

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
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 10.05.02 –

Специализация -

Информационная безопасность
телекоммуникационных систем
Разработка защищенных
телекоммуникационных систем

ДИПЛОМНЫЙ ПРОЕКТ

на тему

ЛАБОРАТОРНЫЙ ПРАКТИКУМ ПО ПРИМЕНЕНИЮ СИСТЕМЫ
КОНТРОЛЯ И ПРЕДОТВРАЩЕНИЯ УТЕЧЕК ИНФОРМАЦИИ
FALCONGAZE SECURETOWER

Студентка _____ Шишкина Ирина Вячеславовна

Руководитель _____ Фатеев А.Г.

Нормоконтролёр _____ Фатеев А.Г.

Рецензент Зам.ген.директора
по спец. вопросам АО «ПНИЭИ» _____ Сомкин С.А.

Работа допущена к защите (протокол заседания кафедры от _____ № _____)

Заведующий кафедрой _____ С.Л. Зефирова

Работа защищена с отметкой (протокол заседания ГЭК
от _____ № _____)

Секретарь ГЭК _____ А.Г. Фатеев

Пенза 2018

ОГЛАВЛЕНИЕ

Введение.....	5
1 Сравнительный анализ систем контроля и предотвращения утечек информации	7
1.1 Типовые функции систем контроля и предотвращения утечек информации	7
1.2 Сравнительный анализ DLP - систем	8
2 Функциональные возможности системы контроля и предотвращения утечек информации	17
2.1 Применение систем контроля и предотвращения утечек информации Falcongaze SecureTower.....	17
2.2 Функциональные возможности по контролю электронной почты	18
2.3 Контроль действий сотрудников.....	18
2.4 Контроль и индексирование рабочих станций	20
2.5 Технологии анализа информации	21
2.6 Система отчетов.....	22
2.7 Оповещения об инцидентах.....	23
3 Разработка виртуального стенда для изучения применения системы контроля и предотвращения утечек информации Falcongaze SecureTower	24
3.1 Программно – аппаратные требования к персональному компьютеру, используемому для выполнения заданий практикума	24
3.2 Процесс создания виртуальных машин.....	24
3.3 Создание докальной сети, включающей виртуальные машины. .	33
3.4 Настройка локальной сети средствами гостевой операционной системы	35
3.5 Установка ролей и компонентов гостевых ОС	44
3.6 Установка системы контроля и предотвращения утечек информации Falcongaze SecureTower.....	51
3.7 Результат создания виртуального стенда	52

4 Порядок выполнения задания по применению программного комплекса Falcongaze SecureTower	53
4.1 Установка консоли Falcongaze SecureTower на виртуальную машину с установленной операционной системой Windows 8.1	53
4.2 Создание политики безопасности и применение их для контроля устройств	62
5 Описание порядка выполнения заданий практикума и результатов выполнения	70
5.1 Порядок выполнения заданий практикума	70
5.2 Порядок выполнения практического задания по установке программного комплекса Falcongaze SecureTower в локальной сети с доменной структурой	70
5.3 Порядок выполнения практического задания по созданию политики безопасности программного комплекса Falcongaze SecureTower и применение их для контроля устройств	72
6 Описание структуры и содержания отчета о выполнении практических заданий	74
6.1 Порядок выполнения заданий практикума	74
6.2 Структура отчета по выполнению задания по установке программного комплекса Falcongaze SecureTower в локальной сети с доменной структурой	74
6.3 Структура отчета по выполнению задания по созданию политики безопасности программного комплекса Falcongaze SecureTower и применение их для контроля устройств	75
7 Определение порядка контроля выполнения практического задания ...	77
7.1 Общий порядок контроля	77
7.2 Порядок контроля практического задания по установке программного комплекса Falcongaze SecureTower в локальной сети с доменной структурой	77

7.3 Порядок контроля практического задания по созданию политики безопасности программного комплекса Falcongaze SecureTower и применение их для контроля устройств	78
8 Подготовка сценария для автоматизированного развертывания виртуальных машин.....	80
9 Вредные психофизиологические факторы, влияющие на сердечно-сосудистую систему специалиста по защиты информации. Методы и средства физической культуры, снижающие их воздействие.....	82
Заключение	85
Список используемых источников.....	86
Приложение А Состав виртуального стенда, используемого при выполнении практикума.....	87
Приложение Б UML – диаграмма последовательности действий выполнения задания по установке программного комплекса Falcongaze SecureTower в локальной сети с доменной структурой	89
Приложение В UML – диаграмма последовательности действий выполнения задания по созданию политики безопасности программного комплекса Falcongaze SecureTower и применение их для контроля устройств	91
Приложение Г Структура отчетов о выполнении заданий практикума....	93
Приложение Д Контрольный экземпляр отчета по выполнению задания по установке программного комплекса Falcongaze SecureTower в локальной сети с доменной структурой	96
Приложение Е Контрольный экземпляр отчета по выполнению задания по созданию политики безопасности программного комплекса Falcongaze SecureTower и применение их для контроля устройств	99
Приложение Ж Порядок проверки выполнения заданий практикума ...	102
Приложение И Сценарии для автоматизированного развертывания ВМ	105
Приложение К Протокол проверки отчета в системе Антиплагиат	111

ВВЕДЕНИЕ

В последнее время все большее распространение среди средств защиты информации (СЗИ) получают системы контроля и предотвращения утечек информации (СК и ПУИ). Они более известны по своему англоязычному названию DLP-системы. Оно является сокращением от Data Loss Prevention или Data Leak Protection. Существуют и другие варианты названия, дающие сокращение DLP.

Использование СК и ПУИ наиболее актуально для организаций, где риск утечки повлечет серьезный финансовый или репутационный ущерб. Помимо предотвращения утечек информации СК и ПУИ может осуществлять контроль действий пользователей при доступе к различным ресурсам локальной сети и сети общего доступа (Интернет), анализ информационных потоков через электронную почту, социальные сети, внутрикорпоративные коммуникационные ресурсы, чаты и т.п.

Ключевая задача DLP-систем – контроль используемых коммуникационных каналов, а также осуществление проверки содержимого передаваемой информации, с целью выявления попыток несанкционированной передачи информации, копирования и других действий.

В связи с расширением применения таких систем администраторы безопасности должны обладать знаниями и практическими навыками их установки и применения, поэтому подготовка таких специалистов становится в настоящее время актуальной задачей.

Целью выпускной квалификационной работы является разработка практикума, который посвящен применению программного комплекса Falcongaze SecureTower для выявления и предотвращения утечек информации, а также изучению функциональных возможностей, реализуемых Falcongaze SecureTower.

Для изучения программного комплекса Falcongaze SecureTower предлагается использовать виртуальный лабораторный стенд, включающий несколько виртуальных машин, объединенных в локальную сеть.

Такой лабораторный стенд был подготовлен при выполнении задания выпускной квалификационной работы. Он представляет собой несколько виртуальных машин с установленными гостевыми операционными системами (ОС), необходимым программным обеспечением (ПО) и компонентами программного комплекса Falcongaze SecureTower, объединенных в локальную сеть. Кроме того при выполнении дипломного проекта были составлены описания двух заданий, которые входят в состав практикума. Также была определена структура отчета о выполнении заданий, определены требования к содержанию. Был разработан порядок контроля выполнения заданий. Для автоматизации развертывания стенда были разработаны сценарии развертывания виртуальных машин, входящих в его состав.

1 Сравнительный анализ систем контроля и предотвращения утечек информации

1.1 Типовые функции систем контроля и предотвращения утечек информации

Предотвращение утечек данных или DLP – система (Data Leak Prevention) – это программное обеспечение, направленное на предотвращения потери данных путем обнаружения возможных нарушений при их рассылке или фильтрации. Сервисы таких систем осуществляют мониторинг, обнаружение и, если это необходимо, блокирование информации при ее использовании, хранении или распространении [1].

Кроме описанной выше задачи, направленной на предотвращение утечек информации, DLP- системы также решают ряд и других задач, связанных с контролем действий персонала. Наиболее часто системы применяются также и для решения следующих задач:

- контроль использования рабочего времени и ресурсов персоналом;
- мониторинг общения сотрудников со сторонними организациями;
- контроль правомерности действий сотрудников, таких как предотвращение печати поддельных документов и других.

Системы контроля и предотвращения утечек информации позволяют контролировать информацию, передаваемую по следующим каналам:

- электронная почта (протоколы SMTP, POP3, IMAP, MAPI, NNTP, S/MIME);
- системы мгновенного обмена сообщений (протоколы OSCAR, MMP, MSN, XMPP, YMSG, HTTPIM, Microsoft Lync, Skype);
- протокол HTTP и его модификации (веб-почта, социальные сети, отправка SMS, контроль поисковых запросов, форумы, видеохостинги (загрузка файлов), фотохостинги (загрузка файлов), файлообменники (загрузка файлов));
- протоколы FTP и P2P;
- туннелирующие протоколы (IP-in-IP, L2TP, PPTP, PРоЕ и другие);

– внешние устройства (USB, DVD/CD-ROM, COM, LPT, USB, IrDA, FireWire, модемы, Bluetooth, принтеры, сетевые принтеры, камеры, сканеры и т.д.). Поддерживаются определенные типы устройств. Может быть реализована возможность запретить или разрешить использование устройства, получить тень копию информации, при её передаче на устройство, блокировки копируемой на устройство информации. Могут быть реализованы ограничения доступа в зависимости от типа съемного носителя (производитель, серия, модель, экземпляр). В системах может быть реализована возможность разрешать копирование только на доверенные носители, шифрование файлов на USB-устройствах, контроль беспроводной передачи данных (разрешение, запрет), контроль сетевых подключений (домены, сегменты сети), контроль буфера обмена, контроль запуска процессов;

– мобильные устройства;

– прочие протоколы. К ним относятся дополнительные возможности по контролю и выявлению утечек информации. Например, мониторинг активности на файл-серверах и в общих сетевых папках, контроль файлов, передаваемых отдельными приложениями (iTunes, Dropbox, Яндекс.Диск, uTorrent, GoogleDrive, Evernote), контроль IP-телефонии и т.д. [1].

1.2 Сравнительный анализ DLP – систем

1.2.1 DLP – системы могут быть как программными, так и программно-аппаратными комплексами. В них, как правило, входят модули сетевого уровня и модули уровня хоста (устанавливаются на локальных компьютерах пользователей).

Для анализа было проведено сравнение систем контроля и предотвращения утечек конфиденциальной информации. Для этого были рассмотрены СК и ПУИ, обладающие расширенным функционалом по сравнению с другими DLP – системами, а именно:

- Falcongaze SecureTower;
- DeviceLock;

- Zlock.

Все рассматриваемые системы имеют действующие сертификаты Федеральной службы по техническому и экспортному контролю (ФСТЭК).

1.2.2 Основные возможности Falcongaze SecureTower.

Назначение: контроль корпоративной информации за счет мониторинга максимального числа коммуникационных каналов и протоколов передачи данных.

Целевой сегмент: крупные корпоративные клиенты, решения для малого и среднего бизнеса.

Сравниваемая версия: Falcongaze SecureTower 5.9.

Системные требования:

- для системного оборудования:
 - процессор: 2 ГГц и выше (4 ядра и более);
 - оперативная память: 6 ГБ и более;
 - поддерживаемые ОС: Microsoft Windows Server 2008/2012/2016 (x64);
- для клиентской части:
 - процессор: 2 ГГц и выше;
 - оперативная память: не менее 4 ГБ;
 - поддерживаемые ОС: Microsoft Windows Vista/7/8/10/2008/2012/2016 (x86/x64) [2].

Сертификаты: сертификат ФСТЭК №3421 от 25.06.2015, что SecureTower является программным средством защиты от неправомерной передачи информации из информационной системы и соответствует требованиям руководящего документа "Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей" - по 4 уровню контроля и технических условий при выполнении указаний по эксплуатации [3].

Режимы работы: работа в режиме мониторинга, в режиме блокировки, работа системы вне сети компании.

Чтобы критически важная информация не покидала периметр компании, а доступ к этой информации внутри компании был строго ограничен, Falcongaze SecureTower осуществляет анализ внутреннего и исходящего сетевого трафика организации.

Режимы перехвата информации: осуществляется сетевой перехват, а также ведется работа в режиме перехвата трафика через агенты на рабочих станциях и в режиме перехвата трафика через интеграцию со сторонними сервисами.

Интеграция: осуществляется интеграция почтовыми сервисами, инсталляция и управление через групповые политики, масштабируемость (возможность подключения нескольких баз данных), возможность развертывания в виртуальных средах, удаленный контроль. Возможность интеграции со сторонними решениями для защиты конечных точек с использованием Device Lock.

Выполняемые функции: обеспечивает контроль всех сообщений популярных сервисов, социальных сетей, составляет полную картину веб – активности сотрудников, а именно отслеживает приложения, в которых ведется работа с корпоративной информацией, осуществляет контроль пользователей и рабочих станций, а также выявляются взаимосвязи сотрудников со сторонними организациями.

Создаются отчеты для службы безопасности по активности пользователей.

Производительность и отказоустойчивость: осуществляется автоматическая запись и индексация перехваченных данных, а также привязка информации к пользователям и компьютерам. Осуществляется контроль поступления перехваченной информации.

Соблюдены возможности резервирования, даже если нет соединения с сервером, агенты создают резервную копию.

Контролируемые каналы:

- электронная почта – SMTP, POP3, IMAP, MAPI;
- обмен сообщениями – OSCAR (например, QIP и ICQ), MMP (Mail.ru Агент), HTTPIM (обмен сообщениями в социальных сетях), Skype (текстовые сообщения, файлы, голосовой трафик);
- веб – каналы – HTTP и его модификации, Веб – почта, социальные сети, форумы, файлообменники;
- внешние устройства – USB-устройства, съёмные жёсткие диски, карты памяти, локальные и сетевые принтеры, переносные устройства Windows; поддерживается возможность разрешения или запрета использования устройств, а также получение теневой копии информации при ее передаче на устройство, возможность блокировки информации, копируемой на устройство, осуществление копирования только на доверенные устройства, контроль печати, контроль буфера обмена.

Контроль пользователей: контроль выполняется с заданным интервалом времени, снимки экрана, просмотр рабочего стола в режиме реального времени, запись звука через микрофон ноутбука или подключенную гарнитуру, протоколирование времени работы в приложениях, сканирование рабочих станций.

Реакция на инциденты: ведется запись в журналах безопасности, теневое копирование, уведомление администратора безопасности, блокировка соединения, карантин, фильтрация трафика [4].

1.2.3 Основные возможности Device Lock.

Назначение: предотвращения утечки информации с помощью контекстного контроля, путем блокирования или разрешения передачи данных для определенных пользователей и в зависимости от типа интерфейса.

Целевой сегмент: крупные корпоративные клиенты, решения для малого и среднего бизнеса, государственный сектор.

Сравниваемая версия: Device Lock 8.2.

Системные требования:

- агенты – Windows NT/2000/XP/Vista/7/8/8.1/10/Server 2003-2016 (32/64-бита); память от 64 Мб, дисковое пространство от 100 Мб и выше, дополнительное место для теневых копий;

- консоли – Windows 2000/XP/Vista/7/8/8.1/10/Server 2003-2016 (32/64-бита); память 2 Гб, дисковое пространство 600 Мб;

- DeviceLock Enterprise Server, DeviceLock Discovery Server, Device Lock Search Server – Windows Server 2003-2016 (32/64-бита), память 8 Гб, диск 800 Гб (меньше, если не используется БД SQL) [5].

Сертификаты: действующий сертификат соответствия ФСТЭК России № 3465 от 05.11.2015 г. Программный комплекс соответствует требованиям документов «Требования к средствам контроля съемных машинных носителей информации, ФСТЭК России», утверждённых Приказом ФСТЭК России от 28 июля 2014 г. N 87 - по 4 классу защиты и «Профиль защиты средств контроля подключения съемных машинных носителей информации четвертого класса защиты», руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей» (Гостехкомиссия России, 1999) [3].

Режимы работы: работа в режиме контентной фильтрации, в режиме блокировки, в режиме защиты от локального администратора, в режиме контроля сетевых коммуникаций.

Режимы перехвата информации: осуществляется контроль буфера обмена, что позволяет снизить возможность перехвата передающих данных, создание белых списков устройств и носителей информации.

Интеграция: полная интеграция в групповые политики позволяет автоматически устанавливать программный продукт на новые компьютеры, подключаемые к корпоративной сети и осуществлять настройку для новых компьютеров в автоматическом режиме, интеграция с внешними средствами шифрования, позволяющая разрешить запись только зашифрованных данных на съемные устройства или запретить запись незашифрованных данных.

Выполняемые функции: обеспечивается контроль доступа к устройствам и интерфейсам, контроль сетевых коммуникаций обеспечивается через компонент NetworkLock, который распознает сетевые протоколы, обеспечивает детектирование приложений, а также ведет событийное протоколирование и теневое копирование передаваемых данных, через компонент ContentLock ведется контентную фильтрацию данных, копируемых на съемные устройства, а также передаваемых по сетевым каналам персонального компьютера, ведется защита от локального администратора, путем обеспечения необходимого уровня защиты, даже если пользователи в сети имеют административные привилегии на локальных компьютерах, ведется централизованное управление, осуществляется контроль как над буфером обмена, так и по типу файлов. Создаются белые списки устройств, протоколируются все действия пользователя, контроль виртуальных и терминальных сред.

Производительность и отказоустойчивость: позволяет формировать графические отчеты на основе данных отчета аудита и теневого копирования, проводится централизованный мониторинг, который позволяет контролировать текущее состояние агентов на удаленных компьютерах.

Контролируемые каналы:

- почтовые протоколы: MAPI, SMTP/SMTPS;
- веб-сервисы: Почта Mail.Ru, Рамблер-Почта, Яндекс.Почта, Gmail, AOL Mail, Hotmail/Outlook.com, Yahoo! Mail, Outlook Web App/Access (OWA).
- социальные сети: ВКонтакте (включая API), Одноклассники, LiveJournal, LiveInternet.ru, Facebook (включая API), Twitter, Google+, LinkedIn, Tumblr;
- сетевые сервисы файлового обмена и синхронизации: Яндекс.Диск, Google Drive, Dropbox, OneDrive, RapidShare;
- службы мгновенных сообщений: Skype, Агент Mail.Ru, ICQ/AOL, MSN Messenger, Jabber, IRC, Yahoo! Messenger;
- сетевые протоколы: HTTP/HTTP-SSL, FTP/FTP-SSL, Telnet;

– прочее: внутрисетевые файловые ресурсы (SMB), звонки Skype, FTP и FTP-SSL, HTTP/HTTPS, POP3, SMTP.

Контроль пользователей: DeviceLock обеспечивает полный контроль доступа пользователей и пользовательских групп к портам ввода-вывода (USB, FireWire, COM, LPT, IrDA), сетевым адаптерам WiFi и Bluetooth, любым типам принтеров (локальные, сетевые и виртуальные), мобильным устройствам (на базе iOS, Android, Windows Phone и других платформ), а также сменным носителям CD/DVD и т. п. Для любого типа устройства или порта можно задать доступ в зависимости от времени и дня недели, а также задать тип доступа «только чтение» для сменных носителей.

Реакция на инцидент: DeviceLock обеспечивает отправку тревожных оповещений для администратора в режиме реального времени. Оповещения могут отправляться в почтовых сообщениях по протоколам SMTP и/или SNMP. Также может выполнять селективную блокировку, реконструкцию сообщений и сессий с восстановлением файлов, данных и параметров, а также протоколирование и теневое копирование передаваемых файлов [5].

1.2.4 Основные возможности Zlock.

Назначение: предназначен для защиты информации от утечек на конечных точках сети.

Целевой сегмент: крупные корпоративные клиенты, средний бизнес, государственный сектор.

Сравниваемая версия: Zlock 6.0.

Системные требования для клиентского модуля, сервера журналов, сервера поиска, сервера конфигураций и консоли управления:

- процессор: Pentium 4 или выше;
- оперативная память: от 1ГБ;
- поддерживаемые ОС: для клиентской части – MS Windows XP SP3/2003/ Vista/2008 / 7 / 8 (32 и 64 бит); для всего остального – MS Windows XP SP3 (32бита)/ 2003 SP1 (32 и 64 бит)/ Vista SP1(32 и 64 бит)/ 2008/Windows 7/8 (32 и 64 бит)/2008 R2/2012 [6].

Сертификаты: сертификат ФСТЭК России №2753 удостоверяет, что средство защиты информации Zlock соответствует требованиям руководящего документа "Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей" по 4 уровню контроля и технических возможностей и может использоваться при создании автоматизированных систем до класса защищенности 1Г включительно и для защиты информации в ИСПДн до 1 класса включительно[3].

Режимы работы: работа в режиме мониторинга, в режиме сбора и анализа событий.

Режимы перехвата информации: осуществляет мониторинг клиентских модулей, которые позволяют администратору в реальном времени получать всю информацию о пользователях, что в свою очередь позволяет оперативно реагировать на несанкционированные действия злоумышленника, работа в режиме перехвата трафика через агенты на рабочих станциях, работа в режиме перехвата трафика через интеграцию со сторонними сервисами.

Интеграция: осуществляется интеграция почтовыми сервисами, инсталляция и управление через групповые политики, масштабируемость (возможность подключения нескольких баз данных), возможность развертывания в виртуальных средах, удаленный контроль.

Выполняемые функции: удаленное управление, с помощью которой администратор может устанавливать клиентские части, осуществляется мониторинг клиентских рабочих станций, функции по ведению и анализу журнала теневого копирования, теневое копирование, контроль целостности настроек и параметров компонентов, сервер журналирования.

Производительность и отказоустойчивость: позволяет формировать отчет по журналу событий и теневого копирования, проводится мониторинг клиентских рабочих станций, что позволяет отследить возможные попытки

несанкционированного отключения Zlock на рабочей станции, изменения настроек или политик доступа.

Контролируемые каналы:

- электронная почта – SMTP, POP3, IMAP, MAPI (через агенты);
- обмен сообщениями – OSCAR (например, QIP и ICQ), MMP (Mail.ru Агент), HTTPIM (обмен сообщениями в социальных сетях), Skype (текстовые сообщения, файлы, голосовой и видео трафик);
- веб – каналы – HTTP и его модификации, Веб – почта, социальные сети, форумы, файлообменники;
- внешние устройства – USB-устройства, съёмные жёсткие диски, карты памяти, локальные и сетевые принтеры, переносные устройства Windows. Поддерживается возможность разрешения или запрета использования устройств, а также получение теневой копии информации при ее передаче на устройство, возможность блокировки информации, копируемой на устройство, осуществление копирования только на доверенные устройства, контроль печати, контроль буфера обмена на любых поддерживаемых устройствах.

Контроль пользователей: осуществляются снимки экрана, сканирование рабочих станций.

Реакции на инциденты: ведется запись в журналах безопасности, теневое копирование, уведомление администратора безопасности, блокировка соединения, карантин, фильтрация трафика[6].

В результате проведенного детального сравнения систем контроля и предотвращения утечек конфиденциальной информации DLP – систем было выявлено, для дальнейшего рассмотрения функциональных возможностей была выбрана система контроля и предотвращения утечек конфиденциальной информации Falcongaze SecureTower, обладающая наиболее расширенным функционалом по сравнению с другими DLP – системами.

2 Функциональные возможности системы контроля и предотвращения утечек информации Falcongaze SecureTower

2.1 Применение системы контроля и предотвращения утечек информации Falcongaze SecureTower

Результаты сравнительного анализа показали, что среди рассмотренных СК и ПУИ программный комплекс Falcongaze SecureTower обладает наибольшими функциональными возможностями, позволяющими контролировать используемые каналы передачи информации и действия пользователей. Кроме того, Falcongaze SecureTower является одной из наиболее востребованной СК и ПУИ. Программный комплекс Falcongaze SecureTower применяется как в органах государственной власти, так и в негосударственных организациях различных форм собственности, относящихся к таким экономическим отраслям как:

- банковский и финансовый сектор;
- энергетика;
- здравоохранение;
- торговые компании;
- телекоммуникации;
- промышленность;
- образование;
- государственный сектор;
- научно-исследовательский сектор.

Для оценки функциональных возможностей СК и ПУИ Falcongaze SecureTower и целесообразности применения разработчик предлагает демонстрационную версию. Она является полнофункциональной версией. Действует ограничение срока использования. Он составляет один месяц.

Рассмотренные широко применяемые функциональные возможности системы контроля и предотвращения утечек информации Falcongaze SecureTower позволяют контролировать корпоративную информацию за счет

мониторинга максимального числа коммуникационных каналов и протоколов передачи данных [2].

2.2 Функциональные возможности по контролю электронной почты

Электронная почта, как правило, является наиболее часто используемым сервисом для передачи информации, как внутри организации, так и между различными организациями. Она может использоваться и для несанкционированной передачи информации, например, посторонним лицам. Поэтому использование электронной почты, а именно, действия пользователей, содержимое сообщений и файлов, которые пересылаются с ее использованием, должно обязательно контролироваться.

Falcongaze SecureTower обеспечивает контроль всех сообщений большинства популярных почтовых серверов, по протоколам POP3, SMTP и IMAP, а также перехватывает и блокирует сообщения по протоколу MAPI. Основной возможностью SecureTower контроля электронной почты, является то, что в процессе работы выполняется проверка сообщений на нарушение политик безопасности. Также система позволяет перехватывать и анализировать сообщения бесплатных почтовых сервисов.

Интеграция с почтовыми серверами осуществляется по протоколам POP3 или SMTP. При использовании интеграции по протоколу POP3 почтовый сервер должен настраиваться таким образом, чтобы копии всех проходящих через него почтовых отправок собирались на специальный внутренний почтовый ящик, с которого их будет забирать для анализа Сервер обработки почты SecureTower. При использовании протокола SMTP почтовый сервер настраиваться таким образом, чтобы копии всех проходящих через него почтовых отправок отправлялись на специальный внешний почтовый ящик, где их будет принимать Сервер обработки почты SecureTower [2].

