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 100503 –	Информационная безопасность автоматизированных систем
Специализация -	Защищенные автоматизированные системы управления

ДИПЛОМНАЯ РАБОТА

на тему

ПРАКТИКУМ ПО ПРИМЕНЕНИЮ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ ПРОГРАММНОГО СРЕДСТВА ЗАЩИТЫ ZECURION ZLOCK ДЛЯ КОНТРОЛЯ И ПРЕДОТВРАЩЕНИЯ УТЕЧЕК ИНФОРМАЦИИ

Студент _____ Забирова Анна Александровна

Руководитель _____ Фатеев А.Г.

Нормоконтролёр _____ Фатеев А.Г.

Рецензент начальник НИС _____ Зорин А.Н.

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

Заведующий кафедрой _____ С.Л. Зефиров

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

Секретарь ГЭК _____ А.П. Иванов

Пенза 2017

СОДЕРЖАНИЕ

Введение……....8

1 Обзор систем контроля по защите информации от ее утечки…….....10

1.1 Общая характеристика DLP систем……..10

1.2 Этапы развития DLP-систем……..10

1.3 Типовые функциональные возможности систем контроля и предотвращения утечек информации …….13

1.4 Структура и компоненты систем контроля и предотвращения утечек информации…….....16

1.5 Сравнение систем контроля и средств защиты информации от утечки информации……...17

1.6 Применение систем контроля и предотвращения утечек информации……18

2 Функции, реализуемые программным комплексом Zecurion Zlock……20

2.1 Общая характеристика и назначение системы контроля и предотвращения утечек информации Zecurion Zlock……20

2.2 Структура и компоненты систем контроля и предотвращения утечек информации Zecurion Zlock……..21

2.2.1 Консоль управления……..21

2.2.2 Клиентский модуль……...21

2.2.3 Сервер журналов……...21

2.2.4 Сервер поиска……22

2.2.5 Сервер конфигураций……...22

2.3 Принцип работы Zecurion Zlock……23

2.3.1 Политики и правила доступа Zecurion Zlock ……23

2.3.2 Применение политик и приоритеты……25

2.3.3 Теневое копирование файлов и печати……...26

2.3.4 Журналирование и обработка файловых операций…...26

2.3.5 Типы устройств……27

2.3.6 Каталог устройств…….28
2.3.7 Мониторинг……...28
2.3.8 Конфигурации……...29
2.3.9 Шифрование файлов……29
2.3.10Консоль управления……..29
3 Описание подготовки лабораторного стенда, используемого при проведении лабораторных работ…….31
3.1 Установка VirtualBox и Extension Pack…….....31
3.2 Процесс создания виртуальных машин с использованием ПО Oracle VM VirtualBox 4.3……..34
3.3 Установка гостевых ОС……..39
3.4 Настройка виртуальной локальной сети……...39
3.5 Настройка гостевых ОС……..41
3.6 Установка системы контроля и предотвращения утечек информации Zecurion Zlock……..45
3.7 Результат создания виртуального стенда…….45
4 Порядок выполнения задания по применению программного комплекса Zecurion Zlock, для выявления и предотвращения утечек информации……..……47
4.1 Создание учетных записей пользователей……47
4.2 Включение и настройка аудита…….48
4.3 Создание политики доступа к устройству……....50
5 Порядок выполнения задания по изучению функций мониторинга и защиты агентов, реализуемых программным комплексом Zecurion Zlock……..61
5.1 Настройка отображения компьютеров домена и параметров соединения с компьютерами домена……...61
5.2 Настройка сервера конфигураций…….62
5.3 Настройка сервера журналов и отображение записей в журнале событий …….....68
5.4 Настройка задач мониторинга……..…....73

5.5 Просмотр текущего статуса компьютеров……..76
5.6 Изменение конфигурации……..77
5.7 Экспорт данных, буфер обмена и просмотр конфигурации...77
6 Описание порядка выполнения заданий практикума и результатов выполнения заданий……..……79
6.1 Порядок выполнения заданий практикума……...79
6.2 Порядок выполнения практического задания по применению программного комплекса Zecurion Zlock для выявления и предотвращения утечек информации……...79
6.2.1 Начало выполнения задания практикума……. …….79
6.2.2 Создание политики доступа к устройству ……80
6.2.3 Проверка настроек политики доступа на защищаемом компьютере……..80
6.2.4 Порядок выполнения задания в виде UML-диаграммы……80
6.3 Порядок выполнения практического задания по изучению функций мониторинга и защиты агентов, реализуемых программным комплексом Zecurion Zlock……...81
6.3.1 Начало выполнения задания практикума……...81
6.3.2 Настройка сервера конфигураций……...81
6.3.3 Создание задач мониторинга……...82
6.3.4 Порядок выполнения задания в виде UML-диаграммы……..82
7 Описание структуры и содержания отчета о выполнении практических заданий……...83
7.1 Общий перечень данных, содержащихся в отчете……..83
7.2 Структура отчета по выполнению задания по применению функциональных возможностей программного средства защиты Zecurion Zlock для контроля и предотвращения утечек информации……...83

7.3 Структура отчета по выполнению задания по изучению функций мониторинга и защиты агентов, реализуемых программным комплексом Zecurion Zlock……...84

8 Определение порядка контроля выполнения практического задании.85

8.1 Общий порядок контроля……...85

8.2 Порядок контроля практического задания по применению программного комплекса Zecurion Zlock для выявления и предотвращения утечек информации……...85

8.3 Порядок контроля практического задания по изучению функций мониторинга и защиты агентов, реализуемых программным комплексом Zecurion Zlock……...86

9 Подготовка сценария для автоматизированного развертывания виртуальных машин……..89

Список использованных источников…….90

Приложение А Структура виртуального стенда……..91

Приложение Б UML-диаграмма последовательности действий выполнения задания по применению программного комплекса Zecurion Zlock для выявления и предотвращения утечек информации…….93

Приложение В UML-диаграмма последовательности действий выполнения задания по изучению функций мониторинга и защиты агентов, реализуемых программным комплексом Zecurion Zlock……..…….....95

Приложение Г Структура отчета о выполнении заданий практикума..….97

Приложение Д Контрольный экземпляр отчета по выполнению задания по применению программного комплекса Zecurion Zlock для выявления и предотвращения утечек информации……..99

Приложение Е Контрольный экземпляр отчета по выполнению задания по изучению функций мониторинга и защиты агентов, реализуемых программным комплексом Zecurion Zlock…….103

Приложение Ж Порядок проверки выполнения заданий практикума….10

Приложение И Сценарии для автоматизированного развертывания ВМ……115

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

DLP – Data Loss Prevention (действия по предотвращению утечки информации);

DNS – Domain Name System (система доменных имен);

HTTP – Hyper Text Transfer Protocol (протокол передачи гипертекста);

SMTP - Simple Mail Transfer Protocol (простой протокол передачи почты);

VM – Virtual Machine (виртуальная машина);

ZL – Zecurion Zlock;

БД – база данных;

ВМ – виртуальная машина;

ИБ – информационная безопасность;

ИС – информационная система;

ИТ – информационная технология;

ОС – операционная система;

ПК – программный комплекс;

ПО – программное обеспечение.

