

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт
Факультет приборостроения
Информационных технологий и
электроники

Кафедра
«Информационная безопасность
систем и технологий»

Специальность 10.05.03

Информационная безопасность
автоматизированных систем

Специализация

Защищенные автоматизированные
системы управления

ДИПЛОМНЫЙ ПРОЕКТ

на тему

ПРАКТИКУМ ПО АДМИНИСТРИРОВАНИЮ СИСТЕМЫ ЗАЩИТЫ СРЕДЫ
ВИРТУАЛИЗАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА НА
ОСНОВЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ VGATE.

Студент		Деревягин Роман Евгеньевич
Руководитель		А.Г. Фатеев
Нормоконтролёр		А.Г. Фатеев
Рецензент	ведущий инженер АО «ПНИЭИ» Е.А. Анапьев	

Работа допущена к защите (протокол заседания кафедры от 15.06.20 № 13)
Заведующий кафедрой  С.Л. Зефирова

Работа защищена с отметкой хорошо (протокол заседаний ГЭК
от 25.06.20 № 2)
Секретарь ГЭК  А.П. Иванов

Пенза 2020

Оглавление

Введение.....	6
1 Обзор программно-аппаратных средства защиты среды виртуализации от несанкционированного доступа.....	7
2 Анализ возможности применения программно-аппаратных средств защиты среды виртуализации от несанкционированного доступа.....	9
3 Создание виртуальных машин, входящих в состав стенда.....	14
3.1 Краткое описание ВМ и структуры стенда.....	14
3.2 Создание ВМ с установленной гостевой ОС Windows Server 2012 R2, являющейся контроллером домен.....	15
3.3 Создание ВМ с установленной гостевой ОС Windows Server 2012 R2, являющейся сервером авторизации.....	38
3.4 Создание ВМ с установленной гостевой ОС Windows 8.1, являющейся рабочим местом администратора виртуальной инфраструктуры...43	
3.5 Создание ВМ с установленным гипервизором Hyper-V Server 2012 R2, являющейся сервером виртуализации.....	47
4 Создание и конфигурирование локальной сети, состоящей из виртуальных машин.....	55
4.1 Проверка работоспособности сети до создания домена.....	55
4.2 Установка роли контроллера домена.....	59
4.3 Создание домена.....	65
4.4 Результаты создания локальной сети.....	72
5 Установка СЗИ vGate.....	73
5.1 Установка сервера авторизации.....	73
5.2 Установка агента аутентификации.....	79
5.3 Результат создания стенда.....	83
6 Порядок выполнения практического задания: «Управление виртуальной инфраструктурой и безопасностью виртуальной инфраструктуры при использовании СЗИ vGate».....	85

6.1	Общие сведения о СЗИ vGate.....	85
6.2	Создание учетных записей администраторов.....	85
6.3	Управление учетными записями пользователей.....	89
6.4	Настройка прав на управление виртуальной инфраструктурой и управление информационной безопасностью с проверкой возможности применения этих прав.....	91
6.5	Управление политиками безопасности.....	94
6.6	Регистрация событий информационной безопасности.....	96
6.7	Управление режимами работы vGate.....	98
6.8	Мониторинг безопасности.....	100
6.9	Базовый и повышенные уровни сложности задания «Управление виртуальной инфраструктурой и безопасностью виртуальной инфраструктуры при использовании СЗИ vGate».....	108
7	Порядок выполнения практического задания: «Управление доступом к ресурсам виртуальной инфраструктуры и контроль целостности, реализуемые СЗИ vGate».....	109
7.1	Аутентификация.....	109
7.2	Управление доступом к защищаемым серверам.....	111
7.3	Настройка полномочного управления доступом к конфиденциальным ресурсам. Настройка с помощью консоли. Настройка меток безопасности. Проверка с имитацией попыток доступа к ресурсам.....	115
7.4	Контроль целостности и доверенная загрузка.....	122
7.5	Регистрация событий информационной безопасности.....	125
7.6	Базовый и повышенные уровни сложности задания «Управление доступом к ресурсам виртуальной инфраструктуры и контроль целостности, реализуемые СЗИ vGate».....	127
8	Описание порядка выполнения заданий практикума и результатов выполнения заданий.....	128

8.1	Описание порядка выполнения практического задания по управлению виртуальной инфраструктурой и безопасностью виртуальной инфраструктуры при использовании СЗИ vGate.....	128
8.2	Описание порядка выполнения практического задания по управлению доступом к ресурсам виртуальной инфраструктуры и контролю целостности, реализуемые СЗИ vGate.....	130
9	Описание структуры и содержания отчета о выполнении практических заданий.....	132
9.1	Структура и содержание отчета о выполнении практических заданий.....	132
9.2	Содержание отчета о выполнении практической работы «Управление виртуальной инфраструктурой и безопасностью виртуальной инфраструктуры при использовании СЗИ vGate».....	132
9.3	Содержание отчета о выполнении практической работы «Управление доступом к ресурсам виртуальной инфраструктуры и контроль целостности, реализуемые СЗИ vGate».....	134
10	Определение порядка контроля выполнения практического задания	136
11	Подготовка сценариев для автоматизированного развертывания виртуальных машин.....	137
12	Вредные психофизиологические факторы, влияющие на сердечно-сосудистую систему специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие.....	139
12.1	Вредные психофизиологические факторы, влияющие на сердечно-сосудистую систему специалиста по защите информации.....	139
12.2	Методы и средства физической культуры, снижающие их воздействие.....	140
	Заключение	144
	Список используемых источников.....	146

Приложение А Состав виртуального стенда, использующегося при выполнении практикума.....	148
Приложение Б UML – диаграмма последовательности действий выполнения практических заданий.....	150
Приложение В Структура отчета о выполнении практических заданий.....	153
Приложение Г Порядок контроля выполнения практических заданий.....	155
Приложение Д Сценарии автоматизированного развертывания виртуальных машин.....	157
Приложение Е Протокол проверки ВКР в системе Антиплагиат.....	166

Введение

Технологии виртуализации в последнее время получают все большее распространение, так как позволяют более эффективно и рационально использовать вычислительные ресурсы. При этом сохраняется привычная функциональность устройств и появляются преимущества по сравнению с традиционной физической средой.

Современные технологии виртуализации в своем составе содержат компоненты защиты, но они неспособны нейтрализовать весь спектр современных угроз, в частности, несанкционированный доступ к информации, а также не могут полностью выполнить требования законодательства в области обеспечения информационной безопасности. Это приводит к необходимости использования специальных средств защиты, предназначенных для использования в виртуальных инфраструктурах.

Выпускная квалификационная работа посвящена применению средства защиты среды виртуализации vGate. Тема была сформулирована следующим образом «Практикум по администрированию системы защиты среды виртуализации от несанкционированного доступа на основе средства защиты информации vGate».

Актуальность темы выпускной квалификационной работы обуславливается тем, что в настоящее время в различных компаниях и государственных организациях все больше используются технологии виртуализации. Для защиты виртуальных инфраструктур необходимо применять специальные средства защиты информации. Их применение требует от администратора соответствующих знаний и практических навыков, включая навыки по развертыванию таких средств защиты. Для получения таких знаний и навыков требуется использовать необходимые обучающие средства, которые будут подготовлены в рамках выполнения ВКР.

1 Обзор программно-аппаратных средств защиты среды виртуализации от несанкционированного доступа

В настоящее время в Государственном реестре сертифицированных средств защиты информации есть сведения о двух средствах защиты от несанкционированного доступа применяемыми для защиты виртуальных инфраструктур являются – vGate от компании «Код безопасности» [1] и ПАК Аккорд-В. от компании «ОКБ САПР»[2].

СЗИ vGate является сертифицированным средством защиты платформ виртуализации на базе VMware vSphere, Microsoft Hyper-V и Скала-Р. Продукт обеспечивает защиту от специфических угроз виртуализации, позволяет контролировать действия администраторов виртуальной инфраструктуры и осуществляет фильтрацию трафика на уровне гипервизора.

vGate предназначен для решения следующих задач:

- разграничение доступа к управлению виртуальной инфраструктурой;
- контроль действий привилегированных пользователей;
- контроль целостности виртуальных машин;
- регистрация и мониторинг событий безопасности виртуальной инфраструктуры;
- фильтрация сетевого трафика на уровне гипервизора;
- выполнение требований и рекомендаций по защите виртуальной инфраструктуры.

СЗИ vGate имеет сертификат соответствия ФСТЭК РФ №2308, который подтверждает соответствие требованиям руководящих документов в части защиты от несанкционированного доступа – по 5 классу защищенности (СВТ5) и контроля отсутствия недеklarированных возможностей – по 4 уровню контроля (НДВ4), а также может использоваться в АС до класса защищенности 1Г включительно и для защиты информации в ИСПДн до 1 уровня

включительно, ГИС до 1 класса включительно[3].

Кроме СЗИ vGate в реестре ФСТЭК есть сведения о сертификате, выданном ПАК Аккорд-В. Программно-аппаратный комплекс Аккорд-В. предназначен для защиты инфраструктуры виртуализации VMware vSphere 4.1, VMware vSphere 4.0 и VMware Infrastructure 3.5.

ПАК Аккорд-В. обеспечивает защиту всех компонентов среды виртуализации: ESX (ESXi) - серверов и самих виртуальных машин, серверов управления vCenter и дополнительных серверов со службами VMware (например, VMware Consolidated Backup).

ПАК Аккорд-В предназначен для решения следующих задач:

- доверенная загрузка и контроль целостности всех элементов инфраструктуры виртуализации;
- разграничение доступа администраторов виртуальной инфраструктуры и администраторов безопасности информации;
- разграничение доступа пользователей внутри виртуальных машин;
- аппаратная идентификация всех пользователей и администраторов инфраструктуры виртуализации.

ПАК Аккорд-В. имеет сертификат Соответствия ФСТЭК РФ №2308 который подтверждает соответствие требованиям руководящих документов в части защиты от несанкционированного доступа – по 3 классу защищенности и технических условий (СВТЗ, ТУ) и контроля отсутствия недеklarированных возможностей – по 2 уровню контроля (НДВ2).

2 Анализ возможности применения программно-аппаратных средств защиты среды виртуализации от несанкционированного доступа

С целью выполнения анализа возможности применения программно-аппаратных средств защиты среды виртуализации от НСД были рассмотрены два приказа ФСТЭК [4] [5]. При этом была проведена оценка возможности применения ПАСЗИ от НСД для реализации мер защиты среды виртуализации, указанных в приказах ФСТЭК.

ЗСВ.1 Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации.

В vGate реализована модель разделения прав на управление виртуальной инфраструктурой и на управление безопасностью. Таким образом, выделяются две основные роли – это администратор виртуальной инфраструктуры (АВИ) и администратор информационной безопасности (АИБ).

Доступ на управление виртуальной инфраструктурой или параметрами безопасности предоставляется только аутентифицированным пользователям. Причем процедура аутентификации пользователей и компьютеров (рабочих мест АИБ и АВИ) осуществляется по протоколам, нечувствительным к попыткам перехвата паролей и атакам типа Man in the Middle.

Для обеспечения защиты средств управления виртуальной инфраструктурой применяется функционал дискреционного разграничения доступа к объектам, которые размещены внутри защищаемого периметра. Правила разграничения доступа работают на основе заданных ACL и параметров соединения (протоколов, портов). Сетевой трафик между аутентифицированными субъектами и защищаемыми объектами подписывается, тем самым обеспечивается защита от атак типа Man in the Middle в процессе сетевого взаимодействия.

В Аккорд-В. реализован механизм аппаратной идентификации и

парольной аутентификации всех пользователей и администраторов инфраструктуры виртуализации.

ЗСВ.2 Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин.

В vGate реализован мандатный принцип контроля доступа на основе меток конфиденциальности. При выполнении ряда стандартных операций с объектами виртуальной инфраструктуры осуществляется сравнение меток безопасности учетных записей администратора информационной безопасности и ресурсов. Благодаря этому возможно создание логических групп и сфер администрирования через бизнес – категоризацию, например, финансовый и коммерческий отделы и т.д.

В Аккорд-В. реализованы:

- механизм дискреционного контроля доступа пользователей и процессов к защищаемым объектам инфраструктуры виртуализации, включая ресурсы внутри ВМ;

- механизм мандатного контроля доступа пользователей и процессов к защищаемым объектам инфраструктуры виртуализации, включая ресурсы внутри ВМ.

ЗСВ.3 Регистрация событий безопасности в виртуальной инфраструктуре.

СЗИ vGate обеспечивает расширенную регистрацию событий безопасности для всех защищаемых компьютеров, в том числе и компьютеров, относящихся к средствам управления виртуальной инфраструктурой. Вся полученная информация заносится в журнал событий безопасности и хранится на сервере авторизации. В процессе аудита можно осуществлять сбор и просмотр событий данного журнала.

В Аккорд-В. обеспечено централизованное автоматизированное управление сбором, записью и хранением информации о событиях безопасности.

ЗСВ.4 Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры.

СЗИ vGate реализует функцию защиты трафика между компонентами ВИ и администратором.

В Аккорд-В. данное требование выполняется другими типами СЗИ или организационными мерами.

ЗСВ.5 Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией.

В vGate существует политика доверенной загрузки виртуальных машин. Есть возможность детально настроить параметры, которые будут контролироваться, а также функционал, позволяющий сделать выбор – разрешить или запустить виртуальную машину при нарушении целостности конфигурации.

Также есть возможность контроля целостности перечня снимков виртуальной машины. После назначения политики доверенной загрузки при старте виртуальной машины, а также по тайм-ауту будет проводиться проверка целостности. При изменениях виртуальной машины происходит оповещение администратора информационной безопасности, который может согласовать или отклонить изменения. При отклонении изменений настройки виртуальной машины будут возвращены в то состояние, в котором они были при назначении политики.

Доверенная загрузка серверов ESXi и vCenter обеспечивается с помощью модуля Аккорд-АМДЗ.

Доверенная загрузка ВМ обеспечивается с помощью СПО «Аккорд-В.».

ЗСВ.6 Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных.

В vGate реализует эту меры посредством управления доступом к ВМ.

Обеспечивают средства управления средой виртуализации (например, VMware vCenter), а также средства виртуализации, контроля и анализа сетевого взаимодействия (например, VMware NSX, принявшего в себя функции продукта vCenter Networking and Security).

Аккорд-В. обеспечивает:

- полный запрет Storage vMotion;
- запрет старта ВМ после смены хранилища в выключенном состоянии.

ЗСВ.7 Контроль целостности виртуальной инфраструктуры и ее конфигураций.

В vGate существует политика доверенной загрузки виртуальных машин. Есть возможность детально настроить параметры, которые будут контролироваться, а также функционал, позволяющий сделать выбор – разрешить или запустить виртуальную машину при нарушении целостности конфигурации.

Также есть возможность контроля целостности перечня снимков виртуальной машины. После назначения политики доверенной загрузки при старте виртуальной машины, а также по тайм-ауту будет проводиться проверка целостности. При изменениях виртуальной машины происходит оповещение администратора информационной безопасности, который может согласовать или отклонить изменения. При отклонении изменений настройки виртуальной машины будут возвращены в то состояние, в котором они были при назначении политики.

В Аккорд-В. реализован механизм пошагового контроля целостности физического оборудования, гипервизора, виртуальных машин, файлов внутри виртуальных машин и серверов управления виртуальной инфраструктурой, рабочих мест администраторов безопасности и виртуальной инфраструктуры.

ЗСВ.8 Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры.

ЗСВ.9 Реализация и управление антивирусной защитой в виртуальной инфраструктуре.

В vGate меры ЗСВ.8 и ЗСВ.9 не реализуются. Однако возможно установить резервный сервер авторизации. Для резервного копирования необходимо использовать специальные программные средства.

В Аккорд-В. данные требования выполняются другими типами СЗИ или организационными мерами.

ЗСВ.10 Разбиение виртуальной инфраструктуры на сегменты(сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей.

В vGate реализован мандатный принцип контроля доступа на основе меток конфиденциальности. При выполнении ряда стандартных операций с объектами виртуальной инфраструктуры осуществляется сравнение меток безопасности учетных записей администратора информационной безопасности и ресурсов. Благодаря этому возможно создание логических групп и сфер администрирования через бизнес – категоризацию, например, финансовый и коммерческий отделы и т.д.

В Аккорд-В. данное требование выполняется другими типами СЗИ или организационными мерами.

Таким образом был сделан вывод о том, что vGate обеспечивает реализацию мер защиты от ЗСВ.1 до ЗСВ.7 и ЗСВ.10, а Аккорд-В. только ЗСВ.1-ЗСВ.3 и ЗСВ.5 и ЗСВ.7.

3 Создание виртуальных машин, входящих в состав стенда

3.1 Краткое описание ВМ и структуры стенда

Для развертывания лабораторного стенда, применяемого для выполнения заданий, необходимо следующие программно-аппаратное обеспечение:

- персональный компьютер с установленной операционной системой (ОС) Windows 8 и выше или ОС на базе дистрибутива Linux;
- средство виртуализации Oracle VM VirtualBox версии не ниже 5.2;
- объем оперативной памяти: не менее 8 Гб;
- свободное место на жестком диске: не менее 150Гб для хранения образов виртуальных машин;
- центральный процессор с поддержкой технологии аппаратной виртуализации.

В состав стенда входит 4 виртуальные машины:

- ВМ 1 с установленной гостевой операционной системой (ОС) Windows 2012 R2, которая является контроллером домена;
- ВМ 2 с установленной гостевой ОС Windows 2012 R2, которая является сервером авторизации;
- ВМ 3 с установленной гостевой ОС Windows 8.1, которая является рабочим местом администратора виртуальной инфраструктуры;
- ВМ 4 с установленным гипервизором ОС Hyper-V 2012 которая является сервером виртуализации.

Все ВМ должны входить в информационную систему, созданную на основе локальной сети Active Directory. Стенд должен представлять собой локальную сеть, которая создана и функционирует как домен Active Directory.

Для взаимодействия всех ВМ в рамках локальной сети должен использоваться тип сетевого подключения «внутренняя сеть» (intnet).

Для автоматизации развертывания всех ВМ должны быть подготовлены сценарии.

Аппаратная конфигурация каждой ВМ должна включать:

- центральный процессор;
- оперативная память. Для ВМ с гостевой ОС Windows 2012 R2 объем должен составлять - 1,5Гбайт, для ВМ с гостевой ОС Windows 8.1 - 1Гбайт, для ВМ с гостевой ОС Hyper-V 2012 – 512Мбайт;
- виртуальный жесткий диск, подключаемый с использованием интерфейса SATA;
- привод оптических дисков, подключаемый с использованием интерфейса SATA;
- видеопамять объемом 128 Мбайт;
- сетевой адаптер с типом подключения «внутренняя сеть» (intnet).
Тип адаптера Intel PRO/1000;
- общая папка обмена между гостевой и основной ОС.

Для создания и настройки виртуальных машин использовалось средство виртуализации Oracle VM VirtualBox версии 5.2 [6].

3.2 Создание ВМ с установленной гостевой ОС Windows Server 2012 R2, являющейся контроллером домена

Для создания ВМ с гостевой ОС Windows Server 2012 R2 необходимо запустить программу Oracle VirtualBox Менеджер. После запуска нажать кнопку «Создать» на панели инструментов. В диалоговом окне мастера создания ВМ на первом этапе надо указать имя ВМ, тип ОС и версию ОС. На следующем шаге определяется объем оперативной памяти, выделяемой ВМ. Он зависит от версии ОС. Для ОС Windows Server 2012 R2 по умолчанию выделяется 2048 Мбайт. Это значение можно при необходимости изменить. Затем необходимо указать вариант создания нового виртуального жесткого

диска. На следующем этапе надо выбрать формат хранения, выбрав динамический виртуальный жесткий диск. На заключительном этапе надо указать имя файла виртуального жесткого диска, каталог в котором он будет храниться и максимальный размер файла динамического виртуального жесткого диска.

Было назначено имя виртуальной машины - «vGate-DC», тип ОС - «Microsoft Windows», версия операционной системы - «Microsoft 2012 (64-bit)», объем оперативной памяти - 1536МБ и был выбран динамический виртуальный жесткий диск. Результат представлен на рисунке 1.

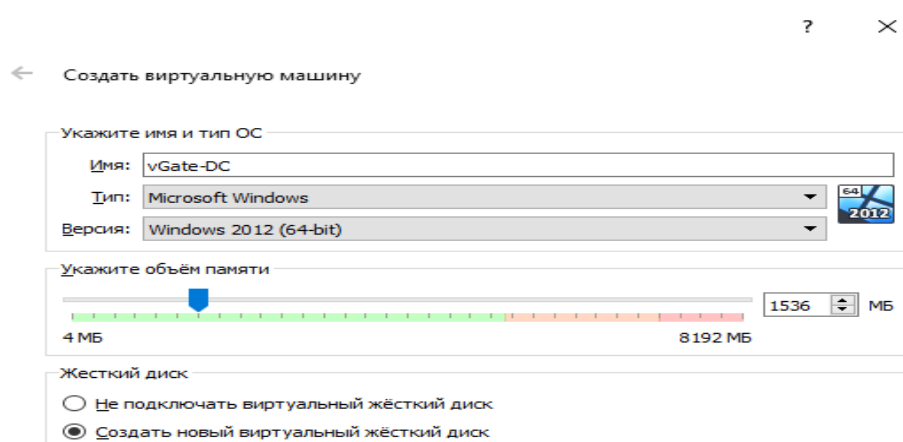


Рисунок 1 — Настройка имени, типа и версии гостевой ОС для VM 1

Был настроен общий буфер обмена. Для этого необходимо выбрать виртуальную машину, нажать кнопку «Настроить» в панели инструментов и выбрать раздел параметров «Общие». Результат представлен на рисунке 2.

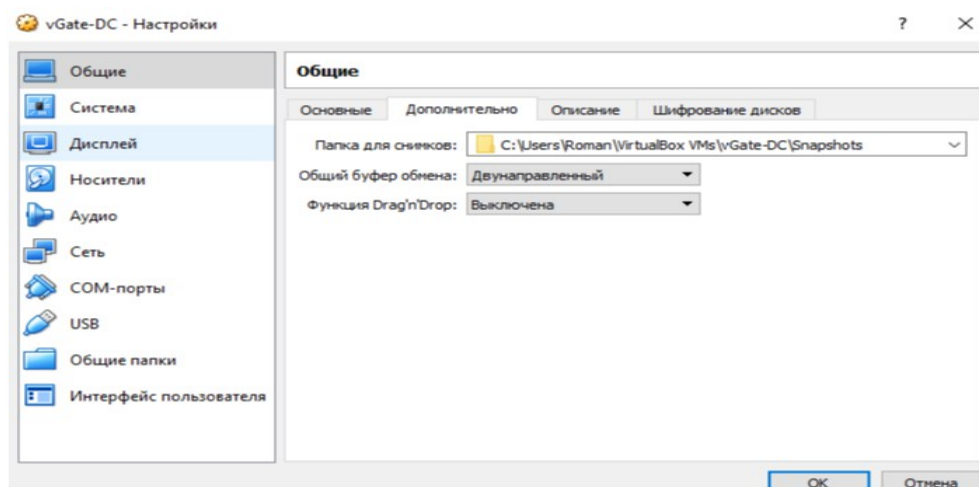


Рисунок 2 - Настройка общего буфера обмена

Был определен порядок загрузки гостевой ОС. Для этого необходимо выбрать виртуальную машину в панели инструментов, нажать кнопку «Настроить». Затем выбрать раздел параметров «Система», указав порядок загрузки гостевой ОС. Результат представлен на рисунке 3.

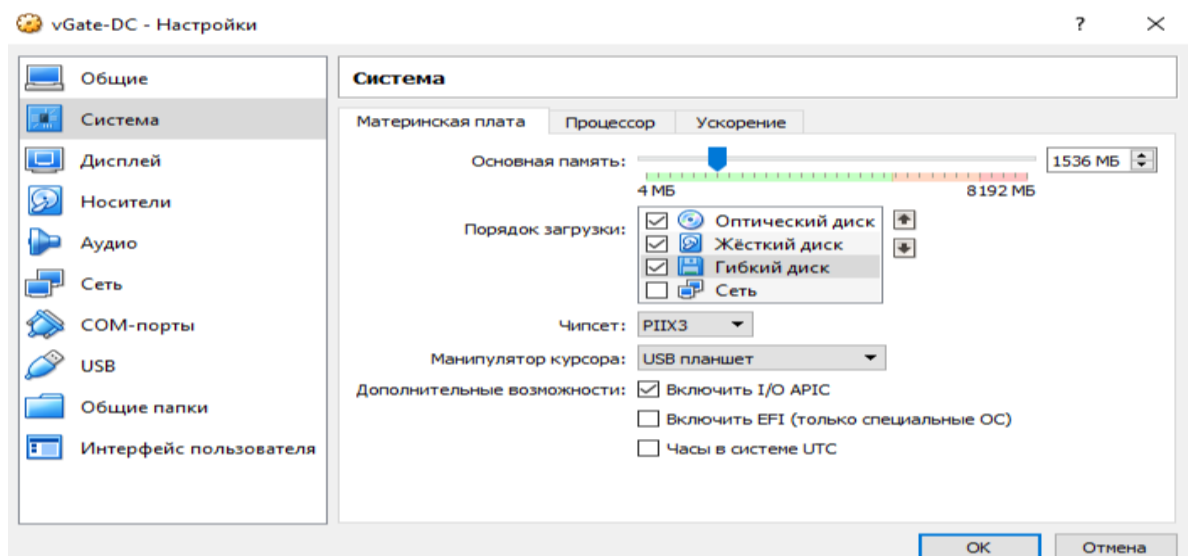


Рисунок 3 - Настройка порядка загрузки гостевой ОС

Далее была выполнена настройка адаптера сети. Для этого необходимо выбрать виртуальную машину и в панели инструментов нажать кнопку «Настроить», выбрать раздел параметров «Сеть». Указать тип подключения «внутренняя сеть», имя «intnet», тип адаптера «Intel PRO/1000 MT Desktop», неразборчивый режим - «разрешить все». Результат представлен на рисунке 4.

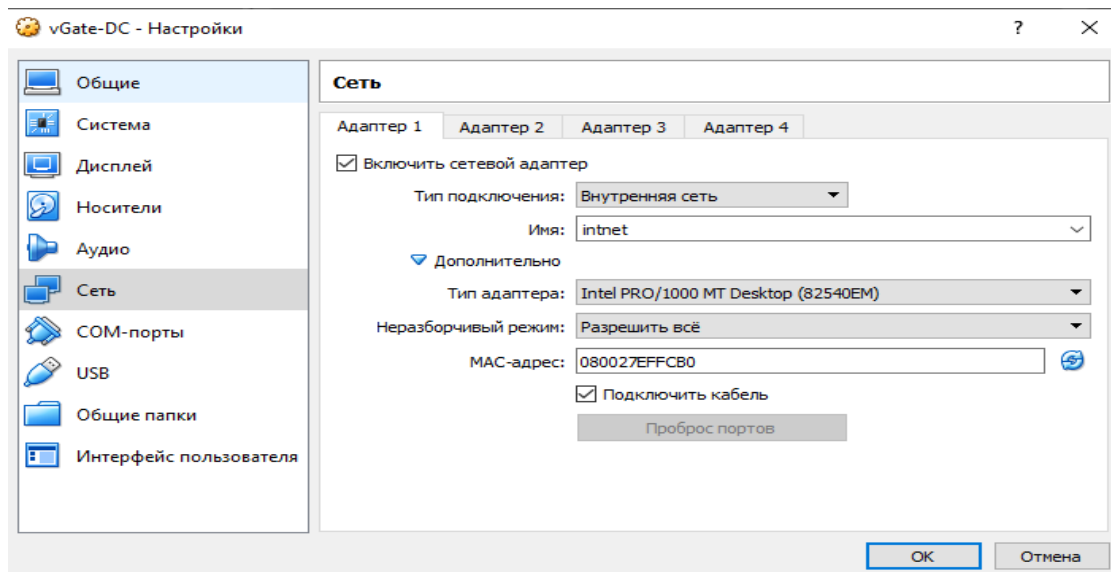


Рисунок 4 — Настройка сетевого адаптера VM1

Была настроена общая папка. Для этого необходимо выбрать виртуальную машину и в панели инструментов нажать кнопку «Настроить», выбрать раздел параметров «Общие папки». Результат представлен на рисунке 5.

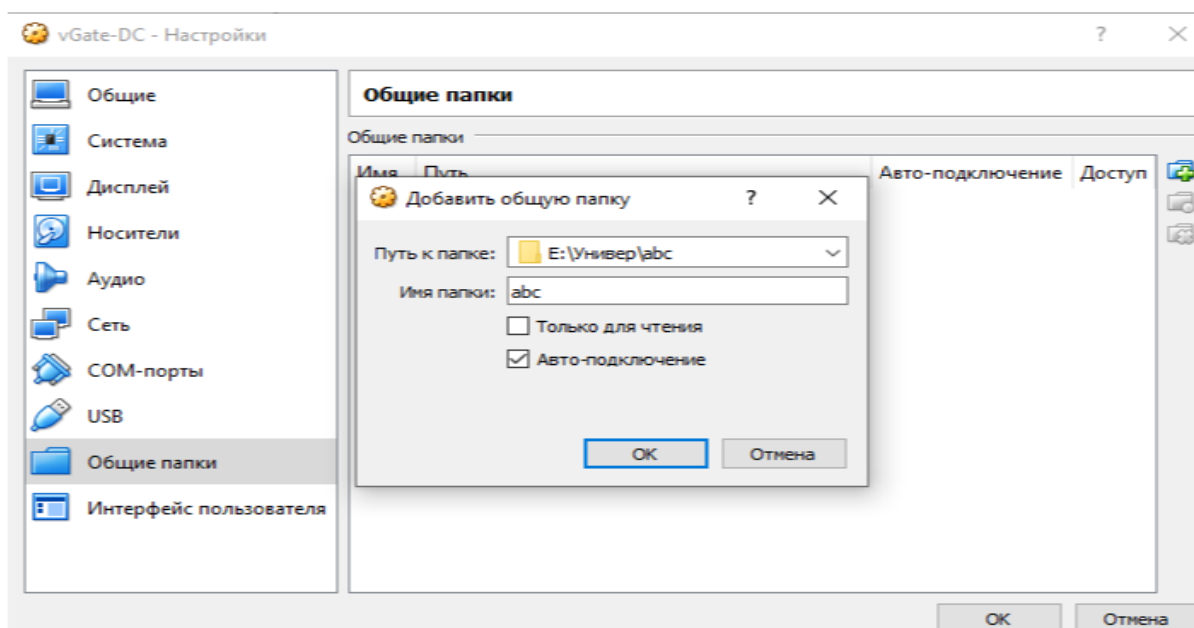


Рисунок 5 - Настройка общей папки

В составе стенда будет использоваться еще одна ВМ с такой же гостевой системой Windows Server 2012 R2. Она получается из исходной путем клонирования.

Гостевая ОС устанавливалась в соответствии с документацией разработчика ОС — компании Microsoft [7].

При установке гостевой ОС были настроены параметры учетной записи Администратора — имя и пароль. Имя — Администратор, пароль — P.ssw0rd.

После установки гостевой ОС, запуска ВМ1 и входа с использованием учетной записи администратора необходимо установить дополнения гостевой ОС для ВМ. Результат представлен на рисунке 6.

После установки гостевой ОС для ВМ1, ВМ2 была получена из нее путем клонирования. ВМ 2 будет являться сервером авторизации vGate. Создание ВМ 2 описано в параграфе 2.3.

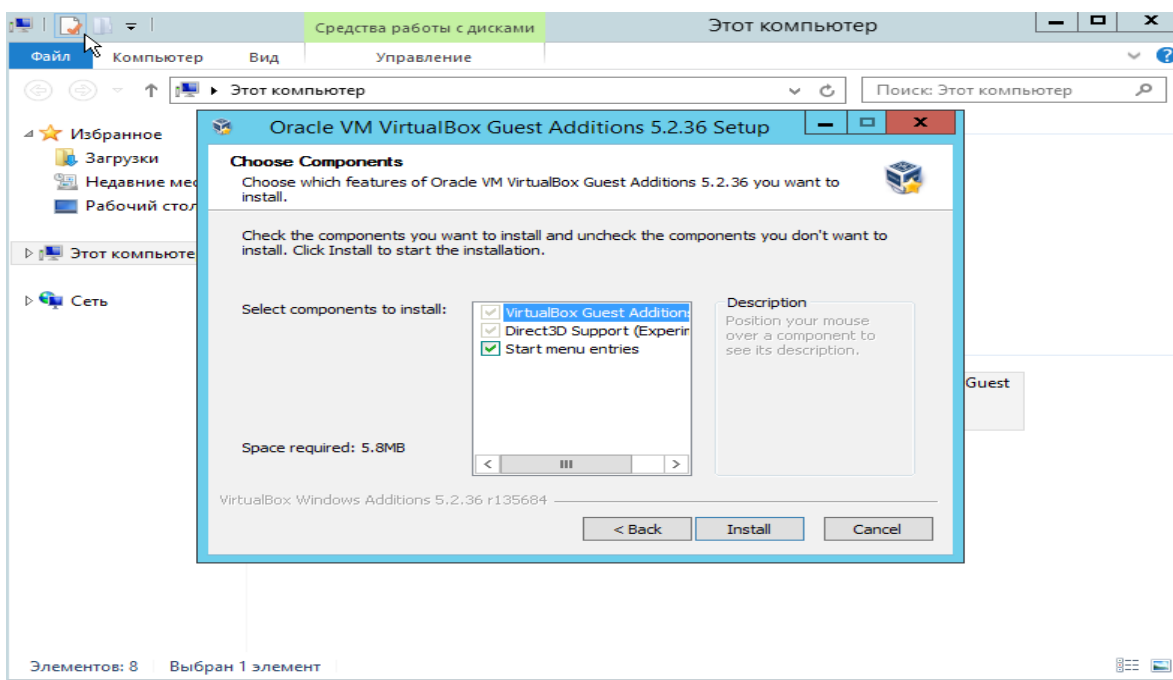


Рисунок 6 — Установка дополнений гостевой ОС

Далее необходимо настроить вид папок (отключить параметр «Скрывать расширения для зарегистрированных типов файлов»). Результат представлен на рисунке 7.

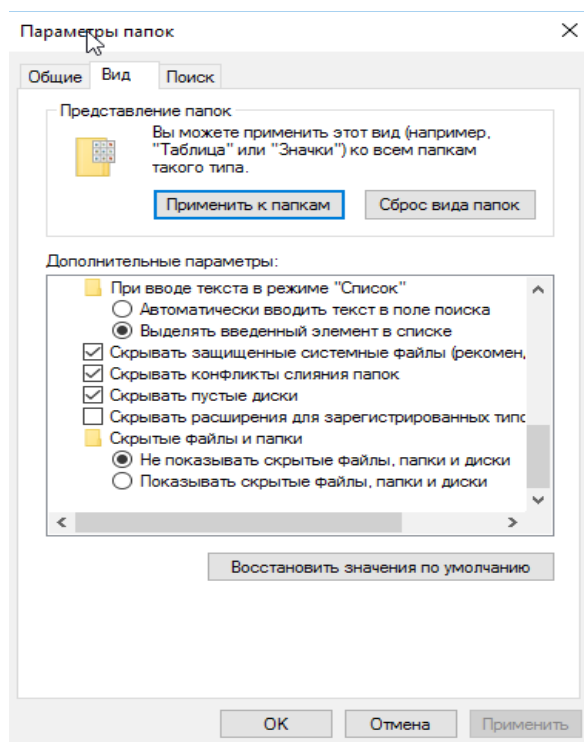


Рисунок 7 - Настройка вида папок

Далее необходимо было изменить имя компьютера. Для этого необходимо запустить программу «Диспетчер серверов», перейти в раздел «Локальный сервер» и выбрать параметр «Имя компьютера». Оно было изменено на vGate-DC. После этого необходимо перезагрузить виртуальную машину. Результат представлен на рисунке 8.

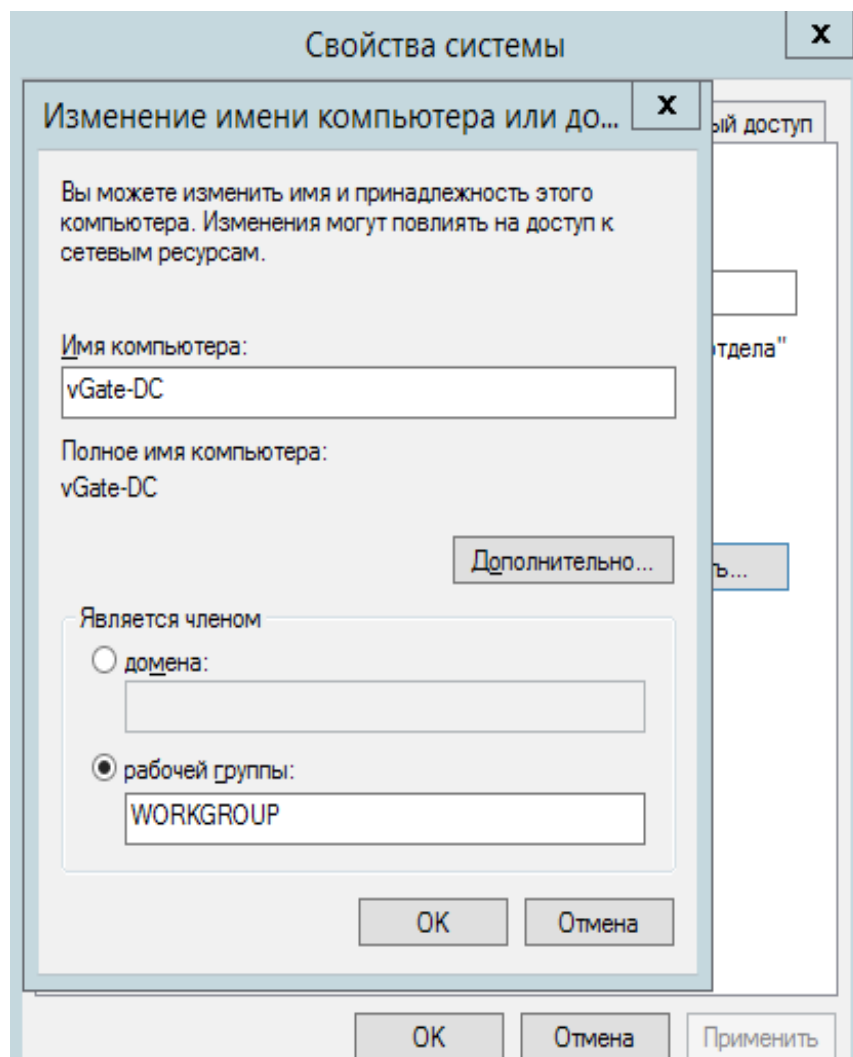


Рисунок 8 - Изменение имени компьютера

После перезагрузки необходимо установить для сетевого адаптера статический IP-адрес-192.168.100.1 и маску подсети- 255.255.255.0. При этом адрес настроить для протокола IP версии 4. Отключить использование IP-адресов версии 6. В качестве шлюза по умолчанию указать адрес самого сервера. Результат представлен на рисунке 9.

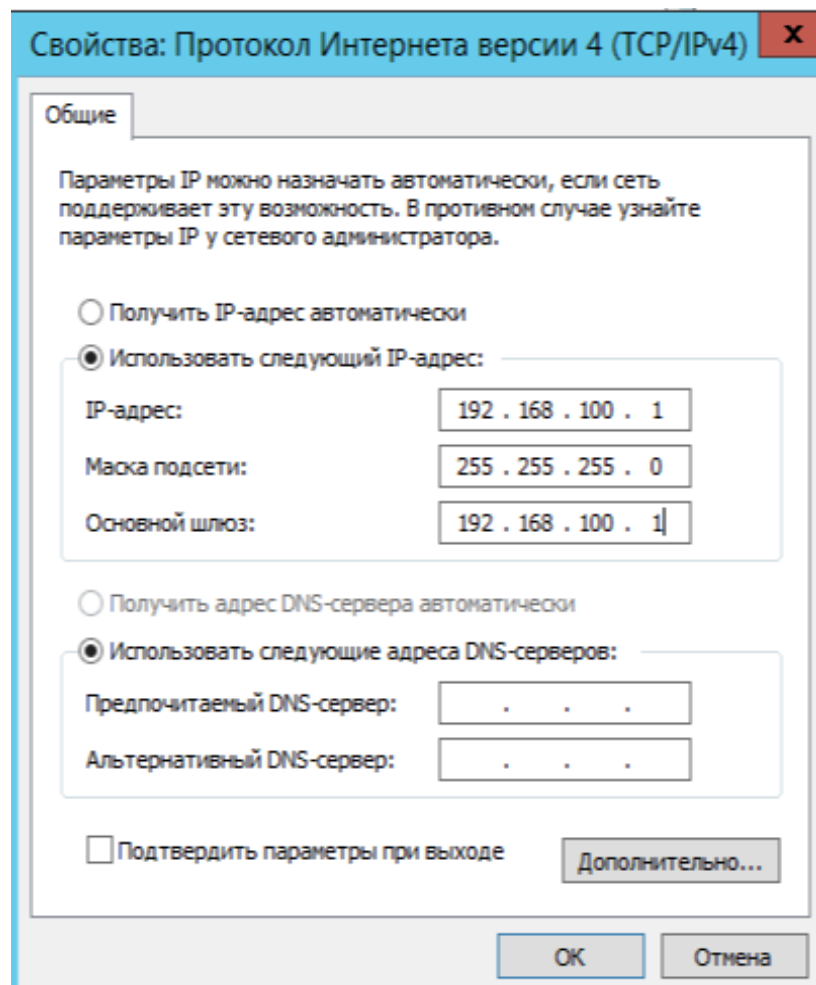


Рисунок 9 - Настройка статического адреса для IPv4

Необходимо проверить системные дату и время и выставить их в соответствии с текущими. Далее для учетной записи администратора установить параметр «Срок действия пароля не ограничен». Для этого надо запустить программу «Диспетчер серверов», выбрать пункт «Средства», далее в выпадающем списке консоли «Управление компьютером», раздел «Локальные пользователи», подраздел «Пользователи». В диалоговом окне свойств учетной записи администратора во вкладке «Общие» установить параметр «Срок действия пароля не ограничен».

Далее необходимо установить роль DNS-сервера.

Для этого необходимо в Диспетчере серверов выбрать пункт Управление, далее команду «Добавить роли и компоненты». После запуска консоли «Мастер добавления ролей и компонентов», необходимо выбрать тип установки

«Установка ролей или компонентов». В списке ролей сервера необходимо выбрать «Средства DNS-сервера» и выполнить установку. Результат представлен на рисунках с 10 по 13.

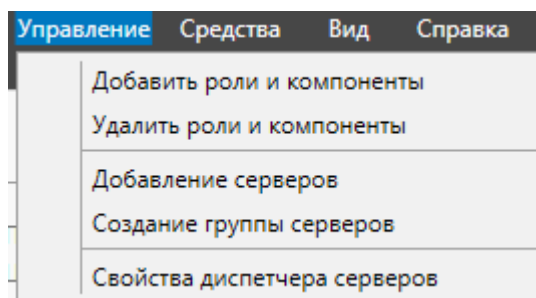


Рисунок 10 - Выбор в меню Управление команды для запуска Мастера добавления ролей и компонентов

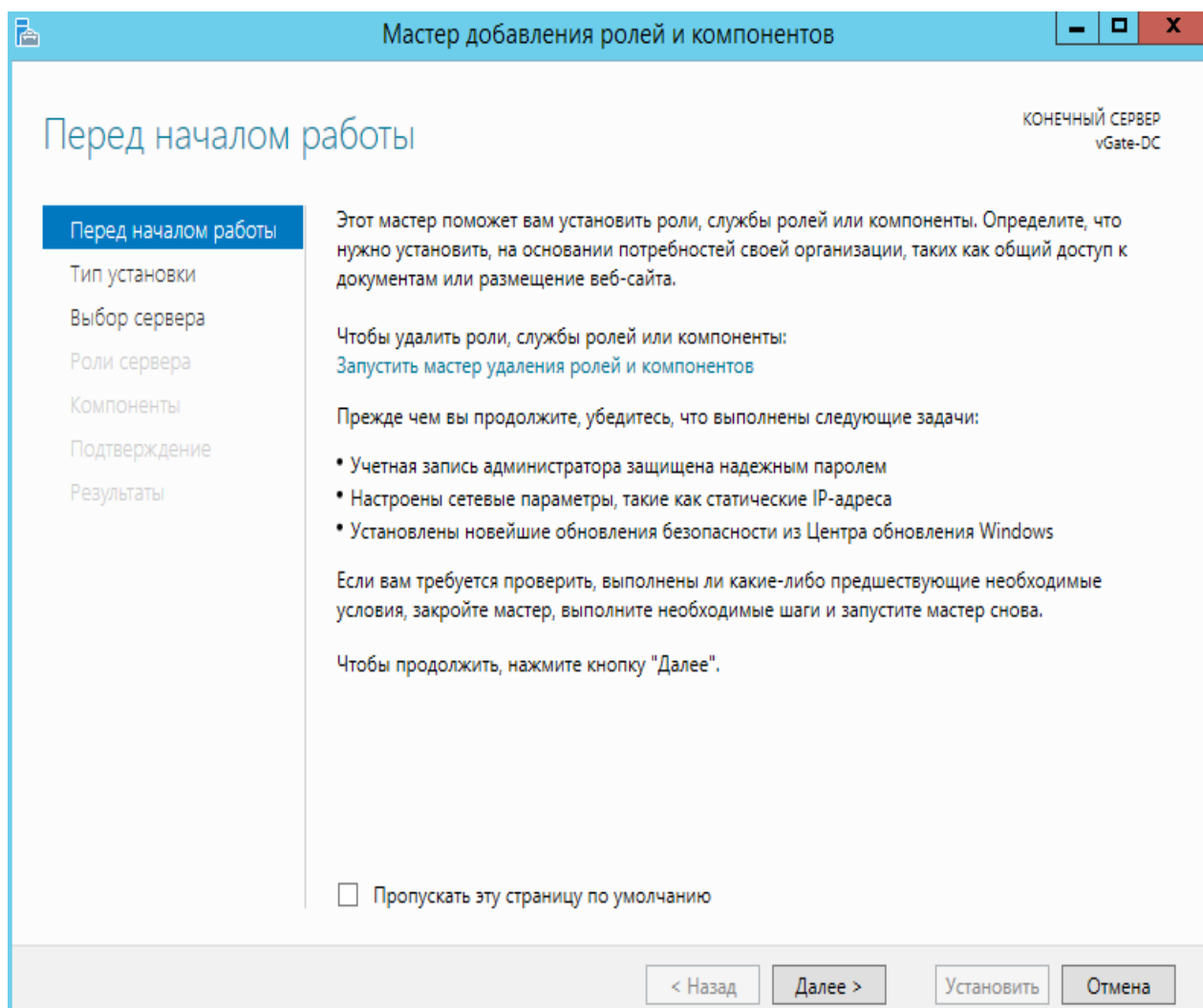


Рисунок 11 - Запуск мастера добавления ролей и компонентов

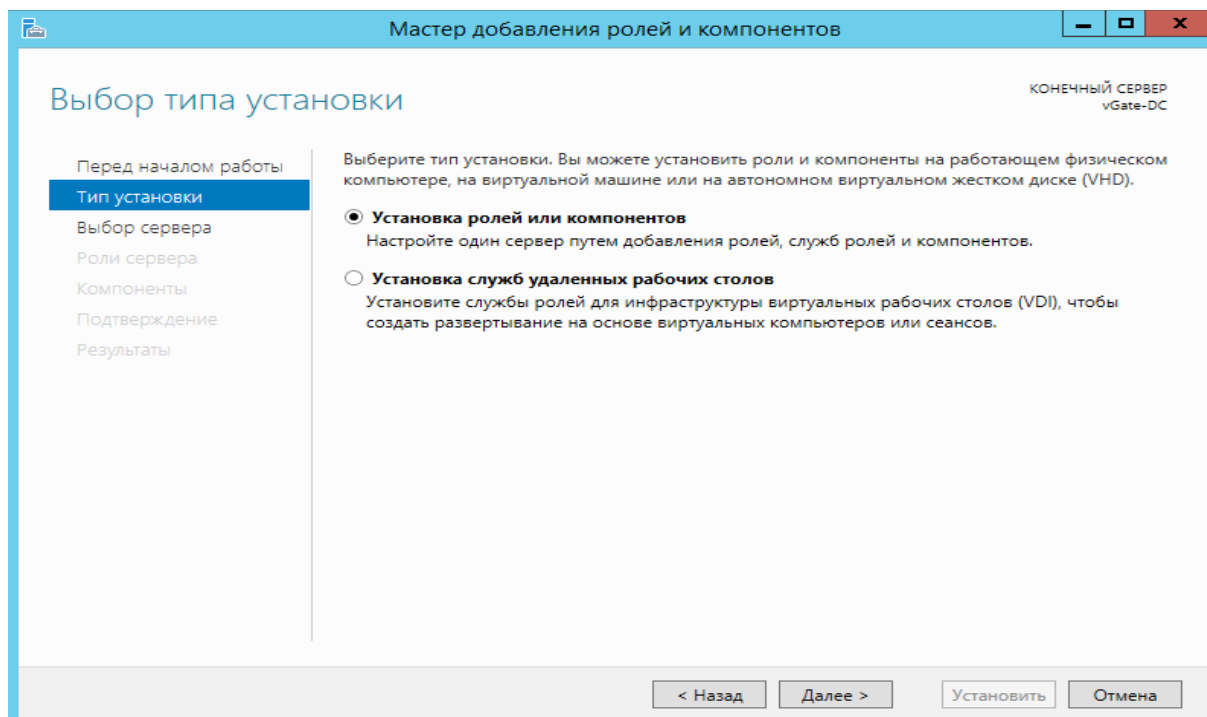


Рисунок 12 - Выбор типа установки

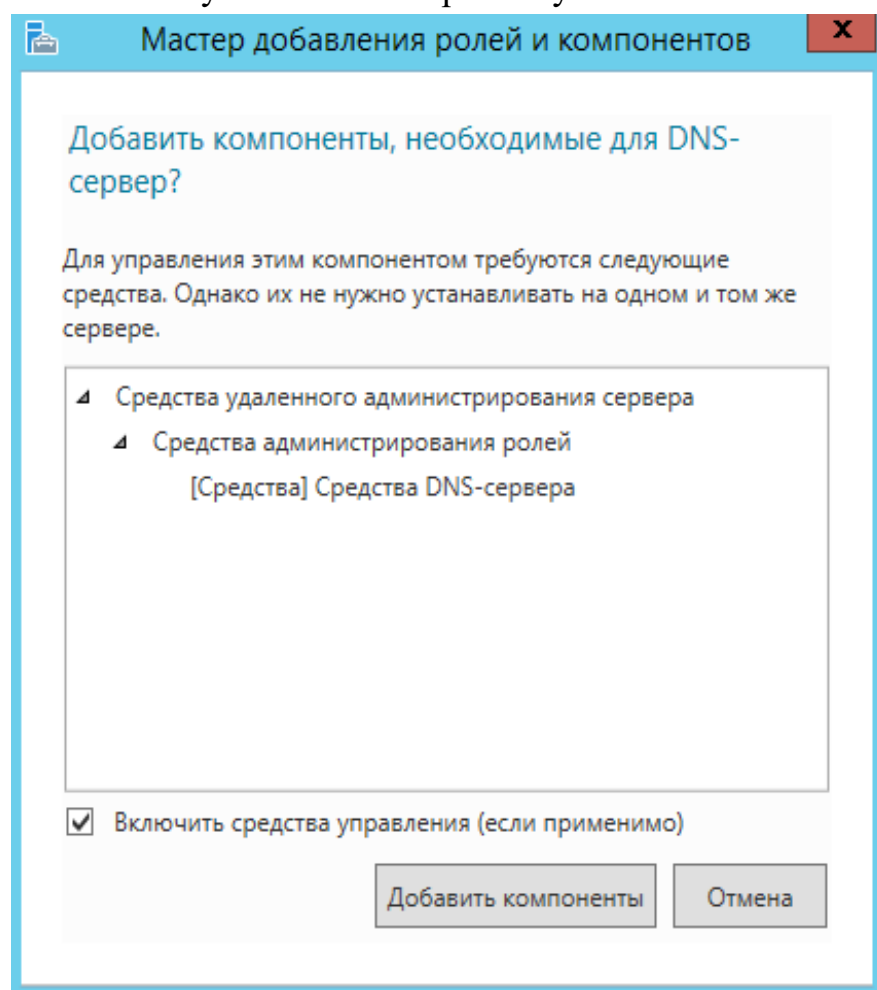


Рисунок 13 - Выбор компонентов

Необходимо создать зону прямого просмотра.

Для этого необходимо в Диспетчере серверов выбрать пункт Средства, далее в выпадающем списке консоль «DNS». После запуска консоли «Диспетчер DNS», необходимо в колонке «Зоны прямого просмотра» создать новую зону. Для этого надо щелкнуть правой клавишей мыши по строке «Зона прямого просмотра» и в контекстном меню выбрать команду «Уточнить название команды». Запускается мастер создания новой зоны, далее выбрать «Основная зона», указать имя зоны «vgate.psu» и выбрать тип динамического обновления-«разрешить любые динамические обновления». Результат представлен на рисунках с 14 по 18.

