Министерство образования Красноярского края

краевое государственное бюджетное

профессиональное образовательное учреждение

«Красноярский колледж радиоэлектроники и информационных технологий»

**ОТЧЕТ ПО УЧЕБНОЙ ПРАКТИКЕ**

09.02.02 Компьютерные сети

код и наименование специальности

КГБПОУ «Красноярский колледж радиоэлектроники и информационных технологий»

место прохождения практики

МДК.03.01 Эксплуатация объектов сетевой инфраструктуры

Код и наименование профессионального модуля и междисциплинарного курса

Студент 9КС-1.17, 25538 Е.В. Аверяскин

Номер группы, зачетной книжки подпись, дата инициалы, фамилия

Руководитель от колледжа М.В. Приходько

подпись, дата инициалы, фамилия

оценка

Красноярск, 2021

# АННОТАЦИЯ

Данный документ является пояснительной запиской к УП. 03 Учебная практика.

Учебная практика проходила в КГБПОУ «Красноярский колледж радиоэлектроники и информационных технологий».

При выполнении работ использовалось следующее оборудование: Персональный компьютер (технические характеристики: Intel Pentium Gold G5400, 8 Gb ОЗУ); Межсетевой экран Cisco ASA 5506-X.

При выполнении работ использовалось следующее программное обеспечение: Командная строка Windows, эмулятор терминала PuTTY, Cisco ASDM.

Пояснительная записка состоит из 64 страниц, 92 рисунков.

# СОДЕРЖАНИЕ

[АННОТАЦИЯ 2](#_Toc67394375)

[СОДЕРЖАНИЕ 3](#_Toc67394376)

[ВВЕДЕНИЕ 4](#_Toc67394377)

[1. Настройка межсетевого экрана Cisco ASA 5506-X 5](#_Toc67394378)

[1.1. Сброс CISCO ASA 5506-X до заводских настроек 6](#_Toc67394379)

[1.2. Назначение имени устройства 9](#_Toc67394380)

[1.3. Настройка времени и даты 10](#_Toc67394381)

[1.4. Создание нового пользователя 10](#_Toc67394382)

[1.5. Удаление BVI1 интерфейса 10](#_Toc67394383)

[1.6. Настройка порта для подключения внутренних устройств 11](#_Toc67394384)

[1.7. Настройка IP-адресации 12](#_Toc67394385)

[1.8. Настройка SSH-сервера на межсетевом экране 13](#_Toc67394386)

[1.9. Настройка DHCP-сервера 13](#_Toc67394387)

[1.10. Резервная копия конфигурационного файла 14](#_Toc67394388)

[1.11. Настройка ASDM 14](#_Toc67394389)

[1.12. Использование утилит ping, traceroute, packet tracer 17](#_Toc67394390)

[1.13. Перезагрузка Cisco ASA 5506-X с помощью ASDM 20](#_Toc67394391)

[1.14. Резервная копия конфигурации и её восстановление 21](#_Toc67394392)

[1.15. Настройка списков доступа 23](#_Toc67394393)

[1.16. Создание группы сервисов в ASDM 24](#_Toc67394394)

[1.17. Создание группы сетевых объектов 25](#_Toc67394395)

[1.18. Настройка доступа в сеть Интернет 26](#_Toc67394396)

[1.19. Настройка VPN-сервера 28](#_Toc67394397)

[1.20. Настройка доступа к веб-серверу из сети Интернет 34](#_Toc67394398)

[1.21. Сброс пароля для входа в привилегированный режим с сохранением конфигурации 38](#_Toc67394399)

[2. Администрирование 1С: Предприятие 41](#_Toc67394400)

[2.1 Создание виртуальной машины VMware 41](#_Toc67394401)

[2.2 Установка 1С:Предприятие 42](#_Toc67394402)

[2.3 Установка конфигурацию для 1C:Предприятия 44](#_Toc67394403)

[2.4 Добавление информационных баз в 1C:Предприятие 45](#_Toc67394404)

[2.5 Применение фильтров в Журнале регистрации 46](#_Toc67394405)

[2.6 Выгрузка конфигурации информационной базы в файл 49](#_Toc67394406)

[2.7 Создание информационную базу данных из шаблона 51](#_Toc67394407)

[2.8 Создание новых пользователей 52](#_Toc67394408)

[2.9 Загрузка конфигурации из файла 54](#_Toc67394409)

[2.10 Выгрузка информационной базы 56](#_Toc67394410)

[2.11 Загрузка информационной базы 57](#_Toc67394411)

[2.12 Тестирование информационной базы 58](#_Toc67394412)

[ЗАКЛЮЧЕНИЕ 60](#_Toc67394413)

[БИБЛИОГРАФИЧЕСКОЕ ОПИСАНИЕ 61](#_Toc67394414)

# ВВЕДЕНИЕ

Программное обеспечение компьютерных сетей – это специализированное программное обеспечение, задачами которого является проектирование, тестирование, мониторинг, обнаружение ошибок в компьютерных сетях и рабочих станциях.

Целями учебной практики являются получение навыков настройки межсетевого экрана Cisco ASA 5506-X и 1С.

Задачами учебной практики были:

1. Настройка межсетевого экрана

# Настройка межсетевого экрана Cisco ASA 5506-X

Межсетевой экран (сетевой экран, брандмауэр, файрволл) — программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами.

Назначение межсетевых экранов:

* среди задач, которые решают межсетевые экраны, основной является защита сегментов сети или отдельных хостов от несанкционированного доступа с использованием уязвимых мест в протоколах сетевой модели OSI или в программном обеспечении, установленном на компьютерах сети. межсетевые экраны пропускают или запрещают трафик, сравнивая его характеристики с заданными шаблонами.
* наиболее распространённое место для установки межсетевых экранов — граница периметра локальной сети для защиты внутренних хостов от атак извне. однако атаки могут начинаться и с внутренних узлов — в этом случае, если атакуемый хост расположен в той же сети, трафик не пересечёт границу сетевого периметра, и межсетевой экран не будет задействован. поэтому в настоящее время межсетевые экраны размещают не только на границе, но и между различными сегментами сети, что обеспечивает дополнительный уровень безопасности.

Cisco ASA 5506-X ­– многофункциональное устройство обеспечения безопасности для малого и среднего бизнеса, способное ограничить внутренние ресурсы компании от внешнего воздействия из сети Интернет. Межсетевой экран позволяет фильтровать трафик на различных уровнях стека TCP/IP, может выступать VPN-сервером для подключения удаленных сотрудником компании к внутренней сети, предоставлять доступ к общедоступным ресурсам, находящимся во внутренней сети из сети Интернет, например веб-сервер (рисунок 1).



Рисунок 1 ­– Cisco ASA 5506-X

Технические характеристики Cisco ASA 5506-X

* технология доступа: Ethernet
* общее количество интерфейсов(портов): 8 шт
* тип интерфейсов: 10/100/1000 BASE-TX (1000 мбит/с)
* порты USB 2.0: 1 шт
* протоколы ethernet: IEEE 802.3, IEEE 802.3ab, IEEE 802.3u
* пропускная способность межсетевого экрана: 750 mбит/с
* поддержка AUTO-MDI/MDI-X: есть
* максимальное количество одновременных сессий: 20000
* количество подключений в секунду: 5000
* пакетов в секунду (64 байт): 85000
* пропускная способность 3DES/AES VPN: 100
* пользователи IPsec VPN: 10
* объем системной флеш-памяти: 8192 мб
* память: 4096 мб

# Сброс CISCO ASA 5506-X до заводских настроек

Сброс до заводских настроек необходим, когда нужно удалить старую конфигурацию с уже настроенного оборудования.

Чтобы сбросить до заводских настроек Cisco ASA 5506-x необходимо отключить оборудование от электросети, подключить синий консольный кабель к USB-порту компьютера и к межсетевому экрану. (рисунок 2)



Рисунок 2 ­– Подключение с помощью консольного кабеля

Запустить программу PuTTY и выбрать COM-порт, к которому подключен межсетевой экран и нажать кнопку соединиться. (рисунок 3)

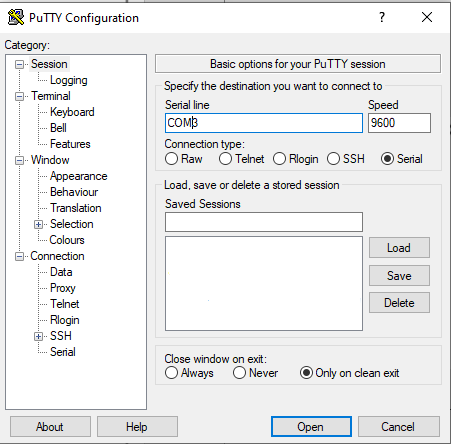


Рисунок 3 ­– Программа PuTTY

Подключить оборудование к электросети и нажимать на клавишу ESC до появления сообщения ROMMON> в командной строке. (рисунок 4)

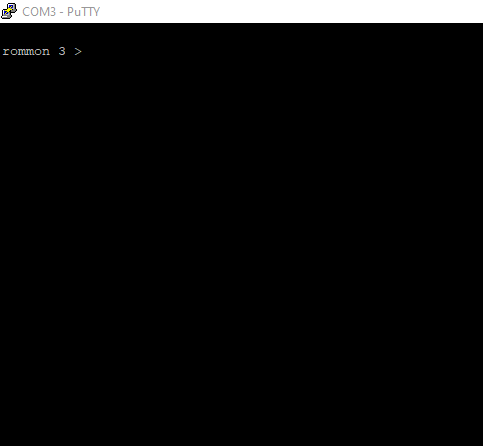


Рисунок 4 ­– режим rommon

Далее нужно вести команду *confreg* и ответить на несколько вопросов. На вопрос **Do you wish to change this configuration? y/n [n]:** нужно ответь положительно (клавиша y), на все остальные вопросы отрицательно (клавиша n). (рисунок 5)

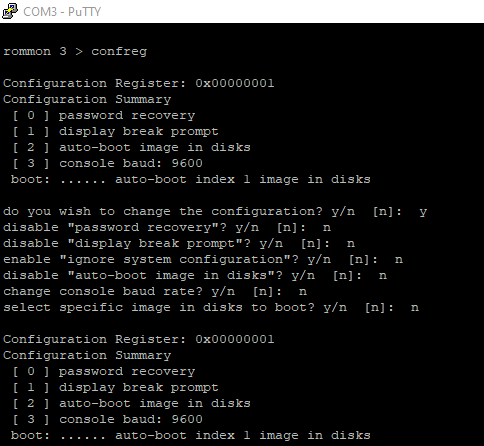


Рисунок 5 ­– Сброс конфигурации

Далее нужно написать команду *boot*, чтобы продолжить запуск оборудования. После появления сообщения ciscoasa> нужно ввести команду *enable* и нажать два раза клавишу Enter. Далее нужно ввести команду configure terminal и нажать Enter. Появится сообщение ciscoasa(config)#, введите команду *config factory-default*, чтобы загрузить заводские настройки. Начнется автоматическая процедура, которая будет вставлять команды. В конце появится сообщение Factory-default configuration is completed, что означает успешное окончание сброса настроек. (рисунок 6)

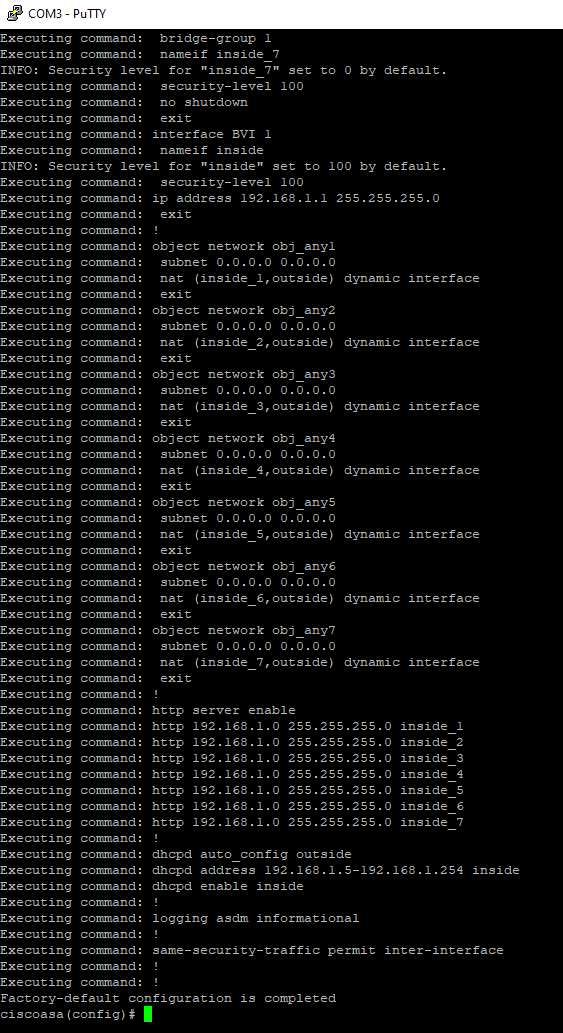


Рисунок 6 ­– Успешный сброс настроек

Для завершения сброса и сохранения новых настроек нужно ввести команды *config-register 0x10011* и сохранить конфигурацию командой *write memory.* (рисунок 7)

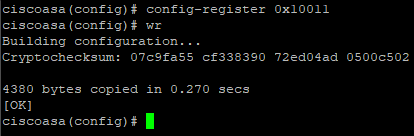


Рисунок 7 ­– Сохранение настроек

# Назначение имени устройства

Имя устройства задается, чтобы при наличии нескольких одинаковых устройств отличать их.

Чтобы назначить имя Cisco ASA 5506-X нужно войти режим глобальный конфигурации с помощью команды configure terminal и ввести команду hostname и указать имя для устройства. (рисунок 8)

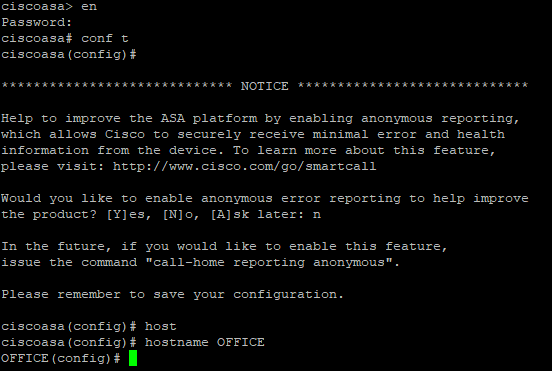


Рисунок 8 ­– Назначение имени межсетевому экрану

# Настройка времени и даты

Настройка даты и времени осуществляется с помощью команды clock set и указанием текущей даты и времени. (рисунок 9)

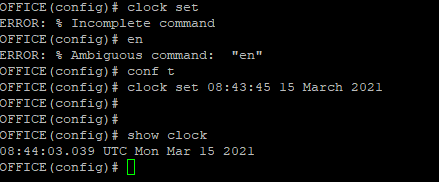


Рисунок 9 ­– Настройка времени и даты

* 1. **Создание нового пользователя**

Создание нового пользователя нужно, что новый работник смог подключиться к устройству и мог делать только то, что ему разрешено. Для этого при создании пользователя указывается привилегии, где 15 — это максимальные привилегии и пользователь может совершать любые действия с оборудованием.

Что бы создать нового пользователя, нужно в режиме глобальной конфигурации ввести команду username \* password \* privilege \*, где \* – это конкретное имя, пароль и уровень привилегий соответственно. (рисунок 10)



Рисунок 10 ­– Создание пользователя

* 1. **Удаление BVI1 интерфейса**

BVI – это виртуальный интерфейс группы мостов, который создается автоматически и объединяет все интерфейсы межсетевого экрана, кроме первого. Из-за это нельзя задать IP-адрес интерфейсам, входящих в группу. Чтобы удалить BVI интерфейс нужно удалить, входящие в него интерфейсы. Для этого нужно в режиме глобальной конфигурации ввести команду interface и указать интерфейс с номером. После этого ввести команды no nameif и no bridge-group 1. (рисунок 11)

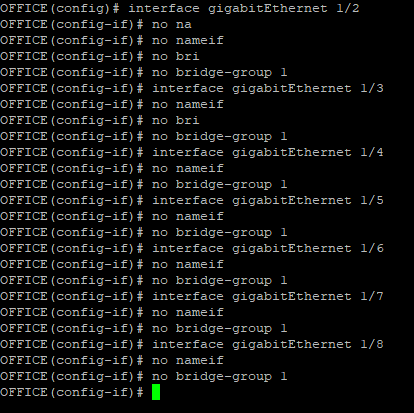


Рисунок 11 ­– Удаление интерфейсов из группы

После того, как все интерфейсы из группы были удалены, можно удалить интерфейс BVI с помощью команды clear configure interface BVI 1. (рисунок 12)



Рисунок 12 ­– Удаление интерфейса BVI

* 1. **Настройка порта для подключения внутренних устройств**

Особенностью межсетевого экрана является то, что он делит интерфейсы на внешние и внутренние и позволяет установить уровень безопасности для интерфейса. По умолчанию устройства из более безопасного интерфейса могут отправлять данные в менее безопасный интерфейс, но устройства из менее безопасного интерфейса не могу отправлять данный в более безопасный интерфейс, если нет особенных списков доступа.

Нужно настроить интерфейс, к которому будут подключаться устройства в локальной сети. Локальная сеть является безопасным местом и имеет наивысший уровень безопасности 100.