ВВЕДЕНИЕ

Для контроля и предотвращения несанкционированных попыток передачи данных за пределы локальной сети предназначены системы контроля и предотвращения утечек информации (Data Loss Prevention - DLP).

В последнее время такие системы защиты информации получают все большее распространение. Они зачастую рассматриваются как замена традиционным классическим средствам защиты информации. Принцип работы этих механизмов идентичен, однако DLP-системы основаны на другом подходе к контролю за использованием защищаемых информационных ресурсов.

Применение систем контроля и предотвращения утечек информации основывается на анализе автоматизированной системы и выявлении возможных каналов передачи информации, использование которых может нарушить безопасность информации и нанести ущерб. Следует отметить, что системы контроля и предотвращения утечек информации также, как и традиционные СЗИ от НСД, реализуют управление доступом, основанное на формальных атрибутах безопасности. Однако принципиальным отличием СЗИ от НСД и систем контроля и предотвращения утечек информации является их установка, ввод в действие и последующая эксплуатация.

Ключевыми отличиями при сравнении СЗИ от НСД и систем контроля и предотвращения утечек информации являются контроль за содержанием информационного потока, возникающего при доступе пользователь к защищаемым ресурсам, типовая структура и типовые функциональные возможности, которые определяются с учетом различных факторов, настройка, которая в свою очередь является более сложной и требует корректировки для обеспечения корректного контроля.

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

ВКР посвящена разработке практикума, который посвящен применению программного комплекса Zecurion Zlock для выявления и предотвращения утечек информации, а также изучению функции мониторинга и защиты агентов, реализуемых Zecurion Zlock.

Для изучения программного комплекса Zecurion Zlock используется виртуальный лабораторный стенд, включающий несколько виртуальных машин, объединенных в локальную сеть.

Для выполнения задания ВКР были подготовлены виртуальные машины и составлены описания двух заданий, которые входят в состав практикума.

1 Обзор систем контроля по защите информации от ее утечки

1.1 Общая характеристика DLP систем

DLP расшифровывается как Data Loss Prevention и используется для обозначения продуктов и систем для защиты от утечек информации.

Технология DLP – это технология предотвращения утечек информации из информационной системы за ее пределы, а также технические средства (программные или программно-аппаратные) реализующие эту технологию.

DLP-системы строятся на анализе потоков данных, пересекающих периметр защищаемой информационной системы. При детектировании в этом потоке информации, которая не должна передаваться за пределы защищаемой ИС, срабатывает активный компонент системы, и передача сообщения (пакета, потока, сессии) блокируется.

Для обозначения средств защиты информации, реализующих такую технологию, используются следующие наименования:

- Data Loss Protection (DLP);
- Data Leak Prevention (DLP);
- Data Leakage Protection (DLP);
- Information Leak Protection (ILP);
- Information Protection and Control (IPC).

Используется также название таких средств защиты информации – системы (средства) контроля и предотвращения утечек информации.

DLP-системы направлены на минимизацию рисков внутренних угроз информационной безопасности. Утечка информации может происходить не только по злому умыслу, но и по невнимательности, к примеру, сотрудников или незнанию правил информационной безопасности. Однако DLP-система предусматривает все возможные сценарии и защищает как от случайных утечек, так и от намеренной кражи информации сотрудниками.[1]

1.2 Этапы развития DLP-систем

Необходимость защиты от внутренних угроз была очевидна на всех этапах развития средств информационной безопасности. Однако первоначально

внешние угрозы считались более опасными. В последние годы на внутренние угрозы стали обращать больше внимания, и популярность DLP-систем возросла. Специализированные технические средства для защиты от внутренних угроз стали массово выпускаться только после 2000 года. Ранее задача предотвращения утечек конфиденциальных данных из информационных систем решались в основном тремя способами. Во-первых, методом ограничения прав доступа субъектов к различным информационным ресурсам (ролевое управление, дискреционный и мандатный допуск к ресурсам) во-вторых, за счет использования программного обеспечения (ПО) контроля внешних устройств (USB, CDROM и пр.) – на уровне можно/нельзя использовать этот носитель, и, в третьих, за счет шифрования данных.

Однако данные способы статичны и позволяют обеспечить защиту конфиденциальной информации, только в местах ее хранения (Data-at-Rest), и не дают возможности контроля над процессом обработки и передачи информации.

В результате появились специализированные технологии и решения, которые могут контролировать данные в процессе обработки и передачи (Data-in-Motion) по различным каналам: HTTP, SMTP, передача данных на сменные устройства, печать на локальные и сетевые принтеры и т.д. При этом охват каналов должен быть как можно более полным, чтобы решение можно было назвать полноценным. Не менее важна и задача анализа передаваемой информации. Система должна реагировать только на конфиденциальную информацию и свободно пропускать информацию, которая не относится к этой категории.

Современные системы DLP (Data Leak Prevention) – это технологии, позволяющие предотвратить утечку из организации именно конфиденциальной информации. При этом информация, которая не попадает в категорию «конфиденциальная» может свободно передаваться по любым электронным каналам.

В течение последних нескольких лет использовалась разная терминология: Information Leakage Protection (ILP), Information Leak Protection (ILP), Information Leakage Detection & Prevention (ILDP), Content Monitoring and Filtering (CMF), Extrusion Prevention System (EPS) и др. Но наиболее точным термином принято считать Data Leak Prevention. В качестве русского аналога принято словосочетание «системы защиты конфиденциальных данных от внутренних угроз».

При этом, под внутренними угрозами подразумевают как умышленные злоупотребления, так и непреднамеренные действия сотрудников в рамках своих прав доступа к данным.