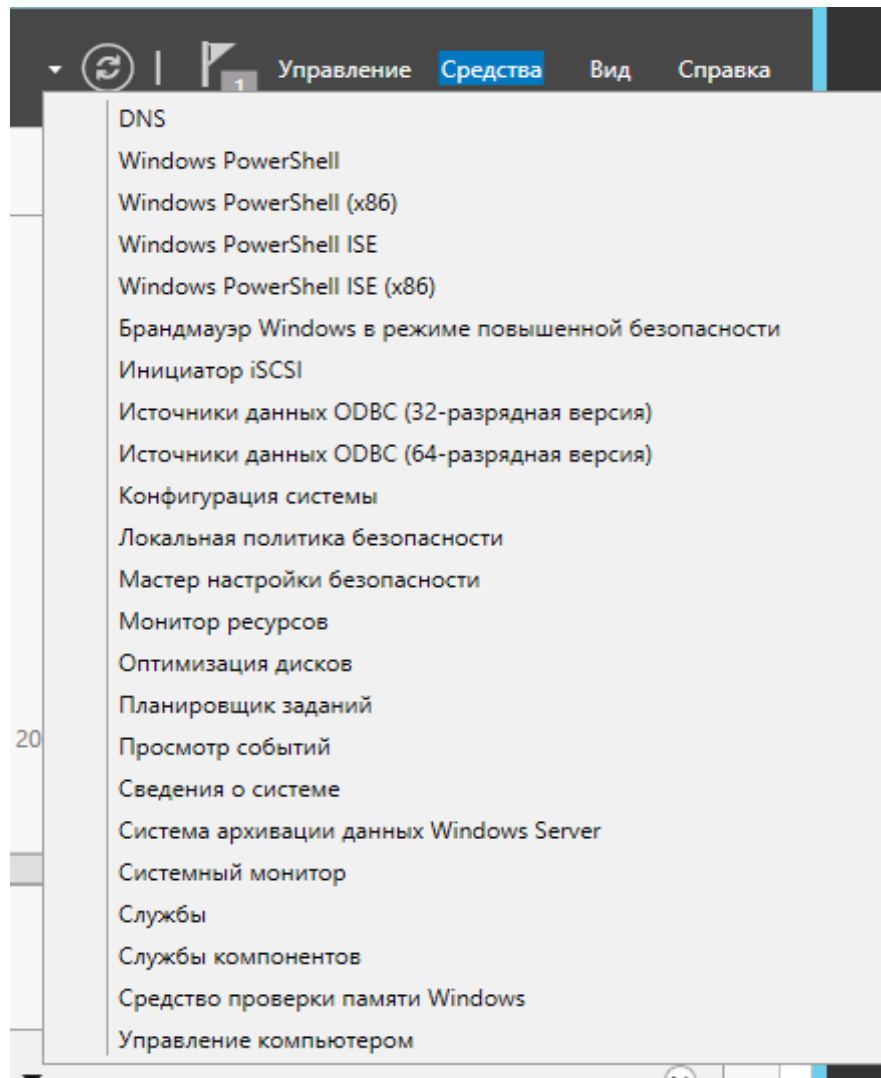


Рисунок 14 - Создание зоны прямого просмотра

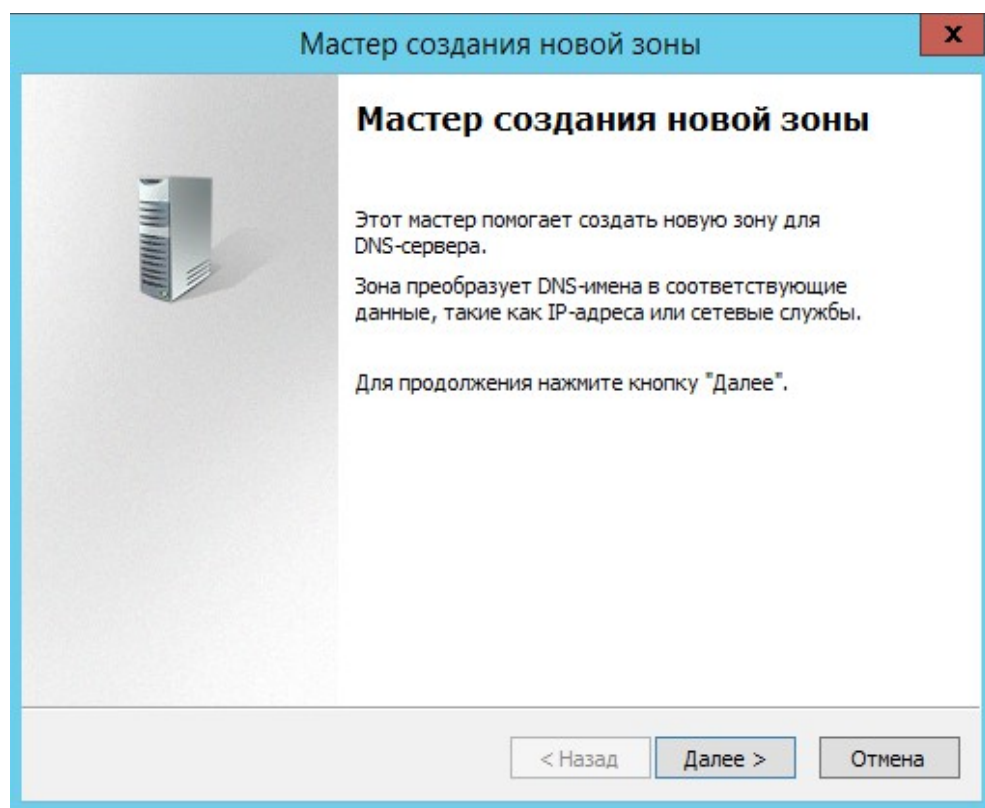


Рисунок 15 - Запуск мастера создания новой зоны

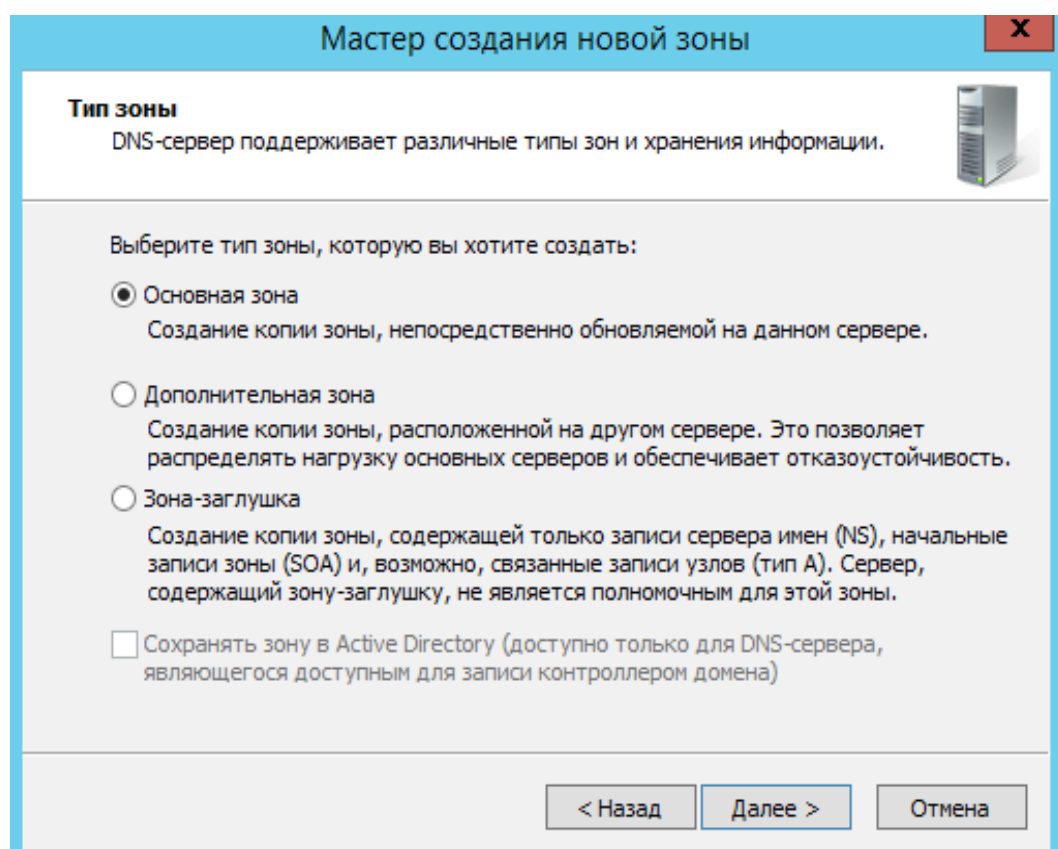


Рисунок 16 - Выбор типа зоны

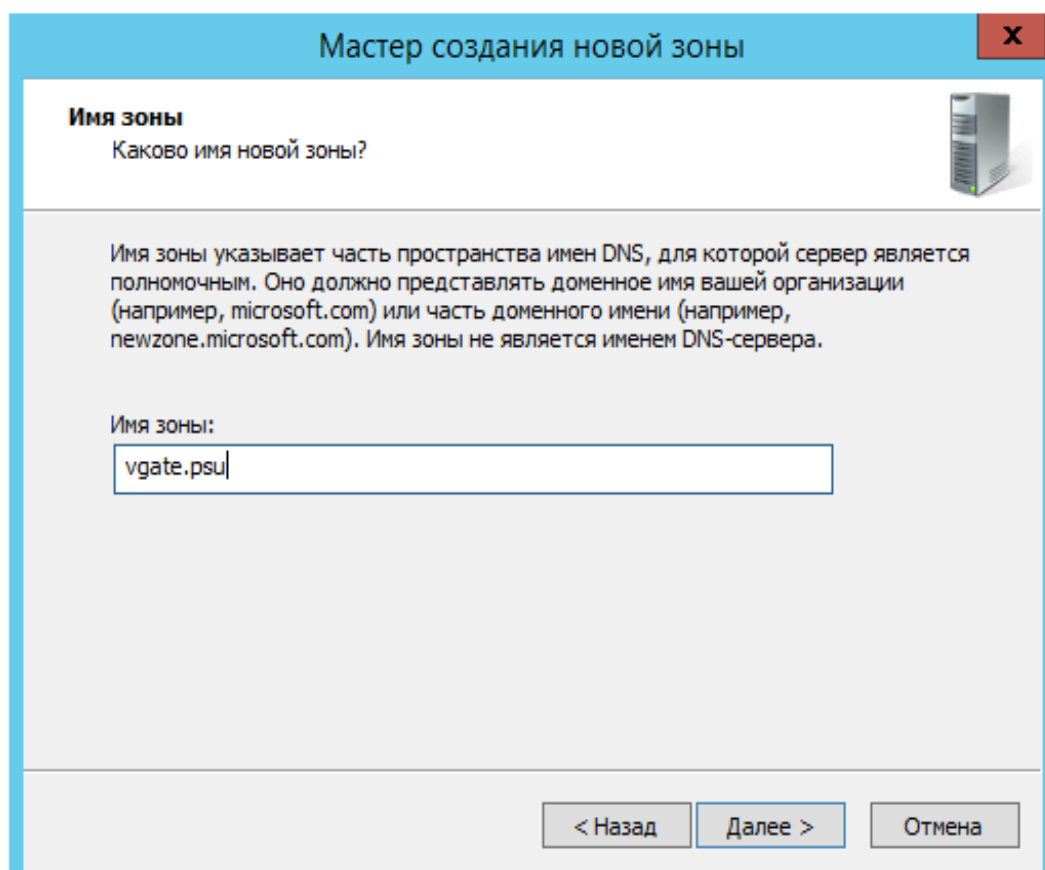


Рисунок 17 - Ввод имени зоны

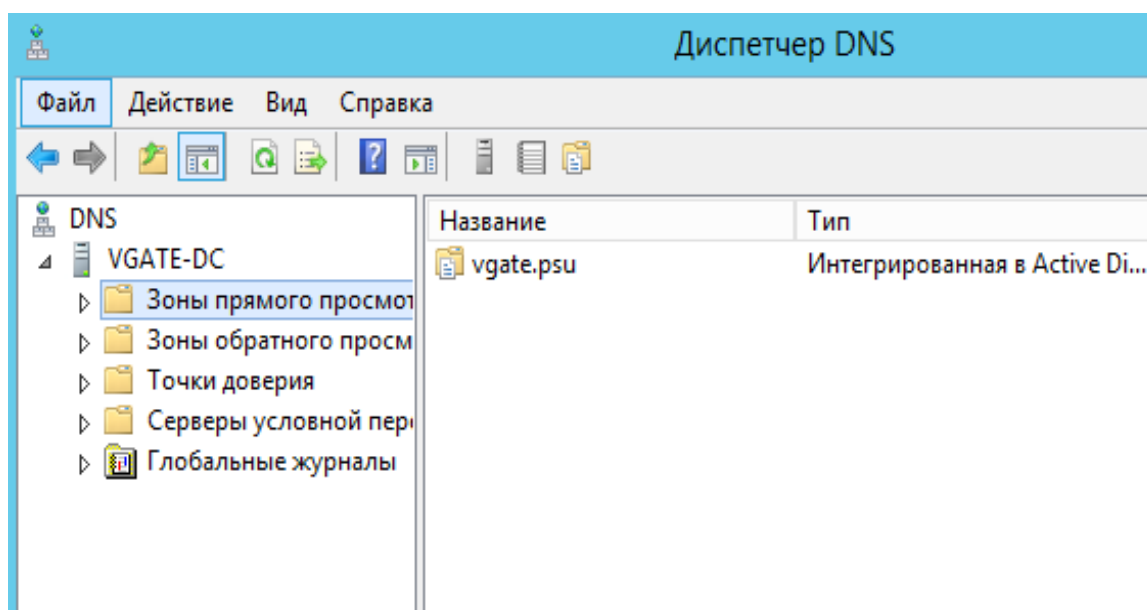


Рисунок 18 – Созданная зона в консоли управления DNS

Для сетевого адаптера указать адрес предпочитаемого DNS-сервера и альтернативный адрес. Результат представлен на рисунке 19.

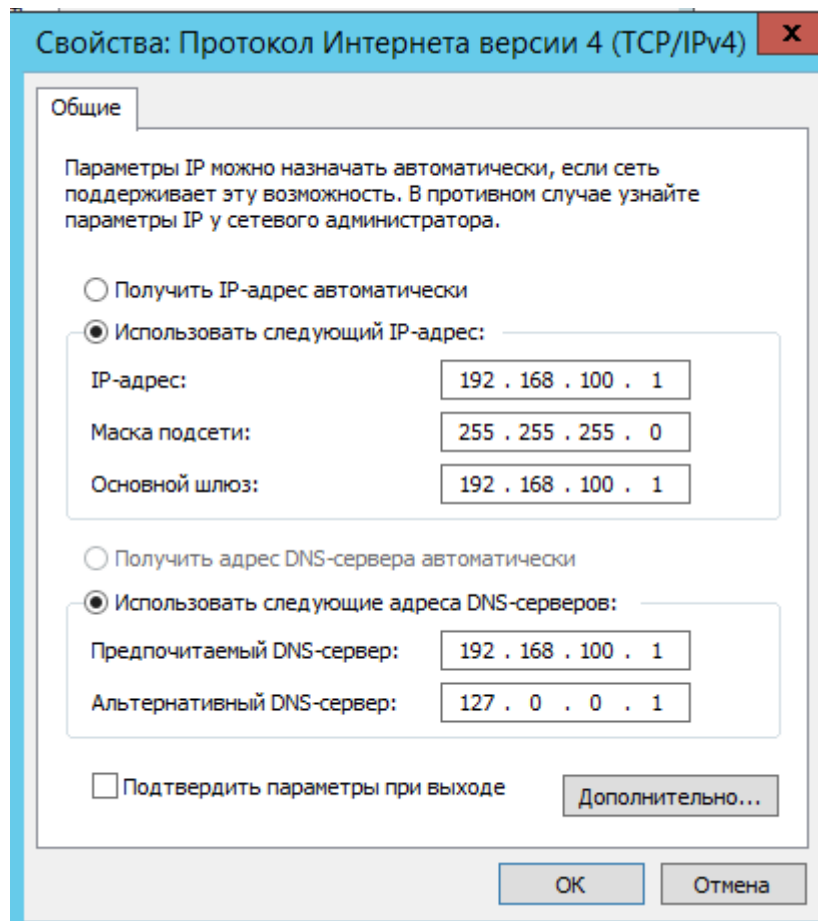


Рисунок 19 - Настройка предпочитаемого и альтернативного адреса DNS-сервера

С помощью Диспетчера серверов необходимо скорректировать настройки имени сервера. Необходимо добавить «Основной DNS-суффикс этого компьютера» и указать имя зоны прямого просмотра. После изменения настроек ВМ необходимо перезагрузить. Результат представлен на рисунке 20.

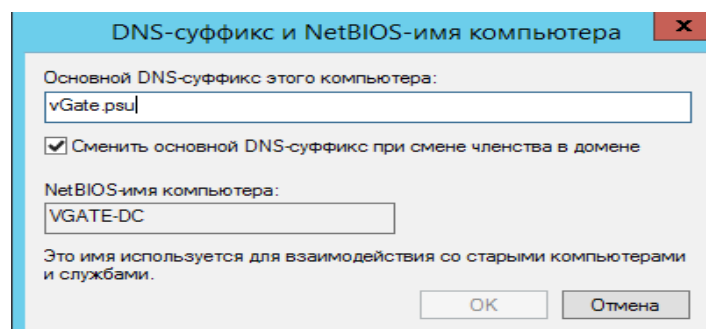


Рисунок 20 - Добавление DNS-суффикса

Далее из списка компонентов необходимо установить NET Framework 3.5.

Для этого необходимо в Диспетчере серверов выбрать пункт Управление, далее команду «Добавить роли и компоненты». После запуска консоли «Мастер добавления ролей и компонентов», необходимо выбрать тип установки «Установка ролей или компонентов». В списке компонентов необходимо выбрать «Функции NET Framework 3.5» и выполнить установку. Результат представлен на рисунках с 21 по 23.

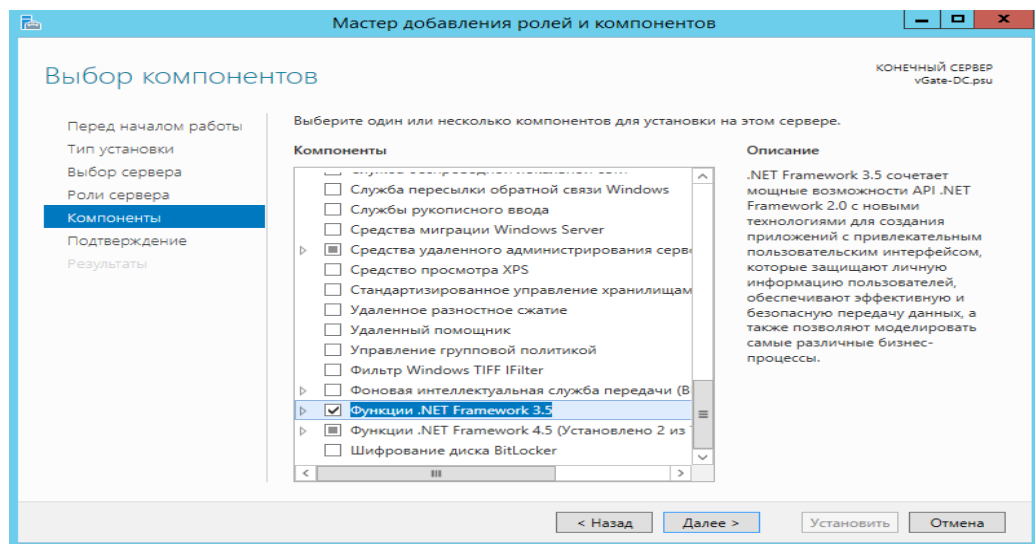


Рисунок 21 - Установка компонента NET Framework 3.5.

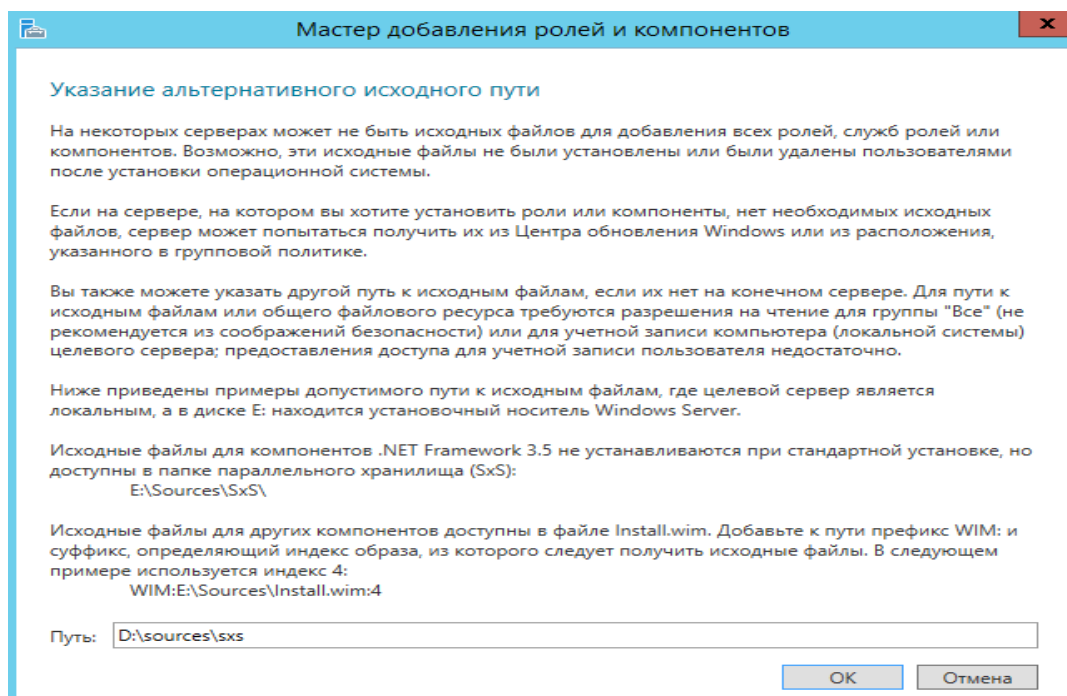


Рисунок 22 - Указание альтернативного исходного пути

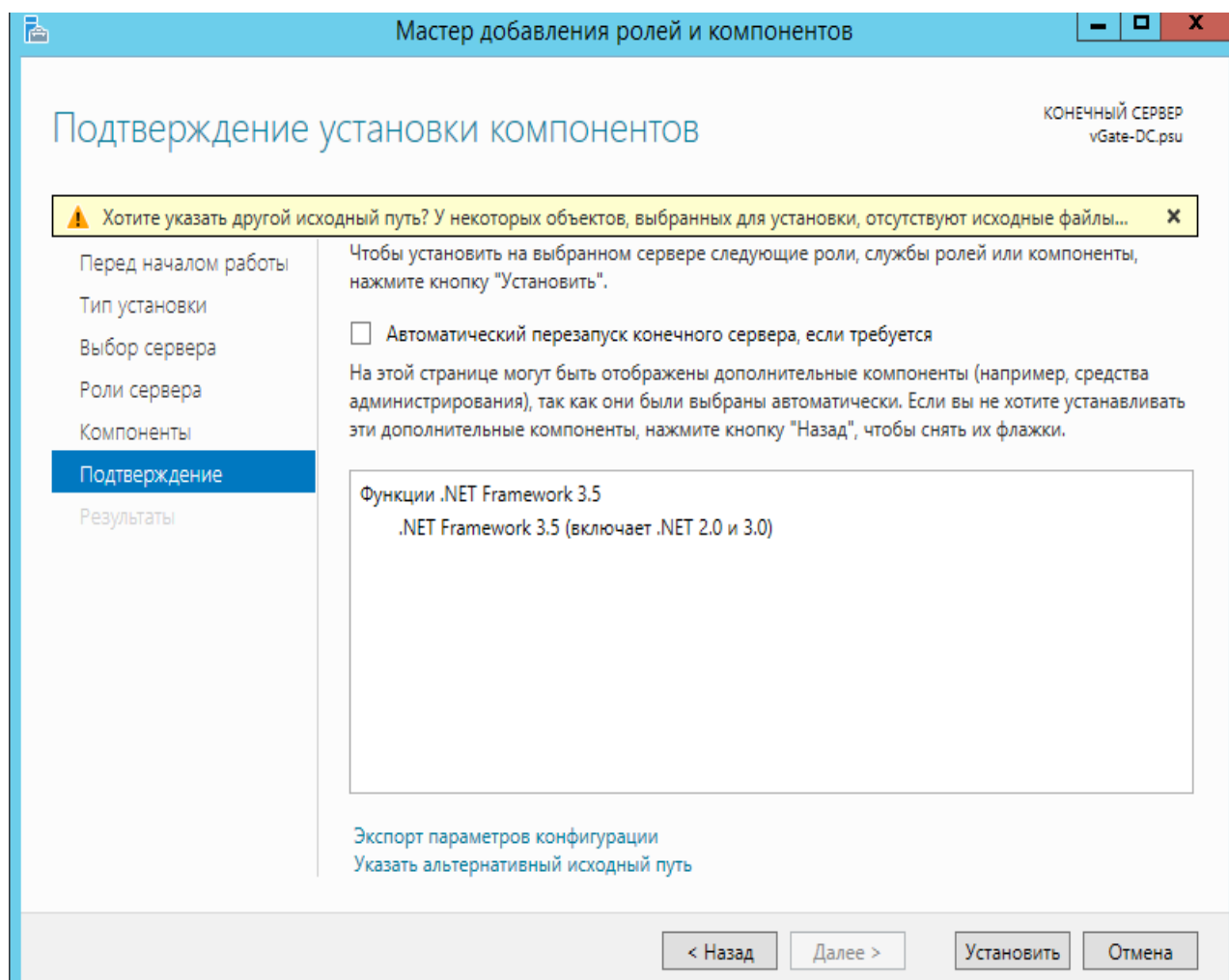


Рисунок 23 - Подтверждение установки компонента NET Framework 3.5.

Далее необходимо установить роль Веб-сервера (IIS).

Для этого необходимо в Диспетчере серверов выбрать пункт Управление, далее команду «Добавить роли и компоненты». После запуска консоли «Мастер добавления ролей и компонентов», необходимо выбрать тип установки «Установка ролей или компонентов». В списке ролей необходимо выбрать «Веб-сервер (IIS)», в списке службы ролей не должны быть отмечены роли, которые предполагают использование сертификатов, трассировку, перенаправление и публикацию, разработку приложений, сжатие динамического содержимого и расширяемость FTP. После этого была выполнена установка. Результат представлен на рисунке 24.

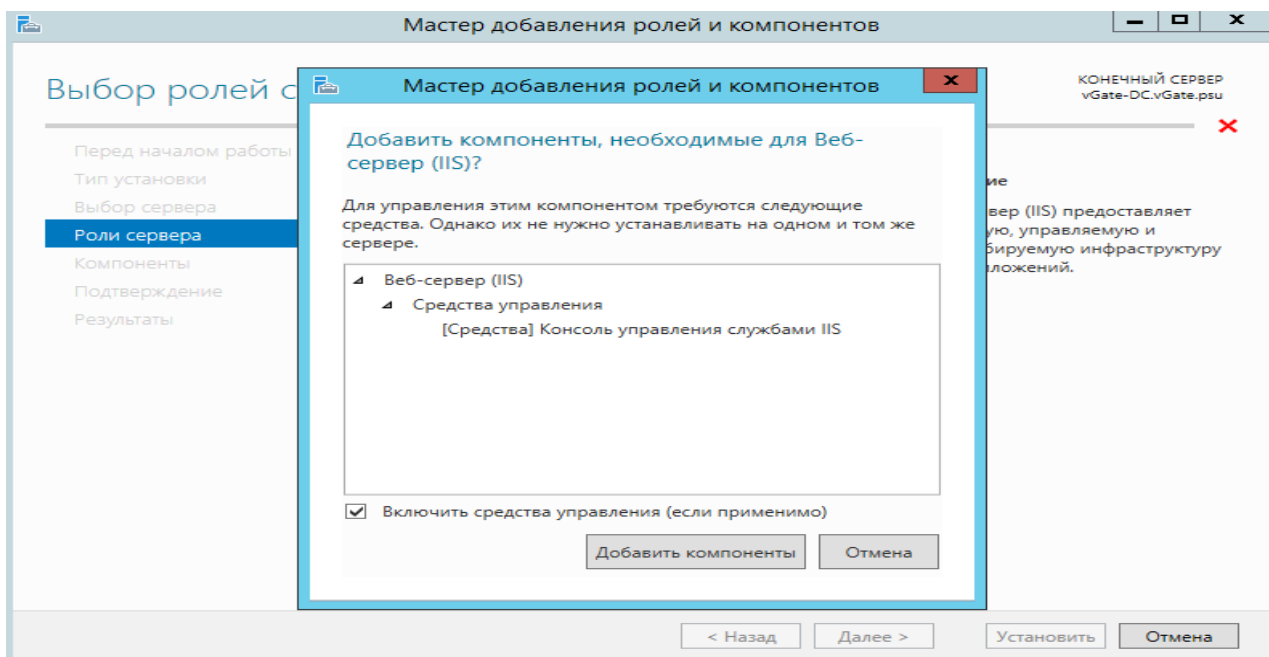


Рисунок 24 - Установка роли Веб-сервера (IIS)

Затем необходимо установить сервер приложений.

Для этого необходимо в Диспетчере серверов выбрать пункт Управление, далее команду «Добавить роли и компоненты». После запуска консоли «Мастер добавления ролей и компонентов», необходимо выбрать тип установки «Установка ролей или компонентов». В списке ролей необходимо выбрать «Сервер приложений», в списке службы ролей были выбраны все компоненты, кроме компонента распределенных транзакций. После этого была выполнена установка. Результат представлен на рисунках 25 и 26.

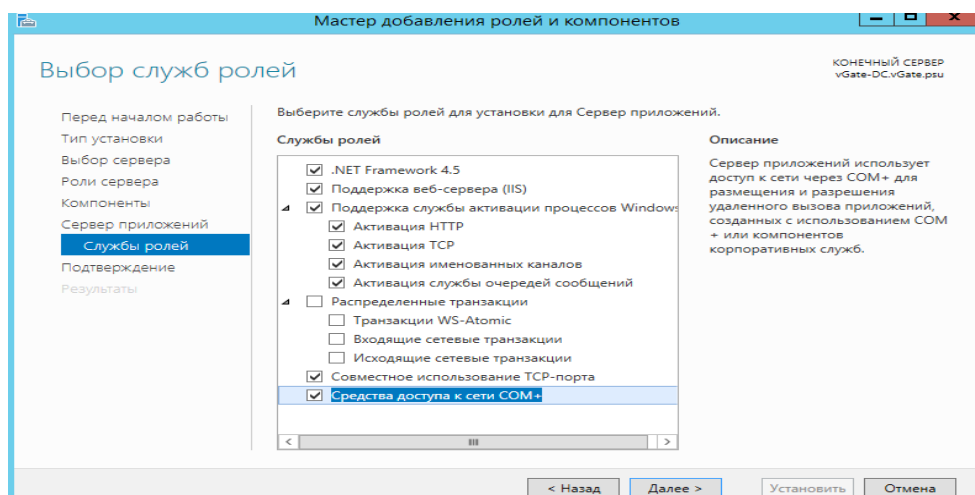


Рисунок 25 - Установка роли сервера приложений

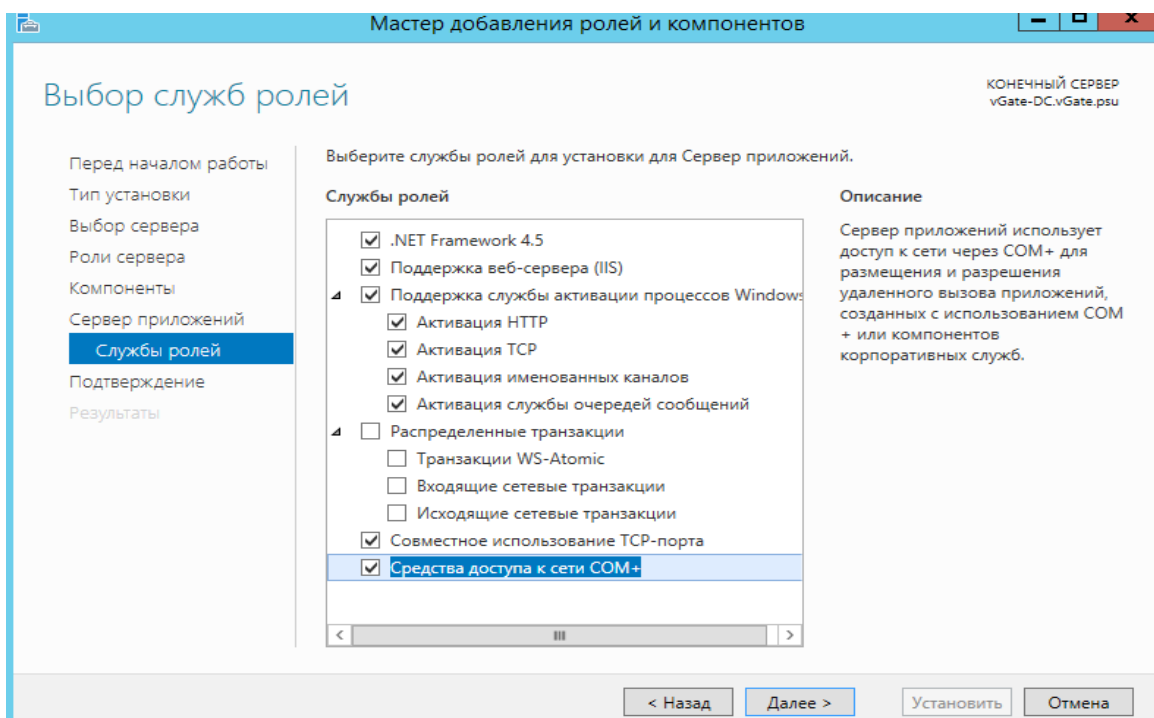


Рисунок 26 - Выбор служб ролей

Далее аналогично установлены компоненты Средство просмотра XPS и SMTP-сервер и Фоновая интеллектуальная служба передачи (BITS). Результат представлен на рисунках с 27 по 29.

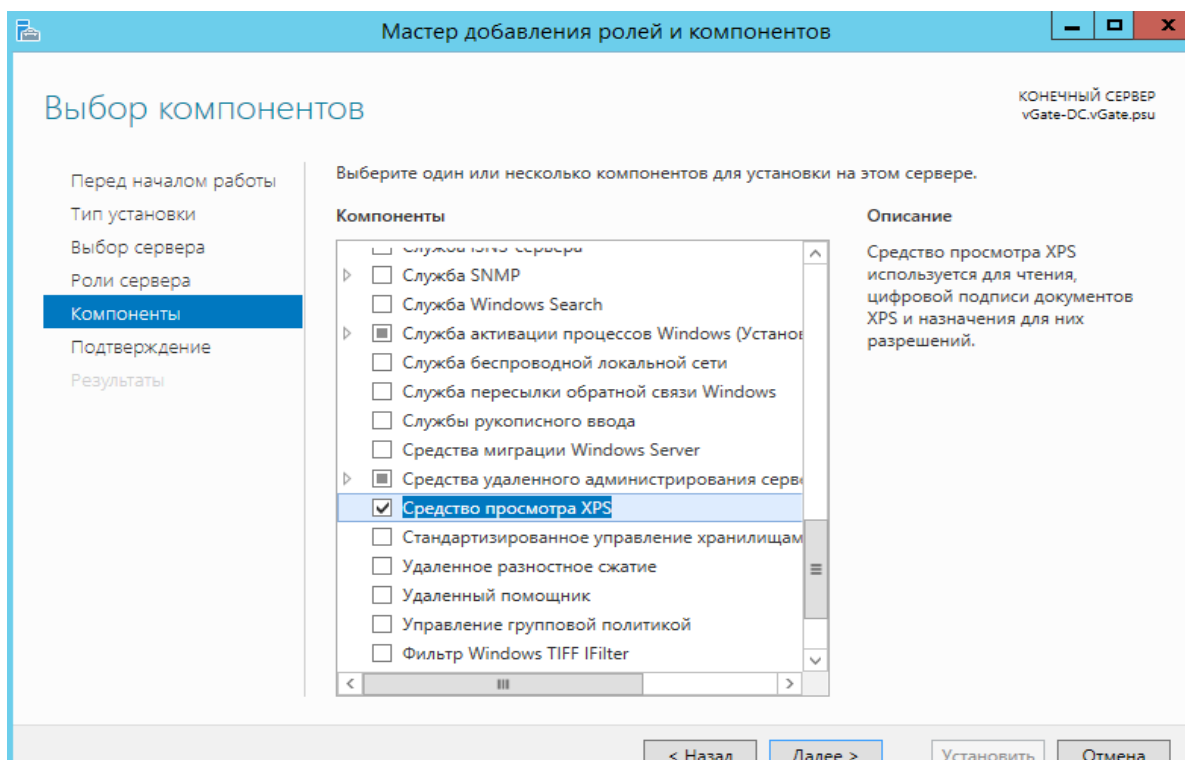


Рисунок 27 – Установка компонента Средства просмотра XPS

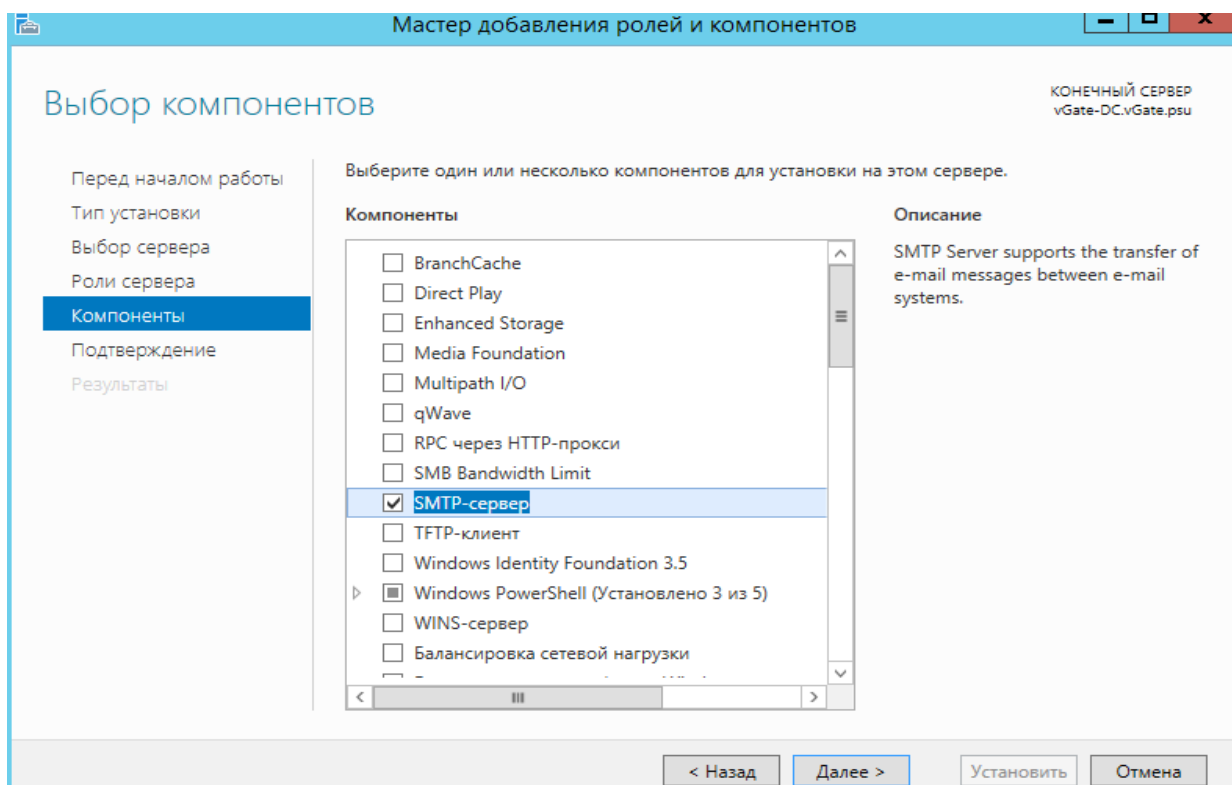


Рисунок 28 - Установка компонента SMTP-сервера

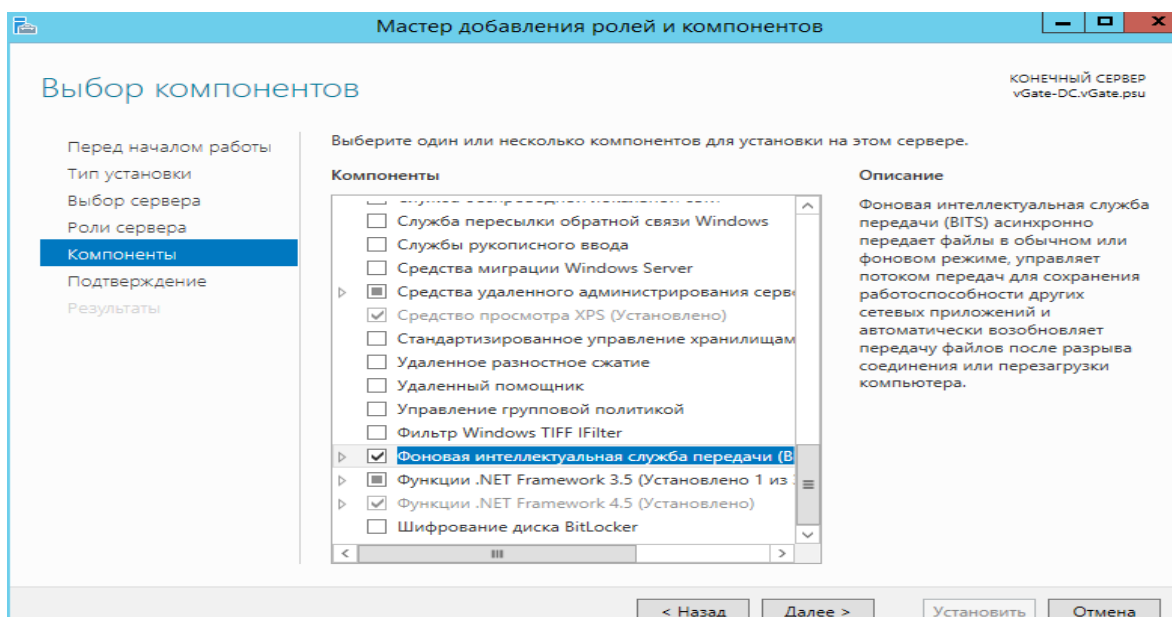


Рисунок 29 - Установка компонента Фоновой интеллектуальной службы передачи (BITS)

После этого необходимо проверить работу локальных служб: Браузер компьютеров, Журналы и оповещения производительности, Обнаружение SSDP, Служба SFTP, Удаленный вызов процедур (RPC), Удаленный реестр, Узел универсальных PNP-устройств, Фоновая интеллектуальная служба передачи

(BITS). Для этого необходимо комбинацией клавиш «WIN + R» запустить программу «Выполнить» и ввести значение «services.msc» и найти нужные службы. Результат представлен на рисунках с 30 по 37.

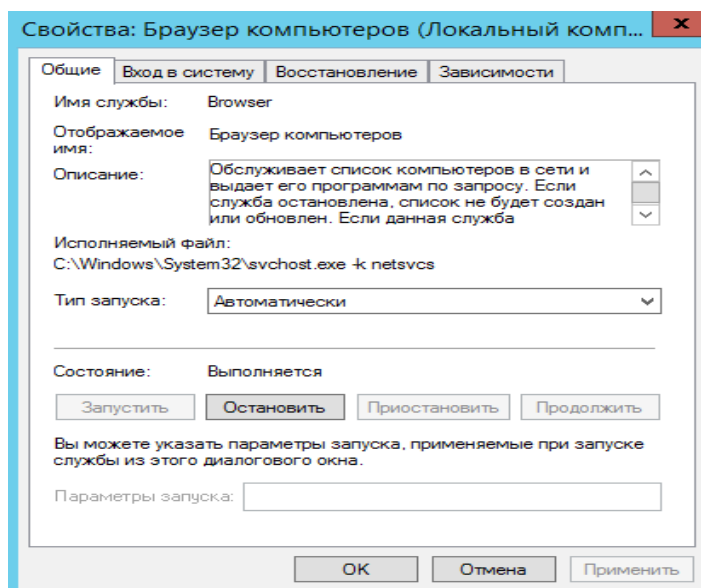


Рисунок 30 - Проверка службы Браузер компьютеров

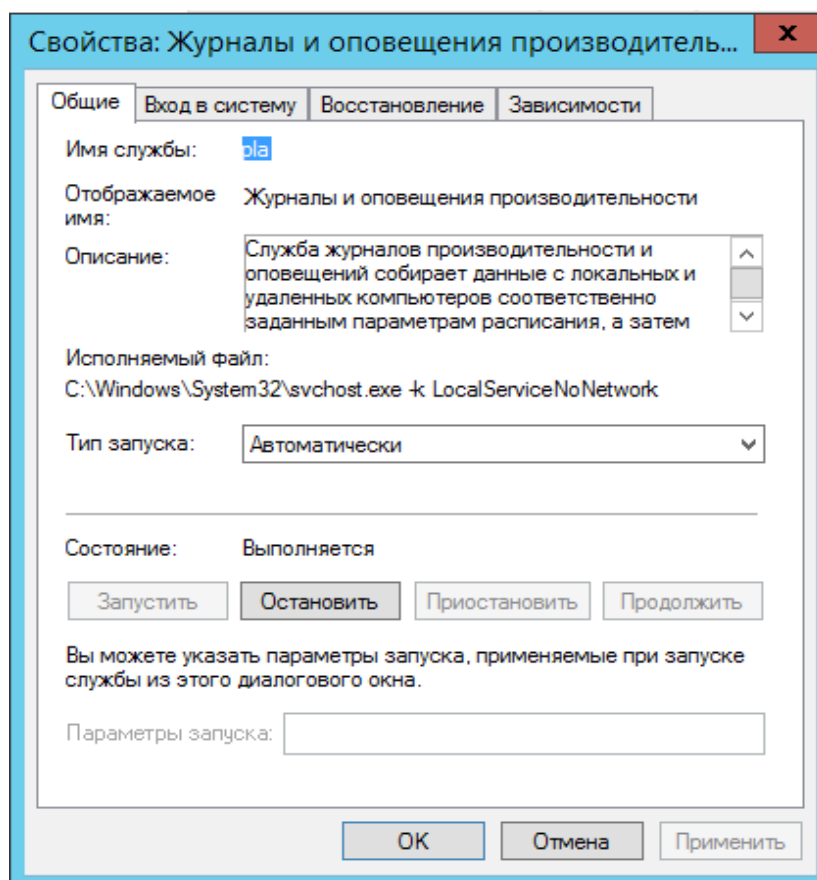


Рисунок 31 - Проверка службы Журналы и оповещения производительности

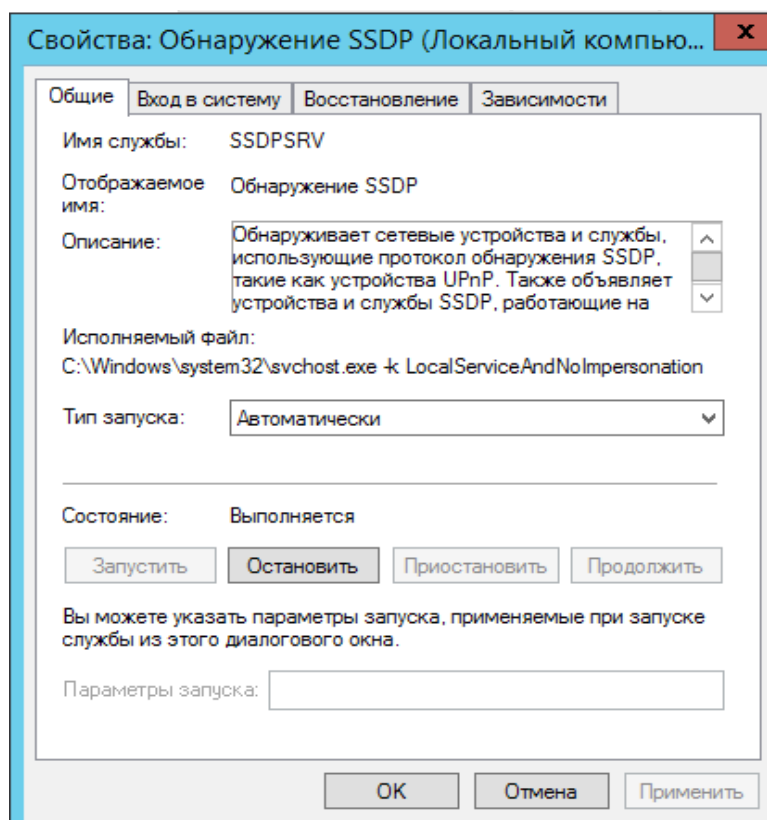


Рисунок 32 - Проверка службы Обнаружение SSDP

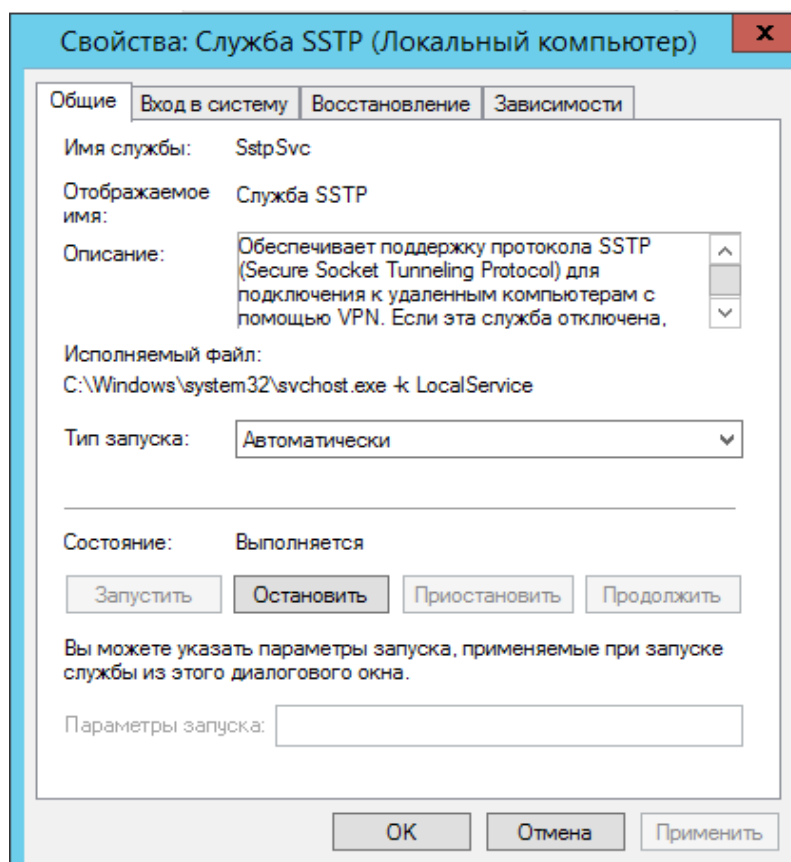


Рисунок 33 - Проверка службы Служба SSTP

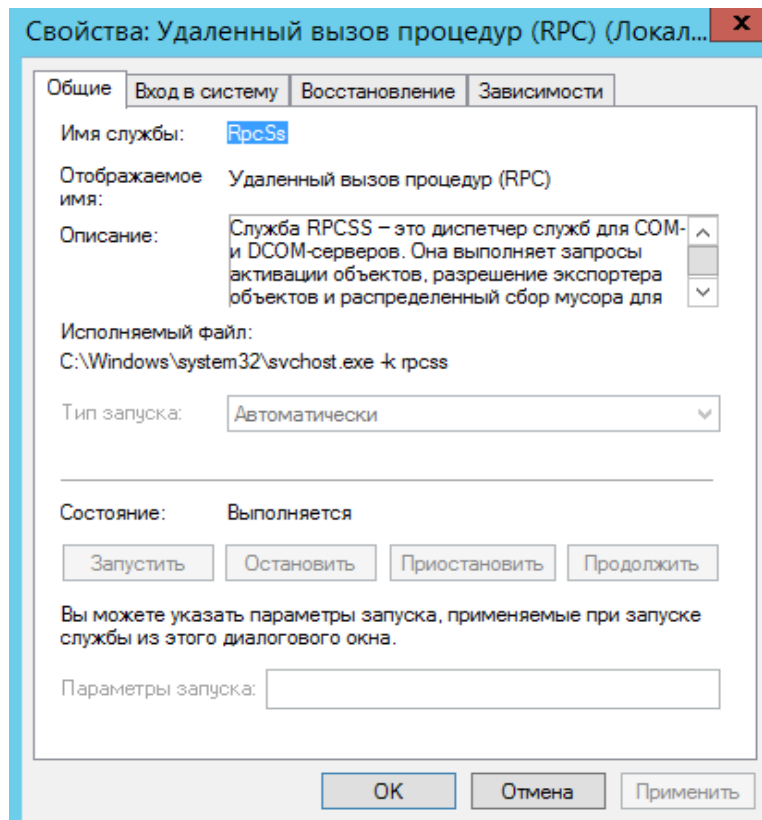


Рисунок 34 - Проверка службы Удаленный вызов процедур (RPC)

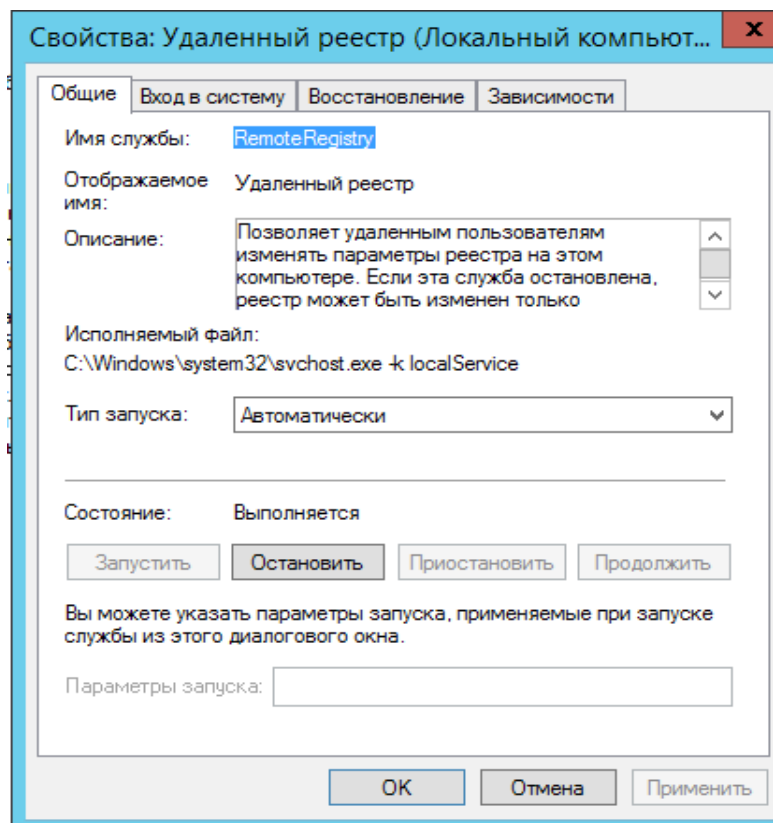


Рисунок 35 - Проверка службы Удаленный реестр

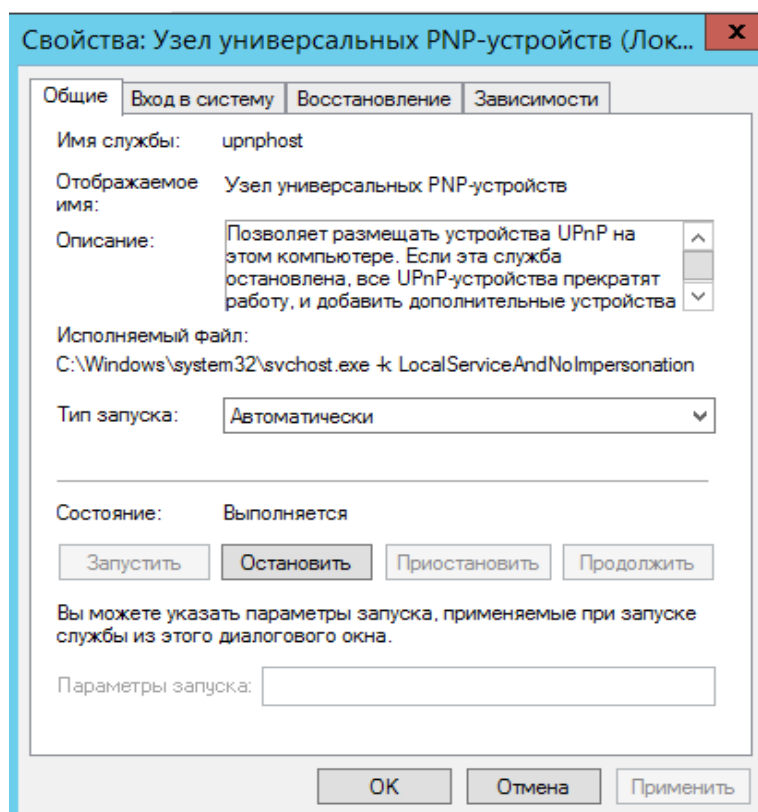


Рисунок 36 - Проверка службы Узел универсальных PNP-устройств

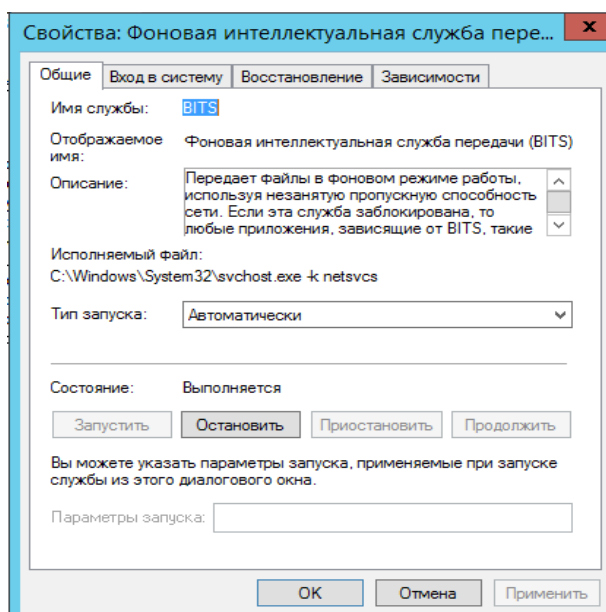


Рисунок 37 - Проверка службы Фоновая интеллектуальная служба передачи (BITS)

Для перечисленных локальных служб надо указать тип запуска Автоматически. При необходимости запустить службу.

В Центре управления сетями и общим доступом необходимо настроить

дополнительные параметры общего доступа. Для всех сетевых профилей следует включить сетевое обнаружение и общий доступ к файлам и принтерам. В профиле «Все сети» отключить общий доступ с парольной защитой. Результат представлен на рисунках с 38 по 40.

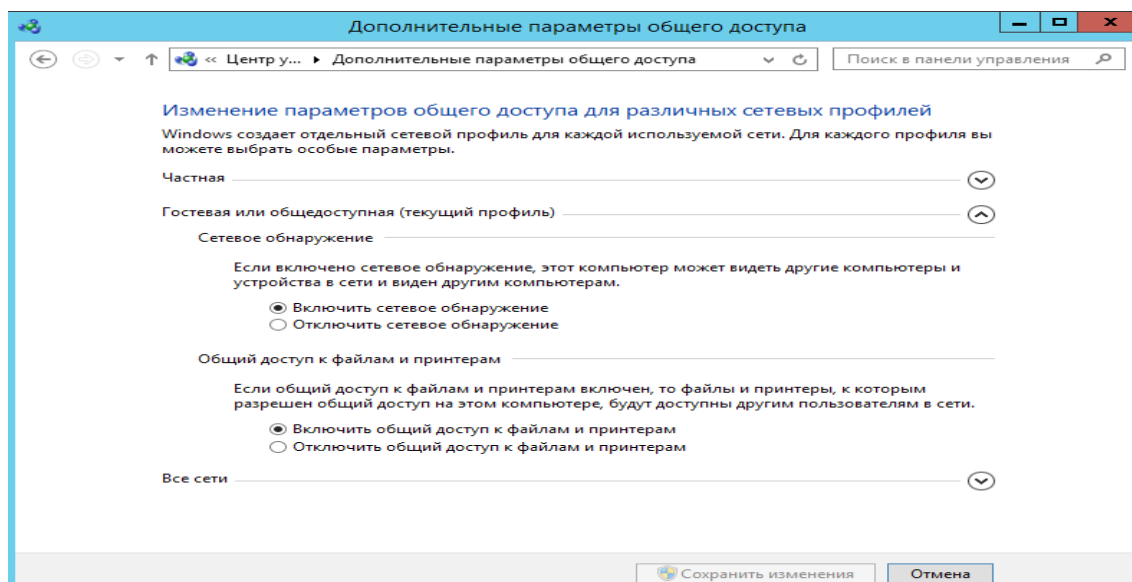


Рисунок 38 - Настройка профиля для гостевой или общедоступной сети

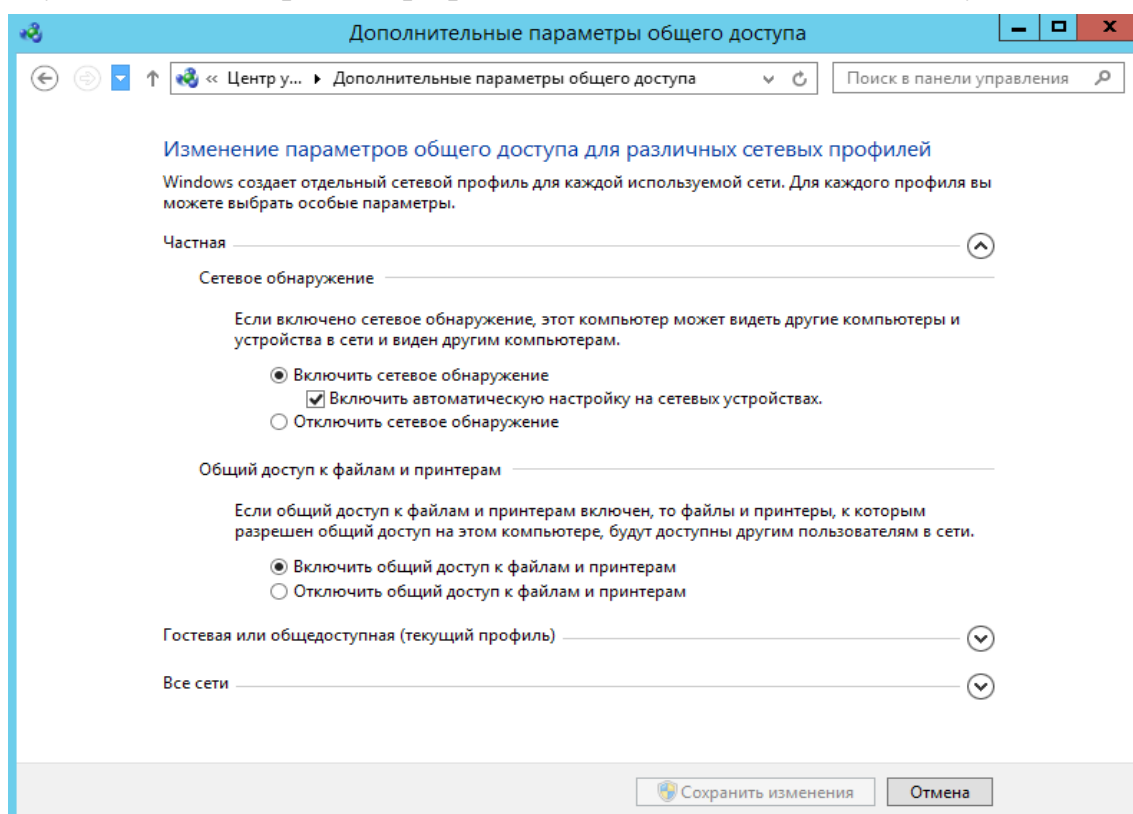


Рисунок 39 - Настройка профиля для частной сети

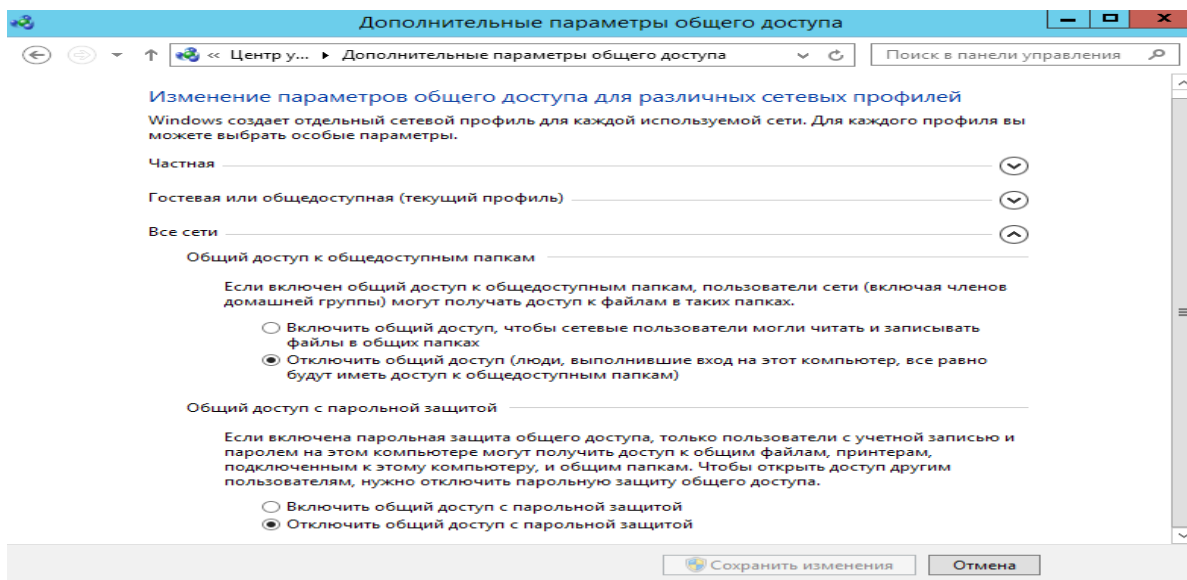


Рисунок 40 - Настройка профиля для всех сетей

После настройки гостевой ОС, необходимо выполнить перезагрузку ВМ и проверить работоспособность всех запущенных служб и сохранения настроек сетевых профилей.

