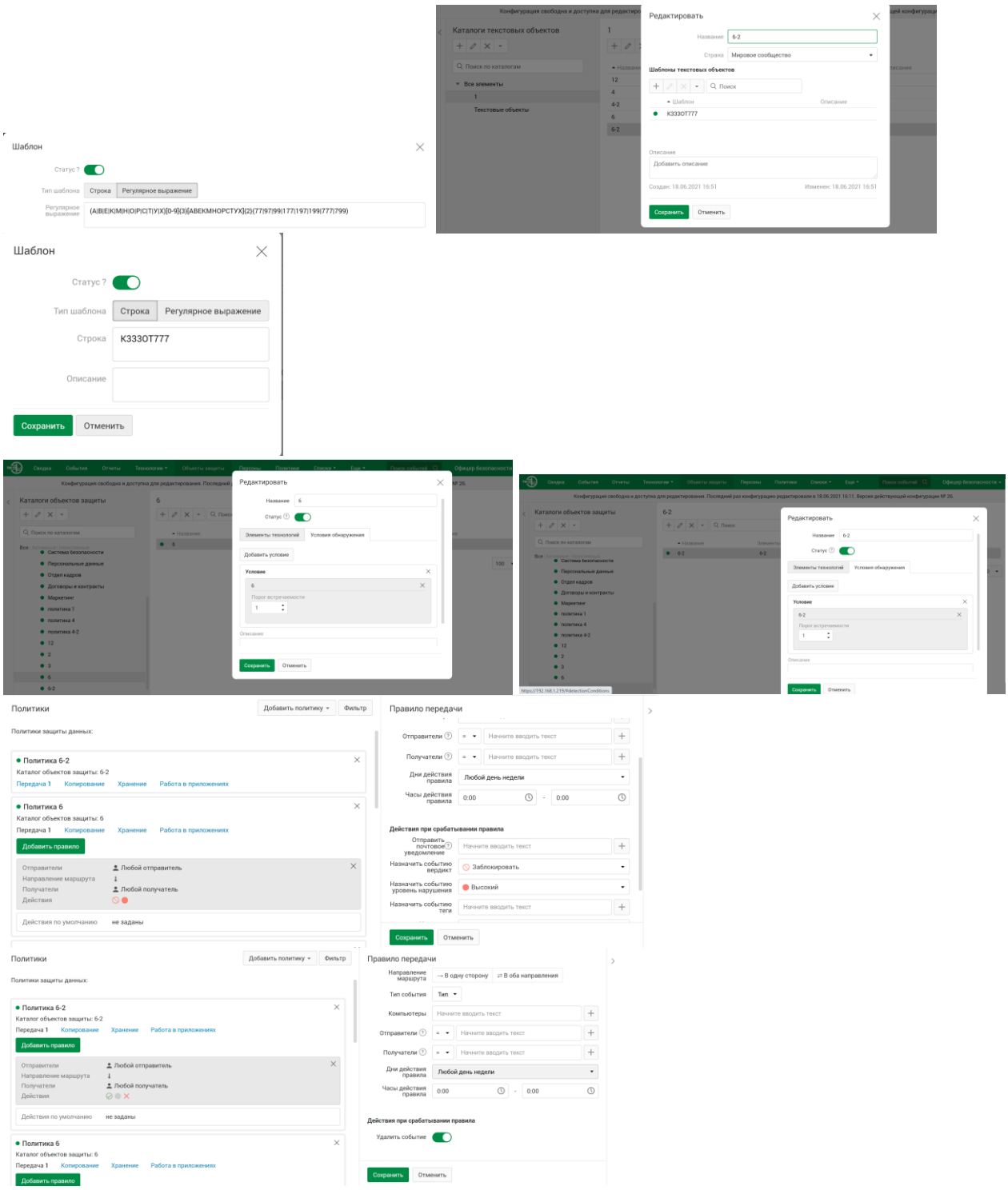
Сотрудники охраны ведут журнал учета автомобилей в электронном виде иобмениваются между собой данными о припаркованных автомобилях.

Необходимо детектировать номера всех автомобилей, которые незаконно парковались на частной территории компании ООО «Повозка», исключая номер автомобиля генерального директора К333ОТ777.

Буквы, используемые в автомобильных номерах:

А, В, Е, К, М, Н, О, Р, С, Т, У, Х (Верхний регистр)
Цифры, используемые в автомобильных номерах:
000 – 999
Регионы автомобильных номеров, подлежащие детектированию:
77, 97, 99, 177, 197, 199, 777, 799
Вердикт: заблокировать ×
Уровень нарушения: Высокий •
Тег: Политика 6





<u>В отчёт вставить скриншот с настроенной политикой.</u>
<u>В отчет вставить скриншоты, подтверждающие работоспособность политики.</u>

Политика 7

В честь юбилея компании была запущена акция с промокодами на скидку в 50% на перевозки для постоянных клиентов. По условиям акции промокод выдается только по запросу постоянного клиента. Есть вероятность утечки промокодов, в связи с этим необходимо контролировать защитить учечку текстового документа, содержащего промокоды («промокоды.docx»). Стоит учесть, что сотрудники могут воспользоваться жестким диском или флешнакопителем, для того чтобы завладеть акционными купонами, а также слить не весь файл,

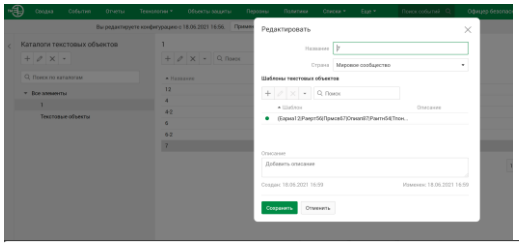
а один или несколько купонов. Запретить передачу данных, содержащих информацию об этих купонах, а также отслеживать копирование этой информации на внешние носители, тег «Политика 7»

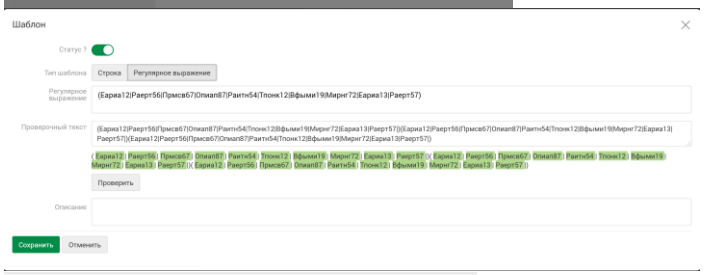
Проверить работоспособность на все купоны и на 1-2 купона.

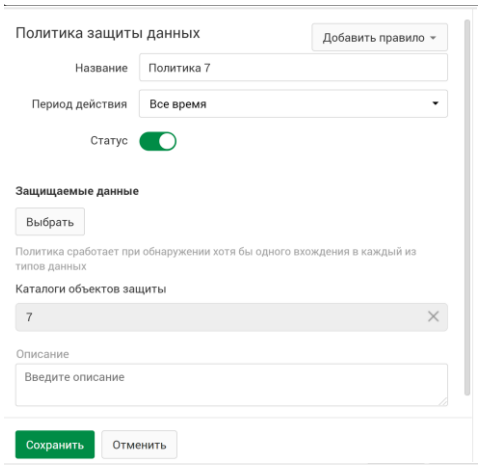
Вердикт: заблокировать ×

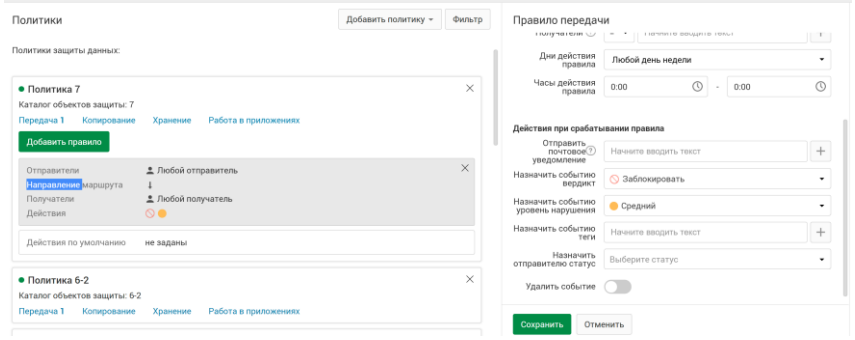
Уровень нарушения: средний •

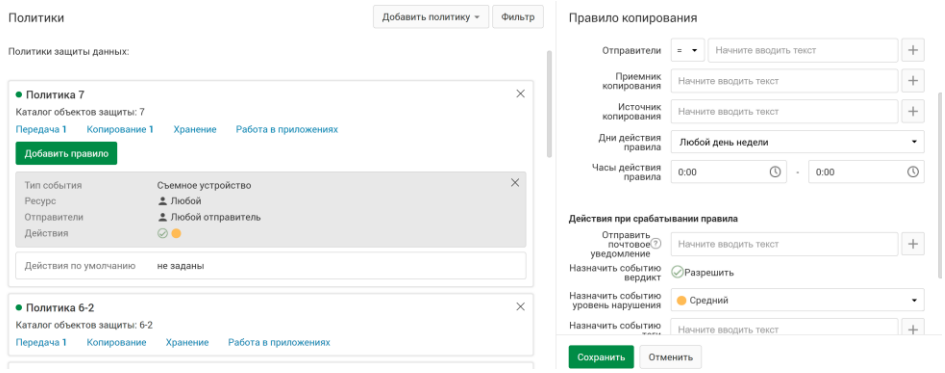
Тег: Политика 7











В отчёт вставить скриншот с настроенной политикой.
В отчет вставить скриншоты, подтверждающие работоспособность политики.

Политика 5

Необходимо создать политики для отслеживания документов (передача икопирование), содержащих договор компании (договор компании.docx).

Политики должны работать следующим образом (за периметр компании):

1. Если передается только договор компании (шаблон и заполненныйшаблон, до 25% изменений) – разрешать передачу, уровень угрозы низкий, тег «Политика 5.1».
2. Если передается договор компании, в котором присутствует фамилия генерального директора, а также главного бухгалтера – разрешать передачу, уровень угрозы средний, дополнительный тег «Политика 5.2». Политика не должна срабатывать, если в документе только фамилия директора или только фамилия бухгалтера.
3. Если передается договор компании, в котором присутствует фамилия генерального директора, главного бухгалтера, а также стоит печать компании (ООО Повозка) – разрешить передачу, уровень угрозы высокий, тег «Политика 5.3».

Проверить работоспособность. Политики не должны срабатывать внутри компании, только при передаче за периметр.

Все политики, объекты и прочие элементы должны называться в соответствии с номерами (например Объект 5.1, Политика 5.2, Технология 5.3 и т.д.)

Вердикт 1: Разрешить □

Уровень нарушения 1: низкий •

Тег 1: Политика 5.1

Вердикт 2: Разрешить □

Уровень нарушения 2: средний •

Тег 2: Политика 5.2

Вердикт 3: Заблокировать ×

Уровень нарушения 3: высокий •

Тег 3: Политика 5.3

В отчёт вставить скриншот с настроенной политикой.
В отчет вставить скриншоты, подтверждающие работоспособность политики.

Практическая работа № 36 «Создание и изменение виджетов в Traffic Monitor»

Задание 1
Создайте новую вкладку сводки в разделе «Сводка» под названием «Чемпионат» и создайте в ней 4 виджета:

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

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

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

Задание 4
Сделайте выборку (запрос), в котором будет отображено только по одному событию каждого типа: передачи, копирования, буфера обмена и хранения.

Вставьте скриншоты по каждому заданию в отчёт.
Корректно выполненным заданием является наличие событий в системе и наличие скриншотов событий.

Практическая работа № 37 «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.

Практическая работа № 38 «Работа с требованиями и рекомендациями по технической защите конфиденциальной информации»»

Задание 1:

Используя текст выписки из специальных требований и рекомендаций по технической защите конфиденциальной информации ответить на следующие вопросы:

- ✓ Кем и в каком году утверждён документ СТР-К?
- ✓ Какие вопросы определяет документ СТР-К?
- ✓ Перечислите объекты защиты документа СТР-К

Задание 2:

Используя текст Руководящего документа Безопасность информационных технологий Критерии оценки безопасности информационных технологий от 19.06.2020 г. №187 ответить на следующие вопросы:

- ✓ Перечислите источники требований безопасности для ОО
- ✓ Объясните связь между данными пользователей и данными ФБО
- ✓ Что включает в себя аудит безопасности?
- ✓ Какие компоненты входят в аудит безопасности?
- ✓ Какие компоненты входят в связь?
- ✓ Какие компоненты входят в защиту данных пользователя?
- ✓ Какие компоненты входят в идентификацию и аутентификацию?
- ✓ Какие компоненты входят в управление безопасностью?

Практическая работа № 39 «Работа с нормативно-правовой документацией, регламентирующей порядок проведения аттестации объектов информатизации

Задание 1:

Используя текст ГОСТ РО 0043-004-2013 ответить на следующие вопросы:

- ✓ Что должна включать программа аттестационных испытаний АС?
- ✓ Что такое АС?
- ✓ Что должна включать программа аттестационных испытаний ВП?
- ✓ Что такое ВП?
- ✓ Что должны содержать методики аттестационных испытаний АС?
- ✓ Что должны содержать методики аттестационных испытаний ВП?

Задание 2:

Придумайте организацию. Используя ГОСТ РО 0043-004-2013 Приложение Б заполните для своей придуманной организации Программу и методику аттестационных испытаний объектов информатизации (раздел «Общие положения»).

Практическая работа № 40 «Развёртывание защищённой сети ViPNet»

Задание 1 Установка ПК ViPNet Administrator 4:

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

Формулировка задания

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

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

Установка серверного приложения ViPNet ЦУС

1. Для установки серверного приложенйя ViPNet Центр управления сетью откройте файл Setup.exe из каталога серверного приложения ViPNet Administrator.

2. В окне Установка ViPNet Administrator Центр управления сетью будет предложено установить дополнителъиде программное обеспечение. Список необходимого дополнительного ПО зависит от ранее установленных на компьютер программ. Чтобы начать установку, нажмите, кнопку Продолжить

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

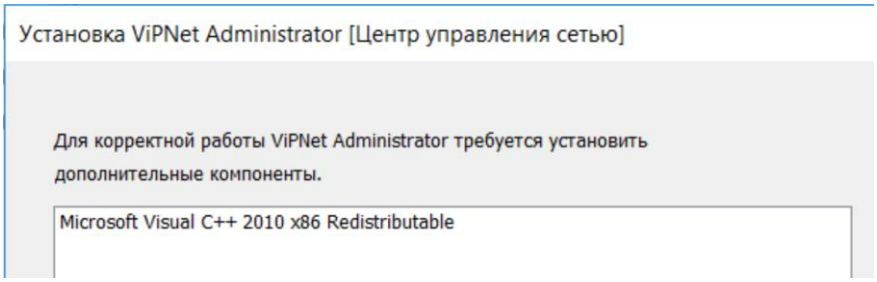


Рис. Установка дополнительного ПО

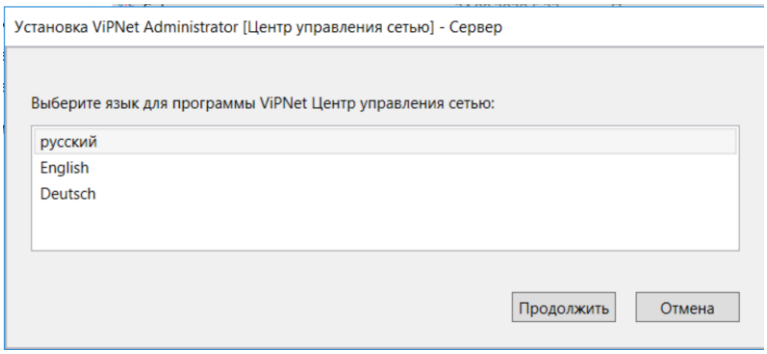


Рис. Выбор языка программы

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

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

6. В появившемся окне о создании сервера базы данных нажмите кнопку Да.

При этом на SQL-сервере будут созданы:

• База данных с именем ViPNetAdministrator.

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

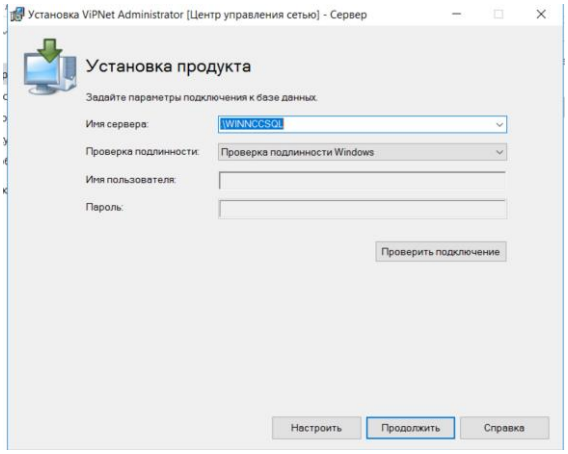


Рис. Параметры подключения к базе данных

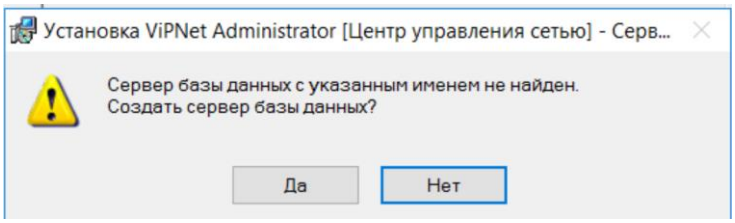


Рис. Создание сервера базы данных

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

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

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

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

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

9. На странице Установка продукта нажмите Продолжить.

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

11. По завершении установки нажмите кнопку Закрыть.

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

В отчёт вставить скриншот с установленным серверным приложением ЦУС.

Установка клиентского приложения ViPNet ЦУС

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

1. Для установки клиентского приложения ViPNet Центр управления сетью откройте файл Setup.exe из каталога клиентского приложения ViPNet Administrator.

2. В появившемся окне выберите язык для клиентского приложения ViPNet ЦУС и нажмите Продолжить (рис.).

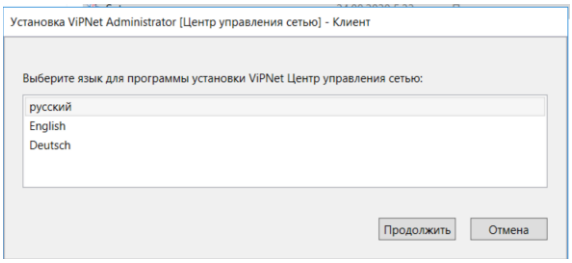


Рис. Выбор языка программы

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

4. На странице Способ установки нажмите Установить сейчас (рис.).

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

— путь к папке установки программы на компьютере;

— имя пользователя и название организации;

— название папки программы и ее расположение в меню Пуск.

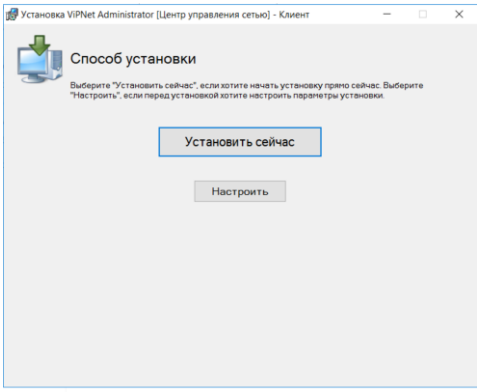


Рис. Способ установки

5. По завершении установки нажмите кнопку Закрыть.

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

В отчёт вставить скриншот с установленным клиентским приложением ЦУС.

Установка ViPNet Удостоверяющий и ключевой центр

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

1. Для установки компонента ViPNet Удостоверяющий и ключевой центр откройте файл Setup.exe из каталога удостоверяющего и ключевого центра ViPNet Administrator.

2. Подождите, пока на компьютер будет автоматически установлено необходимое программное обеспечение, в том числе программа ViPNet CSP.

3. В окне Установка ViPNet Administrator [Удостоверяющий и ключевой центр] на странице Лицензионное соглашение ознакомьтесь с условиями лицензионного соглашения. В случае согласия установите соответствующий флажок. Затем нажмите кнопку Продолжить.

4. На странице Способ установки нажмите кнопку Установить сейчас (рис.).

5. Если потребуется настроить параметры установки, то нажмите кнопку Настроить на странице Способ установки и укажите:

— путь к папке установки программы на компьютере;

— имя пользователя и название организации;

— название папки программы и её расположение в меню Пуск.

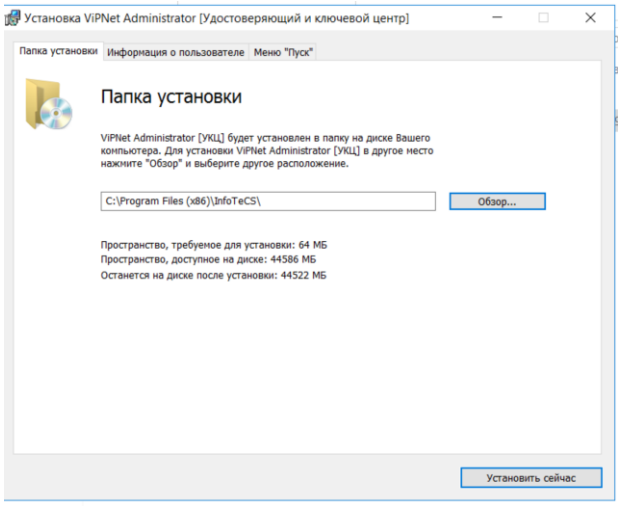


Рис. Настройка установки

6. По окончании установки нажмите кнопку Закрыть,

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

В отчёт вставить скриншот с установленным УКЦ.

Задание 2:

Ответить на следующие вопросы:

— Из каких компонентов состоит программный комплекс ViPNet Administrator 4?

— Какие функции выполняет ЦУС?

— Какие функции выполняет УКЦ?

— Какие функции выполняет ViPNet Coordinator?

— Какие функции выполняет ViPNet Client?

— Назовите состав ЦУС

— Назовите рабочие каталоги ЦУС/УКЦ?

Практическая работа № 41 «Создание структуры защищённой сети ViPNet»

Задание:

Создать структуру защищенной сети в соответствии с заданной схемой, настроить связи пользователей (в соответствии с матрицей связей (табл. 2.4) в ЦУС и сформировать дистрибутивы Ключей для сетевых узлов В УКЦ.

Таблица Пользователи и сетевые узлы (клиенты)

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

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

— Связь узла с Центром управления сетью.

— Между координатором и зарегистрированными на нем клиентами.

— Связи между координатором и клиентами, для которых данный координатор назначен сервером IP-адресов.

— Связь между сетевым узлом и координатором, выбранным для организации соединений с внешними узлами.

— Между координаторами, образующие межсерверный канал.

— Связь между узлом с ПО ViPNet Policy Manager и подчиненными ему СУ

— Связи шлюзовых координаторов своей сети со шлюзовыми координаторами доверенных сетей

— Связи Центра управления сетью с Центрами управления сетью доверенных сетей.

Таблица. Матрица связей пользователей

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

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

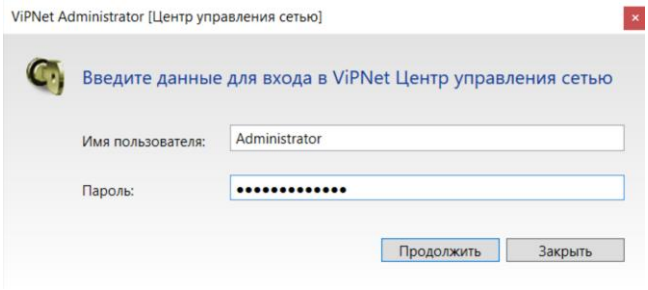
Рекомендуется устанавливать в первую очередь связи пользователей, так как в данном случае связи узлов будут установлены автоматически.

На каждом защищенном узле в программе ViPNet Монитор в разделе «Защищенная сеть» отображается список сетевых узлов, с которыми, связан данный узел. Однако для отображе-

ния в программе ViPNet Монитор узла с программой ViPNet ЦУС необходимо дополнительно создать связь между пользователями СУ и ЦУС.

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

Для начала работы с программой ViPNet ЦУС:



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

2. В появившемся окне введите имя и пароль - Administrator, нажмите кнопку Продолжить (рис.).

3. После загрузки программы будет предложено сменить пароль! Чтобы сменить пароль, введите текущий пароль (Administrator)} новый пароль, а затем нажмите кнопку Продолжить. В рамкам практического занятия задайте новый пароль - 11111111 (рис.).

4. В окне Начало работы с ViPNet Центр, управления сетью с помощью кнопки Обзор укажите путь к. файлу лицензии на сеты ViPNet (*.itcslic или infotecs.reg) и нажмите кнопку Продолжить (рис.)

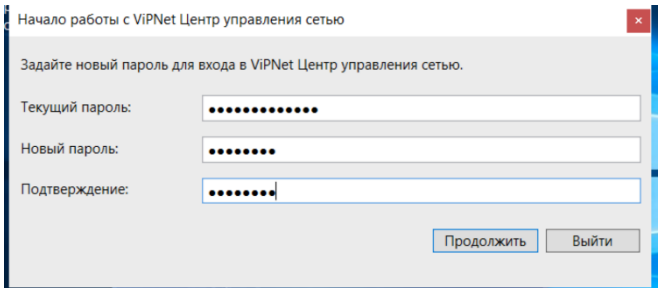


Рис. Смена пароля

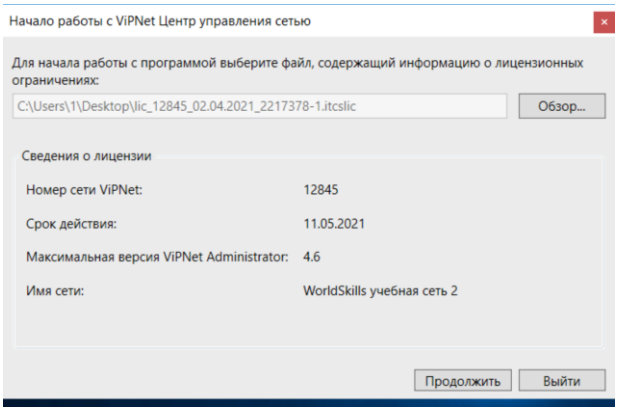


Рис. Выбор файла лицензии

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

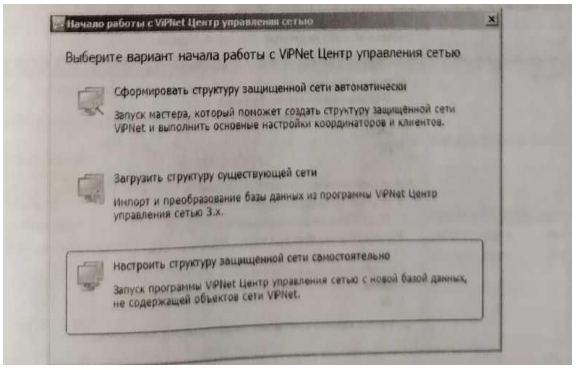
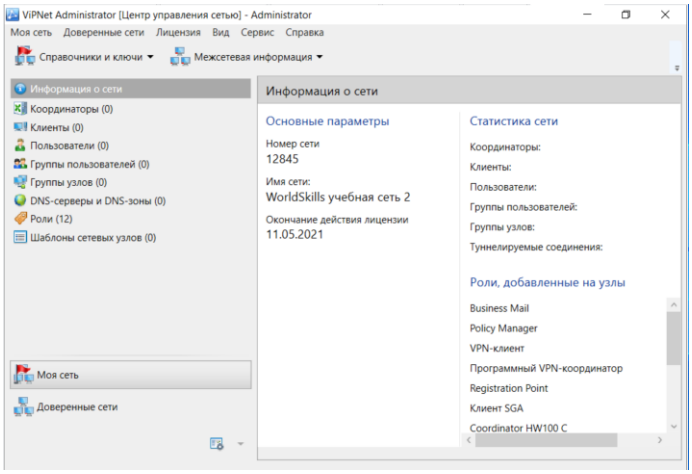


Рис. Выбор варианта начала работы с ЦУС



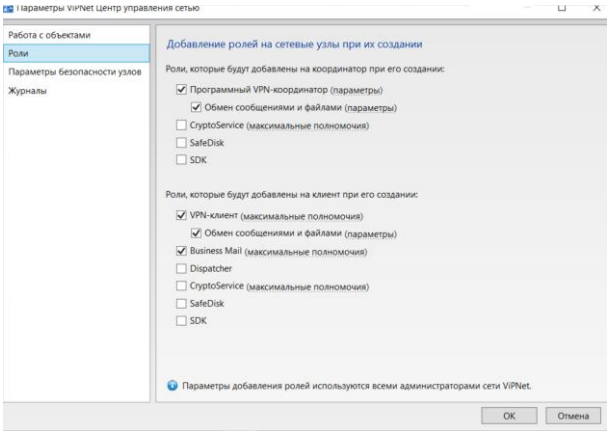
6. Откроется главное окно программы (рис).

7. Проверьте первоначальные настройки программы ViPNet Центр управления сетью. Для этого выполните следующие действия:

— В меню Сервис выберите пункт Параметры;

— В открывшемся окне перейдите в раздел Роли;

— Затем, если обнаружите различия, задайте значения п ров в соответствии с рис.



Примечание. В реальной сети рекомендуется задавать средний или минимальный уровень полномочий. Полномочия задаются при нажатии на подчеркнутые мелким пунктиром параметры, расположенные в скобочках.

Теперь можно приступить к созданию структуры защищённой сети.

Создание координаторов

В соответствии со схемой развертывания ViPNet в локальной сети компании необходимо создать сетевые узлы: Координатор Центр офис и Координатор Филиал.

— Для добавления в сеть ViPNet нового координатора выполните следующие действия:

— В окне ViPNet Центр управления сетью выберите представление Моя сеть.

— На панели навигации выберите раздел Координаторы.

— В разделе Координаторы на панели нажмите кнопку Создать.

— В появившемся окне задайте имя Координатор Центр офис, оставьте флажок Создать одноименного пользователя и нажмите кнопку Создать. В данном случае нам не требуется снимать флажок, так как имя узла и имя пользователя координатора, будут совпадать. Таким образом не придется совершать лишних действий (это ускорит процесс создания структуры сети).