Для этого в режиме глобальной конфигурации введите команду interface и выберите интерфейс для настройки. После этого нужно ввести команду nameif inside и security-level 100. (рисунок 13)



Рисунок 13 ­– Настройка внутреннего интерфейса

* 1. **Настройка IP-адресации**

Для обмена информации в компьютерной сети необходимо, чтобы каждый компьютер имел уникальный IP-адрес. Кроме конечных устройств, таких как компьютер и сервер, IP-адреса должны иметь и промежуточные устройства, такие как роутеры или межсетевые экраны. IP-адрес может быть настроен вручную или получен автоматически с помощью DHCP-сервера.

В нашем случае межсетевой экран имеет два физических интерфейса, внешний должен получать IP-адрес автоматически, а внутреннему интерфейсу и саб-интерфейсу назначен вручную.

Для это нужно ввести в режиме глобальной конфигурации команду interface и выбрать интерфейс. После этого ввести команду для автоматического назначения IP-адреса ip address dhcp. Для ручного назначения нужно ввести команду ip address x.x.x.x x.x.x.x, где первые четыре числа — это адрес хоста, а вторые маска подсети. (рисунок 14-16)



Рисунок 14 ­– Настройка внешнего интерфейса



Рисунок 15 ­– Настройка внутреннего интерфейса



Рисунок 16 ­– Настройка сабинтерфейса интерфейса

* 1. **Настройка SSH-сервера на межсетевом экране**

SSH используется для удаленного управления сетевыми устройствами, обеспечивая шифрование трафика, в том числе паролей.

Для настройки SSH-сервера на Cisco ASA 5506-X нужно в режиме глобальной конфигурации ввести команду ssh и указать с какого ip-адреса будет доступно удаленное управление. Это может быть одно конкретное устройство или целая подсеть.

Также нужно ввести команду aaa authentication ssh console LOCAL, чтобы для аутентификации использовалась локальная база SSH-сервера. (рисунок 17)

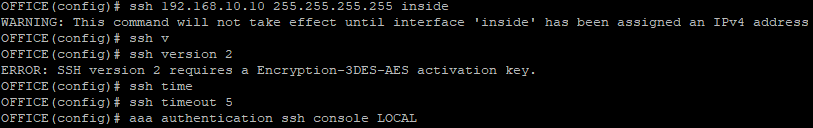


Рисунок 17 ­– Настройка SSH-сервера

* 1. **Настройка DHCP-сервера**

DHCP — протокол прикладного уровня модели TCP/IP, служит для назначения IP-адреса клиенту.

Для настройки DHPC-сервера на Cisco ASA 5506-X нужно ввести команду dhcp address и указать диапазон адресов и название интерфейса. (рисунок 18)



Рисунок 18 ­– Настройка DHPC -сервера

* 1. **Резервная копия конфигурационного файла**

Чтобы в случае выхода из строя оборудования не тратить время на настройку, можно восстановить конфигурационный файл из резервной копии. Чтобы сделать резервную копию необходим tftp-сервер.

Для того чтобы сохранить файл конфигурации нужно ввести в режиме глобальной конфигурации команду copy running-config tftp: и указать какой файл копировать, адрес tftp-сервера и как будет называться файл на сервере. (рисунок 19)

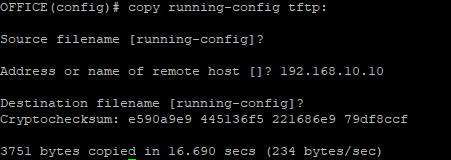


Рисунок 19 ­– Сохранение файла конфигурации

* 1. **Настройка ASDM**

Система Cisco Adaptive Security Device Manager (ASDM) предоставляет функции управления и мониторинга через наглядный и простой в использовании управляющий Web-интерфейс, который позволяет ускорить процесс развертывания устройств защиты с помощью интеллектуальных настройщиков, эффективных инструментальных средств администрирования и гибких функций мониторинга.

Чтобы загрузить клиент ASDM нужно активировать http-сервер на Cisco ASA 5506-X, для этого нужно ввести команду http server enable и http 192.168.10.0 255.255.0 inside, что указать с какой подсети можно подключиться к веб-серверу и с какого интерфейса. (рисунок 20)



Рисунок 20 ­– Активация веб-сервера на Cisco ASA 5506-X

Далее нужно выбрать образ ASDM. Для этого нужно ввести команду asdm image flash:asdm-771.bin. (рисунок 21)



Рисунок 21 ­– Выбор образа ASDM

После перейдите на адресу внутреннего интерфейса Cisco ASA в веб-браузере и должно открыться окно с предложение скачать установщик ASDM. (рисунок 22)

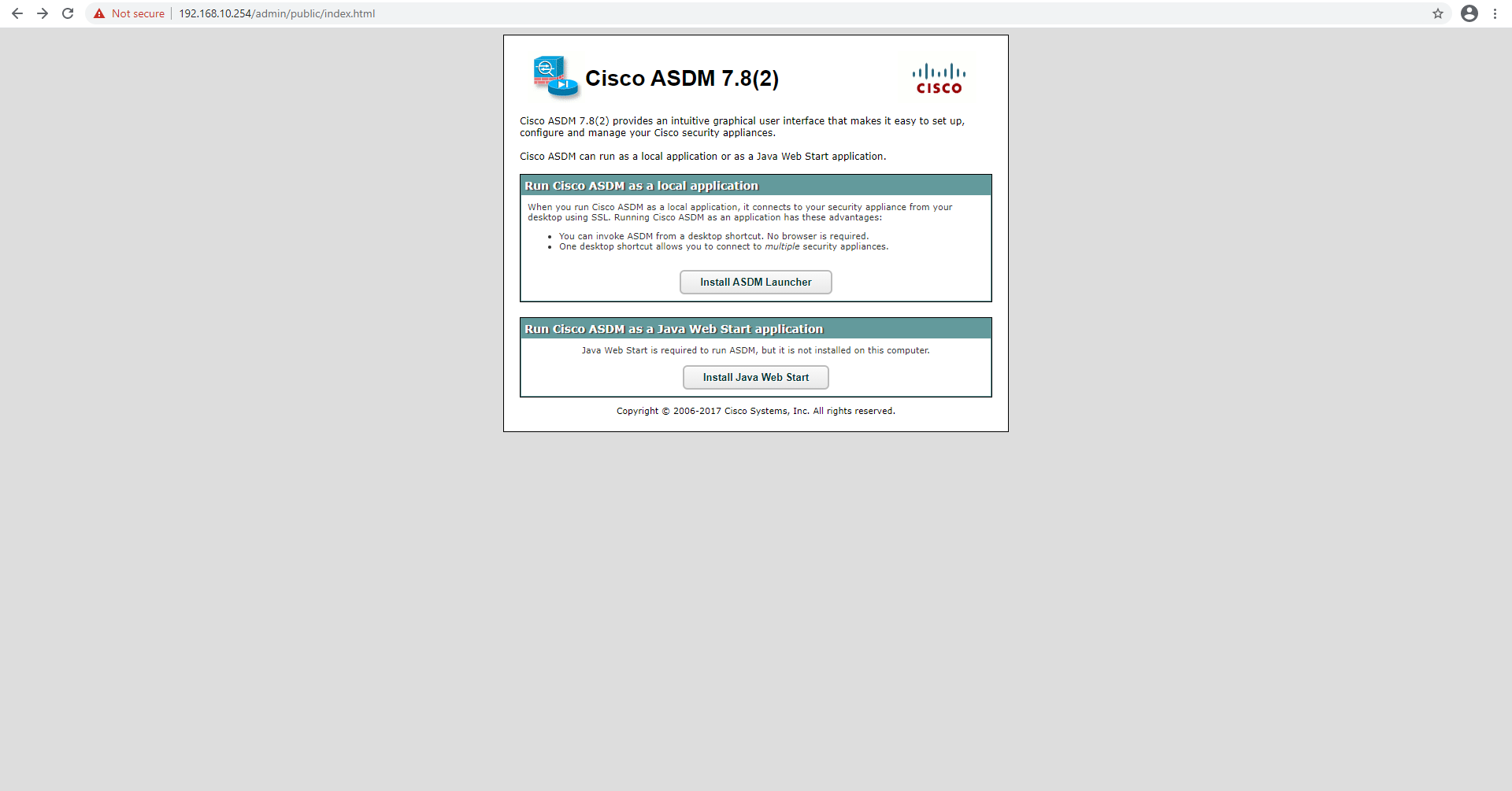


Рисунок 22 ­– Веб-страница для скачивания ASDM

Запустите установщик и следуйте его указаниям. (рисунок 23)

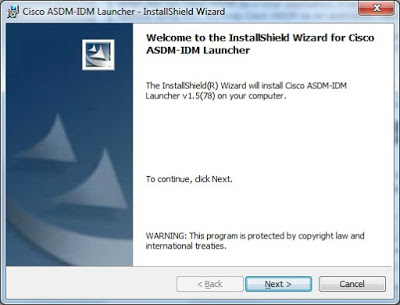


Рисунок 23 ­– Установка ASDM

Запустите приложение ASDM и должно открыться окно входа. Введите IP-адрес Cisco ASA и свои данные. (рисунок 24)

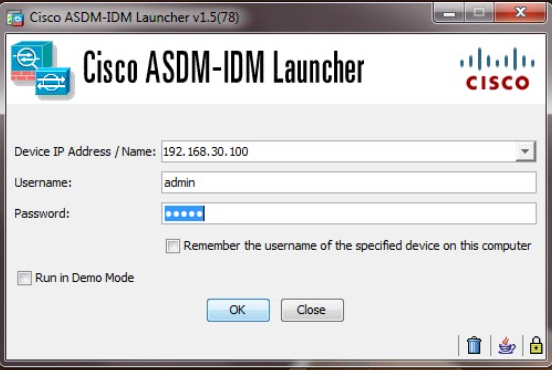


Рисунок 24 ­– Окно входа в ASDM

Если данные верны, появится предупреждение, нажмите кнопку продолжить. (рисунок 25)

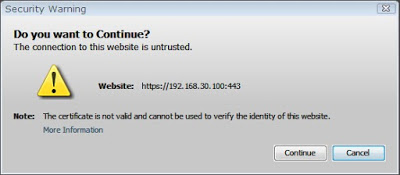


Рисунок 25 ­– Предупреждение

В результате откроется окно программы ASDM. (рисунок 26)

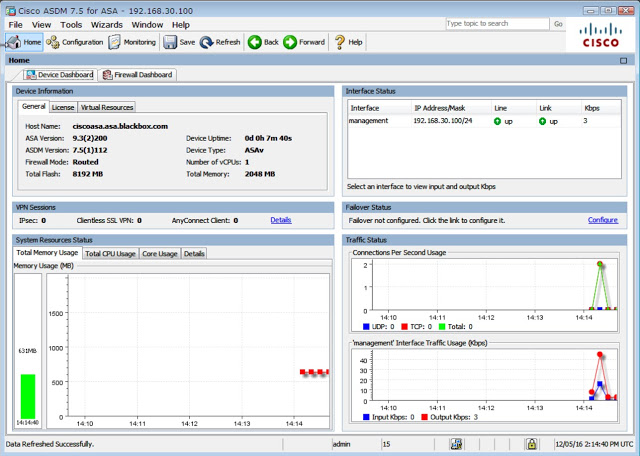


Рисунок 26 ­– Интерфейс ASDM

* 1. **Использование утилит ping, traceroute, packet tracer**

Ping — утилита для проверки целостности и качества соединений в сетях на основе TCP/IP. Для запуска утилиты ping нужно в программе ASDM на вкладке Tools выбрать утилиту ping. (рисунок 27)

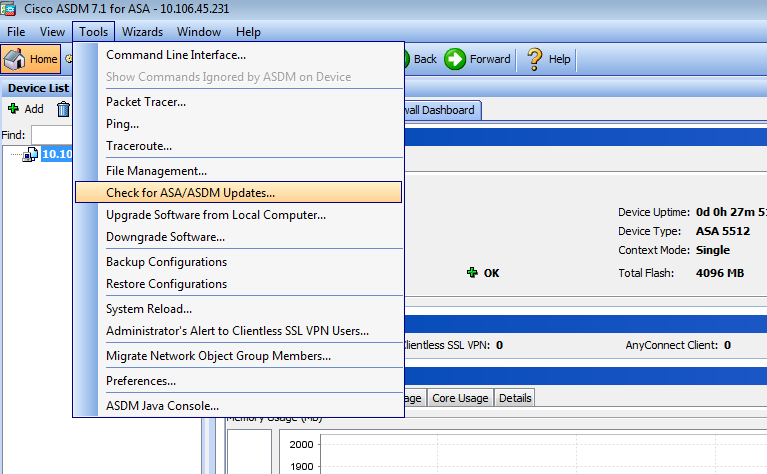


Рисунок 27 ­– Список инструментов

Откроется окно утилиты, в котором можно выбрать тип пакета, адрес назначения и адрес источника. После нажатия кнопки Ping в окне вывода появится сообщение об успешной или неуспешной проверке доступности. (рисунок 28)

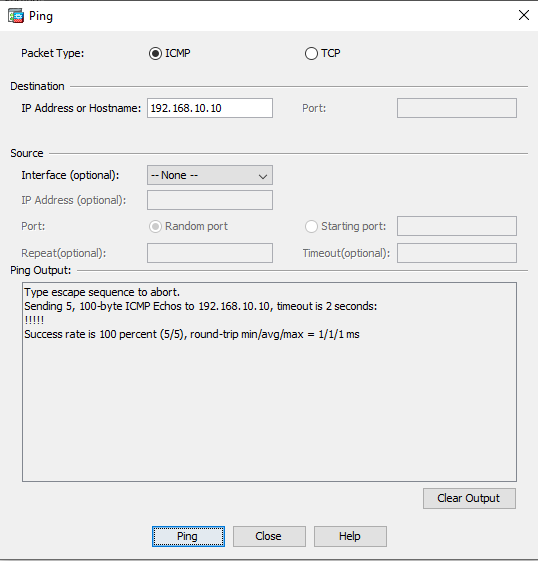


Рисунок 28 ­– Результат проверки доступности

Утилита Packet Tracer в ASDM показывает какие проверки прошел пакет от источника до фактического пункта назначения. Для запуска утилиты packet tracer нужно в программе ASDM на вкладке Tools выбрать утилиту Packet Tracer. (рисунок 27)

Откроется окно, в котором нужно указать интерфейс, тип пакета, адреса отправления и назначения и tcp/udp порт. После нажатия кнопки Start, будет показана анимация прохождения пакета и результаты его проверки. (рисунок 29)

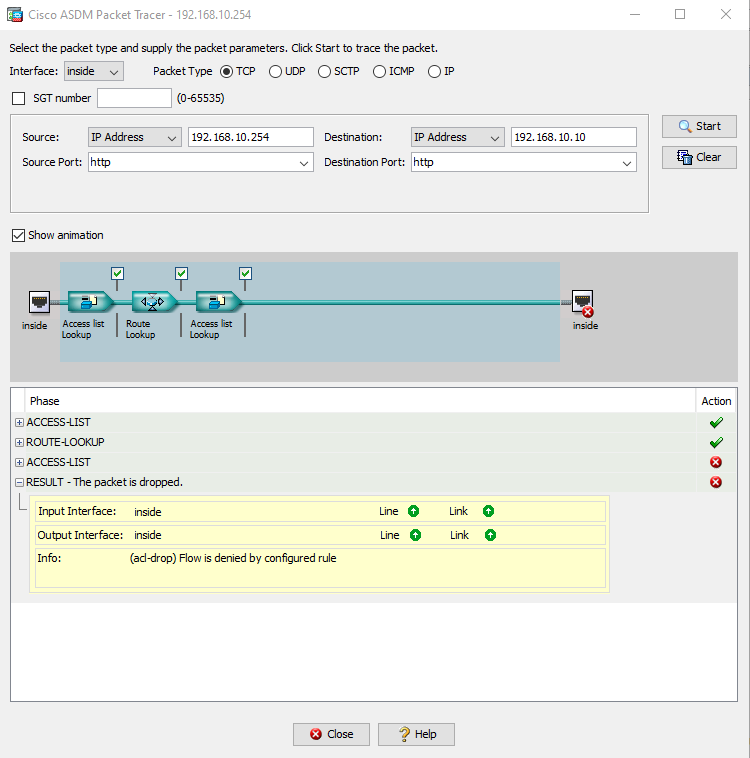


Рисунок 29 ­– Результат проверки пакета

Traceroute — это служебная компьютерная программа, предназначенная для определения маршрутов следования данных в сетях TCP/IP. Для запуска утилиты traceroute нужно в программе ASDM на вкладке Tools выбрать утилиту traceroute. (рисунок 27)

Откроется окно, в котором надо указать адрес назначения и дополнительные параметры, после нажатия кнопки trace route в окне вывода появится информация о результате прохождения пакета. (рисунок 30)

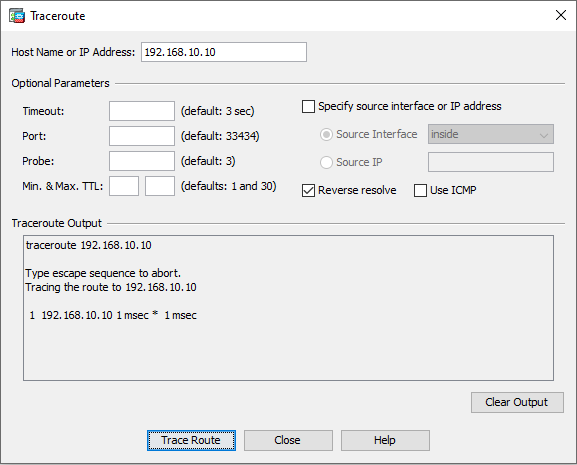


Рисунок 30 ­– Результат прохождения пакета

* 1. **Перезагрузка Cisco ASA 5506-X с помощью ASDM**

Для перезагрузки устройства нужно в программе ASDM на вкладке Tools выбрать функцию System Reload. (рисунок 27)

Откроется окно, в котором можно указать, сохранять ли конфигурацию при перезагрузке, через сколько совершить перезагрузку устройства и при нажатии кнопки Schedule Reload начнется перезагрузка. (рисунок 31)

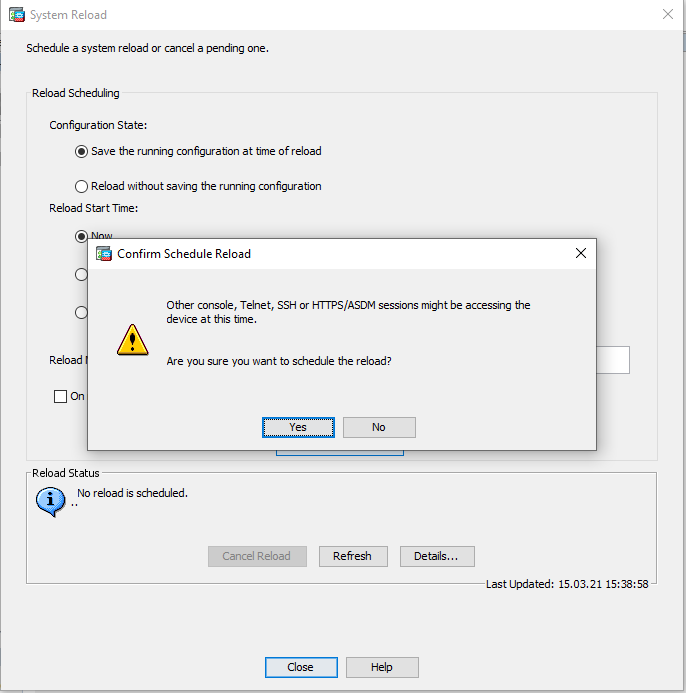


Рисунок 31 ­– Перезагрузка устройства

* 1. **Резервная копия конфигурации и её восстановление**

Чтобы в случае выхода из строя оборудования не тратить время на настройку, можно восстановить конфигурационный файл из резервной копии.