В истории развития DLP-технологий первыми появились технологии сетевого мониторинга – без возможности блокировки утечки через сетевые протоколы (HTTP, SMTP и пр.). В дальнейшем производители решений добавляли функции блокировки информации при передаче через сеть. Затем появились возможности контроля рабочих станций за счет внедрения программных «агентов», чтобы можно было предотвратить передачу конфиденциальной информации с этих устройств: контроль функций копирования фрагмента текста (copy/paste), снятия снимков экрана, а также контроль передачи информации на уровне приложений. В дальнейшем появились технологии поиска конфиденциальной информации на сетевых ресурсах и ее защиты, если информация обнаружена в тех местах, где ее не должно быть. Конфиденциальная информация при этом задается предварительно ключевыми словами, словарями, регулярными выражениями, «цифровыми отпечатками» и др. В результате поиска система может показать – где она обнаружила конфиденциальную информацию, и какие политики безопасности при этом нарушаются. Далее служба безопасности может принимать соответствующие меры, в соответствии с инструкцией по расследованию инцидентов по нарушению ИБ. Есть решения, которые не просто показывают наличие конфиденциальной информации в неположенном месте, а переносят эту информацию «в карантин» (по аналогии с

антивирусными системами), оставляя в файле, где была обнаружена информации, запись – куда перенесена конфиденциальная информация и к кому обратиться за получением доступа к этой информации.

В настоящее время на рынке представлено довольно много DLP-решений, позволяющих определять и предотвращать утечку конфиденциальной информации по тем или иным каналам. Однако действительно комплексных решений, покрывающих все существующие каналы, значительно меньше. В этих условиях чрезвычайно важным становится выбор технологии, обеспечивающей защиту от утечек конфиденциальной информации с максимальной эффективностью и минимальным количеством ложных срабатываний.[1]

1.3 Типовые функциональные возможности систем контроля и предотвращения утечек информации

Поиск защищаемой информации ограниченного доступа в информационной системе. При этом могут выполняться следующие действия:

– сканирование рабочих станций локальной сети, общих сетевых хранилищ;

– создание теневых копий найденных документов;

– удаление или перемещение конфиденциальных данных в карантин;

– использование специальных политик для зашифрованных файлов и файлов, защищённых паролем.

Контроль действий пользователей предусматривает:

– просмотр рабочего стола в режиме реального времени;

– протоколирование времени работы в приложениях.

Мониторинг и защита агентов включает:

– контроль работы, целостности, политик агентов;

– защита от выключения и удаления;

– маскировка агента в системе;

– возможность настройки реагирования на события.

При возникновении инцидента могут выполняться следующие действия:

– запись в журнал;

– сохранение файлов (теневое копирование);

– уведомление администратора безопасности;

– блокировка соединения.

Системы контроля и предотвращения утечек информации могут функционировать в различных режимах. Режимы работы обычно предусматриваются следующие:

– работа в режиме мониторинга (пассивный) – используется на этапе настройки системы для проверки и корректировки настроек, когда высока доля ложных срабатываний. В этом случае нарушения политик фиксируются, но ограничения на перемещение информации не налагаются;

– работа в режим блокировки (активный) – основной режим работы, при котором происходит блокировка действий, нарушающих политики безопасности, например, отправка конфиденциальной информации на внешний почтовый ящик.

Также предусматривается несколько режимов перехвата информации:

– сетевой перехват;

– перехват трафика через агенты на рабочих станциях;

– перехват трафика через интеграцию со сторонними сервисами;

– перехват в разрыв.

Системы контроля и предотвращения утечек информации реализуют возможности повышения производительности при обработке информации и обеспечения отказоустойчивого функционирования.

Производительность и отказоустойчивость достигается за счет:

– автоматического управления перехваченной информацией (например, посредством автоматической записи и индексации перехваченных данных, а также привязки информации к пользователям и компьютерам);

– контроль поступления перехваченной информации;

– возможность резервирования (при невозможности соединения с сервером, агенты могут сохранять перехваченные данные в собственное резервное хранилище либо может использоваться резервный сервер).

Системы контроля и предотвращения утечек информации реализуют возможности регистрации событий и последующего анализа накопленных сведений о событиях безопасности. Кроме того реализуется управление доступом к этой информации.

Работа с отчетами включает:

– разграничение прав на доступ к перехваченной информации;

– поиск похожего документа в архиве;

– статистика работы пользователей с установленными программами.

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.

Для анализа и поиска информации реализуются следующие технологии:

– поиск по составным регулярным выражениям (несколько регулярных выражений, объединённых логикой);

– лингвистический анализ (поиск слов по словарям), морфологический анализ (с учетом поддерживаемого языка);

– цифровые отпечатки документов (бинарные, текст).[2]

1.4 Структура и компоненты систем контроля и предотвращения утечек информации

Система DLP состоит из множества компонент. В состав типового решения систем контроля и предотвращения утечек информации, как правило, входят:

– центральный сервер управления (монитор обращений), выполняющий следующие функции:

  – объединение всех остальных компонентов DLP - решения в единую систему;

  – определение данных, содержащих конфиденциальную информацию;

  – создание, редактирование и распространение политик безопасности для работы с конфиденциальными данными;

  – реализация правил разграничения доступом;

  – сбор, хранение и обработку инцидентов, создание и рассылку отчетов;

  – предоставление ролевого доступа к управлению системой сотрудникам службы информационной безопасности;

– модули мониторинга и блокировки конфиденциальной информации, передаваемой по сетевым каналам. Они могут быть представлены как одним устройством, реализующим обе функции, так и отдельными (например, Network Monitor, Network Prevent for Web, Network Prevent for E-mail);

– агенты для рабочих станций и серверов, обеспечивающие контроль:

  – перемещения конфиденциальных данных на сменные носители информации (USB, CD/DVD и др.);

  – помещения данных в буфер обмена (функция «Вставка/Копирование»); функции снятия снимка с экрана («Print Screen»);

– контроль функции поиска конфиденциальных данных на локальных дисках.

Системы DLP на сегодняшний день достаточно эффективный инструмент для защиты конфиденциальной информации только в интеграции с другими сервисами безопасности и актуальность интегрированных решений будет со временем только увеличиваться.[2]

1.5 Сравнение систем контроля и средств защиты информации от утечки информации

DLP-системы обеспечивают отслеживание и пресечение следующих действий с защищаемыми документами:

– копирование, как целиком документов, так и фрагментов содержащейся в них информации;

– изменение документов, их атрибутов, содержащейся информации;

– пересохранение копий документов;

– попытки сделать снимки экрана документов;

– отправка документов или информации через веб-сервисы электронной почты;

– передача документов или информации через социальные сети;

– публикация документов или информации через веб-интерфейсы;

– печать документов на принтере;

– доступ к документам через ftp-соединения;

– копирование документов на любые внешние накопители – диски, флеш-накопители, на мобильные устройства;

– передача документов через сетевые соединения, включая беспроводные Bluetooth и Wi-Fi;

– передача документов в облачные хранилища.