Аналогичным образом создается сетевой узел Координатор Филиал.

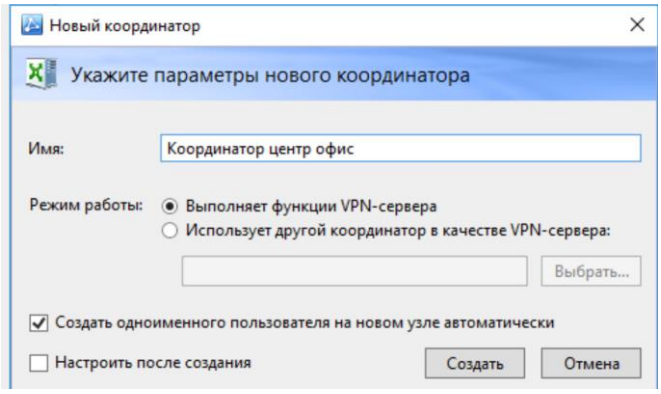


Рис. Параметры нового координатора

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

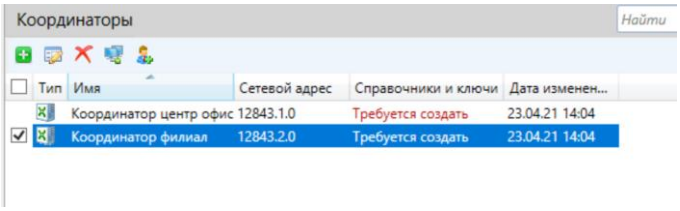


Рис. Раздел «Координаторы» — «Моя сеть»

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. (рис. 2.19).

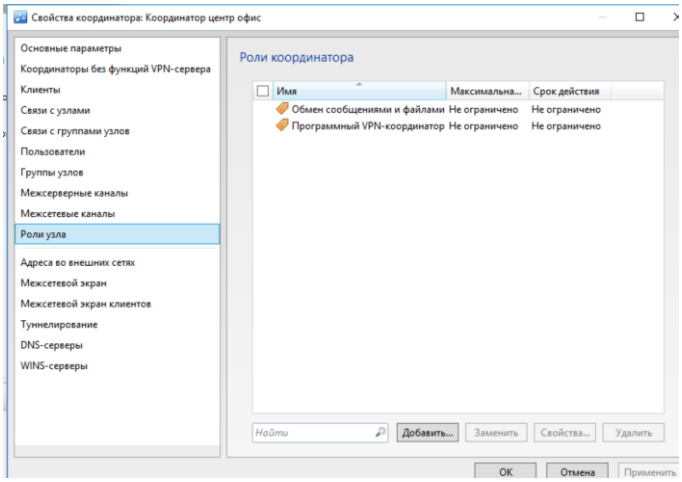


Рис. Роли координатора

Практическая работа № 42 «Создание 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 (рис.) 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.

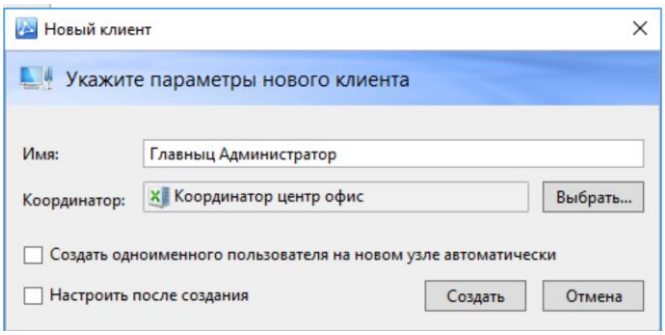


Рис. Параметры нового клиента

Аналогичным образом создаются остальные клиенты.

После создания клиентов раздел Клиенты окна ViPNet ЦУС представления Моя сеть имеет следующий вид (рис.):

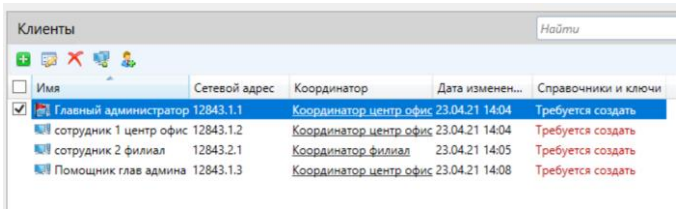


Рис. Раздел «Клиенты» представления «Моя сеть»

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.

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 admin Петров, выберите сетевой узел Главный администратор и нажмите кнопку Создать (рис.)

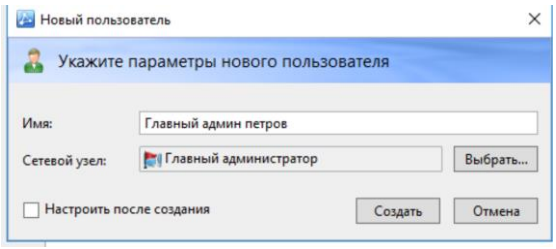


Рис. Параметры пользователя

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.):

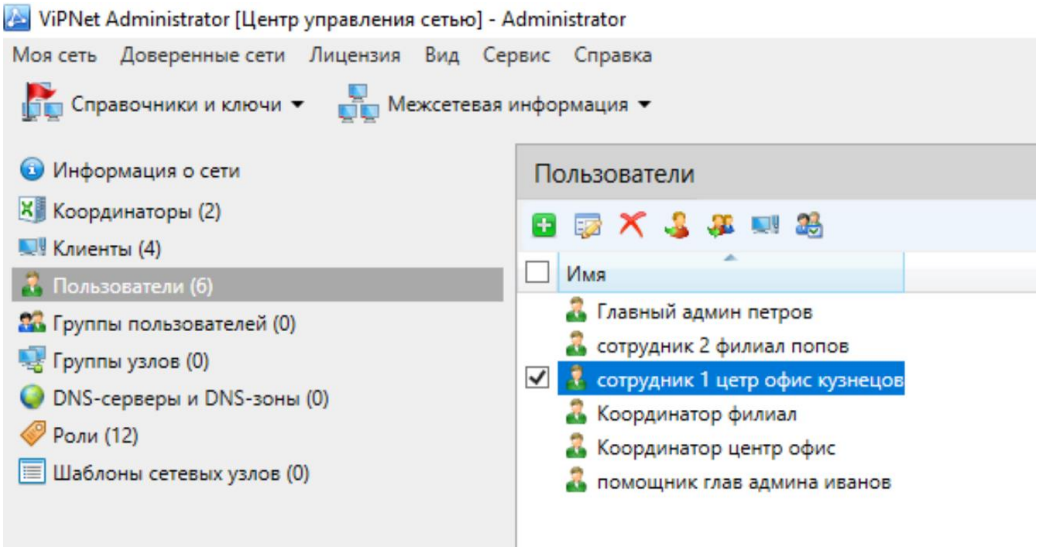


Рис. Раздел «Пользователи» («Моя сеть»)

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 (рис.).

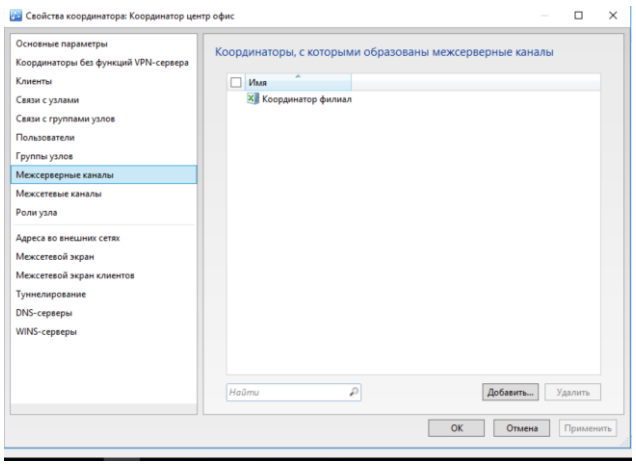


Рис. Фрагмент вкладки «Межсерверные каналы»

Теперь необходимо создать связи между пользователями в соответствии с матрицей связей пользователей защищенной сети (табл.).

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 (рис.).

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 (рис.):

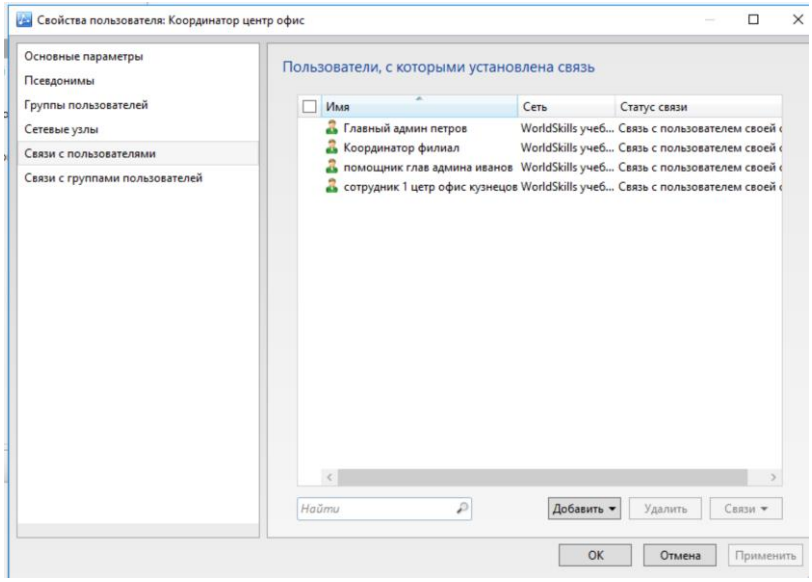


Рис. Вкладка «Связи с пользователями» Координатора Центр офис

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

После этого автоматически будут созданы связи между узлами, к которым относятся связанные пользователи (см. Вкладку Связи с узлами - рис.).

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» (рис.).

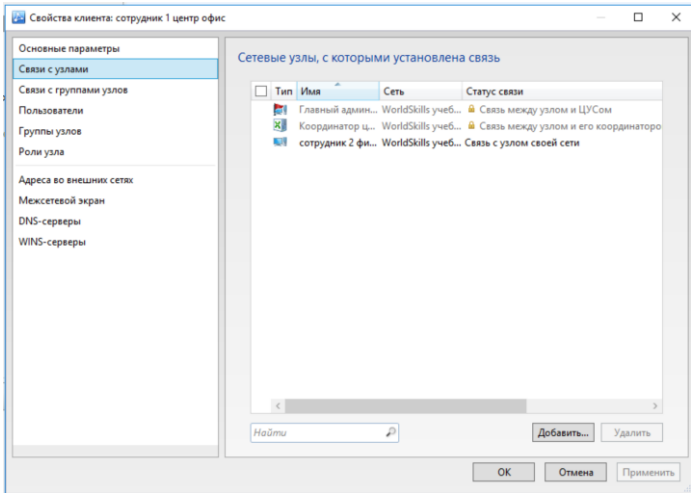


Рис. Вкладка «Связи с у злами» клиента Сотрудник. 1 Центр

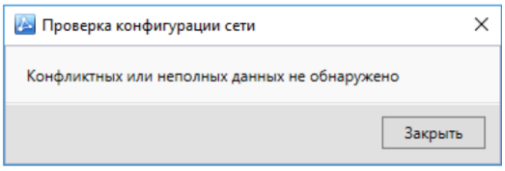
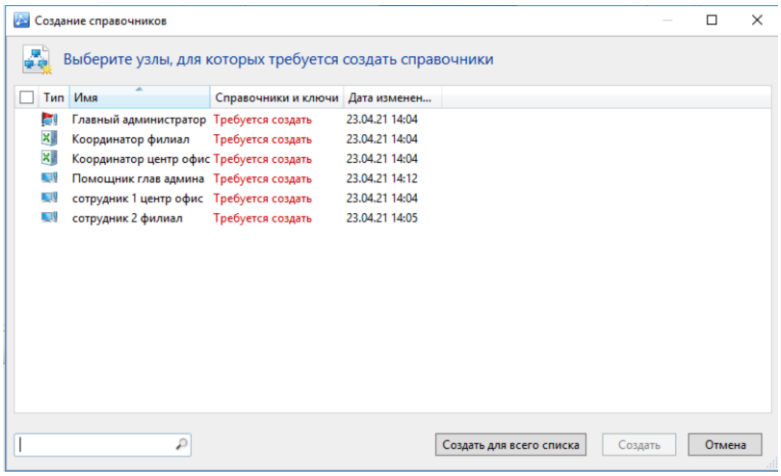


Рис.Положительный результат проверки конфигурации сети

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 (рис.).



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.

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 пер-

вичной инициализации (рис.).

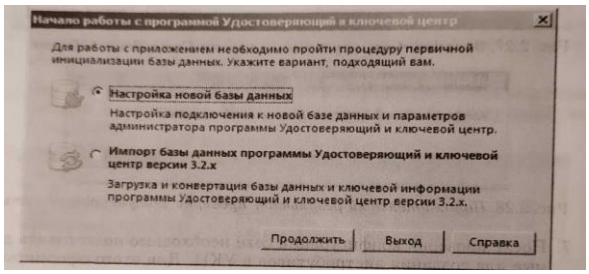


Рис. Выбор базы данных

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 (рис.).

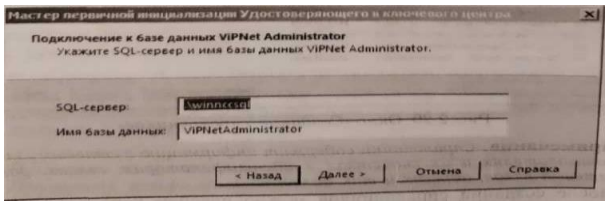


Рис. Подключение к базе данных ViPNet Administrator

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 (рис.).

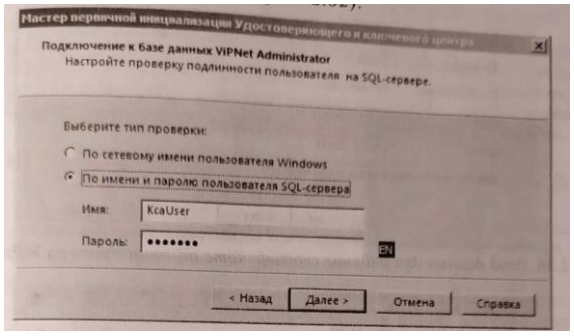


Рис. Задание имени и пароля для подключения к SQL-серверу

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

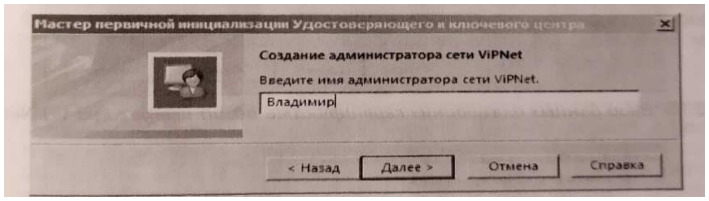
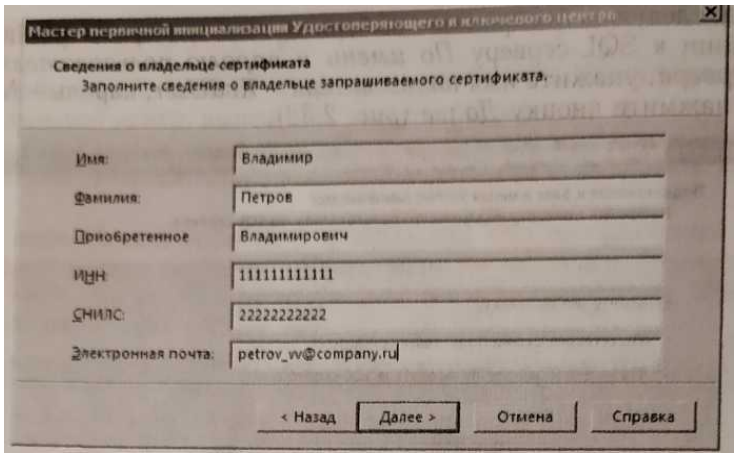
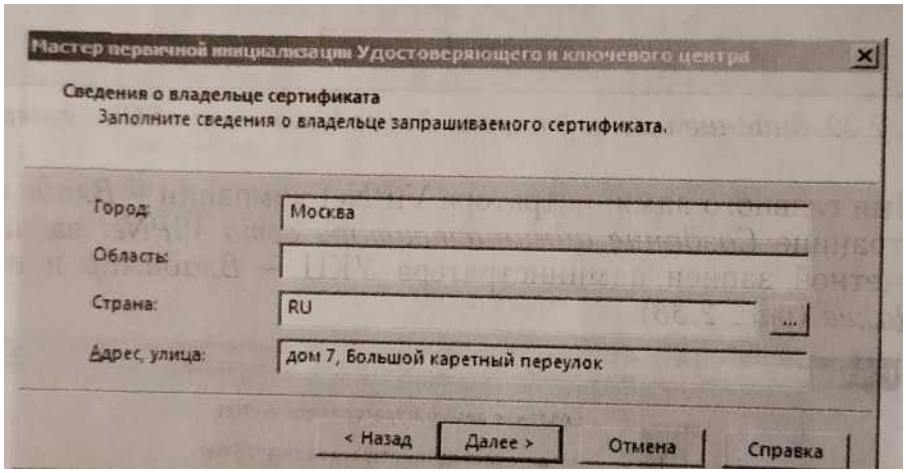


Рис. Ввод имени администратора ViPNet

7. На страницах Владелец сертификата введите личные данные, которые будут указаны в



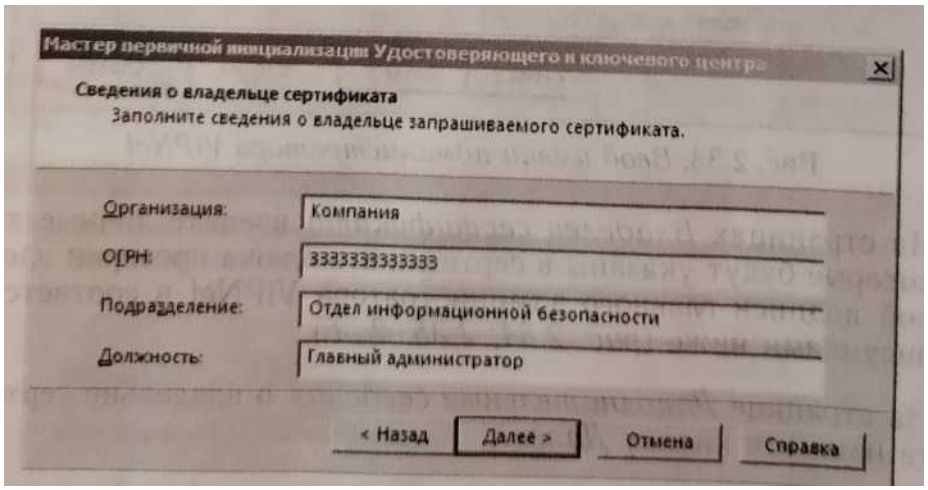
сертификате ключа проверки электронной подписи главного администратора ViPNet в соот-



ветствии с рисунками ниже (рис.).

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 из-

дателя, 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.

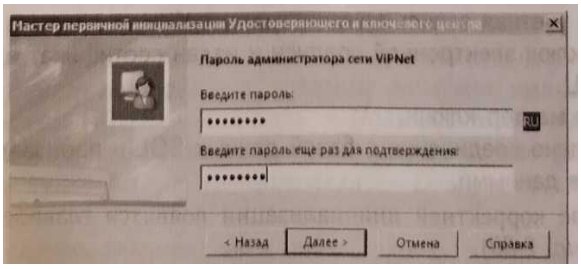
12. На странице Автоматический режим работы нажмите Далее.

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

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) (рис.).

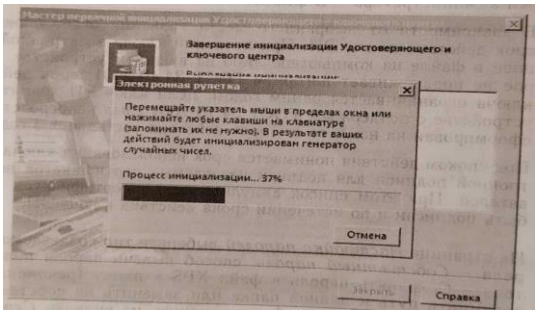


СОВЕТ. При выполнении практических занятий рекомендуется использовать, простые запоминающиеся пароли во всех программах (например, 11111111 - восемь единиц).

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 (рис.) 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.

В случае корректной инициализации появится главное окно программы (рис.).

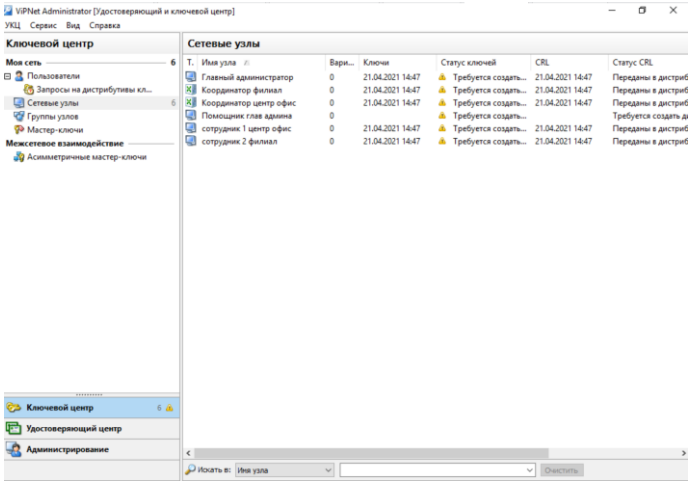


Рис. Главное окно УКЦ

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

После проверки первоначальных настроек необходимо снять вручную флажок Создавать ключи электронной подписи в свойствах пользователей (УКЦ Моя сеть Пользователи, кликнуть правой кнопкой мыши на пользователя и выбрать пункт Ключи пользователя → Создавать ключи электронной подписи).

Теперь можно приступить к созданию дистрибутивов ключей.

Примечание. В разделе Сервис → Настройка... → Сертификаты, стоит обратить внимание на второй пункт Создавать ключи электронной подписи. В случае если в вашей сети для большинства узлов (клиентов) требуется выпуск электронной подписи и сертификата проверки электронной подписи (например, для обеспечения юридически значимого электронного документооборота), то рекомендуется оставить данный флажок включенным.

Но главное - не забывать снимать вручную данный флажок в свойствах конкретного пользователя, которому не нужно выпускать электронную подпись (УКЦ → Моя сеть → Пользова-

тели, 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, 1 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... (рис.).

— Задайте пароль пользователя — 11111111 по очереди для каждого пользователя защищенной сети (рис).

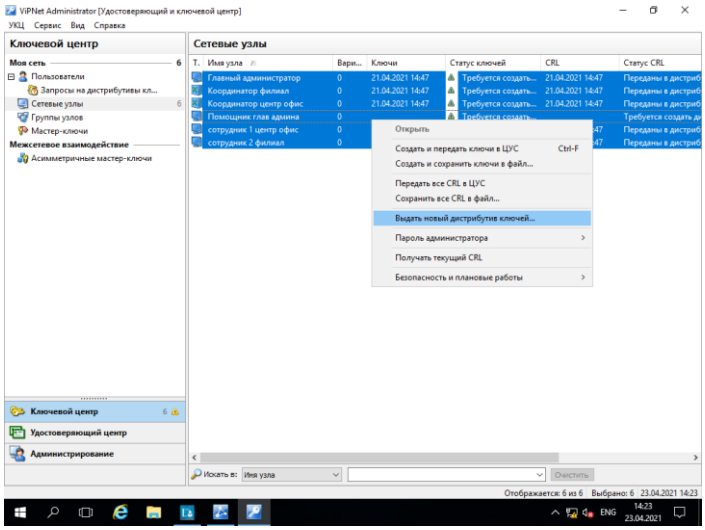
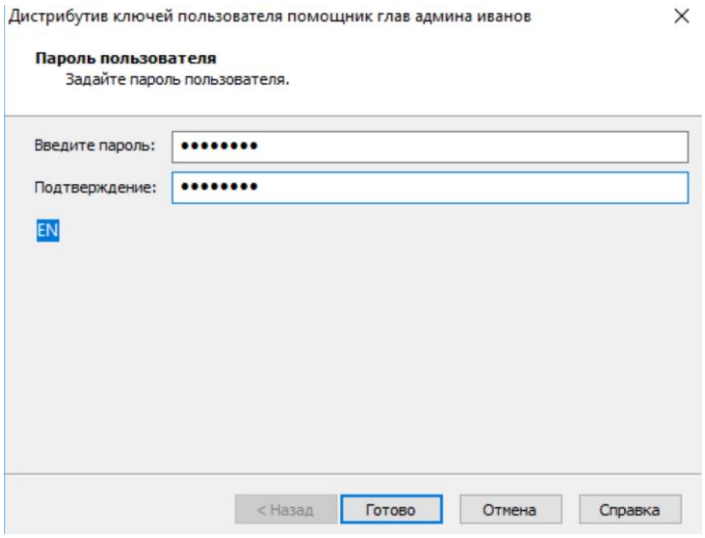


Рис Задание пароля пользователя

После окончания выдачи дистрибутива откроется окно проводника с папкой, содержащей подкаталоги сетевых узлов с готовыми дистрибутивами (рис.). 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.

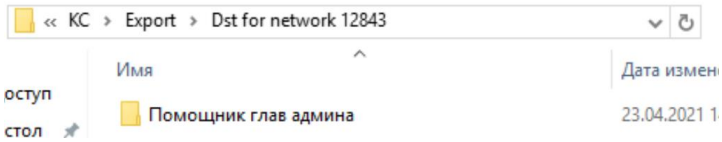


Рис. Папка с дистрибутивами ключей

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.

Практическая работа № 43 «Развёртывание рабочего места помощника главного администратора»

Задание:

1. На виртуальной машине (VM_1 - рабочее место главного администратора сети), где уже установлен ЦУС и УКЦ, доустановить ViPNet Client и активировать его с помощью dst-

файла, выпущенного для СУ Главный администратор.

2. Развернуть на виртуальной машине (VM_2 - рабочее место помощника главного администратора) необходимое ПО - клиентскую часть ViPNet Administrator ЦУС и ViPNet Client, который необходимо активировать с помощью dst-файла, выпущенного для СУ *Помощник глав админа.*

Установка ViPNet Client

Программное обеспечение VipNet Client необходимо установить на VM_1 и VM_2. Для этого выполните следующие действия:

1. На рабочем месте главного администратора сети (VM_1) запустите установочный файл <имя_файла>.exe. Дождитесь завершения подготовки к установке VipNet Client.

2. Ознакомьтесь с условиями лицензионного соглашения, установите флажок подтверждения вашего согласия и нажмите Продолжить.

3. На странице Способ установки установите флажок, чтобы после завершения установки компьютер был перезагружен автоматически, и нажмите кнопку Установить сейчас (рис.).

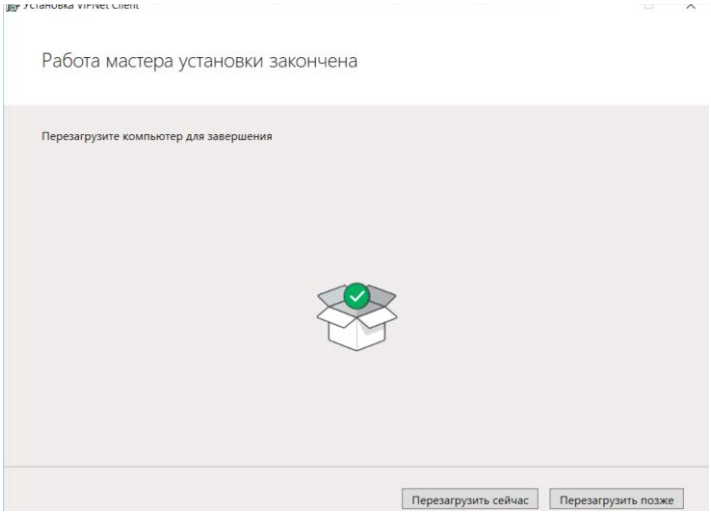


Рис. Способ установки

4. Если потребуется настроить параметры установки, то на странице Способ установки нажмите кнопку Настроить и укажите:

— путь к папке установки программы на компьютере;

— имя пользователя и название организации;

— название папки программы и ее расположение в меню Пуск.

5. После перезагрузки компьютера на экран будет выведено диалоговое окно об отсутствие ключей. Необходимо подтвердить установку ключей (рис.).

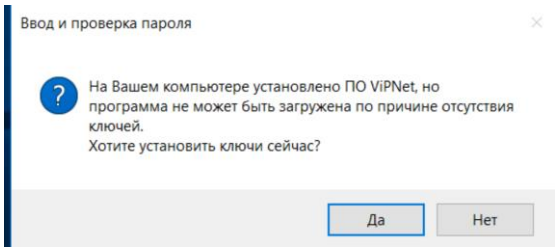


Рис. Диалоговое окно с вопросом об установке ключей

6. На странице Установка ключей сети VipNet укажите файл дистрибутива ключей *.dst для пользователя Глав админ Петров сетевого узла Главный администратор и нажмите кнопку Установить ключи (рис.). Дистрибутивы ключей были созданы при выполнении предыдущих заданий.

7. По завершении процедуры установки ключей нажмите Закрыть.