3.3 Создание ВМ с установленной гостевой ОС Windows Server 2012 R2, являющейся сервером авторизации

ВМ 2 была получена путем клонирования ВМ 1. Для этого в менеджере VirtualBox необходимо выбрать функцию «Клонировать». Результат представлен на рисунке 41.

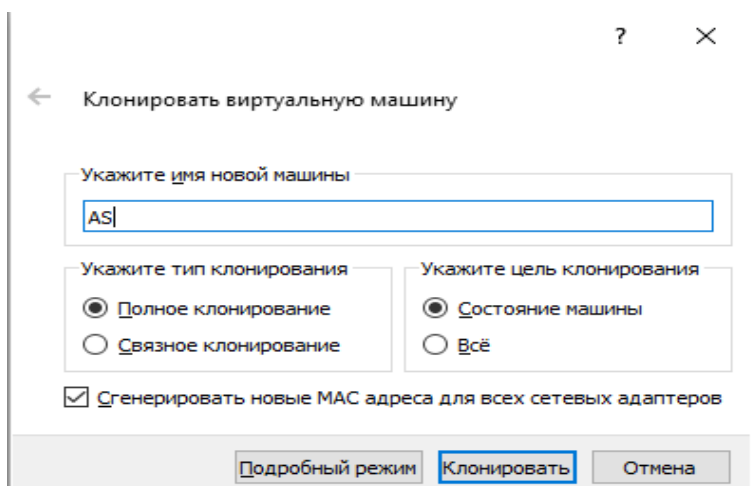


Рисунок 41 - Клонирование ВМ 1 с новым именем

Для настройки VM 2 с гостевой ОС Windows Server 2012 R2 необходимо запустить программу Oracle VirtualBox Менеджер. После запуска выбрать VM 2 и нажать кнопку «Настроить» на панели инструментов.

Была произведена настройка виртуальной машины аналогичная настройке VM 1. Были настроены: общий буфер обмена, порядок загрузки, адаптер сети и общая папка. Результат представлен на рисунках с 42 по 45.

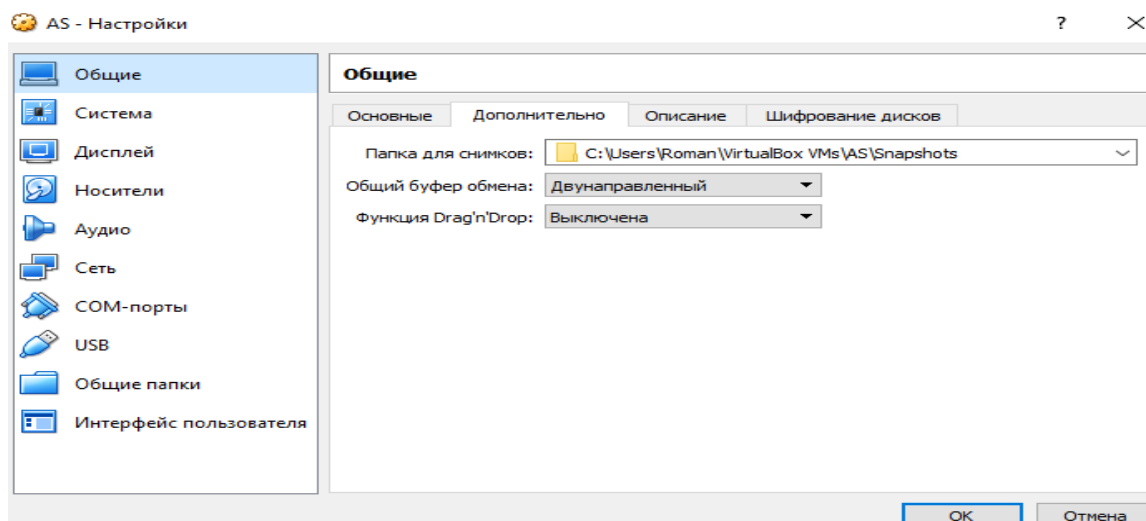


Рисунок 42 - Настройка общего буфера обмена

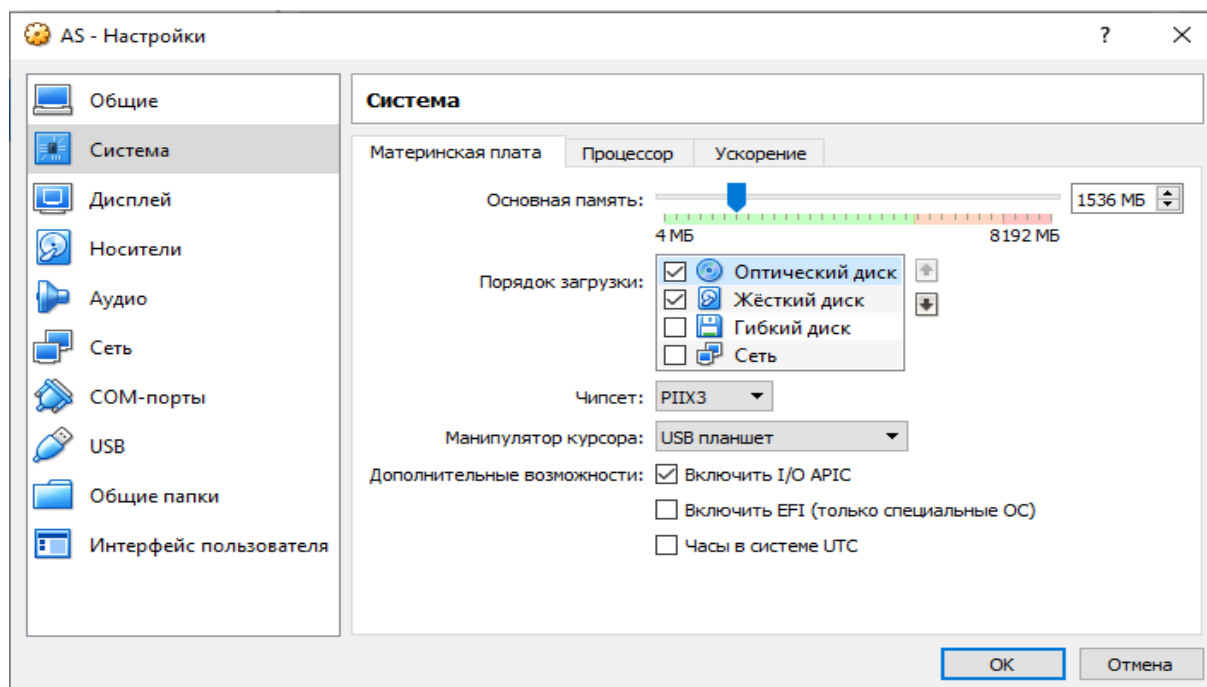


Рисунок 43 - Настройка порядка загрузки гостевой ОС

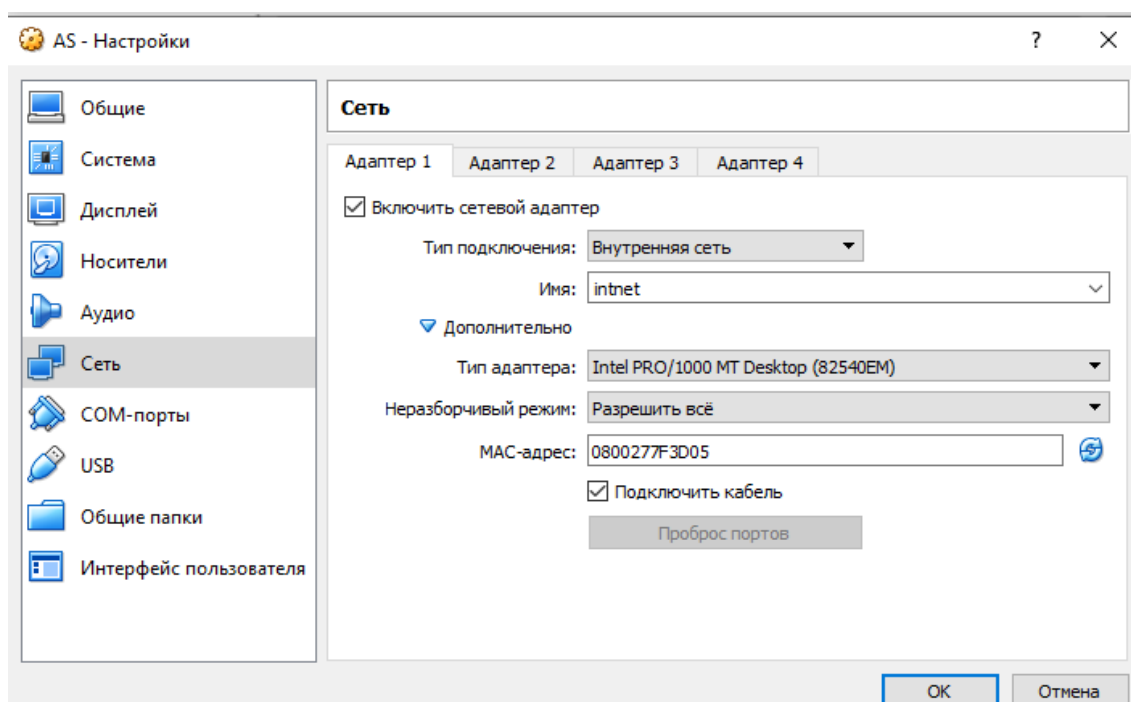


Рисунок 44 — Настройка сетевого адаптера VM2

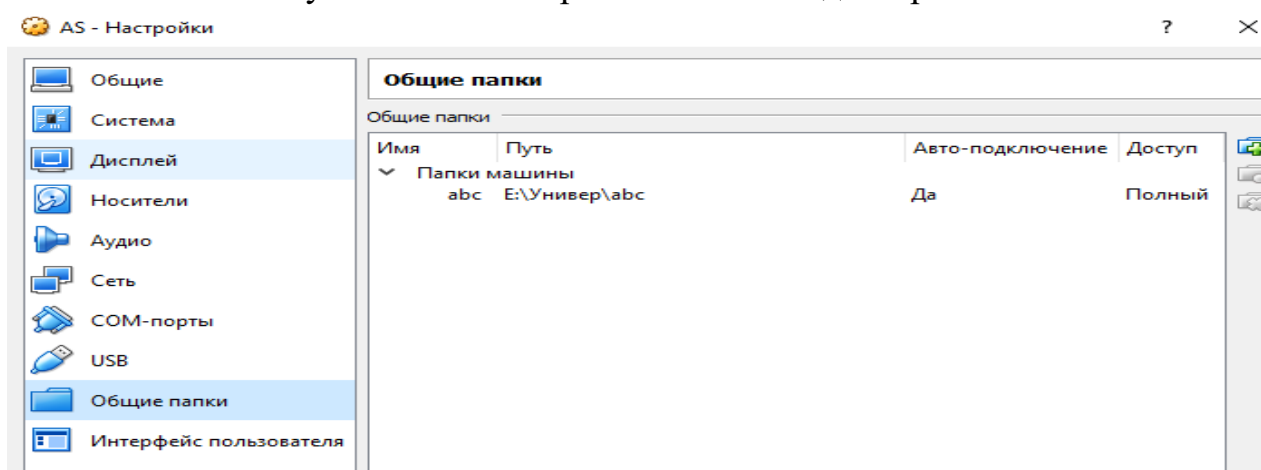


Рисунок 45 - Настройка общей папки

Для этой виртуальной машины был изменен идентификатор безопасности (SID). Это необходимо чтобы идентификатор безопасности не совпадал с идентификатором безопасности VM 1. Была запущена утилита Sysprep. Она находится по следующему пути – C:\Windows\system32\Sysprep. В этом каталоге находится программа sysprep.exe. После запуска программы появилось диалоговое окно программы подготовки системы, в котором необходимо выбрать параметр «Подготовка к использованию». Остальные параметры оставлены по умолчанию. После завершения работы выполнить перезагрузку.

После перезагрузки настроить параметры системы такие как «Страна или регион». «Язык приложений», «Раскладка клавиатуры». Значения этих параметров оставить по умолчанию. На заключительном этапе настройки указать пароль администратора. Результаты представлены на рисунках 46 и 47.

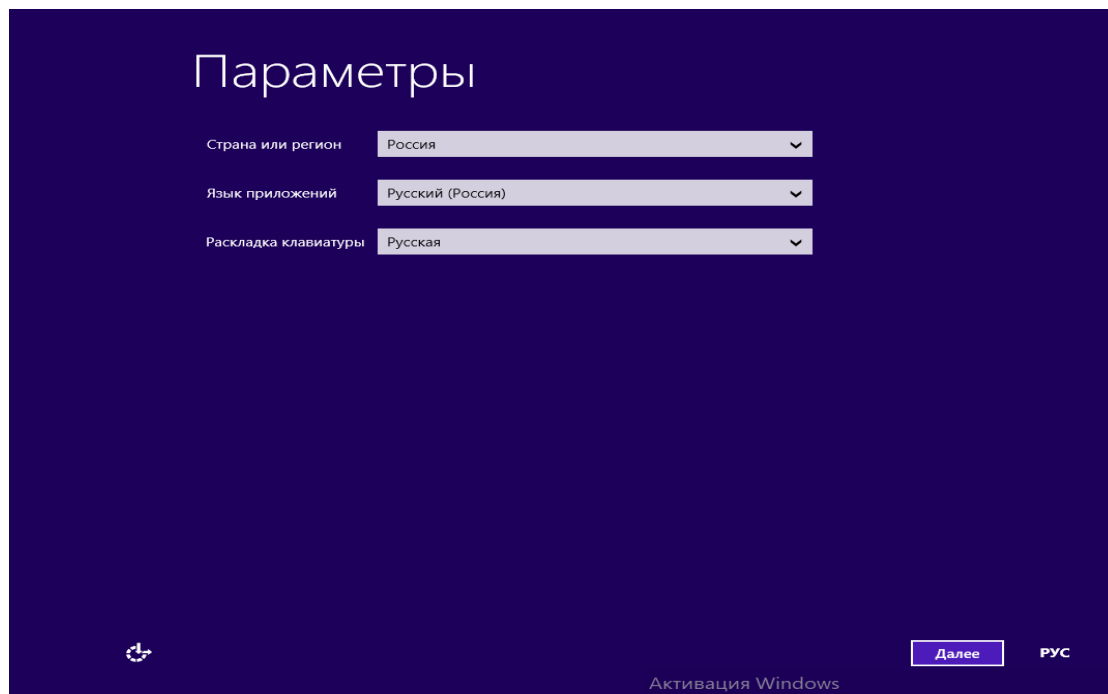


Рисунок 46 – Настройка региональных параметров

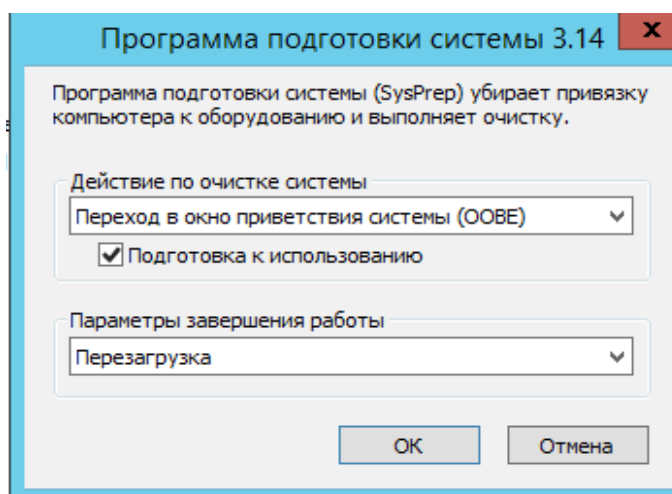


Рисунок 47 - Настройка параметров утилиты sysprep.exe

При запуске ВМ 2 необходимо изменить имя компьютера. Для этого необходимо запустить программу «Диспетчер серверов» и выбрать функцию «Имя компьютера». Оно было изменено на AS. После этого необходимо перезагрузить виртуальную машину. Результат представлен на рисунке 48.

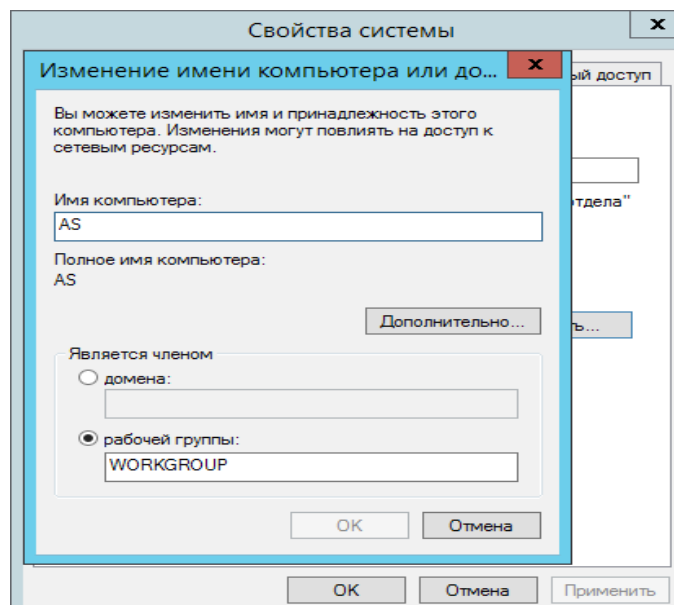


Рисунок 48 - Изменение имени компьютера

После перезагрузки необходимо установить для сетевого адаптера статический IP-адрес - 192.168.100.2 и маску подсети - 255.255.255.0. При этом адрес настроить для протокола IP версии 4. Отключить использование IP-адресов версии 6. В качестве шлюза по умолчанию указать адрес сервера «vGate-DC» - 192.168.100.1. Необходимо установить адрес предпочитаемого DNS-сервера - 192.168.100.1. Результат представлен на рисунке 49.

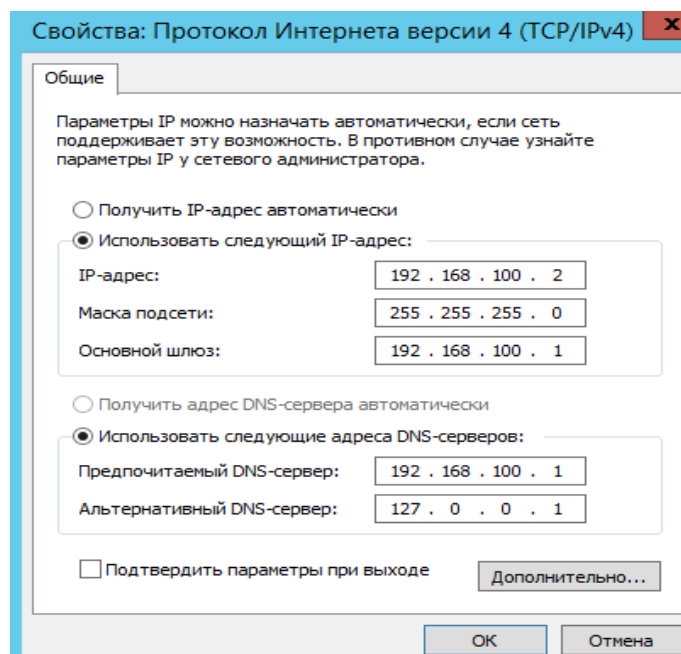


Рисунок 49 - Настройка сетевого адаптера

С помощью Диспетчера серверов необходимо скорректировать настройки имени сервера. Необходимо добавить «Основной DNS-суффикс этого компьютера», который совпадает с именем зоны прямого просмотра. После изменения настроек ВМ необходимо перезагрузить. Результат представлен на рисунке 50.

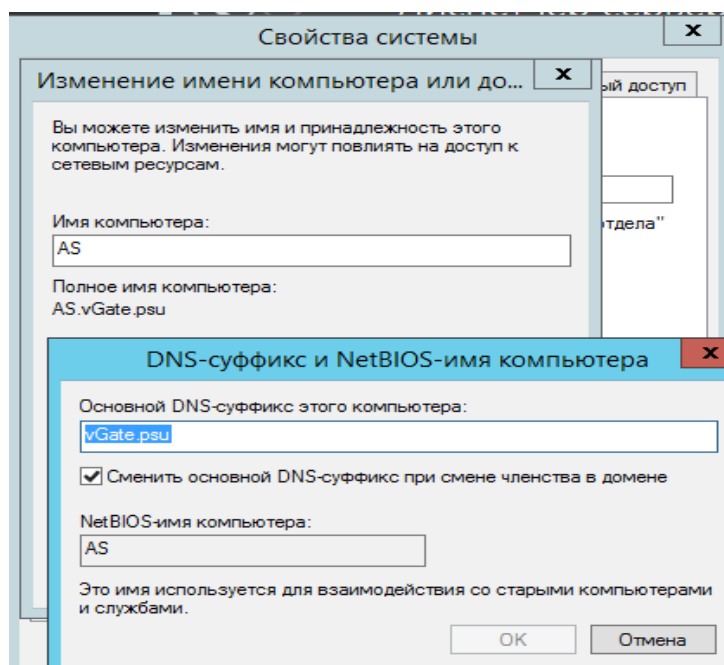


Рисунок 50 - Добавление DNS-суффикса

3.4 Создание ВМ с установленной гостевой ОС Windows 8.1, являющейся рабочим местом администратора виртуальной инфраструктуры

Для создания ВМ с гостевой ОС Windows 8.1 необходимо запустить программу Oracle VirtualBox Менеджер. После запуска нажать кнопку «Создать» на панели инструментов. В диалоговом окне мастера создания ВМ на первом этапе надо указать имя ВМ, тип ОС и версию ОС. На следующем шаге определяется объем оперативной памяти, выделяемой ВМ. Он зависит от версии ОС. Это значение можно при необходимости изменить. Затем необходимо указать вариант создания нового виртуального жесткого диска. На следующем этапе надо выбрать формат хранения, выбрав динамический виртуальный жесткий диск. На заключительном этапе надо указать имя файла

виртуального жесткого диска, каталог в котором он будет храниться и максимальный размер файла динамического виртуального жесткого диска.

Было назначено имя виртуальной машины - «WS-AVI», тип ОС - «Microsoft Windows», версия операционной системы - «Microsoft 8.1 (64-bit)», объем оперативной памяти - 1024МБ и был динамический виртуальный жесткий диск. Результат представлен на рисунке 51.

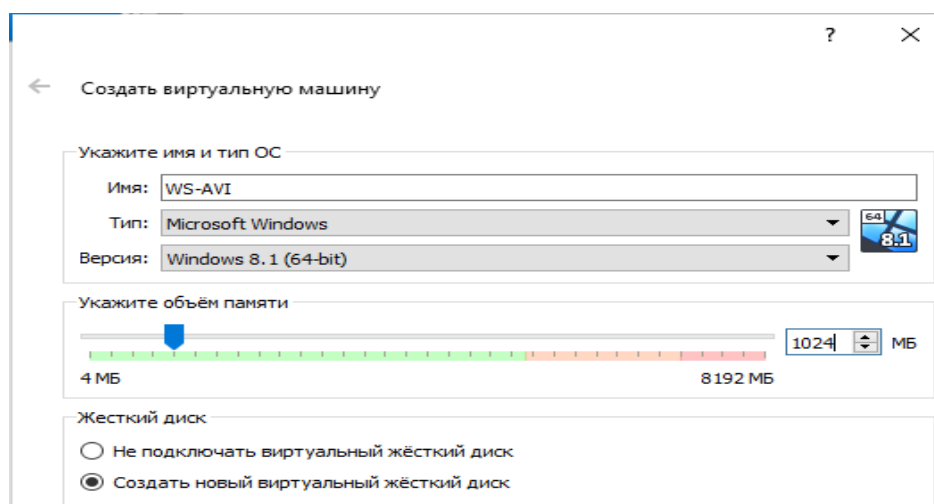


Рисунок 51 – Настройка имени, типа и версии гостевой ОС для VM 3

Остальные настройки аналогичны настройкам VM 1 и VM 2. Были настроены: общий буфер обмена, порядок загрузки, адаптер сети и общая папка. Результат представлен на рисунках с 52 по 55.

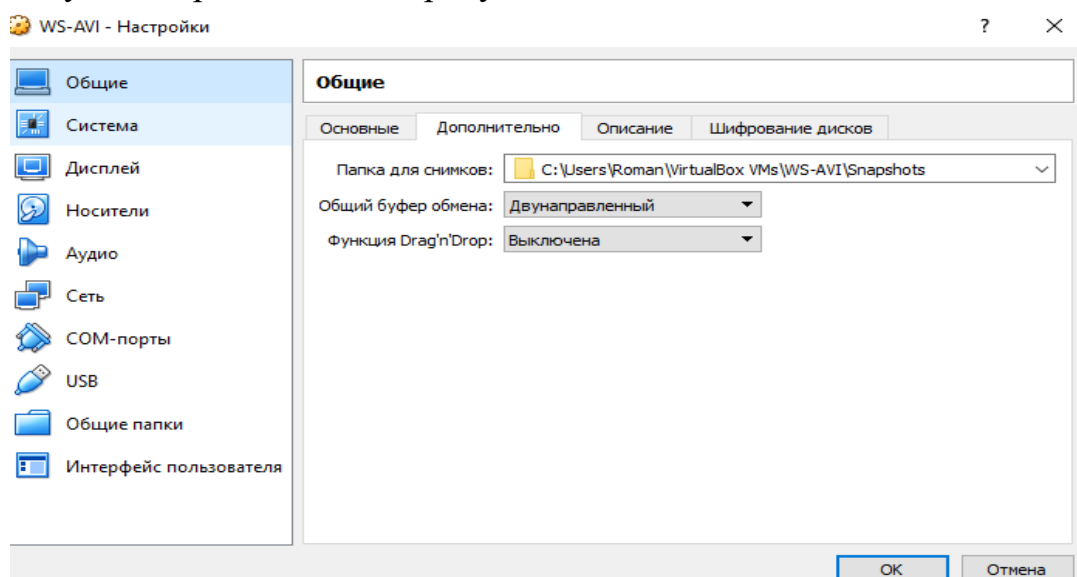


Рисунок 52 - Настройка общего буфера обмена

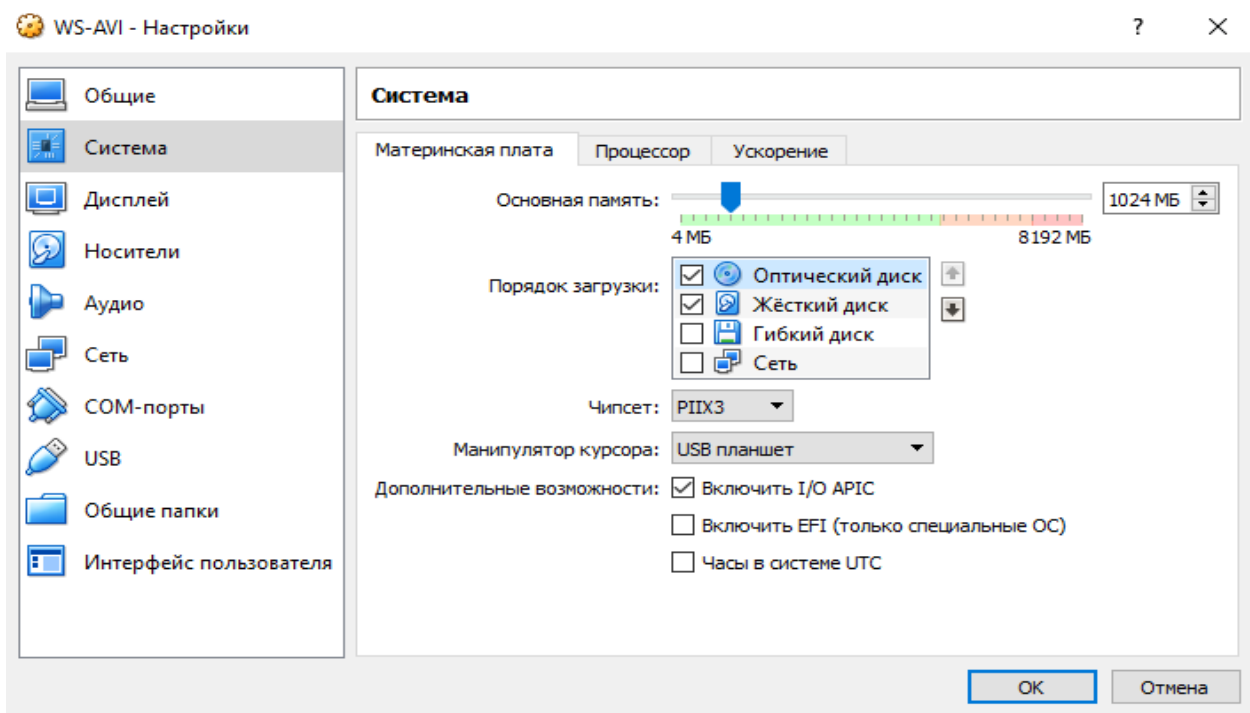


Рисунок 53 - Настройка порядка загрузки гостевой ОС

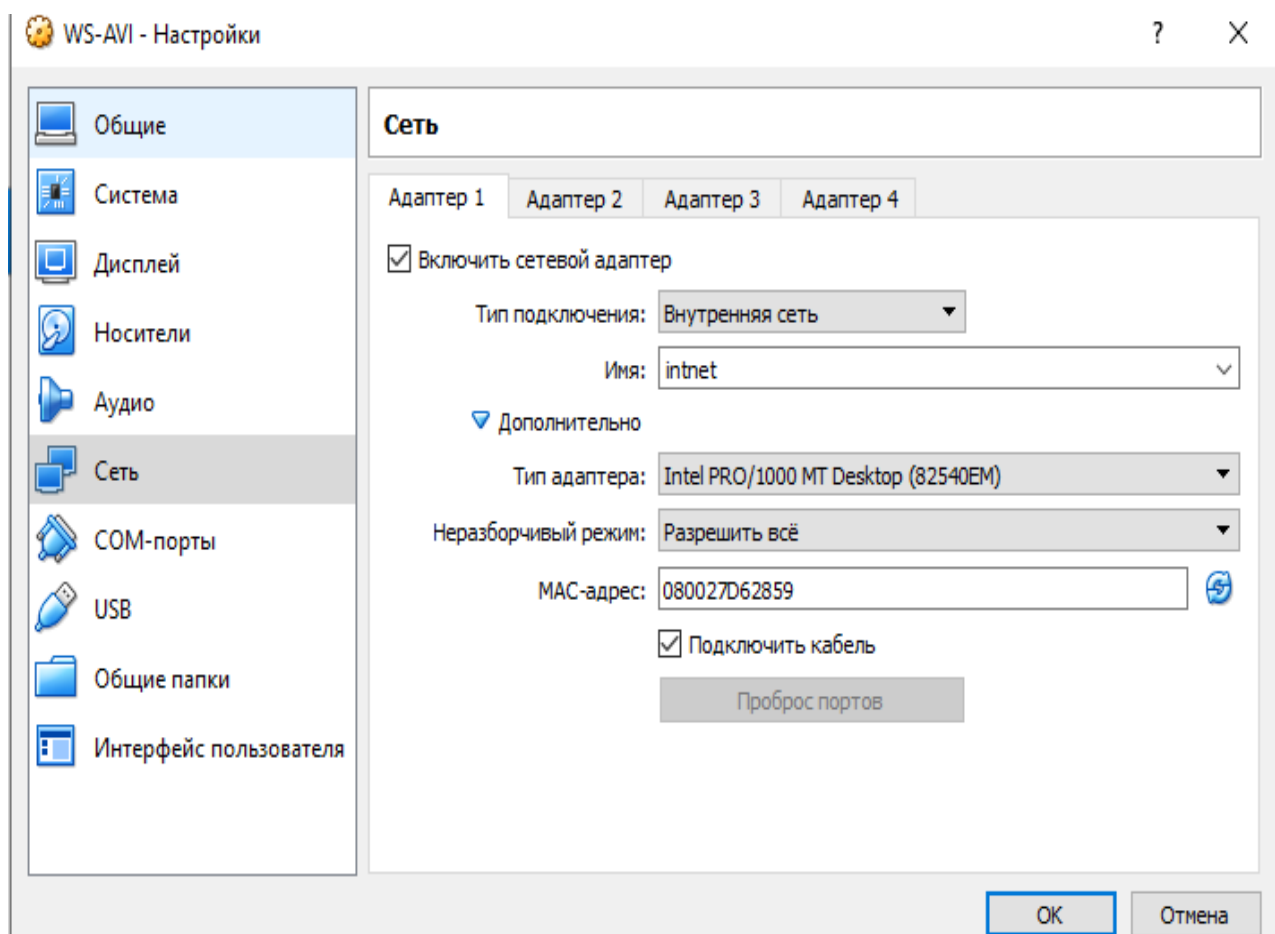


Рисунок 54 — Настройка сетевого адаптера VM3

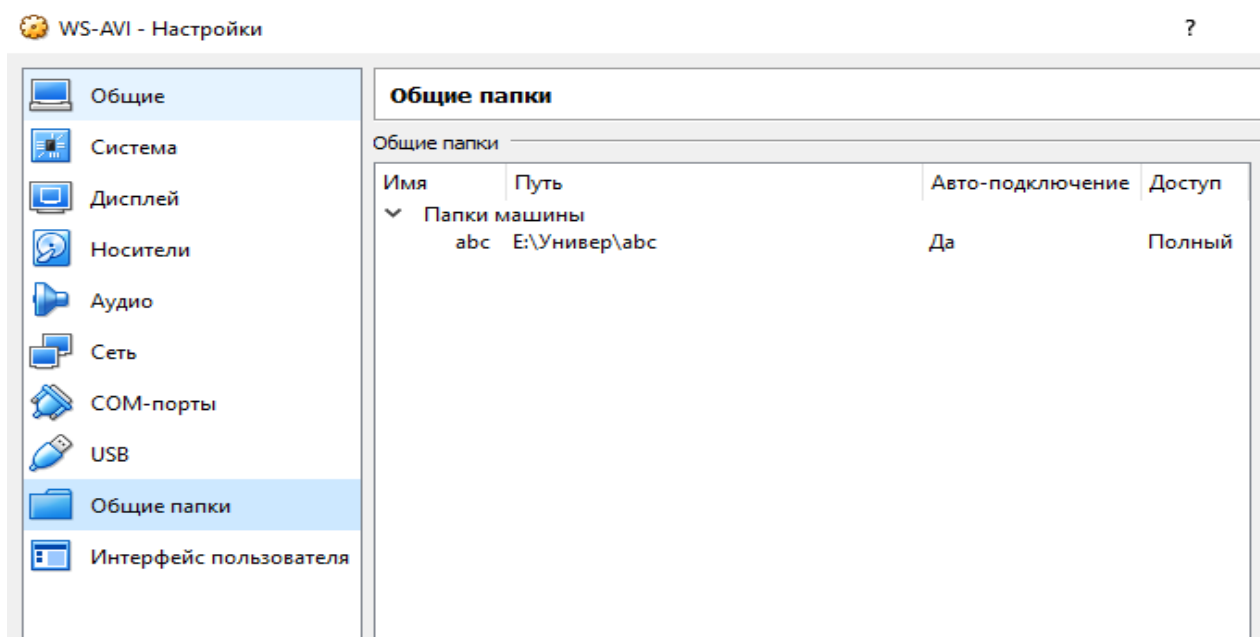


Рисунок 55 - Настройка общей папки

Гостевая ОС устанавливалась в соответствии с документацией разработчика ОС — компании Microsoft.

Были настроены параметры учетной записи Администратора — имя и пароль. Имя — Администратор, пароль — P.ssw0rd.

После установки гостевой ОС, запуска VM3 и входа с использованием учетной записи администратора необходимо установить дополнения гостевой ОС для VM.

Далее необходимо было изменить имя компьютера. Для этого через поиск необходимо запустить «Просмотр имени компьютера» и выбрать функцию «Переименование компьютера». Оно было изменено на WS-AVI. После этого необходимо перезагрузить виртуальную машину Результат представлен на рисунке 56.

Компьютер

Имя компьютера

WS-AVI

Рисунок 56 - Изменение имени компьютера

После перезагрузки необходимо установить для сетевого адаптера

статический IP-адрес - 192.168.100.11. При этом адрес настроить для протокола IP версии 4. Отключить использование IP-адресов версии 6. В качестве шлюза по умолчанию указать адрес сервера «vGate-DC» - 192.168.100.1 и маску подсети - 255.255.255.0. Установить адрес предпочитаемого DNS-сервера - 192.168.100.1. Результат представлен на рисунке 57.

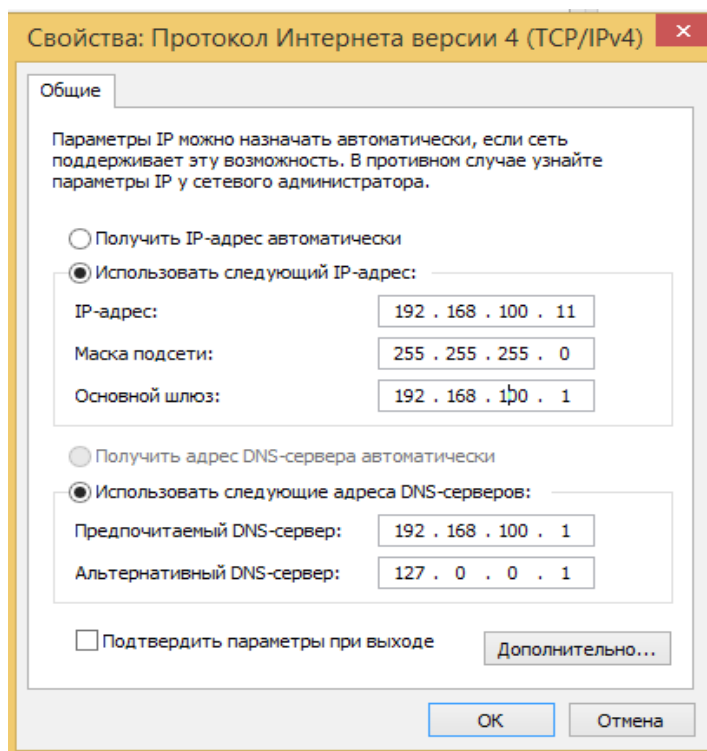


Рисунок 57 - Настройка сетевого адаптера

После настройки гостевой ОС, необходимо выполнить перезагрузку ВМ и проверить сохранение настроек сети.

3.5 Создание ВМ с установленным гипервизором Hyper-V Server 2012, R2, являющейся сервером виртуализации

Для создания ВМ с установленным гипервизором Hyper-V Server 2012 R2 необходимо запустить программу Oracle VirtualBox Менеджер. После запуска нажать кнопку «Создать» на панели инструментов. В диалоговом окне мастера создания ВМ на первом этапе надо указать имя ВМ, тип ОС и версию ОС. На следующем шаге определяется объем оперативной памяти, выделяемой ВМ. Он зависит от версии ОС. Это значение можно при необходимости изменить. Затем

необходимо указать вариант создания нового виртуального жесткого диска. На следующем этапе надо выбрать формат хранения, выбрав динамический виртуальный жесткий диск. На заключительном этапе надо указать имя файла виртуального жесткого диска, каталог в котором он будет храниться и максимальный размер файла динамического виртуального жесткого диска.

Было назначено имя виртуальной машины - «VGATE-HSV», тип ОС- «Microsoft Windows», версия операционной системы - «Microsoft 2012 (64-bit)», объем оперативной памяти - 512МБ и был выбран динамический виртуальный жесткий диск. Результат представлен на рисунке 58.

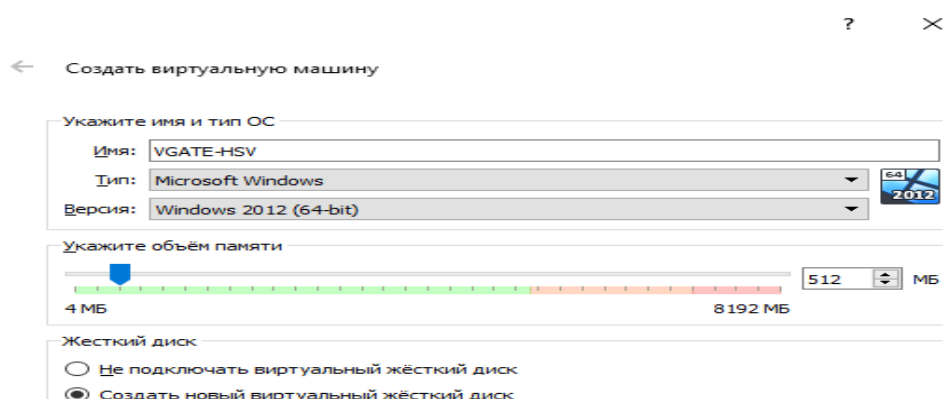


Рисунок 58 – Настройка имени, типа и версии гостевой ОС для ВМ 3

Остальные настройки аналогичны настройкам ВМ 1 и ВМ 2. Результат представлен на рисунках с 59 по 62.

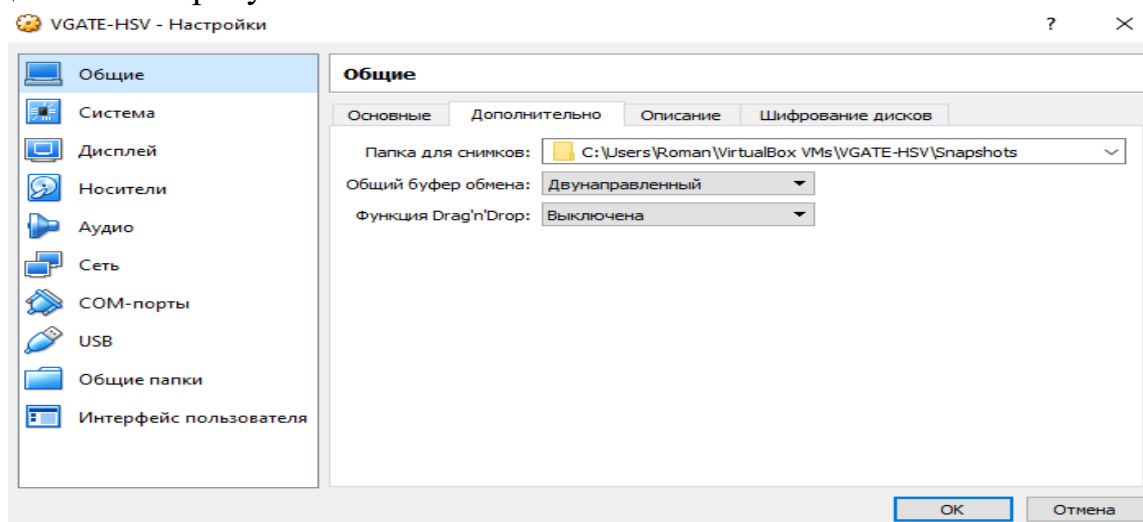


Рисунок 59 - Настройка общего буфера обмена

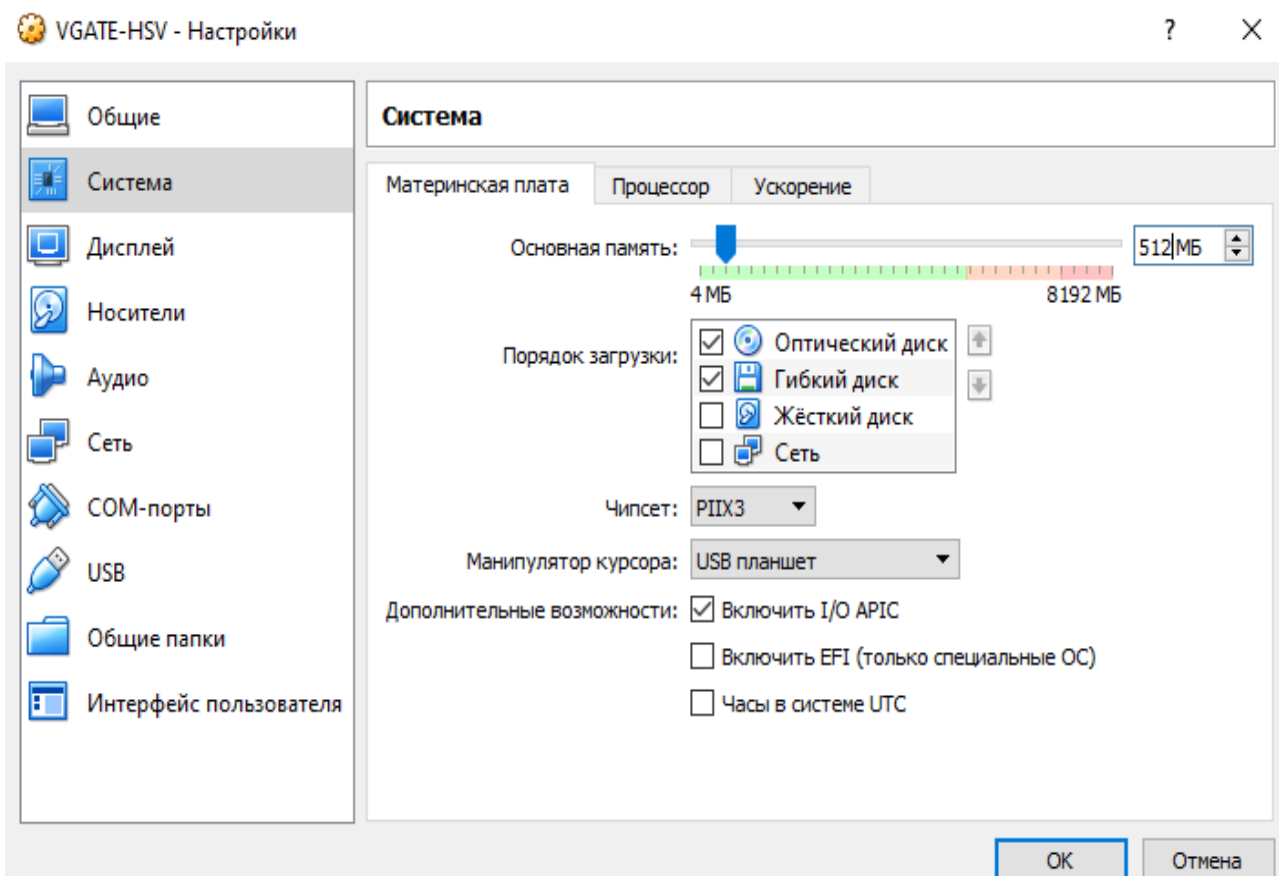


Рисунок 60 - Настройка порядка загрузки гостевой ОС

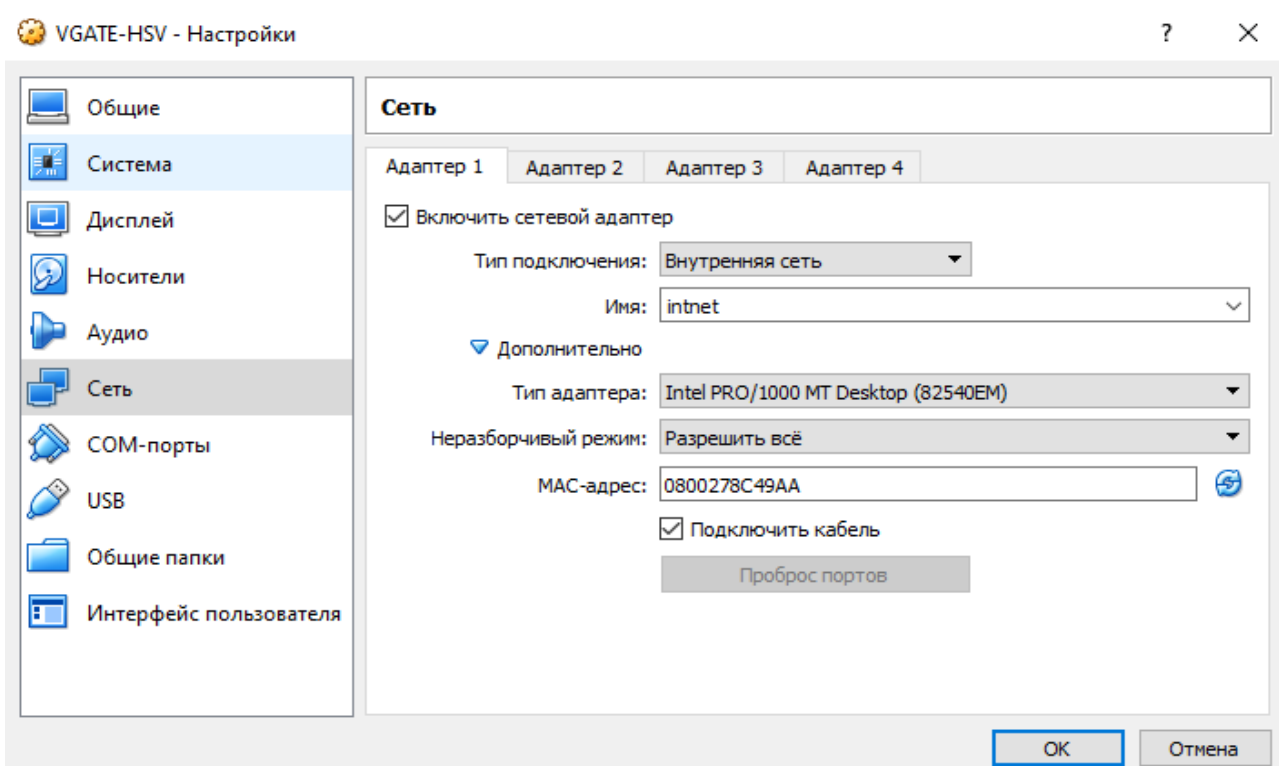


Рисунок 61 — Настройка сетевого адаптера VM4

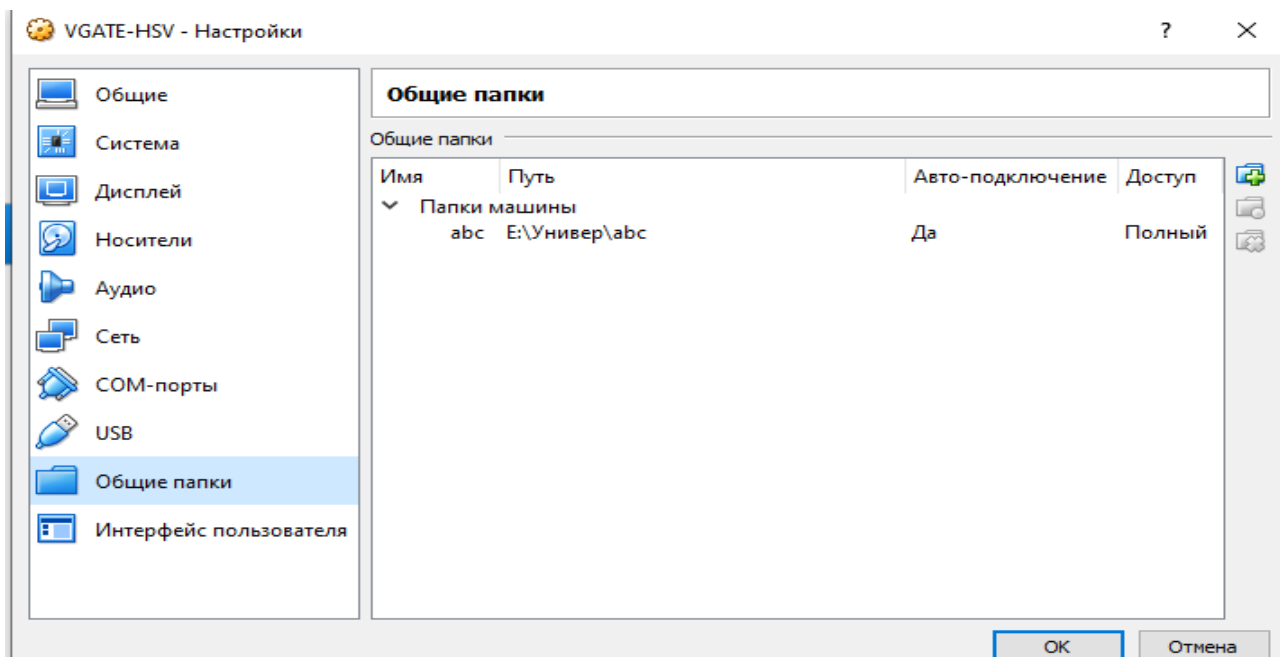


Рисунок 62 - Настройка общей папки

Гостевая ОС устанавливалась в соответствии с документацией разработчика ОС — компании Microsoft.

Были настроены параметры учетной записи Администратора — имя и пароль. Имя — Администратор, пароль — P.ssw0rd.

После установки гостевой ОС, запуска VM4 и входа с использованием учетной записи администратора необходимо установить дополнения гостевой ОС для VM. Для этого необходимо подключить образ диска Дополнений гостевой ОС в меню устройства. С помощью командной строки запустить текстовый редактор Блокнот, используя команду `notepad`. В меню «Файл» выбрать команду «Открыть». Для параметра «Тип файлов» установить значение «Все файлы». Выбрать устройство для работы с оптическими дисками и открыть содержимое подключенного образа оптического диска с дополнениями гостевой ОС. Выбрать файл `VBoxWindowsAdditions-amd64.exe` щелкнув по его имени один раз правой клавишей мыши. В контекстном меню выбрать команду «Запуск от имени администратора». Используя мастер установки установить дополнения гостевой ОС и выполнить перезагрузку VM. Результат представлен на рисунке 63.