В рамках функциональных возможностей такие внедрения имеют ряд преимуществ перед иными средствами и методами защиты информации – шифрованием, системами разграничения доступа и другими, а именно:

– осуществление контроля всех возможных каналов и способов передачи информации в электронном виде;

– контроль содержимого, а не документов, используя контентный анализ, анализ по словарям, лингвистический анализ, анализ транслитерации и многоязыковой анализ, выявление замаскированного текста и т.п. Это позволяет обнаружить информацию вне зависимости от видов и форматов ее хранения, передачи и способов сокрытия;

– автоматическое реагирование и пресечение обнаруженной утечки – интерактивное блокирование канала утечки (копирования, передачи, распечатки и т.п.), а не просто детектирование действий.

DLP-система может быть развернута в информационной инфраструктуре любого масштаба и сложности, она легко масштабируется без ущерба функциональным возможностям, работает в автономном режиме. Внедрение решения позволит:

– полностью контролировать использование конфиденциальной информации на всех этапах ее жизненного цикла, включая места хранения, применение, соблюдение принятых политик работы с ней;

– обеспечить надежную защиту от распространения конфиденциальной информации за пределы организации, немедленно пресекать соответствующие инциденты;

– повысить эффективность и безопасность использования конфиденциальной информации на основе аудита и собираемой статистики;

– повысить общий уровень информационной безопасности компании, выполнить требования регулирующей нормативной документации.[1]

1.6 Применение систем контроля и предотвращения утечек информации

Использование DLP системы наиболее актуально для организаций, где риск утечки конфиденциальной информации повлечет серьезный финансовый ущерб, ущерб репутации, а также для организаций, которые настороженно относятся к лояльности своих сотрудников. Решения класса DLP по

предотвращению утечек информации обеспечивают защиту такой конфиденциальной информации, как условия тендеров, заказы на услуги и решения, номера пластиковых карт, сведения о счетах клиентов, персональные данные сотрудников и клиентов, финансовые данные и т.д.

Помимо предотвращения утечек информации DLP система может выполнять контроль действий пользователей, анализ информационных потоков через электронную почту, социальные сети, внутрикорпоративные коммуникационные ресурсы, чаты и т.п. Ключевая задача DLP-систем - обеспечение соблюдения политики конфиденциальности, принятой в компании.[3]

2 Функции, реализуемые программным комплексом Zecurion Zlock

2.1 Общая характеристика и назначение системы контроля и предотвращения утечек информации Zecurion Zlock

Zecurion Zlock предназначен для разграничения доступа к аппаратным ресурсам компьютера и выявления ситуаций, связанных с нарушением корпоративных политик безопасности. Для различных устройств и классов устройств могут назначаться правила: разрешение или запрет доступа, доступ только на чтение, а также управление доступом на основе списка контроля доступа (access control list — ACL).

Кроме управления доступом к аппаратным ресурсам, Zlock обеспечивает контроль операций с файлами на USB-носителях и контроль печати документов. Контроль может быть организован как по типам файлов, так и по их содержимому. При контроле по содержимому файла выполняется контентный анализ текста, содержащегося в файле. На основе полученных результатов выполняются действия политик безопасности.

Сервер конфигураций Zlock позволяет централизовано управлять настройками и политиками Zlock для компьютеров вне зависимости от того, находятся ли они в домене или объединены в рабочие группы.

Для централизованного создания, редактирования, хранения и обновления словарей, шаблонов, цифровых отпечатков и др. применяется сервер поиска.

Zlock может создавать особое виртуальное пространство, которое обеспечивает автоматическое прозрачное шифрование носителей внутри него, и невозможность расшифровывания данных за его пределами. Зашифрованная информация доступна только на компьютерах, находящихся в таком пространстве.

Zlock с заданной периодичностью может формировать графические файлы, с изображением активных экранов пользователей.

При записи файлов на внешний носитель Zlock позволяет создавать теневые копии файлов. Также выполняется теневое копирование содержимого

буфера обмена, распечатываемых документов и контроль устройств, подключенных с помощью RDP (Remote Desktop Protocol).

Файлы из локального хранилища теневых копий могут быть переданы на сервер журналов для их дальнейшего хранения и просмотра.

Zlock контролирует доступ в интернет вне сети организации, разрешая доступ только по определенным VPN-каналам.[1]

2.2 Структура и компоненты систем контроля и предотвращения утечек информации Zecurion Zlock

2.2.1 Консоль управления

Консоль управления является основным средством управления работой системы и может быть установлена на любом компьютере. Запуск консоли выполняется из меню «Пуск» — «Программы» — «Zecurion». Для разграничения полномочий по управлению системой могут использоваться средства авторизации Microsoft Windows либо внутренний механизм — авторизация пользователей Zecurion.

На главной странице консоли управления при подключении к контролируемому компьютеру отображаются данные о версии, состоянии и основных настройках выбранного клиента.

2.2.2 Клиентский модуль

Клиентский модуль устанавливается на каждый контролируемый системой Zlock компьютер и обеспечивает применение политик доступа, т.е. выполняет разграничение доступа к портам и устройствам этого компьютера.

Клиентскому модулю соответствует значок в области уведомлений панели задач. Двойной щелчок мышью по нему открывает окно с перечислением всех доступных устройств и политик их использования.

Клиентский модуль обеспечивает информирование пользователя о работе Zlock и дает возможность создать запрос на доступ к устройству.

2.2.3 Сервер журналов

Сервер журналов предназначен для централизованного хранения и обработки событий, информация о которых передается клиентскими модулями

Zlock, сервером конфигураций, сервером поиска, модулем мониторинга и другими компонентами Zlock. Он обеспечивает одновременную работу большого количества клиентов с одним хранилищем журналов и быструю обработку запросов по просмотру журналов администратором.

Сервер журналов может записывать информацию о событиях на сервер баз данных (Microsoft SQL Server или Oracle), или в локальный XML-файл.

Для управления сервером журналов, просмотра и анализа содержимого сервера журналов используется консоль управления.

2.2.4 Сервер поиска

Сервер поиска предназначен для работы с инструментами контент-анализа — словарями, цифровыми отпечатками и др. Он обеспечивает создание, редактирование и обновление указанных массивов данных.

Клиентский компьютер периодически запрашивает с сервера поиска средства контент-анализа. В случае, когда словари, шаблоны или отпечатки изменены, происходит их загрузка с сервера. Настройка сервера поиска для клиентского компьютера выполняется на сервере конфигураций.

2.2.5 Сервер конфигураций

Сервер конфигураций предназначен для централизованного управления конфигурациями Zlock.

Для управления, просмотра и настройки сервера конфигураций используется консоль управления.

Сервер конфигураций периодически запрашивает с сервера поиска словари, шаблоны, отпечатки и таблицы замен и распространяет их в соответствии с политиками и настройками, заданными для клиентских модулей.[2]

2.3 Принцип работы Zecurion Zlock

2.3.1 Политики и правила доступа Zecurion Zlock

2.3.1.1 Политика доступа определяет связь устройства или файла с правилами доступа к нему.