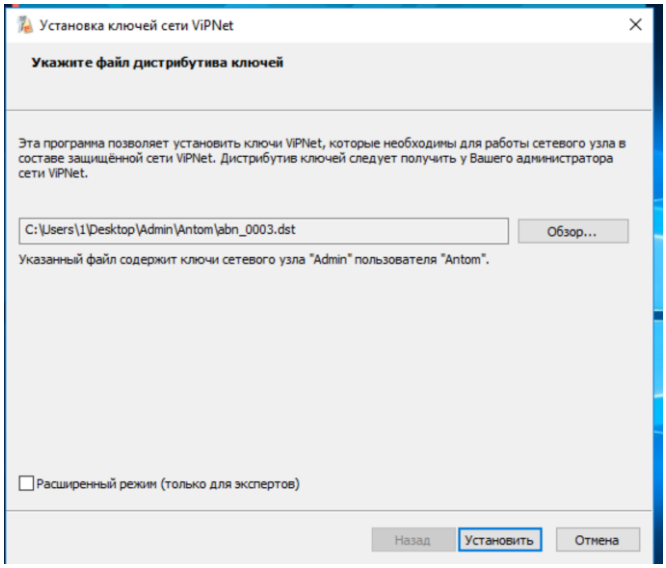


Рис.. Выбор дистрибутива ключей

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

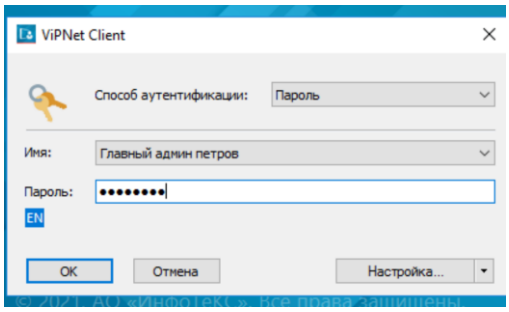


Рис. Окно аутентификации VipNet Client

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

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

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

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

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

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

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

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

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

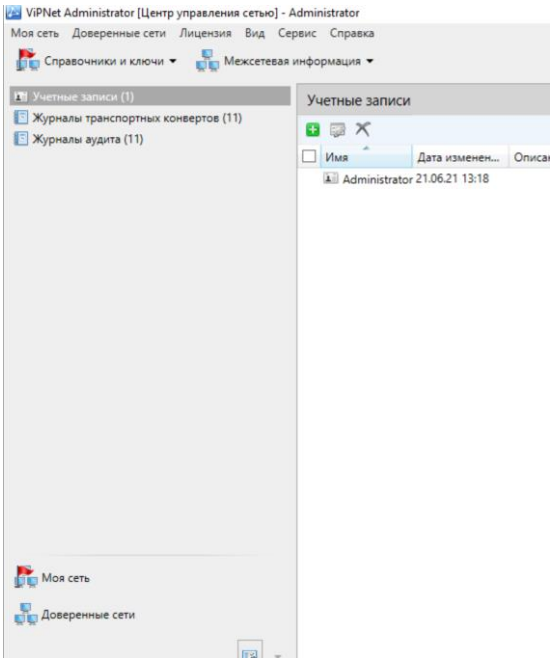


Рис. Раздел «Администрирование»

3. В разделе Учетные записи на панели инструментов нажмите кнопку Добавить.

4. Откроется окно Новая учетная запись. В поле Имя укажите Administrator 2, пароль - 11111111, описание - Помощник главного администратора сети (рис.).

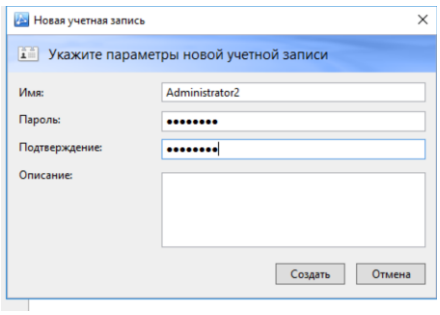


Рис. Создание второго администратора ЦУС

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

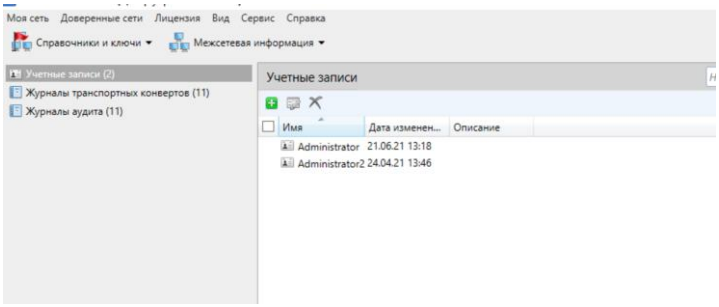


Рис. Раздел «Учетные записи ЦУС»

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

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

1. Запустите клиентскую часть VipNet Administrator ЦУС.

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

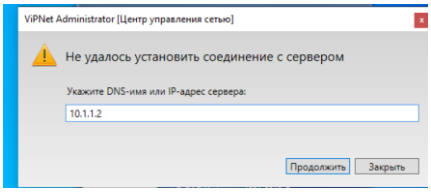


Рис. Ввод адреса СУ с установленной серверной частью ЦУС

3. Если связь с сервером установилась, то появится окно для ввода имени пользователя и пароля для входа. Введите имя пользователя — Administrator2, пароль — 11111111.

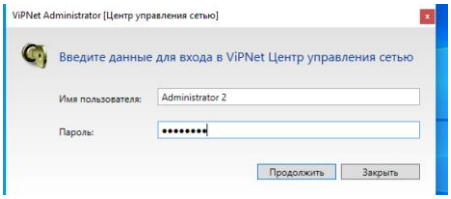


Рис. Окно аутентификации клиентской части ЦУС

4. После успешного подключения клиентской части ЦУС, расположенной на рабочем месте помощника главного администратора будет выведено диалоговое окно, в котором необходимо задать новый пароль. Введите старый пароль 11111111, новый пароль - 11111111.

Таким образом, теперь управлять защищенной сетью ViPNet можно двух рабочих мест.

Практическая работа № 44 «Модификация защищённой сети VipNet»

Задание:

Для выполнения практического задания потребуется две виртуальные машины VM_1 (Главный администратор) и VM 2 (Помощник главного администратора). В предыдущем практическом занятии они были уже настроены, но лучше еще раз убедитесь в корректности сетевых настроек, а также ПО ViPNet (рис).

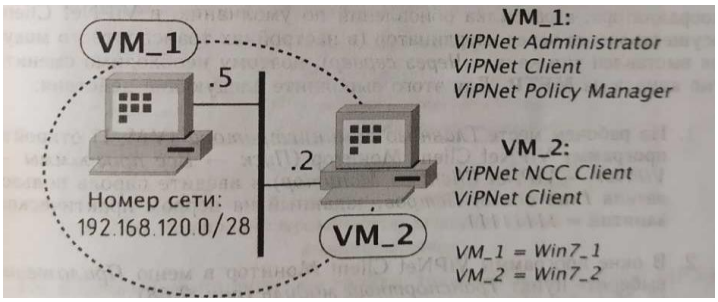
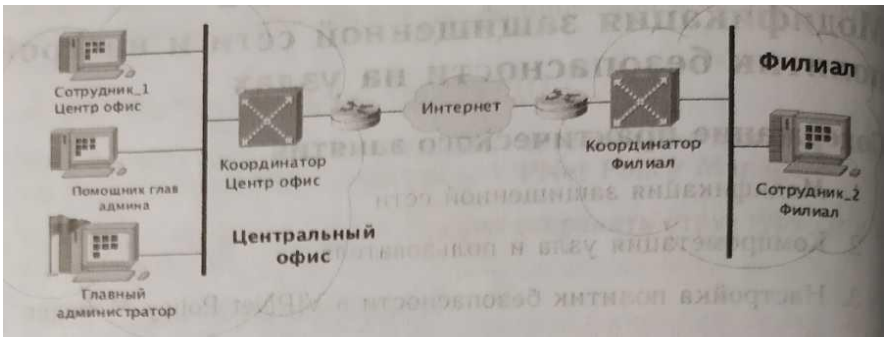


Рис. Схема стенда для Практического занятия

Настройка программного обеспечения ViPNet

Для обеспечения более быстрого прохождения обновлений на клиентах при выполнений настоящего практического задания необходимо настроить *Транспортный модуль,* обеспечивающий обмен служебными конвертами. Так как на данном этапе в сети нет развернутого координатора, а рассылка обновлений по умолчанию в ViPNet Client осуществляется через координатор (в настройках транспортного модуля выставлен тип канала *Через сервер)*, поэтому необходимо сменить тип канала на MFTP. Для этого выполните следующие действия:

На рабочем месте Главного администратора (VM_1) откройте программу ViPNet Client Монитор (Пуск → Все программы → VipNet → ViPNet Client → Монитор) и введите пароль



пользователя Глав админ Петров, заданный на первом практическом занятии — 11111111.

В окне программы ViPNet Client Монитор в меню Приложения выберите пункт Транспортный модуль (рис.).

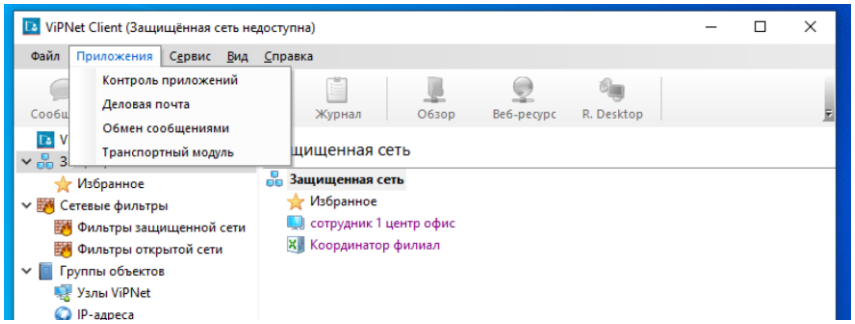


Рис. Фрагмент окна программы VipNet Client Монитор

В открывшемся окне приложения ViPNet Client MFTP зайдите в пункт меню Настройки (рис.).

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

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

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

Добавление сетевого узла

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

1. В окне ViPNet Центр управления сетью выберите представление Моя сеть.
2. На панели навигации выберите раздел Клиенты.
3. В разделе Клиенты на панели инструментов нажмите Добавить,
4. В появившемся окне задайте имя Директор, выберите координатор Координатор Центр офис для регистрации на нем создаваемого клиента, уберите флажок Создать одноименного пользователя и нажмите кнопку Создать (рис.).

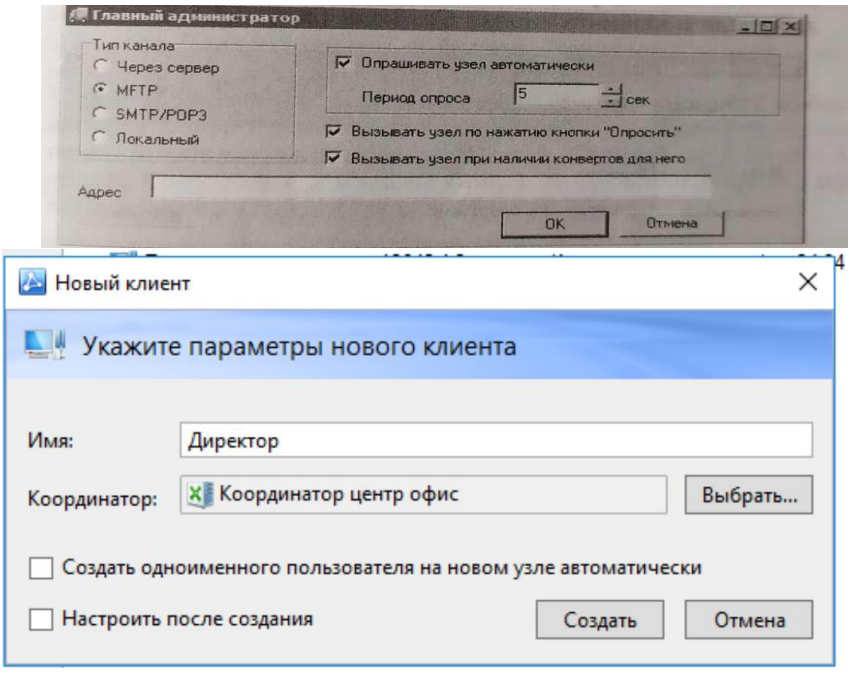


Рис. Параметры нового клиента Директор

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

1. В окне ViPNet Центр управления сетью выберите представление Моя сеть.
2. На панели навигации выберите раздел Пользователи.
3. В разделе Пользователи на панели инструментов нажмите кнопку Добавить.
4. В появившемся окне задайте имя пользователя Директор Соколов, выберите сетевой узел Директор и нажмите кнопку Создать (рис.).

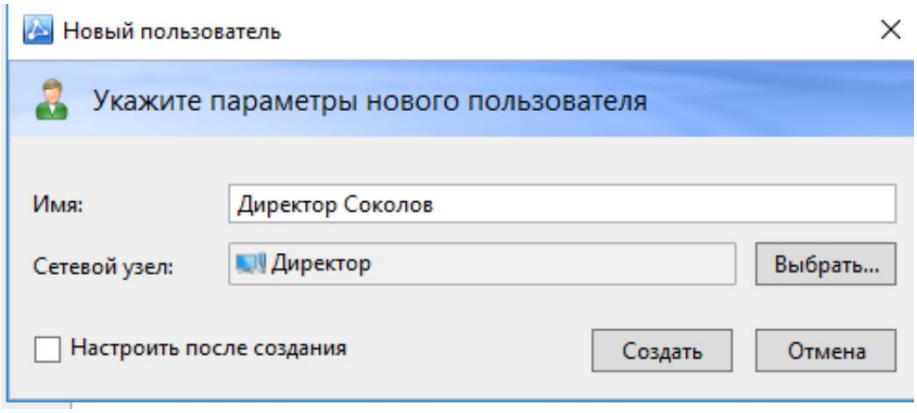


Рис. Параметры нового пользователя Директор Соколов

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

1. В окне ViPNet Центр управления сетью выберите представление Моя сеть.

2. На панели навигации выберите раздел Пользователи.

3. В списке Пользователей выберите Директор Соколов и на панели инструментов нажмите кнопку Свойства,

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

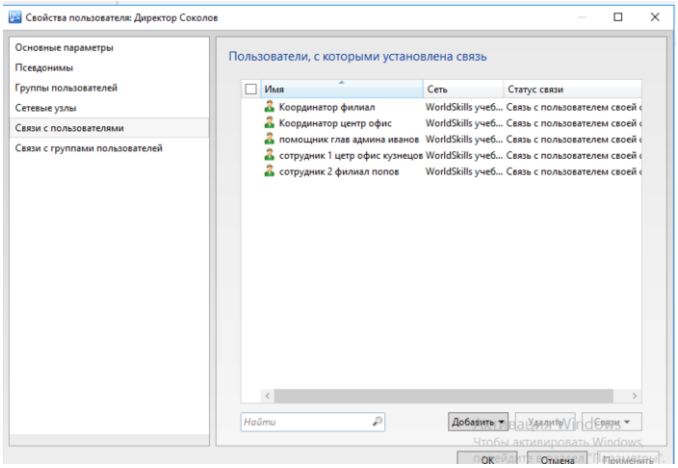


Рис. Окно Свойства пользователя Директор Соколов

Сформируйте справочники следующим образом:

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

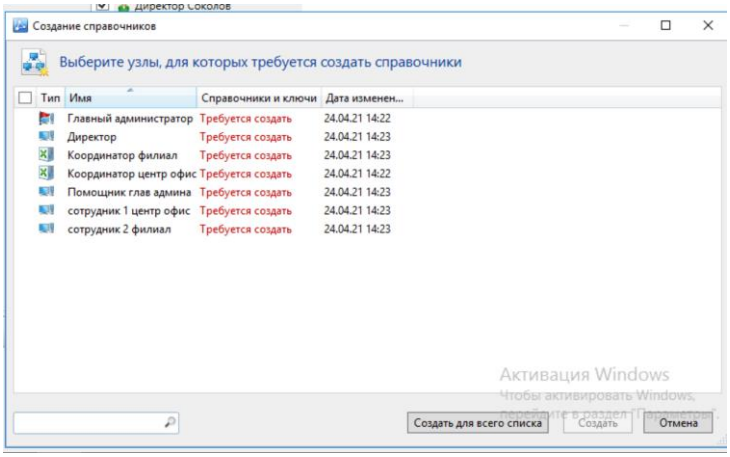


Рис. Создание справочников

После формирования справочников в программе ViPNet УКЦ необходимо выдать дистрибутив ключей для сетевого узла Директор и ключи для сетевых узлов, которых коснулись изменения в ЦУС: Главный администратор, Помощник глав админа Иванов, Сотрудник_1 Центр Кузнецов, Сотрудник_2 Филиал Попов, Координатор Центр офис, Координатор Филиал.

Выдайте дистрибутив ключей для пользователя Директор Соколов следующим образом:

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

2. Задайте пароль администратора для сетевого узла Директор.

3. Выделите сетевой узел Директор и вызовите правой кнопкой мыши контекстное меню.

4. В этом меню выберите Выдать новый дистрибутив ключей.

5. При создании дистрибутива ключей задайте пароль пользователя — 11111111.

Сформируйте ключи для сетевых узлов следующим образом:

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

2. Выделите сетевые узлы, для которых необходимо создать ключи (комбинация горячих клавиш Ctrl-W), и вызовите правой кнопкой мыши контекстное меню.

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

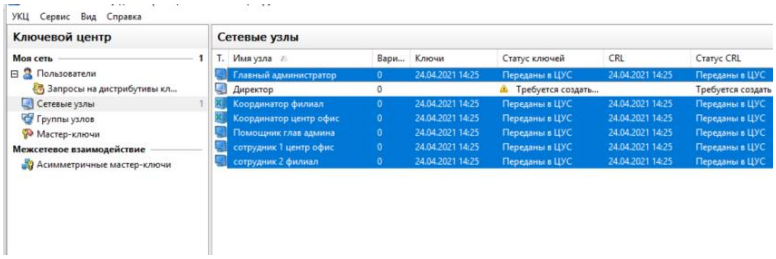


Рис. Сетевые узлы, для которых необходимо создать ключи

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

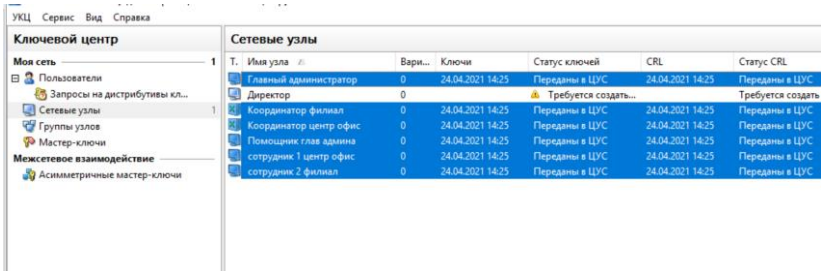


Рис. Статус ключей, переданных в ЦУС

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

Пои успешном прохождении обновлений окно Отправка справочников и ключей примет следующий вид (рис.).

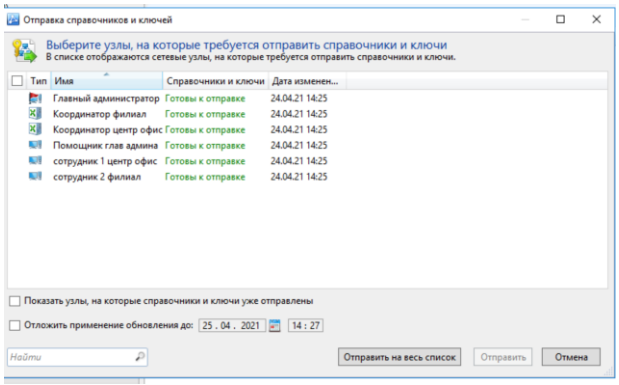


Рис. Окно отправки ключей и справочников

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

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

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

Сформировать справочники и ключи, разослать их на узлы.

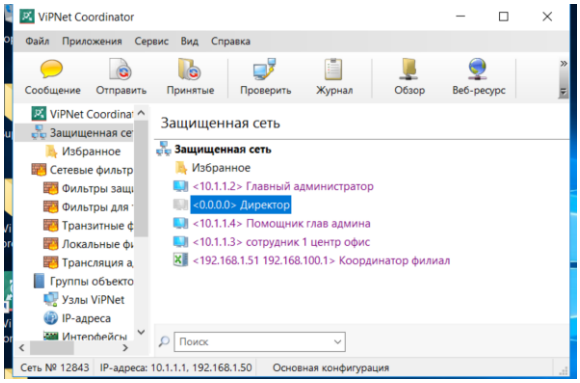


Рис. Окно программы ViPNet Client Монитор после обновления

Создание групп узлов

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

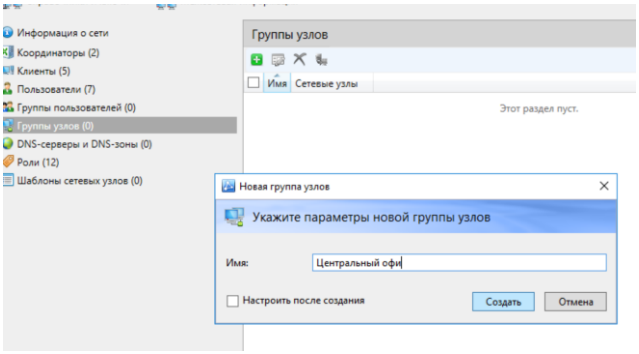


Рис. Создание группы узлов Центральный офис

Аналогичным образом создайте группу узлов Филиал.

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

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

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

В результате вкладка Сетевые узлы примет вид (рис.):

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

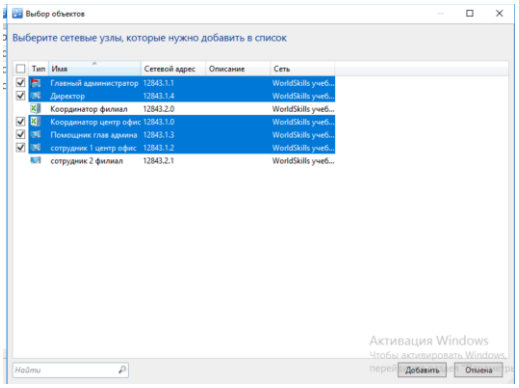


Рис. Добавление узлов в группу узлов Центральный офис

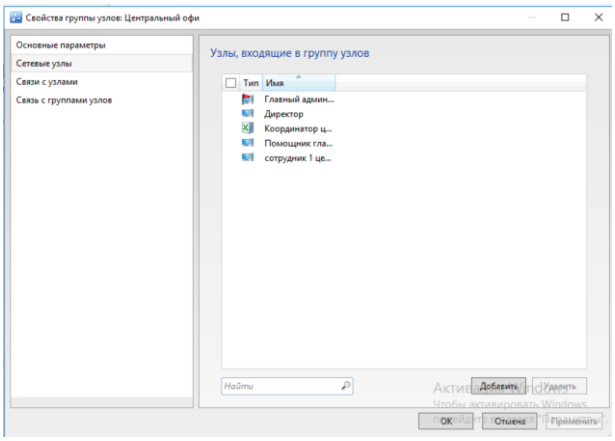


Рис. Вкладка .Сетевые узлы» в группе узлов «Центральный офис»

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

1. Перейдите в раздел Группы узлов окна VipNet Удостоверяющий и ключевой центр (рис.).

2. Дважды щелкните группу Центральный офис.

3. В открывшемся окне перейдите на вкладку Пароль администратора и нажмите кнопку Создать.

4. Задайте пароль — 22222222 и нажмите ОК (рис.).

Созданный пароль отобразится на вкладке Пароль администратора (рис.).

Аналогичным образом задайте пароль администратора для группы узлов Филиал — 33333333.

Отправьте обновления ключей на узлы следующим образом:

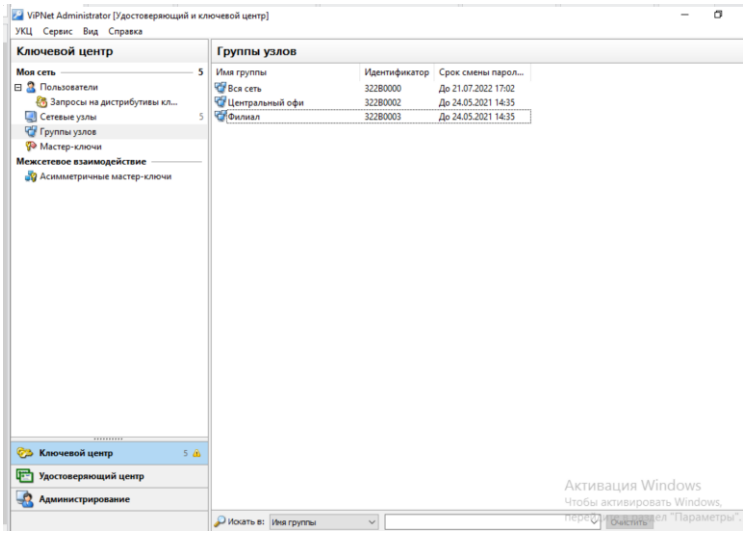


Рис. Вкладка «Группы узлов» в УКЦ

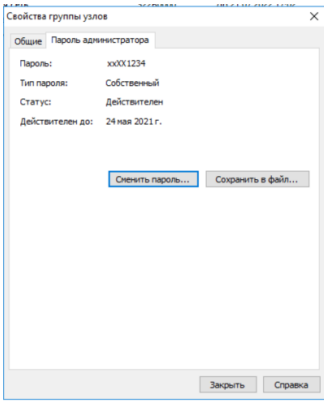


Рис. Создание пароля администратора для группы узлов

1. В разделе Сетевые узлы окна VipNet Удостоверяющий и ключевой центр выберите все узлы, вызовите контекстном меню правой кнопкой мыши и нажмите Создать и предать ключи в ЦУС.

2. В окне VipNet Центр управления сетью нажмите кнопку Справочники и ключи → Отправить спровчники и ключи… и в открывшемся окне отправьте ключи на веь список.

3. Проконтролируйте прохождение обновления на узлах Главный администратор, Помощник глав админа.

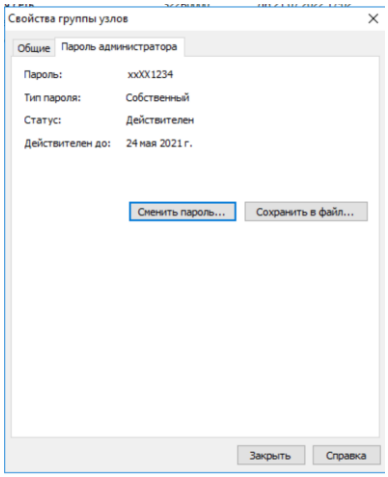


Рис. Вкладка 'Пароль администратора» для группы узлов «Центральный офис

Теперь для выполнения настроек узлов Центрального офиса и Филиала не потребуется разглашать пароль администратора всей сети, достаточно сообщить пароль группы, в которой находится требуемый узел (данный пароль, а также пароль администратора сетевого узла нельзя сообщать пользователям).

Для настройки программы ViPNet Client перейдите на рабочее м сто Помощник глав админа в программу ViPNet Client Монитор. В верхнем меню выберите Файл → Войти в режим администратора... и введите пароль администратора группы узлов Центральный офис (рис.).

После входа в режим администратора узла можно осуществлять настройку программного обеспечения ViPNet Client (в настоящем задании на данный момент вносить или изменять настройки не требуется, достаточно убедиться в наличии такой возможности).

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

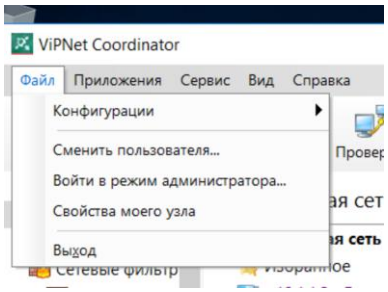


Рис. Вход в режим администратора

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

Добавление нового пользователя

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

1. В разделе Пользователи окна ViPNet Центр управления сетью нажмите кнопку Создать нового пользователя, задайте имя Бухгалтер Захарова и выберите сетевой узел Бухгалтер.

2. В разделе Пользователи окна ViPNet Центр управления сетью выделите пользователя Бухгалтер Захарова, нажмите кнопку Свойства пользователя, перейдите на вкладку Связи с

пользователями и добавьте в список пользователей Бухгалтер Прохорова, Помощник глав админа, Сотруд_1 Центр Кузнецов.

3. В окне ViPNet Центр управления сетью нажмите кнопку Справочники и ключи → Создать справочники... и в открывшемся окне нажмите кнопку Создать для всего списка.

4. В разделе Сетевые узлы окна ViPNet Удостоверяющий и ключевой центр выделите узел Бухгалтер, в контекстном меню выберите пункт Выдать новый дистрибутив ключей. При создании дистрибутива ключей задайте пароль пользователя Бухгалтер Захарова - 11111111

5. Передайте доверенным способом дистрибутив ключей и пароль пользователю Бухгалтер Захарова (в рамках настоящего задания передавать дистрибутив ключей никуда не нужно).

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

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

8. Проконтролируйте прохождение обновления на узлах Главный администратор, Помощник глав админа.

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

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

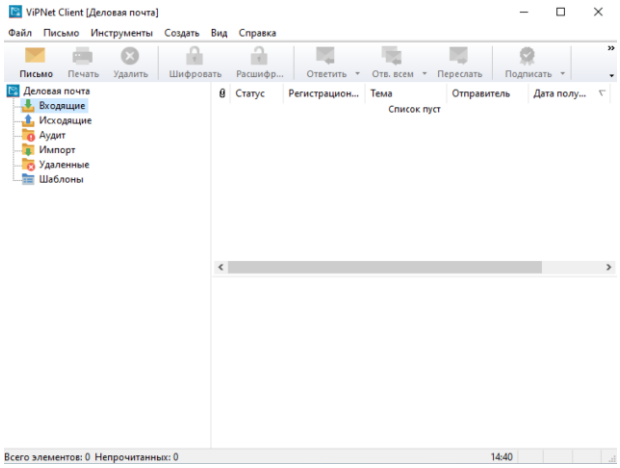


Рис. Общий вид программы «ViPNet Client Деловая почта»

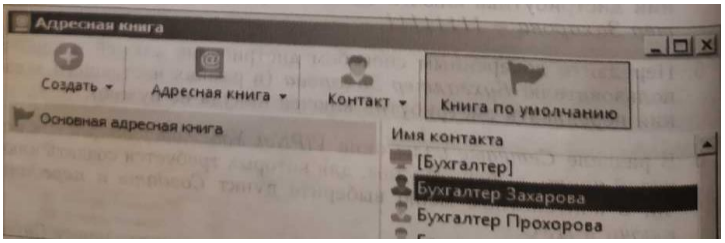
В меню Инструменты выберите пункт Адресная книга… и убедитесь, что пользователь Бухгалтер Захарова добавился в список (рис.).