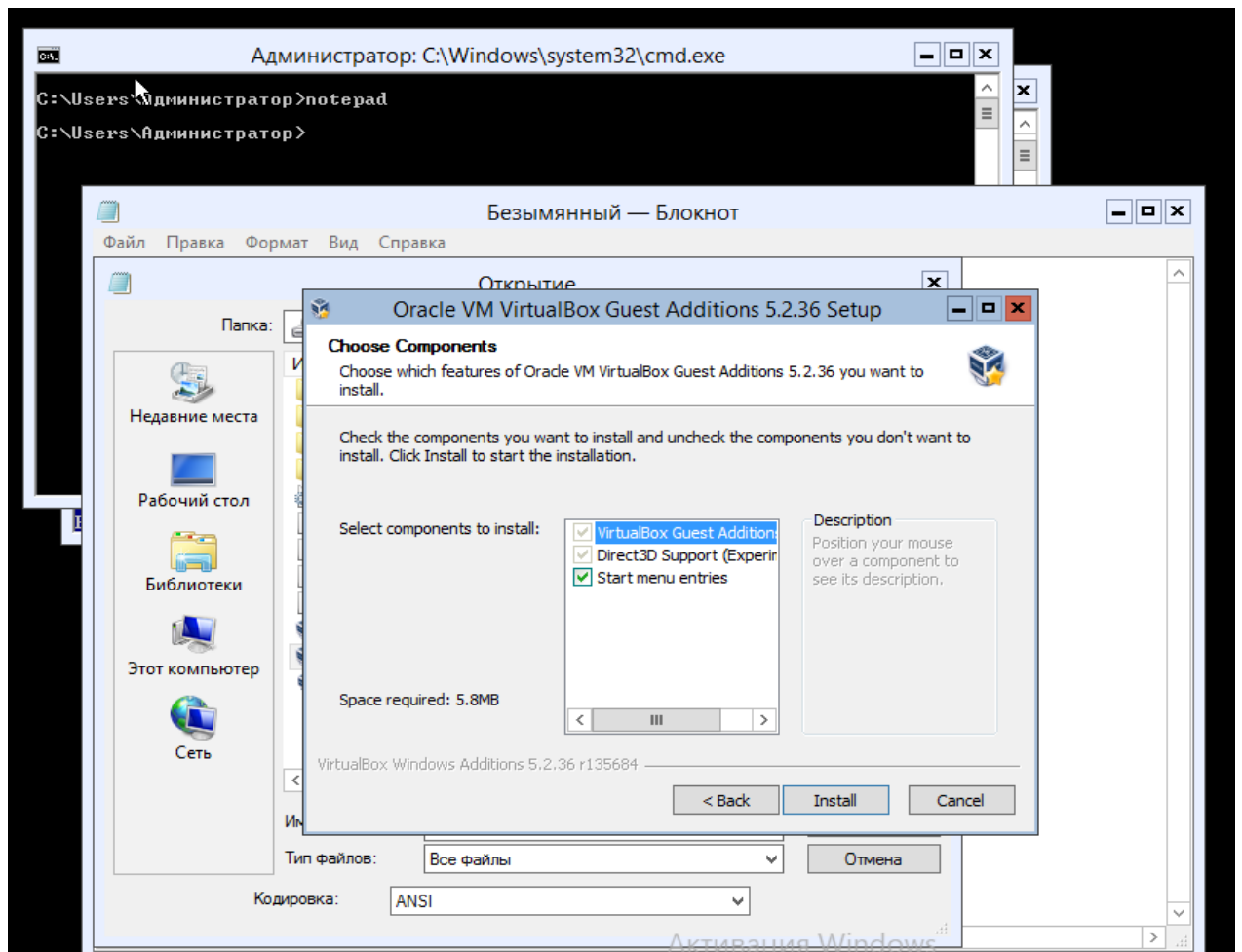


Рисунок 63 — Установка дополнений гостевой ОС на VM4

После установки гостевой ОС, запуска VM4 и входа с использованием учетной записи администратора необходимо было изменить имя компьютера. Для этого с помощью утилиты `sconfig` выбрать параметр 2. Имя компьютера было изменено на VGATE-HSV. После этого необходимо перезагрузить виртуальную машину. Результат представлен на рисунке 64.

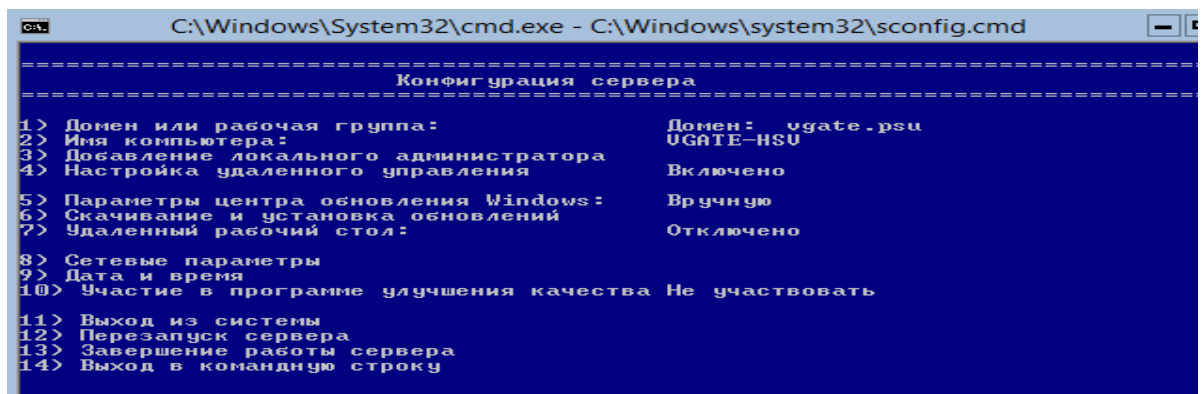


Рисунок 64 - Изменение имени компьютера

Далее необходимо проверить и настроить системную дату и время. Для изменения даты и времени надо выбрать параметр 9. После ввода его номера на экран выводится диалоговое окно настройки даты и времени. Результат представлен на рисунке 65.

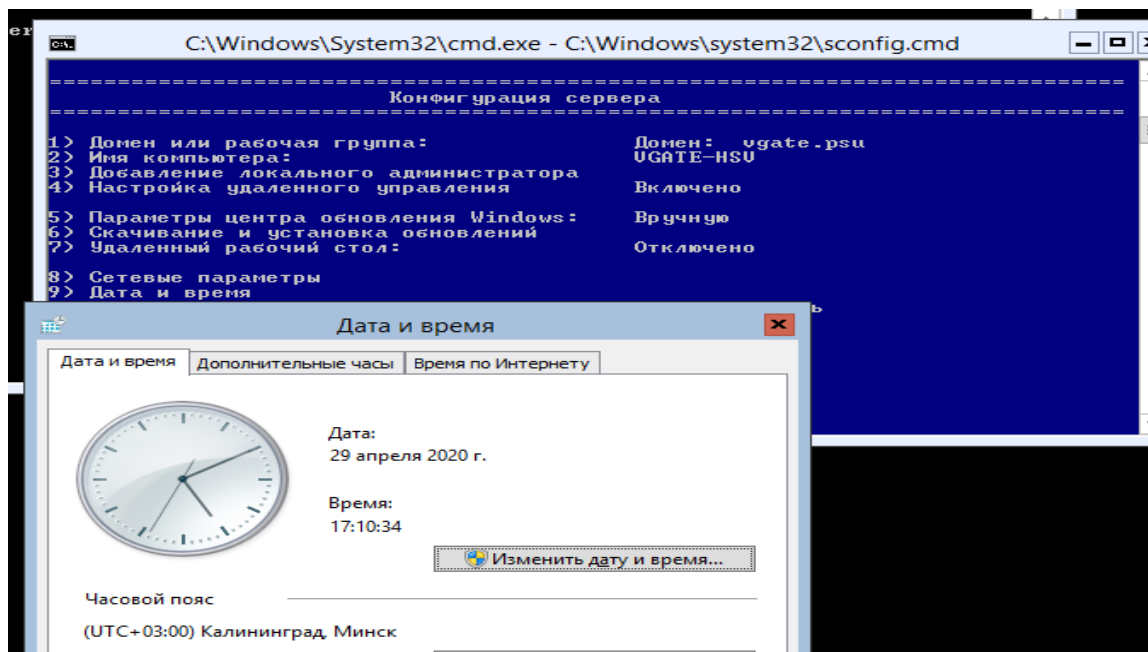


Рисунок 65 - Настройка даты и времени

Необходимо изменить язык по умолчанию. Для получения текущей локализации необходимо, использовать командлет `Get-WinDefaultInputMethodOverride` в консоли Windows PowerShell. Для изменения языка по умолчанию нужно использовать команду `Set-WinDefaultInputMethodOverride "0409:00000409"`. После этого необходимо перезагрузить ВМ. Результат представлен на рисунках 66 и 67.

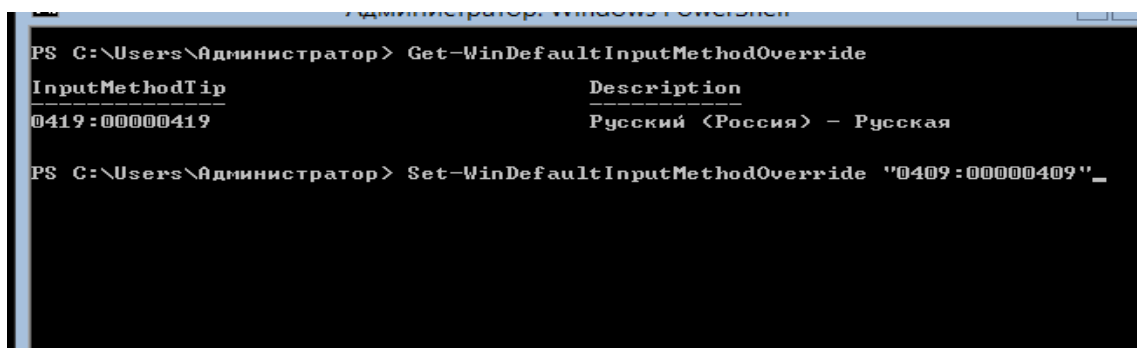


Рисунок 66 - Язык по умолчанию и его изменение

```

PS C:\Users\Администратор> get-WinDefaultInputMethodOverride
InputMethodTip                                     Description
-----
0409:00000409                                     Английский <США> - США

PS C:\Users\Администратор> _

```

Рисунок 67 - Измененный язык по умолчанию

Далее необходимо установить для сетевого адаптера статический IP-адрес - 192.168.100.12. При этом адрес настроить для IP версии 4. Отключить использование IP-адресов версии 6. В качестве шлюза по умолчанию указать адрес сервера «vGate-DC» - 192.168.100.1. Установить адрес предпочитаемого DNS- сервера - 192.168.100.1. Результат представлен на рисунках 68 и 69.

```

C:\Windows\System32\cmd.exe - C:\Windows\system32\sconfig.cmd
Введите новый основной DNS-сервер <для отмены оставьте пустым>: 192.168.100.1
Введите альтернативный DNS-сервер <для отмены оставьте пустым>: 127.0.0.1
Альтернативный DNS-сервер установлен.

-----
Параметры сетевого адаптера
-----

Индекс адаптера          11
Описание                 Адаптер рабочего стола Intel(R) PRO/1000 MT
IP-адрес                 192.168.100.12 fe80::e5ef:5dc8:e59a:1498
Маска подсети            255.255.255.0
DHCP включен             Ложь
Шлюз по умолчанию       192.168.100.1
Основной DNS-сервер      192.168.100.1
Альтернативный DNS-сервер 127.0.0.1

1> Установка адреса сетевого адаптера
2> Установить DNS-серверы
3> Очистить параметры DNS-сервера
4> Вернуться в главное меню

Выберите параметр: _

```

Рисунок 68 - Настройка сетевого адаптера

```

Администратор: Windows PowerShell
PS C:\Users\Администратор> Disable-NetAdapterBinding -InterfaceAlias "Ethernet 2" -ComponentID ms_tcpip6
PS C:\Users\Администратор> ipconfig

Настройка протокола IP для Windows

Ethernet adapter Ethernet 2:

    DNS-суффикс подключения . . . . . : 
    IPv4-адрес . . . . . : 192.168.100.12
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз . . . . . : 192.168.100.1

Туннельный адаптер isatap.{4863D1B3-612A-44EF-954F-09707D3C59F3}:

    Состояние среды. . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . : 

PS C:\Users\Администратор> _

```

Рисунок 69 - Отключение использования IP-адресов версии 6

Далее необходимо установить компоненты .NET Framework 3.5. Для этого необходимо к ВМ с гостевой ОС Hyper-V Server 2012 R2 подключить образ оптического диска с дистрибутивом ОС Windows Server 2012 R2. В PowerShell использовать команду `Add-WindowsFeature NET-Framework-Core -Source D:\sources\sxs`. После установки проверить с помощью команды `Get-WindowsOptionalFeature -Online | Where FeatureName -Like "NetFx3"`. Результат представлен на рисунке 70.

```
PS C:\Users\Администратор> Add-Windowsfeature NET-Framework-Core -Source D:\sources\sxs
```

Success	Restart	Needed	Exit Code	Feature Result
True	No		Success	<.NET Framework 3.5 (включает .NET 2.0...

ПРЕДУПРЕЖДЕНИЕ: Автоматическое обновление Windows отключено. Чтобы обеспечить автоматическое обновление только что установленной роли или компонента, включите "Центр обновления Windows".

```
PS C:\Users\Администратор> Get-WindowsOptionalFeature -Online | Where FeatureName -Like "NetFx3"
```

Feature Name : NetFx3
State : Enabled

```
PS C:\Users\Администратор>
```

Рисунок 70 - Установка компонента .NET Framework 3.5 и проверка установки

После установки всех настроек необходимо выполнить перезагрузку ВМ. После этого необходимо проверить сохраненные настройки.

4 Создание и конфигурирование локальной сети, состоящей из виртуальных машин

4.1 Проверка работоспособности сети до создания домена

Необходимо проверить работоспособность сети с помощью утилиты ping. Для этого необходимо запустить командную строку и используя утилиту ping проверить доступ к локальной сети к ВМ. В качестве параметра указывается сетевой адрес ВМ и сетевое имя. Проверки показали что ВМ 1 , ВМ 2 и ВМ 3 доступны между собой, а ВМ 4 нет. Результат представлен на рисунках с 71 по 82.

```
C:\Users\Администратор>ping 192.168.100.2
Обмен пакетами с 192.168.100.2 по 32 байтами данных:
Ответ от 192.168.100.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.2: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.100.2:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    <0% потерь>
    Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек

C:\Users\Администратор>ping AS
Обмен пакетами с AS [192.168.100.2] с 32 байтами данных:
Ответ от 192.168.100.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.2: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.100.2:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    <0% потерь>
    Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
```

Рисунок 71 - Проверка доступа с ВМ 1 к ВМ 2

```
C:\Users\Администратор>ping 192.168.100.11
Обмен пакетами с 192.168.100.11 по 32 байтами данных:
Ответ от 192.168.100.11: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.11: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.11: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.11: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.100.11:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    <0% потерь>
    Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек

C:\Users\Администратор>ping WS-AUI
Обмен пакетами с WS-AUI [192.168.100.11] с 32 байтами данных:
Ответ от 192.168.100.11: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.11: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.11: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.11: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.100.11:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    <0% потерь>
    Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
```

Рисунок 72 - Проверка доступа с ВМ 1 к ВМ 3

```

C:\Users\Администратор>ping 192.168.100.12

Обмен пакетами с 192.168.100.12 по с 32 байтами данных:
Ответ от 192.168.100.1: Заданный узел недоступен.
Ответ от 192.168.100.1: Заданный узел недоступен.
Ответ от 192.168.100.1: Заданный узел недоступен.
Ответ от 192.168.100.1: Заданный узел недоступен.

Статистика Ping для 192.168.100.12:
  Пакетов: отправлено = 4, получено = 4, потеряно = 0
  <0% потеря>

C:\Users\Администратор>ping UGATE-HSU

Обмен пакетами с UGATE-HSU [192.168.100.12] с 32 байтами данных:
Ответ от 192.168.100.1: Заданный узел недоступен.
Ответ от 192.168.100.1: Заданный узел недоступен.
Ответ от 192.168.100.1: Заданный узел недоступен.
Ответ от 192.168.100.1: Заданный узел недоступен.

Статистика Ping для 192.168.100.12:
  Пакетов: отправлено = 4, получено = 4, потеряно = 0
  <0% потеря>

```

Рисунок 73 - Проверка доступа с ВМ 1 к ВМ 4

```

C:\Users\Администратор>ping 192.168.100.1

Обмен пакетами с 192.168.100.1 по с 32 байтами данных:
Ответ от 192.168.100.1: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.1: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.1: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.1: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.100.1:
  Пакетов: отправлено = 4, получено = 4, потеряно = 0
  <0% потеря>
  Приблизительное время приема-передачи в мс:
  Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек

C:\Users\Администратор>ping UGATE-DC

Обмен пакетами с UGATE-DC [192.168.100.11] с 32 байтами данных:
Ответ от 192.168.100.1: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.1: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.1: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.1: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.100.1:
  Пакетов: отправлено = 4, получено = 4, потеряно = 0
  <0% потеря>
  Приблизительное время приема-передачи в мс:
  Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек

```

Рисунок 74 - Проверка доступа с ВМ 2 к ВМ 1

```

C:\Users\Администратор>ping 192.168.100.11

Обмен пакетами с 192.168.100.11 по с 32 байтами данных:
Ответ от 192.168.100.11: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.11: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.11: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.11: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.100.11:
  Пакетов: отправлено = 4, получено = 4, потеряно = 0
  <0% потеря>
  Приблизительное время приема-передачи в мс:
  Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек

C:\Users\Администратор>ping WS-AVI

Обмен пакетами с WS-AVI [192.168.100.11] с 32 байтами данных:
Ответ от 192.168.100.11: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.11: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.11: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.11: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.100.11:
  Пакетов: отправлено = 4, получено = 4, потеряно = 0
  <0% потеря>
  Приблизительное время приема-передачи в мс:
  Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек

```

Рисунок 75 - Проверка доступа с ВМ 2 к ВМ 3

```

C:\Users\Администратор>ping 192.168.100.12

Обмен пакетами с 192.168.100.12 по с 32 байтами данных:
Ответ от 192.168.100.2: Заданный узел недоступен.
Ответ от 192.168.100.2: Заданный узел недоступен.
Ответ от 192.168.100.2: Заданный узел недоступен.
Ответ от 192.168.100.2: Заданный узел недоступен.

Статистика Ping для 192.168.100.12:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)

C:\Users\Администратор>ping VGATE-HSU

Обмен пакетами с VGATE-HSU [192.168.100.12] с 32 байтами данных:
Ответ от 192.168.100.2: Заданный узел недоступен.
Ответ от 192.168.100.2: Заданный узел недоступен.
Ответ от 192.168.100.2: Заданный узел недоступен.
Ответ от 192.168.100.2: Заданный узел недоступен.

Статистика Ping для 192.168.100.12:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)

```

Рисунок 76 - Проверка доступа с ВМ 2 к ВМ 4

```

C:\Users\Администратор>ping 192.168.100.1

Обмен пакетами с 192.168.100.1 по с 32 байтами данных:
Ответ от 192.168.100.1: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.1: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.1: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.1: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.100.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
    Приблизительное время приема-передачи в мс:
        Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек

C:\Users\Администратор>ping VGATE-DC

Обмен пакетами с vgate-dc [192.168.100.1] с 32 байтами данных:
Ответ от 192.168.100.1: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.1: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.1: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.1: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.100.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
    Приблизительное время приема-передачи в мс:
        Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек

```

Рисунок 77 - Проверка доступа с ВМ 3 к ВМ 1

```

C:\Users\Администратор>ping 192.168.100.2

Обмен пакетами с 192.168.100.2 по с 32 байтами данных:
Ответ от 192.168.100.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.2: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.100.2:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
    Приблизительное время приема-передачи в мс:
        Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек

C:\Users\Администратор>ping AS

Обмен пакетами с AS [192.168.100.2] с 32 байтами данных:
Ответ от 192.168.100.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.2: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.100.2:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
    Приблизительное время приема-передачи в мс:
        Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек

```

Рисунок 78 - Проверка доступа с ВМ 3 к ВМ 2

```

C:\Users\Администратор>ping 192.168.100.12
Обмен пакетами с 192.168.100.12 по с 32 байтами данных:
Ответ от 192.168.100.11: Заданный узел недоступен.
Ответ от 192.168.100.11: Заданный узел недоступен.
Ответ от 192.168.100.11: Заданный узел недоступен.
Ответ от 192.168.100.11: Заданный узел недоступен.

Статистика Ping для 192.168.100.12:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    <0% потерь>

C:\Users\Администратор>ping UGATE-HSU
Обмен пакетами с UGATE-HSU [192.168.100.12] с 32 байтами данных:
Ответ от 192.168.100.11: Заданный узел недоступен.
Ответ от 192.168.100.11: Заданный узел недоступен.
Ответ от 192.168.100.11: Заданный узел недоступен.
Ответ от 192.168.100.11: Заданный узел недоступен.

Статистика Ping для 192.168.100.12:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    <0% потерь>
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    <0% потерь>
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек

```

Рисунок 79 - Проверка доступа с ВМ 3 к ВМ 4

```

C:\Users\Администратор>ping 192.168.100.1
Обмен пакетами с 192.168.100.1 по с 32 байтами данных:
Ответ от 192.168.100.12: Заданный узел недоступен.
Ответ от 192.168.100.12: Заданный узел недоступен.
Ответ от 192.168.100.12: Заданный узел недоступен.
Ответ от 192.168.100.12: Заданный узел недоступен.

Статистика Ping для 192.168.100.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    <0% потерь>

C:\Users\Администратор>ping UGATE-DC
При проверке связи не удалось обнаружить узел UGATE-DC.
Проверьте имя узла и повторите попытку.

```

Рисунок 80 - Проверка доступа с ВМ 4 к ВМ 1

```

C:\Users\Администратор>ping 192.168.100.2
Обмен пакетами с 192.168.100.2 по с 32 байтами данных:
Ответ от 192.168.100.12: Заданный узел недоступен.
Превышен интервал ожидания для запроса.
Ответ от 192.168.100.12: Заданный узел недоступен.
Превышен интервал ожидания для запроса.

Статистика Ping для 192.168.100.2:
    Пакетов: отправлено = 4, получено = 2, потеряно = 2
    <50% потерь>

C:\Users\Администратор>ping AS
При проверке связи не удалось обнаружить узел AS.
Проверьте имя узла и повторите попытку.

```

Рисунок 81 - Проверка доступа с ВМ 4 к ВМ 2

```

C:\Users\Администратор>ping 192.168.100.11
Обмен пакетами с 192.168.100.11 по с 32 байтами данных:
Ответ от 192.168.100.12: Заданный узел недоступен.
Ответ от 192.168.100.12: Заданный узел недоступен.
Ответ от 192.168.100.12: Заданный узел недоступен.
Ответ от 192.168.100.12: Заданный узел недоступен.

Статистика Ping для 192.168.100.11:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    <0% потерь>

C:\Users\Администратор>ping WS-AVI
При проверке связи не удалось обнаружить узел WS-AVI.
Проверьте имя узла и повторите попытку.

```

Рисунок 82 - Проверка доступа с ВМ 4 к ВМ 3

Отсутствие соединения с ВМ 4 произошло в результате того, что на ВМ 4 не настроены правила межсетевого экрана. В дальнейшем необходимо настроить правила, разрешив входящие подключения.

4.2 Установка роли контроллера домена

Перед созданием локальной сети были проверены настройки сетевых адаптеров всех виртуальных машин:

- ВМ 1 (контроллер домена):
 - IP адрес — 192.168.100.1;
 - маска подсети — 255.255.255.0;
 - основной шлюз — 192.168.100.1;
 - предпочитаемый DNS-сервер — 192.168.100.1;
 - альтернативный DNS-сервер — 127.0.0.1;
- ВМ 2 (сервер авторизации):
 - IP адрес — 192.168.100.2;
 - маска подсети — 255.255.255.0;
 - основной шлюз — 192.168.100.1;
 - предпочитаемый DNS-сервер — 192.168.100.1;
 - альтернативный DNS-сервер — 127.0.0.1;
- ВМ 3 (рабочее место АБИ):
 - IP адрес — 192.168.100.11;
 - маска подсети — 255.255.255.0;
 - основной шлюз — 192.168.100.1;
 - предпочитаемый DNS-сервер — 192.168.100.1;
 - альтернативный DNS-сервер — 127.0.0.1;
- ВМ 4 (сервер виртуализации):
 - IP адрес — 192.168.100.11;

- маска подсети — 255.255.255.0;
- основной шлюз — 192.168.100.1;
- предпочитаемый DNS-сервер — 192.168.100.1;
- альтернативный DNS-сервер — 127.0.0.1.

Необходимо выполнить проверку того, что все ВМ отображаются в зоне прямого просмотра. Для этого необходимо запустить «Диспетчер серверов», выбрать раздел «Средства» и выбрать пункт «DNS». После запуска консоли, выбрать пункт «Зона прямого просмотра», выбрать зону «vgate.psu». В появившемся списке отображаются все ВМ. Результат представлен на рисунке 83.

 as	Узел (A)	192.168.100.2
 vgate-dc	Узел (A)	192.168.100.1
 VGATE-HSV	Узел (A)	192.168.100.12
 WS-AVI	Узел (A)	192.168.100.11

Рисунок 83 - Отображение все ВМ в зоне прямого просмотра

После этого на контроллере домена (ВМ 1) необходимо установить доменные службы Active Directory.

Для этого необходимо в Диспетчере серверов выбрать пункт Управление, далее «Добавить роли и компоненты». Запускается «Мастер добавления ролей и компонентов», необходимо выбрать тип установки «Установка ролей или компонентов». В списке ролей сервера необходимо выбрать «Доменные службы Active Directory» и выполнить установку. Необходимо повысить роль сервера до роли контроллера домена. Выбрать вариант создания нового леса, в качестве имени корневого домена указать имя зоны прямого просмотра DNS. В качестве пароля для режима восстановления служб каталогов (DSRM) указать пароль администратора сервера. При настройке делегирования DNS указать имя и пароль администратора сервера. В качестве имени домена NetBIOS указать имя домена (зоны прямого просмотра) без точки и имени домена первого уровня. Результат представлен на рисунках с 84 по 88.

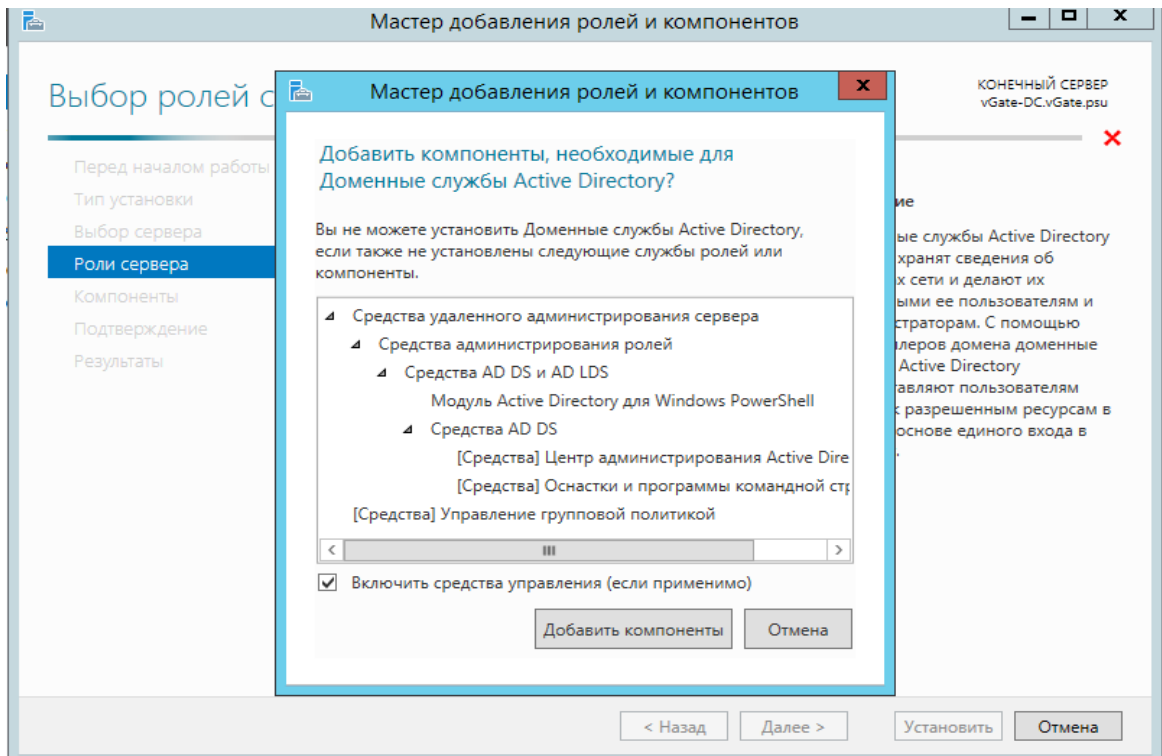


Рисунок 84 - Установка доменных служб Active Directory

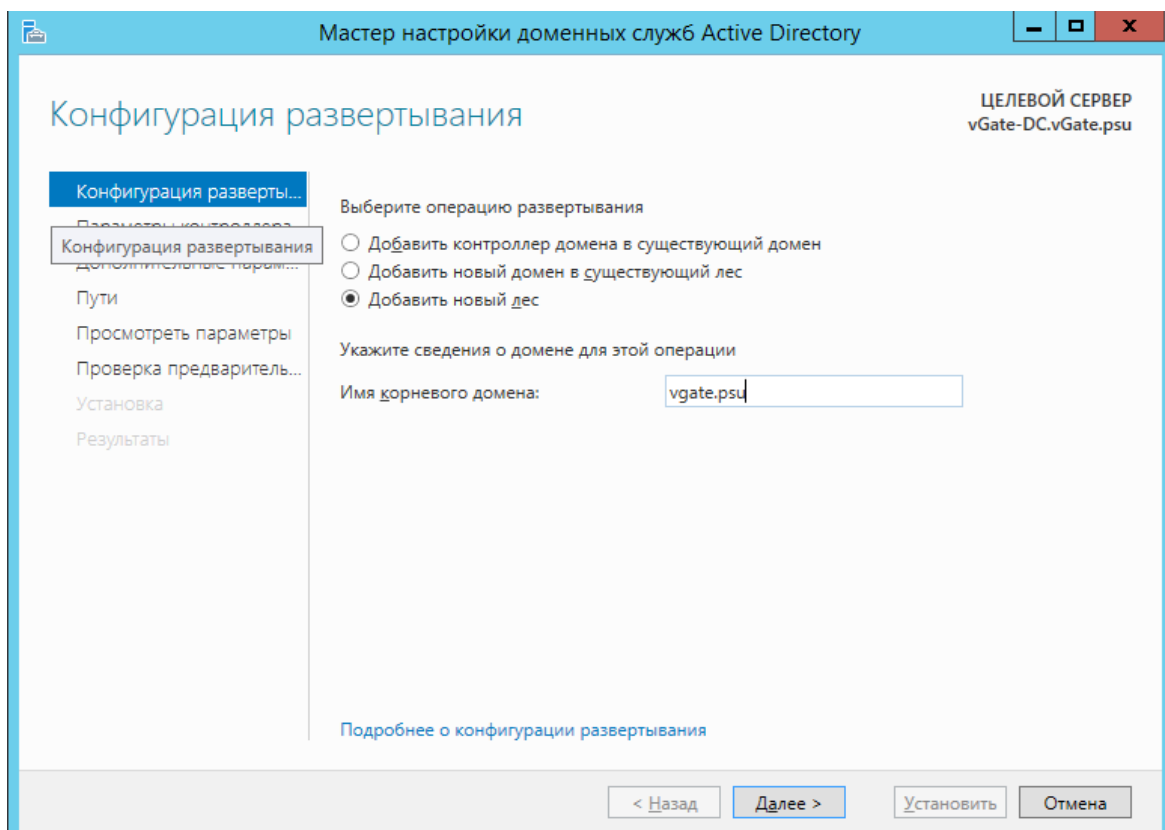


Рисунок 85 - Создание нового леса

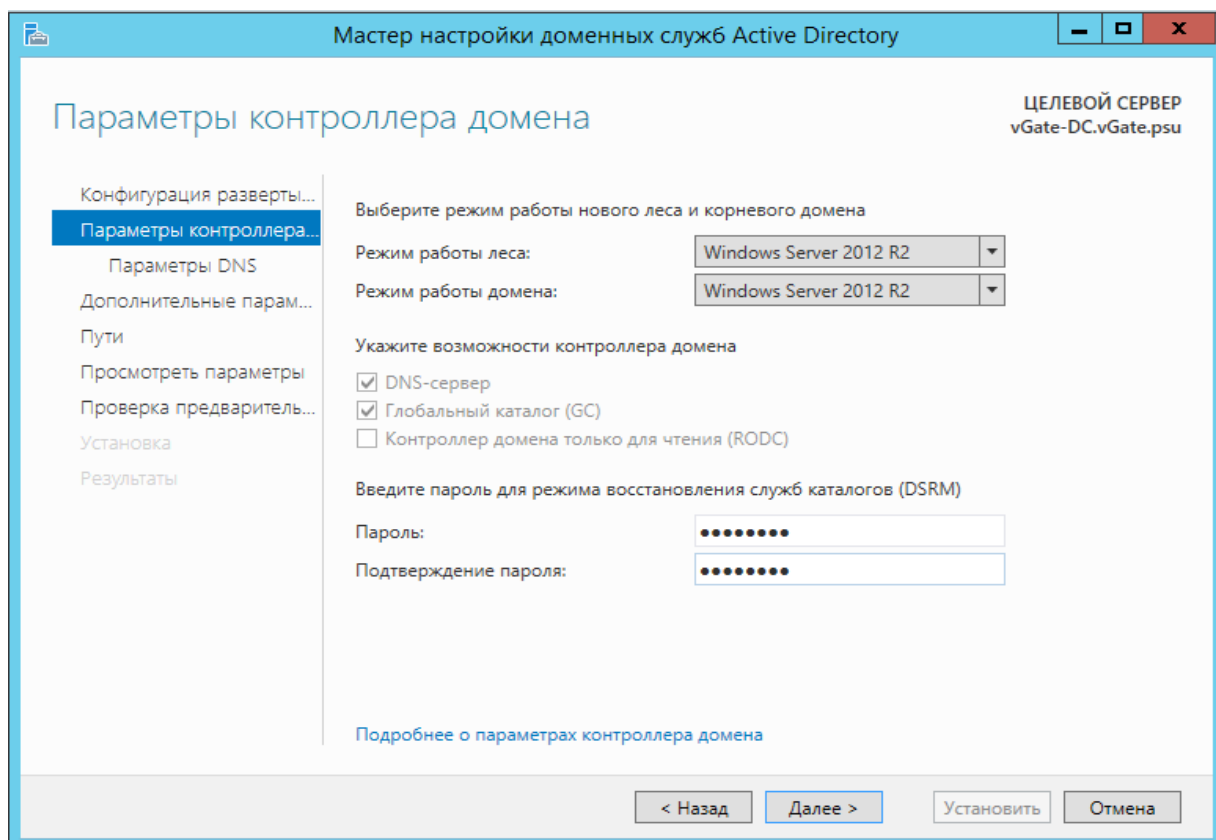


Рисунок 86 - Указание пароля для восстановления

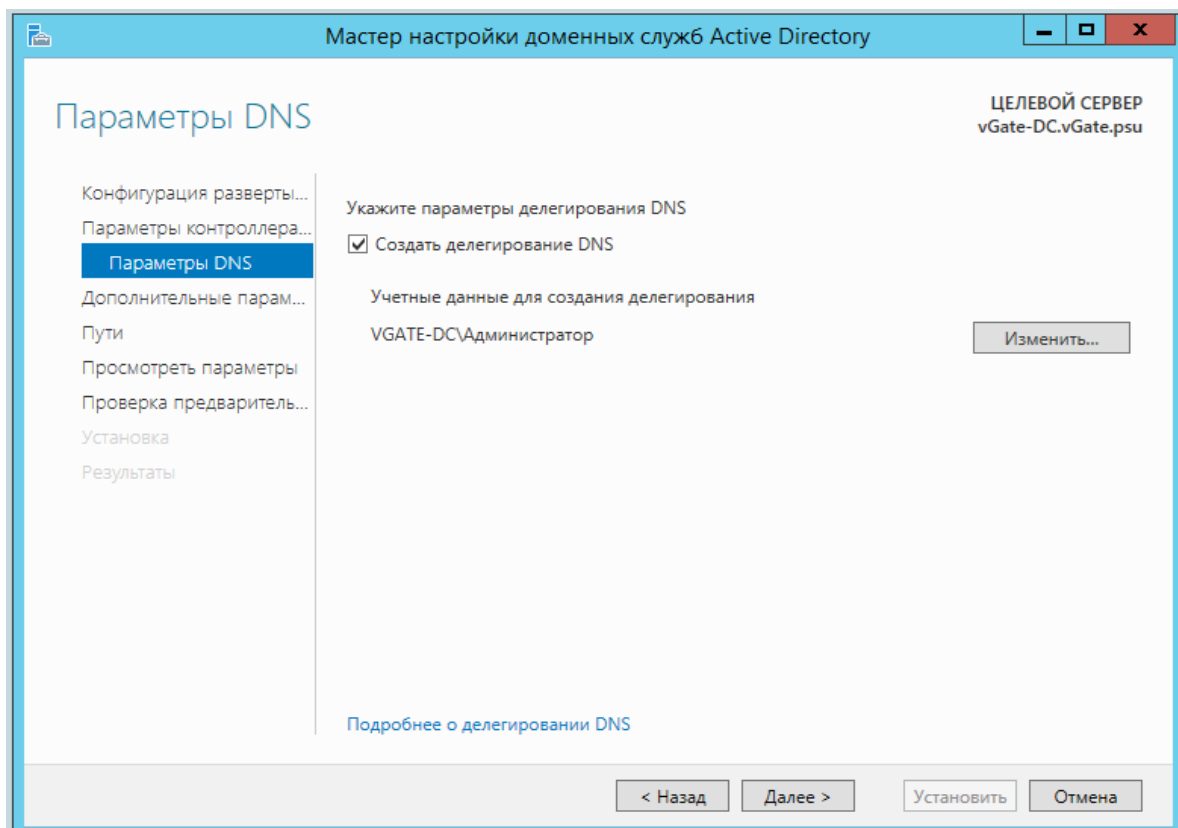


Рисунок 87 - Настройка делегирования DNS локальному администратору

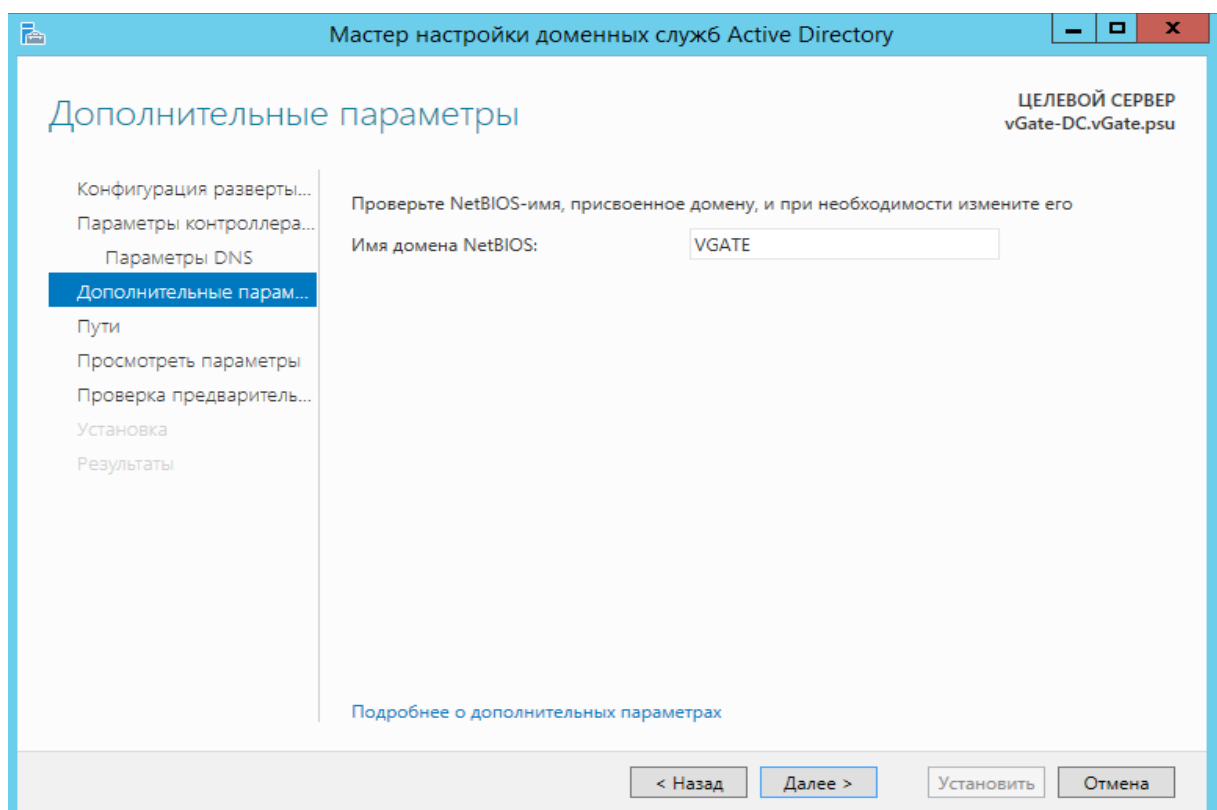


Рисунок 88 - Указание имени домена NetBIOS

После этого необходимо выполнить перезагрузку ВМ. После перезагрузки выполнить вход с использованием учетной записи доменного администратора. После входа необходимо проверить настройки общего доступа. Для этого надо в панели управления открыть центр управления сетями и общим доступом выбрать в правой части окна гиперссылку «Изменить дополнительные параметры общего доступа». Для всех сетевых профилей разрешить общий доступ и включить сетевое обнаружение. Повторить настройку общего доступа и сетевого обнаружения и проверить сохранение настроек. Далее необходимо проверить настройки сетевого адаптера. В случае необходимости установить адрес адаптера и DNS-сервера.

Далее необходимо выполнить проверку создания домена. Для этого необходимо запустить программу «Диспетчер серверов», выбрать раздел «Локальный сервер» и выбрать пункт «Домен». В нем должно быть указано имя созданного домена — vgate.psu. Результат представлен на рисунке 89.

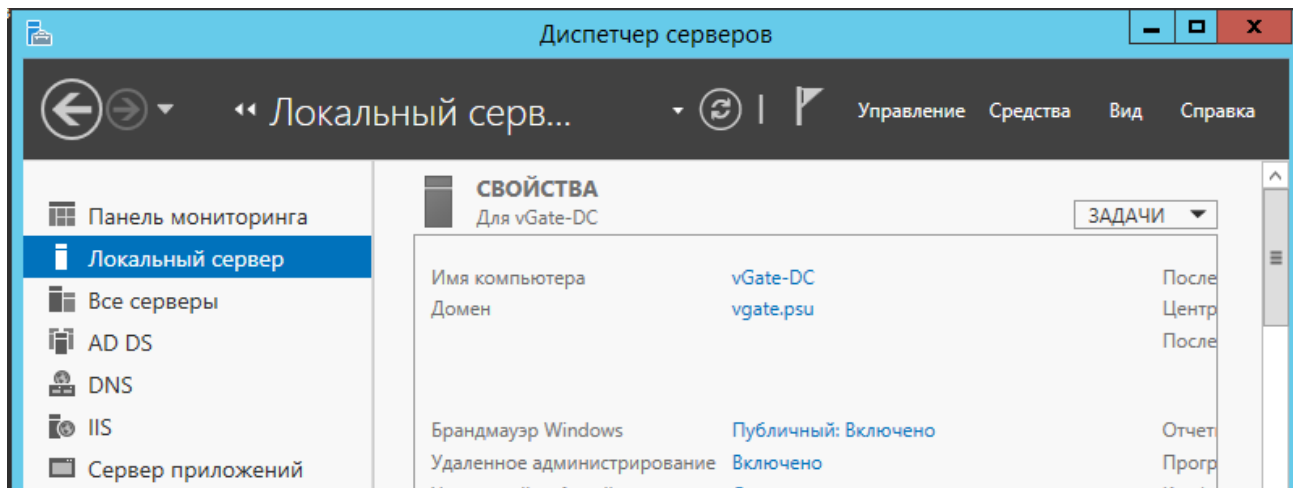


Рисунок 89 - Проверка создания домена

Необходимо интегрировать зоны прямого просмотра DNS и Active Directory. Для этого в консоли DNS открыть диалоговое окно свойств зоны и на вкладке «Общие» выбрать «Изменить». Установить параметр Хранить зону в Active Directory. Результат представлен на рисунке 90.

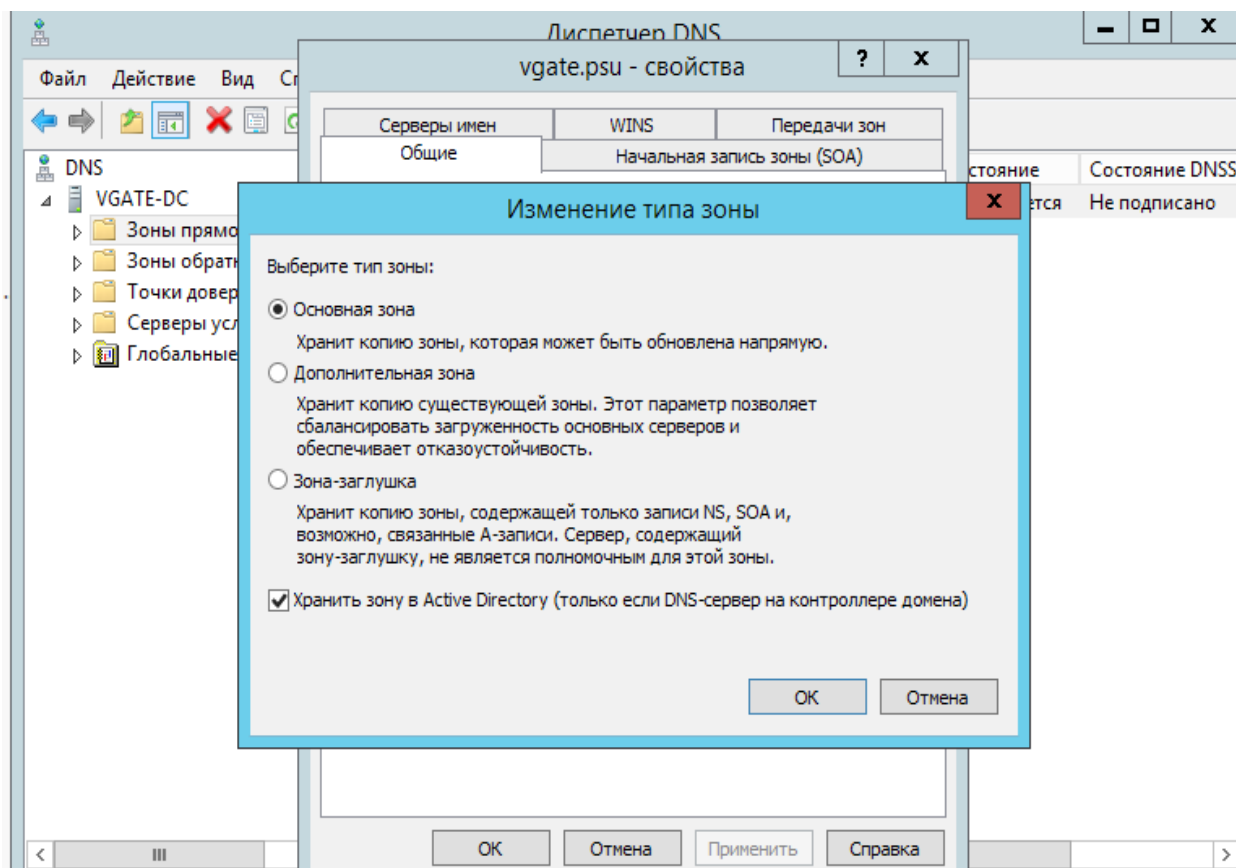


Рисунок 90 - Интеграция зоны прямого просмотра и Active Directory

4.3 Создание домена

После этого необходимо сервер авторизации (ВМ 2) подключить к созданному домену.

Для этого необходимо запустить программу «Диспетчер серверов» и выбрать функция «Домен». Указать созданный домен vgate.psu. Далее указать имя и пароль администратора и после этого необходимо перезагрузить виртуальную машину. Результат представлен на рисунках 91 и 92.

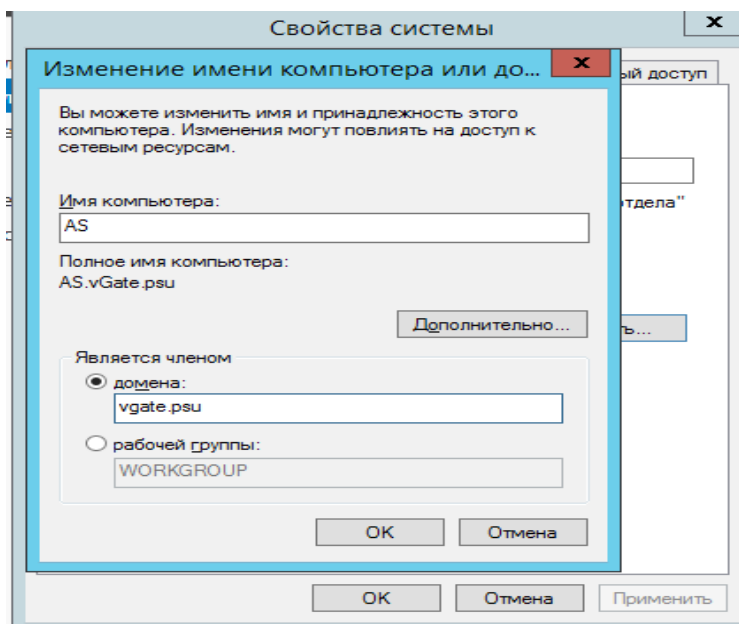


Рисунок 91 - Указание созданного домена

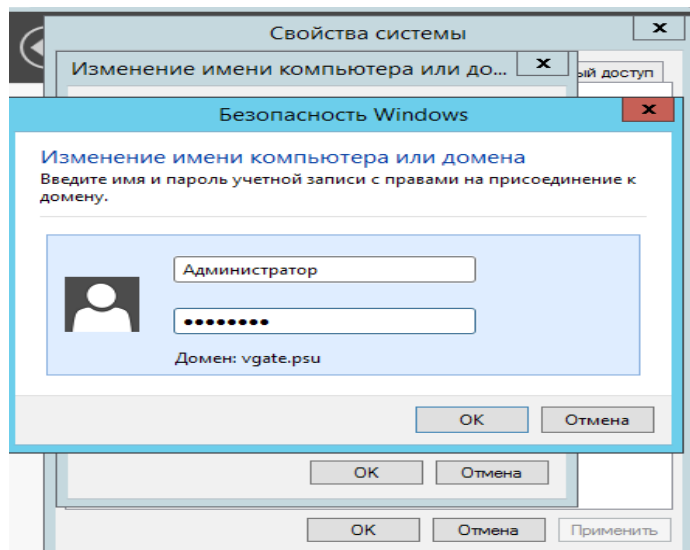
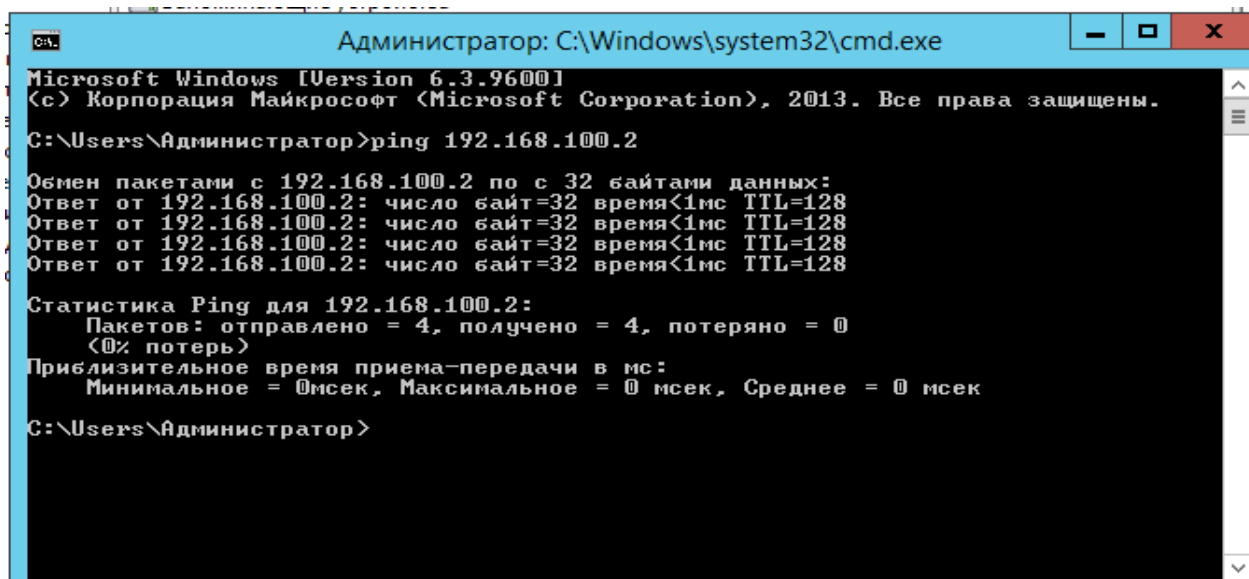


Рисунок 92 - Указание имени и пароля администратора

После этого необходимо настроить правила межсетевого экрана. Необходимо запустить программу «Брандмауэр Windows в режиме повышенной безопасности», выбрать «Правила для входящих подключений» и включить все правила под названием «DCOM-входящий трафик» и правила удаленного управления журналом регистрации событий (аудита) и производительности.

Необходимо провести проверку того что компьютер добавлен в домен. Для этого он необходимо использовать команду ping 192.168.100.2 в командной строке на компьютере домена. Результат представлен на рисунках 93 и 94.



```
Администратор: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) Корпорация Майкрософт (Microsoft Corporation), 2013. Все права защищены.

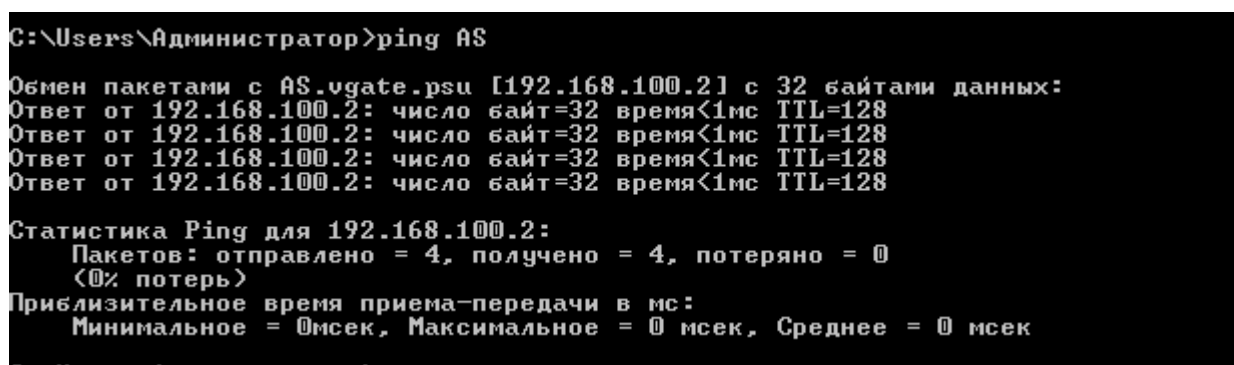
C:\Users\Администратор>ping 192.168.100.2

Обмен пакетами с 192.168.100.2 по 32 байтами данных:
Ответ от 192.168.100.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.2: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.100.2:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
    Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек

C:\Users\Администратор>
```

Рисунок 93 - Проверка добавления компьютера в домен с помощью сетевого адреса



```
C:\Users\Администратор>ping AS

Обмен пакетами с AS.vgate.psu [192.168.100.2] с 32 байтами данных:
Ответ от 192.168.100.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.2: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.100.2:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
    Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
```

Рисунок 94 - Проверка добавления компьютера в домен с помощью сетевого имени

Также на компьютере домена в Диспетчере серверов необходимо запустить консоль Пользователи и компьютеры Active Directory и проверить

возможность запуска консоли управления компьютером. Результат представлен на рисунке 95.

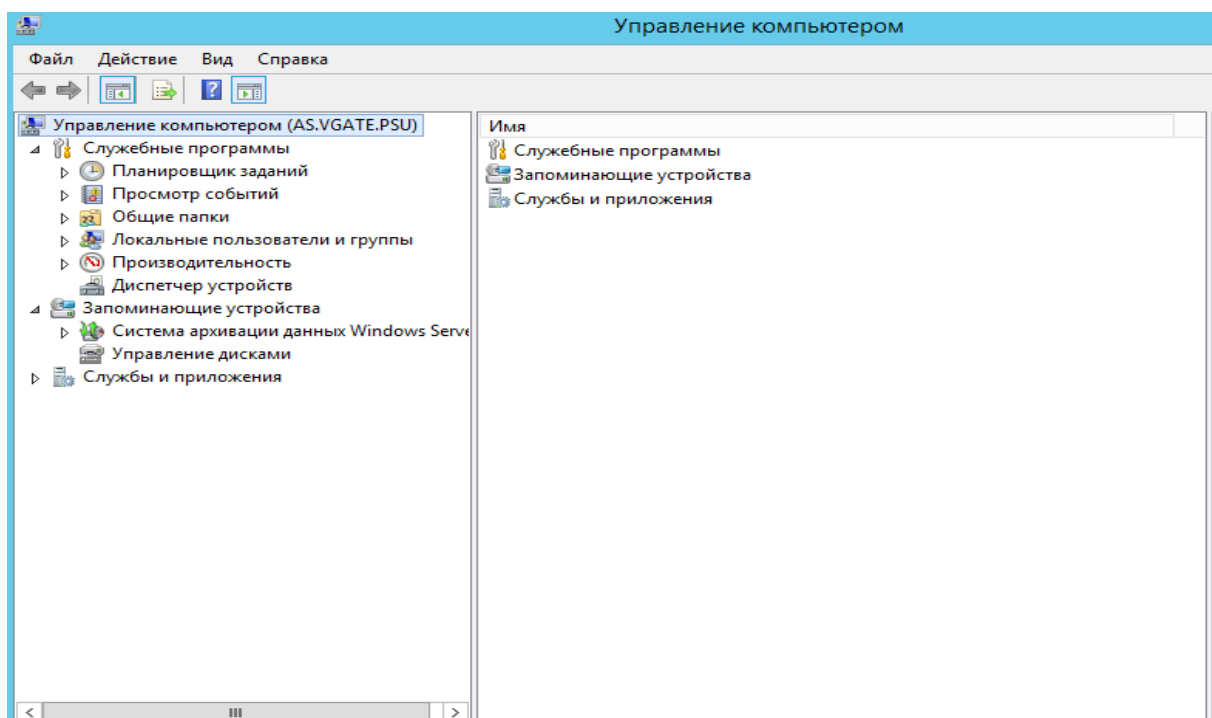


Рисунок 95 - Запуск консоли Управление компьютером AS

После этого рабочее место АВИ (ВМ 3) необходимо подключить к созданному домену.

