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

ПРИНЯТО

на заседании педагогического совета

Протокол № 2

«26» декабря 2023 г.

УТВЕРЖДАЮ

Директор СПб ГБПОУ «АУГСГиП»

_____ А.М. Кривоносов

«26» декабря 2023 г.

КОМПЛЕКТ КОНТРОЛЬНО-ОЦЕНОЧНЫХ СРЕДСТВ

по текущему контролю успеваемости
и промежуточной аттестации
по профессиональному модулю
ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ

по специальности
10.02.05 Обеспечение информационной безопасности автоматизированных систем

Квалификация
Техник по защите информации

Форма обучения
очная

Санкт-Петербург
2023 год

Комплект контрольно-оценочных средств по профессиональному модулю ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами разработан на основе Федерального государственного образовательного стандарта по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Минобрнауки России от 09.12.2016 № 1553.

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

Комплект контрольно-оценочных средств по профессиональному модулю рассмотрен на заседании методического совета СПб ГБПОУ «АУГСГиП»

Протокол № 2 от «29» ноября 2023 г.

Комплект контрольно-оценочных средств по профессиональному модулю рассмотрен на заседании цикловой комиссии общетехнических дисциплин и компьютерных технологий

Протокол № 4 от «21» ноября 2023 г.

Председатель цикловой комиссии: Караченцева М.С. _____

СОДЕРЖАНИЕ

1. ПАСПОРТ КОМПЛЕКТА ОЦЕНОЧНЫХ СРЕДСТВ

Результатом освоения профессионального модуля является готовность обучающегося к выполнению вида профессиональной деятельности по участию в планировании и организации работ по обеспечению защиты объекта и составляющих его профессиональных компетенций, а также общих компетенций, формирующихся в процессе освоения ППССЗ в целом.

Комплект контрольно-оценочных средств позволяет оценивать:

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

Код	Наименование результата обучения
ПК 2.2.	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
ПК 2.3.	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.
ПК 2.4.	Осуществлять обработку, хранение и передачу информации ограниченного доступа.
ПК 2.5.	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.
ПК 2.6	Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.
ПК 2.7.	*Администрирование компонентов ИТ-инфраструктуры*
ПК 2.8	*Обеспечение мер по информационной безопасности сетевой инфраструктуры и ее компонентов*
ПК 2.9.	*Проведение анализа компонентов ИТ-инфраструктуры на наличие уязвимостей*
ПК 2.10.	*Проведение мониторинга и анализа инцидентов информационной безопасности*
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях

ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности
ОК 9.	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

2. Приобретение в ходе освоения профессионального модуля практического опыта:

Освоение практического опыта

Иметь практический опыт	**Виды работ на учебной и/ или производственной практике и требования к их выполнению**
установки, настройки программных средств защиты информации в автоматизированной системе; обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации; решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации;	Установка программных средств защиты информации в автоматизированной системе Настройка программных средств защиты информации в автоматизированной системе Применение средств защиты от НСД для информации ограниченного доступа Установка программно-аппаратных средств защиты информации в автоматизированной системе Настройка программно-аппаратных средств защиты информации в автоматизированной системе Установка и настройка средств антивирусной защиты информации
применения электронной подписи, симметричных и асимметричных криптографических алгоритмов, и средств шифрования данных; учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности; работы с подсистемами регистрации собы-	Использование криптографических алгоритмов для шифрования информации, для которой установлен режим конфиденциальности; Использование программных средств для регистрации событий; выявления событий и инцидентов безопасности в автоматизированной системе Анализ журналов безопасности для регистрации событий; выявления событий и инцидентов безопасности в автоматизированной системе

Иметь практический опыт	Виды работ на учебной и/ или производственной практике и требования к их выполнению
тий; выявления событий и инцидентов безопасности в автоматизированной системе.	

3. Освоение умений и усвоение знаний:

№	Освоенные умения, усвоенные знания
З1	особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;
З2	методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;
З3	типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;
З4	основные понятия криптографии и типовых криптографических методов и средств защиты информации;
З5	особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;
З6	типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.
З7	*принципы виртуализации.*
З8	*различные методологии поиска уязвимостей информационных ресурсов, компьютерных сетей и приложений.*
З9	*популярные методы компьютерных атак*
З10	*основные способы защиты от атак на типовые уязвимости*
З11	*основные методы сбора информации для расследования инцидента.*
З12	*принципы функционирования, способы настройки и управления различными операционными системами и серверами.*
З13	*способы настройки сетевого оборудования и программного обеспечения.*
У1	устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;
У2	устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;
У3	диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;
У4	применять программные и программно-аппаратные средства для защиты информации в базах данных;
У5	проверять выполнение требований по защите информации от несанкциони-

№	**Освоенные умения, усвоенные знания**
	рованного доступа при аттестации объектов информатизации по требованиям безопасности информации;
У6	применять математический аппарат для выполнения криптографических преобразований;
У7	использовать типовые программные криптографические средства, в том числе электронную подпись;
У8	применять средства гарантированного уничтожения информации;
У9	устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;
У10	осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак
У11	*администрировать веб-сервера, почтовые сервера, прокси.*
У12	*настраивать межсетевые экраны, маршрутизаторы, сетевое оборудование и программное обеспечение.*
У13	*работать с кластерными файловыми системами, организовывать RAID-массивы.*
У14	*настраивать виртуальные частные сети.*
У15	*организовывать удаленный доступ к ресурсам.*
У16	*устанавливать и настраивать безопасную конфигурацию операционной системы, серверов и программного обеспечения с учетом предъявляемых требований.*
У17	*использовать штатные и специальные средства мониторинга безопасности операционных систем*
У18	*работать со сканерами уязвимости*
У19	*осуществлять мониторинг и анализ инцидентов информационной безопасности, в том числе и анализ системных журналов и логов.*

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

2. СИСТЕМА КОНТРОЛЯ И ОЦЕНКИ ОСВОЕНИЯ ПРОГРАММЫ ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами»

2.1. Формы промежуточной аттестации по ППССЗ при освоении профессионального модуля

Элементы модуля, профессиональный модуль	Формы промежуточной аттестации
МДК.02.01. Программные и программно-аппаратные средства защиты информации	Экзамен
МДК.02.02. Криптографические средства защиты информации	Дифференцированный зачет
МДК.02.03. Кибербезопасность	Дифференцированный зачет
Учебная практика	Дифференцированный зачет
Производственная практика	Дифференцированный зачет
ПМ	**Экзамен**

2.2. Организация контроля и оценки освоения программы ПМ

Итоговый контроль освоения вида профессиональной деятельности ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами» осуществляется на экзамене. Условием допуска к экзамену является положительная аттестация по МДК, учебной и производственной практикам.

Экзамен проводится в виде выполнения практического экзаменационного задания.

Условием положительной аттестации по ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами» (вид профессиональной деятельности освоен) на экзамене квалификационном является положительная оценка освоения всех профессиональных компетенций по всем контролируемым показателям. При отрицательном заключении хотя бы по одной из профессиональных компетенций принимается решение «вид профессиональной деятельности не освоен».

Промежуточный контроль освоения профессионального модуля осуществляется при проведении экзамена по МДК.02.01 «Применение программных и программно-аппаратных средств защиты информации», дифференцированного зачета по МДК.02.02 «Применение криптографических средств защиты информации», дифференцированного зачета по МДК.02.03 «Кибербезопасность» и дифференцированного зачета по учебной и производственной практике. Предметом оценки освоения МДК являются знания. Экзамен и комплексный экзамен по МДК проводятся по заранее подготовленным и утвержденным экзаменационным вопросам. Условием положительной аттестации является получение обучающимся на экзамене оценки «удовлетворительно», «хорошо», «отлично».

Предметом оценки по учебной практике является приобретение практического опыта по ведению учета и оформления бумажных и машинных носителей конфиденциальной информации, работе с информационными системами электронного документооборота. Контроль и оценка по учебной практике проводится на основе Аттестационного листа обучающегося с места прохождения практики.

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

3. КОМПЛЕКТ МАТЕРИАЛОВ ДЛЯ ОСВОЕНИЯ УМЕНИЙ И УСВОЕНИЯ ЗНАНИЙ, ОЦЕНКИ СФОРМИРОВАННОСТИ ОБЩИХ И ПРОФЕССИОНАЛЬНЫХ КОМПЕТЕНЦИЙ ПО ВИДУ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ

3.1. Задания для оценки освоения теоретического курса профессионального модуля

3.1.1. Оценка освоения теоретического курса профессионального модуля по МДК.02.01

<table>
<tr><th rowspan="2">Дидактические единицы</th><th rowspan="2">Проверяемые ОК, ПК, У, З</th><th colspan="2">Формы контроля (наименование контрольной точки)</th></tr>
<tr><th>Текущая аттестация</th><th>Промежуточная аттестация</th></tr>
<tr><td>Тема 1.1. Общие понятия программно-аппаратных средств защиты информации
Тема 1.2. Защита программ и данных
Тема 1.3. Защита в компьютерных сетях</td><td>З1-З6
У1-У5
ОК1-ОК11
ПК2.1-ПК2.6</td><td>Устный зачет по темам 1.1. – 1.3.</td><td rowspan="3">устные ответы на экзамене</td></tr>
<tr><td rowspan="2">Тема 1.5. Средства защиты на компьютерах с операционной системой Windows
Тема 1.4. Антивирусная защита данных</td><td>З1-З6
У1-У5
ОК1-ОК11
ПК2.1-ПК2.6</td><td>Практическое занятие № 11 Работа с действующими средствами локальной защиты с помощью Secret Net Studio</td></tr>
<tr><td>З1-З5
ОК1-ОК11
ПК2.1-ПК2.6</td><td>Устный зачет по темам 1.4-1.5.</td></tr>
</table>

Дидактические единицы	Проверяемые ОК, ПК, У, З	Формы контроля (наименование контрольной точки)	
		Текущая аттестация	Промежуточная аттестация
Тема 1.6 Использование DLP-системы Infowatch для защиты от внутренних утечек информации	З1-З6 У1-У5 ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 18 «Установка и настройка Traffic monitor»	
		Практическое занятие № 19 «Установка и настройка Device monitor»	
		Практическое занятие № 20 «Установка клиента Device monitor. Настройка периметра компании, добавление пользователей и компьютеров в домен»	
		Практическое занятие № 23 «Создание правил с использованием «белых» и «чёрных» списков в Device monitor»	
		Практическое занятие № 25 Добавление ролей, редактирование ролей, удаление ролей в Traffic monitor	
		Практическое занятие № 31 «Создание политик с использованием правил передачи в Traffic monitor»	
		Практическое занятие № 35 Создание политик с использованием регулярных выражений в Traffic Monitor	
		Практическое занятие № 37 «Создание и изменение отчётов в Traffic Monitor»	
Тема 1.7. Методики проверки защищённости объектов информатизации	З1-З5 ОК1-ОК11 ПК2.1-ПК2.6	Устный опрос по теме 1.7.	
Тема 1.8. Использование программно-аппаратных	З1-З6 У1-У5 ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 41 Создание структуры защищённой сети ViPNet	
		Практическое занятие № 43 Развёртывание рабочего места помощника главного администратора защищённой сети ViPNet	
		Практическое занятие № 46 Настройка политик безопасности в VipNet Policy Manager	
		Практическое занятие № 47	

Дидактические единицы	Проверяемые ОК, ПК, У, З	Формы контроля (наименование контрольной точки)	
		Текущая аттестация	Промежуточная аттестация
		Организация межсетевого взаимодействие	
		Практическое занятие № 48 Модификация межсетевого взаимодействия в защищённой сети ViPNet	
Тема 1.9. Защита передачи данных через Интернет Тема 1.10 Средства защиты на компьютерах с операционной системой Linux	З1-З6 У1-У5 ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 52 Применение сертификата	
		Практическое занятие № 55 Настройка прокси-сервера с помощью Nginx	
	З1-З6 У1-У5 ОК1-ОК11 ПК2.1-ПК2.6	Практическое занятие № 61 Установка системы обнаружения и предотвращения вторжения Snort	
	З1-З5 ОК1-ОК11 ПК2.1-ПК2.6	Устный зачет по темам 1.9-1.10	

1. Устный зачет по темам 1.1.-1.3

Инструкция для обучающихся
Зачет сдается в рамках учебного занятия. Каждый студент отвечает в устной форме на предложенные преподавателем 2 вопроса.

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

Перечень вопросов:

1. Виды программно-аппаратных средств защиты информации
2. Понятие комплексных решений SIEM
3. Методы скрытия информации
4. Структура и функции подсистемы безопасности операционных систем
5. Подсистема безопасности Windows.
6. Подсистема безопасности Linux.
7. Средства обеспечения защиты информации в системах управления базами данных
8. Критерии защищённости компьютерных систем.
9. Средства защиты в вычислительных сетях
10. Защита информации в VPN-сетях.

Эталоны ответов: приведены в Учебном пособии по МДК.02.01 «Программные и программно-аппаратные средства защиты информации».

1. Практическое занятие № 11
«Работа с действующими средствами локальной защиты с помощью Secret Net Studio»

Задание 1:

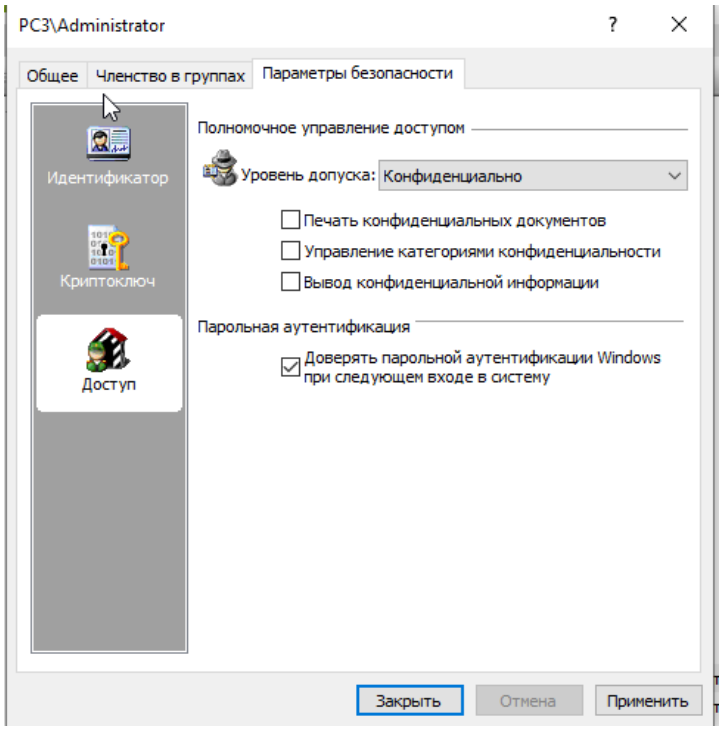
1. Запустите управление параметрами безопасности пользователей. Откройте свойства вашего пользователя → Параметры безопасности → Доступ. Установите уровень допуска Конфиденциально. В отчёт вставьте скриншот с выполненным заданием.
2. Добавьте нового пользователя из AD (не создавать нового). Должна появиться надпись после добавления Доменный пользователь. В отчёт вставьте скриншот с добавленным пользователем.
3. Запустите Локальный центр управления Secret Net Studio — Настройки. Смените максимальный период неактивности до блокировки экрана. В отчёт вставьте скриншот с выполненным заданием.
4. В базовой защите на вход в систему установите количество неудачных попыток аутентификации на 1 попытку. В отчёт вставьте скриншот с выполненным заданием.
5. Установите в базовой защите в журнале не затирать события. В отчёт вставьте скриншот с выполненным заданием.
6. Перейдите в Локальную защиту → Замкнутая программная среда → Удалите возможность у пользователей создавать криптоконтейнеры. В отчёт вставьте скриншот с выполненным заданием.

7. Перейдите в Сетевую защиту → Обнаружение вторжений → измените время блокировки атакующего хоста. Внесите в белый список любой IP-адрес. В отчёт вставьте скриншот с выполненным заданием.
8. Перейдите в Регистрации событий → Дискреционное управление доступом → включите регистрацию доступа к файлам и каталогам. В отчёт вставьте скриншот с выполненным заданием.
9. Выйдите с вкладки Настройки, перейдите на вкладку Журналы. Создайте журнал по событиям Secret Net Studio. Получите журнал и экспортируйте. В отчёт вставьте скриншот с выполненным заданием.
10. Перейдите на вкладку Отчёты → Ресурсы АРМ→ выберете несколько пунктов для будущего отчёта → нажмите Построить → Просмотреть. В отчёт вставьте скриншот с выполненным заданием.
11. Закройте данный программный компонент. Откройте Контроль программ и данных. Просмотрите структуру Субъектов управления. В отчёт вставьте скриншот и ответьте на вопрос: Для чего предназначен компонент Контроль программ и данных?
12. Закройте все компоненты Secret Net Studio. На Рабочем столе создайте новую папку. Откройте контекстное меню папки. В отчёт вставьте скриншот и ответьте на вопрос: что появилось в контекстном меню от Secret Net Studio и что это означает?
13. Откройте Свойства новой созданной папки, перейдите на вкладку Secret Net Studio. Измените на Категорию Конфиденциально. В отчёт вставьте скриншот с выполненным заданием.

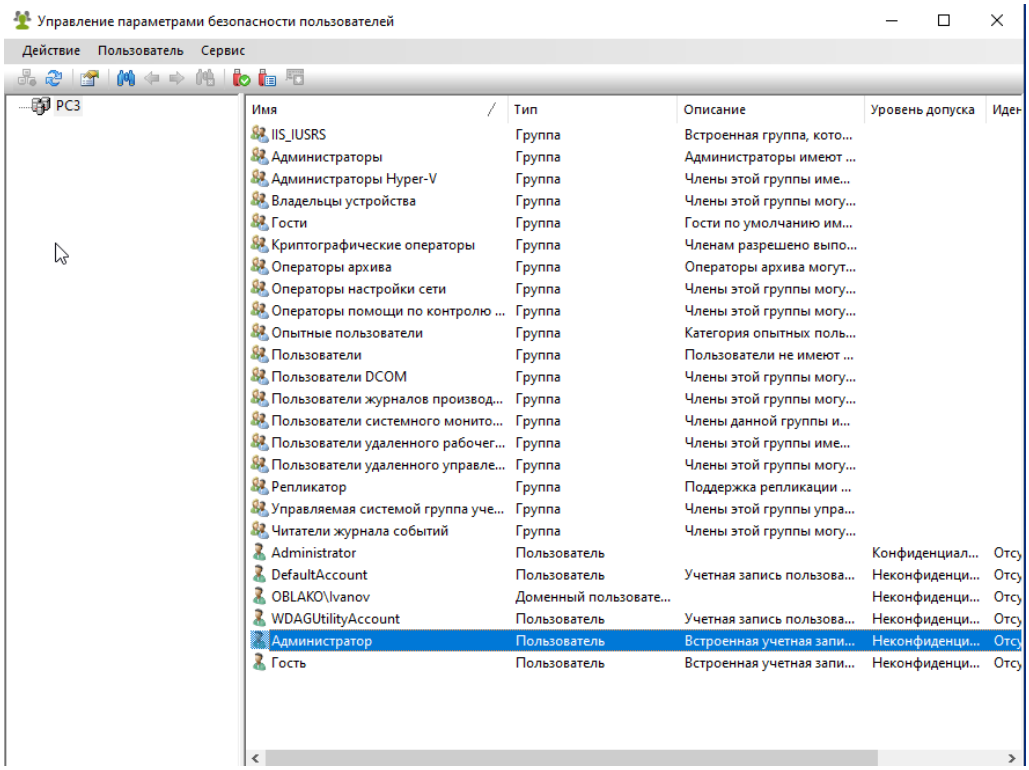
Эталон ответа:

Задание 1:

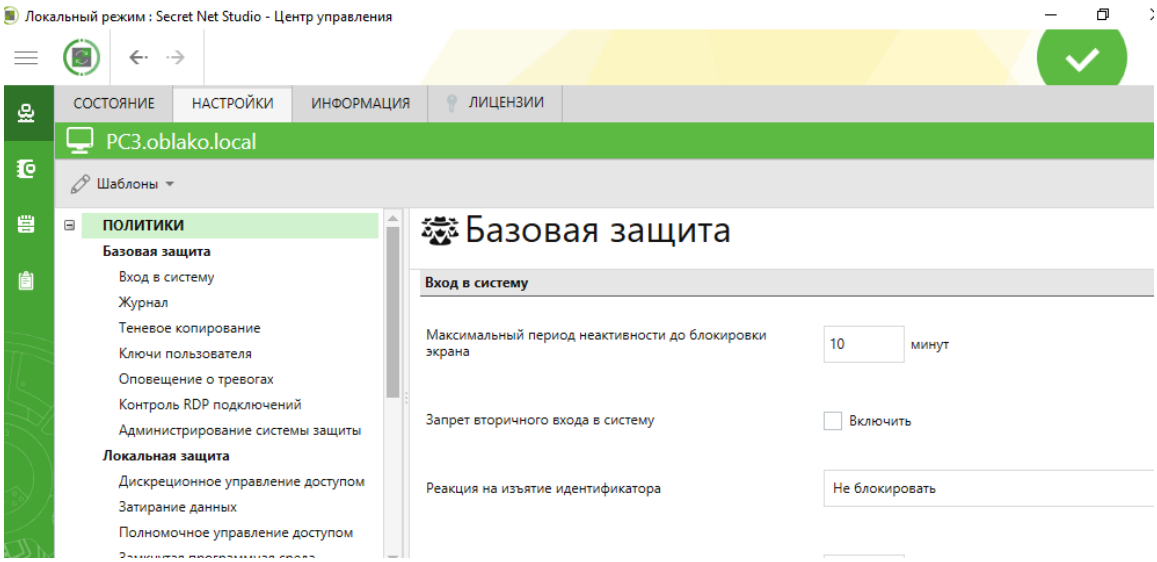
Запустите управление параметрами безопасности пользователей. Откройте свойства вашего пользователя → Параметры безопасности → Доступ. Установите уровень допуска Конфиденциально. В отчёт вставьте скриншот с выполненным заданием.



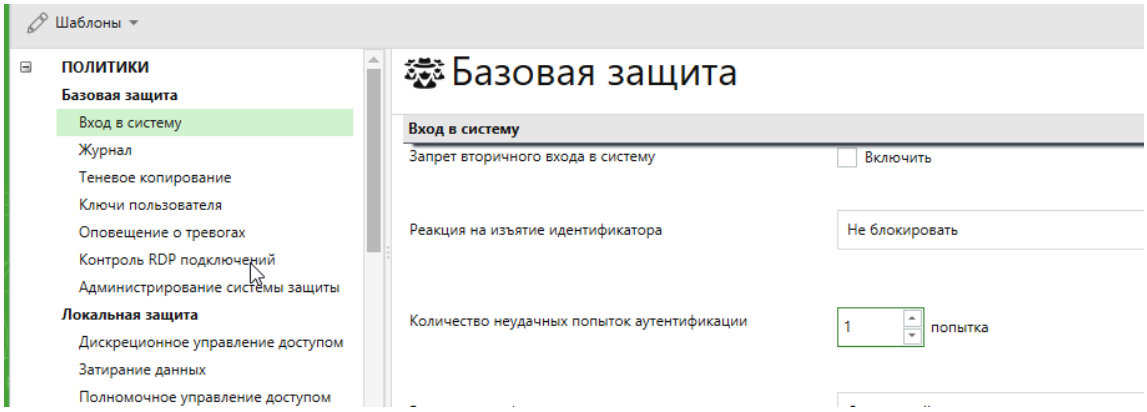
Добавьте нового пользователя из AD (не создавать нового). Должна появиться надпись после добавления Доменный пользователь. В отчёт вставьте скриншот с добавленным пользователем.



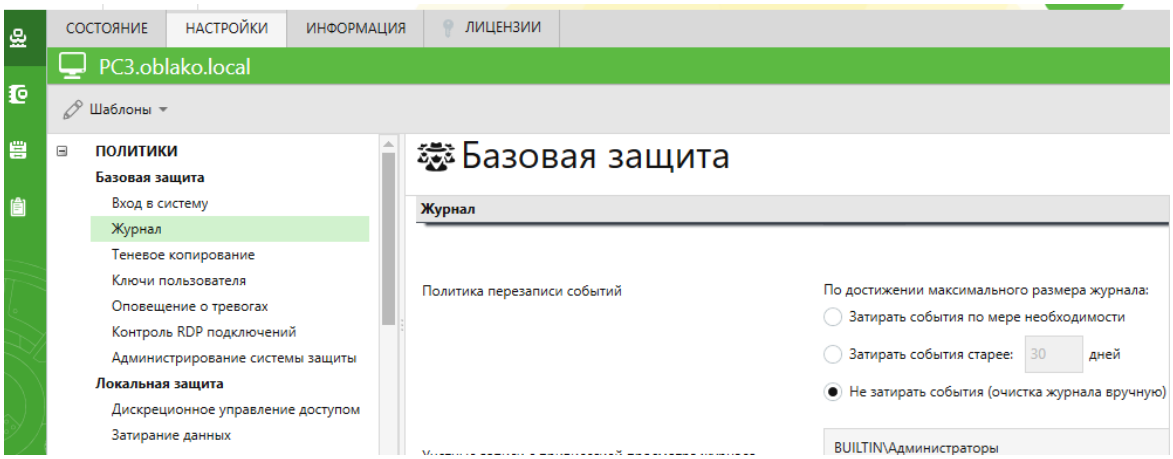
Запустите Локальный центр управления Secret Net Studio — Настройки. Смените максимальный период неактивности до блокировки экрана. В отчёт вставьте скриншот с выполненным заданием.



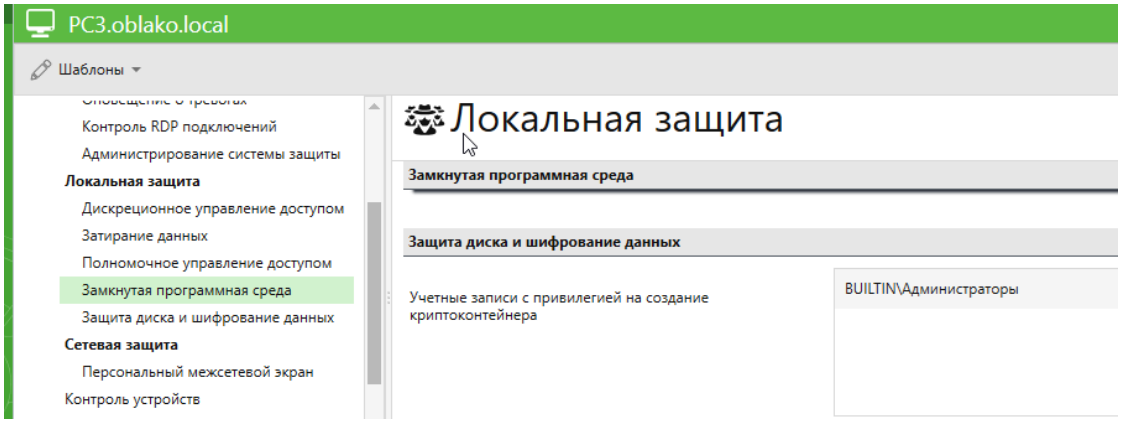
В базовой защите на вход в систему установите количество неудачных попыток аутентификации на 1 попытку. В отчёт вставьте скриншот с выполненным заданием.



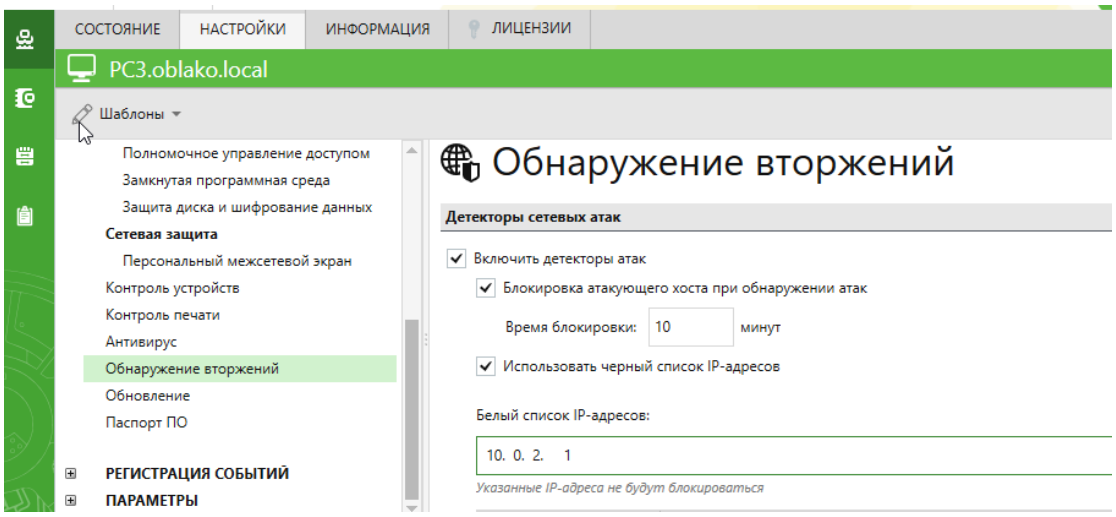
Установите в базовой защите в журнале не затирать события. В отчёт вставьте скриншот с выполненным заданием.



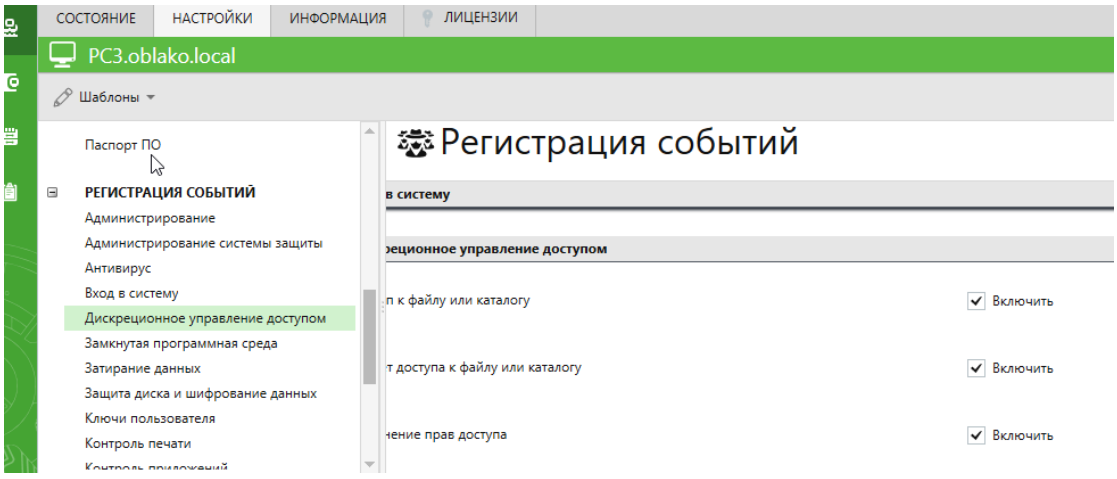
Перейдите в Локальную защиту → Замкнутая программная среда → Удалите возможность у пользователей создавать криптоконтейнеры. В отчёт вставьте скриншот с выполненным заданием.



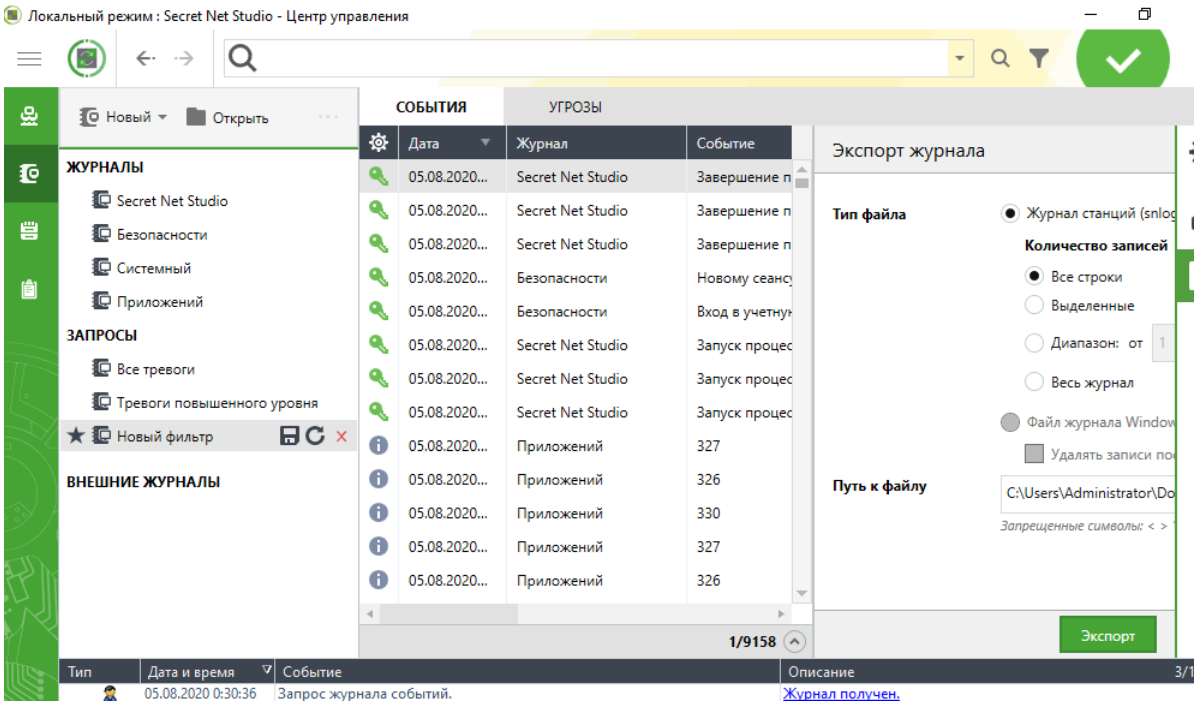
Перейдите в Сетевую защиту → Обнаружение вторжений → измените время блокировки атакующего хоста. Внесите в белый список любой IP-адрес. В отчёт вставьте скриншот с выполненным заданием.



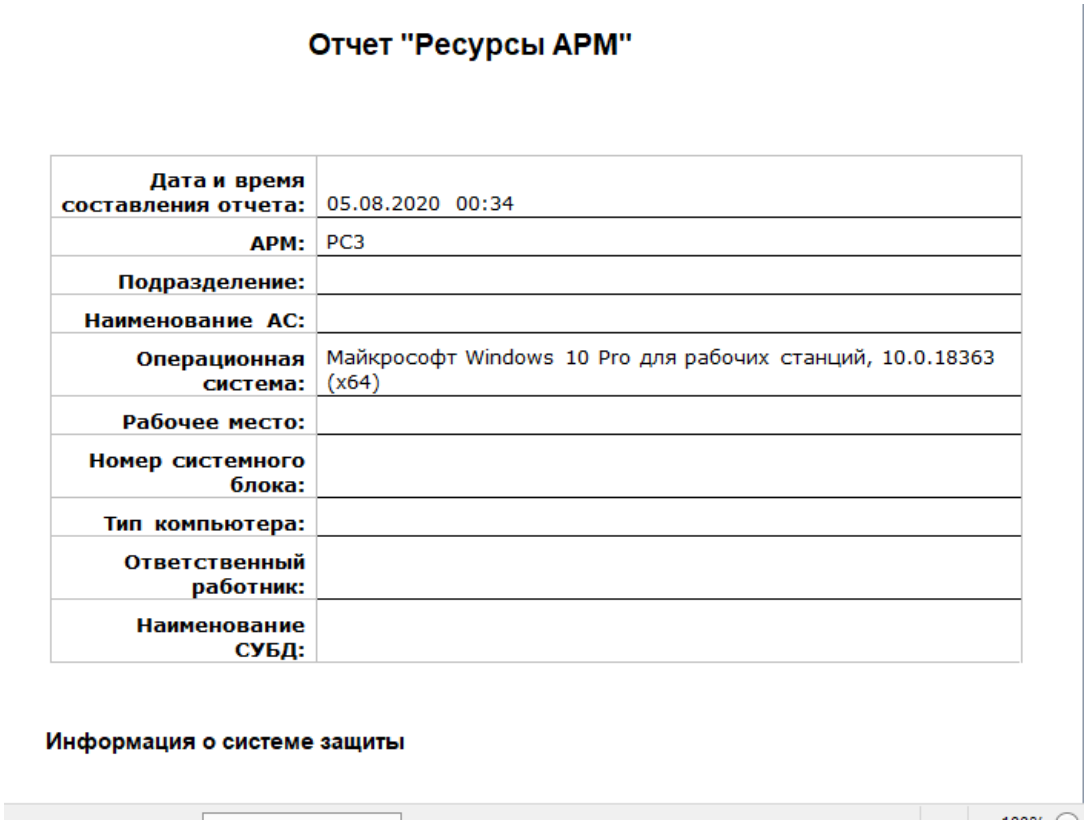
Перейдите в Регистрации событий → Дискреционное управление доступом → включите регистрацию доступа к файлам и каталогам. В отчёт вставьте скриншот с выполненным заданием.



Выйдите с вкладки Настройки, перейдите на вкладку Журналы. Создайте журнал по событиям Secret Net Studio. Получите журнал и экспортируйте. В отчёт вставьте скриншот с выполненным заданием.



Перейдите на вкладку Отчёты → Ресурсы АРМ→ выберете несколько пунктов для будущего отчёта → нажмите Построить → Просмотреть. В отчёт вставьте скриншот с выполненным заданием.

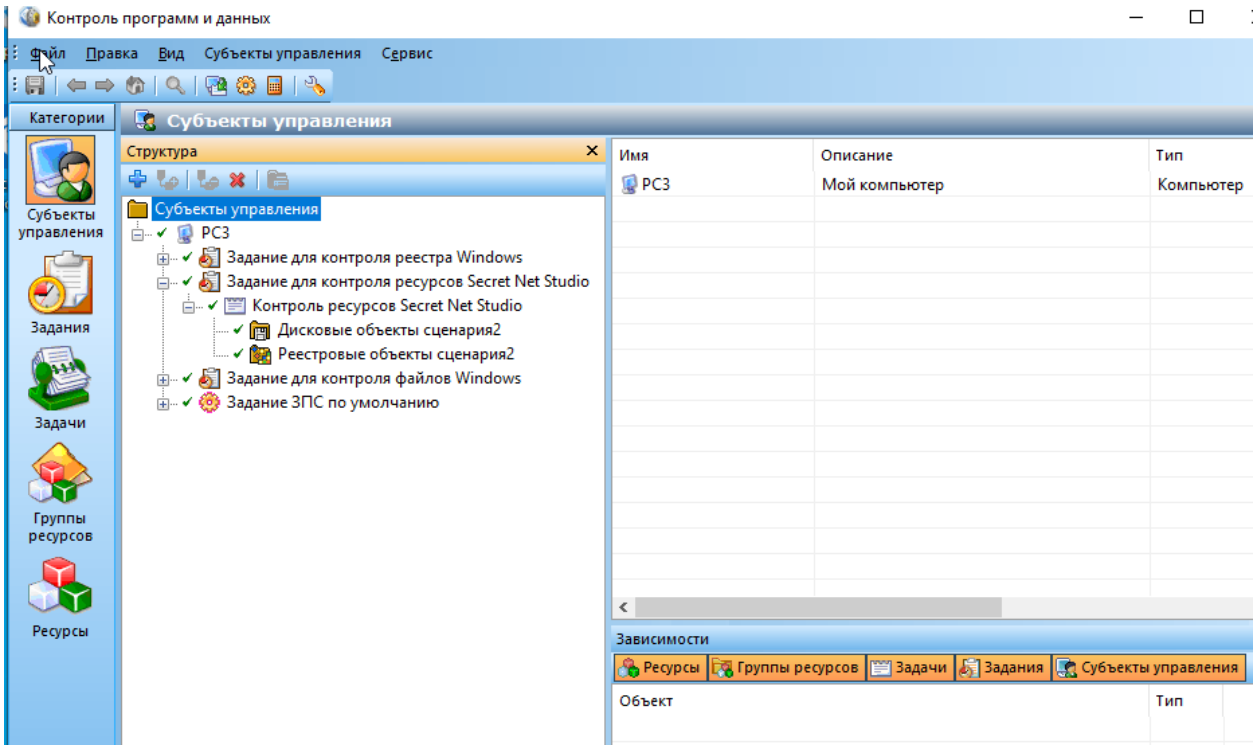


Отчет "Ресурсы АРМ"

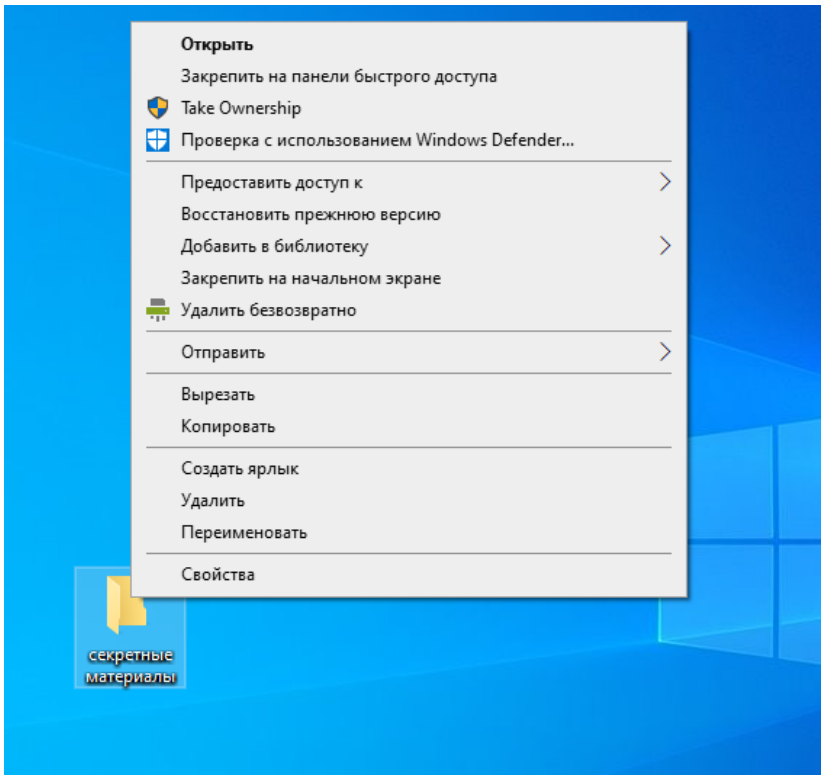
Дата и время составления отчета:	05.08.2020 00:34
АРМ:	PC3
Подразделение:	
Наименование АС:	
Операционная система:	Майкрософт Windows 10 Pro для рабочих станций, 10.0.18363 (x64)
Рабочее место:	
Номер системного блока:	
Тип компьютера:	
Ответственный работник:	
Наименование СУБД:	

Информация о системе защиты

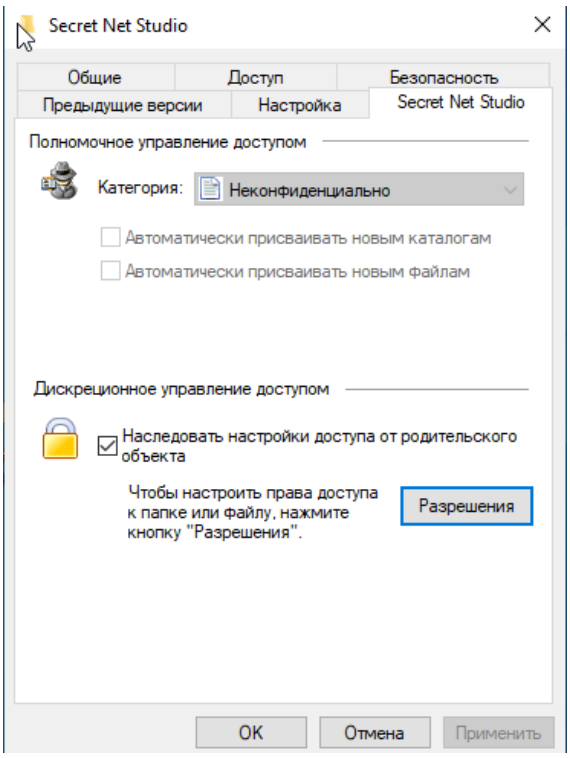
Закройте данный программный компонент. Откройте Контроль программ и данных. Просмотрите структуру Субъектов управления. В отчёт вставьте скриншот и ответьте на вопрос: Для чего предназначен компонент Контроль программ и данных?



Закройте все компоненты Secret Net Studio. На Рабочем столе создайте новую папку. Откройте контекстное меню папки. В отчёт 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. В отчёт вставьте скриншот с выполненным заданием.



3. Устный зачет по темама 1.4.-1.5

Инструкция для обучающихся

Зачет сдается в рамках учебного занятия. Каждый студент отвечает в устной форме на предложенные преподавателем 2 вопроса.

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

Перечень вопросов:

1. Современные программные средства для защиты от вредоносных программ
2. Использование Active Directory и политик безопасности. Понятие домена. Роли контроллера домена Структура и функции подсистемы безопасности операционных систем
3. Средство защиты информации Secret Net Studio.Возможности Secret Net Studio. Принцип работы.
4. Параметры установки Подсистема безопасности Linux.
5. Средства защиты информации Dallas Lock.
6. Возможности Dallas Lock. Принцип работы. Параметры установки Критерии защищённости компьютерных систем.

Эталоны ответов: приведены в Учебном пособии по МДК.02.01 «Программные и программно-аппаратные средства защиты информации».

4.Практическое занятие № 18 «Установка и настройка Traffic monitor»

Задание 1:

1. Установить InfoWatch Traffic Monitor Enterprise:

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

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

- Выбор базы данных;
- выбор режима установки;
- выбор часового пояса;
- установка пароля суперпользователя Системы;
- выбор способа разбиения дискового пространства;
- настройка сети;
- настройка синхронизации времени (NTP-server);
- настройка локализации;
- настройка автоматического удаления событий из БД;
- завершение установки.

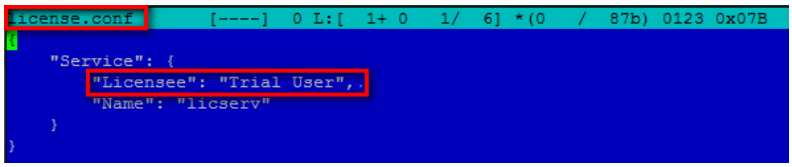
Задание 2 Настройка InfoWatch Traffic Monitor:

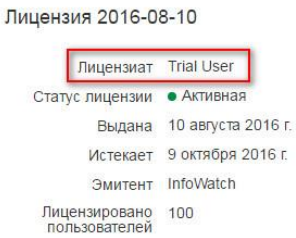
- Откройте интернет-браузер (рекомендуется использовать браузер Google Chrome.
- В адресной строке введите адрес сервера InfoWatch Traffic Monitor.
- В поле Логин укажите имя пользователя.
- В поле Пароль укажите пароль.
- Нажмите Войти.

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

Войдите в интерпретатор командной строки сервера Traffic Monitor.

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





перезапустите сервер Traffic Monitor следующей командой:

service iwtm restart

Как проверить статус/запустить компоненты InfoWatch Traffic Monitor?

Войдите в интерпретатор командной строки сервера Traffic Monitor и выполните необходимую команду.

service iwtm status (отобразить статус всех компонентов Traffic Monitor)

service iwtm start (запустить все компоненты Traffic Monitor)

service iwtm stop (остановить все компоненты Traffic Monitor)

service iwtm restart (перезапустить все компоненты Traffic Monitor)

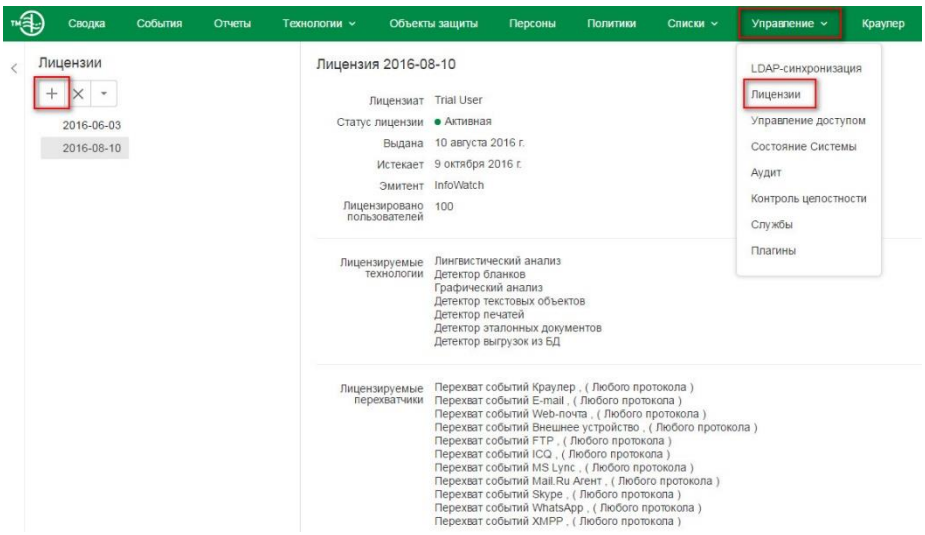
service iwtm restart xapi_xapi (перезапустит только компонент xapi)

service iwtm stop cas (остановит только компонент cas)

Как проверить и очистить место на сервере InfoWatch Traffic Monitor?

Для проверки свободного места на сервере Traffic Monitor подключитесь к серверу с помощью SSH-клиента и выполните следующую команду:

df –h



Для очистки места на сервере Traffic Monitor вы можете удалить:

Дистрибутив системы из директории /opt/distr/

rm –rf /opt/distr/ (удаление дистрибутивов Traffic Monitor)

Информацию из временной директории Traffic Monitor:

service iwtm stop (остановка сервера Traffic Monitor)

rm –rfd /opt/iw/tm5/tmp/* (удаление временных файлов Traffic Monitor)

service iwtm start (запуск сервера Traffic Monitor)

Лог-файлы (с расширением .gz) в директории /var/log

rm –rf /var/log/infowatch/*.gz (удаление лог-файлов Traffic Monitor с расширением gz)

С более детальной информацией об очистке места можно ознакомиться в статье Базы Знаний “Очистка InfoWatch Traffic Monitor от временных файлов”.

Как проверить и очистить очередь на сервере InfoWatch Traffic Monitor?

Очереди событий хранятся в каталоге /opt/iw/tm5/queue/. Войдите в интерпретатор командной строки сервера Traffic Monitor под пользователем iwtm и запустите скрипт iw_qtool для ознакомления с доступными опциями:

su – iwtm (смена пользователя на iwtm)

./bin/iw_qtool (запуск скрипта iw_qtool)

./bin/iw_qtool stat /opt/iw/tm5/queue/db/ (отображение актуальной информации о количестве событий в очереди загрузки в базу данных)

./bin/iw_qtool erase /opt/iw/tm5/queue/errors/ (удаление событий из очереди ошибок)

./bin/iw_qtool move /opt/iw/tm5/queue/errors/ /opt/iw/tm5/queue/db/ (перемещение объектов из очереди ошибок в очередь загрузки в базу данных)

Задание 3:

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

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

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

Эталон ответа:

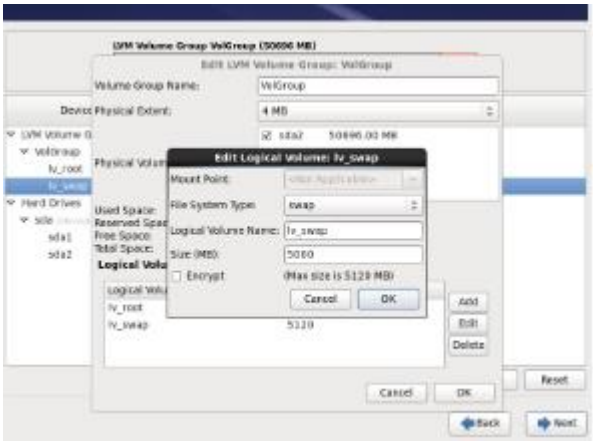
Задание 1:

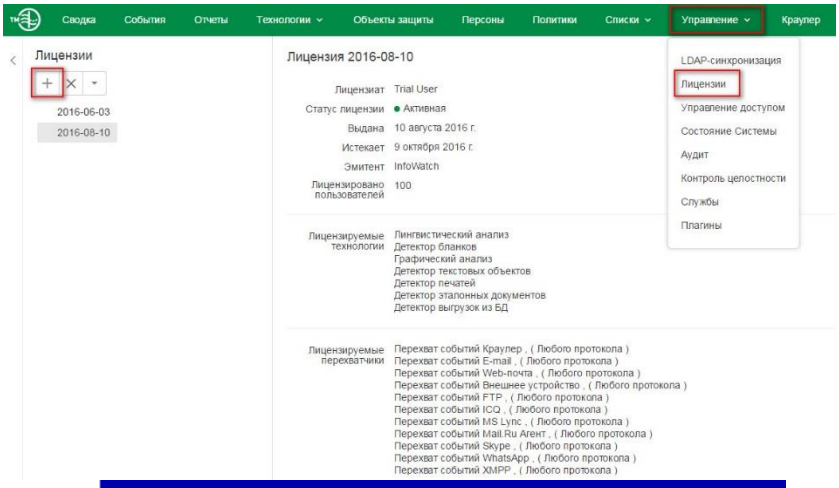
1. Установить InfoWatch Traffic Monitor Enterprise:

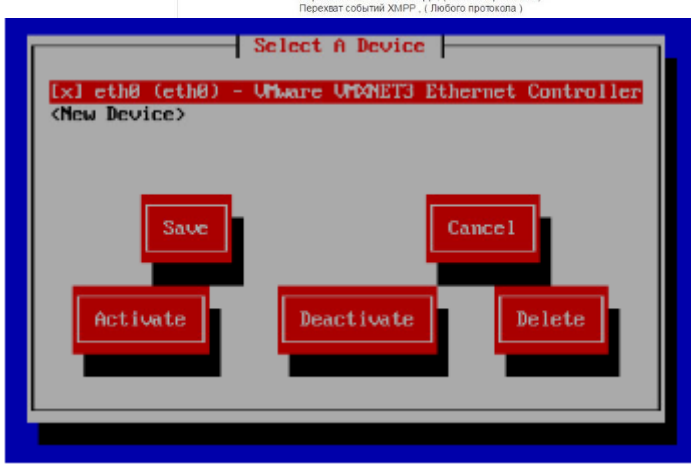
Тип установки: Все-в-одном Enterprise – все компоненты Системы (с СУБД Oracle Enterprise или PostgreSQL) устанавливаются на один сервер. Такая установка используется, если с учетом предполагаемой нагрузки на сервере будет обеспечен ресурс как для СУБД, так и для сервисов Traffic Monitor.

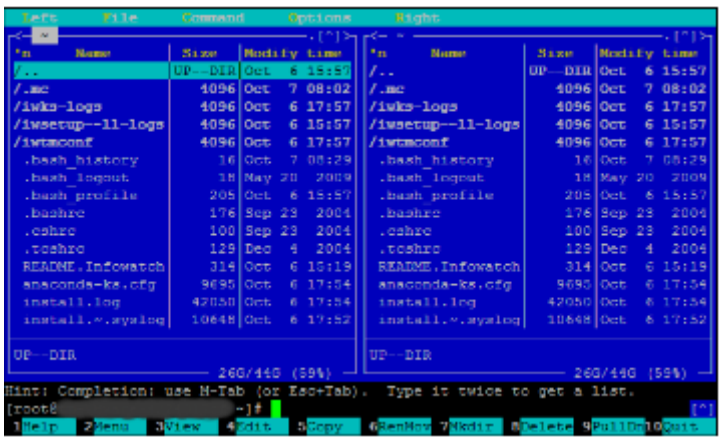
2. Установка системы Red Hat Enterprise Linux (IW TM 6 Enterprice в режиме «все в одном»):

- Выбор базы данных;
- выбор режима установки;
- выбор часового пояса;
- установка пароля суперпользователя Системы;
- выбор способа разбиения дискового пространства;
- настройка сети;
- настройка синхронизации времени (NTP-server);
- настройка локализации;
- настройка автоматического удаления событий из БД;
- завершение установки.









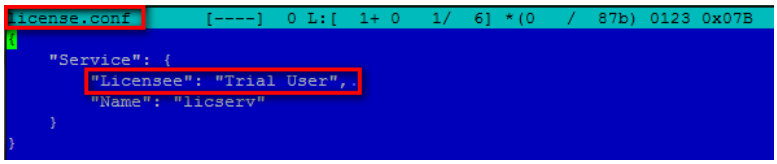
Задание 2 Настройка InfoWatch Traffic Monitor:

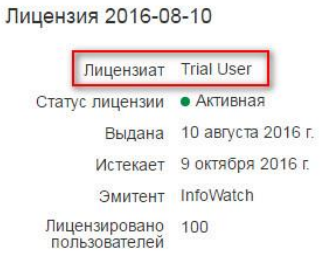
- Откройте интернет-браузер (рекомендуется использовать браузер Google Chrome.
- В адресной строке введите адрес сервера InfoWatch Traffic Monitor.
- В поле Логин укажите имя пользователя.
- В поле Пароль укажите пароль.
- Нажмите Войти.

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

Войдите в интерпретатор командной строки сервера Traffic Monitor.

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





перезапустите сервер Traffic Monitor следующей командой:

service iwtm restart

Как проверить статус/запустить компоненты InfoWatch Traffic Monitor?

Войдите в интерпретатор командной строки сервера Traffic Monitor и выполните необходимую команду.

service iwtm status (отобразить статус всех компонентов Traffic Monitor)

service iwtm start (запустить все компоненты Traffic Monitor)

service iwtm stop (остановить все компоненты Traffic Monitor)

service iwtm restart (перезапустить все компоненты Traffic Monitor)

service iwtm restart xapi_xapi (перезапустит только компонент xapi)

service iwtm stop cas (остановит только компонент cas)

Как проверить и очистить место на сервере InfoWatch Traffic Monitor?

Для проверки свободного места на сервере Traffic Monitor подключитесь к серверу с помощью SSH-клиента и выполните следующую команду:

df –h

Для очистки места на сервере Traffic Monitor вы можете удалить:

Дистрибутив системы из директории /opt/distr/

rm –rf /opt/distr/ (удаление дистрибутивов Traffic Monitor)

Информацию из временной директории Traffic Monitor:

service iwtm stop (остановка сервера Traffic Monitor)

rm –rfd /opt/iw/tm5/tmp/* (удаление временных файлов Traffic Monitor)

service iwtm start (запуск сервера Traffic Monitor)

Лог-файлы (с расширением .gz) в директории /var/log

rm –rf /var/log/infowatch/*.gz (удаление лог-файлов Traffic Monitor с расширением gz)

С более детальной информацией об очистке места можно ознакомиться в статье Базы Знаний “Очистка InfoWatch Traffic Monitor от временных файлов”.

Как проверить и очистить очередь на сервере InfoWatch Traffic Monitor?

Очереди событий хранятся в каталоге /opt/iw/tm5/queue/. Войдите в интерпретатор командной строки сервера Traffic Monitor под пользователем iwtm и запустите скрипт iw_qtool для ознакомления с доступными опциями:

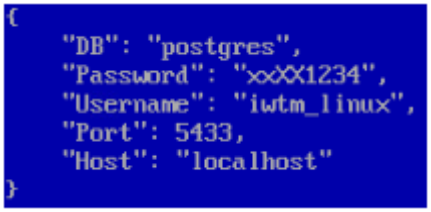
su – iwtm (смена пользователя на iwtm)

./bin/iw_qtool (запуск скрипта iw_qtool)

./bin/iw_qtool stat /opt/iw/tm5/queue/db/ (отображение актуальной информации о количестве событий в очереди загрузки в базу данных)

./bin/iw_qtool erase /opt/iw/tm5/queue/errors/ (удаление событий из очереди ошибок)

./bin/iw_qtool move /opt/iw/tm5/queue/errors/ /opt/iw/tm5/queue/db/ (перемещение объектов из очереди ошибок в очередь загрузки в базу данных)

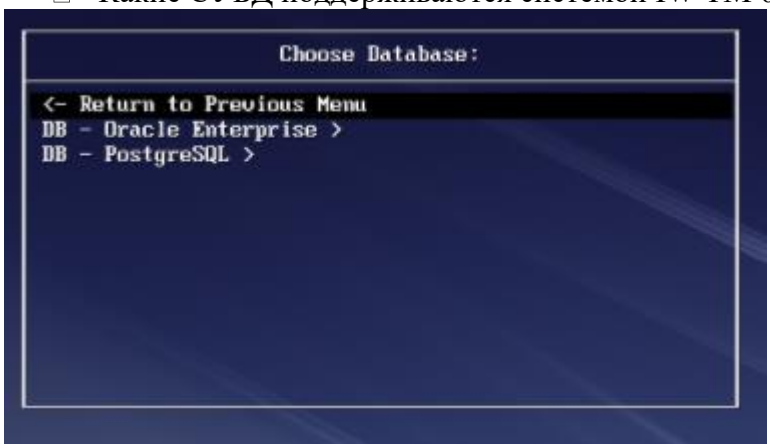


Задание 3:

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

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

- Какие СУБД поддерживаются системой IW TM 6?



- За прием каких данных отвечают компоненты sniffer и proxy?

Сохраняют перехваченные пакеты, распределенные по сессиям.

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

Подсистема анализа

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

Подсистема применения политик

- Для чего используется связка компонент системы SMTPD и Deliverd?

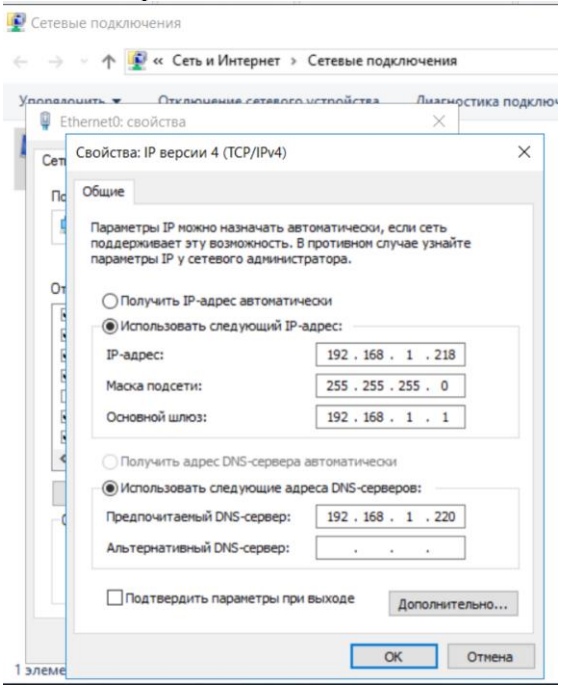
Процесс iw_deliverd, выполняющий доставку SMTP-писем адресатам при интеграции с почтовым relay-сервером

Процесс iw_smtpd, выполняющий перехват SMTP-трафика с почтового relay-сервера

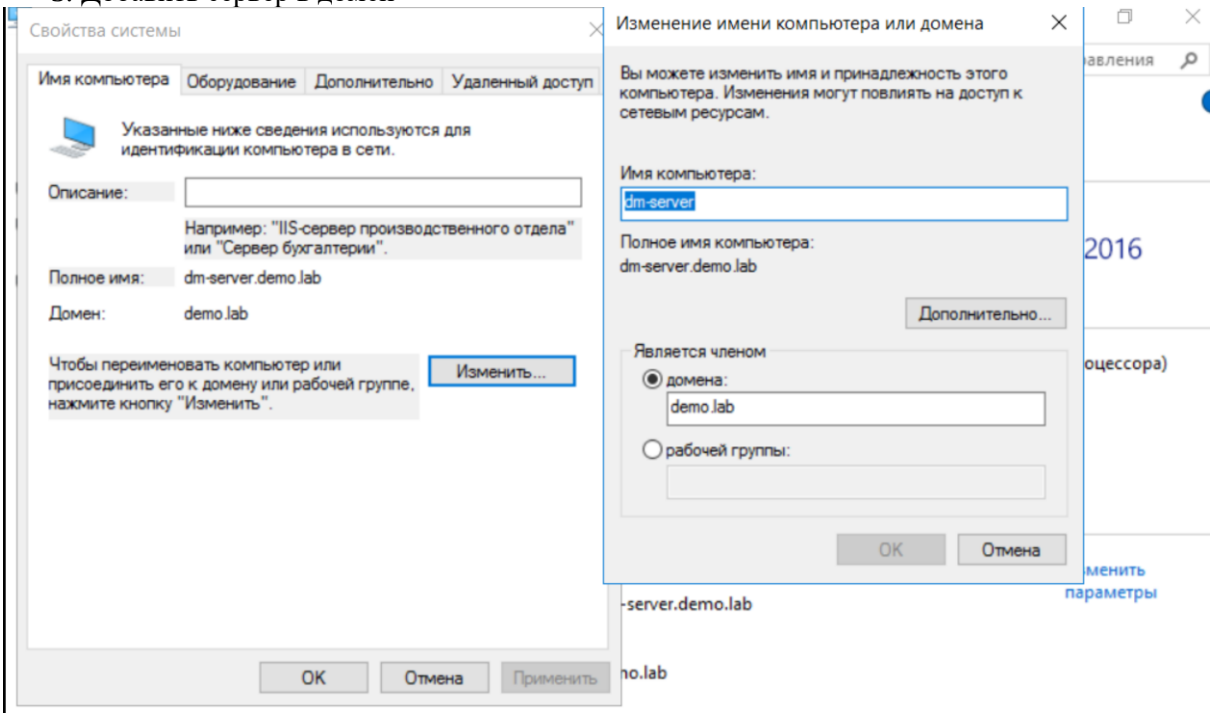
5.Практическое занятие № 19 «Установка и настройка Device monitor»

Задание:

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

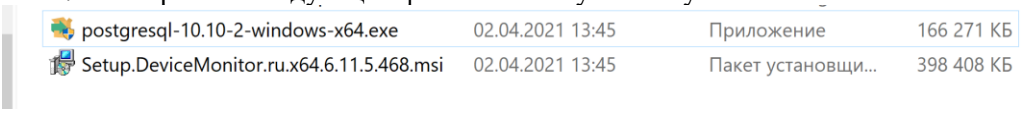


3. Добавить сервер в домен

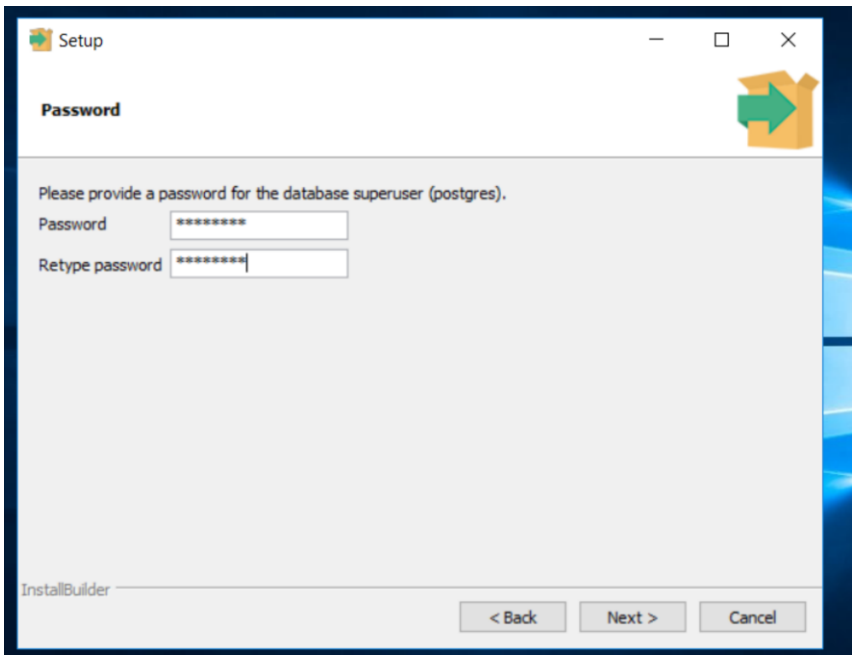


Выполнить перезагрузку системы. Войти под доменным пользователем.

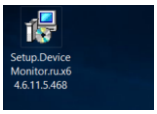
4. Скопировать следующие файлы на вашу машину:



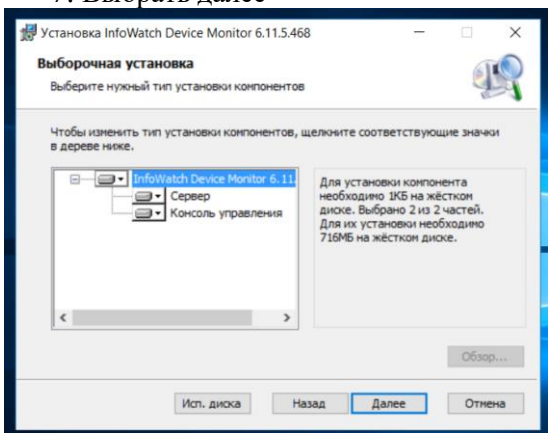
5. Установить базу данных



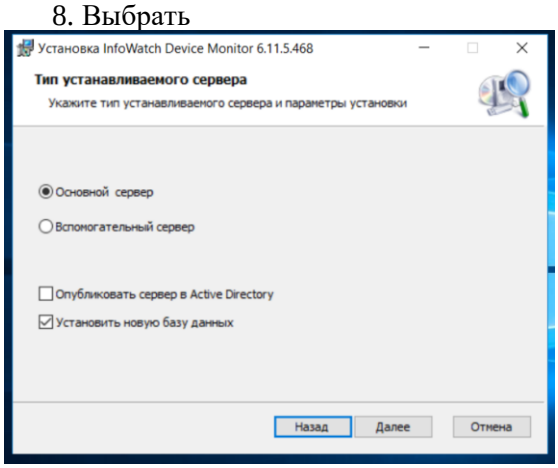
Запомнить пароль.

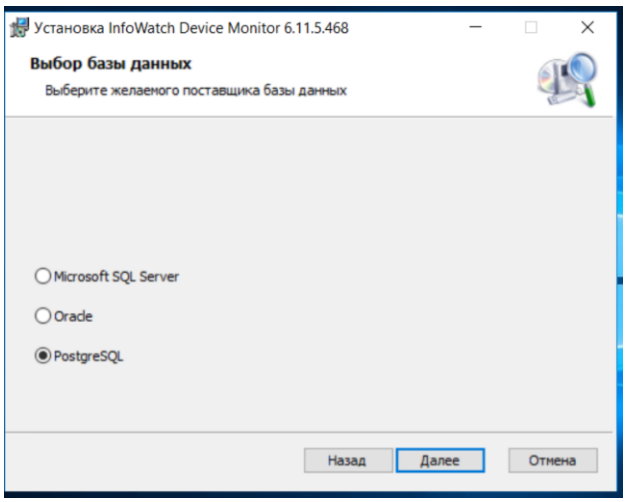
6. Запустить: 

7. Выбрать далее

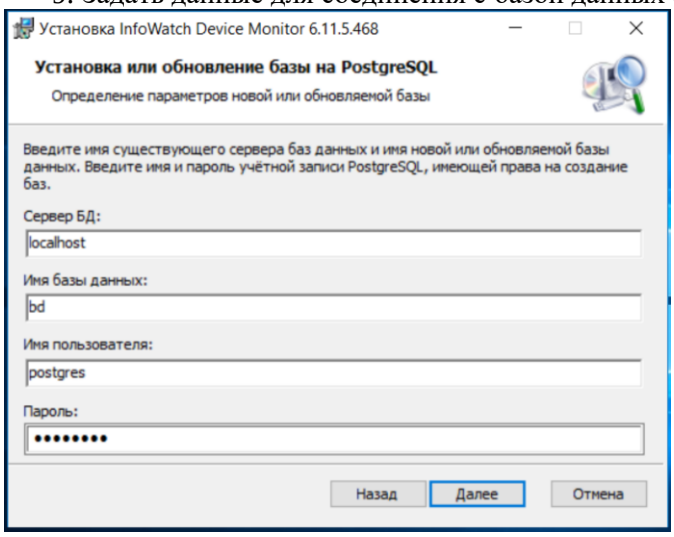


8. Выбрать

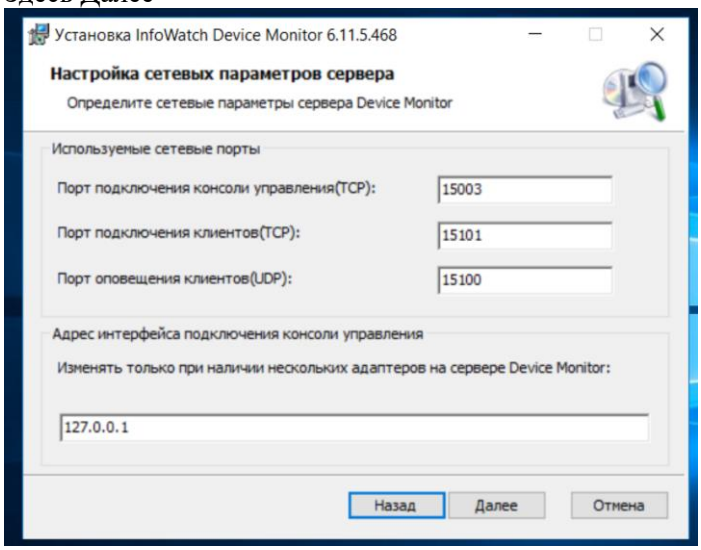




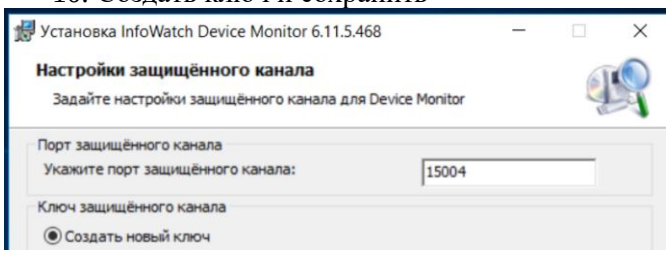
9. Задать данные для соединения с базой данных (пароль из пункта 5)



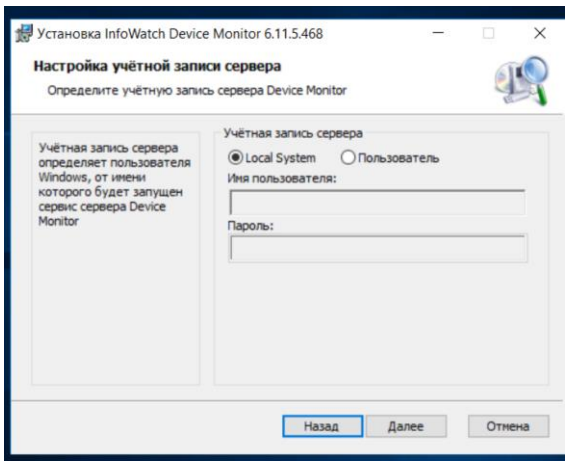
Здесь Далее



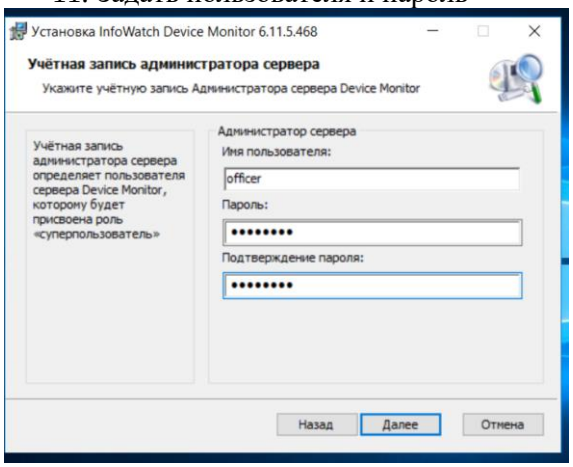
10. Создать ключ и сохранить



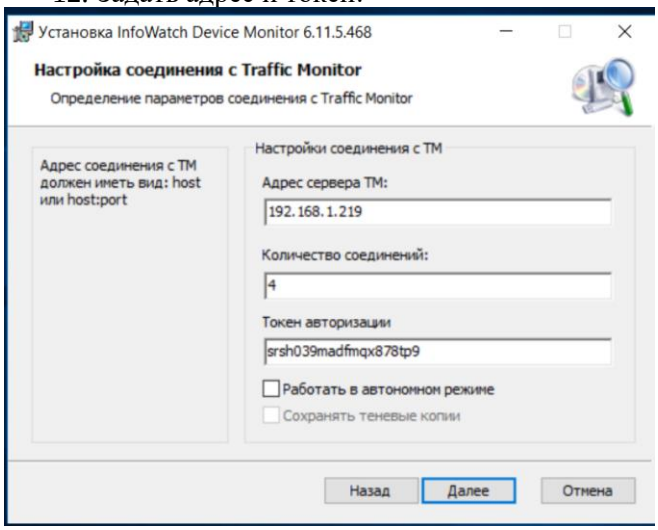
Далее



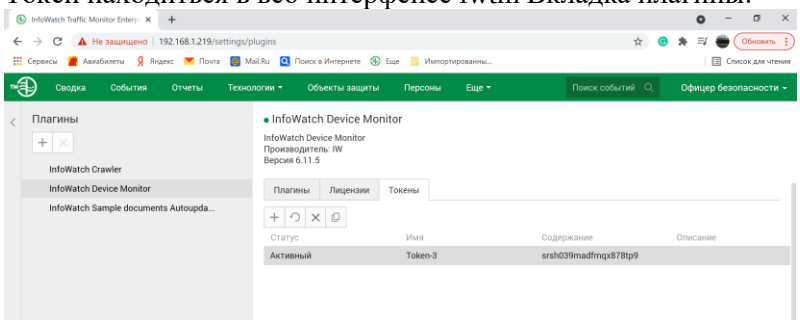
11. Задать пользователя и пароль



12. Задать адрес и токен:

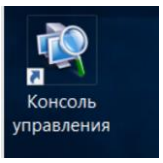


Токен находиться в веб интерфейсе iwtm Вкладка плагины:

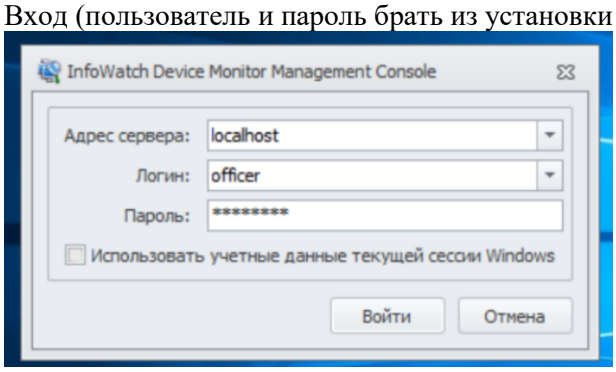


Далее устанавливаем.