2.3 Контроль действий сотрудников

Одним из важнейших факторов при выборе DLP-системы является возможность контролировать действия сотрудников организации в течение

рабочего дня. Для этого в SecureTower реализован функционал для контроля рабочего времени, позволяющий отследить время, которое работник затратил на выполнение той или иной задачи.

С помощью программного комплекса SecureTower руководители структурных подразделений и специалисты по информационной безопасности могут отслеживать каждодневную работу сотрудников всей компании, а также возможность отслеживать общение работников компании с клиентами и партнерами компании, а также внутри организации.

Контроль работников в SecureTower реализован несколькими способами, позволяющими отследить активность пользователей:

- автоматическое снятие скриншотов рабочего стола с заданной периодичностью, или при смене активного окна, а также при нажатии клавиши Print Screen;
- запись статистики по времени активной работы и простоя компьютера;
- контроль времени активной работы пользователей в конкретных приложениях;
- контроль буфера обмена;
- перехват нажатия клавиш (кейлоггер);
- отслеживание активности пользователя в браузерах.

Для обеспечения эффективной работы компании SecureTower полностью сохраняет всю деловую переписку персонала, а также статистические сведения об использовании веб-ресурсов или программ. Опираясь на эти сведения можно уведомлять или блокировать пользователей при повышении статистики посещения определенных сайтов или программ.

Все полученные SecureTower данные представляются в виде информативных отчетов, в которых отображается ежедневная деятельность персонала [2].

2.4 Контроль и индексирование рабочих станций

SecureTower позволяет контролировать и предотвращать передачу файлов на внешние носители. Система автоматически сканирует отправляемые на печать или USB-устройство документы на наличие в них конфиденциальной информации, а в случае обнаружения такой информации уведомляет администратора безопасности.

Также в SecureTower существует возможность отслеживания подключения и отключения устройств на рабочей станции, контроль копирования информации, и осуществлять аудит доступа к компьютеру.

Также реализована такая функция, как индексация рабочих станций, которая позволяет сканировать диски компьютеров на наличие в них конфиденциальной информации. С помощью этой функции можно выявлять конфиденциальные корпоративные документы, которые по какой-то причине оказались на компьютерах сотрудников – получены от коллег по почте или в мессенджерах, записаны с USB-носителей, скачаны с облачных хранилищ или скопированы из сетевых папок.

Для контроля передвижения критически важных данных в системе может быть создан банк эталонных документов, оборот которых необходимо контролировать. Мониторинг рабочих станций сотрудников осуществляется автоматически: настроенные в системе правила безопасности срабатывают при появлении на компьютере документа, совпадающего с образцом, хранящимся в банке эталонных данных.

Индексирование рабочих станций сотрудников позволяет предупреждать утечки информации ограниченного доступа. При своевременном выявлении несанкционированного доступа к конфиденциальным документам можно оперативно принять меры и предотвратить инцидент, связанный с несанкционированным копированием и распространением информации ограниченного доступа [2].

2.5 Технологии анализа информации

2.5.1 Системы контроля и предотвращения утечек информации реализуют различные технологии анализа информации, передаваемой по каналам передачи информации (возможным каналам утечки). Анализ информации применяется для выявления попыток несанкционированного копирования информации, несанкционированной передачи информации за периметр защищаемой информационной системы и блокирования таких действий. Системы контроля и предотвращения утечек информации осуществляют перехват и анализ содержания информационного потока, передаваемого по каждому контролируемому каналу.

В системе Falcongaze SecureTower реализованы такие виды анализа информации, как контентный, атрибутивный и статический.

Контентный анализ состоит из поиска информации по ключевым словам или фразам, поиск по регулярным выражениям, а также используется технология цифровых отпечатков для документов и баз данных. Для более эффективного контроля система SecureTower выполняет функцию проверки информации, содержащей транслитерированные слова или символы, что позволяет предотвратить бесконтрольную пересылку конфиденциальной информации в сети организации и за ее пределы [7].

2.5.2 Контроль информации с полной или частичной транслитерацией.

Falcongaze SecureTower выполняет проверку всех данных на содержание транслитерированных слов или символов. Проверка осуществляется по правилам как строгой, так и ослабленной транслитерации, то есть при проверке учитываются несколько различных способов транслитерации. И если, например, в словах, написанных кириллицей, заменить лишь часть букв на аналогичные по написанию латинские, то система обязательно обнаружит этот факт [2].

2.5.3 Нечеткий поиск.

Функция нечеткого поиска позволяет корректно проверять на соответствие политикам безопасности информацию, даже если в ней имеются опечатки и грамматические ошибки. Это очень важно при контроле сообщений мессенджеров или в социальных сетях, а также в случае контроля переведенных в электронный формат бумажных документов.

Также нечеткий поиск поможет выявить нарушения политик безопасности в случае контроля переведенных в электронный формат бумажных документов. При распознавании таких документов специальными программами неизбежно возникновение в тексте опечаток и лишних символов. Система SecureTower даже при передаче такого документа проверяет его содержимое на наличие конфиденциальной информации и в случае возникновения угрозы уведомляет службу безопасности [2].

2.5.4 Поиск по регулярным выражениям.

Реализованная функция в Falcongaze SecureTower поиска по регулярным выражениям обеспечивает возможность определения попыток передачи формализованных данных. Данная функция активно используется для защиты персональных данных, которые легко описываются шаблонами: паспортные данные, ИНН и пр. Количество шаблонов может задаваться самостоятельно с учетом специфики обрабатываемых данных в организации [2].

2.6 Система отчетов

Для сотрудников службы безопасности и руководителей структурных подразделений доступна функция построения настраиваемых отчетов по ежедневной работе сотрудников и инцидентов безопасности. Также в SecureTower можно настроить автоматическое создание отчетов по расписанию и отправку их на электронную почту.

В SecureTower реализовано несколько видов отчетов: индивидуальные, комплексные и по различным критериям. Индивидуальные отчеты могут создаваться по конкретному пользователю. При построении комплексных отчетов руководители структурных подразделений или специалисты службы

безопасности могут просмотреть статистику, как по подразделению, так и по отдельным сотрудникам. Этот вид отчетов позволяет получить статистическую информацию о деятельности пользователей за компьютером за определенный промежуток времени.

С помощью SecureTower можно формировать отчеты по различным критериям, например, получить сведения о включении или выключения рабочего компьютера пользователя, и таким образом можно проанализировать продолжительность рабочего времени сотрудников организации. Также можно сформировать отчеты, отражающие количественную информацию об отправленных пользователями сообщений. Возможность просмотра средних показателей по различным критериям позволяет выявить общие тенденции работы организации, которые могут свидетельствовать о нарушении рабочих процессов. Для наглядного представления статистических данных в отчетах системы SecureTower содержатся графики и диаграммы.

Для максимального удобства пользования интерфейсом системы, разработчики реализовали в SecureTower возможность экспорта созданных отчетов в документы популярных форматов (.XLS, .PDF, .RTF, .IMG и др.), а также прямого вывода их на печать. Благодаря этому специалист по защите информации или руководитель подразделения может оперативно предоставить руководству необходимые данные[2].

2.7 Оповещения об инцидентах

В Falcongaze SecureTower реализована система автоматического оповещения обо всех случаях нарушения заданных политик безопасности. В случае обнаружения инцидента, ответственному сотруднику службы информационной безопасности будет незамедлительно отправлено электронное письмо с уведомлением об этом инциденте и его кратким описанием [2].

3 Разработка виртуального стенда для изучения применения системы контроля и предотвращения утечек информации Falcongaze SecureTower

3.1 Программно-аппаратные требования к персональному компьютеру, используемому для выполнения заданий практикума

Для выполнения лабораторного практикума на персональный компьютер (ПЭВМ) необходимо установить стенд, включающий несколько виртуальных машин. Персональный компьютер, на который устанавливается стенд, должен отвечать следующим требованиям:

- должна быть установлена операционная система (ОС) Windows 8.1 и выше;
- должны быть установлены программное обеспечение Oracle VM VirtualBox версии 5.0.32 и расширение VirtualBox Extension Pack, соответствующий версии Oracle VM VirtualBox;
- центральный процессор должен поддерживать технологию аппаратной виртуализации;
- объем оперативной памяти должен быть не менее 8 Гб;
- свободное место на жестком диске должно быть не менее 100 Гб, которое понадобится для хранения образов виртуальных машин.

Для создания виртуальных машин и всего стенда в целом используемый персональный компьютер должен отвечать тем требованиям. Исключение составляет объем свободного места на жестком диске. необходимо как минимум 200 Гбайт для того чтобы дополнительно сохранить эталонные образы виртуальных машин. Эти образы нужны для восстановления работы стенда в случае, если какая-либо виртуальная машина перестанет функционировать.

3.2 Процесс создания виртуальных машин

3.2.1 Создание виртуальных машин с различными гостевыми операционными системами выполняется с использованием программного обеспечения виртуализации Oracle VM VirtualBox. Для этого необходимо

запустить Oracle VM VirtualBox Менеджер. После запуска вид главного окна Oracle VM VirtualBox Менеджер представлен на рисунке 1.

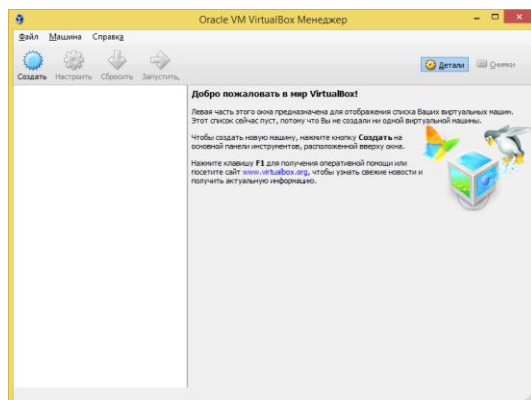


Рисунок 1 – Вид окна Oracle VM VirtualBox Менеджер

3.2.2 Создание виртуальной машины с установленной операционной системой Windows Server 2003.

Для запуска процесса создания виртуальной машины необходимо на главной панели Oracle VM VirtualBox Менеджер нажать кнопку «Создать». В открывшемся диалоговом окне необходимо выбрать имя для создаваемой виртуальной машины, установить тип и версию машины. В качестве имени записывается название гостевой операционной системы, например w2k3. Тип указывается – Microsoft Windows, версия – Windows 2003, разрядность указывается 32-битная (см. рисунок 2). Далее необходимо нажать кнопку «Next».

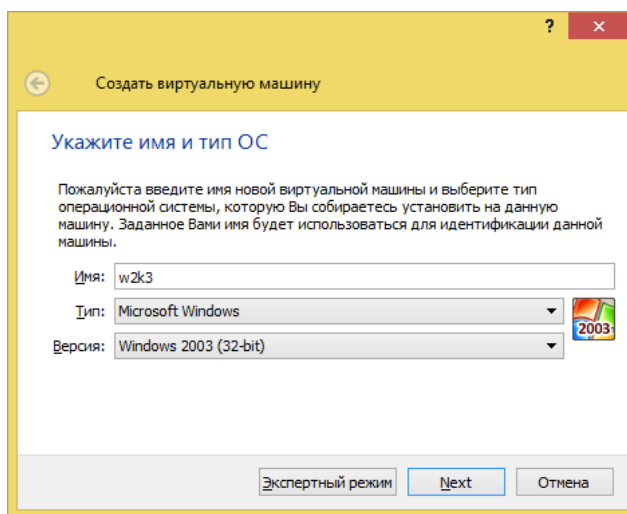


Рисунок 2 – Определение имени виртуальной машины, типа и версии гостевой ОС

В следующем диалоговом окне следует указать рекомендуемый объем оперативной памяти, выделенной для данной виртуальной машины (см. рисунок 3). Автоматически программа предлагает минимальный объем памяти в 512 Мб. Он может быть оставлен без изменения, а в дальнейшей работе может быть скорректирован. Далее необходимо нажать кнопку «Next».

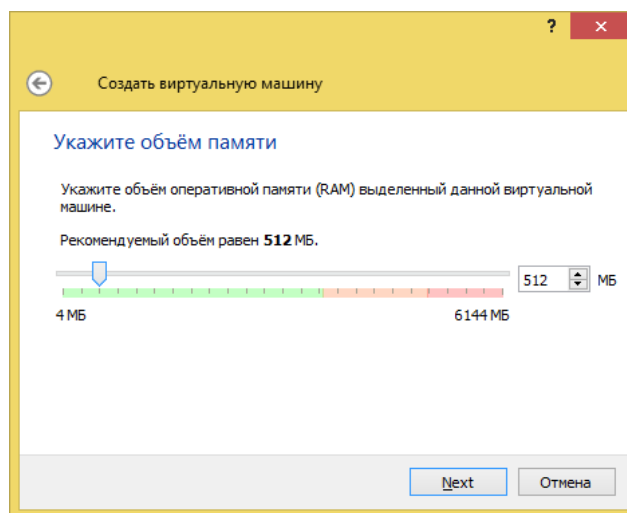


Рисунок 3 – Объем оперативной памяти виртуальной машины

На следующем шаге требуется подключить новый или уже имеющийся виртуальный жесткий диск к новой виртуальной машине (см. рисунок 4). Жесткий диск представляет собой файл, который хранится в файловой системе основной ОС на персональном компьютере. Необходимо выбрать пункт «Создать новый виртуальный жесткий диск» и нажать кнопку «Создать».

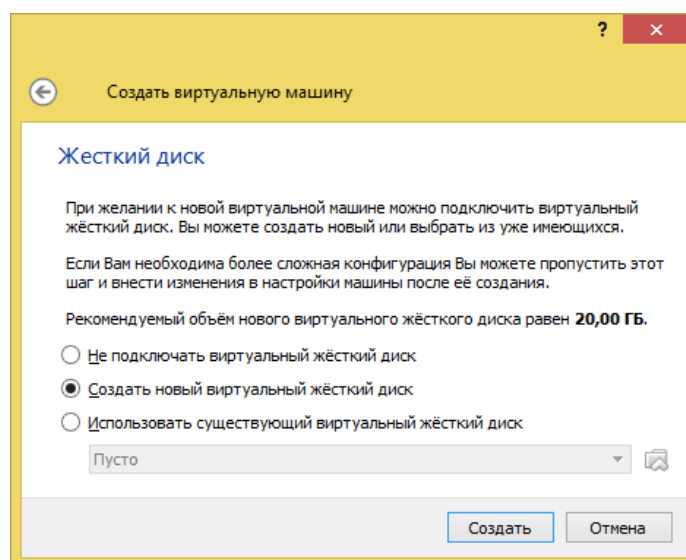


Рисунок 4 – Создание виртуального жесткого диска

При создании нового жесткого диска необходимо выбрать его тип (см. рисунок 5). Так как для запуска виртуальных машин будет использоваться только программа Oracle VM VirtualBox, выбирается формат «VDI (VirtualBox Disk Image)». После выбора формата, необходимо нажать кнопку «Next».

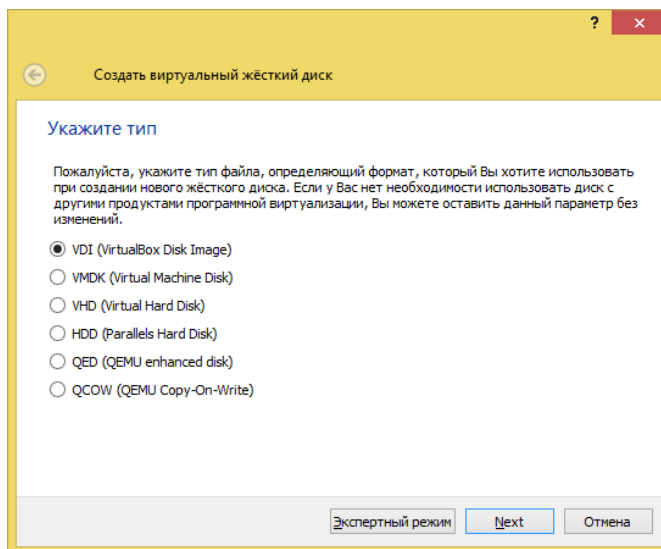


Рисунок 5 – Тип виртуального жесткого диска

На следующем шаге необходимо выбрать формат для хранения данных (см. рисунок 6). В качестве формата, для экономии пространства на компьютере, выбирается «Динамический виртуальный жесткий диск». Размер такого диска может быть увеличен по мере его использования, но при этом он не превысит максимального размера, указанного при создании виртуального диска. После выбора формата, необходимо нажать кнопку «Next».

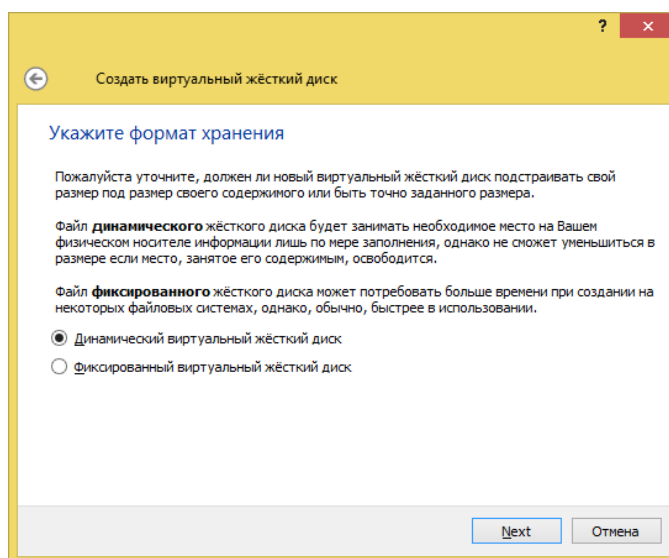


Рисунок 6 – Выбор формата хранения данных

В качестве имени нового виртуального жесткого диска указывается такое же имя, что и при создании новой виртуальной машины. Затем на шкале, показывающей объем создаваемого жесткого диска, указывается необходимое значение объема виртуального жесткого диска, например, равное 30 Гб. Формат хранения виртуального диска был выбран с целью оптимального расходования объема жесткого диска ПЭВМ, который будет использоваться для развертывания создаваемого стенда. Динамический диск при создании имеет минимальный размер и увеличивается по мере его заполнения информацией. Статический диск сразу занимает весь выделенный объем, при том что файл жесткого диска не заполнен информацией. После выбора имени и объема виртуального жесткого диска, нажимается кнопка «Создать» (см. рисунок 7).

После всех проделанных операций создается виртуальная машина с пустым виртуальным жестким диском и с неустановленным программным обеспечением.

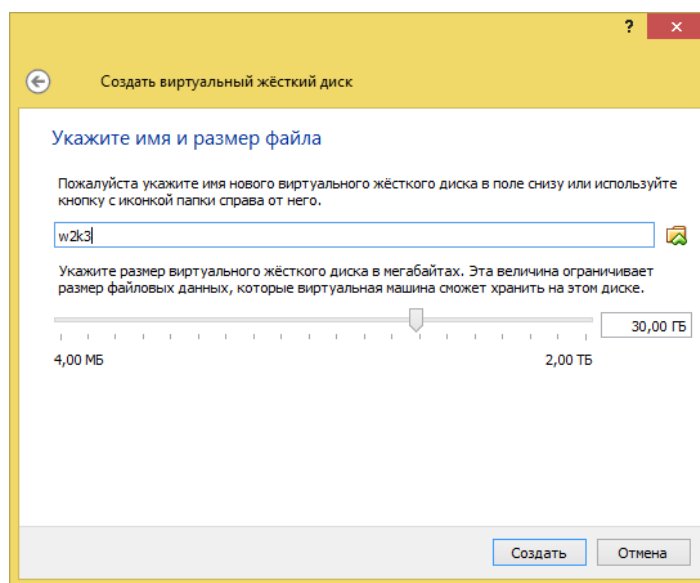


Рисунок 7 – Выбор имени и размера виртуального жесткого диска

После подготовки виртуальной машины выполняется установка гостевой операционной системы Windows Server 2003 R2 Enterprise Edition в соответствии с документацией разработчика Microsoft.

3.2.3 Создание виртуальной машины с установленной операционной системой Windows Server 2012 R2.

Для запуска процесса создания виртуальной машины необходимо на главной панели Oracle VM VirtualBox Менеджер нажать кнопку «Создать». В открывшемся диалоговом окне необходимо выбрать имя для создаваемой виртуальной машины, установить тип и версию машины. В качестве имени записывается название гостевой операционной системы, например w2k12. Тип указывается – Microsoft Windows, версия – Windows 2012, разрядность указывается 64-битная (см. рисунок 8). Далее необходимо нажать кнопку «Next».

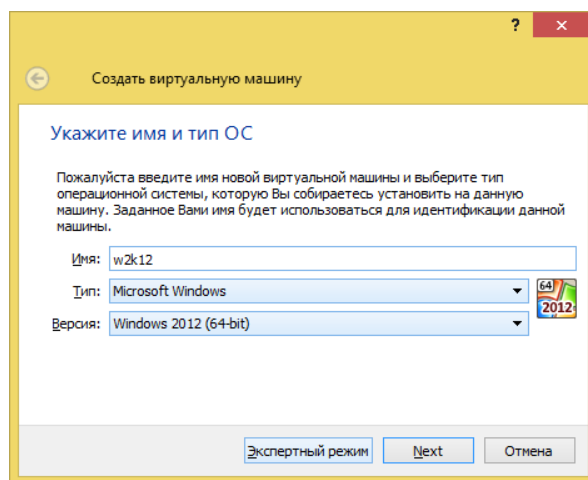


Рисунок 8 – Определение имени виртуальной машины, типа и версии гостевой ОС

В следующем диалоговом окне следует указать рекомендуемый объем оперативной памяти, выделенной для данной виртуальной машины (см. рисунок 9). Автоматически программа предлагает минимальный объем памяти в 2048 Мб. Он может быть оставлен без изменения, а в дальнейшей работе может быть скорректирован. Далее необходимо нажать кнопку «Next».

На следующем шаге требуется подключить новый или уже имеющийся виртуальный жесткий диск к новой виртуальной машине (см. рисунок 10). Жесткий диск представляет собой файл, который хранится в файловой системе операционной системы на персональном компьютере. Необходимо выбрать пункт «Создать новый виртуальный жесткий диск» и нажать кнопку «Создать».

При создании нового жесткого диска необходимо выбрать его тип (см. рисунок 11). Так как для запуска виртуальных машин будет использоваться

только программа Oracle VM VirtualBox, выбирается формат «VDI (VirtualBox Disk Image)». После выбора формата, необходимо нажать кнопку «Next».

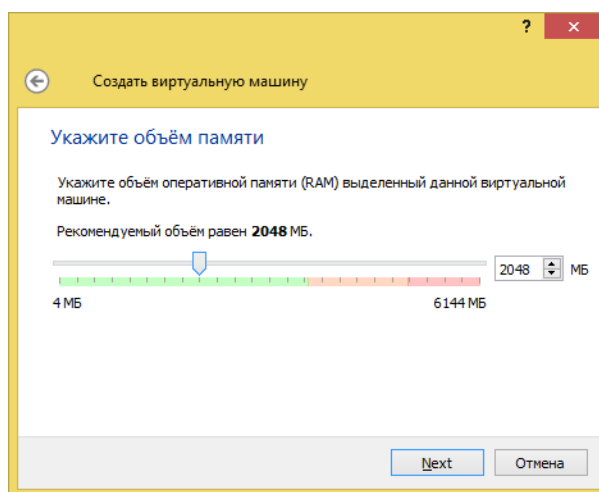


Рисунок 9 – Объем оперативной памяти виртуальной машины

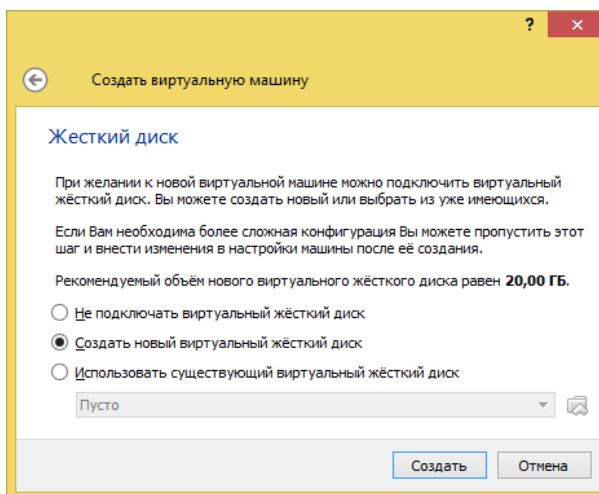


Рисунок 10 – Создание нового виртуального жесткого диска

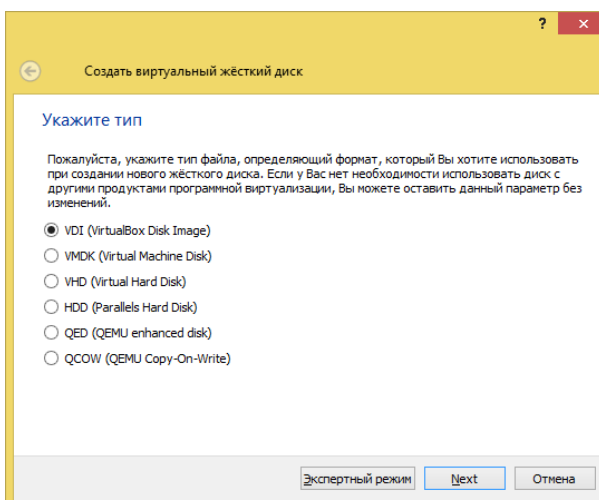


Рисунок 11 – Выбор типа виртуального жесткого диска

На следующем шаге необходимо выбрать формат для хранения данных (см. рисунок 12). В качестве формата, для экономии пространства на компьютере, выбирается «Динамический виртуальный жесткий диск». Размер такого диска может быть увеличен по мере его использования, но при этом он не превысит максимального размера, указанного при создании виртуального диска. После выбора формата, необходимо нажать кнопку «Next».