Удаление связей пользователей

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

1. В разделе Пользователи Окна ViPNet Центр управления сетью выделите пользователя Бухгалтер Захарова, нажмите кнопку Свойства пользователя.

2. Перейдите на вкладку Связи с пользователями, в списке пользователей отметьте Помощник глав админа Иванов и нажмите кнопку Удалить.



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

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

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

6. Проконтролируйте прохождение обновления на узле Помощник глав админа.

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

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

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

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

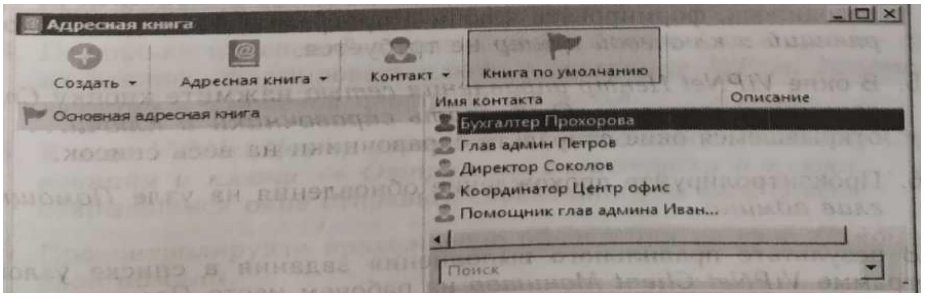


Рис. Изменение имени сетевого узла

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

Поскольку изменений в связях узлов или пользователей не производилось, формировать ключи в программе VipNet Удостоверяющий и ключевой центр не требуется.

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

Проконтролируйте прохождение обновления на узле Помощник глав админа.

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

Для изменения имени пользователя Директор Соколов на Директор Абросимов выполните следующие действия:

1. В окне ViPNet Центр управления сетью выберите раздел Пользователи, выделите пользователя Директор Соколов и нажмите кнопку Свойства пользователя.

2. В свойствах пользователя Директор Соколов измените имя на Директор Абросимов и нажмите кнопку ОК. Появится диалоговое окно, в котором будет сообщаться, что данный пользователь единственный на данном узле и вам нужно выбрать переименовывать узел или нет. В данной ситуации переименование узла не требуется, поэтому нажмите кнопку Нет.

3. В окне ViPNet Центр управления сетью нажмите кнопку Справочники и ключи → Создать справочники… и в открывшемся к окне нажмите кнопку Создать для всего списка.

4. Поскольку изменений в связях узлов или пользователей не производилось, формировать ключи в программе ViPNet Удостоверяющий и ключевой центр не требуется.

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

6. Проконтролируйте прохождение обновления на узле Помощник глав админа.

В результате правильного выполнения задания в адресной книге в программе ViPNet Client Деловая почта на рабочем месте Помощник глав админа имя пользователя Директор Соколов будет изменено на Директор Абросимов (рис.).

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

Удаление пользователя

Для удаления пользователя *Бухгалтер Прохорова* выполните следующие действия:

1. В разделе *Пользователи* окна *ViPNet Центр управления сетью* выберите пользователя *Бухгалтер Прохорова* и нажмите кнопку *Удалить.* При этом удалять клиента, на котором зарегистрирован пользователь не требуется *(рис.).*

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

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

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

5. Проконтролируйте прохождение обновления на узле Помощник глав админа.

В результате правильного выполнения задания в списке адресатов в программе VipNet Client Деловая почта на рабочем месте Помощник глав админа будет удалён пользователь Бухгалтер Прохорова.

Удаление сетевого узла

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

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

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

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

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

Смена пароля администратора УКЦ

Для смены пароля администратора УКЦ, выполните следующие действия:

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

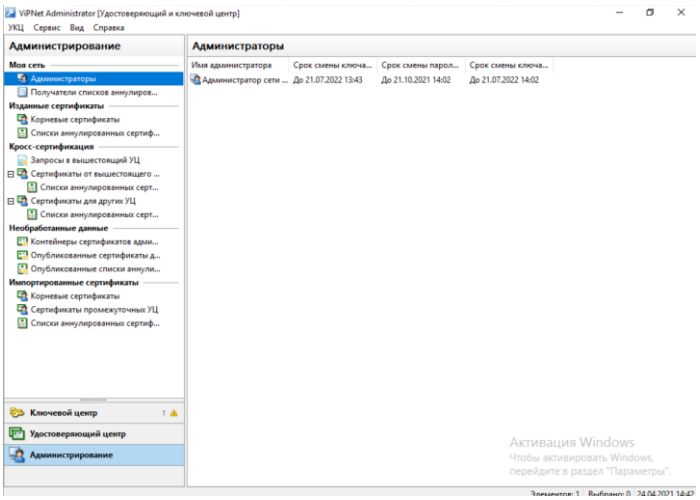


Рис. Раздел «Администраторы» в УКЦ

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

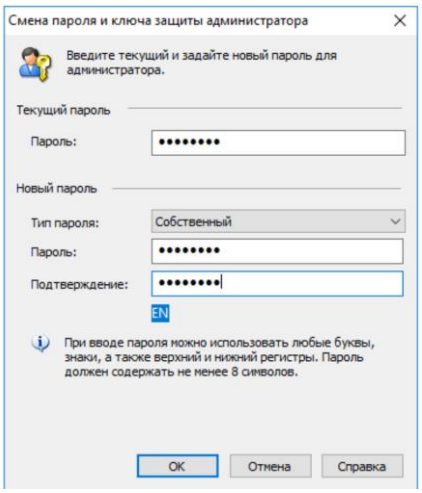


Рис. Смена пароля администратора УКЦ

Смена мастер-ключей

Смена мастер-ключей влечет за собой смену всех ключей в сети ViPNet. Она может быть, как плановой, так и внеплановой. Плановая смена мастер-ключей проводится с определенной периодичностью, обычно не реже одного раза в год. Внеплановая смена мастер-ключей производится при компрометации ключей.

Перед сменой мастер-ключей выполните следующие действия:

✓ Убедитесь, что в промежуток времени, отведенный на смену ключей, все пользователи сети ViPNet смогут выполнить вход в программу ViPNet (обычно 5-10 дней, в течение которых нельзя проводить другие обновления).

✓ Убедитесь, что у каждого пользователя на узле имеется резервный набор персональных ключей. Если пользователь зарегистрирован на нескольких узлах, то его резервный набор ключей должен присутствовать на каждом из узлов. Без резервного набора новые ключи на узлах не вступят в действие. Резервный набор перс по умолчанию сохраняется в папке установки ViPNet.

Пример:
C:\Program Files (x 86) \InfoTeCS\ViPNet Client\user_<****>\key_disk\dom*.pk, где **** — идентификатор узла.

✓ Проинформируйте всех пользователей и администраторов сети ViPNet о планируемом обновлении ключей и сроках его проведения.

✓ Рекомендуйте пользователям расшифровать все сообщения программы ViPNet Деловая почта, включая архивные сообщения. После того как будет принято обновление с новыми мастер-ключами, сообщения, зашифрованные на старых ключах, невозможно будет прочитать.

✓ Перед сменой мастер-ключей рекомендуется выгрузить РНПК в файл: УКЦ → Ключевой центр → Пользователи, правой кнопкой мыши по пользователю, выбрать раздел Ключи пользователя → Создать и сохранить РНПК в файл... .

Для смены мастер-ключей перейдите на рабочее место Главного администратора и выполните следующие действия:

1. В окне ViPNet Удостоверяющий и ключевой центр выберите представление Ключевой центра выберите раздел Моя сеть → Мастер-ключи.

2. Поочередно в контекстном меню каждого из трех мастер-ключей выберите пункт Сменить.

3. В появившемся окне с сообщением о смене мастер-ключа уста новите флажок Сменить <название мастер-ключа> и нажмите кнопку Продолжить (рис.).

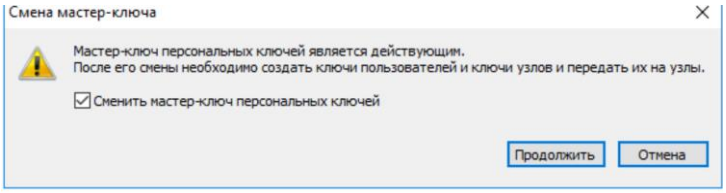


Рис. Смена мастер-ключа

4. В окне ViPNet Удостоверяющий и Ключевой центр перейдите в раздел Пользователи, выделите всех пользователей, в контекстном меню выберите пункт Ключи пользователя → Создать к передать ключи в ЦУС.

5. В разделе Сетевые узлы, окна ViPNet Удостоверяющий и ключевой центр выберите всё узлы, в контекстном меню выберите пункт Создать и передать ключи в ЦУС.

6. В окне ViPNet Центр управления сетью нажмите кнопку Справочники и ключи → Отправить справочники и ключи...

7. В открывшемся окне, установите флажок Отложить применение обновления до, установите дату и время таким образом, чтобы обновление было применено через 5 минут от текущей даты и времени (обратите внимание, на дату, по умолчанию при активации отложенного применения обновления дата сдвинута на 1 день вперед) и нажмите кнопку Отправить на весь список (в реальной сети при смене мастер-ключей необходимо применять обновлений через 5-10 дней после их отправки, стоит учитывать тот факт; что сетевые узлы могут быть выключены, и если они будут неактивны большее время, то может возникнуть ситуация при которой обновления вообще не дойдут до сетевого узла. Это связано с тем что на координаторе, за которым находятся такие узлы установит обновления, ключи изменяться и те сетевые узлы станут не доступны. Поэтому рекомендуется распланировать рассылку обновлений при смене мастер-ключей так, чтобы не возникло вышеизложенной ситуации (рис.).

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

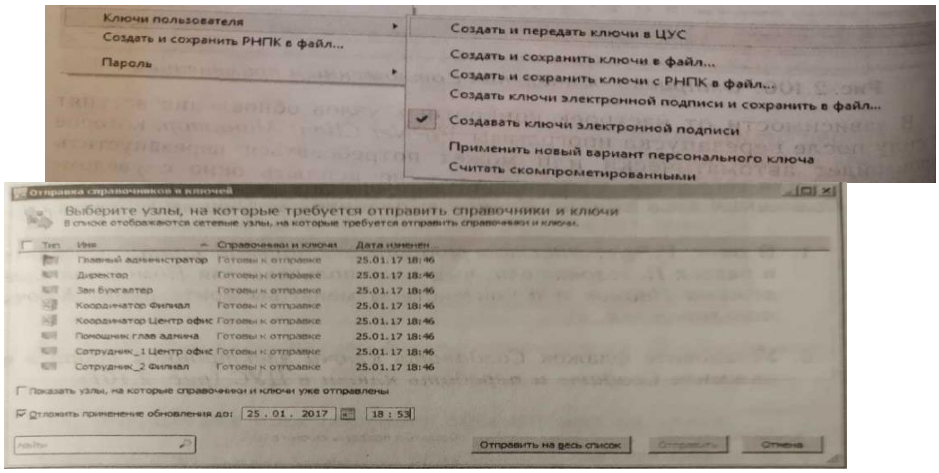


Рис. Отправка обновления с отложенным применением

В зависимости от настроек конкретных узлов обновления вступят в силу после перезапуска программы *ViPNet Client Монитор,* которое произойдет автоматически или может потребоваться перезапустить *ViPNet Client Монитор* вручную (должно всплыть окно с уведомление о необходимости перезапуска). Во втором случае необходимо будет выполнить следующие действия:

1. На рабочем месте Главного администратора в области уведомлений на панели задач Windows щелкните значок программы ViPNet Client Монитор и в открывшемся окне нажмите Файл → Выход.

2. Теперь откройте программу ViPNet Client Монитор - меню Пуск → Все программы ViPNet → ViPNet Client → Монитор.

Аналогично перезапустить ViPNet Client Монитор на рабочем месте Помощник глав админа.

После перезагрузки на экран будет выведено сообщение о необходимости указать путь до места расположения резервного набора персональных ключей. Указываете путь до файла резервного набора персональных ключей и вводите пароль пользователя.

После корректного обновления загрузится ViPNet Client Монитор.

Формирование нового сертификата ключа проверки электронной подписи

Если пользователь на сетевом узле по каким-то причинам не смог сделать запрос на сертификат ключа проверки электронной подписи самостоятельно (например, срок действия сертификата закончился), то сформировать новый сертификат и ключ электронной подписи возможно в программе ViPNet *Удостоверяющий и ключевой центр* в промессе создания ключей пользователя.

Для того чтобы сформировать новый сертификат для пользователя Помощник глав админа Иванов выполните следующие действия:

1. В окне ViPNet Удостоверяющий и ключевой центр перейдите в раздел Пользователи, выделите пользователя Помощник глав админа Иванов и в контекстном меню выберите пункт Ключи пользователя.

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

3. В окне ViPNet Центр управления сетью нажмите кнопку Справочники и ключи → Отправить справочники и ключи…

4. В открывшемся нажмите кнопку Отправить на весь список.

5. Аналогичным образом создать и отправить на весь список ключи узлов.

6. Проконтролируйте применение обновлений на узле Помощник глав админа.

7. На рабочем месте Помощник глав админа в области уведомлений на панели задач Windows щелкните по значку программы ViPNet Client Монитор и в открывшемся окне в меню Сервис выберите пункт Настройка параметров безопасности.

8. В окне Настройка параметров безопасности перейти на вкладку Электронная подпись, нажать кнопку Выбрать и выбрать новый сертификат пользователя Помощник глав админа Иванов (рис.).

Обновление программного обеспечения на узлах

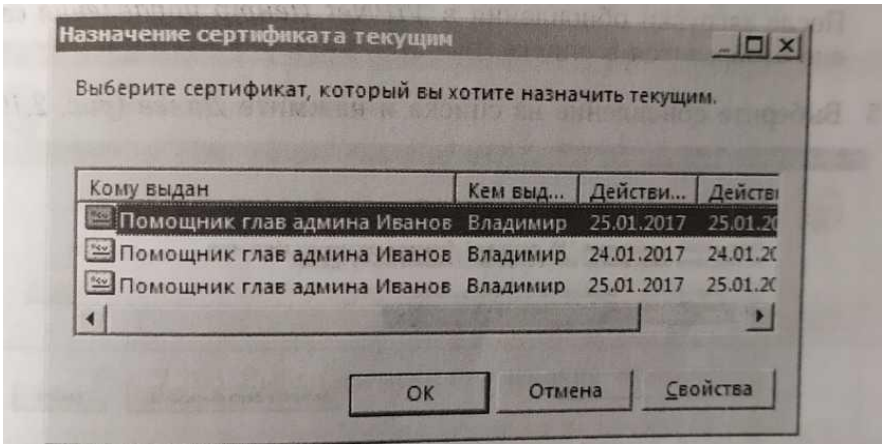
Чтобы обновить программное обеспечение VipNet Client на узле Помощник глав админа выполните следующие действия:

1. В окне VipNet Центр управления сетью в меню Моя сеть выберите пункт Обновить программное обеспечение на узлах.

2. В появившемся окне нажмите кнопку Далее.

3. Нажмите кнопку Загрузить файл обновления → Обзор и выберите файл с обновлением *.lzh. (файл с обновлением в рамках данного практического занятия находится в папке дистрибутивом… \VipNet4\Client|RUS\Software\SP).

4. Нажмите кнопку ОК (рис.).



После загрузки обновления в *ViPNet Центр управления сетью* оно отобразится в списке.

5. Выберите обновление из списка и нажмите *Далее (рис.)*

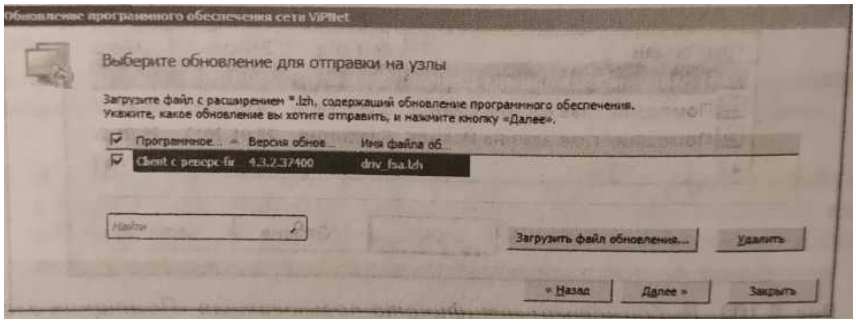


Рис. Список обновлений программного обеспечения

6. На следующем шаге укажите сетевой узел Помощник глав админа (рис.).

7. Теперь задайте время применения обновления - текущее время и установите флажок Перезагружать Windows на сетевых узлах после обновления программного обеспечения (рис.).

8. Следуйте указаниям мастера, нажимая кнопку Далее. На заключительном шаге дождитесь окончания отправки обновления и перезагрузки операционной системы.

9. Для проверки версии программного обеспечения на узле Помощник глав админа зайдите в программу ViPNet Client Монитор → Справка → О программе.

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

Практическая работа № 45 «Компрометация ключей в защищённой сети VipNet»

Задание:

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

О компрометации

Компрометация может происходить с удалением или без удаления сетевого узла, пользователя.

Как правило, ключи считаются скомпрометированными в следующих случаях:

✓ посторонним лицам мог стать доступным файл дистрибутива ключей пользователя;

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

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

✓ уволился пользователь, имевший доступ к паролям и ключам;

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

Компрометация ключей пользователя

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

1. В окне ViPNet Удостоверяющий и ключевой центр перейдите в раздел Пользователи,

2. Выделите там Помощник глав админа Иванов и в контекстном меню выберите пункт Считать скомпрометированными.

3. В появившемся окне Компрометация ключей пользователей нажмите кнопку Да (после этого пользователь Помощник глав админа Иванов будет помечен красным цветом). Если вместе с ключами пользователя были скомпрометированы его ключи электронной подписи, установите флажок Аннулировать сертификаты выбранных пользователей (рис.).

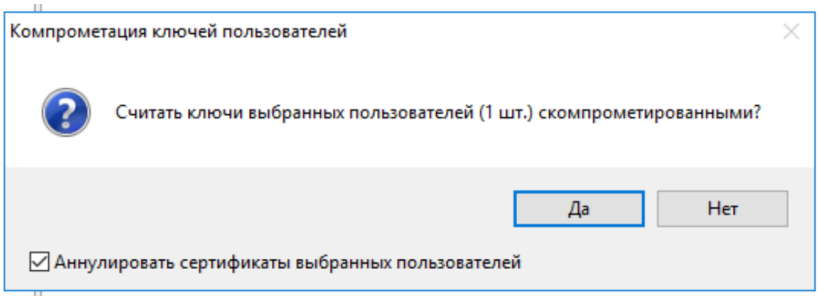


Рис. Окно «Компрометация ключей пользователя»

4. Повторно вызовите нажатием «правой, кнопки мыши на пользователя Помощник глав админа Иванов контекстное меню и выберите пункт Ключи пользователя Создать и передать ключи в ЦУС.

5. В окне ViPNet Удостоверяющий - ключевой центр перейдите в раздел Сетевые узлы.

6. После этого создайте и передайте в ЦУС ключи для узла Помощник глав админа.

7. Затем выделите правой кнопкой мыши (или сочетанием клавиш Ctrl+W) остальные узлы, для которых нужно создать ключи и в контекстном меню выберите пункт Создать и передать ключи в ЦУС (или сочетанием клавиш Ctrl+F).

Примечание. Если у скомпрометированного пользователя есть в наличии ключи электронной подписи й сертификат, которые хранятся на его узле, то создайте для него новые ключи и сертификат. Это связано с тем, что на узле ключи электронной подписи защищены персональным ключом пользователя. Поэтому после смены персонального ключа пользователь не сможет получить доступ к своим текущим ключам электронной подписи и сертификату.

8. В окне ViPNet Центр управления сетью нажмите кнопку Справочники и ключи → Отправить справочники и ключи...

9. В открывшемся окне выберите узел Помощник глав админа и нажмите кнопку Отправить (рис.).

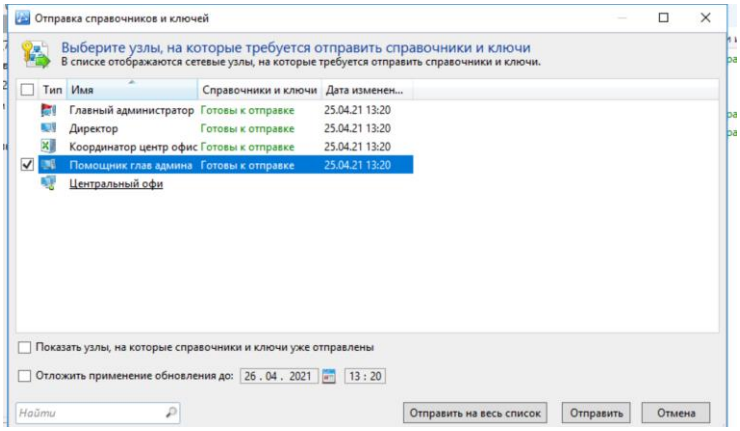


Рис. Отправка ключей на узел «Помощник глав админа»

10. Проконтролируйте доставку обновления на узел Помощник глав админа.

11. Проконтролируйте применение обновления на скомпрометированном узле Помощник глав админа.

12. После перезапуска ПО ViPNet Client, появиться диалоговое окно, в котором необходимо будет указать путь до РНПК и ввести пароль пользователя.

13. После успешного обновления на узле Помощник глав админа появиться диалоговое окно с информацией о том, что текущий пароль истек и его следует сменить. Для смены пароля необходимо выбрать пункт Открыть настройки пароля и установит новый пароль - 11111111 (рис.).

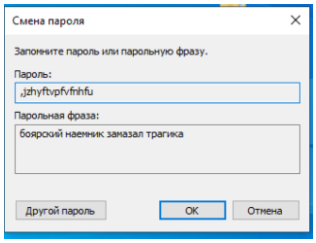


Рис. Смена пароля на узле «Помощник глав админа»

14. Отправьте обновления на остальные узлы.

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

Практическая работа № 46 «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 аутентификации - Аутентификация Windows (рис.).

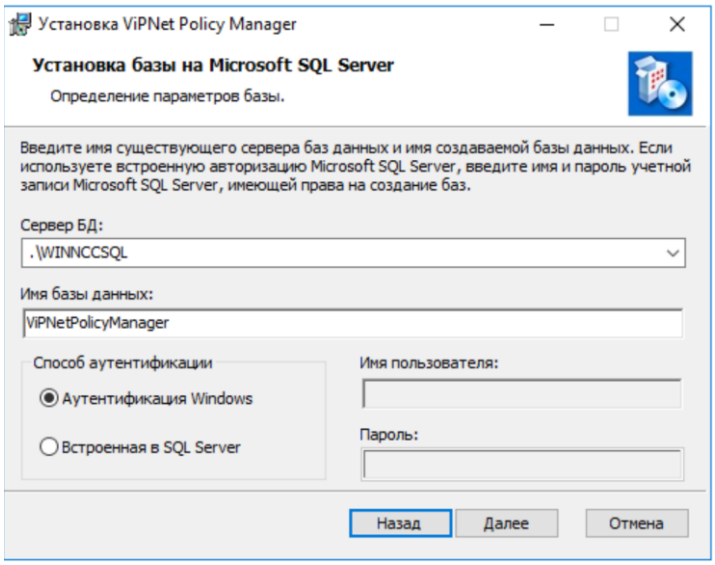


Рис. Параметры базы данных при установке ViPNet Policy Manager

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 (рис.).

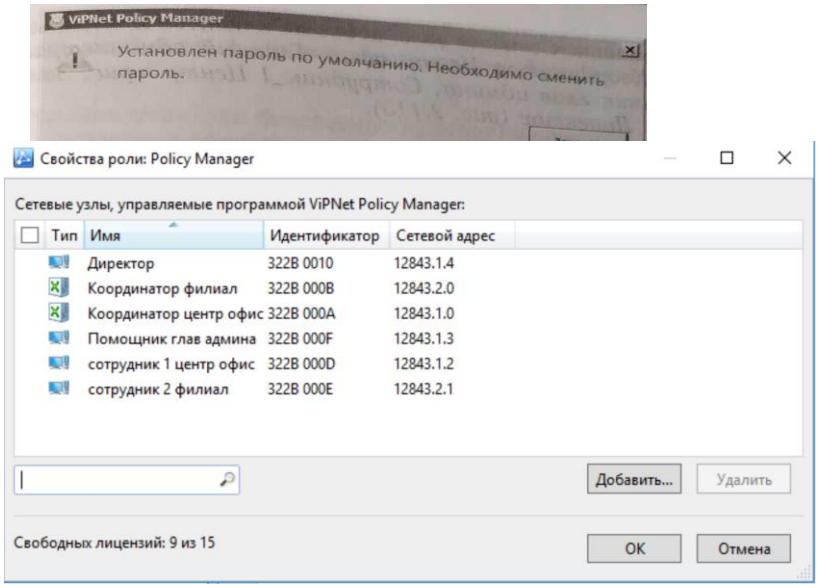


Рис. Добавление узлов для роли Policy Manager

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 (рис.).

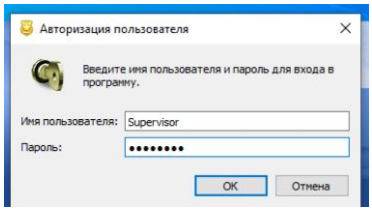


Рис. Вход в программу VipNet Policy Manager

5. На экран будет выведено предупреждение о необходимости смены пароля пользователя Supervisor (рис.)

Рис. Предупреждение о необходимости смены пароля

6. После авторизации под стандартным паролем перейдите в раздел Файл → Сменить пароль пользователя и задайте пароль — 11111111 (восемь единиц).

7. В окне программы VipNet Policy Manager перейдите в раздел Сетевые узлы. Если предыдущие шаги выполнены верно, то в списке будут отображены все узлы сети VipNet (рис.).

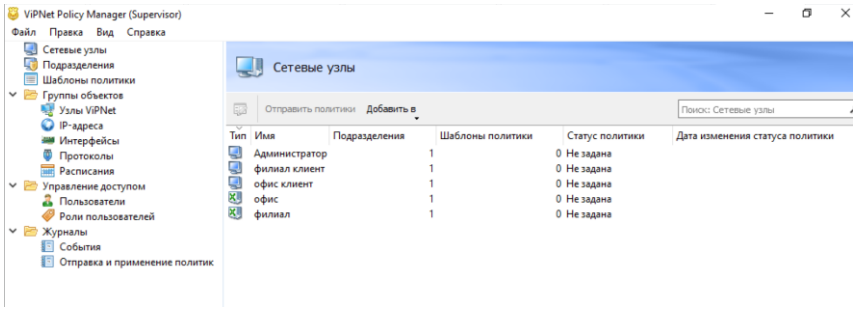


Рис. Раздел Сетевые узлы» ПО ViPNet Policy Manager

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 (рис.).

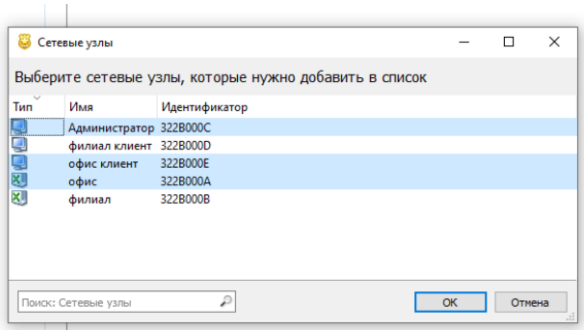


Рис. Добавление клиентов в подразделение «Центральный офис»

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 (рис.):

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 (рис).

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 (рис.).

8. На вкладке Локальные фильтры открытой сети нажмите кнопку Создать...

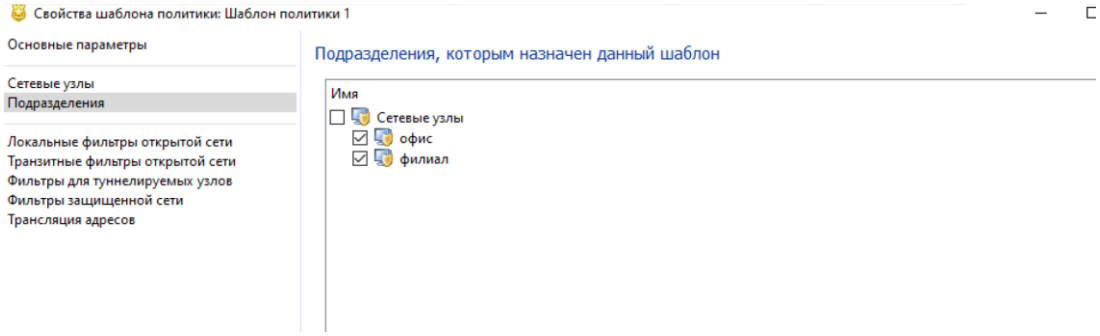
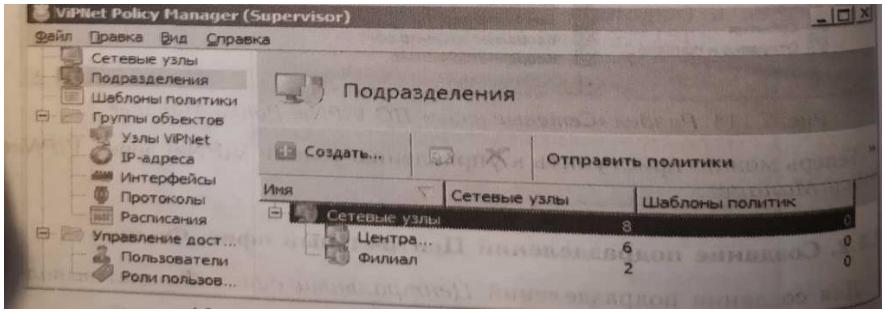


Рис. Вкладка «Подразделения» окна Свойства шаблона политик

9. В открывшемся окне Свойства фильтра открытой сети на вкладке Основные параметры



задайте имя фильтра Запрет социальных сетей и установите переключатель в положение Блокировать трафик (рис).

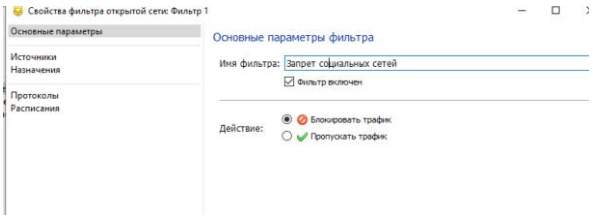


Рис. Вкладка «Основные параметры»

10. На вкладке Назначения нажмите кнопку Добавить... р пы IP-адресов и выберите группу Социальные сети (рис.)