13. После установки заходим в Консоль управления.

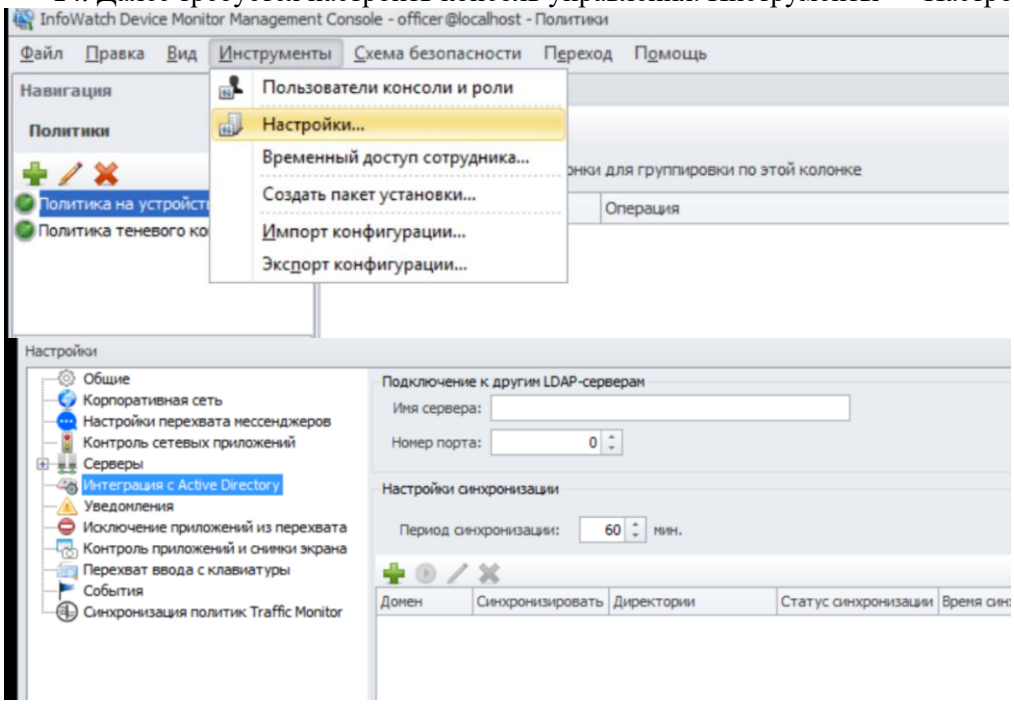


Вход (пользователь и пароль брать из установки iwdm):

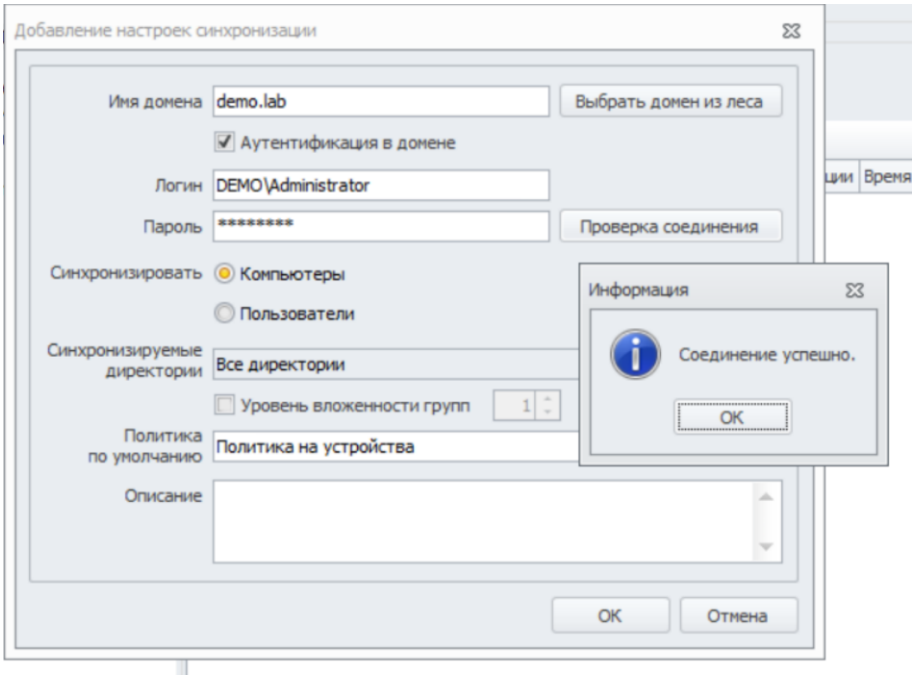


Вставляем в отчёт скриншот Консоли управления с удачным входом в неё.

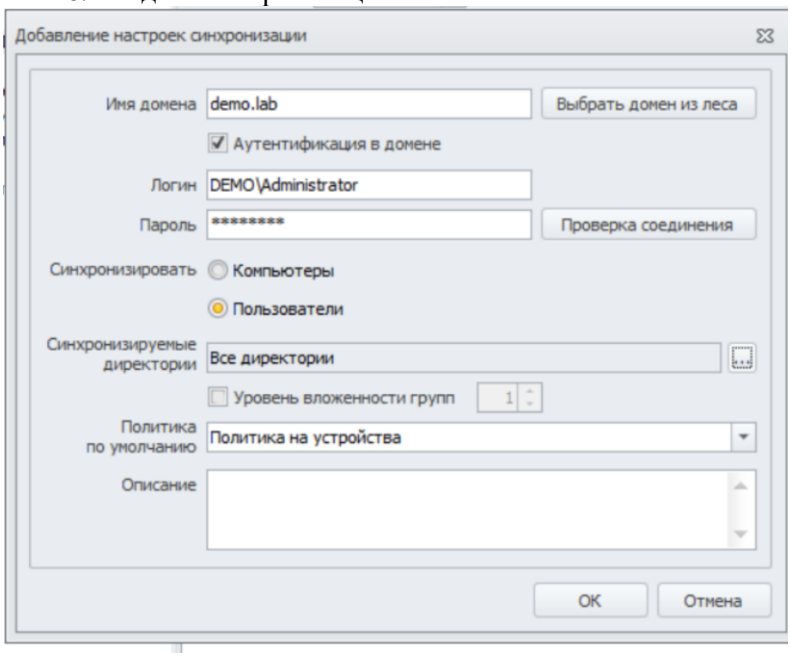
14. Далее требуется настроить консоль управления. Инструменты → Настройки:



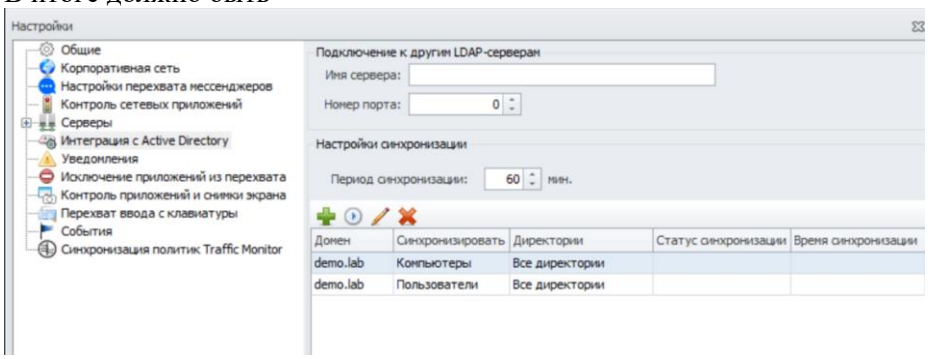
15. Задаем параметры соединения с AD



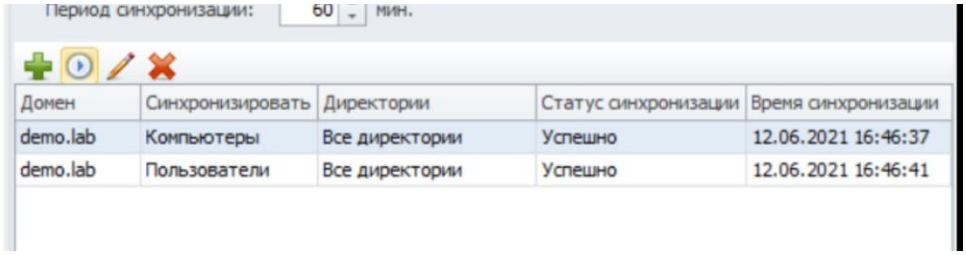
16. Создать синхронизацию пользователей



В итоге должно быть



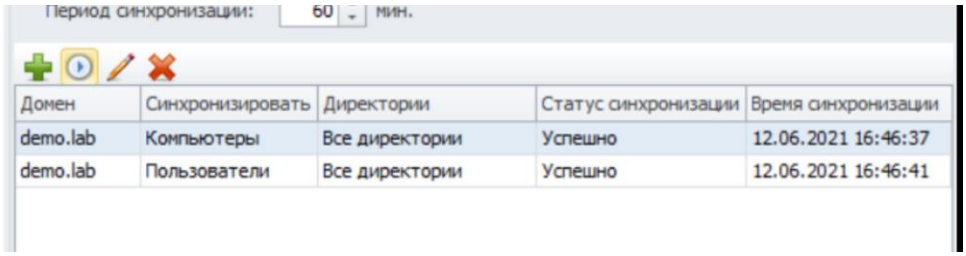
17. Сохранить и выполнить синхронизацию



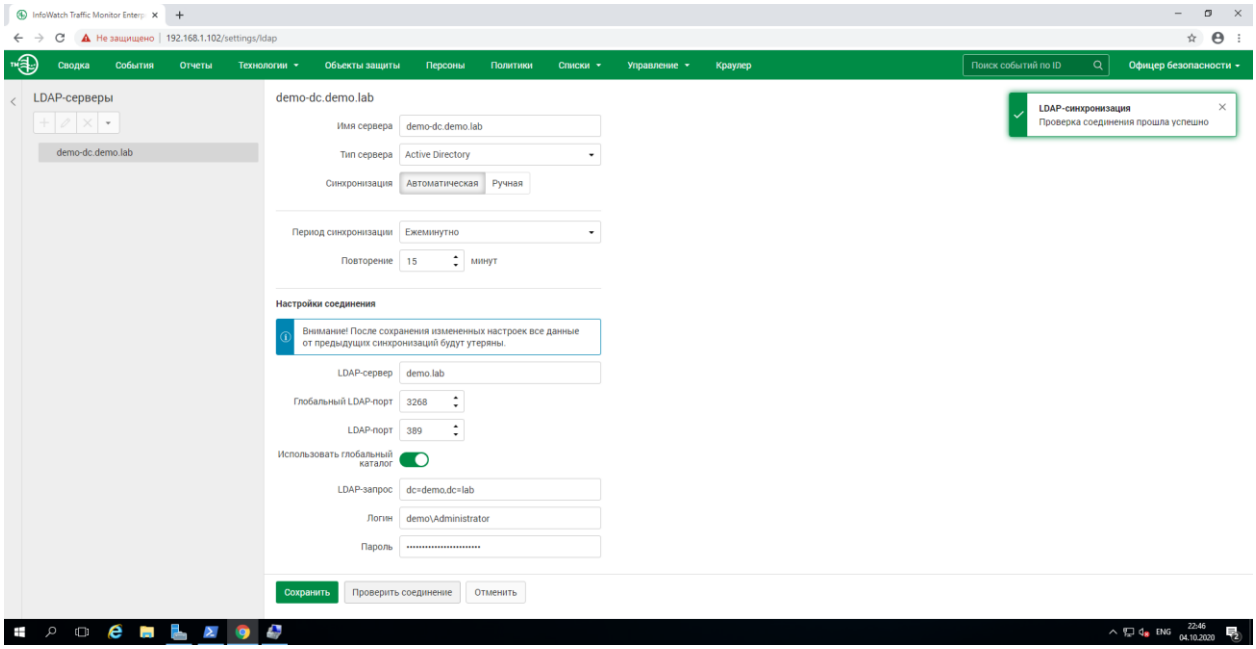
В отчёт вставить скриншоты с выполненной синхронизацией.
Проверить синхронизацию политик ТМ. Вставить скриншот с удачной синхронизацией.

Эталон ответа:

Скриншот с выполненной синхронизацией:

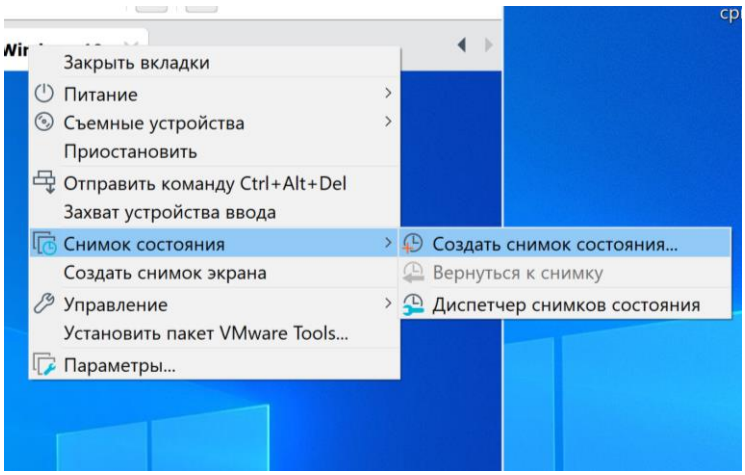


LDAP-синхронизация:



6. Практическое занятие № 20 «Установка клиента Device monitor. Настройка периметра компании, добавление пользователей и компьютеров в домен»

Задание:



Установить клиент можно тремя способами.

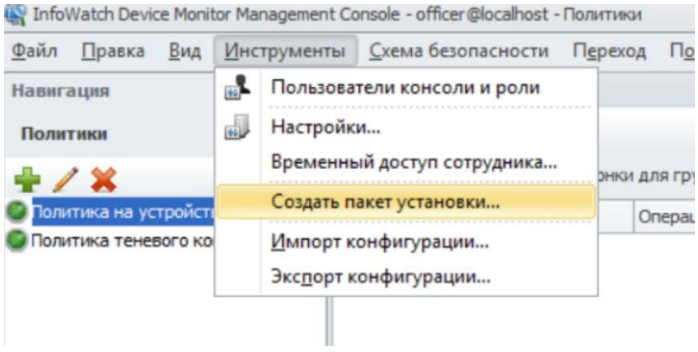
Предпочтительный способ — установка через групповые политики (в отчёте должны быть скриншоты, подтверждающие подобное выполнение).

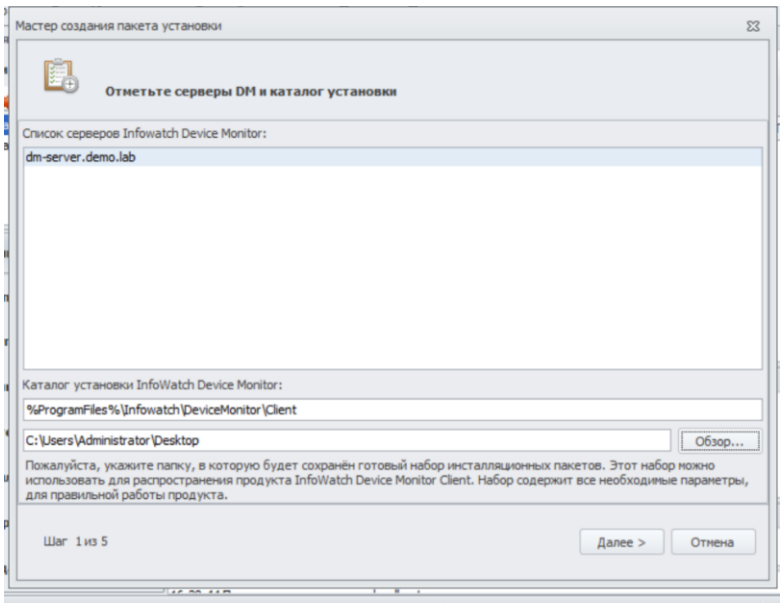
Второй по значимости способ — установка через задачу первичного распространения (в отчёте должны быть скриншоты, подтверждающие подобное выполнение).

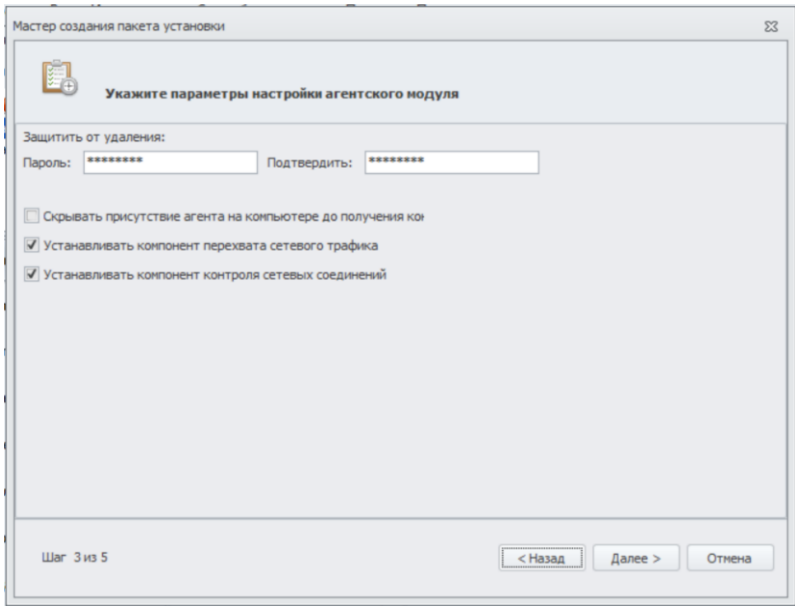
Самый простой способ — установка с помощью пакета установки с последующим переносом его на машину потенциального нарушителя и установки.

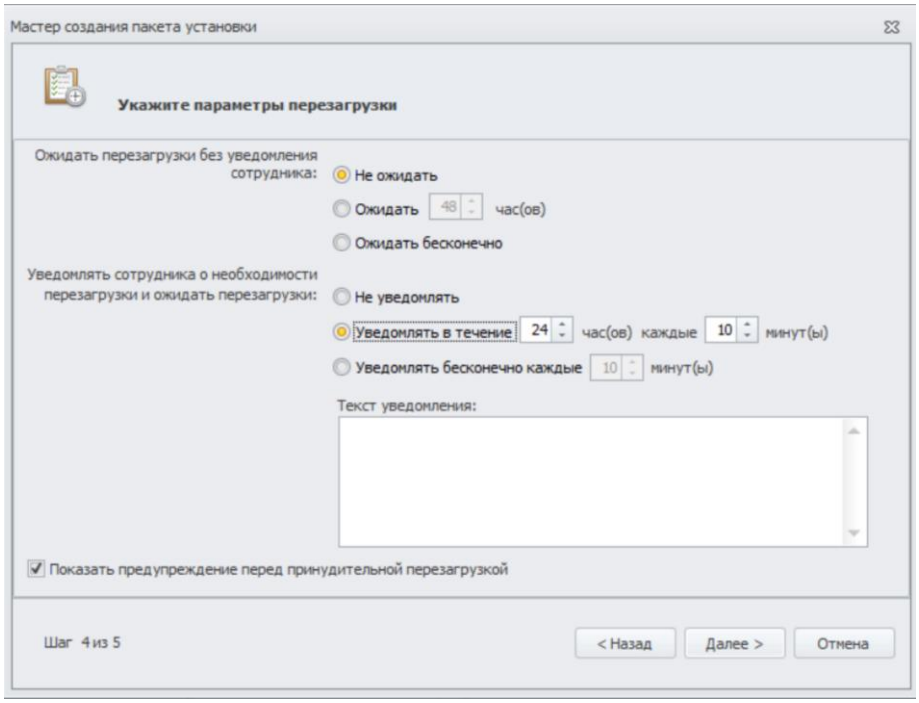
Способ 1 (самый простой и в реальных боевых условиях неправильный) с помощью пакета установки

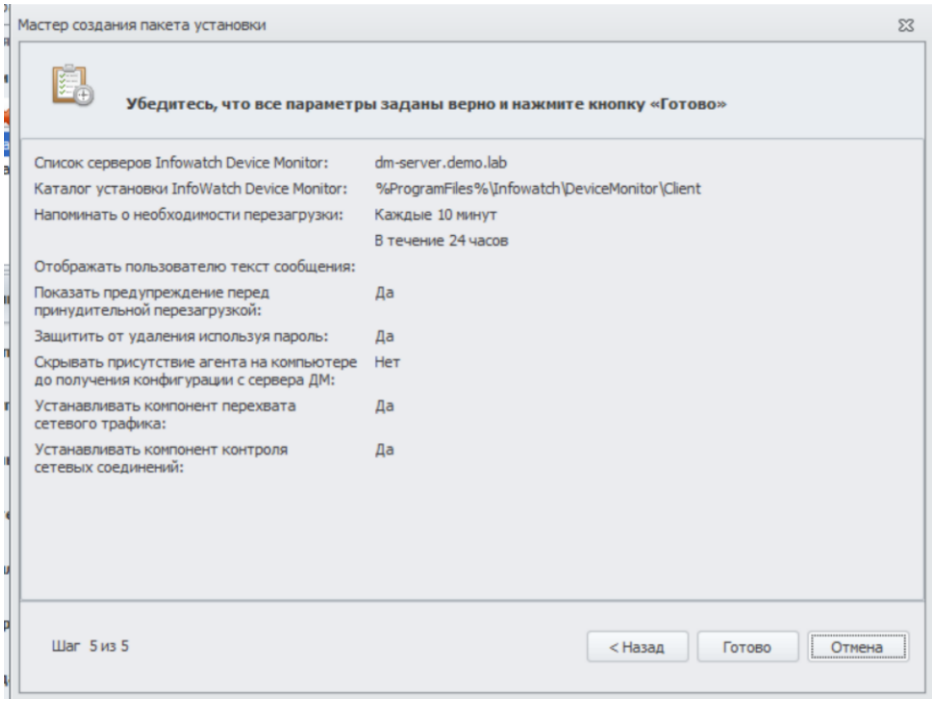
На сервере с iwdm зайти в консоль управления iwdm

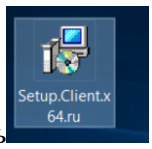



Мастер создания пакета установки
Отметьте серверы DM и каталог установки
Список серверов Infowatch Device Monitor:
dm-server.demo.lab
Каталог установки InfoWatch Device Monitor:
%ProgramFiles%\Infowatch\DeviceMonitor\Client
C:\Users\Administrator\Desktop
Обзор...
Пожалуйста, укажите папку, в которую 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

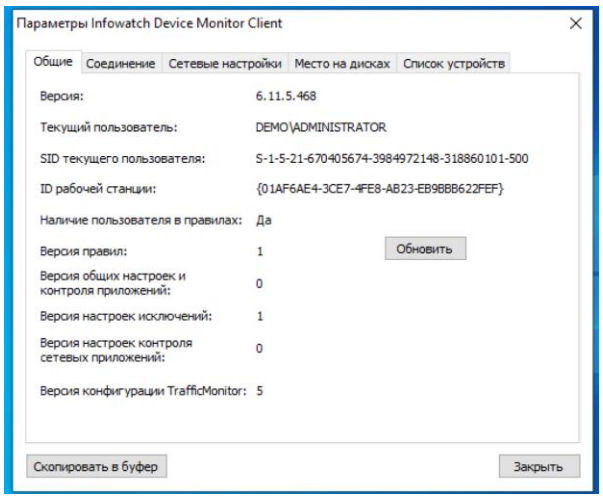

Мастер создания пакета установки
Укажите параметры настройки агентского модуля
Защитить от удаления:
Пароль:
****
Подтвердить:
****
Скрывать присутствие агента на компьютере до получения ко
Устанавливать компонент перехвата сетевого трафика
Устанавливать компонент контроля сетевых соединений
Шаг 3 из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





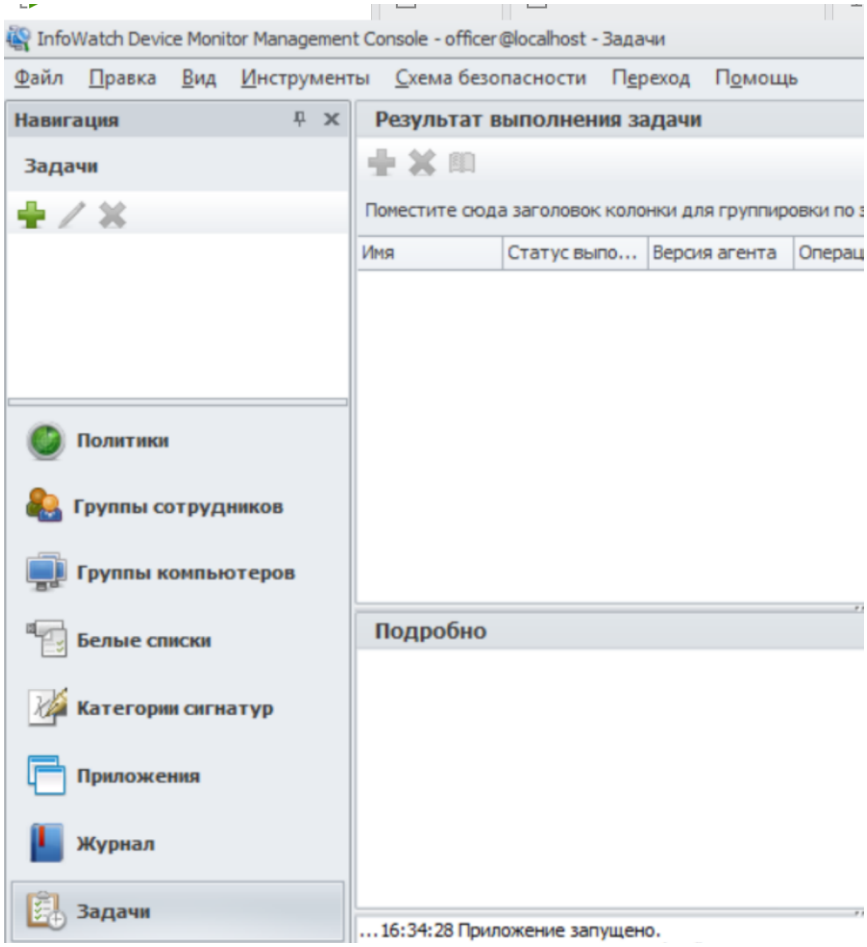
Скопировать на машину нарушитель и запустить 

Должно установиться и в системном трее можете увидеть:

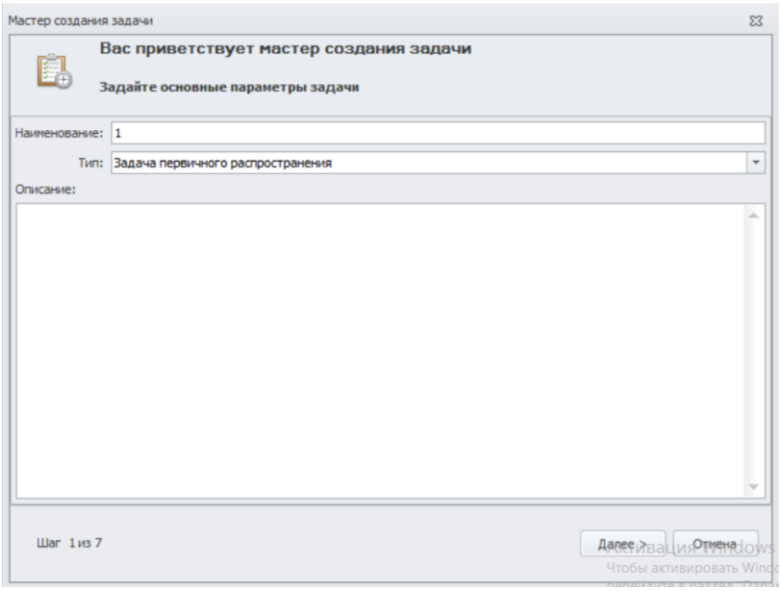


Способ 2 — установка через задачу первичного распространения

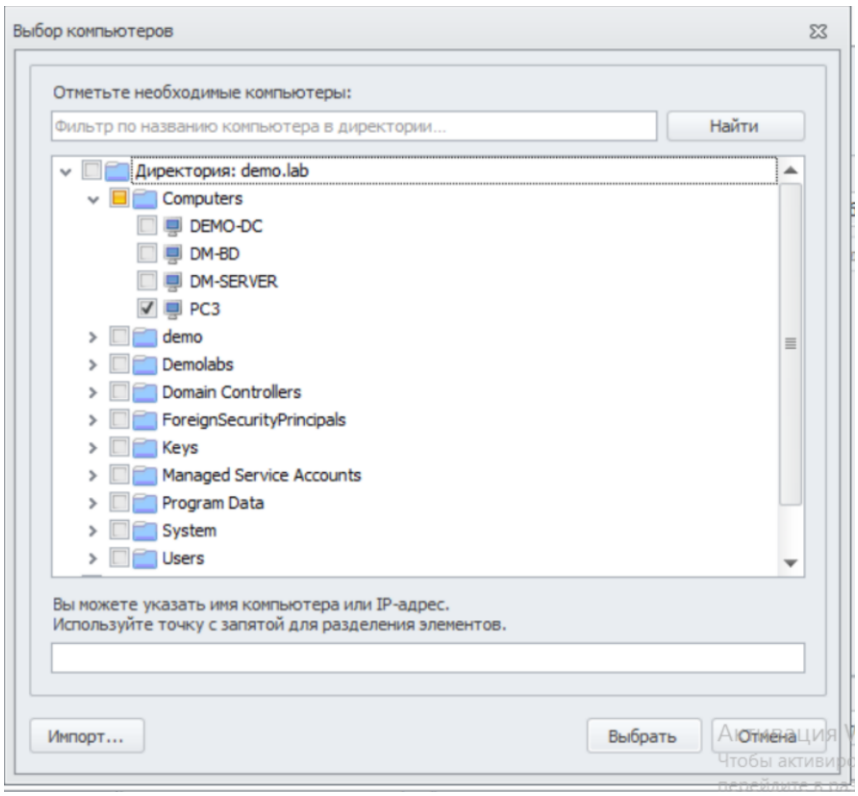
В консоле управления iwdm выбрать Задачи:

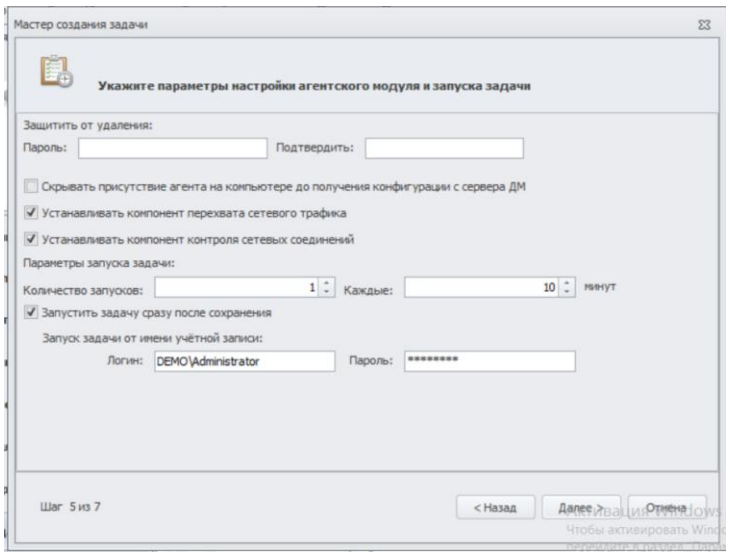


Создать задачу

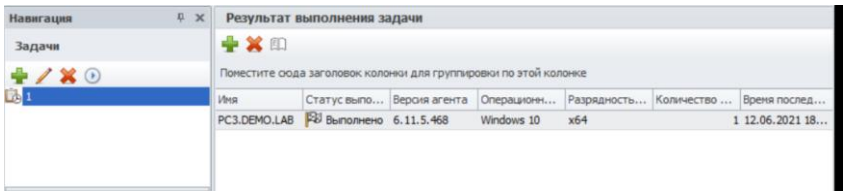


Добавить нужный пк

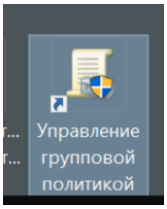




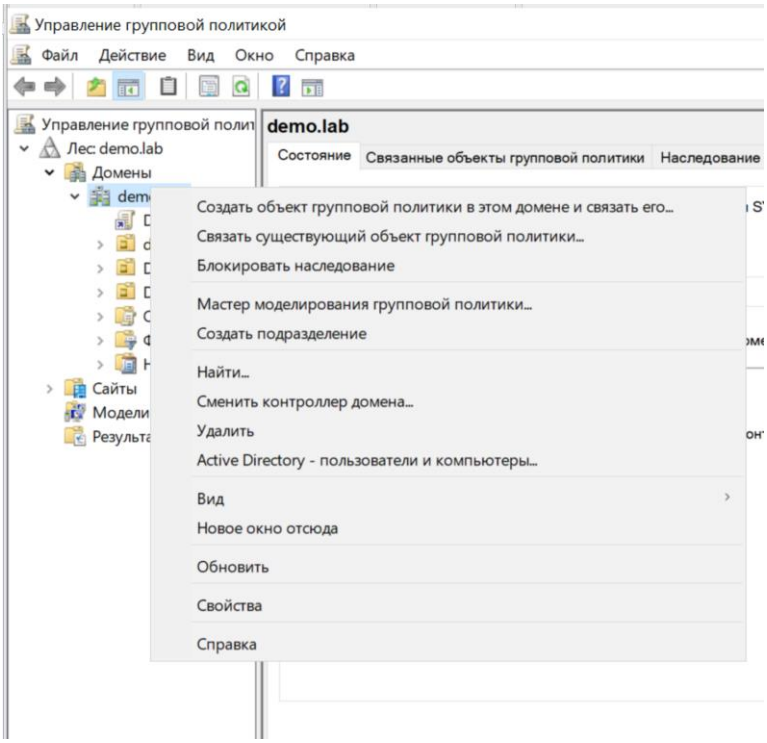
В результате должно быть



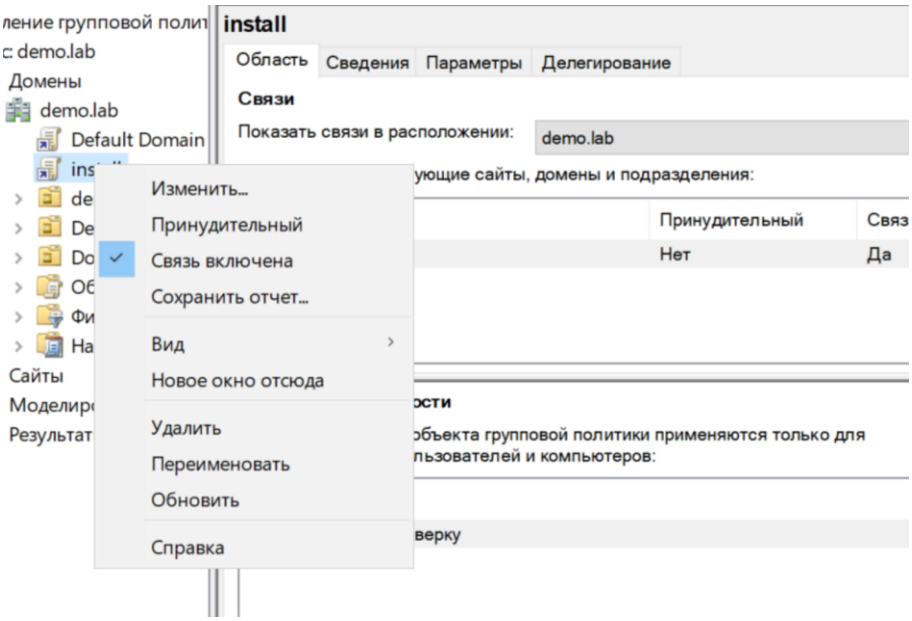
<u>Способ 3 установка через политики AD</u>

На сервере с AD Зайти в 

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

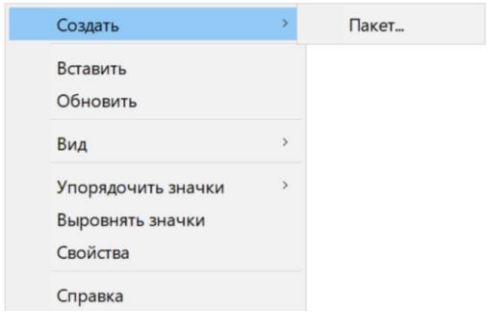


Выбрать Изменить

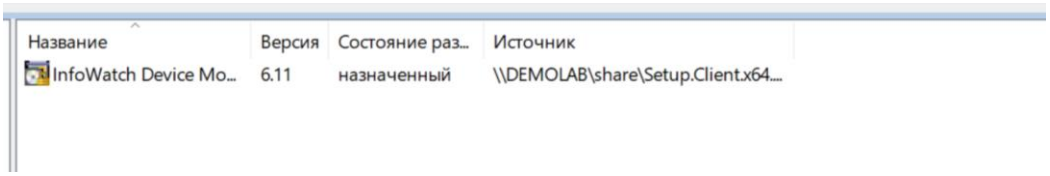


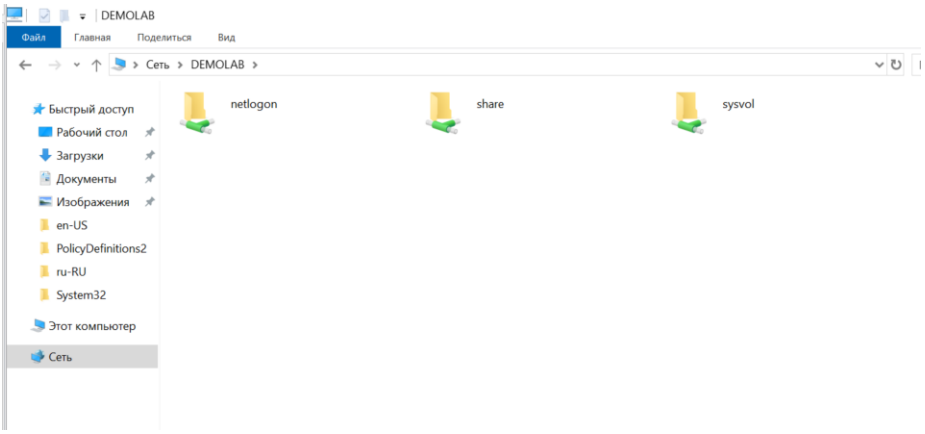
Перейти в

Создать пакет

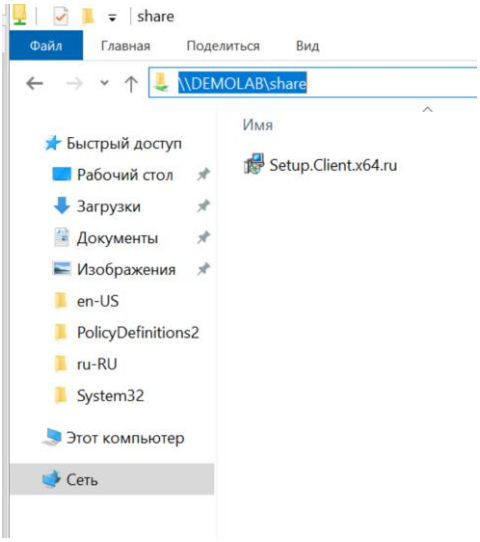


Выбрать msi пакет из 1 способа установки Файл должен быть в общей папке

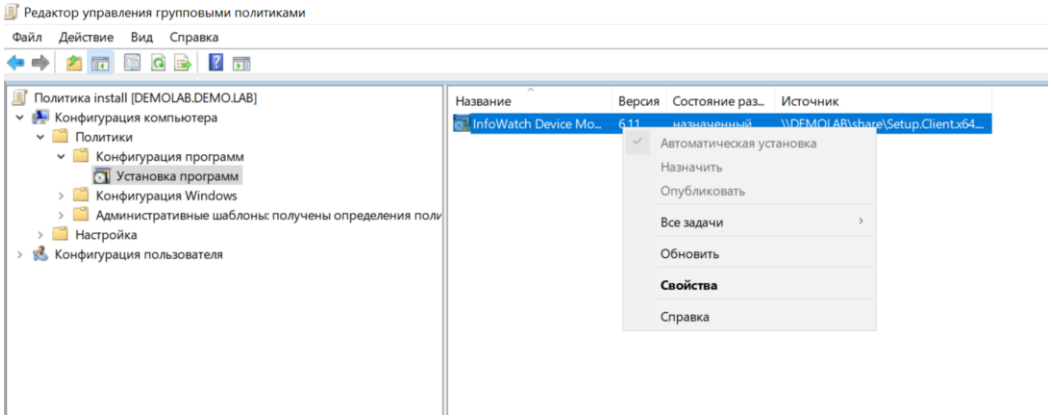




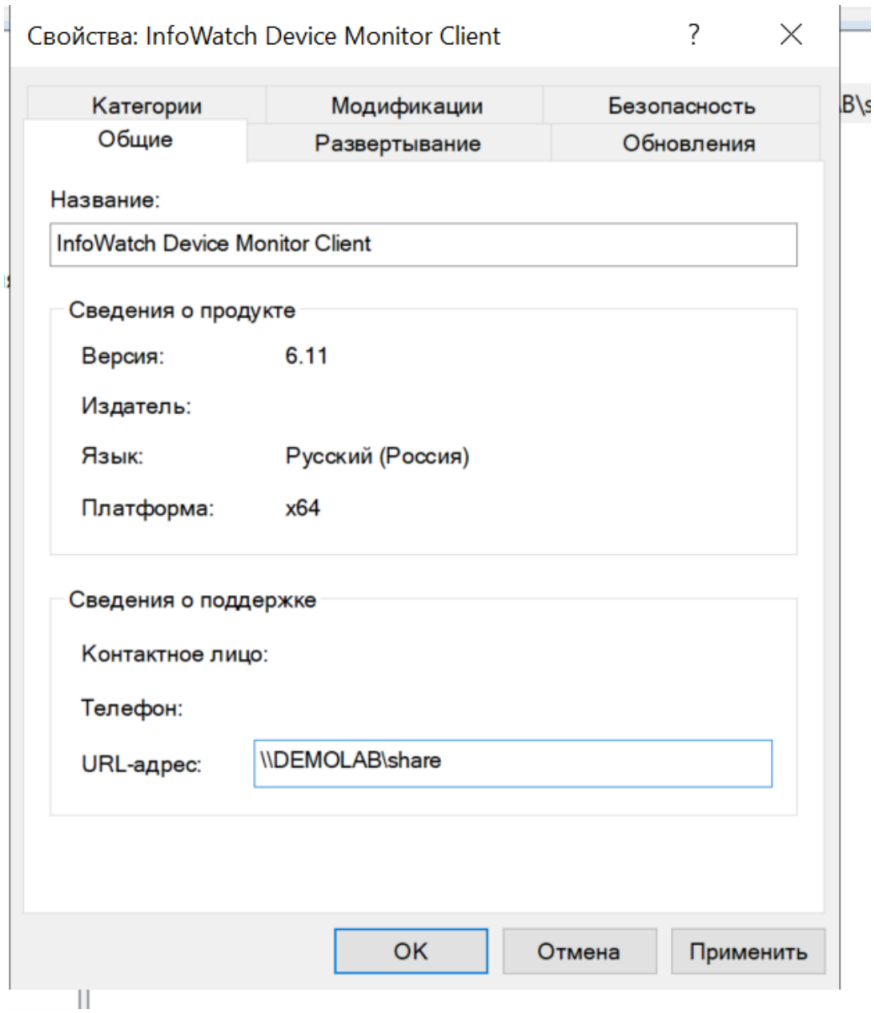
Скопировать адрес до файла установки



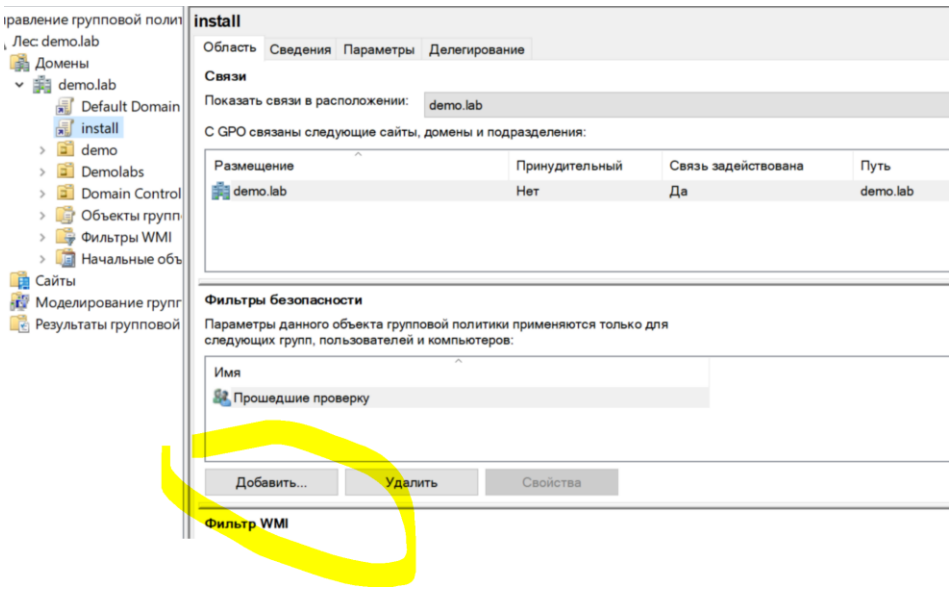
Зайти в свойства пакета

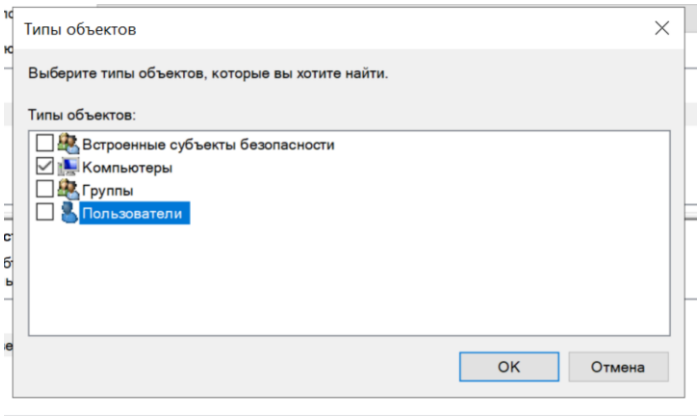


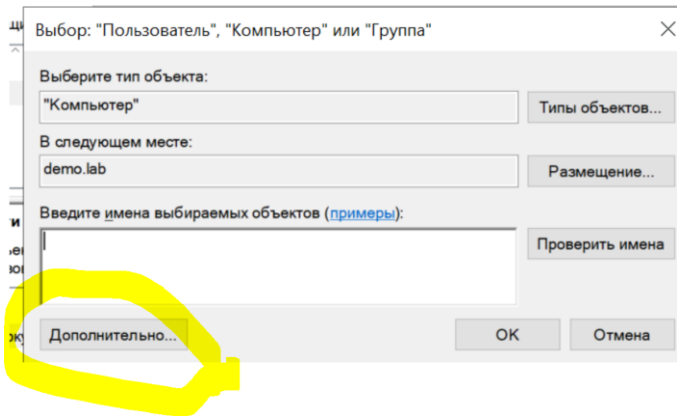
Вставить путь до файла

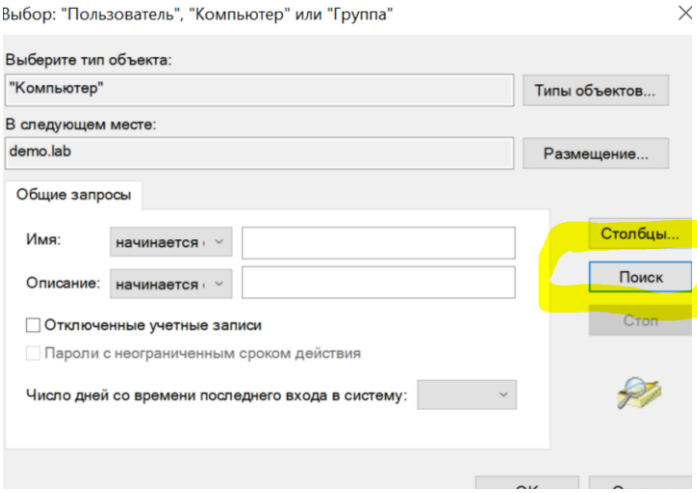


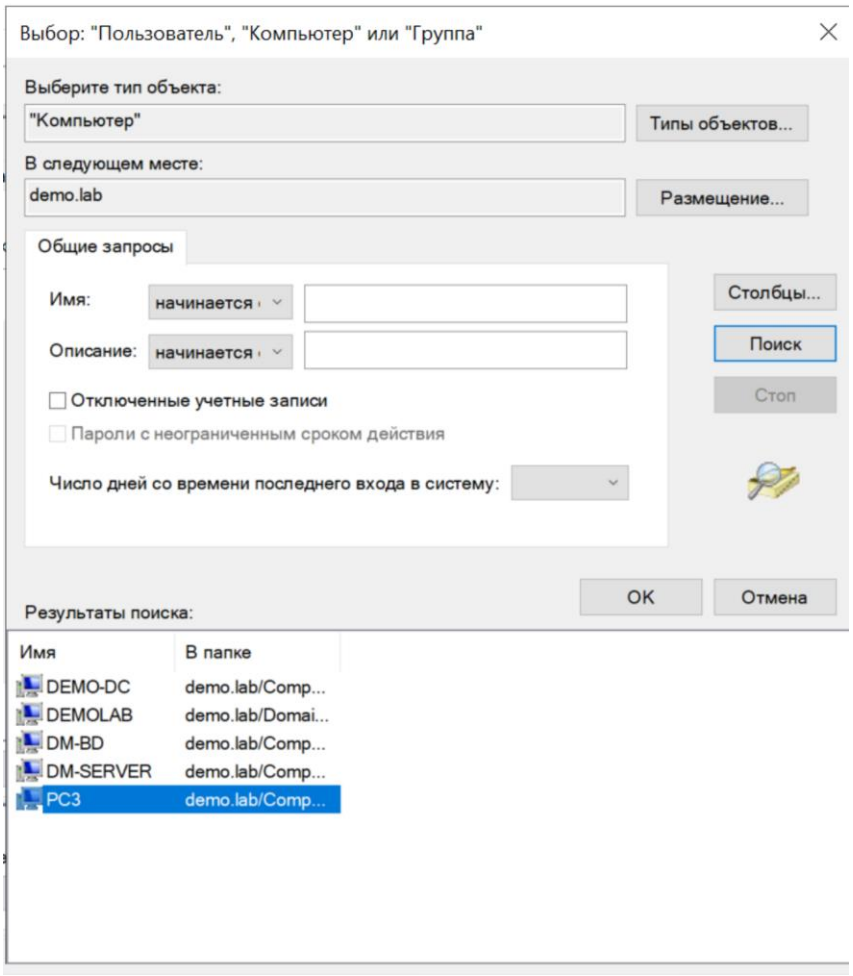
Выйти из редактирования политики, добавить компьютер, на который будет распространяться политика

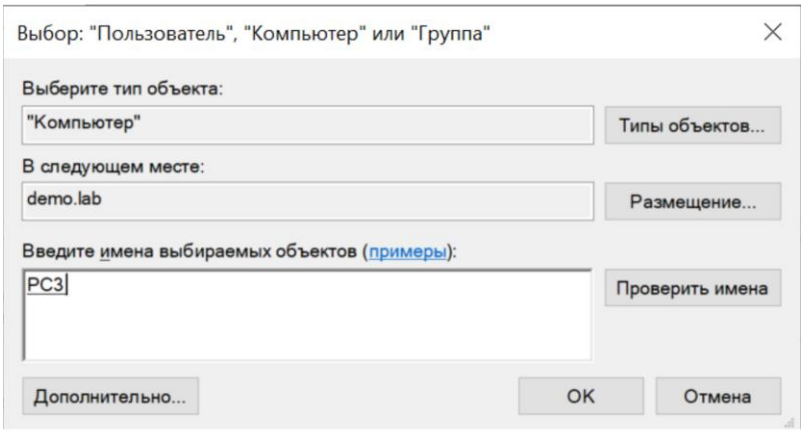

install
Область
Сведения
Параметры
Делегирование
Связи
Показать связи в расположении:
demo.lab
С GPO связаны следующие сайты, домены и подразделения:
Размещение
Принудительный
Связь задействована
Путь
demo.lab
Нет
Да
demo.lab
Фильтры безопасности
Параметры данного объекта групповой политики применяются 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

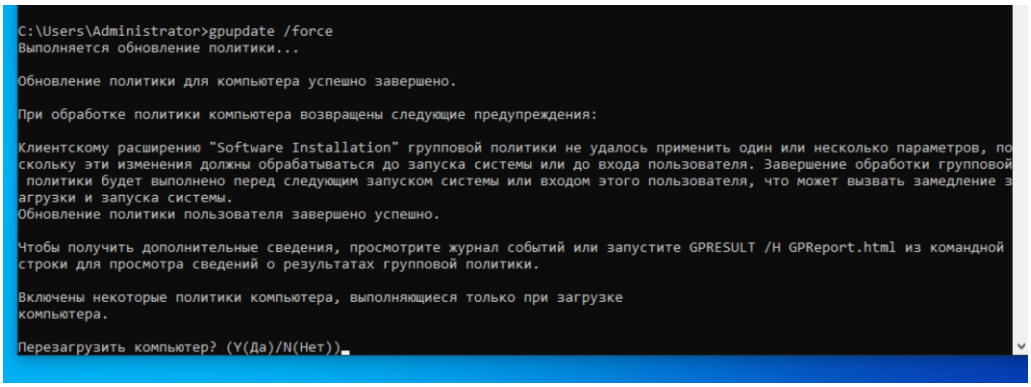

Выбор: "Пользователь", "Компьютер" или "Группа"
Выберите тип объекта:
"Компьютер"
Типы объектов...
В следующем месте:
demo.lab
Размещение...
Введите имена выбираемых объектов (примеры):
Проверить имена
Дополнительно...
OK
Отмена


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:

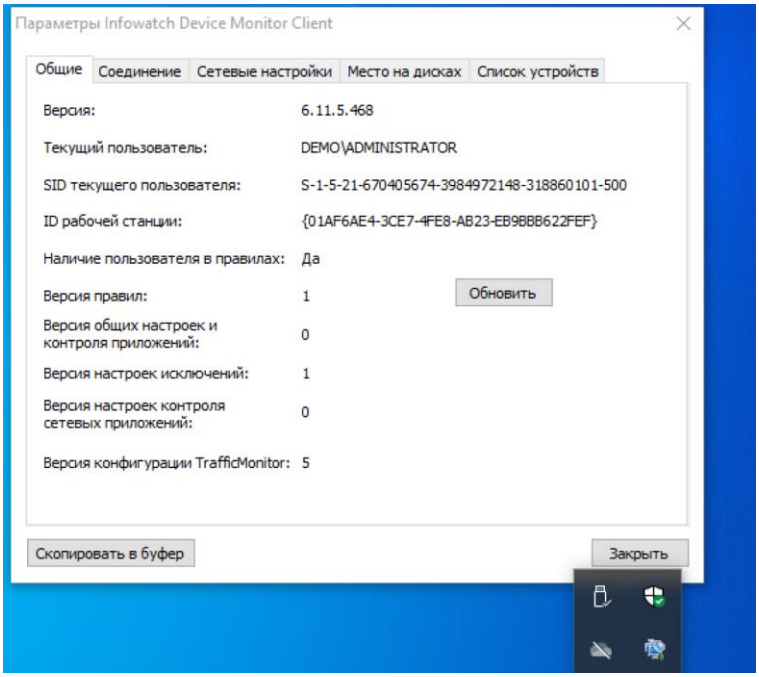

Выбор: "Пользователь", "Компьютер" или "Группа"
Выберите тип объекта:
"Компьютер"
Типы объектов...
В следующем месте:
demo.lab
Размещение...
Общие запросы
Имя:
начинается
Описание:
начинается
Столбцы...
Поиск
Стоп
Отключенные учетные записи
Пароли с неограниченным сроком действия
Число дней со времени последнего входа в систему:
OK
Отмена
Результаты поиска:
Имя
В папке
DEMO-DC
demo.lab/Comp...
DEMOLAB
demo.lab/Domai...
DM-BD
demo.lab/Comp...
DM-SERVER
demo.lab/Comp...
PC3
demo.lab/Comp...



На пк нарушителе выполнить:



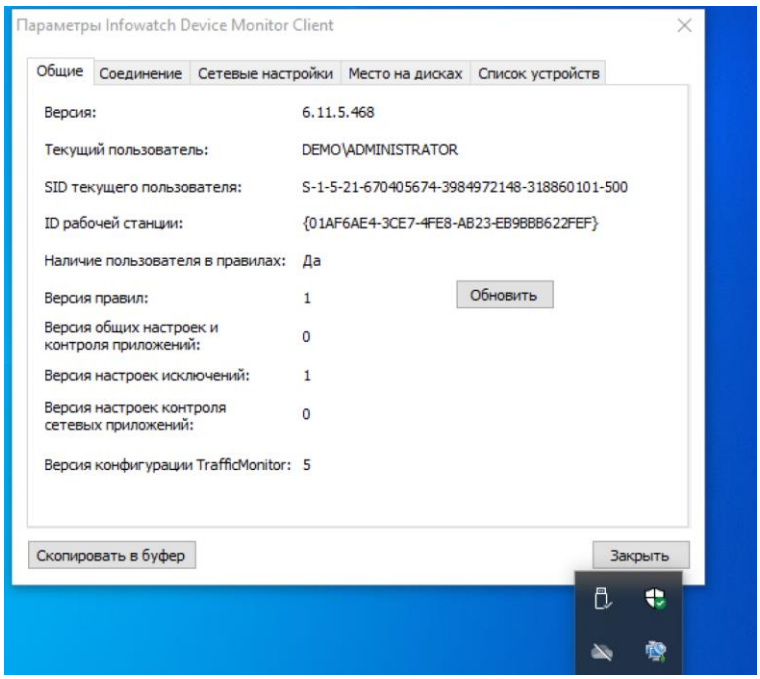
Итогом будет



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

Эталон ответа:

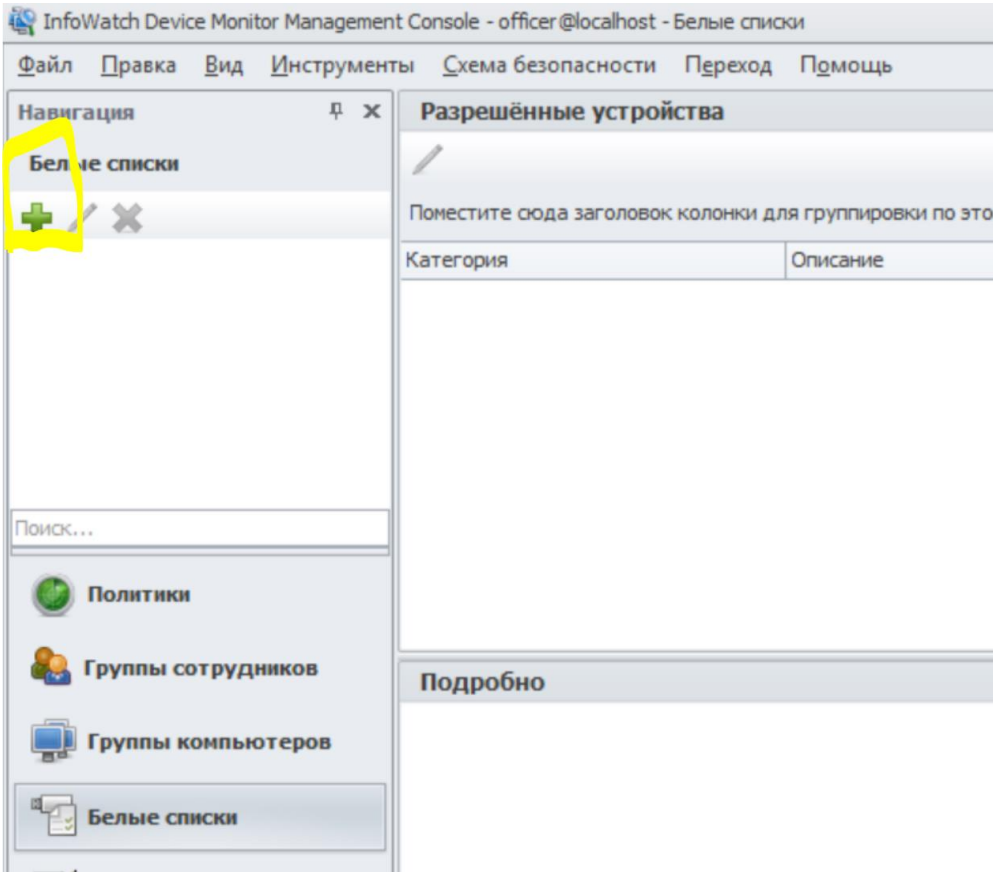
Скриншот с успешной установкой клиента:

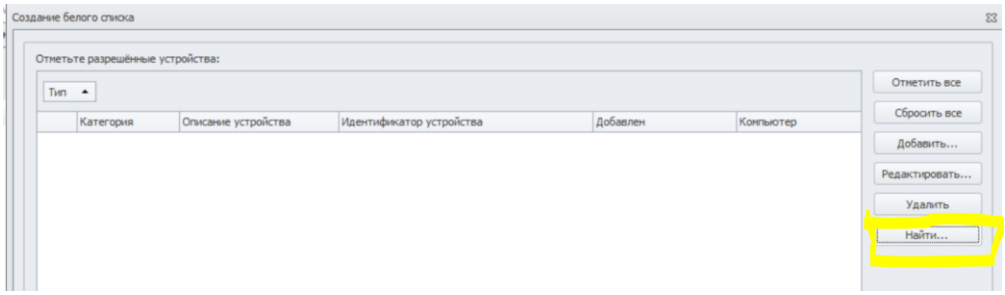


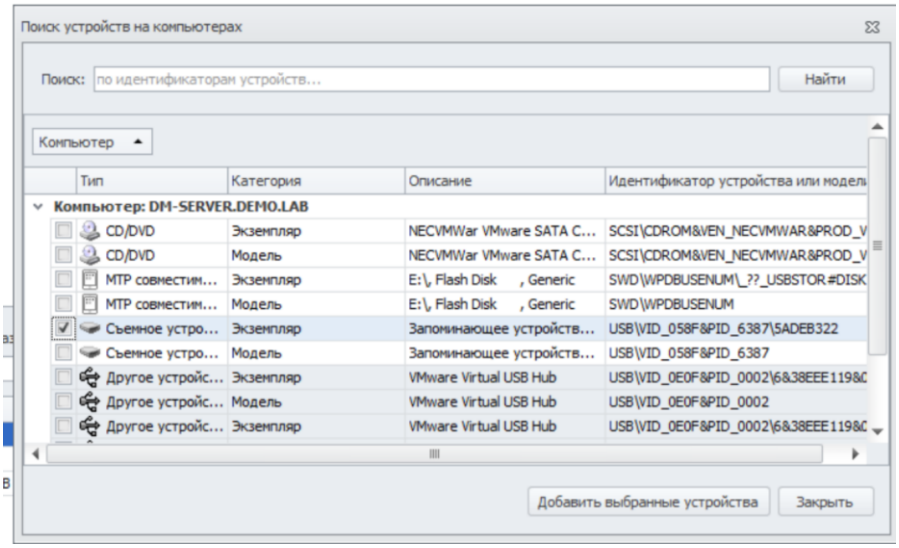
7.Практическое занятие № 23 «Создание правил с использованием «белых» и «чёрных» списков в Device monitor»

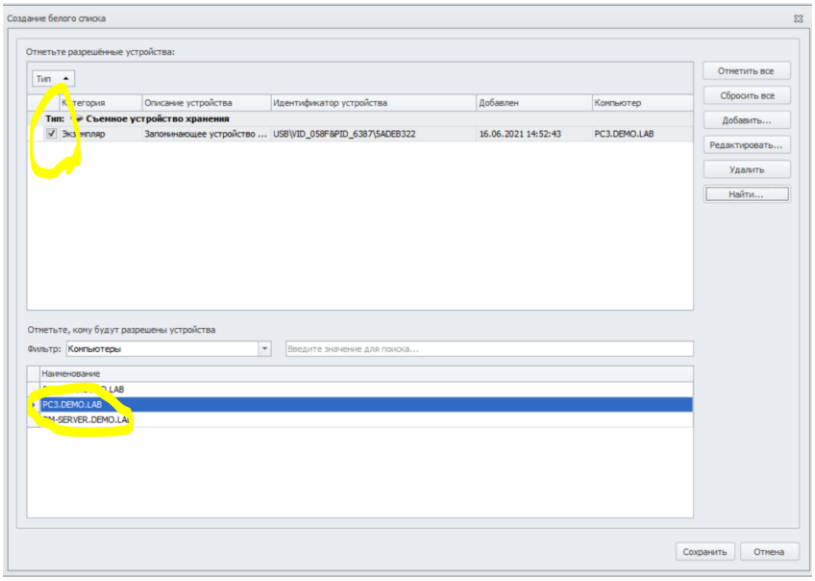
Задание:

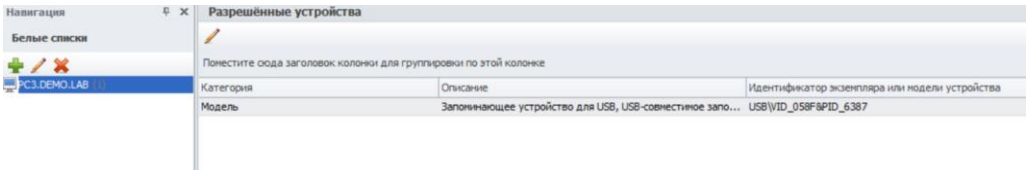
Правило 6. С учетом ранее созданной политики необходимо разрешить запись файлов на доверенный носитель. Запрет на запись на остальные носители оставить в силе. Проверить работоспособность и зафиксировать настройку и выполнение скриншотами.









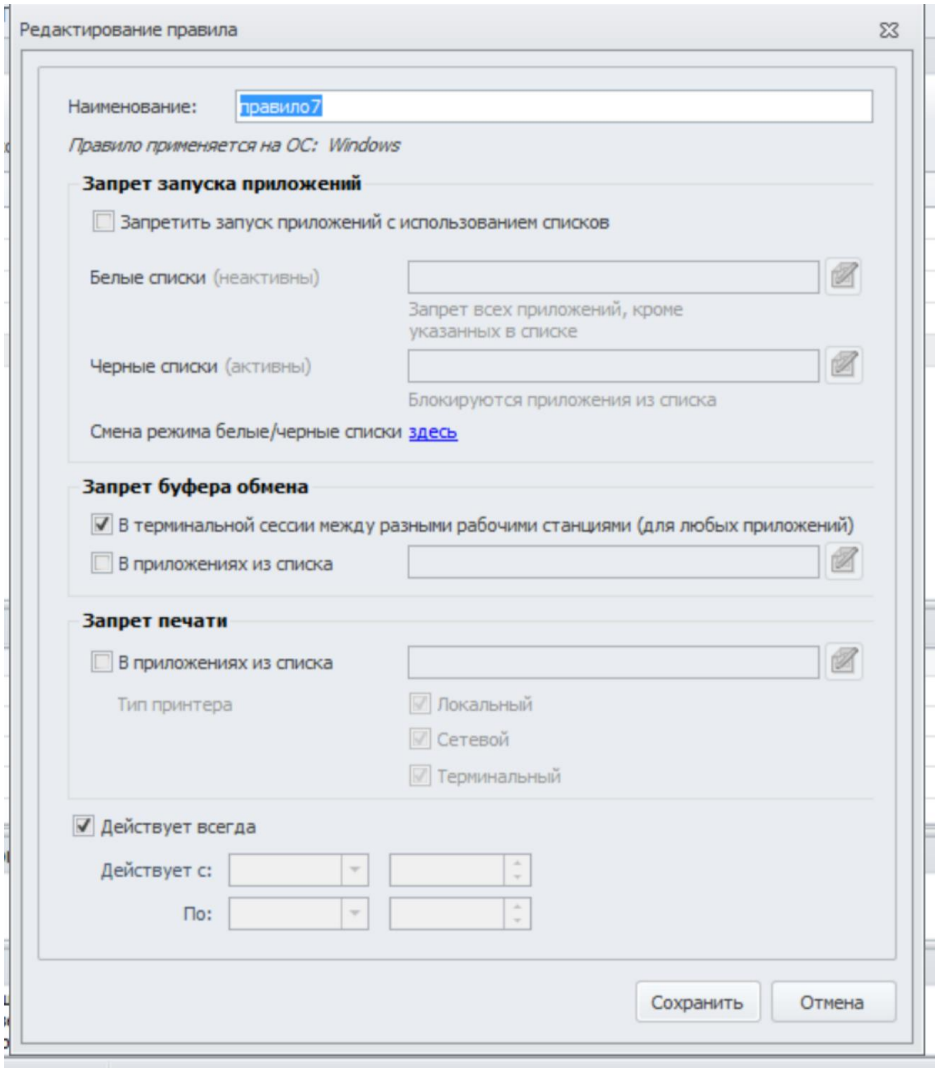


Убедиться в возможности записи на устройство файла.

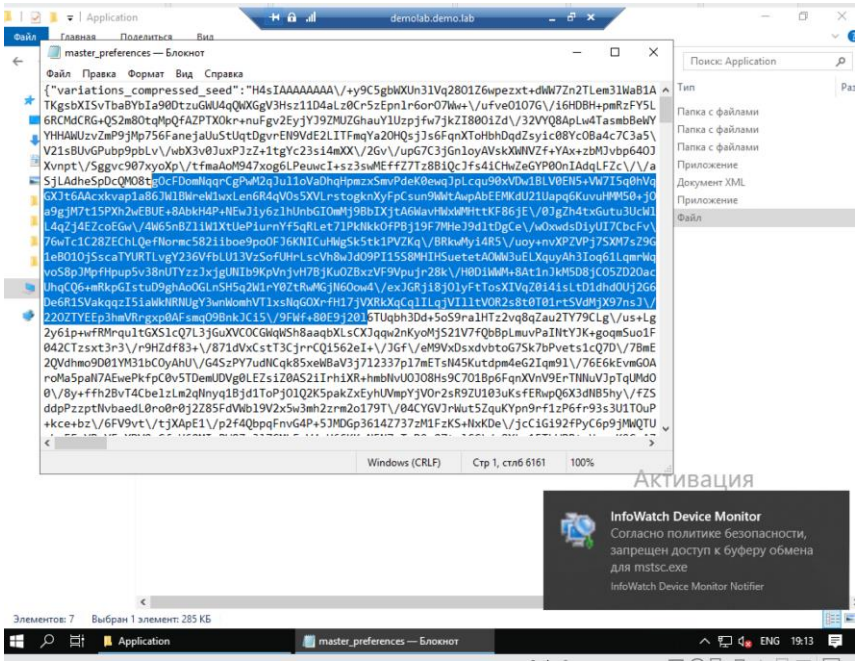
В отчёт вставить скриншоты, подтверждающие создание данного правила, а также скриншот, подтверждающий работоспособность созданного правила.

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.