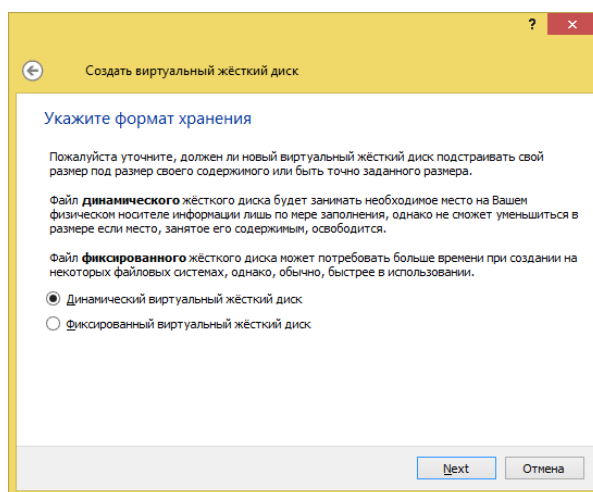


Рисунок 12 – Выбор формата хранения данных

В качестве имени нового виртуального жесткого диска указывается такое же имя, что и при создании новой виртуальной машины. Затем на шкале, показывающей объем создаваемого жесткого диска, указывается необходимое значение объема виртуального жесткого диска, например, равное 50 Гб. Формат хранения виртуального диска был выбран с целью оптимального расходования объема жесткого диска ПЭВМ, который будет использоваться для развертывания создаваемого стенда. Динамический диск при создании имеет минимальный размер и увеличивается по мере его заполнения информацией. Статический диск сразу занимает весь выделенный объем, при том что файл жесткого диска не заполнен информацией. После выбора имени и объема виртуального жесткого диска, нажимается кнопка «Создать» (см. рисунок 13).

После всех проделанных операций создается виртуальная машина с пустым виртуальным жестким диском и с неустановленным программным обеспечением.

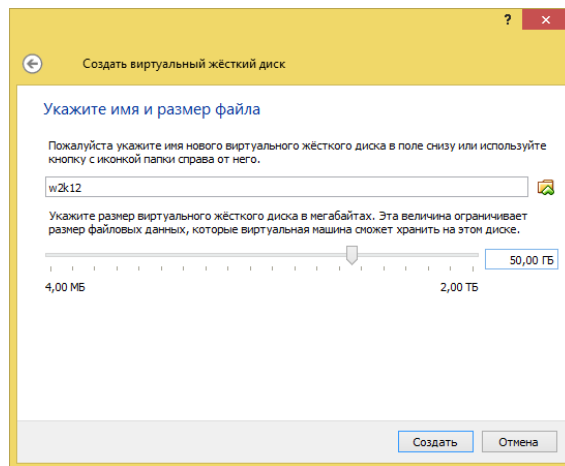


Рисунок 13 – Выбор имени и размера виртуального жесткого диска

После подготовки виртуальной машины выполняется установка гостевой операционной системы Windows Server 2012 R2 в соответствии с документацией разработчика Microsoft.

3.2.4 Создание виртуальной машины с установленной операционной системой Windows 8.1.

Создание виртуальной машины, с установленной ОС Windows 8.1, проводилось аналогично созданию виртуальных машин с установленными ОС Windows Server 2003 и Windows Server 2012 R2. В качестве имени записывается название гостевой операционной системы, например, Win81. Тип указывается – Microsoft Windows, версия – Windows 8.1, разрядность указывается 64-битная.

В качестве имени нового виртуального жесткого диска указывается такое же имя, что и при создании новой виртуальной машины. Затем на шкале указывается объем виртуального жесткого диска равный 20 Гб.

После всех проделанных операций создается виртуальная машина с пустым виртуальным жестким диском и с неустановленным программным обеспечением.

После подготовки виртуальной машины выполняется установка гостевой операционной системы Windows 8.1 в соответствии с документацией разработчика Microsoft.

3.3 Создание локальной сети, включающей виртуальные машины

После создания ВМ и установки на них ОС необходимо настроить ряд параметров функционирования ВМ и сетевое взаимодействие для всех созданных ВМ, поэтому следующим этапом создания лабораторного стенда является настройка параметров ВМ и объединение виртуальных машин в локальную сеть. Процесс настройки параметров подключения к локальной сети одинаковый независимо от версий гостевых ОС, установленных на ВМ. Поэтому подробное описание настройки локальной сети было рассмотрено на примере виртуальной машины, с установленной операционной системой Windows Server 2003.

Для настройки параметров ВМ и локальной сети необходимо запустить программу Oracle VM VirtualBox Менеджер на компьютере. Выбрать ВМ, щелкнув по ее имени в списке правой клавишей мыши. В открывшемся контекстном меню выбрать команду «Настроить». В диалоговом окне настроек необходимо выбрать раздел настроек «Общие», далее выбрать вкладку «Дополнительно». На вкладке «Дополнительно» необходимо настроить параметр «Общий буфер обмена», позволяющий выбрать режим копирования информации между гостевой и основной операционной системой. Для включения указанного режима буфера обмена необходимо установить значение параметра «Двунаправленный» (см. рисунок 14).

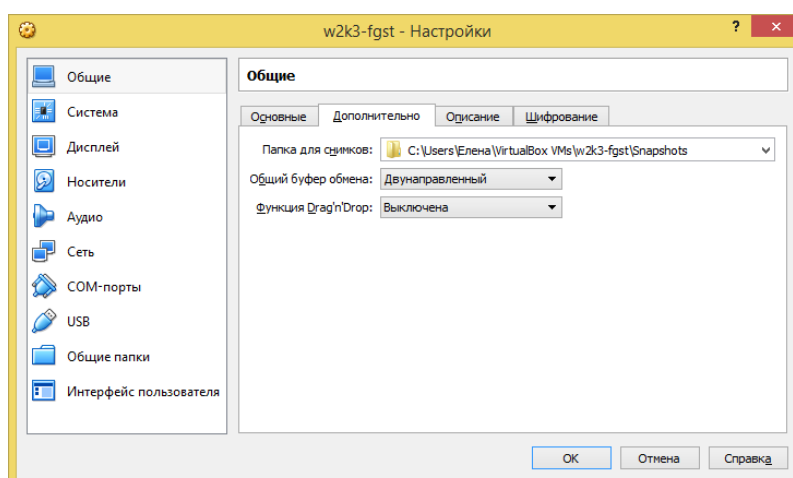


Рисунок 14 – Настройка буфера обмена

Далее необходимо осуществить настройку параметров локальной сети. Для этого нужно перейти в раздел настроек «Сеть». В этом разделе происходит настройка типа подключения и сетевого адаптера. Для настройки подключения указывается значение параметра «Тип подключения», позволяющий выбрать способ, которым виртуальный сетевой адаптер присоединяется к реальной сети хоста. Для создания локальной сети из ВМ надо выбрать значение «Внутренняя сеть». Затем осуществляется переход к дополнительным настройкам сетевого адаптера и для параметра «Неразборчивый режим» устанавливается значение из открывшегося контекстного меню «Разрешить всё». Тип адаптера из контекстного меню устанавливается – PCnet – FAST III (см. рисунок 15). Далее нажимается кнопка «ОК» для сохранения всех установленных параметров настройки.

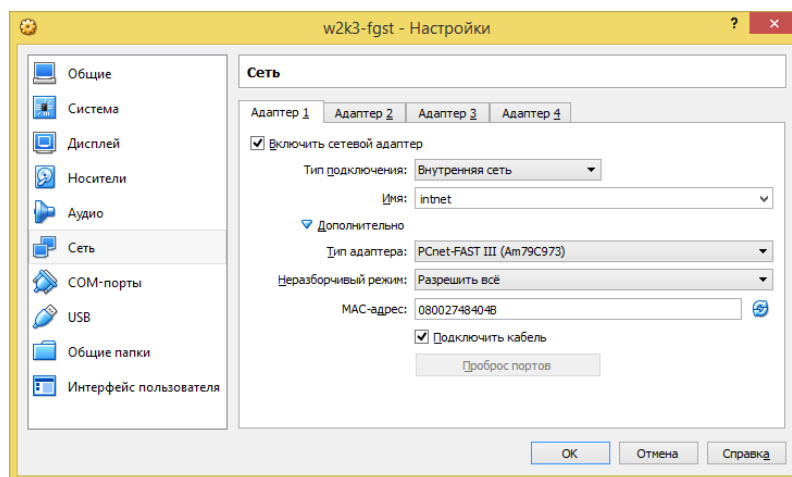


Рисунок 15 – Настройка сетевого адаптера

Для настройки общей папки необходимо перейти в раздел настроек «Общие папки». Общая папка настраивается для обмена основной и гостевой операционной системой. При настройке необходимо учесть то, что папка не должна размещаться на системном диске. Для создания необходимо щелкнуть правой клавишей мыши по «Папки машины» и в контекстном меню выбрать «Добавить общую папку» (см. рисунок 16). В открывшемся окне необходимо задать путь к папке и имя папки. Далее необходимо нажать «ОК» для сохранения созданной папки.

Далее необходимо нажать кнопку «ОК» для сохранения всех установленных параметров настройки.

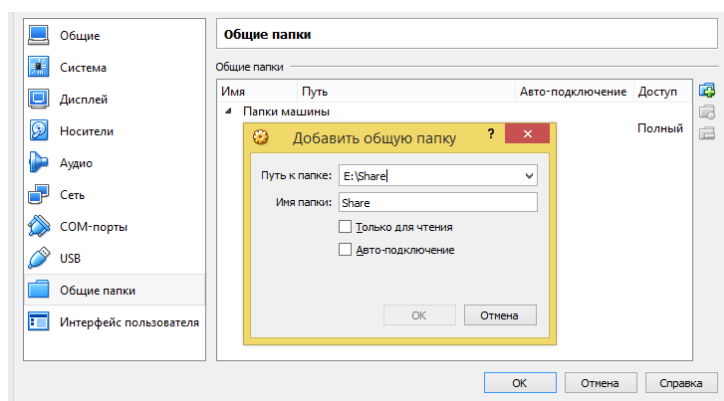


Рисунок 16 – Добавление общей папки

На следующем шаге была произведена настройка локальной сети для виртуальных машин с установленной операционной системой Windows 8.1 и с установленной операционной системой Windows Server Server 2012 R2. Тип адаптера выбирается в зависимости от гостевой ОС, установленной на виртуальной машине. Например, для виртуальной машины с установленной операционной системой Windows 8.1 был выбран тип адаптера – Intel PRO/1000 MT Desktop, а для виртуальной машины с установленной операционной системой Windows Server Server 2012 R2 – Intel PRO/1000 MT Server.

3.4 Настройка локальной сети средствами гостевой операционной системы

3.4.1 Настройка локальной сети средствами операционной системы Windows Server 2012 R2.

Для настройки локальной сети средствами ОС необходимо запустить ВМ с установленной операционной системой Windows Server 2012 R2 через программу Oracle VM VirtualBox Менеджер. Для этого необходимо выбрать виртуальную машину и на консоли меню выбрать «Запустить». После запуска виртуальной машины необходимо осуществить вход в учетную запись. Для этого посылается команда Ctrl – Alt – Del и вводится пароль для учетной записи. После того как запуск завершен необходимо выйти в меню Пуск и выбрать «Панель управления» (см. рисунок 17).

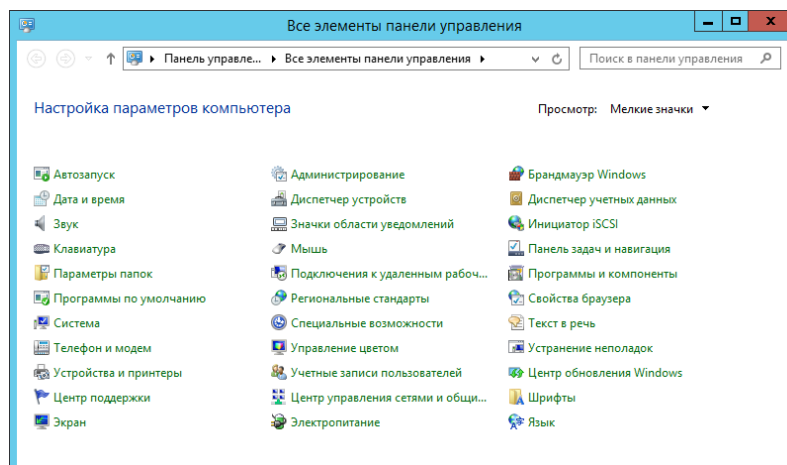


Рисунок 17 – Панель управления

В открывшемся окне необходимо выбрать «Центр управления сетями и общим доступом», а затем вкладку «Изменение параметров адаптера» (см. рисунок 18).

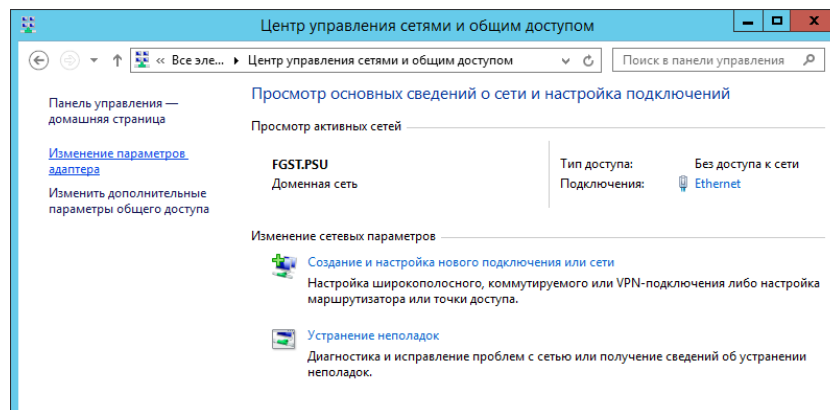


Рисунок 18 – Цент управления сетями и общим доступом

Для определения IP – адреса необходимо щелкнуть правой клавишей мыши по представленному сетевому подключению, и в контекстном меню выбрать «Свойства». В открывшемся окне из списка компонентов, использованных доменом, выбирать «Протокол Интернета версии 4 (TCP/IPv4)». Далее на консоли выбрать вкладку «Свойства», в открывшемся окне можно увидеть IP – адрес, присвоенный виртуальной машине. Для данной виртуальной машины был присвоен IP – адрес – 192.168.51.1 (см. рисунок 19). После того как все параметры проверены необходимо нажать кнопку «ОК» для первого окна и «Заккрыть» для второго окна соответственно.

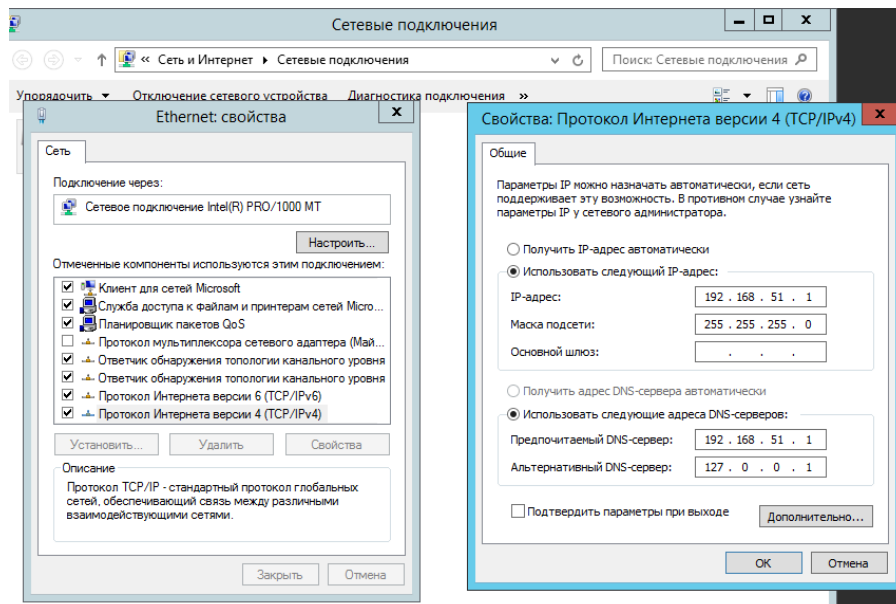


Рисунок 19 – Свойства сетевого подключения

Для настройки параметров общего доступа в окне «Центр управления сетями и общим доступом» необходимо выбрать вкладку «Изменить дополнительные параметры общего доступа». В открывшемся окне необходимо установить параметры общего доступа для сетевого обнаружения, путем включения сетевого обнаружения (см. рисунок 20). После внесенных изменений необходимо нажать «Сохранить изменения».

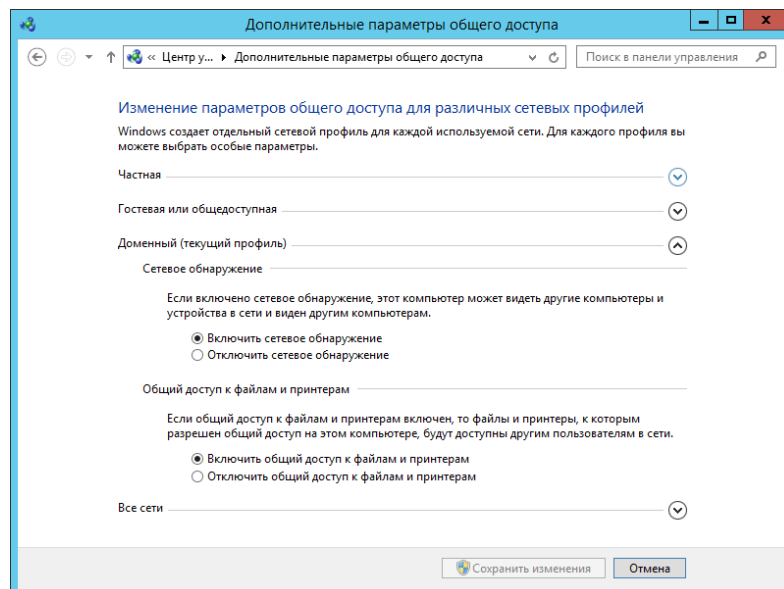


Рисунок 20 – Настройка параметров общего доступа

Далее необходимо запустить программу управления «Диспетчер серверов». Для этого нужно выйти в меню Пуск и выбрать «Диспетчер серверов». В открывшемся окне необходимо выбрать вкладку «Локальный

сервер» и проверить назначение адреса, и если все предыдущие параметры настройки были установлены верно, то в открывшемся окне будут представлены сведения о сервере (см. рисунок 21).

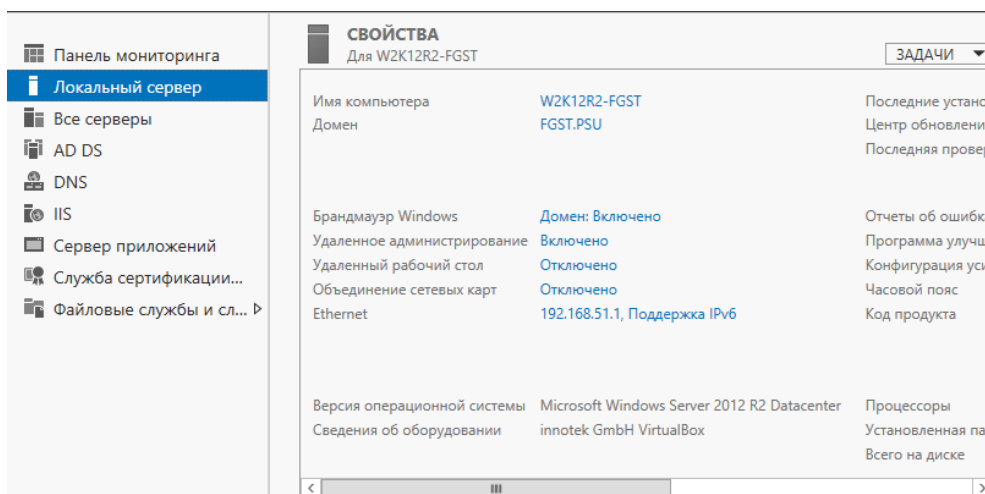


Рисунок 21 – Сведения о локальном сервере

Для того чтобы проверить работу локальной сети средствами операционной системы необходимо запустить в виртуальной машине командную строку. В открывшемся окне ввести команду «ipconfig /all». Если все команды по настройке локальной сети были выполнены правильно, то на экране, после выполнения команды, появятся сведения о настройке IP протокола, Ethernet adapter и туннельного адаптера (см. рисунок 22).

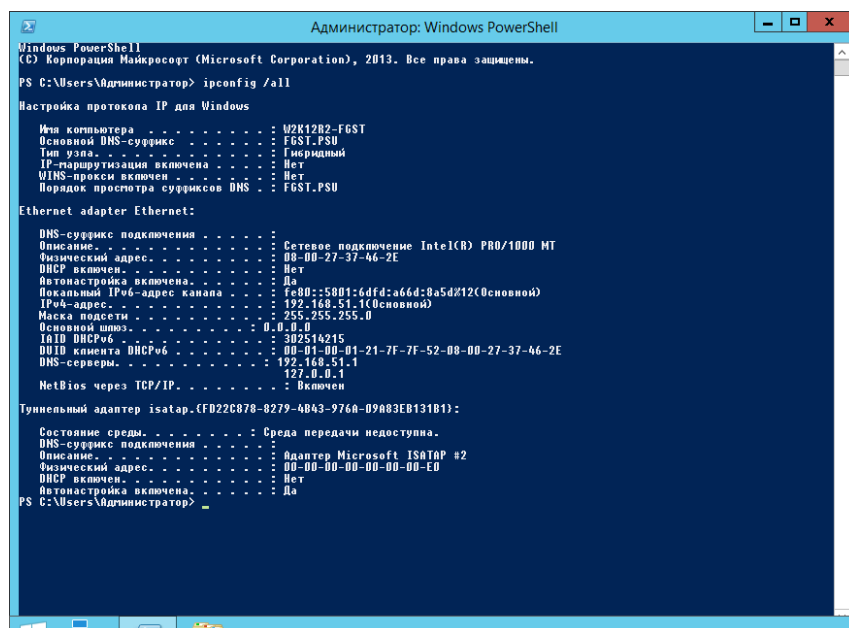


Рисунок 22 – Проверка настройки локальной средствами гостевой ОС Windows Server 2012 R2

3.4.2 Настройка локальной сети средствами гостевой операционной системы Windows Server 2003 R2.

Для настройки локальной сети средствами операционной системы необходимо запустить виртуальную машину с установленной операционной системой Windows Server 2003 R2 через программу Oracle VM VirtualBox Менеджер. Для этого необходимо выбрать виртуальную машину и на консоли меню выбрать «Запустить». После запуска виртуальной машины необходимо осуществить вход в учетную запись. Для этого посылается команда Ctrl – Alt – Del и вводится пароль для учетной записи.

После того как запуск завершен необходимо выйти в меню Пуск и выбрать «Панель управления». В контекстном меню выбирать «Сетевые подключения» и «Подключения по локальной сети». В открывшемся окне в разделе «Общие» выбрать «Свойства» (см. рисунок 23).

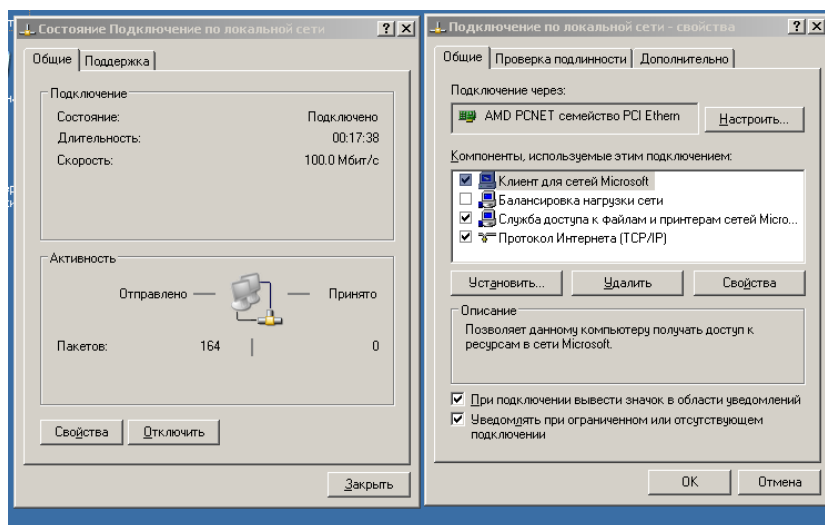


Рисунок 23 – Свойства подключения по локальной сети

В открывшемся окне из списка компонентов, использованных этим подключением, выбрать «Протокол Интернета (TCP/IP)». Далее на консоли выбрать вкладку «Свойства», в открывшемся окне можно увидеть IP – адрес, присвоенный виртуальной машине. Для данной виртуальной машины был присвоен IP – адрес – 192.168.51.2 (см. рисунок 24). После того как все параметры проверены необходимо нажать кнопку «ОК» для первого окна и «Заккрыть» для второго окна соответственно.

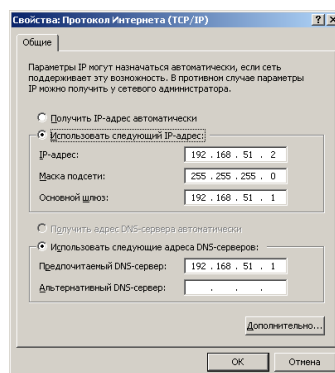


Рисунок 24 – Свойства сетевого подключения

Для того чтобы проверить работу локальной сети средствами операционной системы необходимо запустить в виртуальной машине командную строку. В открывшемся окне ввести команду «ipconfig /all». Если все команды по настройке локальной сети были выполнены правильно, то на экране, после выполнения команды, появятся сведения о настройке IP протокола, Ethernet adapter (см. рисунок 25).