Для того чтобы сохранить файл конфигурации нужно в программе ASDM на вкладке Tools выбрать функцию Backup Configurations (рисунок 27)

Откроется окно, в котором нужно указать путь сохранения резервной копии и её имя, а также что нужно сохранить. (рисунок 32)

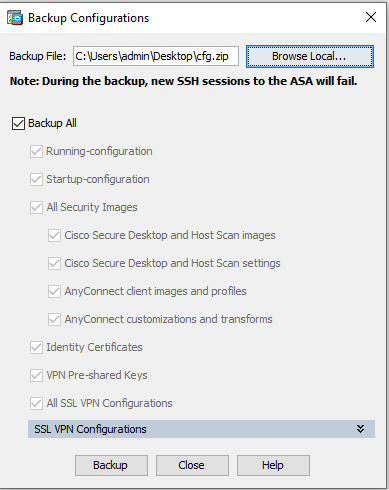


Рисунок 32 ­– Резервное копирование

Для того чтобы восстановить файл конфигурации нужно в программе ASDM на вкладке Tools выбрать функцию Restore Configurations (рисунок 27)

Откроется окно, в котором нужно указать путь расположения резервной копии и её имя, а также что нужно восстановить. (рисунок 33)

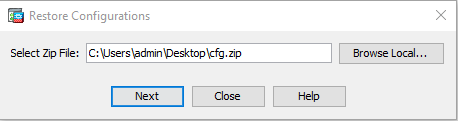


Рисунок 33 ­– Восстановления конфигурации

* 1. **Настройка списков доступа**

В сетях ACL представляют список правил, определяющих порты служб или имена доменов, доступных на узле или другом устройстве третьего уровня OSI, каждый со списком узлов и/или сетей, которым разрешен доступ к сервису. Сетевые ACL могут быть настроены как на обычном сервере, так и на маршрутизаторе и могут управлять как входящим, так и исходящим трафиком, в качестве межсетевого экрана.

Для настройки списков доступа нужно в программе ASDM открыть меню Firewall, выбрать пункт Access Rules и нажать кнопку Add. (рисунок 34)

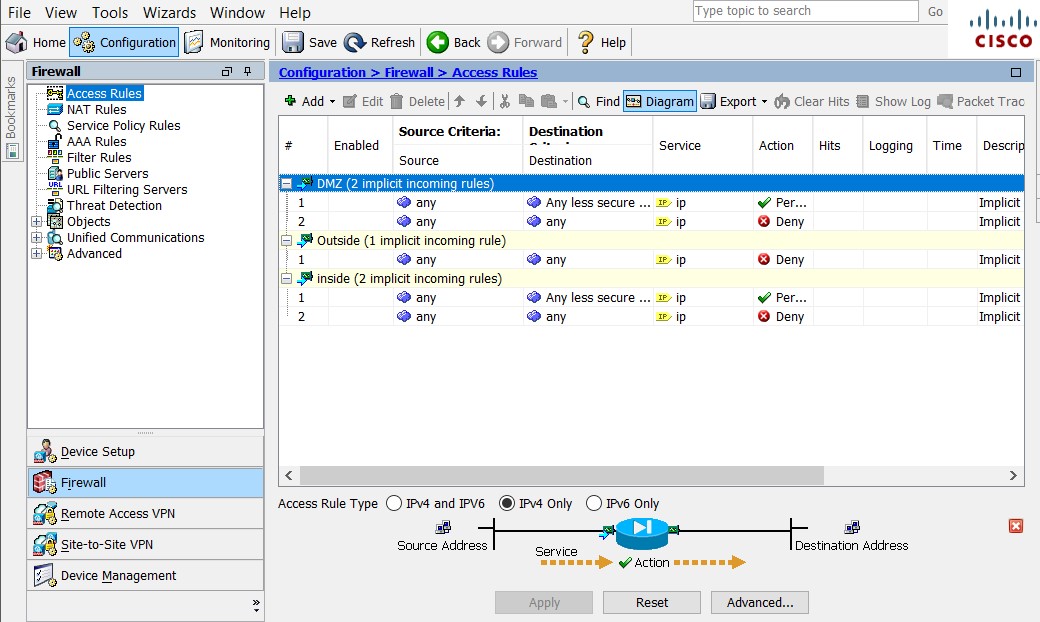


Рисунок 34 ­– Меню Access Rules

Откроется окно, в котором нужно выбрать интерфейс, выбрать действие разрешить или запретить, указать адрес источника и адрес назначения, а также службу, которой может быть tcp/udp порт. (рисунок 35)

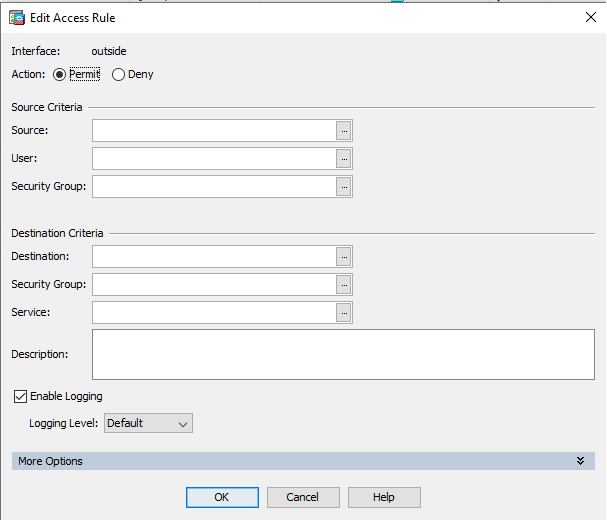


Рисунок 35 ­– Настройка списка доступа

Настроим списки доступа, чтобы был разрешен протокол ICMP, а также 80 и 443 порт TCP, для доступа к веб-сайтам, но без DNS веб-сайты открываться не будут, так что разрешим протокол DNS. (рисунок 36)

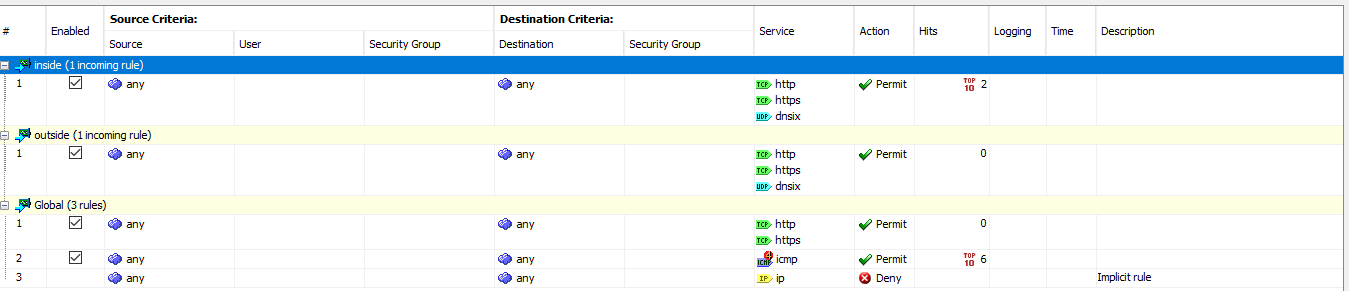


Рисунок 36 ­– Настроенные списки доступа

* 1. **Создание группы сервисов в ASDM**

Группа сервисов используется для объединения TCP/UDP портов, которые отвечают за какую-то одну службу, например для удаленного управления Windows RDP.

Для создания группы сервисов нужно в программе ASDM, в меню Firewall, в правой части программы выбрать вкладку Services и нажать кнопку Add. (рисунок 37)

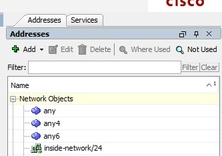


Рисунок 37 ­– Добавления группы сервисов

Откроется окно, в котором нужно ввести имя группы и указать tcp/udp порты. (рисунок 38)

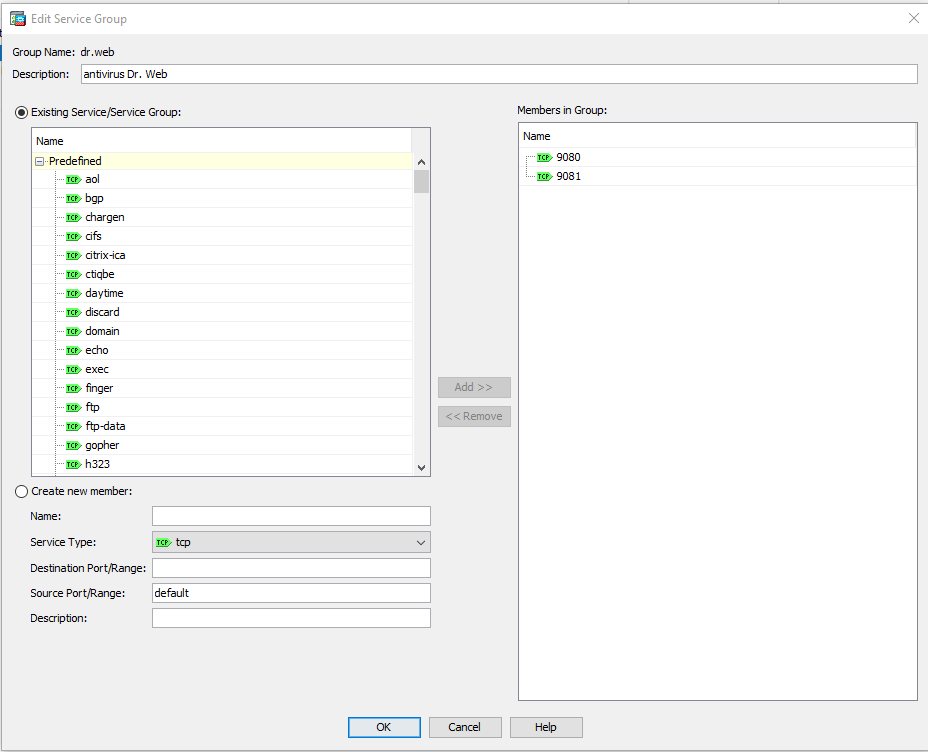


Рисунок 38 ­– Параметры группы сервисов

* 1. **Создание группы сетевых объектов**

Группа сетевых объектов используется для объединения ip-адресов, которые отвечают какому-то одному критерия, например ip-адреса всех серверов.

Для создания группы сетевых объектов нужно в программе ASDM, в меню Firewall, в правой части программы выбрать вкладку Addresses и нажать кнопку Add. (рисунок 39)

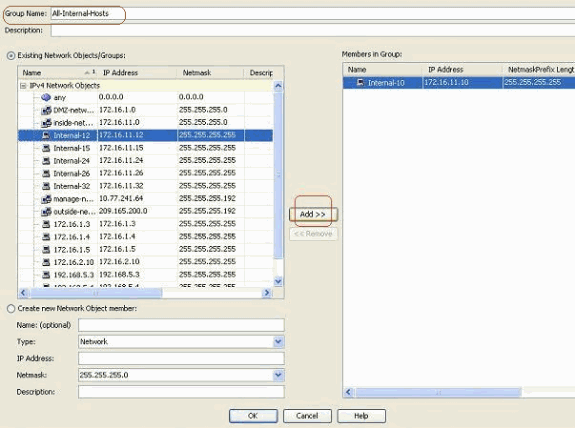


Рисунок 39 ­– Параметры группы сетевых объектов

Теперь разрешим группе сетевых объектов к службе torrent. Для этого создадим список доступа, в котором укажем в графе источником созданную группу сетевых объектов, а в графе службы tcp/udp порты, отвечающие за службу torrent. (рисунок 40)

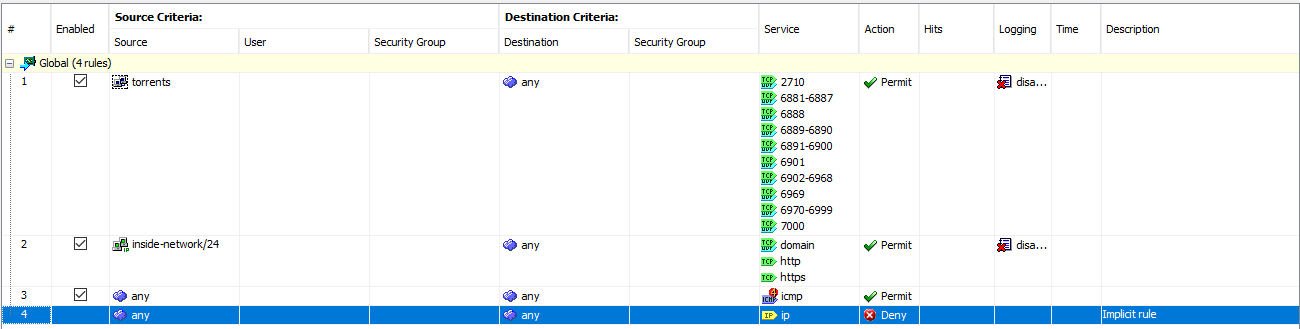


Рисунок 40 ­– Список доступа для группы сетевых объектов

* 1. **Настройка доступа в сеть Интернет**

Для того, чтобы локальные пользователи смогли получить доступ к сети Интернет, нужно настроить межсетевой экран, чтобы он пропускал трафик от внутреннего интерфейса на внешний интерфейс, для этого нужно настроить список доступа.

Также из-за того, что на внешнем интерфейсе настроен один IP-адрес, а локальная сеть может иметь много IP-адрес, нужно использовать технологию трансляции сетевых адресов (NAT).

Для настройки списков доступа нужно в программе ASDM открыть меню Firewall, выбрать пункт Access Rules и нажать кнопку Add. (рисунок 34)

Настроим списки доступа, чтобы был разрешен протокол ICMP, а также 80 и 443 порт TCP, для доступа к веб-сайтам, но без DNS веб-сайты открываться не будут, так что разрешим протокол DNS. (рисунок 36)

Для настройки NAT нужно в программе ASDM открыть меню Firewall, выбрать пункт NAT Rules и нажать кнопку Add. (рисунок 41)

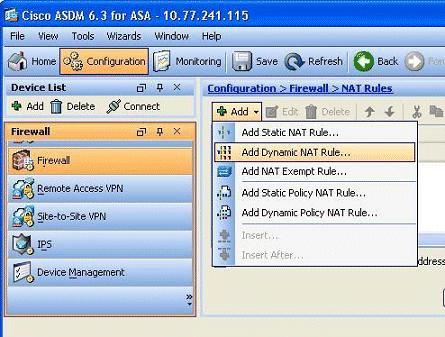


Рисунок 41 ­– Добавление NAT

Откроется окно, в котором нужно указать интерфейс источника и интерфейс назначения, адрес источника и адреса назначения, а также указать тип NAT, и с какого интерфейса будут отправляться пакеты в сеть Интернет. (рисунок 42)



Рисунок 42 ­– Параметры NAT

* 1. **Настройка VPN-сервера**

VPN используется для обеспечения доступа удаленных пользователей до внутренних ресурсов компании. Cisco ASA 5506-X может выступать в качестве VPN-сервера. Для настройки Remote access VPN нужно в программе ASDM во вкладке Wizard выбрать VPN Wizard и следовать инструкциям.