Для этого через поиск необходимо запустить программу «Просмотр имени компьютера» и выбрать функцию «Добавить в домен». Указать имя домена vgate.psu. После этого необходимо перезагрузить виртуальную машину. Результат представлен на рисунке 96.

Компьютер

Имя компьютера WS-AVI

Домен VGATE

Переименование компьютера

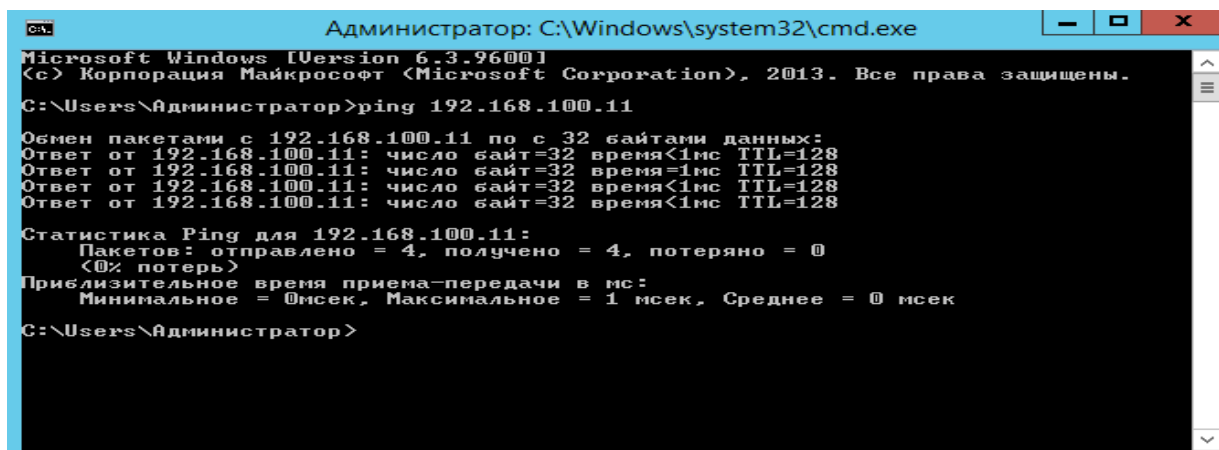
Выход из домена

Рисунок 96 - Добавление компьютера в домен

После этого необходимо настроить правила межсетевого экрана. Необходимо запустить программу «Брандмауэр Windows в режиме повышенной

безопасности», выбрать «Правила для входящих подключений» и включить все правила под названием «DCOM-входящий трафик» и правила удаленного управления журналом регистрации событий (аудита) и производительности.

Необходимо провести проверку того что компьютер добавлен в домен. Для этого он необходимо использовать команду `ping 192.168.100.11` в командной строке на компьютере домена. Результат представлен на рисунках 97 и 98.



```
Администратор: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) Корпорация Майкрософт (Microsoft Corporation), 2013. Все права защищены.

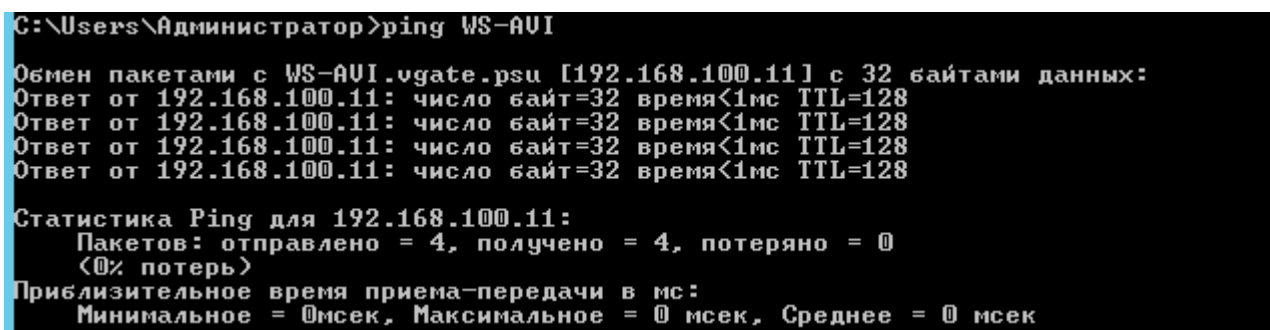
C:\Users\Администратор>ping 192.168.100.11

Обмен пакетами с 192.168.100.11 по 32 байтами данных:
Ответ от 192.168.100.11: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.11: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.11: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.11: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.100.11:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
    Приблизительное время приема-передачи в мс:
        Минимальное = 0мсек, Максимальное = 1 мсек, Среднее = 0 мсек

C:\Users\Администратор>
```

Рисунок 97 - Проверка добавления компьютера в домен с помощью сетевого адреса



```
C:\Users\Администратор>ping WS-AUI

Обмен пакетами с WS-AUI.vgate.psu [192.168.100.11] с 32 байтами данных:
Ответ от 192.168.100.11: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.11: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.11: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.11: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.100.11:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
    Приблизительное время приема-передачи в мс:
        Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
```

Рисунок 98 - Проверка добавления компьютера в домен с помощью сетевого имени

Также на компьютере домена в Диспетчере серверов необходимо запустить консоль Пользователи и компьютеры Active Directory и проверить возможность запуска консоли управления компьютером. Результат представлен на рисунке 99.

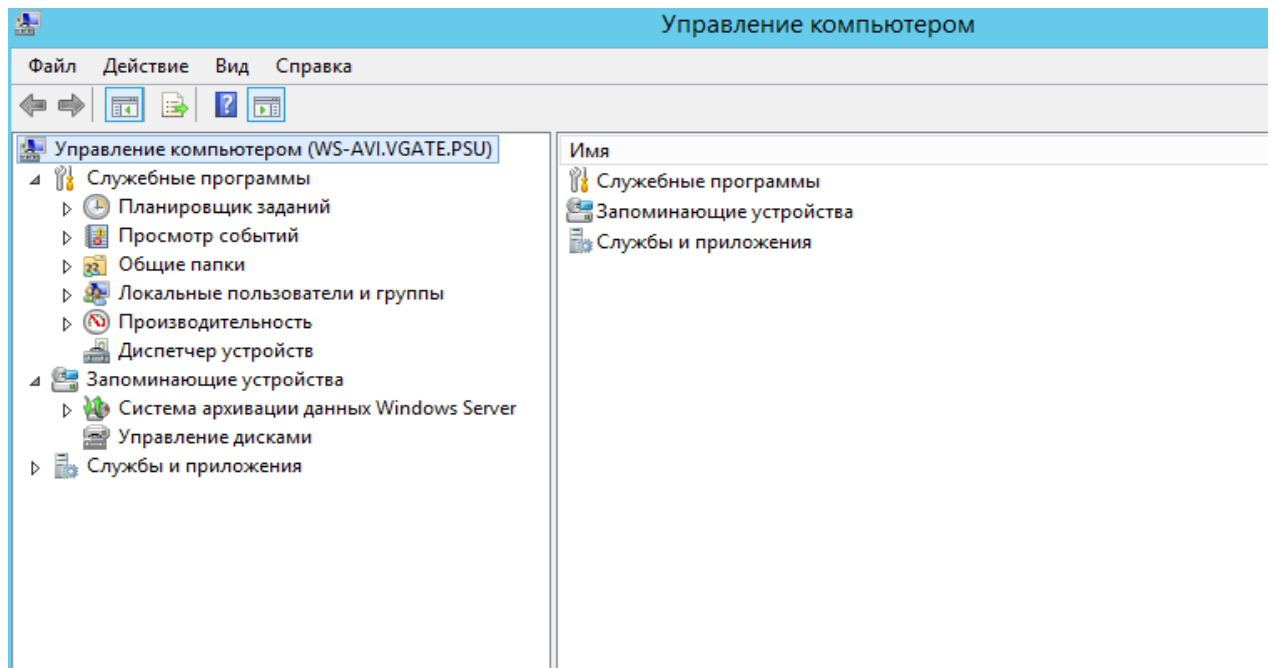


Рисунок 99 - Запуск консоли Управление компьютером WS-AVI

После этого сервер виртуализации (ВМ 4) необходимо подключить к созданному домену.

С помощью оболочки PowerShell необходимо скорректировать настройки имени сервера. Добавить «Основной DNS-суффикс этого компьютера» и указать имя зоны прямого просмотра. После изменения настроек ВМ необходимо перезагрузить. Результат представлен на рисунке 100.

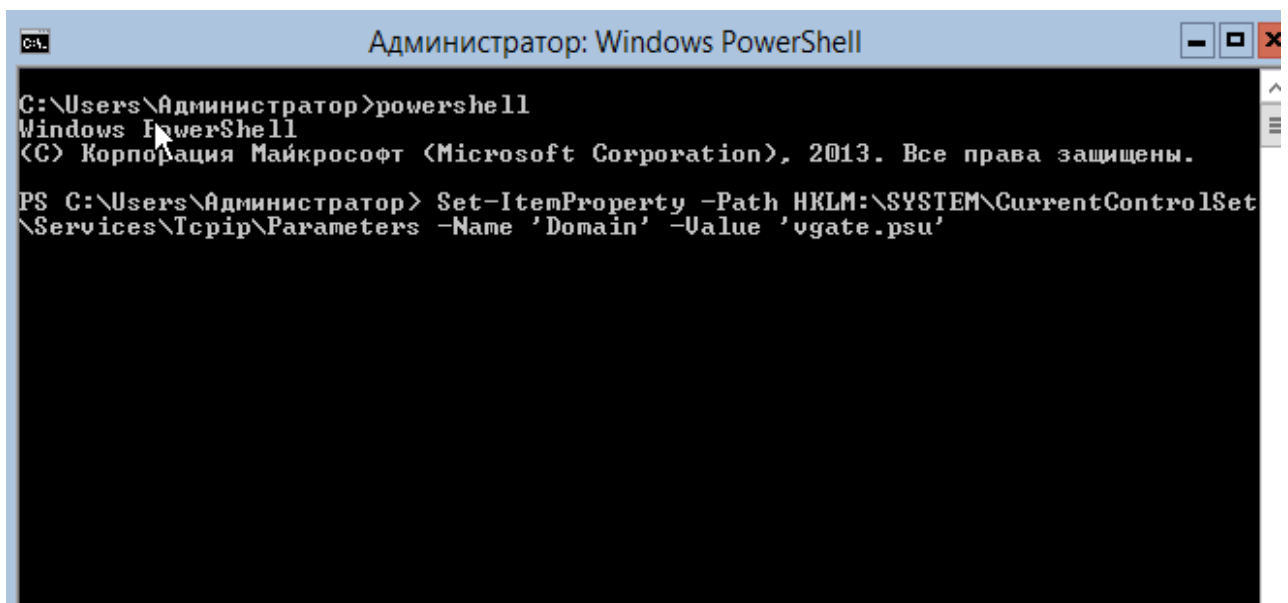


Рисунок 100 - Добавление DNS-суффикса

Далее с помощью оболочки PowerShell компьютер необходимо добавить в домен. После выполнения команды добавления компьютера в домен необходимо указать имя доменного администратора и пароль. После этого ВМ необходимо перезагрузить. Результат представлен на рисунке 101.

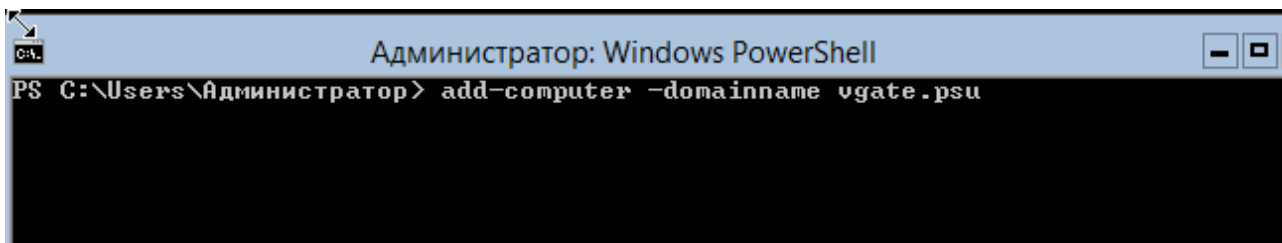


Рисунок 101 - Добавление компьютера в домен

После этого необходимо настроить правила межсетевого экрана. Необходимо запустить Powershell и с помощью команды `Enable-NetFirewallRule -DisplayGroup` настроить правила, разрешив входящие подключения. Результат представлен на рисунке 102.

Список необходимых групп:

- удаленное управление томами;
- удаленное управление брандмауэром Windows;
- инструментарий управления Windows (WMI);
- журналы и оповещения производительности;
- удаленное управление Windows;
- удаленное управление журналом событий;
- наблюдение за виртуальной машиной;
- дистанционное управление рабочим столом;
- icmp-протокол.

```
PS C:\Users\Администратор> Enable-NetFirewallRule -DisplayGroup "Удаленное управ  
ление Windows"  
PS C:\Users\Администратор> Enable-NetFirewallRule -DisplayGroup "Удаленное управ  
ление томами"  
PS C:\Users\Администратор> Enable-NetFirewallRule -DisplayGroup "Удаленное управ  
ление брандмауэром Windows"  
PS C:\Users\Администратор> Enable-NetFirewallRule -DisplayGroup "Инструментарий  
управления Windows(WMI)"
```

Рисунок 102 - Настройка правил межсетевого экрана на гипервизоре

Необходимо провести проверку того что компьютер добавлен в домен. Для этого он необходимо использовать команду ping 192.168.100.12 в командной строке на компьютере домена. Результат представлен на рисунках 103 и 104.

```
C:\Users\Администратор>ping 192.168.100.12

Обмен пакетами с 192.168.100.12 по 32 байтами данных:
Ответ от 192.168.100.12: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.12: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.12: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.12: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.100.12:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
```

Рисунок 103 - Проверка добавления компьютера в домен с помощью сетевого адреса

```
C:\Users\Администратор>ping VGATE-HSV

Обмен пакетами с VGATE-HSV.vgate.psu [192.168.100.12] с 32 байтами данных:
Ответ от 192.168.100.12: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.12: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.12: число байт=32 время<1мс TTL=128
Ответ от 192.168.100.12: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.100.12:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
```

Рисунок 104 - Проверка добавления компьютера в домен с помощью сетевого имени

Также на компьютере домена в Диспетчере серверов необходимо запустить консоль Пользователи и компьютеры Active Directory и проверить возможность запуска консоли управления компьютером. Результат представлен на рисунке 105.

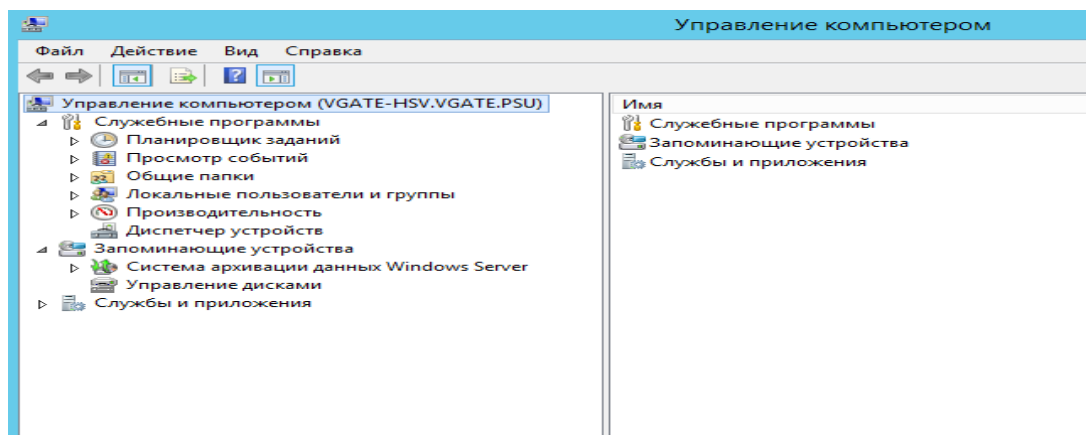


Рисунок 105 - Запуск консоли Управление компьютером VGATE-HSV

Таким образом был создан домен `vgate.psu` в который входят все 4 виртуальные машины, которые могут управляться удаленно и входят в одну локальную сеть.

4.4 Результаты создания локальной сети

В процессе создания стенда была создана локальная сеть состоящая из 4 ВМ:

- ВМ 1 контроллер домена;
- ВМ 2 сервер авторизации;
- ВМ 3 агент аутентификации;
- ВМ 4 сервер виртуализации.

Данная локальная сеть может применяться для управления доступом к ресурсам виртуальной инфраструктуры и контролем целостности, реализуемые средством защиты информации `vGate` и для управления виртуальной инфраструктурой и безопасностью виртуальной инфраструктуры при использовании средства защиты информации `vGate`.

5 Установка СЗИ vGate

5.1 Установка сервера авторизации

Перед установкой консоли управления vGate для Hyper-V на сервер авторизации (ВМ 2), в настройках ВМ2 необходимо создать еще один сетевой адаптер. С помощью менеджера Oracle VirtualBox создать новый сетевой адаптер 2 с настройками аналогичными настройкам сетевого адаптера 1. Для этого необходимо выбрать виртуальную машину и нажать кнопку «Настроить» и выбрать пункт «Сеть» и «Адаптер 2». Результат представлен на рисунке 106.

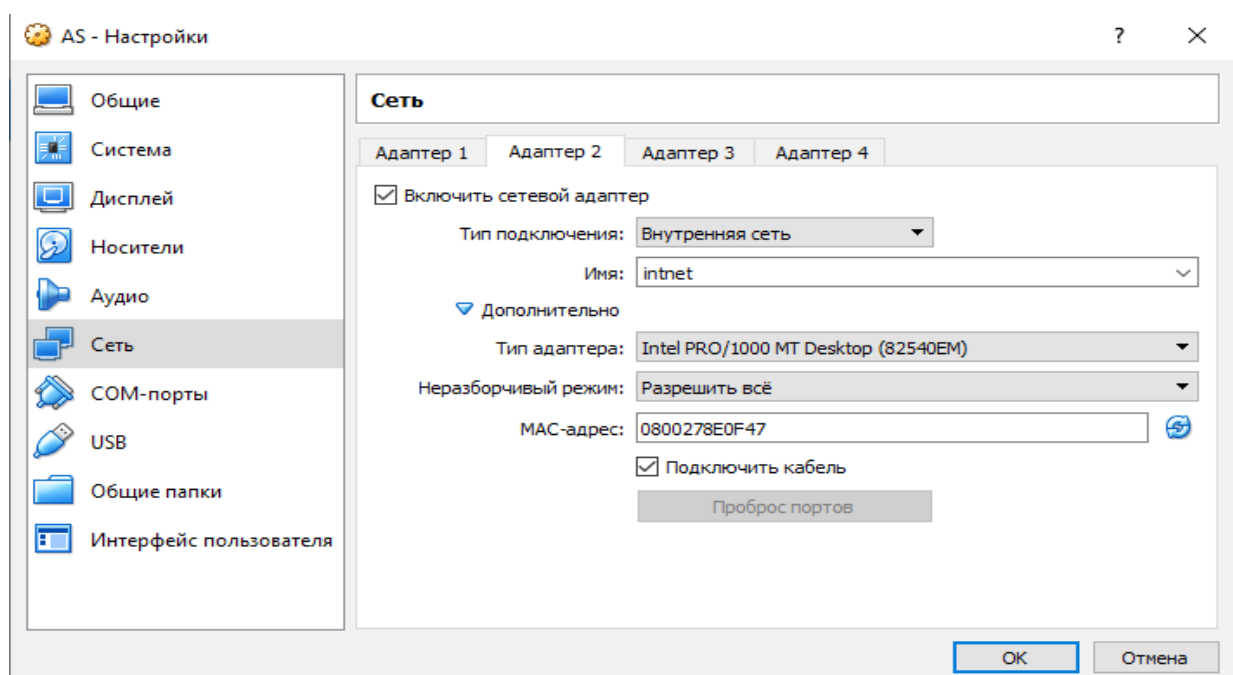


Рисунок 106 — Настройка адаптера сети 2

После этого локальную сеть необходимо разделить на две подсети:

- внешняя подсеть (контроллер домена, рабочее место АВИ);
- внутренняя защищаемая подсеть (сервер виртуализации).

Для этого для сетевого адаптера 2 на сервере авторизации установить статический IP-адрес - 192.168.50.2 и маску подсети - 255.255.255.0. При этом адрес настроить для протокола IP версии 4. Отключить использование IP-адресов версии 6. В качестве шлюза по умолчанию указать адрес самого

сервера. Установить адрес предпочитаемого DNS-сервера - 192.168.50.2. Результат представлен на рисунке 107.

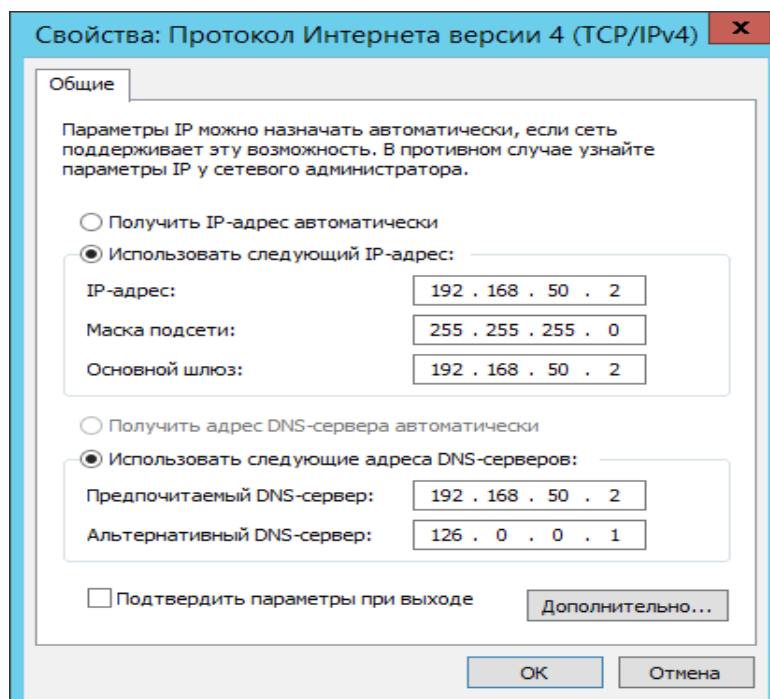


Рисунок 107 - Настройка второго сетевого адаптера

Далее необходимо исправить настройки сетевого адаптера на рабочем месте АВИ. В качестве шлюза по умолчанию указать адрес 192.168.50.2. и маску подсети - 255.255.255.0. Результат представлен на рисунке 108.

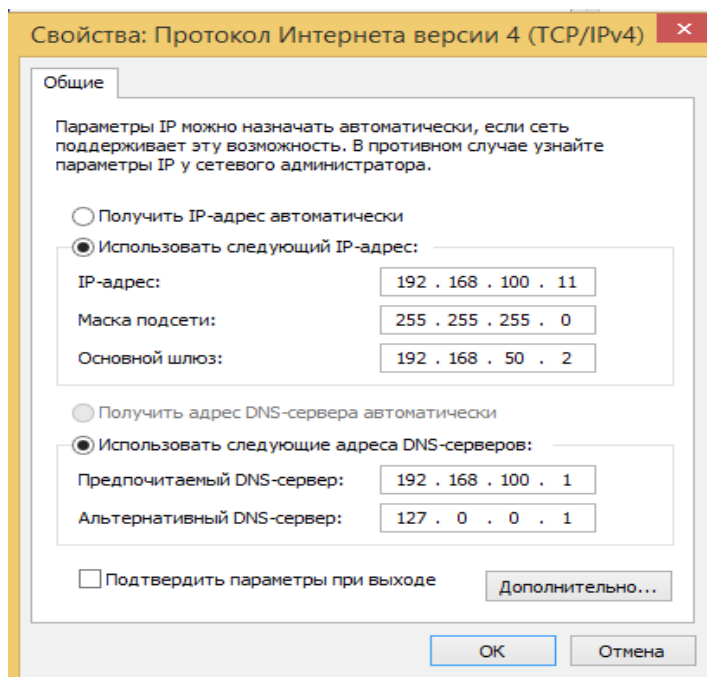


Рисунок 108 - Исправление настроек сетевого адаптера на рабочем месте АВИ

Далее на сервере авторизации (ВМ 2) необходимо запустить установщик vGate. Выбрать «для защиты Microsoft Hyper-V» и выбрать тип установки «Сервер авторизации». Компоненты установки выбрать по умолчанию. Для установки сервера баз данных PostgreSQL 9.4. указать имя пользователя (postgres) и пароль (P.ssw0rd). Выбрать способ маршрутизации «Маршрутизацию осуществляет сервер авторизации vGate». Указать IP-адреса сетевых адаптеров для внешней (192.168.50.2) и внутренней сети (192.168.100.2) и маску подсети (192.168.100/24). Указать имя реестра учетных записей (vGate) - (admin) и пароль (P.ssw0rd) главного администратора информационной безопасности. После этого сервер авторизации был установлен. Результат представлен на рисунках с 109 по 115.

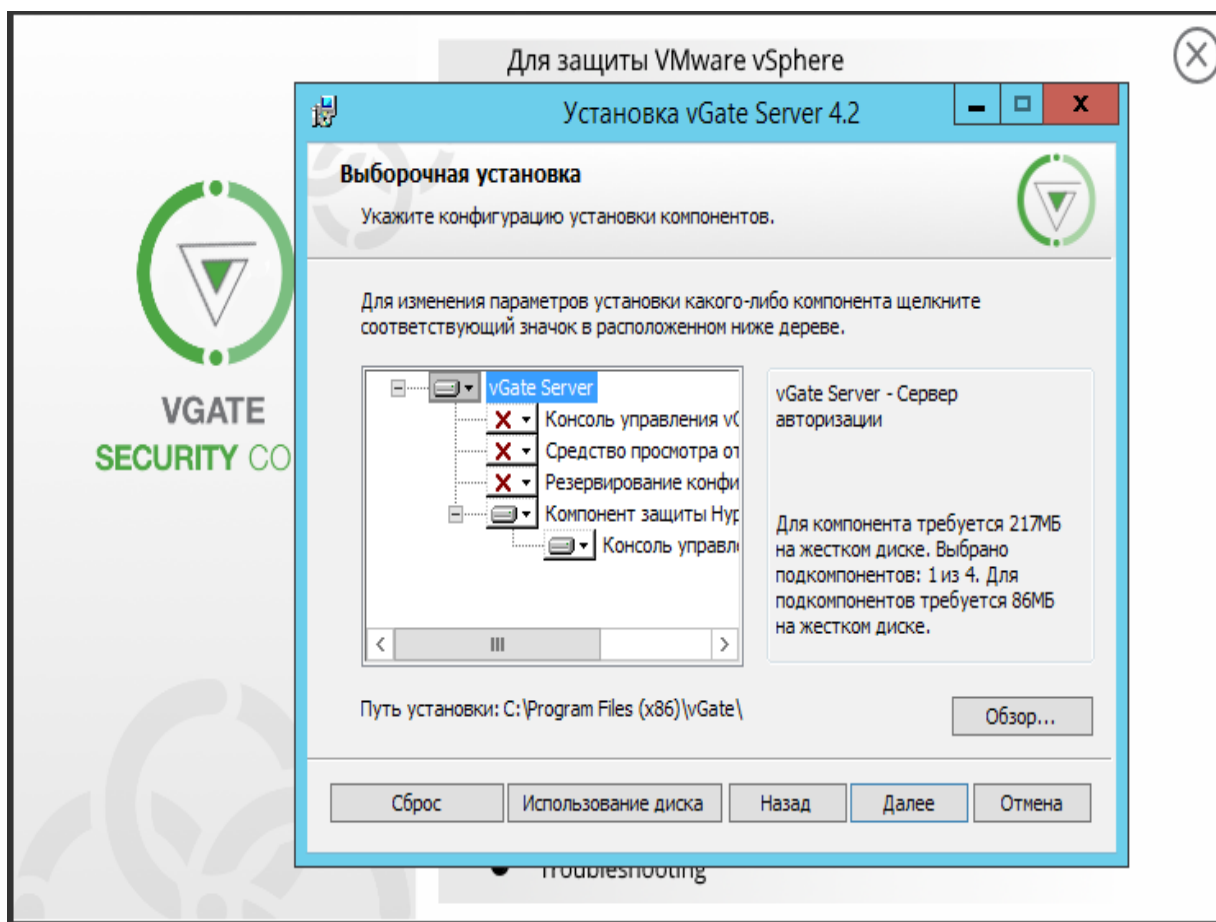


Рисунок 109 - Выбор компонентов установки

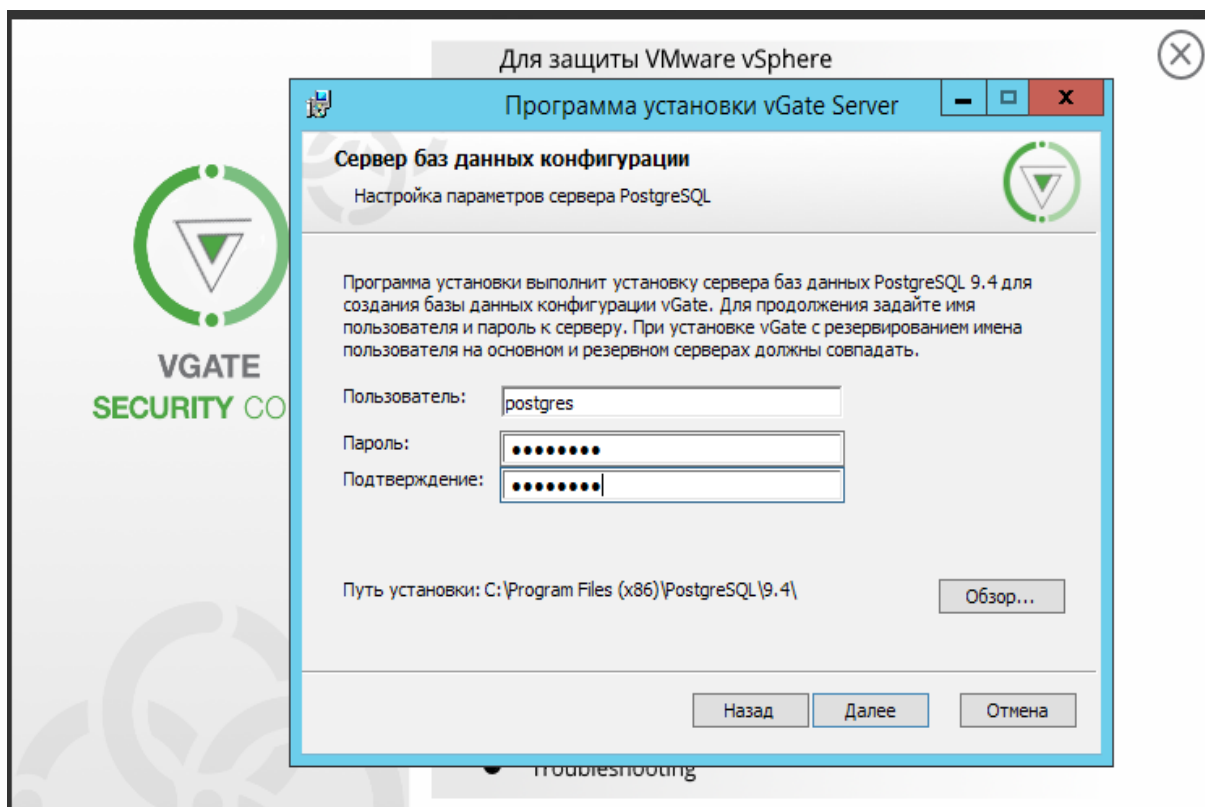


Рисунок 110 - Установка сервера баз данных PostgreSQL 9.4

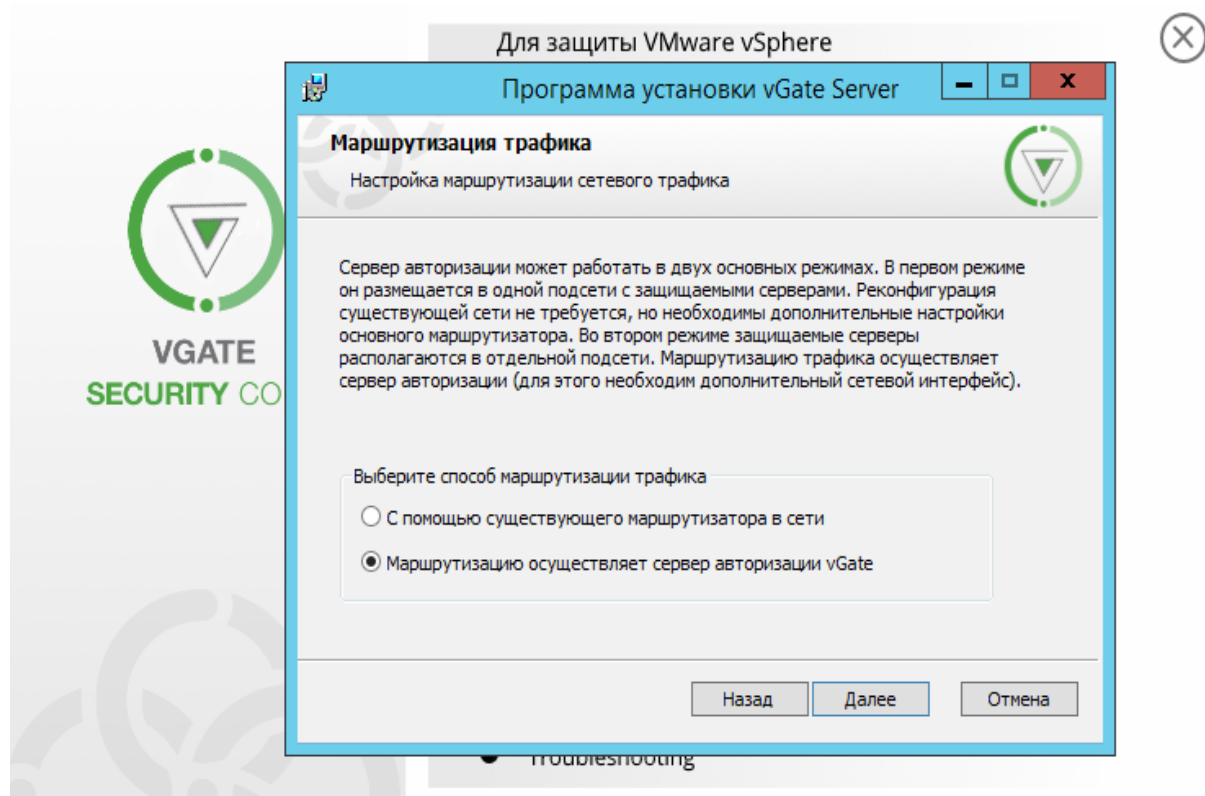


Рисунок 111 - Выбор способа маршрутизации

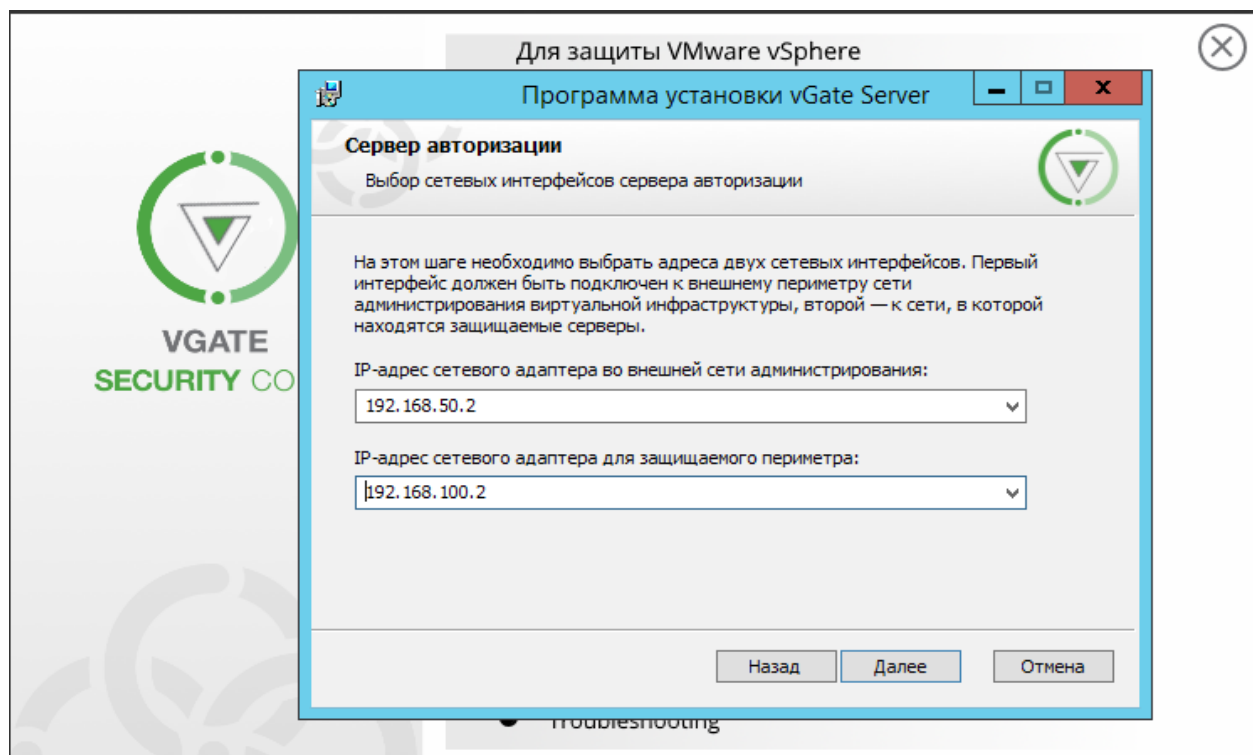


Рисунок 112 - Указание IP-адресов сетевых адаптеров для внешней и внутренней сети и маска подсети

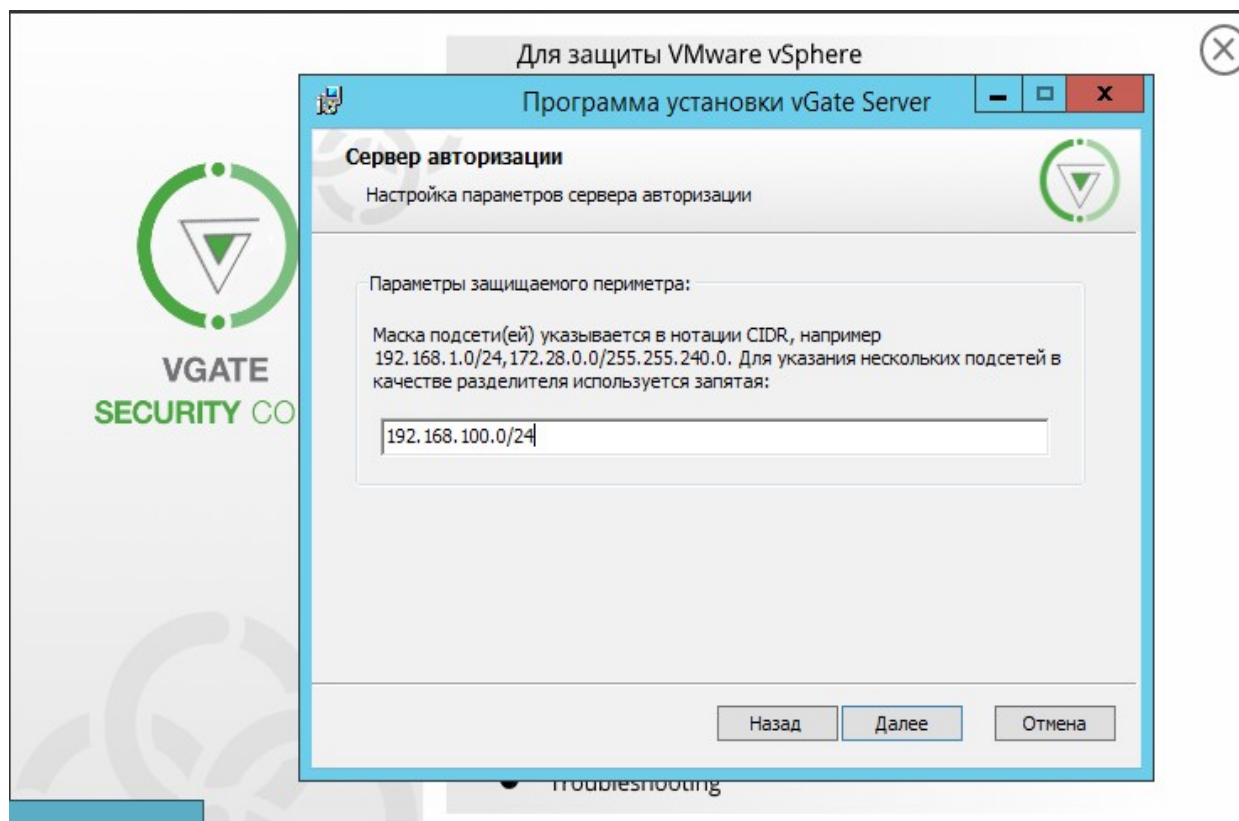


Рисунок 113 - Указание маски подсети

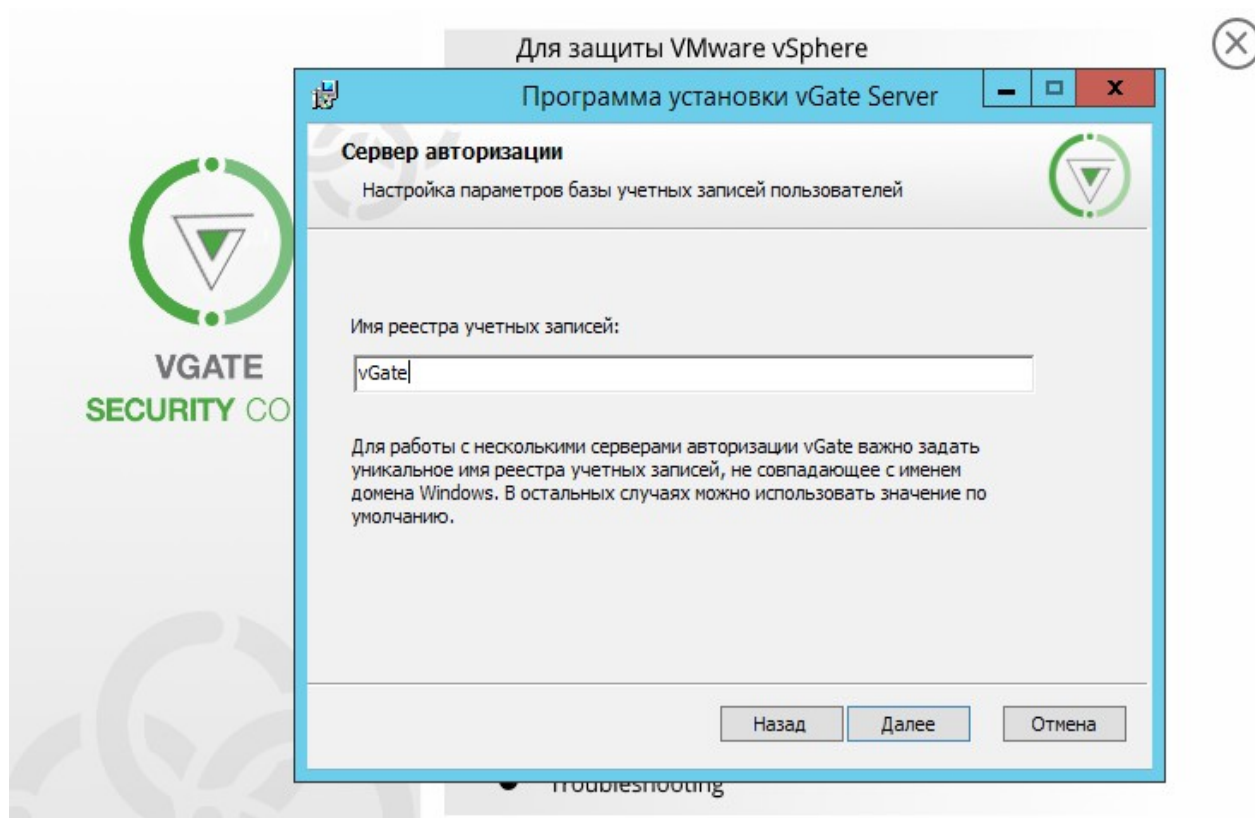


Рисунок 114 - Указание имени реестра учетных записей

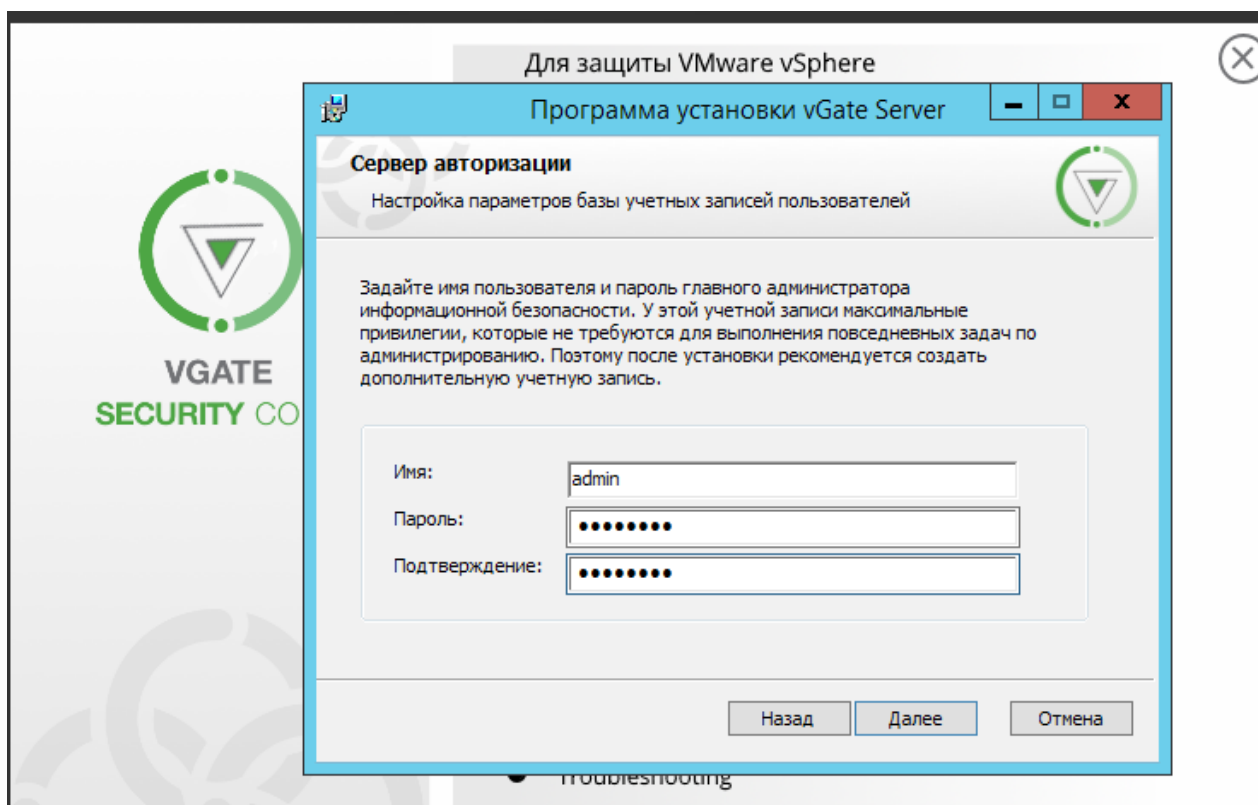


Рисунок 115 - Указание имени и пароля главного администратора информационной безопасности

5.2 Установка агента аутентификации

На рабочем месте АВИ (ВМ 3) необходимо запустить установщик vGate. Выбрать «для защиты Microsoft Hyper-V» и выбрать тип установки «Агент аутентификации». Компоненты установки выбрать по умолчанию. После установки компьютер необходимо перезагрузить. Результат представлен на рисунке 116.

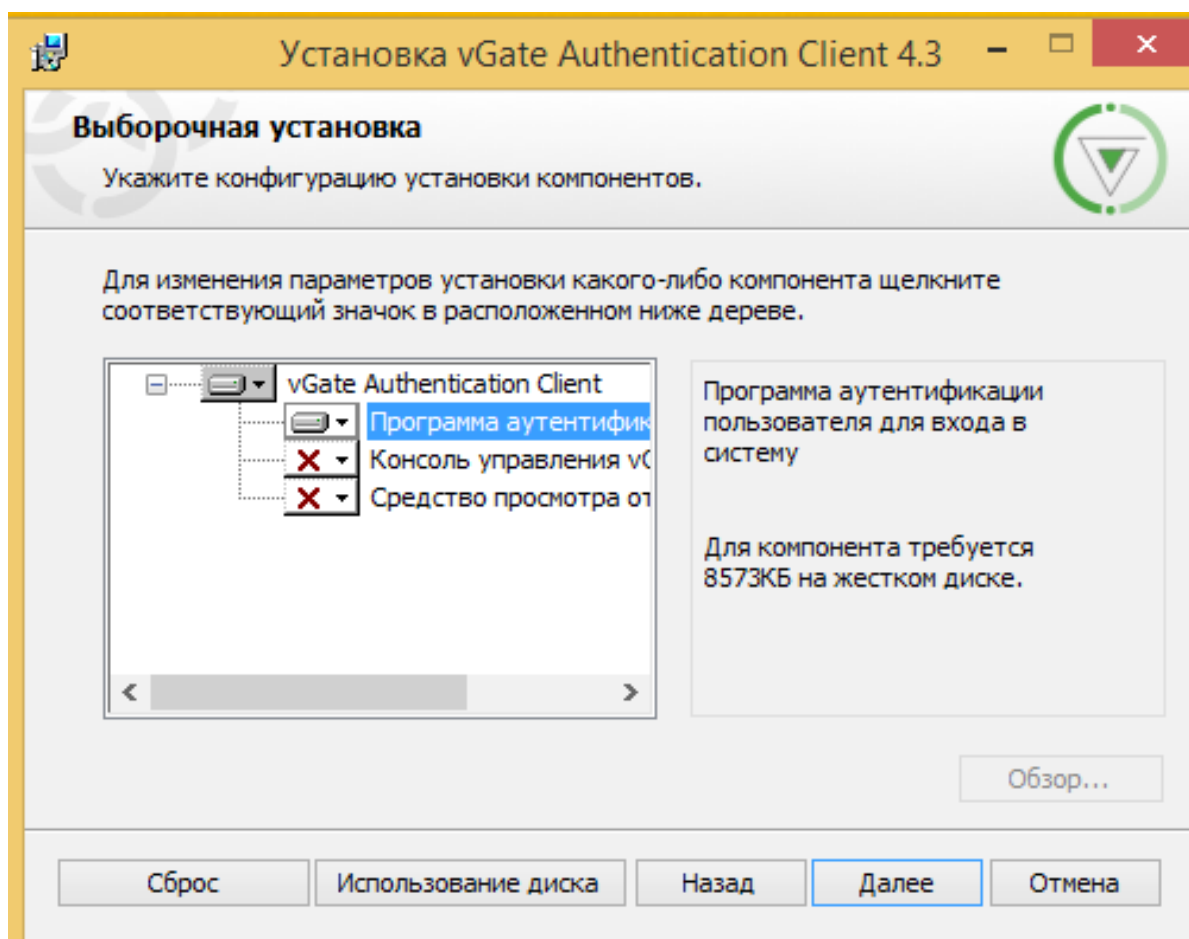


Рисунок 116 - Выбор компонентов установки агента аутентификации

На сервере авторизации необходимо запустить консоль управления vGate для Hyper-V. С помощью мастера первоначальной настройки vGate для Hyper-V сервер Hyper-V добавить в список защищаемых серверов. Указать IP-адрес сервера, домен, имя администратора и пароль. После этого сервер добавлен в список защищаемых. Результат представлен на рисунках с 117 по 119.

Добавление объектов в список защищаемых серверов

Добавление объектов в список защищаемых серверов

Установка компонента защиты на сервер

Происходит автоматическая установка модуля для защиты сервера

Идет установка агента на защищаемый сервер 

Операция является обязательной для обеспечения контроля над объектами виртуальной инфраструктуры.

< Назад

Далее >

Отмена

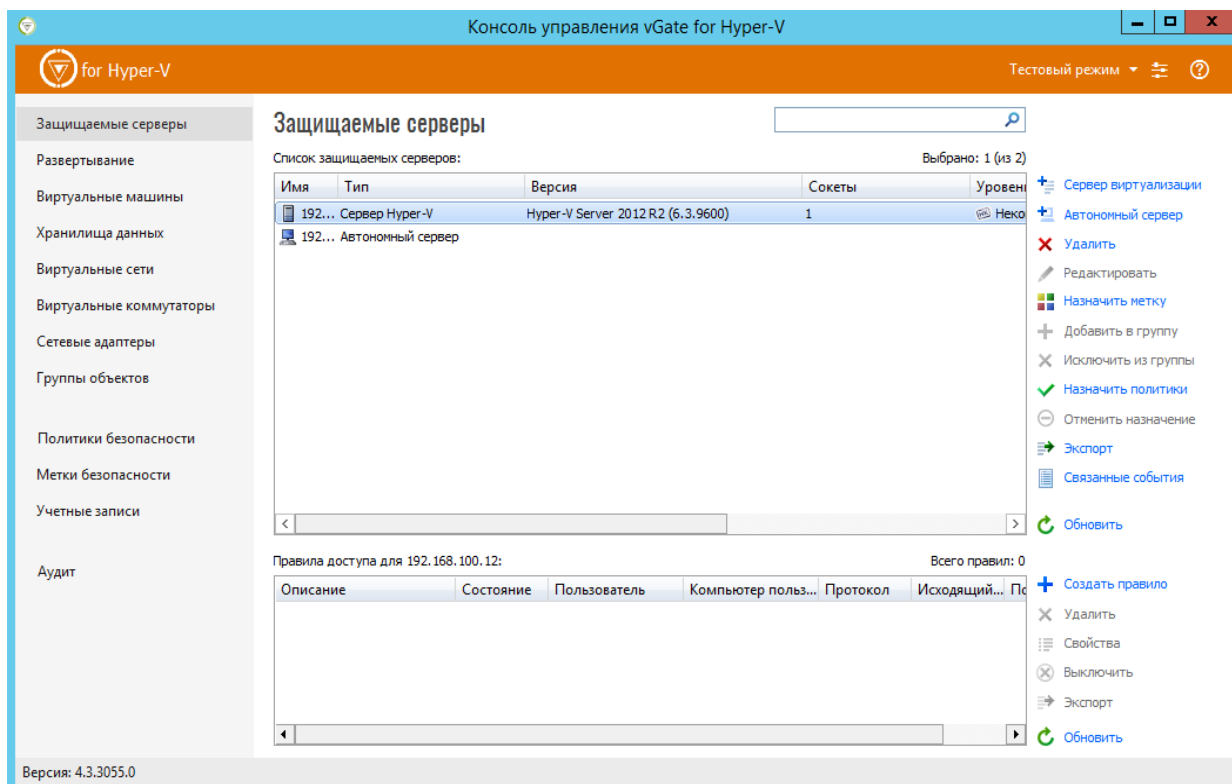


Рисунок 119 – Сервер виртуализации добавлен в список защищаемых

В результате на VM 2 был установлен сервер авторизации vGate, а на VM 3 был установлен агент аутентификации. Также сервер Hyper-V был добавлен в список защищаемых.

Необходимо создать тестовый набор политик безопасности для проверки того, что сервер Hyper-V был добавлен в список защищаемых. Результаты представлены на рисунках с 120 по 123.