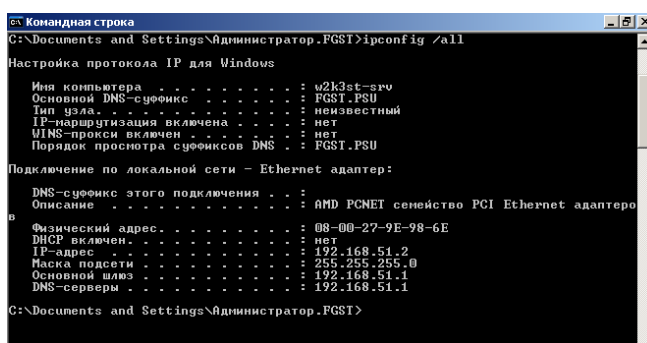


Рисунок 25 – Проверка настройки локальной сети средствами гостевой ОС Windows Server 2003 R2

3.4.3 Настройка локальной сети средствами гостевой операционной системы Windows 8.1.

Для настройки локальной сети средствами операционной системы необходимо запустить виртуальную машину с установленной операционной системой Windows 8.1 через программу Oracle VM VirtualBox Менеджер. Для этого необходимо выбрать виртуальную машину и на консоли меню выбрать «Запустить». После запуска виртуальной машины необходимо осуществить вход в учетную запись. Для этого необходимо послать команду Ctrl – Alt – Del и ввести пароль для учетной записи. После того как запуск завершен

необходимо выйти в меню Пуск, далее «Приложения» и из списка всех приложений выбрать «Панель управления».

В открывшемся окне необходимо выбрать «Центр управления сетями и общим доступом» и выбрать вкладку «Изменение параметров адаптера» (см. рисунок 26).

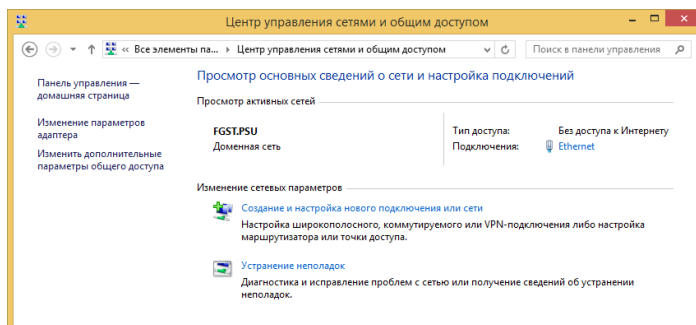


Рисунок 26 – Центр управления сетями и общим доступом

В открывшемся окне щелкнуть правой клавишей мыши по представленному сетевому подключению, и в контекстном меню выбрать «Свойства». В открывшемся окне из списка компонентов, использованных доменом, выбрать «Протокол Интернета версии 4 (TCP/IPv4)». Далее на консоли выбрать вкладку «Свойства», в открывшемся окне можно увидеть IP – адрес, присвоенный виртуальной машине. Для данной виртуальной машины был присвоен IP – адрес – 192.168.51.11 (см. рисунок 27). После того как все параметры проверены необходимо нажать кнопку «ОК» для первого окна и «Заккрыть» для второго окна соответственно.

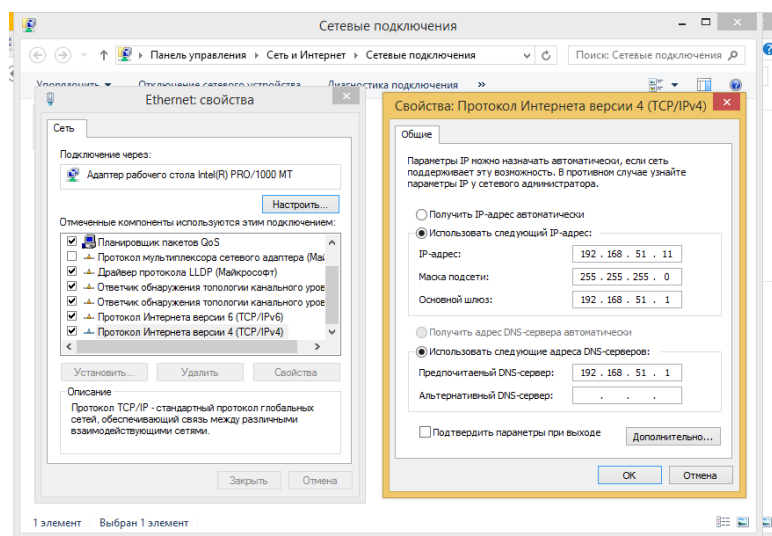


Рисунок 27 – Свойства сетевого подключения

Для настройки параметров общего доступа в окне «Центр управления сетями и общим доступом» выбрать вкладку «Изменить дополнительные параметры общего доступа». В открывшемся окне необходимо установить параметры общего доступа для сетевого обнаружения, путем включения сетевого обнаружения. После внесенных изменений необходимо нажать «Сохранить изменения» (см. рисунок 28).

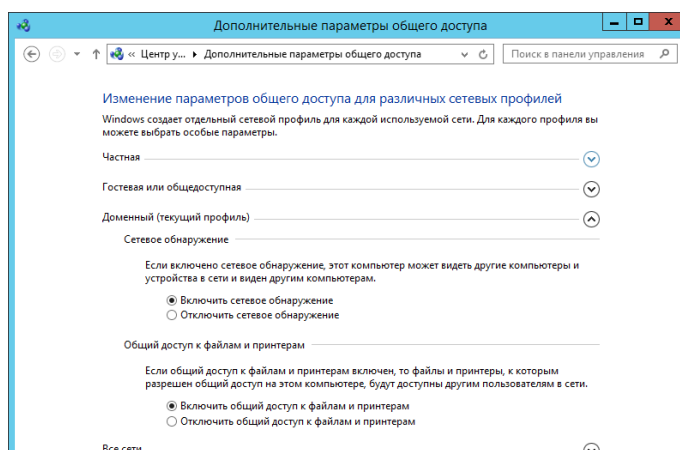


Рисунок 28 – Параметры общего доступа

Для того чтобы проверить работу локальной сети средствами операционной системы необходимо запустить в виртуальной машине командную строку. В открывшемся окне ввести команду «ipconfig /all». Если все команды по настройке локальной сети были выполнены правильно, то на экране, после выполнения команды, появятся сведения о настройке IP протокола, Ethernet adapter и туннельного адаптера (см. рисунок 29).

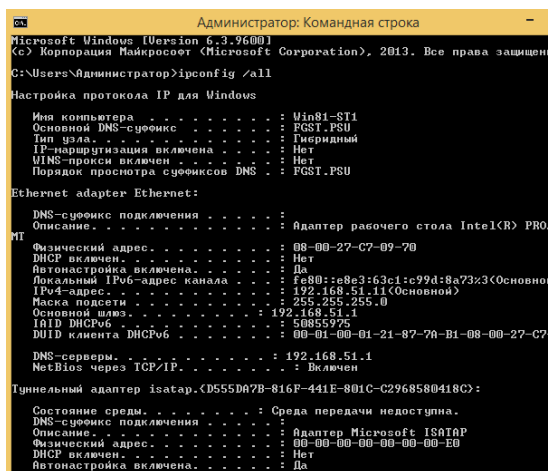
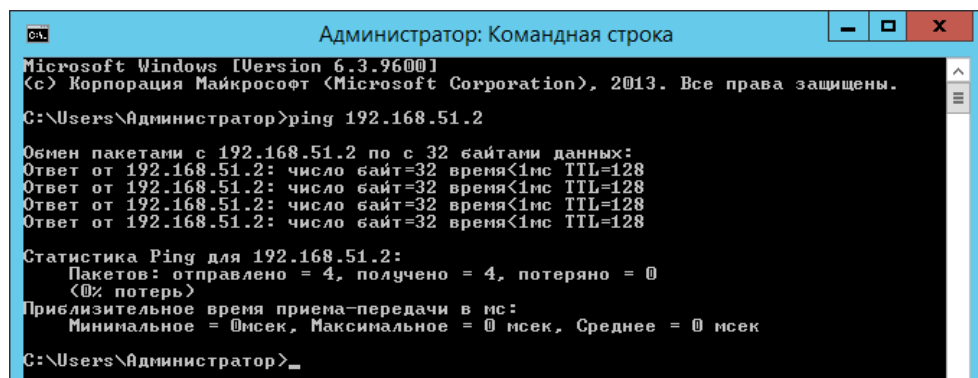


Рисунок 29 – Проверка настройки локальной сети средствами гостевой ОС Windows 8.1

3.4.4 Проверка работоспособности локальной сети.

Для проверки функционирования локальной сети, настроенной средствами операционной системы, необходимо запустить все виртуальные машины, а именно виртуальную машину с установленной операционной системой Windows Server 2012 R2, с установленной гостевой операционной системой Windows Server 2003 R2 и с установленной операционной системой Windows 8.1. На каждой виртуальной машине запускается командная строка.

На виртуальной машине с установленной операционной системой Windows Server 2012 R2 в командной строке выполняется команда «ping», и в конце команды дописывается IP – адрес другой виртуальной машины, например, виртуальной машины, с установленной гостевой операционной системой Windows Server 2003 R2. Получается команда «ping 192.168.51.2». Если обмен пакетами между виртуальными машинами происходит, значит, локальная сеть настроена (см. рисунок 30).



```
Администратор: Командная строка
Microsoft Windows [Version 6.3.9600]
(c) Корпорация Майкрософт (Microsoft Corporation), 2013. Все права защищены.

C:\Users\Администратор>ping 192.168.51.2

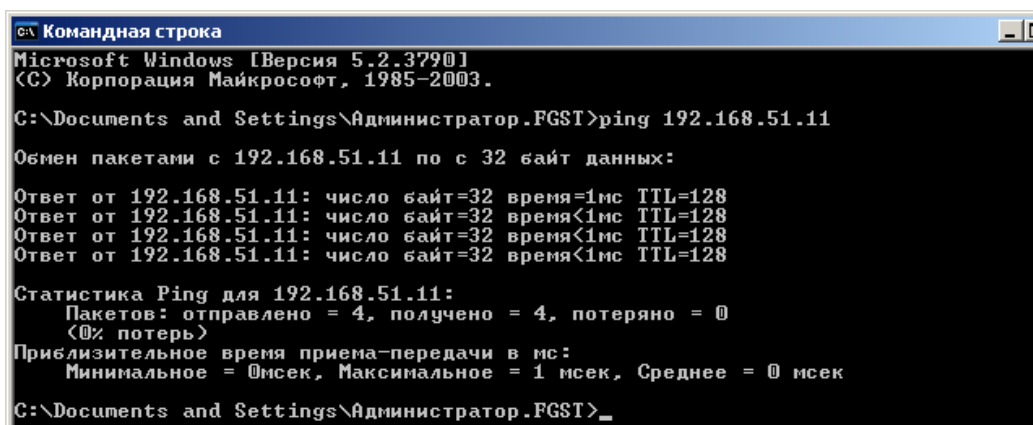
Обмен пакетами с 192.168.51.2 по 32 байтами данных:
Ответ от 192.168.51.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.51.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.51.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.51.2: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.51.2:
    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>
```

Рисунок 30 – Проверка функционирования локальной сети на ВМ с установленной ОС Windows Server 2012 R2

Далее, на виртуальной машине с установленной операционной системой Windows Server 2003 R2 в командной строке выполняется команда «ping», и в конце команды дописывается IP – адрес другой виртуальной машины, например, виртуальной машины, с установленной гостевой операционной системой Windows 8.1. Получается команда «ping 192.168.51.11» (см. рисунок 31). Локальная сеть настроена правильно.



```
С:\ Командная строка
Microsoft Windows [Версия 5.2.3790.1
(C) Корпорация Майкрософт, 1985-2003.

C:\Documents and Settings\Администратор.FGST>ping 192.168.51.11

Обмен пакетами с 192.168.51.11 по 32 байт данных:

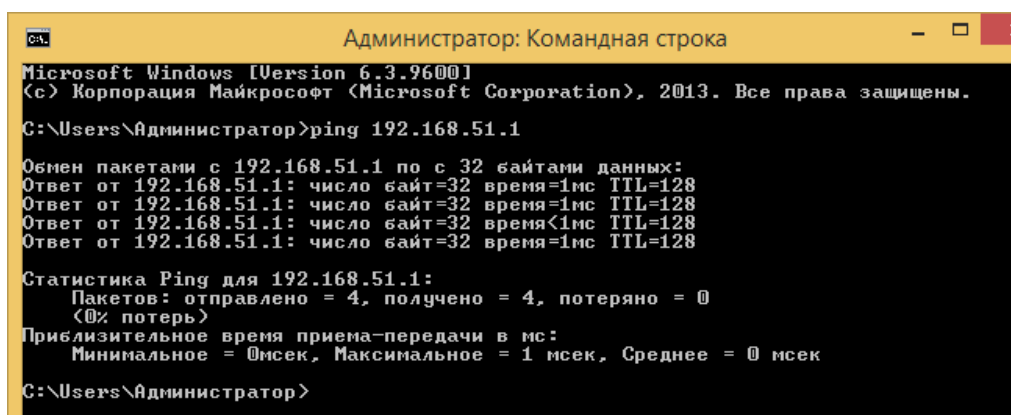
Ответ от 192.168.51.11: число байт=32 время=1мс TTL=128
Ответ от 192.168.51.11: число байт=32 время<1мс TTL=128
Ответ от 192.168.51.11: число байт=32 время<1мс TTL=128
Ответ от 192.168.51.11: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.51.11:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 1 мсек, Среднее = 0 мсек

C:\Documents and Settings\Администратор.FGST>
```

Рисунок 31 – Проверка функционирования локальной сети на VM с установленной ОС Windows Server 2003 R2

Далее, на виртуальной машине с установленной операционной системой Windows 8.1 в командной строке выполняется команда «ping», и в конце команды дописывается IP – адрес другой виртуальной машины, например, виртуальной машины, с установленной гостевой операционной системой Windows Server 2012 R2 . Получается команда «ping 192.168.51.1» (см. рисунок 32). Локальная сеть настроена правильно.



```
Администратор: Командная строка
Microsoft Windows [Version 6.3.9600.1
(c) Корпорация Майкрософт (Microsoft Corporation), 2013. Все права защищены.

C:\Users\Администратор>ping 192.168.51.1

Обмен пакетами с 192.168.51.1 по 32 байтами данных:
Ответ от 192.168.51.1: число байт=32 время=1мс TTL=128
Ответ от 192.168.51.1: число байт=32 время=1мс TTL=128
Ответ от 192.168.51.1: число байт=32 время<1мс TTL=128
Ответ от 192.168.51.1: число байт=32 время=1мс TTL=128

Статистика Ping для 192.168.51.1:
    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 32 –Проверка функционирования локальной сети на VM с установленной ОС Windows 8.1

3.5 Установка ролей и компонентов гостевых ОС

3.5.1 Установка ролей и компонентов гостевой операционной системы Windows Server 2012 R2.

Для начала необходимо осуществить вход в виртуальную машину, с установленной операционной системой Windows Server 2012 R2, через программу Oracle VM VirtualBox Менеджер. После запуска виртуальной

машины необходимо осуществить вход в учетную запись. Для этого посылается команда Ctrl – Alt – Del и вводится пароль для учетной записи.

Далее необходимо осуществить вход в «Диспетчер серверов», для этого нужно выйти в меню Пуск и выбрать «Диспетчер серверов». В открывшемся меню необходимо открыть вкладку «Панель мониторинга». Для установки ролей и компонентов операционной системы необходимо перейти по вкладке «Добавить роли и компоненты» (см. рисунок 33).

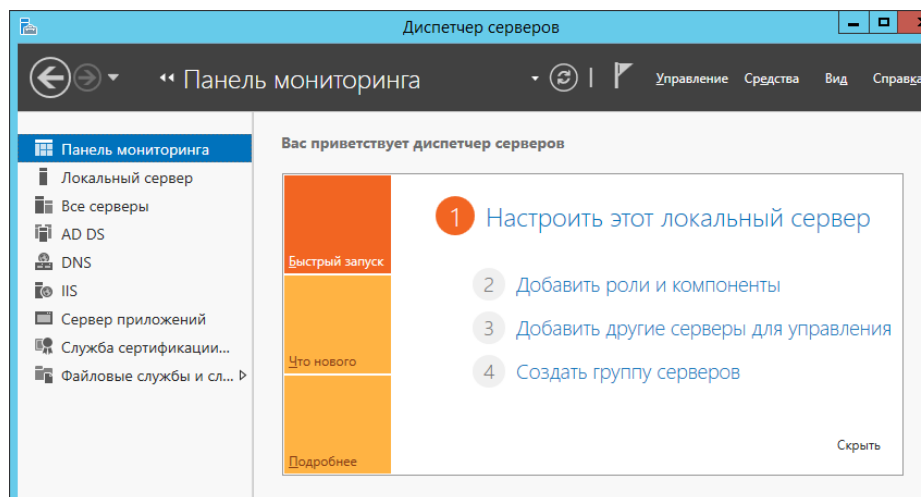


Рисунок 33 – Установка ролей и компонентов

Для настройки необходимо выбрать тип установки, а именно «Установка ролей и компонентов» и нажать «Далее» (см. рисунок 34). Затем необходимо выбрать сервер и нажать «Далее». Установка ролей и компонентов осуществляется поочередно:

а) устанавливается DNS – сервер, обеспечивающий разрешение имен для сетей TCP/IP. DNS – сервер устанавливается на том же сервере, что и доменные службы Active Directory;

б) устанавливается веб – сервер (IIS). Веб – сервер представляет надежную, управляемую и масштабируемую инфраструктуру веб – приложений;

в) устанавливается сервер приложений, обеспечивающий централизованное управление и размещение высокопроизводительных распределенных приложений;

г) устанавливаются службы Active Directory, позволяющие хранить сведения об объектах сети, а также предназначенные для создания центров сертификации.

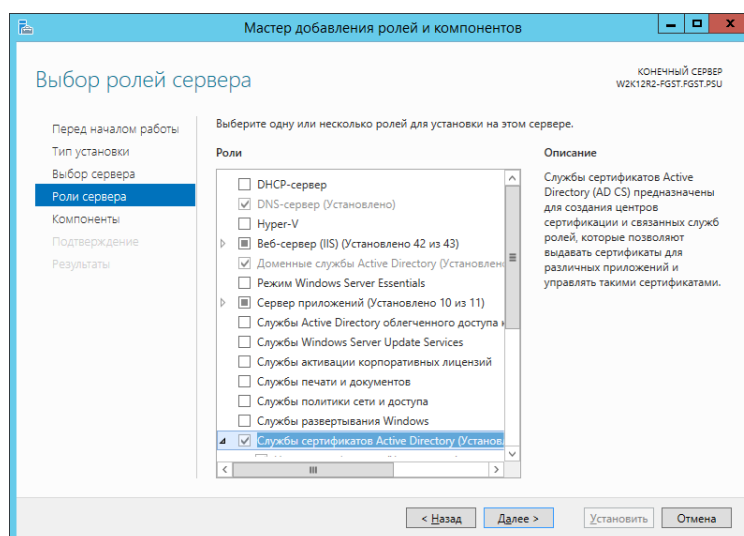


Рисунок 34 – Установка ролей и компонентов

После установки служб Active Directory VM с гостевой ОС Windows Server 2012 R2 назначается роль первичного контроллера домена.

Далее после установки ролей необходимо установить дополнительные компоненты. Из списка компонент, которые могут быть установлены на VM с гостевой ОС Windows Server 2012 R2, были выбраны и установлены следующие компоненты (см. рисунок 35):

- Windows PowerShell, позволяющий автоматизировать локальное и удаленное администрирование Windows;
- службы очереди сообщений, гарантирующие доставку сообщений, безопасность и передачу сообщений между приложениями;
- пользовательские интерфейсы.

После подтверждения всех действий были установлены роли и компоненты гостевой операционной системы Windows Server 2012 R2.

Для настройки DNS необходимо осуществить вход в «Диспетчер серверов». Затем нажать «Средства» и выбрать из выпадающего списка «DNS». На вкладке «Действия» необходимо выбрать «Настроить DNS – сервер». При установке «DNS» были установлены такие параметры, как создание зоны

прямого просмотра, чтобы данная зона сохранялась в Active Directory, данный DNS должен быть реализован для всех DNS – серверов, работающих на контроллере домена в этом домене, задать имя для зоны, например, fgst.psu. Виртуальной машине с установленной гостевой операционной системы Windows Server 2012 R2 был присвоен DNS – 192.168.51.1.

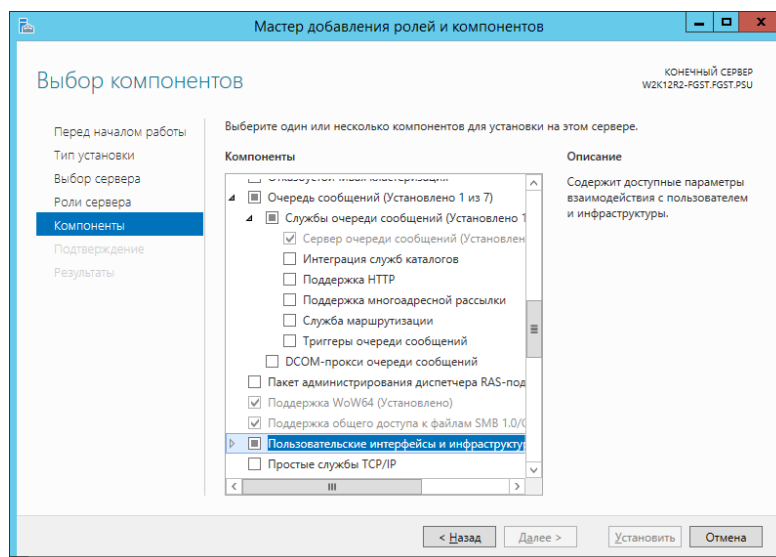


Рисунок 35 – Установка ролей и компонентов

3.5.2 Установка ролей и компонентов гостевой операционной системы Windows Server 2003 R2.

Для начала необходимо осуществить вход в виртуальную машину, с установленной операционной системой Windows Server 2003 R2, через программу Oracle VM VirtualBox Менеджер. После запуска виртуальной машины необходимо осуществить вход в учетную запись. Для этого посылается команда Ctrl – Alt – Del и вводится пароль для учетной записи. После того как запуск завершен необходимо войти в меню Пуск и выбрать «Управление данными сервера». В открывшемся окне в разделе «Управление ролями данного сервера» нажать «Добавить роль». В открывшемся окне установлены следующие роли сервера (см.рисунок 36):

- сервер приложений (IIS, ASP.NET), обеспечивающий базовые технологии для работы веб – приложений и распределенных приложений;
- почтовый сервер, обеспечивающий доставку на почтовых сервисах электронной почты.

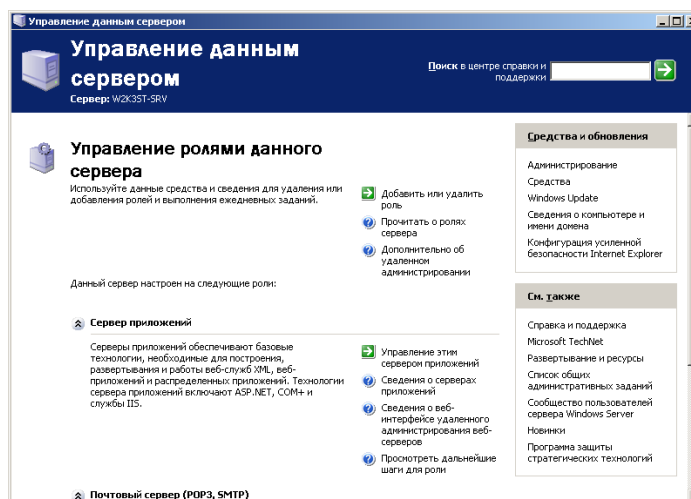


Рисунок 36 – Установка ролей и компонентов

Сервер включается в состав домена в качестве компьютера, домена.

Виртуальной машине с установленной гостевой операционной системы Windows Server 2003 R2 был присвоен IP–адрес 192.168.51.2.

3.5.3 Установка ролей и компонентов гостевой операционной системы Windows 8.1.

Для начала необходимо осуществить вход в виртуальную машину, с установленной операционной системой Windows 8.1, через программу Oracle VM VirtualBox Менеджер. После запуска виртуальной машины необходимо осуществить вход в учетную запись. Для этого посылается команда Ctrl – Alt – Del и вводится пароль для учетной записи.

Далее необходимо осуществить вход в «Компоненты Windows» через меню Пуск и осуществить установку компонентов Windows (см. рисунок 37).

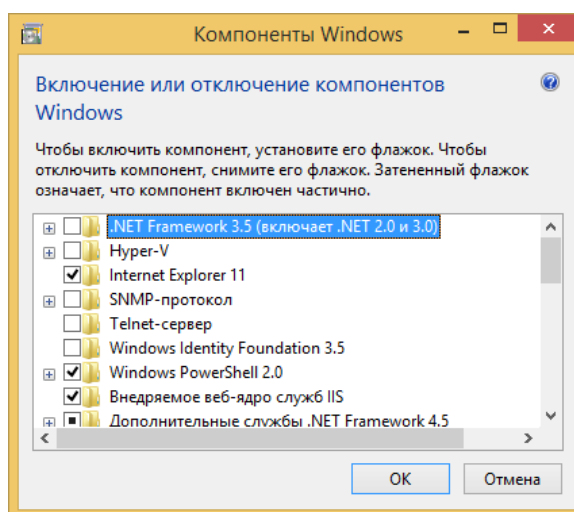


Рисунок 37 – Установка компонентов Windows 8.1

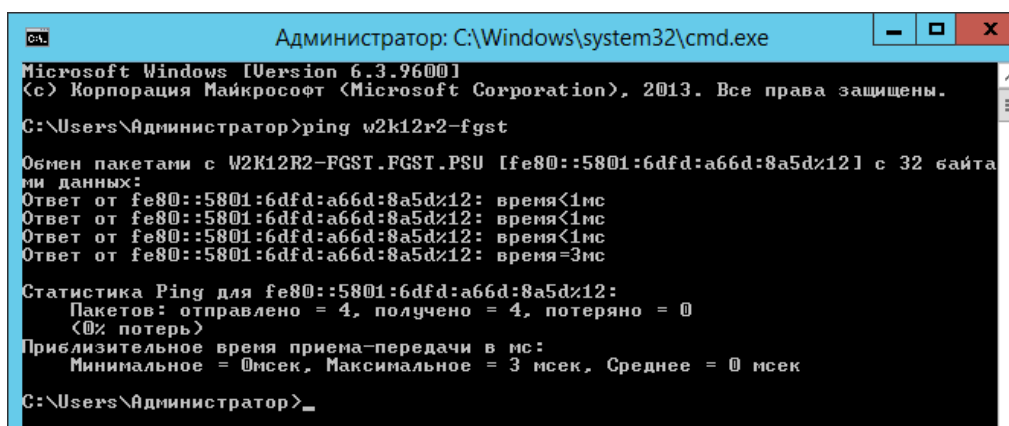
Для настройки DNS в главном меню необходимо выбрать пункт «Панель управления» — «Сетевые подключения», а затем правой кнопкой мыши щелкнуть по пункту «Подключение по локальной сети». Из контекстного меню выбрать «Свойства» и в окне свойств подключения к локальной сети выбрать пункт «Протокол сети Интернет TCP/IP», а далее «Свойства». В открывшемся окне свойств протокола TCP/IP в поле «Предпочитаемый сервер DNS» был введен IP-адрес сервера 192.168.51.11, после чего последовательным нажатием на кнопку «ОК» были закрыты все окна.

На операционную систему Windows 8.1 устанавливается DNS – клиент и компьютер включается в состав домена.

3.5.4 Проверка локальной сети после установки компонентов гостевой операционной системы.

Осуществляется проверка локальной сети после установки компонентов гостевой операционной системы. Для этого на каждой виртуальной машине запускается командная строка.

На виртуальной машине с установленной операционной системой Windows Server 2012 R2 в командной строке выполняется команда «ping», и в конце команды дописывается DNS – имя виртуальной машины, например, получается команда «ping w2k12r2-fgst» (см. рисунок 38). IP – адрес транслируется, значит, проверка прошла.