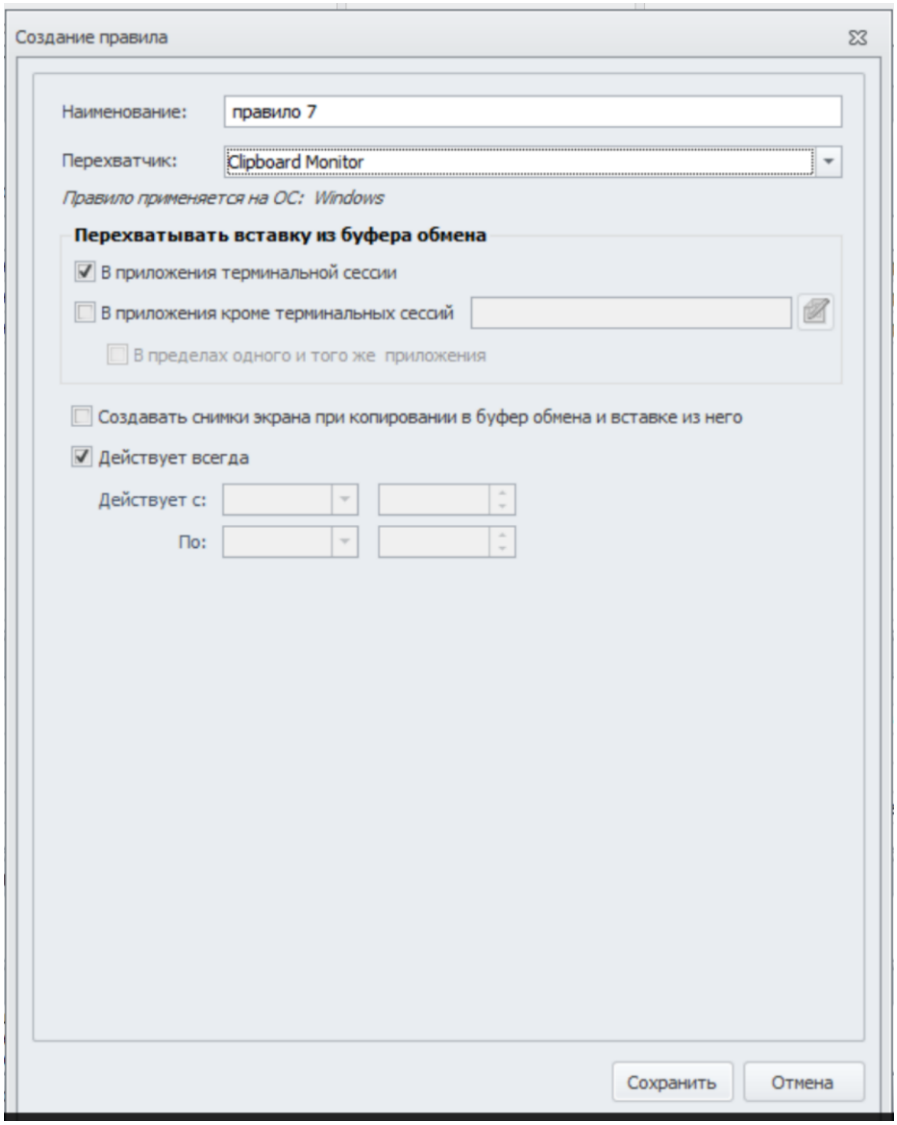


Должно получиться:

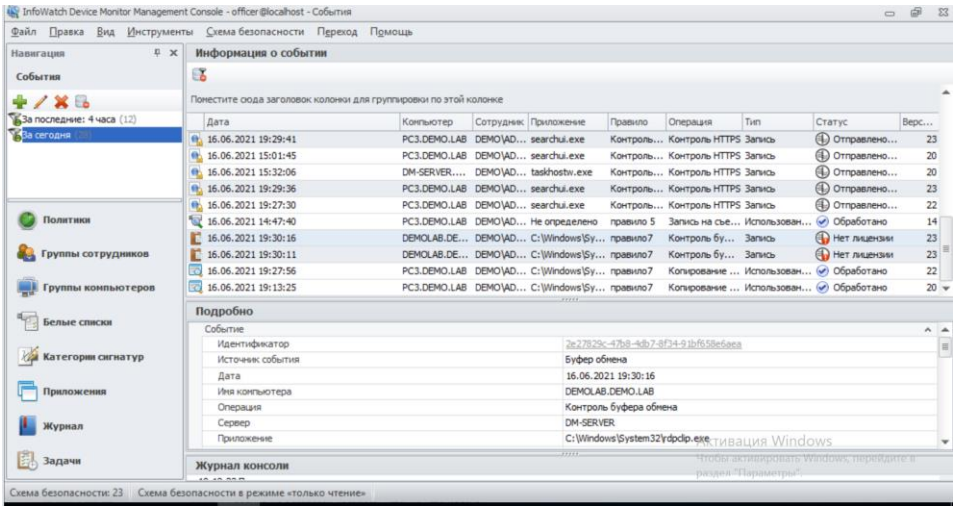


В отчёт вставить скриншоты, подтверждающие создание данного правила, а также скриншот, подтверждающий работоспособность созданного правила.

Удалить правило 7 для выполнения 2 части задания.

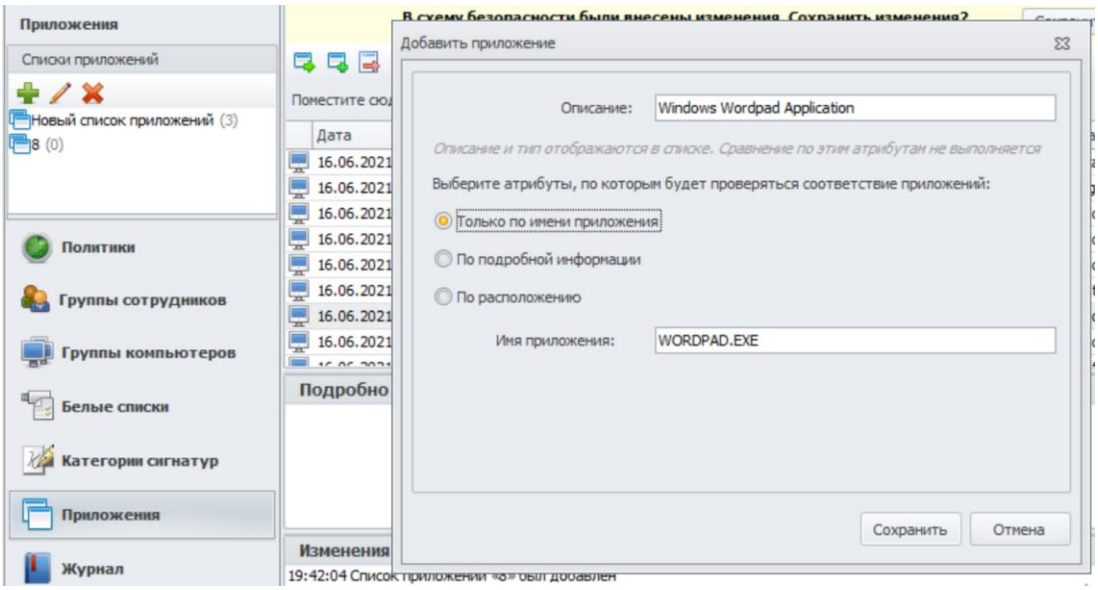


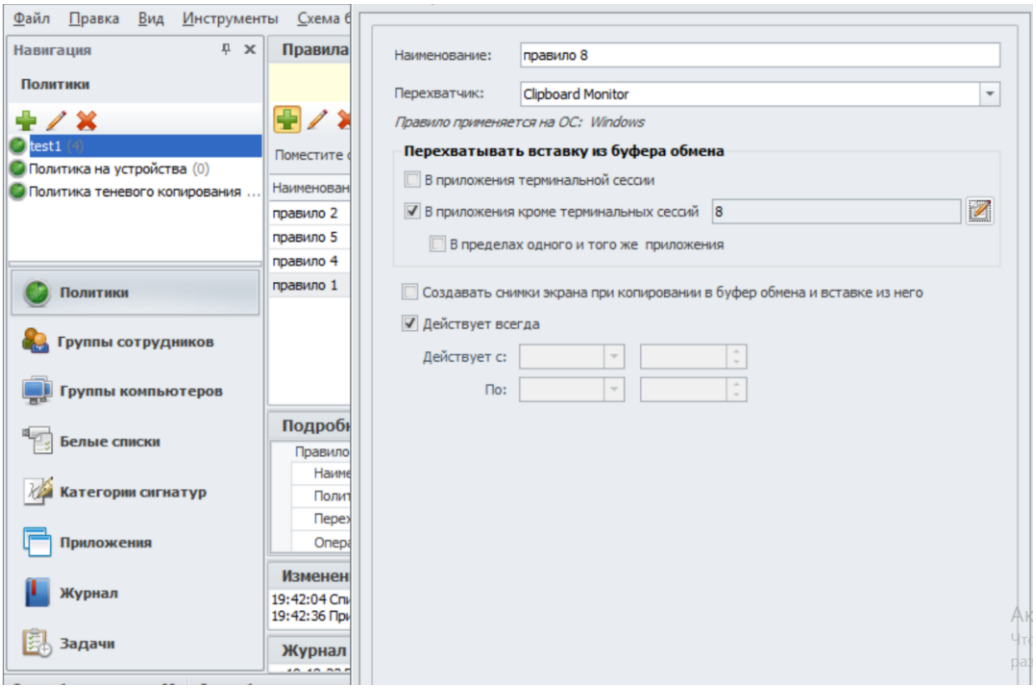
Должны быть события:



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

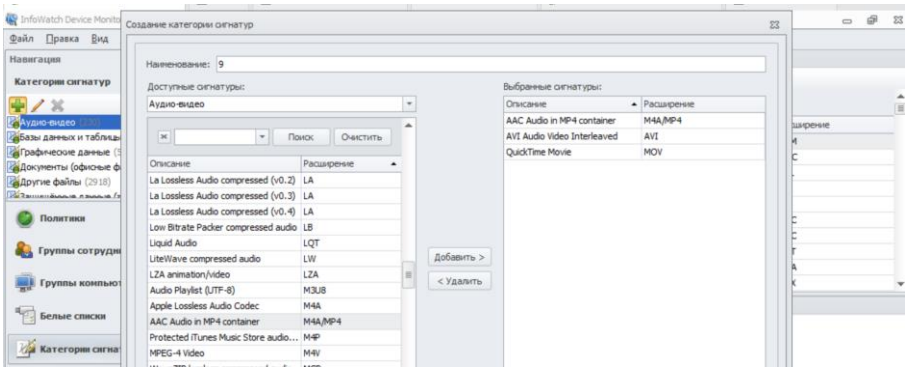
Правило 8. Необходимо поставить на контроль буфер обмена в текстовых процессорах (Word или Writer или Wordpad). Проверить работоспособность и зафиксировать выполнение занесением пары событий в IWTM на любые политики.

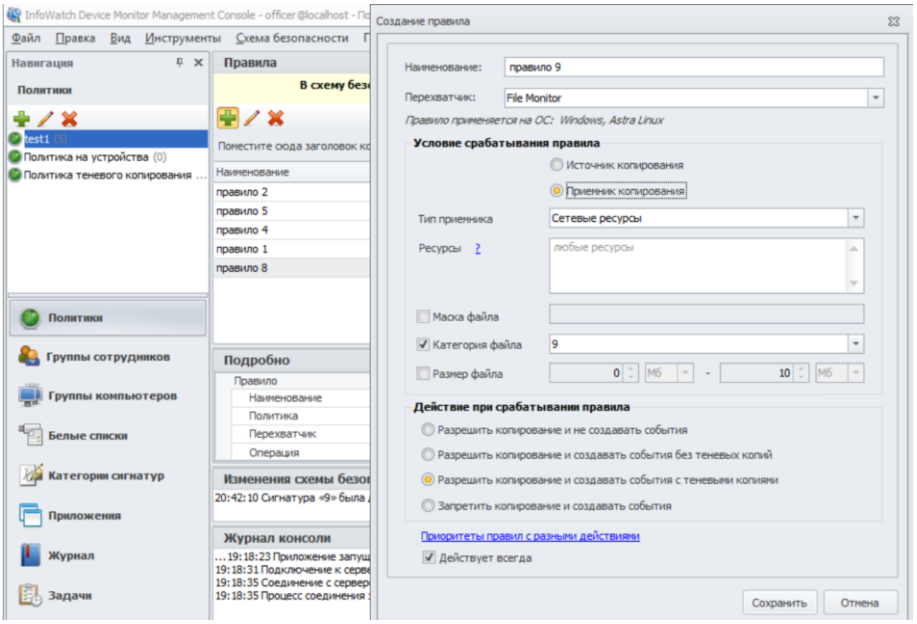


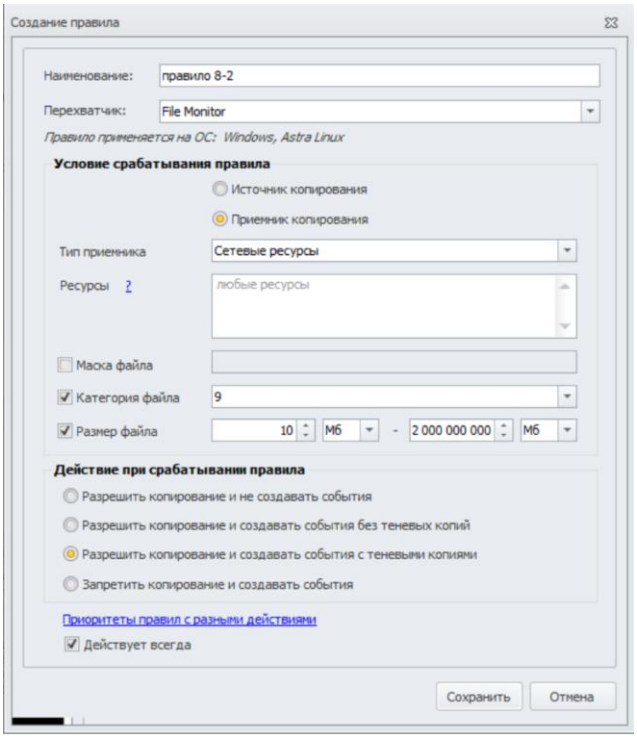


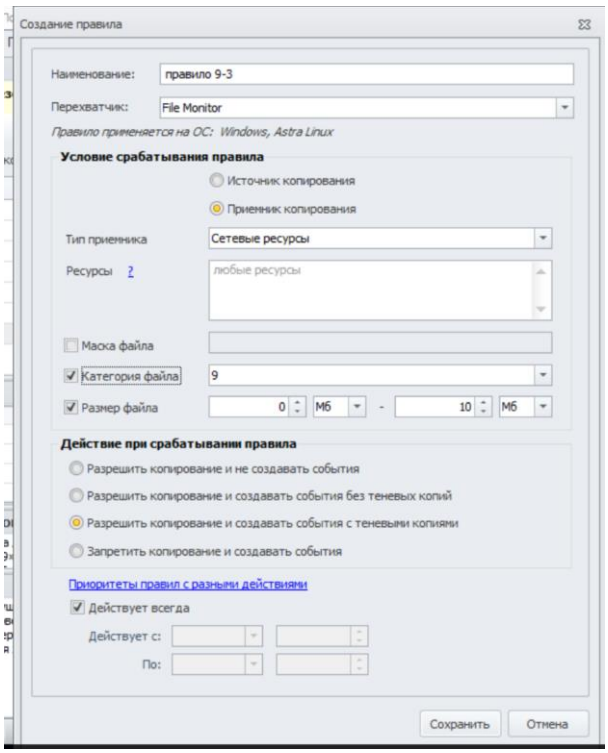
<u>В отчёт вставить скриншоты, подтверждающие создание данного правила, а также скриншот, подтверждающий работоспособность созданного правила.</u>

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


Создание категории сигнатур
Наименование: 9
Доступные сигнатуры:
Аудио-видео
Поиск
Очистить
Описание
Расширение
La Lossless Audio compressed (v0.2) LA
La Lossless Audio compressed (v0.3) LA
La Lossless Audio compressed (v0.4) LA
Low Bitrate Packer compressed audio LB
Liquid Audio LQT
LiteWave compressed audio LW
LZA animation/video LZA
Audio Playlist (UTF-8) M3U8
Apple Lossless Audio Codec M4A
AAC Audio in MP4 container M4A/MP4
Protected iTunes Music Store audio... M4P
MPEG-4 Video M4V
Добавить >
< Удалить
Выбранные сигнатуры:
Описание
Расширение
AAC Audio in MP4 container M4A/MP4
AVI Audio Video Interleaved AVI
QuickTime Movie MOV


Файл Правка Вид Инструменты Схема безопасности
Навигация
Политики
test1 (5)
Политика на устройства (0)
Политика теневого копирования
Правила
правило 2
правило 5
правило 4
правило 1
правило 8
Подробно
Правило
Наименование
Политика
Перехватчик
Операция
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

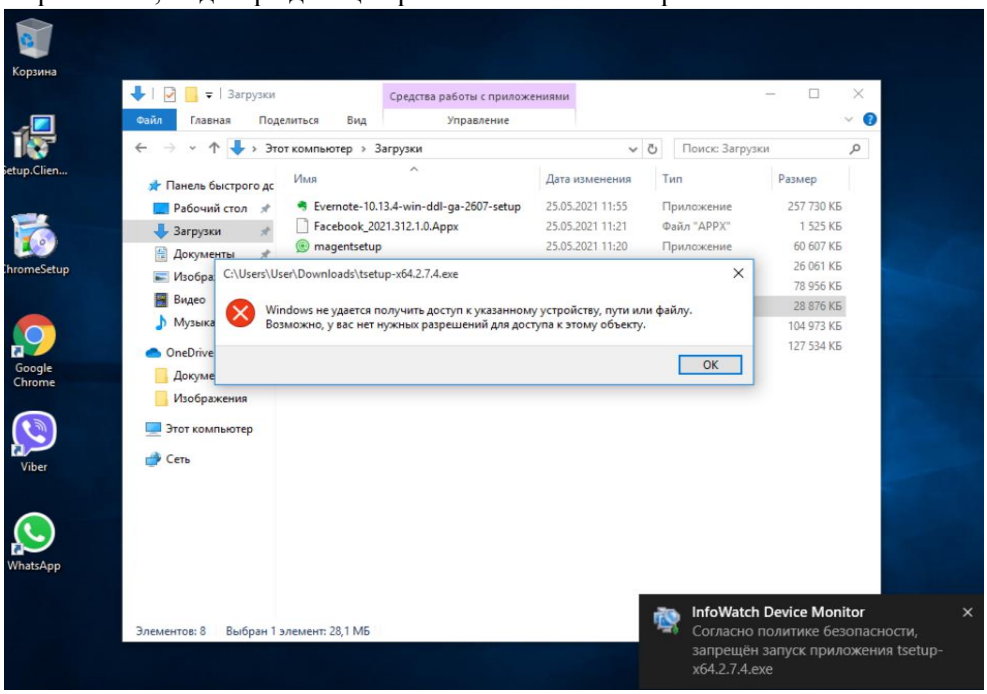

Создание правила
Наименование: правило 8-2
Перехватчик: File Monitor
Правило применяется на ОС: Windows, Astra Linux
Условие срабатывания правила
Источник копирования
Приемник копирования
Тип приемника
Сетевые ресурсы
Ресурсы ?
любые ресурсы
Маска файла
Категория файла 9
Размер файла 10 Мб - 2 000 000 000 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

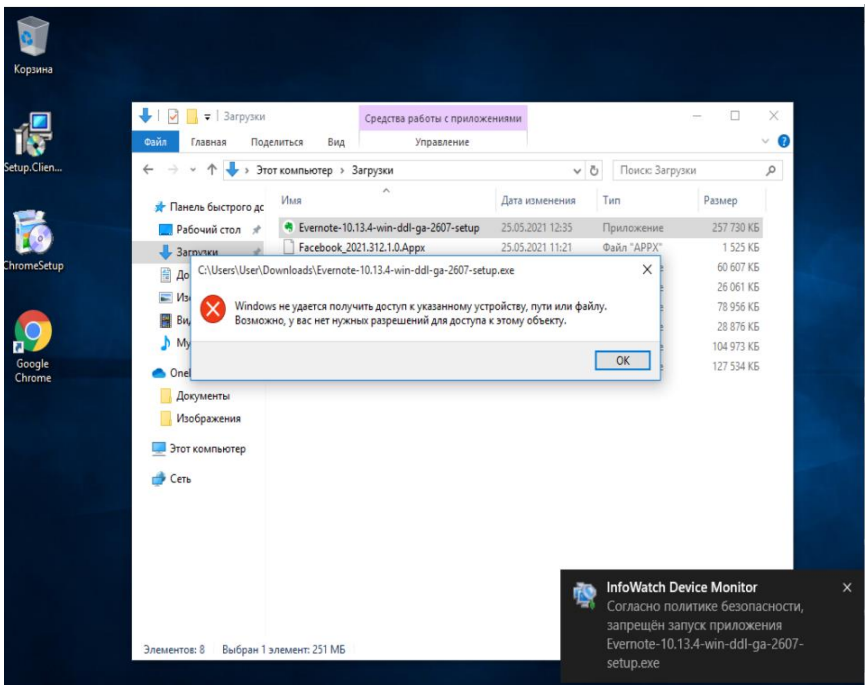


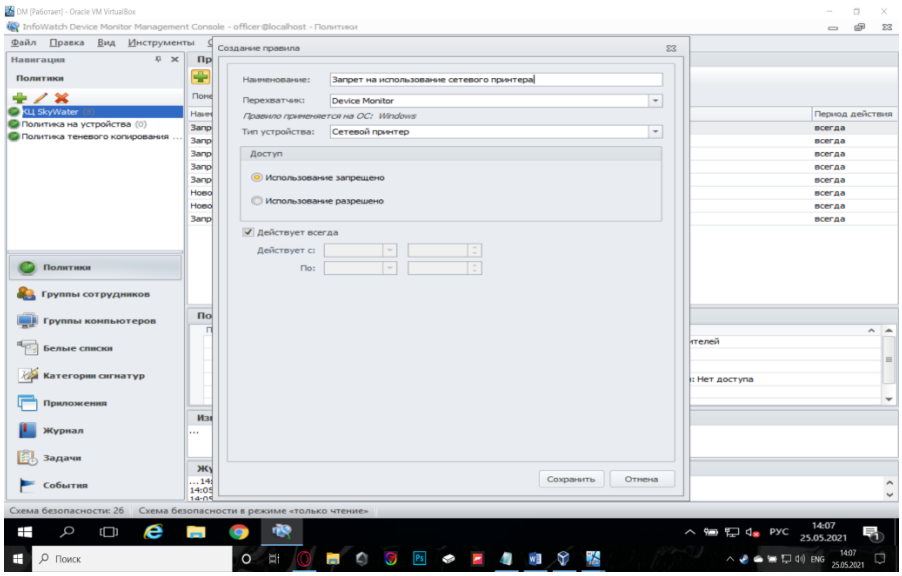
В отчёт вставить скриншоты, подтверждающие создание данного правила, а также скриншот, подтверждающий работоспособность созданного правила.

Эталон ответа:

Скриншоты, подтверждающие работоспособность правил:







8. Практическое занятие № 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. Необходимо импортировать пользователя из Active Directory.
   Чтобы импортировать учетную запись:

- Перейдите в раздел Управление → Управление доступом.
- Перейдите на вкладку Пользователи.
- На панели инструментов нажмите  Добавить пользователя из LDAP.
- Установите флажок для требуемых пользователей.

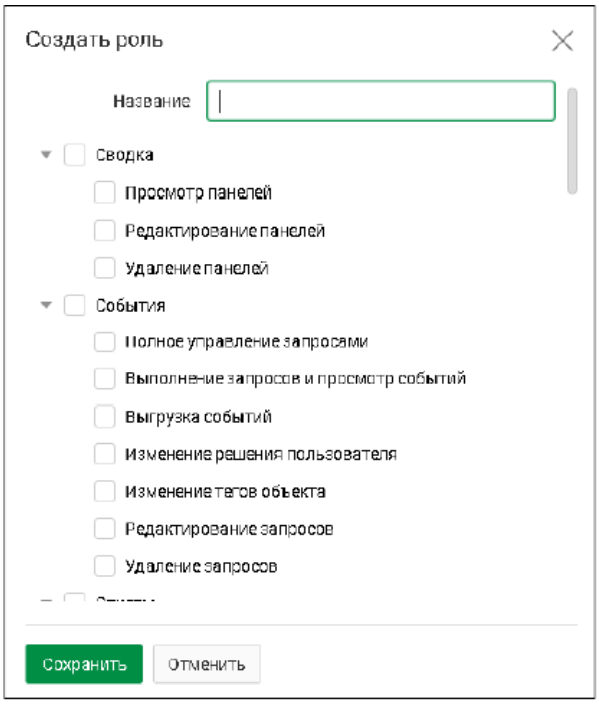
Подтвердите выполнение задания скриншотами.

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

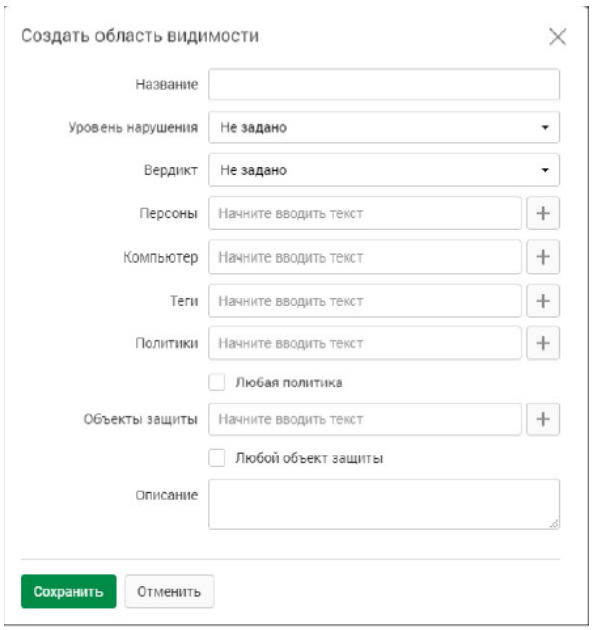
Создайте область видимости, добавьте нового импортированного пользователя.

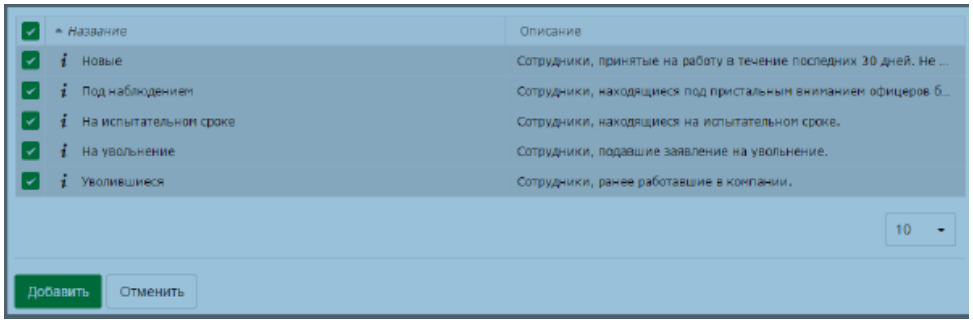
Эталон ответа:

Создание новой роли:



Создание области видимости:





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

Задание:

<u>Политика А</u>

Необходимо поставить на мониторинг все зашифрованные и запароленные данные, т.к. попытки передачи таких данных несут потенциальную опасность утечки.

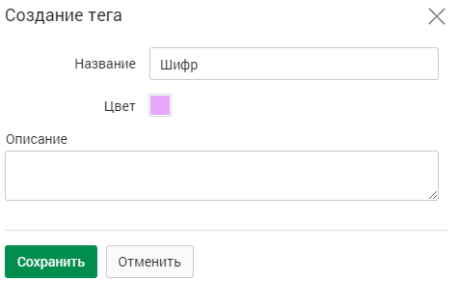
Уровень угрозы низкий, не блокировать, тег «Шифр».

Мониторинг данных

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

Добавление тега

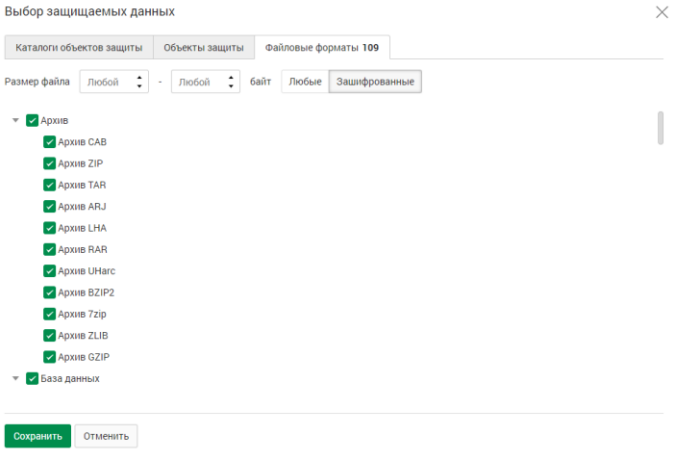
Перейти в раздел «Списки» → «Теги», откроется страница управления тегами. Нажать знак «+», указать название тега «Шифр» и цвет



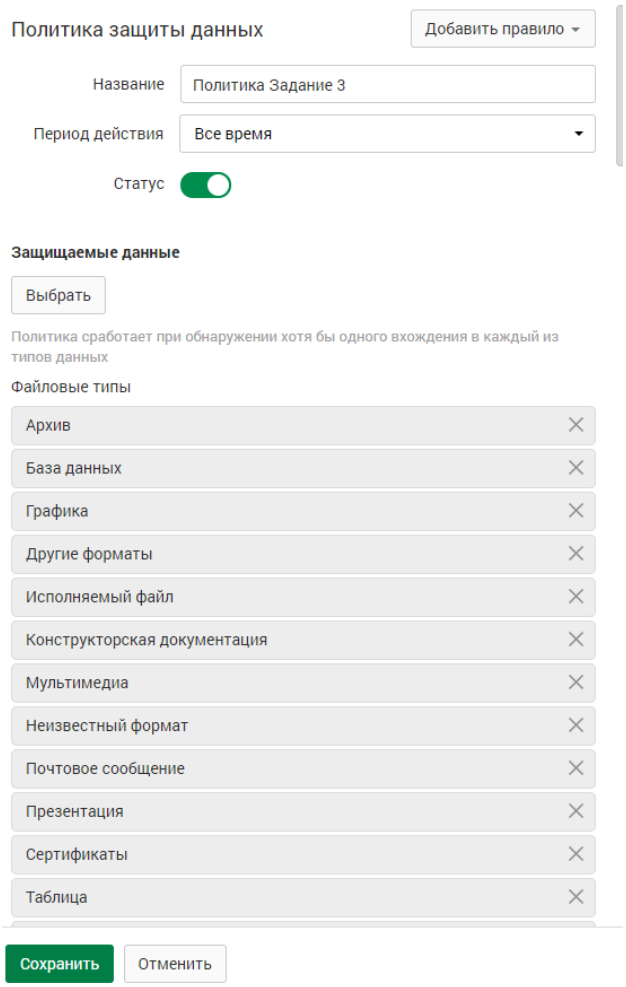
Создание политики

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

файлов

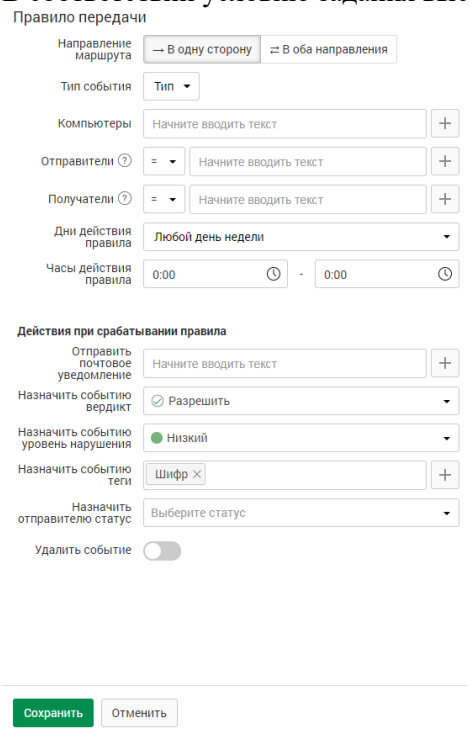


В результате созданная политика выглядит, как представлено:



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»

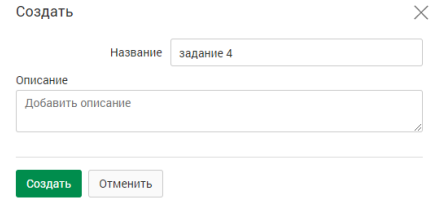
В отчёт вставить скриншот, подтверждающий создание политики.
В отчет вставить скриншот, подтверждающий работоспособность политики.

Политика В

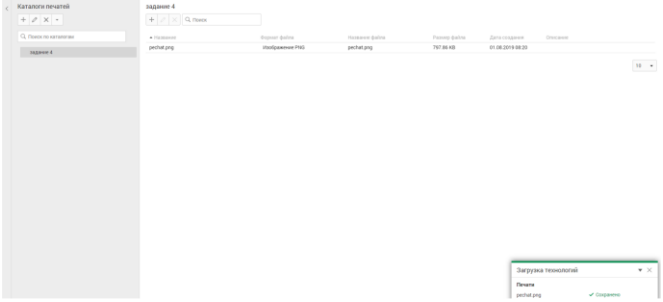
Для контроля за движением официальных документов необходимо вести наблюдение за передачей любых документов с печатями за пределы компании.
Уровень угрозы низкий, не блокировать, тег «Печать».
Для выполнения задания используется файл pechat.png.

Контроль документов с печатями

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

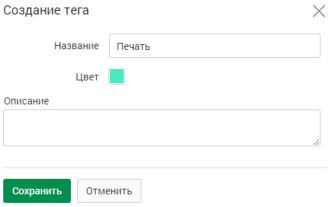


Создания каталога, в котором вводим название и нажимаем «Создать». Затем в самом каталоге снова нажать «+» и выбрать файл с печатью. После этот файл будет загружен в систему и добавлен в каталог



Добавление тега

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



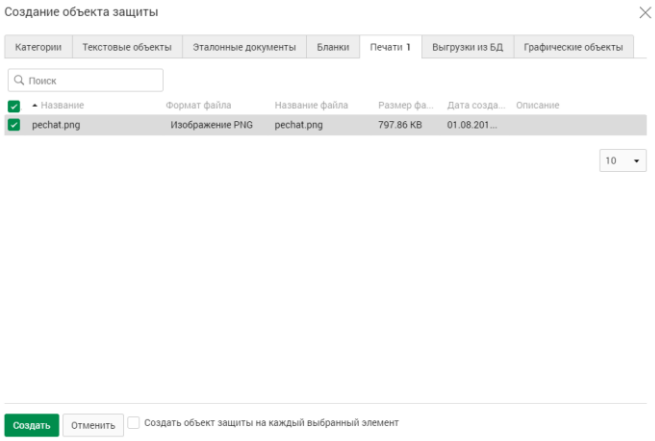
Создание объекта защиты

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

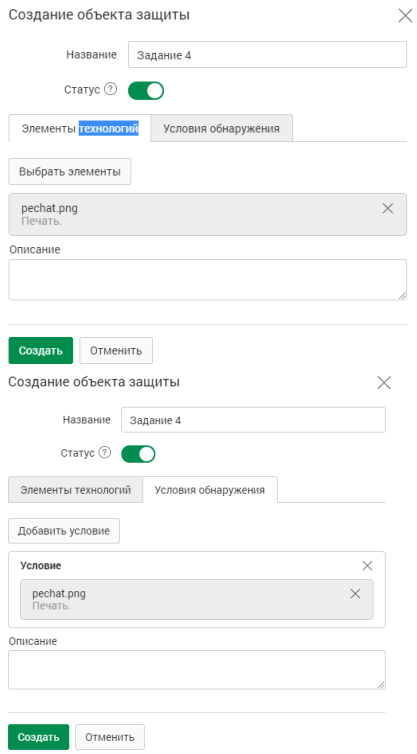
Создать каталог объектов защиты с названием «Задание 4».

Для создания объекта защиты требуется выбрать созданный каталог и нажать знак «+», в появившемся окне:

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

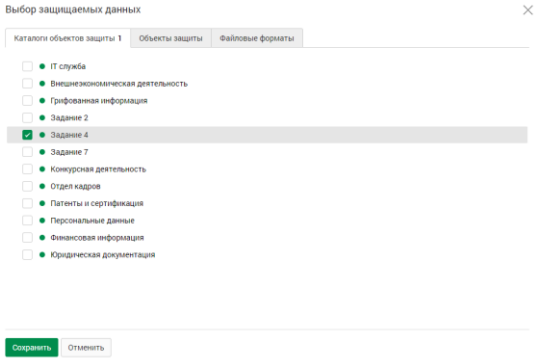


–Нажать «Создать»

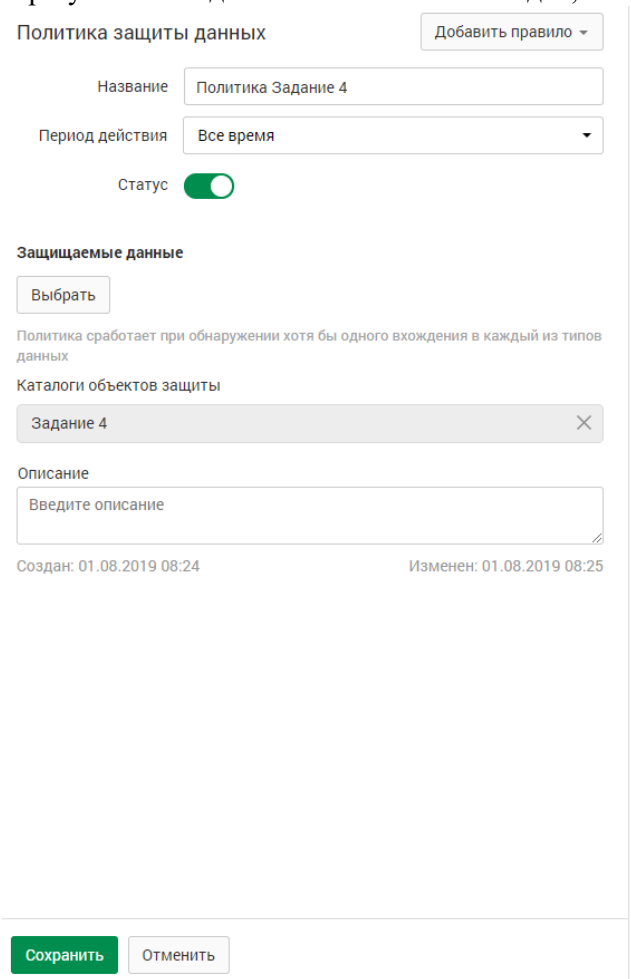


Создание политики

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

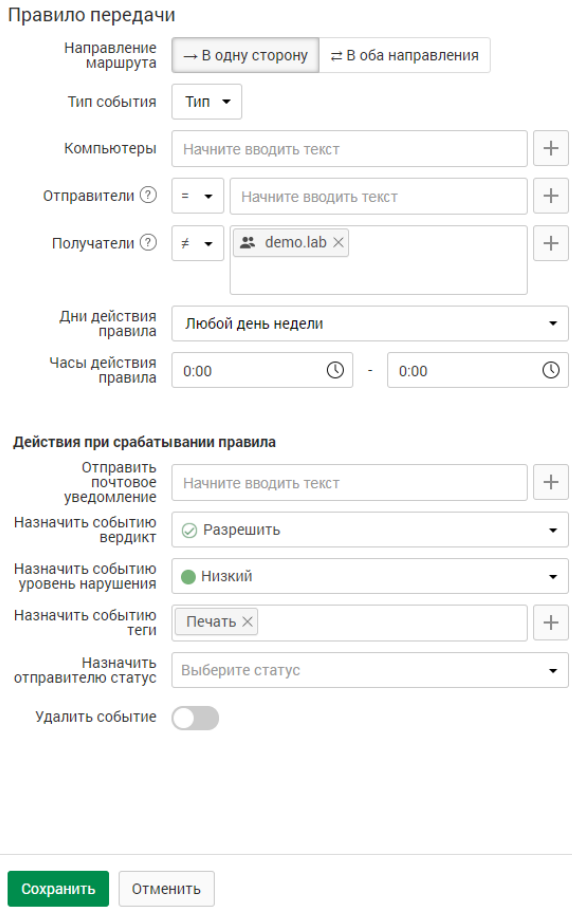


В результате создаваемая политика выглядит, как представлено:



Добавление правила передачи

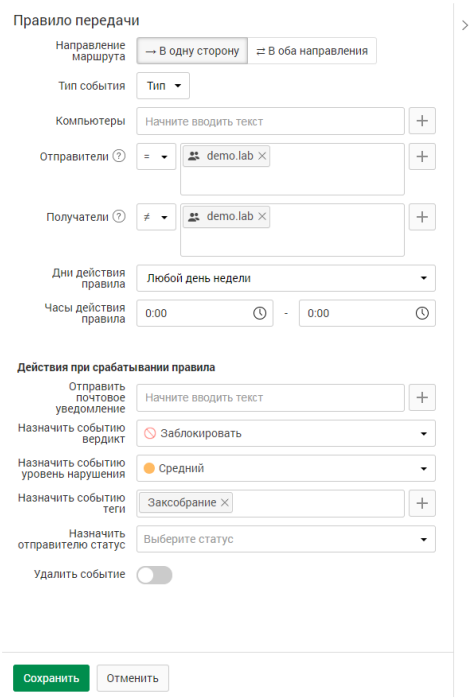
В соответствии условию задания выставляем следующие параметры:

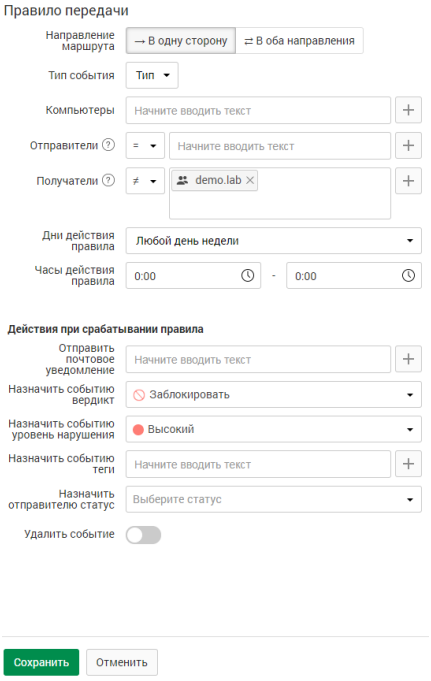


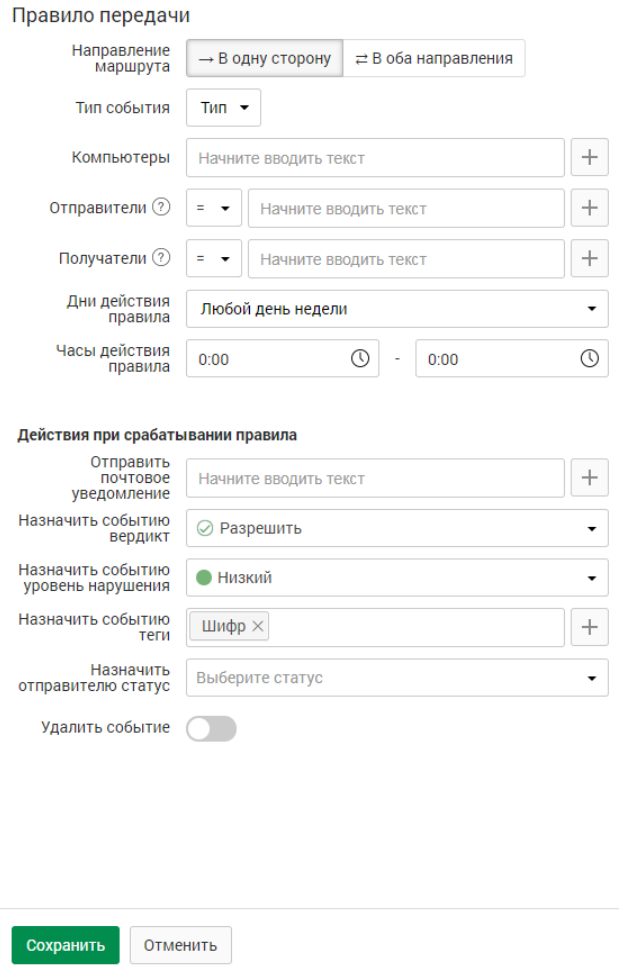
–В поле «Получатели» выбираем операцию ≠, затем знак «+» → вкладка «Группы» → поставить галочку «demo.lab»
–Назначить событию вердикт «Разрешить»
–Назначить событию уровень «Низкий»
–Тег «Печать»
–Нажать «Сохранить»

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

Эталон ответа


Правило передачи
Направление маршрута
→ В одну сторону
⇄ В оба направления
Тип события
Тип
Компьютеры
Начните вводить текст
Отправители
=
demo.lab
Получатели
≠
demo.lab
Дни действия правила
Любой день недели
Часы действия правила
0:00
0:00
Действия при срабатывании правила
Отправить почтовое уведомление
Начните вводить текст
Назначить событию вердикт
Заблокировать
Назначить событию уровень нарушения
Средний
Назначить событию теги
Заксобрание
Назначить отправителю статус
Выберите статус
Удалить событие
Сохранить
Отменить

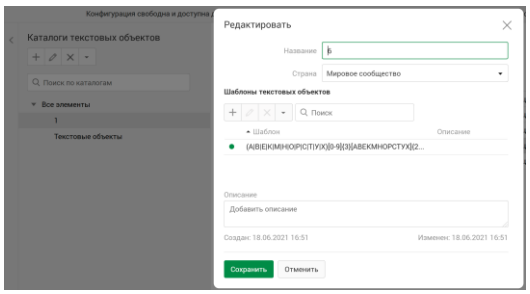

Правило передачи
Направление маршрута
→ В одну сторону
⇄ В оба направления
Тип события
Тип
Компьютеры
Начните вводить текст
Отправители
=
Начните вводить текст
Получатели
≠
demo.lab
Дни действия правила
Любой день недели
Часы действия правила
0:00
0:00
Действия при срабатывании правила
Отправить почтовое уведомление
Начните вводить текст
Назначить событию вердикт
Заблокировать
Назначить событию уровень нарушения
Высокий
Назначить событию теги
Начните вводить текст
Назначить отправителю статус
Выберите статус
Удалить событие
Сохранить
Отменить

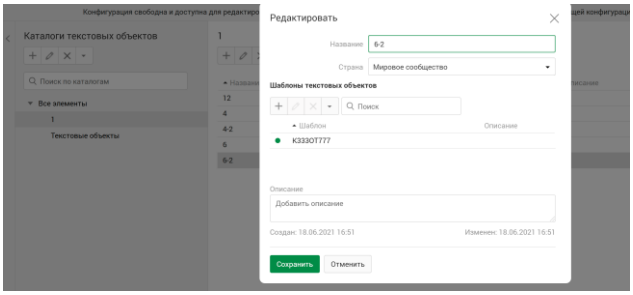


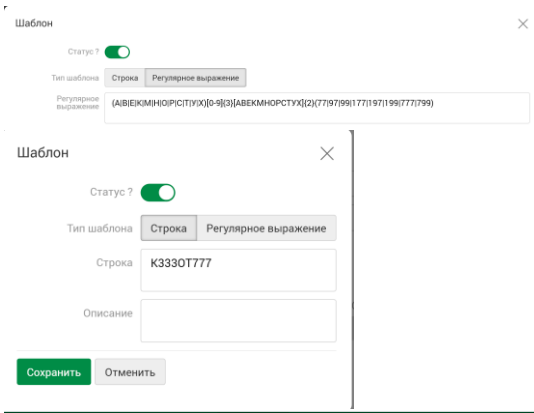
10.Практическое занятие № 35 Создание политик с использованием регулярных выражений в Traffic Monitor

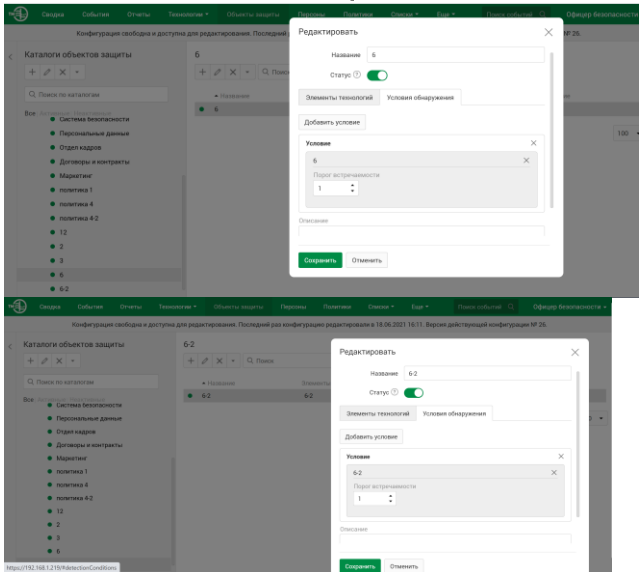
Задание:
Политика 6
Стало известно, что сотрудники охраны (Security) ООО «Повозка» за определенную сумму пропускают автомобили из близлежащих домов наслужебную парковку. В связи с ужесточением корпоративной политики в компании, правом въезда на территорию обладает только генеральный директор.
Сотрудники 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:

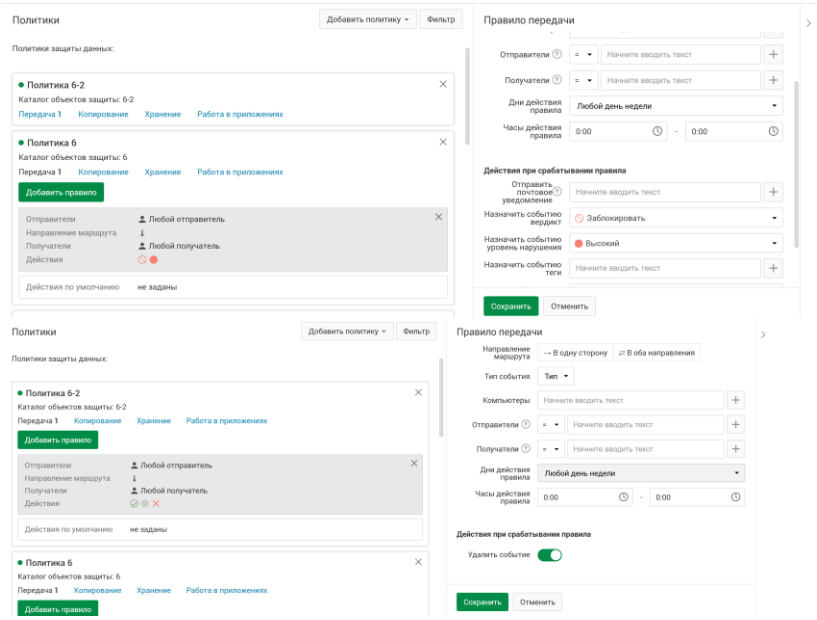
А, В, Е, К, М, Н, О, Р, С, Т, У, Х (Верхний регистр) Цифры, используемые в автомобильных номерах:
000 – 999
Регионы автомобильных номеров, подлежащие детектированию:
77, 97, 99, 177, 197, 199, 777, 799
Вердикт: заблокировать ×
Уровень нарушения: Высокий •
Тег: Политика 6


Редактировать
Каталоги текстовых объектов
Название
Страна
Мировое сообщество
Шаблоны текстовых объектов
Описание
Добавить описание
Сохранить
Отменить


Редактировать
Каталоги текстовых объектов
Название
6-2
Страна
Мировое сообщество
Шаблоны текстовых объектов
К333ОТ777
Описание
Добавить описание
Сохранить
Отменить

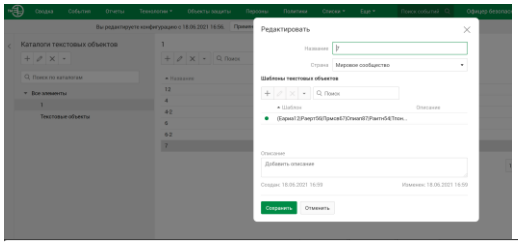

Шаблон
Статус ?
Тип шаблона
Строка
Регулярное выражение
Строка
К333ОТ777
Описание
Сохранить
Отменить

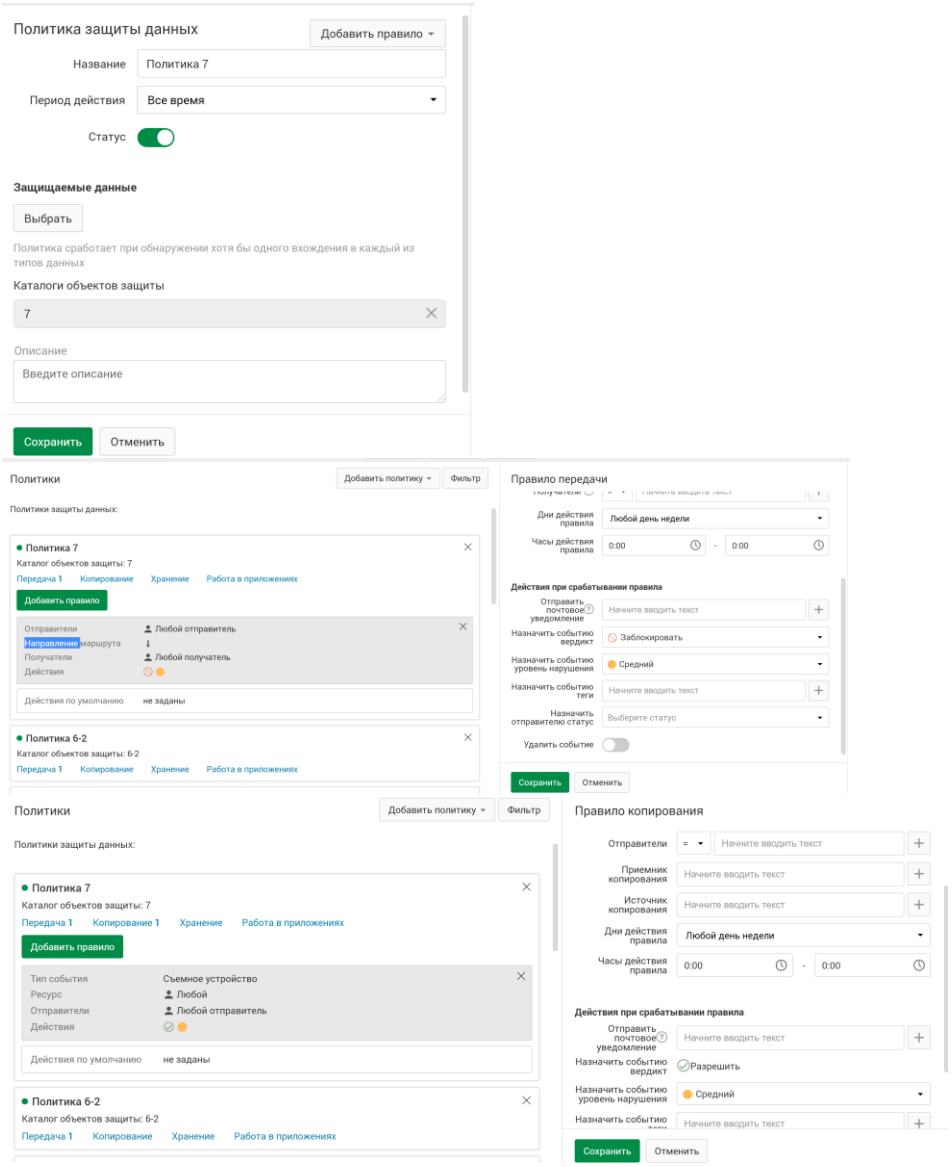

Редактировать
Каталоги объектов защиты
Название
Статус
Элементы технологий
Условия обнаружения
Добавить условие
Условие
Порог встречаемости
Описание
Сохранить
Отменить



<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 флеш-накопителем, для того чтобы завладеть акционными купонами, а также слить не весь файл, а один или несколько купонов. Запретить передачу данных, содержащих информацию об этих купонах, а также отслеживать 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.

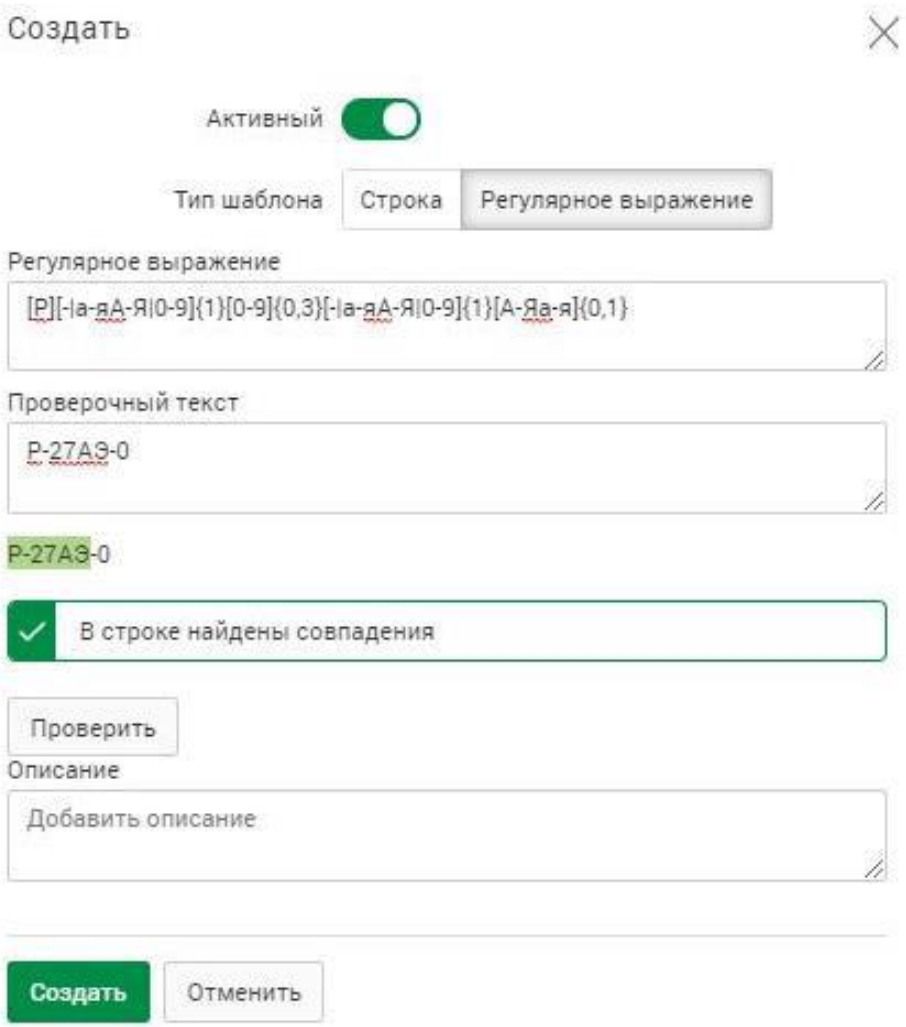
Все политики, объекты и прочие элементы должны называться в соответствии с номерами (например Объект 5.1, Политика 5.2, Технология 5.3 и т.д.)

Вердикт 1: Разрешить

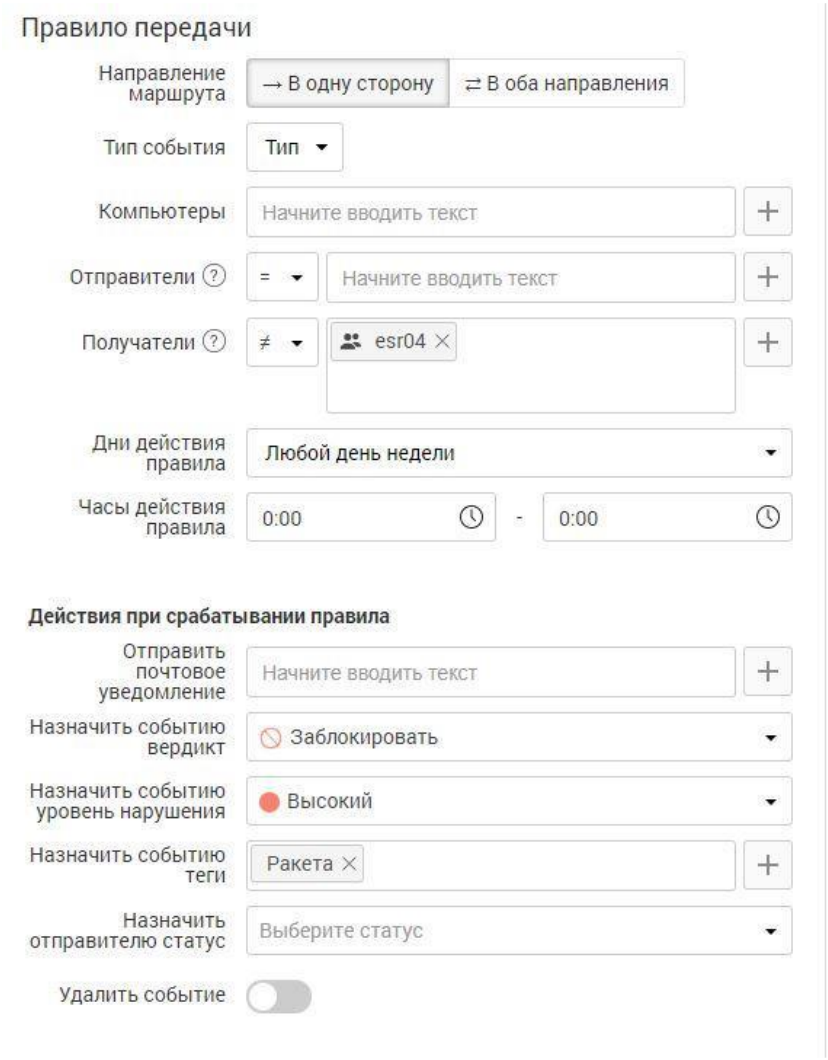
Уровень нарушения 1: низкий

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.

Эталон ответа:
Создание регулярного выражения:



Создание политики:



11. Практическое занятие № 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.

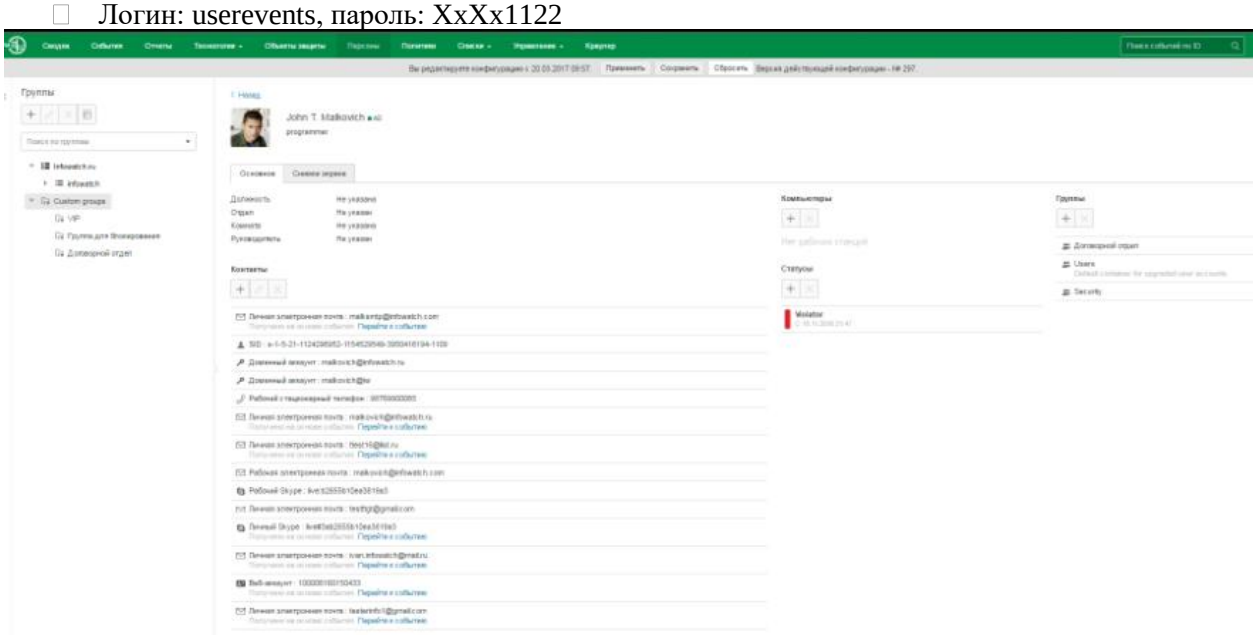
По каждому заданию в отчёт вставить скриншоты.

Эталон ответа:

Задание 1:

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

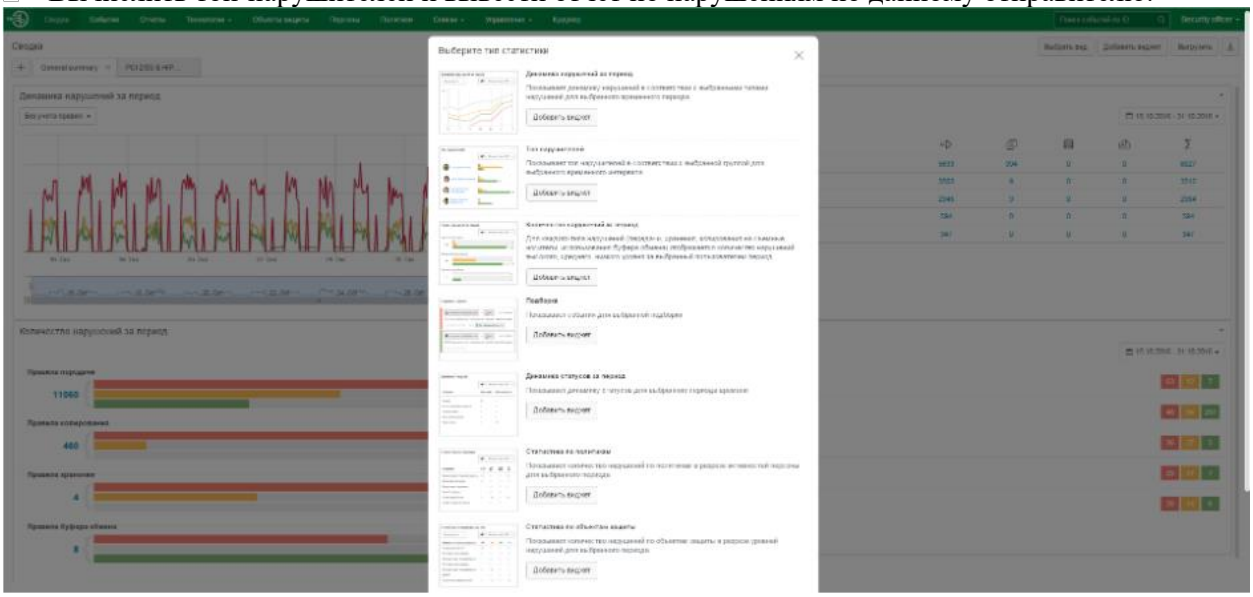
- Логин: userevents, пароль: XxXx1122



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.

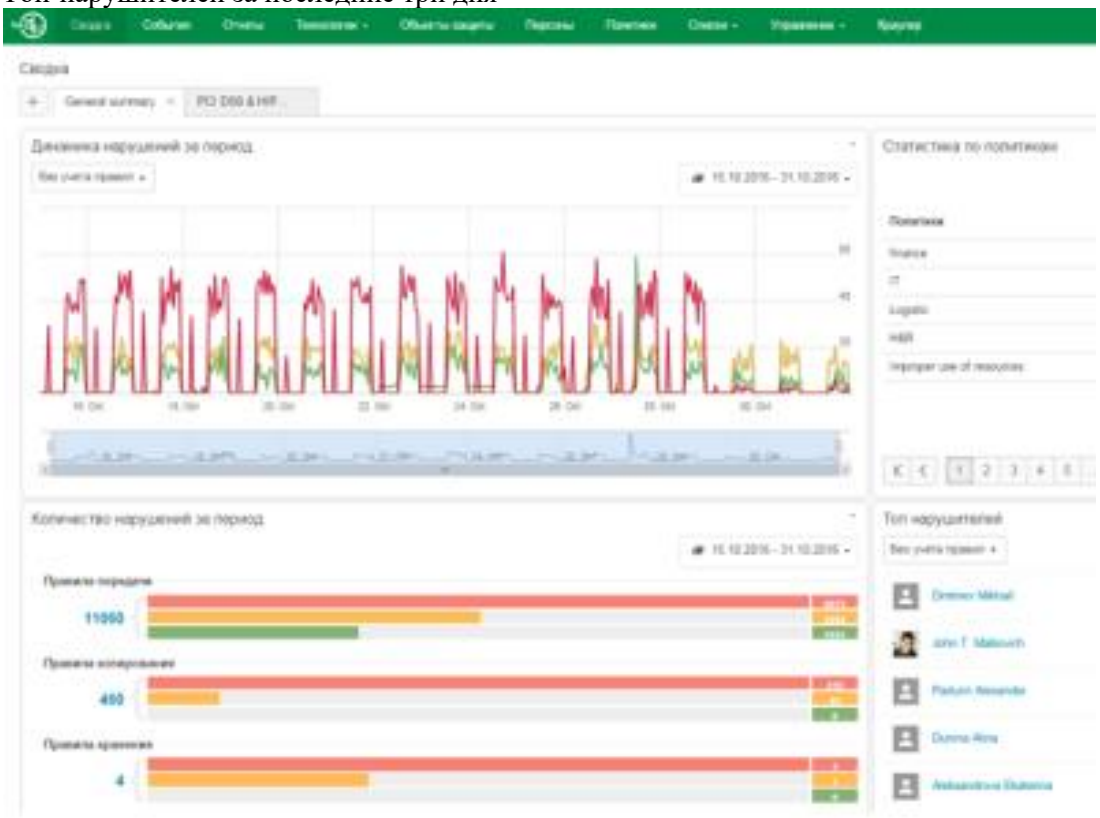


Задание 3: Создание сводки

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

Добавить 4 виджета на панель сводки:

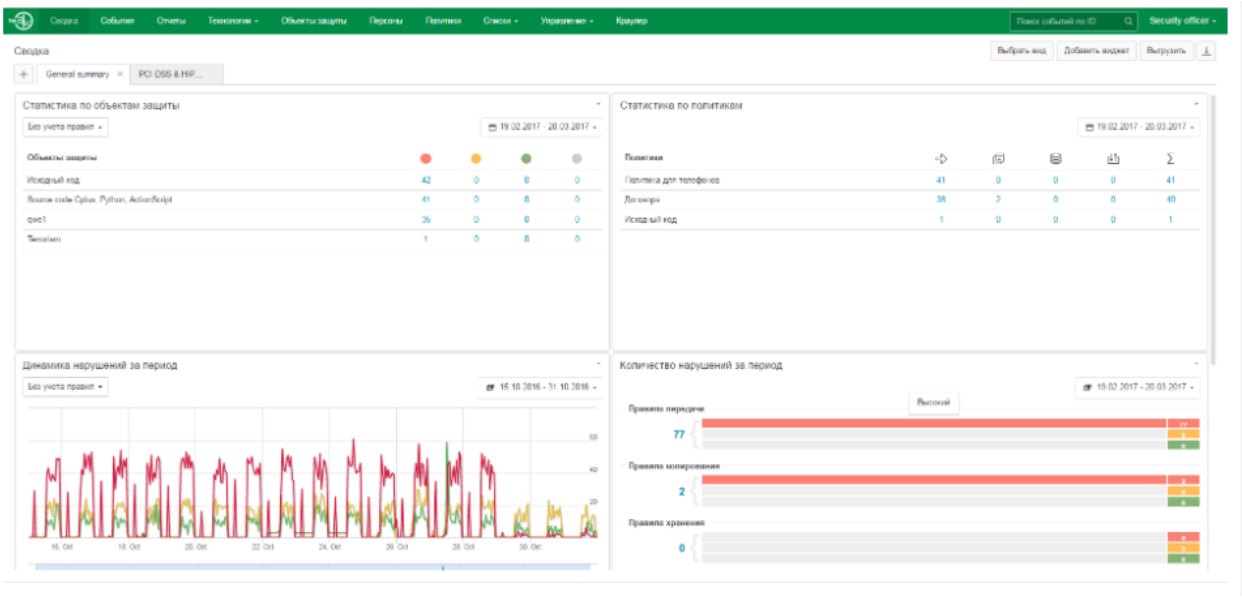
- Динамика нарушений за последние три дня
- Статистика по политикам за последние три дня
- Количество нарушений за последние три дня
- Топ-нарушителей за последние три дня



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.



11.Устный опрос по теме 1.7

Инструкция для обучающихся

Зачет сдается в рамках учебного занятия. Каждый студент отвечает в устной форме на предложенные преподавателем 2 вопроса.

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

Перечень вопросов:

1. Кем и в каком году утверждён документ СТР-К?
2. Какие вопросы определяет документ СТР-К?
3. Перечислите объекты защиты документа СТР-К
4. Перечислите источники требований безопасности для ОО
5. Объясните связь между данными пользователей и данными ФБО
6. Что включает в себя аудит безопасности?
7. Какие компоненты входят в аудит безопасности?

Эталоны ответов: приведены в Учебном пособии по МДК.02.01 «Программные и программно-аппаратные средства защиты информации».

13.Практическое занятие № 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. 1.4) 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 администратора	Помощник глав администратора 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 возможности их удаления между некоторыми сетевыми узлами (в списке связей помечаются серым цветом, ЦУС → Свойства узла):

Таблица. Матрица связей пользователей

Связи пользователей	Координатор Центр офис	Глав администратор Петров	Помощник глав администратора Иванов	Сотруд_1 Центр Кузнецов	Координатор Филиал	Сотруд_2 Филиал Попов
Координатор Центр офис		•	•	•	•	
Глав администратор Петров	•		•			
Помощник глав администратора Иванов	•	•				
Сотруд_1 Центр Кузнецов	•					•
Координатор Филиал	•					•
Сотруд_2 Филиал Попов				•	•	

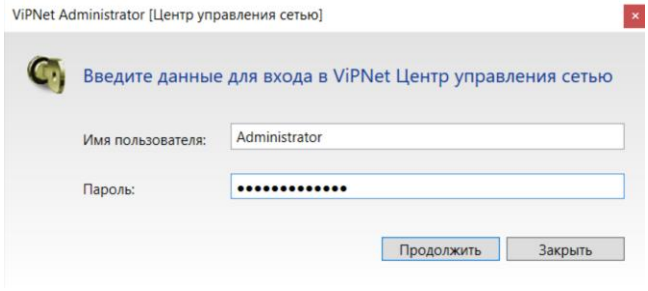
Примечание. Связь узла с Центром управления сетью является технологической и используется только для обеспечения возможности рассылки справочников, ключей и обновлений программного обеспечения.