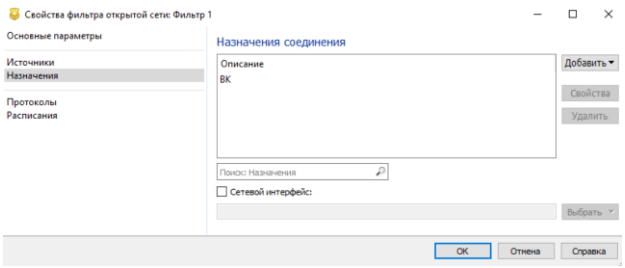


Рис. Вкладка «Назначение» окна «Свойства фильтра»

11. 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 (рис.):

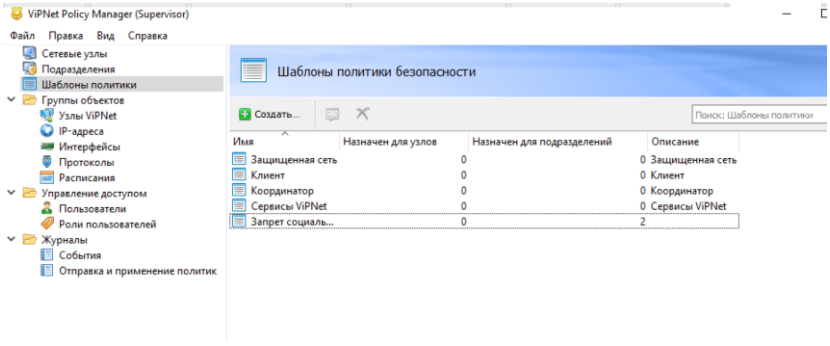


Рис. Раздел «Шаблоны политики» с политикой «Запрет социальных сетей»

12. Отправьте политики на узлы. Для этого в окне программы ViPNet Policy Manager перейдите в раздел Подразделения.

13. Выделите подразделения Центральный офис и Филиал, нажмите кнопку Отправить политики (рис).

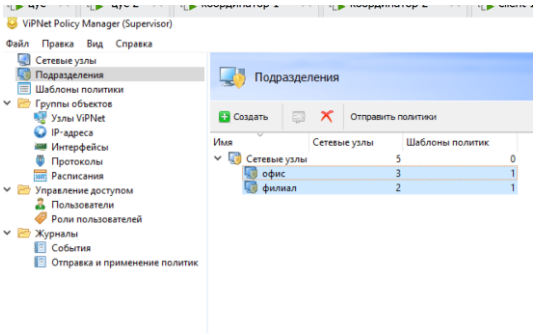


Рис Выбор подразделений для отправки политик безопасности

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

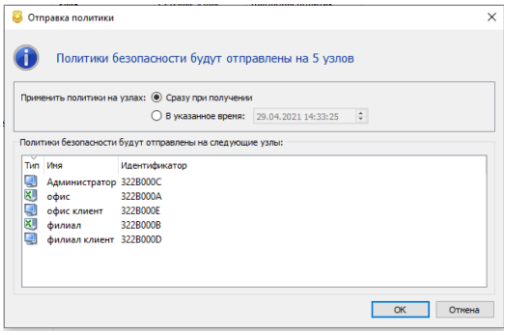


Рис. Отправка политики

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 (рис.).

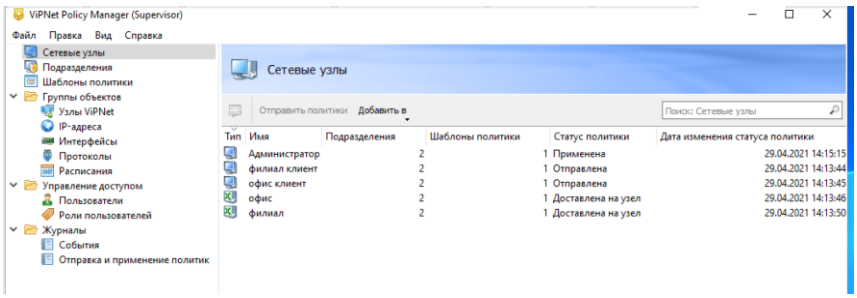


Рис. Контроль отправки и применения политик

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 (рис.).

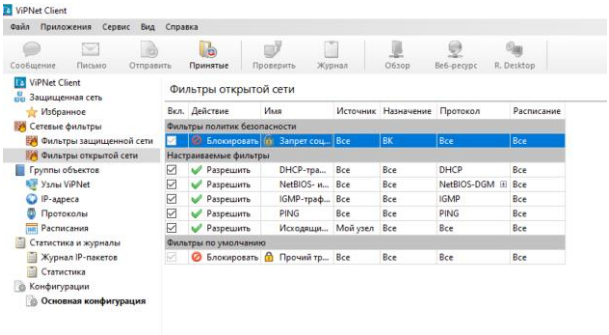


Рис. Окно ViPNet Client Монитор после применения политик

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 (рис.).

6. Остальные параметры окна Свойства фильтра открытой сети и Свойства шаблона политики менять не требуется.

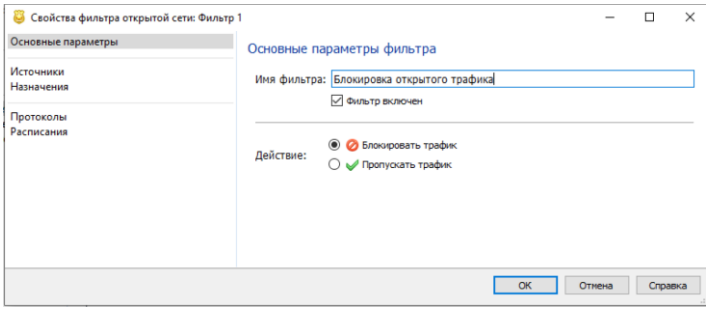


Рис. Вкладка. «Основные параметры» окна «Свойства фильтр

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.

Практическая работа № 47 «Организация межсетевого взаимодействия»

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 (рис.):

Данная схема должна быть реализована в виде стенда, собранного в соответствии с рис.

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.

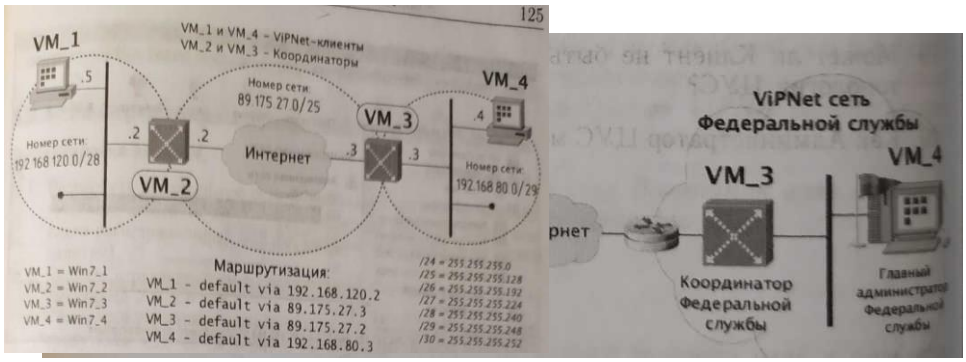


Рис. Схема стенда для практической работы

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

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

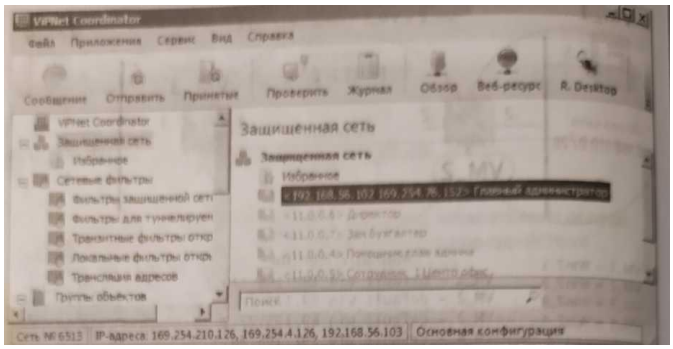
Установка ViPNet Coordinator в качестве межсетевого шлюза

В первую очередь развернем Координатор Центр офис для ранее созданной сети. Запустите установочный файл ViPNet Coordinator <имя_файла>. exe. Прочесе установки аналогичен

установке ViPNet Client. При этом необходимо установись ключи пользователя Координатор Центр офис.

Проверка доступности узлов в защищенной сети

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



(рис.).

Рис. Окно ViPNet Coordinator Монитор

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.

3. Сформировать справочники и ключи и на основе созданных дистрибутивов ключей развернуть на виртуальных машинах Координатор Федеральной службы и Администратор ViPNet Федеральной службы.

Пояснение к заданию

На виртуальной машине VM_4 необходимо установить программное обеспечение ViPNet Administrator и ViPNet Client, а на виртуальной машине VM_3 - ViPNet Coordinator.

Защищенная сеть Федеральной службы состоит из 3 узлов - 1 координатор и 2 клиента (табл.).

Таблица Состав защищенной сети Федеральной службы

	Тип	Название	Расположе-	Комментарии 1
1	Координа-тор	Координатор Федераль-ной службы	Федераль-ная служба	Для развертывания ПК ViPNet Coordinator
2	Клиент	Администратор ViPNet Федеральной службы		Для развертывания ПК ViPNet Administrator
3		Специалист по приёму отчётности		Рабочее место специалиста по приему отчетности

Матрица связей узлов защищённой сети Федеральной службы представлена в таблице.

На каждом узле защищенной сети присутствует по одному пользователю (табл.).

Связи между пользователями не установлены.

Не забудьте отключить у пользователей создание ЭП.

Таблица Матрица связей узлов в сети Федеральной службы

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

Таблица Определение пользователей

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

Порядок выполнения задания:

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

При настройке программ ViPNet задайте пароли:

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

— 11111111 — для пользователей защищённой сети.

Имя администратора VipNet Федеральной службы — Константин.

Настройка межсетевого взаимодействия с использованием индивидуального симметричного ММК

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

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

Пояснение к заданию

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

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

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

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

Организация межсетевого взаимодействия между сетями ViPNet состоит из следующих этапов:

1. Администратор первой сети ViPNet, инициирующий межсетевое взаимодействие, создает в Центре управления сетью файл мел сетевой информации, а в Удостоверяющем и ключевом центре межсетевой мастер-ключ. Затем по доверенным каналам связи он передает файл межсетевой информации и межсетевой маете ключ администратору второй сети ViPNet.

2. Администратор второй сети ViPNet принимает межсетевую информацию, затем создает файл с ответной межсетевой информацией и передает его администратору первой сети.

3. Администратор второй сети импортирует переданный ему межсетевой мастер-ключ.

4. Администратор первой сети завершает организацию межсетевого взаимодействия приемом ответной межсетевой информации.

5. Администратор каждой сети создаёт новые справочники и ключи и отправляет их на узлы своей сети.

После этого узлы доверенных сетей, участвующие в межсетевом взаимодействии, смогут обмениваться информацией друг с другом.

Внимание! Необходимо учитывать, что при организации межсетевого взаимодействия в реальной сети, пользователя Главный администратор не рекомендуется включать в межсетевую информацию и связывать его с другими пользователями доверенной сети из соображений безопасности. Также следует обратить внимание, что в Фильтрах защищенной сети по умолчанию разрешено подключение по RDP (на клиентах и координаторах), поэтому при организации межсетевого взаимодействия, необходимо будет запретить подключение по RDP из доверенной сети, а также проверить настройки удалённого доступа в ОС.

Порядок выполнения задания

Инициация межсетевого взаимодействия

Чтобы инициировать межсетевое взаимодействие с сетью ViPNet Федеральной службы, выполните следующие действия на рабочем месте Главный администратор сети Компании:

1. В окне ViPNet Центр управления сетью в меню Доверенные сети выберите пункт Установить взаимодействие. Будет запущен мастер Установка межсетевого взаимодействия.

2. На первой странице мастера выберите вариант Я инициатор межсетевого взаимодействия и нажмите кнопку Далее.

3. На странице Задайте информацию о другой сети ViPNet и координатор для связи с ней (необходимо правильно указать номер доверенной сети, с которой вы устанавливаете межсетевое взаимодействие, в противном случае могут возникнуть проблемы), впишите имя сети - Федеральная служба, которое будет отображаться в программе ViPNet Центр управления сетью, и выберите шлюзовой координатор своей сети - Координатор Центр офис. Затем нажмите Далее (рис.).

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.

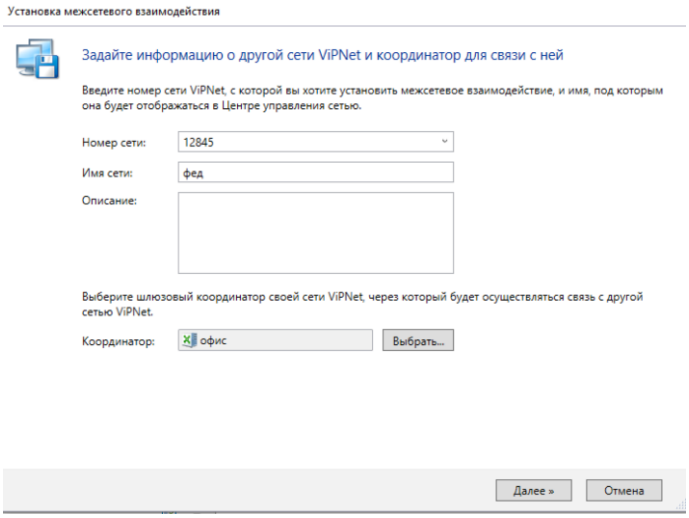


Рис. Фрагмент окна «Установка межсетевого взаимодействия»

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 (рис.):

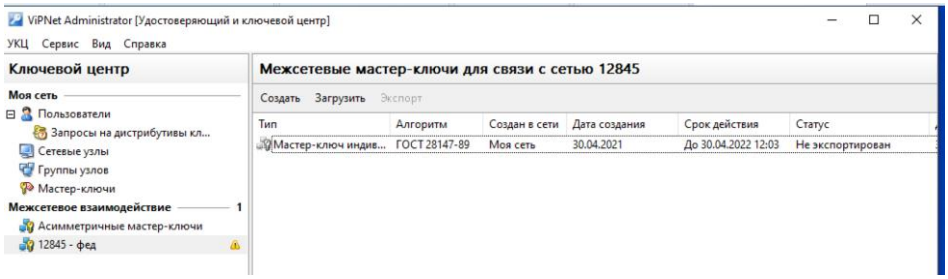


Рис. Создание ИСММК

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 (рис. 2.132).

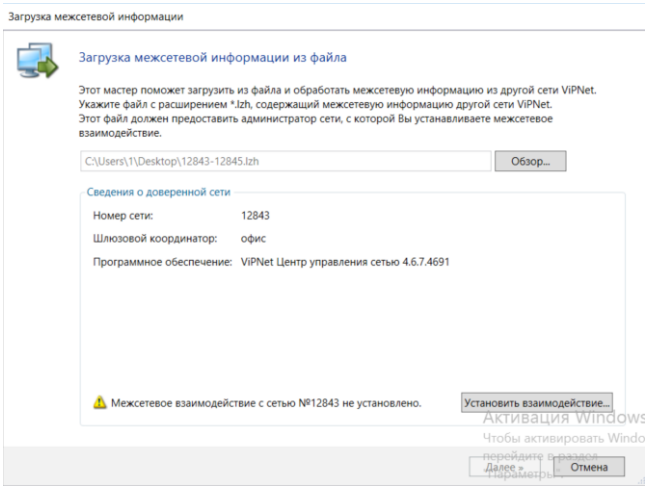


Рис Прием первичной межсетевой информации

1. Чтобы продолжить загрузку межсетевой информации, нажмите кнопку Установить взаимодействие.

2. На странице Задайте информацию о другой сети ViPNet и координатор для связи с ней выберите шлюзовой координатор - Координатор Федеральной службы, затем нажмите Далее.

3. 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.

4. 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.

5. Чтобы продолжить обработку межсетевой информации, нажмите кнопку Далее.

6. На странице Загрузка межсетевой информации после завершения обработки информации нажмите кнопку Готово.

7. 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 (рис.).

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 (рис.).
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

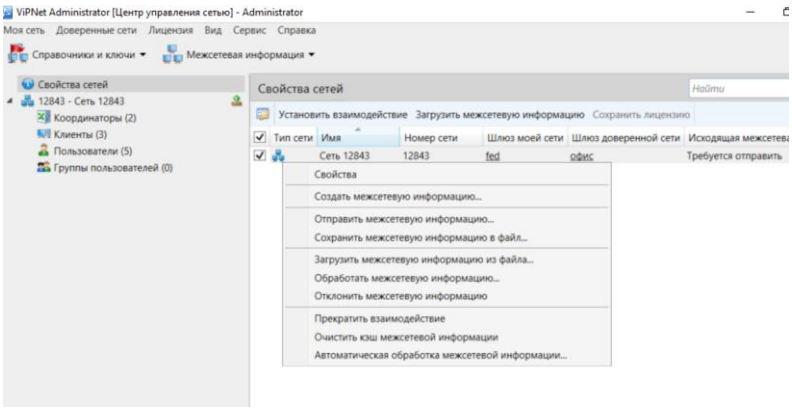


Рис. Создание ответной межсетевой информации для доверенной сети

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 (рис.).

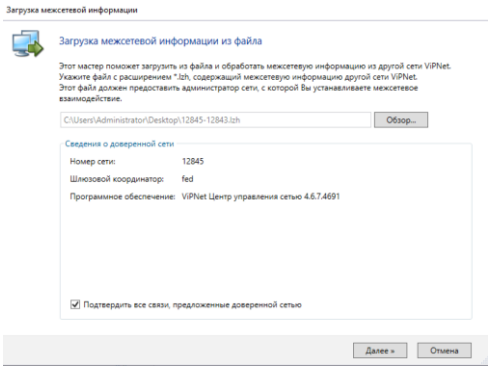


Рис. Прием ответной межсетевой информации из сети Федеральной службы

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 (рис.)*.

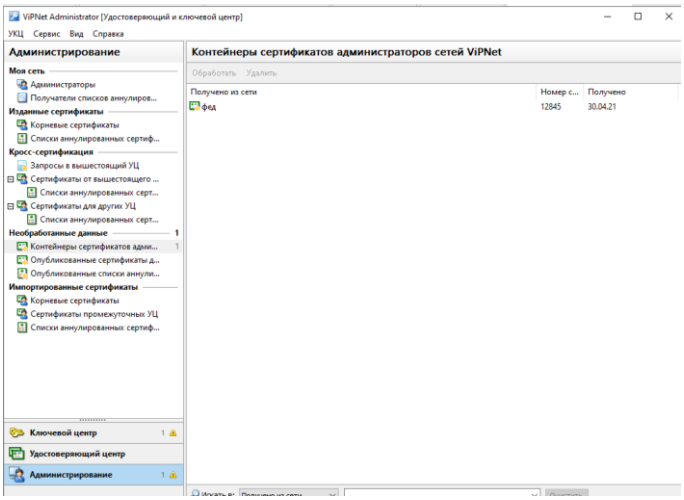


Рис. Обработка контейнеров сертификатов и CRL Фед. службы

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

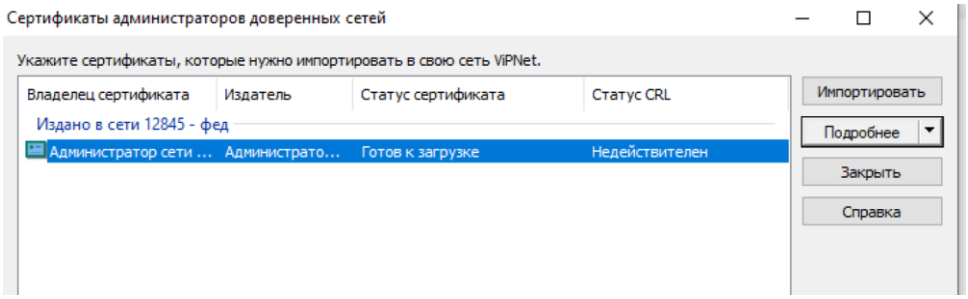


Рис. Сертификаты администраторов доверенных сетей

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.

Практическая работа № 48 «Модификация межсетевого взаимодействия в защищённой сети VipNet

Задание:

В настоящем задании необходимо:

1. Установить связи между пользователями доверенных сетей.

2. Удалить связи между пользователями доверенных сетей.

3. Прекращение межсетевого взаимодействия

Установление связей между пользователями доверенных се гей

Формулировка задания

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

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

Пояснение к заданию

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

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

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

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

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

Порядок выполнения задания

Чтобы добавить связи пользователей сети ViPNet Компании и Федеральной службы, выполните следующие действия на рабочем месте Главный администратор (сеть Компании):

1. В окне программы ViPNet Центр управления сетью в представлении Доверенные сети выберите сеть Федеральная служба и перейдите на вкладку Пользователи.

2. Зайдите в свойства пользователя Координатор Федеральной службы (рис.).

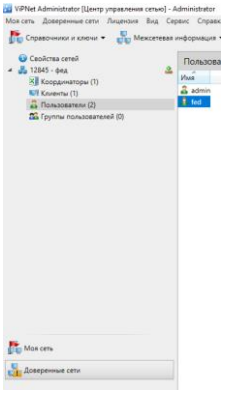


Рис. Пользователь «Координатор Фед службы»

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

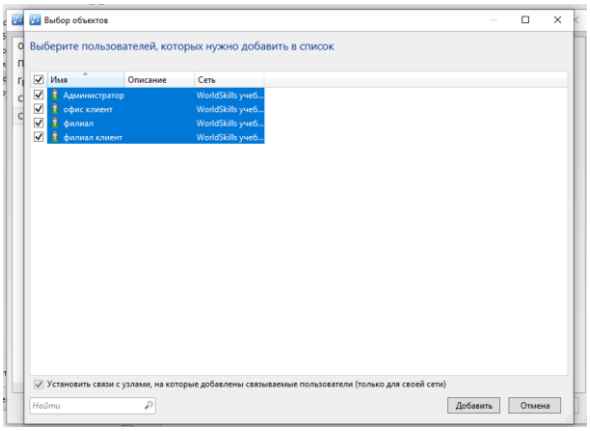


Рис. Добавление связей пользователю «Координатор Фед службы»

4. В представлении Доверенные сети выберите раздел Свойства сетей.

5. На панели просмотра щелкните правой кнопкой мыши на доверенную сеть Федеральная служба и в контекстном меню выберите пункт Создать межсетевую информацию. В открывшемся окне установите флажок Отправить межсетевую информацию после создания и нажмите кнопку Создать (рис.)

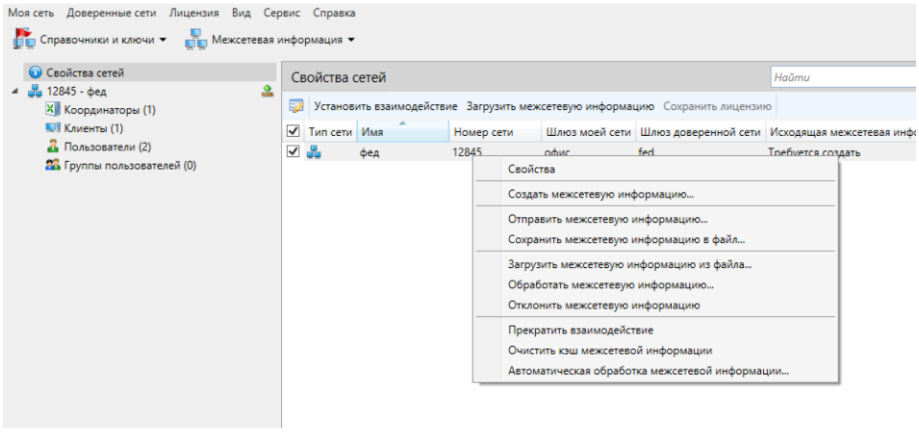


рис. Создание межсетевой информации для сети Фед. службы

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

1. В окне программы ViPNet Центр управления сетью в меню Доверенные сети выберите пункт Обработать межсетевую информацию.

2. В открывшемся окне выберите сеть Компании и нажмите кнопку Обработать выбранные.

3. В представлении Доверенные сети выберите раздел Свойства сетей.

4. На панели просмотра щелкните правой кнопкой мыши доверенную сеть Компании и в контекстном меню выберите пункт Создать межсетевую информацию.

5. В открывшемся окне установите флажок Отправить межсетевую информацию после создания и нажмите кнопку Создать.

6. Создайте и отправьте новые справочники и ключи для узла Координатор Федеральной службы.

Чтобы принять ответную межсетевую информацию от сети Федеральной службы, перейдите на рабочее место Главный администратор сети Компании и выполните следующие действия:

1. В окне программы ViPNet Центр управления сетью в меню Доверенные сети выберите пункт Обработать межсетевую информацию.

2. В открывшемся окне выберите сеть Федеральная служба и нажмите кнопку Обработать выбранные.

3. Создайте и отправьте новые справочники и ключи для узлов Сотрудник_1 Центр офис, Зам бухгалтера, Директор.

Для проверки правильности выполнения задания перейдите на узел Координатор Федеральной службы и убедитесь, что в списке узлов защищенной сети в программе ViPNet Coordinator Монитор появились клиенты Сотрудник_1 Центр офис, Зам бухгалтера, Директор.

Удаление связей между пользователями доверенных сетей

Формулировка задания

Удалить связи между пользователями сети Компании Директор Абросимов и сети Федеральной службы Координатор Федеральной службы. При этом из списка защищенной сети узла Координатор Федеральной службы будет исключен клиент Директор.

Порядок выполнения задания

Чтобы удалить связи пользователей сети ViPNet Компании и Федеральной службы, выполните следующие действия на рабочем месте Главный администратор (сеть Компании):

1. В окне программы ViPNet Центр управления сетью в представлении Доверенные сети выберите сеть Федеральная служба и перейдите на вкладку пользователи.

2. Зайти в свойства пользователя Координатор Фед. службы.

3. В открывшемся окне перейдите на вкладку Связи с пользователями и удалите из списка пользователей Директор Абросимов.

4. В представлении Доверенные сети выберите Свойства сетей.

5. На панели просмотра щелкните правой кнопкой мыши доверенную сеть Федеральная служба и в контекстном меню выверите пункт Создать межсетевую информацию.

6. В открывшемся окне установите флажок Отправить межсетевую информацию после создания и нажмите кнопку Создать.

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

1. В окне программы ViPNet Центр управления сетью в меню Доверенные сети выберите пункт Обработать межсетевую информацию.

2. В открывшемся окне выберите сеть и нажмите кнопку Обработать выбранные.

3. В представлении Доверенные сети выберите Свойства сетей.

4. На панели просмотра щелкните правой кнопкой мыши доверенную сеть Компании и в контекстном меню выберите пункт Создать межсетевую информацию.

5. В открывшемся окне установите флажок Отправить межсетевую информацию после создания и нажмите кнопку Создать.

6. Создайте и отправьте новые справочники и ключи для узла Координатор Федеральной службы.

Чтобы принять ответную межсетевую информацию от сети Федеральной службы, перейдите на рабочее место Главный администратор (сеть Компании) и выполните следующие действия:

1. В окне программы ViPNet Центр управления сетью в меню Доверенные сети выберите пункт Обработать межсетевую информацию.

2. В открывшемся окне выберите сеть Федеральной службы и нажмите кнопку Обработать выбранные.

3. Создайте и отправьте новые справочники и ключи для узла Директор.

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

Прекращение межсетевого взаимодействии

Формулировка задания

Прекратить межсетевое взаимодействия Компании и Федеральной службы.

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

Порядок выполнения задания

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

1. В окне программы ViPNet Центр управления сетью выберите представление Доверенные сети.

2. На панели навигации выберите раздел Свойства сетей.

3. На панели просмотра щелкните правой кнопкой мыши доверенную сеть Федеральная служба, межсетевое взаимодействие с которой требуется прекратить, и в контекстном меню выберите пункт Прекратить взаимодействие.

4. В окне подтверждения установите флажок Прекратить взаимодействие, затем нажмите кнопку Прекратить взаимодействие.

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

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

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

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

Практическая работа № 49 «Установка openssl в centos»

Задание:

Используйте ОС centos 7 версии.

1. Перед началом установки обновить систему до последних пакетов:
   sudo yum update

2. Далее проверить какая версия OpenSSL установлена:
   openssl version –a

3. Для установки средств разработки OpenSSL:
   sudo yum group install 'Development Tools'

4. Для установки необходимых пакетов:
   sudo yum install perl-core zlib-devel –y

В отчёт вставить скриншот с командами.

В отчёте вставить пояснения по пакетам perl-core и zlib-devel

5. Для скачивания последней версии:
   cd /usr/local/src/ - для перехода в папку

sudo wget https://www.openssl.org/source/openssl-1.1.1c.tar.gz - скачиваем в папку, в которую перешли

6. Для извлечения скачанного каталога:

sudo tar -xf openssl-1.1.1c.tar.gz

7. Для перехода в извлеченный каталог:

cd openssl-1.1.1c

8. Теперь можно установить, то что загрузили. Для этого используем команду:

sudo ./config --prefix=/usr/local/ssl --openssldir=/usr/local/ssl shared zlib

В отчёт вставить скриншот с командами.

В отчёте пояснить подробно команду установки.

9. Далее запускаем и проверяем:

sudo make

sudo make test

sudo make install

10. Для создания нового файла конфигурации openssl-1.1.1c.conf.:

cd /etc/ld.so.conf.d/ - команда перехода в папку

sudo nano openssl-1.1.1c.conf – команда запуска редактирования конфигурационного файла

11. В открытом файле ввести:
    /usr/local/ssl/lib

12. Затем следуя подсказкам внизу окна редактора nano Сохранить и выйти с сохранениями.

13. Затем перезагрузите, введя следующую команду:
    sudo ldconfig –v

14. Следующим шагом установки является замена в системе версии по умолчанию OpenSSL на новую версию.