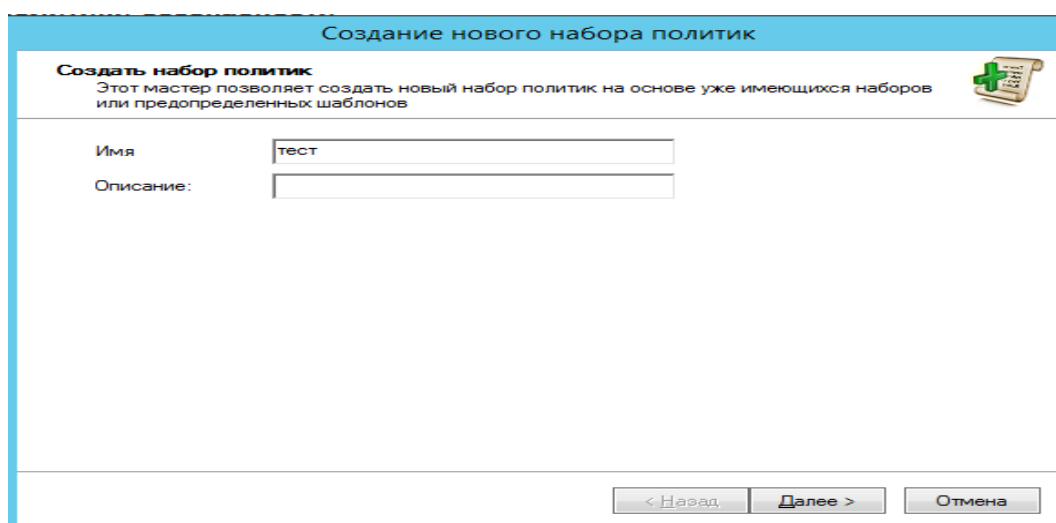


Рисунок 120 - Создание набора политик

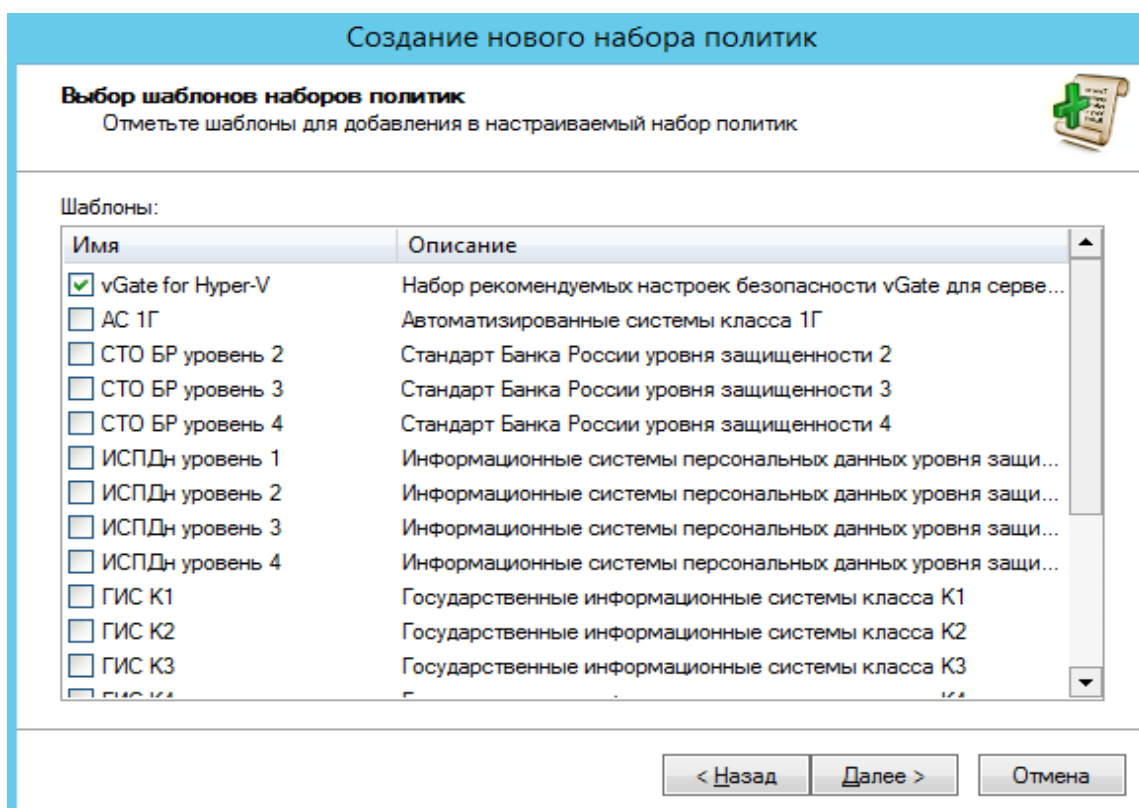


Рисунок 121 - Выбор шаблонов наборов политик

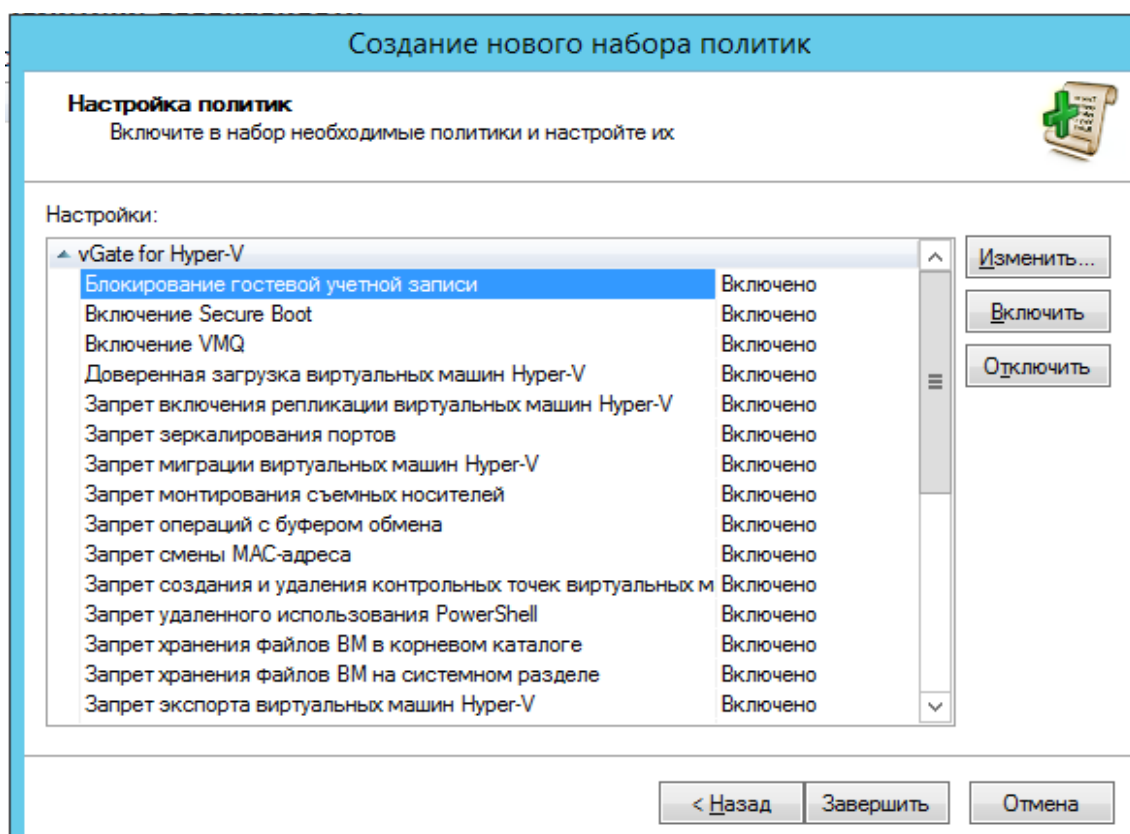


Рисунок 122 - Настройка политик

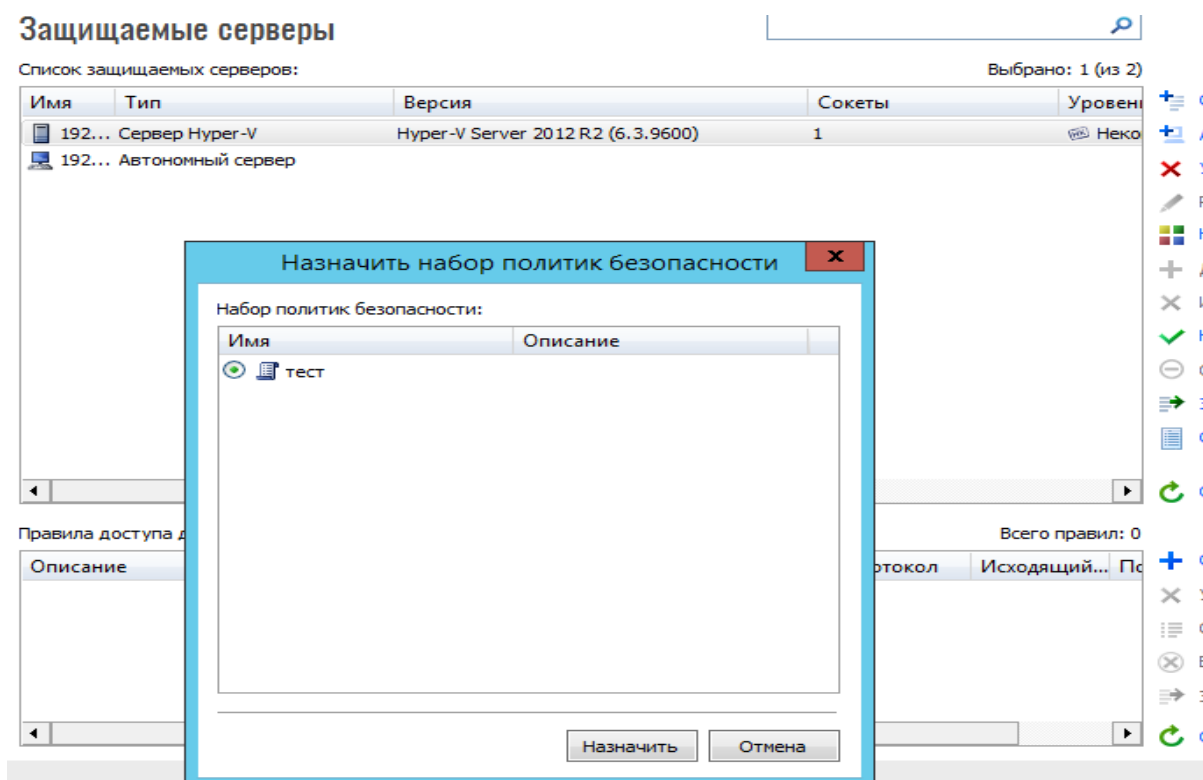


Рисунок 123 — Применение политик к защищаемому серверу

В результате на VM 2 был установлен сервер авторизации vGate, на VM 3 был установлен агент аутентификации. Сервер Hyper-V был добавлен в список защищаемых и для него был создан и применен набор политик безопасности.

5.3 Результат создания стенда

В результате был создан стенд в который входят 4 VM, где:

- VM 1 — контроллер домена с установленной гостевой ОС Windows 2012 R2;
- VM 2 — сервер авторизации vGate с установленной гостевой ОС Windows 2012 R2;
- VM 3 — рабочее место администратора виртуальной инфраструктуры с установленной гостевой ОС Windows 8.1, с установленным агентом аутентификации;
- VM 4 — сервер виртуализации Hyper-V с установленным гипервизором ОС Hyper-V 2012.

Конфигурация стенда соответствует требованиям ТЗ на ВКР, которые описаны в главе 1.

Общая структура стенда представлена в приложении А на рисунке А.1.

6 Порядок выполнения практического задания: «Управление виртуальной инфраструктурой и безопасностью виртуальной инфраструктуры при использовании СЗИ vGate»

6.1 Общие сведения о СЗИ vGate

СЗИ vGate является сертифицированным средством защиты платформ виртуализации на базе VMware vSphere, Microsoft Hyper-V и Скала-Р. Продукт обеспечивает защиту от специфических угроз виртуализации, позволяет контролировать действия администраторов виртуальной инфраструктуры и осуществляет фильтрацию трафика на уровне гипервизора.

vGate предназначен для решения следующих задач:

- разграничение доступа к управлению виртуальной инфраструктурой;
- контроль действий привилегированных пользователей;
- контроль целостности виртуальных машин;
- регистрация и мониторинг событий безопасности виртуальной инфраструктуры;
- фильтрация сетевого трафика на уровне гипервизора;
- выполнение требований и рекомендаций по защите виртуальной инфраструктуры.

6.2 Создание учетных записей администраторов

Для начала работы необходимо открыть программу Oracle VM Virtual Box и запустить ВМ 1, ВМ 2, ВМ 3 и ВМ 4. После запуска произвести ввод логина и пароля администратора на каждой запущенной машине.

Необходимо запустить программу «Консоль управление vGate для Hyper-V», которая находится на рабочем столе ВМ 2.

В появившемся окне необходимо указать пароль.

Для создания учетной записи необходимо запустить консоль «Мастер создания пользователя». Далее нажать кнопку «Создать». Необходимо указать

имя пользователя и дважды указать пароль, также есть функции по настройке свойств пароля. Результат представлен на рисунке 124.

The screenshot shows a window titled "Мастер создания пользователя" (Master of user creation). The current step is "Свойства учетной записи" (Account properties), with the instruction: "Настройте учетную запись пользователя: укажите имя пользователя, пароль и задайте свойства пароля" (Configure the user account: specify the username, password, and set password properties). The form contains three input fields: "Пользователь:" (Username) with the value "Test", "Пароль:" (Password) with masked characters "*****", and "Подтверждение:" (Confirmation) also with "*****". Below these are three unchecked checkboxes: "Срок действия пароля неограничен" (Password validity is unlimited), "Учетная запись отключена" (Account is disabled), and "Сменить пароль при следующем входе в систему" (Change password at next system login). At the bottom are three buttons: "< Назад" (Back), "Далее >" (Next), and "Отмена" (Cancel).

Рисунок 124 — Указание свойств учетной записи

Затем нажать кнопку «Далее», появится окно настройки прав доступа для администратора виртуальной инфраструктуры. Для создания учетной записи АВИ необходимо выбрать пункт «Разрешен доступ к виртуальной инфраструктуре» и выбрать список действий, которые будут доступны АВИ. Результат представлен на рисунке 125.

The screenshot shows the same window "Мастер создания пользователя", but the current step is "Настройка прав доступа" (Access rights configuration), with the instruction: "Настройка прав доступа администратора виртуальной инфраструктуры" (Access rights configuration for the virtual infrastructure administrator). The first checkbox, "Разрешен доступ к виртуальной инфраструктуре" (Access to virtual infrastructure is allowed), is checked. Below it is a list of permissions, each with a checked checkbox: "Администратор виртуальных машин" (Virtual machine administrator), "Пользователь виртуальных машин" (Virtual machine user), "Администрирование сетей" (Network administration), "Администрирование серверов виртуализации" (Virtualization server administration), "Администрирование хранилищ" (Storage administration), "Операции с файлами в хранилищах" (File operations in storage), and "Администрирование SCVMM и кластеров Hyper-V" (SCVMM and Hyper-V cluster administration). At the bottom are the same three buttons: "< Назад" (Back), "Далее >" (Next), and "Отмена" (Cancel).

Рисунок 125 — Настройка прав доступа для АВИ

Затем необходимо нажать кнопку «Далее», появится окно настройки прав доступа для администратора информационной безопасности, в нем будут доступны 3 типа учетных записей:

- Администратор информационной безопасности (необходимо отметить это поле, если создается учетная запись АИБ);
- Оператор учетных записей (необходимо отметить это поле, если необходимо чтобы создаваемая учетная запись имела права на управление списком пользователей, при выборе данного параметра пользователю автоматически будут предоставлены права доступа АИБ);
- Аудитор безопасности (необходимо отметить это поле, если необходимо предоставить пользователю права только на просмотр данных в программе управления vGate, без возможности внесения изменений).

Для того чтобы завершить работу мастера необходимо нажать кнопку «Завершить». Созданная учетная запись появится в списке. Результат представлен на рисунке 126 и 127.

Мастер создания пользователя

Настройка прав доступа
Настройка прав доступа администратора безопасности

☒ Администратор информационной безопасности

☐ Оператор учетных записей

☐ Аудитор безопасности

< Назад Завершить Отмена

Рисунок 126 — Настройка прав доступа для АИБ

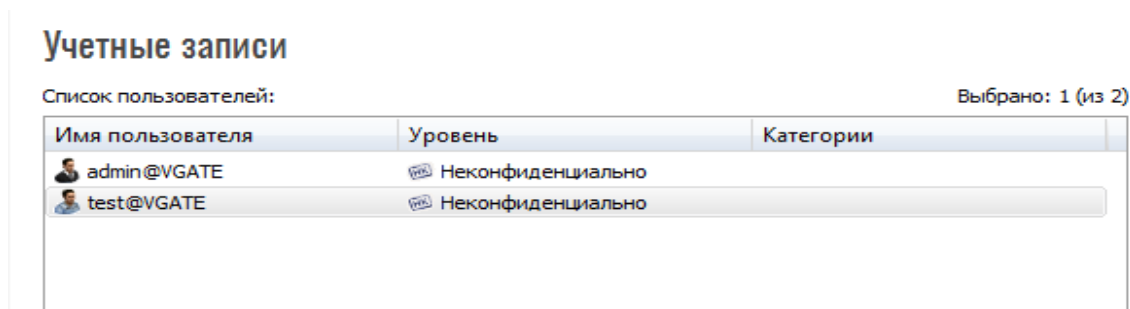


Рисунок 127 — Результат создания учетной записи

Для отключения учетной записи необходимо выбрать учетную запись и нажать кнопку «Редактировать». Необходимо отметить поле «Учетная запись отключена» и нажать кнопку «ОК». Авторизованный пользователь сможет продолжить работу и после отключения учетной записи, вплоть до следующей попытки авторизации. Результат представлен на рисунке 128 и 129.

Рисунок 128 — Отключение учетной записи АВИ

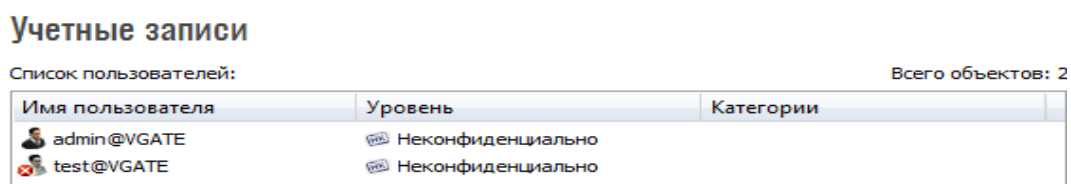


Рисунок 129 — Результат отключения учетной записи

Необходимо аналогично создать учетную запись АИБ.

Для проверки создания учетных записей необходимо авторизоваться, используя созданные данные. Результаты создания учетных записей и проверки авторизации представить в виде снимков экрана.

6.3 Управление учетными записями пользователей

Политики паролей позволяют обеспечить использование паролей необходимого уровня сложности. Все пароли, настраиваемые для учетных записей АВИ и АИБ, должны удовлетворять политикам. При смене пароля пользователя как через консоль управления, так и с помощью агента аутентификации проверяется соответствие нового пароля настроенным политикам паролей.

Для настройки парольной политики необходимо выбрать пункт «Учетные записи» и нажать кнопку «Политики паролей». Появится окно «Политики паролей пользователей». Необходимо изменить значение нужного параметра и нажать кнопку «Сохранить». Результат представлен на рисунке 130.

Политики паролей пользователей	
Максимальный срок действия пароля:	30 дней
Минимальная длина пароля:	7 символов
Хранить историю:	4 паролей
Разница при смене пароля:	4 символов
Минимальное количество классов символов:	3
Отключить учетную запись, неиспользуемую более:	
90	дней
Отключить учетную запись после:	
3	неуспешных попыток входа
<div>OK Отмена</div>	

Рисунок 130 — Политики паролей пользователей

Список доступных параметров:

— «Максимальный срок действия пароля». Определяет период времени, на протяжении которого действителен текущий пароль пользователя. По истечении заданного периода времени текущий пароль пользователя перестает быть действительным и его требуется изменить. Этот параметр может принимать значение от 1 до 365 дней;

— «Минимальная длина пароля». Определяет минимальное количество символов в пароле. Пользователю нельзя назначить пароль,

количество символов в котором меньше значения данного параметра. Этот параметр может принимать значение от 1 до 100;

— «Хранить историю». Определяет число старых паролей каждого пользователя, информация о которых будет храниться системой. При смене пароля пользователя осуществляется сопоставление нового пароля со списком старых паролей этого пользователя. Если новый пароль совпал с одним из старых паролей, то такой пароль запрещается использовать. Этот параметр может принимать значение от 1 до 15;

— «Разница при смене пароля». Определяет количество символов, на которое новый пароль должен отличаться от старого при смене пароля. Этот параметр может принимать значение от 1 до 100;

— «Минимальное количество классов символов». Определяет, сколько именно классов символов (буквы в верхнем и нижнем регистрах, цифры и т. п.) должно присутствовать в пароле. Этот параметр принимает значение от 1 до 4. Значение "1" означает, что пароль может содержать любые символы, например, только буквы в нижнем регистре;

— «Отключить учетную запись, не используемую более». Определяет период времени, через который будут отключены неиспользуемые учетные записи. При необходимости АИБ может включить отключенную учетную запись. Этот параметр может принимать значение от 1 до 1095 дней;

— «Отключить учетную запись после». Определяет количество неуспешных попыток ввода пароля при входе, после которых учетная запись будет отключена. При необходимости АИБ может включить отключенную учетную запись. Этот параметр может принимать значение от 1 до 255.

Необходимо установить политику паролей чтобы она удовлетворяла следующим условиям:

- максимальный срок действия пароля — 90 дней;
- минимальная длина пароля — 8 символов;

- хранить историю — 15 паролей;
- разница при смене пароля — 8 символов;
- минимальной количество классов символов — 4 класса;
- отключить учетную запись ,не используемую более — 45 дней;
- отключить учетную запись запись после — 5 неуспешных

попыток входа.

Необходимо попробовать создать учетную запись чтобы она не удовлетворяла требованиям политики паролей. Результат создание учетной записи не удовлетворяющей требованиям политики паролей представить в виде снимков экрана.

6.4 Настройка прав на управление виртуальной инфраструктурой и управление информационной безопасностью с проверкой возможности применения этих прав

В vGate реализован принцип разделения ролей — разделение прав на управление виртуальной инфраструктурой и управление информационной безопасностью. При установке сервера авторизации vGate создается учетная запись главного администратора информационной безопасности. Изначально главный АИБ распределяет права между пользователями vGate, используя для этого две основные роли — администратор виртуальной инфраструктуры (АВИ) и администратор информационной безопасности (АИБ). Данные роли обладают следующими полномочиями.

Необходимо в консоли управления выбрать пункт «Учетные записи» и выбрать «Редактировать». Результат представлен на рисунке 131.

Необходимо настроить права доступа учетным записям АВИ и АИБ.

Для первой учетной записи АВИ необходимо установить следующие параметры:

- «Администратор виртуальных машин»;

- «Пользователь виртуальных машин»;
- «Администрирование сетей».

Для второй учетной записи АВИ необходимо установить следующие параметры:

- «Администрирование серверов виртуализации»;
- «Администрирование хранилищ»;
- «Операции с файлами в хранилищах».

Также необходимо настроить права доступа учетной записи АИБ. Необходимо установить следующие параметры:

- «Администратор информационной безопасности»;
- «Оператор учетных записей»;
- «Аудитор безопасности».

Мастер изменения пользователя testaib@VGATE

Свойства учетной записи
 Настройте учетную запись пользователя: укажите имя пользователя, пароль и задайте свойства пароля

Пользователь:

Пароль:

Подтверждение:

☐ Срок действия пароля неограничен

☐ Учетная запись отключена

☐ Сменить пароль при следующем входе в систему

< Назад Далее > Отмена

Рисунок 131 — Редактирование прав учетной записи

Результаты создание учетных записей представлены на рисунках с 132 по 134.

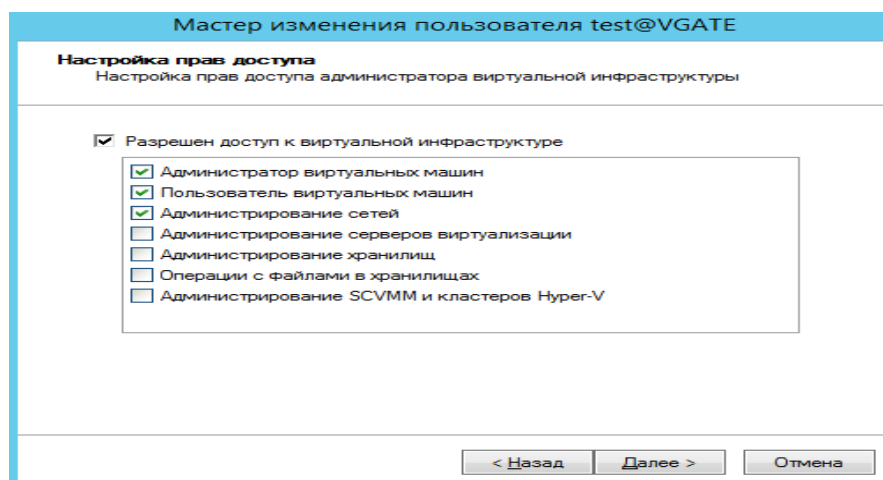


Рисунок 132 — Настройка прав доступа для 1 АВИ

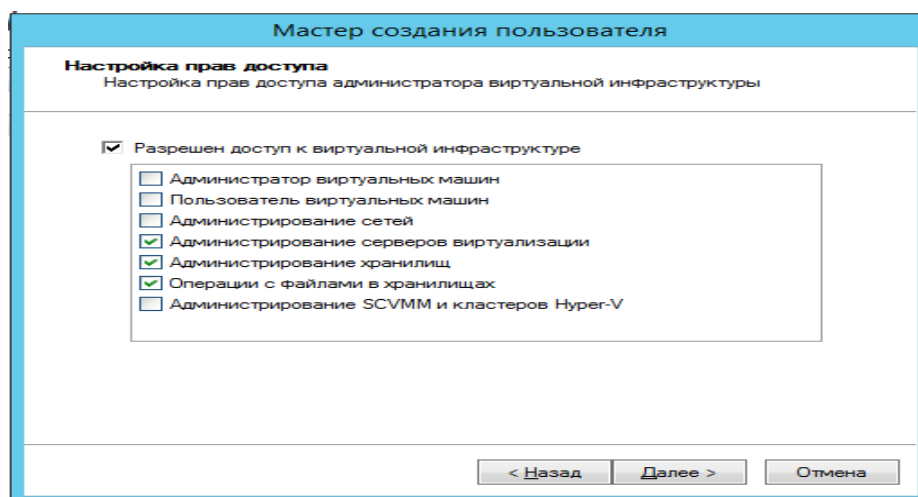


Рисунок 133 — Настройка прав доступа для 2 АВИ

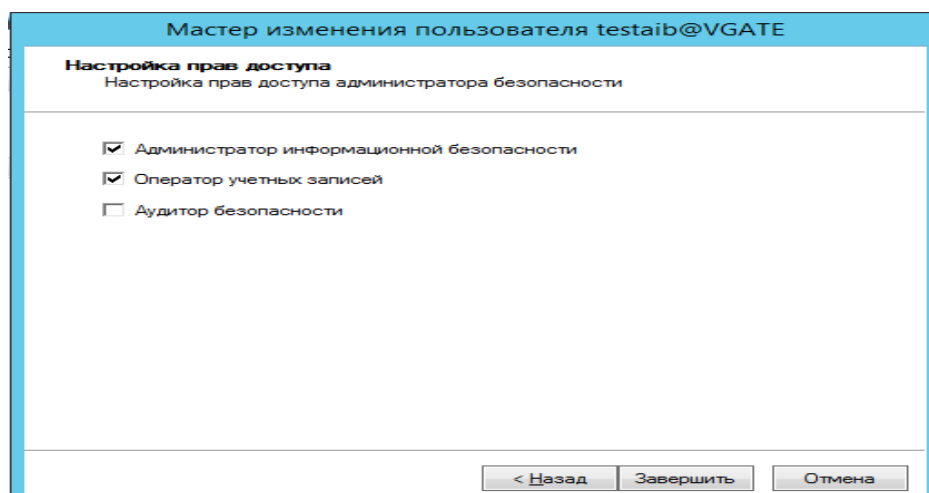


Рисунок 134 — Настройка прав доступа для АИБ

Для проверки настроенных прав доступа необходимо с помощью учетной записи АВИ авторизоваться в Агенте аутентификации и проверить доступные им функции, а с помощью учетной записи АИБ авторизоваться в Консоли управления и проверить доступные ему функции. Результаты авторизации учетных записей и проверки доступных им функций представить в виде снимков экрана.

6.5 Управление политиками безопасности

Политики безопасности содержат настройки для серверов Hyper-V и VM, позволяющие обеспечить определенную степень защиты данных и соответствие требованиям некоторых стандартов безопасности. Применение политик безопасности и механизма полномочного управления доступом позволяет обеспечить необходимый уровень безопасности.

Необходимо в консоли управления выбрать пункт Политики безопасности. Далее нажать кнопку «Добавить», указать имя набора политик и его описание (при необходимости). Выбрать «Новый набор политик» и нажать кнопку «Далее». Из списка шаблонов наборов политик, выбрать нужный и нажать кнопку «Далее». Из списка параметров политик включить необходимые и нажать кнопку «Завершить». Результат создания политики представлен на рисунках с 135 по 138.

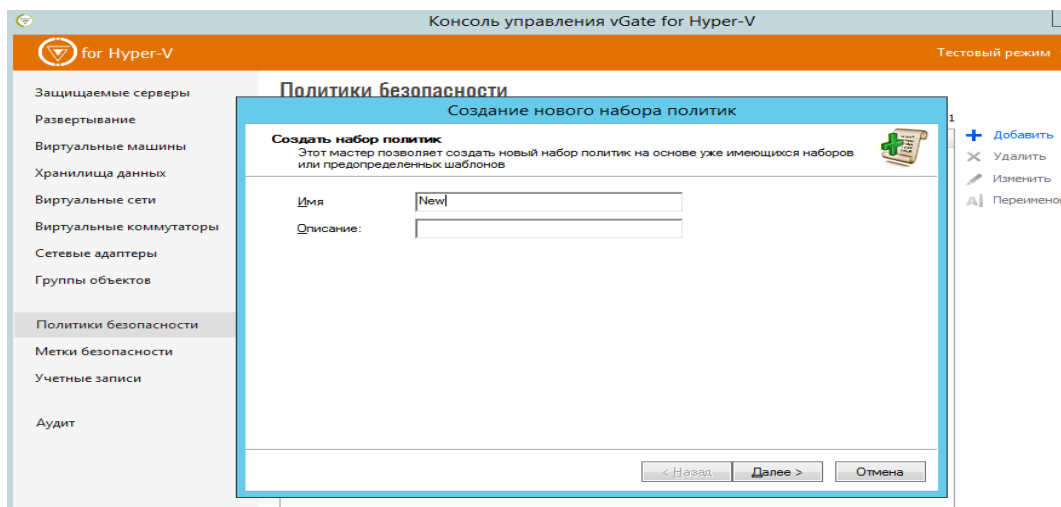


Рисунок 135 — Задание имени политики

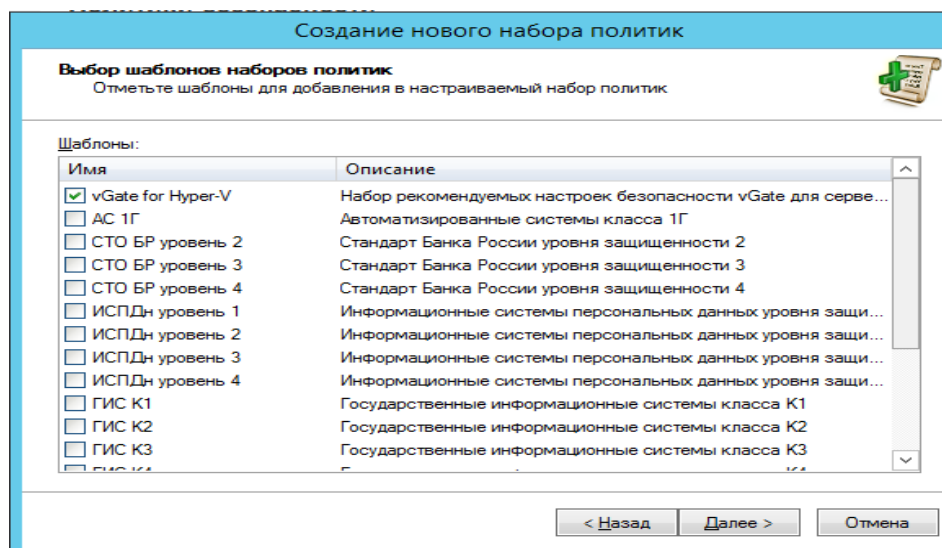


Рисунок 136 — Выбор шаблона политики

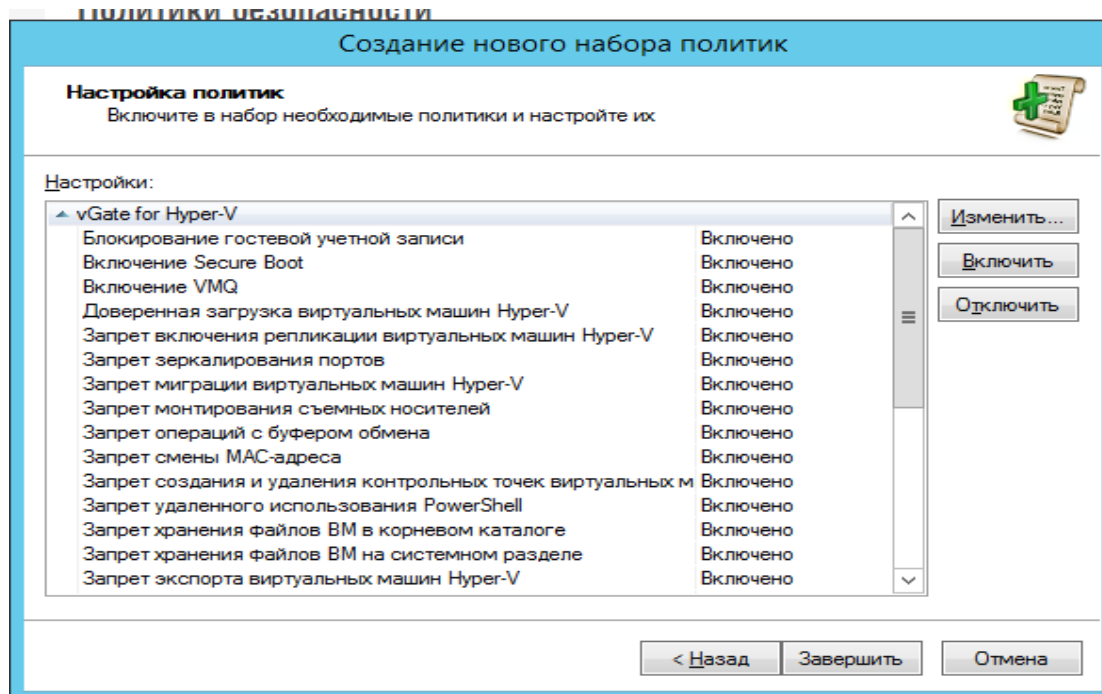


Рисунок 137 — Настройка политик

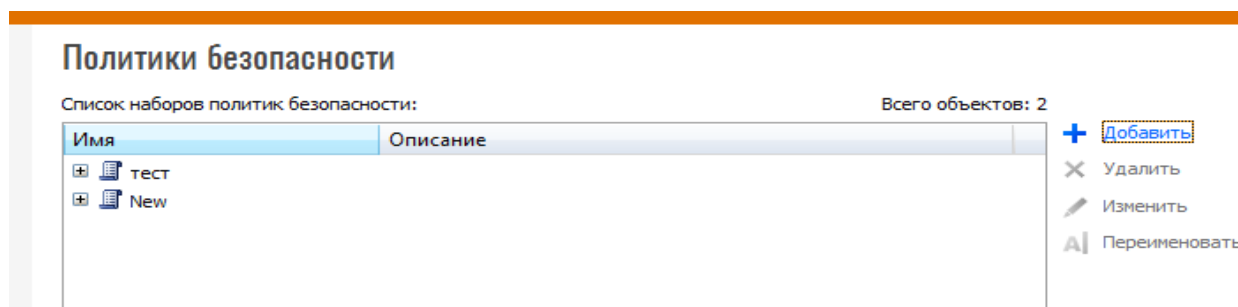


Рисунок 138 — Созданная политика

Для назначения набора политик необходимо выбрать объект которому необходимо назначить политики и нажать кнопку «Назначить политики». Выбрать нужный набор политик и нажать кнопку «Назначить». Название набора политик будет отображено в колонке «Наборы политик безопасности». Результат представлен на рисунках 139 и 140.

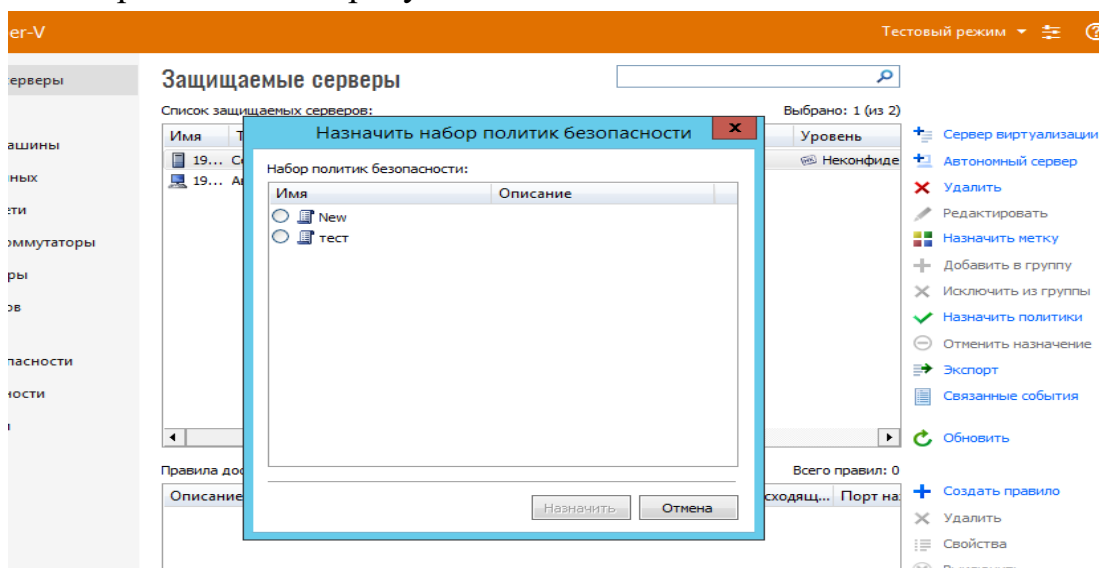


Рисунок 139 — Назначение набора политик безопасности

Список защищаемых серверов:							Выбрано: 1 (из 2)
	Сокеты	Уровень	Категор...	Разрешен...	Пояснение	Группа	Наборы ...
600)	1	Неконфиденци...		Да	VGATE-HSV.vgat...		New
Сервер авториз...							

Рисунок 140 — Проверка назначения политики безопасности

Для проверки применения политик необходимо попробовать выполнить любое действие, указанное при настройке политики. Результаты работы политики безопасности представить в виде снимков экрана.

6.6 Регистрация событий информационной безопасности

События безопасности регистрируются на всех защищаемых серверах, на которых установлены компоненты защиты vGate, а затем пересылаются на сервер авторизации для централизованного хранения.

Необходимо в консоли управления выбрать пункт «Аудит». Появится таблица со списком событий, а над ней группа параметров для формирования условий отбора записей.

Необходимо указать условия отбора записей. Для выбора параметров отбора записей установить отметки рядом с названиями нужных характеристик в раскрывающихся списках - Типы событий, Компоненты и Категории. При необходимости выбрать период времени регистрации событий в поле Время событий. Для ограничения длины списка указать нужное значение в поле Событий, не более. Для возврата к набору параметров фильтрации записей, предлагаемому по умолчанию нажать кнопку «Сбросить». Далее нажать кнопку «Применить». Для детального просмотра отдельных записей необходимо выделить нужную запись и нажать кнопку «Свойства». Результат настройки аудита представлен на рисунках 141 и 142.

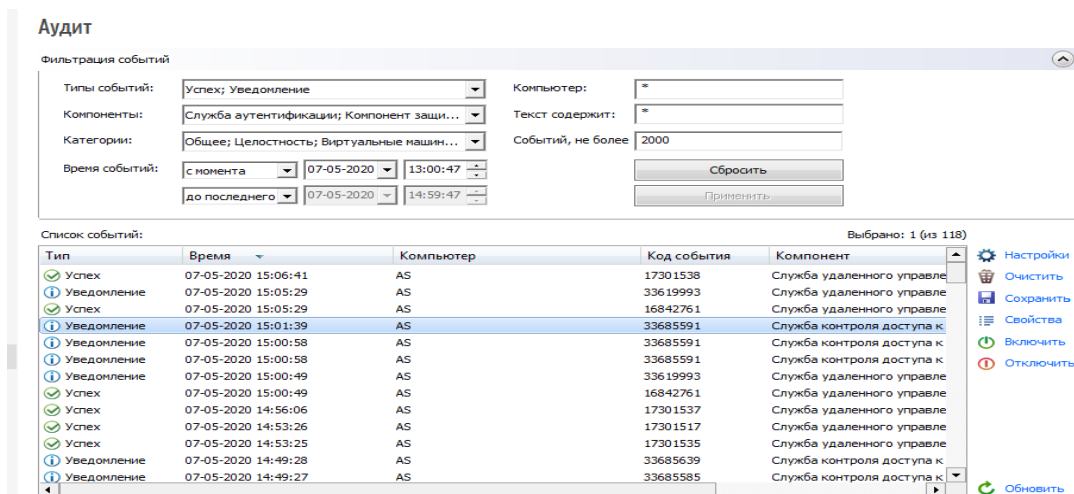


Рисунок 141 — Настройка аудита

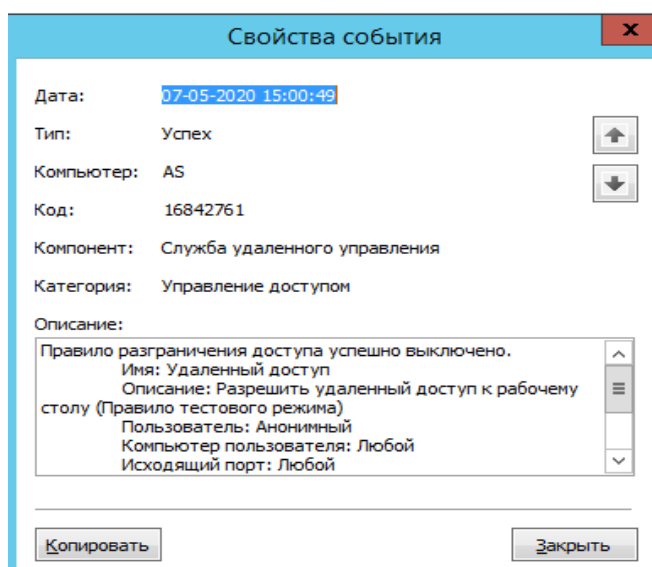


Рисунок 142 — Детальный просмотр записи аудита

Для сохранения журнала событий безопасности необходимо в консоли управления выбрать «Аудит». Нажать кнопку «Сохранить». Задать имя файла и нажать кнопку «Сохранить». Результат сохранения журнала безопасности представлен на рисунке 143.

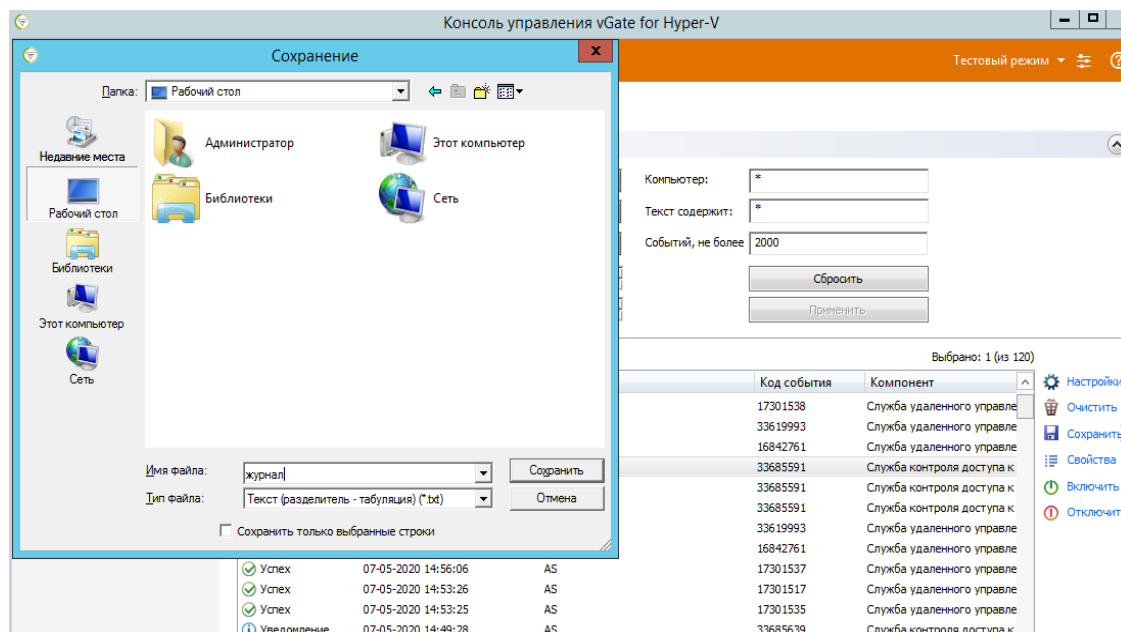


Рисунок 143 — Сохранение журнала безопасности

Необходимо получить всю информацию, относящуюся к применению и отмене политик безопасности, а также информацию об виртуальных машинах Hyper-V. Результаты представить в виде снимков экрана. В отчет необходимо включить сохраненный журнал безопасности.

6.7 Управление режимами работы vGate

Помимо штатного режима работы в vGate предусмотрены дополнительные режимы для ослабления контроля за администрированием виртуальной инфраструктуры в служебных целях.

— «Штатный режим». В данном режиме могут использоваться все функциональные возможности vGate по защите виртуальной инфраструктуры. Режим должен быть включен для обеспечения полноценной защиты;

— «Тестовый режим». Данный режим позволяет выполнить ввод в эксплуатацию или настройку конфигурации vGate, не ограничивая работу существующей сетевой инфраструктуры. Обеспечивает доступ к серверам виртуальной инфраструктуры вне зависимости от настроенных в vGate правил разграничения доступа. Режим включен по умолчанию только после первоначальной установки vGate;

— «Аварийный режим». Режим предназначен для приостановки защиты в случае выхода из строя элементов ИТ-инфраструктуры. Позволяет обойти установленные vGate ограничения доступа к администрированию виртуальной среды на время восстановления работоспособности инфраструктуры. В отличие от штатного и тестового режимов работы, в аварийном режиме не регистрируются события безопасности.

Для переключения vGate в штатный режим необходимо нажать кнопку «Тестовый режим» и выбрать вариант «Штатный режим». Нажать кнопку «Продолжить». После этого штатный режим vGate будет включен. Результат переключения режима представлен на рисунках 144 и 145.

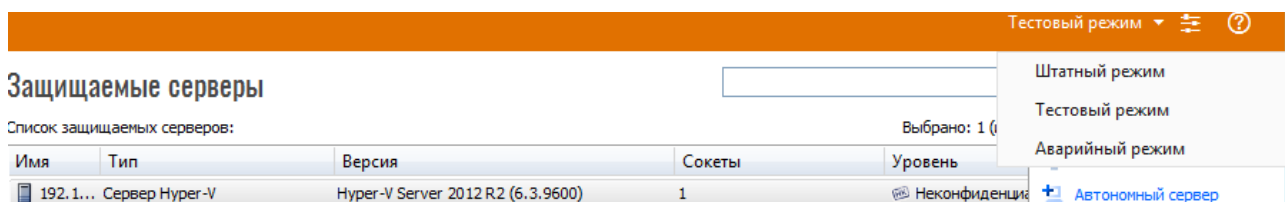


Рисунок 144 — Переключение vGate в штатный режим

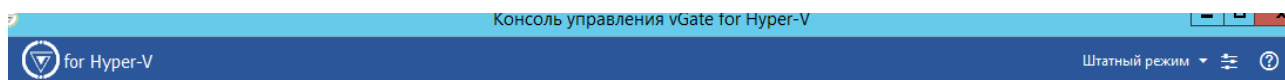


Рисунок 145 — Работа vGate в штатном режиме

Для переключения vGate в тестовый режим необходимо нажать кнопку «Штатный режим» и выбрать вариант «Тестовый режим». Нажать кнопку «Продолжить». После этого тестовый режим vGate будет включен.

Для переключения vGate в аварийный режим необходимо нажать кнопку текущего режима и выбрать вариант «Аварийный режим». Нажать кнопку «Продолжить». После этого аварийный режим vGate будет включен.

Необходимо переключить режим работы vGate в штатный и проверить работу настроенных правил разграничения доступа.

Необходимо переключить режим работы vGate в аварийный и проверить работу настроенных правил разграничения доступа.

Результаты переключения режимов работы vGate и проверка работы настроенных правил представить в виде снимков экрана.

6.8 Мониторинг безопасности

Общее описание соответствующего механизма.

Мониторинг безопасности vGate позволяет осуществлять сбор и анализ данных о событиях на объектах виртуальной инфраструктуры: сервере авторизации vGate, защищаемых серверах, компьютерах сети администрирования, на которых установлен агент аутентификации vGate.

Правила корреляции позволяют отслеживать конкретные события, происходящие при заданных условиях в виртуальной инфраструктуре. При срабатывании правил создаются инциденты.

Инциденты — это события, которые создаются при срабатывании правил корреляции.

Описание его параметров и настроек.

Для работы функции мониторинга необходимо выполнить подключение к серверу мониторинга vGate, развернутому в сети.

Для развертывания сервера мониторинга необходимо в диспетчере Hyper-V создать виртуальную машину, удовлетворяющую следующим требованиям:

- процессор- 2 ГГц;
- память- 4Гб;
- сеть- LAN.

Для этого с рабочего места АВИ необходимо запустить программу «Диспетчер» Hyper-V». Появится консоль «Мастер создания виртуальной

машины», необходимо нажать кнопку «Далее», нужно указать имя виртуальной машины и нажать кнопку «Далее», необходимо выбрать поколение виртуальной машины, выбрать Поколение 1 и нажать кнопку «Далее», нужно указать объем памяти, выделяемой при запуске (32Мб) и выбрать пункт «Использовать для этой виртуальной машины динамическую память» и нажать кнопку «Далее», выбрать тип подключения «Локальная» и нажать кнопку «Далее», выбрать пункт использовать имеющийся виртуальный жесткий диск и нажать кнопку «Обзор», выбрать жесткий диск, расположенный на установочном диске vGate в архиве \monitoring\Monitoring-1.zip и нажать кнопку «Далее», выбрать пункт установить операционную систему позднее и нажать кнопку «Готово». После создания ВМ необходимо выбрать ее в Диспетчере Hyper-V, нажать кнопку «Параметры», выбрать пункт «Память» и указать минимальный (4096МБ) и максимальный (4096Мб) объем ОЗУ.

Результат представлен на рисунках с 146 по 149.

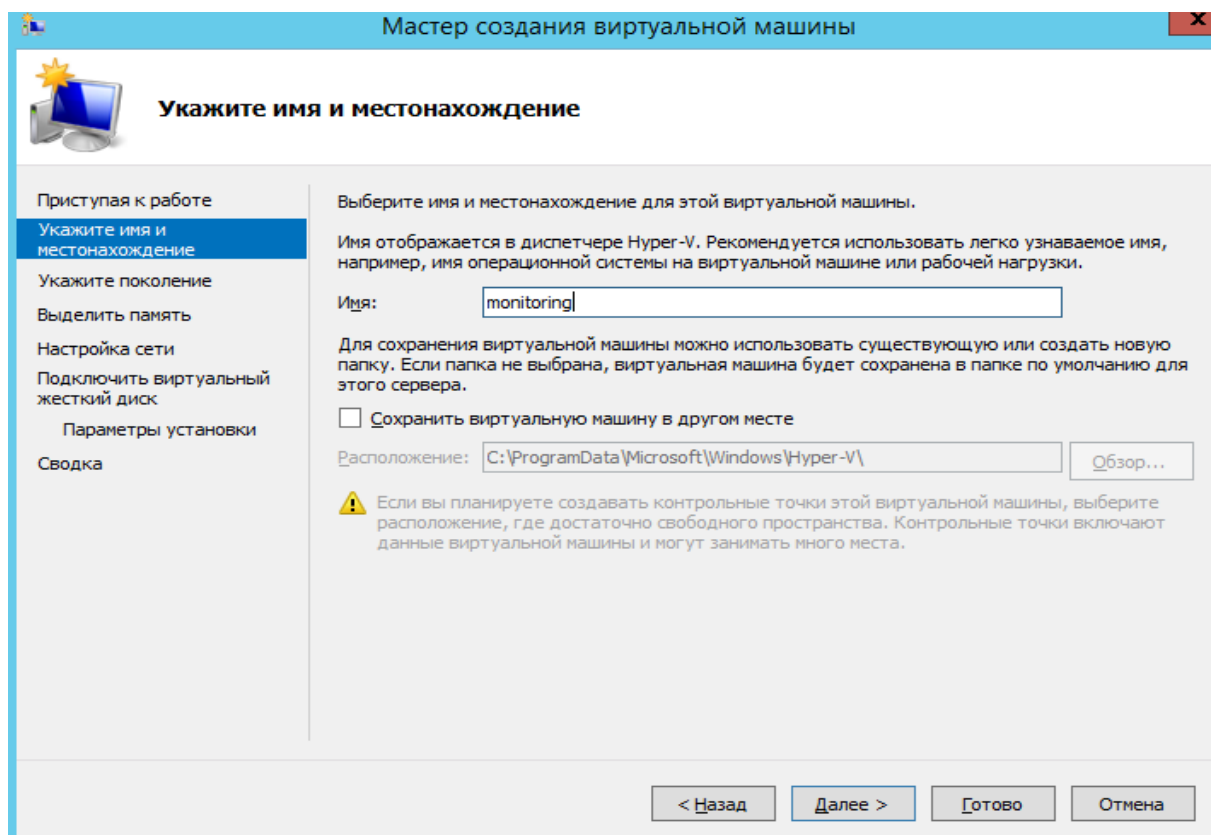


Рисунок 146 — Указание имени ВМ

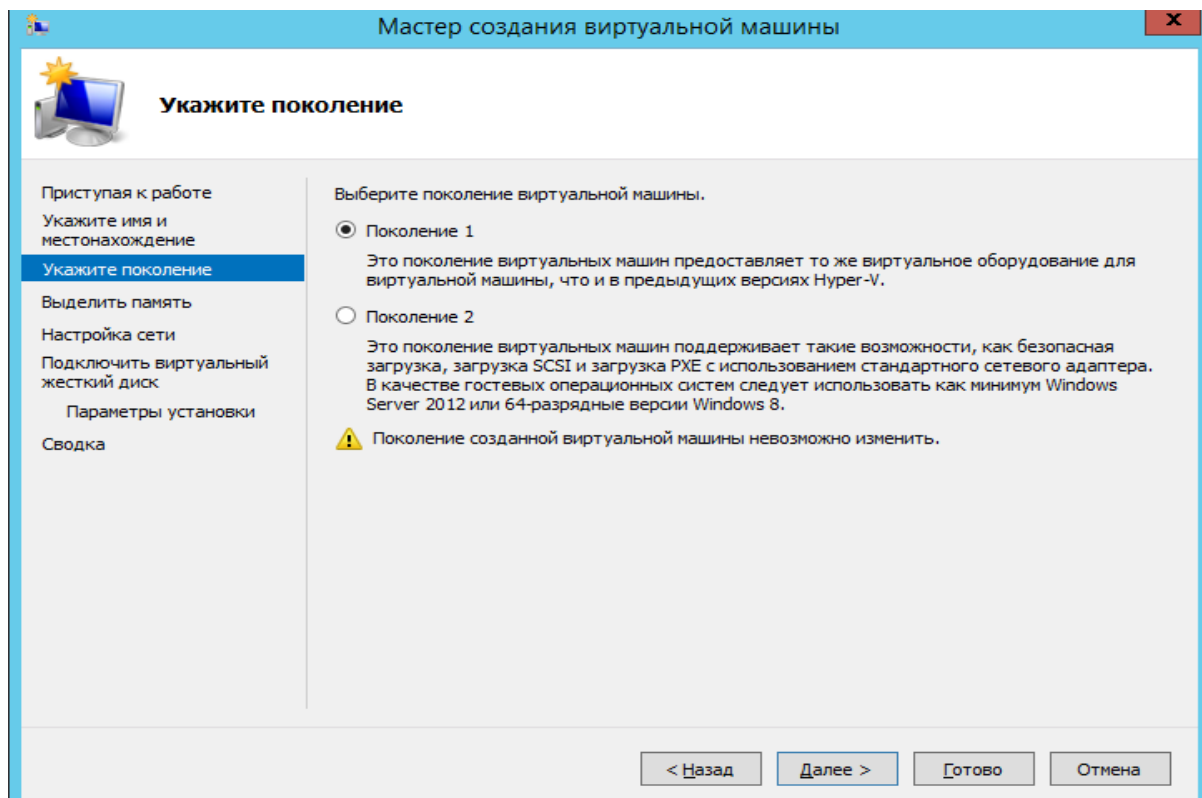


Рисунок 147 — Указание поколения ВМ

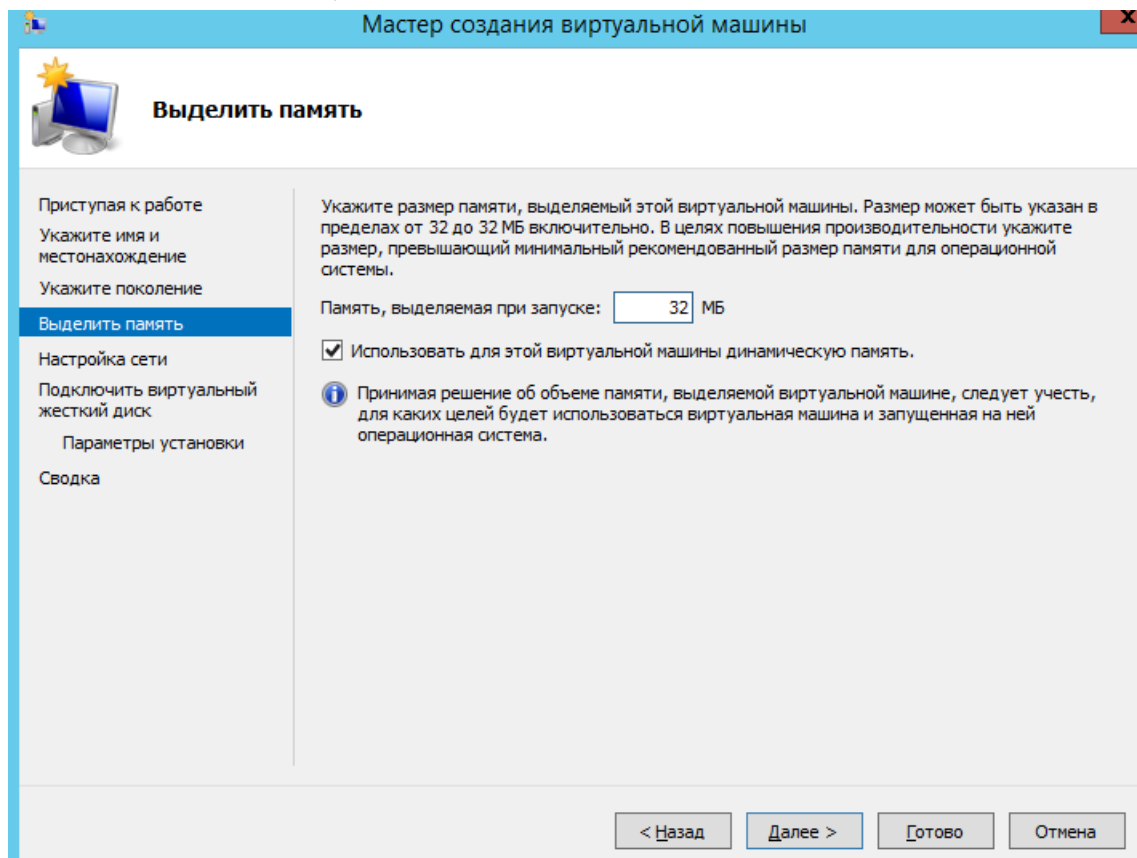


Рисунок 148 — Указание памяти, выделяемой при запуске

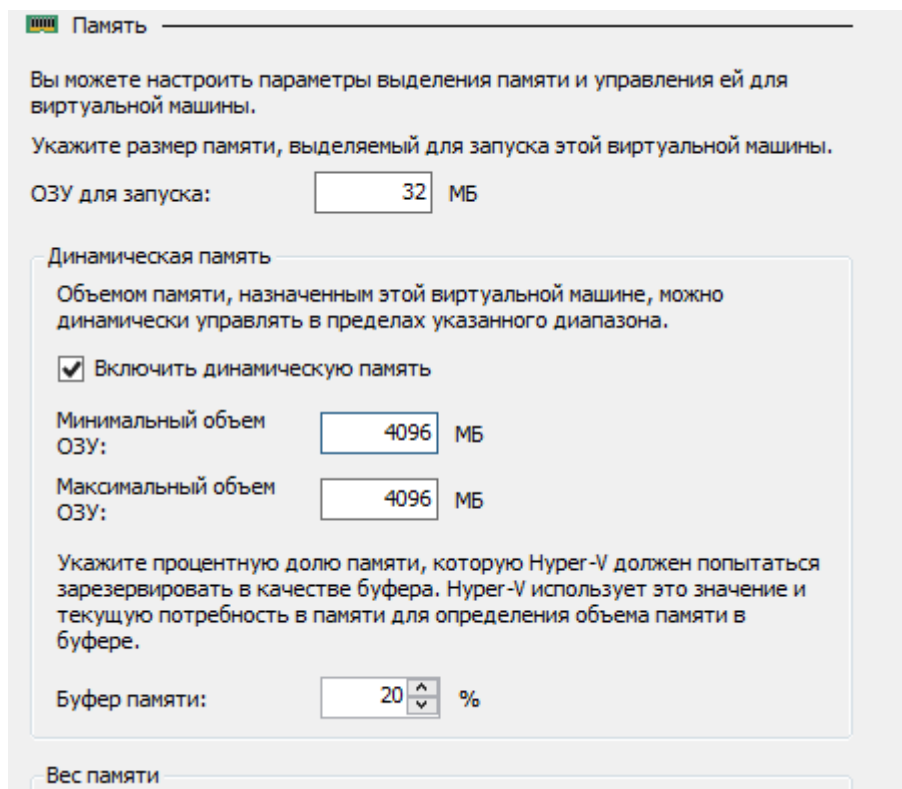


Рисунок 149— Настройка объема ОЗУ после создания VM

После запуска VM необходимо ввести учетные данные: имя (administrator) и пароль (qwe). Выполнить команду: `sudo vgate-config`, Далее выполнить команду: `sudo vgate-config network`. Необходимо указать IP-адрес сервера мониторинга, маску подсети, сетевой шлюз и DNS-сервер. Далее необходимо создать учетную запись пользователя для подключения к серверу мониторинга. Необходимо выполнить команду и задать имя и пароль пользователя: `sudo vgate-config users create`.