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

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

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

Для начала работы с программой ViPNet ЦУС:



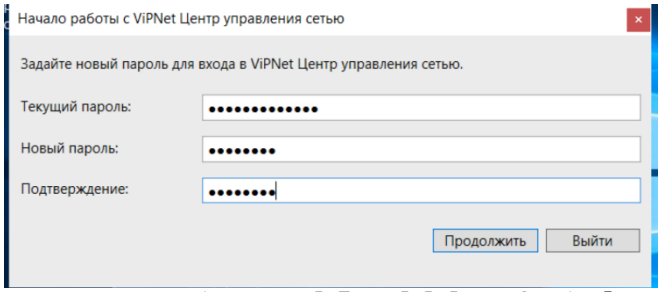


Рис. Смена пароля

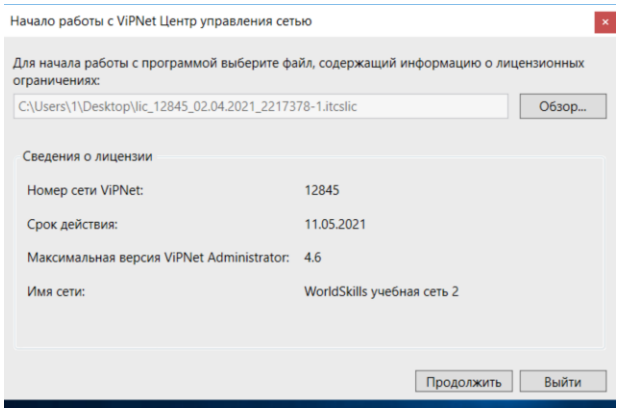


Рис. Выбор файла лицензии

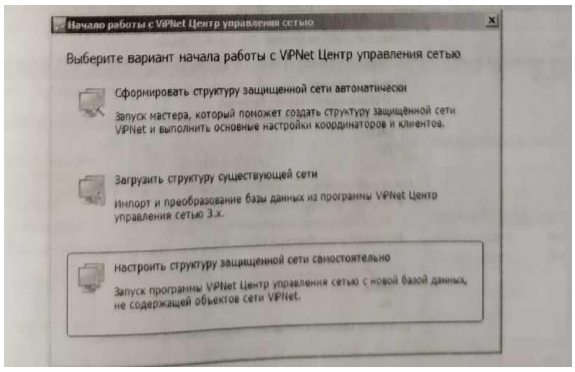
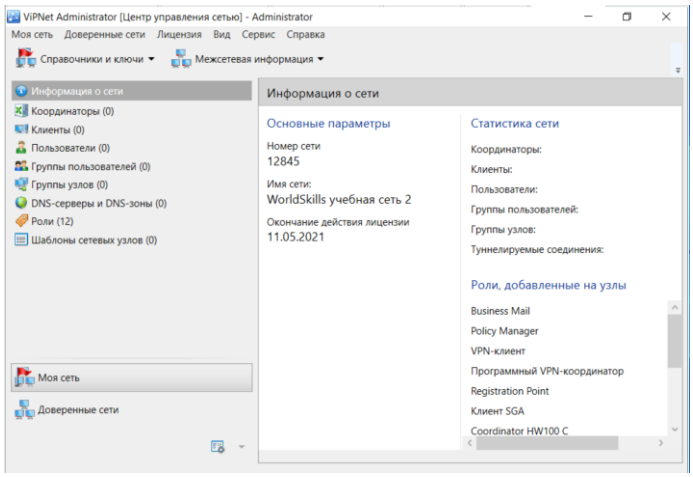
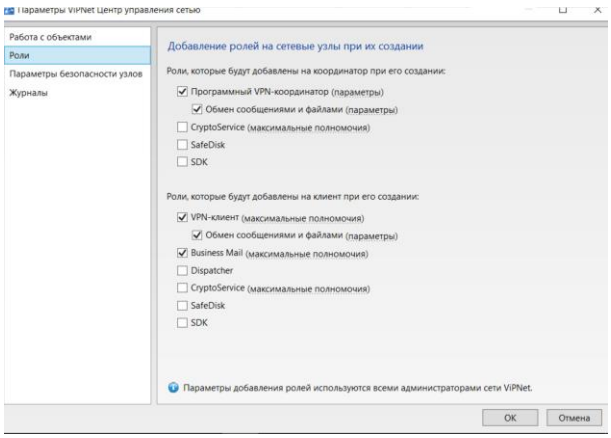


Рис. Выбор варианта начала работы с ЦУС





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.

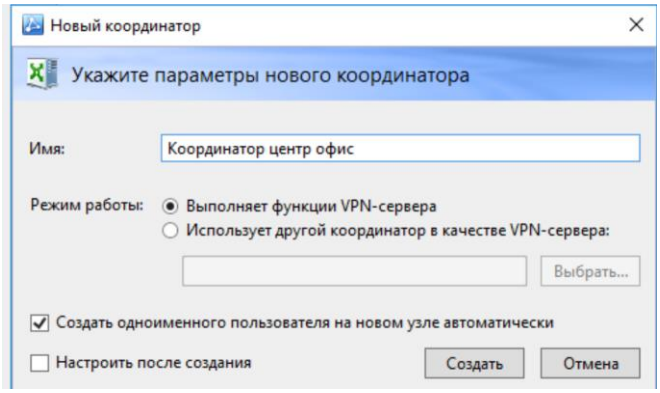


Рис. Параметры нового координатора

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

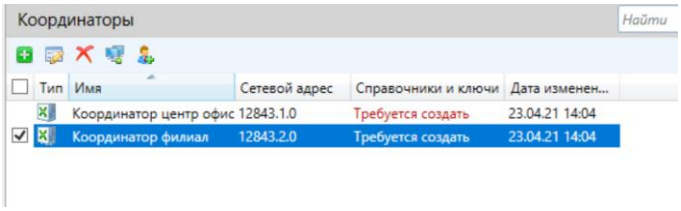


Рис. Раздел «Координаторы» — «Моя сеть»

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.).

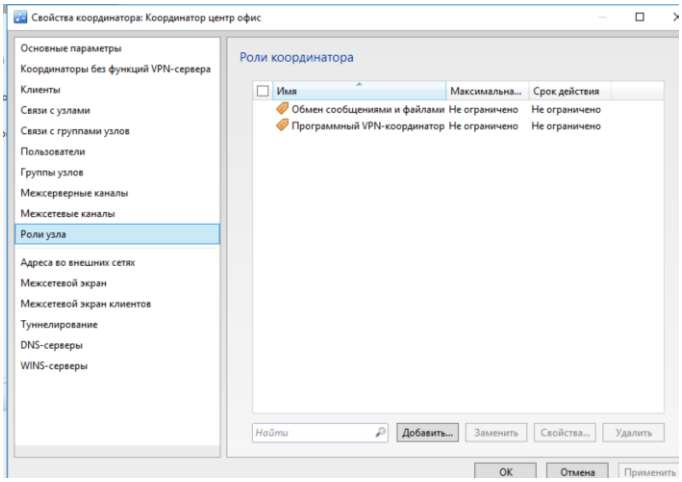
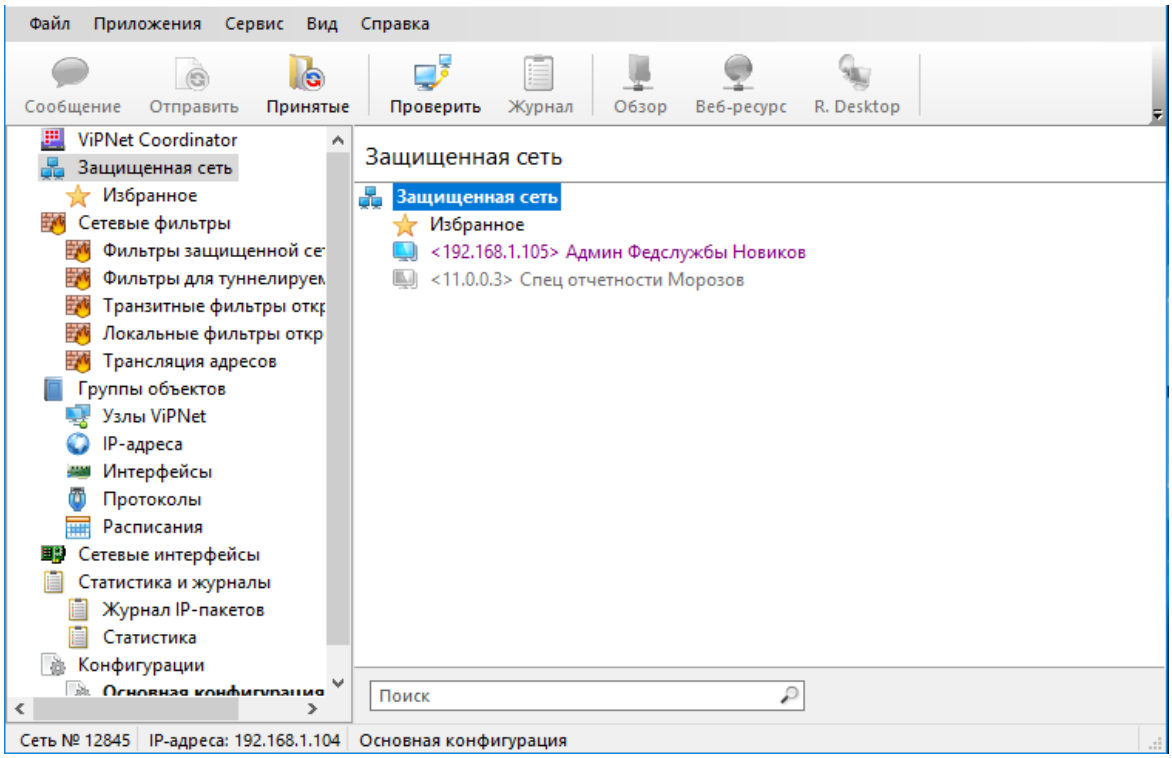
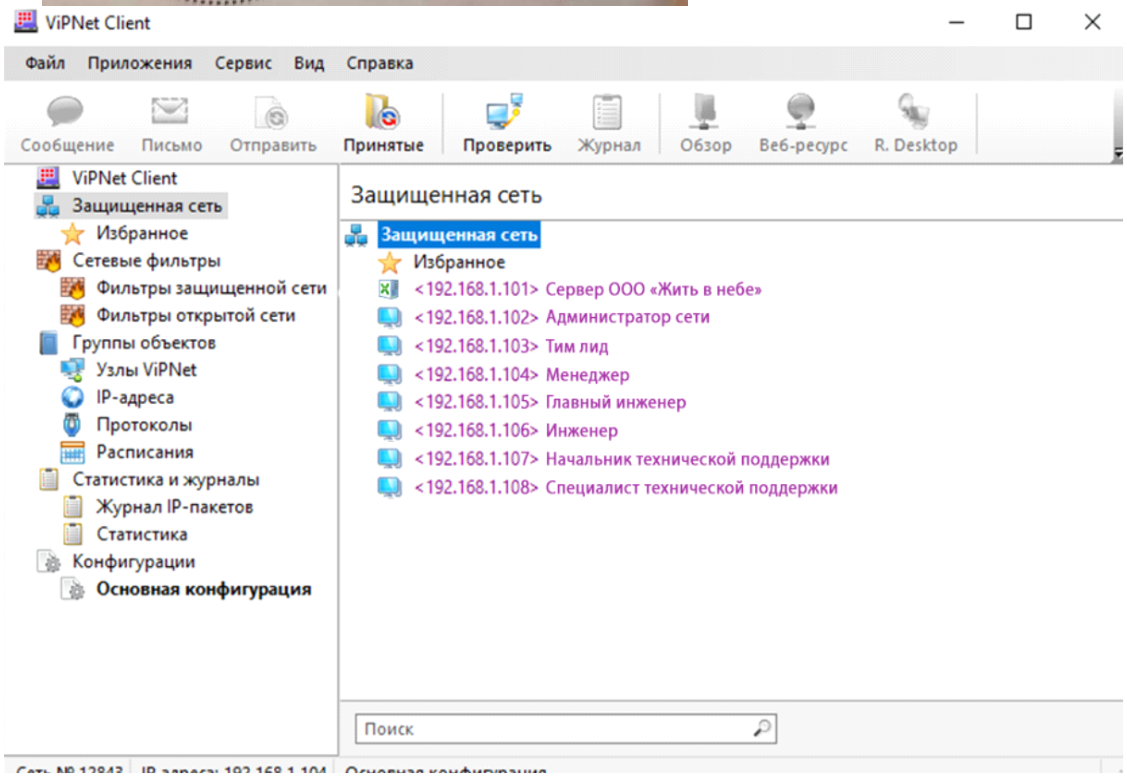


Рис. Роли координатора

Эталон ответа:





14.Практическое занятие № 43 Развёртывание рабочего места помощника главного администратора защищённой сети ViPNet

Задание:

1. На виртуальной машине (VM_1 - рабочее место главного администратора сети), где уже установлен ЦУС и УКЦ, доустановить ViPNet Client и активировать его с помощью dst-файла, выпущенного для СУ Главный администратор.
2. Развернуть на виртуальной машине (VM_2 - рабочее место помощника главного администратора) необходимое ПО - клиентскую часть ViPNet Administrator ЦУС и ViPNet Client, который необходимо активировать с

помощью dst-файла, выпущенного для СУ *Помощник глав администратора.*

Установка ViPNet Client

Программное обеспечение VipNet Client необходимо установить на VM_1 и VM_1. 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.).

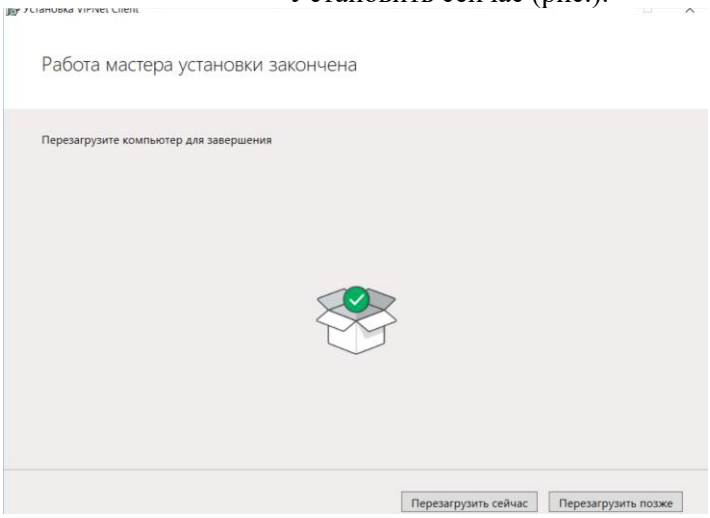


Рис. Способ установки

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.).

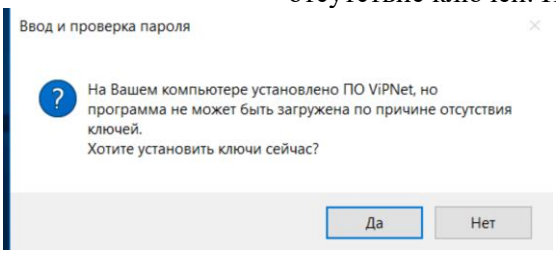


Рис. Диалоговое окно с вопросом об установке ключей

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.

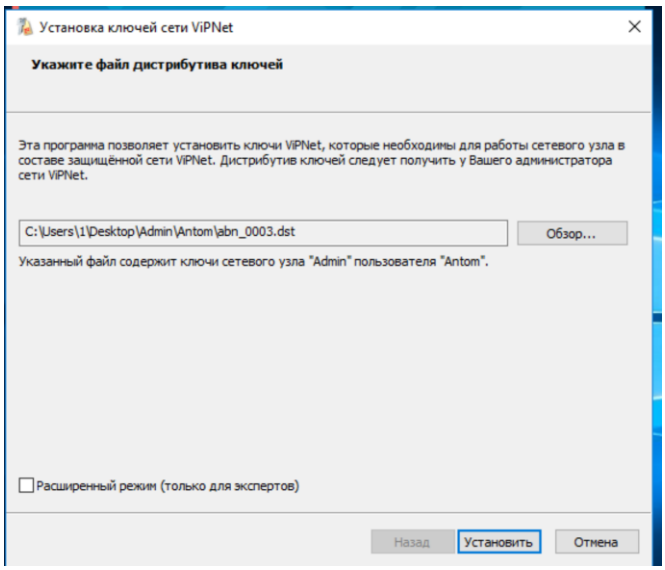


Рис.. Выбор дистрибутива ключей

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

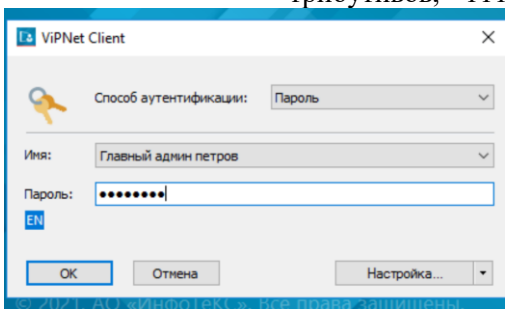


Рис. Окно аутентификации VipNet Client

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 адмна Иванов сетевого узла Помощник глав адмна.

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.).

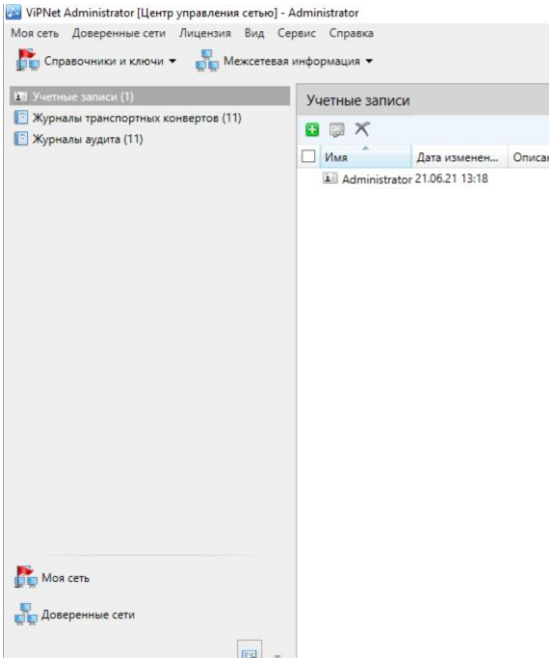


Рис. Раздел «Администрирование»

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.).

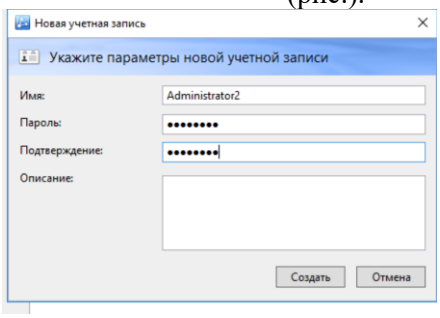


Рис. Создание второго администратора ЦУС

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

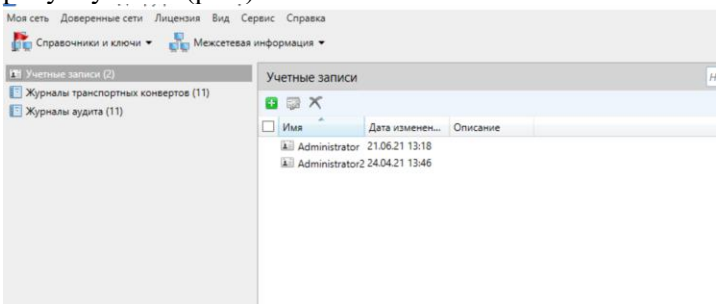


Рис. Раздел «Учетные записи ЦУС»

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.).

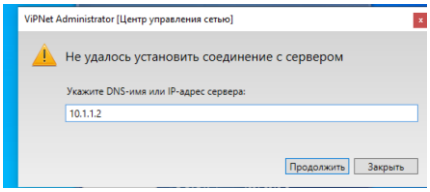


Рис. Ввод адреса СУ с установленной серверной частью ЦУС

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

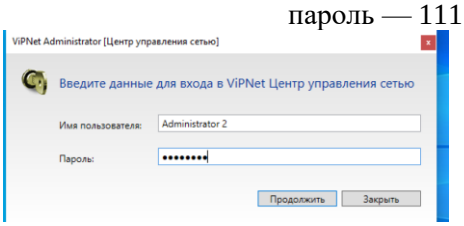


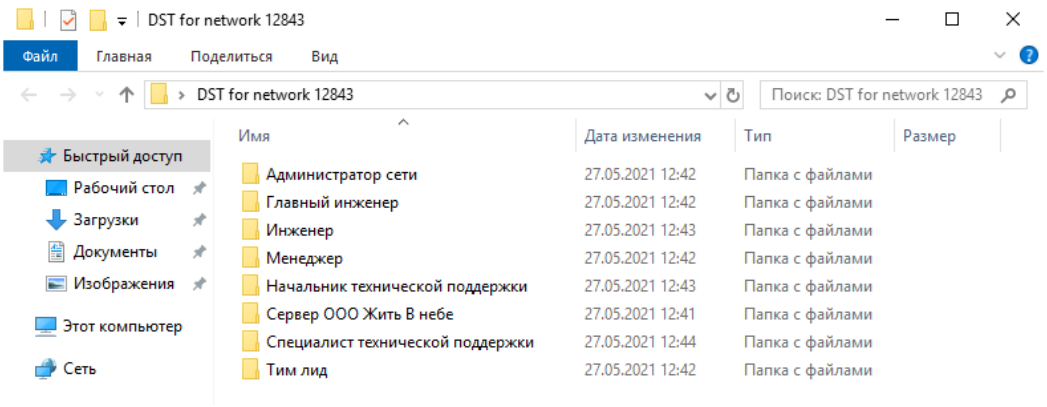
Рис. Окно аутентификации клиентской части ЦУС

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.

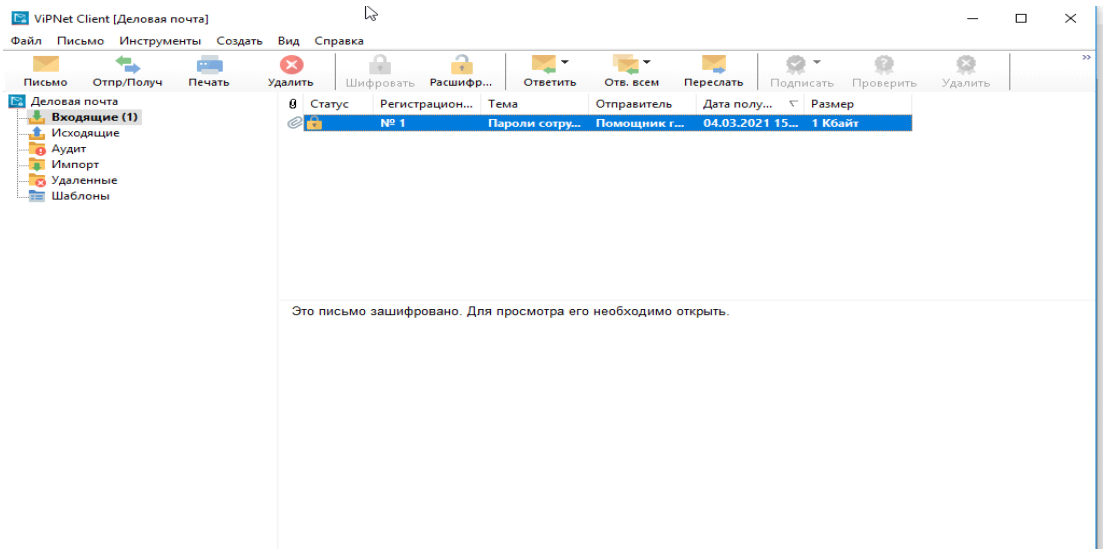
Таким образом, теперь управлять защищенной сетью ViPNet можно двух рабочих мест.

Эталон ответа:

Выдача дистриубтива для помощника:



Деловая почта:



15. Практическое занятие № 46 «Настройка политик безопасности в защищённой сети VipNet Policy Manager»

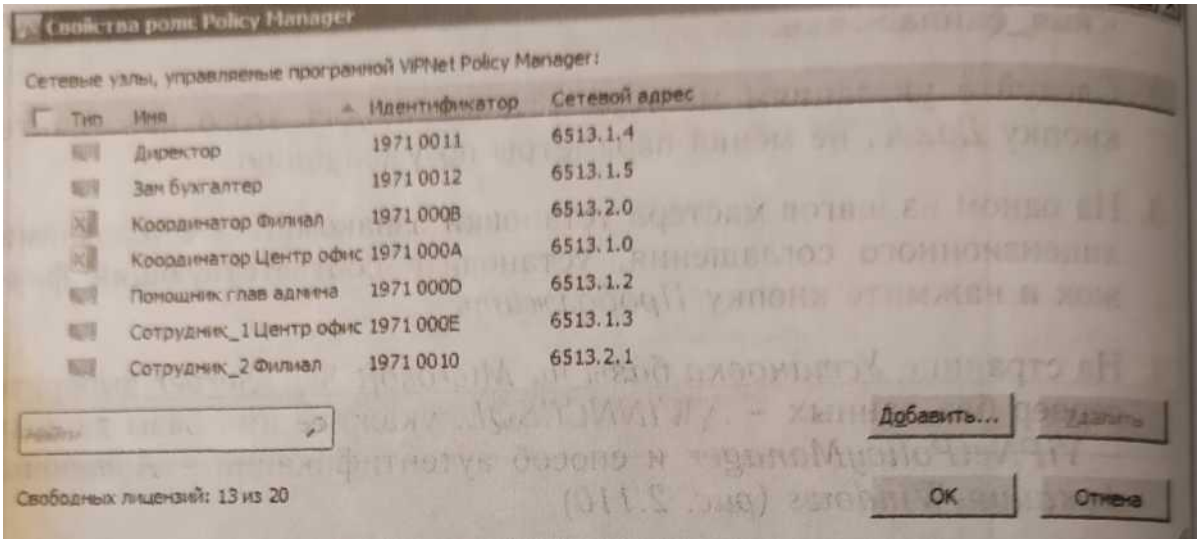
Задание:

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.

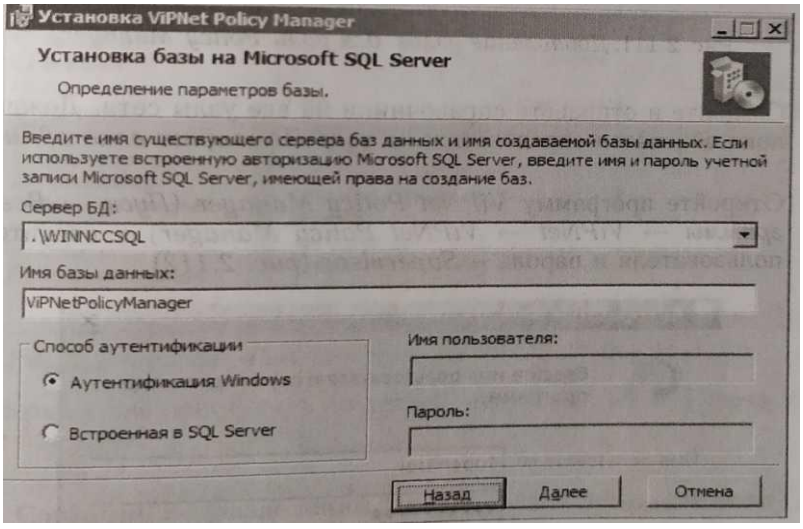
Установка ViPNet Policy Manager

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
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 → Свой-



ства и добавьте в список все узлы сети (рис.).
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.).
5. На экран будет выведено предупреждение о необходимости смены пароля пользователя Supervisor.
6. После авторизации под стандартным паролем перейдите в раздел Файл → Сменить пароль пользователя и задайте пароль — 11111111 (восемь единиц).
7. В окне программы VipNet Policy Manager перейдите в раздел Сетевые узлы. Если предыдущие шаги выполнены верно, то в списке будут отображены все узлы сети VipNet
Теперь можно приступить к управлению узлами ViPNet через ViPNet Policy Manager.
Создание подразделений Центральный офис, Филиал
Для создания подразделений Центральный офис, Филиал выполните следующие действия:
1. В окне программы VipNet Policy Manager перейдите в раздел Подразделения и нажмите кнопку Создать.

2. В открывшемся окне Свойства подразделения на вкладке Основные параметры задайте имя Центральный офис.
3. На вкладке Сетевые узлы добавьте клиентов Центрального офиса: Координатор Центр офис, Главный администратор, Помощник глав админа, Сотрудник_1 Центр офис, Зам бухгалтер, Директор.
Остальные настройки в окне Свойства подразделения менять не требуется.
Аналогичным образом создайте подразделения Филиал, добавив в него сетевые узлы Координатор Филиал, Сотрудник_2 Филиал.
Если все выполнено правильно, раздел Подразделения программы ViPNet Policy Manager примет следующий вид
Создание политики безопасности, ограничивающей доступ работников компании к социальным сетям Вконтакте и Одноклассники
Для создания политики безопасности, ограничивающей доступ работников компании к социальным сетям Вконтакте и Одноклассники, выполните следующие действия:
1. В окне программы ViPNet Policy Manager перейдите в раздел Группы объектов —* IP-адреса и нажмите кнопку Создать.
2. В открывшемся окне Свойства группы IP-адресов на вкладке Основные параметры затаите имя Социальные сети.
3. 3 На вкладке Состав нажмите кнопку Добавить → DNS-имя... и добавьте имя vk.com.
4. Аналогичным образом добавьте DNS-имена согласно рисунку ниже (в рамках практического занятия не обязательно вбивать все DNS-имена, они приведены в качестве примера, чтобы было понятно, как действовать в реальной ситуации, для эффективного закрытия доступа к ресурсам). Соответствующие IP-адреса будут определены автоматически

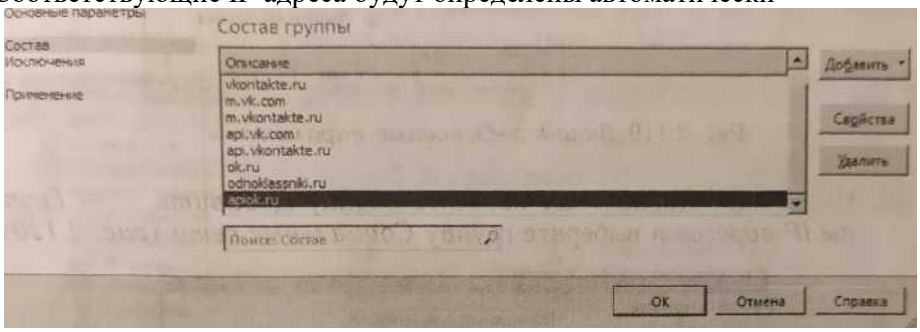


Рис. Список DNS-имен социальных сетей «Вконтакте» и *«Одноклассники»*
5. В окне программы ViPNet Policy Manager перейдите в раздел Шаблоны политики и нажмите кнопку Создать.
6. В открывшемся окне Свойства шаблона политики на вкладке Основные параметры задайте имя Запрет социальных сетей.
7. На вкладке Подразделения отметьте подразделения Центральный офис и На вкладке Локальные фильтры открытой сети нажмите кнопку Создать...
Рис.. Вкладка «Подразделения» окна Свойства шаблона политик
8. В открывшемся окне Свойства фильтра открытой сети на вкладке Основные параметры задайте имя фильтра Запрет социальных сетей и установите переключатель в положение Блокировать трафик.
Рис. Вкладка «Основные параметры»
9. На вкладке Назначения нажмите кнопку Добавить... р пы IP-адресов и выберите группу Социальные сети
10. Остальные параметры окна Свойства фильтра открытой сети и Свойства шаблона политики менять не требуется.
После создания политики Запрет социальных сетей раздел Шаблоны политики примет следующий вид.
11. Отправьте политики на узлы. Для этого в окне программы
ViPNet Policy Manager перейдите в раздел Подразделения.
12. Выделите подразделения Центральный офис и Филиал, нажмите кнопку Отправить политики.
13. На экран будет выведено окно Отправка политики. Не меняя параметров, нажмите кнопку ОК
Для контроля за ходом отправки политик на узлы в окне программы *ViPNet Policy Manager* перейдите в раздел Журналы → Отправка и применение политик. Статус политик на узлах Главный администратор и Помощник глав админа должен измениться на Применена.

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

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

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

1. В окне программы ViPNet Policy Manager перейдите в раздел Шаблоны политики и нажмите кнопку Создать.
2. В открывшемся окне Свойства шаблона политики на вкладке Основные параметры задайте имя Блокировка открытого трафика.
3. На вкладке Сетевые узлы добавьте Сотрудник_1 Центр офис.
4. На вкладке Локальные фильтры открытой сети нажмите кнопку Создать…
5. В открывшемся окне Свойства фильтра открытой сети на вкладке Основные параметры задайте имя фильтра Блокировка открытого трафика, установите переключатель в положение Блокировать трафик и нажмите ОК
6. Остальные параметры окна Свойства фильтра открытой сети и Свойства шаблона политики менять не требуется.

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

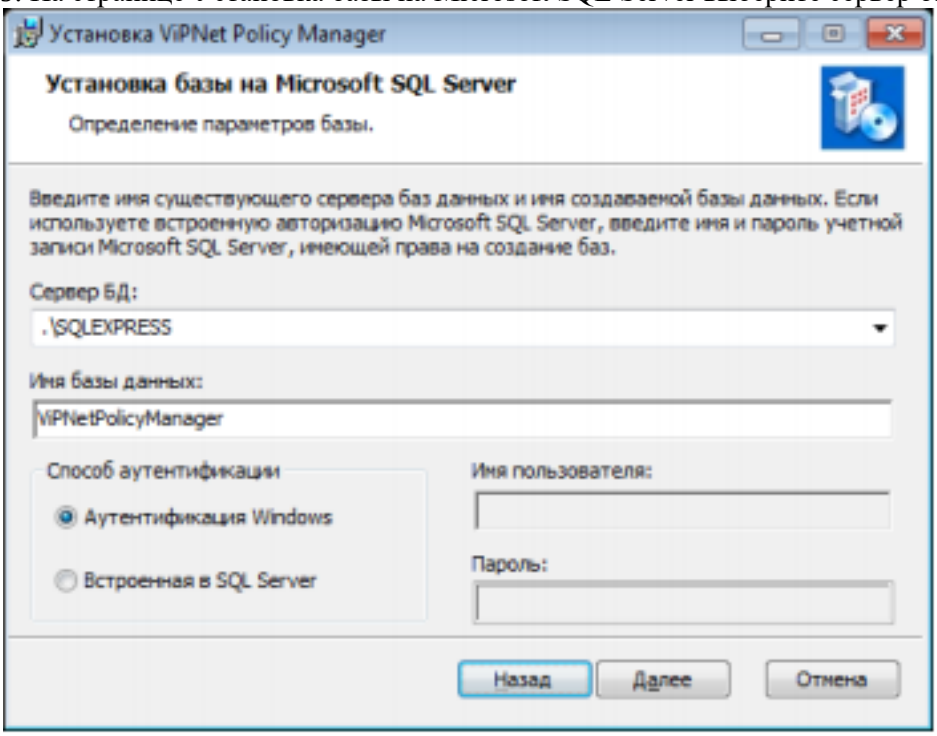
Эталон ответа:

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

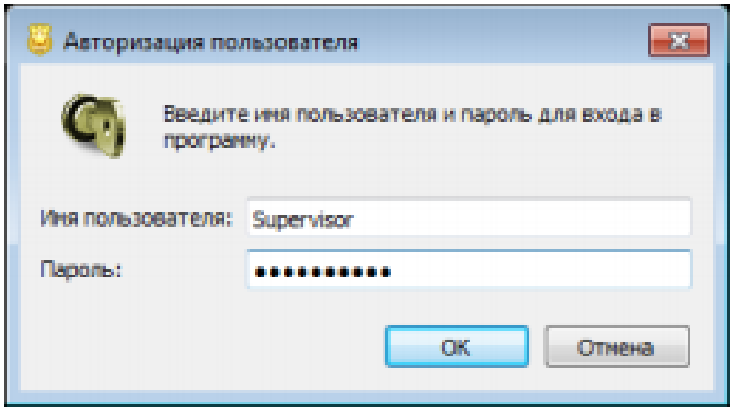
ПО ViPNet Policy Manager допускается развертывать только на клиенте с ролью Network Control Center, поэтому клиенту Главный администратор была автоматически назначена роль Policy Manager.

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

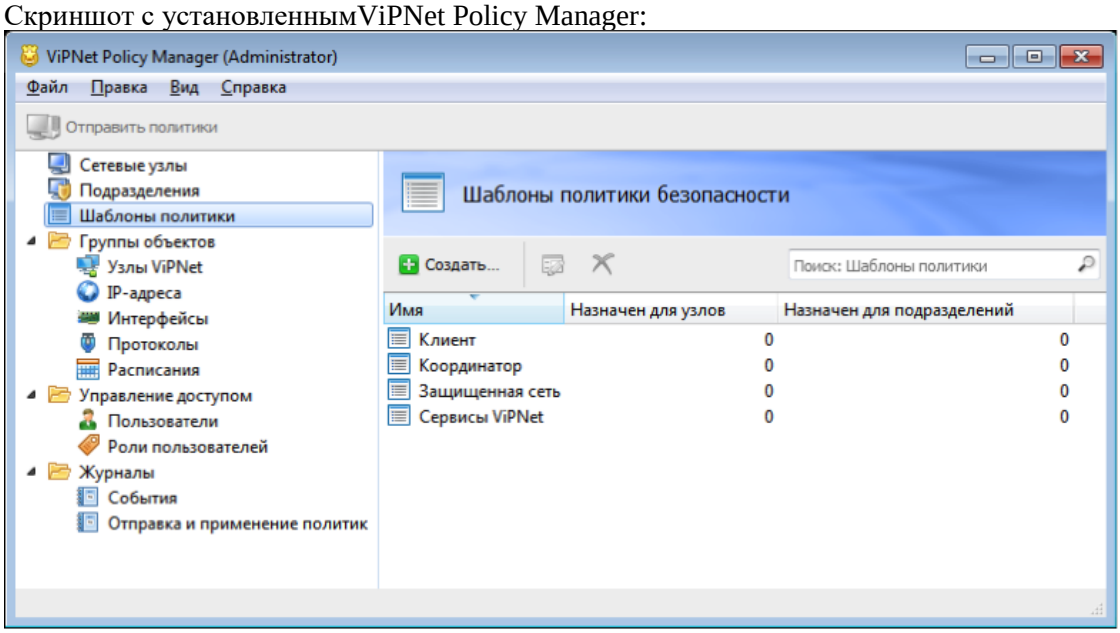


.\WINNCCSQL, укажите имя базы данных - ViPNetPolicyManager и способ аутентификации - Аутентификация Windows (рис. 1.110).

10. В процессе установки может появиться окно со списком приложений которые требуется закрыть. Выберите Закрыть приложения и попытаться перезапустить их и нажмите ОК.
Для обеспечения нормальной работы продукта VipNet Policy Manager выполните следующие действия:
8. В окне VipNet Центр управления сетью перейдите в раздел Клиенты.
9. В свойствах клиента Главный администратор выберите Роли узла → Policy Manager → Свойства и добавьте в список все узлы сети .

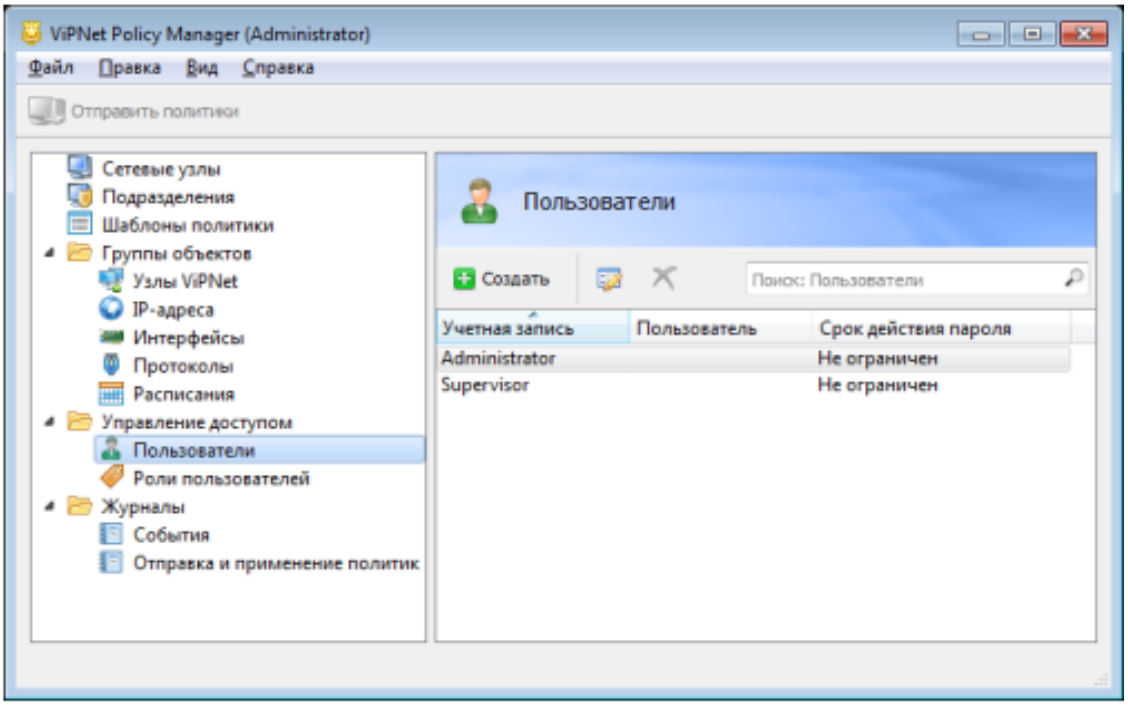


10. Создайте и отправьте справочники на все узлы сети. Дождитесь пока обновятся справочники на узле Помощник глав админа.
11. Откройте программу ViPNet Policy Manager (Пуск → Все программы → ViPNet →ViPNet Policy Manager) и введите им пользователя и пароль - Supervisor
12. На экран будет выведено предупреждение о необходимости смены пароля пользователя Supervisor
13. После авторизации под стандартным паролем перейдите в раздел Файл → Сменить пароль пользователя и задайте пароль — 11111111 (восемь единиц).
14. В окне программы VipNet Policy Manager перейдите в раздел Сетевые узлы. Если предыдущие шаги выполнены верно, то в списке будут отображены все узлы сети VipNet Теперь можно приступить к управлению узлами ViPNet через ViPNet Policy Manager.
Скриншот с установленнымViPNet Policy Manager:



Создание подразделений Центральный офис, Филиал
Для создания подразделений Центральный офис, Филиал выполните следующие действия:
4. В окне программы VipNet Policy Manager перейдите в раздел Подразделения и нажмите кнопку Создать.

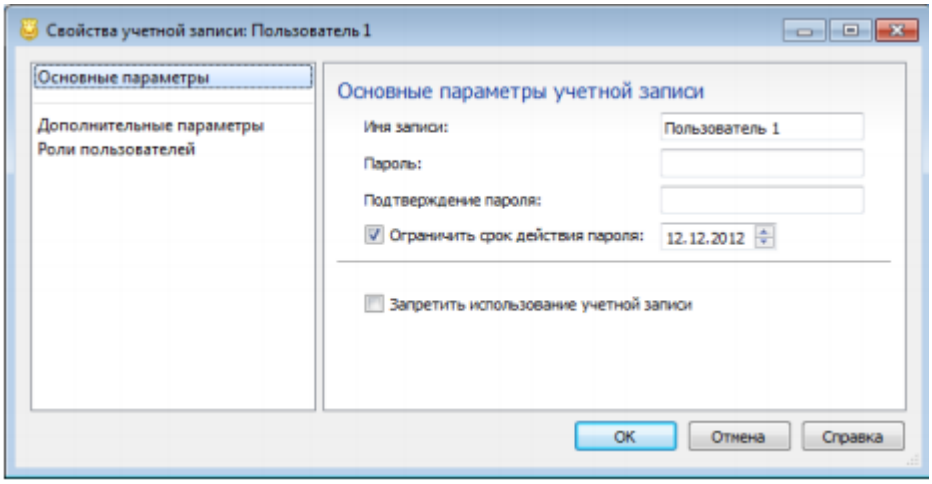
5. В открывшемся окне Свойства подразделения на вкладке Основные параметры задайте имя Центральный офис.



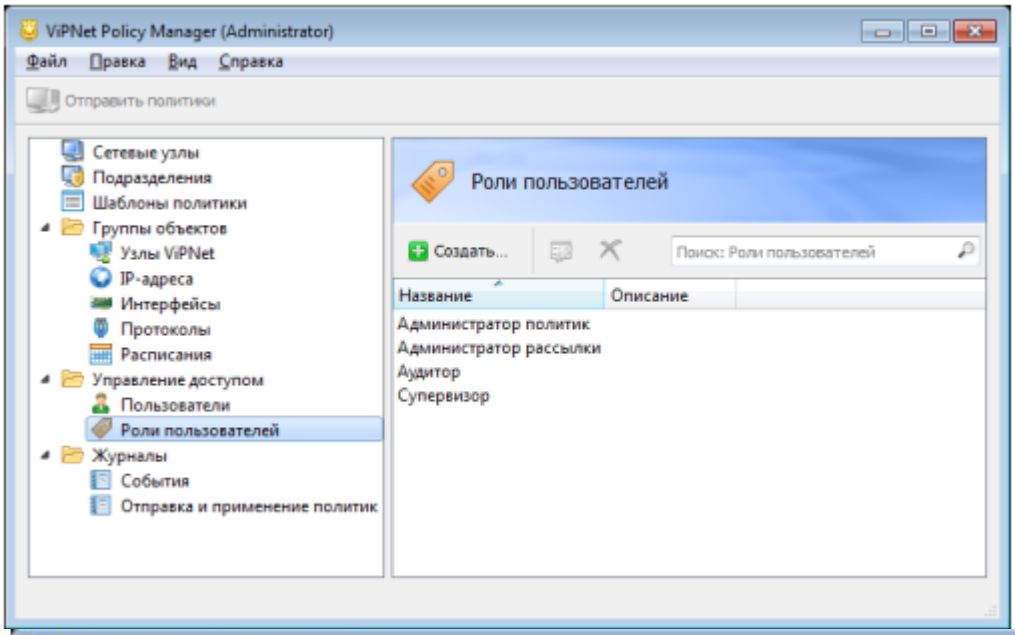
6. На вкладке Сетевые узлы добавьте клиентов Центрального офиса: Координатор Центр офис, Главный администратор, Помощник глав админа, Сотрудник_1 Центр офис, Зам бухгалтер, Директор

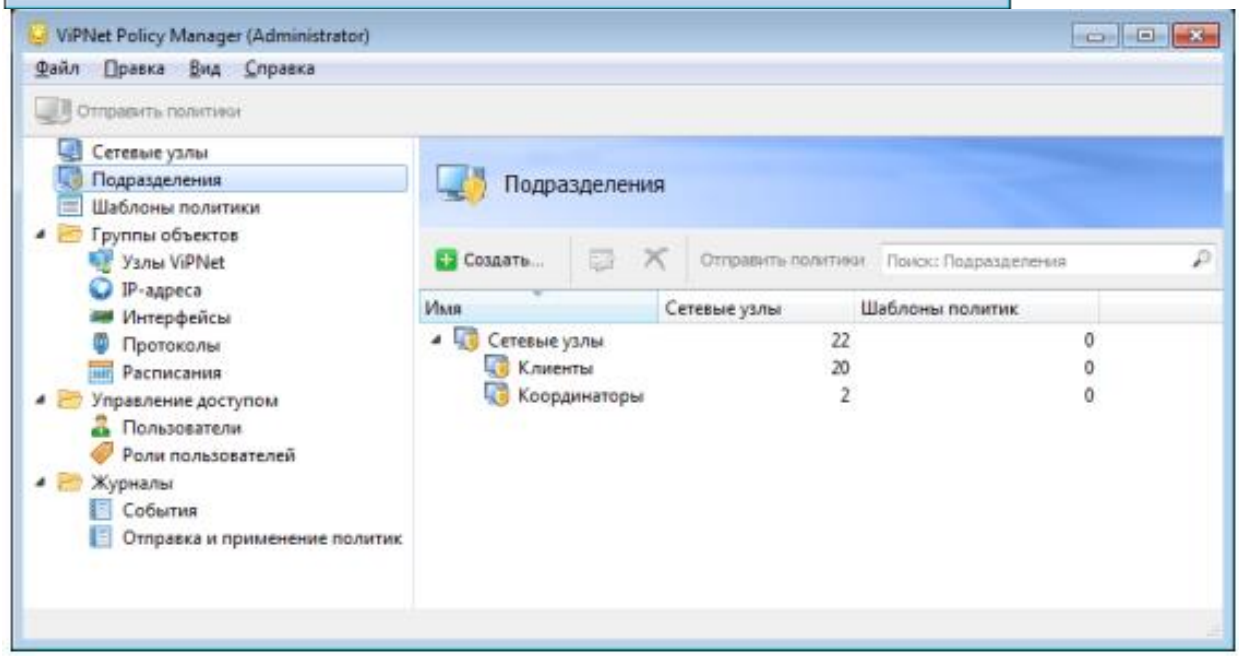
Остальные настройки в окне Свойства подразделения менять не требуется.

Аналогичным образом создайте подразделения Филиал, добавив в него сетевые узлы Координатор Филиал, Сотрудник_2 Филиал.



Если все выполнено правильно, раздел Подразделения программы ViPNet Policy Manager примет следующий вид



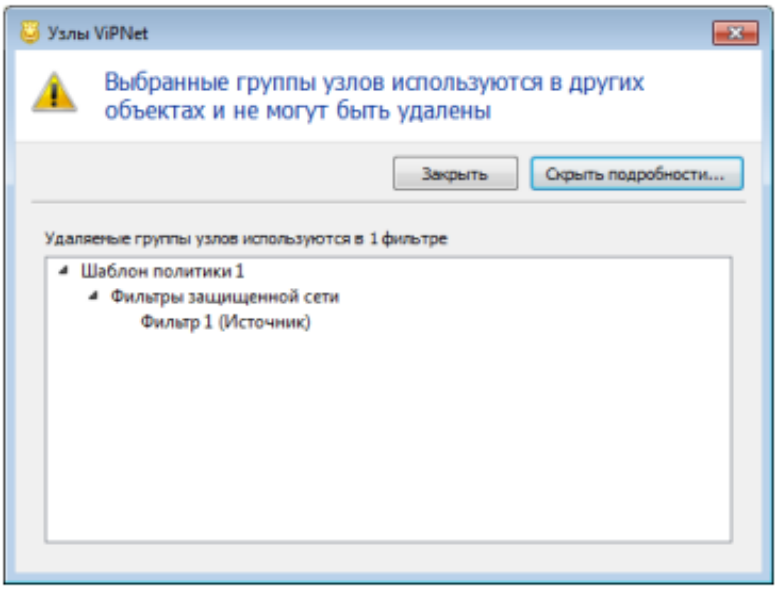


Создание политики безопасности, ограничивающей доступ работников компании к социальным сетям Вконтакте и Одноклассники

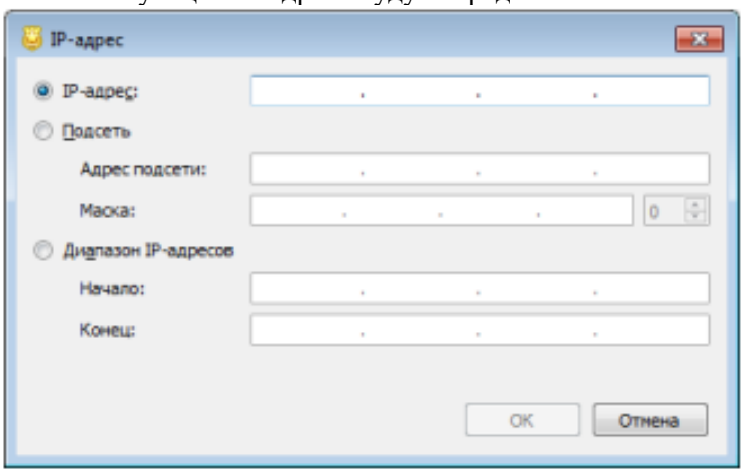
Для создания политики безопасности, ограничивающей доступ работников компании к социальным сетям Вконтакте и Одноклассники, выполните следующие действия:

14. В окне программы ViPNet Policy Manager перейдите в раздел Группы объектов —* IP-адреса и нажмите кнопку Создать.

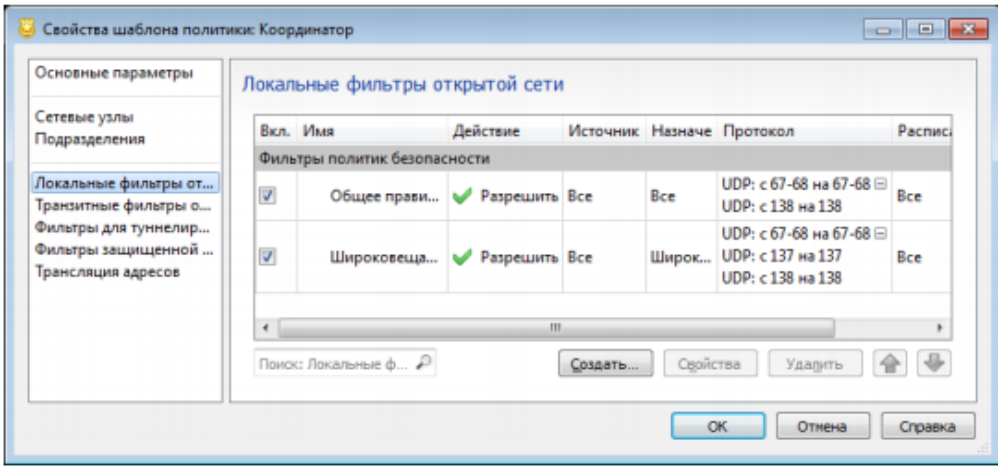
15. В открывшемся окне Свойства группы IP-адресов на вкладке Основные параметры затаите имя Социальные сети.

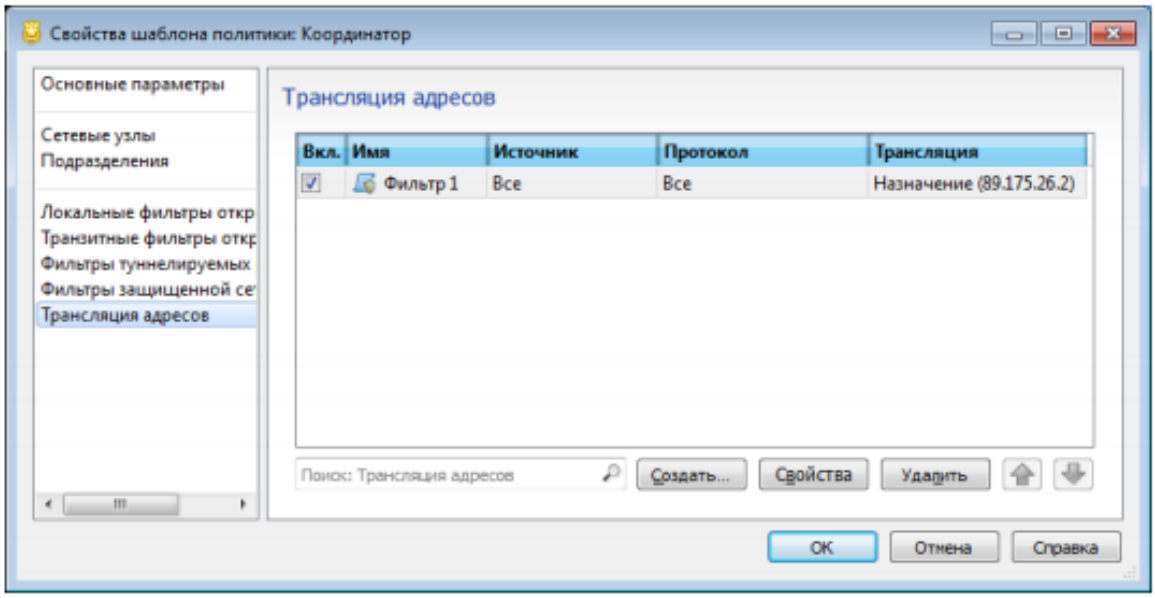


16. 3 На вкладке Состав нажмите кнопку Добавить → DNS-имя... и добавьте имя vk.com.
17. Аналогичным образом добавьте DNS-имена согласно рисунку ниже (в рамках практического занятия не обязательно вбивать все DNS-имена, они приведены в качестве примера, чтобы было понятно, как действовать в реальной ситуации, для эффективного закрытия доступа к ресурсам). Соответствующие IP-адреса будут определены автоматически

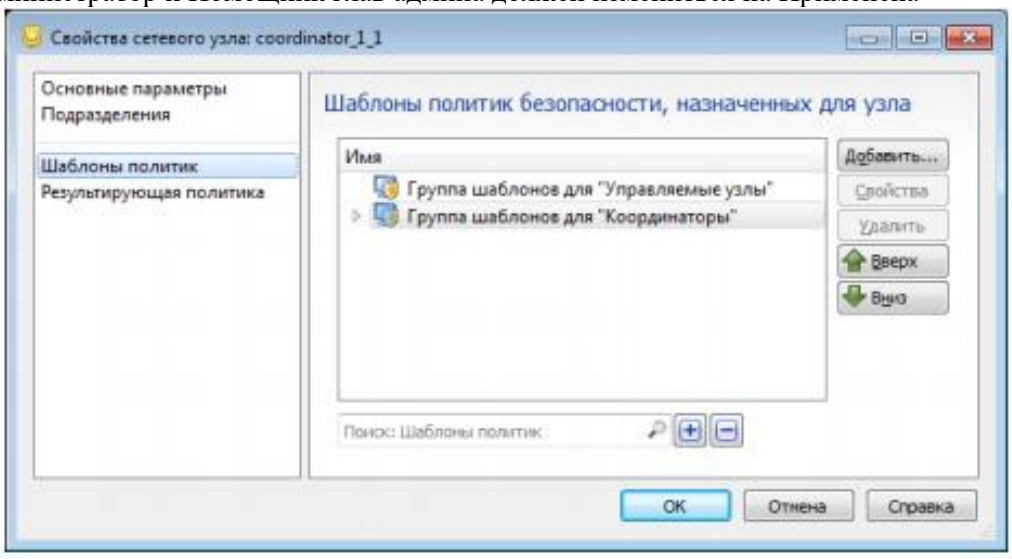


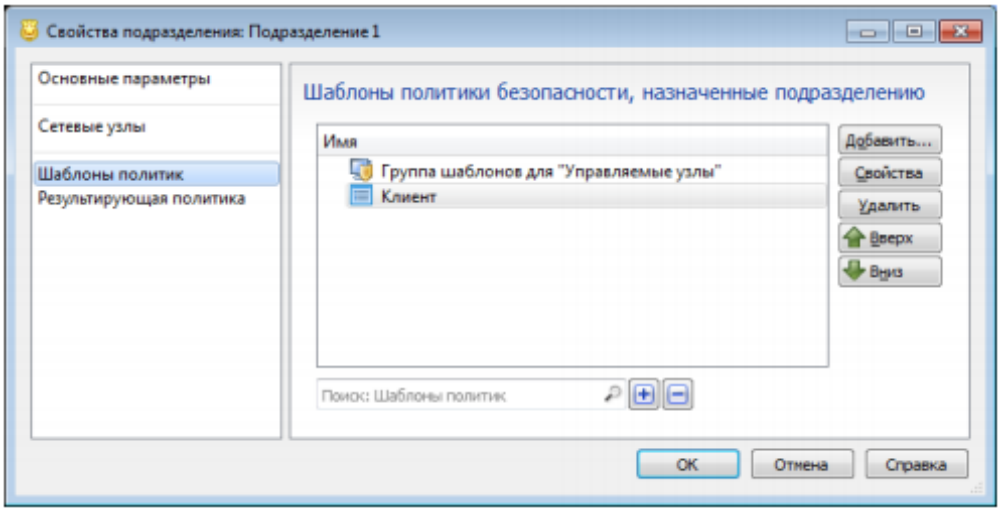
18. В окне программы ViPNet Policy Manager перейдите в раздел Шаблоны политики и нажмите кнопку Создать.
19. В открывшемся окне Свойства шаблона политики на вкладке Основные параметры задайте имя Запрет социальных сетей.
20. На вкладке Подразделения отметьте подразделения Центральный офис и Филиал
На вкладке Локальные фильтры открытой сети нажмите кнопку Создать...
21. В открывшемся окне Свойства фильтра открытой сети на вкладке Основные параметры задайте имя фильтра Запрет социальных сетей и установите переключатель в положение Блокировать трафик
22. На вкладке Назначения нажмите кнопку Добавить... р пы IP-адресов и выберите группу Социальные сети
23. 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
24. Отправьте политики на узлы. Для этого в окне программы
ViPNet Policy Manager перейдите в раздел Подразделения.
25. Выделите подразделения Центральный офис и Филиал, нажмите кнопку Отправить политики





На экран будет выведено окно Отправка политики. Не меняя параметров, нажмите кнопку ОК
Для контроля за ходом отправки политик на узлы в окне программы *ViPNet Policy Manager* перейдите в раздел Журналы → Отправка и применение политик. Статус политик на узлах Главный администратор и Помощник глав администратора должен измениться на Применена





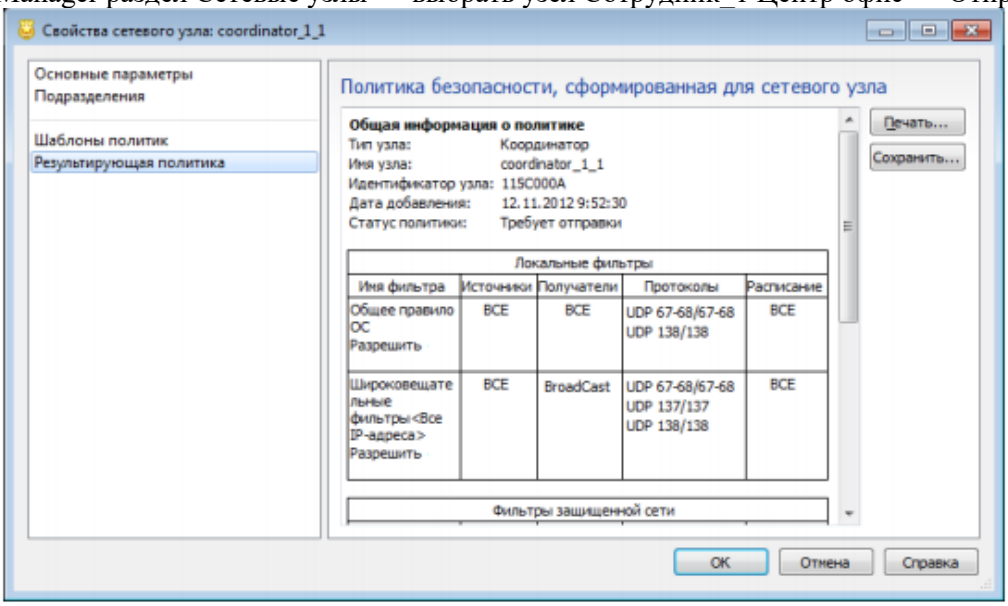
Для проверки применения политик на рабочих местах Главный администратор и Помощник глав админа зайдите в программу ViPNet Client Монитор Сетевые фильтры → Фильтры открытой сети. Убедитесь, что добавлен новый фильтр Запрет социальных сетей

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

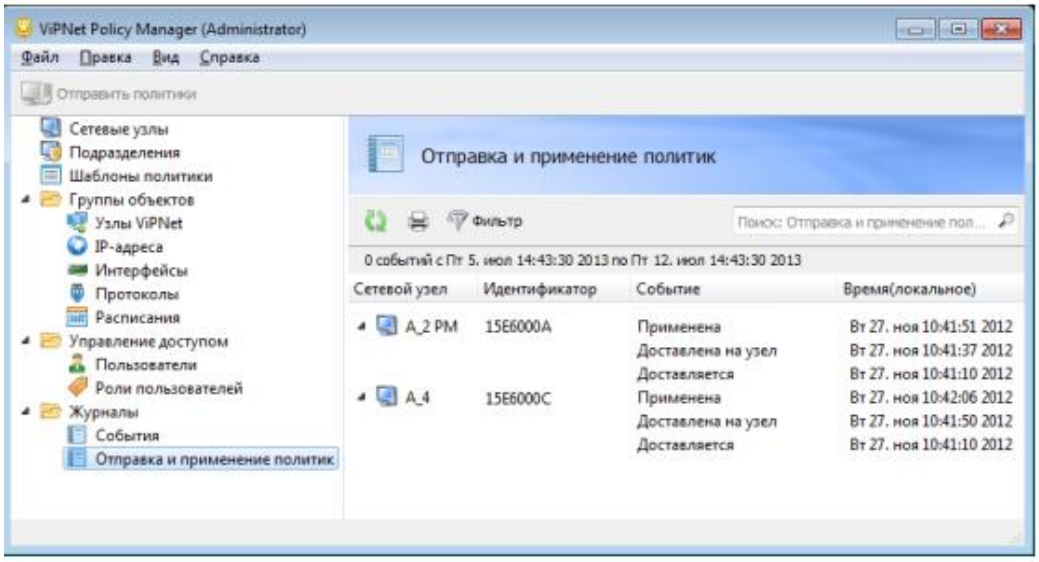
Для создания политики безопасности, блокирующей весь открытый трафик на рабочем месте Сотрудник_1 Центр офис, выполните следующие действия:

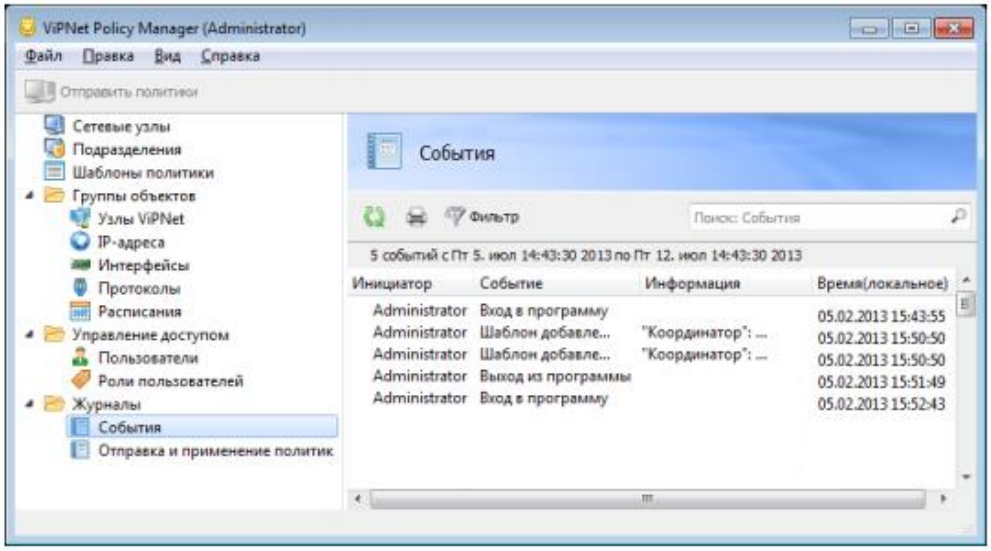
7. В окне программы ViPNet Policy Manager перейдите в раздел Шаблоны политики и нажмите кнопку Создать.
8. В открывшемся окне Свойства шаблона политики на вкладке Основные параметры задайте имя Блокировка открытого трафика.
9. На вкладке Сетевые узлы добавьте Сотрудник_1 Центр офис.
10. На вкладке Локальные фильтры открытой сети нажмите кнопку Создать…
11. В открывшемся окне Свойства фильтра открытой сети на вкладке Основные параметры задайте имя фильтра Блокировка открытого трафика, установите переключатель в положение Блокировать трафик и нажмите ОК
12. Остальные параметры окна Свойства фильтра открытой сети и Свойства шаблона политики менять не требуется.

Отправьте теперь политики на узел Сотрудник_1 Центр офис (в окне программы ViPNet Policy Manager раздел Сетевые узлы → выбрать узел Сотрудник_1 Центр офис → Отправить политики).



Проверить были ли приняты политики или нет в данном случае» получится, так как данный узел не был развернут.





16. Практическое занятие № 47 «Межсетевое взаимодействие»

Задание:

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

В рамках практического занятия необходимо смоделировать ситуацию, в которой компания с уже имеющейся сетью ViPNet решила организовать межсетевое взаимодействие с сетью ViPNet Федеральной службы для организации юридически значимого электронного документооборота посредством ПО ViPNet Деловая почта.

При организации межсетевого взаимодействия, как и при любой модификации сети, тем более реальной, стоит заранее продумывал все этапы запланированного мероприятия от начала до конца. Поэтому из уже имеющейся сети и сети Федеральной службы выделим только те сетевые узлы, которые нам понадобиться связать, и представим их в виде схемы

Данная схема должна быть реализована в виде стенда, собранного в соответствии

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

Установка ViPNet Coordinator в качестве межсетевого шлюза

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

Проверка доступности узлов в защищенной сети

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

Во вкладке Защищенная сеть отображаются сетевые узлы, с которыми есть связи. Проверьте доступность сетевых узлов. Для этого щелкните правой кнопкой мыши узел Главный администратор и выберите пункт Проверить соединение.

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

Первоначальная настройка межсетевого взаимодействия

В настоящем задании необходимо:

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

Предварительные настройки:

- Для подготовки к заданию выполните следующие действия:
- Проверьте, что на виртуальной машине VM_1 установлено ПО VipNet Administrator, VipNet Policy Manager и VipNet Client.
- Проверьте, что на виртуальной машине VM_2 установлено программное обеспечение VipNet Coordinator с установленными ключами пользователя Координатор Центр офис.
- На виртуальных машинах VM_3 и VM_4 удалите программное обеспечение VipNet (если оно было установлено ранее).

Развертывание защищенной сети Фед. Службы

1. Развернуть защищенную сеть Федеральной службы на базе виртуальных машин VM_3 и VM_4 (используя при этом второй комплект регистрационных файлов, которые были выданы на первом занятии).
2. Создать структуру сети в соответствии с предложенными ниже таблицами 1.5, 1.6 и 1.7.
3. Сформировать справочники и ключи и на основе созданных дистрибутивов ключей развернуть на виртуальных машинах Координатор Федеральной службы и Администратор ViPNet Федеральной службы.

Пояснение к заданию

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

Таблица Состав защищенной сети Федеральной службы

	Тип	Название	Расположение	Комментарии 1
1	Координатор	Координатор Федеральной службы	Федеральная служба	Для развертывания ПК ViPNet Coordinator
2	Клиент	Администратор ViPNet Федеральной службы		Для развертывания ПК ViPNet Administrator

3		Специалист по приёму отчётности		Рабочее место специалиста по приему отчетности

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

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

Таблица. Определение пользователей

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

Порядок выполнения задания:
Развертывание программного обеспечения ViPNet Центр управления сетью, ViPNet Удостоверяющий и ключевой центр, ViPNet Client и ViPNet Coordinator осуществляется в том же порядке, что и в предыдущих практических занятиях.
При настройке программ ViPNet задайте пароли:

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

Имя администратора VipNet Федеральной службы — Константин.
Настройка межсетевого взаимодействия с использованием индивидуального симметричного ММК
Настроить взаимодействие защищённой сети Компании и защищенной сети Федеральной службы таким образом, чтобы узлы Координатор Центр офис и Координатор. Федеральной службы могли взаимодействовать друг с другом по шифрованному каналу.

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

Пояснение к заданию

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

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

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

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

Организация межсетевого взаимодействия между сетями ViPNet состоит из следующих этапов:

1. Администратор первой сети ViPNet, инициирующий межсетевое взаимодействие, создает в Центре управления сетью файл мел сетевой информации, а в Удостоверяющем и ключевом центре межсетевой мастер-ключ. Затем по доверенным каналам связи он передает файл межсетевой информации и межсетевой маете ключ администратору второй сети ViPNet.
2. Администратор второй сети ViPNet принимает межсетевую информацию, затем создает файл с ответной межсетевой информацией и передает его администратору первой сети.
3. Администратор второй сети импортирует переданный ему межсетевой мастер-ключ.
4. Администратор первой сети завершает организацию межсетевого взаимодействия приемом ответной межсетевой информации.
5. Администратор каждой сети создаёт новые справочники и ключи и отправляет их на узлы своей сети.

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

Порядок выполнения задания

Инициация межсетевого взаимодействия

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

1. В окне ViPNet Центр управления сетью в меню Доверенные сети выберите пункт Установить взаимодействие. Будет запущен мастер Установка межсетевого взаимодействия.
2. На первой странице мастера выберите вариант Я инициатор межсетевого взаимодействия и нажмите кнопку Далее.
3. На странице Задайте информацию о другой сети ViPNet и координатор для связи с ней (необходимо правильно указать номер доверенной сети, с которой вы устанавливаете межсетевое взаимодействие, в противном случае могут возникнуть проблемы), впишите имя сети - Федеральная служба, которое будет отображаться в программе ViPNet Центр управления сетью, и выберите шлюзовой координатор своей сети - Координатор Центр офис. Затем нажмите Далее

4. На странице Укажите сетевые узлы своей сети ViPNet для связывания выберите узлы сети, которые будут участвовать во взаимодействии с узлами сети Федеральной службы — Главный администратор и Координатор Центр.
5. Центр управления сетью и шлюзовой координатор своей сети должны обязательно присутствовать в списке узлов для взаимодействия, их невозможно удалить. Выбрав узлы, нажмите кнопку Далее.
6. На странице Укажите пользователей своей сети ViPNet для связывания выберите пользователя Координатор Центр офис.
7. Если для межсетевого взаимодействия выбран сетевой узел, но не выбран ни один пользователь этого узла, сведения об этом узле не будут включены в межсетевую информацию. Исключениями являются Центр управления сетью и шлюзовой координатор. Выбрав пользователей, нажмите кнопку Далее.
8. На открывшейся странице Подготовка к сохранению межсетевой информации завершена при необходимости укажите комментарий для администратора сети Федеральной службы и нажмите кнопку Далее.
9. На странице Укажите файл для сохранения межсетевой информации нажмите кнопку Обзор и укажите каталог для сохранения файла межсетевой информации - Рабочий стол. Затем нажмите кнопку Далее.
10. На странице Сохранение межсетевой информации после завершения записи файла нажмите кнопку Далее, на следующей странице нажмите кнопку Готово.
Чтобы создать индивидуальный симметричный межсетевой мастер ключ, выполните следующие действия:
1. В окне программы ViPNet Удостоверяющий и ключевой центр на панели навигации выберите представление Ключевой центр
2. Перейдите в раздел с номером доверенной сети, для связи с которой будет использоваться межсетевой мастер-ключ, и на панели инструментов нажмите кнопку Создать.
3. Появится окно с сообщением о необходимости согласования мастер-ключа с администратором доверенной сети. Нажмите в данном окне кнопку Да. В результате межсетевой мастер-ключ будет создан и отобразится в соответствующем разделе
4. Щелкните по созданному межсетевой мастер-ключу правой кноп кой мыши и в контекстном меню выберите пункт Экспорт.
5. Появится окно ввода пароля. Укажите в нем пароль - 11111111 и нажмите кнопку ОК. На указанном пароле будет зашифрован экспортируемый ключ.
6. В появившемся окне укажите каталог, в который будет сохранен межсетевой мастер-ключ - Рабочий стал, затем нажмите кнопку ОК.
7. Передайте доверенным способом файл межсетевой информации с расширением*. lzh, межсетевой мастер-ключ «net ****.key» и пароль, на котором зашифрован межсетевой мастер-ключ - 11111111, администратору сети Федеральной службы.
Прием первичной межсетевой информации
Чтобы принять межсетевую информацию перейдите на рабочее место администратора сети Федеральной службы и выполните следующие действия:
1. В окне программы ViPNet Центр управления сетью в меню Доверенные сети выберите пункт Установить взаимодействие. Запустится мастер Установка межсетевого взаимодействия.
2. На первой странице мастера выберите вариант Я принимаю файл с межсетевой информацией и нажмите кнопку Далее.
3. На странице Загрузка межсетевой информации из файла укажите файл с межсетевой информацией, полученный от Главного администратора сети ViPNet Компании, который инициировал межсетевое взаимодействие. После указания файла в окне мастера появится предупреждение, что взаимодействие с сетью не установлено
4. Чтобы продолжить загрузку межсетевой информации, нажмите кнопку Установить взаимодействие.