```
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 w2k12r2-fgst

Обмен пакетами с W2K12R2-FGST.FGST.PSU [fe80::5801:6dfd:a66d:8a5d%12] с 32 байта
ми данных:
Ответ от fe80::5801:6dfd:a66d:8a5d%12: время<1мс
Ответ от fe80::5801:6dfd:a66d:8a5d%12: время<1мс
Ответ от fe80::5801:6dfd:a66d:8a5d%12: время<1мс
Ответ от fe80::5801:6dfd:a66d:8a5d%12: время=3мс

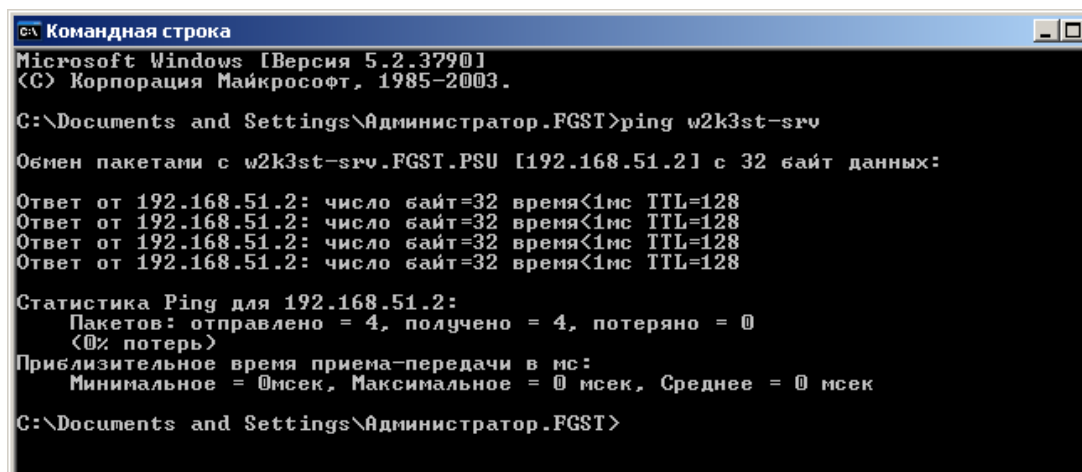
Статистика Ping для fe80::5801:6dfd:a66d:8a5d%12:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    <0% потеря>
    Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 3 мсек, Среднее = 0 мсек

C:\Users\Администратор>
```

Рисунок 38 – Проверка функционирования локальной сети ВМ
Windows Server 2012 R2

На виртуальной машине с установленной операционной системой Windows Server 2003 R2 в командной строке выполняется команда «ping», и в конце команды дописывается DNS – имя виртуальной машины, например, получается команда «ping w2k3st-srv» (см. рисунок 39). IP – адрес транслируется, значит, проверка прошла.

На виртуальной машине с установленной операционной системой Windows 8.1 в командной строке выполняется команда «ping», и в конце команды дописывается DNS – имя виртуальной машины, например, получается команда «ping win81-st1» (см. рисунок 40). IP – адрес транслируется, значит, проверка прошла.



```
С:\ Командная строка
Microsoft Windows [Версия 5.2.3790]
(C) Корпорация Майкрософт, 1985-2003.

C:\Documents and Settings\Администратор.FGST>ping w2k3st-srv

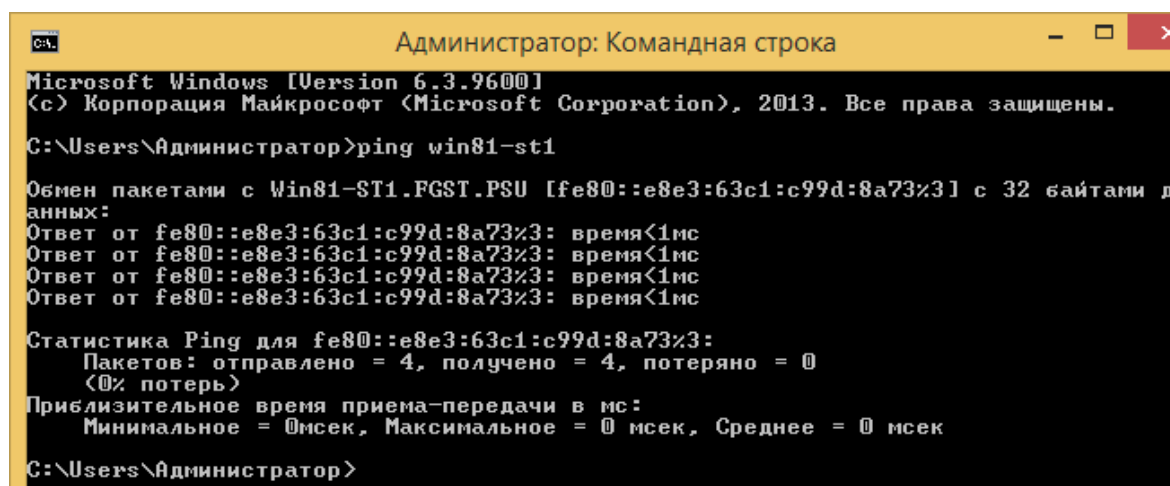
Обмен пакетами с w2k3st-srv.FGST.PSU [192.168.51.2] с 32 байт данных:

Ответ от 192.168.51.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.51.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.51.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.51.2: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.51.2:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек

C:\Documents and Settings\Администратор.FGST>
```

Рисунок 39 – Проверка функционирования локальной сети ВМ
Windows Server 2003 R2



```
Администратор: Командная строка
Microsoft Windows [Version 6.3.9600]
(c) Корпорация Майкрософт (Microsoft Corporation), 2013. Все права защищены.

C:\Users\Администратор>ping win81-st1

Обмен пакетами с Win81-ST1.FGST.PSU [fe80::e8e3:63c1:c99d:8a73%3] с 32 байтами д
анных:
Ответ от fe80::e8e3:63c1:c99d:8a73%3: время<1мс
Ответ от fe80::e8e3:63c1:c99d:8a73%3: время<1мс
Ответ от fe80::e8e3:63c1:c99d:8a73%3: время<1мс
Ответ от fe80::e8e3:63c1:c99d:8a73%3: время<1мс

Статистика Ping для fe80::e8e3:63c1:c99d:8a73%3:
    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 40 – Проверка функционирования локальной сети ВМ
Windows 8.1

3.6 Установка системы контроля и предотвращения утечек информации Falcongaze SecureTower

Установка осуществляется в соответствии с руководством администратора, входящим в комплект документации. Серверная часть системы контроля и предотвращения утечек информации устанавливается на виртуальную машину с установленной операционной системой Windows Server 2012 R2. На эту же ВМ были установлены компоненты управления Falcongaze SecureTower (см. рисунок 41).

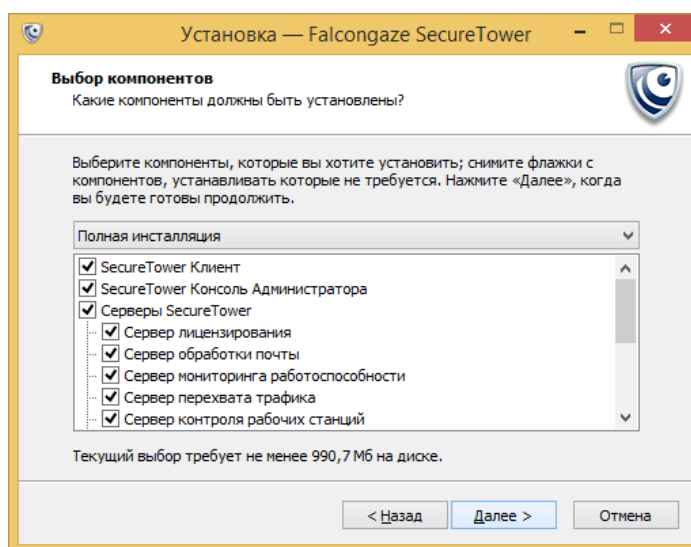


Рисунок 41 – Установка компонентов Falcongaze SecureTower

На виртуальную машину с установленной операционной системой Windows Server 2003 R2 компоненты системы контроля и предотвращения утечек информации Falcongaze SecureTower устанавливаться не будет. На данную виртуальную машину была установлена БД Microsoft SQL Express 2008. Эта БД нужна для работы серверной части Falcongaze SecureTower. Ее можно устанавливать на тот же сервер, что СК и ПУИ Falcongaze SecureTower, Однако при создании лабораторного стенда был выбран вариант организации сети с установкой БД и Falcongaze SecureTower на разных серверах. То есть в качестве сервера для БД Microsoft SQL Express будет использоваться виртуальная машина с установленной операционной системой Windows Server 2003 R2.

Установка клиентской части Falcongaze SecureTower будет произведена на виртуальную машину с установленной операционной системой Windows 8.1.

После установки программного обеспечения была проверена работоспособность посредством подключения сервера Falcongaze SecureTower. Подключение выполнилось, все компоненты работают корректно, сбоев не происходит (см. рисунок 42).

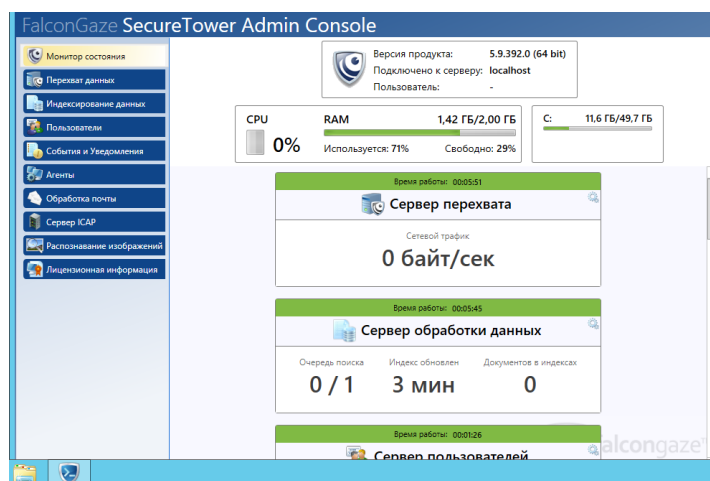


Рисунок 42 – Проверка работоспособности Falcongaze SecureTower

3.7 Результат создания виртуального стенда

В результате описанных в параграфах 3.1 – 3.6 действий был разработан виртуальный стенд, включающий следующие виртуальные машины:

- виртуальная машина с установленной операционной системой Windows Server 2012 R2 с именем w2k12r2 – fgst и установленной серверной частью системы контроля и предотвращения утечек информации Falcongaze SecureTower;

- виртуальная машина с установленной операционной системой Windows Server 2003 R2 с именем w2k3st – srv и с установленной БД Microsoft SQL Express;

- виртуальная машина с установленной операционной системой Windows 8.1 с именем win81 – st1 и установленной клиентской частью системы контроля и предотвращения утечек информации Falcongaze SecureTower.

Состав виртуального стенда, используемого при выполнении практикума, представлен в приложении А.

4 Порядок выполнения задания по применению программного комплекса Falcongaze SecureTower

4.1 Установка консоли Falcongaze SecureTower на виртуальную машину с установленной операционной системой Windows 8.1

4.1.1 Подготовительный этап перед установкой программного обеспечения.

Так как установка агентов происходит в рабочей группе на Windows 8.1, то необходимо отключить на них UAC (User Account Control – Контроль учётных записей пользователей). Для этого необходимо зайти в «Параметры управления учетными записями пользователей» и опустить ползунок на отметку «Никогда не уведомлять» (см. рисунок 43).

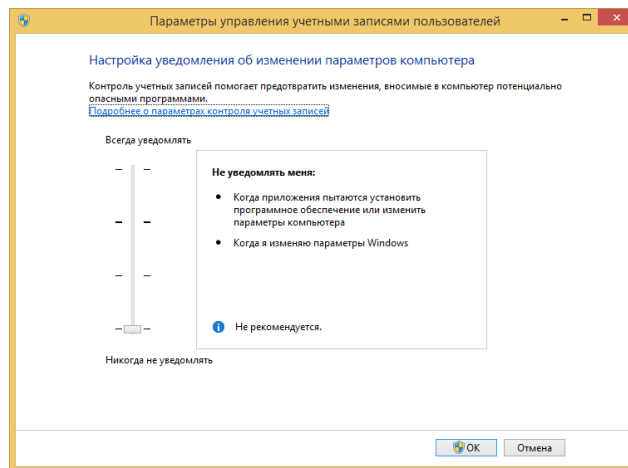


Рисунок 43 – Отключение контроля учетных записей пользователей

На следующем шаге включить обнаружения и доступа к файлам и принтерам, для этого необходимо в окне «Центр управления сетями и общим доступом» выбрать вкладку «Изменить дополнительные параметры общего доступа». В открывшемся окне необходимо установить параметры общего доступа для сетевого обнаружения, путем включения сетевого обнаружения. После внесенных изменений необходимо нажать «Сохранить изменения» (см. рисунок 44).

Далее в расширенных настройках брандмауэра Windows для входящих соединений проверить, чтобы там были включены правила «Общий доступ к файлам и принтерам для IPv4 и IPv6». Для этого необходимо запустить

«Панель управления – Брандмауэр Windows – Дополнительные параметры – Правила для входящих соединений» и проверить включение правил (см. рисунок 45).

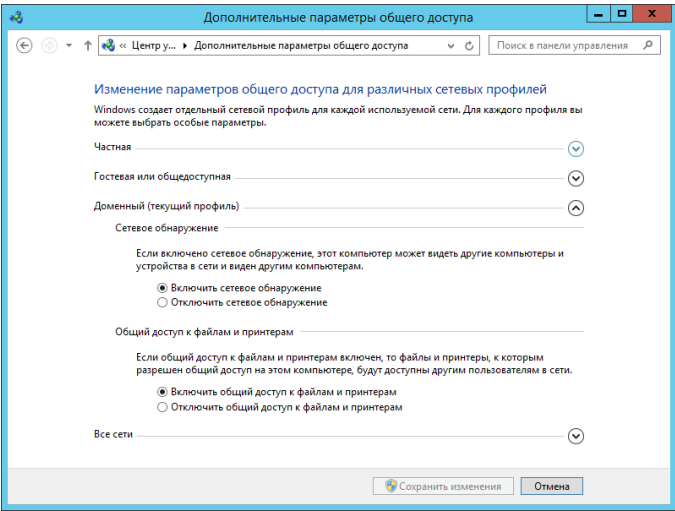


Рисунок 44 – Параметры общего доступа

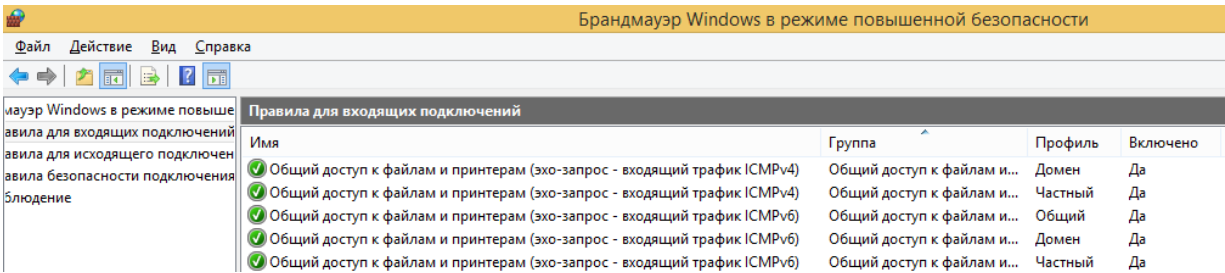


Рисунок 45 – Правила для входящих соединений

4.1.2 Установка компонентов программного комплекса Falcongaze SecureTower.

В папке с комплектом поставки программного комплекса SecureTower на компьютер необходимо установить из папки Common все необходимые приложения (Microsoft Visual C++ 2008/2010/2015 и Microsoft .NET Framework) для обеспечения работы его компонентов. После проделанной установки необходимо запустить исполнительный файл Мастера установки FalcongazeSecureTowerSetup.exe и выбрать язык установки в открывшемся диалоговом окне.

Ознакомиться с версией программного продукта и рекомендациями по установке и нажать «Далее» для продолжения установки программного комплекса (см. рисунок 46).

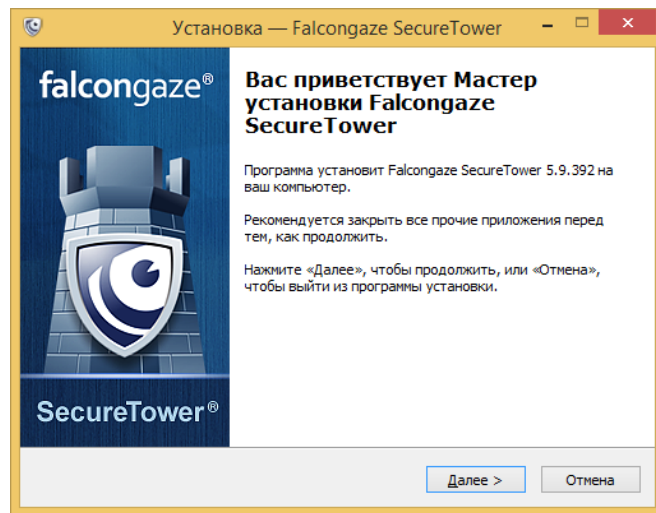


Рисунок 46 – Установка Falcongaze SecureTower

Далее необходимо принять условия лицензионного соглашения и нажать «Далее». Выбрать папку для установки и нажать «Далее». Убедиться, что выбраны все компоненты для установки Falcongaze SecureTower и нажать «Далее» (см. рисунок 47).

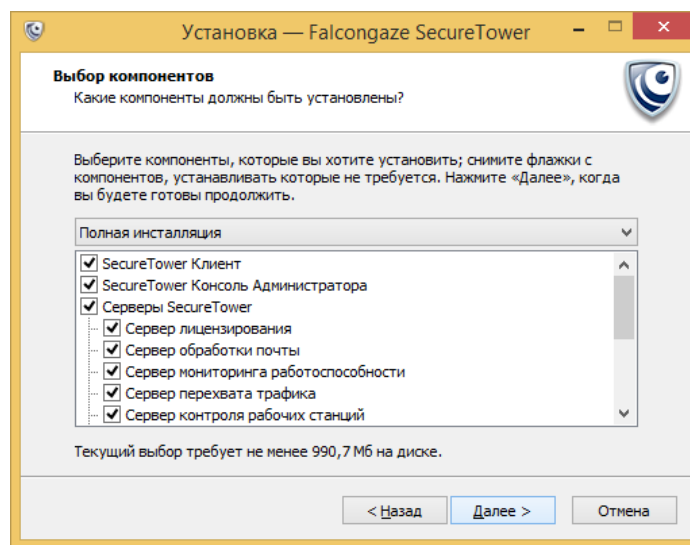


Рисунок 47 – Выбор компонентов для установки

Нажать «Далее» для размещения ярлыков в папке меню Пуск и на рабочем столе компьютера

Ознакомиться с итоговыми настройками и нажать «Установить» (см. рисунок 48).

После завершения установки необходимо нажать «Завершить» (см. рисунок 49).

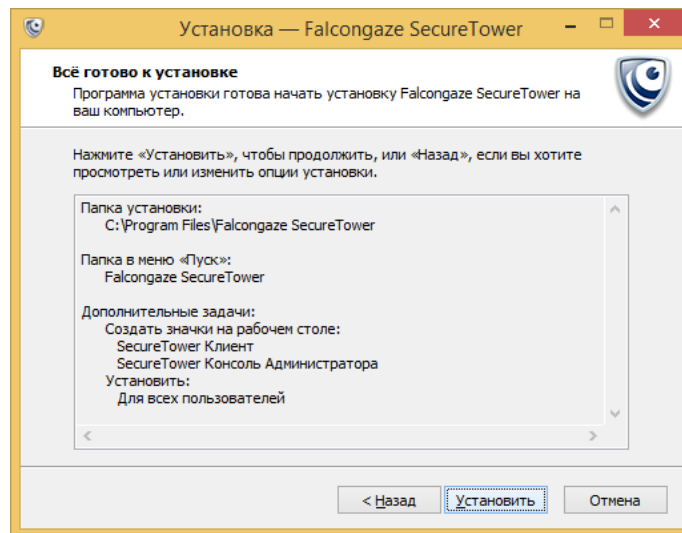


Рисунок 48 – Итоговые настройки



Рисунок 49 – Завершение установки

4.1.3 Запуск Консоли системного администратора Falcongaze SecureTower Admin Console.

Запустить Консоль администратора, используя ярлык консоли, размещенный в папке Falcongaze SecureTower в меню Пуск или через ярлык консоли на рабочем столе компьютера (см. рисунок 50).

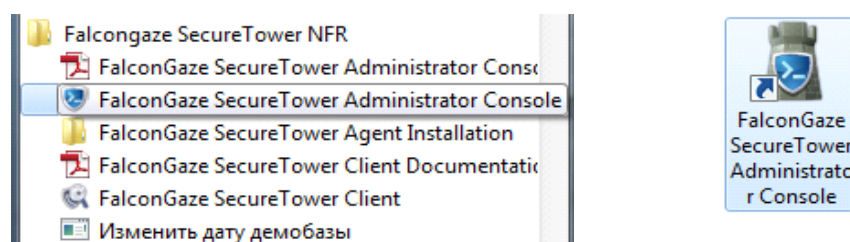


Рисунок 50 – Вид файлов для запуска консоли

В открывшемся диалоговом окне выбрать «Подключиться к локальному компьютеру» и нажать кнопку «Подключиться к серверу» (см. рисунок 51).

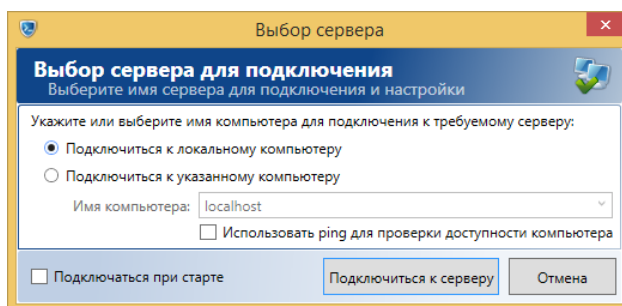


Рисунок 51 – Подключение к серверу

Далее необходимо перейти в раздел «Индексирование данных» и нажать на кнопку «Очисть индекс» (см. рисунок 52). Затем в разделе «Индексирование данных» нажать кнопку «Обновить индекс».

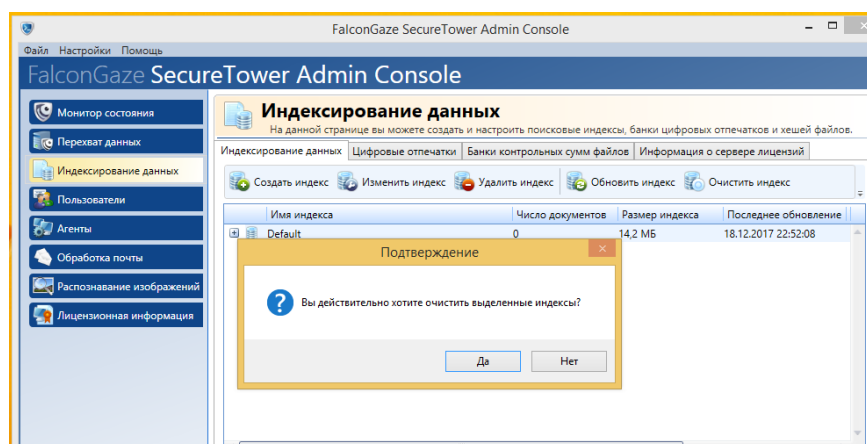


Рисунок 52 – Индексирование данных

4.1.4 Установка агентов на рабочие станции.

Для установки агентов необходимо перейти во вкладку «Агенты». Далее необходимо выбрать опцию «Устанавливать агенты на указанные компьютеры» в разделе «Стратегии установки агентов» и нажать «Список компьютеров для установки» (см. рисунок 53). Затем нажать на кнопку «Добавить объект».