На первом этапе нужно выбрать тип VPN, нужно указать Remote access и выбрать внешний интерфейс. (рисунок 43)

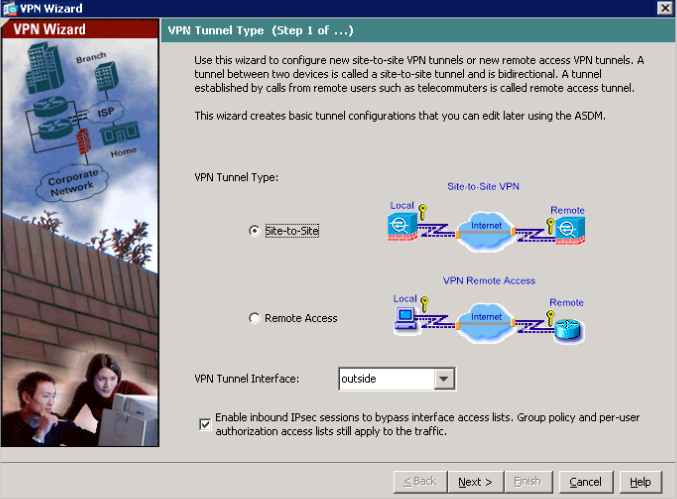


Рисунок 43 ­– Настройка VPN

На втором этапе нужно выбрать тип клиента, нужно выбрать Microsoft Windows и указать протоколы аутентификации. (рисунок 44)

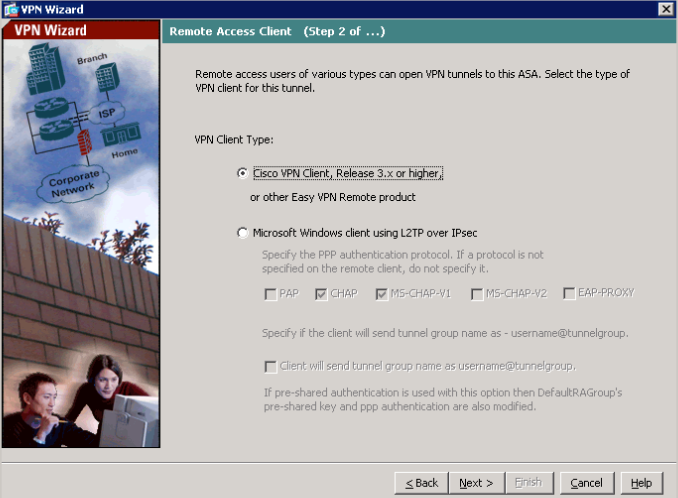


Рисунок 44 ­– Настройка VPN

На третьем этапе нужно указать метод аутентификации, нужно выбрать Pre-shared key и ввести общий ключ. (рисунок 45)

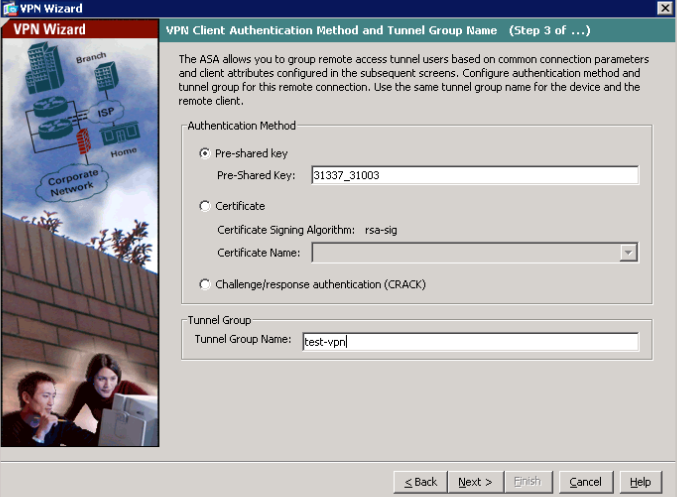


Рисунок 45 ­– Настройка VPN

На четвертом этапе нужно указать базу данных для аутентификации, нужно выбрать локальную базу данных. (рисунок 46)

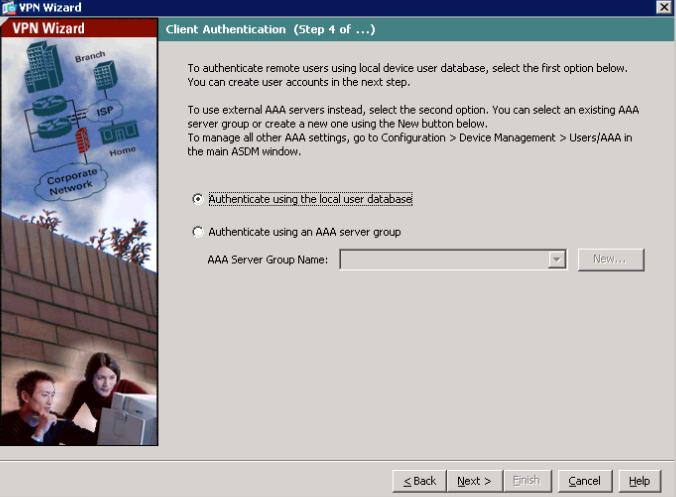


Рисунок 46 ­– Настройка VPN

На пятом этапе нужно добавить новых пользователей, указываем имя пользователя и пароль дважды. (рисунок 47)

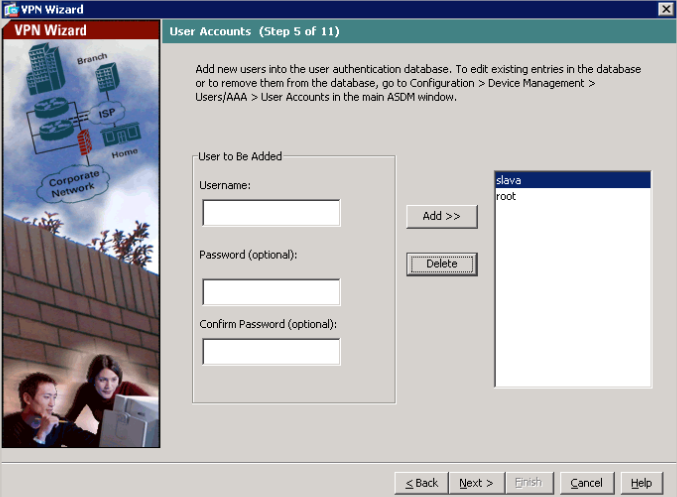


Рисунок 47 ­– Настройка VPN

На шестом этапе нужно выбрать диапазон IP-адресов для удаленных пользователей, создаем новый диапазон и выбираем IP-адреса. (рисунок 48)

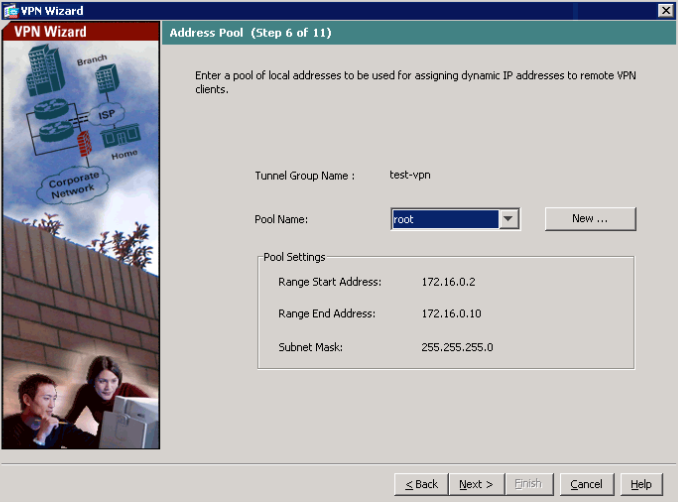


Рисунок 48 ­– Настройка VPN

На седьмом этапе нужно указать IP-адреса DNS-сервера, WINS-сервера и доменное имя. (рисунок 49)

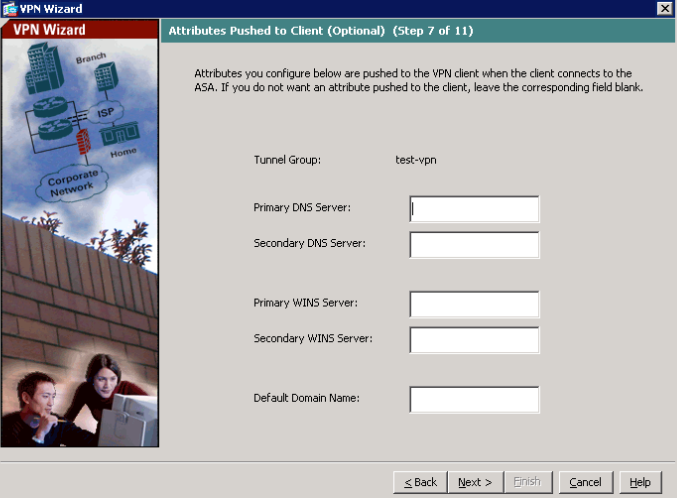


Рисунок 49 ­– Настройка VPN

На девятом этапе нужно указать какие сети будут доступны удаленным пользователям. Можно выбрать интерфейс или подсеть. (рисунок 50)

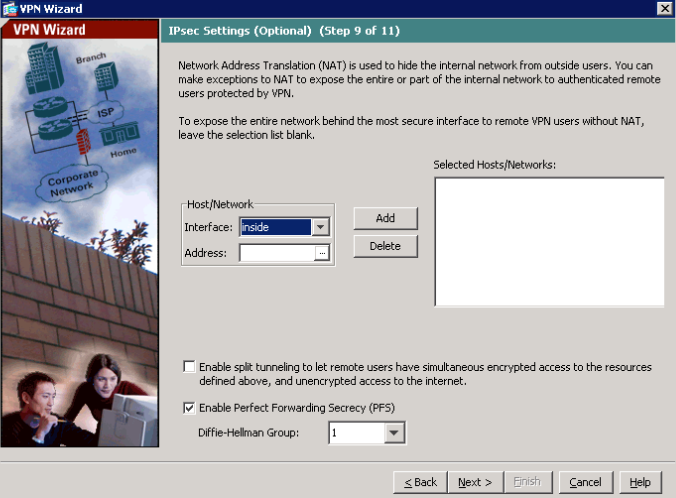


Рисунок 50 ­– Настройка VPN

При следующем нажатии на кнопку Next отобразится вся указанная информация и при правильном выборе настроек нажмите кнопку Finish. (рисунок 51)

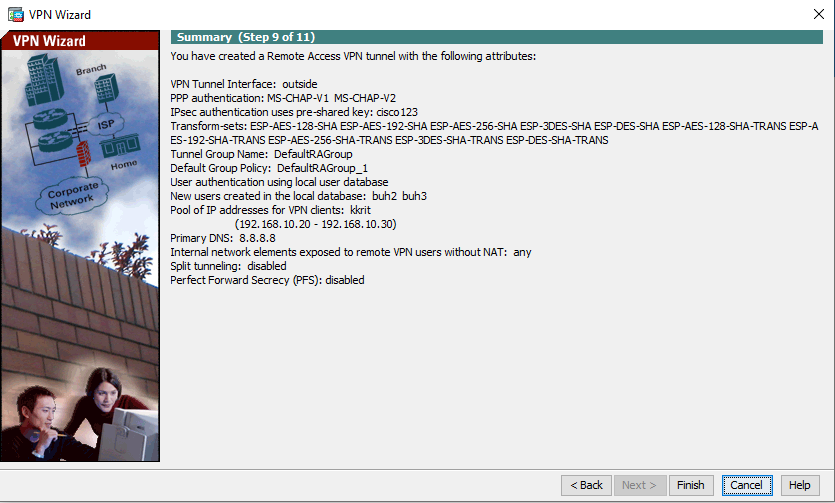


Рисунок 51 ­– Финальное окно настройки VPN

Для проверки доступности VPN-сервера добавим новое VPN-подключение в операционной системе Windows 10 с такими параметрами. (рисунок 52)

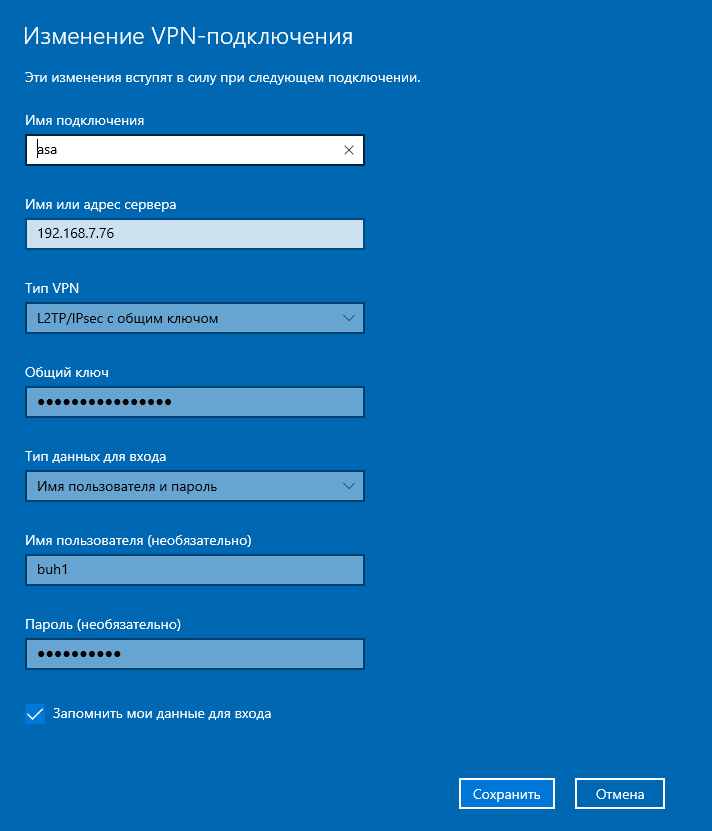


Рисунок 52 ­– Добавление VPN-подключения

Подключимся к VPN-серверу и проверяем доступ к сети Интернет. (рисунок 53)

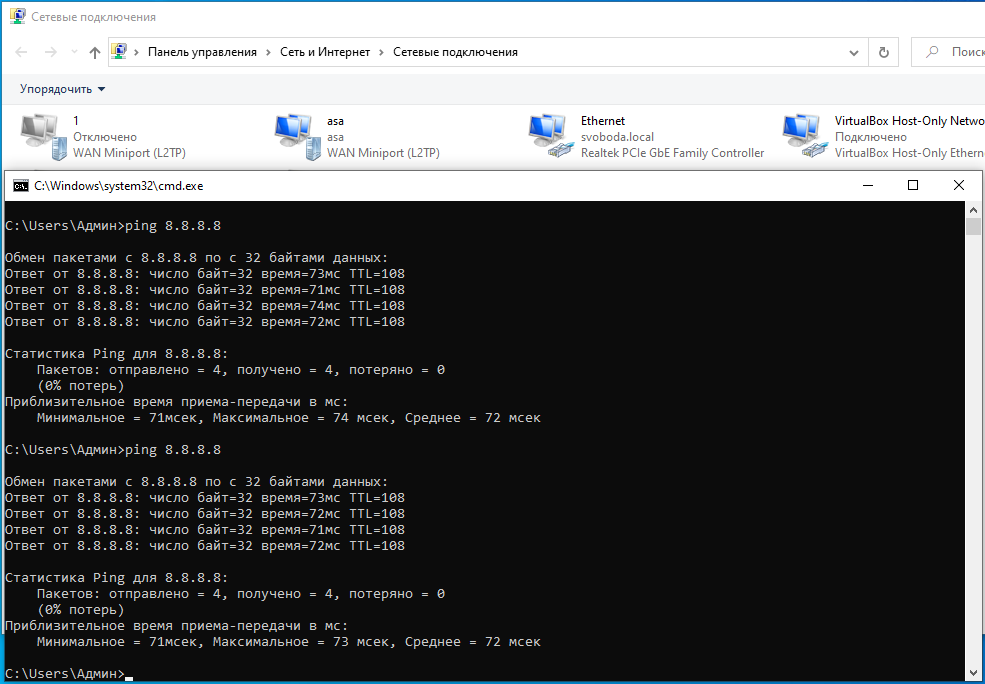


Рисунок 53 ­– Проверка работоспособности VPN-сервера

* 1. **Настройка доступа к веб-серверу из сети Интернет**

Когда в локальной сети присутствует сервер, на котором находятся службы, которые должны быть доступны за пределами внутренней сети, например, веб-сервер или почтовый сервер. Для этого нужно правильно настроить, чтобы межсетевой экран разрешал трафик из внешней сети только к общедоступному серверу и не допускал к другим внутренним пользователям сети. Для решения такой задачи в программе ASDM есть два решения, первый это вручную настроить списки доступа и NAT, а второй используя функцию Public Servers. Первый способ подходит, когда в наличии только один публичный IP-адрес и он назначен внешнему интерфейсу межсетевого экрана, а второй, когда имеется дополнительный публичный адрес именно для сервера.