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

1. В окне программы на панели навигации выберите представление Ключевой центр и прейдите в раздел с номером доверенной сети, из которой поступил данный мастер-ключ.
2. На панели инструментов нажмите кнопку Загрузить.
3. При импорте ИСММК «net ****.key» появится окно ввода пароля. Введите пароль, на котором был зашифрован данный ключ - 11111111. При правильном вводе пароля мастер-ключ будет импортирован.
   Импортированный мастер-ключ будет сразу добавлен в список межсетевых мастер-ключей выбранного раздела.
   После того, как ключ будет импортирован, в УКЦ необходимо зайти в раздел Межсетевое взаимодействие выбрать строку с ИСММК, щелкнуть по строке правой кнопкой мыши и выбрать пункт Использовать.
4. Подготовьте сертификаты администраторов и списки аннулированных сертификатов вашей сети для передачи в доверенную сеть (сеть Компании) в составе ответной межсетевой информации. Для этого в программе ViPNet Удостоверяющий и ключевой центр в меню Сервис выберите пункт Экспорт межсетевой информации.
5. В программе ViPNet Центр управления сетью в представлении Доверенные сети выберите раздел Свойства сетей.
6. На панели просмотра щелкните правой кнопкой мыши добавленную доверенную сеть и в контекстном меню выберите пункт Создать межсетевую информацию
   В появившемся окне нажмите кнопку Создать.
7. После создания ответной межсетевой информации сохраните ее на жесткий диск. Для этого снова щелкните доверенную сеть правой кнопкой мыши и в контекстном меню выберите пункт Сохранить межсетевую информацию в файл, затем в окне Сохранить как укажите папку для сохранения файла межсетевой информации *****-****.lzh — Рабочий стол.
8. Создайте новые справочники и ключи для узлов сети Федеральной службы, участвующих в межсетевом взаимодействии - Администратор ViPNet Федеральной службы и Координатор Федеральной службы, и отправьте их на узлы.
9. Передайте администратору сети Компании созданный файл межсетевой информации *****-****.lzh

Завершение организации межсетевого взаимодействия

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

1. Получите у администратора доверенной сети ViPNet Федеральной службы файл, содержащий ответную межсетевую информацию ****-****.lzh.
2. В окне программы ViPNet Центр управления сётью в меню Доверенные сети выберите пункт Загрузить межсетевую информацию из файла.
3. В окне Загрузка межсетевой информации укажите файл межсетевой информации, полученной от администратора другой сети ViPNet, и следуйте мастеру, нажимая кнопку Далее, а на заключительном шаге — Готово.
4. Примите ответную межсетевую информацию с помощью мастера Обработка межсетевой информации.
5. В окне программы ViPNet Удостоверяющий и ключевой центр перейдите в представление Администрирование и на панели навигации выберите раздел Необработанные данные → Контейнеры сертификатов администраторов сетей VipNet.
6. На панели просмотра выберите контейнер *Федеральная служба* и на панели инструментов нажмите *Обработать.*
7. В появившемся окне будет представлен список администраторов, сертификаты и CRL которых содержатся в выбранных контейнерах Выберите администратора Константин и нажмите кнопку Импортировать.
8. В окне программы ViPNet Удостоверяющий и ключевой центр в представлении Ключевой центр выберите раздел Межсетевое взаимодействие Федеральная служба.
9. Выберите межсетевой мастер-ключ и щелкните по нему правой кнопкой мыши. В контекстном меню выберите команду Текущий для ввода межсетевого мастер-ключа в действие.
10. Для узлов сети Компании, участвующих в межсетевом взаимодействии, Главный администратор и Координатор Центр офис, создайте и отправьте новые справочники и ключи.
11. Проверьте взаимодействие узлов Координатор Федеральной службы (сеть Федеральной службы) и Координатор Центр офис (сеть Компании).
12. На рабочем месте Главного администратора (сеть Компании) отправьте межсетевую информацию по защищенному каналу.
13. Убедитесь, что межсетевая информация поступила в ЦУС Федеральной службы и обработайте ее.

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

Эталон ответа:

Задание:

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

В рамках практического занятия необходимо смоделировать ситуацию, в которой компания с уже имеющейся сетью ViPNet решила организовать межсетевое взаимодействие с сетью ViPNet Федеральной службы для организации юридически значимого электронного документооборота посредством ПО ViPNet Деловая почта.

При организации межсетевого взаимодействия, как и при любой модификации сети, тем более реальной, стоит заранее продумывал все этапы запланированного мероприятия от начала до конца. Поэтому из уже имеющейся сети и сети Федеральной службы выделим только те сетевые узлы, которые нам понадобиться связать, и представим их в виде схемы

В реальной ситуации количество узлов, которые потребуется связать, может оказаться

гораздо больше, и поэтому вовсе не обязательно их отражать на схеме, однако общую модель и план действия лучше составить, а остальные связи узлов проработать в виде таблицы.

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

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

Установка ViPNet Coordinator в качестве межсетевого шлюза

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

Проверка доступности узлов в защищенной сети

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

Во вкладке Защищенная сеть отображаются сетевые узлы, с которыми есть связи. Проверьте доступность сетевых узлов. Для этого щелкните правой кнопкой мыши узел Главный администратор и выберите пункт Проверить соединение.

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

Первоначальная настройка межсетевого взаимодействия

В настоящем задании необходимо:

3. Развернуть защищенную сеть Федеральной службы.
4. 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).

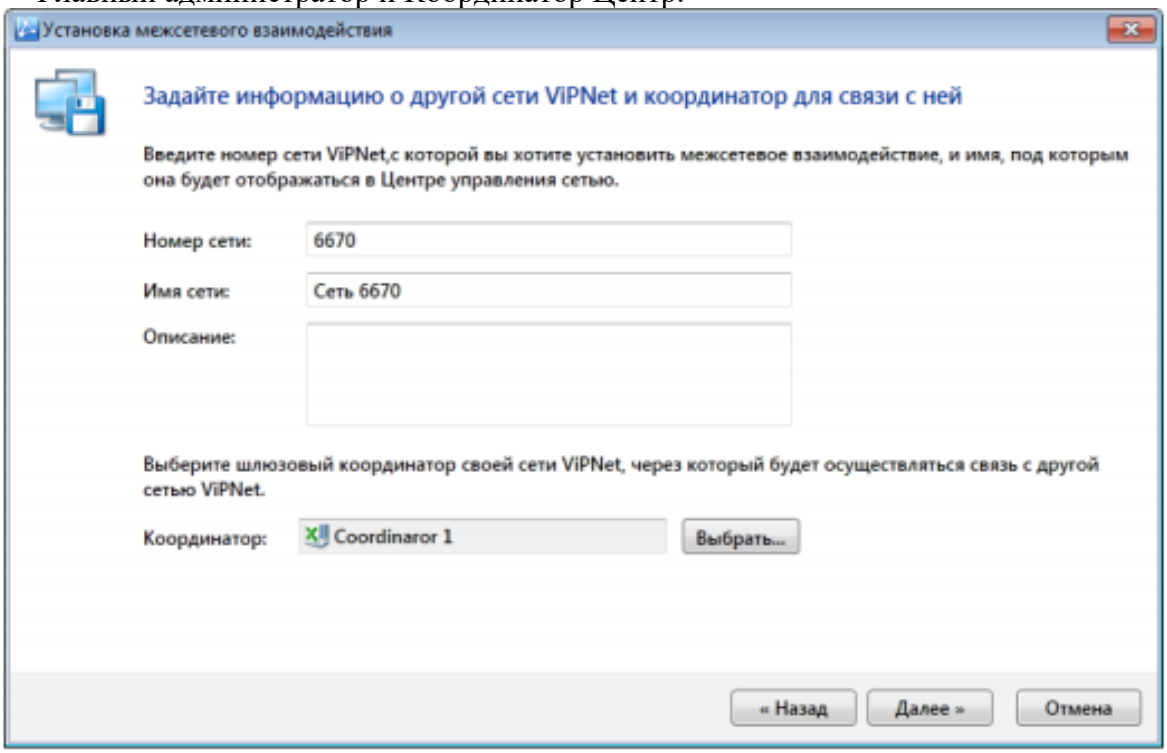
Развертывание защищенной сети Фед. Службы

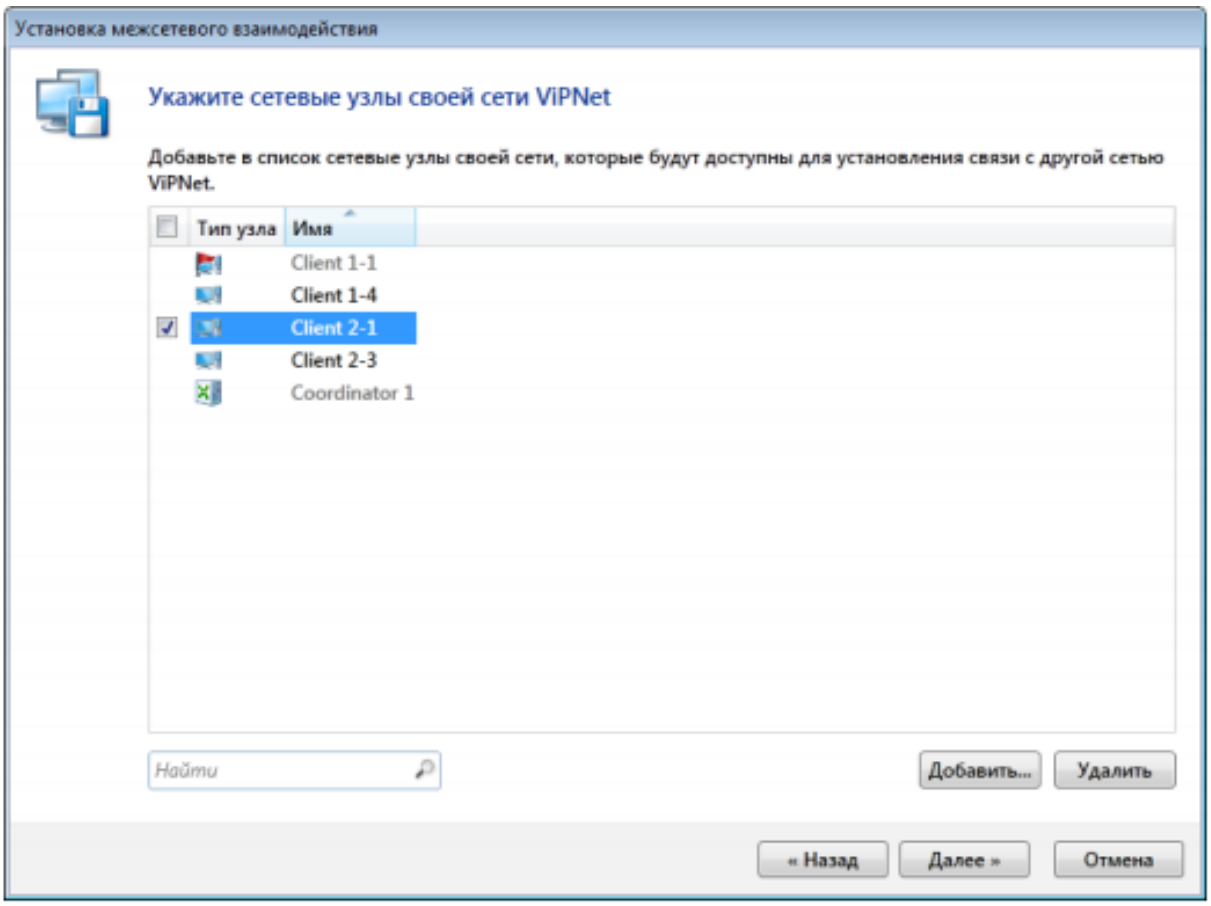
4. Развернуть защищенную сеть Федеральной службы на базе виртуальных машин VM_3 и VM_4 (используя при этом второй комплект регистрационных файлов, которые были выданы на первом занятии).
5. Создать структуру сети в соответствии с предложенными ниже таблицами 1.5, 1.6 и 1.7.
6. Сформировать справочники и ключи и на основе созданных дистрибутивов ключей развернуть на виртуальных машинах Координатор Федеральной службы и Администратор ViPNet Федеральной службы.

Инициация межсетевого взаимодействия

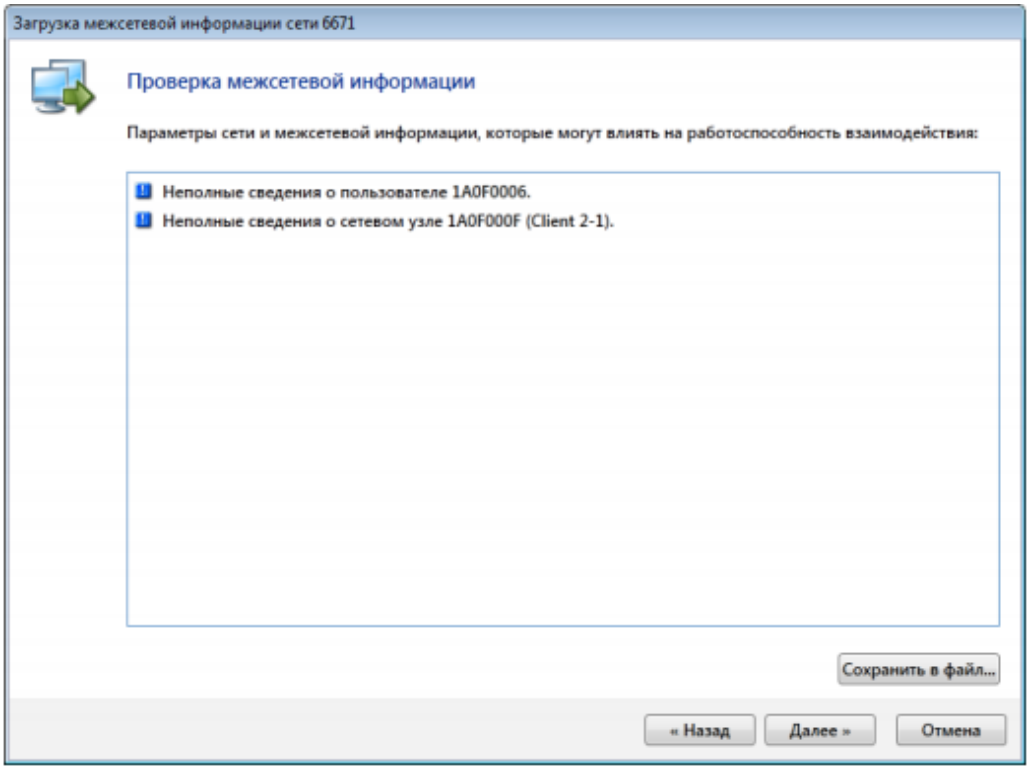
Чтобы инициировать межсетевое взаимодействие с сетью ViPNet Федеральной службы, выполните следующие действия на рабочем месте Главный администратор сети Компании:

11. В окне ViPNet Центр управления сетью в меню Доверенные сети выберите пункт Установить взаимодействие. Будет запущен мастер Установка межсетевого взаимодействия.
12. На первой странице мастера выберите вариант Я инициатор межсетевого взаимодействия и нажмите кнопку Далее.
13. 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. 1.130).
14. 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.





15. Центр управления сетью и шлюзовой координатор своей сети должны обязательно присутствовать в списке узлов для взаимодействия, их невозможно удалить. Выбрав узлы, нажмите кнопку Далее.
16. На странице Укажите пользователей своей сети ViPNet для связывания выберите пользователя Координатор Центр офис.
17. 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.
18. На открывшейся странице Подготовка к сохранению межсетевой информации завершена при необходимости укажите комментарий для администратора сети Федеральной службы и нажмите кнопку Далее.
19. 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.



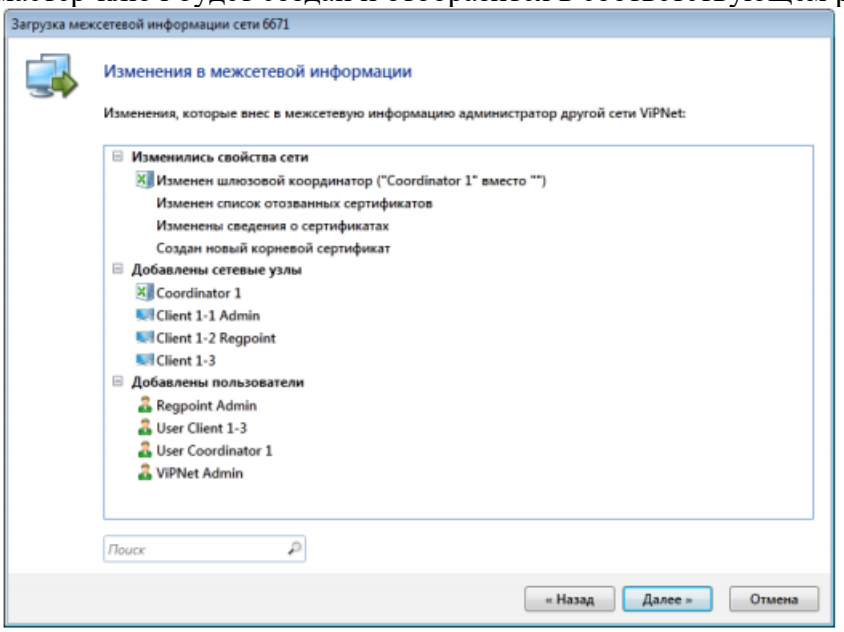
20. На странице Сохранение межсетевой информации после завершения записи файла нажмите кнопку Далее, на следующей странице нажмите кнопку Готово.

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

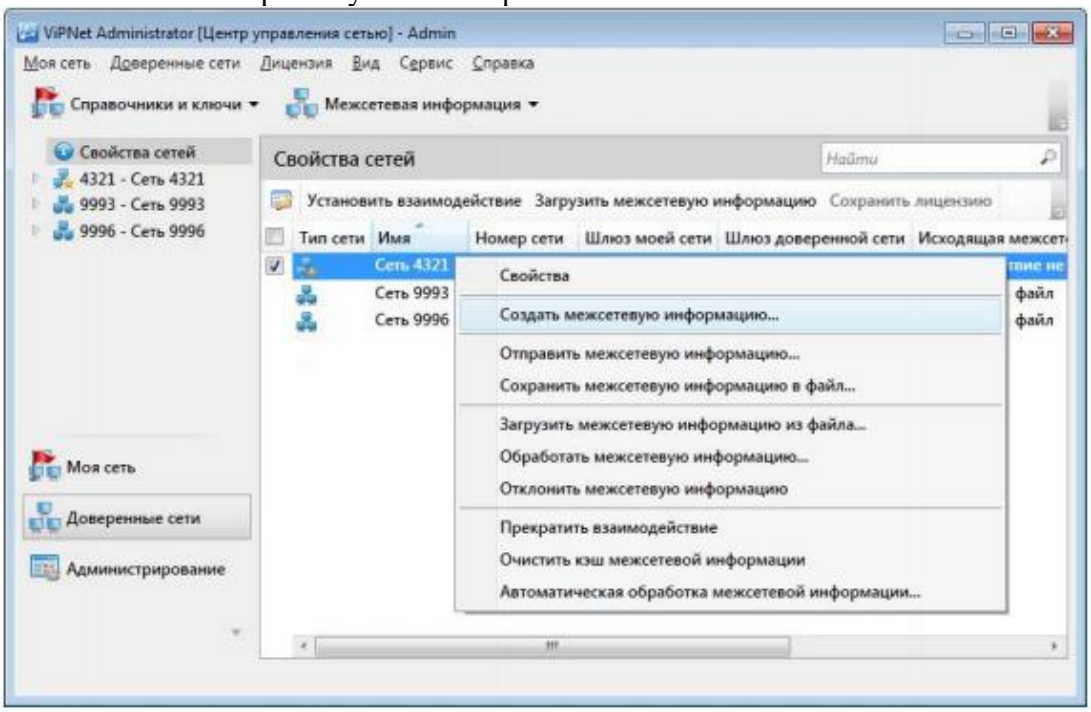
8. В окне программы ViPNet Удостоверяющий и ключевой центр на панели навигации выберите представление Ключевой центр

9. Перейдите в раздел с номером доверенной сети, для связи с которой будет использоваться межсетевой мастер-ключ, и на панели инструментов нажмите кнопку Создать.

10. Появится окно с сообщением о необходимости согласования мастер-ключа с администратором доверенной сети. Нажмите в данном окне кнопку Да. В результате межсетевой мастер-ключ будет создан и отобразится в соответствующем разделе



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



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

Прием первичной межсетевой информации

Чтобы принять межсетевую информацию перейдите на рабочее место администратора сети Федеральной службы и выполните следующие действия:
11. В окне программы ViPNet Центр управления сетью в меню Доверенные сети выберите пункт Установить взаимодействие. Запустится мастер Установка межсетевого взаимодействия.
12. На первой странице мастера выберите вариант Я принимаю файл с межсетевой информацией и нажмите кнопку Далее.
13. 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
14. Чтобы продолжить загрузку межсетевой информации, нажмите кнопку Установить взаимодействие.
15. На странице Задайте информацию о другой сети ViPNet и координатор для связи с ней выберите шлюзовой координатор - Координатор Федеральной службы, затем нажмите Далее.
16. 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.
17. 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 невоз-

можна. В этом случае обратитесь к администратору доверенной сети для устранения конфликтов.
18. Чтобы продолжить обработку межсетевой информации, нажмите кнопку Далее.
19. На странице Загрузка межсетевой информации после завершения обработки информации нажмите кнопку Готово.
20. В представлении Доверенные сети выберите Сеть №**** (вместо звездочек будет номер сети, инициировавшей межсетевое взаимодействие) и перейдите на вкладку Пользователи. В свойствах пользователя Координатор Центр офис на вкладке Связи с пользователями установите связь с Координатор Федеральной службы
После приема первичной межсетевой информации в ПО VipNet УКЦ импортируйте переданный Главным администратором Компании межсетевой мастер-ключ:

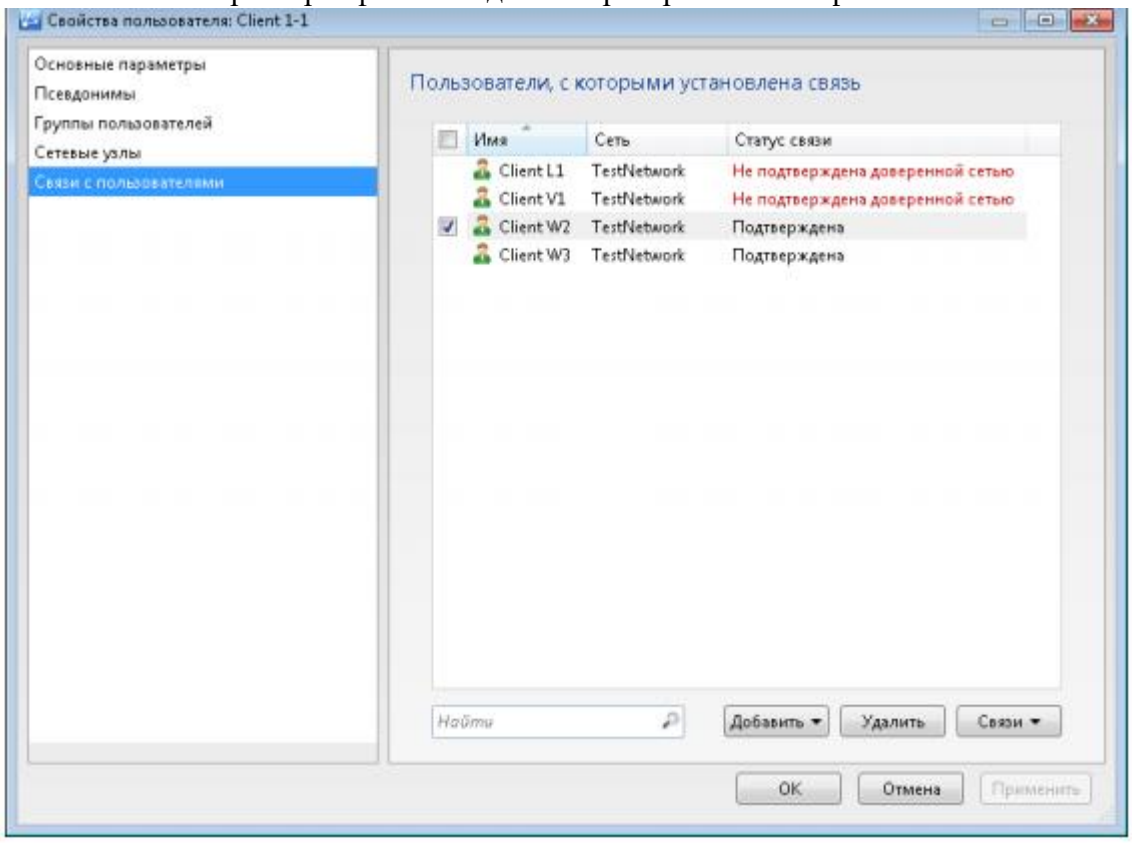
10. В окне программы на панели навигации выберите представление Ключевой центр и прейдите в раздел с номером доверенной сети, из которой поступил данный мастер-ключ.
11. На панели инструментов нажмите кнопку Загрузить.
12. При импорте ИСММК «net ****.key» появится окно ввода пароля. Введите пароль, на 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.

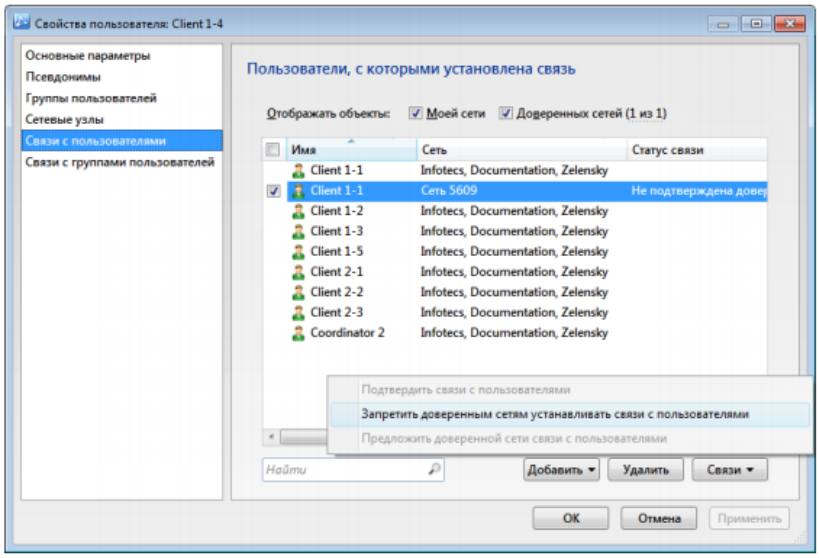
13. Подготовьте сертификаты администраторов и списки аннулированных сертификатов вашей сети для передачи в доверенную сеть (сеть Компании) в составе ответной межсетевой информации. Для этого в программе ViPNet Удостоверяющий и ключевой центр в меню Сервис выберите пункт Экспорт межсетевой информации.
14. В программе ViPNet Центр управления сетью в представлении Доверенные сети выберите раздел Свойства сетей.
15. На панели просмотра щелкните правой кнопкой мыши добавленную доверенную сеть и в контекстном меню выберите пункт Создать межсетевую информацию
16. В появившемся окне нажмите кнопку Создать.
17. 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.
18. 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.
19. Передайте администратору сети Компании созданный файл межсетевой информации *****-****.lzh

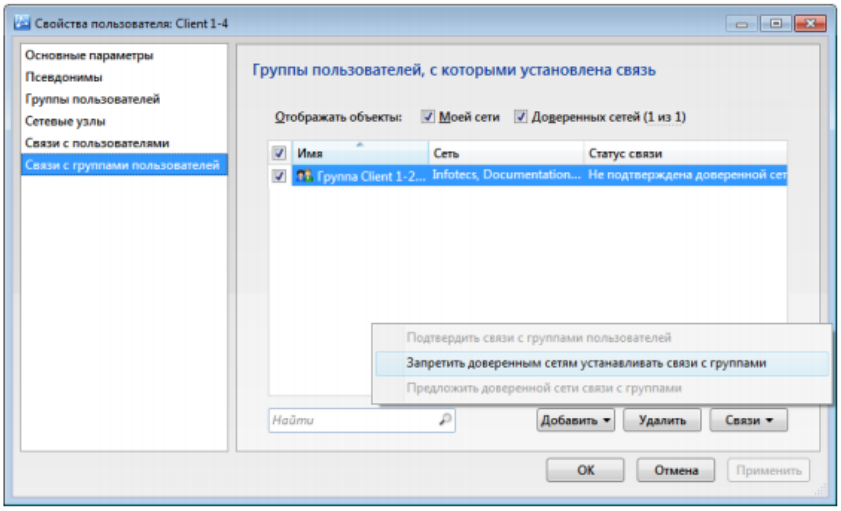
Завершение организации межсетевого взаимодействия
Чтобы принять ответную межсетевую информацию и завершить организацию взаимодействия, выполните следующие действия на рабочем месте Главный администратор (сеть Компании):
14. Получите у администратора доверенной сети ViPNet Федеральной службы файл, содержащий ответную межсетевую информацию ****-****.lzh.
15. В окне программы ViPNet Центр управления сётью в меню Доверенные сети выберите пункт Загрузить межсетевую информацию из файла.

16. В окне Загрузка межсетевой информации укажите файл межсетевой информации, полученной от администратора другой сети ViPNet, и следуйте мастеру, нажимая кнопку Далее, а на заключительном шаге — Готово.
17. Примите ответную межсетевую информацию с помощью мастера Обработка межсетевой информации
18. В окне программы ViPNet Удостоверяющий и ключевой центр перейдите в представление Администрирование и на панели навигации выберите раздел Необработанные данные → Контейнеры сертификатов администраторов сетей VipNet.



19. На панели просмотра выберите контейнер *Федеральная служба* и на панели инструментов нажмите *Обработать*
20. В появившемся окне будет представлен список администраторов, сертификаты и CRL которых содержатся в выбранных контейнерах Выберите администратора Константин и нажмите кнопку Импортировать
21. В окне программы ViPNet Удостоверяющий и ключевой центр в представлении Ключевой центр выберите раздел Межсетевое взаимодействие Федеральная служба.
22. Выберите межсетевой мастер-ключ и щелкните по нему правой кнопкой мыши. В контекстном меню выберите команду Текущий для ввода межсетевого мастер-ключа в действие.
23. Для узлов сети Компании, участвующих в межсетевом взаимодействии, Главный администратор и Координатор Центр офис, создайте и отправьте новые справочники и ключи.
24. Проверьте взаимодействие узлов Координатор Федеральной службы (сеть Федеральной службы) и Координатор Центр офис (сеть Компании).
25. На рабочем месте Главного администратора (сеть Компании) отправьте межсетевую информацию по защищенному каналу.
26. 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.





17.Практическое занятие № 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 бух-галтера 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.).

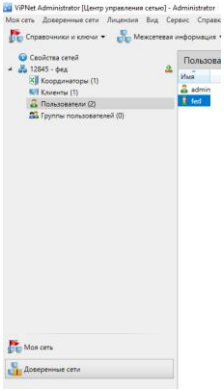


Рис. Пользователь «Координатор Фед службы»
3. В открывшемся окне перейдите на вкладку Связи с пользователями и добавьте в список пользователей Сотрудник 1 Центр Кузнецов, Зам бухгалтера Захарова, Директор Абросимов (рис

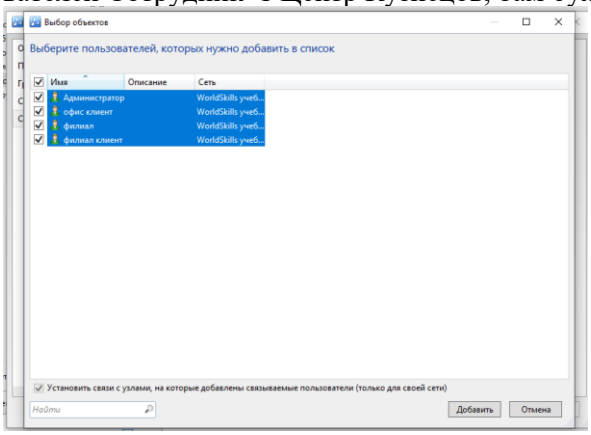


Рис. Добавление связей пользователю «Координатор Фед службы»
4. В представлении Доверенные сети выберите раздел Свойства сетей.
5. На панели просмотра щелкните правой кнопкой мыши на доверенную сеть Федеральная служба и в контекстном меню выберите пункт Создать межсетевую информацию. В открывшемся окне установите флажок Отправить межсетевую информацию после создания и нажмите кнопку Создать (рис.)

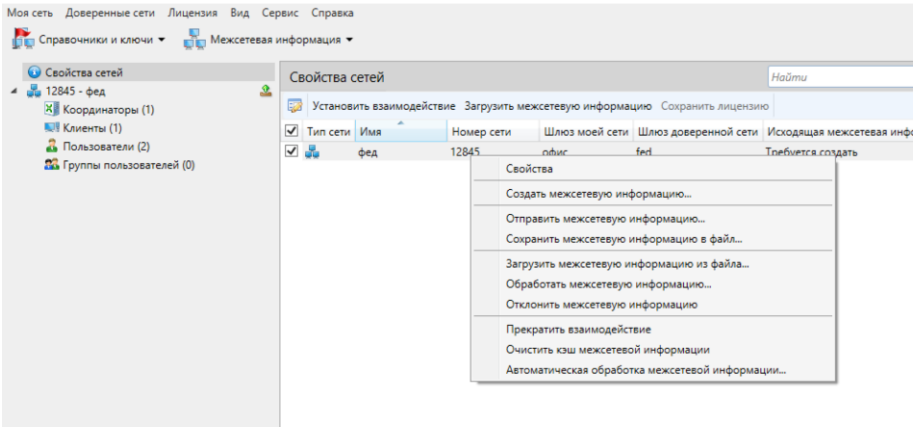


рис. Создание межсетевой информации для сети Фед. службы

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):

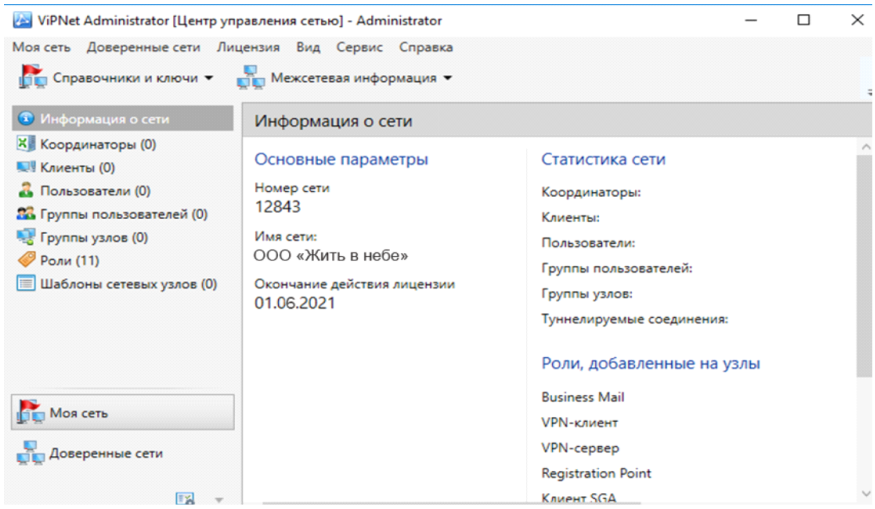
1. В окне программы ViPNet Центр управления сетью в представлении Доверенные сети выберите сеть Федеральная служба и перейдите на вкладку пользователи.
2. Зайти в свойства пользователя Координатор Фед. службы.
3. В открывшемся окне перейдите на вкладку Связи с пользователями и удалите из списка пользователей 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.

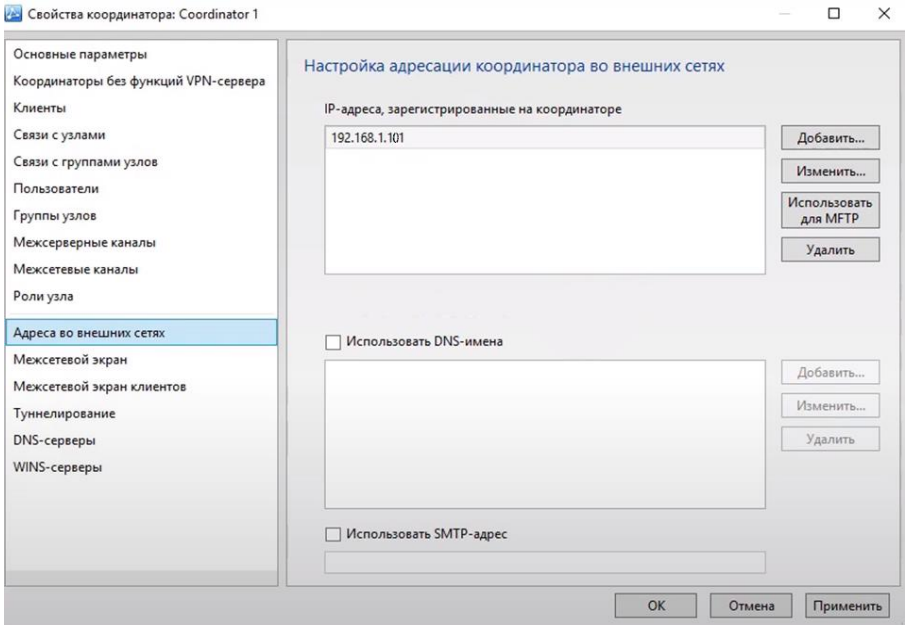
Чтобы принять межсетевую информацию от сети Компании, перейдите на рабочее место администратора сети Федеральной службы и выполните следующие действия:

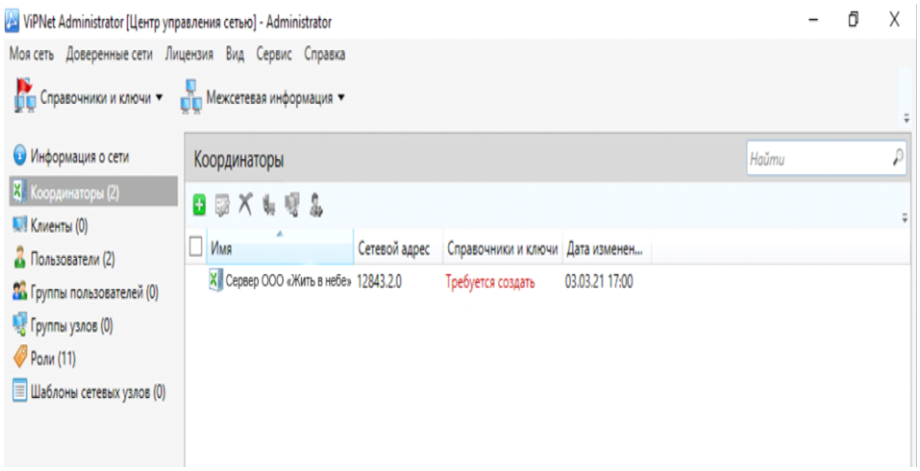
1. В окне программы ViPNet Центр управления сетью в меню Доверенные сети выберите пункт Обработать межсетевую информацию.

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.

Эталон ответа:







18.Практическое занятие № 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.

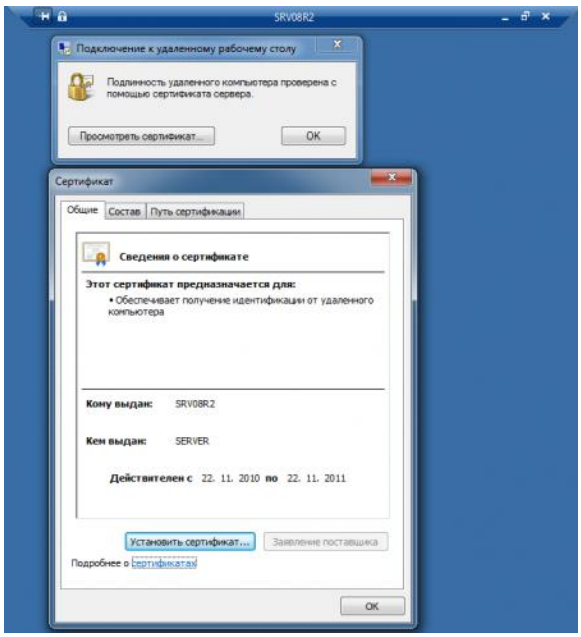
7. Для шифрования SSL создадим и откроем файл:
   sudo nano /etc/httpd/conf.d/non-ssl.conf
8. Внутри создайте `VirtualHost`блок для соответствия запросов на порт 80. Внутри используйте `ServerName`директиву, чтобы снова соответствовать вашему доменному имени или IP-адресу. Затем используйте `Redirect`для соответствия любым запросам и отправьте их на SSL `VirtualHost`. Не забудьте включить конечную косую черту:
   /etc/apache2/sites-available/000-default.conf

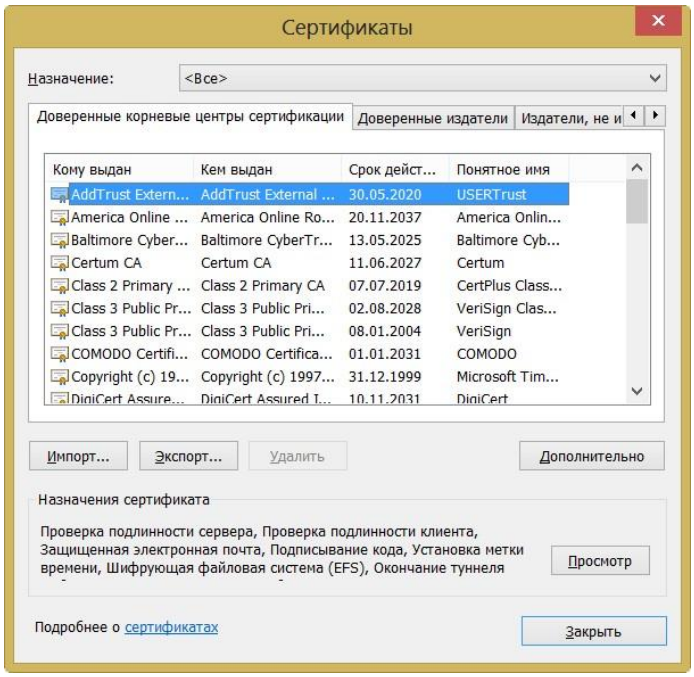
```
<VirtualHost *:80>
        ServerName www.example.com
        Redirect "/" "https://www.example.com/"
</VirtualHost>
```

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.

Эталон ответа:





19.Практическое занятие № 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 подходящим 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.

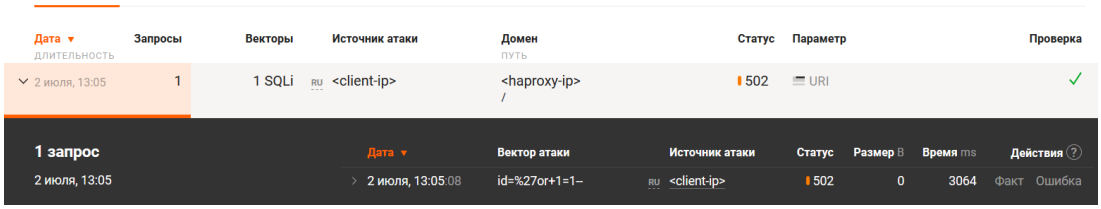
5. Чтобы применить новую конфигурацию, отправьте сигнал reload nginx'у, как описывалось в предыдущих разделах.

В отчет вставить скриншоты с командами и результатом выполнения.
В помощь к работе: https://nginx.org/ru/docs/beginners_guide.html

Эталон ответа:

Скриншот конфигурации nginx:

```
server {
  listen 80;
  listen [::]:80 ipv6only=on;

  # the domains for which traffic is processed
  server_name example.com;
  server_name www.example.com;

  # turn on the monitoring mode of traffic processing
  wallarm_mode monitoring;

  location / {
    # setting the address for request forwarding
    proxy_pass http://10.80.0.5;
    proxy_set_header Host $host;
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
  }
}
```



20. Практическое занятие № 61 «Установка системы обнаружения и предотвращения вторжения Snort»

Задание:

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-1.0.7.tar.gz
4. Загрузка займёт несколько секунд. По завершении исходный код нужно извлечь из архива и перейти в новый каталог:
tar -xvzf daq-1.0.7.tar.gz
cd daq-1.0.7
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-1.9.16.tar.gz
9. После завершения загрузки извлеките исходный код и перейдите в каталог:
tar -xvzf snort-1.9.16.tar.gz
cd snort-1.9.16
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-1.9.16/etc/*.conf* /etc/snort
sudo cp ~/snort_src/snort-1.9.16/etc/*.map /etc/snort
В отчёт вставить скриншот с результатом.
Затем нужно загрузить правила обнаружения, которыми Snort будет следовать для выявления потенциальных угроз. Snort предоставляет три уровня набора правил:

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

18. Для быстрого тестирования Snort можно скачать правила:
wget https://www.snort.org/rules/community -O ~/community.tar.gz
19. Извлекаем правила и копируем в конфигурационную папку:
sudo tar -xvf ~/community.tar.gz -C ~/
sudo cp ~/community-rules/* /etc/snort/rules
В отчёт вставить скриншот с результатом.
20. По умолчанию Snort ожидает некоторые правила, которые не включены в файл правил. С помощью следующей команды можно закомментировать ненужные строки в файле правил:
sudo sed -i 's/include \$RULE_PATH/#include \$RULE_PATH/' /etc/snort/snort.conf
21. Далее вам нужно зарегистрироваться на сайте Snort, зайти на него под своим аккаунтом, открыть данные своего аккаунта, перейти в Oinkcode, скопировать данный код и в следующую команду его вставить:
wget https://www.snort.org/rules/snortrules-snapshot-29160.tar.gz?oinkcode=oinkcode -O ~/registered.tar.gz
В отчёт вставить скриншот с результатом.
22. Регистрация нужна для загрузки правил. Далее распаковываем в папку:
sudo tar -xvf ~/registered.tar.gz -C /etc/snort
23. После установки отредактируем конфигурационный файл:
sudo nano /etc/snort/snort.conf
24. Найдите разделы, которые указаны ниже и измените параметры по образцу:

```
# Setup the network addresses you are protecting
ipvar HOME_NET 10.0.1.15/24
# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET !$HOME_NET
# Path to your rules files (this can be a relative path)
var RULE_PATH /etc/snort/rules
var SO_RULE_PATH /etc/snort/so_rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules
# Set the absolute path appropriately
var WHITE_LIST_PATH /etc/snort/rules
var BLACK_LIST_PATH /etc/snort/rules
```

25. В шестом разделе измените следующее:
unified2
Recommended for most installs
output unified2: filename snort.log, limit 128
В отчёт вставить скриншот с результатом.
26. Далее найдите список включённых наборов правил. Раскомментируйте следующую строку для возможности загружать пользовательские правила:
include $RULE_PATH/local.rules
27. Также можно добавить строку:
include $RULE_PATH/community.rules
28. Сохраните и выйдите.
В отчёт вставить скриншот с результатом.
29. Проверьте конфигурацию:
sudo snort -T -c /etc/snort/snort.conf
30. После запуска проверки должен появиться текст похожий на:

```
--== Initialization Complete ==--
,,_     -*> Snort! <*-
o"  )~   Version 1.9.16 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: 1.1.11
Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.1
Preprocessor Object: SF_DCERPC2  Version 1.0
Preprocessor Object: SF_SSH  Version 1.1
Preprocessor Object: SF_FTPTELNET  Version 1.2
Preprocessor Object: SF_SDF  Version 1.1
Preprocessor Object: SF_DNP3  Version 1.1
Preprocessor Object: SF_REPUTATION  Version 1.1
Preprocessor Object: SF_IMAP  Version 1.0
Preprocessor Object: SF_SMTP  Version 1.1
Preprocessor Object: SF_GTP  Version 1.1
Preprocessor Object: appid  Version 1.1
Preprocessor Object: SF_MODBUS  Version 1.1
Preprocessor Object: SF_POP  Version 1.0
Preprocessor Object: SF_DNS  Version 1.1
Preprocessor Object: SF_SSLPP  Version 1.1
Preprocessor Object: SF_SIP  Version 1.1
```

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

В отчёт вставить скриншот с результатом.

31. Для проверки Snort на регистрацию предупреждений добавьте предупреждение:

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

32. Следующую строку в файл:

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

В отчёт вставить скриншот с результатом.

33. Правило состоит из следующих частей:

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

Сохраните, выйдите.

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

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

Для проверки интерфейса можно воспользоваться командой:

ip addr

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

07/12-11:20:33.501624 [**] [1:10000001:1] ICMP test [**] [Priority: 0] {ICMP}
83.136.251.119 -> 80.69.173.202

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

35. Прочитать логи можно с помощью команды внизу:

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

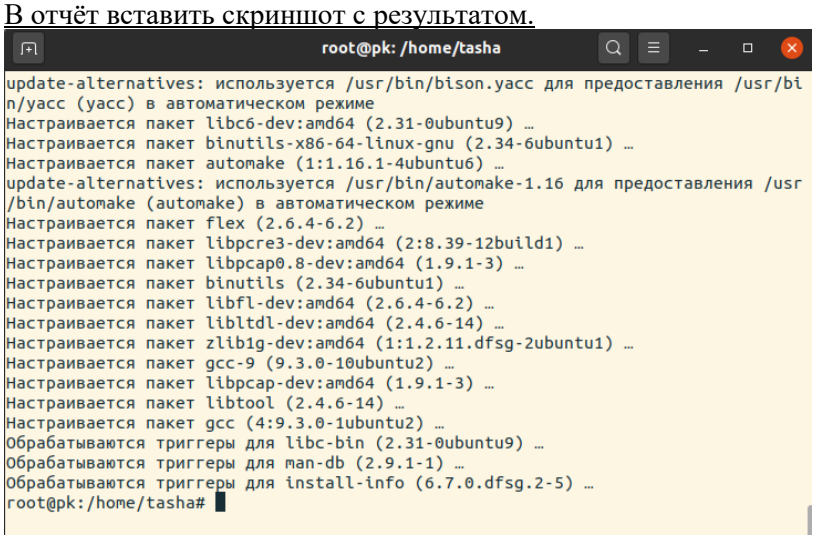
В отчёт вставить скриншот с результатом.
36. Для запуска snort в фоновом режиме в качестве службы нужно отредактировать следующий файл:

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

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

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

Следующей командой перезагрузите демон systemctl:
sudo systemctl daemon-reload
37. Затем выполните старт snort:
sudo systemctl start snort
38. Увидеть статус можно следующей командой:
sudo systemctl status snort
В отчёт вставить скриншот с результатом.
Система обнаружения вторжений установлена и протестирована.

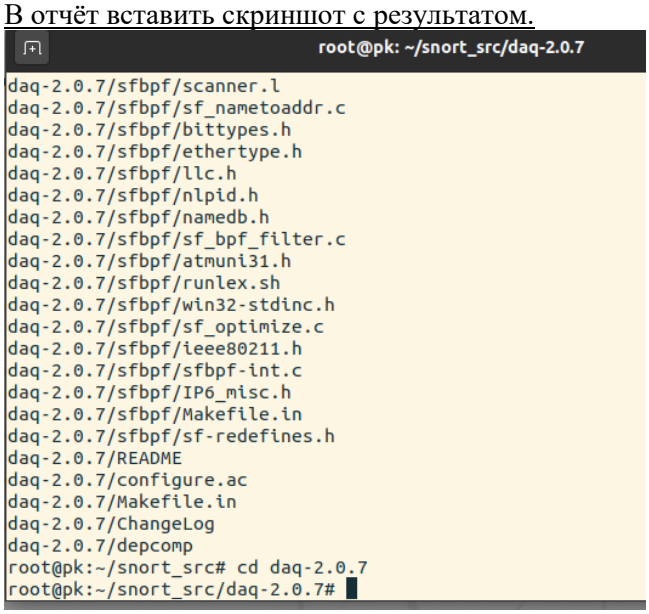
Эталон ответа:

Задание:
1. 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.

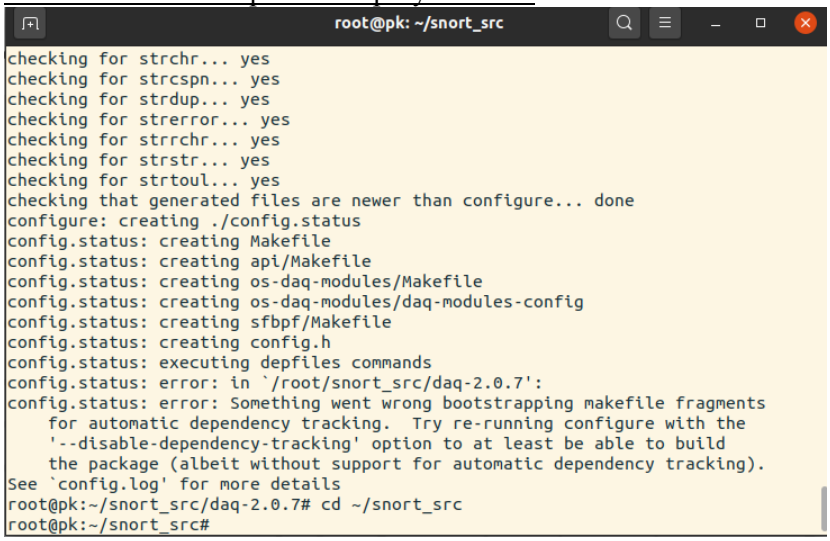


2. Установка состоит из нескольких шагов:
Загрузка кода, его настройка, компиляция кода, установка его в соответствующих каталог и настройка правил обнаружения.
Создадим временную папку для загрузки:
mkdir ~/snort_src && cd ~/snort_src
3. Snort использует библиотеку сбора данных DAQ. Загрузите последний пакет с веб-сайта с помощью команды wget:
wget https://www.snort.org/downloads/snort/daq-1.0.7.tar.gz

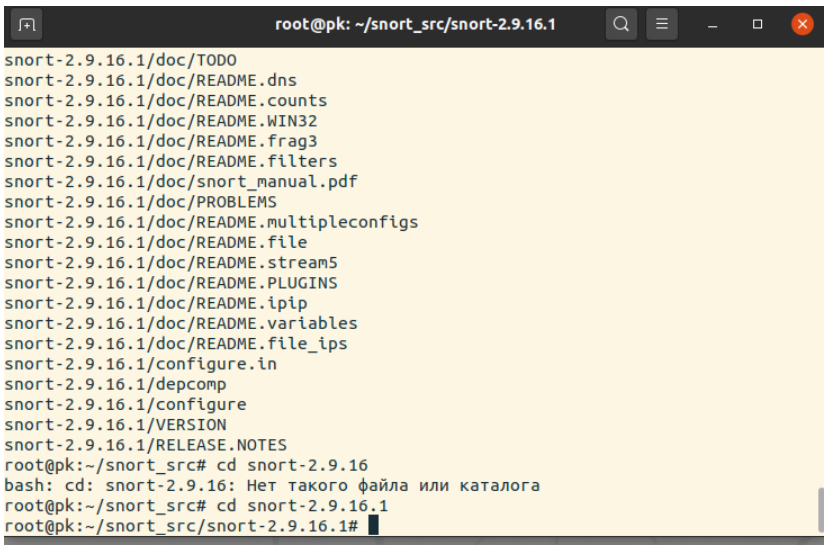
4. Загрузка займёт несколько секунд. По завершении исходный код нужно извлечь из архива и перейти в новый каталог:
tar -xvzf daq-1.0.7.tar.gz
cd daq-1.0.7
В отчёт вставить скриншот с результатом.



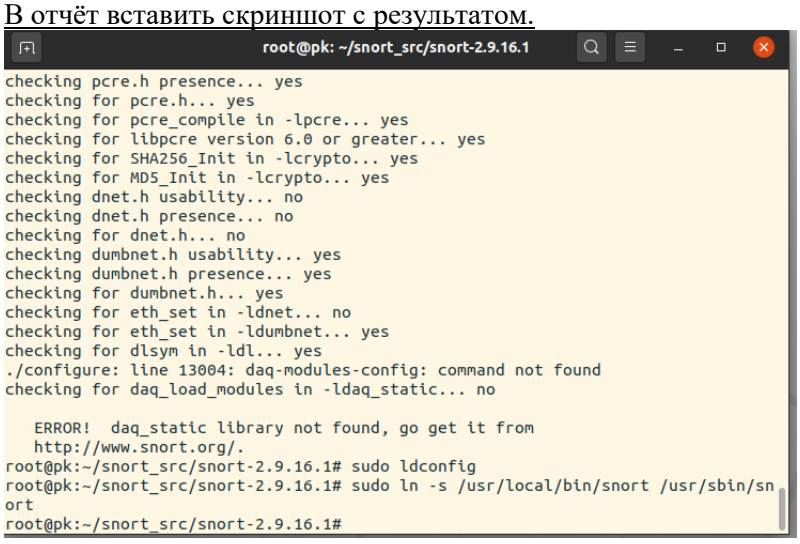
5. Последняя версия требует дополнительного шага для автоматической перенастройки DAQ перед запуском конфигурации:
autoreconf -f -i
6. После этого запустите скрипт конфигурации и скомпилируйте программу с помощью команды:
./configure && make && sudo make install
7. С установленным DAQ можно начинатать 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-1.9.16.1.tar.gz
9. После завершения загрузки извлеките исходный код и перейдите в каталог:
tar -xvzf snort-1.9.16.1.tar.gz
cd snort-1.9.16.1
В отчёт вставить скриншот с результатом.

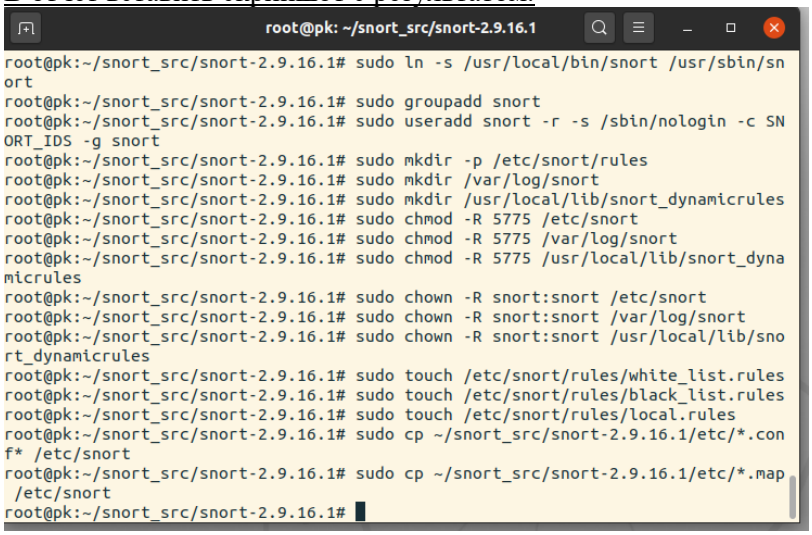


10. Затем настройте установку с включённым sourcefire:
./configure --enable-sourcefire && make && sudo make install
11. Далее необходимо настроить Snort для системы. Для этого нужно отредактировать некоторые файлы конфигурации, загрузку правил и пробный запуск. Начнём с обновления общих библиотек:
sudo ldconfig
12. Snort устанавливается в /usr/local/bin/snort директорию, рекомендуется создать ссылку на /usr/sbin/snort.
sudo ln -s /usr/local/bin/snort /usr/sbin/snort
В отчёт вставить скриншот с результатом.



13. Для безопасного запуска Snort без доступа root нужно создать нового непривилегированного пользователя и новую группу пользователей для запуска демона
sudo groupadd snort
sudo useradd snort -r -s /sbin/nologin -c SNORT_IDS -g snort
14. Затем создайте папки для размещения конфигураций Snort:
sudo mkdir -p /etc/snort/rules
sudo mkdir /var/log/snort
sudo mkdir /usr/local/lib/snort_dynamicrules
15. Установите разрешения для новых папок:
sudo chmod -R 5775 /etc/snort
sudo chmod -R 5775 /var/log/snort
sudo chmod -R 5775 /usr/local/lib/snort_dynamicrules
sudo chown -R snort:snort /etc/snort
sudo chown -R snort:snort /var/log/snort
sudo chown -R snort:snort /usr/local/lib/snort_dynamicrules
16. Создайте новые файлы для белых и чёрных списков и локальные правила:

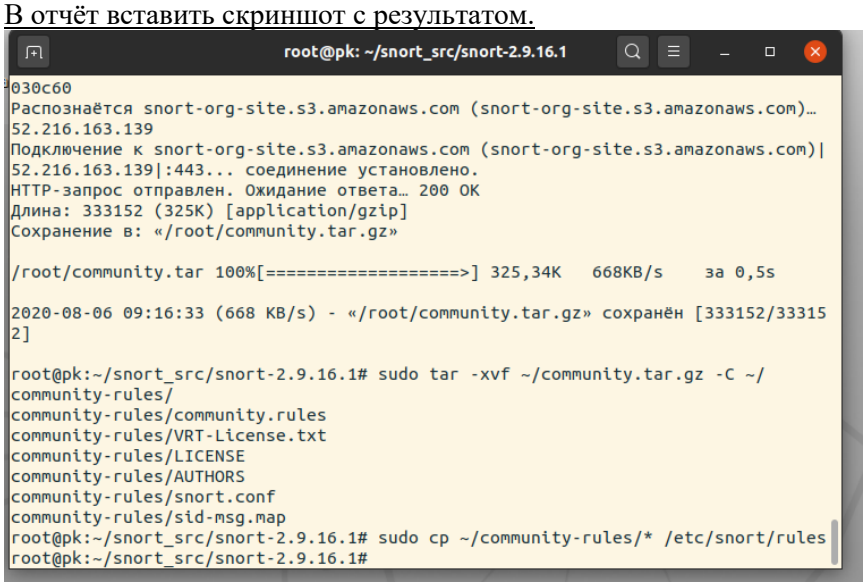
sudo touch /etc/snort/rules/white_list.rules
sudo touch /etc/snort/rules/black_list.rules
sudo touch /etc/snort/rules/local.rules
17. Затем скопируйте конфигурационный файл из папки загрузки:
sudo cp ~/snort_src/snort-1.9.16.1/etc/*.conf* /etc/snort
sudo cp ~/snort_src/snort-1.9.16.1/etc/*.map /etc/snort
В отчёт вставить скриншот с результатом.



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

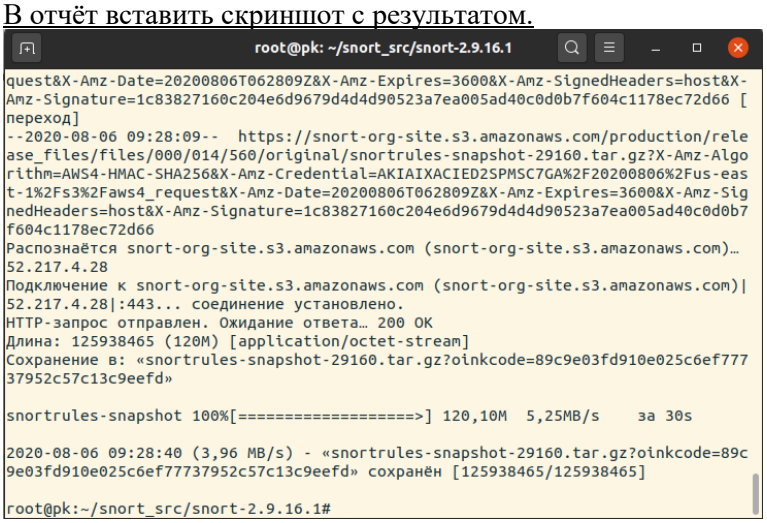
- Community rules are freely available although slightly limited.
- By registering for free on their website you get access to your Oink code, which lets you download the registered users rule sets.
- Lastly, subscriber rules are just that, available to users with an active subscription to Snort services.

18. Для быстрого тестирования Snort можно скачать правила:
wget https://www.snort.org/rules/community -O ~/community.tar.gz
19. Извлекаем правила и копируем в конфигурационную папку:
sudo tar -xvf ~/community.tar.gz -C ~/
sudo cp ~/community-rules/* /etc/snort/rules
В отчёт вставить скриншот с результатом.



20. По умолчанию Snort ожидает некоторые правила, которые не включены в файл правил. С помощью следующей команды можно закомментировать ненужные строки в файле правил:
sudo sed -i 's/include \$RULE_PATH/#include \$RULE_PATH/' /etc/snort/snort.conf

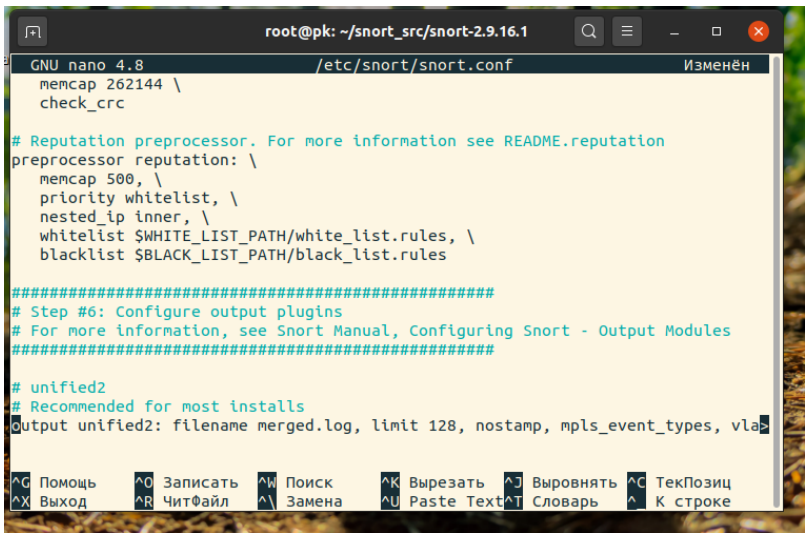
21. Далее вам нужно зарегистрироваться на сайте Snort, зайти на него под своим аккаунтом, открыть данные своего аккаунта, перейти в Oinkcode, скопировать данный код и в следующую команду его вставить:
wget https://www.snort.org/rules/snortrules-snapshot-29160.tar.gz?oinkcode=
89c9e03fd910e025c6ef77737952c57c13c9eefd
https://www.snort.org/rules/snortrules-snapshot-29160.tar.gz?oinkcode=89c9e03fd910e025c6ef77737952c57c13c9eefd
В отчёт вставить скриншот с результатом.



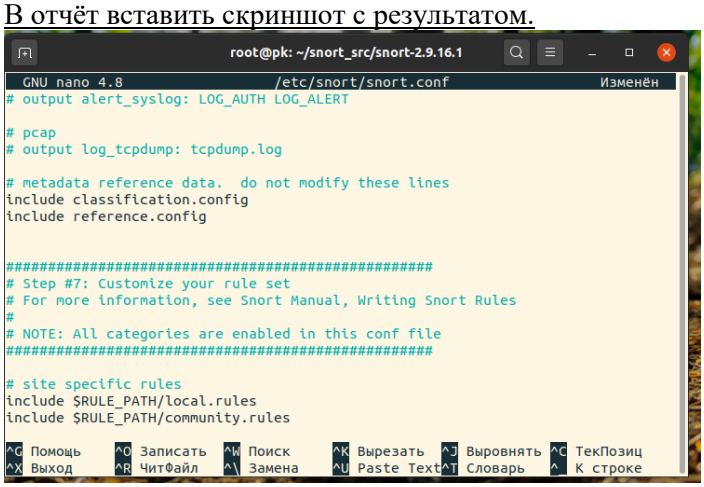
22. Регистрация нужна для загрузки правил. Далее распаковываем в папку:
sudo tar -xvf ~/registered.tar.gz -C /etc/snort
sudo tar -xvf snortrules-snapshot-29160.tar.gz?oinkcode=89c9e03fd910e025c6ef77737952c57c13c9eefd.1
Через sudo nautilus всё было скопировано в /etc/snort
23. После установки отредактируем конфигурационный файл:
sudo nano /etc/snort/snort.conf
24. Найдите разделы, которые указаны ниже и измените параметры по образцу:

```
# Setup the network addresses you are protecting
ipvar HOME_NET 10.0.1.14/24
# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET !$HOME_NET
# Path to your rules files (this can be a relative path)
var RULE_PATH /etc/snort/rules
var SO_RULE_PATH /etc/snort/so_rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules
# Set the absolute path appropriately
var WHITE_LIST_PATH /etc/snort/rules
var BLACK_LIST_PATH /etc/snort/rules
```

25. В шестом разделе измените следующее:
unified2
Recommended for most installs
output unified2: filename snort.log, limit 128
В отчёт вставить скриншот с результатом.



26. Далее найдите список включённых наборов правил. Раскомментируйте следующую строку для возможности загружать пользовательские правила:
include $RULE_PATH/local.rules
27. Также можно добавить строку:
include $RULE_PATH/community.rules
28. Сохраните и выйдите.
В отчёт вставить скриншот с результатом.



29. Проверьте конфигурацию:
sudo snort -T -c /etc/snort/snort.conf
30. После запуска проверки должен появиться текст похожий на:

```
--== Initialization Complete ==--
,,_     -*> Snort! <*-
o"  )~   Version 1.9.16 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: 1.1.11
Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.1
Preprocessor Object: SF_DCERPC2  Version 1.0
Preprocessor Object: SF_SSH  Version 1.1
Preprocessor Object: SF_FTPTELNET  Version 1.2
Preprocessor Object: SF_SDF  Version 1.1
Preprocessor Object: SF_DNP3  Version 1.1
Preprocessor Object: SF_REPUTATION  Version 1.1
Preprocessor Object: SF_IMAP  Version 1.0
Preprocessor Object: SF_SMTP  Version 1.1
```

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

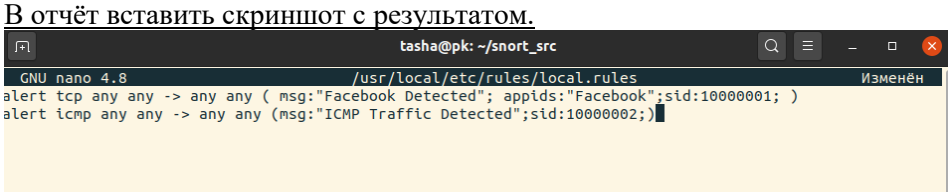
В случае возникновения ошибок читаем ошибки, ищем где и исправляем. Чаще всего это отсутствие папок/файлов.

В отчёт вставить скриншот с результатом.

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

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

31. Для проверки Snort на регистрацию предупреждений добавьте предупреждение:
sudo nano /etc/snort/rules/local.rules
32. Следующую строку в файл:
alert icmp any any -> $HOME_NET any (msg:"ICMP test"; sid:10000001; rev:001;)

В отчёт вставить скриншот с результатом.



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

Сохраните, выйдите.

34. Запустите Snort с опциями печати предупреждений. Нужно будет правильно выбрать сетевой интерфейс.
sudo snort -A consolecd -i **eth0** -u snort -g snort -c /etc/snort/snort.conf
Для проверки интерфейса можно воспользоваться командой:
ip addr
С включённым Snort при пинге вашего сервера вы должны увидеть уведомление для каждого ICMP-вызова в терминале.
07/12-11:20:33.501624 [**] [1:10000001:1] ICMP test [**] [Priority: 0] {ICMP}
83.136.251.119 -> 80.69.173.202
После появления предупреждений вы можете остановить их Ctrl+C. Все предупреждения записываются в журнал /var/log/snort/snort.log.timestamp.
35. Прочитать логи можно с помощью команды внизу:
snort -r /var/log/snort/snort.log.
В отчёт вставить скриншот с результатом.

```
-------------------------------------------------
rule counts
       total rules loaded: 2
              text rules: 2
            option chains: 2
            chain headers: 2
-------------------------------------------------
port rule counts
             tcp     udp    icmp      ip
     any       1       0       1       0
   total       1       0       1       0
-------------------------------------------------
ips policies rule stats
              id  loaded  shared enabled    file
               0       2       0       2    /usr/local/etc/snort/snort.lua
-------------------------------------------------
pcap DAQ configured to passive.
Commencing packet processing
++ [0] enp0s3
08/06-17:38:05.321637 [**] [1:10000001:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP}
10.0.2.14:41492 -> 157.240.203.35:443
08/06-17:38:05.321634 [**] [1:10000001:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP}
157.240.203.35:443 -> 10.0.2.14:41492
08/06-17:38:05.321646 [**] [1:10000001:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP}
157.240.203.35:443 -> 10.0.2.14:41492
08/06-17:38:05.321853 [**] [1:10000001:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP}
10.0.2.14:41492 -> 157.240.203.35:443
08/06-17:38:05.321850 [**] [1:10000001:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP}
157.240.203.35:443 -> 10.0.2.14:41492
08/06-17:38:05.321862 [**] [1:10000001:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP}
157.240.203.35:443 -> 10.0.2.14:41492
08/06-17:38:05.322028 [**] [1:10000001:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP}
10.0.2.14:41492 -> 157.240.203.35:443
08/06-17:38:05.322025 [**] [1:10000001:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP}
157.240.203.35:443 -> 10.0.2.14:41492
08/06-17:38:05.322174 [**] [1:10000001:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP}
10.0.2.14:41492 -> 157.240.203.35:443
08/06-17:38:05.322162 [**] [1:10000001:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP}
157.240.203.35:443 -> 10.0.2.14:41492
08/06-17:38:05.322887 [**] [1:10000001:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP}
10.0.2.14:41492 -> 157.240.203.35:443
08/06-17:38:05.323005 [**] [1:10000001:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP}
157.240.203.35:443 -> 10.0.2.14:41492
08/06-17:38:05.329119 [**] [1:10000001:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP}
157.240.203.35:443 -> 10.0.2.14:41492
08/06-17:38:05.329147 [**] [1:10000001:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP}
10.0.2.14:41492 -> 157.240.203.35:443
tasha@pk:~/snort_src$ sudo chmod a+r /var/log/snort/appid_stats.log
tasha@pk:~/snort_src$ cat /var/log/snort/appid_stats.log
1596724669,DNS,362,450
1596724669,Facebook,4783,128541
1596724669,HTTPS,4783,128541
1596724669,SSL client,4783,128541
1596724717,DNS,196,240
1596724717,Facebook,4837,138717
1596724717,HTTPS,4837,138717
1596724717,SSL client,4837,138717
tasha@pk:~/snort_src$
```

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

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

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

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

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

Следующей командой перезагрузите демон systemctl:
sudo systemctl daemon-reload
37. Затем выполните старт snort:
sudo systemctl start snort
38. Увидеть статус можно следующей командой:

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

21. Устный зачет по теме 1.9 - 1.10

Инструкция для обучающихся
Зачет сдается в рамках учебного занятия. Каждый студент отвечает в устной форме на предложенные преподавателем 2 вопроса.

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

Перечень вопросов:

1. Понятие протокола https
2. Понятие технологии SSL
3. Средства защиты компьютерных сетей с использованием Samba и политик безопасности на Linux-сервере.
4. Особенности серверов на Linux.
5. Программные средства для поднятия контроллера домена на Linux
6. Принципы использования систем обнаружения вторжения

Эталоны ответов: приведены в Учебном пособии по МДК.03.02 «Программно-аппаратные средства защиты информации»

3.1.2. Оценка освоения теоретического курса профессионального модуля по МДК.02.02

Дидактические единицы	Проверяемые ОК, У, З	Формы контроля (наименование контрольной точки)	
		Текущая аттестация	Промежуточная аттестация
Тема 2.1. Основные термины и определения	ОК 1, ОК 2, ОК 4, ОК 9, ПК 3.1. З1-З2	Устный зачет по Теме 2.1	Устные ответы на дифференцированном зачете
Тема 2.2. Классификация шифров	ОК 2, ОК 4, ОК 9, ОК 5, ПК3.2. У1	Практическая работа №1 Алгоритмизация шифра Цезаря	
	ОК 2, ОК 4, ОК 9, ОК 5, ПК 3.2.,ПК 3.1. У2	Практическая работа №2 Декодирование моноалфавитного подстановочного шифра частотным методом	
	ОК 1, ОК 2, ОК 4, ОК 9, З1-З2	Устный зачет по Теме 2.2	
Тема 2.3. Криптографические протоколы	ОК 1, ОК 2, ОК 4, ОК 9, ОК 5, ПК 3.2., ПК 3.1. У3	Практическая работа № 3 Метод шифрования с открытым ключом RSA	
	ОК 1, ОК 2, ОК 4, ОК 9, ОК 5, ПК 3.2., ПК 3.1. У4	Практическая работа № 4 Разработка хэш-функции	
	ОК 1, ОК 2, ОК 4, ОК 9, З1-З2	Устный зачет по теме 2.3	
Тема 2.5. Стеганография	ОК 2, ОК 4, ОК 9, ПК 3.4. У5	Практическая работа №5: Анализ графических изображений на наличие скрытой информации.	