На следующем шаге выбирается опция «Имя компьютера», а затем в выпадающем меню выбирается опция «Вручную». Далее вводится имя компьютера win81-st в поле ввода «Имена компьютеров» и нажимается клавиша «ОК».

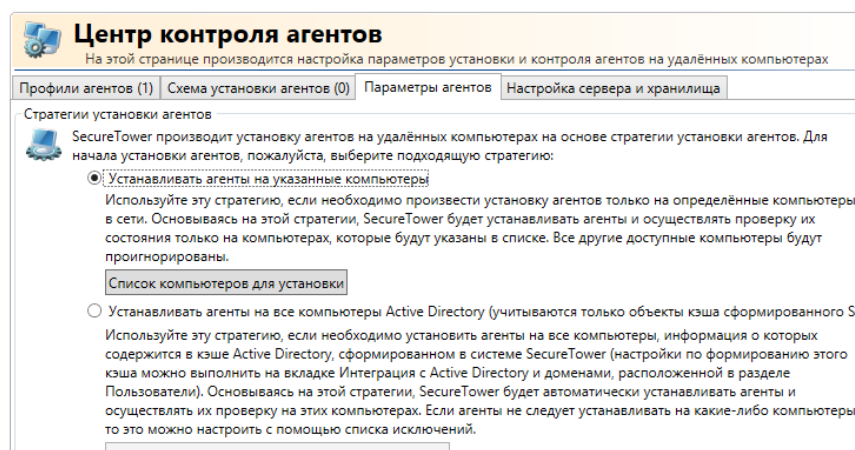


Рисунок 53 – Установка агентов

Во вкладке «Схема установки агента» необходимо указать имя компьютера, на котором был установлен агент в списке компьютеров. Если индикатор состояния зеленого цвета, то агент установлен правильно (см. рисунок 54), если индикатор другого цвета, то необходимо повторить установку агента.

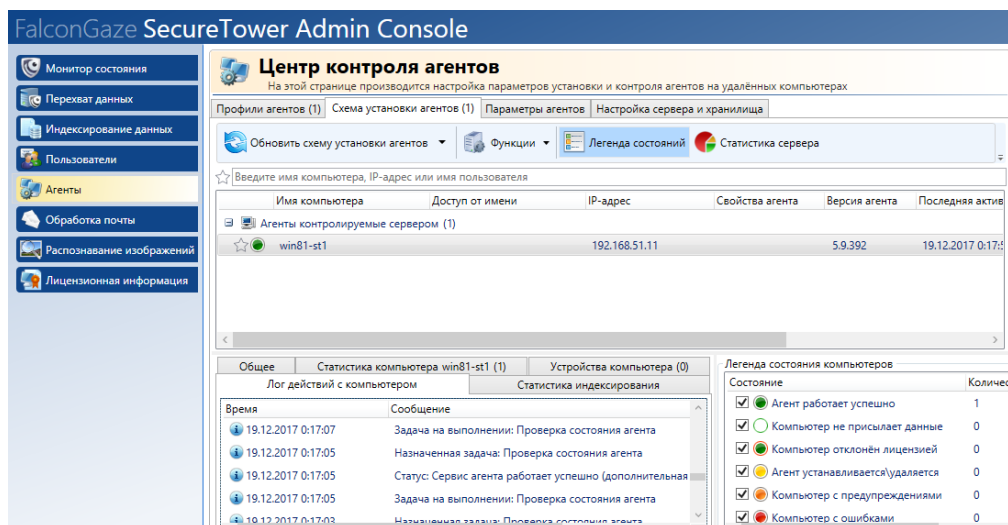


Рисунок 54 – Результат установки агента

4.1.5 Конфигурация профиля работы агентов.

Для настройки работы агента необходимо в окне «Профили агентов» перейти во вкладку «Контроль сетевого трафика» и убедиться, что включен перехват шифрованного и нешифрованного трафика в поле «Режим перехвата» (см. рисунок 55).

Из списка протоколов выбирается протокол FTP и нажимается «Расширенные настройки протокола». В открывшемся окне необходимо

отметить опцию «Перехватывать входящие файлы» и подтвердить настройки (см. рисунок 56).

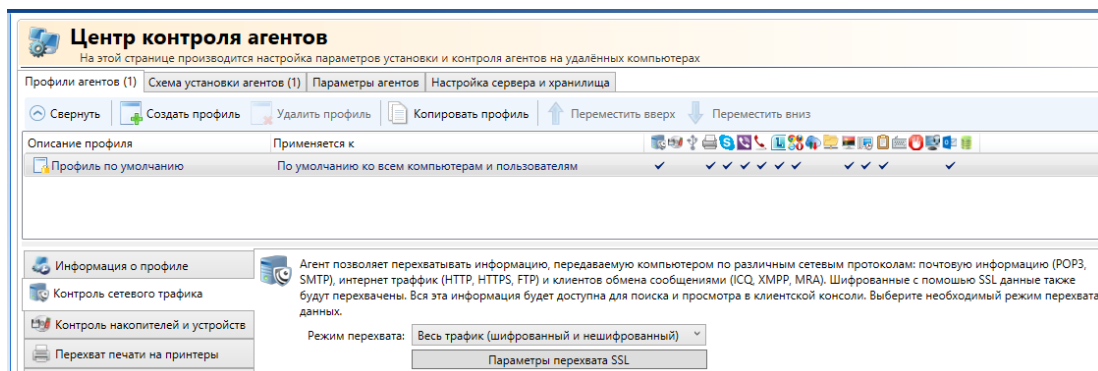


Рисунок 55 – Контроль сетевого трафика

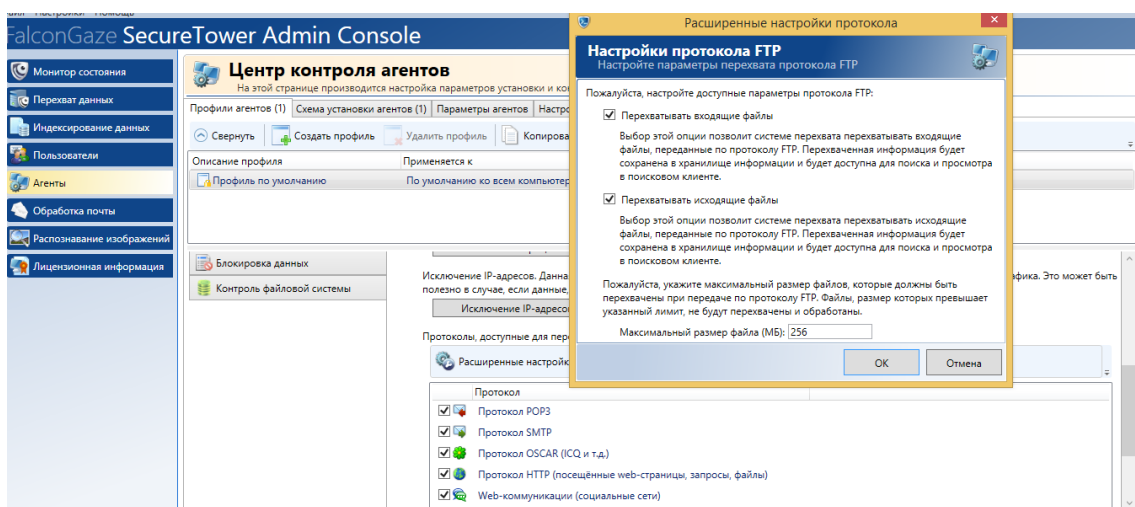


Рисунок 56 – Настройка протокола FTP

На следующем шаге осуществить переход во вкладку «Контроль накопителей и устройств» и в настройках контроля накопителей необходимо включить опции «Включить контроль накопителей информации» и «Сохранять теньовую копию данных, переданных на накопители» (см. рисунок 57).

Далее во вкладке «Контроль устройств» включить опцию «Включить контроль устройств» (см. рисунок 58).

На вкладке «Активность рабочего стола» включить опцию «Сохранять снимки экрана при изменении активного окна» (см. рисунок 59).

Далее необходимо применить все изменения для сохранения настроенных параметров агента.

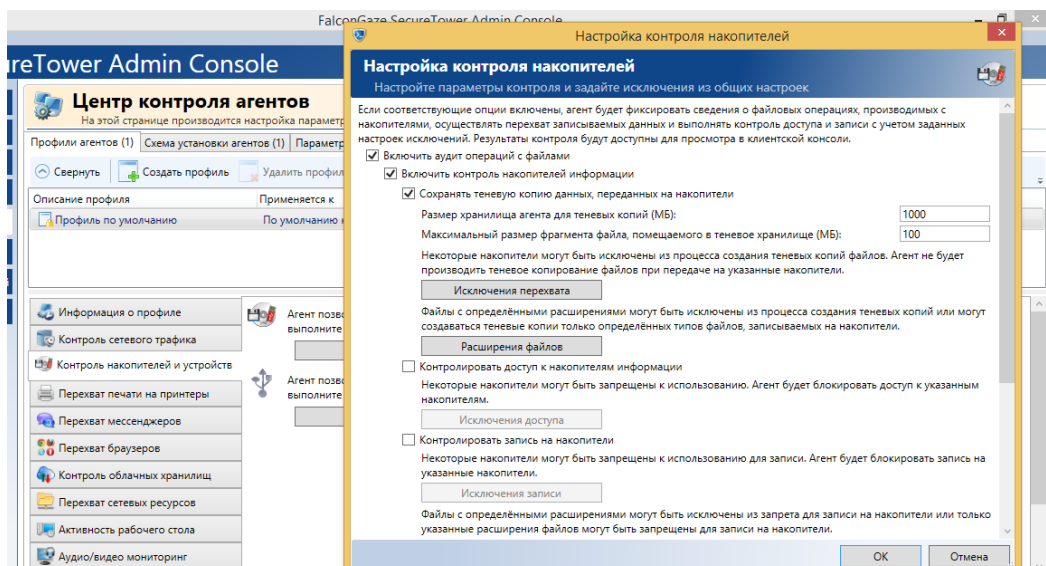


Рисунок 57 – Контроль накопителей

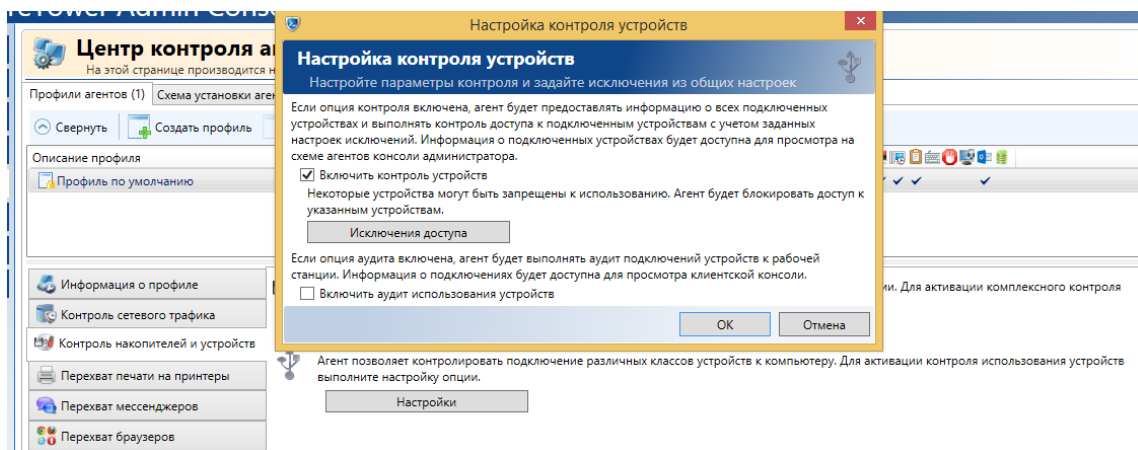


Рисунок 58 – Контроль устройств

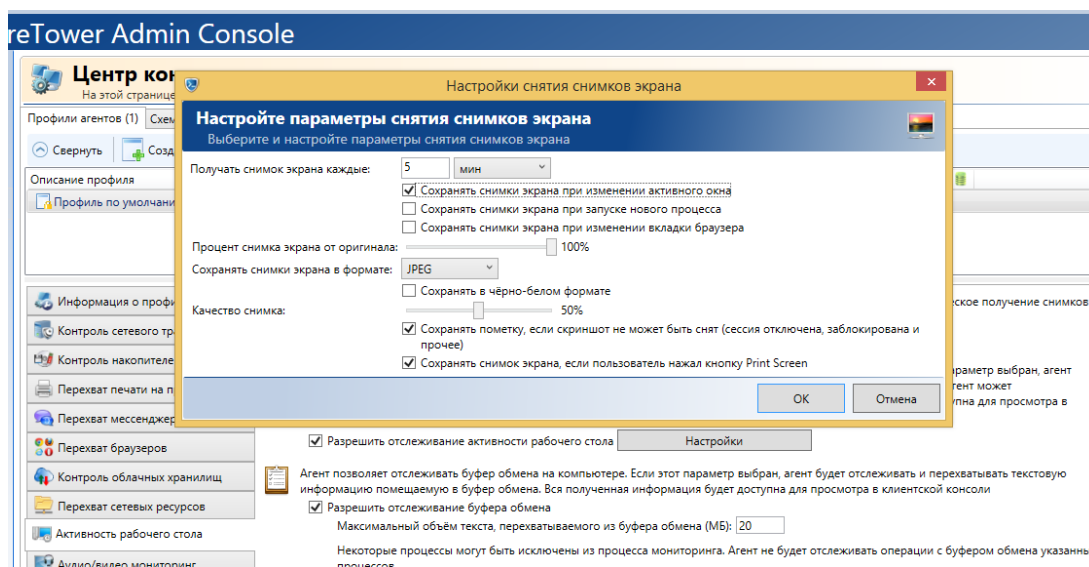


Рисунок 59 – Активность рабочего стола

4.1.6 Добавление пользователей.

Для добавления пользователей необходимо перейти в раздел «Пользователи» главного окна Консоли администратора и выбрать вкладку «Пользователи» (см. рисунок 60) и нажать «Добавить пользователя».

В открывшемся окне «Карточка пользователя» необходимо ввести имя и фамилию пользователя компьютера, на котором был установлен агент, а также заполнить остальные поля по желанию (см. рисунок 61).

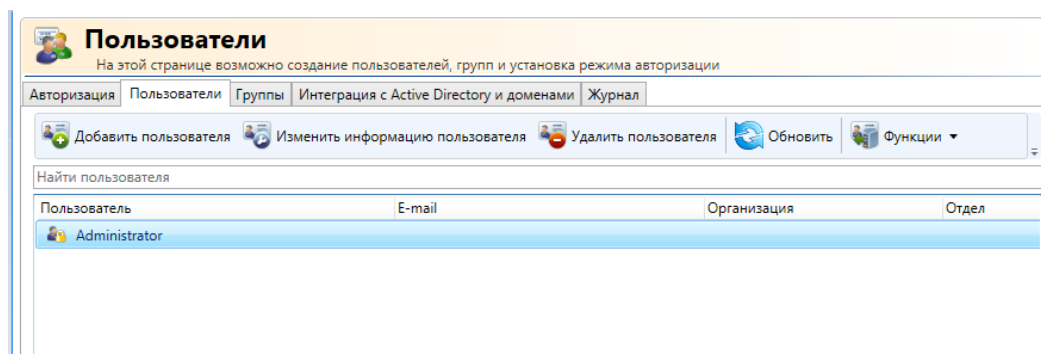


Рисунок 60 – Пользователи

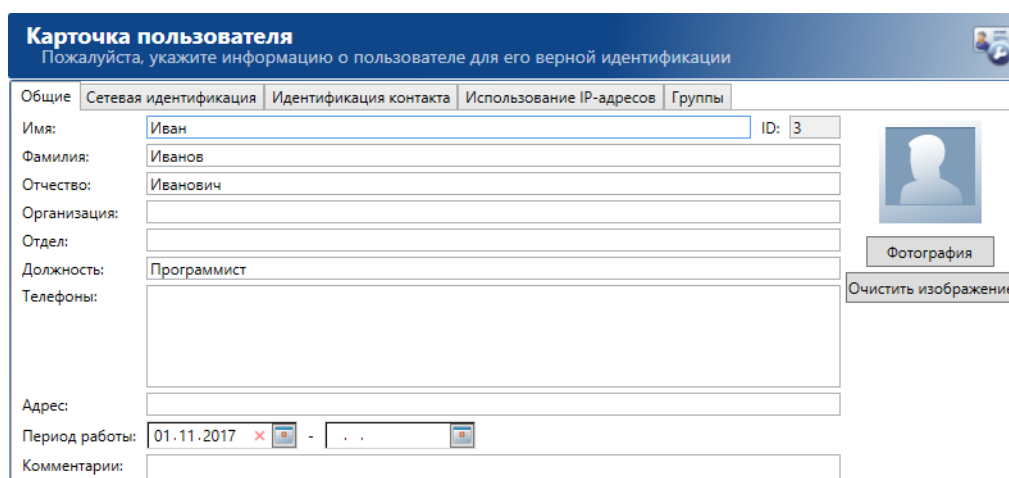


Рисунок 61 – Карточка пользователя

Далее необходимо перейти во вкладку «Сетевая идентификация» и в разделе «Учетная запись Windows» нажать кнопку «Добавить учетную запись Windows с помощью указания SID» и вставить SID. Для того чтобы скопировать SID в буфер обмена необходимо на главной панели консоли перейти в раздел «Агенты» и в нижней части окна перейти «Статистика компьютера». Из списка пользователей выбрать Администратора и, нажав

правую клавишу мыши по имени пользователя, выбрать «Скопировать SID в буфер обмена» (см. рисунок 62) .

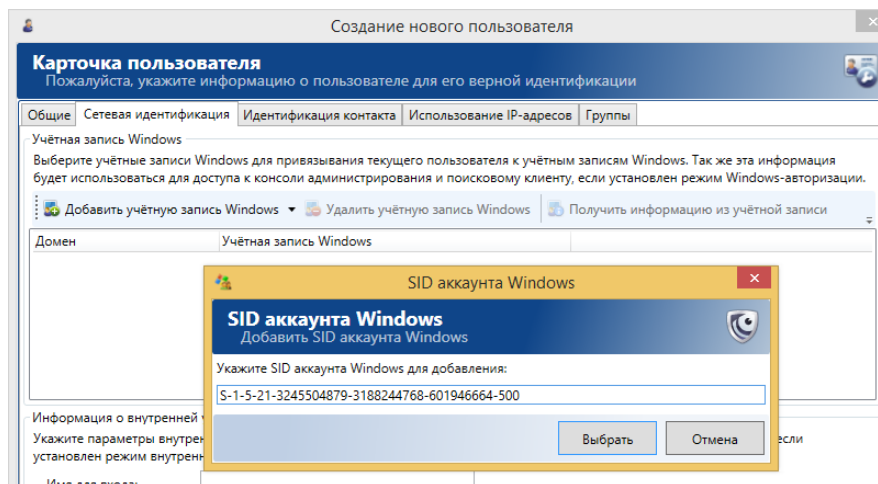


Рисунок 62 – Добавление учетной записи Windows

В дальнейшем могут быть созданы группы пользователей. Для этого необходимо нажать «Добавить членство в группе» и в открывшемся окне выбрать пользователей для включения их в группу.

В конце проделанной работы необходимо применить все изменения для сохранения настроенных параметров.

4.2 Создание политики безопасности и применение их для контроля устройств

4.2.1 Создание учетных записей пользователей.

Создать учетную запись локального пользователя на виртуальной машине с установленной операционной системой Windows 8.1 с использованием системы контроля и предотвращения утечек информации Falcongaze SecureTower можно через Admin Console. Для этого необходимо убедиться, что данная консоль установлена на рабочем компьютере, и запустить. После запуска Консоли подключиться к локальному серверу через локальный компьютер.

После прохождения авторизации необходимо в главном меню перейти в раздел «Пользователи» и заполнить карточку пользователя компьютера, на котором был установлен агент, а также заполнить остальные поля по желанию.

Подробное описание добавления пользователя было представлено в пункте 4.1.6.

4.2.2 Создание статического правила.

Для создания политики безопасности и применение их для контроля документов, выводимых на печать необходимо осуществить вход в Client Console через меню Пуск и или через ярлык на рабочем столе компьютера. После запуска Консоли осуществить подключение сервера. Вид консоли представлен на рисунке 63.

На виртуальный компьютер предварительно были установлены бесплатные виртуальные принтеры:

- PDFCreator;
- Foxit Reader.

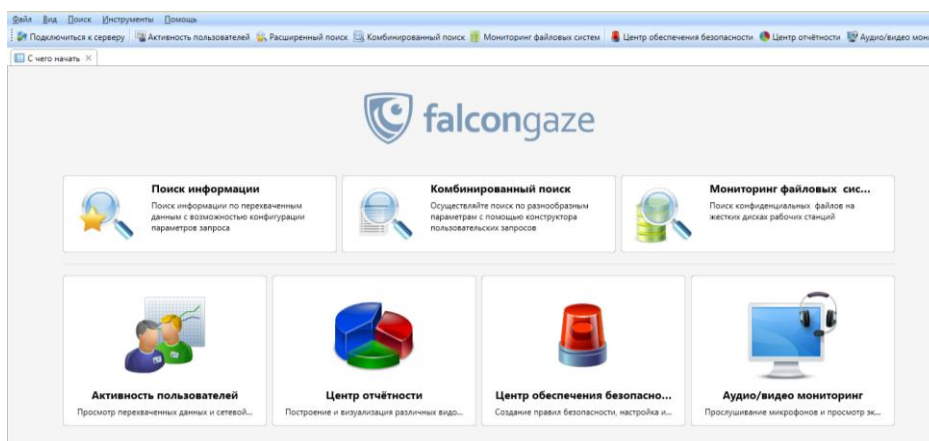


Рисунок 63 – Клиентская консоль

Для настройки системы контроля печати необходимо настроить правила для печати документов, содержащих конфиденциальную информацию. Правила безопасности применяются только для тех документов, которые были индексированы и внесены в базу данных индексов. Для имитации нарушений нужно использовать только те правила, которые проиндексированы.

Для установки правила необходимо осуществить переход по вкладке «Центр обеспечения безопасности» и выбрать «Добавить - Статическое» (см. рисунок 64).

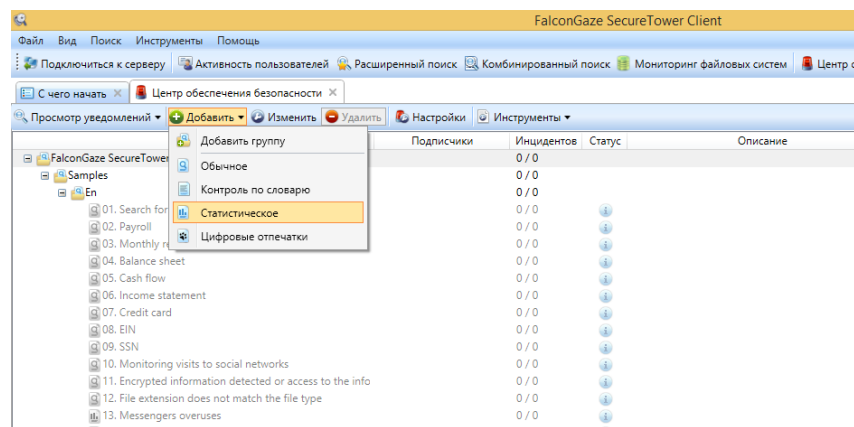


Рисунок 64 – Настройка статического правила

Для первого статического правила необходимо установить ограничения на количество страниц в документе, выводимых на печать для всех пользователей (см. рисунок 65). Были установлены такие условия, что контроль печати осуществлялся в течение дня и количество распечатанных страниц должно быть не меньше 7.

Под учетными данными пользователей было распечатано несколько документов, содержащих количество страниц меньше заявленного условия в правиле. Результат можно посмотреть в правилах в графе «Инциденты», а также в виде отчета по пользователям.

Рисунок 65 – Создание статического правила контроля количества распечатанных страниц

На следующем шаге создается второе статическое правило для этого необходимо установить ограничения на количество страниц в документе,

выводимых на печать для всех пользователей и ограничение по времени печати (см. рисунок 66). Были установлены такие условия, что контроль печати осуществлялся в течение рабочего дня, а именно с 9 до 18 часов, и количество распечатанных страниц должно быть не больше 5.

Добавление статистического правила безопасности
Укажите список поисковых условий, при достижении которых будет формироваться уведомление

Параметры Подписчики на уведомления

Название правила: Контроль печати

Описание:

Статистическое условие

Тип условия: Принтеры

Произвольный временной интервал От: 9 час. До: 18 час.

Количество распечатанных страниц 5

☒ Применять для каждого отдельного пользователя

Выберите операцию, применяемую к условиям в блоке: ☒ И ☐ Или ☐ Не (отрицание)

[Добавить условие](#) [Добавить блок](#) [Обрамить блоком](#)

☒ Включить правило безопасности

☐ Применить данное правило ко всем проиндексированным данным (это может занять много времени)

OK Отмена

Рисунок 66 – Создание статического правила контроля количества страниц и времени печати документа

Далее создается еще одно статическое правило для этого необходимо установить ограничения на количество страниц в документе и на тип документа, выводимых на печать для всех пользователей (см. рисунок 67). Были установлены такие условия, что контроль печати осуществлялся в течение рабочего дня, а именно с 9 до 18 часов, и количество распечатанных страниц должно быть не больше 10 и документы должны быть распечатаны только в формате pdf.

На следующем шаге создается еще одно статическое правило для этого необходимо установить ограничения на количество страниц в документе и на тип документа, выводимых на печать для всех пользователей (см. рисунок 68). Были установлены такие условия, что контроль печати осуществлялся в течение дня, количество распечатанных документов должно быть не больше 2 и документы должны быть распечатаны только в формате doc и статус документа должен быть зашифрованным или доступ к документу запрещен.

Добавление статистического правила безопасности
Укажите список поисковых условий, при достижении которых будет формироваться уведомление

Параметры Подписчики на уведомления

Название правила:

Описание:

Статистическое условие

Тип условия:

От: час. До: час.