Сначала нужно включить и настроить веб-сервер, для этого создадим виртуальную машину с установленной операционной системой Windows 7 и программой Denwer. (рисунок 54)



Рисунок 54 ­– Виртуальная машина с веб-сервером

Особенностью Denwer является, то, чтобы открыть веб-сайт используя IP-адрес сервера нужно, чтобы папка веб-сайта имела в название IP-адрес. (рисунок 55)

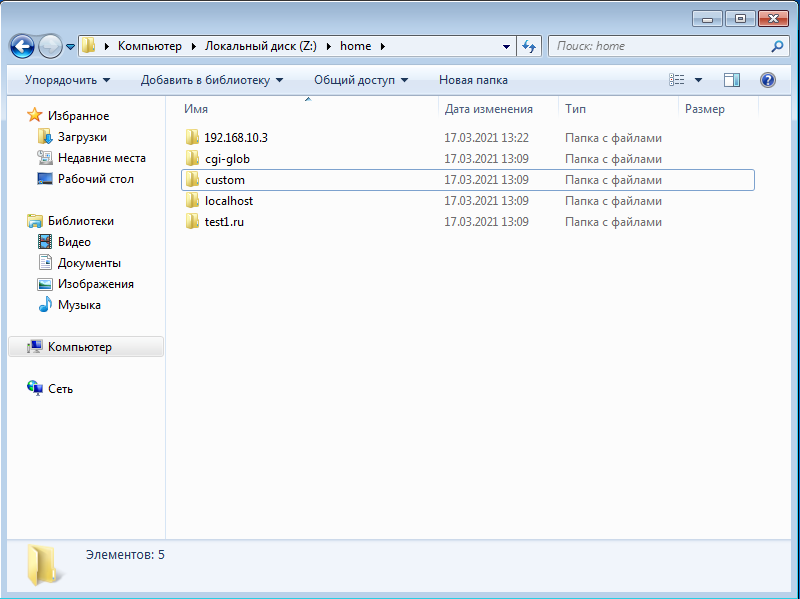


Рисунок 55 ­– Папка веб-сайта

Используя первый способ настроим NAT и списки доступа в соответствующих пунктах программы ASDM. (рисунки 56-57)

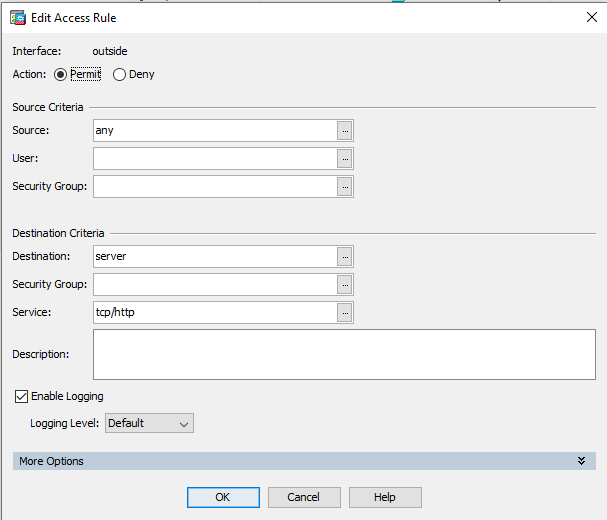


Рисунок 56 ­– Список доступа для сервера

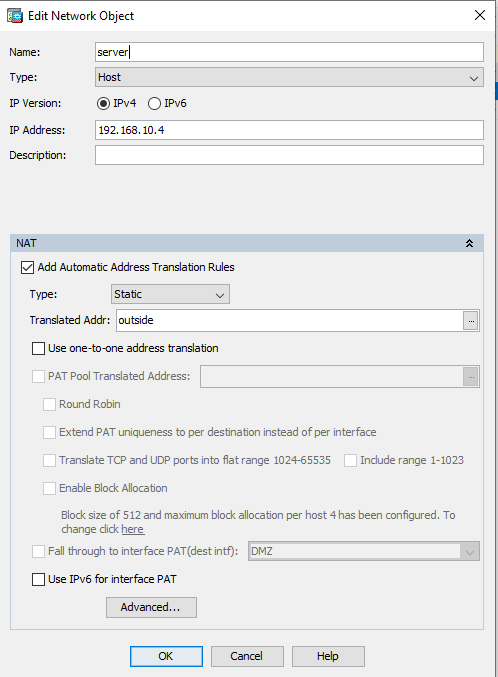


Рисунок 57 ­– Настройка NAT для сервера

Теперь при переходе по адресу внешнего интерфейса Cisco ASA будет открываться веб-сайт. (рисунок 58)

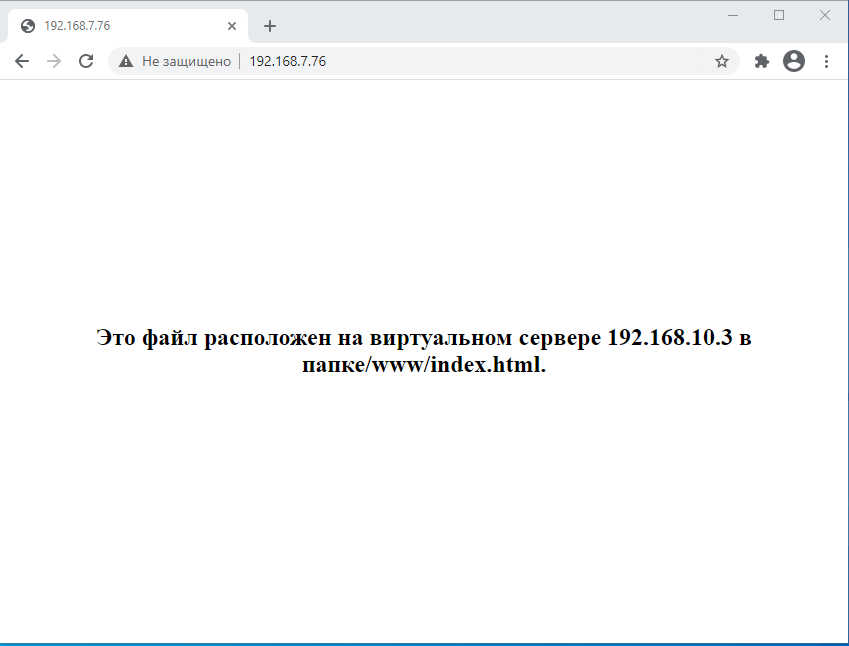


Рисунок 58 ­– Открытый веб-сайт через первый способ

Второй способ немного проще, необходимо указать внешний и внутренний интерфейс, внешний и внутренний IP-адрес, а также tcp-порт. (рисунок 59)

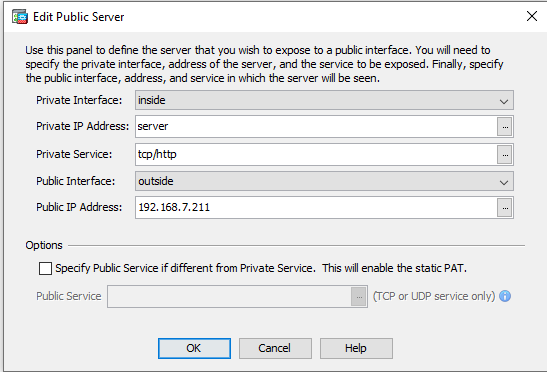


Рисунок 59 ­– Настройка Public Server

Теперь при переходе по указанному внешнему адресу, должен открываться веб-сайт. (рисунок 60)

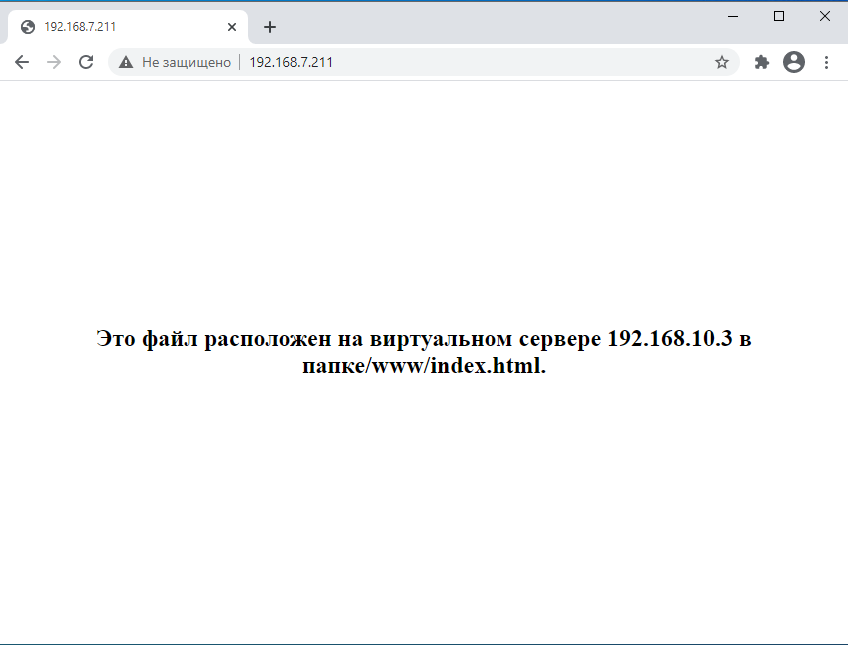


Рисунок 60 ­– Открытый веб-сайт через второй способ

* 1. **Сброс пароля для входа в привилегированный режим с сохранением конфигурации**

Бывает, что пароль был забыт или утерян, либо новый системный администратор его не знает, но необходимо внести изменения в конфигурацию устройства, а без пароля этого сделать невозможно и необходимо его сбросить, при этом не сбрасывать настройки межсетевого экрана.

Для это нужно подключить Cicso ASA консольным кабелем к ПК и открыть программу PuTTY и при включении устройства нажимать клавишу ESC. Должно открыться меню ROMmon. Далее нужно ввести команду confreg 0x41, которая указывает устройству не загружать файл конфигурации при старте и продолжить запуск командой boot. (рисунок 61)

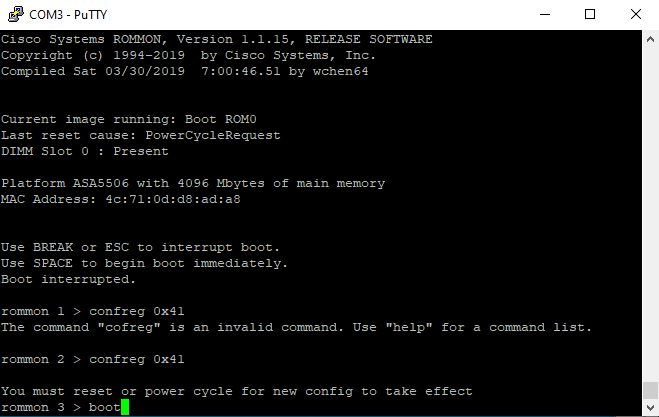


Рисунок 61 ­– режим rommon

После запуска будут применены заводские настройки. (рисунок 62)

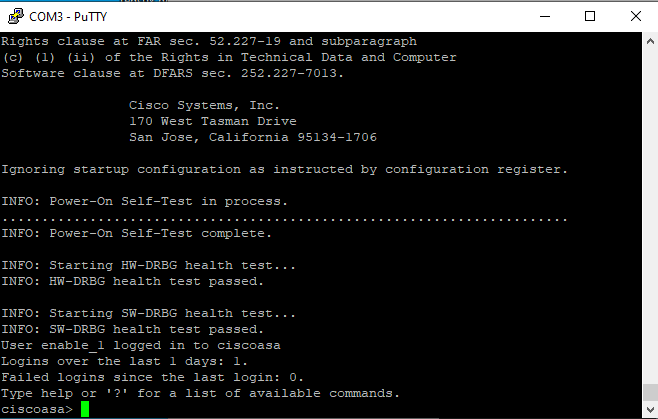


Рисунок 62 ­– Заводские настройки

Необходимо скопировать настройки из файла стартовой конфигурации в текущую, установить новый пароль на привилегированный режим и изменить параметр запуска по умолчанию. Сохранить текущую конфигурацию и перезагрузить устройство. (рисунки 63-65)

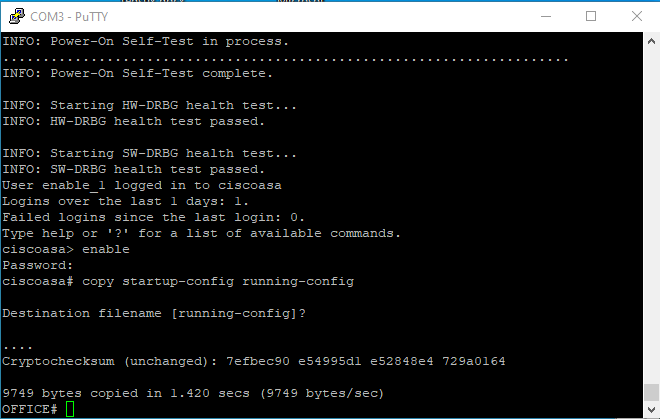


Рисунок 63 ­– Копирования стартовых настроек

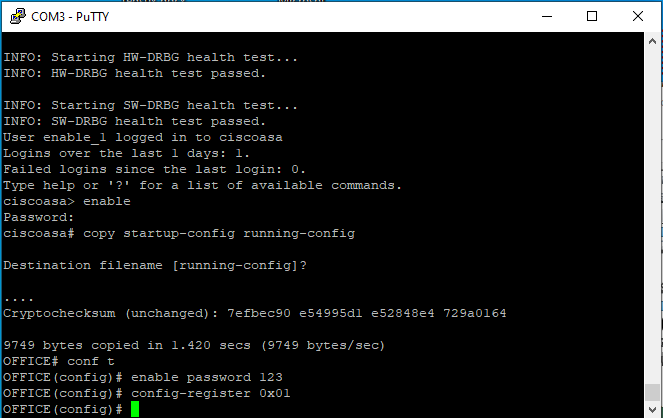


Рисунок 64 ­– Изменение пароля и параметра запуска

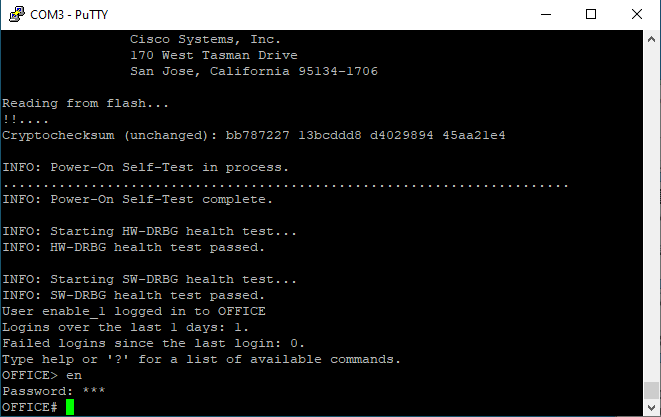


Рисунок 65 ­– Перезагрузка и проверка нового пароля

1. **Администрирование 1С: Предприятие**
   1. **Создание виртуальной машины VMware**

Для создания виртуальной машины нужно запустить программу VMware и создать новую виртуальную машину для операционной системы Windows 7. (рисунок 66)

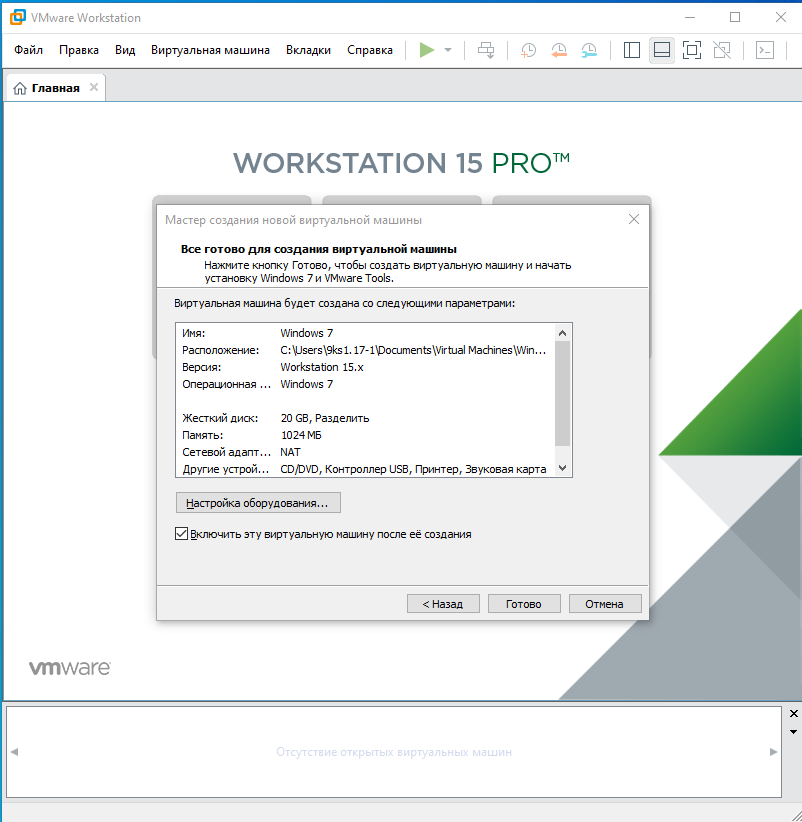


Рисунок 66 ­– Настройки виртуальной машины

Устанавливаем операционную систему Windows 7. (рисунок 67)

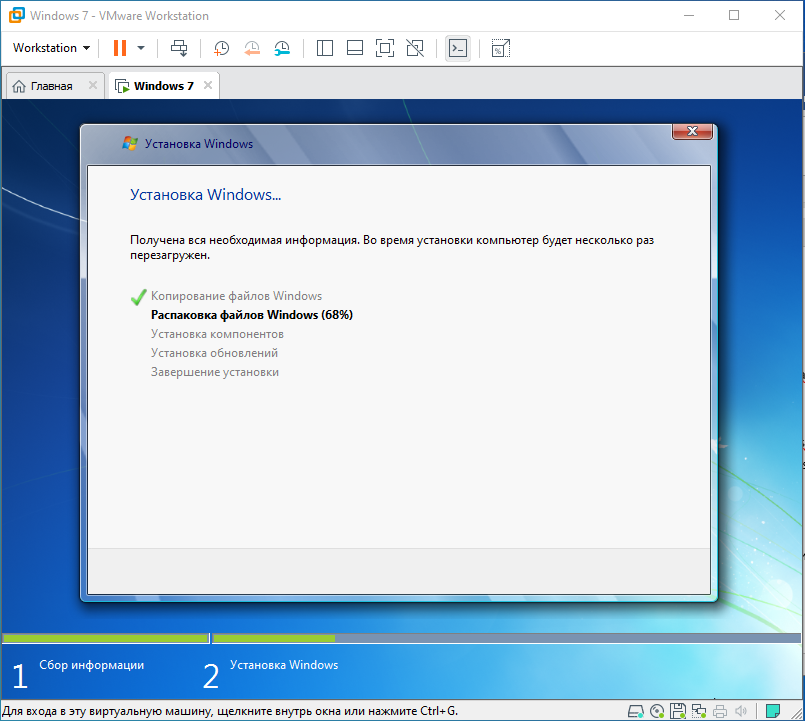


Рисунок 67 ­– Установка операционной системы

* 1. **Установка 1С:Предприятие**

«1С:Предприятие» предназначено для автоматизации бухгалтерского и управленческого учётов (включая начисление зарплаты и управление кадрами), экономической и организационной деятельности предприятия.