В системе используются два типа политик — политики доступа к устройствам и политики контроля файлов. Политика доступа к устройствам управляет доступом к устройствам, политика контроля файлов управляет операциями с файлами на USB-носителях и печатью документов.

2.3.1.2 Параметры политики доступа к устройствам.

Каждая политика доступа к устройствам обладает следующими параметрами:

– уникальное имя политики;

– приоритет — число в диапазоне от 0 до 32 (0 — наименьший, 32 — наивысший приоритет). Если устройство подпадает более чем под одну политику, то применяется только политика с наивысшим приоритетом. Специальная политика доступа к устройствам — политика по умолчанию, предназначена для определения доступа к устройствам, которые не попали ни в одну из существующих политик. Её приоритет ниже, чем политики с приоритетом 0;

– набор описаний устройств, к которым будет применяться политика;

– расписание политики, задающее её время действия;

– опция Постоянная политика определяет, будет ли данная политика удаляться, если политики будут загружены через групповые политики или с сервера конфигураций;

– настройки теневого копирования, обработки файловых операций и шифрования файлов;

– правило применения политики в зависимости от нахождения компьютера в локальной сети или за ее пределами;

– флаг отключения контроля файловых операций для устройства;

– тип доступа к устройствам.

При записи действий, выполняемых в рамках политики доступа к устройствам, происходит протоколирование всех файловых операций. Полученная информация используется для последующего анализа

2.3.1.3 Параметры политики контроля файлов.

Политики контроля файлов, также как и политики доступа к устройствам, имеют уникальное имя, приоритет, разрешенные операции и характеристику «Постоянная политика». При работе с файловыми политиками контролируются операции по типам файлов и по содержимому файлов, которые содержат текст, а также выполняется контроль печати документов.

При контроле доступа по содержимому файла, Zlock выполняет контентный анализ текста, содержащегося в файле. По результатам анализа происходит разрешение или запрет чтения, записи или печати согласно политике. Контролировать доступ можно только для файлов на USB-носителях.

Контроль по типу файлов для печати не поддерживается. Печать контролируется только по содержимому файлов.

При контент-анализе, кроме поиска текста с использованием морфологического анализа, спецсимволов и транслитерации могут быть использованы словари, цифровые отпечатки или шаблоны.

При чтении, записи или печати файлов или документов, подпадающих под действие политики можно выполнять операции журналирования и теневого копирования. При формировании политики контроля файлов, записываемые файлы, подпадающие под данную политику, могут быть зашифрованы.

При использовании функции журналирования в политиках доступа к устройству выполняется журналирование всех файловых операций.

При использовании политики контроля файлов журналируются только те операции, которые подпадают под действие политики. Иными словами, если файл не содержит искомый текст, действия с ним журналироваться не будут.[2]

2.3.2 Применение политик и приоритеты

2.3.2.1 Применение политики доступа к устройствам.

При подключении устройства к компьютеру Zlock просматривает все описания устройств и пытается найти политику, к которой можно его отнести:

– если устройство подходит более чем к одной политике, то выбирается политика с максимальным приоритетом;

– если устройство подходит более чем к одной политике с одинаковым наивысшим приоритетом, то выбирается политика с максимальным запрещающим уровнем доступа (уровни доступа в порядке возрастания запрета: полный доступ, выборочный доступ, только чтение, запрет);

– если ни одной подходящей политики не найдено, то применяется Политика по умолчанию.

2.3.2.2 Применение политики контроля файлов и печати.

Применение политики контроля файлов и печати происходит следующим образом:

– если обрабатываемый файл подпадает под действие одной или нескольких политик, то выбирается политика с максимальным приоритетом;

– если не найдено ни одной политики, под действие которой подпадает файл, то пользователю разрешается полный доступ для работы с такими файлами;

– если найдено несколько политик с одинаковым максимальным приоритетом, то среди этой группы выбирается политика с максимальным запрещающим уровнем доступа, при этом у выбранной политики будут выставлены флаги журналирования и создания теневой копии, если они выставлены, хотя бы в одной из политик группы. Уровни доступа в порядке возрастания запрета: полный доступ, выборочный доступ, только чтение, запрет.

При отсутствии файловых политик всем пользователям предоставляется полный доступ ко всем файлам.

2.3.3 Теневое копирование файлов и печати

Zlock позволяет обрабатывать и журналировать операции с файлами и принтерами и создавать теневые копии копируемых файлов и распечатываемых документов.

В Zlock поддерживается:

- теневое копирование файлов;
- теневое копирование записи на CD/DVD;
- теневое копирование печати;
- теневое копирование буфера обмена;
- теневое копирование файлов, записываемых на RDP-диски.

Теневое копирование файлов предназначено для контроля информации, которая записывается на внешние носители. При включенной опции теневого копирования файл перед записью на сменный носитель сначала копируется в локальное хранилище — каталог на локальном жестком диске.

Теневое копирование записи на CD/DVD предназначено для контроля информации, которая записывается на диск. При включенной опции теневого копирования параллельно с записью данных на CD/DVD создается образ диска. После завершения записи файлы извлекаются из образа диска и копируются в локальное хранилище — каталог на локальном жестком диске. Теневое копирование печати предназначено для контроля документов, которые печатаются на локальных или сетевых принтерах. При включенном теневом копировании печати данные сохраняются в локальном хранилище в виде файлов с изображением в формате PDF.

Из локального хранилища файлы могут быть перенесены на сервер журналов или Microsoft SQL Server. Параметры операции сохраняются для последующего анализа.[2]

2.3.4 Журналирование и обработка файловых операций

В свойствах каждой политики можно настроить журналирование и обработку файловых операций и печати.

Обработка файловых операций возможна для устройств, имеющих файловую систему (флеш-диски, жесткие диски, дискеты, RDP-диски и т.д.), при работе с MTP-устройствами при записи на CD/DVD и при печати документов на принтере.

В зависимости от типа доступа к съемным носителям журналируются следующие операции с файлами и каталогами:

- создание файла;
- запись в файл;
- чтение из файла;
- переименование файла;
- удаление файла;
- создание каталога;
- удаление каталога;
- переименование каталога.

При записи на CD/DVD список записанных файлов извлекается из образа диска, созданного при теневом копировании. В папке локального хранилища необходимо наличие достаточного количества свободного места для создания образа диска.

При использовании функции журналирования в политике доступа к устройству выполняется журналирование файловых операций только для USB-устройств, имеющих файловую систему.

При применении политики контроля файлов журналируются только операции чтения или записи с теми файлами, которые подпадают под эту политику.