<

☒ Применять для каждого отдельного пользователя

Выберите операцию, применяемую к условиям в блоке: ☒ И ☐ Или ☐ Не (отрицание)

[\[Добавить условие\]](#) [\[Добавить блок\]](#) [\[Обрамить блоком\]](#)

☒ Включить правило безопасности
☐ Применить данное правило ко всем проиндексированным данным (это может занять много времени)

Рисунок 67 – Создание статического правила контроля времени печати, количества страниц и формата файла

Добавление статистического правила безопасности
Укажите список поисковых условий, при достижении которых будет формироваться уведомление

Параметры Подписчики на уведомления

Название правила:

Описание:

Статистическое условие

Тип условия:

☒ учитывается календарный день

<

☒ Применять для каждого отдельного пользователя

Выберите операцию, применяемую к условиям в блоке: ☒ И ☐ Или ☐ Не (отрицание)

И

[\[Добавить условие\]](#) [\[Добавить блок\]](#) [\[Обрамить блоком\]](#)

☒ Включить правило безопасности
☐ Применить данное правило ко всем проиндексированным данным (это может занять много времени)

Рисунок 68 – Создание статического правила контроля количества документов, формата и статуса документа

Когда настраиваются правила, кроме принтера существует возможность использования других устройств и по различным признакам. В виду возможностей создания лабораторного стенда из всех устройств в лабораторных работах был использован только принтер.

4.2.3 Построение отчетов о пользовательской активности при помощи Центра отчетности SecureTower.

Для построения отчета необходимо перейти в Клиентскую консоль. В главном окне Клиентской консоли выбрать вкладку «Центр отчетности» и нажать «Обновить отчеты» в панели задач окна Центр отчетности.

Для построения отчета по определенному пользователю и с определенными параметрами необходимо нажать «Добавить – Отчет по пользователю» и в открывшемся окне заполнить необходимые критерии для построения отчета (см. рисунок 69). Выстроенный отчет можно посмотреть в окне консоли (см. рисунок 70), формат отчетов сформированных отчет .rpx. Поэтому при загрузке таких отчетов и дальнейшего просмотра необходимы специальные программы, поддерживающие данный формат.

Добавление отчёта
Укажите параметры формирования отчёта

Название отчёта:

Описание:

Параметры отчета **Планировщик**

Пользователь:

Отчет за определённый период:

- ☒ За всё время
- ☐ За предыдущий день
- ☐ За текущую календарную неделю
- ☐ За предыдущую календарную неделю
- ☐ За текущий календарный месяц
- ☐ За 30 последних дней
- ☐ Произвольный временной интервал

☒ Не учитывать текущий день при построении отчёта

Фильтры отображения:

- ☒ Тип данных для отображения
 - ☒ Почта
 - ☒ Мессенджеры
 - ☒ Web
 - ☒ Прочее
- ☒ Активность пользователя за компьютером
- ☒ Общая статистика

OK Отмена

Рисунок 69 – Создание отчета по пользователю по критериям

Центр отчетности может сформировать несколько видов отчетов:

- ТОП – отчет по пользователям - отчет по активности определенного количества пользователей;
- отчет пользователя – отчет по активности конкретно выбранного пользователя;
- отчет по Центру безопасности – отчет о статистике срабатывания правил безопасности;

– сводный отчет – отчет о сводных статических данных о показателях активности пользователей за определенный промежуток времени.

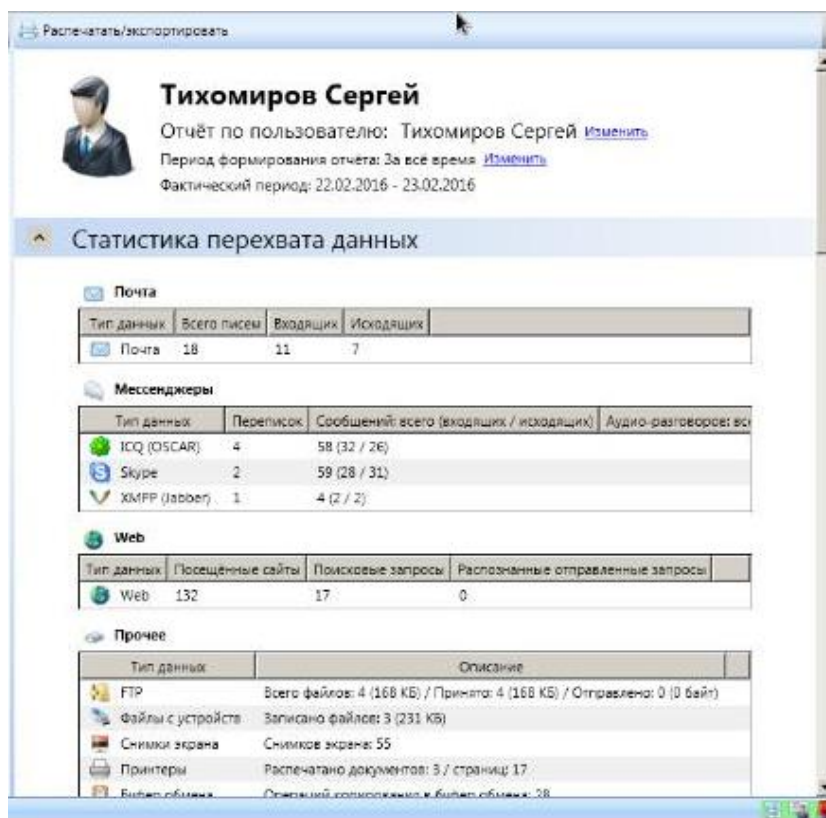


Рисунок 70 – Сформированный отчет по пользователю

Также в Клиентской консоли могут быть построены собственные отчеты. Для этого из перечня видов отчетов в «Центр отчетности» необходимо выбрать правой клавишей мыши «Мои отчеты» и «Добавить – Отчет по пользователю». В открывшемся окне установить критерии формирования отчета, например, указать название отчета «Отчет по пользователю Иванов И.И.», выбрать из перечня пользователей Иванова И.И., указать период сбора отчета «За текущую календарную неделю» и настроить фильтр отображения, а именно, выбрать все типы данных, все виды активности пользователя и установить время контроля работы пользователя (рабочее время с 9 до 18). Сформированный отчет представлен в виде диаграмм.

Для построения отчета Аудита необходимо осуществить вход в консоль «Центр обеспечения безопасности» и нажать «Инструменты – Журнал аудита» (см. рисунок 71).

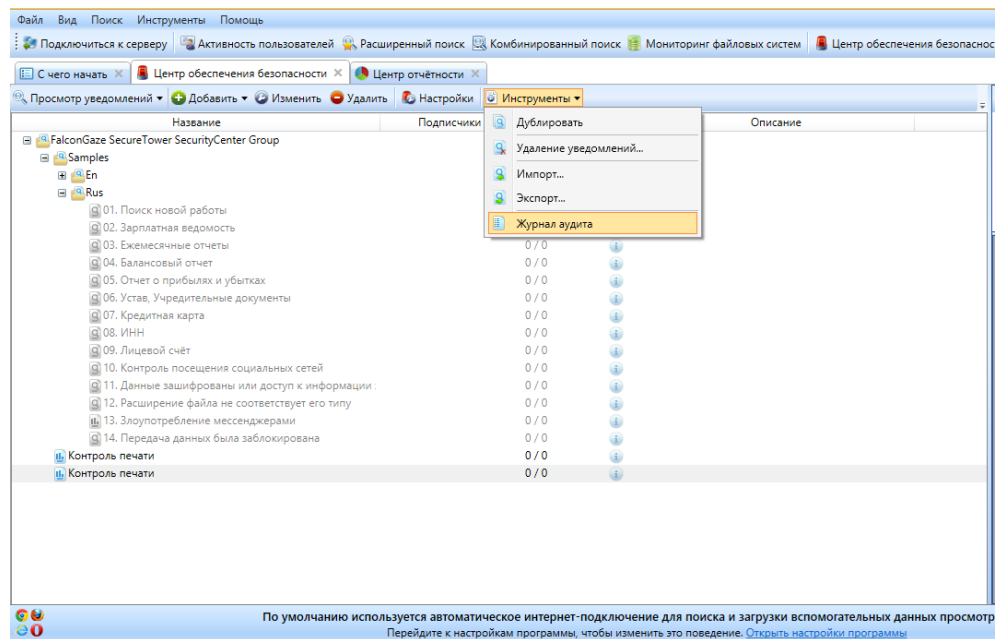


Рисунок 71 – Журнал аудита

При построении отчета Аудита можно настроить критерии построения журнала. Журнал может быть сформирован как по всем действиям пользователей, так и по отдельным критериям, а именно, по конкретному пользователю или за определенный период.

5 Описание порядка выполнения заданий практикума и результатов выполнения

5.1 Порядок выполнения заданий практикума

Выполнение задания практикума предполагает следующую последовательность действий:

- изучение теоретического материала, приведенного в методических указаниях к практическим занятиям и на лекциях;
- выполнение задания практикума;
- подготовка отчета о выполнении задания практикума;
- защита отчета о выполнении заданий практикума, ответы на контрольные вопросы.

Каждое задание практикума предполагает его выполнение за два академических часа.

Выполнение задания разбито на несколько этапов, выполнение задания включает промежуточный контроль отдельных этапов.

Промежуточный контроль включает после выполнения задания проверку преподавателем, при этом проверяется полнота и правильность, а также соответствие результатов.

Порядок выполнения является общим для выполнения заданий практикума.

5.2 Порядок выполнения практического задания по установке программного комплекса Falcongaze SecureTower в локальной сети с доменной структурой

5.2.1 Начало выполнения задания практикума.

5.2.1.1 Осуществить вход на виртуальную машину с установленной операционной системой Windows 8.1.

5.2.1.2 С помощью параметров управления учетными записями пользователей отключить контроль учетных записей пользователей.

5.2.1.3 С помощью консоли центра управления сетями и общим доступом включить сетевое обнаружение.

5.2.1.4 С помощью консоли общего доступа к файлам и принтерам для протоколов IPv4 и IPv6 включить правила для входящих соединений.

5.2.2 Установка компонентов программного комплекса Falcongaze SecureTower.

5.2.2.1 Установить из папки для установки Common все необходимые приложения.

5.2.2.2 Запустить исполнительный файл Мастера установки.

5.2.2.3 Ознакомиться с версией программного продукта и рекомендациями по установке.

5.2.2.4 Принять лицензионное соглашение и выбрать папку для сохранения.

5.2.2.5 Выбрать компоненты для установки и ознакомиться с итоговыми настройками и установить программный продукт.

5.2.3 Запустить консоль и осуществить подключение к серверу, в разделе «Индексирование» проиндексировать данные.

5.2.4 Перейти в раздел «Агенты» и установить агент на рабочие станции.

5.2.5 Настроить в разделе «Агенты» работу агента по контролю сетевого трафика, активности рабочего стола, контролю накопителей и устройств.

5.2.6 Создать учетную запись пользователя Windows по SID в консоли Falcongaze SecureTower.

5.2.7 Порядок выполнения задания в виде UML-диаграммы

Порядок выполнения практического задания по установке программного комплекса Falcongaze SecureTower в локальной сети с доменной структурой представлен в виде UML-диаграммы в приложении Б.

5.3 Порядок выполнения практического задания по созданию политики безопасности программного комплекса Falcongaze SecureTower и применение их для контроля устройств

5.3.1 Начало выполнения задания практикума

5.3.1.1 Осуществить вход на виртуальную машину с установленной операционной системой Windows 8.1, используя учетную запись доменного администратора.

5.3.1.2 Запустить Консоль администратора и клиентскую консоль программного комплекса Falcongaze SecureTower.

5.3.1.3 Выполнить подключение сервера к локальному компьютеру.

5.3.1.4 В консоли администратора создать учетные записи пользователей.

5.3.2 Создание статического правила.

5.3.2.1 В клиентской консоли в разделе «Центр обеспечения безопасности» создать статическое правило по контролю печати.

5.3.2.2 Создание статического правила по ограничению времени и количества страниц для печати.

5.3.2.3 Проверка применения статического правила при печати документов.

5.3.2.4 Создание статического правила по контролю времени печати, количества страниц и формата файлов.

5.3.2.5 Проверка применения статического правила при печати документов.

5.3.2.6 Создание статического правила по контролю времени печати, количества документов, формата файлов и статуса документа.

5.3.2.7 Проверка применения статического правила при печати документов.

5.3.3 Построение отчетов.

5.3.3.1 В Клиентской консоли осуществить вход в «Построение отчетов».

5.3.3.2 Перед построением отчетов обновить все отчеты.

5.3.3.3 Построить отчет Центра безопасности и посмотреть его результат.

5.3.3.4 Построить отчет по активности пользователей и посмотреть его результат.

5.3.3.5 Построить отчет аудита.

5.3.4 Порядок выполнения задания в виде UML-диаграммы.

Порядок выполнения практического задания по созданию политики безопасности программного комплекса Falcongaze SecureTower и применение их для контроля устройств представлен в виде UML-диаграммы в приложении В.

6 Описание структуры и содержания отчета о выполнении практических заданий

6.1 Общий перечень данных, содержащихся в отчете

Результаты выполнения заданий, входящих в практикум, оформляются в виде отчетов. Содержание отчета выполнения каждого задания включает в себя:

- титульный лист отчета о выполнении задания с указанием названия задания;
- цель задания;
- содержание задания;
- описание выполнения задания, иллюстрируемое снимками экрана;
- выводы по результатам выполнения задания;
- отчеты, построенные после выполнения задания с использованием накопленных записей аудита.

Снимки экранов необходимо делать в процессе выполнения заданий практикума и сохранять их. Эти снимки экранов не приведены в рекомендациях по выполнению лабораторных работ, поэтому студенты заранее не знают, что на них будет.

Графически общая структура отчета показана в приложении Г.

6.2 Структура отчета по выполнению задания по установке программного комплекса Falcongaze SecureTower в локальной сети с доменной структурой

Отчет должен включать в себя:

- титульный лист отчета о выполнении задания с указанием названия задания;
- цель задания, представляющую собой краткое описание задач на задание практикума;
- задание практикума, представляющее собой краткий обзор последовательности действий при выполнении задания практикума;

- описание порядка выполнения действий, а именно:
 - установка программного продукта Falcongaze SecureTower;
 - индексирование данных;
 - настройка профиля агента;
 - создание учетных записей пользователя;
- вывод, включающий в себя описание навыков, которые были получены в ходе выполнения задания практикума.

Общая структура отчета о выполнении заданий, а также содержание контрольных экземпляров отчетов представлены в приложении Д.

6.3 Структура отчета по выполнению задания по созданию политики безопасности программного комплекса Falcongaze SecureTower и применение их для контроля устройств

Отчет должен включать в себя:

- цель задания, представляющую собой краткое описание задач на задание практикума;
- задание практикума, представляющее собой краткий обзор последовательности действий при выполнении задания практикума;
- описание порядка выполнения действий, а именно:
 - создание учетных записей пользователей;
 - создание статического правила контроля количества страниц при печати документа;
 - создание статического правила контроля количества страниц и времени печати документа;
 - создание статического правила контроля количества страниц, времени печати, формата документа при печати;
 - создание статического правила контроля количества документов ,времени печати, формата и статуса документа при печати;
 - построение отчетов;

– вывод, включающий в себя описание навыков, которые были получены в ходе выполнения задания практикума.

Общая структура отчета о выполнении заданий, а также содержание контрольных экземпляров отчетов представлены в приложении Е.

7 Определение порядка контроля выполнения практического задания

7.1 Общий порядок контроля

Порядок контроля выполнения заданий практикума является общим для двух заданий, входящих в практикум, и включает в себя проверку:

- полноты выполнения практической работы;
- соответствия созданных снимков экрана пунктам задания.

Дополнительным критерием контроля выполнения второго практического задания является проверка полноты сформированных отчетов по файлам и журналам на сервере событий в ходе выполнения задания практикума.

После выполнения задания практикума результаты работы предоставляются для проверки. Предъявляются снимки экранов с указанием того пункта задания, при выполнении которого они формировались.

После проверки правильности результатов должен быть оформлен отчёт о выполнении задания. К отчету должны прилагаться сформированные отчеты по файлам журналов на сервере. Перед защитой работы проверяется правильность оформления отчет. Если данные соответствуют заданию и отчёт выполнен по требованиям, то он допускается к защите, если не выполнено хотя бы одно из условий, то отчет отправляется на доработку.

Порядок проверки выполнения заданий практикума представлен в приложении Ж.

7.2 Порядок контроля выполнения практического задания по установке программного комплекса Falcongaze SecureTower в локальной сети с доменной структурой

После выполнения задания проверяется наличие снимков экрана, которые должны быть включены в отчет:

- процесс и результат установки компонентов программного комплекса Falcongaze SecureTower;
- результат запуска консоли и подключения к локальному серверу;
- результат индексирования данных;

- процесс установки агента на рабочие станции;
- индикация агента после установки;
- настройка конфигурации профиля работы агента: контроль сетевого трафика, перехват входящих файлов в протоколе FTP, контроль накопителей и устройств, активность рабочего стола;
- процесс и результат добавления пользователей.

Проверка полноты выполнения задания включает:

- наличия снимков экранов с указанием описания того пункта задания, при выполнении которого они формировались;
- выполнение каждого пункта задания;
- сформированный отчет о выполнении практического задания.

7.3 Порядок создания политик безопасности программного комплекса Falcongaze SecureTower и применение их для контроля устройств

Должны быть показаны в виде снимков экрана:

- процесс создания учетных записей пользователей;
- процесс создания статических правил контроля печати:
 - создание статического правила контроля количества страниц при печати документов;
 - создание статического правила контроля количества страниц и времени печати документа;
 - создание статического правила контроля времени печати, количества страниц и формата файла;
 - создание статического правила контроля количества документов, формата и статуса документа;
- построение отчетов о пользовательской активности.

Должны быть сформированы и представлены отчеты о пользовательской активности, отчеты по Центру безопасности и отчет аудита.

Проверка полноты выполнения задания включает:

- наличия снимков экранов с указанием описания того пункта задания, при выполнении которого они формировались;
- выполнение каждого пункта задания;
- сформированный отчет о выполнении практического задания.

Проверка полноты сформированных отчетов по файлам и журналам на сервере событий в ходе выполнения задания практикума включает:

- сформированный отчет по активности пользователя, в котором отражены все действия конкретного пользователя;
- сформированный отчет по Центру безопасности, отражающего статистику срабатывания всех правил безопасности, примененных при выполнении задания;
- сформированный отчет аудита, в котором отражены все действия пользователей.

8 Подготовка сценария для автоматизированного развертывания виртуальных машин

Для автоматизации процесса развертывания ВМ на стенде были разработаны сценарии, которые определяют конфигурацию ВМ после их создания, а также режимы их работы.

Сценарий описывает аппаратную конфигурацию ВМ, которая была определена при создании ВМ в разделе 3. Аппаратная конфигурация подразумевает наличие у ВМ следующих устройств:

- процессор;
- оперативная память;
- видеопамять;
- подключаемый виртуальный жесткий диск;
- привод оптического диска;
- буфер обмена;
- USB-устройства;
- сетевой адаптер.

У ВМ с установленной ОС Windows Server 2012 R2 были установлены следующие конфигурации:

- основная память – 2048 МБ;
- видеопамять – 128Мб;
- носители – виртуальный жесткий диск – w2k12r2-fgst.vdi;
- сетевой адаптер – тип: Intel PRO/1000 MT Server;
- общие папки: D:\share.

У ВМ с установленной ОС Windows Server 2003 R2 были установлены следующие конфигурации:

- основная память – 512 МБ;
- видеопамять – 16 Мб;
- носители – виртуальный жесткий диск – w2k3st-srv.vdi;
- сетевой адаптер – тип: PCnet – FAST III;

- общие папки: D:\share.

У ВМ с установленной ОС Windows 8.1 были установлены следующие конфигурации:

- основная память – 1024 МБ;
- видеопамять – 128Мб;
- носители – виртуальный жесткий диск – win81-st1.vdi;
- сетевой адаптер – тип: Intel PRO/1000 MT Desktop;
- общие папки: D:\share.

Также в сценарии задается режим работы ВМ immutable – это означает, что ВМ возвращается в исходное состояние при закрытии VirtualBox. Это сделано для того, чтобы ВМ автоматически сбрасывались в исходное состояние по окончании лабораторных работ.

Для автоматизированного развертывания виртуальных машин было подготовлено три сценария. Разработанные сценарии представлены в приложении И.

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

К вредным и даже опасным психофизическим факторам, влияющим на сердечнососудистую систему специалиста по защите информации, относятся нервно-психические и физические перегрузки.

Труд специалистов по защите информации характеризуется многочасовой работой с малой активностью и однообразным положением. Такое положение оказывает большую нагрузку на значительное количество мышц, в том числе ног, плеч, шеи и рук. В результате появляются болевые ощущения, и ухудшается кровообращение, снижается затрата кислорода тканями организма.

Трудовая деятельность специалиста по защите информации связана с длительной работой на компьютеризированном рабочем месте с использованием огромного объема информации, принятием ответственных решений в условиях дефицита времени. Такая деятельность чаще всего приводит к нервно-психической перегрузке, расстройствам в деятельности и развивает усталость, утомления, переутомления и стресс.

Усталость представляет собой совокупность временных изменений в психофизиологическом состоянии человека, которые появляются из-за длительной работы или напряжений, что может привести к ухудшению таких показателей, как качественных и количественных. Основными показателями развития утомляемости является частота пульса, изменения в составе крови, артериальное давление.

Переутомление представляет собой совокупность неблагоприятных для здоровья человека функциональных изменений в организме, которые возникают из-за длительной усталости работника.

Развитие утомления и переутомления может привести к нарушению координации движений, рассеянности, потере контроля. При таких симптомах

работник допускает много ошибок в своей деятельности и, кроме того, переутомление и утомление могут привести к кислородной недостаточности.

Основными проявлениями переутомления являются повышенная утомляемость, головные боли, а также способствует появлению таких заболеваний как вегето-сосудистая дистония, ишемическая болезнь сердца, артериальная гипертония.

При наличии симптомов утомления или переутомления у работника снижается концентрация и координация, замедляются процессы мышления, повышается раздражительность, увеличивается время реакции, снижается эффективность профессиональных знаний. Усталость сопровождается состоянием, при котором работник совершает много ошибок при работе, которые могут привести к опасным ситуациям или даже несчастным случаям.

Неблагоприятные нарушения в организме работника часто не ликвидируются полностью, а могут перейти в хроническую стадию. Самыми распространенными заболеваниями, связанными с деятельностью специалистов по защите информации, являются гипертония, атеросклероз, неврозы, инфаркты и инсульты.

Борьба с этими неблагоприятными психофизическими изменениями работника сводится к улучшению санитарно-гигиенических условий труда и применению специальных методов, которые восстанавливают функциональное состояние опорно-двигательного аппарата, усиливают мозговое кровообращение.

К специальным методам можно отнести физическую культуру, направленную на повышение профессиональной работоспособности. Она помогает снизить утомляемость и ускорить процесс восстановления организма.

Специалисты рекомендуют начинать свой рабочий день с вводной гимнастики, которая выполняется в течение интервала от 5 до 7 минут и активизирует деятельность органов, которые играют ведущую роль в трудовой деятельности специалиста по защите информации. Или если такой возможности нет, необходимо выполнять физкультурные паузы через каждые 2

– 2,5 часа работы. Упражнения должны выполняться такие, чтобы нагрузку получали и те органы, которые не принимают активного участия в процессе труда.

Положение сидя наиболее частая поза работы для специалиста по защите информации. При таком режиме работы необходимо проводить упражнения, регулирующие кровообращение. Как правило, упражнения подбираются самостоятельно и их воздействие направлено на наиболее утомляемую группу мышц или часть тела.

Для улучшения кровообращения к таким упражнениям можно отнести наклоны вперед туловища, ходьба и дыхательные упражнения. Некоторые упражнения могут возникать непроизвольно – это вращения головой, плечами, туловищем.

Если в обеденный перерыв осталось свободное время, то для восстановления от нагрузки организма необходимо спокойно походить, делая при этом дыхательные упражнения, в лучшем случае сделать это необходимо не в душном помещении, а на свежем воздухе.

В конце рабочего дня полезно выполнять восстановительную гимнастику, в которой используются только упражнения, помогающие снять утомление с наиболее загруженных систем организма.

Любые физические упражнения в той или иной степени воздействуют на многие системы и органы. Для работников с малоподвижным видом труда, небольшими физическими нагрузками, особое значение представляют упражнения, совершенствующие сердечно-сосудистую и дыхательные системы. Данные упражнения повышают выносливость организма к работе, способствуют противостоять утомлению. Такие упражнения должны быть невысокой интенсивности, но достаточной продолжительности, например, ходьба.

Выбор места для занятий зависит от условий и возможностей каждого человека.

ЗАКЛЮЧЕНИЕ

В результате выполнения ВКР был разработан практикум по применению функциональных возможностей программного средства защиты Falcongaze SecureTower для контроля и предотвращения утечек информации.

Первое задание практикума посвящено установке программного комплекса Falcongaze SecureTower в локальной сети с доменной структурой.

Второе задание практикума посвящено созданию политик безопасности программного комплекса Falcongaze SecureTower и применению их для контроля устройств.

В ходе дипломного проектирования был произведен обзор систем контроля и предотвращения утечек информации, а также функций, реализуемые программным комплексом Falcongaze SecureTower, 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 применению функциональных возможностей программного средства защиты Falcongaze SecureTower для контроля и предотвращения утечек информации.

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

Результаты ВКР были представлены на международной научно-практической конференции «Особенности современного этапа развития естественных и технических наук» в секции «Технические науки», проводимой Агентством перспективных научных исследований. Публикация, содержащие представленные результаты, включена в сборник статей [8] конференции.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1 Структура и функциональные возможности систем контроля и предотвращения утечек информации // Общая характеристика и типовые функции систем контроля и предотвращения утечек информации. Лекции по системам контроля и предотвращения утечек информации.