15. Сначала сделаем резервную копию:
    sudo mv /bin/openssl /bin/openssl.backup

16. Затем создадим новые файлы для OpenSSL:
    sudo nano /etc/profile.d/openssl.sh

17. В файле необходимо набрать следующую информацию:

```
#Set OPENSSL_PATH
OPENSSL_PATH="/usr/local/ssl/bin"
export OPENSSL_PATH
PATH=$PATH:$OPENSSL_PATH
export PATH
```

Далее Сохранить и выйти.

18. Затем сделайте файл openssl.sh исполняемым:
    sudo chmod +x /etc/profile.d/openssl.sh

В отчёт вставить скриншоты с командами.

19. Затем перезагрузите среду OpenSSL (команда есть выше).

20. Затем проверьте каталог bin PATH, используя следующие команды:
    source /etc/profile.d/openssl.sh

echo $PATH

21. Проверяем версию установленной OpenSSL:
    which openssl

openssl version –a

В отчёт вставить скриншоты с командами.

Практическая работа № 50 «Создание самоподписанного сертификата SSL »

Задание:

1. Откройте Centos с установленным openssl.

2. Установить Apache для того, чтобы настроить для него виртуальные хосты:
   sudo yum install httpd

3. Затем включите Apache как службу CentOS, чтобы он автоматически запускался после перезагрузки:
   sudo systemctl enable httpd.service

4. Установить модуль mod_ssl
   udo yum install mod_ssl

5. Создать каталог для хранения закрытого ключа:
   sudo mkdir /etc/ssl/private

6. Изменить разрешения доступа (только для root):
   sudo chmod 700 /etc/ssl/private

7. Создать ключ SSL:
   sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/apache-selfsigned.key -out /etc/ssl/certs/apache-selfsigned.crt

В отчёт вставить скриншот с командами.

В отчёт вставить подробную информацию по команде создания SSL-ключа.

Практическая работа № 51 «Заполнение анкеты для сертификата»

Задание:

1. После генерации сертификата (CSR) откроется форма для заполнения информации о сертификате:

- **Country Name** (двухбуквенный код страны) - **RU** (для России)
- **State or Province** (Район, Область) - **Saint Petersburg**
- **Locality** (Полное название города) - **Saint Petersburg**
- **Organization** (Официальное наименование организации) - **Full Company Name LLC**
  Примечение: *При заказе сертификата физическим лицом (актуально для SSL-сертификатов с проверкой домена (**DV-Domain Validation**), в этом поле необходимо указать полное имя владельца сертификата, а в поле **Organizational Unit** - название вашей площадки или бренда.*
- **Organizational Unit** (необязательное поле: отдел/департамент) - **IT**
- **Common Name** (Имя домена, на который оформляется SSL-сертификат) - **www.mydomain.com**
  Примечание:*Если вы заказываете Wildcard-сертификат (сертификат для домена и его поддоменов), указанное здесь доменное имя должно начинаться с символа * (***.mydomain.com**).*

2. Заполняем все поля. В качестве common name вводим ip-адрес вашего IWTM.

После генерации в директории появятся файлы закрытого ключа (.key) и запроса на подпись сертификата (.csr).
Оба созданных вами файла будут помещены в соответствующие подкаталоги /etc/ssl каталога.

3. После создания сертификата просмотрите содержимое файла с помощью утилиты cat.

В отчет вставить скриншот с информацией по заполненной анкете.

4. Далее нужно создать Diffie-Hellman, которая используется для переговоров с Perfect Forward Secrecy с клиентами:
sudo openssl dhparam -out /etc/ssl/certs/dhparam.pem 2048
5. Добавляем вручную сгенерированный файл в конец нашего самозаверяющего сертификата:
cat /etc/ssl/certs/dhparam.pem | sudo tee -a /etc/ssl/certs/apache-selfsigned.crt
6. Выполните просмотр файла apache-selfsigned.crt

В отчёт вставить скриншот с информацией внутри вашего файла.

Практическая работа № 52 «Применение сертификата»

Задание:

1. Для применения созданных сертификатов нужно настроить виртуальные хосты для отображения нового сертификата.

Откройте файл конфигурации протокола Apache в текстовом редакторе с правами root:
sudo nano /etc/httpd/conf.d/ssl.conf

2. Найдите раздел, который начинается с <VirtualHost _default_:443>. Здесь необходимо внести несколько изменений, чтобы гарантировать, что наш сертификат SSL правильно применяется на нашем сайте.

3. Раскомментируйте DocumentRoot строку и отредактируйте адрес в кавычках в месте расположения корня документа вашего сайта. По умолчанию это будет /var/www/html, и вам не нужно менять эту строку, если вы не изменили корень документа для своего сайта.

4. Затем раскомментируйте ServerNameстроку и замените ее www.example.com, где IP-адресом вашего домена или сервера (в зависимости от того, что вы указали как общее имя в своем сертификате): /etc/httpd/conf.d/ssl.conf

5. Далее, найти SSLProtocoli SSLCipherSuite и закомментировать их.

6. Найти SSLCertificateFileи SSLCertificateKeyFile и изменить их в каталог , который мы сделали в /etc/httpd/ssl:
/etc/httpd/conf.d/ssl.conf

В отчёт вставить скриншоты с информацией по изменению файла конфигурации.

7. Для шифрования SSL создадим и откроем файл:
sudo nano /etc/httpd/conf.d/non-ssl.conf

8. Внутри создайте `VirtualHost`блок для соответствия запросов на порт 80. Внутри используйте `ServerName`директиву, чтобы снова соответствовать вашему доменному имени или IP-адресу. Затем используйте `Redirect`для соответствия любым запросам и отправьте их на SSL `VirtualHost`. Не забудьте включить конечную косую черту:
/etc/apache2/sites-available/000-default.conf

```
<VirtualHost *:80>
        ServerName www.example.com
        Redirect "/" "https://www.example.com/"
</VirtualHost>
```

9. Проверьте конфигурационный файл на наличие синтаксических ошибок, набрав:
sudo apachectl configtest

10. Перезапустите сервер Apache, чтобы применить изменения, введя:
sudo systemctl restart httpd.service

В отчёт вставить скриншоты с информацией по командам.

Попробуйте зайти на ваш IWTM через браузер. Должна быть информация о наличии сертификата.

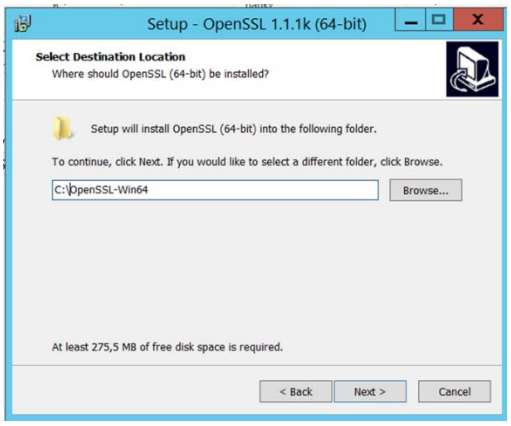
В отчет вставить скриншот о входе и о наличии сертификата.

Практическая работа № 53
«Перемещение ssl-сертификата с сервера windows на сервер, отличный от windows»

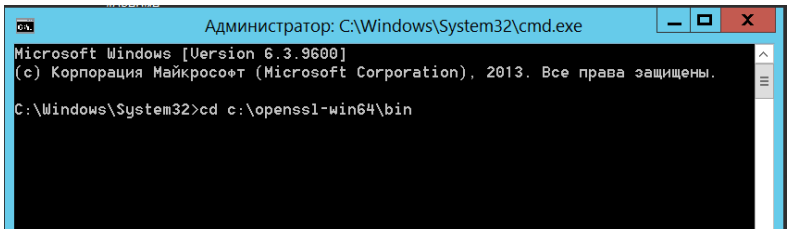
Задание:

1. Скачать Win32OpenSSL (https://slproweb.com/products/Win32OpenSSL.html)

При установке указываем путь попроще, к примеру:



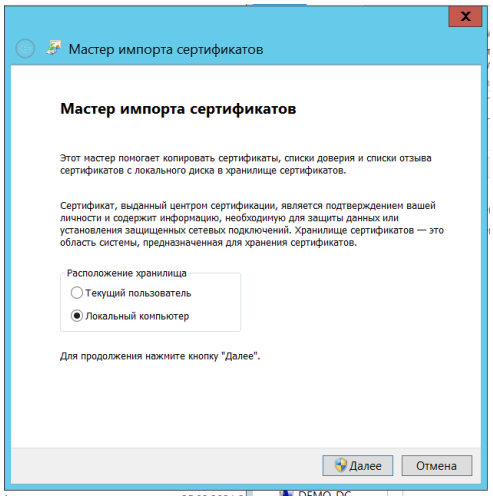
2. Открываем CMD от имени администратора, переходим в каталог, указанный при установке openssl в папку bin

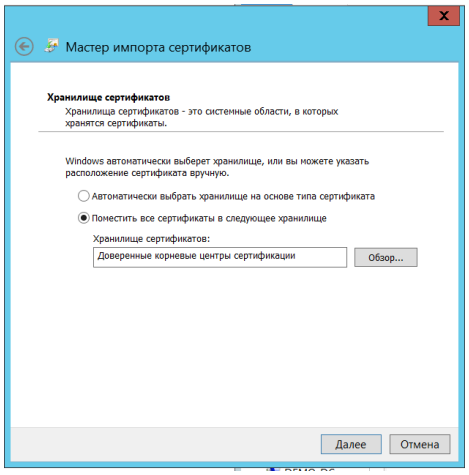


3. Создаем наше CA
openssl genrsa -out CA.key 4096

4. Создаем корневой сертификат
openssl req -x509 -new -key CA.key -days 365 -out CA.crt

5. Устанавливаем сертификат





6. Создаем сертификат сервера подписанный нашим CA
openssl genrsa -out web-server.key 4096

Создаем запрос на сертификат.
openssl req -new -key web-server.key -out web-server.csr
и подписать запрос на сертификат нашим корневым сертификатом.
openssl x509 -req -in web-server.csr -CA CA.crt -CAkey CA.key -CAcreateserial -out web-server.crt -days 365
Тут важно указать имя сервера: домен или IP
Common Name (eg, YOUR name) []:

7. Создаем сертификат пользователя подписанный нашим CA

openssl genrsa -out user.key 4096

Создаем запрос на сертификат.
openssl req -new -key user.key -out user.csr
и подписать запрос на сертификат нашим корневым сертификатом.
openssl x509 -req -in user.csr -CA CA.crt -CAkey CA.key -CAcreateserial -out user.crt -days 365
Тут важно указать имя сервера: домен или IP *Common Name (eg, YOUR name) []:*

8. Скопировать из папки bin в папку на рабочем Certificates IWTM столе получившиеся 3 ключа key и 3 сертификата cer.

9. Скопировать в Certificates IWTM файл web-server.crt и переименовать его в web-server.pem

10. На сервер TM при помощи MC (Left – FTP link…) скопировать с заменой в раздел /etc/infowatch/certification/ web-server.pem и web-server.key

11. На домене удалить web-server.pem, в папке должно остаться 3 сертификата и 3 ключа

12. В папке создать файл (блокнот) файл demo.p12, скопировать в него последовательно содержимое ca.cer, web-server.cer, user.ser ОБЯЗАТЕЛЬНО проверить, что файл не txt а p12
openssl pkcs12 -export -out certificate.p12 -inkey ca.key -in certificate.crt -certfile more.crt

В отчёт вставить скриншоты, подтверждающие выполнение задания.

Практическая работа № 54 «Установка nginx для последующей настройки прокси-сервера»

Задание:

1. Добавьте EPEL-репозиторий:
sudo yum install epel-release

2. Установите Nginx:
sudo yum install nginx

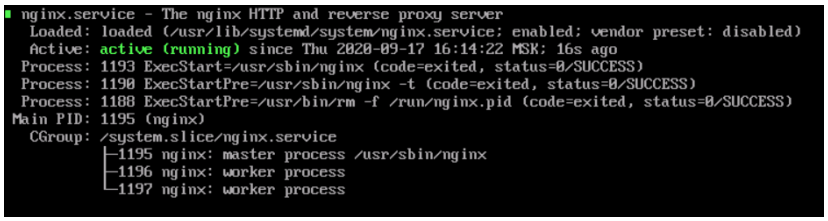
3. Разрешите HTTP и HTTPS-трафик на брандмауэре:
sudo firewall-cmd --permanent --add-service=http
sudo firewall-cmd --permanent --add-service=https

4. Перезагрузите брандмауэр:
sudo firewall-cmd --reload

5. Запустите Nginx:
sudo systemctl start nginx

6. Настройте автозапуск Nginx при перезагрузке системы:
sudo systemctl enable nginx

7. Проверьте статус службы Nginx:
sudo systemctl status nginx
Он должен быть active:



8. Перейдите в браузере по адресу http://имя_сервера_или_IP/.
Если по адресу откроется стартовая страница CentOS Nginx, то установка выполнена верно:

Готово, Nginx установлен.
В отчёт вставить скриншоты с командами установки.
В отчет вставить скриншоты с результатом установки Nginx

9. Как работают nginx и его модули, определяется в конфигурационном файле. По умолчанию, конфигурационный файл называется nginx.conf и расположен в каталоге /usr/local/nginx/conf, /etc/nginx или /usr/local/etc/nginx.
Зайти в каталог с конфигурационным файлом. Просмотреть содержимое каталога. Просмотреть содежимое файла конфигурации.

В отчёт вставить скриншоты с командами просмотра.

Практическая работа № 55 «Настройка прокси-сервера с помощью nginx»

Задание:

Одним из частых применений nginx является использование его в качестве прокси-сервера, то есть сервера, который принимает запросы, перенаправляет их на проксируемые сервера, получает ответы от них и отправляет их клиенту.

Мы настроим базовый прокси-сервер, который будет обслуживать запросы изображений из локального каталога и отправлять все остальные запросы на проксируемый сервер. В этом примере оба сервера будут работать в рамках одного экземпляра nginx.

1. Во-первых, создайте проксируемый сервер, добавив ещё один блок server в конфигурационный файл nginx со следующим содержимым:

```
server {
   listen 8080;
   root /data/up1;

   location / {
   }
}
```

Это будет простой сервер, слушающий на порту 8080 (ранее директива listen не указывалась, потому что использовался стандартный порт 80) и отображающий все запросы на каталог /data/up1 в локальной файловой системе. Создайте этот каталог и положите в него файл index.html. Обратите внимание, что директива root помещена в контекст server. Такая директива root будет использована, когда директива location, выбранная для выполнения запроса, не содержит собственной директивы root.

В отчёт вставьте скриншот содержимого конфигурационного файла.

2. Далее, используйте конфигурацию сервера из предыдущего раздела и видоизмените её, превратив в конфигурацию прокси-сервера. В первый блок location добавьте директиву proxy_pass, указав протокол, имя и порт проксируемого сервера в качестве параметра (в нашем случае это http://localhost:8080):

```
server {
   location / {
      proxy_pass http://localhost:8080;
   }

   location /images/ {
      root /data;
   }
}
```

3. Мы изменим второй блок location, который на данный момент отображает запросы с префиксом /images/ на файлы из каталога /data/images так, чтобы он подходил для запросов изображений с типичными расширениями файлов. Изменённый блок location выглядит следующим образом:

```
location ~ \.(gif|jpg|png)$ {
   root /data/images;
}
```

Параметром является регулярное выражение, дающее совпадение со всеми URI, оканчивающимися на .gif, .jpg или .png. Регулярному выражению должен предшествовать символ ~. Соответствующие запросы будут отображены на каталог /data/images.

Когда nginx выбирает блок location, который будет обслуживать запрос, то вначале он проверяет директивы location, задающие префиксы, запоминая location с самым длинным подхо-

дящим префиксом, а затем проверяет регулярные выражения. Если есть совпадение с регулярным выражением, nginx выбирает соответствующий location, в противном случае берётся запомненный ранее location.

4. Итоговая конфигурация прокси-сервера выглядит следующим образом:

```
server {
   location / {
      proxy_pass http://localhost:8080/;
   }

   location ~ \.(gif|jpg|png)$ {
      root /data/images;
   }
}
```

Этот сервер будет фильтровать запросы, оканчивающиеся на .gif, .jpg или .png, и отображать их на каталог /data/images (добавлением URI к параметру директивы root) и перенаправлять все остальные запросы на проксируемый сервер, сконфигурированный выше.

5. Чтобы применить новую конфигурацию, отправьте сигнал reload nginx'у, как описывалось в предыдущих разделах.

В отчет вставить скриншоты с командами и результатом выполнения.
В помощь к работе: https://nginx.org/ru/docs/beginners_guide.html

Практическая работа № 56 «Настройка правильной работы сети при использовании nginx»

1. Получение SSL сертификата необходимо для использования протокола HTTPS. Данный протокол защищает соединение между сервером и клиентом, особенно критично для чувствительных данных, таких как логины, пароли, данные по банковским картам, переписка и так далее. Последние несколько лет поисковые системы наиболее лояльны к сайтам, использующих данный протокол, есть прекрасная возможность получить ssl сертификат бесплатно от Let's Encrypt, устанавливаем его клиент certbot из официального репозитория:
apt install certbot python3-certbot-nginx

Будет задан вопрос: Do you want to continue? [Y/n]
Нажимаем Y, затем ENTER.

2. Запрашиваем сертификат у Certbot:
certbot certonly --agree-tos -m mymail@yandex.ru --webroot -w
/home/webuser/www/sampledomain.ru/ -d sampledomain.ru

3. Появится вопрос о передаче вашего адреса электронной почты компании партнеру:
(Y)es/(N)o:
Жмем Y, потом ENTER.

Сертификат успешно получен, если появилось сообщение:

```
IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have
been saved at:
   /etc/letsencrypt/live/sampledomain.ru/fullchain.pem
   Your key file has been saved at:
   /etc/letsencrypt/live/sampledomain.ru/privkey.pem
   Your cert will expire on 2021-05-27. To obtain a
new or tweaked
   version of this certificate in the future, simply
run certbot
   again. To non-interactively renew *all* of your
certificates, run
   "certbot renew"
 - Your account credentials have been saved in your
Certbot
   configuration directory at /etc/letsencrypt. You
should make a
   secure backup of this folder now. This
configuration directory will
   also contain certificates and private keys obtained
by Certbot so
   making regular backups of this folder is ideal.
 - If you like Certbot, please consider supporting our
work by:

   Donating to ISRG / Let's Encrypt:
https://letsencrypt.org/donate
   Donating to EFF:
https://eff.org/donate-le
```

Сертификат действителен 90 дней. Теперь необходимо позаботиться об автоматическом продлении сертификатов, открываем файл:

nano /etc/cron.d/certbot

4. Приводим его к следующему виду:

SHELL=/bin/sh

PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

0 */12 * * * root test -x /usr/bin/certbot -a \! -d /run/systemd/system && perl -e 'sleep int(rand(43200))' && certbot -q renew --renew-hook "systemctl reload nginx"

Нажимаем комбинацию клавиш Ctrl+O, внизу появится строка подтверждения: File Name to Write: /etc/cron.d/certbot, нажимаем ENTER для сохранения изменений, затем Ctrl+X для выхода из редактора.

Дважды в день будет происходить проверка необходимости обновления сертификатов на сервере, если какому-либо осталось 30 дней и меньше до истечения срока действия – он будет обновлен, а nginx перезагружен.

В отчёт вставить скриншот с командами.

5. Протестируем процесс обновления без внесения изменений:

certbot renew --dry-run

Ждем около полминуты, на экран будет выведен подробный отчет. Если присутствует строка Congratulations, all renewals succeeded – значит все настроено правильно. Если когда-либо в процессе обновления произойдет сбой – Let’s Encrypt уведомит о приближающимся конце срока действия сертификата по электронной почте, указанной при первом запросе.

6. После получения сертификата необходимо прописать директивы в файл конфигурации виртуального хоста, отвечающие за поддержку SSL. Сразу же реализуем перенаправление всех запросов, приходящих на 80-й порт к порту 443, т.е. с http протокола на https. Открываем файл:

nano /etc/nginx/sites-available/sampledomain.ru.conf

7. Приводим его к следующему виду:

```
server {
        listen 80;
        server_name sampledomain.ru www.sampledomain.ru;
        root /home/webuser/www/sampledomain.ru;
        return 301 https://sampledomain.ru$request_uri;
        }
server
        {
        listen 443 ssl;
        server_name sampledomain.ru www.sampledomain.ru;
        # SSL support
        ssl_certificate
/etc/letsencrypt/live/sampledomain.ru/fullchain.pem;
        ssl_certificate_key
/etc/letsencrypt/live/sampledomain.ru/privkey.pem;
        charset utf-8;
        root /home/webuser/www/sampledomain.ru;
        index index.php index.html index.htm;

        # Static content
        location ~* ^.+.
(jpg|jpeg|gif|png|css|zip|tgz|gz|rar|bz2|doc|xls|exe|pdf|ppt|txt|tar|mid|
midi|wav|mp3|bmp|flv|rtf|js|swf|iso)$ {
                        root /home/webuser/www/sampledomain.ru;
                }

        location ~ \.php$
        {
                include fastcgi.conf;
                fastcgi_intercept_errors on;
                try_files $uri =404;
                fastcgi_pass unix://var/run/php/sampledomain.ru.sock;
        }

        location / {
                try_files $uri $uri/ /index.php?q=$uri$args;
        }
        }
```

8. Нажимаем комбинацию клавиш Ctrl+O, внизу появится строка подтверждения: File Name to Write: /etc/nginx/sites-available/sampledomain.ru.conf, нажимаем ENTER для сохранения изменений, затем Ctrl+X для выхода из редактора.

9. Перезапускаем веб-сервер:

service nginx restart

10. Теперь в браузере при попытке перехода по адресу http://sampledomain.ru будет выполнено перенаправление на https://sampledomain.ru

11. Открываем файл нашего тестового виртуального хоста:

nano /etc/nginx/sites-available/sampledomain.ru.conf

В отчёт вставить скриншот с командами.

12. Находим location, указывающий на отдачу статического контента и добавляем директиву expires:

```
# Static content
        location ~* ^.+.
(jpg|jpeg|gif|png|css|zip|tgz|gz|rar|bz2|doc|xls|exe|pdf|ppt|t
xt|tar|mid|midi|wav|mp3|bmp|flv|rtf|js|swf|iso)$ {
                        root
/home/webuser/www/sampledomain.ru;
                        expires 1d;
                }
```

Как обычно сохраняем результат Ctrl+O, подтверждаем нажатием ENTER, выходим из редактора Ctrl+X. В данном случае файлы, расширения которых соответствуют приведенным выше, будут храниться в браузере клиента, только после истечения суток – они будут запрошены повторно.

Кэширование позволяет значительно уменьшить время доставки контента и его объем, снизить нагрузку на сервер, а значит, ваш сайт сможет работать значительно быстрее и принять больше посетителей.

13. В nginx существует стандартная возможность мониторинга работы сервера, выясним доступность модуля в нашей сборке:

nginx -V 2>&1 | grep -o with-http_stub_status_module

14. Если в ответ получили with-http_stub_status_module – модуль доступен. Рассмотрим включение мониторинга на примере виртуального хоста, открываем файл:

nano /etc/nginx/sites-available/sampledomain.ru.conf

15. Добавляем location /nginx_status, в итоге файл выглядит следующим образом:

```
server {
        listen 80;
        server_name sampledomain.ru www.sampledomain.ru;
        root /home/webuser/www/sampledomain.ru;
        return 301 https://sampledomain.ru$request_uri;
        }
server
        {
        listen 443 ssl;
        server_name sampledomain.ru www.sampledomain.ru;
        # SSL support
        ssl_certificate
/etc/letsencrypt/live/sampledomain.ru/fullchain.pem;
        ssl_certificate_key
/etc/letsencrypt/live/sampledomain.ru/privkey.pem;
        charset utf-8;
        root /home/webuser/www/sampledomain.ru;
        index index.php index.html index.htm;

        # Static content
        location ~* ^.+.
(jpg|jpeg|gif|png|css|zip|tgz|gz|rar|bz2|doc|xls|exe|pdf|ppt|txt|tar|mid|
midi|wav|mp3|bmp|flv|rtf|js|swf|iso)$ {
                        root /home/webuser/www/sampledomain.ru;
                        expires 1d;
                }

        location ~ \.php$
        {
                include fastcgi.conf;
                fastcgi_intercept_errors on;
                try_files $uri =404;
                fastcgi_pass unix://var/run/php/sampledomain.ru.sock;
        }

        location / {
                try_files $uri $uri/ /index.php?q=$uri$args;
        }
        location /nginx_status {
                stub_status on;
                access_log off;

        }
        }
```

Сохраняем результат Ctrl+O, подтверждаем нажатием ENTER, выходим из редактора Ctrl+X. Перезапускаем веб-сервер:

service nginx restart

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

16. В браузере при переходе по адресу sampledomain.ru/nginx_status будет представлена статистика работы сервера:

```
Active connections: 2
server accepts handled requests
 797 797 334
Reading: 0 Writing: 1 Waiting: 1
```

Active connections – текущее количество клиентских соединений;

accepts – принятые соединения;

handled – обработанные, обычно равно количеству принятых;

requests – количество клиентских запросов;

Reading – текущее количество соединений, для которых сервер читает заголовок запроса;

Writing – текущее количество соединений, для которых сервер отправляет ответ клиенту;

Waiting – текущее количество простаивающих соединений, для которых сервер ожидает запроса.

Также статистику можно получить из командной строки:

curl https://sampledomain.ru/nginx_status

Не рекомендуется статистику выставлять на всеобщее обозрение, ниже рассмотрим вопросы безопасности и ограничений доступа.

В отчёт вставить скриншот с командами.

Практическая работа № 57 «Установка серверной версии Ubuntu»

Задание 1:

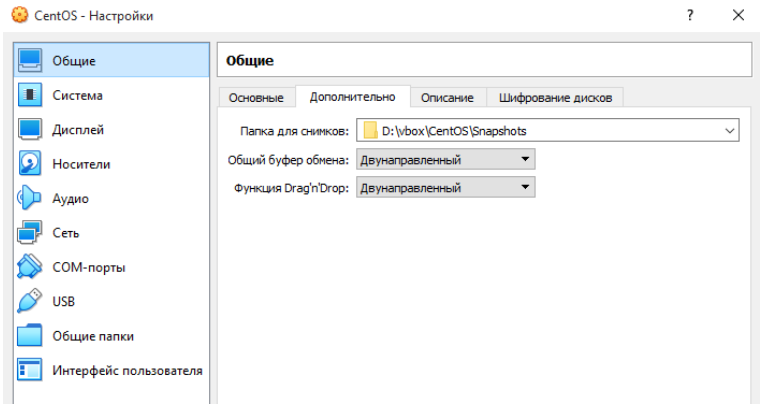
1. Создать новую виртуальную машину в VitrualBox. Для вашей машины выбрать следующие параметры:

В качестве имени указать название ОС и ваши фамилии.

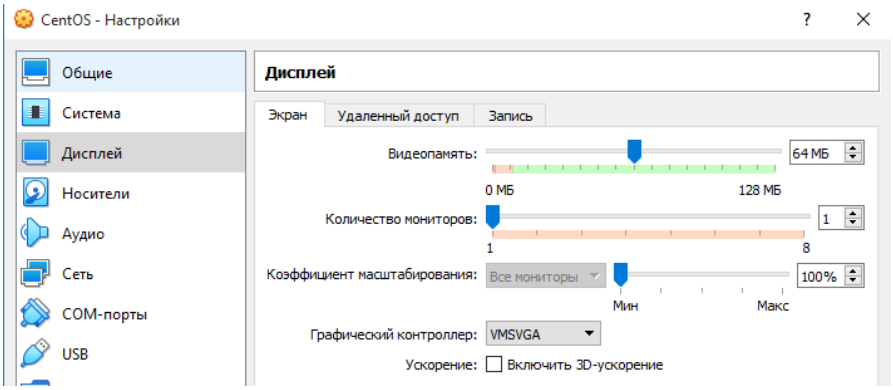
Объём оперативной памяти от 2048 Мб.

Размер виртуального жёсткого диска 20 Гб.

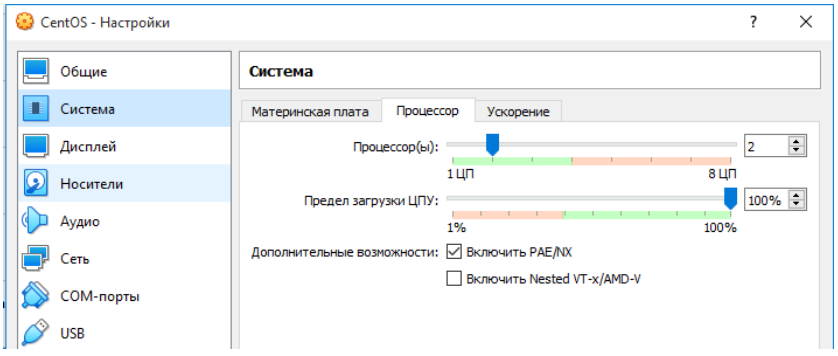
После создания виртуальной машины зайдите в Настройки созданной машины и выставите двунаправленный общий буфер обмена и функцию Drag’n’Drop:



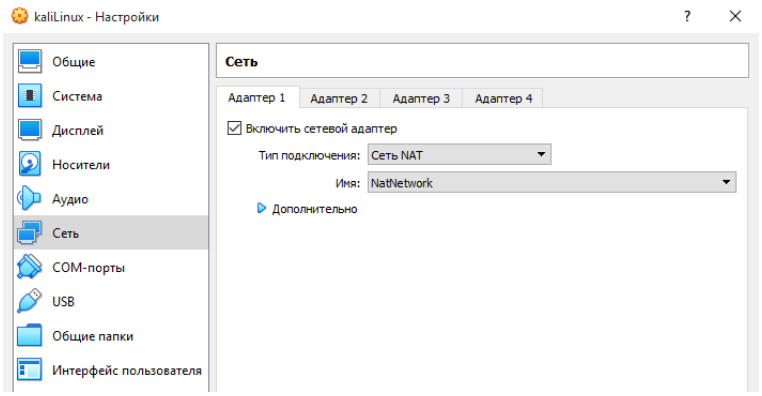
Далее на вкладке Дисплей:



Если есть возможность, то на вкладке Процессор поставить 2:

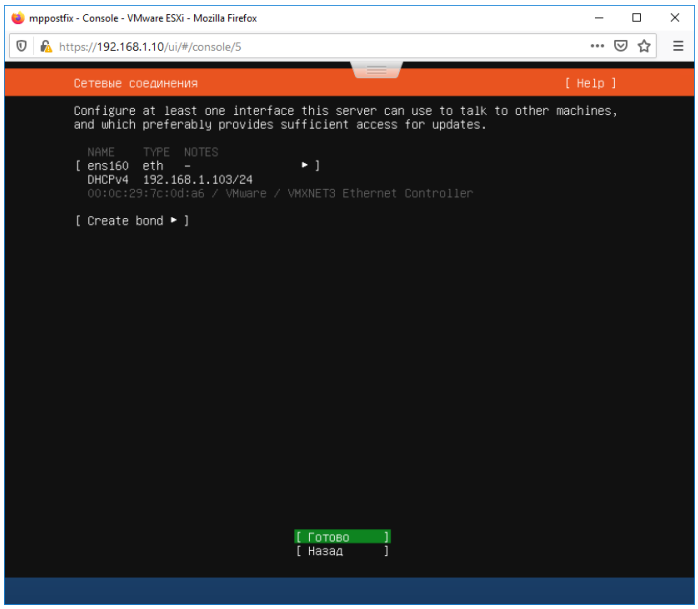


Далее в настройках поставить:



2. Запустить виртуальную машину, выбрать iso-файл с дистрибутивом Ubuntu Server.