Далее с помощью учетной записи АИБ, открыть веб-консоль и в главном меню выбрать раздел «Настройки» и перейти на вкладку «Мониторинг». Необходимо указать параметры для подключения к серверу мониторинга и нажать кнопку сохранить.

Далее выбрать раздел «Мониторинг», а затем «Панель мониторинга». Нажать кнопку «Добавить виджет», откроется панель добавления виджетов. Выбрать из списка виджеты, которые необходимо отображать на панели

мониторинга. Выбранные диаграммы появятся на панели мониторинга. Результат представлен на рисунках с 150 по 152.

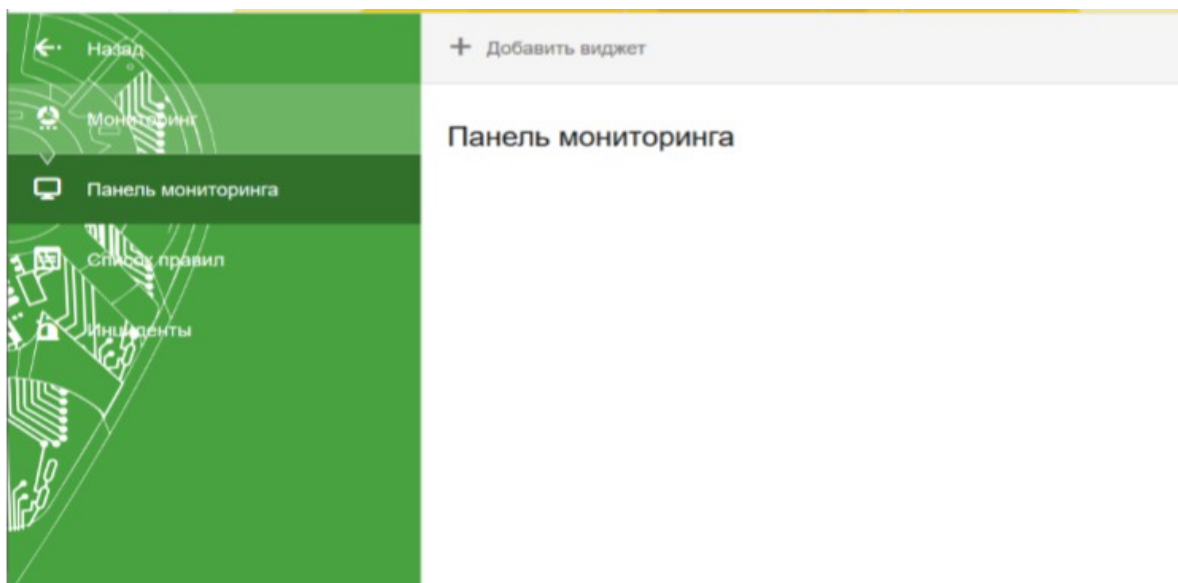


Рисунок 150 — Выбор Панели мониторинга

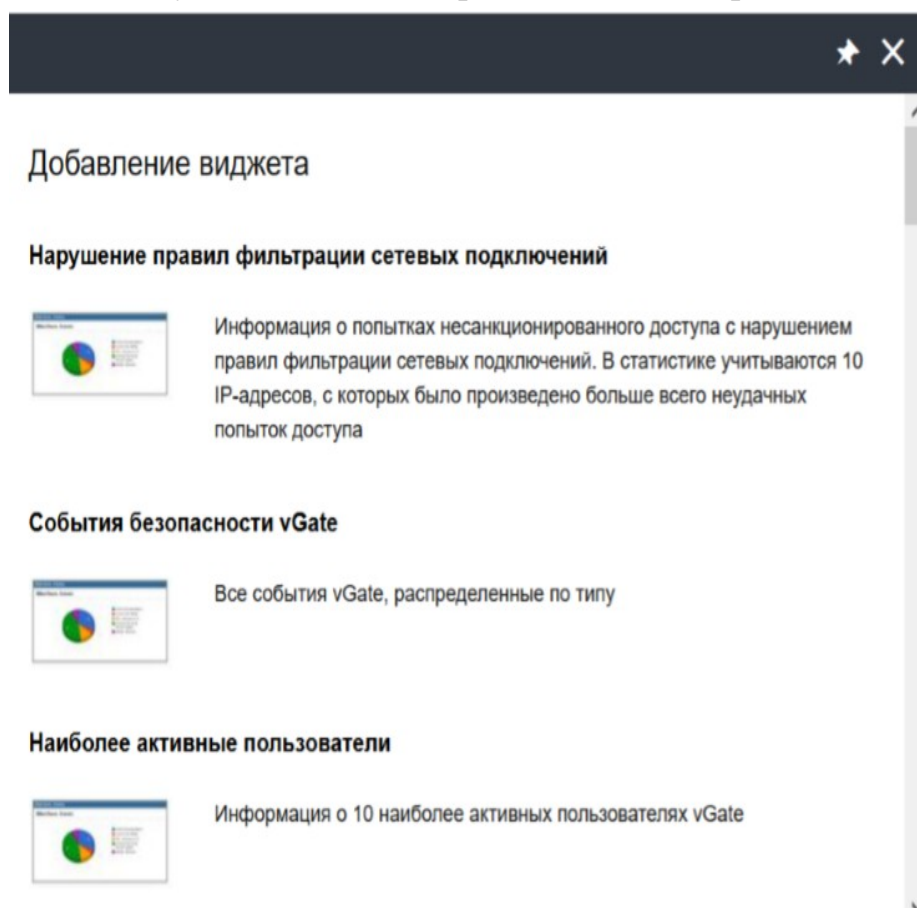


Рисунок 151 — Добавление виджета

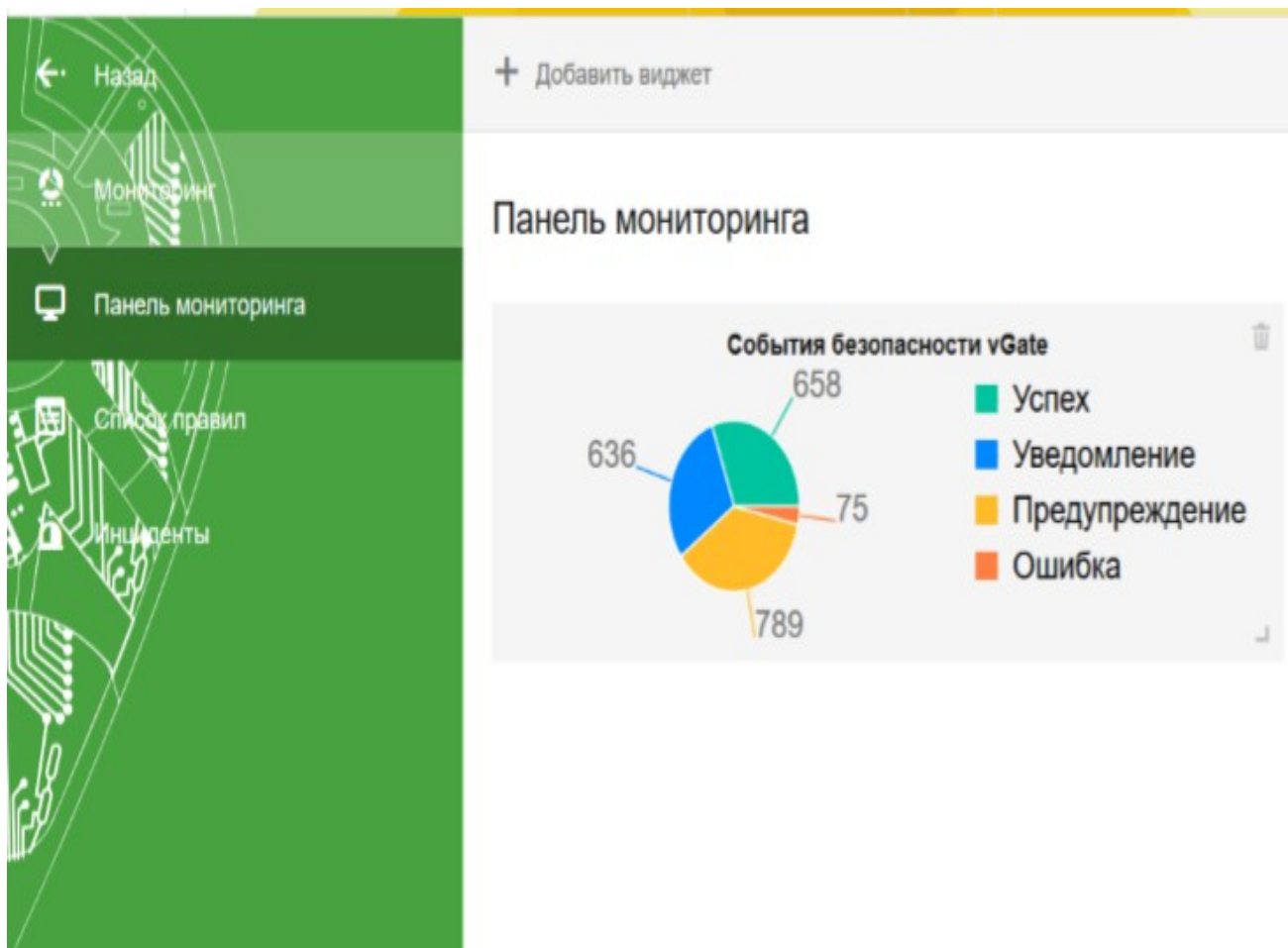


Рисунок 152 — Отображение виджетов на Панели мониторинга

Для создания правила необходимо выбрать раздел «Мониторинг» и перейти на вкладку «Список правил». Нажать на кнопку «Добавить» и выбрать тип создаваемого правила:

- новое правило;
- правило по шаблону;
- правило в обход vGate.

Для добавления нового правила необходимо указать его параметры: название, критичность (приоритет правила), интервал (проверки событий в секундах, минутах или часах), способ оповещения, группировать по (выбрать параметр, по которому необходимо группировать произошедшие события). Результат представлен на рисунках с 153 по 156.

★ ✕

Добавление нового правила

Название правила:

Введите текст

Критичность: ⓘ

Выберите значение ▾

Интервал: ⓘ

Введите число

Выберите значение ▾

Способ оповещения: ⓘ

Выберите значение ▾

Группировать по: ⓘ

Выберите значение ▾

Для сохранения правила необходимо добавить от одного до 8 событий.

Сохранить

Список событий

Сброс

Рисунок 153 — Добавление нового правила

★ ✕

Добавление правила на основе шаблона

Название правила:

Введите текст

Критичность: ⓘ

Выберите значение ▾

Интервал: ⓘ

Введите число

Выберите значение ▾

Способ оповещения: ⓘ

Выберите значение ▾

Группировать по: ⓘ

Выберите значение ▾

Для сохранения правила необходимо добавить от одного до 8 событий.

Сохранить

Список шаблонов

Сброс

Рисунок 154 — Добавление нового правила на основе шаблона

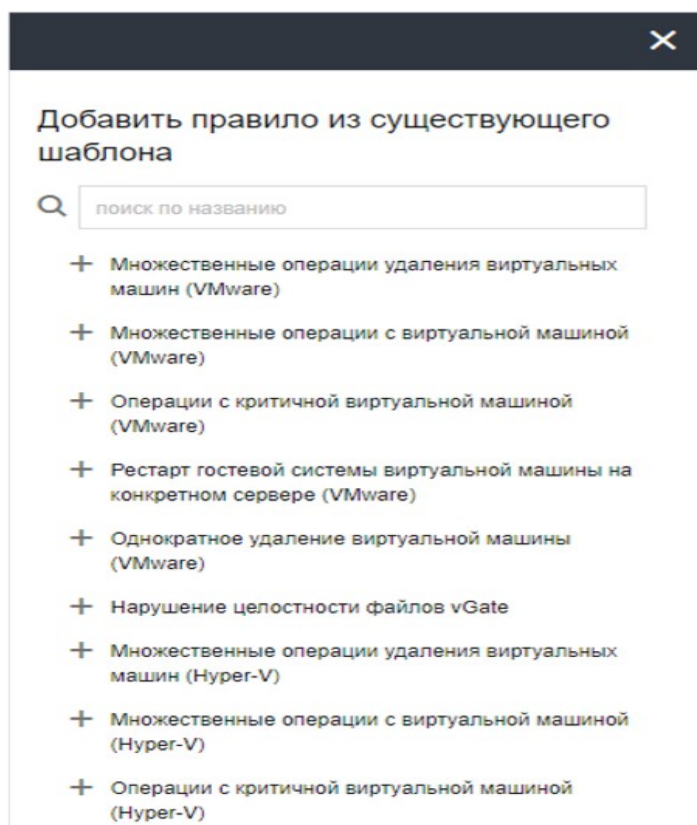


Рисунок 155 — Выбор существующих шаблонов

Добавление правила в обход vGate

Название правила:

Критичность: ☐ ☐ ☐

Интервал: ☐ ☐ ☐

Способ оповещения: ☐ ☐ ☐

Группировать по: ☐ ☐ ☐

Рисунок 156 — Добавление правила в обход vGate

Нажать кнопку «Список событий», для того чтобы выбрать отслеживаемые правила. Выбрать из списка событие и нажать +. Указать количество событий, необходимых для срабатывания правила и нажать кнопку «Применить». Указать параметры фильтра и нажать кнопку «Добавить правило». Нажать кнопку «Сохранить».

Для просмотра списка инцидентов необходимо выбрать раздел «Мониторинг» и перейти на вкладку «Инциденты». Для просмотра подробной информации о событии, выбрать его и нажать кнопку «Свойства». Для того чтобы пометить инцидент просмотренным, нажать кнопку «Пометить как обработанный».

Для создания отчетов необходимо выбрать пункт «Создание отчетов», выбрать нужный отчет в одной из категорий и нажать кнопку «Создать и загрузить отчет».

Для проверки работоспособности необходимо настроить панель мониторинга. Создать несколько правил корреляции. Выполнить проверку инцидентов. Создать отчет о событиях безопасности. Результаты представить в виде снимков экрана. В отчет необходимо включить сохраненный отчет.

6.9 Базовый и повышенные уровни сложности задания «Управление виртуальной инфраструктурой и безопасностью виртуальной инфраструктуры при использовании СЗИ vGate»

Базовому уровню сложности задания «Управление виртуальной инфраструктурой и безопасностью виртуальной инфраструктуры при использовании СЗИ vGate» соответствуют задачи, описанные в пунктах с 6.2 по 6.7. Повышенному уровню сложности соответствует задача, описанная в пункте 6.8.

7 Порядок выполнения практического задания: «Управление доступом к ресурсам виртуальной инфраструктуры и контроль целостности, реализуемые СЗИ vGate»

7.1 Аутентификация

Доступ к управлению виртуальной инфраструктурой получают только пользователи, прошедшие аутентификацию. В vGate предусмотрена процедура аутентификации пользователей (администраторов виртуальной инфраструктуры) и компьютеров. Аутентификация компьютеров выполняется автоматически.

Для выполнения процедуры аутентификации необходимо запустить ВМ с рабочим местом АВИ. Далее на рабочем столе запустить программу «Агент аутентификации vGate», необходимо выбрать пункт «Новое подключение», указать IP-адрес сервера авторизации, домен, имя пользователя — администратора виртуальной инфраструктуры и пароль. После этого подключение к серверу авторизации появится в списке. Результат представлен на рисунках с 157 по 159.

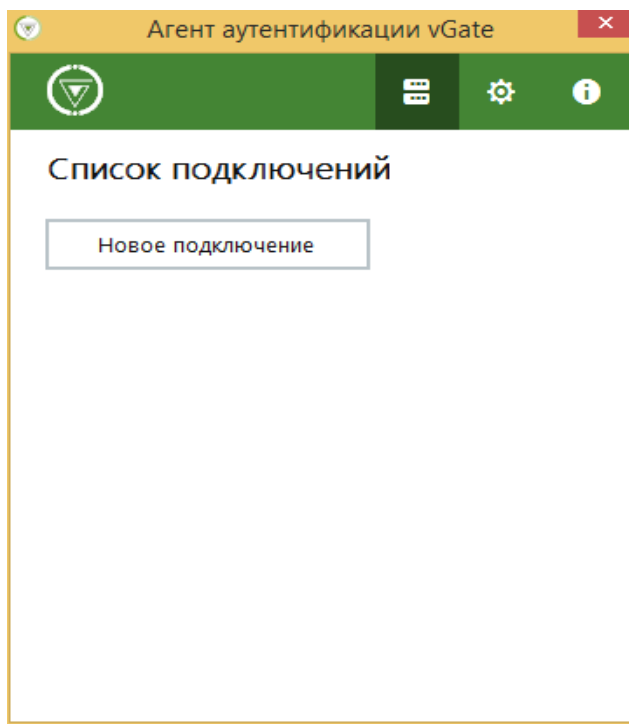


Рисунок 157 — Создание нового подключения

Агент аутентификации vGate

←

Новое подключение

Имя пользователя и пароль

192.168.50.2

vgate

avi

••••••••

☐ Подключать автоматически

Отмена Подключить

Рисунок 158 — Ввод данных для подключения

Агент аутентификации vGate

←

192.168.50.2 ● Подключен

avi@vgate

Неконфиденциально

Сменить пароль

Отключить

Рисунок 159 — Проверка подключения к серверу авторизации

Для проверки работоспособности необходимо выполнить аутентификацию с помощью учетной записи АВИ. Результат представить в виде снимков экрана.

7.2 Управление доступом к защищаемым серверам

До выполнения этой процедуры требуется, чтобы были созданы нужные учетные записи пользователей и компьютеров, чей доступ к защищаемым объектам сети администрирования должен быть регламентирован. Для этого необходимо:

- зарегистрировать пользователей vGate;
- при необходимости установить агенты аутентификации на компьютеры сервисных служб, которым требуются входящие соединения в защищаемый периметр для организации санкционированного доступа служб и сервисов компьютеров к защищаемым серверам Hyper-V и другим узлам защищаемой сети.

Для предоставления доступа необходимо в консоли управления выбрать функцию «Защищаемые серверы», выбрать нужный сервер и выбрать пункт «Создать правило». Появится консоль «Мастер добавления правила», необходимо выбрать способ создания правила и нажать кнопку «Далее»:

- использовать шаблон — выбор готового набора правил из списка шаблонов, настроенных для разграничения доступа к различным объектам виртуальной инфраструктуры;
- новое правило — создание и ручная настройка нового правила.

Для создания правил по шаблону необходимо выбрать нужные шаблоны и нажать кнопку «Далее». Появится диалог со списком правил, входящих в выбранные шаблоны, необходимо нажать кнопку «Далее», нужно указать пользователей и компьютеры для которых будут действовать правила и нажать кнопку «Завершить». Результат представлен на рисунках с 160 по 164.

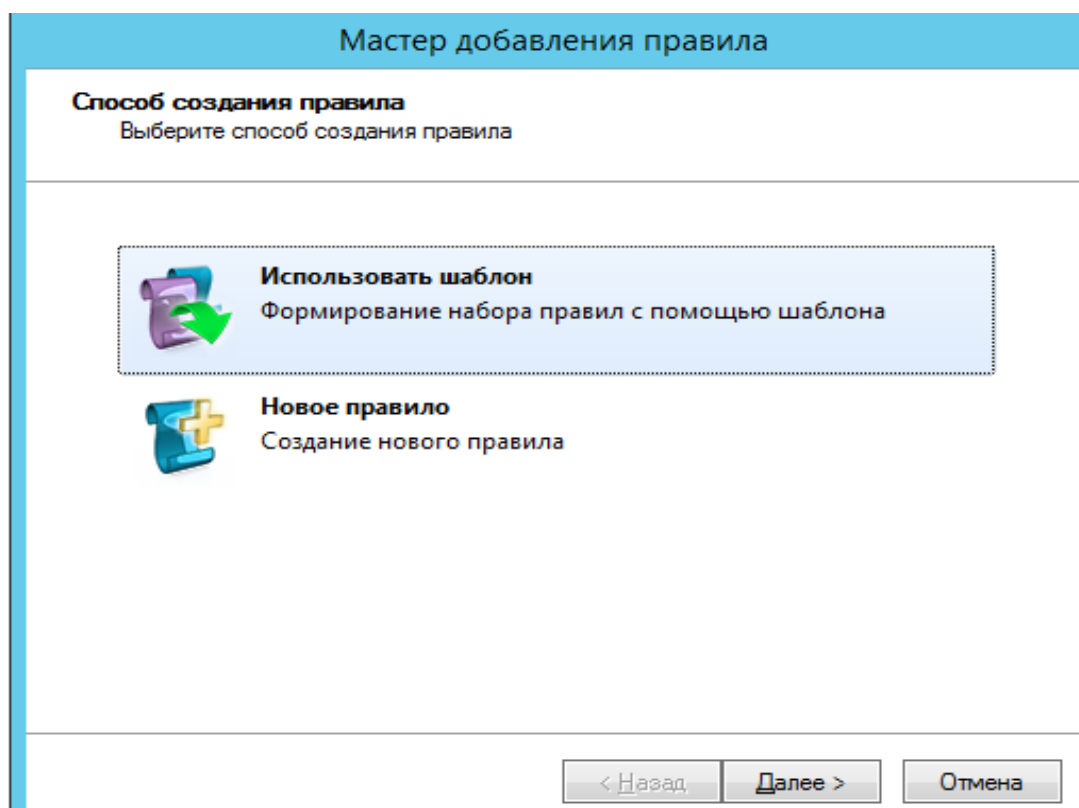


Рисунок 160 — Создание правила на основе шаблона

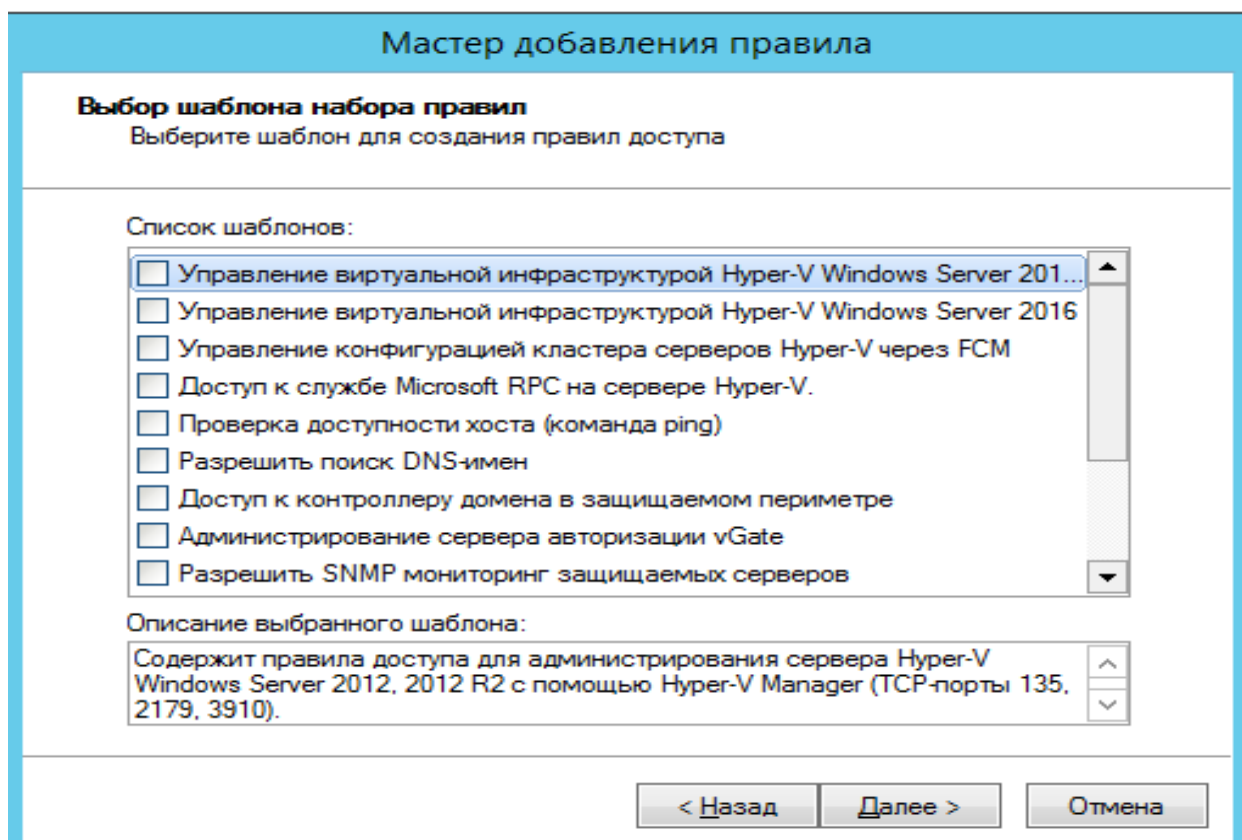


Рисунок 161 — Выбор шаблона набора правил

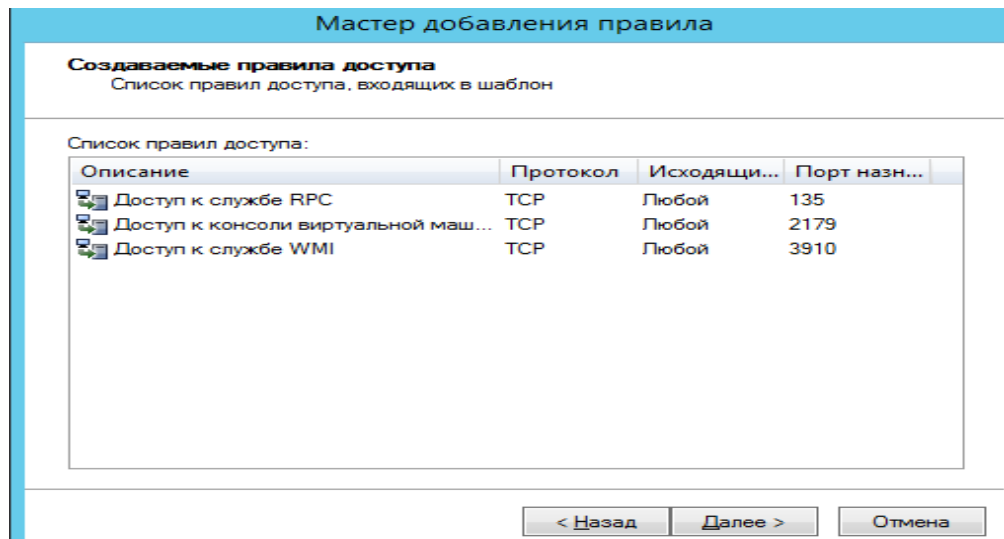


Рисунок 162 — Список правил входящих в шаблон

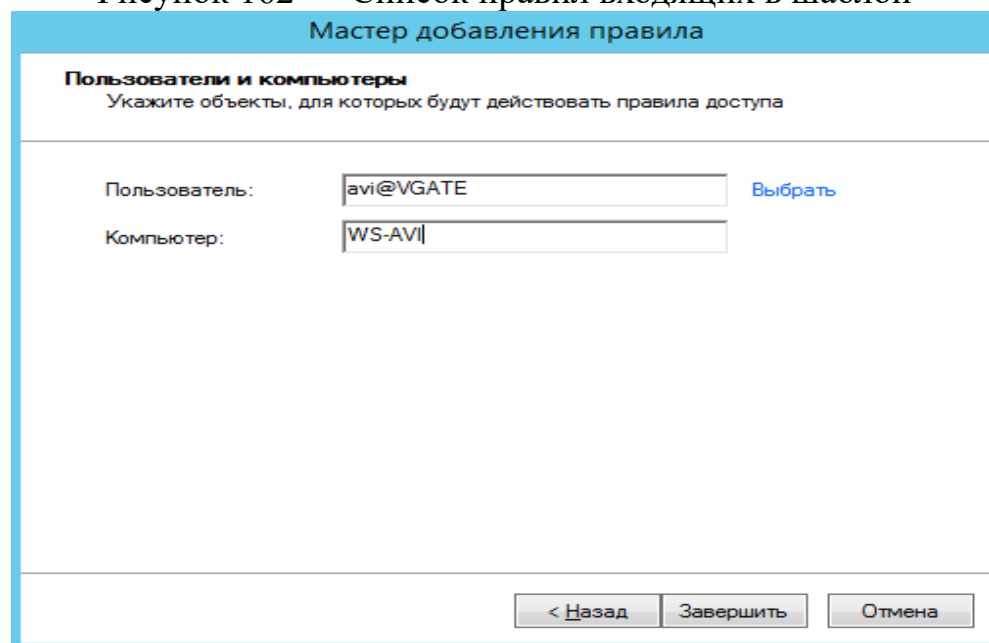


Рисунок 163 — Указание пользователя и компьютера

Правила доступа для 192.168.100.12: Выбрано: 3 (из 3)

Описание	Состоя...	Пользоват...	Компьюте...	Проток...	Исходя...	Порт на...
Доступ к к...	✓ Вкл	avi@VGATE	WS-AVI	TCP	Любой	2179
Доступ к с...	✓ Вкл	avi@VGATE	WS-AVI	TCP	Любой	135
Доступ к с...	✓ Вкл	avi@VGATE	WS-AVI	TCP	Любой	3910

Рисунок 164 — Проверка добавления правил

Для создания нового правила необходимо выбрать пункт «Новое правило», появится диалог создания нового правила. Необходимо указать значения параметров и нажать кнопку «Далее»:

- имя — имя правила;
- описание — описание правила;
- тип протокола — тип протокола соединения: TCP, UDP, ICMP или IP level;
- исходящий порт - исходящий порт. Символ "0" (ноль) означает, что правило действует для всех портов;
- порт назначения – порт назначения. Символ "0" (ноль) означает, что правило действует для всех портов.

Далее необходимо указать пользователей и компьютеры для которых будут действовать правила и нажать кнопку «Завершить». Результат представлен на рисунках с 165 по 167.

Мастер добавления правила

Новое правило
Настройте параметры нового правила

Имя: test

Описание: TCP Любой-Любой

Тип протокола: TCP

Исходящий порт: 0

Порт назначения: 0

< Назад Далее > Отмена

Рисунок 165 — Параметры нового правила

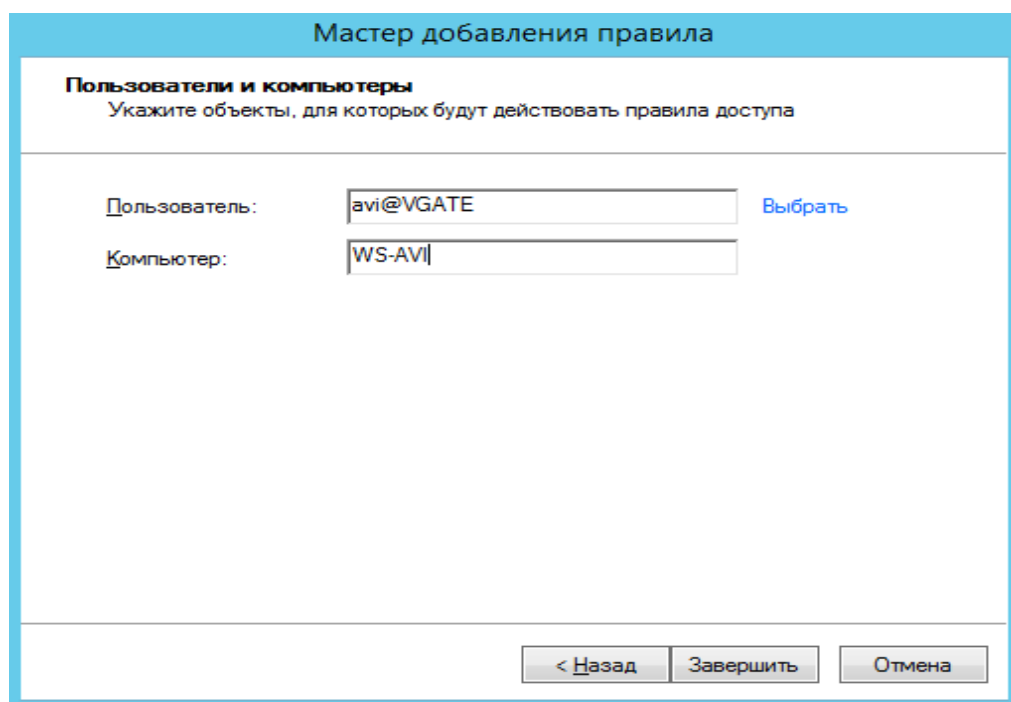


Рисунок 166 — Указание пользователя и компьютера для нового правила

Правила доступа для 192.168.100.12: Выбрано: 1 (из 1)

Описание	Состоя...	Пользов...	Компьюте...	Протоко...	Исходя...	Порт на...
TCP Любо...	✓ Вкл	avi@VGATE	WS-AVI	TCP	Любой	Любой

Рисунок 167 — Проверка создания правила

Для проверки работоспособности необходимо выполнить аутентификацию с помощью учетной записи АВИ на компьютере WS-AVI и с помощью диспетчера Hyper-V получить доступ к консоли виртуальной машины. Результат представить в виде снимков экрана.

7.3 Настройка полномочного управления доступом к конфиденциальным ресурсам. Настройка с помощью консоли. Настройка меток безопасности.

Проверка с имитацией попыток доступа к ресурсам

Настройка полномочного управления доступом осуществляется в следующем порядке:

- выбираются и настраиваются допустимые метки безопасности;

- включается управление доступом по выбранному виду меток безопасности;

- назначаются метки безопасности учетным записям пользователей и ресурсам (объектам виртуальной инфраструктуры) или группам объектов.

При назначении уровней конфиденциальности для объектов виртуальной инфраструктуры необходимо придерживаться следующей последовательности действий.

Необходимо задать уровень конфиденциальности для каждой учетной записи АВИ в соответствии с уровнем допуска пользователя к конфиденциальным ресурсам. В консоли управления выбрать пункт «Учетные записи», выбрать пункт «Назначить метку» и выбрать необходимый уровень конфиденциальности.

Необходимо задать уровень конфиденциальности каждому из защищаемых серверов Hyper-V в соответствии с уровнем конфиденциальности информации, которая будет обрабатываться на нем. Если на сервере Hyper-V планируется обрабатывать информацию разных уровней конфиденциальности, то:

- необходимо отметить поле «разрешено исполнять ВМ с меньшим уровнем»;

- необходимо установить для сервера Hyper-V уровень конфиденциальности, равный максимальному уровню конфиденциальности обрабатываемой на нем информации.

Для этого необходимо в консоли управления выбрать пункт «Защищаемые серверы», выбрать нужный сервер и выбрать пункт «Назначить метку». «Выбрать необходимый уровень конфиденциальности».

Необходимо задать уровень конфиденциальности каждому физическому сетевому адаптеру сервера Hyper-V. Если через один физический сетевой адаптер будет проходить трафик с виртуальных коммутаторов разных уровней

конфиденциальности, то необходимо отметить поле «Разрешено подключать коммутаторы с меньшим уровнем». Для этого необходимо в консоли управления выбрать пункт «Сетевые адаптеры», выбрать нужный адаптер и выбрать пункт «Назначить метку» и указать необходимый уровень конфиденциальности.

Необходимо задать уровень конфиденциальности каждому виртуальному коммутатору сервера Hyper-V. Уровень конфиденциальности виртуального коммутатора должен быть:

- не больше уровня конфиденциальности физического сетевого адаптера, к которому планируется подключать коммутатор;
- равен уровню конфиденциальности физического сетевого адаптера, к которому планируется подключать коммутатор.

Для этого необходимо в консоли управления выбрать пункт «Виртуальные коммутаторы», выбрать нужный коммутатор и выбрать пункт «Назначить метку». Выбрать необходимый уровень конфиденциальности.

Необходимо задать уровень конфиденциальности каждому из хранилищ ВМ в соответствии с уровнем конфиденциальности информации, которая будет в нем храниться. Если в хранилище планируется хранить информацию разных уровней конфиденциальности, то:

- необходимо отметить поле «Разрешено хранить ВМ с меньшим уровнем»;
- необходимо задать уровень конфиденциальности хранилища, равный максимальному уровню конфиденциальности хранимой в нем информации.

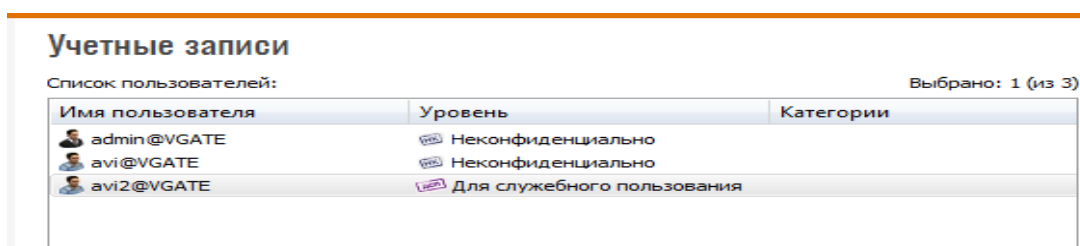
Для этого необходимо в консоли управления выбрать пункт «Хранилища данных», выбрать нужное хранилище и выбрать пункт «Назначить метку». Выбрать необходимый уровень конфиденциальности.

Необходимо задать уровни конфиденциальности для всех существующих ВМ. Уровень конфиденциальности ВМ должен быть:

- не выше уровня конфиденциальности сервера Hyper-V, на котором она выполняется;
- не выше уровня конфиденциальности хранилища, на котором хранятся файлы ВМ или равен уровню конфиденциальности хранилища;
- не выше уровня конфиденциальности виртуального коммутатора, к которому планируется подключать данную ВМ или равен уровню конфиденциальности виртуального коммутатора.

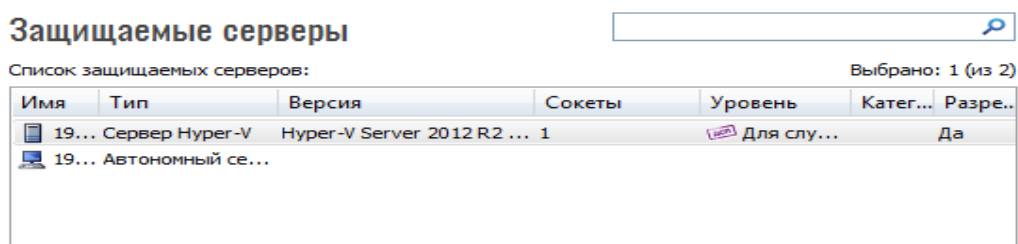
Для этого необходимо в консоли управления выбрать пункт «Виртуальные машины», выбрать нужные ВМ и выбрать пункт «Назначить метку». Выбрать необходимый уровень конфиденциальности.

Результат представлен на рисунках с 168 по 172.



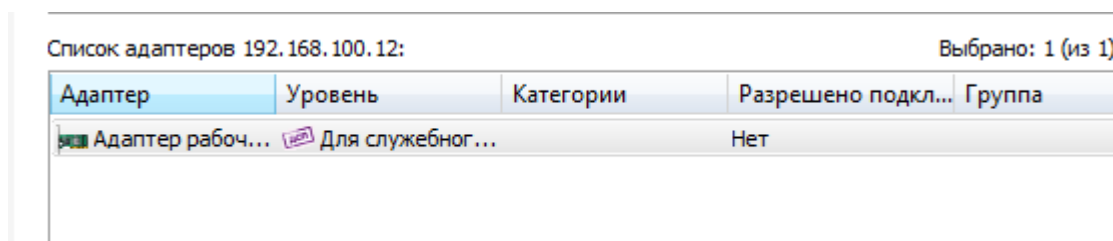
Имя пользователя	Уровень	Категории
admin@VGATE	Неконфиденциально	
avi@VGATE	Неконфиденциально	
avi2@VGATE	Для служебного пользования	

Рисунок 168 — Назначение уровней конфиденциальности пользователям



Имя	Тип	Версия	Сокеты	Уровень	Катег...	Разре..
19... Сервер Hyper-V	Сервер Hyper-V	Hyper-V Server 2012 R2 ...	1	Для слу...		Да
19... Автономный се...	Автономный се...					

Рисунок 169 — Назначение уровня конфиденциальности защищаемому серверу



Адаптер	Уровень	Категории	Разрешено подкл...	Группа
Адаптер рабоч...	Для служебн...		Нет	

Рисунок 170 — Назначение уровня конфиденциальности сетевому адаптеру

Хранилища данных

Список хранилищ:

Выбрано: 1 (из 2)

Путь	Сервер ...	Уровень	Категор...	Тип	Разреше...	Группа
C:\	VGATE-HSV	Для с...		Локально...	Да	
D:\	VGATE-HSV	Некон...		DVD-диск	Да	

Рисунок 171 — Назначение уровня конфиденциальности хранилищам ВМ

Виртуальные машины

Список виртуальных машин:

Выбрано: 1 (из 3)

Имя	Нурег...	Контроль целостн...	Уровень	Категории	Группа
vm1	VGATE-...	Отключен	Для служебн...		
vm2	VGATE-...	Отключен	Для служебн...		
vm33	VGATE-...	Отключен	Неконфиденц...		

Рисунок 172 — Назначение уровня конфиденциальности виртуальным машинам

При назначении категорий конфиденциальности для объектов виртуальной инфраструктуры следует придерживаться следующей последовательности действий.

Необходимо задать категории конфиденциальности для каждой учетной записи АВИ в соответствии с допуском пользователя к определенным категориям ресурсов. Каждый пользователь может быть допущен к одной или нескольким категориям ресурсов. Для этого необходимо в консоли управления выбрать пункт «Учетные записи», выбрать пункт «Назначить метку» и выбрать необходимые категории конфиденциальности.

Необходимо задать одну или несколько категорий конфиденциальности каждому из защищаемых серверов Hyper-V в соответствии с категорией конфиденциальности информации, которая будет обрабатываться на нем. Если на сервере Hyper-V будет обрабатываться информация разных категорий, то необходимо задать список из этих категорий. Для этого необходимо в консоли управления выбрать пункт «Защищаемые серверы», выбрать нужный сервер и

выбрать пункт «Назначить метку». Выбрать необходимые категории конфиденциальности.

Необходимо задать категорию конфиденциальности каждому физическому сетевому адаптеру сервера Hyper-V. При этом список категорий каждого из физических сетевых адаптеров должен иметь хотя бы одну общую категорию со списком категорий сервера Hyper-V. Для этого необходимо в консоли управления выбрать пункт «Сетевые адаптеры», выбрать нужный адаптер и выбрать пункт «Назначить метку и указать необходимую категорию конфиденциальности».

Необходимо задать категорию конфиденциальности каждому виртуальному коммутатору в соответствии с категорией конфиденциальности. При этом список категорий каждого коммутатора должен иметь хотя бы одну общую категорию со списком категорий физического сетевого адаптера. Для этого необходимо в консоли управления выбрать пункт «Виртуальные коммутаторы», выбрать нужный коммутатор и выбрать пункт «Назначить метку». Выбрать необходимую категорию конфиденциальности.

Необходимо задать категории конфиденциальности каждому из хранилищ ВМ, равные категориям конфиденциальности хранящейся на них информации. Для этого необходимо в консоли управления выбрать пункт «Хранилища данных», выбрать нужное хранилище и выбрать пункт «Назначить метку». Выбрать необходимые категории конфиденциальности.

Необходимо задать категории конфиденциальности для всех существующих ВМ. Список категорий ВМ должен иметь хотя бы одну общую категорию:

- со списком категорий сервера Hyper-V, на котором она выполняется;
- со списком категорий хранилища, на котором хранятся файлы ВМ.

Для этого необходимо в консоли управления выбрать пункт «Виртуальные машины», выбрать нужные ВМ и выбрать пункт «Назначить метку». Выбрать необходимые категории конфиденциальности.

Результат настройки категорий конфиденциальности представлен на рисунках с 173 по 177.

Учетные записи

Список пользователей: Выбрано: 1 (из 3)

Имя пользователя	Уровень	Категории
 admin@VGATE	 Неконфиденциально	
 avi@VGATE	 Неконфиденциально	 Зеленый
 avi2@VGATE	 Неконфиденциально	 Красный

Рисунок 173 — Назначение категорий конфиденциальности пользователям

Список защищаемых серверов: Выбрано: 1 (из 2)

Имя	Тип	Версия	Сокеты	Уровень	Катег...	Разре..
 19... Сервер Hyper-V	Сервер Hyper-V	Hyper-V Server 2012 R2 ...	1	 Неконфи...	 	К Да
 19... Автономный се...	Автономный се...					

Рисунок 174 — Назначение категорий конфиденциальности защищаемому серверу

Список адаптеров 192.168.100.12: Выбрано: 1 (из 1)

Адаптер	Уровень	Категории	Разрешено подкл...	Группа
 Адаптер рабоч...	 Неконфиденци...	  Красный; З...	Нет	

Рисунок 175 — Назначение категорий конфиденциальности сетевому адаптеру

Список хранилищ: Выбр

Путь	Сервер ...	Уровень	Категор...	Тип	Разреше...	Группа
 C:\	VGATE-HSV	 Некон...	 Зел...	Локально...	Да	
 D:\	VGATE-HSV	 Некон...	 Кра...	DVD-диск	Да	

Рисунок 176 — Назначение категорий конфиденциальности хранилищам ВМ

Список виртуальных машин: Выбрано: 1 (из 3)

Имя	Hyper...	Контроль целостн...	Уровень	Категории	Группа
vm1	VGATE-...	Отключен	Неконфиденц...		Кра...
vm2	VGATE-...	Отключен	Неконфиденц...		Кра...
vm33	VGATE-...	Отключен	Неконфиденц...		Красный

Рисунок 177 — Назначение категорий конфиденциальности виртуальным машинам

Для проверки работоспособности необходимо выполнить настройку полномочного управления доступом и осуществить попытки доступа к ресурсам с различных учетных записей АВИ. Результат представить в виде снимков экрана.

7.4 Контроль целостности и доверенная загрузка

В vGate средства контроля целостности (КЦ) используются для защиты следующих объектов на сервере авторизации, серверах Hyper-V и рабочих местах АВИ и АИБ.

Контроль целостности (КЦ) осуществляется только для тех ВМ, которым назначена политика "Доверенная загрузка виртуальных машин Hyper-V". Настройка объектов контроля vGate позволяет выполнить детальную настройку контроля целостности ВМ:

- разрешить или запретить запуск ВМ при нарушении целостности конфигурации;
- включить или отключить контроль поддерева контрольных точек ВМ;
- выбрать параметры конфигурации ВМ, изменение значений которых будет контролироваться политикой "Доверенная загрузка виртуальных машин Hyper-V".

Настройка выполняется в диалоге редактирования параметров политики "Доверенная загрузка виртуальных машин Hyper-V".

Для настройки параметров политики необходимо в Консоли управления выбрать пункт «Политики безопасности», нажать кнопку «Добавить», выбрать пункт «Создание нового набора политик» и нажать кнопку «Далее», выбрать шаблон набора политик и нажать кнопку «Далее», в предложенном списке политик выбрать политику «Доверенная загрузка виртуальных машин Hyper-V» и нажать кнопку «Изменить». В появившемся диалоге настройки параметров политики необходимо отредактировать нужные параметры и нажать кнопку «ОК». После этого необходимо нажать кнопку «Завершить». Далее необходимо применить созданный набор политик на нужную ВМ, для этого необходимо в Консоли управления выбрать пункт «Виртуальные машины» и нажать кнопку «Назначить политики», выбрать набор политики и нажать кнопку «Назначить». Результат представлен на рисунках 178 и 179.

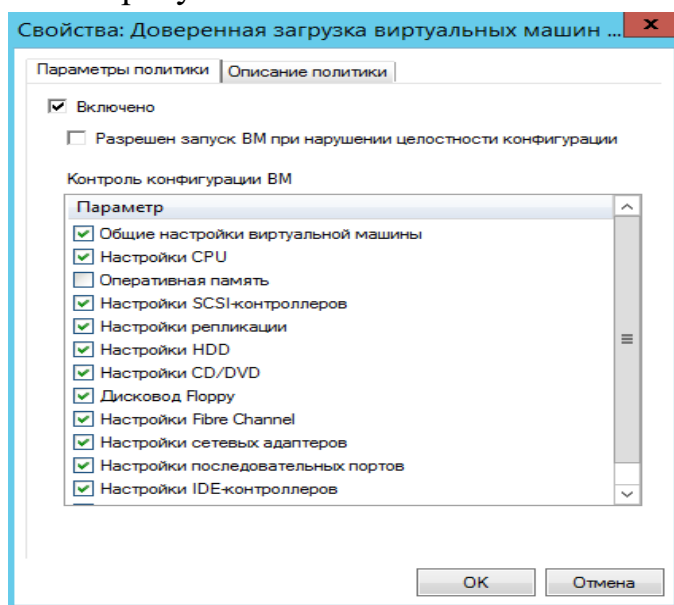


Рисунок 178 — Настройка политики доверенной загрузки ВМ

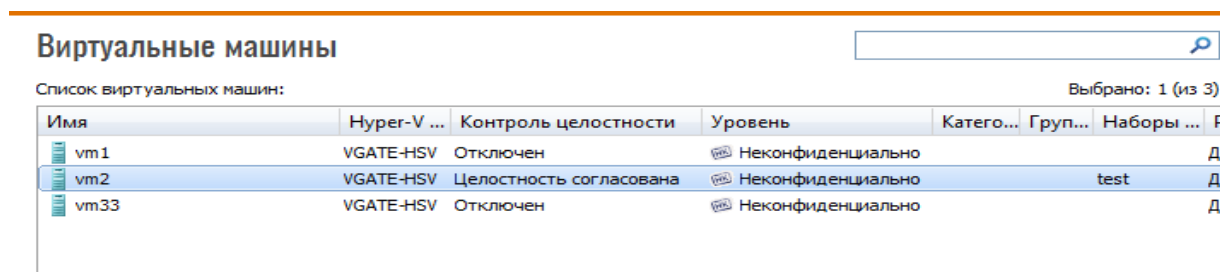


Рисунок 179 — Применение политики доверенной загрузки ВМ

Целостность ВМ контролируется компонентами защиты, установленными на сервер Hyper-V. Для каждой новой ВМ рассчитывается эталонная контрольная сумма (КС), которая используется для контроля целостности. При создании новой ВМ на сервере Hyper-V и при клонировании ВМ расчет контрольной суммы нужно запустить, согласовав изменения виртуальной машины в консоли управления. При миграции ВМ с другого сервера необходимо пересчитать КС, иначе будет зафиксировано нарушение целостности. Для того чтобы рассчитать контрольную сумму для ВМ необходимо в Консоли управление выбрать пункт «Виртуальные машины», выбрать нужную ВМ и нажать кнопку «Согласовать».

На сервере Hyper-V каждые 10 минут выполняется сравнение эталонной контрольной суммы ВМ с текущей. При несовпадении контрольных сумм ВМ фиксируется нарушение целостности, изменяется статус ВМ (значение в колонке "Контроль целостности") и может быть запрещен запуск данной ВМ.

Администратор может в зависимости от статуса ВМ принять изменения (согласовать) либо отклонить их. При согласовании изменений эталонная контрольная сумма ВМ заменяется текущей (т.е. контрольная сумма пересчитывается). Кроме того, при согласовании изменений в базе сохраняется текущий конфигурационный файл ВМ. При отклонении изменений текущий конфигурационный файл заменяется эталонным (сохраненным в базе при последнем согласовании).

Для согласования и отклонения изменений необходимо в Консоли управления выбрать функцию «Виртуальные машины», выбрать нужную ВМ и нажать кнопку «Согласовать». На экране появится диалог с изменениями, обнаруженными при проверке виртуальной машины. Для того чтобы принять изменения необходимо нажать кнопку «Принять», Для того чтобы отклонить изменения, нажать кнопку «Отклонить». После этого система выполнит пересчет контрольных сумм всех файлов ВМ и после окончания выдаст сообщение об этом. Далее необходимо нажать кнопку «ОК».

Для проверки работоспособности необходимо выполнить настройку контроля целостности ВМ и используя учетную запись АВИ изменить конфигурацию ВМ. Результат представить в виде снимков экрана.

7.5 Регистрация событий информационной безопасности

События безопасности регистрируются на всех защищаемых серверах, на которых установлены компоненты защиты vGate, а затем пересылаются на сервер авторизации для централизованного хранения.

Необходимо в консоли управления выбрать пункт «Аудит». Появится таблица со списком событий, а над ней группа параметров для формирования условий отбора записей.

Необходимо указать условия отбора записей. Для выбора параметров отбора записей установить отметки рядом с названиями нужных характеристик в раскрывающихся списках - Типы событий, Компоненты и Категории. При необходимости выбрать период времени регистрации событий в поле Время событий. Для ограничения длины списка указать нужное значение в поле Событий, не более. Для возврата к набору параметров фильтрации записей, предлагаемому по умолчанию нажать кнопку «Сбросить». Далее нажать кнопку «Применить». Для детального просмотра отдельных записей необходимо выделить нужную запись и нажать кнопку «Свойства». Результат представлен на рисунках 180 и 181.

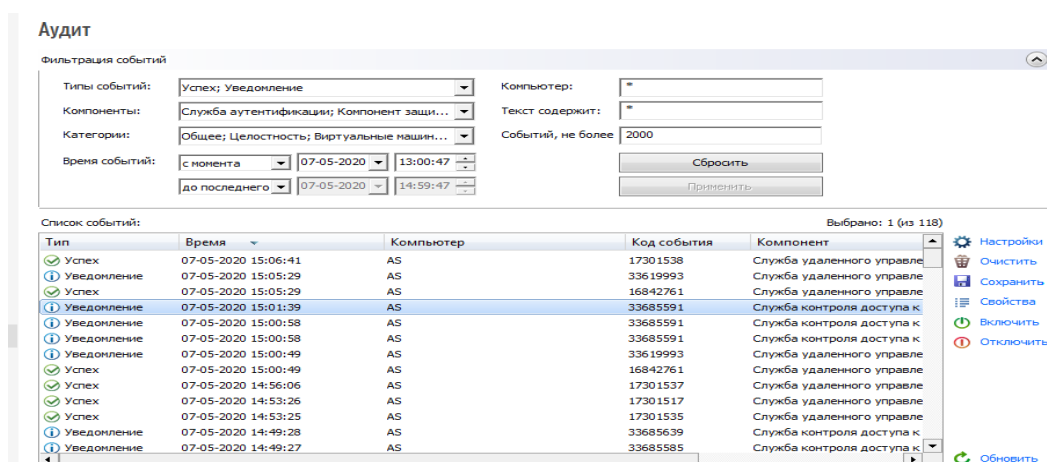


Рисунок 180 — Настройка аудита

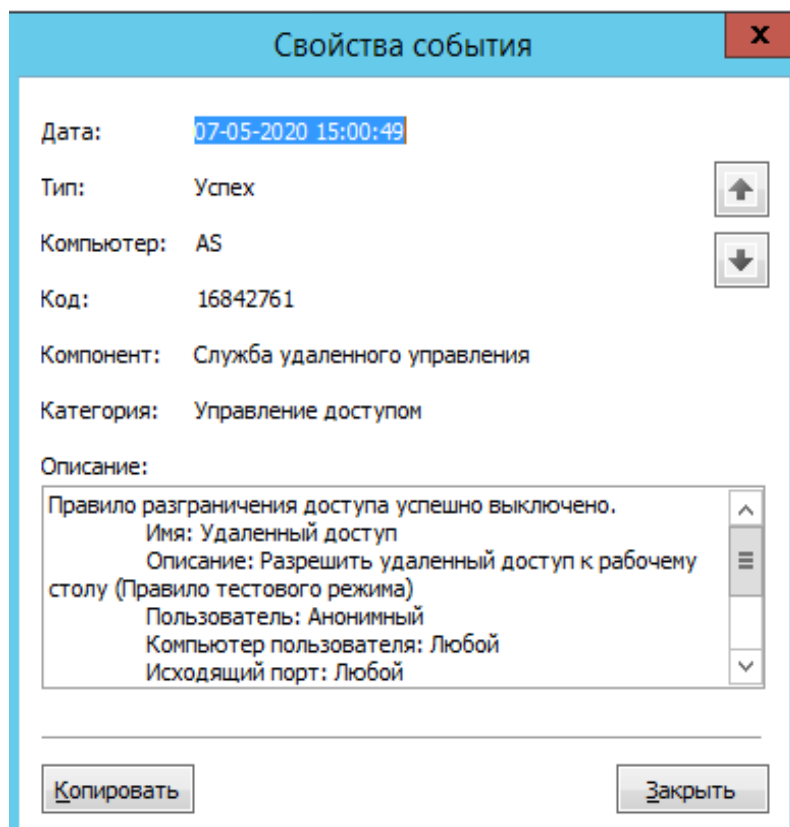


Рисунок 181 — Детальный просмотр записи аудита

Для сохранения журнала событий безопасности необходимо в консоли управления выбрать «Аудит». Нажать кнопку «Сохранить». Задать имя файла и нажать кнопку «Сохранить». Результат представлен на рисунке 182.