2.3.5 Типы устройств

Политики могут быть применены как к отдельному физическому устройству (порты COM и LPT, контроллеры SCSI, сетевые устройства, жесткие диски и т.д.) или принтеру, так и к группе устройств, имеющих

определенные характеристики. К таким характеристикам, позволяющим объединить устройства, можно отнести:

– тип устройства (например, накопитель, к которым относятся все накопители с интерфейсом USB, в том числе брелки флэш-памяти, MP3-плееры, фотокамеры и т.п.);

– отдельные характеристики USB-устройств, в частности: класс, интерфейс, подкласс, протокол, идентификатор производителя, идентификатор продукта, название производителя, название продукта, серийный номер устройства;

– классы физических устройств (например, все устройства чтения смарт-карт).

2.3.6 Каталог устройств

Каталог устройств используется для хранения списка аппаратных устройств с их характеристиками, подключаемых пользователями к отдельным компьютерам в сети.

На основе этих данных в политику можно добавить любые устройства из каталога.

2.3.7 Мониторинг

Zlock позволяет вести мониторинг состояния удаленных компьютеров для выявления несанкционированных действий. Через заданные промежутки времени модуль мониторинга, устанавливаемый совместно с консолью администратора, производит опрос клиентских модулей и выявляет ситуации несанкционированного изменения конфигурации Zlock или нарушения его целостности.

При наступлении такой ситуации модуль мониторинга выполняет действия, заранее заданные в окне Обработка событий при мониторинге. Такими действиями могут быть журналирование в системный журнал или в файл, журналирование на сервер, отправка письма или вызов скрипта.

Текущий статус опрашиваемых компьютеров отображается в консоли управления Zlock.

2.3.8 Конфигурации

Конфигурация представляет собой файл с расширением .zcfg, который содержит наборы политик доступа к различным устройствам, файловых политик, правил доступа, методов обработки событий и другие настройки. Этот файл используется для распространения настроек на компьютеры, группы компьютеров, сервера конфигурации и групповые политики.

2.3.9 Шифрование файлов

Zlock может автоматически зашифровывать файлы, записываемые на внешние носители. Расшифровывание таких файлов может быть выполнено на компьютерах с установленным клиентским модулем Zlock и подключенных к локальной сети организации.

Ключ шифрования хранится на сервере конфигураций и загружается на клиентский модуль при старте ОС. Клиентский модуль сохраняет ключ шифрования в защищенном локальном хранилище, что позволяет выполнять шифрование даже при временной недоступности сервера.

Новые ключи шифрования могут быть сгенерированы автоматически с заданной периодичностью. В этом случае на сервере конфигураций будут храниться ранее использованные ключи, чтобы можно было открыть зашифрованные ими файлы.

Зашифровывание файла при записи осуществляется только в том случае, если файл или устройство подпадают под политику с включенным шифрованием.

Если опция шифрования включена, а ключ для шифрования отсутствует на клиентском компьютере и его не удалось загрузить с сервера конфигураций, то запись файла на носитель не выполняется.

2.3.10 Консоль управления

Консоль управления выполняет администрирование Zlock. Используя консоль можно редактировать политики доступа и настройки Zlock, управлять сервером журналов, сервером конфигураций и сервером поиска. Консоль может

соединяться с отдельными компьютерами и администрировать установленные на них клиентские модули Zlock.

В меню «Вид» консоли управления можно выбрать способ группировки элементов в левой части консоли управления. Существует два вида группировки — «По приложениям» и «По компьютерам». В виде «По приложениям» в меню «Вид» появляется опция «Отображать домены и группы в приложениях».[2]

3 Описание подготовки лабораторного стенда, используемого при проведении лабораторных работ

3.1 Установка VirtualBox и Extension Pack

Для создания ВМ, входящих в состав виртуального стенда использовалось ПО виртуализации Oracle VM VirtualBox 4.3.30. Дистрибутив был загружен с официального ресурса компании Oracle [4]. Данная программа является бесплатной, проста в установке, многофункциональна и удобна для использования.

Для установки необходимо запустить на исполнение файл установки. После запуска данной программы необходимо нажать кнопку «Next», как показано на рисунке 1.

Рисунок 1 – Установка Oracle VM VirtualBox 4.3.30

Далее было выведено диалоговое окно, в котором требовалось выбрать компоненты установки. Программа может включать следующие компоненты:

– VirtualBox Application - основной компонент VirtualBox, без него запуск программы будет невозможен;

– VirtualBox USB Support – компонент поддержки USB драйверов;

– VirtualBox Networking – компонент поддержки драйверов сетевых устройств;

– VirtualBox Python 2.x Support – компонент поддержки Python.

Для установки выбирается вариант, который включает все компоненты, необходимые для функционирования программы. Установка остается без изменений, после чего нажата кнопка «Next», как показано на рисунке 2.