1. Устный зачет по Теме 2.1

Инструкция для обучающихся
Понятийный диктант сдается в рамках учебного занятия. Каждый студент отвечает в устной форме на предложенные преподавателем 2 вопроса.
Выполнение задания: одному студенту на ответ выделяется 3 мин., группа сдает зачет за одно учебное занятие.

Перечень вопросов:

1. Понятие шифра
2. Составные элементы шифра
3. Алгоритм криптографического преобразования
4. Понятие азбуки
5. Шифрование (зашифрование)
6. Дешифрование (расшифрование)
7. Ключ, виды ключей
8. Понятие криптографии
9. Понятие криптоанализа
10. Вскрытие (взламывание) шифра

Эталоны ответов: приведены в Учебном пособии МДК.02.02 «Криптографические средства защиты информации».

2. Практическая работа № 1 Алгоритмизация шифра Цезаря

Инструкция для обучающихся
Внимательно прочитайте задание. Расшифруйте закрытый текст с помощью шифра Цезаря.

Время выполнения задания – 45 минут.

Задание

1. Запустите программу Microsoft Excel.
2. На первом листе электронной книги запишите в столбец А буквы русского алфавита. В столбце В – номер букв, в столбце С – опять буквы (такая запись будет необходима для использования функции ВПР).

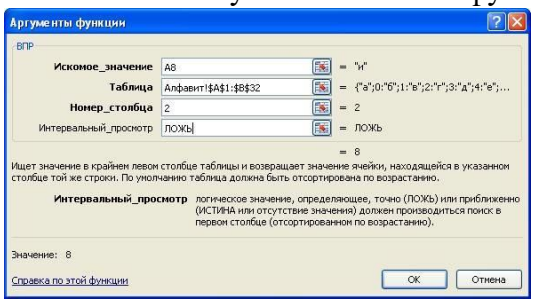
	A	B	C	D
1	а	0	а	
2	б	1	б	
3	в	2	в	
4	г	3	г	
5	д	4	д	
6	е	5	е	
7	ж	6	ж	
8	з	7	з	
9	и	8	и	
10	й	9	й	
11	к	10	к	
12	л	11	л	
13	м	12	м	
14	н	13	н	
15	о	14	о	
16	п	15	п	
17	р	16	р	
18	с	17	с	
19	т	18	т	
20	у	19	у	
21	ф	20	ф	
22	х	21	х	
23	ц	22	ц	
24	ч	23	ч	
25	ш	24	ш	
26	щ	25	щ	
27	ъ	26	ъ	
28	ы	27	ы	
29	ь	28	ь	
30	э	29	э	
31	ю	30	ю	
32	я	31	я	

3. Переименуйте лист1 в Алфавит.
4. На втором листе электронной книги запишите название работы, ключ и название столбцов таблицы (S – исходные символы, X – числа исходных символов, Y – пересчитанные по формуле значения, S1 – символы закрытого текста). Значение ключа можно взять любым и обязательно его значение записать в отдельную ячейку (B5). В столбец S, начиная с 8 строки, впишите фамилию и имя, каждую букву в отдельной ячейке.

	A	B	C	D	E	F	G
1					**Шифр Цезаря**		
2							
3	**1. Зашифровывание**						
4							
5	k=	5					
6							
7	**S**	**X**	**Y**	**S1**			
8	и						
9	в						
10	а						
11	н						
12	о						
13	в						
14	а						
15	н						
16	д						
17	р						
18	е						
19	й						
20							

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

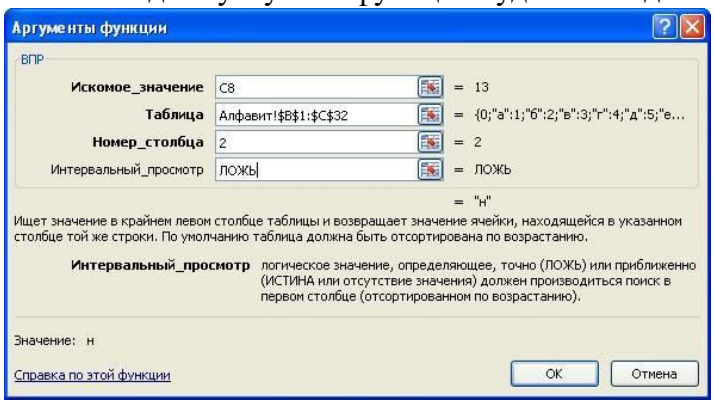
Встаем в ячейку B8 и вызываем функцию ВПР. Заполняем ее окно следующим образом:



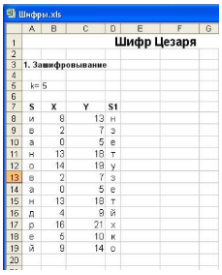
6. Растянуть формулу вниз до конца таблицы.
7. В ячейку C8 (столбец Y) записывается формула для шифрования. Исходная формула метода Цезаря имеет вид: $y_i = (x_i + k) \mathrm{mod} n$. Операции mod в Excel соответствует функция **ОСТАТ(число; делитель)**. В нашем случае **число** – это $(x_i + k)$, а **делитель** – 32.

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

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

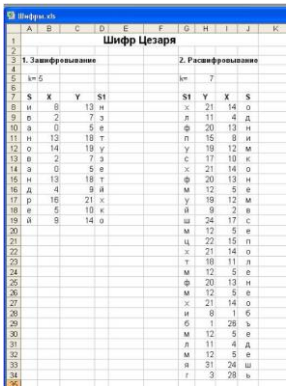


10. Окончательно таблица должна выглядеть следующим образом:



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

12. Проведите дешифрования текста по аналогии с зашифровыванием. Для расшифровывания (столбца X) используйте формулу $x_i = (y_i + (32-k)) \mathrm{mod} 32$.



13. Запишите полученную фразу.

Эталон ответа

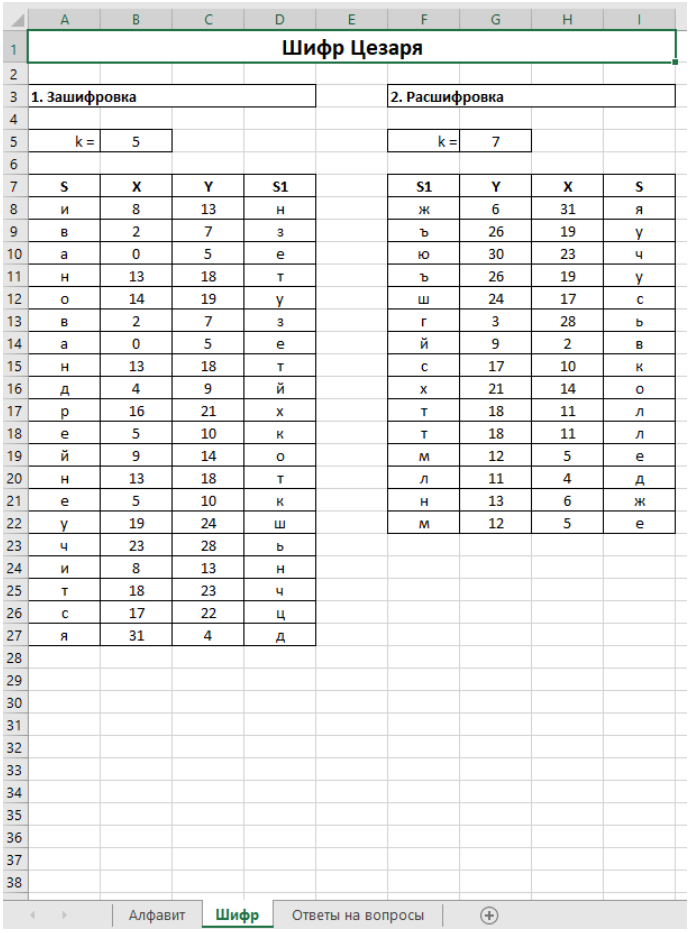
На первом листе электронной книги записываем в столбец А буквы русского алфавита. В столбце В – номер букв, в столбце С – опять буквы (для использования функции ВПР)

	A	B	C
1	а	0	а
2	б	1	б
3	в	2	в
4	г	3	г
5	д	4	д
6	е	5	е
7	ж	6	ж
8	з	7	з
9	и	8	и
10	й	9	й
11	к	10	к
12	л	11	л
13	м	12	м
14	н	13	н
15	о	14	о
16	п	15	п
17	р	16	р
18	с	17	с
19	т	18	т
20	у	19	у
21	ф	20	ф
22	х	21	х
23	ц	22	ц
24	ч	23	ч
25	ш	24	ш
26	щ	25	щ
27	ъ	26	ъ
28	ы	27	ы
29	ь	28	ь
30	э	29	э
31	ю	30	ю
32	я	31	я

Алфавит | Шифр | Ответы на вопросы

На втором листе электронной книги записываем название работы, ключ и название столбцов таблицы (S – исходные символы, X – числа исходных символов, Y – пересчитанные по формуле значения, S1 – символы закрытого текста). Значение ключаберём равное 5. В столбец S, начиная с 8 строки, вписываем фамилию и имя, каждую букву в от-

дельной ячейке. Далее по заданию проводим зашифровку и расшифровку текста, результат показан на рис.2.



Шифр Цезаря

1. Зашифровка

k = 5

S	X	Y	S1
и	8	13	н
в	2	7	з
а	0	5	е
н	13	18	т
о	14	19	у
в	2	7	з
а	0	5	е
н	13	18	т
д	4	9	й
р	16	21	х
е	5	10	к
й	9	14	о
н	13	18	т
е	5	10	к
у	19	24	ш
ч	23	28	ь
и	8	13	н
т	18	23	ч
с	17	22	ц
я	31	4	д

2. Расшифровка

k = 7

S1	Y	X	S
ж	6	31	я
ъ	26	19	у
ю	30	23	ч
ъ	26	19	у
ш	24	17	с
г	3	28	ь
й	9	2	в
с	17	10	к
х	21	14	о
т	18	11	л
т	18	11	л
м	12	5	е
л	11	4	д
н	13	6	ж
м	12	5	е

Алфавит | Шифр | Ответы на вопросы

3. Практическая работа № 2

Декодирование моноалфавитного подстановочного шифра частотным методом

Инструкция для обучающихся

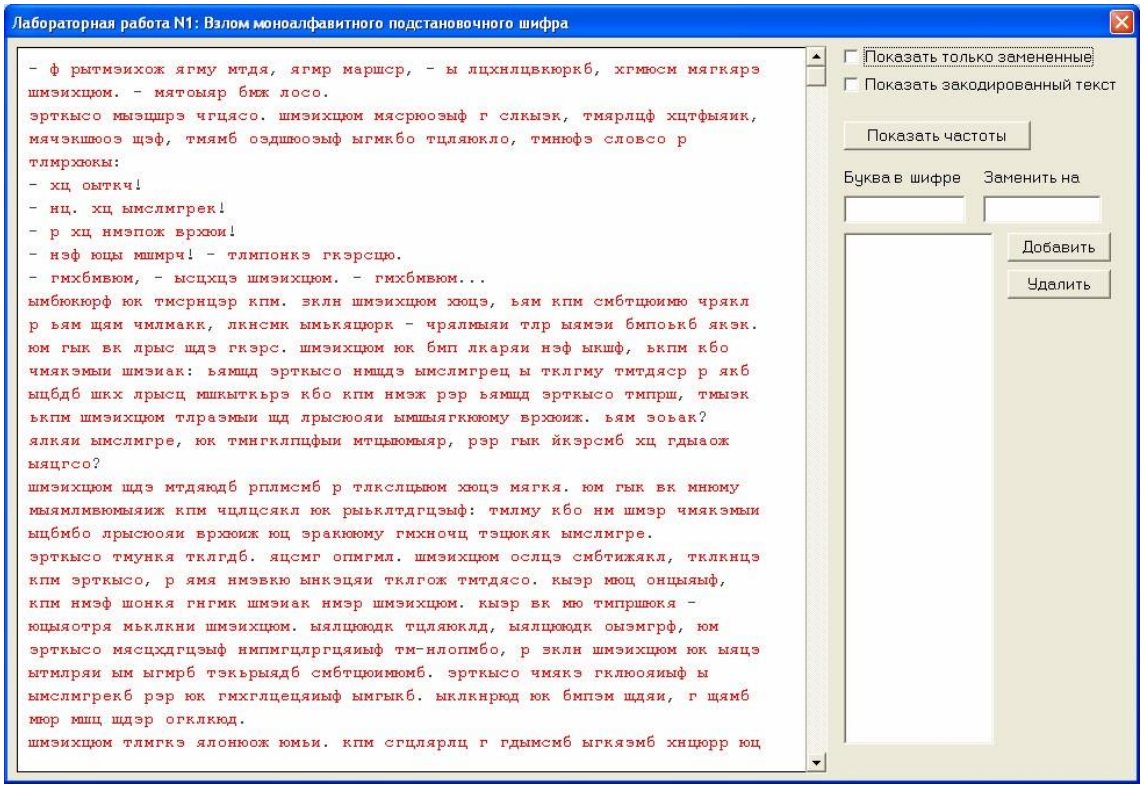
Внимательно прочитайте задание. Расшифруйте закрытый текст.

Время выполнения задания – 45 минут.

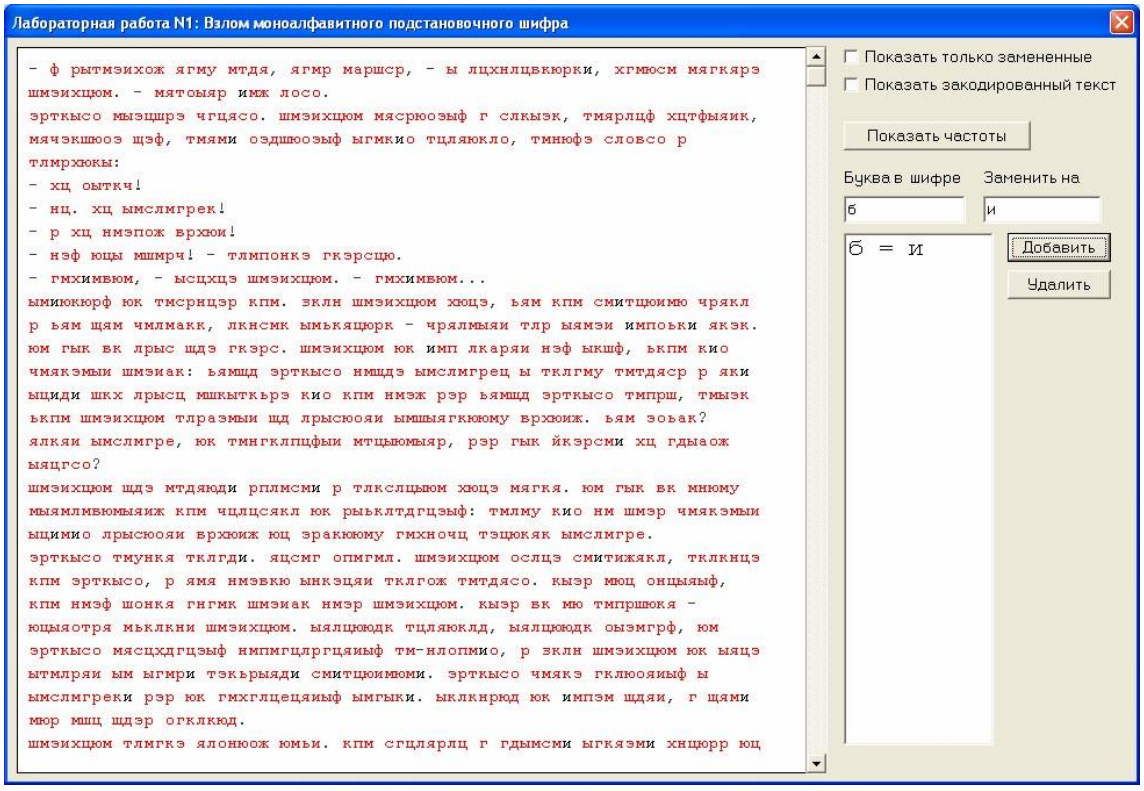
Задание

1. Запустить на выполнение файл labw01.exe

На экране появится окно выполнения лабораторной работы (рис. 1):

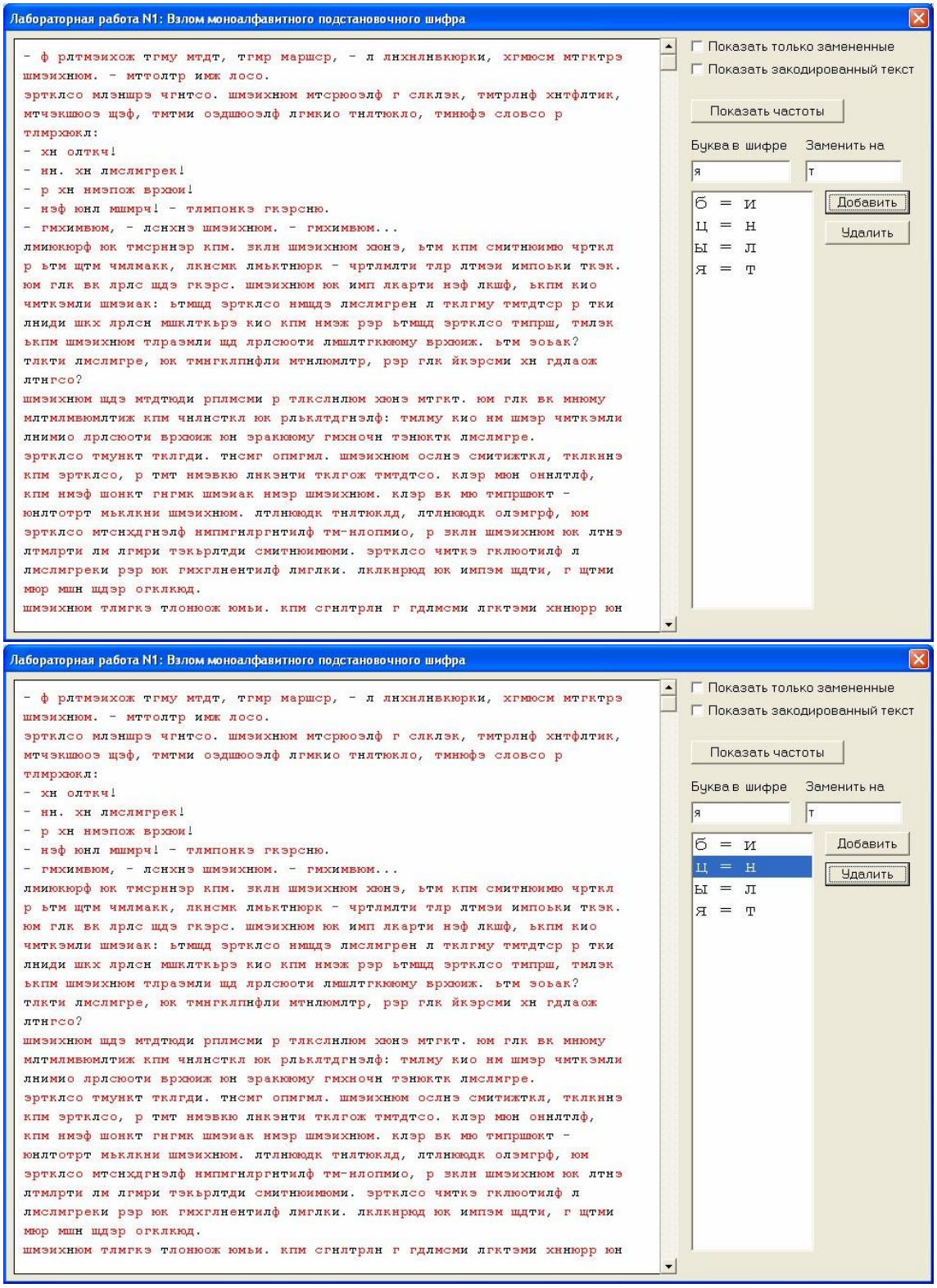


В левой части окна находится зашифрованный текст (буквы, выделенные красным цветом). В процессе расшифровки расшифрованные (правильно или неправильно) буквы текста меняют цвет с красного на черный.



Чтобы указать для какой-либо буквы шифра ее истинное (расшифрованное) значение, нужно в поле «Буква в шифре» указать значение буквы, например, “б”, а в поле «Заменить на» - ее истинное значение, например, “и”, а затем нажать кнопку “Добавить“. Результат такого действия приведен на рис. 2.

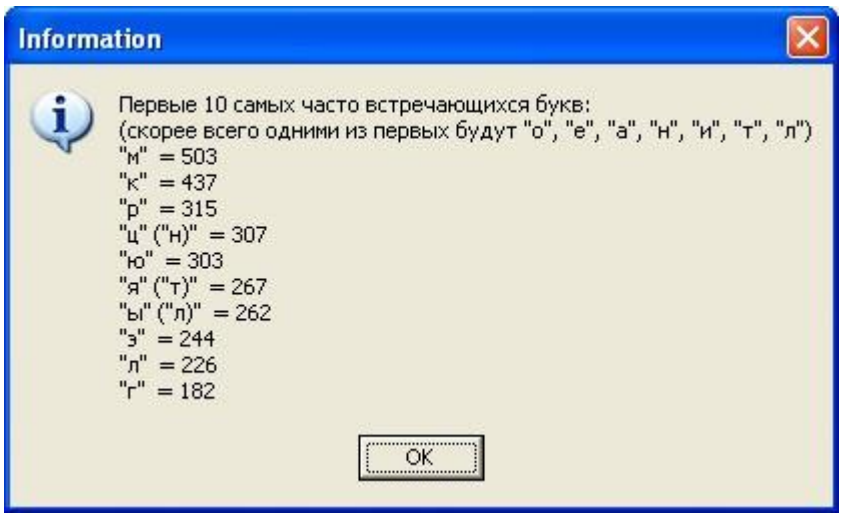
На рис. 3. Приведено окно выполнения лабораторной работы после добавления расшифровок нескольких букв.



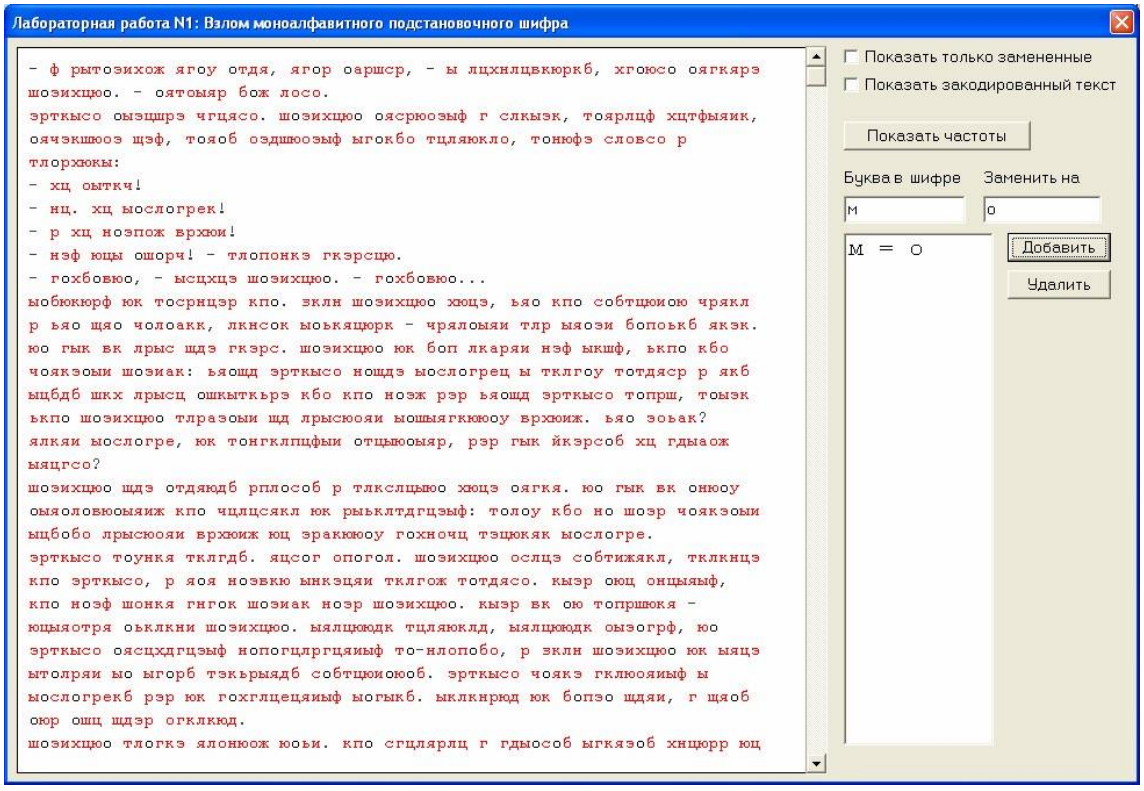
Чтобы отменить указанную расшифровку буквы, нужно в списке расшифровок мышкой указать соответствующую пару букв и нажать кнопку «Удалить» (рис. 4).

Полоса вертикального скроллинга служит для навигации по расшифровываемому тексту.

2. Начинается частотная атака с анализа частот встречаемости букв в шифровке. Для этих целей в окне выполнения лабораторной работы предусмотрена кнопка «Показать частоты». При ее нажатии на экран выводится перечень десяти наиболее часто встречаемых букв в шифре, а также перечень букв, наиболее часто встречаемых в русском языке (рис. 5).

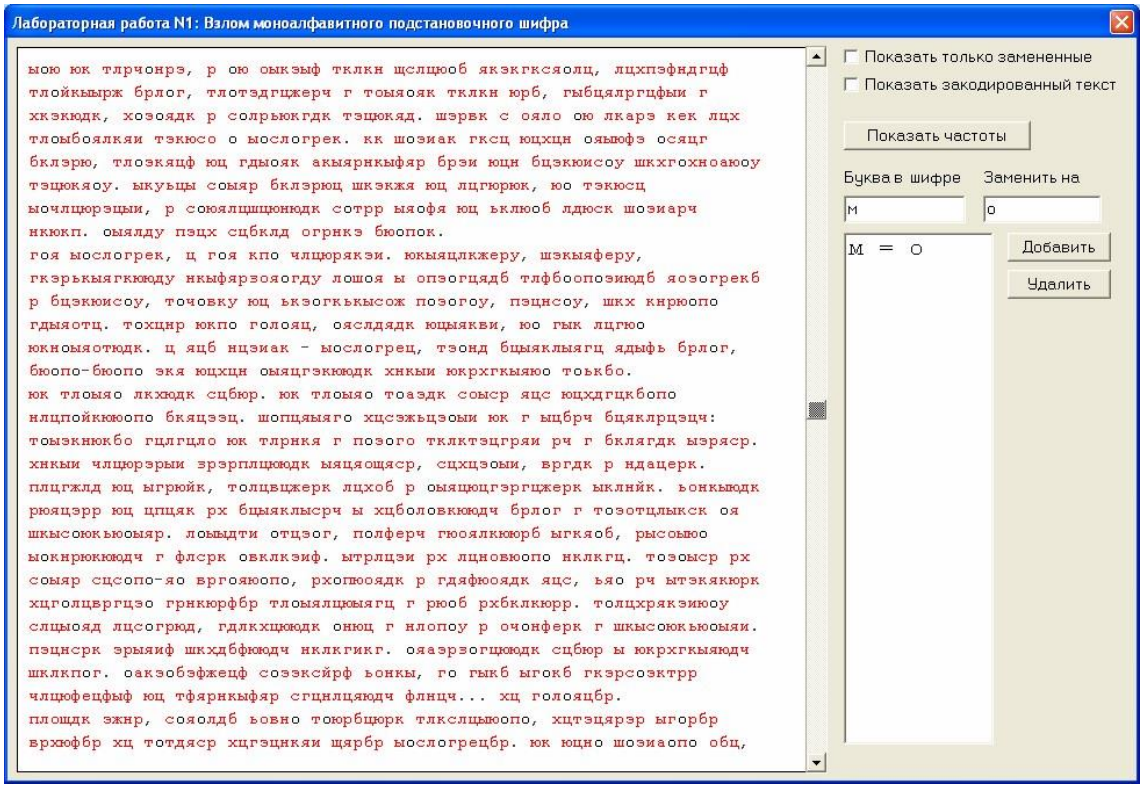


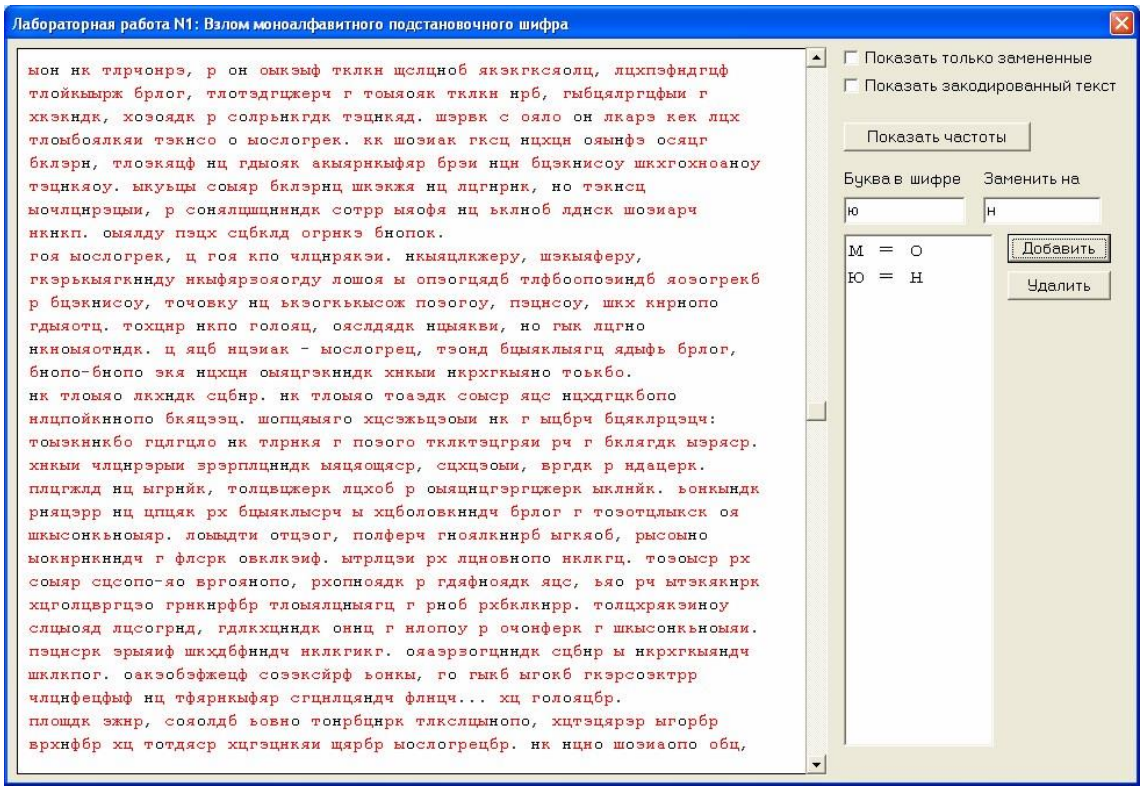
Первым шагом в расшифровке текста может быть указание расшифровки для самой часто встречаемой буквы - буквы «о». Для случая, приведенного на рис. 5, указывается «о» как расшифровка буквы «м» шифра (см. рис. 6).



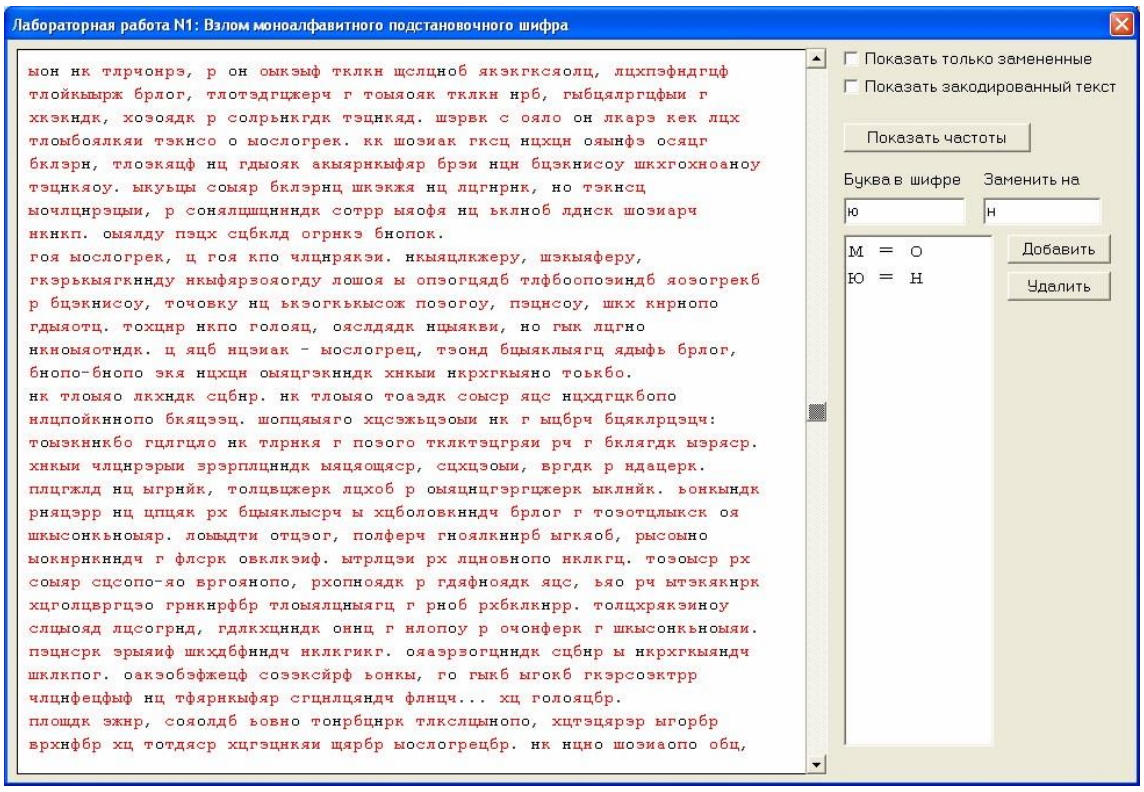
Следует помнить, что для конкретного текста частота встречаемости букв может быть несколько иной, чем в среднем для русского языка. Если в русском языке, например, буква «т» встречается чаще, чем буква «л», то в каком-то конкретном тексте буква «л» вполне может встречаться чаще буквы «т». Поэтому слепо опираться на данные частотного анализа не следует.

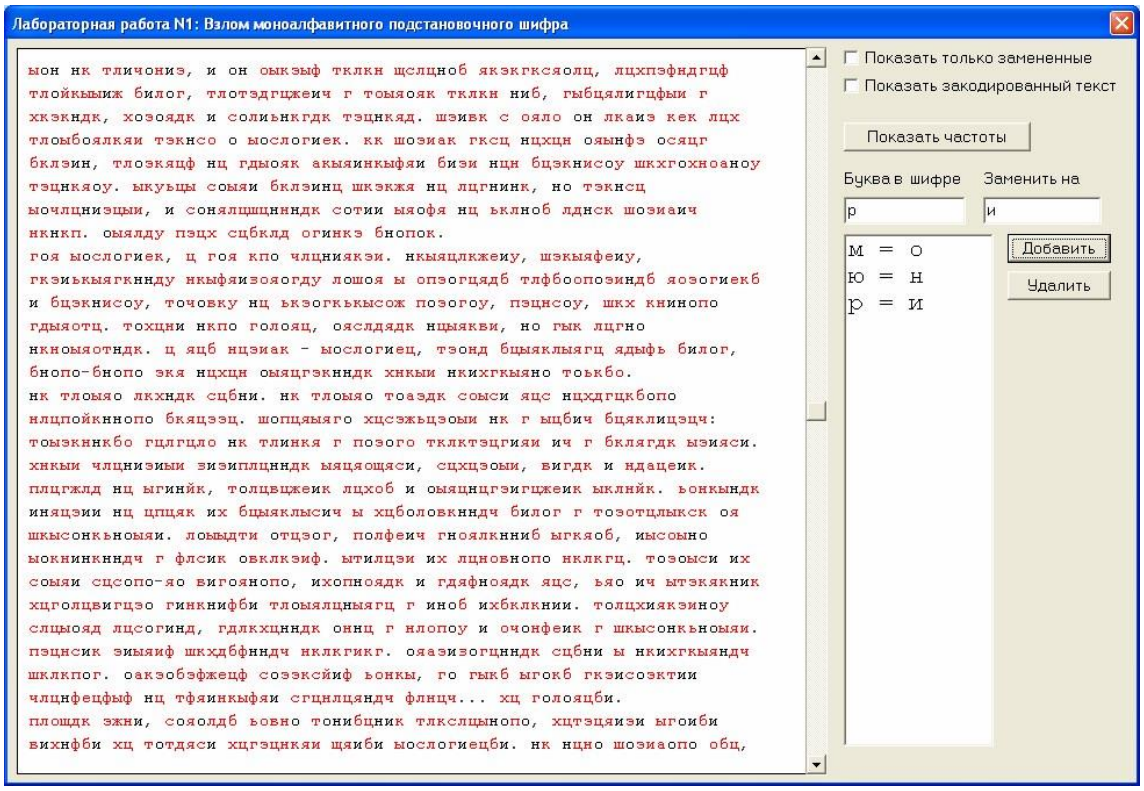
3. В зашифрованном тексте осуществляется поиск коротких слов, зашифрованные буквы которых можно предсказать по уже расшифрованным буквам и частотной информации из рис. 5. На рис. 7. в верхней строчке есть фрагмент текста « ою », где «о» уже известно





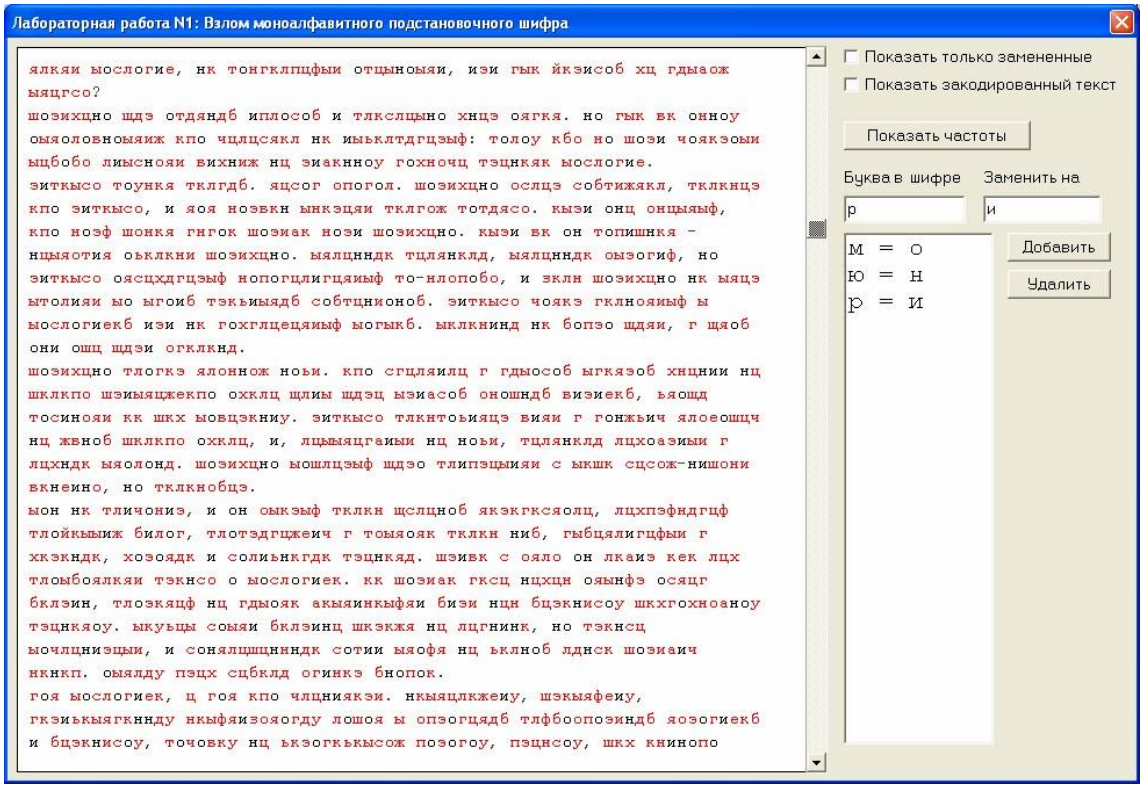
Этот фрагмент может быть скорее всего словом « он » В таблице частот (рис. 5) буква «ю» шифра стоит на 5-м месте, что примерно соответствует позиции буквы «н» русского языка (4-е место). Значит разумно попробовать поменять «ю» на «н». Результат приведен на рис. 8.

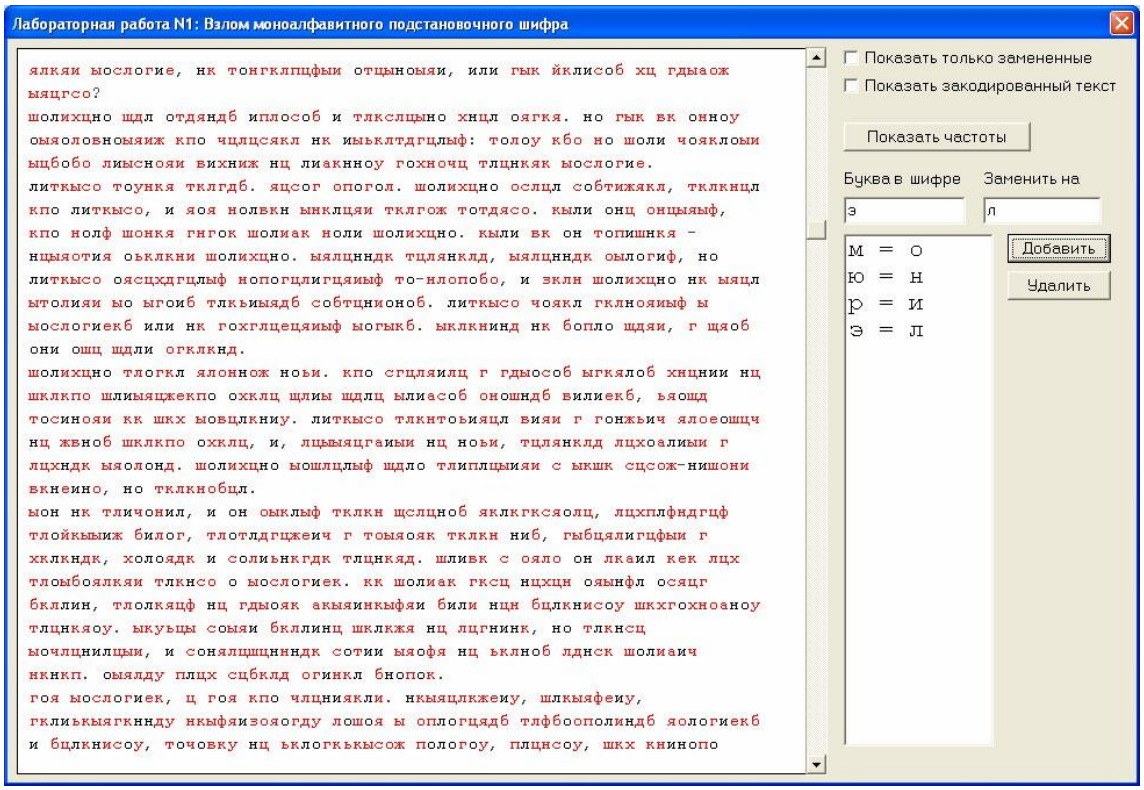




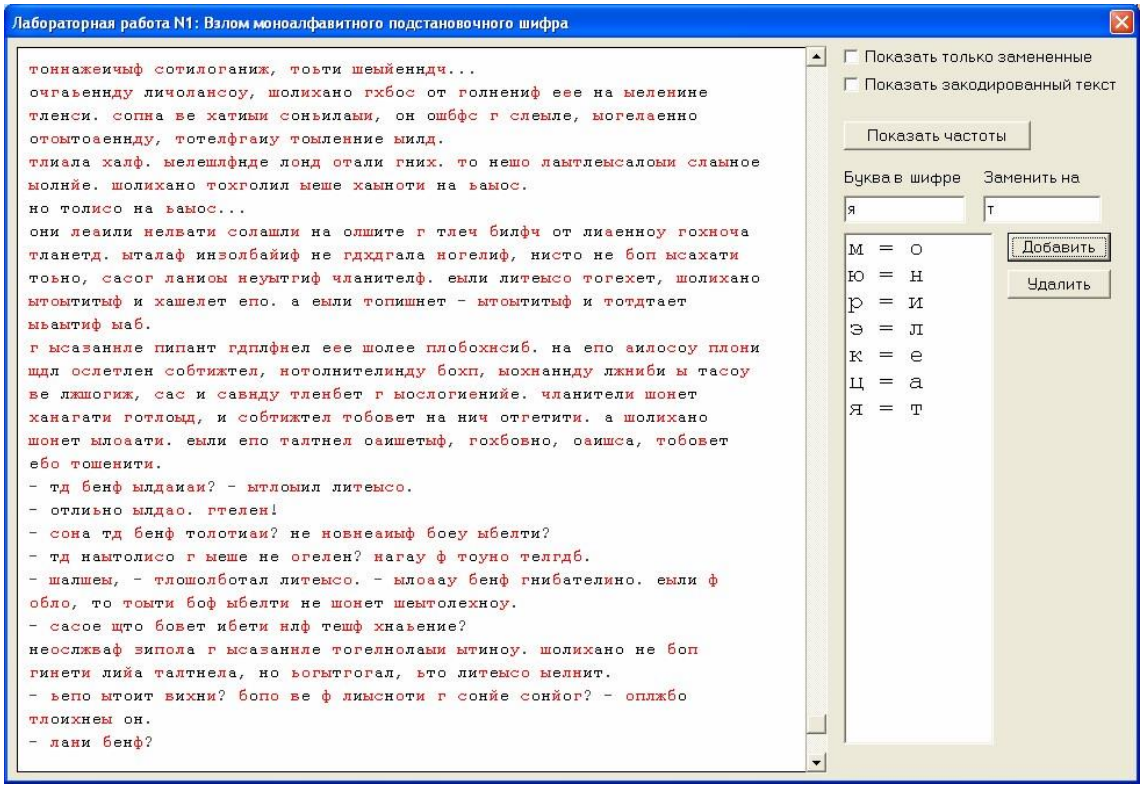
Далее повторяется поиск коротких слов, в которых можно догадаться о значении зашифрованных букв. На рис. 9 в первой и третей строках есть отдельно стоящее «р». Скорее всего это предлог «и», что согласуется и с информацией на рис. 5. Результат замены приведен на рис. 10.

На рис. 11 в первой строке обнаруживается слово из двух известных «и» и шифрованной буквы «э» между ними. Скорее всего это буква «л», образующая слово «или» (рис. 12).

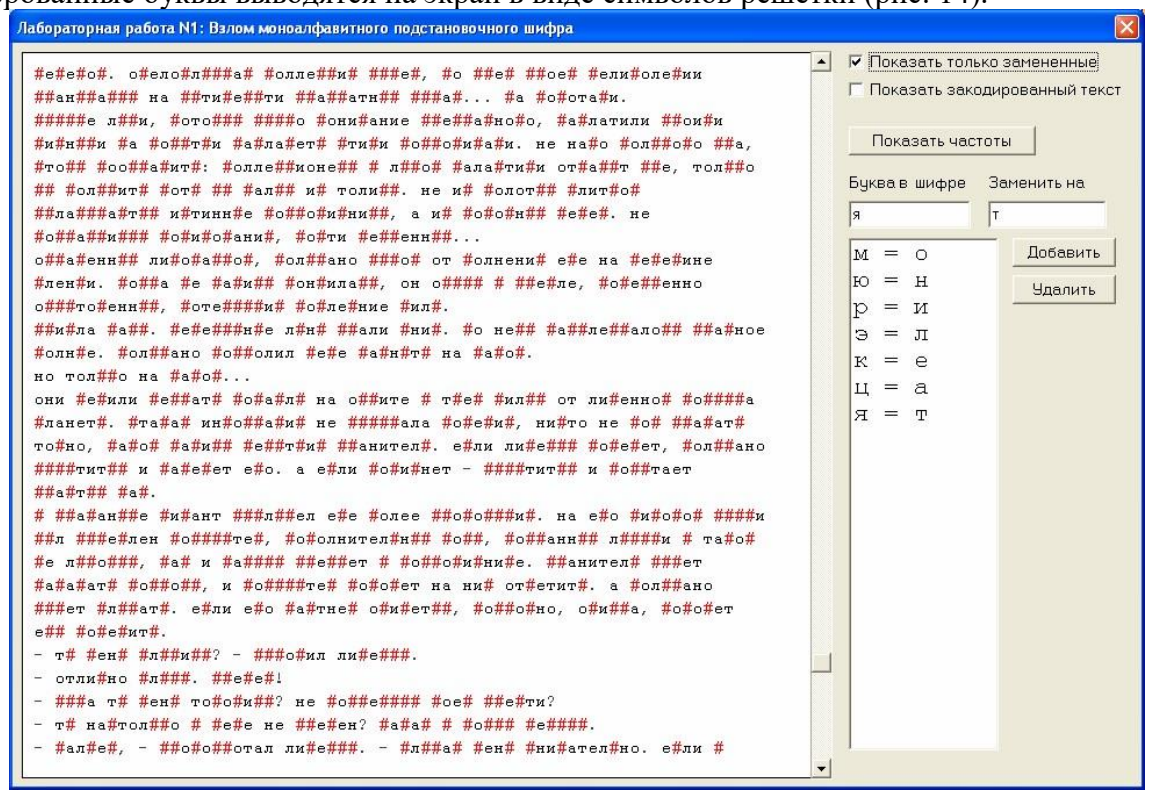




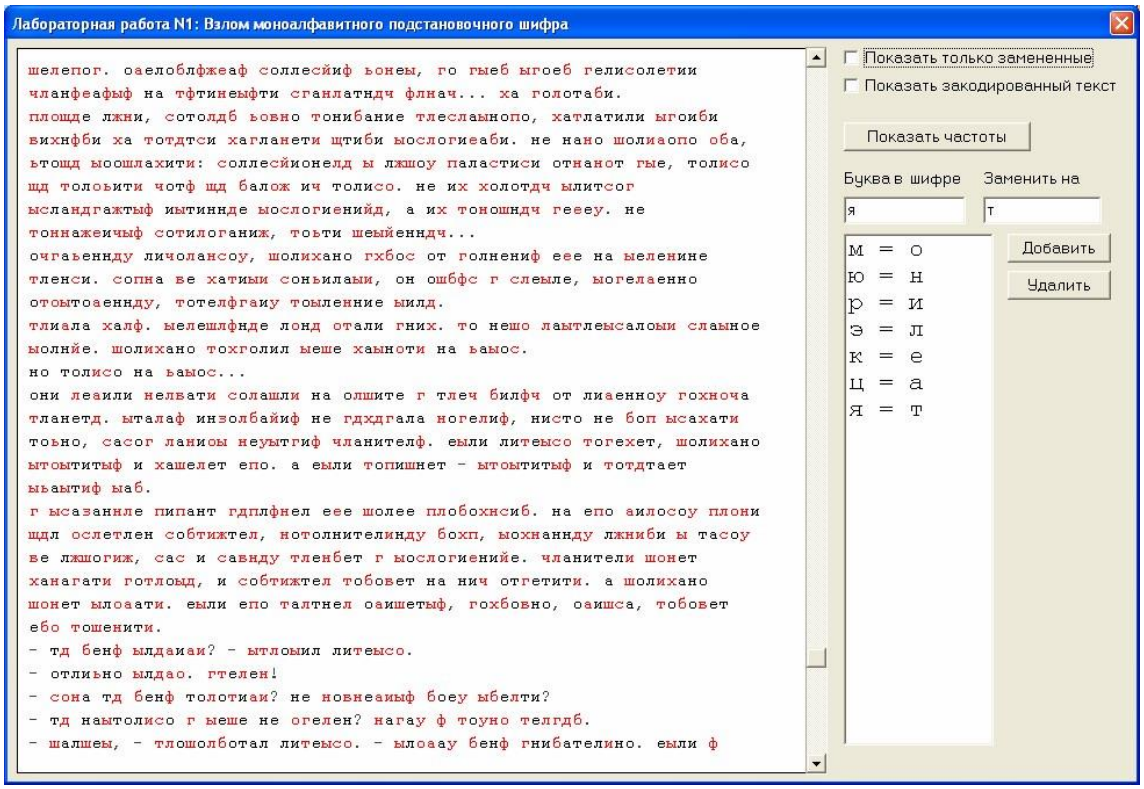
После расшифровки аналогичным образом букв «к» на «е», «ц» на «а» и «я» на «т» окно выполнения лабораторной работы приобретает следующий вид (рис. 13):



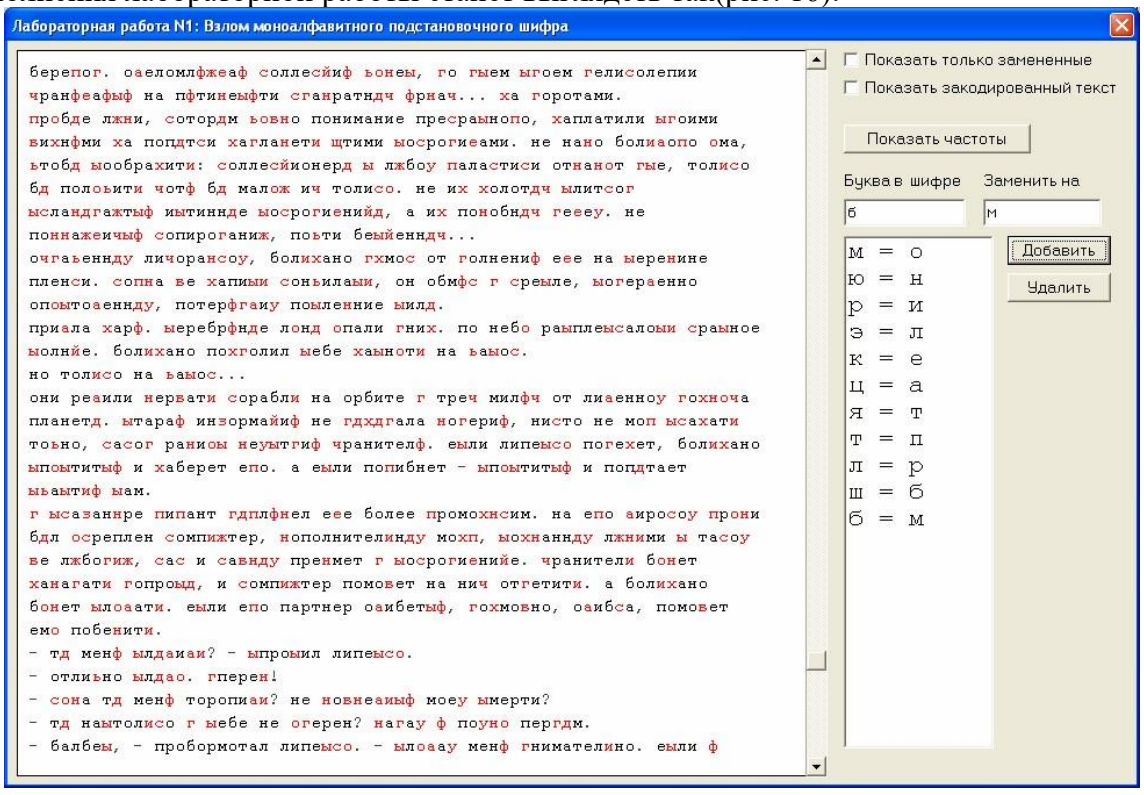
Когда так много букв уже известно, зашифрованные буквы могут мешать для понимания слов. Для облегчения дальнейшего анализа в программе предусмотрена возможность выставления флага «Показать только замененные», при выставлении которого все зашифрованные буквы выводятся на экран в виде символов решетки (рис. 14).



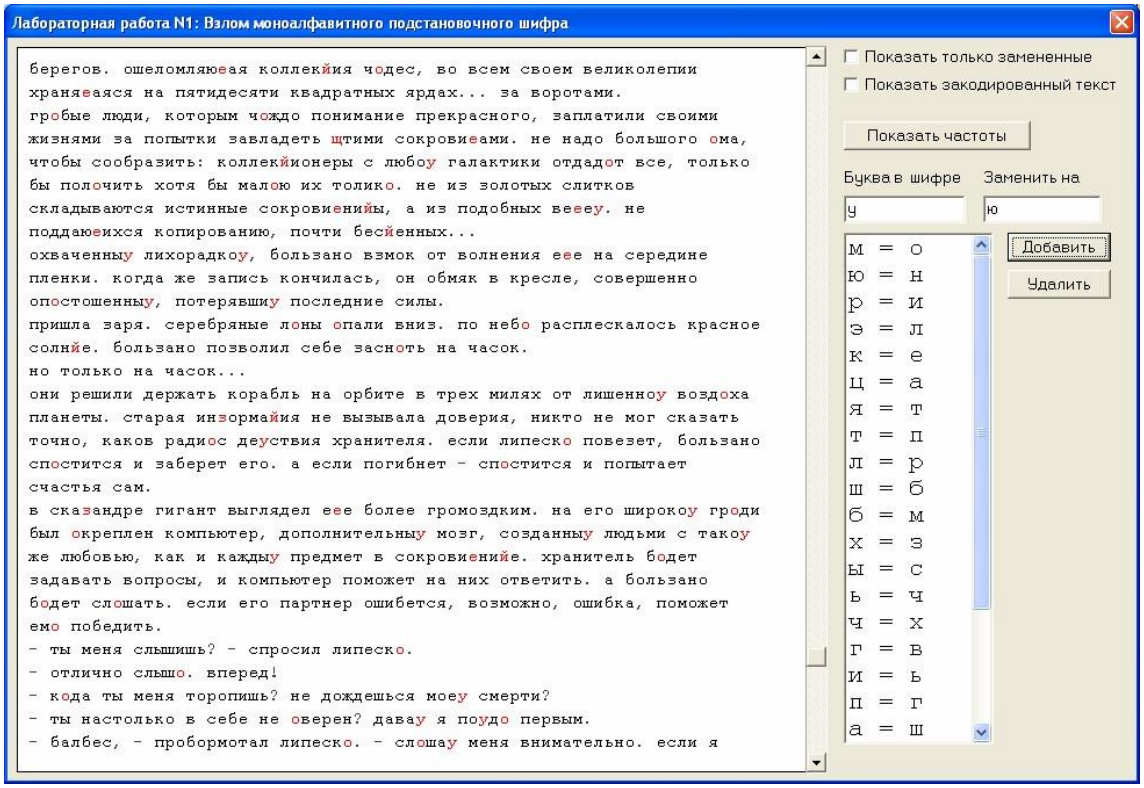
Теперь видно, что слово «##о#о##отал» в нижней строке вполне может быть словом «пробормотал». Если теперь выключить флаг, то можно получить косвенное подтверждение этого - на позициях двух букв «р» в этом слове в шифре также находится одинаковая буква «л» (рис. 15).



Если заменить теперь букву «т» на «п», «л» на «р», «ш» на «б» и «б» на «м», то окно выполнения лабораторной работы станет выглядеть так(рис. 16):

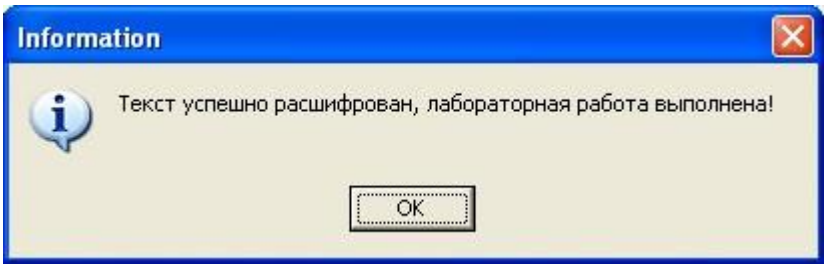


Хорошо видно, что дальнейший анализ значительно упрощается. Например, очевидно по слову «хаплатили», что буква «х» шифра соответствует букве «з» исходного текста. На рис. 17 приведено окно программы, когда анализ уже близок к завершению (осталось совсем немного нерасшифрованных букв).



Когда же все буквы текста расшифрованы, на экран выводится информационное окно

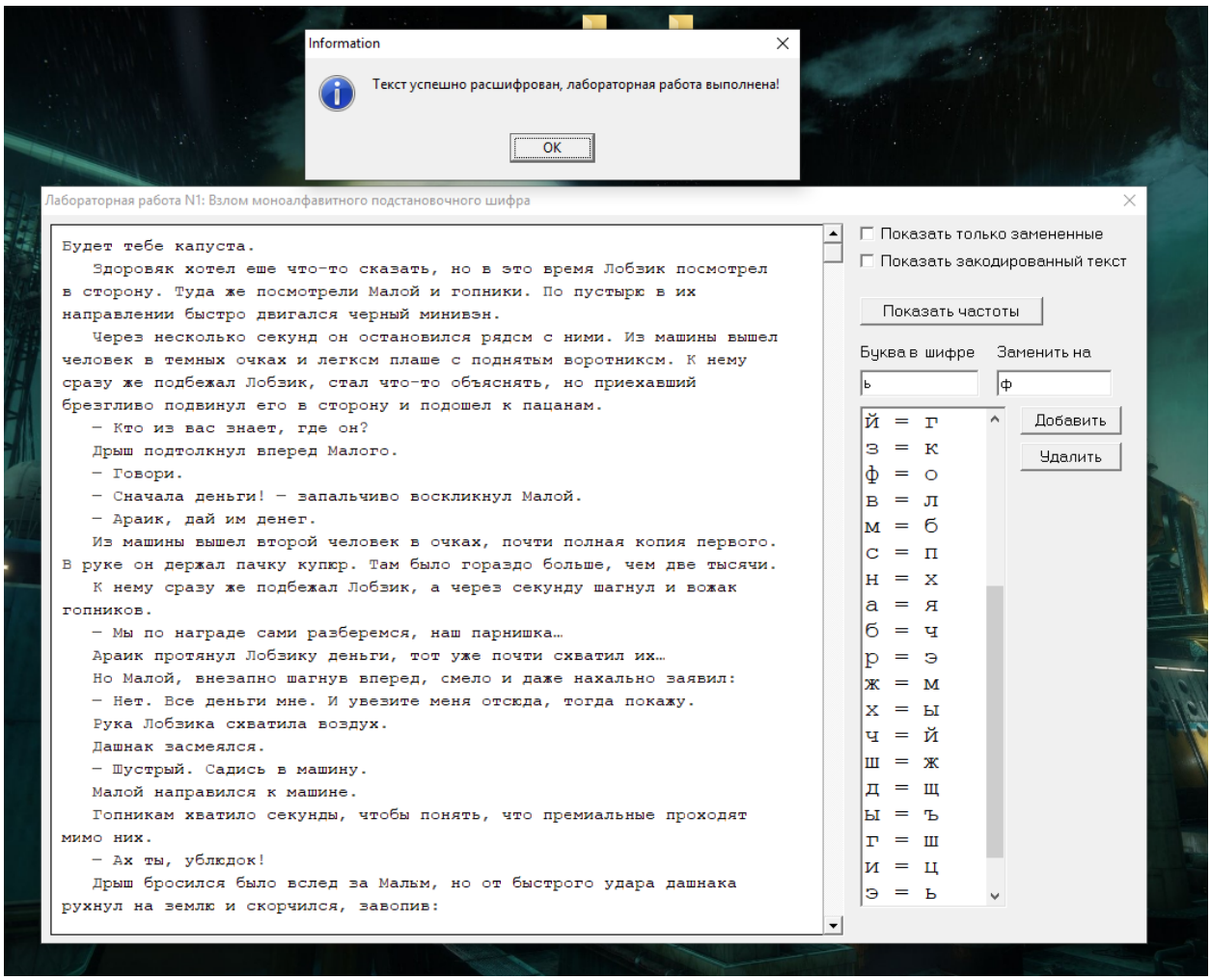
(рис. 18):



Появление этого окна на экране свидетельствует об успешном выполнении практической работы.

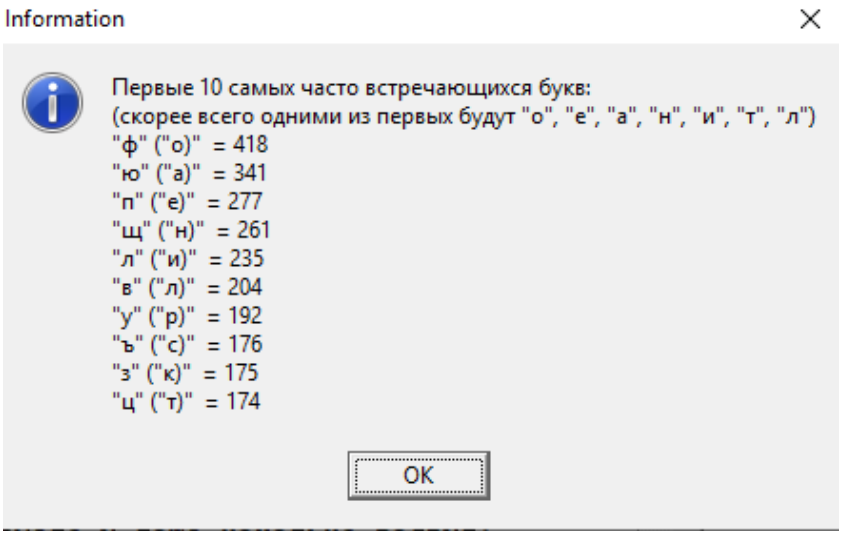
Эталон ответа

В ходе выполнения практической работы был расшифрован текст методом частотного анализа. Расшифровка прошла успешно



Появление окна об успешной расшифровке текста на экране свидетельствует об успешном выполнении практической работы.

10 наиболее встречающихся букв в тексте были заменены на наиболее встречающиеся буквы в Русском алфавите (рис. 2)



Вывод: На практике я познакомился с методом использования частотной криптоатаки при взломе подстановочных шифров.

4 Устный зачет по Теме 2.2

Инструкция для обучающихся

Зачет сдается в рамках учебного занятия. Каждый студент отвечает в устной форме на предложенные преподавателем 2 мини вопроса.

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

Перечень вопросов:

1. Какой текст называется открытым?
2. Какой текст называется закрытым?
3. Что такое ключ?
4. Как осуществляется процесс шифрования в методе Цезаря?
5. Что такое «шифрование методом перестановки»?
6. Как работает функция ОСТАТ?
7. Что делает функция ВПР?

Эталоны ответов: приведены в Учебном пособии МДК.02.02 «Криптографические средства защиты информации».

5. Практическая работа № 3. Метод шифрования с открытым ключом RSA

Инструкция для обучающихся

Внимательно прочитайте задание. Сформируйте зашифрованное сообщение по алгоритму RSA с помощью открытого ключа, произведите дешифрование криптограммы.

Время выполнения задания – 45 минут.

Задание 1.

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

Таблица 1

Таблица кодирования символов открытого текста

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

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

Таблица 2

Варианты задания

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

Пример 1

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

2. Подготовить открытый текст к шифрованию, закодировав его с помощью табл. 3.7:

м — 23, а — 11, й - 20.

Получили открытое сообщение X = 231120.

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

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

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

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

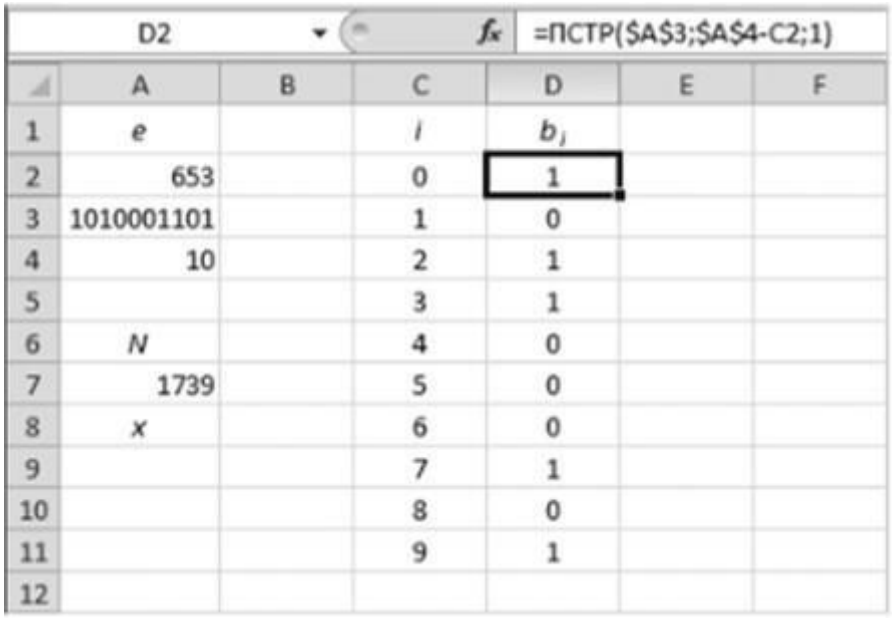
Если число e выходит за рамки указанного диапазона, следует воспользоваться стандартным приложением MS Windows Калькулятор, режим (вид) Программист. В этом случае следует установить переключатель системы счисления в позицию Dec (десятичная), ввести число e, а затем установить переключатель в позицию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

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

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

- определить p — число разрядов двоичного представления числа e. В среде MS Excel для этих целей можно воспользоваться функцией ДЛСТР группы Текстовые. Пусть значение e в двоичной системе счисления занесено в ячейку A3. Тогда в ячейку A4 следует занести формулу =ДЛСТР(A3);
- теперь следует сформировать таблицу для вычисления степени e по модулю N. В ячейки столбца C занести значения от 0 до p - 1 (в примере - от 0 до 9), задав заголовок столбца — i;
- в соответствующие ячейки столбца D занести значения двоичных разрядов b_i (начиная с младшего разряда), для чего воспользоваться функцией ПСТР группы Текстовые. Если двоичное значение e находится в ячейке A3, число разрядов h занесено в ячейку A4, а значения i содержатся в ячейках C2:C11, формула в ячейке D2 примет вид: =ПСТР($A$3;$A$4-C2;1). Ссылки на значения e и r должны быть абсолютными (преобразовать ссылку щелкнув на ней мышью, а затем нажав кноп-

ку F4). Скопировать сформированную формулу в диапазон ячеек столбца D (D3:D11 в примере) рис. 1;



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

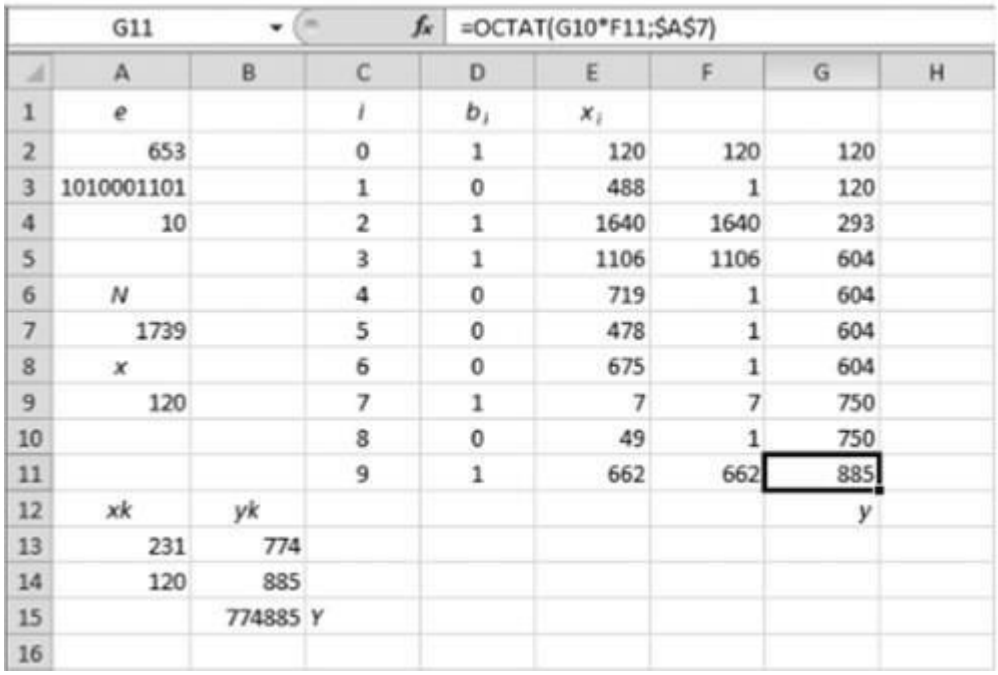
Рис. 1. Занесение на лист MS Excel разрядов числа e

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

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

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

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



G11 =ОСТАТ(G10*F11;$A$7)

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

Рис. 2. Вычисление блоков шифротекста

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

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

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

Задание 2.

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

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

Пример 2

N = 1739, e = 653, требуется дешифровать RSA криптограмму У = 12231108.