Для установки нужно запустить установщик и следовать его командам. При выборе компонентов, нужно отметить 1С:Предприятие – Тонкий клиент и Сервер 1С:Предприятие (рисунок 68)

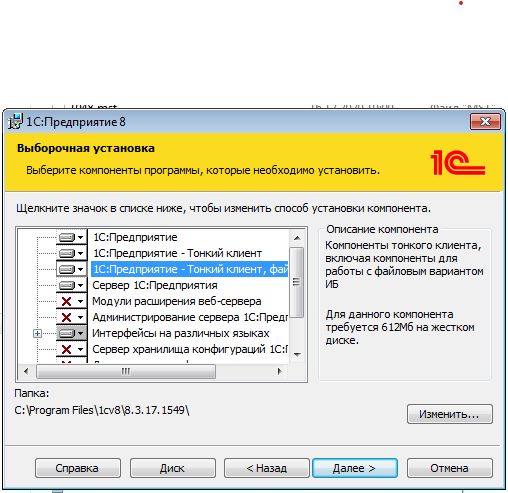


Рисунок 68 ­– Выбор компонентов 1С

При установке может возникнуть ошибка. (рисунок 69)

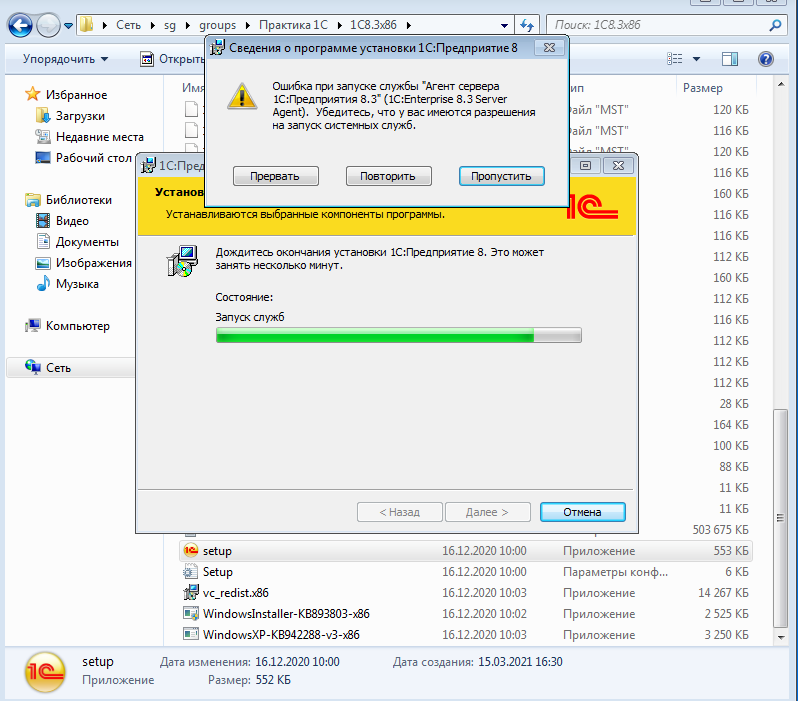


Рисунок 69 ­– Ошибка при установке

Для её решения нужно открыть Службы, выбрать службу Агент сервера 1С:Предприятия. Перейти на вкладку Вход в систему и выбрать Вход в систему С системной учетной записью. (рисунок 70)

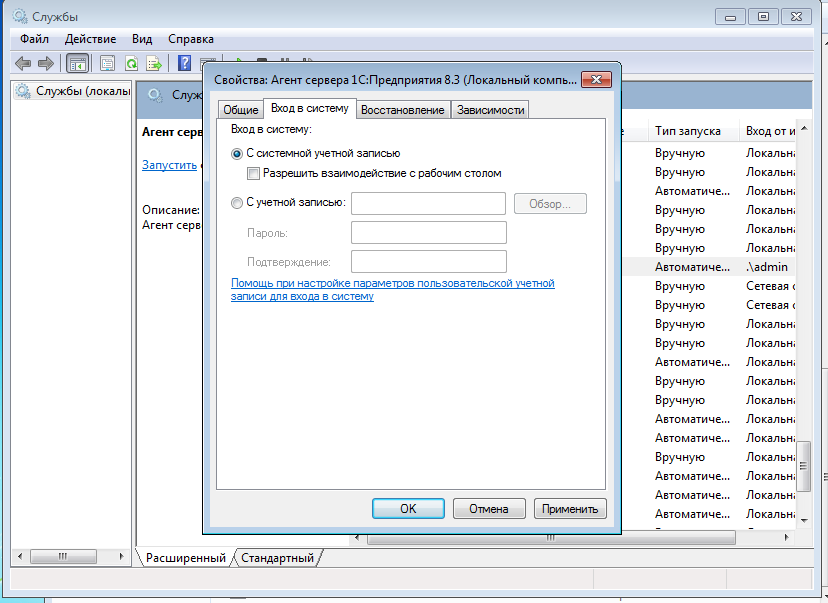


Рисунок 70 ­– Решение ошибки

После этого нажимаем кнопку Повторить и установка успешно завершается. (рисунок 71)

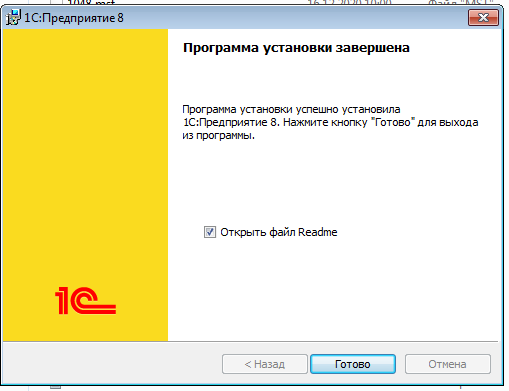


Рисунок 71 ­– Установка завершена

* 1. **Установка конфигурацию для 1C:Предприятия**

Для установки конфигурации AccountingBase 3.0.59.45 нужно запустить установщик и нажать кнопку Далее. (рисунок 72)

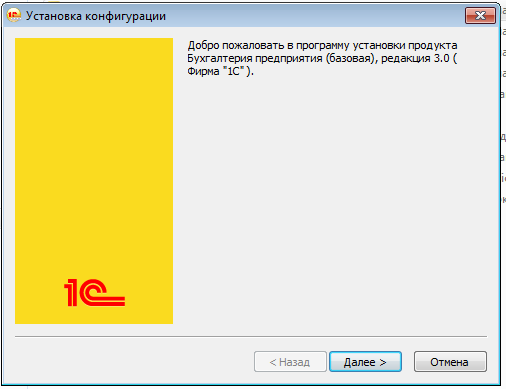


Рисунок 72 ­– Установка конфигурации

Далее нужно выбрать место установки конфигурации и нажать Далее. (рисунок 73)

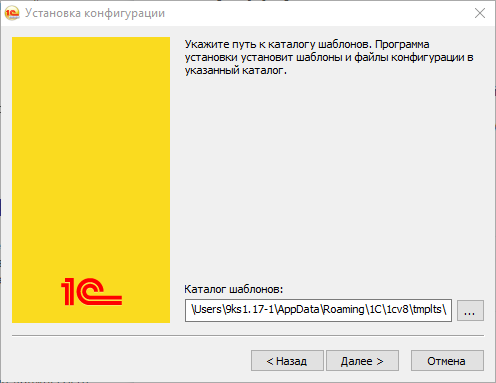


Рисунок 73 ­– Выбор директории для установки

Нужно подождать и установка завершиться. (рисунок 74)

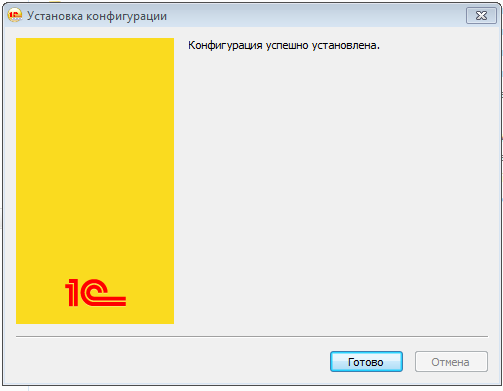


Рисунок 77 ­– Установка завершена

* 1. **Добавление информационных баз в 1C:Предприятие**

Для добавления информационной базы нужно переместить их на локальный диск. (рисунок 78)

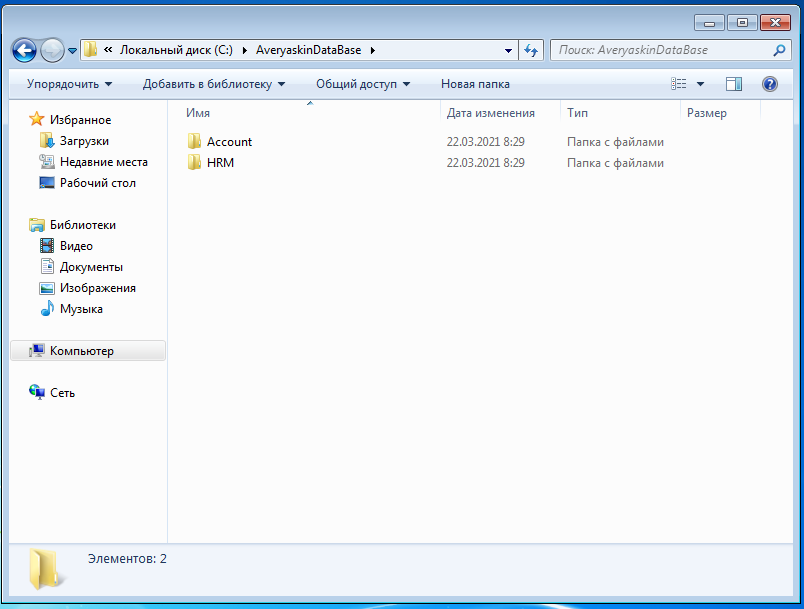


Рисунок 78 ­– Информационные базы на диске

В программе 1С:Предприятие нажать Добавить, указать название и выбрать папку информационной базы. (рисунок 79)

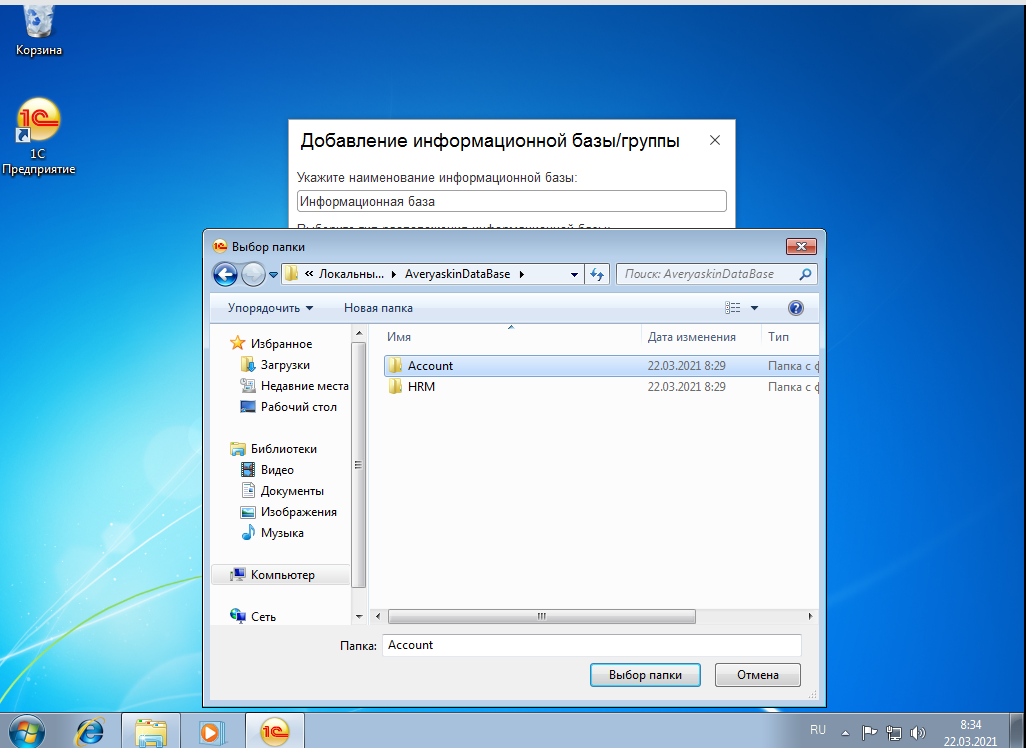


Рисунок 79 ­– Выбор папки

* 1. **Применение фильтров в Журнале регистрации**

Журнал регистрации содержит информацию о том, какие события происходили в информационной базе в определенный момент времени или какие действия выполнял тот или иной пользователь. С помощью различных фильтров можно просматривать только нужную информацию.

Чтобы открыть Журнал регистрации нужно нажать правой кнопкой по информационной базе и выбрать пункт Конфигуратор. (рисунок 80)

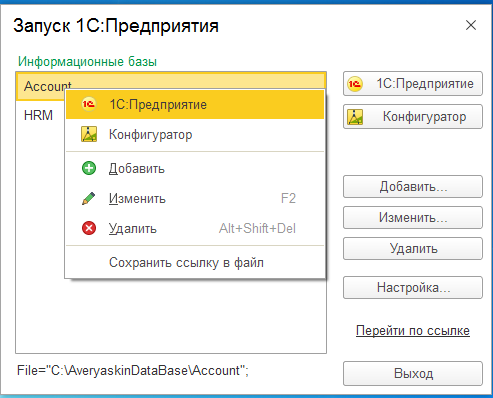


Рисунок 80 ­– Выбор информационной базы

Откроется окно Конфигуратор, на вкладке Администрирование выбрать Журнал регистрации. (рисунок 81)

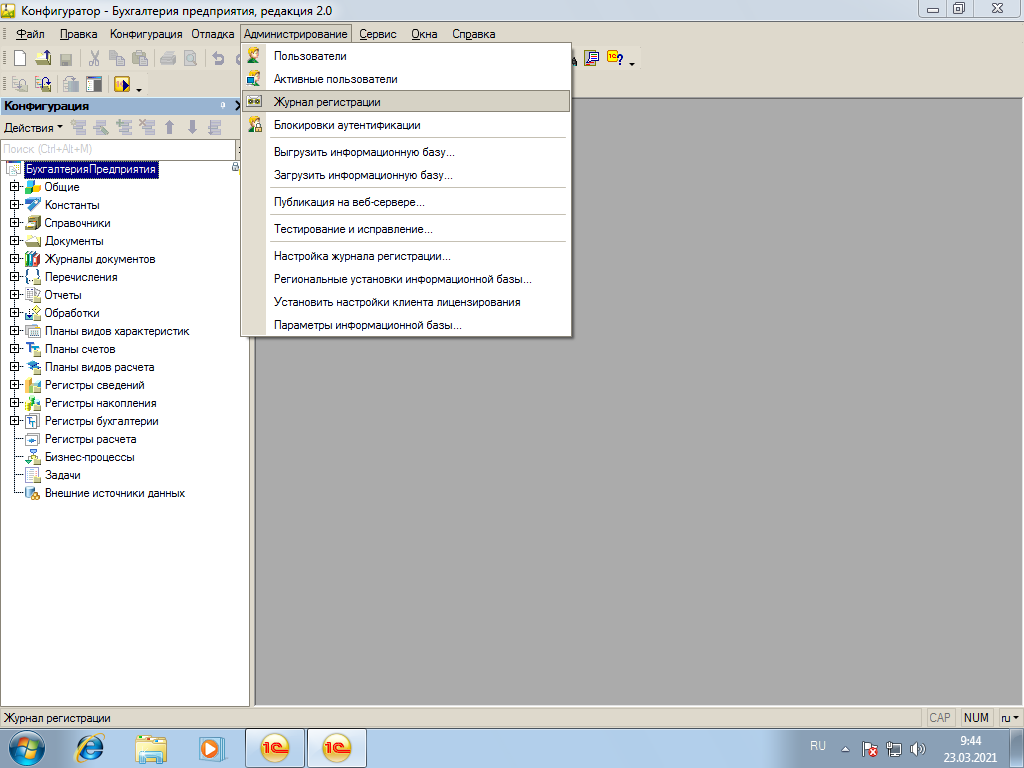


Рисунок 81 ­– Запуск Журнала регистрации

Откроется Журнал регистрации. (рисунок 82) Для применения фильтра нужно нажать кнопку Установить отбор (рисунок 83)