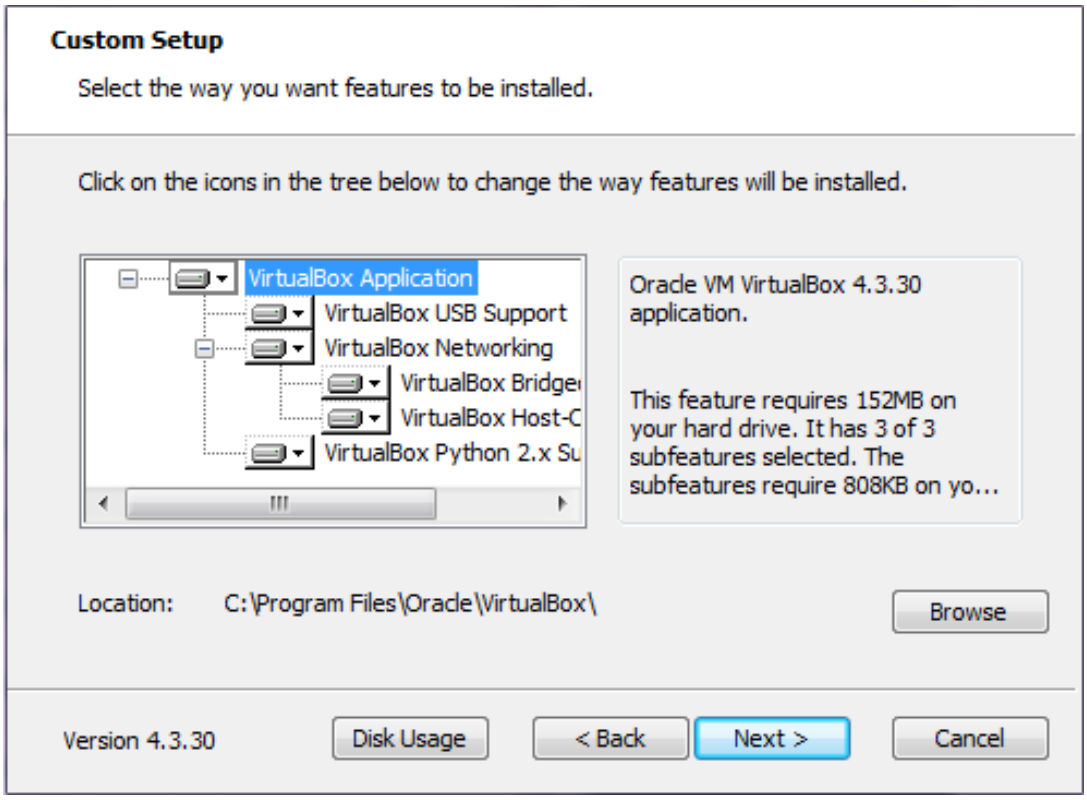

Рисунок 2 – Выбор компонентов установки

Затем выбраны места, где будут созданы ярлыки запуска данной программы. Путь установки остается без изменений, как показано на рисунке 3. По умолчанию установлены параметры:

– «Create a shortcut on the desktop» – выбор этой опции позволяет после установки автоматически поместить ярлык программы на «Рабочий стол»;

– «Create a shortcut in the Quick Launch Bar» - выбор этой опции позволяет после установки автоматически поместить ярлык программы в строку быстрого доступа;

– «Register file associations» - выбор этой опции позволяет после установки программы зарегистрировать в системе все ассоциированные с программой типы файлов.

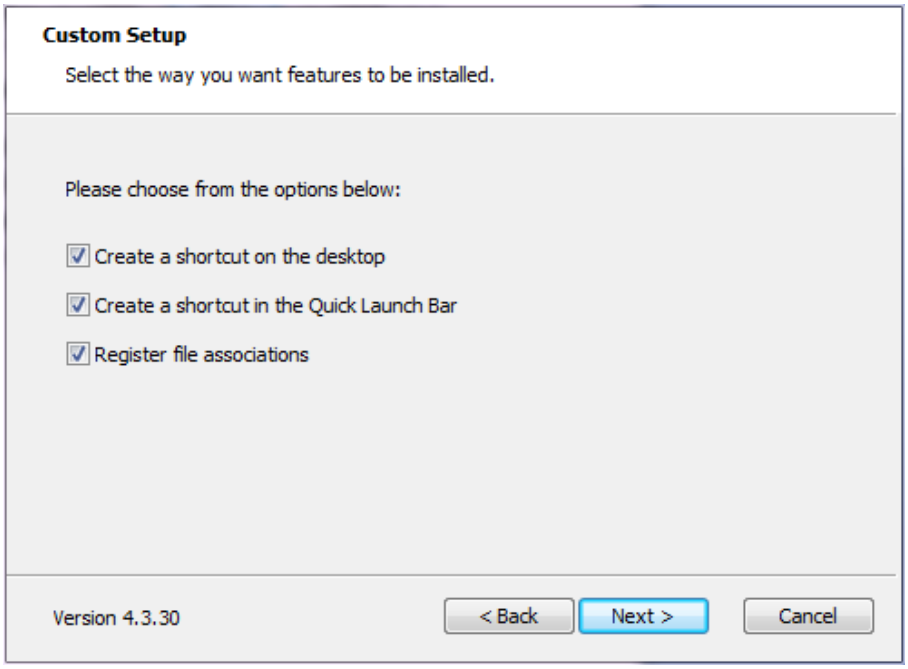

Рисунок 3 – Выбор создания ярлыков

После выбора создания ярлыков, было выведено окно предупреждения на установку драйверов сетевых устройств, выбрана кнопка «Yes», как показано на рисунке 4.

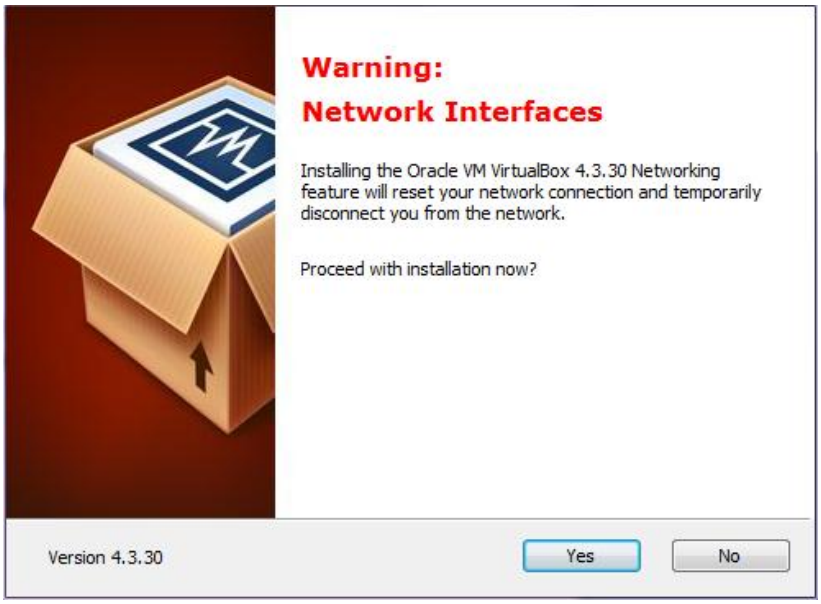

Рисунок 4 – Окно подтверждения установки

Для установки Oracle VM VirtualBox 4.3.30 выбрана кнопка «Install». Для завершения установки нажата кнопка «Finish».

После установки программного обеспечения Oracle VM VirtualBox 4.3.30 необходимо установить пакет расширений VirtualBox Extension Pack, который обеспечивает возможность использования подсистем USB, создание общей

папки обмена между гостевой и основной ОС. Кроме того пакет расширений обеспечивает корректный запуск ВМ.

Для установки файл пакета был скопирован в каталог установки ВМ и запущен на выполнение. Установка осуществляется в автоматическом режиме без вмешательства пользователя.

3.2 Процесс создания виртуальных машин с использованием ПО Oracle VM VirtualBox 4.3

После установки ПО VirtualBox оно было использовано для создания следующих ВМ:

– одна ВМ с гостевой ОС Windows Server 2003;

– две ВМ с гостевой ОС Windows XP.

Для создания ВМ необходимо запустить компонент ПО VirtualBox, который используется для создания и настройки ВМ, – VirtualBox Manager (см. рисунок 5).