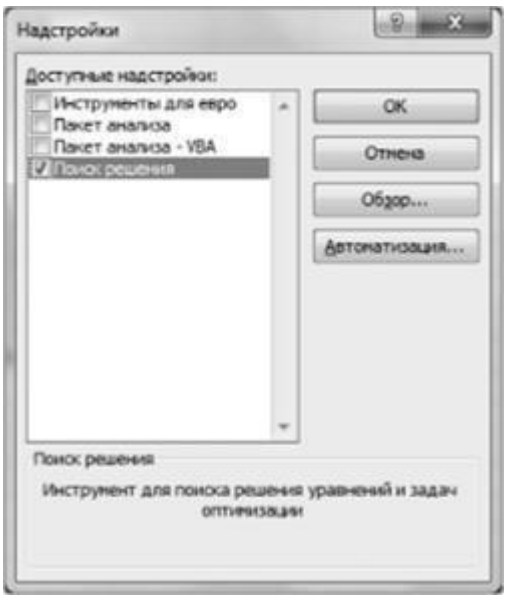


Рис. 3. Включение надстройки «Поиск решения»

В окне Надстройки установить флажок рядом с пунктом Поиск решения и нажать ОК (рис. 3);

- выбрать ячейку B2 (в которой подсчитано произведение двух множителей) и вызвать инструмент Поиск решения на вкладке Данные;
- в окне Поиск решения установить целевую ячейку $B$2 равной значению N (в примере — 1739), в поле Изменяя ячейки переменных выделить диапазон ячеек $A$1:$B$1, в группе В соответствии с ограничениями нажать кнопку Добавить, в окне Добавление ограничения в поле Ссылка на ячейку выделить диапазон ячеек $A$1:$B$1, в следующем поле выбрать значение цел и нажать ОК (рис. 4). Будет установлено ограничение $A$1:$B$1 = целое. Результирующий вид окна настроек инструмента Поиск решения показан на рис. 5;

Рис. 4. Задание ограничений на изменяемые ячейки

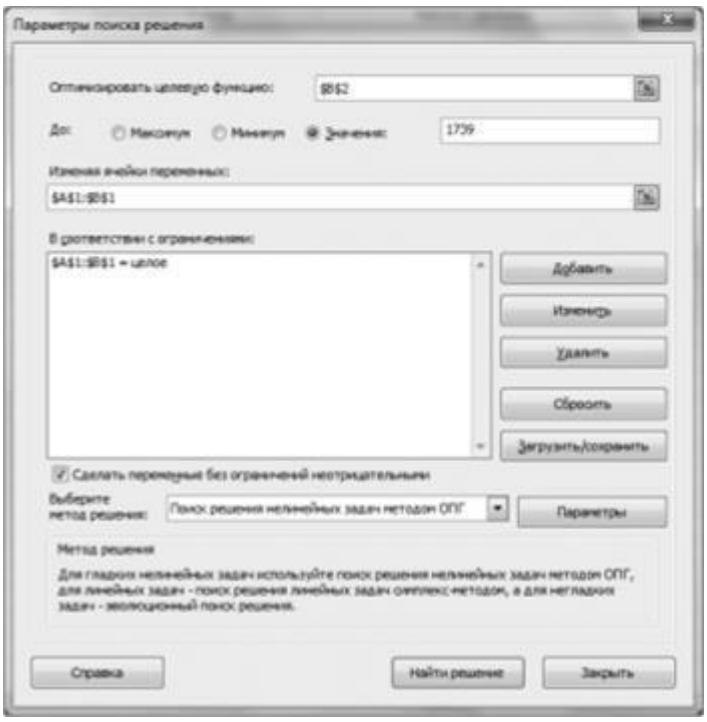


Рис. 5. Настройка инструмента Поиск решения

- в окне Поиск решения выбрать метод решения «Поиск решения нелинейных задач методом ОПГ», затем нажать кнопку «Параметры» и на вкладке «Все методы» установить Максимальное время — 1000 и Предельное число итераций - 10 000. Нажать ОК;
- после того как инструмент Поиск решения полностью настроен, в окне Поиск решения нажать кнопку Выполнить. Будет выдано окно Результаты поиска решения с сообщением о том, что решение найдено — установить переключатель в позицию «Сохранить найденное решение» и нажать ОК. В ячейках A1 и B1 будут получены значения простых множителей числа N.

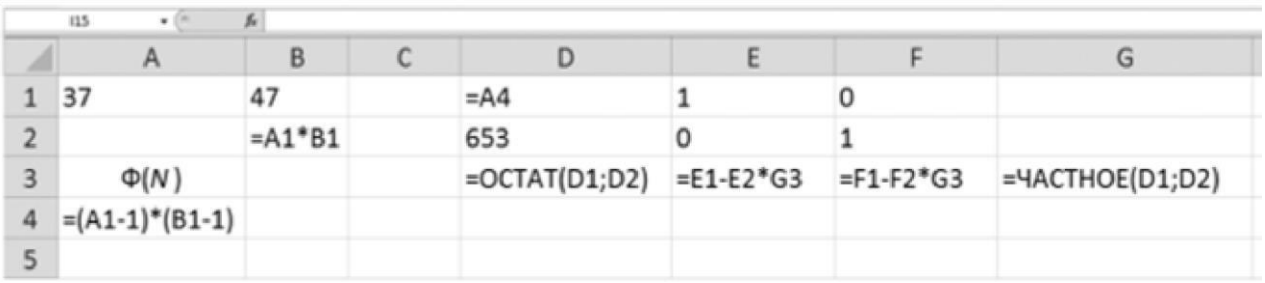
В рассматриваемом примере после выполнения поиска решения в ячейке A1 будет установлено значение 37, а в ячейке B1 — 47. Это и есть множители числа N = 1739. Примечание: если один из множителей получен равным единице, то следует изменить начальные значения в ячейках A1 и B1, а затем повторно выполнить поиск решения.

9. Получили: p = 37, q = 47. Поскольку оба числа простые, легко вычислить значение Φ(N) по формуле: Φ(N) = ϕ(p • q) = (p - 1) • (q - 1). Для вычисления значения Φ(N) занести в ячейку A4 формулу =(A1-1)(B1-1), в ячейку A3 занести подпись к значению. Получено Φ(N) = 1656.

10. Зная значение Φ(N) и e, можно вычислить секретный ключ d. Для вычисления d следует воспользоваться расширенным алгоритмом Евклида:

- сформировать первую строку (U) расширенного алгоритма Евклида: в ячейку D1 занести значение Φ(N) (1656 в рассматриваемом примере), в ячейку E1 —1, в ячейку F1 — 0;
- сформировать вторую строку (V) расширенного алгоритма Евклида: в ячейку D2 занести значение e (в примере — 653), в ячейку E2 — 0, в ячейку F2- 1;

- сформировать строку расширенного алгоритма Евклида: в ячейку G3 занести формулу =ЧАСТНОЕ(D1;D2), в ячейку D3 — формулу =ОСТАТ(D1;D2), в ячейку E3 — формулу =E1-E2*G3, в ячейку F3 — формулу: =F1-F2*G3 (рис. 6);



	A	B	C	D	E	F	G
1	37	47		=A4	1	0	
2		=A1*B1		653	0	1	
3	Φ(N)			=ОСТАТ(D1;D2)	=E1-E2*G3	=F1-F2*G3	=ЧАСТНОЕ(D1;D2)
4	=(A1-1)*(B1-1)						
5							

Рис. 6. Формулы для расчета по алгоритму Евклида

Результаты реализации расширенного алгоритма Евклида для рассматриваемого примера показаны на рис. 7. Получено значение d = 317.

	A	B	C	D	E	F	G	H
1	37	47		1656	1	0		
2		1739		653	0	1		
3	Φ(N)			350	1	-2	2	
4	1656			303	-1	3	1	
5				47	2	-5	1	
6	d			21	-13	33	6	
7	317			5	28	-71	2	
8				1	-125	317	4	
9				0	653	-1656	5	
10				#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!	
11				#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!	
12				#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!	
13								

Рис. 7. Пример реализации расширенного алгоритма Евклида

11. Подготовить последовательность Y к расшифрованию, разбив ее на части $y_к$ таким образом, что $y_к$<N, $y_к$ не содержит ведущих нулей. В рассматриваемом примере N = 1739, Y = 12231108, Y может быть разбито на два блока — y_1 = 1223, y_2 = 1108.

12. Аналогично п. 4 задания 1 подготовить реализацию алгоритма быстрого вычисления степени d по модулю N для дальнейшего определения блоков открытого текста по формуле $x_k = y_к \bmod N$:

- перевести значение степени d в двоичное представление, занести его в ячейку A8. В рассматриваемом примере d = 317 < 511, поэтому можно воспользоваться функцией MS Excel ДЕС.В.ДВ группы Инженерные, тогда в ячейку A8 можно занести формулу =ДЕС.В.ДВ(A7). Получено значение 100111101;

- определить p — число разрядов двоичного представления числа d с помощью функции ДЛСТР, поместить результат в ячейку А9. Получено p = 9;
- занести в ячейку А10 подпись У, в ячейку А2 — подпись N;
- в столбцах I — M сформировать таблицу для вычисления степени d по модулю N: задать заголовки столбцов I, J и К (i, b_i, y_i); в ячейки столбца I занести значения от 0 до 8; в ячейку J2 занести формулу =ПСТР($A$8;$A$9-I2;1), в ячейку К2 — =A11, в ячейку КЗ — =ОСТАТ(К2^2;$B$2), в ячейку L2 — =ЕСЛИ(J2="0";1;K2), в ячейку М2- =L2, в ячейку М3— формулу =ОСТАТ(М2*L3;$B$2). Скопировать последние формулы каждого столбца на оставшийся диапазон ячеек столбца;
- последняя заполненная ячейка столбца M (M10 в примере) содержит результат вычисления степени по модулю. Подписать эту ячейку как x.

13. Получить значения блоков открытого текста $x_к$, последовательно занося значения блоков $y_к$ в подготовленную для этого ячейку А11. Значения блоков $y_к$ и полученные $x_к$ с подписями занести на лист (например, в диапазон ячеек А13:В15) (рис. 8).

Значения блоков открытого текста: x, = 283, x2 = 827.

14. Ниже сформированных блоков открытого текста получить полное значение X, использовав операцию конкатенации &. В примере в ячейку В16 следует занести формулу =B14&B15 и подписать эту ячейку как X. Получено числовое представление открытого текста X = 283827.

M10 | =ОСТАТ(M9*L10;$B$2)

	A	B	C	H	I	J	K	L	M	N
1	37	47			*i*	b_i	y_i			
2	*N*	1739			0	1	1108	1108	1108	
3	*Φ(N)*				1	0	1669	1	1108	
4	1656				2	1	1422	1422	42	
5					3	1	1366	1366	1724	
6	*d*				4	1	9	9	1604	
7	317				5	1	81	81	1238	
8	100111101				6	0	1344	1	1238	
9	9				7	0	1254	1	1238	
10	*y*				8	1	460	460	827	
11	1108								*x*	
12										
13	*yk*	*xk*								
14	1223	283								
15	1108	827								
16		283827	*X*							
17										

Рис. 8. Вычисление блоков открытого текста

15. Разбить X на двузначные числа и провести обратное преобразование чисел в символы языка по табл. 1.

28 - с, 38 - ы, 27 - р.

Получен открытый текст «сыр».

Полученный файл MS Excel показать преподавателю.

Эталон ответа

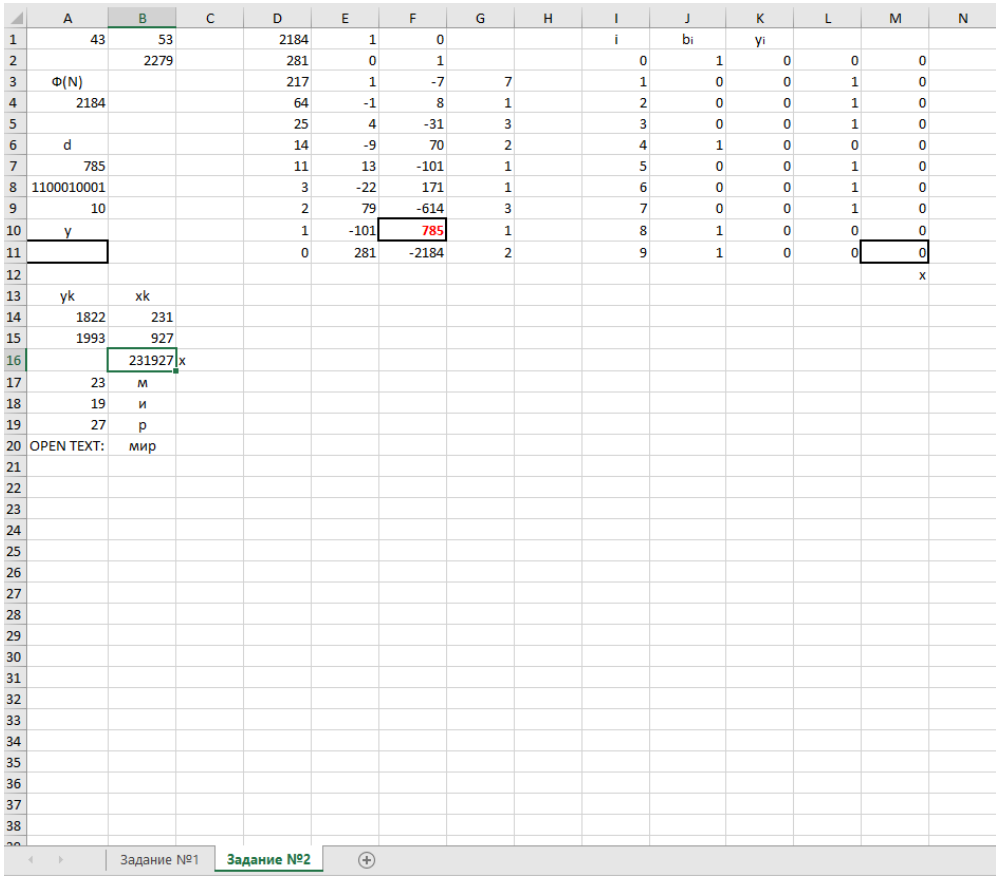
Задание 1. Работа выполняется по варианту №1. Были закодированы символы сообщения с помощью табл.1, а затем зашифровано сообщение по алгоритму RSA с помощью открытого ключа (N, e).

	A	B	C	D	E	F	G	H
1	e		i	b_i	x_j			
2	281		0	1	0	0	0	
3	100011001		1	0	0	1	0	
4	9		2	0	0	1	0	
5			3	1	0	0	0	
6	N		4	1	0	0	0	
7	2279		5	0	0	1	0	
8	x		6	0	0	1	0	
9			7	0	0	1	0	
10			8	1	0	0	0	
11							y	
12	xk	yk						
13	282	746						
14	524	1212						
15		7461212	Y					
16								

Получена шифрограмма Y=746212.

Задание 2. Криптограмма У получена RSA шифрованием на известном открытом ключе (N, e). Определяем секретный ключ d и получаем открытый текст.

Выбираем значения открытого ключа (N, e) и криптограммы У из табл. 2 (в соответствии с номером варианта (Вариант №1). Выполняем дешифрование криптограммы.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	43	53		2184	1	0			i	b_i	y_i			
2		2279		281	0	1			0	1	0	0	0	
3	Φ(N)			217	1	-7	7		1	0	0	1	0	
4	2184			64	-1	8	1		2	0	0	1	0	
5				25	4	-31	3		3	0	0	1	0	
6	d			14	-9	70	2		4	1	0	0	0	
7	785			11	13	-101	1		5	0	0	1	0	
8	1100010001			3	-22	171	1		6	0	0	1	0	
9	10			2	79	-614	3		7	0	0	1	0	
10	y			1	-101	785	1		8	1	0	0	0	
11				0	281	-2184	2		9	1	0	0	0	
12													x	
13	yk	xk												
14	1822	231												
15	1993	927												
16		231927	x											
17	23	м												
18	19	и												
19	27	р												
20	OPEN TEXT:	мир												

Задание №1 | Задание №2

Получен открытый текст «мир».

6. Практическая работа №4 Разработка хэш-функции

Инструкция для обучающихся

Внимательно прочитайте задание. Сформируйте зашифрованное сообщение по алгоритму RSA с помощью открытого ключа, произведите дешифрование криптограммы.

Время выполнения задания – 45 минут.

Задание

1. Подготовьте (создайте или выберите) текстовый файл с семантически понятным содержимым.
2. С помощью OpenSSL вычислите значение хэш-функции MD5 от подготовленного текста. Измерьте время хеширования и запомните (запишите) его.
3. Выполните действие 3 для алгоритма SHA1.
4. Сравните время хеширования с применением двух алгоритмов.
5. Измените содержимое исходного файла.
6. Посчитайте хеш-суммы MD5 и SHA1 от изменённого файла. Убедитесь, что значения сумм от исходного и изменённого файлов не совпадают.

Эталон ответа

Был создан текстовый файл dok.txt (рис. 1)

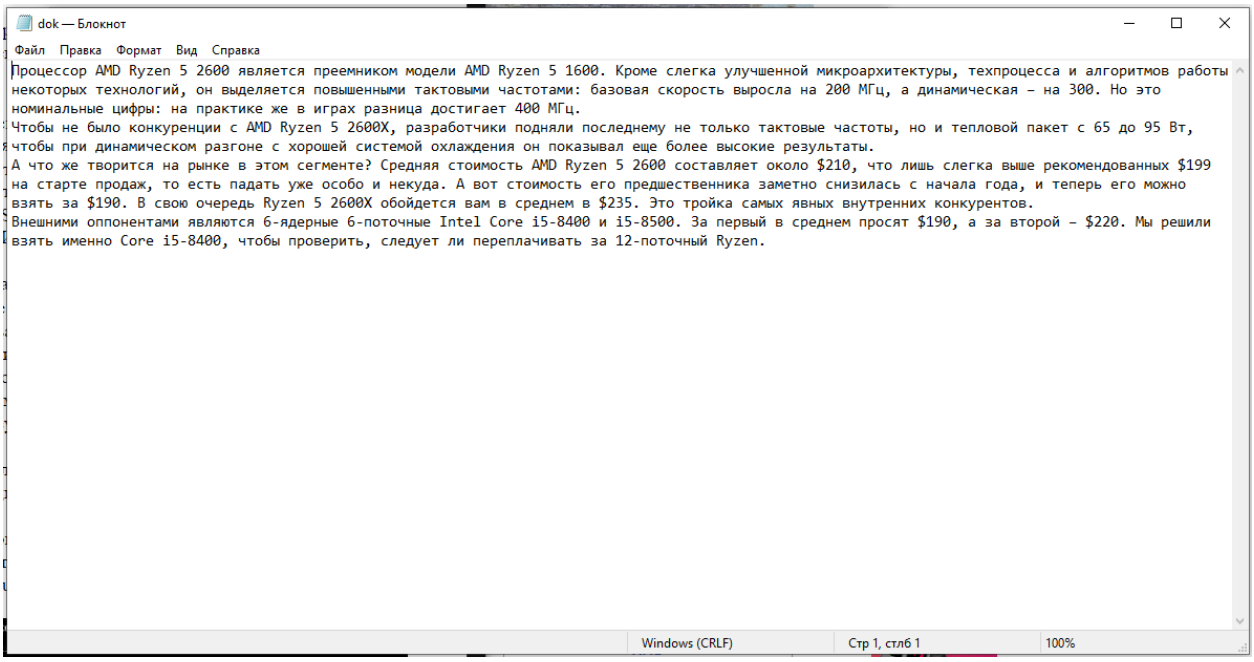


Рисунок 1 «Читаемый исходный текст»

Вычисление значения хэш-функции MD5 от подготовленного текста (рис. 2)

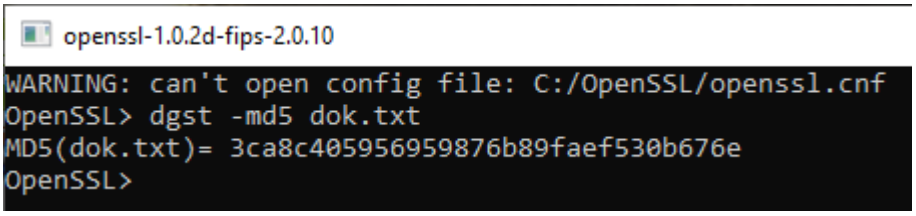


Рисунок 2 «Окно программы с вычисленной хэш-функцией MD5»

Для файлов размером меньше 1ГБ разница во времени хеширования будет не существенной.

Вычисление значения хэш-функции SHA1 от подготовленного текста (рис. 3)

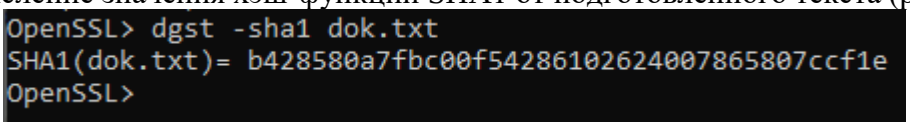


Рисунок 3 «Окно программы с вычисленной хэш-функцией SHA1»

Исходный текст был изменён (рис. 4)

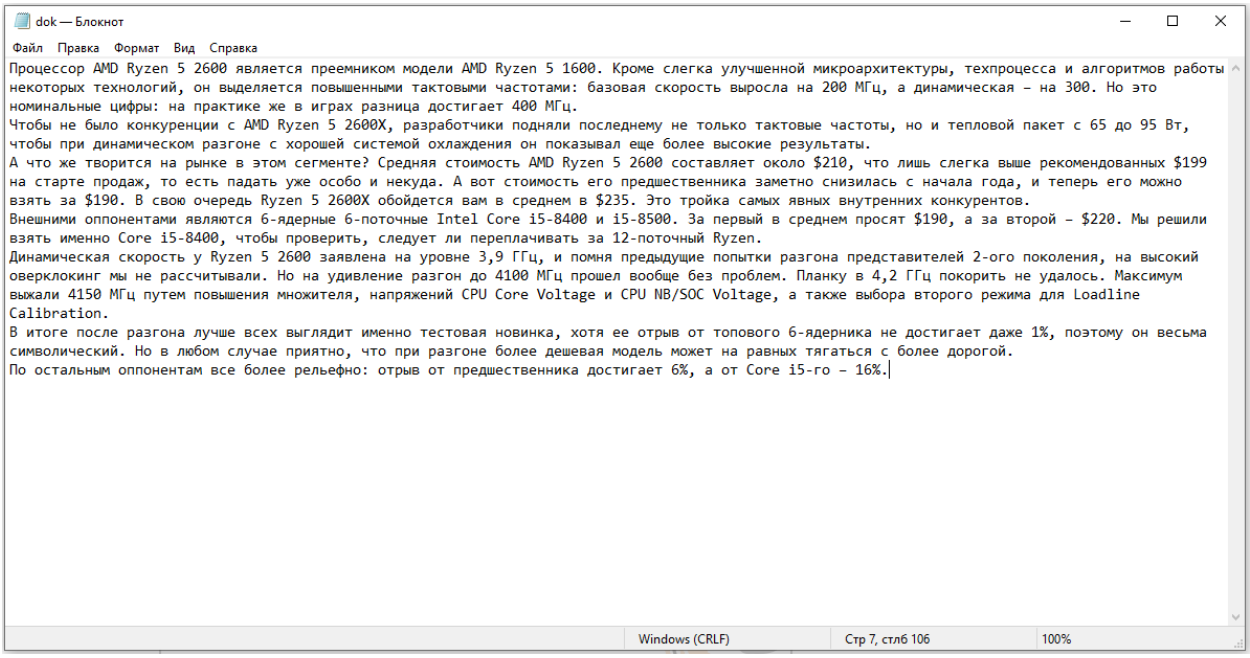


Рисунок 4 «Читаемый изменённый исходный текст»

Вычисление значения хэш-функции MD5 и SHA1 от изменённого подготовленного текста (рис. 5)

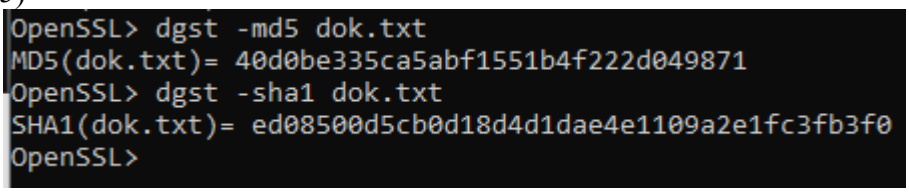


Рисунок 5 «Окно программы с вычисленной хэш-функцией MD5 и SHA1»

Необходимо было сгенерировать закрытый ключ длиной 2048 бит без парольной фразы для алгоритма RSA и записать их в файл keys.rsa (рис. 6)

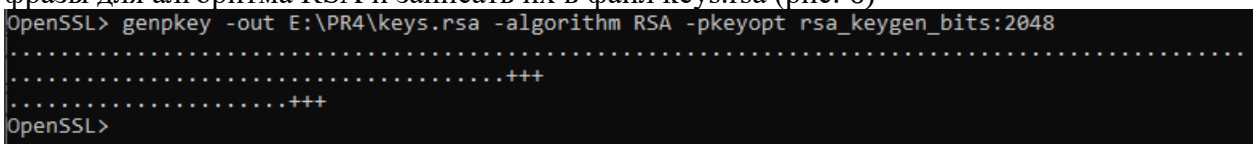


Рисунок 6 «Генерация закрытого ключа»

Была выведена информация о закрытом ключе (рис. 7)

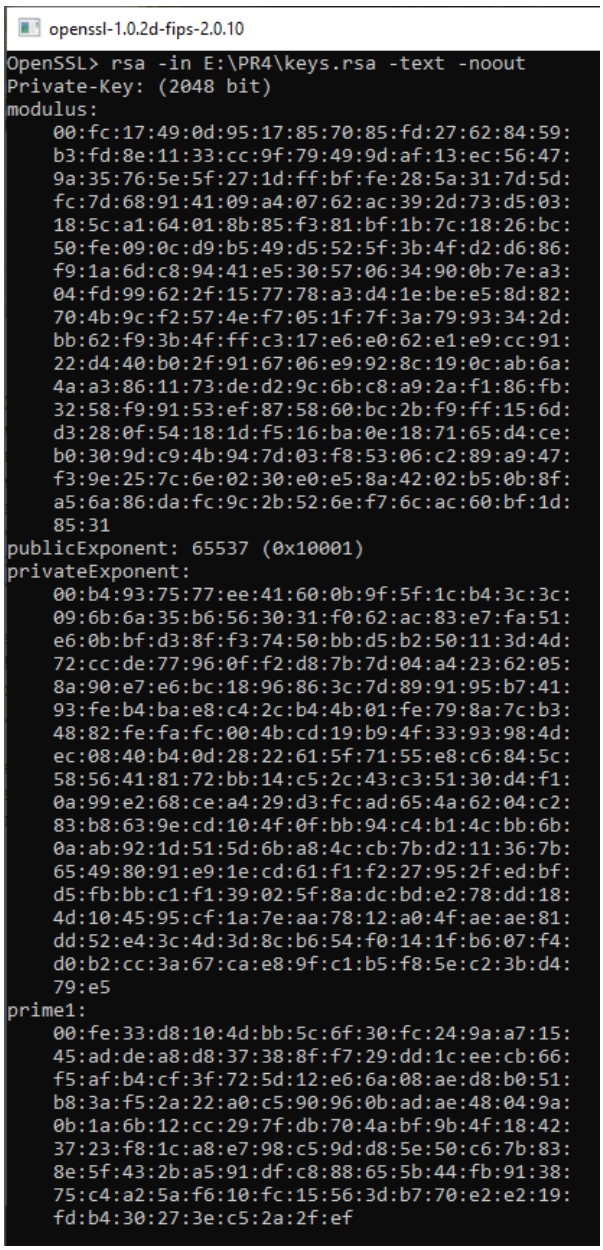


Рисунок 7 «Информация о закрытом ключе»

Извлечение открытого ключа в формате PEM из закрытого ключа (рис. 8)

```
OpenSSL> rsa -in E:\PR4\keys.rsa -pubout -out E:\PR4\pubkey.rsa -outform PEM
writing RSA key
OpenSSL>
```

Рисунок 8 «Извлечение открытого ключа в формате PEM»

Подписание хэш-суммы sha512 от файла file закрытым ключом алгоритма RSA, записание подписи в файл file.sig (рис. 9)

```
OpenSSL> dgst -sha512 -sign E:\PR4\keys.rsa -out E:\PR4\file.sig E:\PR4\dok.txt
OpenSSL>
```

Рисунок 9 «Подписание хэш-суммы sha512»

Проверка подписи хэш-суммы sha512 из файла file.sig для файла file по алгоритму RSA (рис. 10)

```
OpenSSL> dgst -sha512 -verify E:\PR4\pubkey.rsa -signature E:\PR4\file.sig E:\PR4\dok.txt
Verified OK
OpenSSL>
```

Рисунок 10 «Проверка подписи хэш-суммы sha512»

Снятие защиты ключа парольной фразой (рис. 11)

```
OpenSSL> rsa -in E:\PR4\keys.rsa -passin pass:1234 -out keys_nopass.rsa
writing RSA key
OpenSSL>
```

Рисунок 11 «Снятие защиты ключа парольной фразой»

Вывод: На практике я познакомился с программой OpenSSL и научился работать с хэш-суммами текстовых файлов.

7. Устный зачет по Теме 2.3

Инструкция для обучающихся

Зачет сдается в рамках учебного занятия. Каждый студент отвечает в устной форме на предложенные преподавателем 11 минивопросов.

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

Перечень вопросов:

1. В чем заключается суть и основная предпосылка появления шифрования с открытым ключом?
2. Основные требования, предъявляемые к криптосистемам с открытым ключом.
3. Перечислите типы односторонних преобразований, применяемых при асимметричном шифровании.
4. В чем отличие сверхвозрастающей последовательности от обыкновенной?
5. Что означает обратное число по модулю?
6. В чем отличие вероятностного шифрования с открытым ключом от детерминированного?
7. В чем суть задачи дискретного логарифмирования?
8. Что такое аутентификация?
9. Перечислите основные методы аутентификации.
10. Что такое хеш-преобразование?
11. Перечислите основные свойства хеш-функций.

Эталоны ответов: приведены в Учебном пособии МДК.02.02 «Криптографические средства защиты информации».

8. Практическая работа № 5 Анализ графических изображений на наличие скрытой информации

Инструкция для обучающихся

Внимательно прочитайте задание. Проанализируйте графическое изображение на наличие скрытой информации.

Время выполнения задания – 45 минут.

Задание

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

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

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

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

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

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

Эталон ответа:

Картинка с внедрённым сообщением имеет слабозаметные искажения (рис. 1)

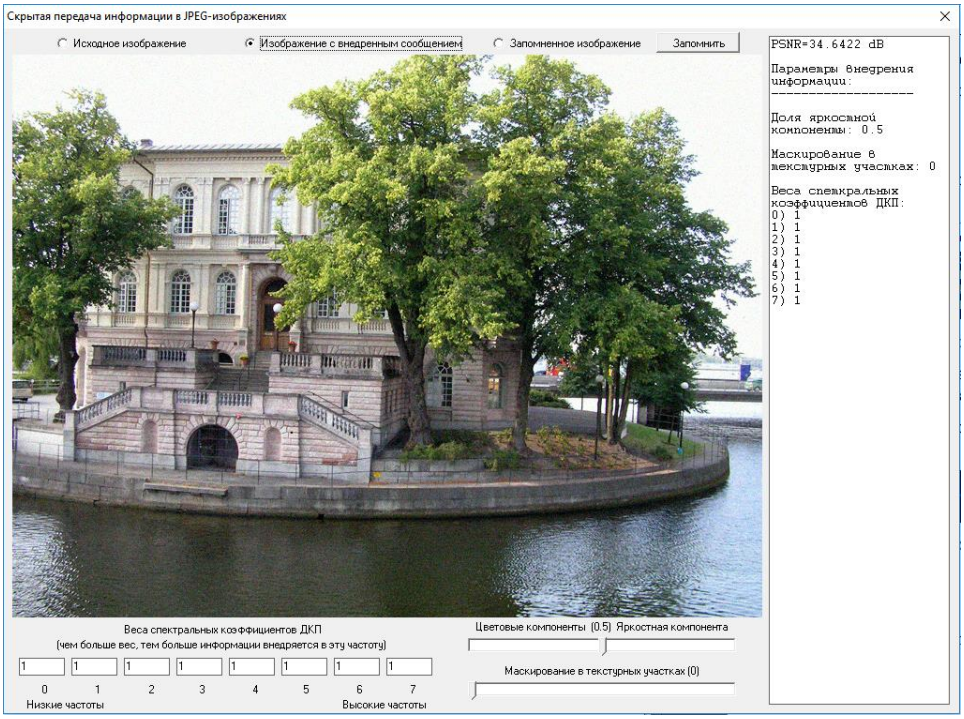


Рисунок 1 «Картинка с сообщением»

В ходе выполнения практической работы было достигнуто значение в 43,3834 дБ (рис. 2)

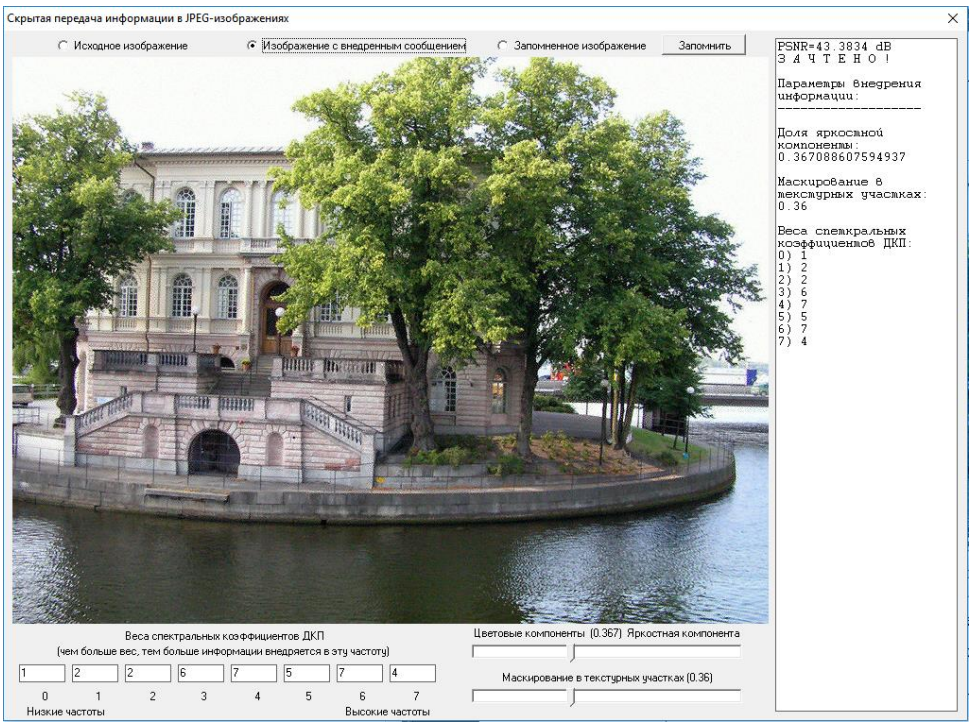


Рисунок 2 «Достигнутое значение»

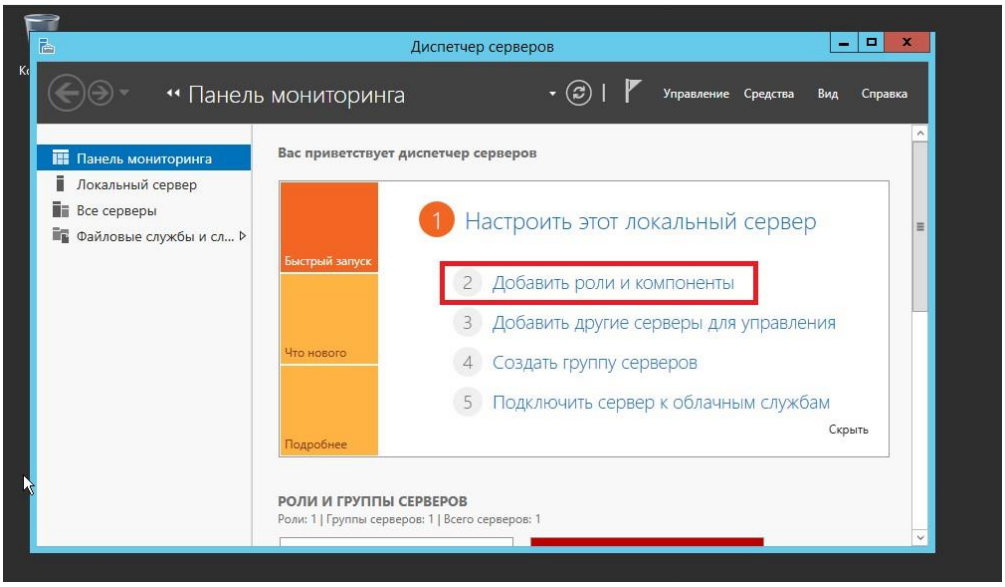
3.1.3. Оценка освоения теоретического курса профессионального модуля по МДК.02.03

Дидактические единицы	Освоенные умения и усвоенные знания	Общие и профессиональные компетенции, формируемые в процессе изучения темы	Формы контроля (наименование контрольной точки)	
			Текущая аттестация (в соответствии с ККЗ)	Промежуточная аттестация
Тема 3.1. Установка и настройка Windows Server 2019	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие № 2. Установка контроллера домена. Использование Windows PowerShell для администрирования AD DS.	Устные ответы на дифференцированном зачете
	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7, ПК 2.8	Устный зачет по теме 3.1	
Тема 3.2. Администрирование Windows Server 2019	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие № 8.Применение технологии DirectAccess с помощью мастера начальной настройки	

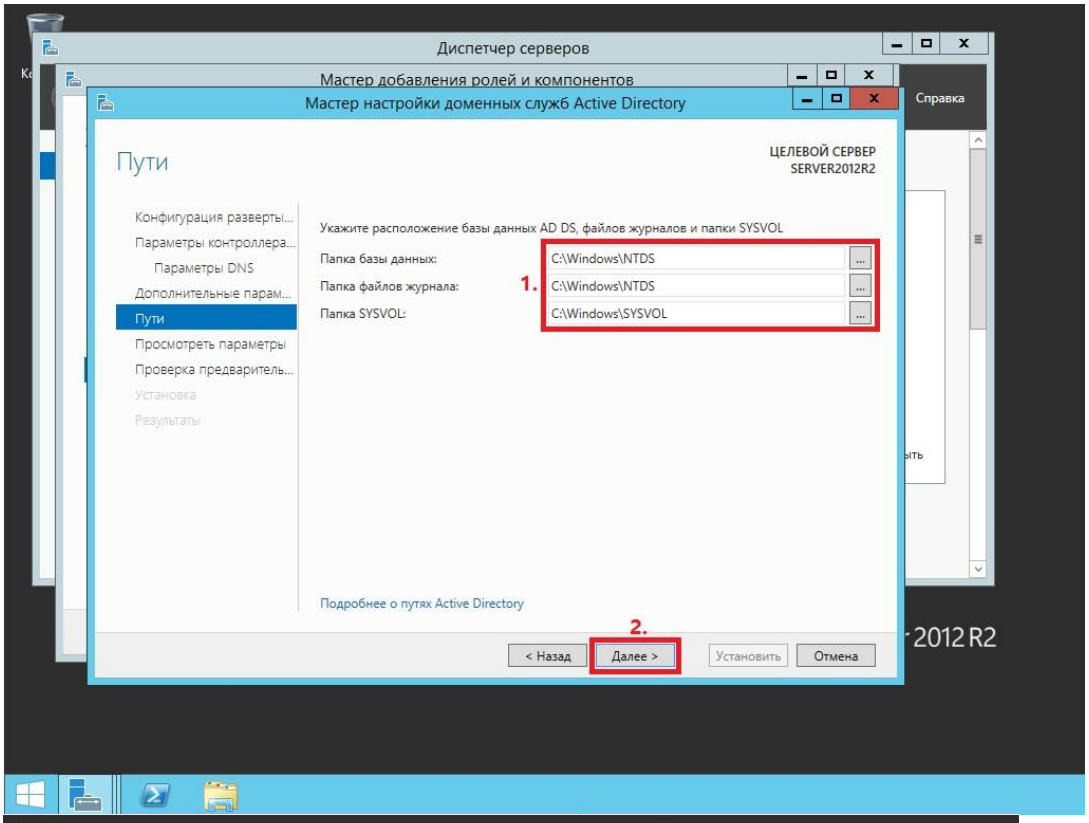
	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие № 17. Настройка групповых политик	
Тема 3.3. Установка и администрирование Linux	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие № 20. Настройка web-сервера в ОС Debian.	
	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие № 26. Настройка web-сервера в CentOS.	
Тема 3.4. Основы кибербезопасности	З8-З11 У17-У19	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие № 37. Поиск уязвимостей информационных систем	
	З8-З11 У17-У19	ОК11-ОК11 ПК2.7, ПК 2.8	Устный зачет по теме 3.4	
Тема 3.5. Поиск уязвимостей	З8-З11 У17-У19	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие № 43. Поиск открытых портов	
	З8-З11 У17-У19	ОК11-ОК11 ПК2.7, ПК 2.8	Устный зачет по теме 3.5	
Тема 3.6. Защита информационной инфраструктуры	З8-З11 У17-У19	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие № 52. Настройка параметров безопасности Windows.	
	З8-З11 У17-У19	ОК11-ОК11 ПК2.7, ПК 2.8	Устный зачет по теме 3.6	
Тема 3.7. Расследование инцидентов	З8-З11 У17-У19	ОК11-ОК11 ПК2.7, ПК 2.8	Устный зачет по теме 3.7	
Тема 3.8. Поиск информации по открытым источникам	З8-З11 У17-У19	ОК11-ОК11 ПК2.7,	Устный зачет по теме 3.8	

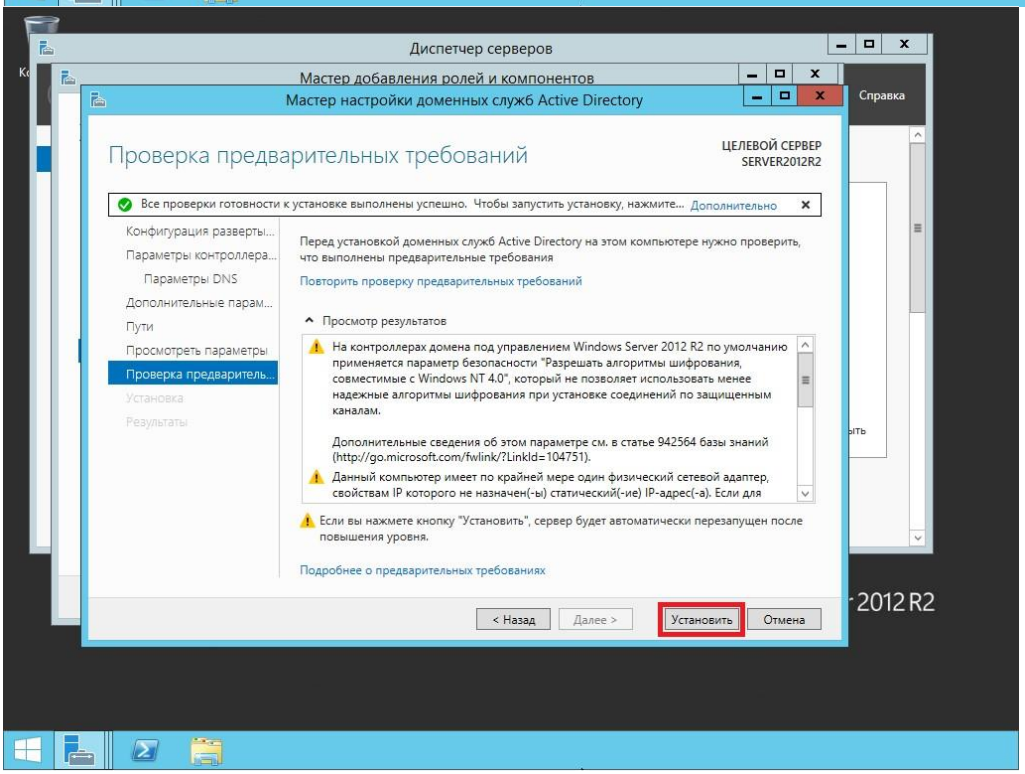
		ПК 2.8		

1. **Практическое занятие № 2. Установка контроллера домена. Использование Windows PowerShell для администрирования AD DS.**
   Инструкция для обучающихся
   Внимательно прочитайте задание. Выполните все действия.
   Задание: установить контроллер домена, настроить базовые параметры.
   Эталоны ответа:
   Был установлен контроллер домена:

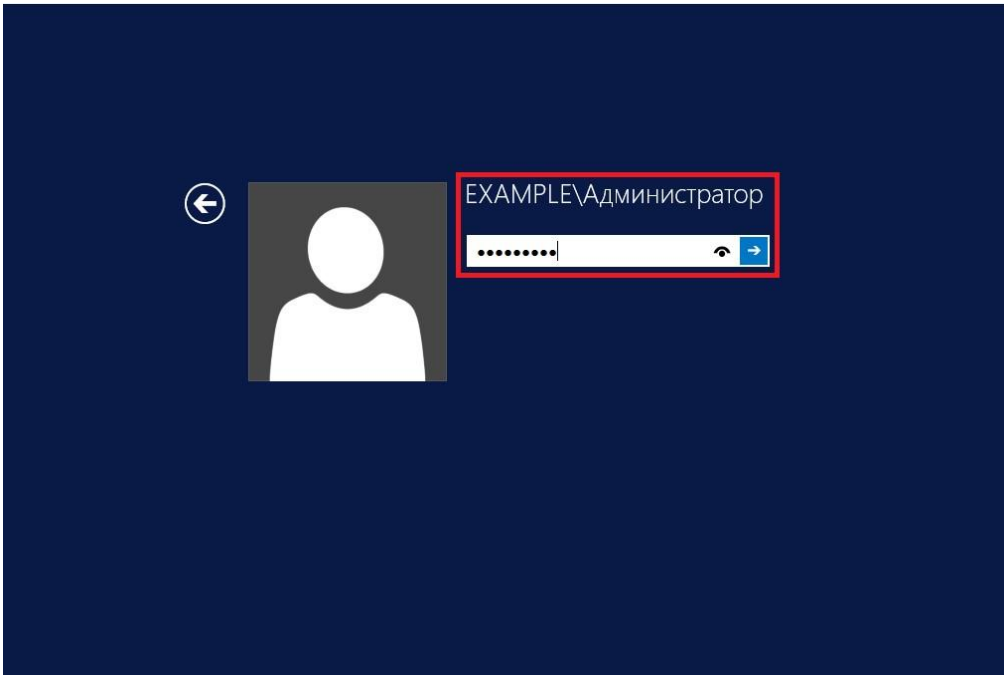


Настроены все роли и компоненты:





Проверена работоспособность :



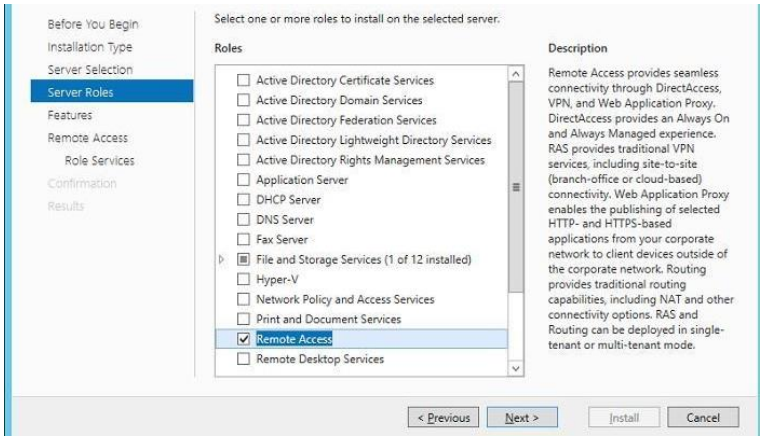
2. **Устный зачет по теме 3.1.**

Инструкция для обучающихся: Зачет проводится в учебное время. Каждый студент отвечает на 5 вопросов по выбору преподавателя. С перечнем вопросов студенты ознакомлены заранее (за неделю). Время ответа 3 минуты. Время проведения зачета для группы – одно учебное занятие.

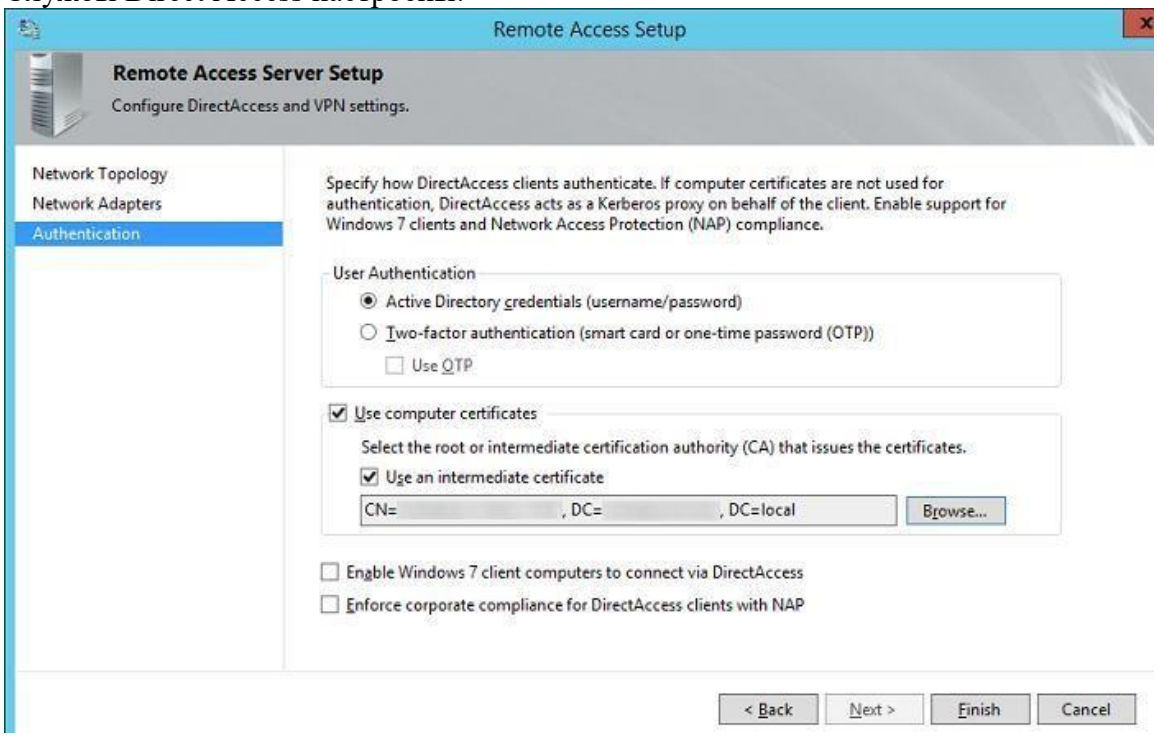
Перечень вопросов:

1. Доменные сервисы Windows Server 2019
2. Службы каталога Windows Server 2019
3. Групповые политики Windows Server 2019
4. Сервер времени Windows Server 2019
5. Центр сертификации Windows Server 2019

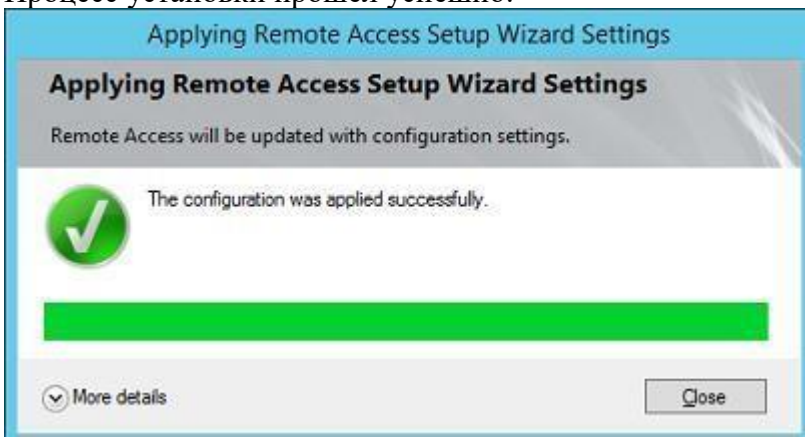
3. **Практическое занятие № 8. Применение технологии DirectAccess с помощью мастера начальной настройки.**
   Инструкция для обучающихся
   Внимательно прочитайте задание. Выполните все действия.
   Задание: установить роль Remote Access, настроить службы Direct Access.
   Эталон ответа:
   Роль Remote Access установлена:



Службы Direct Access настроены:

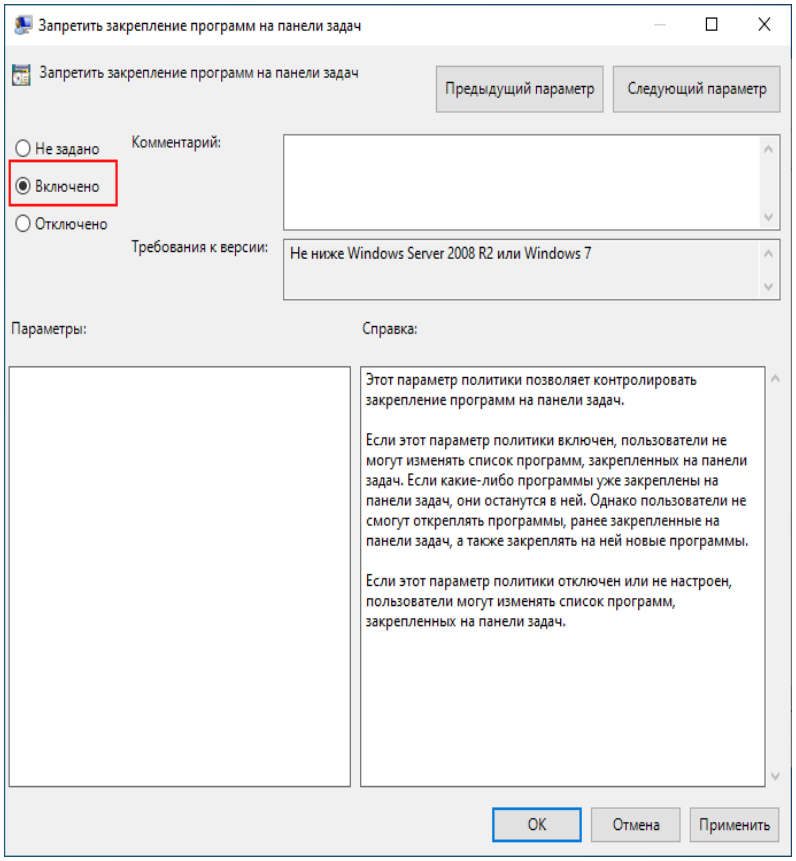


Процесс установки прошел успешно:

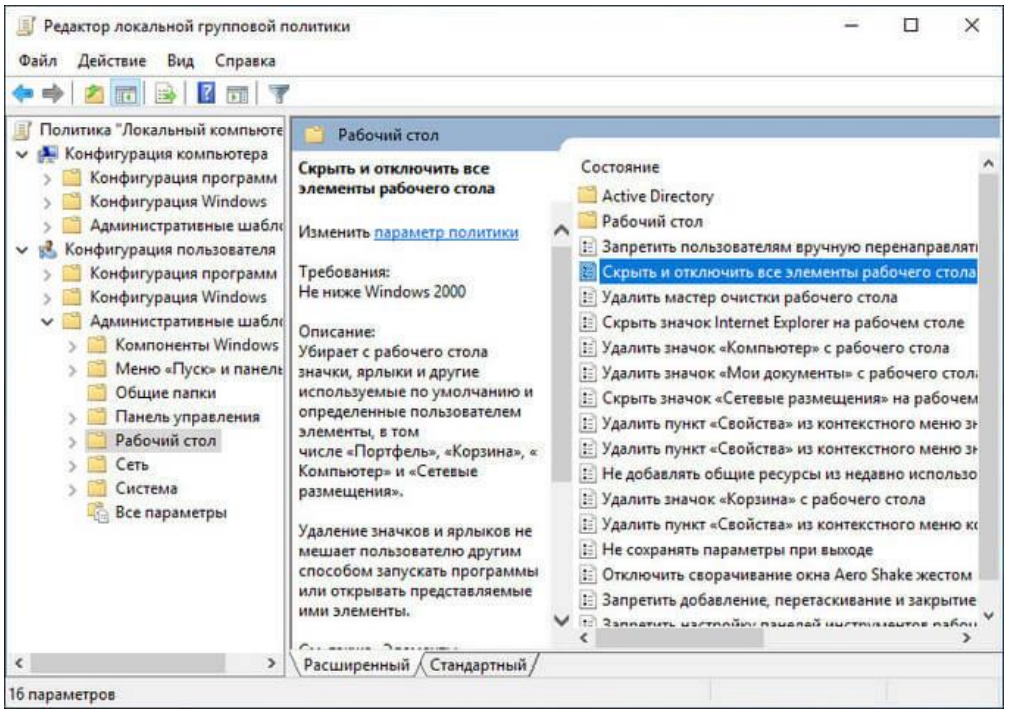


4. **Практическое занятие № 17. Настройка групповых политик**
   Инструкция для обучающихся
   Внимательно прочитайте задание. Выполните все действия.
   Задание: настроить групповые политики.
   Эталон ответа:

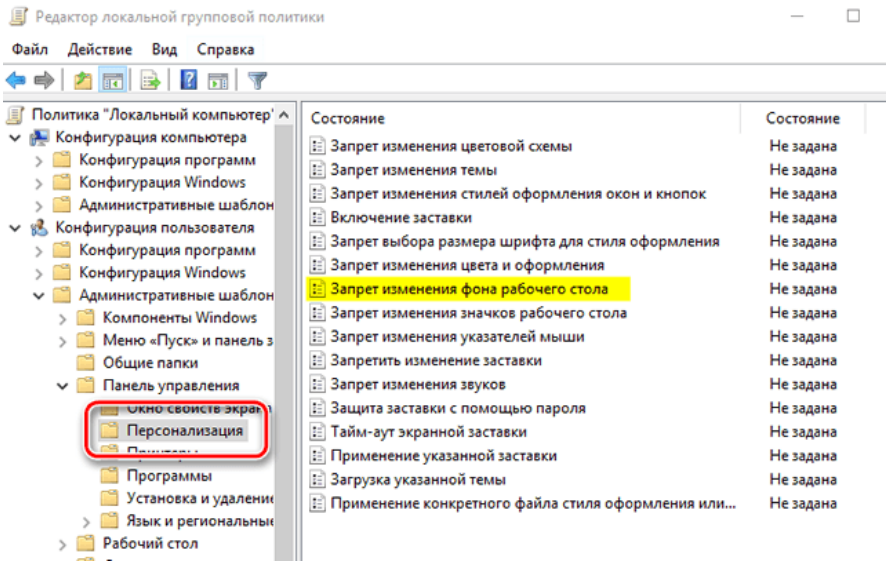
1. Запрет добавление значка ярлыка проигрывателя на рабочий стол пользователя.



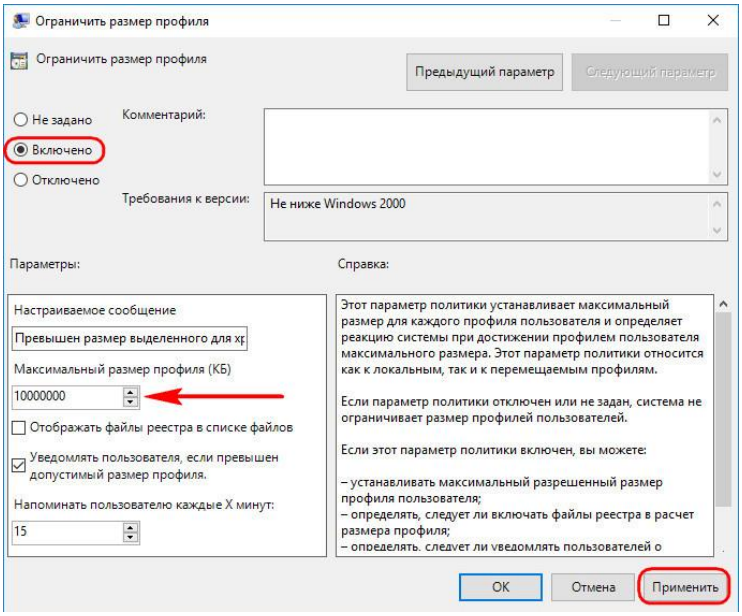
2. Убрать все значки с Рабочего стола.



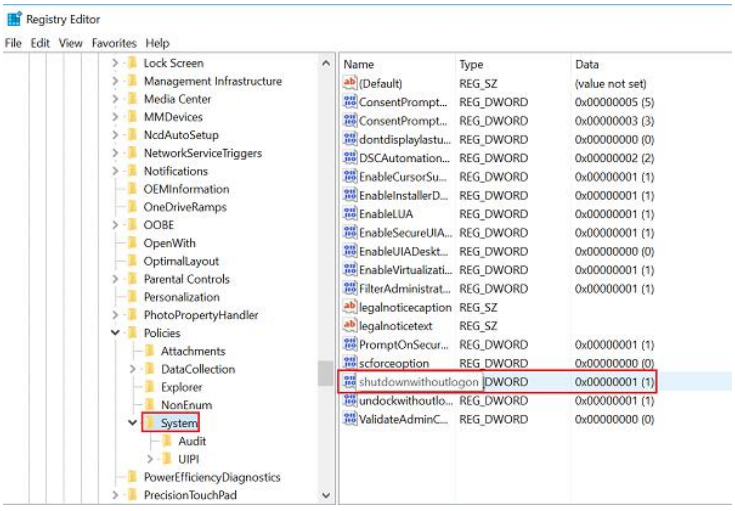
3. Запрещение изменения фонового рисунка Рабочего стола



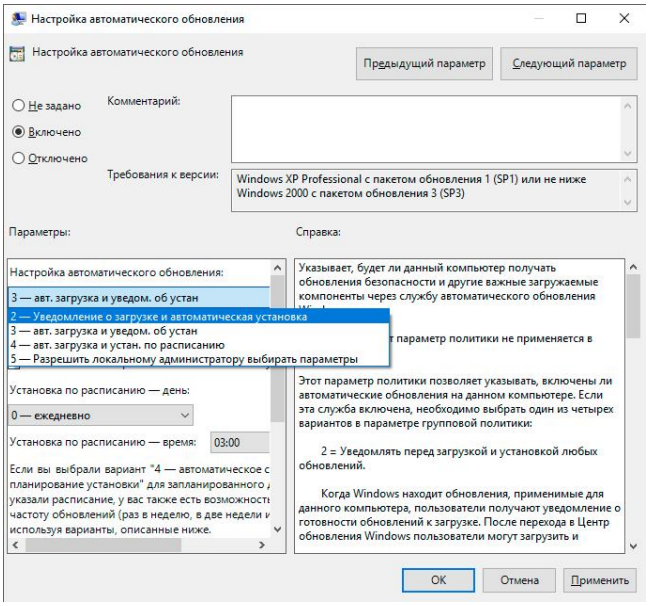
4. Ограничение размера профиля конкретного пользователя.



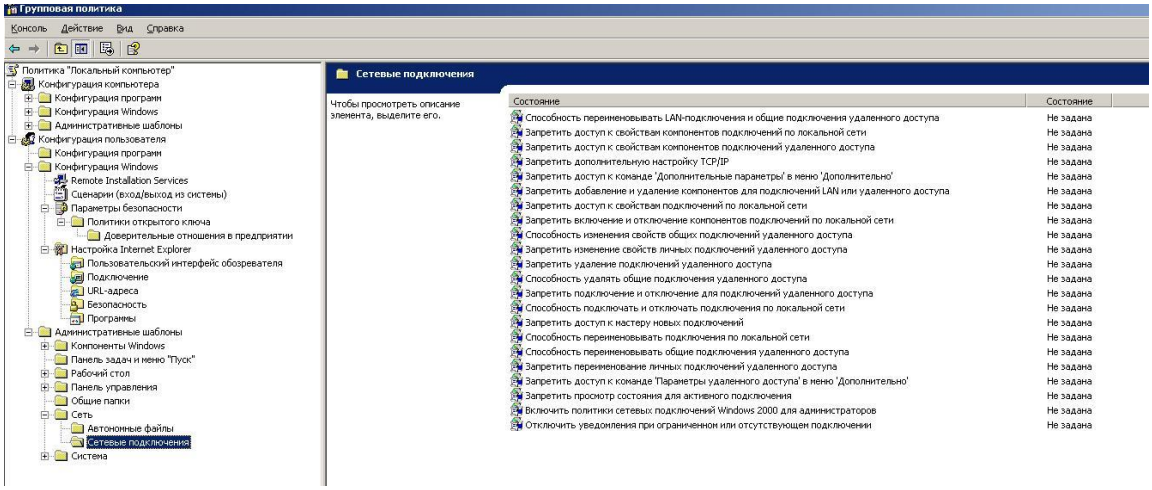
5. Удаление кнопки Завершение работы из меню Пуск.



6. Установка обновления системы безопасности и других важных обновлений. Обновления должны происходить только каждый вторник в 12.00.



7. Запрет пользователям подключать и отключать подключения по локальной сети.



5. Практическое занятие № 20. Настройка web-сервера в ОС Debian.

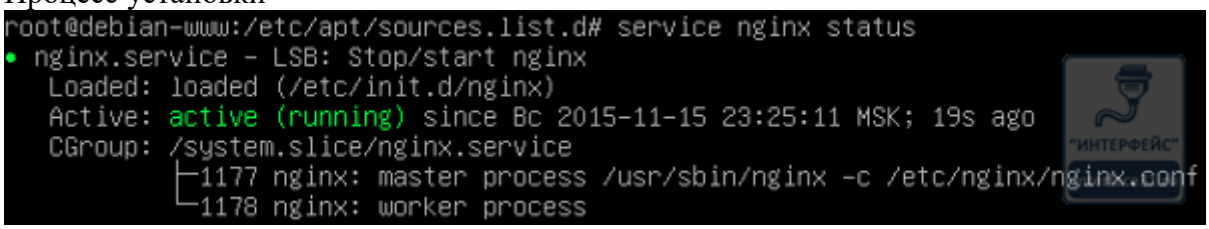
Инструкция для обучающихся

Внимательно прочитайте задание. Выполните все действия.

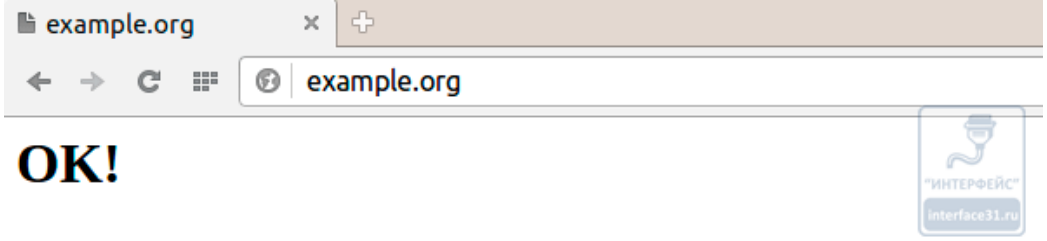
Задание: настроить веб-сервер ОС Debian

Эталон ответа:

Процесс установки



После перезагрузки веб-сервер работает:



Код настройки:

```
worker_processes  2;
```

Приведем секцию **events** к виду:

```
events {
 worker_connections 1024;
 use epoll;
}
```

Первая опция задает количество соединений на рабочий процесс, вторая задает метод обработки соединений, явно укажем наиболее эффективный для Linux.

Теперь перейдем в секцию http и после строки

```
access_log  /var/log/nginx/access.log  main;
```

зададим следующие опции:

```
client_header_timeout 30;
client_body_timeout 30;
reset_timedout_connection on;
```

Они задают таймаут (в секундах) на чтение клиентом тела и заголовка запроса, последняя опция разрешает сброс соединений по таймауту.

```
client_max_body_size 32m;
client_body_buffer_size 128k;
```

Эти параметры ограничивают максимальный размер тела запроса клиента и задают буфер для чтения заголовка запроса. Максимальный размер тела запроса ограничивает размер файла, который может быть загружен веб-сервером.

```
sendfile on;
tcp_nopush on;
```

Также разрешим передачу файлов и оптимизируем этот процесс.

Изменим параметр:

```
keepalive_timeout  30;
```

Он задает таймаут постоянных (keep-alive) соединений, которые позволяют повысить производительность протокола HTTP/1.1, но незакрытое соединений впустую использует ресурсы сервера и поэтому такие соединения следует принудительно завершать.

Ниже зададим параметры **gzip-сжатия**:

```
gzip on;
gzip_disable "msie6";
gzip_proxied any;
gzip_min_length 1024;
gzip_comp_level 4;
gzip_types text/plain text/css application/json application/javascript application/x-javascript
text/xml application/xml application/xml+rss text/javascript application/atom+xml applica-
tion/rdf+xml;
```

Первая опция включает gzip-сжатие, затем отключаем его для младших версий IE (6 и ниже), если такие вдруг зайдут на наш сервер, разрешим сжимать проксированные запросы, это нужно для сжатия динамического содержимого, затем укажем минимальный размер сжимаемого ответа, чтобы не тратить ресурсы сервера на сжатие коротких ответов. Ниже задается уровень сжатия и типы сжимаемых данных.

В самом конце, после

```
include /etc/nginx/conf.d/*.conf;
```

добавим

```
include /etc/nginx/sites-enabled/*;
```

Это позволит подключать конфигурации виртуальных хостов из папки sites-enabled.

Сохраним и проверим конфиг командой:

```
nginx -t
```

После чего можно перезапустить nginx:

```
service nginx restart
```
Теперь можно перейти к настройке виртуальных хостов, создадим две папки:
```
mkdir /etc/nginx/sites-available
mkdir /etc/nginx/sites-enabled
```
В первой будут хранится настройки сайтов, а во второй мы будем создавать символьные ссылки для того, чтобы подключить настройки сайта к конфигурационному файлу nginx.
Перед тем как описывать виртуальные хосты, создадим структуру папок для их хранения:
```
mkdir /var/www
mkdir /var/www/example.org
```
Затем создадим конфигурационный файл для нашего первого сайта:
```
touch /etc/nginx/sites-available/example.org.conf
```
Какого-либо стандарта по названию файлов у nginx нет, поэтому можете придерживаться своей системы, главное, чтобы вам было понятно, какой файл за какой сайт отвечает. Теперь откроем его и внесем следующий текст:
```
server {
  listen 80;

  server_name example.org;
  charset utf-8;

  root /var/www/example.org;
  index index.html index.htm index.php;

  access_log /var/log/nginx/example.org_access.log;
  error_log /var/log/nginx/example.org_error.log;
}

server {

  listen 80;

  server_name www.example.org;
  rewrite ^(.*) http://example.org$1 permanent;
}
```
Его синтаксис достаточно прост и понятен, первая секция **server** задает основные параметры сайта, его имя, кодировку, расположение корневой директории и файлов логов. Вторая секция нужна для перенаправления сайта **с www** на **без www**.
Если вы хотите сделать данный виртуальный хост сайтом по умолчанию, т.е. тем на который будут переадресовываться все запросы, для которых nginx не нашел подходящего виртуального хоста или без имени сервера вообще, например, по IP-адресу, то добавьте к директиве **listen** опцию **default**, начиная с версии 0.8.1 можно использовать опцию **default_server**:
```
 listen 80 default;
```
Директива **index** указывает индексные файлы, которые будет искать в данном расположении веб-сервер в порядке их перечисления, так если в директории имеются одновременно **index.html** и **index.php** - использоваться всегда будет первый. Указанная конструкция универсальна, но на практике лучше указать один тип индексного файла, тот что реально используется.
Сохраняем конфигурацию и подключаем ее к nginx:
```
ln -s /etc/nginx/sites-available/example.org.conf  /etc/nginx/sites-enabled/
```
Проверяем конфигурацию и заставим nginx ее перечитать:

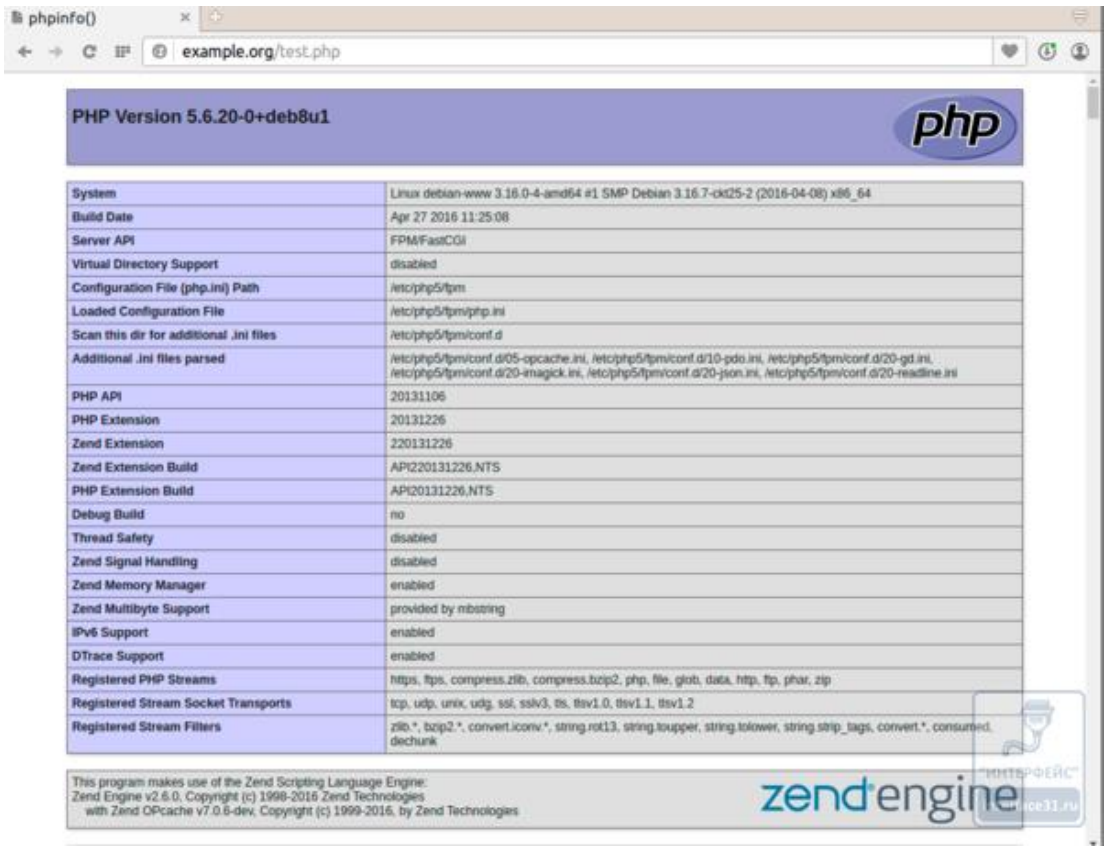
```
nginx -t
service nginx reload
```

6. **Практическое занятие № 26. Настройка web-сервера в CentOS.**
   Инструкция для обучающихся
   Внимательно прочитайте задание. Выполните все действия.
   Задание: установить роль Remote Access, настроить службы Direct Access.
   Эталон ответа:
   Для начала установим сервер MariaDB для этого в командной строке нужно выполнить:

   # yum -y install mariadb-server mariadb
   После установки добавляем сервер MariaDB в автозапуск:
   # systemctl start mariadb.service
   # systemctl enable mariadb.service
   Установка Apache
   Для установки веб-сервера Apache нужно выполнить команду:
   # yum -y install httpd
   После установки добавляем сервер Apache в автозапуск:
   # systemctl start httpd.service
   # systemctl enable httpd.servic

   В CentOS используется firewall Firewall-cmd. Добавим настройку которая разрешает подключения на порт 80 (http) и порт 443 (https)
   # firewall-cmd —permanent —zone=public —add-service=http
   # firewall-cmd —permanent —zone=public —add-service=https
   # firewall-cmd —reload
   После, откройте в браузере http://ip-address , и на экране будет отображаться стандартная страница веб-сервера Apache
   По умолчанию в веб-сервере Apache корневая директория для сайтов (document root) расположена в директории /var/www/html
   Конфигурационный файл (файл с настройками) веб-сервера Apache находится в файле /etc/httpd/conf/httpd.conf
   Дополнительные конфигурационные файлы находятся в директории: /etc/httpd/conf.d/
   Установка PHP
   Для установку PHP необходимо выполнить команду:
   # yum -y install php

   После установки нужно выполнить перезагрузку веб-сервера apache:
   # systemctl restart httpd.service
   Для проверки работы PHP в корневой директории (document root) веб-сервера apache /var/www/html можно создать файл pi.php который будет содержать функцию phpinfo() (функция phpinfo() отображает много полезной информации о настройках веб-сервера и PHP).
   Для это нужно выполнить команду:
   # echo «<?php phpinfo(); ?>» > /var/www/html/pi.php
   После чего в браузере можно открыть страницу:
   http://ip-address/pi.php
   На этой странице отображается вся необходимая информация о веб-сервере Apache и настройках PHP



Настройка поддержки MySQL в PHP

Для поддержки MariaDB в PHP нужно установить пакет php-mysql. Так же можно установить и некоторые другие пакеты для работы PHP с различными модулями, которые могут понадобится. Для этого выполним команду:

yum -y install php-mysql php-gd php-ldap php-odbc php-pear php-xml php-xmlrpc php-mbstring php-snmp php-soap curl curl-devel

После заверешения установки необходимы выполнить перезагрузка apache:

systemctl restart httpd.service

Теперь можно переоткрыть страницу http://ip-address/pi.php и увидеть новую информацию.