2 Официальный сайт продукта DeviceLock [Электронный ресурс], URL: <https://www.devicelock.com/ru/products/features.html> (дата обращения: 30.09.2017).

3 Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК) [Электронный ресурс], URL: <http://fstec.ru> (дата обращения 01.10.2017).

4 Сравнение систем защиты от утечек (DLP) 2014 – часть 1 [Электронный ресурс], URL: https://www.anti-malware.ru/comparisons/data_leak_protection_2014_part1 (дата обращения 04.10.2017).

5 Официальный сайт продукта DeviceLock [Электронный ресурс], URL: <https://www.devicelock.com/ru/products/features.html> (дата обращения 05.10.2017).

6 Официальный сайт продукта Zlock [Электронный ресурс], URL: <http://www.zecurion.ru/products/zlock/> (дата обращения 05.10.2017).

7 Комплексная DLP – система Falcongaze SecureTower [Электронный ресурс], URL: <http://www.azone-it.ru/falcongaze-securetower> (дата обращения 05.10.2017).

8 Шишкина И.В. Современные DLP – системы: проблемы и перспективы развития // Особенности современного этапа развития естественных и технических наук: сборник научных трудов, часть 2 (Белгород, 28 декабря 2017г.) – Белгород, 2018 – С 201 – 204.

ПРИЛОЖЕНИЕ А

(обязательное)

Состав виртуального стенда, используемого при выполнении практикума

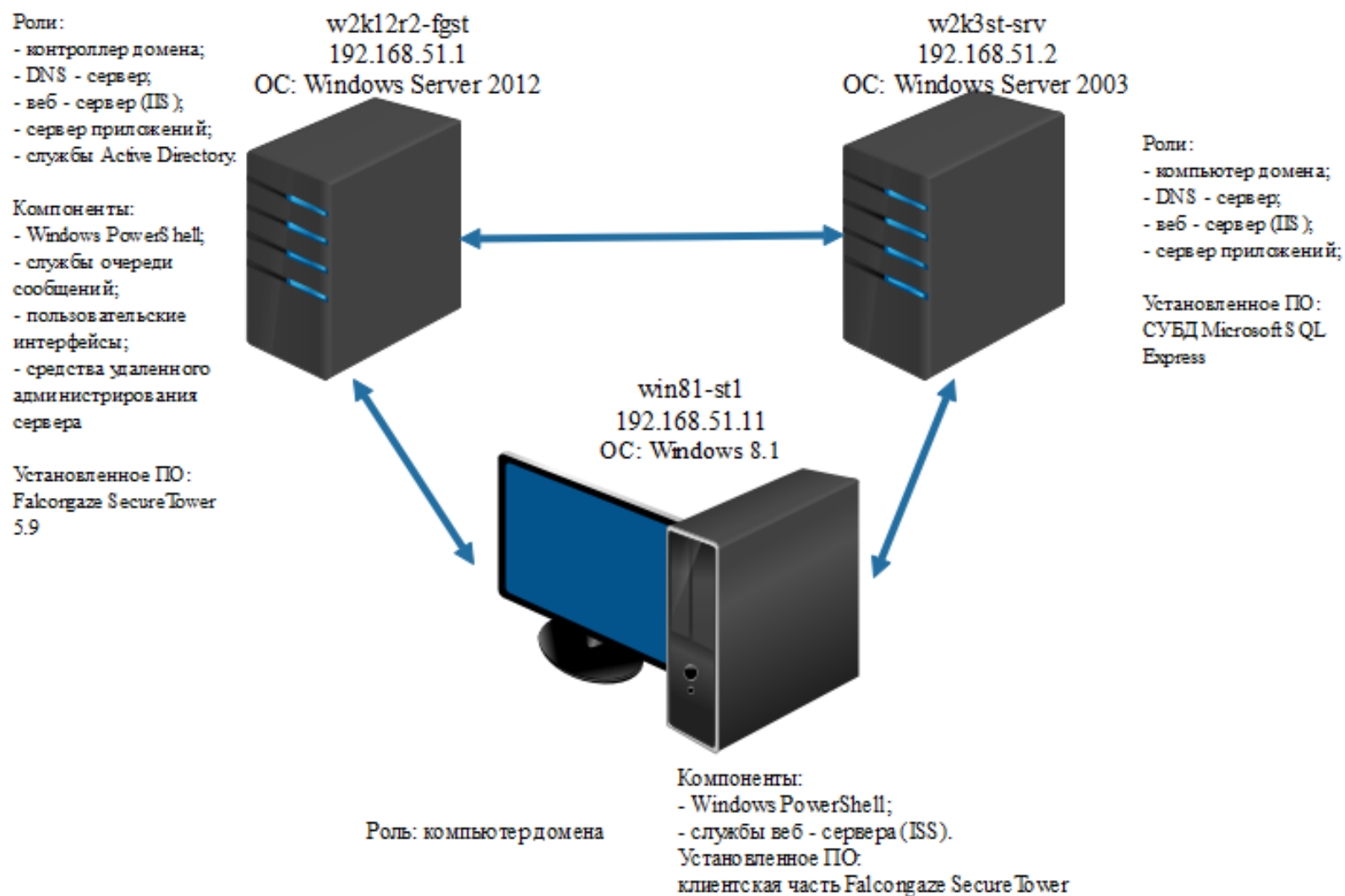


Рисунок А.1

ПРИЛОЖЕНИЕ Б

(обязательное)

UML-диаграмма последовательности действий выполнения задания по установке программного комплекса Falcongaze SecureTower в локальной сети с доменной структурой

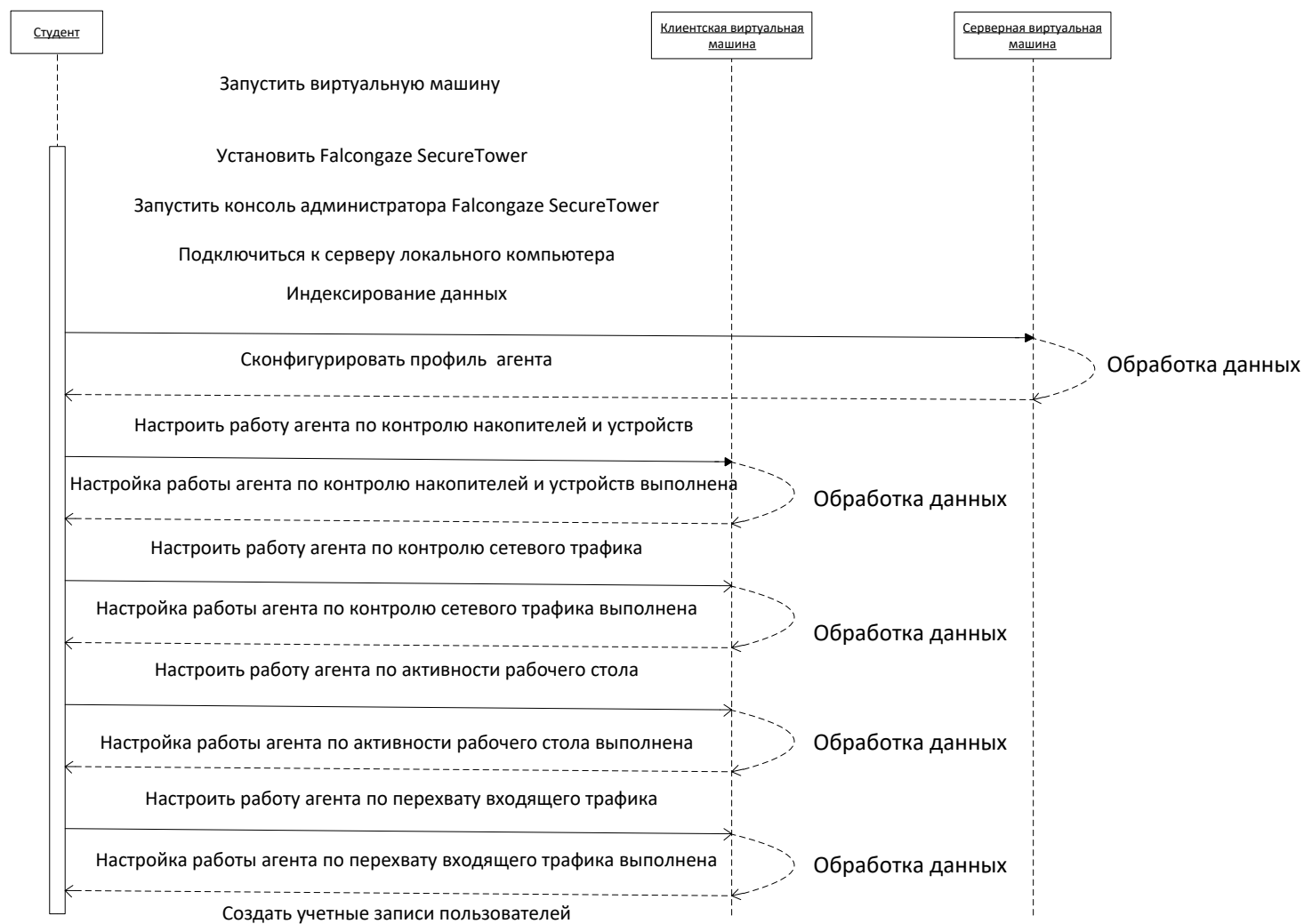


Рисунок Б.1

ПРИЛОЖЕНИЕ В

(обязательное)

UML-диаграмма последовательности действий выполнения задания по созданию политики безопасности программного комплекса Falcongaze SecureTower и применение их для контроля устройств

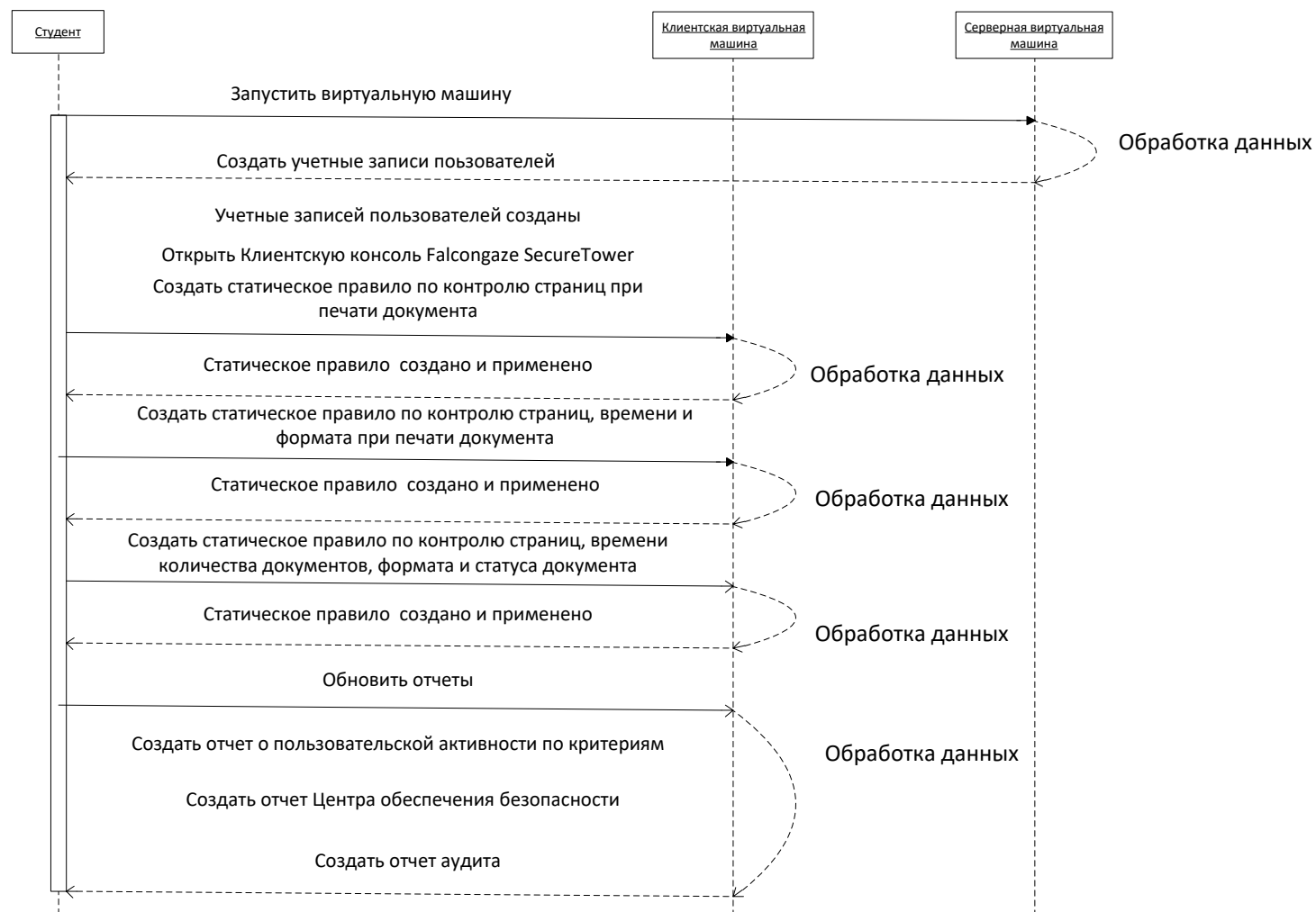


Рисунок В.1

ПРИЛОЖЕНИЕ Г

(обязательное)

Структура отчетов о выполнении заданий практикума

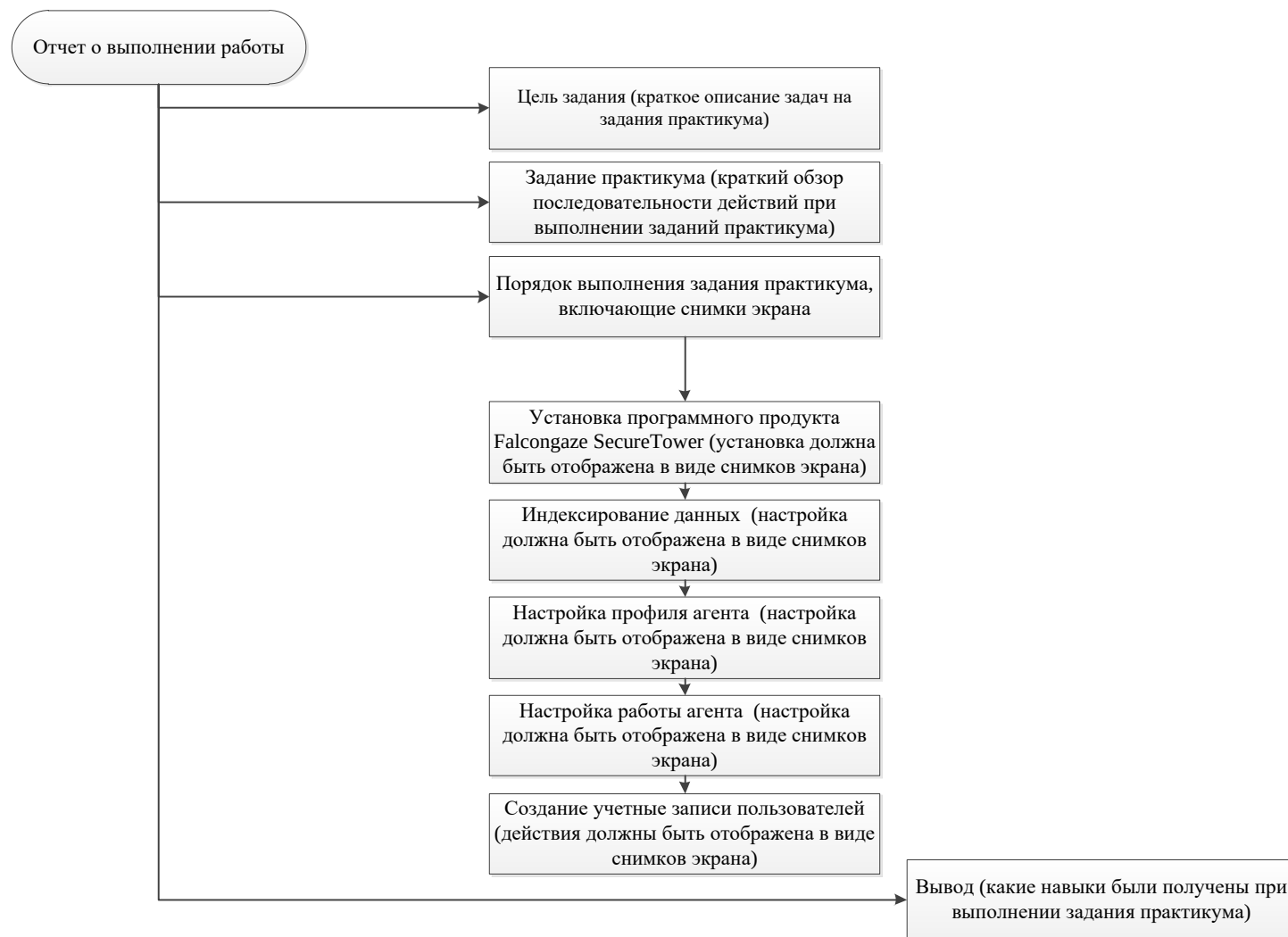


Рисунок Г.1 – Структура отчета о выполнении практикума по порядку установки программного комплекса

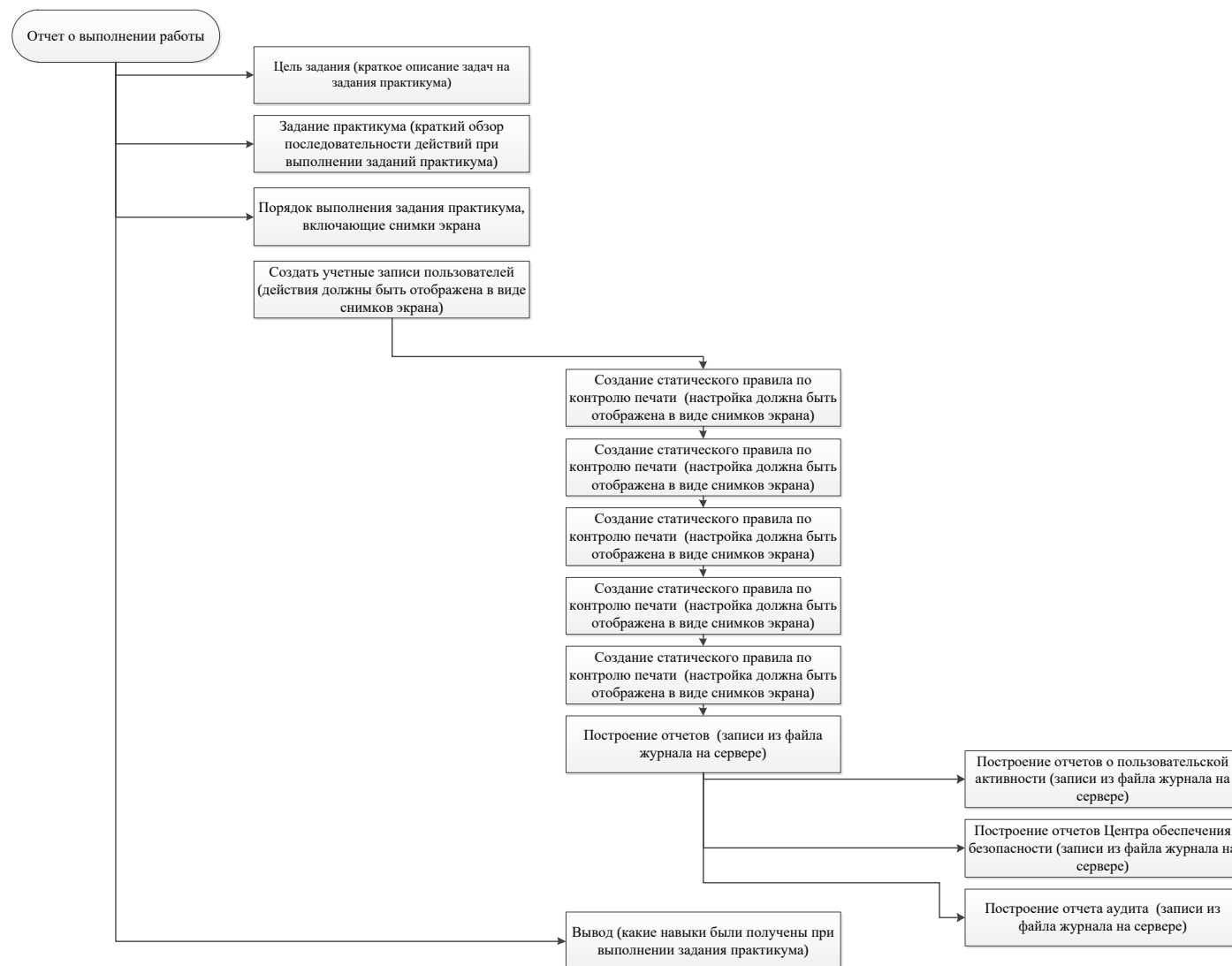


Рисунок Г.2 – Структура отчета о выполнении практикума по порядку создания политик безопасности

ПРИЛОЖЕНИЕ Д

(обязательное)

Контрольный экземпляр отчета по выполнению задания по установке программного комплекса Falcongaze SecureTower в локальной сети с доменной структурой

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
ФГБОУ ВО ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Кафедра «Информационная безопасность систем и технологий»

ОТЧЕТ
о выполнении лабораторной работы
«Установка программного комплекса Falcongaze SecureTower локальной сети с
доменной структурой»

Дисциплина:

Группа:

Выполнил:

Количество баллов:

Дата сдачи:

Принял:

Пенза, 2018

Цель практического задания – получить навыки по установке программного комплекса Falcongaze SecureTower в локальной сети с доменной структурой.

Задание включает:

- установку программного комплекса Falcongaze SecureTower;
- индексирование данных;
- настройку профиля агента;
- настройку контроля накопителей и устройств;
- настройку перехвата входящего трафика;
- настройку контроля сетевого трафика;
- настройку активности рабочего стола;
- создание учетных записей пользователей.

Порядок выполнения задания

Показать в виде снимков экрана результаты установки программного комплекса Falcongaze SecureTower.

Показать в виде снимков экрана результат индексирования данных в консоли администратора Falcongaze SecureTower.

Показать в виде снимков экрана результаты настройки профиля агента Falcongaze SecureTower.

Показать в виде снимков экрана результаты создания учетных записей пользователей.

Вывод:

ПРИЛОЖЕНИЕ Е

(обязательное)

Контрольный экземпляр отчета по выполнению задания по созданию политики безопасности программного комплекса Falcongaze SecureTower и применение их для контроля устройств

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
ФГБОУ ВО ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Кафедра «Информационная безопасность систем и технологий»

ОТЧЕТ
о выполнении лабораторной работы
«Создание политики безопасности программного комплекса Falcongaze
SecureTower и применение их для контроля устройств»

Дисциплина:

Группа:

Выполнил:

Количество баллов:

Дата сдачи:

Принял:

Пенза, 2018

Цель практического задания – получить навыки по созданию политики безопасности программного комплекса Falcongaze SecureTower и применение их для контроля устройств.

Задание включает:

- создание учетных записей локальных пользователей;
- создание статического правила по ограничению времени печати и количества страниц;
- создание статического правила по ограничению времени печати, количества страниц и по типу файла;
- создание статического правила по ограничению времени печати, количества документов, типа файла и статуса документа;
- создание отчета по активности пользователя;
- создание отчета Центра обеспечения безопасности;
- создание отчета аудита;
- вывод по результатам выполнения практического задания.

Порядок выполнения задания

Показать в виде снимков экрана результаты создания учетных записей локальных пользователей.

Показать в виде снимков экрана результаты создания статических правил.

Показать в виде снимков экрана результат сборки отчетов.

Показать в отчете о выполнении лабораторной работы результаты отчетов по активности пользователей, Центра обеспечения безопасности и аудита.

Вывод:

ПРИЛОЖЕНИЕ Ж

(обязательное)

Порядок проверки выполнения заданий практикума



Рисунок Ж.1

ПРИЛОЖЕНИЕ И

(обязательное)

Сценарии для автоматизированного развертывания ВМ

И.1 Сценарий для развертывания ВМ w2k12r2-fgst

```
@echo off

rem *****

rem Universal script for VMs

rem *****

set VHDTYPE="immutable"
set VHDPATH="C:\\w2k12r2-fgst.vdi"


set VMNAME=" w2k12r2-fgst"
set OS_TYPE="Windows2012_64"
REM set OS_TYPE="Windows"


set MEMORY="2048"
set VIDEO="128"
set _ACPI="on"
set _IOAPIC="on"
set _PAE="on"
set _HWVIRTEX="on"
set _VTXVID="on"
set netadapter="Intel PRO/1000 VT Server (82545EM)"


set SHAREPATH="D:\\share"
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% --hvwrtex  
%_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
```

И.2 Сценарий для развертывания ВМ win81-st1

@echo off

rem *****

rem Universal script for VMs

rem *****

set VHDTYPE="immutable"

set VHDPATH="C:\\ win81-st1.vdi"

set VMNAME=" win81-st1"

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 VT Desktop (82540EM)"

set SHAREPATH="D:\\share"

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% --hvwrtex  
%_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
```

И.3 Сценарий для развертывания ВМ w2k3st-srv

@echo off

rem *****

rem Universal script for VMs

rem *****

set VHDTYPE="immutable"

set VHDPATH="C:\\ w2k3st-srv.vdi"

set VMNAME=" w2k3st-srv"

set OS_TYPE="Windows2003_32"

REM set OS_TYPE="Windows"

set MEMORY="512"

set VIDEO="16"

set _ACPI="on"

set _IOAPIC="on"

set _PAE="on"

set _HWVIRTEX="on"

set _VTXVID="on"

set netadapter="Intel PRO/1000 VT Server (82545EM)"

set SHAREPATH="D:\\share"

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% --hvwrtex  
%_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 К
(обязательное)
Протокол проверки в системе Антиплагиат