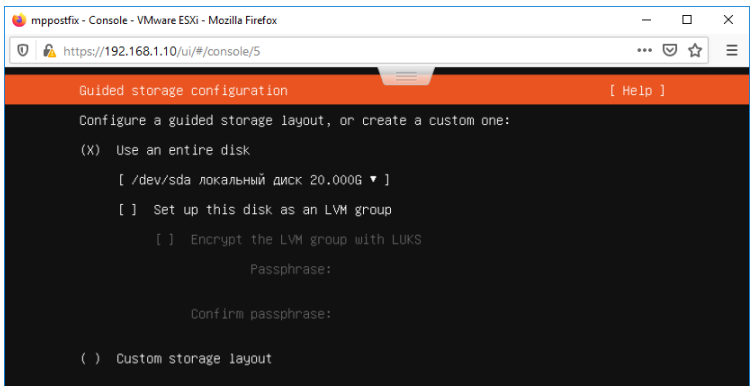
3. Начнётся установка. Выбрать язык Русский. Далее выбрать Установить с обновлениями. Если не получается, то пропустить и поставить без обновлений. Далее Готово → Готово. Сетевые настройки изменить. Для этого нужно выбрать ens160…→ Изменить IPv4→ Enter



Установить следующие настройки сети:

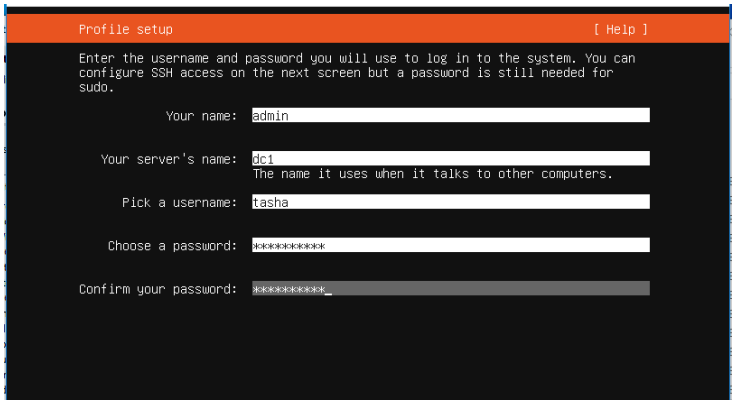
Далее Сохранить и Готово. Далее оставляем пустым поле адреса прокси-сервера и Готово. Далее Готово.

Далее:



Далее смотрим на партиции и нажимаем Готово. Далее выбираем Продолжить.

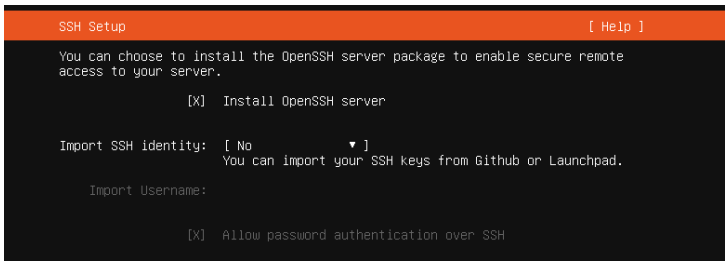
Далее настройки профиля:



Пишем свои данные, придумываем имя своему серверу.

В отчёт поместить скриншот с настройками профиля и написать пароль.

Далее ставим «крестик»:



Далее Готово. Начнётся установка, затем нужна будет перезагрузка.

Обратите внимание на то, что серверная версия Ubuntu 20 не имеет графического интерфейса. Примерно так будет выглядеть ваше приветственное окно:

В отчёт вставить скриншот, подтверждающий успешный вход в систему.

Задание 2:

1. В качестве рабочей станции необходимо установить KaliLinux на виртуальную машину. Назвать новую виртуальную машину KaliLinux и ваши фамилии. Настройки виртуальной машины повторить с настроек виртуальной машины из Задания1.

2. Далее запустить виртуальную машину, указать ей iso-файл установки. Затем выбрать графическую инсталляцию. Язык интерфейса русский. Выберете удобный для вас способ переключения языка.

3. В отчёт запишите Имя вашего компьютера. При установке пропустите имя в сети.

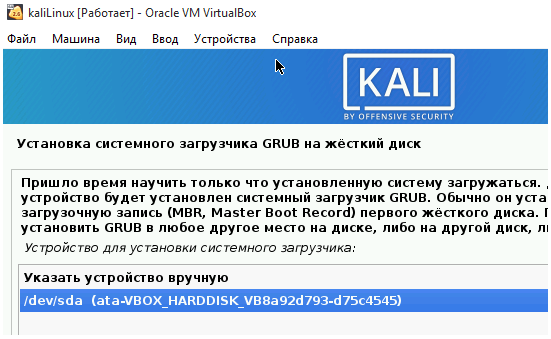
4. Далее придумайте и запишите в отчёт имя пользователя, пароль.

5. Разметка дисков по умолчанию. Обратите внимание, на необходимость согласиться с разбиением дисков.

6. Настройку менеджеров пакетов пропустить.

7. Выбор программного обеспечения по умолчанию.

8. При выборе установки системного загрузчика GRUB выбрать путь как показано ниже:



После установки перезагрузить, зайти в систему.

В отчёт вставить скриншот Рабочего стола с установленного KaliLinux.

Задание 3:

Ответить на следующие вопросы:

- ✓ Чем отличается установка серверной версии Ubuntu от пользовательской?
- ✓ Какие сложности/проблемы возникли при установке операционных систем и как вы их решили?
- ✓ Для чего можно использовать серверную версию Ubuntu?

Практическая работа № 58 «Установка Samba»

Задание 1:

1. Запустите сервер Ubuntu, войдите в систему.

2. Для установки и настройки Samba понадобятся root-права. Чтобы войти в режим суперпользователя нужно набрать команду sudo su. Если у вас удалось войти в режим, то ваше приглашение командной строки будет выглядеть примерно так:

```
root@dc1:/home/tasha# _
```

3. Обновите систему командой: sudo apt update

4. Установить набор сетевых утилит командой sudo apt install net-tools

5. Узнать текущий ip-адрес командой ip addr show или ifconfig. Если правильно уметь читать значения на экране, то в информации содержатся не только ip-адреса, но и имя вашего интерфейса, в дальнейшем эти данные знать необходимо для настройки статического ip-адреса. В отчёт вставьте скриншот с данной информацией.

6. С помощью команды hostnamectl проверьте имя вашего будущего сервера. В отчёт вставьте скриншот с информацией и отдельно напишите имя вашего сервера.

7. Далее для сервера необходим статический ip-адрес. Для настройки необходимо поправить вручную файлик в каталоге /etc/netplan/. Для начала необходимо узнать имя вашего интерфейса командой ifconfig –a. В отчёт запишите название вашего интерфейса.

```
root@dc1:/etc/netplan# ifconfig -a
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe0a:a628  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:0a:a6:28  txqueuelen 1000  (Ethernet)
        RX packets 117310  bytes 122453698 (122.4 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 31705  bytes 1953977 (1.9 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 174  bytes 14804 (14.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 174  bytes 14804 (14.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@dc1:/etc/netplan#
```

8. Теперь можно приступить к правке файла, находящегося в каталоге /etc/netplan/. С помощью команды ls смотрим название вашего файла. Тип файла у всех одинаковый, а название может отличаться.

Пример:

```
root@dc1:/# ls /etc/netplan/
00-installer-config.yaml
root@dc1:/#
```

9. Открываем файл для редактирования. Можно с помощью текстового редактора nano и маски файла *.yaml: nano /etc/netplan/*.yaml

```
  GNU nano 4.8                  /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  ethernets:
    enp0s3:
      dhcp4: no
      dhcp6: no
      addresses: [10.0.2.10/24, ]
      gateway4: 10.0.2.1
      nameservers:
              addresses: [10.0.2.1, ]
  version: 2
```

Далее внизу экрана у вас есть подсказка как записать, подтвердить название и выйти (Ctrl+O, Enter, Ctrl+X).

10. Теперь нужно применить новые сетевые настройки, для этого выполняем команду netplan apply. Кроме этого в VirtualBox поменяйте сеть с NAT на СЕТЬ NAT. При это на экране вы должны увидеть информацию о рестарте сетевого адаптера. В отчёт поместите информацию об изменившихся сетевых настройках (команда ifconfig + скриншот).

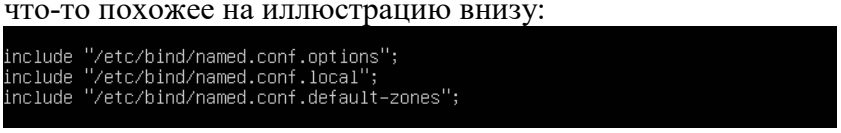
11. Для возможности дальнейшего продолжения установки софта необходимо проверить наличие доступа в интернет. После изменения сетевых настроек могло пойти что-то не так. Проверьте наличие доступа в Интернет с помощью ping, например, ping 8.8.8.8 и ping ya.ru. В отчёт поместите скриншот с удачным результатом.

12. Начинаем установку необходимого софта. Установить bind с помощью команды apt install bind9. Проверяем его версию с помощью команды named –v. В отчёт помещаем скриншот с данной информацией.

13. Далее смотрим где bind держит named.conf. Для этого выполняем команду named –V | grep sysco. В отчёт вставляем скриншот с результатом.
Скорее всего вы увидите, что –sysconfdir=**/etc/bind** – это папка где лежит файл named.conf.

14. Далее смотрим, где днс сервер держит кеш с помощью команды cat /etc/passwd | grep bind. В отчёт помещаем скриншот с результатом. Данная директория понадобится при дальнейшей настройке.

15. Проверяем named.conf с помощью команды nano /etc/bind/named.conf. Должны увидеть что-то похожее на иллюстрацию внизу:



Для дальнейшей работы понадобится первый и последний файлы.

16. Правим named.conf.options, а также первой командой делаем бэкап данного файла
sudo cp /etc/bind/named.conf.options /etc/bind/named.conf.options_bak
sudo nano /etc/bind/named.conf.options
Удаляем содержимое и заменяем следующим текстом:

```
# Глобальные настройки
options {
  auth-nxdomain yes;
  directory "/var/cache/bind"; #Папка с кешем bind
  notify no;
  empty-zones-enable no;
  tkey-gssapi-keytab "/var/lib/samba/private/dns.keytab";
  minimal-responses yes;

  # IP адреса и подсети от которых будут обрабатываться запросы
  allow-query {
    127.0.0.1;
    10.0.2.0/24; #Текущая локальная сеть dc1
  };

  # IP адреса и подсети от которых будут обрабатываться рекурсивные запросы
  # (Зон не обслуживаемых этим DNS сервером)
  allow-recursion {
```

```
    127.0.0.1;
    10.0.2.0/24; #Текущая локальная сеть dc1
  };

  # Перенаправлять запросы, на которые нет информации в локальной зоне
  # на следующие сервера:
  forwarders {
    8.8.8.8; #IP адрес DNS форвардера
    8.8.4.4; #IP адрес DNS форвардера
  };

  # Запрет на трансфер зоны
  allow-transfer {
    none;
  };
};
```

В отчёт вставьте скриншот из изменённого файла.

17. Правим named.conf.default-zones. Также предварительно делаем бэкап. Команды следующие:
sudo cp /etc/bind/named.conf.default-zones /etc/bind/named.conf.default-zones_bak
sudo nano /etc/bind/named.conf.default-zones

Удаляем содержимое и заменяем следующим текстом:

```
# Корневые сервера
# (Необходимы для рекурсивных запросов)
zone "." {
  type hint;
  file "named.root";
};

# localhost zone
zone "localhost" {
  type master;
  file "master/localhost.zone";
};

# 127.0.0. zone.
zone "0.0.127.in-addr.arpa" {
  type master;
  file "master/0.0.127.zone";
};
```

В отчёт вставьте скриншот из изменённого файла.

Практическая работа № 59 «Настройка Samba»

Задание 1:

1. Переходим к конфигурации samba4:

Отключаем systemd-resolved:

Останавливаем сервис: sudo service systemd-resolved stop
Убираем из автозапуска: sudo systemctl disable systemd-resolved.service
Удаляем симлинк /etc/resolv.conf: sudo rm /etc/resolv.conf
Открываем и изменяем конфиг: sudo nano /etc/resolv.conf
Настраиваем адрес сервера имён:
nameserver 10.0.2.1
search domain.local1
Пока nameserver настроен на адрес нашего текущего DNS сервера (10.0.2.1), а имя указано будущего домена – domain.local1.

В отчёт вставьте скриншот с командами на экране.

2. Настраиваем файл /etc/hosts. Открываем файл и вносим изменения sudo nano /etc/hosts:
127.0.0.1 localhost.localdomain localhost
10.0.2.10 dc1.domain.local dc1

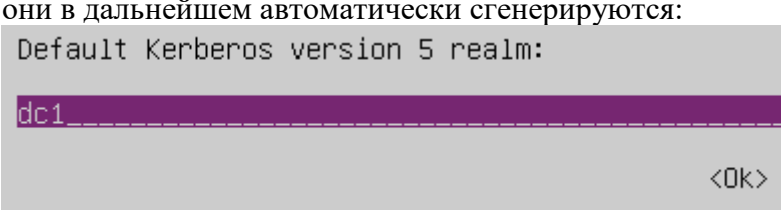
3. Проверяем, что в системе не работают ненужные нам процессы следующей командой:

```
root@dc1:/# ps ax | egrep "samba|smbd|nmbd|winbindd"
   5826 tty1     S+     0:00 grep -E --color=auto samba|smbd|nmbd|winbindd
root@dc1:/#
```

Должен быть результат как на картинке.

4. Приступаем к инсталляции Samba. Используем для установки всех пакетов следующую команду: sudo apt -y install samba krb5-config winbind smbclient krb5-user

5. При запросе о названии вашего сервера/области можно оставить поля пустыми, так как они в дальнейшем автоматически сгенерируются:



6. Ждём окончания установки и строки приветствия после. Далее бэкапим файл с исходными настройками Samba:
sudo mv /etc/samba/smb.conf /etc/samba/smb.conf.bkp

7. Запускаем инициализацию контроллера домена с опцией –interactive:
sudo samba-tool domain provision --use-rfc2307 –interactive
Если в процессе настройки не было допущено ошибок, те параметры которые вам нужно настраивать, кроме DNS backend инсталлятор поместит в квадратные скобки как дефолтные значения.

Realm [ADMINGUIDE.LAN]:
Domain [ADMINGUIDE]:
Server Role (dc, member, standalone) [dc]:
DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) [SAMBA_INTERNAL]: **BIND9_DLZ**

DNS forwarder IP address (write 'none' to disable forwarding) [192.168.1.2]:
Administrator password:
Retype password:

Задайте пароль для контроллера домена. Запиши его в отчёт

В отчёт скриншот с командами на экране.

Задание 2:

Ответить на следующие вопросы:

- ✓ Подробно опишите каждую строчку, которую вы настроили в файле в директории /etc/netplan/
- ✓ Что такое bind? Для чего он нужен?
- ✓ В отчёте объяснить каждую строчку изменения named.conf.options.
- ✓ В отчёте объяснить каждую строчку изменения named.conf.default-zones.

Практическая работа № 60 «Конфигурирование BIND9 на контроллере домена»

Задание 1:

Активируем интеграцию DLZ.

1. Смотрим файл sudo nano /var/lib/samba/bind-dns/named.conf. Здесь необходимо раскомментить информацию для BIND 9.12. Делаем это и помещаем в отчёт скриншот с раскомменченной строкой в файле.

2. Этот же файл нужно заинклудить в основную конфигурацию named. Открываем файл sudo nano /etc/bind/named.conf. Добавляем в конец файла строчку:
include "/var/lib/samba/bind-dns/named.conf";

В отчёт поместить скриншот с новой строчкой в файле named.conf.

3. Проверяем права на dns.keytab, проверяем права на всю папку /bind-dns/ следующими командами:
ls -l /var/lib/samba/private/dns.keytab
ls -l /var/lib/samba/
В отчёт помещаем скриншот с результатами.

4. Смотрим права на /etc/krb5.conf с помощью команды ls -l /etc/krb5.conf
Должно быть: -rw-r--r-- 1 root bind 2891 Apr 3 17:51 /etc/krb5.conf
В случае несоответствия sudo chown root:bind /etc/krb5.conf
Затем снова проверить права на этот файл.
В отчёт скриншот с результатами.

5. Проверяем наличие утилиты nsupdate командой which nsupdate.
Должно быть вот так: /usr/bin/nsupdate

6. Загружаем список корневых днс серверов:
sudo wget -q -O /var/cache/bind/named.root http://www.internic.net/zones/named.root
sudo chown root:bind /var/cache/bind/named.root
sudo chmod 640 /var/cache/bind/named.root

7. Проверяем конфиг:
sudo named-checkconf
sudo service bind9 start
В отчёт скриншоты со всеми командами и результатами.

Если ошибок не будет обнаружено, то named-checkconf не выдаст никакой информации, можно пытаться запустить сервис. Если попытка запуска тоже не выдаст никаких критов прямо в терминал – значит хорошо. DNS сервер почти готов к работе

8. Создаём файлы зон:
sudo mkdir /var/cache/bind/master
sudo chown bind:bind /var/cache/bind/master

Localhost
sudo nano /var/cache/bind/master/localhost.zone

```
$TTL 3D

$ORIGIN localhost.

@       1D      IN      SOA     @       root (
                        2013050101      ; serial
                        8H              ; refresh
                        2H              ; retry
                        4W              ; expiry
                        1D              ; minimum
                        )

@       IN      NS       @
        IN      A        127.0.0.1
```

0.0.127.in-addr.arpa
sudo nano /var/cache/bind/master/0.0.127.zone

```
$TTL 3D

@       IN      SOA     localhost. root.localhost. (
                        2013050101      ; Serial
                        8H              ; Refresh
                        2H              ; Retry
                        4W              ; Expire
                        1D              ; Minimum TTL
                        )

        IN      NS      localhost.

1       IN      PTR     localhost.
```

sudo chown bind:bind /var/cache/bind/master/0.0.127.zone

sudo chmod 640 /var/cache/bind/master/0.0.127.zone

2. Запускаем\перезапускаем bind9, проверяем созданные зоны:
:~$ sudo service bind9 restart

:~$ host -t A localhost 127.0.0.1

```
Using domain server:
Name: 127.0.0.1
Address: 127.0.0.1#53
Aliases:

localhost has address 127.0.0.1
AdminGuide.Ru@ag-dc-1:~$ host -t PTR 127.0.0.1 127.0.0.1
Using domain server:
Name: 127.0.0.1
Address: 127.0.0.1#53
Aliases:

1.0.0.127.in-addr.arpa domain name pointer localhost.
```

Настройка запуска

3. Для корректной работы, все процессы самбы должна запускать сама самба и никто иной. Поэтому выполняем следующие команды для автоматического запуска:
sudo systemctl stop smbd nmbd winbind
sudo systemctl disable smbd nmbd winbind
sudo systemctl mask smbd nmbd winbind

4. Блокируем samba-ad-dc для ручного старта, включаем сервис и включаем его автозапуск:
sudo systemctl unmask samba-ad-dc
sudo systemctl start samba-ad-dc
sudo systemctl enable samba-ad-dc

В отчёт скриншот с командами.

Контроллер домена Ubuntu – Настройка Kerberos

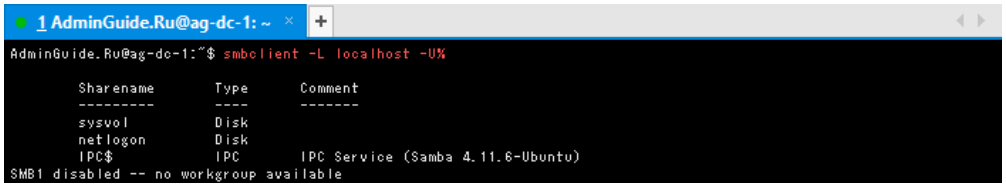
5. При инициализации AD DC, будет создан файл конфигурации керберос, где он расположен, указывается в конце отчета об инициализации. Дабы не делать двойную работу, заменяем существующий файл настроек Kerberos, только что созданным файлом:

sudo cp /var/lib/samba/private/krb5.conf /etc/

6. Убеждаемся что всё работает. Смотрим имеющиеся на контроллере общие каталоги:

smbclient -L localhost -U%

Должно быть:

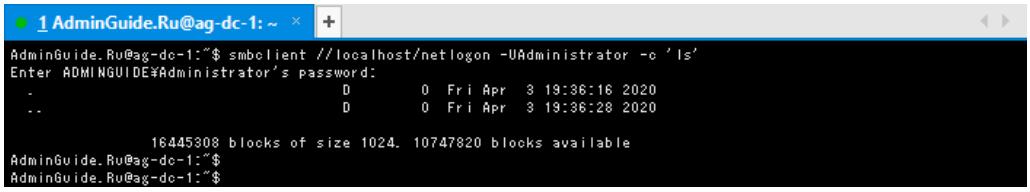


В отчёт вставить скриншот с вашей информацией.

7. Смотрим возможность подключения к netlogon
Теперь сотрим пускает ли доменного админа в каталог netlogon:

smbclient //localhost/netlogon -UAdministrator -c 'ls'

Когда потребуется авторизация, вводим пароль указанный в момент инициализации. Авторизовавшись успешно вы получите доступ к каталогу.
Должно быть:



В отчёт вставить скриншот с вашей информацией.

8. Проверяем правильность настройки DNS. Если bind9 был настроен некорректно, то AD DC не взлетит. Для того чтобы проверить, попытаемся извлечь из днс сервера необходимые записи.
Во-первых смотрим SRV запись _ldap

✓ Во-первых смотрим SRV запись _ldap

$ host -t SRV _ldap._tcp.domain.local.

_ldap._tcp.domain.local has SRV record 0 100 389 dc1.domain.local.

✓ Во-вторых смотрим SRV запись _kerberos

$ host -t SRV _kerberos._udp. domain.local.

_kerberos._udp. domain.local has SRV record 0 100 88 dc1.domain.local.

✓ В-третьих проверяем А запись контроллера домена

$ host -t A dc1.domain.local.

dc1.domain.local has address 10.0.2.10

✓ Проверяем работоспособность Kerberos

$ kinit administrator

Password for administrator@ domain.local:

Warning: Your password will expire in 38 days on Fri May 15 19:36:28 2020

✓ В конечном итоге, смотрим кеш авторизационных тикетов Kerberos

$ klist

Ticket cache: FILE:/tmp/krb5cc_1001

Default principal: administrator@ domain.local

Valid starting Expires Service principal

04/07/20 09:02:16 04/07/20 19:02:16 krbtgt/ domain.local @ domain.local

renew until 04/08/20 09:02:12

В отчёт вставить скриншот со всеми командами и их результатами.

Задание 2:

Ответить на следующие вопросы:

✓ Написать пояснение по термину «заинклудить»

✓ Что означают буквы drwx при проверке прав на файл/папку?

✓ Назначение команд chown и chmod

Практическая работа № 61 «Установка 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 server_public_ip/32
# 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.

Практическая работа № 62 «Настройка Snort»

Задание 1:

1. Для проверки Snort на регистрацию предупреждений добавьте предупреждение:

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

2. Следующую строку в файл:

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

В отчёт вставить скриншот с результатом.

3. 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.

4. 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

5. 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.

6. Прочитать логи можно с помощью команды внизу:

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

В отчёт вставить скриншот с результатом.

7. 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

8. Затем выполните старт snort:
sudo systemctl start snort

9. Увидеть статус можно следующей командой:

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

Задание 2:
Ответьте на следующие вопросы:

- ✓ Из каких частей состоит правило snort?
- ✓ Куда нужно записывать правила для их исполнения в Snort?

Практическая работа № 63 «Запись предупреждений о вторжениях в MySQL»

Задание 1:

Теоретические сведения:
Преобразование бинарных данных в удобочитаемую форму (бинарные-в-ASCII) — задача, отнимающая очень много процессорного времени в любом приложении. Это особенно справедливо для Snort, и поскольку мы хотим выделять на захват и анализ пакетов как можно больше ресурсов нашего компьютера, то значит, нам нужно убрать как можно больше задач, потребляющих большое количество процессорного времени. Для этого и предназначен Barnyard2.

В продакшене мы хотим отправлять данные о событиях из Snort в базу данных. Snort способен использовать любую ODBC базу данных, такую как Oracle, Microsoft SQL Server, PostgreSQL и MySQL. Здесь мы будем использовать MySQL, поскольку это самая распространенная опция для Snort. Если мы сможем отправить предупреждения в базу данных, то мы сможем делать запросы к базе данных другими инструментами так, чтобы иметь возможность анализировать эту информацию. Например, мы можем сделать запрос о том, какими правилами были вызваны предупреждения, какие IP-адреса делали атаки, какой уровень серьезности имели эти вторжения.

Здесь мы сконфигурируем Snort для обработки его предупреждений в двоичной форме — это простейшая и наименее затратная с точки зрения ресурсов процессора форма, а затем используем Barnyard2 для чтения данных этих событий, преобразования в удобочитаемую для человека форму и записи их в базу данных MySQL.

Прежде чем мы начнем, хотелось бы отметить, что Snort будет работать и без Barnyard2, но это замедлит его работу — потенциально Snort не будет обрабатывать и анализировать некоторые пакеты в загруженной среде, что может быть опасно.

1. Установите зависимости для Barnyard:

Сначала нужно установить некоторые библиотеки и приложения, от которых зависит Barnyard2.

ubuntu> sudo apt-get install -y mysql-server libmysqlclient-dev mysql-client autoconf libtool

```
    @ubuntu:~$ sudo apt-get install -y mysql-server libmysqlclient-dev mysql-cl
ient autoconf libtool
```

ubuntu> sudo apt-get install libpcap-dev libmysql-dev libprelude-dev

```
@ubuntu:/$ sudo apt-get install libpcap-dev libmysql-dev libprelude-dev
```

2. Установите Git:

Мы скачаем и установим последнюю версию Barnyard2 с GitHub. Если у вас еще нет git в вашей системе, то вам нужно будет установить его сейчас.

ubuntu> sudo apt-get update

ubuntu> sudo apt-get install git

В отчёт вставьте скриншот с результатом установки.

3. Редактирование конфигурационного файла Snort:

Чтобы направлять наши предупреждения в базу данных, нам нужно отредактировать файл snort.conf. Откройте его с помощью любого текстового редактора и перейдите в раздел вывода (раздел #6). Там мы скажем Snort использовать нашу базу данных MySQL (которую мы создадим позже в этой статье с указанием имени пользователя и пароля, которые вы выберете).

В этом примере мы выбрали простые названия для имени базы данных, пользователя и пароля — все snort.

```
##################################################
# Step #6: Configure output plugins
# For more information, see Snort Manual, Configuring Snort - Output
Modules
##################################################

# unified2
# Recommended for most installs
# output unified2: filename merged.log, limit 128, nostamp,
mpls_event_types, vlan_event_types

# Additional configuration for specific types of installs
# output alert_unified2: filename snort.alert, limit 128, nostamp
# output log_unified2: filename snort.log, limit 128, nostamp

output database log,mysql, user=snort password=snort dbname=snort
host=localhost
```

4. Скачайте Barnyard2:

Barnyard2 — это диспетчер очереди печати, который уменьшает потребление ресурсов демоном Snort. Он позволяет Snort записывать все предупреждения в более эффективном бинарном виде, а затем Barnyard2 берет эти бинарные файлы и преобразует их в удобную для человека форму. Наконец, он записывает их в базу данных MySQL для последующего анализа.

ubuntu> git clone git://github.com/firnsy/barnyard2.git

```
@ubuntu:~$ git clone git://github.com/firnsy/barnyard2.git
Cloning into 'barnyard2'...
remote: Counting objects: 1246, done.
remote: Total 1246 (delta 0), reused 0 (delta 0), pack-reused 1246
Receiving objects: 100% (1246/1246), 1.16 MiB | 642.00 KiB/s, done.
Resolving deltas: 100% (835/835), done.
Checking connectivity... done.
keith@ubuntu:~$
```

Теперь проверим, скачался и установился ли он, выполнив следующую команду в этом каталоге

ubuntu> ls -l

```
drwxrwxr-x 10          4096 Apr 12 13:23 barnyard2
drwxr-xr-x 17          4096 Mar  2 15:45 Desktop
drwxr-xr-x  2          4096 Jan  5 10:16 Documents
drwxr-xr-x  6          4096 Feb 24 14:48 Downloads
-rw-r--r--  1          8980 Jan  5 09:55 examples.desktop
drwxr-xr-x  2          4096 Jan  5 10:16 Music
drwxr-xr-x  2          4096 Jan  5 10:16 Pictures
drwxr-xr-x  2          4096 Jan  5 10:16 Public
drwxr-xr-x  2          4096 Jan  5 10:16 Templates
drwxr-xr-x  2          4096 Jan  5 10:16 Videos
```

В отчёт вставьте скриншот с командами.