Установка phpMyAdmin

phpMyAdmin это программа предоставляющая веб-интерфейс через который можно управлять базами данных MySQL и MariaDB

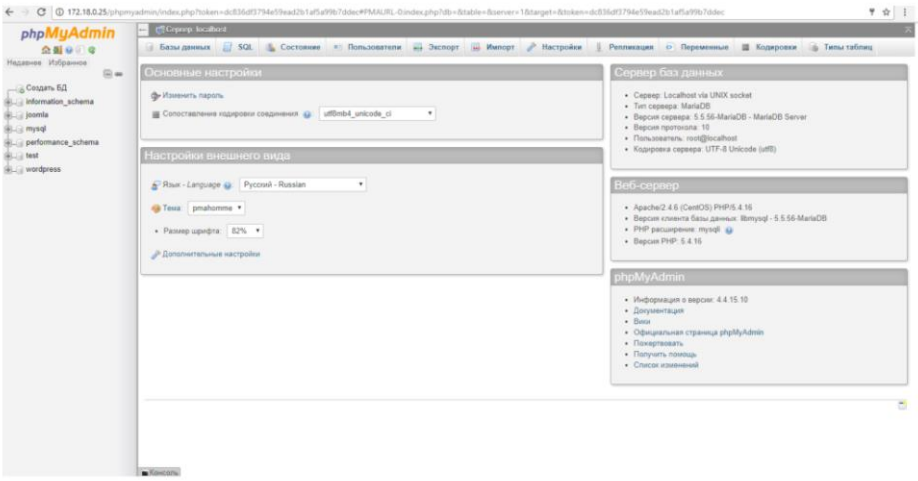
Для установки нужно выполнить инициализиацию репозитория EPEL так как в официальном репозитории CentOS 7 phpMyAdmin отсуствует.

yum -y install epel-release

После добавления репозитория есть возможность установить phpMyAdmin:

yum -y install phpmyadmin

После установки phpMyAdmin будет доступен по адресу: http://ip-address/phpmyadmin/



7. Практическое занятие № 37. Поиск уязвимостей информационных систем

Инструкция для обучающихся

Внимательно прочитайте задание. Выполните все действия.

Задание:

Задание:

Kali включает в себя очень способный OpenVAS, который является бесплатным и с открытым исходным кодом.

Это просто потому, что сканеры уязвимостей часто имеют слабую репутацию, прежде всего потому, что их роль и цель неправильно поняты.

Сканеры Vulnerabilty сканируют уязвимости – но они не являются волшебными машинами эксплойта и должны быть одним из многих источников информации, используемых в оценке безопасности.

Слепой запуск сканера уязвимостей на цель почти наверняка закончится разочарованием и горем, с десятками (или даже сотнями) результатов низкого уровня или неинформативных результатов.

1. Системные Требования

Основная жалоба, которую получают о OpenVAS (или любом другом сканере уязвимостей), можно резюмировать как «она слишком медленная и сбойная и не работает, и это плохо, и очень плохо».

Почти во всех случаях медленность и / или сбои связаны с недостаточными системными ресурсами.

OpenVAS имеет десятки тысяч сигнатур, и если вы не дадите вашей системе достаточного количества ресурсов, особенно оперативной памяти, вы окажетесь в мире страданий.

Для некоторых коммерческих сканеров уязвимостей требуется как минимум 8 ГБ ОЗУ и рекомендуется еще больше.

OpenVAS не требует около такого объема памяти, но чем больше вы можете предоставить ему, тем более плавно система сканирования будет работать.

Для этого урока наша виртуальная машина Kali имеет 3 процессора и 3 ГБ оперативной памяти, что обычно достаточно для сканирования небольшого количества хостов одновременно.

2. Начальная установка OpenVAS в Кали

У OpenVAS много движущихся частей, и настройка вручную может быть проблемой.

К счастью, Kali содержит простую в использовании утилиту под названием «openvas-setup», которая занимается настройкой OpenVAS, загрузкой сигнатур и созданием пароля для пользователя admin.

Эта первоначальная настройка может занять довольно много времени, даже при быстром подключении к Интернету, можно просто сидеть сложа руки.

В конце настройки будет отображаться автоматически созданный пароль для пользователя admin.

Обязательно сохраните этот пароль где-нибудь в безопасности.

```
root@kali:~# openvas-setup

ERROR: Directory for keys (/var/lib/openvas/private/CA) not found!

ERROR: Directory for certificates (/var/lib/openvas/CA) not found!

ERROR: CA key not found in /var/lib/openvas/private/CA/cakey.pem

ERROR: CA certificate not found in /var/lib/openvas/CA/cacert.pem

ERROR: CA certificate failed verification, see /tmp/tmp.7G2IQWtqwj/openvas-manage-certs.log for details. Aborting.ERROR: Your OpenVAS certificate infrastructure did NOT pass validation.

See messages above for details.

Generated private key in /tmp/tmp.PerU5lG2tl/cakey.pem.

Generated self signed certificate in /tmp/tmp.PerU5lG2tl/cacert.pem.

...

/usr/sbin/openvasmd

User created with password 'xxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxx'.
```

3. Работа с ошибками установки

Иногда скрипт «openvas-setup» будет отображать ошибки в конце загрузки NVT, аналогичные приведенным ниже.

```
(openvassd:2272): lib kb_redis-CRITICAL **: get_redis_ctx: redis connection error: No such file or directory

(openvassd:2272): lib kb_redis-CRITICAL **: redis_new: cannot access redis at '/var/run/redis/redis.sock'
```

```
(openvassd:2272): lib kb_redis-CRITICAL **: get_redis_ctx: redis connection error: No such file or directory

openvassd: no process found
```

Если вам посчастливилось столкнуться с этой проблемой, вы можете запустить «openvas-check-setup», чтобы узнать, какой компонент вызывает проблемы.

В этом конкретном случае мы получаем следующее из скрипта:

```
...

ERROR: The number of NVTs in the OpenVAS Manager database is too low.

FIX: Make sure OpenVAS Scanner is running with an up-to-date NVT collection and run 'openvasmd --rebuild'.

...
```

Скрипт «openvas-check-setup» обнаруживает проблему и даже предоставляет команду для запуска (надеюсь) решения этой проблемы.

После восстановления коллекции NVT рекомендуется пройти все проверки.

```
root@kali:~# openvasmd --rebuild

root@kali:~# openvas-check-setup

openvas-check-setup 2.3.7

Test completeness and readiness of OpenVAS-9

...

It seems like your OpenVAS-9 installation is OK.

...
```

4. Управление пользователями OpenVAS

Если вам нужно (или хотите) создать дополнительных пользователей OpenVAS, запустите ‘openvasmd’ с параметром -create-user, который добавит нового пользователя и отобразит случайно сгенерированный пароль.

```
root@kali:~# openvasmd --create-user=dookie

User created with password 'yyyyyyyy-yyyy-yyyy-yyyy-yyyyyyyyyy'.

root@kali:~# openvasmd --get-users

admin

dookie
```

К счастью, изменение паролей пользователей OpenVAS легко осуществляется с помощью опции «openvasmd» и «new-password».

```
root@kali:~# openvasmd --user=dookie --new-password=s3cr3t

root@kali:~# openvasmd --user=admin --new-password=sup3rs3cr3t
```

5. Запуск и остановка OpenVAS

Сетевые службы по умолчанию отключены в Kali Linux, поэтому, если вы не настроили OpenVAS для запуска при загрузке, вы можете запустить необходимые службы, запустив «openvas-start».

```
root@kali:~# openvas-start

Starting OpenVas ServicesПосле того, как у вас есть список хостов, вы можете импортировать их в разделе《Цели》в меню《Конфигурация》.
```

Когда службы завершают инициализацию, вы должны найти TCP-порты 9390 и 9392, которые прослушивают ваш loopback-интерфейс.

```
root@kali:~# ss -ant

State Recv-Q Send-Q Local Address:Port Peer Address:Port

LISTEN 0 128 127.0.0.1:9390 *:*

LISTEN 0 128 127.0.0.1:9392 *:*
```

Из-за нагрузки на системные ресурсы вы, вероятно, захотите остановить OpenVAS, когда вы закончите использовать его, особенно если вы не используете специальную систему для сканирования уязвимостей.

OpenVAS можно остановить, запустив «openvas-stop».

```
root@kali:~# openvas-stop

Stopping OpenVas Services
```

6. Использование Greenbone Security Assistant

Greenbone Security Assistant – это веб-интерфейс OpenVAS, доступный на вашем локальном компьютере (после запуска OpenVAS) на **https://localhost: 9392.**

После принятия самозаверенного сертификата вам будет представлена страница входа в систему и после аутентификации вы увидите основную панель.

Рис. 1

7. Настройка учетных данных

Сканеры уязвимостей обеспечивают наиболее полные результаты, когда вы можете предоставить механизму сканирования учетные данные для использования на сканируемых системах.

OpenVAS будет использовать эти учетные данные для входа в сканированную систему и выполнения подробного перечисления установленного программного обеспечения, патчей и т. д.

Вы можете добавить учетные данные через запись «Credentials» в меню «Configuration».

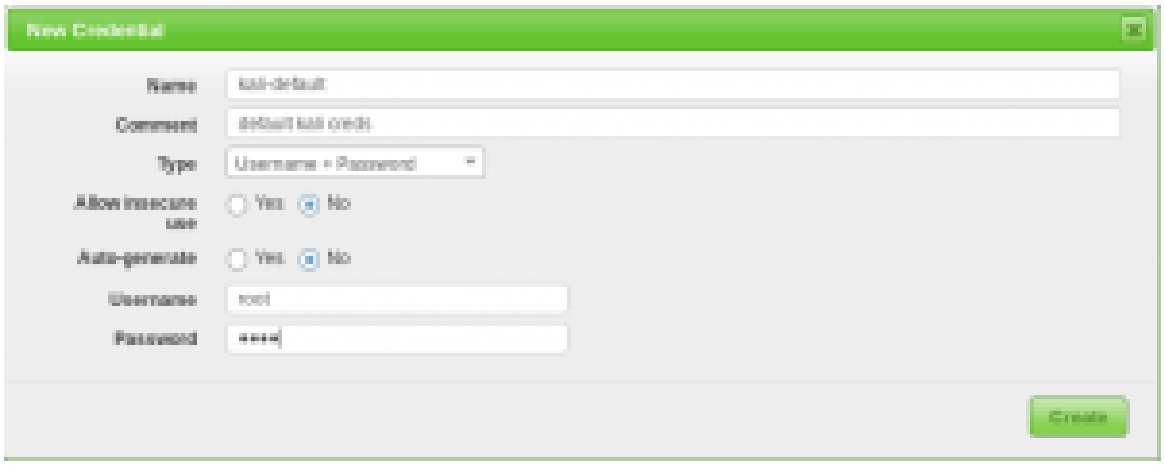


Рис. 2

8. Конфигурация цели

OpenVAS, как и большинство сканеров уязвимостей, может сканировать удаленные системы, но это сканер уязвимостей, а не сканер портов.

Вместо того, чтобы полагаться на сканер уязвимостей для идентификации хостов, вы значительно упростите свою жизнь с помощью специализированного сетевого сканера, такого как Nmap или Masscan, и импортируйте список целей в OpenVAS.

```
root@kali:~# nmap -sn -oA nmap-subnet-86 192.168.86.0/24

root@kali:~# grep Up nmap-subnet-86.gnmap | cut -d " " -f 2 > live-hosts.txt
```

После того, как у вас есть список хостов, вы можете импортировать их в разделе «target» в меню «Configuration».

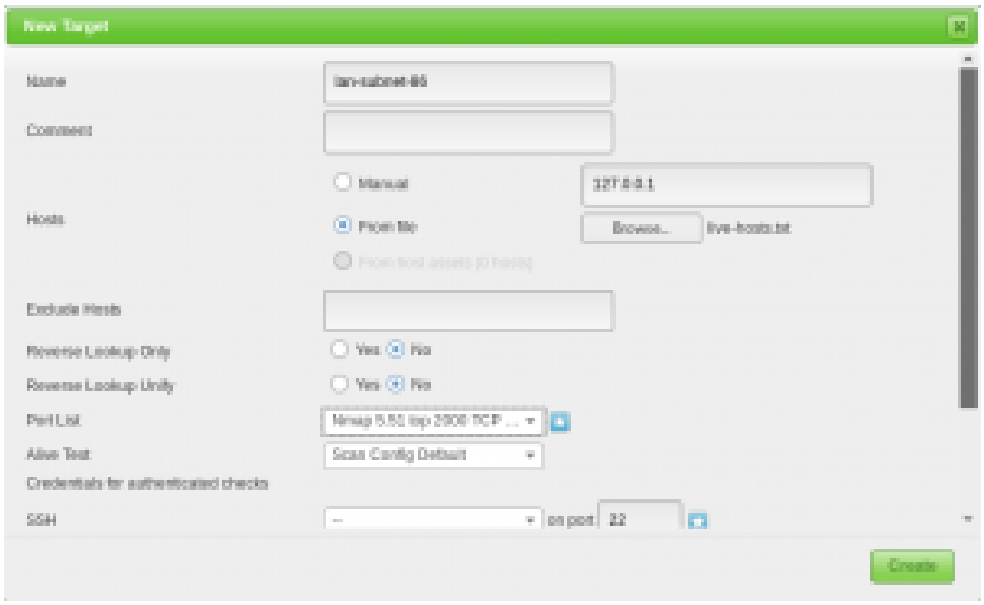


Рис. 3

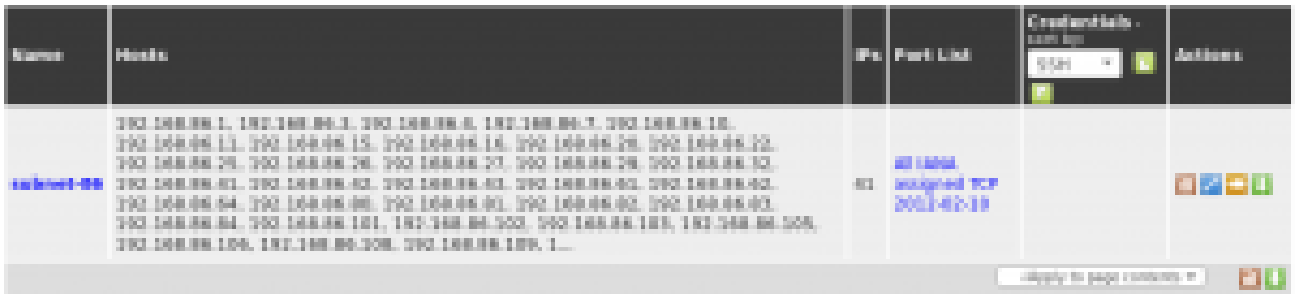


Рис. 4

9. Конфигурация сканирования

Перед запуском сканирования уязвимостей вы должны точно настроить Scan Config/,

Это можно сделать в разделе “Scan Configs” в меню “Config”.

Вы можете клонировать любую конфигурацию сканирования по умолчанию и редактировать ее параметры, отключая любые службы или проверки, которые вам не нужны.

Если вы используете Nmap для проведения предварительного анализа ваших целевых объектов, вы можете сэкономить время сканирования уязвимости.

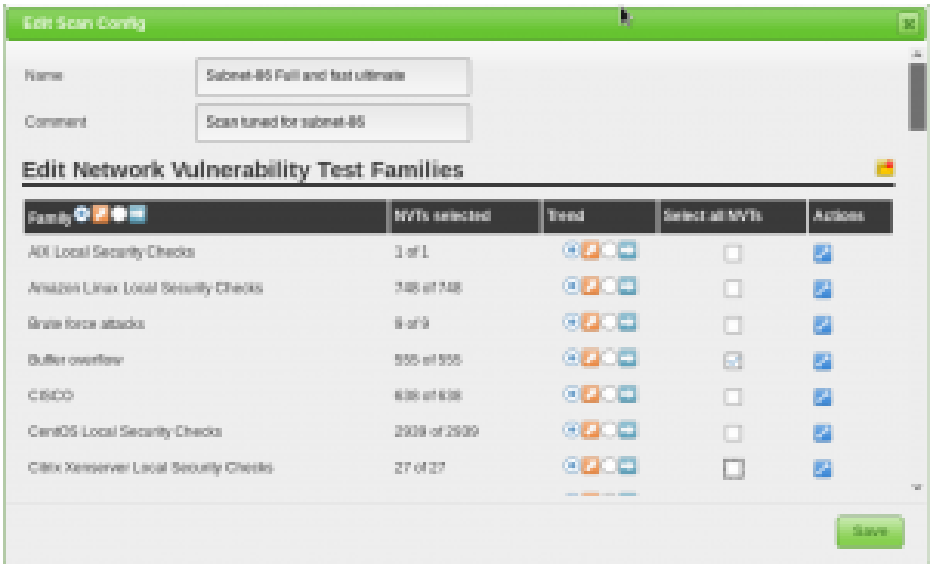


Рис. 5

10. Конфигурация задачи

Ваши учетные данные, цели и конфигурации сканирования настроены таким образом, что теперь вы готовы собрать все вместе и запустить сканирование уязвимостей.

В OpenVAS сканирование уязвимостей проводится как «tasks».

Когда вы настраиваете новую задачу, вы можете дополнительно оптимизировать сканирование путем увеличения или уменьшения одновременных действий, которые происходят.

С нашей системой с 2 ГБ оперативной памяти мы скорректировали наши настройки задач, как показано ниже.

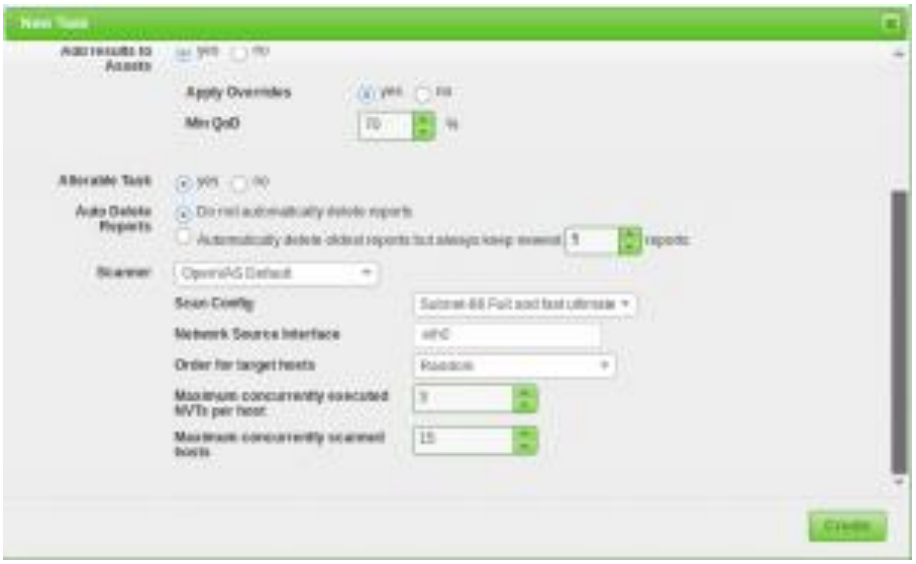


Рис. 6

Благодаря нашим более точно настроенным параметрам сканирования и целевому выбору результаты нашего сканирования намного полезнее.

Рис. 7

11. Автоматизация OpenVAS

Одной из менее известных функций OpenVAS является интерфейс командной строки, с которым вы взаимодействуете с помощью команды «omp».

Его использование не совсем интуитивно, но мы не единственные поклонники OpenVAS, и мы столкнулись с несколькими базовыми скриптами, которые вы можете использовать и расширить сканирование для автоматизации OpenVAS.

Первый – openvas-automate.sh от mgeeky, полуинтерактивный скрипт Bash, который предлагает вам тип сканирования и заботится обо всем остальном.

Конфигурации сканирования жестко закодированы в сценарии, поэтому, если вы хотите использовать свои настроенные конфиги, их можно добавить в разделе «targets».

```
root@kali:~# apt -y install pcregrep

root@kali:~# ./openvas-automate.sh 192.168.86.61:: OpenVAS automation script.

mgeeky, 0.1[>] Please select scan type:

1. Discovery

2. Full and fast

3. Full and fast ultimate

4. Full and very deep

5. Full and very deep ultimate

6. Host Discovery

7. System Discovery

9. Exit
```

```
------------------------------

Please select an option: 5


[+] Tasked: 'Full and very deep ultimate' scan against '192.168.86.61'

[>] Reusing target...

[+] Target's id: 6ccbb036-4afa-46d8-b0c0-acbd262532e5

[>] Creating a task...

[+] Task created successfully, id: '8e77181c-07ac-4d2c-ad30-9ae7a281d0f8'

[>] Starting the task...

[+] Task started. Report id: 6bf0ec08-9c60-4eb5-a0ad-33577a646c9b

[.] Awaiting for it to finish. This will take a long while...

8e77181c-07ac-4d2c-ad30-9ae7a281d0f8 Running 1% 192.168.86.61
```

Мы также наткнулись на сообщение в блоге по code16, которое представляет и объясняет их скрипт Python для взаимодействия с OpenVAS.

Подобно скрипту Bash выше, вам нужно будет внести некоторые изменения в скрипт, если вы хотите настроить тип сканирования.

```
root@kali:~# ./code16.py 192.168.86.27

-------------------------------------------------------------------------------

code16

-------------------------------------------------------------------------------

small wrapper for OpenVAS 6[+] Found target ID: 19f3bf20-441c-49b9-823d-11ef3b3d18c2

[+] Preparing options for the scan...

[+] Task ID = 28c527f8-b01c-4217-b878-0b536c6e6416

[+] Running scan for 192.168.86.27

[+]     Scan     started...     To     get     current     status,     see     be-
low:zZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzz

...

zZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzz

[+] Scan looks to be done. Good.
```

```
[+] Target scanned. Finished taskID : 28c527f8-b01c-4217-b878-0b536c6e6416

[+] Cool! We can generate some reports now ... :)

[+] Looking for report ID...

[+] Found report ID : 5ddcb4ed-4f96-4cee-b7f3-b7dad6e16cc6

[+] For taskID : 28c527f8-b01c-4217-b878-0b536c6e6416

[+] Preparing report in PDF for 192.168.86.27

[+] Report should be done in : Report_for_192.168.86.27.pdf

[+] Thanks. Cheers!
```

Эталон ответа:

Задание:

Kali включает в себя очень способный OpenVAS, который является бесплатным и с открытым исходным кодом.

Это просто потому, что сканеры уязвимостей часто имеют слабую репутацию, прежде всего потому, что их роль и цель неправильно поняты.

Сканеры Vulnerabilty сканируют уязвимости – но они не являются волшебными машинами эксплойта и должны быть одним из многих источников информации, используемых в оценке безопасности.

Слепой запуск сканера уязвимостей на цель почти наверняка закончится разочарованием и горем, с десятками (или даже сотнями) результатов низкого уровня или неинформативных результатов.

1. Системные Требования

Основная жалоба, которую получают о OpenVAS (или любом другом сканере уязвимостей), можно резюмировать как «она слишком медленная и сбойная и не работает, и это плохо, и очень плохо».

Почти во всех случаях медленность и / или сбои связаны с недостаточными системными ресурсами.

OpenVAS имеет десятки тысяч сигнатур, и если вы не дадите вашей системе достаточного количества ресурсов, особенно оперативной памяти, вы окажетесь в мире страданий.

Для некоторых коммерческих сканеров уязвимостей требуется как минимум 8 ГБ ОЗУ и рекомендуется еще больше.

OpenVAS не требует около такого объема памяти, но чем больше вы можете предоставить ему, тем более плавно система сканирования будет работать.

Для этого урока наша виртуальная машина Kali имеет 3 процессора и 3 ГБ оперативной памяти, что обычно достаточно для сканирования небольшого количества хостов одновременно.

2. Начальная установка OpenVAS в Кали

У OpenVAS много движущихся частей, и настройка вручную может быть проблемой.

К счастью, Kali содержит простую в использовании утилиту под названием «openvas-setup», которая занимается настройкой OpenVAS, загрузкой сигнатур и созданием пароля для пользователя admin.

Эта первоначальная настройка может занять довольно много времени, даже при быстром подключении к Интернету, можно просто сидеть сложа руки.

В конце настройки будет отображаться автоматически созданный пароль для пользователя admin.

Обязательно сохраните этот пароль где-нибудь в безопасности.

```
root@kali:~# openvas-setup

ERROR: Directory for keys (/var/lib/openvas/private/CA) not found!

ERROR: Directory for certificates (/var/lib/openvas/CA) not found!

ERROR: CA key not found in /var/lib/openvas/private/CA/cakey.pem

ERROR: CA certificate not found in /var/lib/openvas/CA/cacert.pem

ERROR: CA certificate failed verification, see /tmp/tmp.7G2IQWtqwj/openvas-manage-certs.log for details. Aborting.ERROR: Your OpenVAS certificate infrastructure did NOT pass validation.

See messages above for details.

Generated private key in /tmp/tmp.PerU5lG2tl/cakey.pem.

Generated self signed certificate in /tmp/tmp.PerU5lG2tl/cacert.pem.

...

/usr/sbin/openvasmd

User created with password 'xxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxx'.
```

3. Работа с ошибками установки

Иногда скрипт «openvas-setup» будет отображать ошибки в конце загрузки NVT, аналогичные приведенным ниже.

```
(openvassd:2272): lib kb_redis-CRITICAL **: get_redis_ctx: redis connection error: No such file or directory

(openvassd:2272): lib kb_redis-CRITICAL **: redis_new: cannot access redis at '/var/run/redis/redis.sock'

(openvassd:2272): lib kb_redis-CRITICAL **: get_redis_ctx: redis connection error: No such file or directory
```

```
openvassd: no process found
```

Если вам посчастливилось столкнуться с этой проблемой, вы можете запустить «openvas-check-setup», чтобы узнать, какой компонент вызывает проблемы.

В этом конкретном случае мы получаем следующее из скрипта:

```
...

ERROR: The number of NVTs in the OpenVAS Manager database is too low.

FIX: Make sure OpenVAS Scanner is running with an up-to-date NVT collection and run 'openvasmd --rebuild'.

...
```

Скрипт «openvas-check-setup» обнаруживает проблему и даже предоставляет команду для запуска (надеюсь) решения этой проблемы.

После восстановления коллекции NVT рекомендуется пройти все проверки.

```
root@kali:~# openvasmd --rebuild

root@kali:~# openvas-check-setup

openvas-check-setup 2.3.7

Test completeness and readiness of OpenVAS-9

...

It seems like your OpenVAS-9 installation is OK.

...
```

4. Управление пользователями OpenVAS

Если вам нужно (или хотите) создать дополнительных пользователей OpenVAS, запустите ‘openvasmd’ с параметром -create-user, который добавит нового пользователя и отобразит случайно сгенерированный пароль.

```
root@kali:~# openvasmd --create-user=dookie

User created with password 'yyyyyyyy-yyyy-yyyy-yyyy-yyyyyyyyyy'.

root@kali:~# openvasmd --get-users

admin

dookie
```

К счастью, изменение паролей пользователей OpenVAS легко осуществляется с помощью опции «openvasmd» и «new-password».

```
root@kali:~# openvasmd --user=dookie --new-password=s3cr3t
```

```
root@kali:~# openvasmd --user=admin --new-password=sup3rs3cr3t
```

5. Запуск и остановка OpenVAS

Сетевые службы по умолчанию отключены в Kali Linux, поэтому, если вы не настроили OpenVAS для запуска при загрузке, вы можете запустить необходимые службы, запустив «openvas-start».

```
root@kali:~# openvas-start

Starting OpenVas ServicesПосле того, как у вас есть список хостов, вы можете импортировать их в разделе «Цели» в меню «Конфигурация».
```

Когда службы завершают инициализацию, вы должны найти TCP-порты 9390 и 9392, которые прослушивают ваш loopback-интерфейс.

```
root@kali:~# ss -ant

State Recv-Q Send-Q Local Address:Port Peer Address:Port

LISTEN 0 128 127.0.0.1:9390 *:*

LISTEN 0 128 127.0.0.1:9392 *:*
```

Из-за нагрузки на системные ресурсы вы, вероятно, захотите остановить OpenVAS, когда вы закончите использовать его, особенно если вы не используете специальную систему для сканирования уязвимостей.

OpenVAS можно остановить, запустив «openvas-stop».

```
root@kali:~# openvas-stop

Stopping OpenVas Services
```

6. Использование Greenbone Security Assistant

Greenbone Security Assistant – это веб-интерфейс OpenVAS, доступный на вашем локальном компьютере (после запуска OpenVAS) на **https://localhost: 9392.**

После принятия самозаверенного сертификата вам будет представлена страница входа в систему и после аутентификации вы увидите основную панель.

Рис. 8

7. Настройка учетных данных

Сканеры уязвимостей обеспечивают наиболее полные результаты, когда вы можете предоставить механизму сканирования учетные данные для использования на сканируемых системах.

OpenVAS будет использовать эти учетные данные для входа в сканированную систему и выполнения подробного перечисления установленного программного обеспечения, патчей и т. д.

Вы можете добавить учетные данные через запись «Credentials» в меню «Configuration».

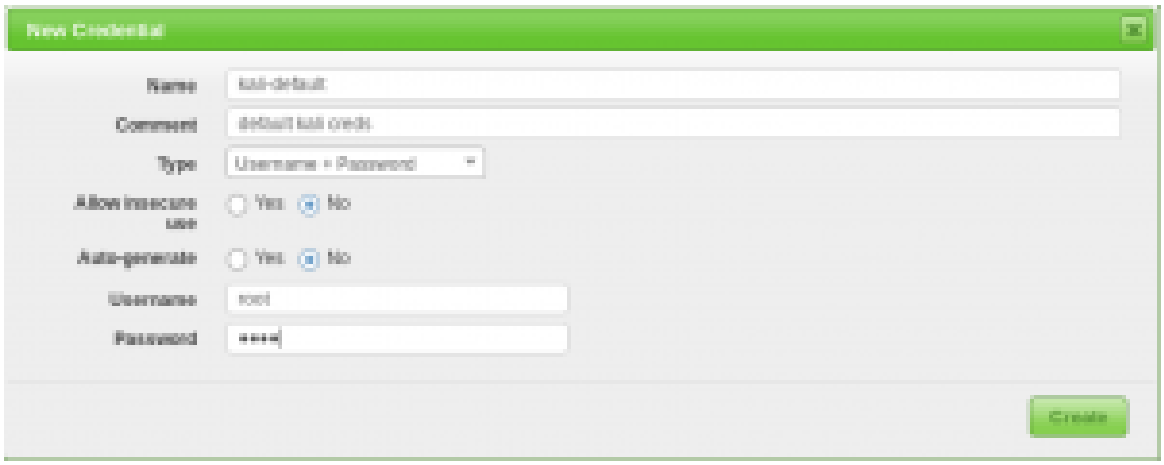


Рис. 9

8. Конфигурация цели

OpenVAS, как и большинство сканеров уязвимостей, может сканировать удаленные системы, но это сканер уязвимостей, а не сканер портов.

Вместо того, чтобы полагаться на сканер уязвимостей для идентификации хостов, вы значительно упростите свою жизнь с помощью специализированного сетевого сканера, такого как Nmap или Masscan, и импортируйте список целей в OpenVAS.

```
root@kali:~# nmap -sn -oA nmap-subnet-86 192.168.86.0/24

root@kali:~# grep Up nmap-subnet-86.gnmap | cut -d " " -f 2 > live-hosts.txt
```

После того, как у вас есть список хостов, вы можете импортировать их в разделе «target» в меню «Configuration».

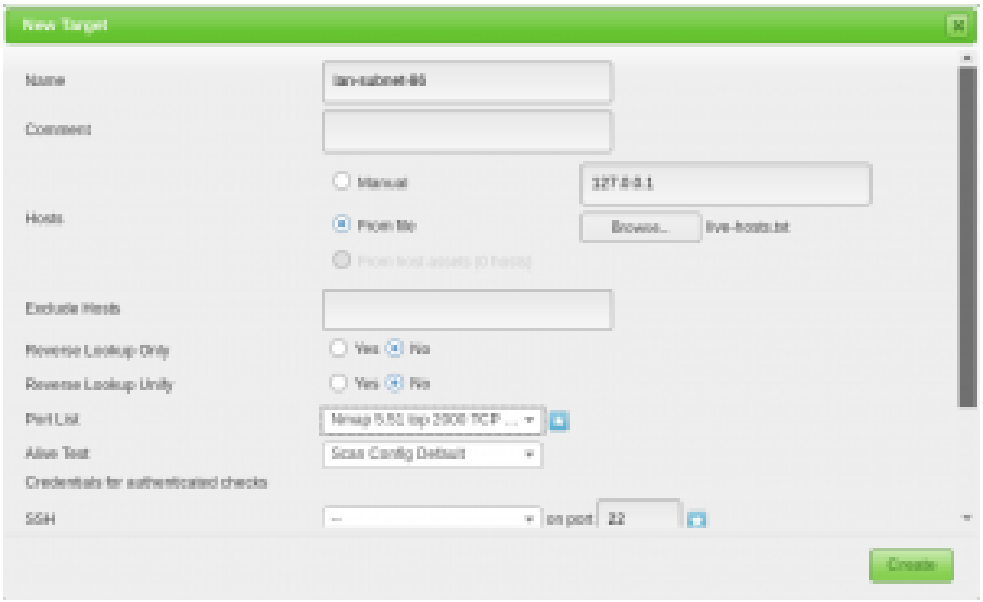


Рис. 10

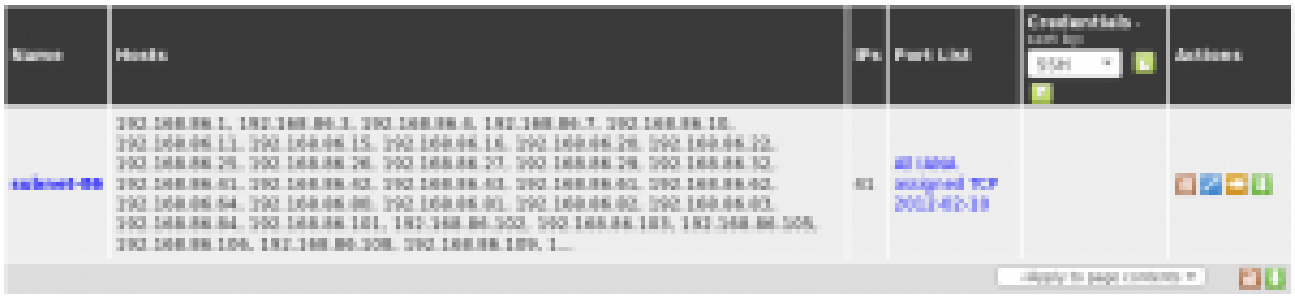


Рис. 11

9. Конфигурация сканирования

Перед запуском сканирования уязвимостей вы должны точно настроить Scan Config/,

Это можно сделать в разделе “Scan Configs” в меню “Config”.

Вы можете клонировать любую конфигурацию сканирования по умолчанию и редактировать ее параметры, отключая любые службы или проверки, которые вам не нужны.

Если вы используете Nmap для проведения предварительного анализа ваших целевых объектов, вы можете сэкономить время сканирования уязвимости.

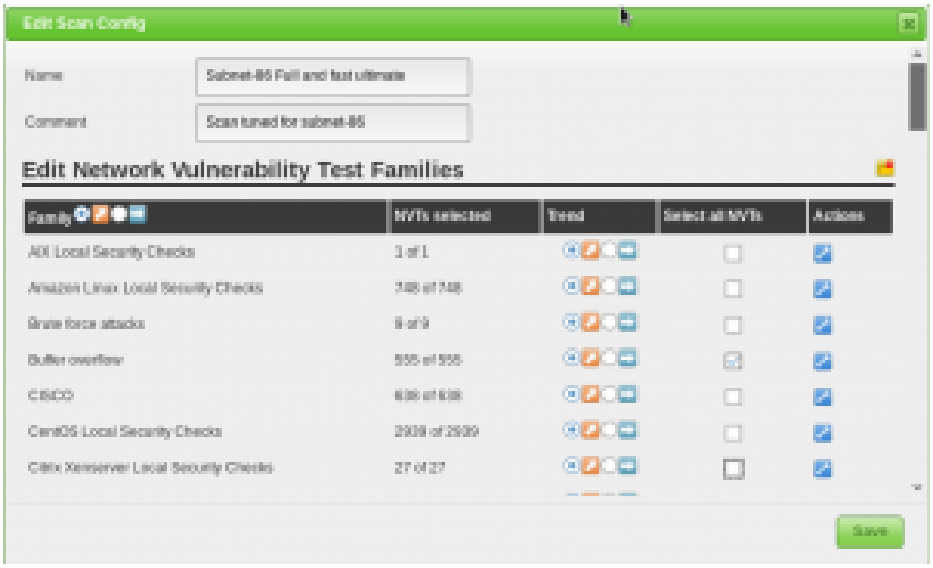


Рис. 12

10. Конфигурация задачи

Ваши учетные данные, цели и конфигурации сканирования настроены таким образом, что теперь вы готовы собрать все вместе и запустить сканирование уязвимостей.

В OpenVAS сканирование уязвимостей проводится как «tasks».

Когда вы настраиваете новую задачу, вы можете дополнительно оптимизировать сканирование путем увеличения или уменьшения одновременных действий, которые происходят.

С нашей системой с 2 ГБ оперативной памяти мы скорректировали наши настройки задач, как показано ниже.

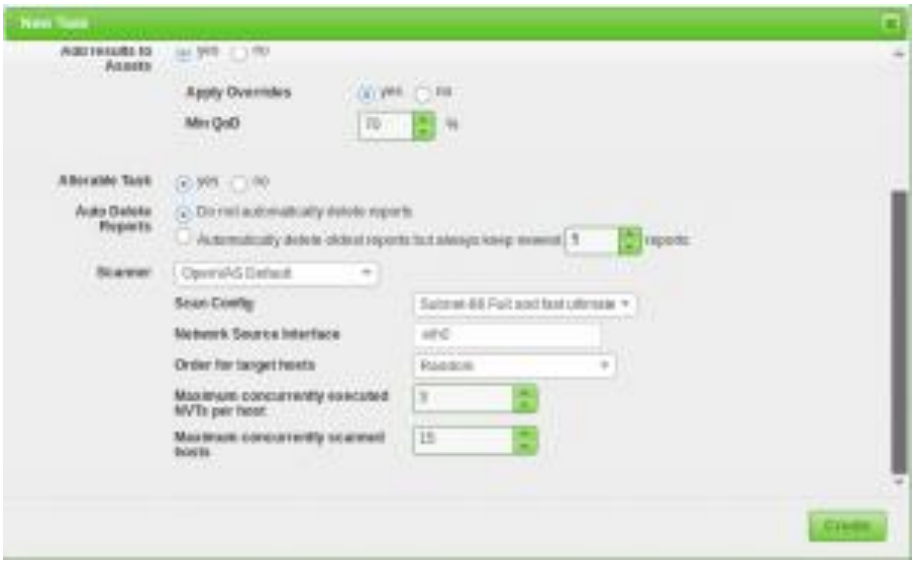


Рис. 13

Благодаря нашим более точно настроенным параметрам сканирования и целевому выбору результаты нашего сканирования намного полезнее.

Рис. 14

11. Автоматизация OpenVAS

Одной из менее известных функций OpenVAS является интерфейс командной строки, с которым вы взаимодействуете с помощью команды «omp».

Его использование не совсем интуитивно, но мы не единственные поклонники OpenVAS, и мы столкнулись с несколькими базовыми скриптами, которые вы можете использовать и расширить сканирование для автоматизации OpenVAS.

Первый – openvas-automate.sh от mgeeky, полуинтерактивный скрипт Bash, который предлагает вам тип сканирования и заботится обо всем остальном.

Конфигурации сканирования жестко закодированы в сценарии, поэтому, если вы хотите использовать свои настроенные конфиги, их можно добавить в разделе «targets».

```
root@kali:~# apt -y install pcregrep

root@kali:~# ./openvas-automate.sh 192.168.86.61:: OpenVAS automation script.

mgeeky, 0.1[>] Please select scan type:

1. Discovery

2. Full and fast

3. Full and fast ultimate

4. Full and very deep

5. Full and very deep ultimate

6. Host Discovery

7. System Discovery

9. Exit
```

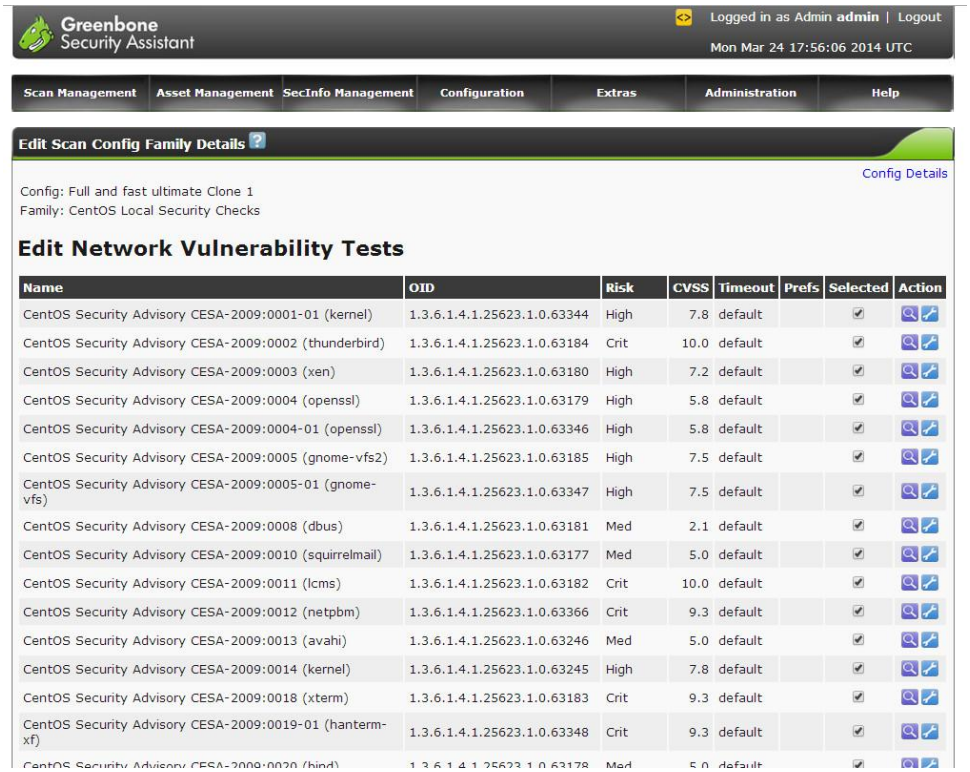
```
------------------------------

Please select an option: 5


[+] Tasked: 'Full and very deep ultimate' scan against '192.168.86.61'

[>] Reusing target...

[+] Target's id: 6ccbb036-4afa-46d8-b0c0-acbd262532e5

[>] Creating a task...

[+] Task created successfully, id: '8e77181c-07ac-4d2c-ad30-9ae7a281d0f8'

[>] Starting the task...

[+] Task started. Report id: 6bf0ec08-9c60-4eb5-a0ad-33577a646c9b

[.] Awaiting for it to finish. This will take a long while...

8e77181c-07ac-4d2c-ad30-9ae7a281d0f8 Running 1% 192.168.86.61
```

Мы также наткнулись на сообщение в блоге по code16, которое представляет и объясняет их скрипт Python для взаимодействия с OpenVAS.

Подобно скрипту Bash выше, вам нужно будет внести некоторые изменения в скрипт, если вы хотите настроить тип сканирования.

```
root@kali:~# ./code16.py 192.168.86.27

-------------------------------------------------------------------------------

code16

-------------------------------------------------------------------------------

small wrapper for OpenVAS 6[+] Found target ID: 19f3bf20-441c-49b9-823d-11ef3b3d18c2

[+] Preparing options for the scan...

[+] Task ID = 28c527f8-b01c-4217-b878-0b536c6e6416

[+] Running scan for 192.168.86.27

[+]     Scan     started...     To     get     current     status,     see     be-
low:zZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzz

...

zZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzz

[+] Scan looks to be done. Good.
```

```
[+] Target scanned. Finished taskID : 28c527f8-b01c-4217-b878-0b536c6e6416

[+] Cool! We can generate some reports now ... :)

[+] Looking for report ID...

[+] Found report ID : 5ddcb4ed-4f96-4cee-b7f3-b7dad6e16cc6

[+] For taskID : 28c527f8-b01c-4217-b878-0b536c6e6416

[+] Preparing report in PDF for 192.168.86.27

[+] Report should be done in : Report_for_192.168.86.27.pdf

[+] Thanks. Cheers!
```



Greenbone Security Assistant

Logged in as Admin **admin** | Logout

Mon Mar 24 17:56:06 2014 UTC

Scan Management | Asset Management | SecInfo Management | Configuration | Extras | Administration | Help

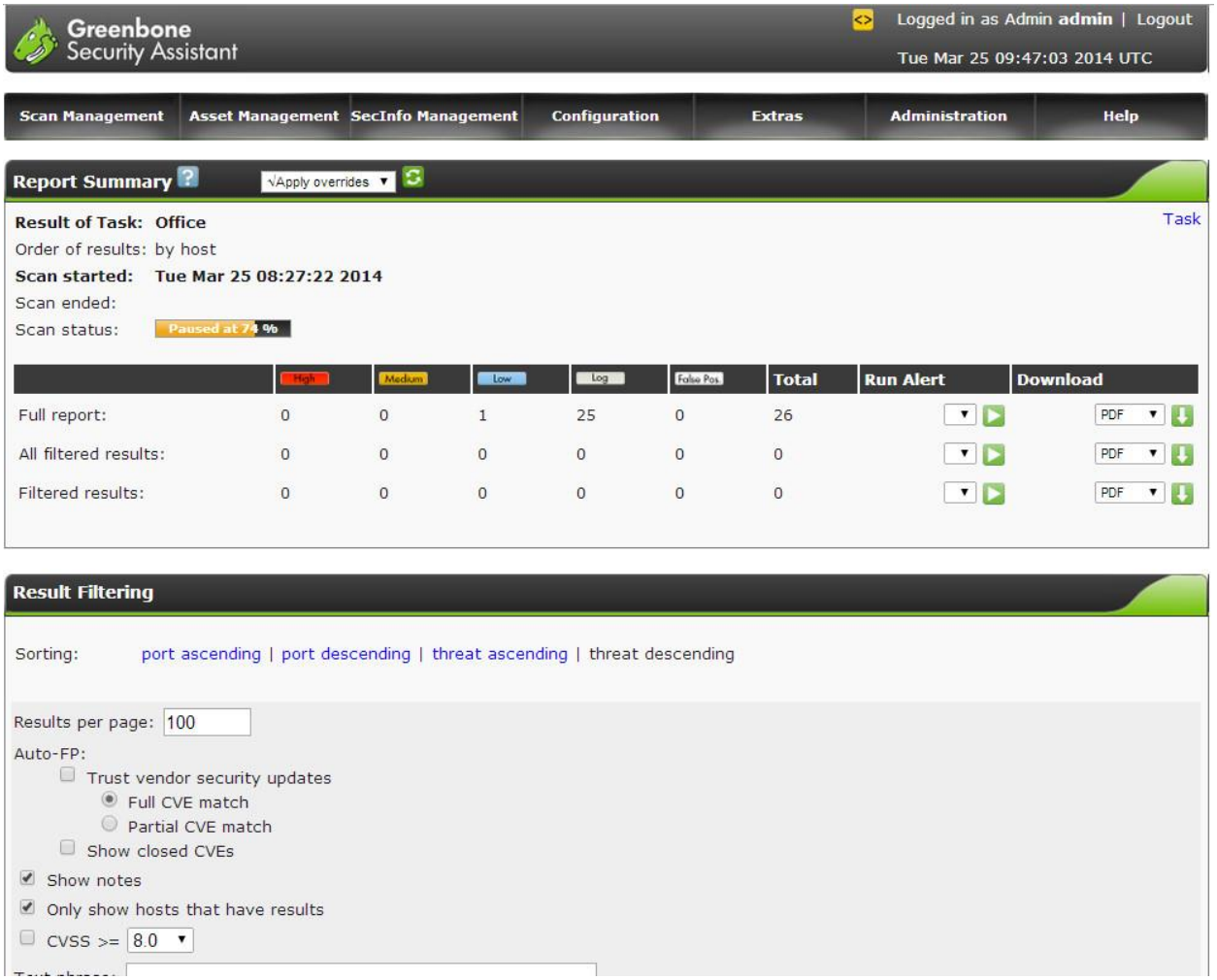
Edit Scan Config Family Details

Config Details

Config: Full and fast ultimate Clone 1
Family: CentOS Local Security Checks

Edit Network Vulnerability Tests

Name	OID	Risk	CVSS	Timeout	Prefs	Selected	Action
CentOS Security Advisory CESA-2009:0001-01 (kernel)	1.3.6.1.4.1.25623.1.0.63344	High	7.8	default		☑	
CentOS Security Advisory CESA-2009:0002 (thunderbird)	1.3.6.1.4.1.25623.1.0.63184	Crit	10.0	default		☑	
CentOS Security Advisory CESA-2009:0003 (xen)	1.3.6.1.4.1.25623.1.0.63180	High	7.2	default		☑	
CentOS Security Advisory CESA-2009:0004 (openssl)	1.3.6.1.4.1.25623.1.0.63179	High	5.8	default		☑	
CentOS Security Advisory CESA-2009:0004-01 (openssl)	1.3.6.1.4.1.25623.1.0.63346	High	5.8	default		☑	
CentOS Security Advisory CESA-2009:0005 (gnome-vfs2)	1.3.6.1.4.1.25623.1.0.63185	High	7.5	default		☑	
CentOS Security Advisory CESA-2009:0005-01 (gnome-vfs)	1.3.6.1.4.1.25623.1.0.63347	High	7.5	default		☑	
CentOS Security Advisory CESA-2009:0008 (dbus)	1.3.6.1.4.1.25623.1.0.63181	Med	2.1	default		☑	
CentOS Security Advisory CESA-2009:0010 (squirrelmail)	1.3.6.1.4.1.25623.1.0.63177	Med	5.0	default		☑	
CentOS Security Advisory CESA-2009:0011 (lcms)	1.3.6.1.4.1.25623.1.0.63182	Crit	10.0	default		☑	
CentOS Security Advisory CESA-2009:0012 (netpbm)	1.3.6.1.4.1.25623.1.0.63366	Crit	9.3	default		☑	
CentOS Security Advisory CESA-2009:0013 (avahi)	1.3.6.1.4.1.25623.1.0.63246	Med	5.0	default		☑	
CentOS Security Advisory CESA-2009:0014 (kernel)	1.3.6.1.4.1.25623.1.0.63245	High	7.8	default		☑	
CentOS Security Advisory CESA-2009:0018 (xterm)	1.3.6.1.4.1.25623.1.0.63183	Crit	9.3	default		☑	
CentOS Security Advisory CESA-2009:0019-01 (hanterm-xf)	1.3.6.1.4.1.25623.1.0.63348	Crit	9.3	default		☑	
CentOS Security Advisory CESA-2009:0020 (bind)	1.3.6.1.4.1.25623.1.0.63178	Med	5.0	default		☑	



8. Устный зачет по теме 3.4

Инструкция для обучающихся: Зачет проводится в учебное время. Каждый студент отвечает на 6 вопросов по выбору преподавателя. С перечнем вопросов студенты ознакомлены заранее (за неделю). Время ответа 3 минуты. Время проведения зачета для группы – одно учебное занятие.

Перечень вопросов:

1. Классификация угроз ИБ
2. Актуальные вирусы
3. Понятие кибербезопасности
4. Антивирусы
5. Защита веб-серверов
6. Защита приложений

9. Практическое занятие № 43. Поиск открытых портов

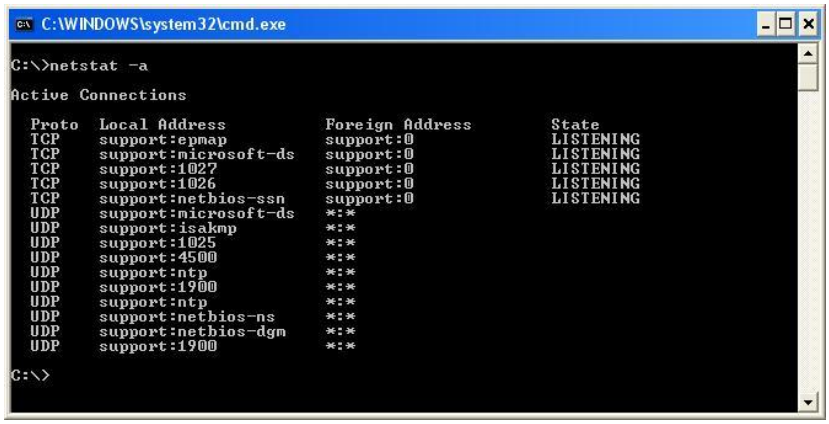
Инструкция для обучающихся

Внимательно прочитайте задание. Выполните все действия.

Задание: просканировать открытые порты и найти цифровые отпечатки.

Эталон ответа:

Были найдены следующие открытые порты:



Средства	Собранная информация
Amap	Открытый порт: 80
	Севрвера: - http-apach-2; - http-iis; - webmin.
	Порты: - 10.0.0.4:75/tcp. - 10.0.0.4:76/tcp. - 10.0.0.4:77/tcp. - 10.0.0.4:78/tcp. - 10.0.0.4:79/tcp. - 10.0.0.4:81/tcp.

10. **Устный зачет по теме 3.5**

Инструкция для обучающихся: Зачет проводится в учебное время. Каждый студент отвечает на 7 вопросов по выбору преподавателя. С перечнем вопросов студенты ознакомлены заранее (за неделю). Время ответа 3 минуты. Время проведения зачета для группы – одно учебное занятие.

Перечень вопросов:

1. Топ-5 уязвимостей сети
2. Топ-5 уязвимостей сайтов
3. SQL-инъекции
4. XSS-уязвимости
5. Уязвимости CSRF
6. Атака типа clickjacking
7. Методы сканирования сети

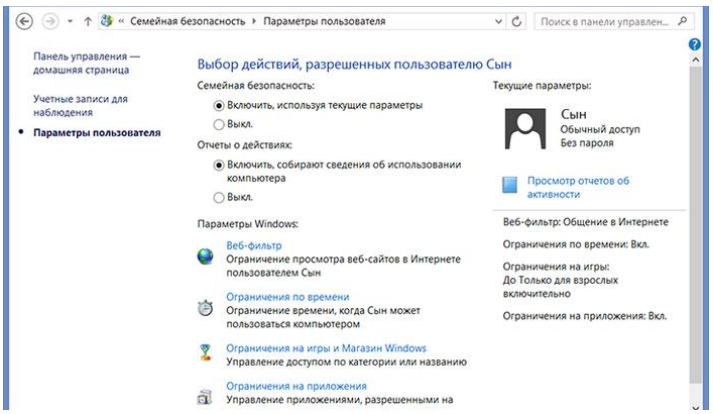
11. Практическое занятие № 52. Настройка параметров безопасности Windows.

Инструкция для обучающихся
Внимательно прочитайте задание. Выполните все действия.
Задание:: настроить параметры безопасности Windows 10:

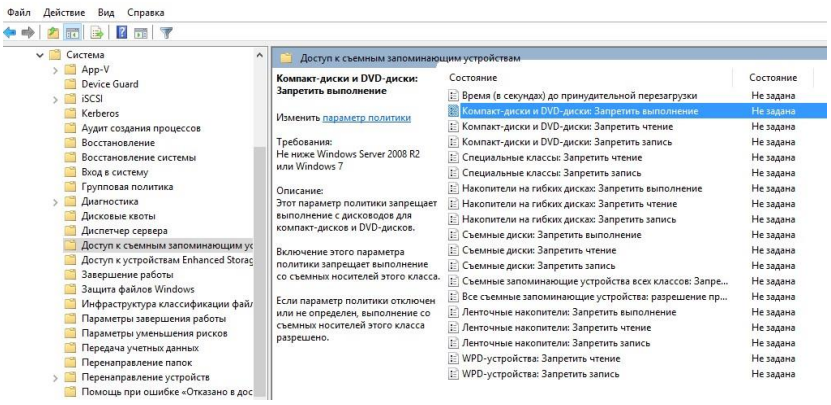
1. Установить ограничения пользователям;
2. Запретить использование USB-носителей;
3. Установить требования к паролям(длину, количество символов и знаков, срок действия);
4. Установить запреты автозапуска установленных приложений;
5. Установить запрет на установку приложений;
6. Запретить изменение реестра;
7. Отключить доступ к реестру;
8. Настроить выключение компьютеров в указанное время (после 19:00);
9. Установить блокировку компьютера при простое (более 30 минут);
10. Отключить принудительный перезапуск;
11. Отключить автоматическое обновление драйверов и ПО.

Эталон ответа:

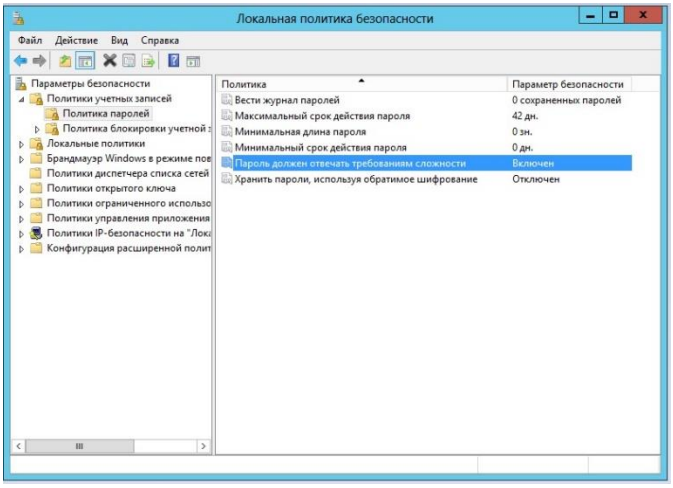
1. Установить ограничения пользователям;



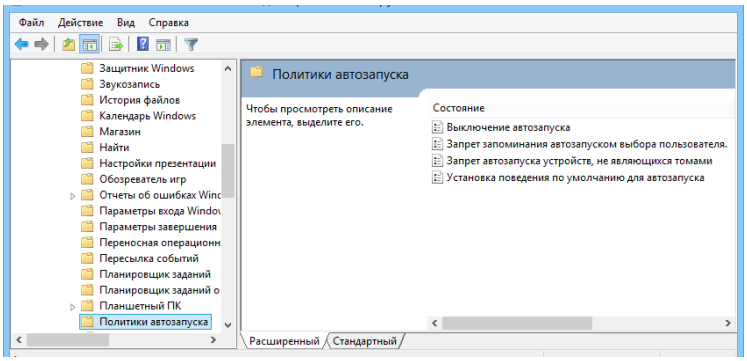
2. Запретить использование USB-носителей;



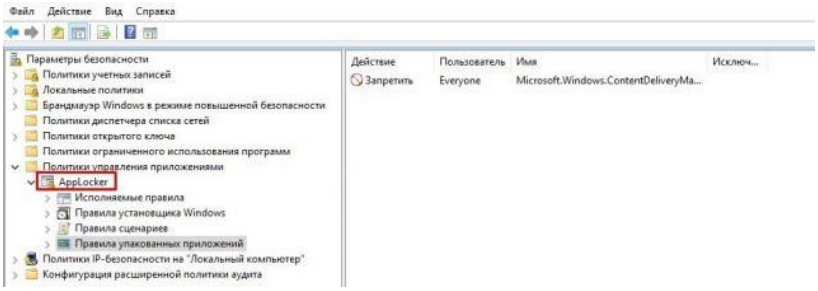
3. Установить требования к паролям(длину, количество символов и знаков, срок действия)



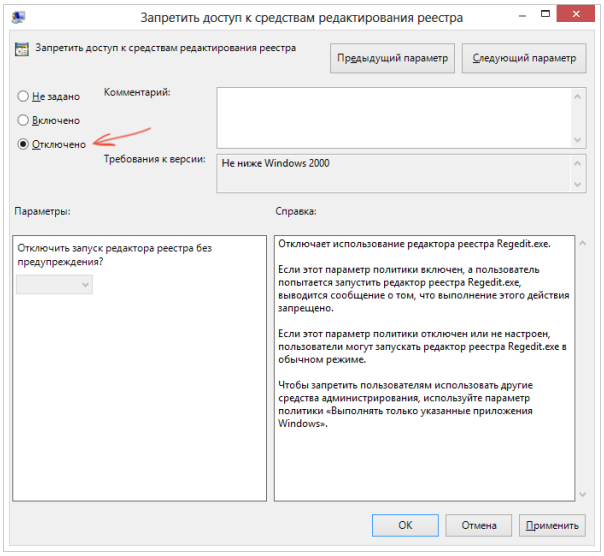
4. Установить запреты автозапуска установленных приложений;



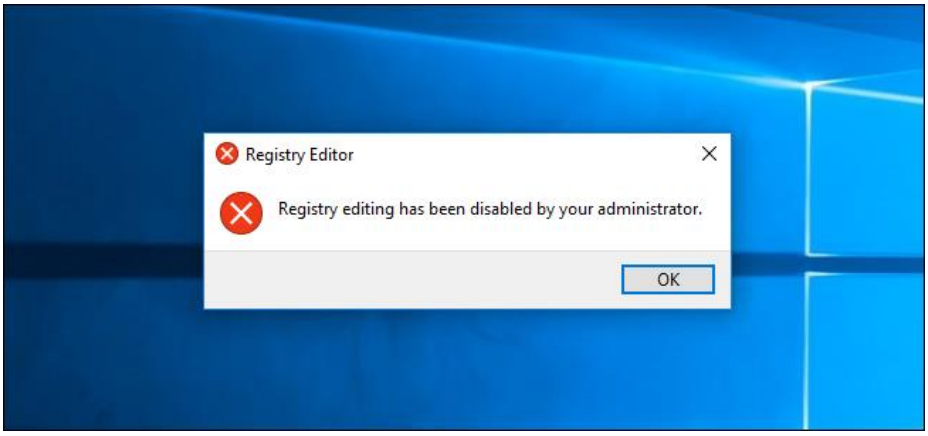
5. Установить запрет на установку приложений;



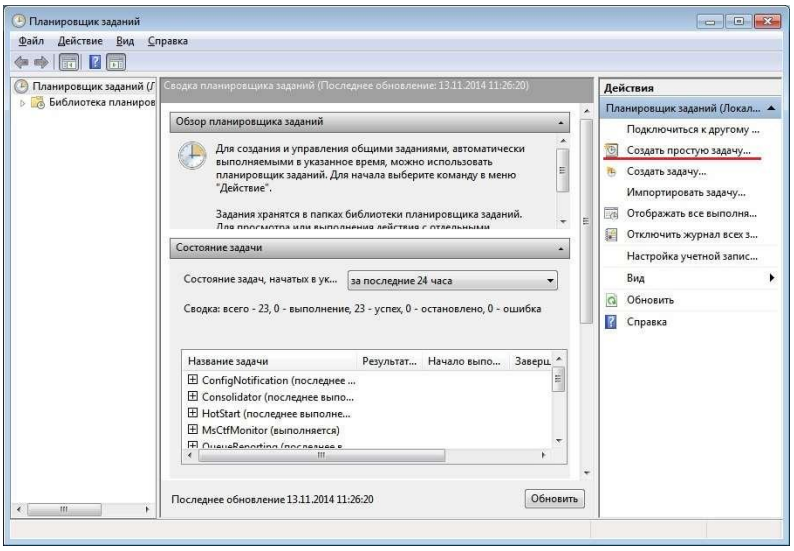
6. Запретить изменение реестра;



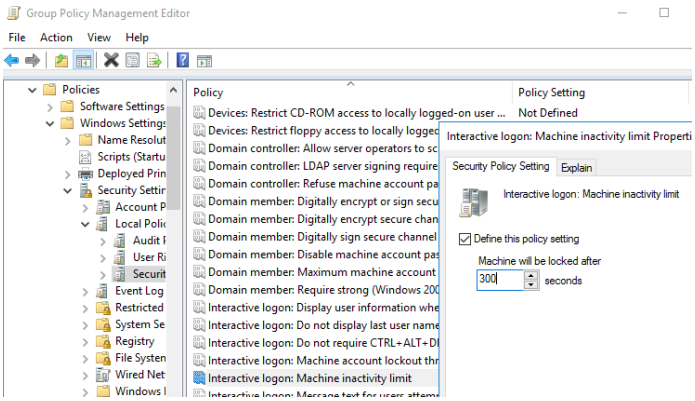
7. Отключить доступ к реестру;



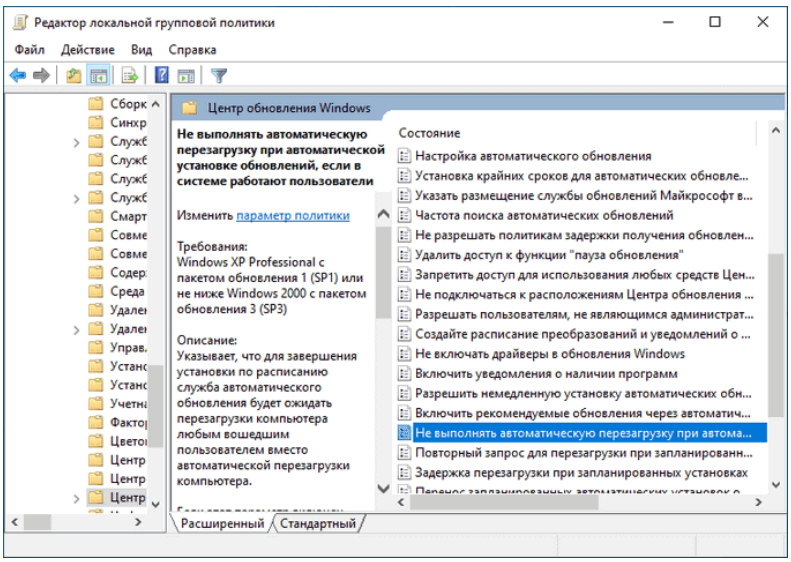
8. Настроить выключение компьютеров в указанное время (после 19:00);



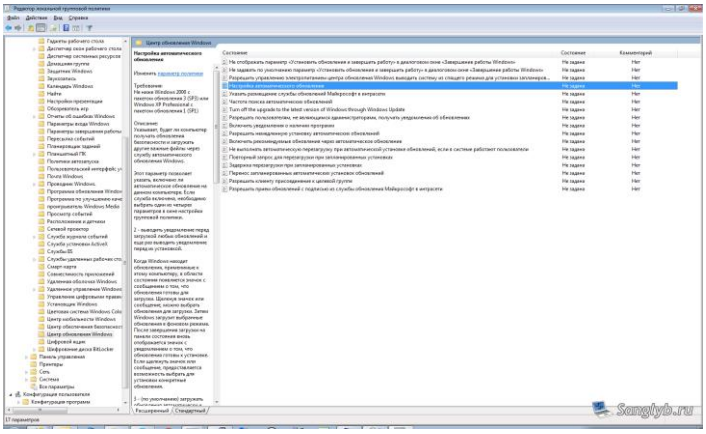
9. Установить блокировку компьютера при простое (более 30 минут);



10. Отключить принудительный перезапуск;



11. Отключить автоматическое обновление драйверов и ПО.



12. **Устный зачет по теме 3.6**

Инструкция для обучающихся: Зачет проводится в учебное время. Каждый студент отвечает на 5 вопросов по выбору преподавателя. С перечнем вопросов студенты ознакомлены заранее (за неделю). Время ответа 3 минуты. Время проведения зачета для группы – одно учебное занятие.

Перечень вопросов:

1. Межсетевые экраны
2. Правила безопасности Windows
3. Правила безопасности Linux
4. Защита ИС
5. Рекомендации по повышению уровня защищенности.

13. Устный зачет по теме 3.7

Инструкция для обучающихся: Зачет проводится в учебное время. Каждый студент отвечает на 6 вопросов по выбору преподавателя. С перечнем вопросов студенты ознакомлены заранее (за неделю). Время ответа 3 минуты. Время проведения зачета для группы – одно учебное занятие.

Перечень вопросов:

1. Компьютерные преступления
2. Виды компьютерных преступлений
3. Мотивация нарушителей
4. Идентификация инцидента
5. Оценка ущерба от инцидента
6. Устранение негативных последствий инцидентов

14. Устный зачет по теме 3.8

Инструкция для обучающихся: Зачет проводится в учебное время. Каждый студент отвечает на 4 вопроса по выбору преподавателя. С перечнем вопросов студенты ознакомлены заранее (за неделю). Время ответа 3 минуты. Время проведения зачета для группы – одно учебное занятие.

Перечень вопросов:

1. Социальная инженерия
2. Методы социальной инженерии
3. Исследование на основе открытых источников
4. Инструменты OSINT

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

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

Курсовая работа выполняется по единой теме по индивидуальным вариантам: «Организация защиты от внутренних угроз в организации с использованием DLP-системы» и носит практический характер.

Проверяемые результаты обучения:

Показатели оценки работы

Проверяемые освоенные умения и усвоенные знания	Общие и профессиональные компетенции, формируемые в процессе выполнения роботы	Этап выполнения курсовой работы
З1-З6 У1-У5	ОК1-11 ПК 2.1-ПК 2.6	Выдача тем курсовых работ. Знакомство с Методическими указаниями по выполнению и оформлению курсовых работ
З1-З6 У1-У5	ОК1-11 ПК 2.1-ПК 2.6	Знакомство с источниками информации, подбор информации в соответствии с планом курсовой работы
З1-З6 У1-У5	ОК1-11 ПК 2.1-ПК 2.6	Выполнение Введения к курсовой работе

Проверяемые освоенные умения и усвоенные знания	Общие и профессиональные компетенции, формируемые в процессе выполнения роботы	Этап выполнения курсовой работы
З1-З6 У1-У5	ОК1-11 ПК 2.1-ПК 2.6	Работа над теоретической частью курсовой работы
З1-З6 У1-У5	ОК1-11 ПК 2.1-ПК 2.6	Работа над практической частью курсовой работы
З1-З6 У1-У5	ОК1-11 ПК 2.1-ПК 2.6	Работа над составлением Заключения к работе
З1-З6 У1-У5	ОК1-11 ПК 2.1-ПК 2.6	Разработка презентации и доклада
З1-З6 У1-У5	ОК1-11 ПК 2.1-ПК 2.6	Подготовка к защите КР

3.3. Контрольно-оценочные материалы для промежуточной аттестации

Формой промежуточной аттестации по МДК.02.01 является экзамен.

Перечень экзаменационных вопросов:

1. Виды политик, способы их создания в Traffic monitor
2. Виды правил и способы создания правил в Device monitor
3. Виды программно-аппаратных средств защиты информации
4. Защита информации в VPN-сетях
5. Защита электронной почты
6. Использование Active Directory и политик безопасности. Понятие домена. Роли контроллера домена
7. Использование систем обнаружения вторжения
8. Критерии защищённости компьютерных систем
9. Методики проверки защищённости объектов информатизации на соответствие требованиям нормативных правовых актов
10. Методы сокрытия информации
11. Мониторинг событий информационной безопасности в DLP-системе Infowatch
12. Общая характеристика и принципы функционирования dlp-системы Infowatch
13. Общая характеристика продуктов ViPNet для создания защищённой сети
14. Подсистема безопасности Linux
15. Подсистема безопасности Windows
16. Понятие построения виртуальной защищённой сети, межсетевой взаимодействие защищённых сетей
17. Современные программные средства для защиты от вредоносных программ
18. Средства защиты в вычислительных сетях
19. Средства защиты информации Dallas Lock Возможности Dallas Lock. Принцип работы. Параметры установки
20. Средства защиты компьютерных сетей с использованием Samba и политик безопасности на Linux-сервере Особенности серверов на Linux. Программные средства для поднятия контроллера домена на Linux
21. Средства обеспечения защиты информации в системах управления базами данных
22. Средство защиты информации Secret Net Studio Возможности Secret Net Studio. Принцип работы
23. Структура и функции подсистемы безопасности операционных систем

Эталон ответов: приведен в Учебном пособии по МДК.02.01
Условия выполнения

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

Результаты промежуточной аттестации фиксируются в протоколе.

Формой промежуточной аттестации по МДК.02.02 является дифференциальный зачет.

Перечень вопросов для дифференциального зачета:

1. Шифры замены. Основы шифрования. Шифры однозначной замены. Полиграммные шифры.
2. Шифры перестановки. Шифры гаммирования
3. Шифрование с открытым ключом
4. Вероятностное шифрование
5. Протоколы обмена ключами. Алгоритм Диффи-Хеллмана-Меркла
6. Протоколы электронной цифровой подписи
7. Методы криптоанализа. Частотный анализ. Метод полного перебора
8. Методы криптоанализа блочных шифров
9. Компьютерная стеганография
10. Неформатные методы сокрытия в графических изображениях

Эталон ответов: приведен в Учебном пособии по МДК 02.02

Условия выполнения

1. Количество билетов для экзаменующегося: 1
2. Время подготовки к ответу: 20 минут
3. Требования к устным ответам:
   Полное овладение содержанием учебного материала, в котором обучающийся легко ориентируется, владение понятийным аппаратом.
4. Оборудование: учебная аудитория, стол, стул, пишущая ручка, бумага.

Результаты промежуточной аттестации фиксируются в протоколе.

Формой промежуточной аттестации по МДК.02.03 является дифференциальный зачет.

Перечень вопросов для дифференциального зачета:

1. Администрирование Windows Server 2019. Службы каталога. Групповые политики.
2. Реализация безопасности клиентских систем.
3. Администрирование Linux. Развертывание веб-серверов Linux.
4. Управление системными сервисами. Аутентификация LDAP.
5. Понятие и виды компьютерных преступлений. Основные стадии компьютерного преступления
6. Классификация угроз информационной безопасности. Методы защиты информационной инфраструктуры.
7. Уязвимости сети. Методы обнаружения уязвимостей сайтов.
8. Уязвимости веб-приложений. Обнаружение уязвимостей веб-приложений.
9. Идентификация нападающего. Мотивация нарушителей. Анализ технических аспектов нападения
10. Идентификация инцидента. Оценка ущерба от произошедшего нарушения информационной безопасности
11. Методы социальной инженерии. Поиск информации по открытым источникам.

Эталон ответов: приведен в Учебном пособии по МДК 02.03

Условия выполнения

1. Количество билетов для экзаменующегося: 1
2. Время подготовки к ответу: 20 минут
3. Требования к устным ответам:
   Полное овладение содержанием учебного материала, в котором обучающийся легко ориентируется, владение понятийным аппаратом.
4. Оборудование: учебная аудитория, стол, стул, пишущая ручка, бумага.

Результаты промежуточной аттестации фиксируются в протоколе.

Критерии оценки устных ответов

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

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

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

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

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