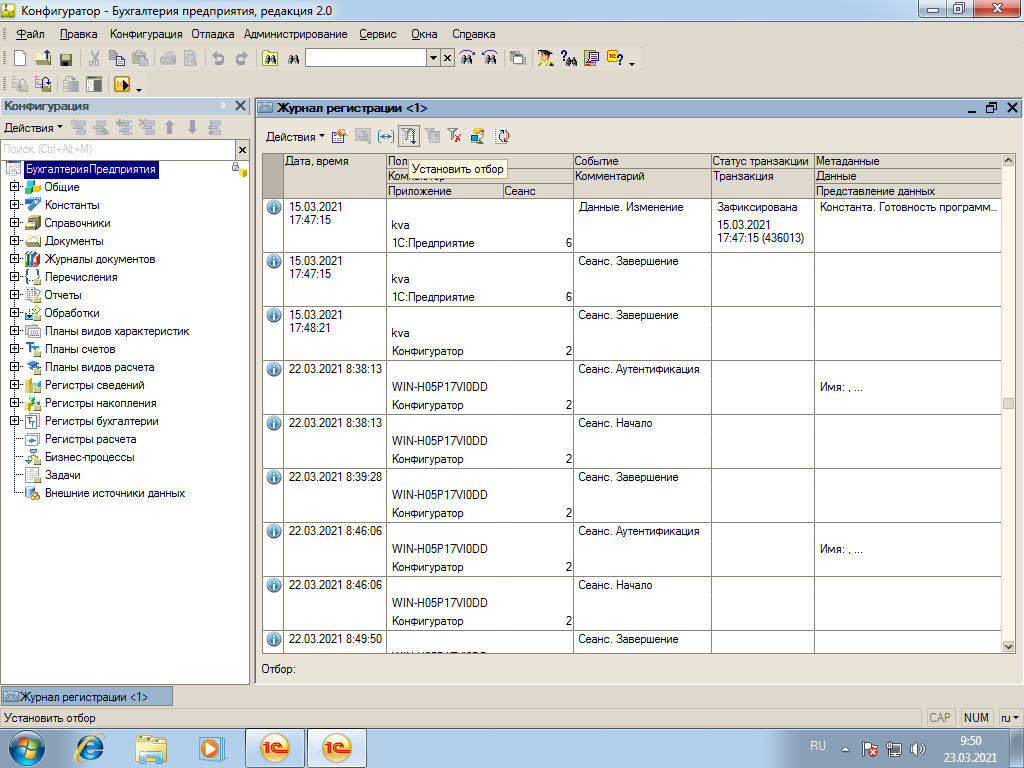


Рисунок 81 ­– Запуск Журнала регистрации

Откроется окно, в котором можно выбрать различные фильтры. (рисунок 82)

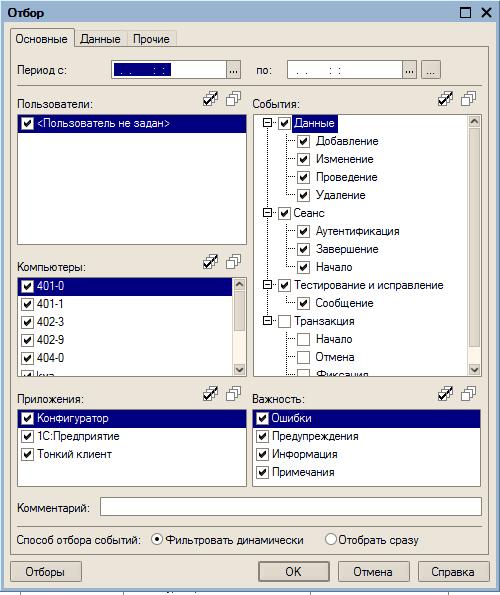


Рисунок 82 ­– Окно отбора

С помощью фильтров покажем события только за 2016. (рисунок 83)

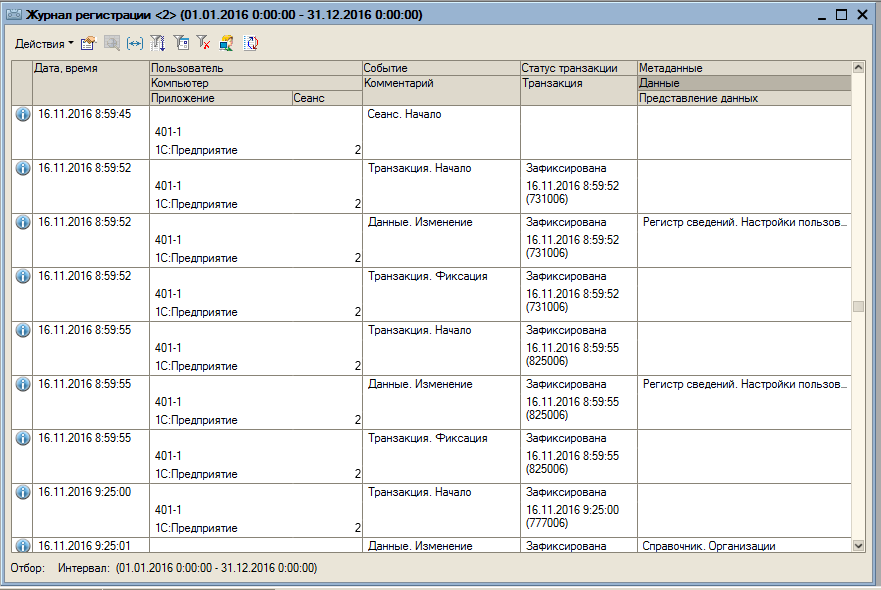


Рисунок 83 ­– События за 2016 год

С помощью фильтров покажем события только за 2016 и выполнявшиеся за компьютером KVA3. (рисунок 84)

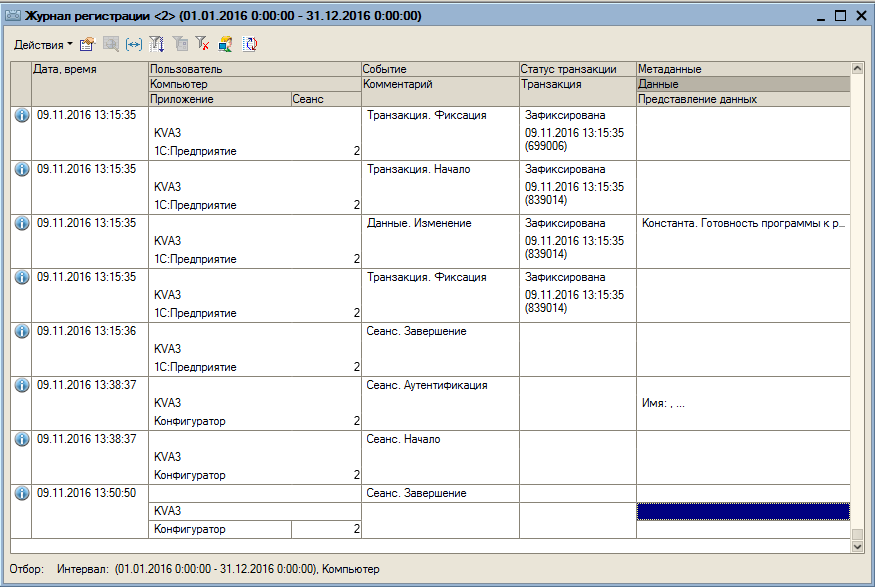


Рисунок 84 ­– События за 2016 год и ПК KVA3

* 1. **Выгрузка конфигурации информационной базы в файл**

Чтобы выгрузить конфигурацию в файл нужно нажать правой кнопкой по информационной базе и выбрать пункт Конфигуратор. (рисунок 80)

На вкладке Конфигурация выбрать пункт Сохранить конфигурацию в файл. (рисунок 85)

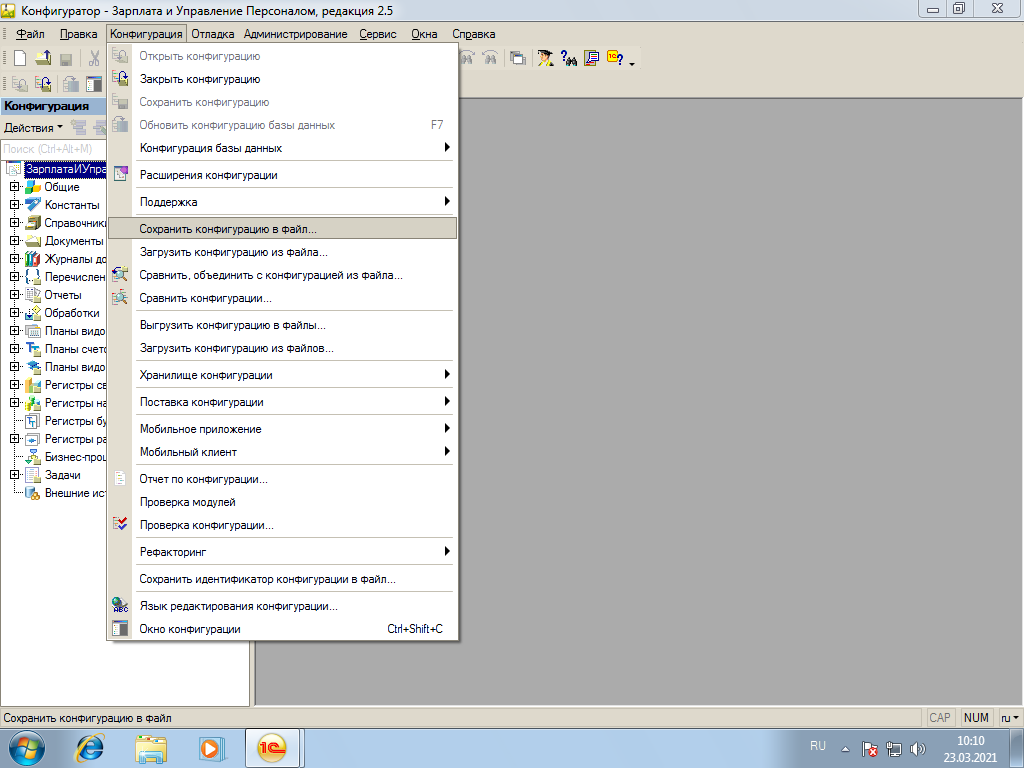


Рисунок 85 ­– Сохранение конфигурации в файл

Откроется окно, в котором нужно выбрать место сохранения файла. (рисунок 86)

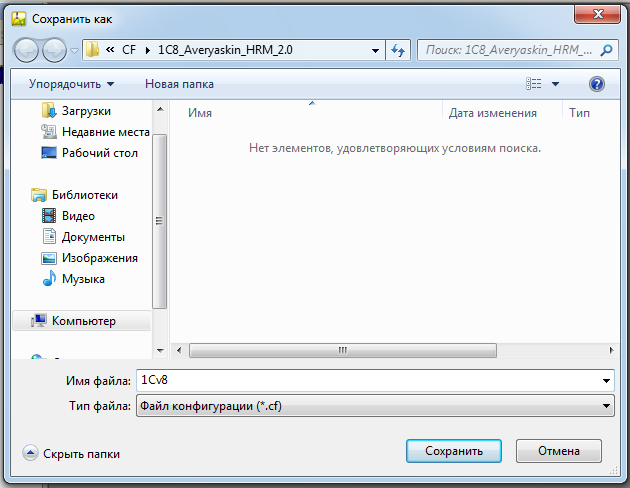


Рисунок 86 ­– Выбор места

После нажатия кнопки Сохранить, откроется окно с результатом. (рисунок 87)

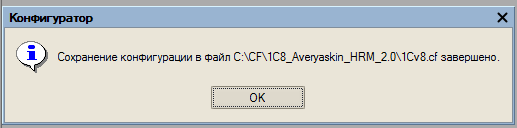


Рисунок 87 ­– Результат сохранения

* 1. **Создание информационную базу данных из шаблона**

Для создания информационной базы нужно в программе 1С:Предприятие нажать Добавить, выбрать пункт Создание новой информационной базы, выбрать шаблон 3.0.59.45, указать название и выбрать папку информационной базы. (рисунки 88-90)

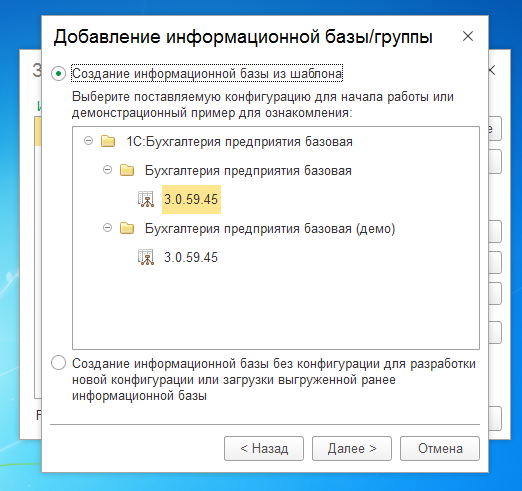


Рисунок 88 ­– Выбор шаблона

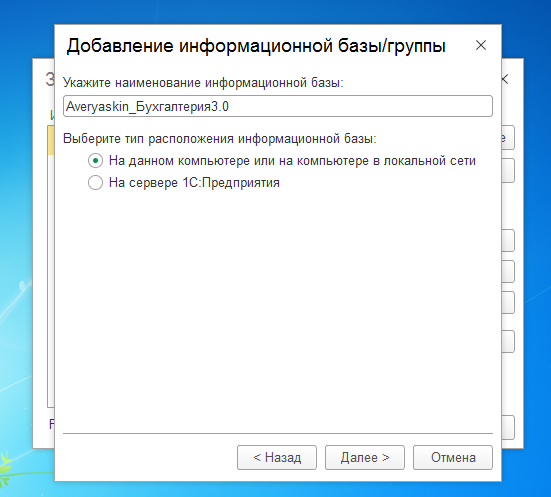


Рисунок 89 ­– Имя базы

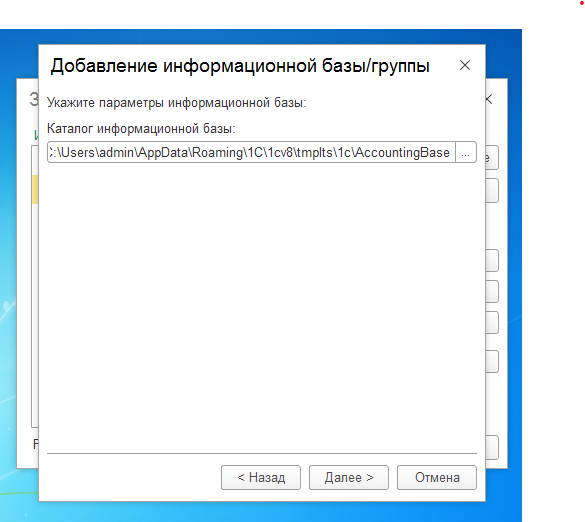


Рисунок 90 ­– Указание информационной базы

* 1. **Создание новых пользователей**

Чтобы создать новых пользователей нужно нажать правой кнопкой по информационной базе и выбрать пункт Конфигуратор. (рисунок 80)

На вкладке Администрирование выбрать пункт Пользователи (рисунок 91)

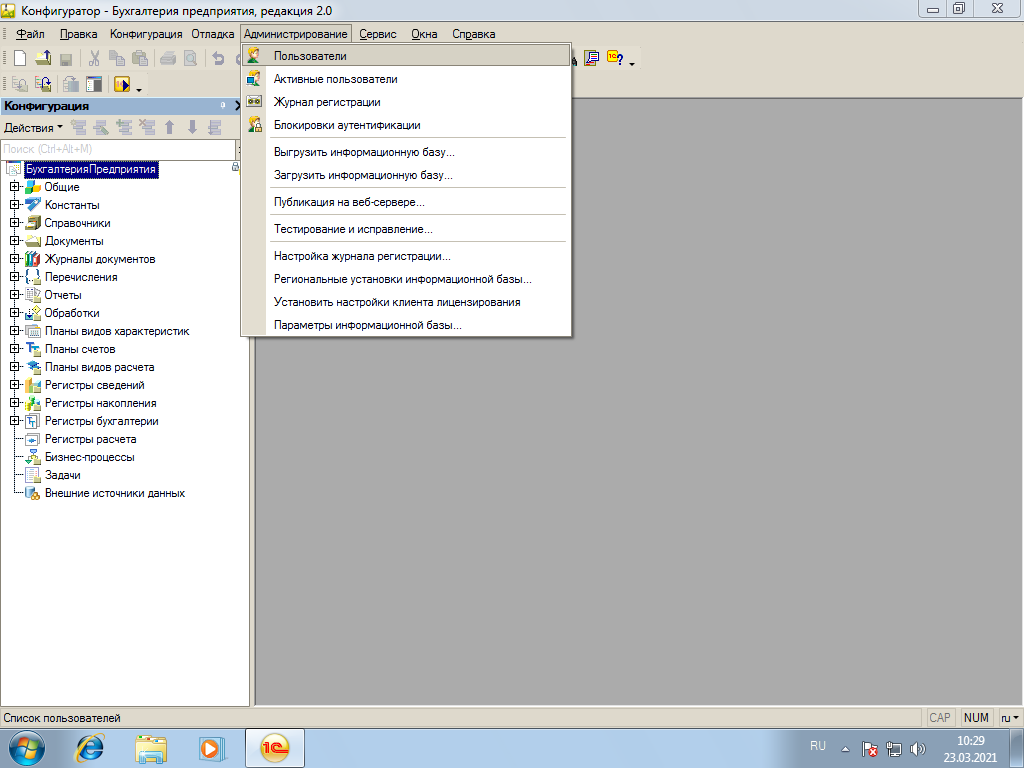


Рисунок 91 ­– Пункт Пользователи

Откроется окно Пользователи и нажать Добавить. (рисунок 92)