Как вы можете видеть, он создал каталог с именем barnyard2. Перейдем в него и посмотрим на его содержимое.

ubuntu> cd barnyard2

ubuntu> ls -l

Обратите внимание на первый файл с именем autogen.sh. Выполним этот скрипт

ubuntu> ./autogen.sh

В отчёт вставьте скриншот с командами.

Затем введите в консоли следующую строку

ubuntu> CFLAGS = '-lpthread'

Затем запустите соответствующую команду configure для вашей системы.

Если вы используете 64-битную архитектуру, то команда configure будет выглядеть следующим образом:

ubuntu> ./configure --with-mysql-libraries=/usr/lib/x86_64-linux-gnu --prefix=$HOME/barnyard2-install

Если вы используете 32-битную архитектуру, то команда configure немного изменится на такую:

ubuntu > ./configure --with-mysql-libraries=/usr/lib/i386-linux-gnu --prefix=$HOME/barnyard2-install

Есть еще одна библиотека, которая нужна Ubuntu для запуска Barnyard2, она называется libdumbnet-dev. Давайте возьмем ее из репозиториев.

sudo apt-get install libdumbnet-dev

Поскольку скрипт make для Barnyard2 ожидает, что у нас есть файл зависимости с именем dnet.h, нам нужно создать символическую ссылку на dumbnet.h, которую мы назовем dnet.h (с момента написания скрипта имена файлов были изменены).

ubuntu> ln -s /usr/include/dumbnet.h /usr/include/dnet.h

Затем обновите библиотеки.

ubuntu> sudo ldconfig

Теперь мы можем выполнить команду make для Barnyard2.

ubuntu> make

```
keith@ubuntu:/snort_source/barnyard2$ make
make  all-recursive
make[1]: Entering directory `/snort_source/barnyard2'
Making all in src
make[2]: Entering directory `/snort_source/barnyard2/src'
Making all in sfutil
make[3]: Entering directory `/snort_source/barnyard2/src/sfutil'
make[3]: Nothing to be done for `all'.
make[3]: Leaving directory `/snort_source/barnyard2/src/sfutil'
Making all in output-plugins
```

Наконец, нам нужно выполнить команды make и install.

ubuntu> sudo make install

В отчёт вставьте скриншот с командами.

5. Конфигурирование Barnyard2:

Нам нужно сделать базовую конфигурацию Barnyard2, чтобы убедиться, что он работает правильно. Сначала скопируем файл конфигурации Barnyard2 в директорию /etc/snort

ubuntu > sudo cp /snort_source /etc/barnyard2.conf /etc/snort

Теперь создадим файл, который будет нужен Barnyard2 в каталоге /var/log. Это файл закладок

ubuntu > touch /var/log/snort/barnyard2.waldo

```
@ubuntu:/etc$ sudo cp /snort_source/barnyard2/etc/barnyard2.conf /etc/snort
@ubuntu:/etc$ touch /var/log/snort/barnyard2.waldo
```

В отчёт вставьте скриншот с командами.

6. Установка MySQL:

Теперь, когда Barnyard2 установлен, скомпилирован и настроен, нужно установить MySQL, куда будут записываться все предупреждения. Для этого нам необходимо:

- ✓ создать базу данных
- ✓ создать схему базы данных для предупреждений
- ✓ создать пользователя
- ✓ предоставить пользователю соответствующие права

Начнем с входа в систему базы данных MySQL

ubuntu> sudo mysql -u root -p

При запросе пароля введите snort.

```
@ubuntu:~$ sudo mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 48
Server version: 5.5.47-0ubuntu0.14.04.1 (Ubuntu)

Copyright (c) 2000, 2015, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

Вы находитесь в системе MySQL и должны видеть приглашение командной строки MySQL. Создадим базу данных для использования системы Snort.

mysql > create database snort;

(Обратите внимание, что snort здесь просто имя базы данных, в которой мы будем хранить полученные предупреждения. Ее можно назвать как угодно, но давайте назовем ее так, чтобы было просто запомнить).

Теперь скажем системе, что хотим использовать эту базу данных.

mysql > use snort;

В отчёт вставьте скриншот с командами.

Barnyard2 поставляется вместе со скриптом для создания схемы базы данных для Snort. Он находится в /snort_source/barnyard2/schemas/create_mysql. Мы можем запустить этот скрипт, набрав:

mysql > /snort_source/barnyard2/schemas/create_mysql

Затем нам нужно создать в MySQL пользователя базы данных snort.

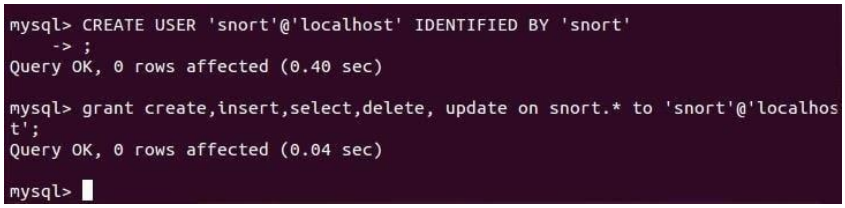
mysql > CREATE USER 'snort'@'localhost' IDENTIFIED BY 'snort';

Эта команда создает пользователя snort на сервере localhost, который использует пароль snort. Имя пользователя и пароль могут отличаться, но они должны соответствовать тому, что вы ввели в файле snort.conf на шаге 3 (выше).

Теперь, нужно предоставить этому пользователю необходимые права

mysql > grant create, insert, select, delete, update on snort.* to 'snort'@'localhost';

Это дает пользователю snort права на создание (create) объектов, вставку (insert) данных, выбор (select) данных, удаление (delete) данных и обновление (update) данных в базе данных snort на локальном сервере (localhost).



В отчёт вставьте скриншот с командами.

Практическая работа № 64 «Настройка веб-интерфейса для системы обнаружения и предотвращения вторжения Snort»

Задание 1:

1. Обновим список пакетов и обновим установленные пакеты:
sudo apt update
sudo apt upgrade –y
В отчёт вставьте скриншот об успешном обновлении.

В отчёт вставьте скриншот с командами.

2. Import the GPG key and add the PPA repository:
sudo apt -y install lsb-release apt-transport-https ca-certificates
sudo wget -O /etc/apt/trusted.gpg.d/php.gpg https://packages.sury.org/php/apt.gpg

3. Then add repository
echo "deb https://packages.sury.org/php/ buster main" | sudo tee /etc/apt/sources.list.d/php.list

4. Проверьте версию php:
php –v
В отчёт вставьте скриншот с версией php

В отчёт вставьте скриншот с командами.

Практическая работа № 65 «Настройка веб-интерфейса для системы обнаружения и предотвращения вторжения Snort»

Задание:

1. Установить пакет:
sudo apt-get install -y php-pear
Затем:
sudo pear install -f --alldeps Image_Graph
Для установки других расширений php:
sudo apt-get install php7.4-{cli,json,imap,bcmath,bz2,intl,gd,mbstring,mysql,zip}
В отчёт вставить скриншот с успешной установкой.

2. Загружаем библиотеку ADODB:
wget https://sourceforge.net/projects/adodb/files/adodb-php5-only/adodb-520-for-php5/adodb-5.20.8.tar.gz
tar -xvzf adodb-5.20.8.tar.gz
sudo mv adodb5 /var/adodb
sudo chmod -R 755 /var/adodb

3. Загружаем BASE:
wget http://sourceforge.net/projects/secureideas/files/BASE/base-1.4.5/base-1.4.5.tar.gz
tar xzvf base-1.4.5.tar.gz
sudo mv base-1.4.5 /var/www/html/base/
В отчёт вставьте скриншот с командами.

В отчёт вставьте скриншот с командами.

4. Копируем конфигурационный файл:
cd /var/www/html/base
sudo cp base_conf.php.dist base_conf.php

5. И приводим некоторые строки в файле /var/www/html/base/base_conf.php к образцам:
$BASE_urlpath = '/base';
$DBlib_path = '/var/adodb/';
$alert_dbname = 'snort';
$alert_host = 'localhost';

$alert_port   = '';
$alert_user   = 'snort';
$alert_password = 'snortpass';

6. необходимо изменить права, чтобы никто не увидел пароль в файле:
sudo chown -R www-data:www-data /var/www/html/base
sudo chown -R www-data:www-data /var/www/html/base

7. Перезапуск apache2:
/etc/init.d/apache2 restart
В отчёт вставьте скриншот.

8. Запустите браузер. Вставьте в него:
http://localhost/base/base_main.php

В отчёт вставьте скриншот с входом в веб-интерфейс.

Практическая работа № 66 «Создание собственных правил для Snort. Синтаксис правил»

Теоретические сведения:

Snort использует правила, написанные простым, но в то же время гибким и достаточно мощным языком. Большинство правил пишутся в одну строку, хотя могут занимать и несколько строк, в этом случае каждая строка, кроме последней, должна заканчиваться символом “" (без кавычек). В более сложных случаях можно также вызывать другие программы, используя инструкцию включения. Правила для Snort делятся на два вида:

• Бесконтекстные (обычные) - применяются для каждого пакета отдельно, без связи с другими пакетами

• Контекстные (правила препроцессоров) - применяться к той или иной совокупности (последовательности) пакетов.

Заголовок							Опции			
Действие	Протокол	IP-адреса отправителей	Порты отправителей	Оператор направления	IP-адреса получателей	Порты получателей	[Мета данные]	[Данные в полезной нагрузке]	[Данные в заголовке]	[Действие после обнаружения]

Правила Snort состоят из заголовка (Rule Header) и опций (Rule Options). Заголовок содержит описание действия, протокол передачи данных, IP-адреса, сетевые маски и порты источника и назначения. После заголовка правила следует необязательная часть правила - его опции, они включают определение дополнительных критериев выполнения правила и определение дополнительных реагирующих действий. Они используются для организации более жесткой и направленной фильтрации траффика. Весь набор опций заключается в круглые скобки, сами опции отделяются друг от друг с помощью точки с запятой “;” (последняя опция в списке тоже должна заканчиваться этим символом). Ключевые слова (keywords) опций отделяются от своих аргументов (values) двоеточием “:”. Структура правил Snort в общем случае выглядит следующим образом:

Синтаксис записи правил Snort:

<Действие> <Протокол> <IP-адреса отправителей> <Порты отправителей> <Оператор направления> <IP-адреса получателей> <Порты получателей> (ключ_1 : значение_1; ключ_2 : значение_2; ... ключ_N : значение_N;)

Заголовок правила

Допустимые параметры для каждого поля заголовка правил Snort:

Действия правила

Действие	Описание
alert	генерирует предупреждение, используя указанное предупреждение, и передаёт информацию системе журналирования
log	просто протоколирует пакеты без предупреждений
pass	игнорирует пакеты
activate	генерирует предупреждение, затем включает указанное динамическое правило
dynamic	остаётся пассивным, пока не активируется динамическим правилом, затем действует как log

В режиме inline к предыдущим действиям добавляются дополнительные действия:

Действие	Описание
drop	блокирует (отбрасывает) пакет и передаёт информацию системе журналирования
sdrop	блокирует (отбрасывает) пакет и не использует систему журналирования
reject	блокирует (отбрасывает) пакет, передаёт информацию системе журналирования, а затем посылает сегмент сброса TCP (TCP RST), если протокол TCP, или сообщение ICMP-порт недоступен, если протокол UDP

Также можно создать свои собственные типы правил и связать один или несколько выходных модулей с ними. Можно затем использовать созданные типы правил в качестве действий в правилах Snort. В примере ниже создаётся тип правила, который будет регистрировать только tcpdump:

```
ruletype suspicious
{
   type log
   output log_tcpdump: suspicious.log
}
```

А в этом примере создаётся тип правила, регистрирующей и tcpdump, и syslog:

```
ruletype redalert
{
   type alert
   output alert_syslog: LOG_AUTH LOG_ALERT
```

```
    output log_tcpdump: suspicious.log
}
```

Протоколы

Обозначает протокол передачи данных. На данный момент Snort умеет анализировать на предмет подозрительного содержания/поведения 4 типа протоколов: TCP, UDP, ICMP, IP, соответственно, возможны 4 значения: tcp, udp, icmp или ip, что означает любой IP-протокол. В будущем, возможно, этот список пополнят и другие протоколы, к примеру, ARP, IGRP, GRE, OSPF, RIP, IPX и другие.

IP-адресация

Поскольку Snort не имеет встроенного механизма получения IP адреса, используя доменное имя, то нужно указывать конкретный IP адрес или же диапазон IP адресов. В этом параметре можно использовать маски. Адреса задаются в формате: IP/mask, где IP – IP-адрес сети или узла, mask – маска сети, которая задаётся как десятичное число, которое равняется числу единиц в двоичной маске. Например, для сетей класса C /24 (число 24 эквивалентное шестнадцатеричной маске FF.FF.FF.0), для сетей класса B - /16, также можно использовать маску /32 и другие. Здесь может применяться и отрицание (инвертирование), обозначаемое символом “!” (Например: !127.0.0.1). Если вместо IP адреса указать ключевое слово any, то это будет подразумевать абсолютно все хосты. Для указания списка можно использовать перечисление IP адресов через “,” содержащихся в квадратных скобках. (Например: [212.116.1.1,10.10.1.0/24]). В качестве IP-адреса можно использовать переменные HOME_NET, EXTERNAL_NET и другие.

Порты

После IP адреса указывается номер порта, с которого отсылаются данные и на который приходят. Можно указать диапазон портов: 1:1024 (все порты в диапазоне от 1 до 1024 включая 1 и 1024). Часто используется оператор отрицания “!” (Например: !123:321 исключает все порты в диапазоне от 123 до 321). Если опущен один из параметров диапазона, например “:321” или “123:”, то пропускаемый параметр принимает крайнее значение общего количества портов, то есть 0 или 65535.

Операторы направления

Оператор направления служит для обозначения направления траффика, для которого применяется правило, и обозначается “->” (знаком минуса и закрывающей угловой скобкой). IP-адрес и номер порта слева от оператора определяют источник траффика, а справа от него - назначение. Существует также оператор так называемой “двунаправленности” и обозначается “<>” (двумя угловыми скобками). Этот оператор говорит Snort рассматривать указанные пары адресов и портов в обе стороны, вне зависимости от того, кто является источником, а кто – получателем. Это удобно в тех случаях, когда нужно сохранить траффик от обеих сторон, например, в Telnet или POP3 сессиях. Важно отметить, что оператор “<-“ не существует.

Опции правила

Все опции можно разделить на четыре большие категории:

- general (meta-data) - данные опции предоставляют информацию о правиле, но никак не влияют на обнаружение;
- payload - данные опции позволяют искать информацию внутри полезной нагрузки (данных пользователя) пакетов и могут быть взаимосвязаны;
- non-payload - данные опции позволяют искать информацию внутри служебной (управляющей) информации о пакете (заголовке);
- post-detection - данные опции являются определёнными триггерами, указывающими задачи, которые необходимо осуществить после срабатывание правила.

General (meta-data)

Задание:
Создать следующие правила, показанные в примерах:

1. gid

Ключевое слово gid (generator id) используется для идентификации того, какая часть Snort генерирует событие, когда срабатывает конкретное правило. Например, gid равный 1 ассоциируется с подсистемой правил, а различные gid свыше 100 предназначены для определённых препроцессоров и декодеров. Опция gid является необязательной, и если она не определена в правиле, то по умолчанию она устанавливается равной 1, и правило будет являться частью общей подсистемы правил. Чтобы избежать потенциальных конфликтов с gid, определёнными в Snort, рекомендуется использовать значения начиная с 1000000. Для общих правил не рекомендуется использовать ключевое слово gid. Данная опция должна быть использована с опцией sid. Файл “etc/gen-msg.map” содержит больше информации о gid препроцессоров и декодеров.

Синтаксис: gid:<generator id>;

Примеры:

alert tcp any any -> any 80 (content:"BOB"; gid:1000001; sid:1; rev:1;)

Вставть в отчёт скриншот с созданным правилом.

2. sid

Ключевое слово sid (Snort id или иногда упоминается как signature id) используется для уникальной идентификации правил Snort. По значению его аргумента можно легко идентифицировать правило. Данное ключевое слово должно использоваться вместе с ключевым словом rev. Файл “sid-msg.map” содержит соответствие предупреждающих сообщений и идентификаторов правил Snort. Значения аргумента:

< 100 зарезервировано разработчиками 100 - 999.999 использованы в правилах, уже включенных в дистрибутив Snort

= 1.000.000 можно использовать для собственных правил

Синтаксис: sid:<snort rules id>;

Примеры:

alert tcp any any -> any 80 (content:"BOB"; sid:1000983; rev:1;)

Вставть в отчёт скриншот с созданным правилом.

3. rev

Указывает значение версии правила. С помощью REV интерпретатор правил Snort определяет версию написанного правила. Этот параметр используется в паре с SID.

Синтаксис: rev:<revision integer>;

Примеры:

alert tcp any any -> any 80 (content:"BOB"; sid:1000983; rev:1;)

Вставть в отчёт скриншот с созданным правилом.

4. classtype

Используется для присвоения категории атаки, к которой необходимо отнести правило, являющееся частью более общего класса атак. Snort предоставляет набор классов, которые используются предоставляемыми правилами по умолчанию. Классификация атак позволяет лучше организовать события, производимые Snort. Классификация атак представлена в файле “classification.conf”. В файле используется следующий синтаксис для каждой записи:

config classification: <имя класса>,<описание класса>,<приоритет по умолчанию>

Приоритет 1 (high) является наиболее высоким, а 4 (very low) - самым низким. Также классификация типов атак представлена в таблице:

Тип класса	Описание	Приоритет
attempted-admin	Попытка получения прав администратора	high
attempted-user	Попытка получения прав пользователя	high
inappropriate-content	Обнаружено неприемлемое (несоответствующее) содержание	high
policy-violation	Потенциальное нарушение корпоративной конфиденциальности	high
shellcode-detect	Обнаружен исполняемый код	high
successful-admin	Успешное получение прав администратора (повышение привилегий)	high
successful-user	Успешное получение прав пользователя (повышение привилегий)	high
trojan-activity	Обнаружена активность сетевой троянской программы	high
unsuccessful-user	Неудачная попытка получения прав пользователя	high
web-application-attack	Атака на Web-приложение	high
attempted-dos	Предпринята попытка атаки отказ в обслуживании (DoS)	medium
attempted-recon	Попытка утечки информации (разведка)	medium
bad-unknown	Потенциально нежелательный траффик	medium
default-login-attempt	Попытка входа с помощью стандартного логина/пароля	medium
denial-of-service	Обнаружена атака отказ в обслуживании (DoS)	medium
misc-attack	Прочие атаки	medium
non-standard-protocol	Обнаружено использование нестандартного протокола или нестандартное событие	medium
rpc-portmap-decode	Decode of an RPC Query (Декодирован удалённый вызов процедуры (RPC)) (Обнаружен запрос RPC)	medium
successful-dos	Успешная DOS-атака	medium
successful-recon-largescale	Крупномасштабная утечка информации	medium
successful-recon-limited	Утечка информации	medium
suspicious-filename-detect	Обнаружено подозрительное имя файла	medium
suspicious-login	Обнаружена попытка входа с подозрительным логином	medium
system-call-detect	Обнаружено обращение к ядру системы (system call) (Обнаружен системный вызов)	medium
unusual-client-port-	Клиент использует нестандартный порт	medium

Тип класса	Описание	Приоритет
connection		
web-application-activity	Доступ к потенциально уязвимому Web-приложению	medium
icmp-event	Общее событие ICMP	low
misc-activity	Прочая активность	low
network-scan	Обнаружена попытка сканирования сети	low
not-suspicious	Не являющийся подозрительным траффик	low
protocol-command-decode	Generic Protocol Command Decode (Обнаружена попытка шифрования) (Обнаружена обычная команда протокола)	low
string-detect	Обнаружена подозрительная строка	low
unknown	Неизвестный траффик	low
tcp-connection	Обнаружено TCP соединение	very low

Синтаксис: classtype:<class name>;

Примеры:

alert tcp any any -> any 25 (msg:"SMTP expn root"; flags:A+; content:"expn root"; nocase; classtype:attempted-recon;)

Предупреждения:

Опция classtype может иметь только те значения для классификации, которые определены в snort.conf с помощью config classification. Snort предоставляет стандартный набор классификации в файле classification.config, который используется в поставляемых наборах правил.

Вставть в отчёт скриншот с созданным правилом.

5. priority

Задаёт правилам уровень важности. Возможно использовать параметр priority вместе с classtype, при этом изменится уровень приоритета параметра classtype.

Синтаксис: priority:<priority integer>;

Примеры:

alert tcp any any -> any 80 (msg:"WEB-MISC phf attempt"; flags:A+; content:"/cgi-bin/phf"; priority:10;)

alert tcp any any -> any 80 (msg:"EXPLOIT ntpdx overflow"; dsize:>128; classtype:attempted-admin; priority:10;)

Вставть в отчёт скриншот с созданным правилом.

6. metadata

Позволяет автору правил включать дополнительную информацию о правиле, как правило, в формате “ключ-значение”. Ключи и значения тега metadata перечислены в таблице ниже:

Ключ	Описание	Формат значения
engine	Указывает правило библиотеки общего пользования (Indicate a Shared Library Rule)	"shared"

Ключ	Описание	Формат значения
soid	GID и SID правила библиотеки общего пользования (Shared Library Rule Generator and SID)	sid
service	Идентификатор сервиса на основе цели (Target-Based Service Identifier)	"http"

Отличные от указанных в таблице ключи Snort фактически игнорирует, поэтому они могут быть записаны в свободной форме в формате “ключ-значение”. Несколько ключей подряд разделяются запятыми, а ключи и значения отделяются между собой пробелом.

Синтаксис:

metadata:key1 value1;

metadata:key1 value1, key2 value2;

Примеры:

alert tcp any any -> any 80 (msg:"Shared Library Rule Example"; metadata:engine shared; metadata:soid 3|12345;)

alert tcp any any -> any 80 (msg:"Shared Library Rule Example"; metadata:engine shared, soid 3|12345;)

alert tcp any any -> any 80 (msg:"HTTP Service Rule Example"; metadata:service http;)

Вставть в отчёт скриншот с созданным правилом.

7. content

Позволяет устанавливать условие в правила, которые ищут определённое содержание (контент) в полезной нагрузке пакетов. Условия могут содержать как двоичные данные, так и текстовые. Двоичные данные должны быть заключены между вертикальными чертами “|” в виде байт-кода. Байт-код представляет двоичные данные в виде шестнадцатеричных чисел. В одном правиле может быть указано несколько content-условий. “!” - модификатор отрицания. Если правилу предшествует модификатор отрицания, то правило срабатывает на пакетах, которые не содержат заданный контент.

Ключевое слово content имеет ряд модификаторов, которые изменяют поведение ранее указанного content. Список модификаторов:

nocase
rawbytes
depth
offset
distance
within
http_client_body
http_client_body
http_cookie
http_raw_cookie
http_header
http_raw_header
http_method
http_uri
http_raw_uri
http_stat_code
http_stat_msg
fast_pattern

Синтаксис: content:[!]"<content string>";

Примеры:

alert tcp any any -> any 139 (content:"|5c 00|P|00|I|00|P|00|E|00 5c|";)

alert tcp any any -> any 80 (content:!"GET";)

Предупреждения:

Необходимо экранировать следующие символы:

; \ "

Вставть в отчёт скриншот с созданным правилом.

8. protected_content

Имеет схожую функциональность с content, однако работает несклько иным образом. Основное преимущество ключевого слова protected_content над content в том, что оно позволяет скрыть целевой контент, раскрывая только хэш-сумму (дайджест) указанного контента. Как и в случае content, основная цель - сопоставить строки определённых байтов. Поиск осуществляется путём хэширования частей входящих сообщений и сравнения полученных результатов с предоставляемой в условии хэш-суммой. Из-за чего проделывается очень большой объём вычислений.

На данный момент с ключевым словом protected_content возможно использование алгоритмов хэширования MD5, SHA256, и SHA512. Алгоритм хэширования должен быть указан в правиле с использованием ключевого слова hash, если он не задан по умолчанию в конфигурации Snort. Кроме того, вместе с protected_content обязательно должен быть указан модификатор length, чтобы указать длину исходных данных.

Как и в случае content, в правиле возможно использование нескольких условий protected_content. В правиле допускается совместное использование content и protected_content. Также в protected_content можно использовать модификатор отрицания “!”.

Ключевое слово protected_content имеет те же модификаторы, что и content, за исключением следующих:

nocase

fast_pattern

depth

within

Синтаксис: protected_content:[!]"<content hash>", length:orig_len[, hash:md5|sha256|sha512];

Примеры:

Следующие правила срабатывают на строке “HTTP”.

alert tcp any any <> any 80 (msg:"MD5 Alert";

protected_content:"293C9EA246FF9985DC6F62A650F78986"; hash:md5; offset:0; length:4;)

alert tcp any any <> any 80 (msg:"SHA256 Alert";

protected_content:"56D6F32151AD8474F40D7B939C2161EE2BBF10023F4AF1DBB3E13260EBDC6342";

hash:sha256; offset:0; length:4;)

Вставть в отчёт скриншот с созданным правилом.

9. nocase

Является модификатором для располагающегося до него ключевого слова content, указывая ему сравнивать содержание без учета регистра символов.

Синтаксис: nocase;

Примеры:

```
alert tcp any any -> any 21 (msg:"FTP ROOT"; content:"USER root"; nocase;)
```

Вставть в отчёт скриншот с созданным правилом.

10. rawbytes

Ключевое слово rawbytes является модификатором для располагающегося до него ключевого слова content, позволяя работать с необработанными данными пакета, игнорируя любое декодирование, произведённое с помощью препроцессоров.

HTTP Inspect имеет набор ключевых слов http_raw_cookie, http_raw_header, http_raw_uri и др. для работы с необработанными данными, которые сопоставляют определённые части HTTP запросов и ответов. С данными ключевыми словами использовать rawbytes не нужно, так как эти условия по умолчанию работают с необработанными данными.

Большинство других препроцессоров по умолчанию используют декодированные/нормализованные данные для сопоставления с образцом. Поэтому для сопоставления с произвольными необработанными данными из пакета необходимо указывать ключевое слово rawbytes.

Синтаксис: rawbytes;

Примеры:

```
alert tcp any any -> any 21 (msg:"Telnet NOP"; content:"|FF F1|"; rawbytes;)
```

Вставть в отчёт скриншот с созданным правилом.

11. http_client_body

Ключевое слово http_client_body ограничивает поиск по телу запроса HTTP-клиента. Ключевое слово http_client_body является модификатором для располагающегося до него ключевого слова content. Размер области данных, по которым производится поиск, зависит от опции post_depth в HttpInspect. Паттерн с данным ключевым словом не будет работать, если post_depth в установлена “-1”.

Синтаксис: http_client_body;

Примеры:

```
alert tcp any any -> any 80 (content:"ABC"; content:"EFG"; http_client_body;)
```

Вставть в отчёт скриншот с созданным правилом.

12. http_header

Ключевое слово http_header ограничивает поиск по извлечённым полям заголовка запроса HTTP-клиента или ответа HTTP-сервера (определяется в конфигурации HttpInspect). Ключевое слово http_method является модификатором для располагающегося до него ключевого слова content. Извлечённые поля заголовка можно нормализовать, определив это в конфигурации HttpInspect.

Синтаксис: http_header;

Примеры:

```
alert tcp any any -> any 80 (content:"ABC"; content:"EFG"; http_header;)
```

Вставть в отчёт скриншот с созданным правилом.

13. http_method

Ключевое слово http_method ограничивает поиск по извлечённому методу из запроса HTTP-клиента. Ключевое слово http_method является модификатором для располагающегося до него ключевого слова content.

Синтаксис: http_method;

Примеры:

alert tcp any any -> any 80 (content:"ABC"; content:"GET"; http_method;)

Вставть в отчёт скриншот с созданным правилом.

14. http_uri

Ключевое слово http_uri ограничивает поиск по нормализованному полю URI запроса. Ключевое слово http_uri является модификатором для располагающегося до него ключевого слова content. Использование опции http_uri после content эквивалентно опции uricontent.

Синтаксис: http_uri;

Примеры:

alert tcp any any -> any 80 (content:"ABC"; content:"EFG"; http_uri;)

Вставть в отчёт скриншот с созданным правилом.

15. http_raw_uri

Ключевое слово http_raw_uri ограничивает поиск по ненормализованному полю URI запроса. Ключевое слово http_raw_uri является модификатором для располагающегося до него ключевого слова content.

Синтаксис: http_raw_uri;

Примеры:

alert tcp any any -> any 80 (content:"ABC"; content:"EFG"; http_raw_uri;)

Вставть в отчёт скриншот с созданным правилом.

16. http_stat_code

Ключевое слово http_stat_code ограничивает поиск по извлечённому полю пояснения к статус коду ответа HTTP-сервера. Ключевое слово http_stat_code является модификатором для располагающегося до него ключевого слова content. Поле пояснения к статус коду будет извлечено, если только задана опция extended_response_inspection в HttpInspect.

Синтаксис: http_stat_code;

Примеры:

alert tcp any any -> any 80 (content:"ABC"; content:"200"; http_stat_code;)

http_stat_msg

Вставть в отчёт скриншот с созданным правилом.

Практическая работа № 67 «Проверка настроенных правил в IDS Snort с помощью сканирования портов»

Задание:

1. Запустить любую виртуальную машину, находящуюся в одной сети с виртуальной машиной с IDS Snort.

2. С помощью команды nmap выполнить сканирование портов на машине с IDS Snort.

В отчёт вставить скриншот с результатом сканирования.

3. Далее запустить syn-пакеты для вирт.машину с помощью команды hping –S –p 80 ваш ip-адрес

В отчёт вставить скриншот с результатом сканирования.

4. С помощью команды tcpreplay –v –I eth0 –l 0 запустить на вашу машину с IDS пакеты *.pcap (с помощью интернета выяснить как работает данная команда и скачать несколько пикап-пакетов для этой команды).

В отчёт вставить скриншот с результатом сканирования.