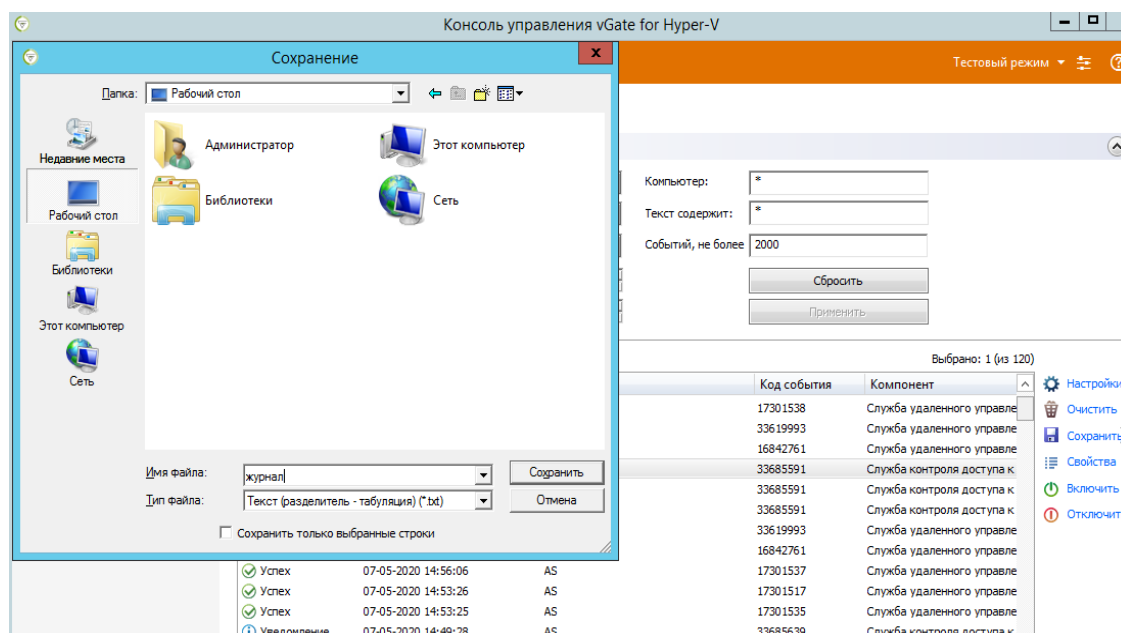


Рисунок 182 — Сохранение журнала безопасности

Необходимо получить всю информацию, относящуюся к аутентификации пользователей, попыткам доступа к защищаемому серверу, настройке полномочного управления доступом и контроле целостности ВМ. Результаты представить в виде снимков экрана. В отчет необходимо включить сохраненный журнал безопасности.

7.6 Базовый и повышенные уровни сложности задания «Управление доступом к ресурсам виртуальной инфраструктуры и контроль целостности, реализуемые СЗИ vGate»

Базовому уровню сложности задания «Управление доступом к ресурсам виртуальной инфраструктуры и контроль целостности, реализуемые СЗИ vGate» соответствуют задачи, описанные в пунктах 7.1-7.2 и 7.4-7.5. Повышенному уровню сложности соответствует задача, описанная в пункте 7.3.

8 Описание порядка выполнения заданий практикума и результатов выполнения заданий

8.1 Описание порядка выполнения практического задания по управлению виртуальной инфраструктурой и безопасностью виртуальной инфраструктуры при использовании СЗИ vGate

Описание порядка выполнения практического задания по управлению виртуальной инфраструктурой и безопасностью виртуальной инфраструктуры при использовании СЗИ vGate было составлено исходя из порядка выполнения практического задания «Управление виртуальной инфраструктурой и безопасностью виртуальной инфраструктуры при использовании СЗИ vGate», описанного в главе 6.

Выполнение задания по управлению виртуальной инфраструктурой и безопасностью виртуальной инфраструктуры при использовании СЗИ vGate осуществляется поэтапно:

- изучение теоретического материала;
- запуск ВМ с контроллером домена, используя учетную запись администратора контроллера домена;
- запуск ВМ с сервером авторизации, используя учетную запись локального администратора;
- запуск ВМ с сервером виртуализации Hyper-V, используя учетную запись локального администратора;
- запуск ВМ с рабочим местом АВИ, используя учетную запись локального администратора;
- запуск консоли управления vGate;
- создание учетных записей администраторов АВИ и АИБ;
- авторизация с помощью созданных учетных записей;
- создание набора политики безопасности;

- применение набора политики безопасности;
- настройка мониторинга;
- настройка аудита СЗИ vGate;
- просмотр сохраненных журналов безопасности;
- создание необходимых снимков экрана;
- подготовка, формирование и защита отчета о выполненном практическом задании.

Практическое задание «Управление виртуальной инфраструктурой и безопасностью виртуальной инфраструктуры при использовании СЗИ vGate» предусматривает базовый и повышенный уровни сложности. Базовый уровень включает в себя выполнение заданий, описанных в пунктах с 6.2 по 6.7 главы 6. Задания повышенного уровня описаны в пункте 6.8 главы 6.

В результате выполнения практического задания «Управление виртуальной инфраструктурой и безопасностью виртуальной инфраструктуры при использовании СЗИ vGate» будет осуществлено знакомство с порядком работы администратора виртуальной инфраструктуры и администратора информационной безопасности, получены практические и теоретические навыки по настройке и администрированию, такие как создание учетных записей администраторов АВИ и АИБ, создание и применение набора политик безопасности, настройка аудита СЗИ vGate, просмотр сохраненных журналов безопасности и настройка мониторинга.

UML – диаграмма последовательности действий выполнения практического задания по управлению виртуальной инфраструктурой и безопасностью виртуальной инфраструктуры при использовании СЗИ vGate представлена в приложении Б на рисунке Б.1.

8.2 Описание порядка выполнения практического задания по управлению доступом к ресурсам виртуальной инфраструктуры и контролю целостности, реализуемые СЗИ vGate

Описание порядка выполнения практического задания по управлению доступом к ресурсам виртуальной инфраструктуры и контролю целостности, реализуемые СЗИ vGate было составлено исходя из порядка выполнения практического задания «Управление доступом к ресурсам виртуальной инфраструктуры и контроль целостности, реализуемые СЗИ vGate», описанного в главе 7.

Выполнение задания по управлению доступом к ресурсам виртуальной инфраструктуры и контролю целостности, реализуемые СЗИ vGate осуществляется поэтапно:

- запуск ВМ с контроллером домена, используя учетную запись администратора контроллера домена;
- запуск ВМ с сервером авторизации, используя учетную запись локального администратора;
- запуск ВМ с сервером виртуализации Hyper-V, используя учетную запись локального администратора;
- запуск ВМ с рабочим местом АВИ, используя учетную запись локального администратора;
- запуск консоли управления vGate;
- аутентификация, используя учетную запись АВИ;
- создание правила доступа на основе шаблона;
- создание новое правило доступа;
- проверка доступа;
- настройка политики доверенной загрузки ВМ;
- расчет контрольную сумму для ВМ;

- настройка уровней конфиденциальности для объектов виртуальной инфраструктуры;
- настройка категорий конфиденциальности для объектов виртуальной инфраструктуры;
- настройка аудита СЗИ vGate;
- просмотр сохраненных журналов безопасности;
- создание необходимых снимков экрана;
- подготовка, формирование и защита отчета о выполненном практическом задании.

Практическое задание «Управление доступом к ресурсам виртуальной инфраструктуры и контроль целостности, реализуемые СЗИ vGate» предусматривает базовый и повышенный уровни сложности. Базовый уровень включает в себя выполнение заданий, описанных в пунктах 7.1 и 7.2 и пунктах 7.4 и 7.5 главы 7. Задания повышенного уровня описаны в пункте 7.3 главы 7.

В результате выполнения практического задания «Управление доступом к ресурсам виртуальной инфраструктуры и контроль целостности, реализуемые СЗИ vGate» будут получены практические и теоретические навыки по настройке и администрированию, такие как создание правил доступа, настройка политики доверенной загрузки ВМ, настройка категорий и уровней конфиденциальности для объектов виртуальной инфраструктуры, настройка аудита СЗИ vGate, просмотр сохраненных журналов безопасности и настройка мониторинга.

UML – диаграмма последовательности действий выполнения практического задания управлению доступом к ресурсам виртуальной инфраструктуры и контролю целостности представлена в приложении Б на рисунке Б.2.

9 Описание структуры и содержания отчета о выполнении практических заданий

9.1 Структура и содержание отчета о выполнении практических заданий

Результатом выполнения заданий практикума является отчет о выполнении практического задания. Он должен включать в себя:

- титульный лист отчета о выполнении практического задания с указанием его названия;
- цель практического задания;
- содержание практического задания;
- описание результатов выполнения практического задания базовой сложности;
- описание результатов выполнения практического задания повышенной сложности;
- снимки экрана;
- вывод по результатам выполнения практического задания;
- содержание журнала безопасности, полученного в результате выполнения практического задания.

Содержание разделов отчета определяется в соответствии с описанием выполнения заданий практикума и в соответствии с содержанием отчета о выполнении практикума.

9.2 Содержание отчета о выполнении практической работы «Управление виртуальной инфраструктурой и безопасностью виртуальной инфраструктуры при использовании СЗИ vGate»

Базовый уровень сложности при выполнении заданий практической работы «Управление виртуальной инфраструктурой и безопасностью

виртуальной инфраструктуры при использовании СЗИ vGate» предполагает выполнение пунктов с 9.2.1 по 9.2.6.

9.2.1 Создание учетных записей администраторов ИБ и ВИ.

В виде снимков экрана отразить результаты создания учетных записей.

В виде снимков экрана отразить результаты авторизации с помощью созданных учетных записей.

9.2.2 Управление учетными записями пользователей.

В виде снимков экрана отразить результаты создания учетной записи не удовлетворяющей требованиям политики паролей представить в виде снимков экрана.

9.2.3 Настройка прав на управление виртуальной инфраструктурой и управление информационной безопасностью с проверкой возможности применения этих прав.

В виде снимков экрана отразить результаты авторизации учетной записи АВИ в Агенте аутентификации и проверки доступных ему функций.

В виде снимков экрана отразить результаты авторизации учетной записи АИБ в Консоли управления и проверки доступных ему функций.

9.2.4 Управление политиками безопасности.

В виде снимков экрана отразить результаты создания и проверки работы политики безопасности.

9.2.5 Регистрация событий информационной безопасности.

Отразить в отчете в виде снимков экрана все действия, относящиеся к применению и отмене политик безопасности, а также информацию об виртуальных машинах Hyper-V.

Сохранить и привести в приложении к отчету о выполнении практической работы журнал безопасности.

9.2.6 Управление режимами работы vGate.

В виде снимков экрана отразить результаты переключения режимов работы vGate и проверки работы настроенных правил.

9.2.7 Мониторинг безопасности.

В виде снимков экрана отразить результаты настройки панели мониторинга.

В виде снимков экрана отразить результаты создания правил корреляции.

В виде снимков экрана отразить результаты проверки инцидентов.

Построить, сохранить и привести в приложении к отчету о выполнении практической работы отчет о событиях безопасности.

Вывод по результатам выполнения задания должен содержать краткие сведения о выполненной работе, полученных знаниях и практических навыках.

9.3 Содержание отчета о выполнении практической работы «Управление доступом к ресурсам виртуальной инфраструктуры и контроль целостности, реализуемые СЗИ vGate»

Базовый уровень сложности при выполнении заданий практической работы «Управление доступом к ресурсам виртуальной инфраструктуры и контроль целостности, реализуемые СЗИ vGate» предполагает выполнение пунктов с 9.3.1 по 9.3.2 и с 9.3.4 по 9.3.5

9.3.1 Аутентификация.

В виде снимков экрана отразить результаты аутентификации с помощью учетной записи АВИ.

9.3.2 Управление доступом к защищаемым серверам.

В виде снимков отразить экрана отразить результаты аутентификации с помощью учетной записи АВИ на компьютере WS-AVI.

В виде снимков экрана отразить результаты доступа к консоли виртуальной машины.

9.3.3 Настройка полномочного управления доступом к конфиденциальным ресурсам. Настройка с помощью консоли. Настройка меток безопасности. Проверка с имитацией попыток доступа к ресурсам.

В виде снимков экрана отразить результаты настройки полномочного управления доступом.

В виде снимков экрана отразить результаты доступа к ресурсам с различных учетных записей АВИ.

9.3.4 Контроль целостности и доверенная загрузка.

В виде снимков экрана отразить результаты настройки контроля целостности ВМ.

В виде снимков экрана отразить результаты попытки АВИ изменить конфигурацию ВМ.

9.3.5 Регистрация событий информационной безопасности.

Отразить в отчете в виде снимков экрана все действия, относящиеся к аутентификации пользователей, попыткам доступа к защищаемому серверу, настройке полномочного управления доступом и контроле целостности ВМ.

Сохранить и привести в приложении к отчету о выполнении практической работы журнал безопасности.

Вывод по результатам выполнения задания должен содержать краткие сведения о выполненной работе, полученных знаниях и практических навыках.

Графическое представление структуры отчета о выполнении практического задания представлено в приложении В на рисунке В.1.

10 Определение порядка контроля выполнения практического задания

Порядок контроля выполнения практического задания выполняется одинаково для двух заданий и предусматривает следующие этапы контроля:

- проверка даты выполнения и сроков формирования отчетов;
- проверка правильности оформления требованиям;
- проверка правильности порядка выполнения заданий базового уровня согласно описанию выполнения заданий;
- проверка наличия и правильности выполнения заданий повышенного уровня сложности;
- проверка наличия всех необходимых снимков экрана;
- проверка составленных отчетов;
- проверка сделанных выводов о результатах выполнения практического задания.

Графическое представление порядка контроля о выполнении практического задания представлено в приложении Г на рисунке Г.1.

11 Подготовка сценариев для автоматизированного развертывания виртуальных машин

В VirtualBox для управления виртуальными машинами из консоли можно использовать утилиту VBoxManage.

VBoxManage это утилита командной строки, позволяющая контролировать все возможности VirtualBox. Утилита VboxManage позволяет изменять свойства созданных виртуальных машин. Большинство возможностей, которые утилита позволяет использовать, соответствуют возможностям, которые доступны в пользовательском графическом интерфейсе Oracle VM VirtualBox которые отображены в диалоговом окне настроек при создании ВМ, однако большинство сложных настроек доступны только с использованием утилиты VBoxManage. К таким настройкам относится разработка сценариев автоматизированного развертывания ВМ.

Сценарий – система взаимодействия, которая обрабатывает и перенаправляет инструкции (команды), выполняемые над объектом от контролирующего к контролируемому.

В качестве управления используется набор команд. Примеры команд:

- `#VBoxManage list vms` - просмотр перечня гостевых операционных систем;
- `#VBoxManage showvminfo "windows2012"` - просмотр подробной информации о конкретной виртуальной ОС;
- `#VBoxManage startvm "WS-AVI"` - запуск гостевой ОС;
- `#VBoxManage startvm "WS-AVI" --type=headless` — запуск гостевой ОС в фоне;
- `#VBoxManage controlvm "WS-AVI" savestate` — выключение гостевой ОС.

Для автоматизации развертывания ВМ входящих в состав стенда разработаны сценарии, определяющие конфигурацию ВМ после их создания, и режимы их работы в момент их использования.

Сценарии определяют аппаратную конфигурацию виртуальной машины, которая была определена при создании ВМ. Аппаратная конфигурация включает в себя следующие параметры:

- оперативная память;
- видеопамять;
- количество процессоров выделяемое ТС для ВМ;
- наличие универсального интерфейса ACPI;
- включение привода оптического диска;
- необходимые сетевые адаптеры подключаемые при запуске ВМ;
- наличие папки обмена основной ОС с гостевой.

В сценариях был задан режим работы ВМ, автоматически возвращающих их в исходное состояние при закрытии, который называется «immutable».

Было подготовлено четыре сценария для автоматизированного развертывания виртуальных машин. Разработанные сценарии представлены в приложении Д.

12 Вредные психофизиологические факторы, влияющие на сердечно-сосудистую систему специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие

12.1 Вредные психофизиологические факторы, влияющие на сердечно-сосудистую систему специалиста по защите информации

По официальной статистике, ежегодно в России от сердечно-сосудистых заболеваний умирает около 1 млн. 300 тысяч человек, смертность по этой причине превышает половину числа всех смертей в стране. Россия лидирует по этому показателю среди развитых стран.

Одной из причин сердечно-сосудистых заболеваний является сидячий образ жизни, а работа специалиста по защите информации подразумевает долгое сидение за рабочим местом. Почему сидячий образ жизни так вреден? В основном потому, что положение сидя (или лежа) уменьшает нагрузку на сердечно-сосудистую систему, а также позволяет сердцу и кровеносным сосудам «расслабиться». В отличие от него, положение стоя вынуждает сердечно-сосудистую систему работать активнее, просто для поддержания нормального уровня артериального давления. Снижение исходного уровня сердечно-сосудистой деятельности, связанного с длительным сидением, может привести к относительной сердечной дезадаптации. Резкая перемена сидячего положения на стоячее может вызвать повышение артериального давления, что в некоторых случаях приводит к потере сознания.

Зачастую, люди, чья работа связана с сидячим образом жизни, страдают от плохой циркуляции крови в нижних конечностях, что приводит к развитию варикозного заболевания вен. При долгом сидении без смены положения сосуды пережимаются, кровь в них застаивается и не может двигаться как положено — вверх. Из-за этого стенки сосудов испытывают давление и когда оно становится избыточно высоким, кровь выталкивается и ее излишки растягивают вены. Но не столь опасно варикозное расширение вен, как являющийся её следствием

тромбофлебит, который ведет к образованию тромбов. Тромбы могут закупоривать вены образуя флелботромбоз либо оторвавшись от стенки сосуда по кровотоку попасть в легкие. Это в большинстве случаев приводит к тяжёлым осложнениям, а иногда и к летальному исходу.

Помимо варикозного расширения вен сидячий образ жизни специалиста по защите информации опасен тем, что продолжительное отсутствие физической активности приводит к гипотоническим (пониженное артериальное давление) и гипертоническим (повышенное артериальное давление) заболеваниям.

12.2 Методы и средства физической культуры, снижающие их воздействие

Для снижения рисков от сидячего образа жизни необходимо заниматься физическими упражнениями, которые являются научно обоснованным методом профилактики заболеваний сердечно-сосудистой системы. Регулярные занятия физическими упражнениями уменьшают вероятность возникновения заболеваний органов кровообращения.

Для предотвращения и профилактики заболеваний сердечно-сосудистой системы физические упражнения рекомендуются всем, но особенно тем, у кого есть факторы риска, такие как сидячий образ жизни. В основном рекомендуются такие виды занятий, как гимнастические упражнения, бег, ходьба, плавание, ходьба на лыжах, туризм.

Гимнастические упражнения развивают мышечную силу, укрепляют связки, делают суставы более подвижными, совершенствуют координацию движений. Например, при гипотонической болезни силовые, скоростно-силовые и статические упражнения повышают артериальное давление, а при гипертонической болезни дыхательные упражнения и упражнения для мелких мышечных групп способствуют его снижению. Дыхательные упражнения и

упражнения в расслаблении мышц также оказывают общее оздоровительное действие для всего организма.

Ходьба — основное средство в оздоровительной и лечебной физической культуре. Она является естественной для организма человека формой мышечной деятельности. Во время ходьбы в работу включается большинство мышц туловища, ног и рук. Поэтому людям, ведущим сидячий образ жизни рекомендуется больше передвигаться пешком, так как это самый доступный способ оздоровления организма, также не требующий практически никаких затрат.

В лечебных целях рекомендуется ходьба в медленном (от 60 до 70 шагов в минуту, скорость продвижения не более 3 км/ч), в среднем (от 80 до 100 шагов в минуту, скорость 4 км/ч) и в быстром (от 100 до 110 шагов в минуту, скорость 5 км/ч). Нежелательно ходить в более быстром темпе. В начале ходьбы следует делать более короткие шаги и держать медленный темп, затем шаг надо удлинять, а темп увеличивать. В время ходьбы необходимо следить за дыханием, а именно согласовывать его с шагами — выдох немного длиннее, чем вдох.

Следующее оздоровительное средство — бег. Бег помогает предупредить заболевания сердечно-сосудистой системы и нормализовать функции при начальных проявлениях болезни, повысить резервы организма. Однако это очень сильное средство, которое предъявляет значительные требования к опорно-двигательному аппарату, сердечно-сосудистой и дыхательной системам, поэтому при серьезных заболеваниях этих систем занятия бегом стоит отложить.

При многих заболеваниях сердечно-сосудистой системы можно подобрать такие скорость и длительность бега, которые не будут перегружать, но в то же время будут тренировать эту систему. Регулярные занятия бегом улучшают деятельность и других систем организма. Его лечебное действие заключается в том, что совершенствуются регулирующие системы (центральная и

вегетативная нервная система, эндокринная система). Помимо этого беговые тренировки повышают тонус парасимпатической системы (в покое снижается артериальное давление). В условиях жизни специалиста по защите информации волнения и стресс являются неотъемлемой частью его профессиональной деятельности и повышают тонус симпатической нервной системы, а беговые тренировки уравнивают взаимодействие этих систем.

Начинать занятия с лечебной целью следует с очень медленного бега — почти со скоростью ходьбы. Только через несколько месяцев занятий можно увеличивать темп, иначе можно вместо оздоровления причинить организму непоправимый вред. После бега рекомендуется выполнять ходьбу, упражнения на расслабление и растягивание мышц туловища и конечностей, а также дыхательные упражнения.

Ходьба на лыжах оказывает разнообразное воздействие на организм и включает в работу все мышечные группы, способствуя их укреплению, ускорению обмена веществ, улучшению функций дыхательной, сердечно-сосудистой и нервной систем, повышению физической работоспособности и закаливанию организма.

При занятиях ходьбой на лыжах стоит варьировать объем занятий в зависимости от температуры воздуха и силы ветра. При морозе и ветре продолжительность пребывания на воздухе необходимо сокращать. Наиболее благоприятными условиями занятий на лыжах является температура воздуха от минус 1 до минус 12° и сила ветра более 10 м/с.

При любом из вышеперечисленных занятий величину нагрузок необходимо дозировать по субъективным ощущениям занимающегося. Нагрузка не должна вызывать сильное утомление, а также необходимо следить за частотой сердечных сокращений (ЧСС), по которой можно судить о доступности физических нагрузок. Допустимый максимум ЧСС в зависимости от возраста определяется расчетом: для здоровых людей возраст вычитается из

220, для людей с факторами риска — из 200, а для людей, уже перенесших заболевания сердечно-сосудистой системы, — из 190.

Людям с активной фазой сердечно-сосудистых заболеваний не рекомендуются все вышеперечисленные занятия до момента выздоровления, а после выздоровления необходимо дозировать нагрузки, чтобы не нанести вред ослабленному болезнью организму.

Результатом выполнения физических упражнений является повышение эффективности работы сердечно-сосудистой системы, повышение липопротеидов высокой плотности, или «хорошего» холестерина, и уменьшение триглицеридов в крови человека.

Можно сделать вывод, что имеет смысл уменьшить время, проводимое сидя, и перераспределить его на время, проводимое на ногах. Практически все люди могут извлечь пользу из регулярных занятий спортом, независимо от того, занимаются ли они спортом интенсивно или придерживаются умеренной оздоровительной нагрузки. Систематизированная физическая деятельность благотворно влияет на весь организм человека и, следовательно, помогает предотвратить большое количество проблем со здоровьем, в том числе снижает риск смертности от сердечно-сосудистых заболеваний.

Заключение

В результате выполнения ВКР был разработан практикум по администрированию системы защиты среды виртуализации от несанкционированного доступа на основе средства защиты информации vGate.

Первое задание практикума посвящено управлению виртуальной инфраструктурой и безопасностью виртуальной инфраструктуры при использовании СЗИ vGate.

Второе задание практикума посвящено управлению доступом к ресурсам виртуальной инфраструктуры и контролю целостности, реализуемые СЗИ vGate

В ходе дипломного проектирования был произведен обзор функций, реализуемых СЗИ vGate, были созданы виртуальные машины, которые использованы для построения лабораторного стенда. Был определен общий порядок выполнения заданий практикума, разработано описание выполнения каждого задания практикума, разработаны контрольные экземпляры отчетов о выполнении заданий практикума, определен порядок контроля выполнения заданий практикума.

В результате выполнения заданий практикума студенты получают навыки по администрированию системы защиты среды виртуализации от несанкционированного доступа на основе средства защиты информации vGate.

В процессе выполнения выпускной квалификационной работы была подготовлена статья на тему «Анализ рынка средств защиты информации от несанкционированного доступа, применяемых для защиты виртуальных инфраструктур» и опубликована в сборнике VII Ежегодной всероссийской межвузовской научно-практической конференции «Информационные технологии в науке и образовании. Проблемы и перспективы»[8] «Информационные технологии в науке и образовании. Проблемы и перспективы» (ВНМПК-2020).[8].

Таким образом, все пункты технического задания на выпускную квалификационную работу выполнены в полном объеме.

Была проведена проверка отчета на оригинальность в системе «Антиплагиат.ВУЗ». Результат проверки представлен в приложении Е на рисунке Е.1.

Список используемых источников

- 1 СЗИ от НСД vGate. [Электронный ресурс] // www.securitycode.ru: официальный сайт разработчиков. Режим доступа: <https://www.securitycode.ru/products/vgate/> (свободный).
- 2 СЗИ от НСД Аккорд-В. [Электронный ресурс] // www.okbsapr.ru: официальный сайт разработчиков. Режим доступа: <https://www.okbsapr.ru/products/virtsys/segment-v/> (свободный).
- 3 Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00 [Электронный ресурс] // fstec.ru: официальный сайт ФСТЭК России. Режим доступа: <https://fstec.ru/tekhnicheskaya-zaschita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591>(свободный)
- 4 Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [Электронный ресурс] // fstec.ru: официальный сайт ФСТЭК Росии. Режим доступа: <https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702> (свободный).
- 5 Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс] // fstec.ru: официальный сайт ФСТЭК Росии. Режим доступа: <https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691>(свободный).
- 6 VirtualBox [Электронный ресурс] // www.virtualbox.org: официальный сайт разработчиков. Режим доступа: <https://www.oracle.com/virtualization/technologies/vm/downloads/virtualbox-downloads.html> (свободный).

7 Операционные системы Windows [Электронный ресурс] // www.microsoft.com: официальный сайт разработчика. Режим доступа: <https://www.microsoft.com/ru-ru> (свободный).

8 Деревягин Р.Е., Фатеев А.Г. «Анализ рынка средств защиты информации от несанкционированного доступа, применяемых для защиты виртуальных инфраструктур». Сборник статей по материалам VII Всероссийской межвузовской научно-практической конференции [Электронный ресурс] // www.elibrary.ru: Режим доступа: <https://elibrary.ru/item.asp?id=42821624> (свободный).

Приложение А

(обязательное)

Состав виртуального стенда, использующегося при выполнении практикума

Состав виртуального стенда, используемого при выполнении практикума

Конфигурация лабораторного стенда для выполнения заданий по темам:

"Управление доступом к ресурсам виртуальной инфраструктуры и контроль целостности, реализуемые средством защиты информации vGate"
 "Управление виртуальной инфраструктурой и безопасностью виртуальной инфраструктуры при использовании средства защиты информации vGate"

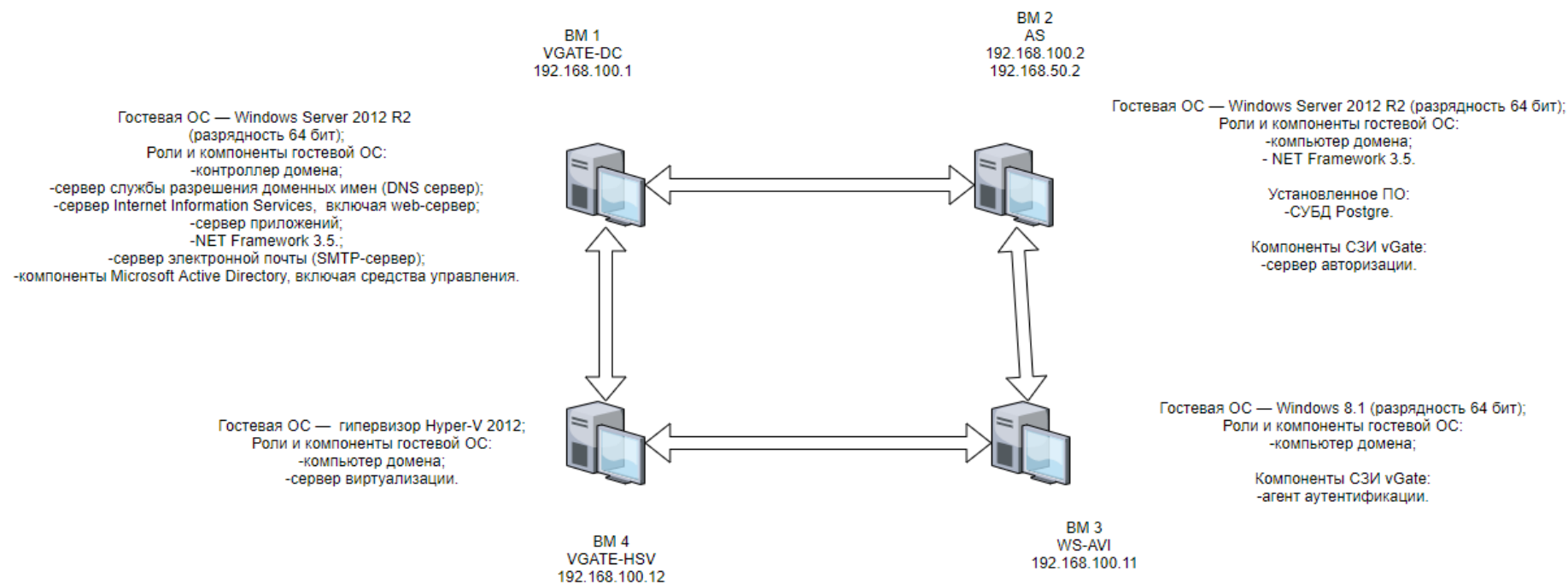


Рисунок А.1 - Состав виртуального стенда, используемого при выполнении практикума

Приложение Б

(обязательное)

UML – диаграмма последовательности действий выполнения практических заданий

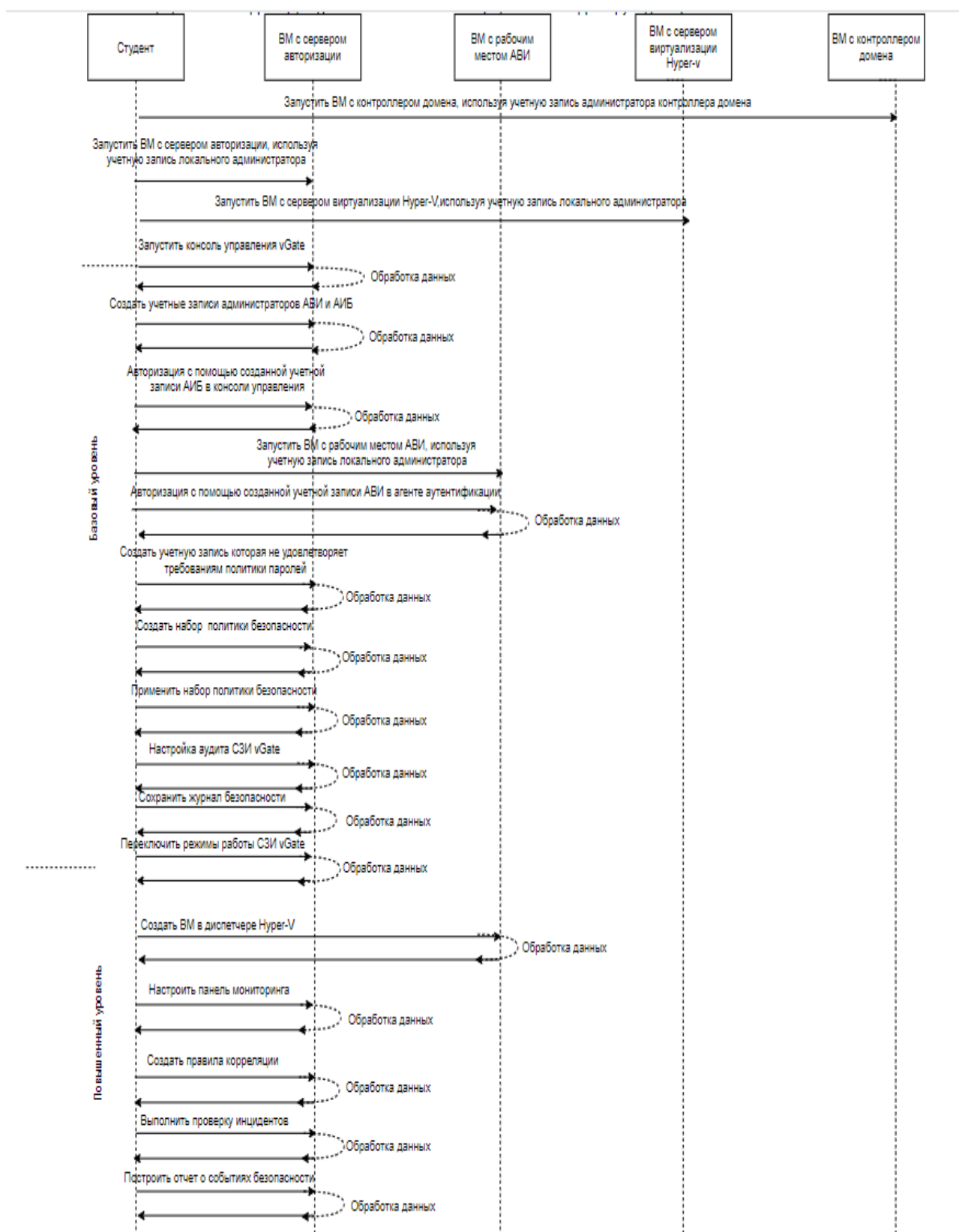


Рисунок Б.1 - UML – диаграмма последовательности действий выполнения практического задания по управлению виртуальной инфраструктурой и безопасностью виртуальной инфраструктуры при использовании C3I vGate

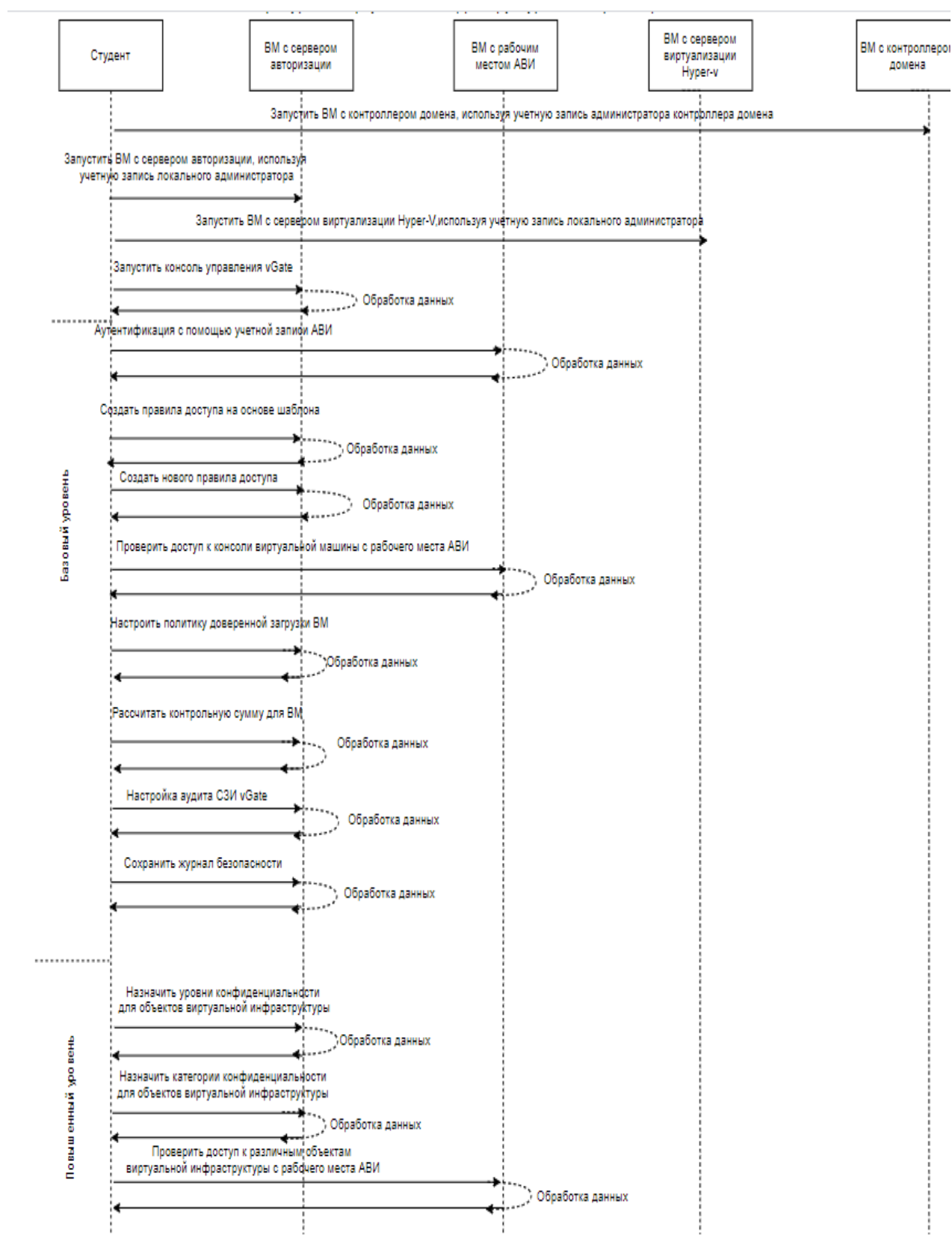


Рисунок Б.2 - диаграмма последовательности действий выполнения практического задания управлению доступом к ресурсам виртуальной инфраструктуры и контролю целостности

Приложение В

(обязательное)

Структура отчета о выполнении практических заданий

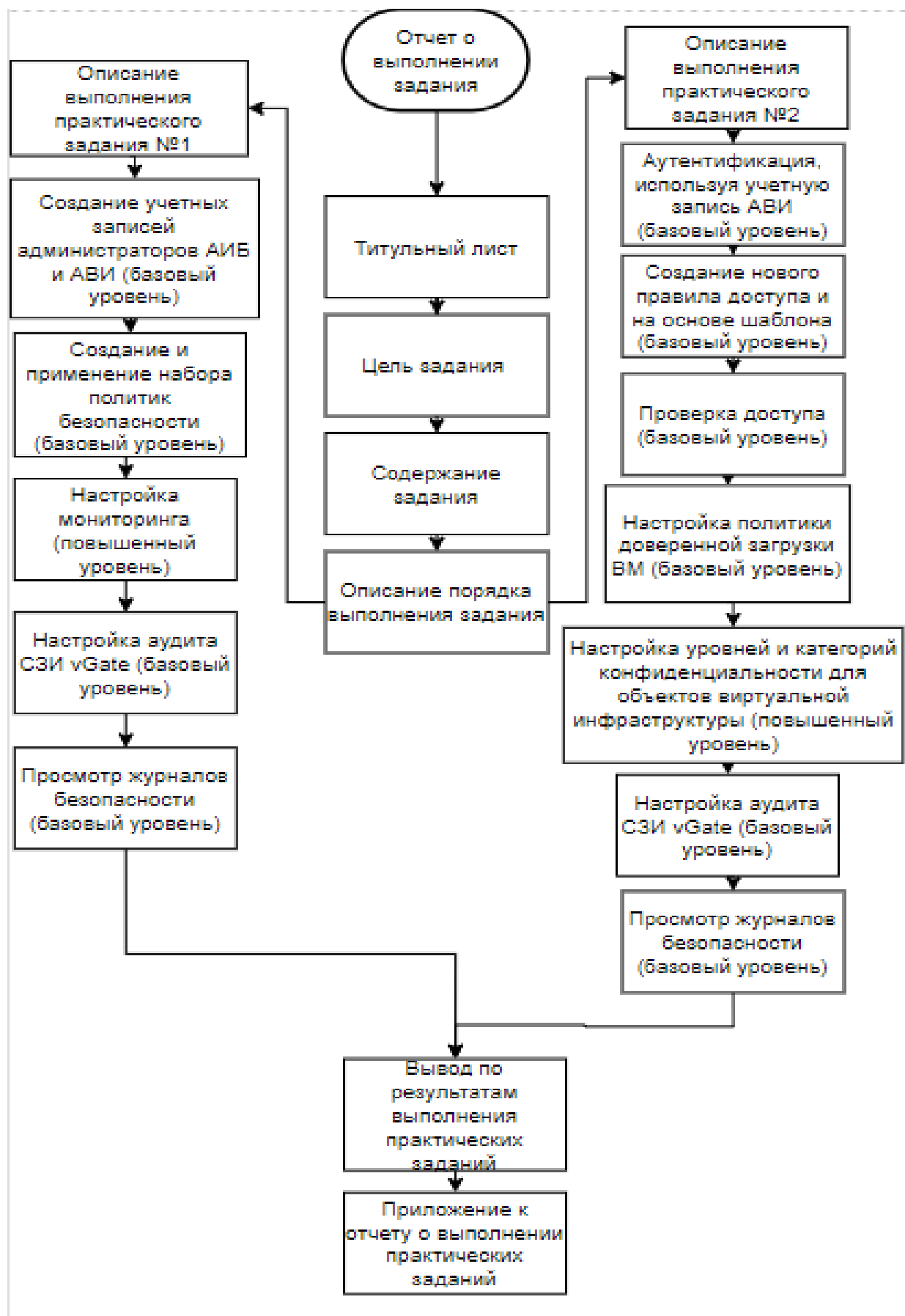


Рисунок В.1- Структура отчета о выполнении практических заданий

Приложение Г
(обязательное)

Порядок контроля выполнения практических заданий

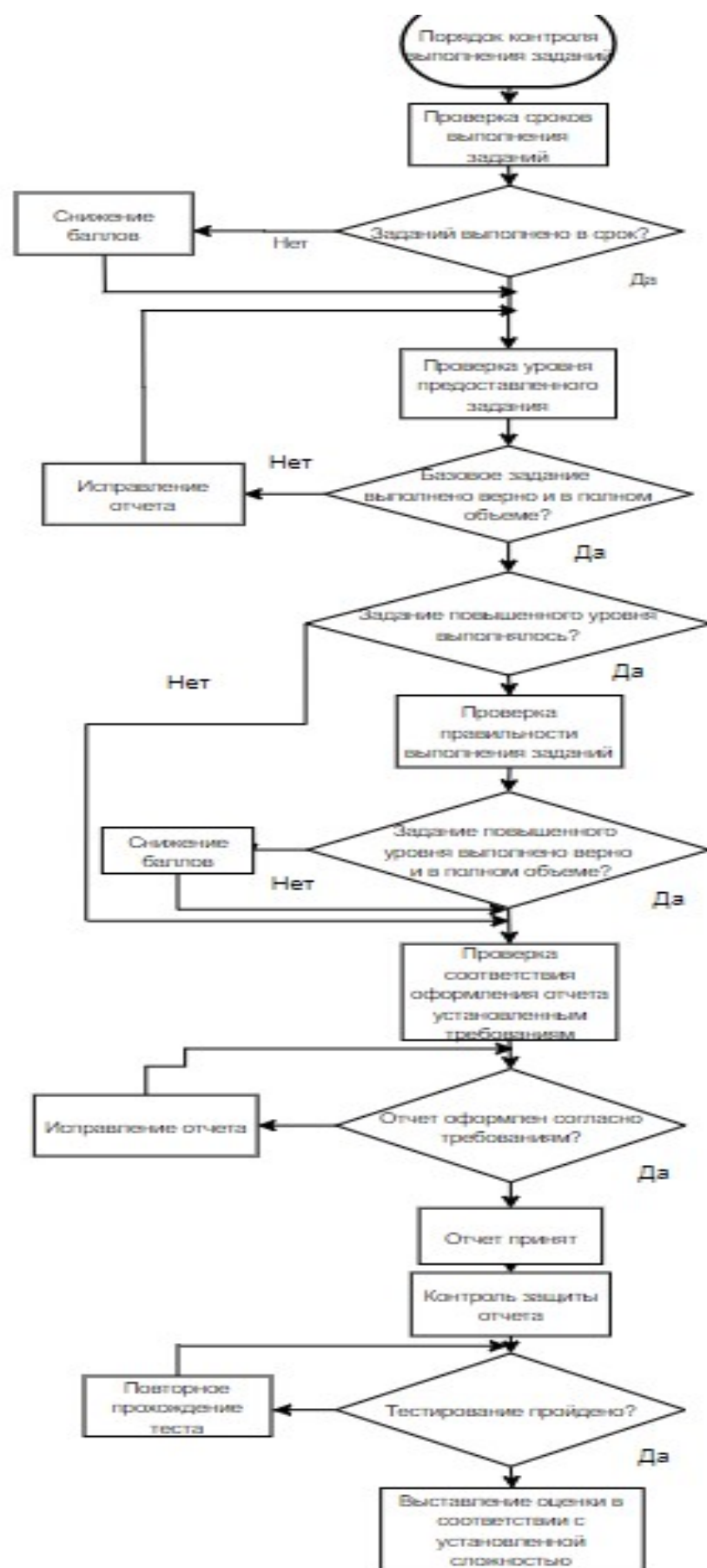


Рисунок Г.1 - Порядок контроля выполнения практических заданий

Приложение Д
(обязательное)

Сценарии автоматизированного развертывания виртуальных машин

Д.1 Сценарий автоматизированного развертывания ВМ под управлением ОС Windows Server 2012 R2

@echo off

rem *****

rem Universal script for VMs

rem *****

set VHDTYPE="immutable"

set VHDPATH="E:\\machine\\WS2012.vdi"

set VMNAME="DC-VGATE"

set OS_TYPE="Windows2012_64"

REM set OS_TYPE="Windows"

set MEMORY="1536"

set VIDEO="128"

set _ACPI="on"

set _IOAPIC="on"

set _PAE="on"

set _HWVIRTEX="on"

set _VTXVID="on"

set netadapter="Intel PRO/1000 MT Desktop (Внутренняя сеть, 'intnet')"

set SHAREPATH="E:\\abc"

REM if == 0 -> not shared folders

set VBOXM="%programfiles%\\Oracle\\VirtualBox\\vboxmanage"

%VBOXM% createvm --name %VMNAME% --ostype %OS_TYPE% --register

%VBOXM% storagectl %VMNAME% --add ide --controller PIIX4 --name
"PIIX4"

%VBOXM% storageattach %VMNAME% --storagectl PIIX4 --port 0 --device 0
--type hdd --medium %VHDPATH% --mtype %VHDTYPE%

%VBOXM% storageattach %VMNAME% --storagectl PIIX4 --port 0 --device 1
--type dvddrive --medium "emptydrive"

%VBOXM% modifyvm %VMNAME% --memory %MEMORY% --vram

```
%VIDEO% --acpi %_ACPI% --ioapic %_IOAPIC% --pae %_PAE% --hwvrtex  
%_HWVIRTEX% --vtxvpid %_VTXVID% --audio none  
%VBOXM% modifyvm %VMNAME% --usb on --usbhci on  
%VBOXM% modifyvm %VMNAME% --clipboard bidirectional  
%VBOXM% modifyvm %VMNAME% --nic1 intnet  
if not %SHAREPATH%=="0" %VBOXM% sharedfolder add %VMNAME%  
--name share --hostpath %SHAREPATH%  
@pause
```

Д.2 Сценарий автоматизированного развертывания ВМ под управлением ОС Windows Server 2012 R2

@echo off

rem *****

rem Universal script for VMs

rem *****

set VHDTYPE="immutable"

set VHDPATH="E:\\machine\\AS.vdi"

set VMNAME="AS"

set OS_TYPE="Windows2012_64"

REM set OS_TYPE="Windows"

set MEMORY="1536"

set VIDEO="128"

set _ACPI="on"

set _IOAPIC="on"

set _PAE="on"

set _HWVIRTEX="on"

set _VTXVID="on"

set netadapter0="Intel PRO/1000 MT Desktop (Внутренняя сеть, 'intnet')"

set netadapter1="Intel PRO/1000 MT Desktop (Внутренняя сеть, 'intnet')"

set SHAREPATH="E:\\abc"

REM if == 0 -> not shared folders

set VBOXM="%programfiles%\\Oracle\\VirtualBox\\vboxmanage"

%VBOXM% createvm --name %VMNAME% --ostype %OS_TYPE% --register

%VBOXM% storagectl %VMNAME% --add ide --controller PIIX4 --name
"PIIX4"

%VBOXM% storageattach %VMNAME% --storagectl PIIX4 --port 0 --device 0
--type hdd --medium %VHDPATH% --mtype %VHDTYPE%

%VBOXM% storageattach %VMNAME% --storagectl PIIX4 --port 0 --device 1
--type dvddrive --medium "emptydrive"

```
%VBOXM% modifyvm %VMNAME% --memory %MEMORY% --vram  
%VIDEO% --acpi %_ACPI% --ioapic %_IOAPIC% --pae %_PAE% --hwvrtex  
%_HWVIRTEX% --vtxvpid %_VTXVID% --audio none  
%VBOXM% modifyvm %VMNAME% --usb on --usbhci on  
%VBOXM% modifyvm %VMNAME% --clipboard bidirectional  
%VBOXM% modifyvm %VMNAME% --nic1 intnet  
if not %SHAREPATH%=="0" %VBOXM% sharedfolder add %VMNAME%  
--name share --hostpath %SHAREPATH%  
@pause
```

Д.3 Сценарий автоматизированного развертывания ВМ под управлением ОС Windows Server 2012 R2

@echo off

```
rem *****
```

```
rem Universal script for VMs
```

```
rem *****
```

```
set VHDTYPE="immutable"
```

```
set VHDPATH="E:\\machine\\Win81.vdi"
```

```
set VMNAME="WS-AVI"
```

```
set OS_TYPE="Windows8.1_64"
```

```
REM set OS_TYPE="Windows"
```

```
set MEMORY="1024"
```

```
set VIDEO="128"
```

```
set _ACPI="on"
```

```
set _IOAPIC="on"
```

```
set _PAE="on"
```

```
set _HWVIRTEX="on"
```

```
set _VTXVID="on"
```

```
set netadapter="Intel PRO/1000 MT Desktop (Внутренняя сеть, 'intnet')"
```

```
set SHAREPATH="E:\\abc"
```

```
REM if == 0 -> not shared folders
```

```
set VBOXM="%programfiles%\\Oracle\\VirtualBox\\vboxmanage"
```

```
%VBOXM% createvm --name %VMNAME% --ostype %OS_TYPE% --register
```

```
%VBOXM% storagectl %VMNAME% --add ide --controller PIIX4 --name  
"PIIX4"
```

```
%VBOXM% storageattach %VMNAME% --storagectl PIIX4 --port 0 --device 0  
--type hdd --medium %VHDPATH% --mtype %VHDTYPE%
```

```
%VBOXM% storageattach %VMNAME% --storagectl PIIX4 --port 0 --device 1  
--type dvddrive --medium "emptydrive"
```

```
%VBOXM% modifyvm %VMNAME% --memory %MEMORY% --vram
```

```
%VIDEO% --acpi %_ACPI% --ioapic %_IOAPIC% --pae %_PAE% --hwvrtex  
%_HWVIRTEX% --vtxvpid %_VTXVID% --audio none  
%VBOXM% modifyvm %VMNAME% --usb on --usbhci on  
%VBOXM% modifyvm %VMNAME% --clipboard bidirectional  
%VBOXM% modifyvm %VMNAME% --nic1 intnet  
if not %SHAREPATH%=="0" %VBOXM% sharedfolder add %VMNAME%  
--name share --hostpath %SHAREPATH%  
@pause
```

Д.4 Сценарий автоматизированного развертывания ВМ под управлением ОС Hyper-V 2012

@echo off

```
rem *****
rem Universal script for VMs
rem *****

set VHDTYPE="immutable"
set VHDPATH="E:\\machine\\HV2012.vdi"
set VMNAME="WS-AVI"
set OS_TYPE="Windows2012_64"
REM set OS_TYPE="Windows"
set MEMORY="512"
set VIDEO="128"
set _ACPI="on"
set _IOAPIC="on"
set _PAE="on"
set _HWVIRTEX="on"
set _VTXVID="on"
set netadapter="Intel PRO/1000 MT Desktop (Внутренняя сеть, 'intnet')"
set SHAREPATH="E:\\abc"
REM if == 0 -> not shared folders
set VBOXM="%programfiles%\\Oracle\\VirtualBox\\vboxmanage"
%VBOXM% createvm --name %VMNAME% --ostype %OS_TYPE% --register
%VBOXM% storagectl %VMNAME% --add ide --controller PIIX4 --name
"PIIX4"
%VBOXM% storageattach %VMNAME% --storagectl PIIX4 --port 0 --device 0
--type hdd --medium %VHDPATH% --mtype %VHDTYPE%
%VBOXM% storageattach %VMNAME% --storagectl PIIX4 --port 0 --device 1
--type dvddrive --medium "emptydrive"
%VBOXM% modifyvm %VMNAME% --memory %MEMORY% --vram
```

```
%VIDEO% --acpi %_ACPI% --ioapic %_IOAPIC% --pae %_PAE% --hwvrtex  
%_HWVIRTEX% --vtxvpid %_VTXVID% --audio none  
%VBOXM% modifyvm %VMNAME% --usb on --usbhci on  
%VBOXM% modifyvm %VMNAME% --clipboard bidirectional  
%VBOXM% modifyvm %VMNAME% --nic1 intnet  
if not %SHAREPATH%=="0" %VBOXM% sharedfolder add %VMNAME%  
--name share --hostpath %SHAREPATH%  
@pause
```

Приложение Е

Протокол проверки ВКР в системе Антиплагиат

Отчет о проверке на заимствования №1



Автор: Деревягин Роман Евгеньевич romanderevyagin@yandex.ru / ID: 2388

Проверяющий: Иванов Алексей Петрович (ap_ivanov@mail.ru) / ID: 256

Организация: Пензенский государственный университет

Отчет предоставлен сервисом «Антиплагиат» - <http://pnzgu.antiplagiat.ru>

ИНФОРМАЦИЯ О ДОКУМЕНТЕ

№ документа: 136
Начало загрузки: 05.06.2020 11:01:48
Длительность загрузки: 00:00:27
Корректировка от 05.06.2020 13:15:10
Имя исходного файла: Неизвестно
Название документа: ПРАКТИКУМ ПО
АДМИНИСТРИРОВАНИЮ СИСТЕМЫ
ЗАЩИТЫ СРЕДЫ ВИРТУАЛИЗАЦИИ ОТ
НЕСАНКЦИОНИРОВАННОГО ДОСТУПА НА
ОСНОВЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ
VGATE
Размер текста: 1 кБ
Тип документа: Выпускная
квалификационная работа
Символов в тексте: 130665
Слов в тексте: 15149
Число предложений: 721

ИНФОРМАЦИЯ ОБ ОТЧЕТЕ

Последний готовый отчет (ред.)
Начало проверки: 05.06.2020 12:54:42
Длительность проверки: 00:00:59
Комментарии: не указано
Модули поиска: Модуль поиска ИПС "Адилет", Модуль выделения библиографических записей, Сводная коллекция ЭБС, Модуль поиска "Интернет Плюс", Коллекция РГБ, Цитирование, Модуль поиска переводных заимствований, Модуль поиска переводных заимствований по eLibrary (EnRu), Модуль поиска переводных заимствований по интернет (EnRu), Коллекция eLIBRARY.RU, Коллекция ГАРАНТ, Коллекция Медицина, Диссертации и авторефераты НББ, Модуль поиска перефразирований eLIBRARY.RU, Модуль поиска перефразирований Интернет, Коллекция Патенты, Модуль поиска "ПГУ", Модуль поиска общеупотребительных выражений, Кольцо вузов



ЗАИМСТВОВАНИЯ
25,37%

САМОЦИТИРОВАНИЯ
0%

ЦИТИРОВАНИЯ
3,01%

ОРИГИНАЛЬНОСТЬ
71,62%

Рисунок Е.1- Отчет о проверке на оригинальность