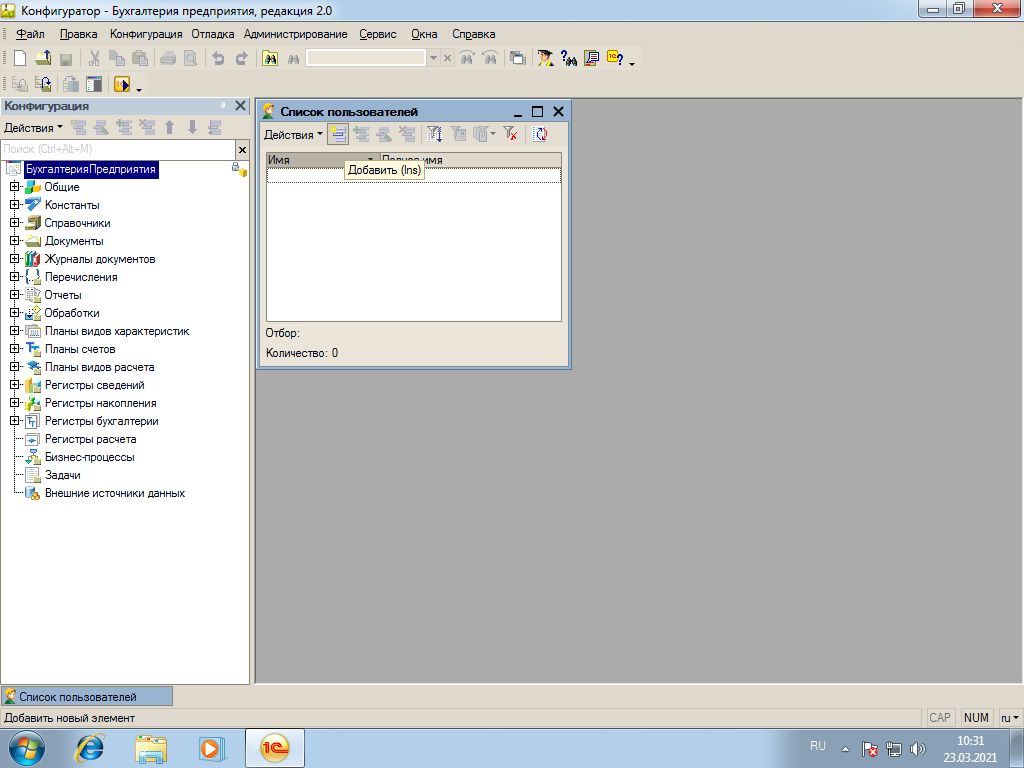


Рисунок 92 ­– Окно Пользователи

Откроется окно добавления пользователя, укажите имя, пароль и в вкладке Прочее указать права (рисунок 93)

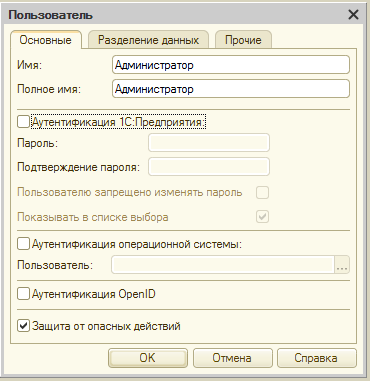


Рисунок 93 ­– Добавление пользователи

После добавление пользователя он отобразится в списке. (рисунок 94)

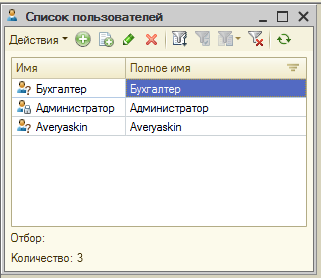


Рисунок 94 ­– Список пользователей

* 1. **Загрузка конфигурации из файла**

Чтобы загрузить конфигурацию из файла нужно нажать правой кнопкой по информационной базе и выбрать пункт Конфигуратор. (рисунок 80)

На вкладке Конфигурация выбрать пункт Загрузить конфигурацию из файла. (рисунок 95)



Рисунок 95 ­– Загрузка конфигурации из файла

Выбираем файл из которого будем загружать конфигурацию. (рисунок 96)

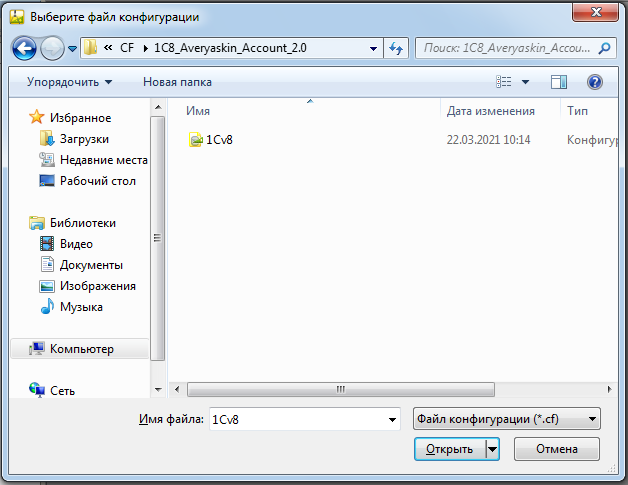


Рисунок 96 ­– Выбор файла конфигурации

Появляется предупреждение, что текущая конфигурация не пустая. (рисунок 97)

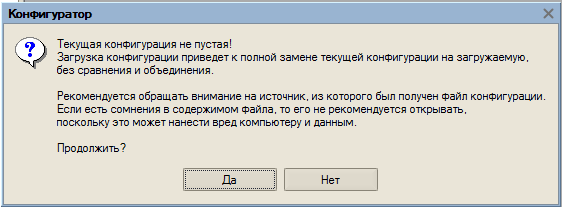


Рисунок 97 ­– Предупреждение

Через некоторое время должно появится сообщение об успешном окончании операции. (рисунок 98)

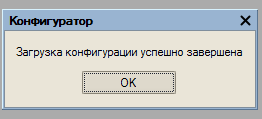


Рисунок 98 ­– Загрузка завершена

* 1. **Выгрузка информационной базы**

Чтобы выгрузить информационной базы нужно нажать правой кнопкой по информационной базе и выбрать пункт Конфигуратор. (рисунок 80)

В вкладке Администрирование выбрать пункт Выгрузить информационную базу. (рисунок 99)

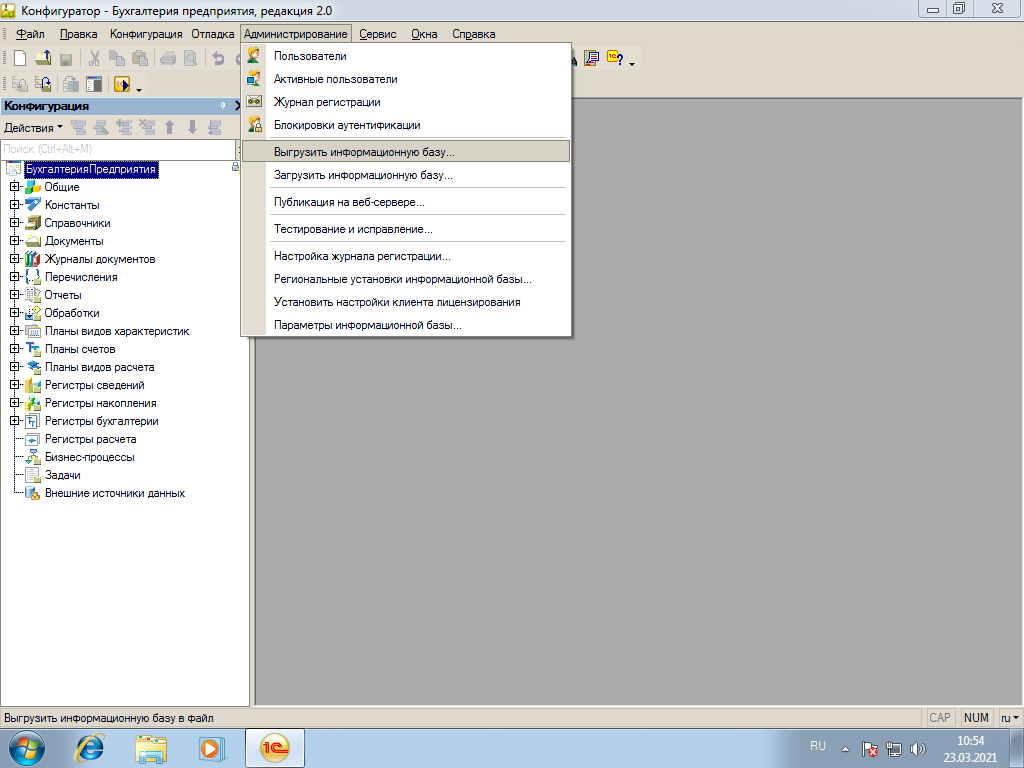


Рисунок 99 ­– Выгрузка информационной базы

Откроется окно выбора места сохранения информационной базы. (рисунок 100)

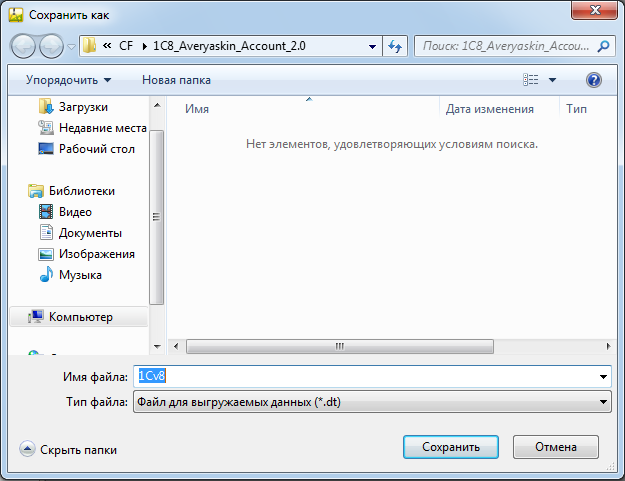


Рисунок 100 ­– Выбор места

Появиться окно об завершении выгрузки информационной базы. (рисунок 101)

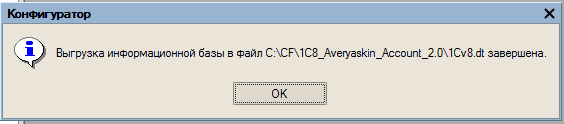


Рисунок 101 ­– Выгрузка завершена

* 1. **Загрузка информационной базы**

Чтобы загрузить информационной базы нужно нажать правой кнопкой по информационной базе и выбрать пункт Конфигуратор. (рисунок 80)

В вкладке Администрирование выбрать пункт Загрузить информационную базу. (рисунок 99)

Откроется окно выбора копии информационной базы. (рисунок 102)

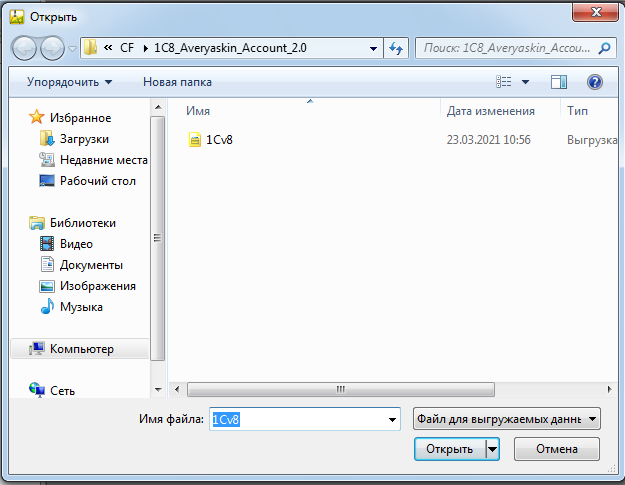


Рисунок 102 ­– Выбор копии

Появится предупреждение о закрытии информационной базы. (рисунок 103)

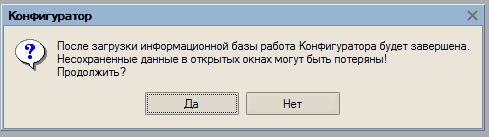


Рисунок 103 ­– Предупреждение

Появится окно об успешной загрузке информационной базы. (рисунок 104)

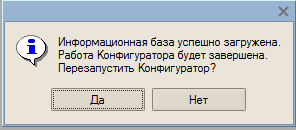


Рисунок 104 ­– Сообщение о завершении

* 1. **Тестирование информационной базы**

Чтобы загрузить информационной базы нужно нажать правой кнопкой по информационной базе и выбрать пункт Конфигуратор. (рисунок 80)

В вкладке Администрирование выбрать пункт Тестирование и исправление. (рисунок 99)

Появится предупреждение, что рекомендуется сделать резервную копию информационной базы. (рисунок 105)



Рисунок 105 ­– Предупреждение

Откроется окно, в котором надо выбрать Проверки и режимы и нажать кнопку Выполнить. (рисунок 106)

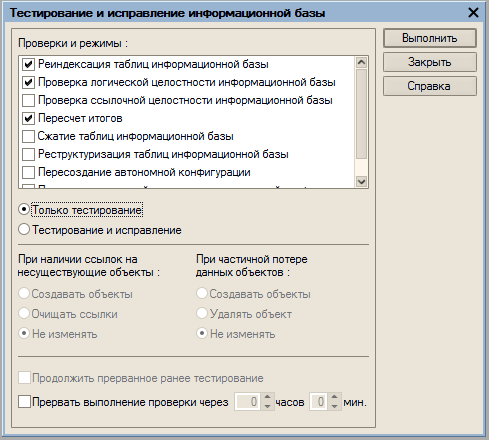


Рисунок 106 ­– Выбор пунктов тестирования

После нажатия кнопки Выполнение начнется тестирование. (рисунок 107)

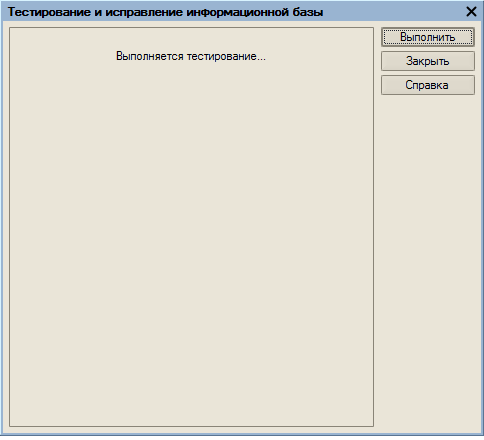


Рисунок 107 ­– Тестирование идет

В конце появится сообщение, что тестирование закончено. (рисунок 108)

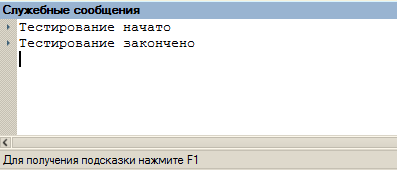


Рисунок 108 ­– Тестирование закончено

# ЗАКЛЮЧЕНИЕ

В результате прохождения учебной практики поставленные цели были достигнуты, а именно:

* изучена Охраны труда и техника безопасности при работе с компьютером;
* изучено программное обеспечение компьютерных сетей:

1. Командной строки Windows;
2. wireshark;
3. NetEmul;
4. MS Office Visio.

Были выполнены в полном объеме следующие задачи:

* + на практике использованы встроенные сетевые утилиты Windows, такие как ipconfig, ping, traceroute, nslookup и arp в Командной строке;
  + изучен интерфейс программы Wireshark, была рассмотрена возможность применения нужных фильтров, изучена структура запросов и ответов протоколов HTTP и DNS;
  + изучен интерфейс программы NetEmul, изучены функции каждого устройства в программе, создана схему компьютерной сети и проверена её работоспособность;
  + изучен интерфейс программы MS Office Visio, изучены присутствующие шаблоны программы, изучены присутствующие фигуры в программе, создана схема компьютерной сети;
  + изучены правила техники безопасности при работе с компьютером и нормы охраны труда в РФ.

# БИБЛИОГРАФИЧЕСКОЕ ОПИСАНИЕ

1. Исаченко, О.В. Программное обеспечение компьютерных сетей /О.В. Исаченко; Беляева Т. Г. — ИНФРА-М, 2012. —
2. Лисьев, Г.А. Программное обеспечение компьютерных сетей и web-серверов /Г.А. Лисьев, Ю.И. Аскерко, П.Ю. Романов; Беляева Т. Г. — ИНФРА-М, 2019. — 145с.
3. Техника безопасности и правила поведения в кабинете информатики [Электронный ресурс] /. — Электрон. журн. — Режим доступа: https://izotop.jimdofree.com/разделы-икт/техника-безопасности/, свободный;
4. Техника безопасности [Электронный ресурс] /. — Электрон. текстовые дан. — Режим доступа: https://ru.wikipedia.org/wiki/Техника\_безопасности, свободный;
5. Служба охраны труда образовательного учреждения и ее функции [Электронный ресурс] /. — Электрон. текстовые дан. — Режим доступа: https://lektsii.com/1-43278.html, свободный;
6. Требования к системе управления охраной труда [Электронный ресурс] /. — Электрон. текстовые дан. — Режим доступа: http://www.znakcomplect.ru/trebovaniya-k-sisteme-upravleniya-ohranoy-truda.php, свободный;
7. Охрана труда - основные понятия и разъяснения [Электронный ресурс] /. — Электрон. текстовые дан. — Режим доступа: https://git87.rostrud.ru/poleznaya\_informatsiya/118679.html, свободный;
8. Программное обеспечение компьютерных сетей [Электронный ресурс] /. — Электрон. текстовые дан. — Режим доступа: https://studfile.net/preview/1105825/, свободный;