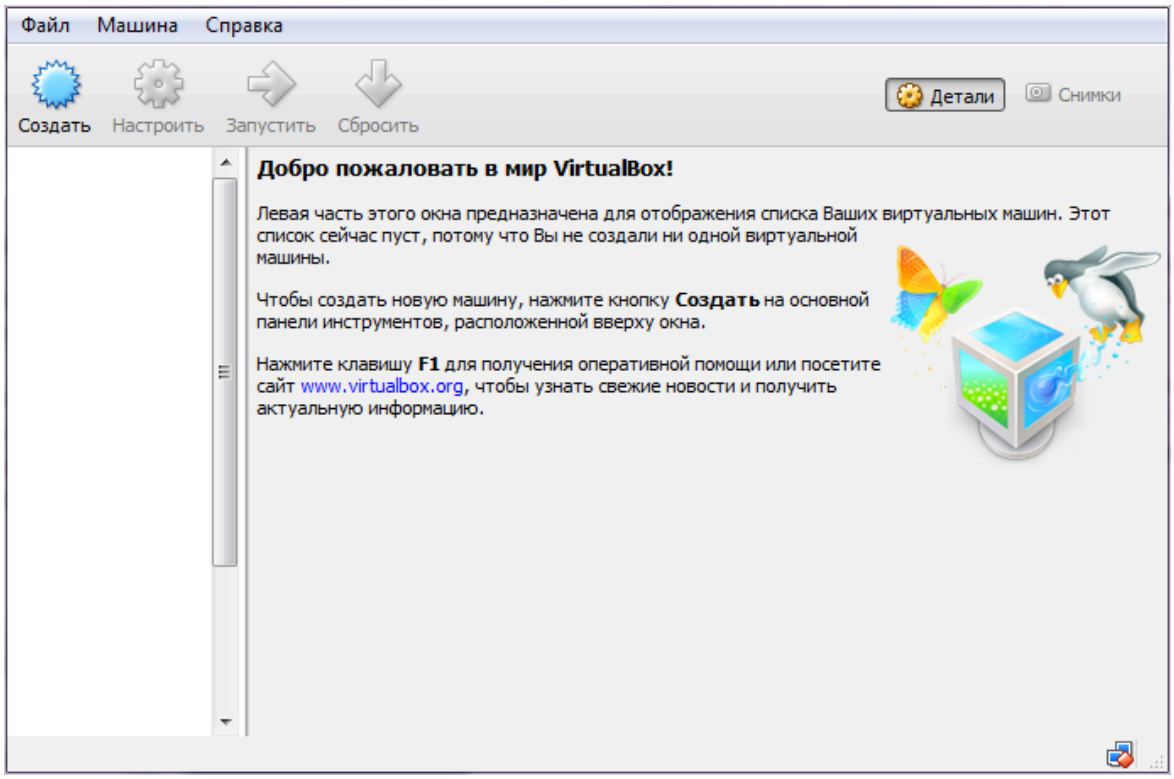

Рисунок 5 – Рабочее окно Oracle VM VirtualBox

Сначала необходимо настроить каталог, в котором хранятся конфигурационные файлы. Для этого был выбран пункт меню «Файл –

Настройки… – Общие». Выбрана папка для машин, в которой будут сохраняться конфигурационные файлы.

Для создания виртуальной машины необходимо нажать кнопку «Создать» в панели инструментов программы Virtual Box Manager. В диалоговом окне необходимо указать имя новой виртуальной машины, выбрать тип ОС, версию ОС (см. рисунок 6).

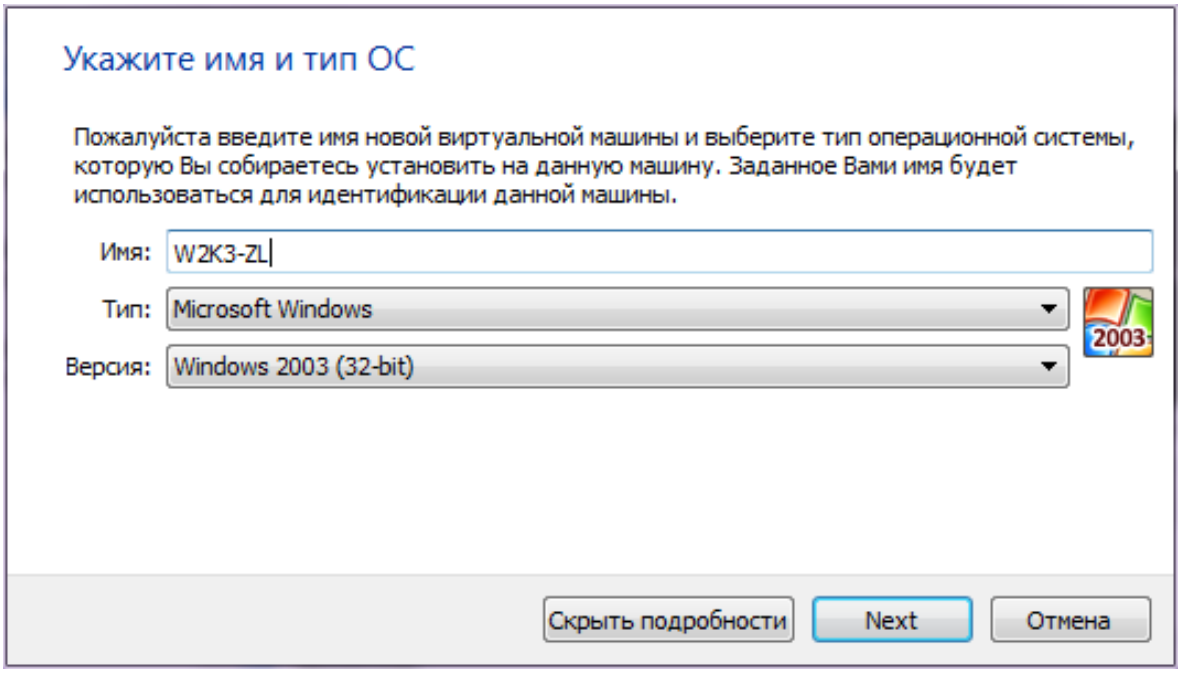

Рисунок 6 – Создание виртуальной машины

Имя ВМ задано с учетом гостевой операционной системы (Microsoft Windows), которая будет установлена на данную машину, версии (Windows Server 2003), а также установленной системы контроля и предотвращения утечек информации Zecurion Zlock.

В следующем диалоговом окне следует указать объем оперативной памяти, выделяемой создаваемой виртуальной машине и нажата кнопка «Next» (см. рисунок 7). В диалоговом окне по умолчанию указывается минимальный объем памяти необходимый для старта ВМ. При необходимости объем можно увеличивать или уменьшать после создания ВМ.

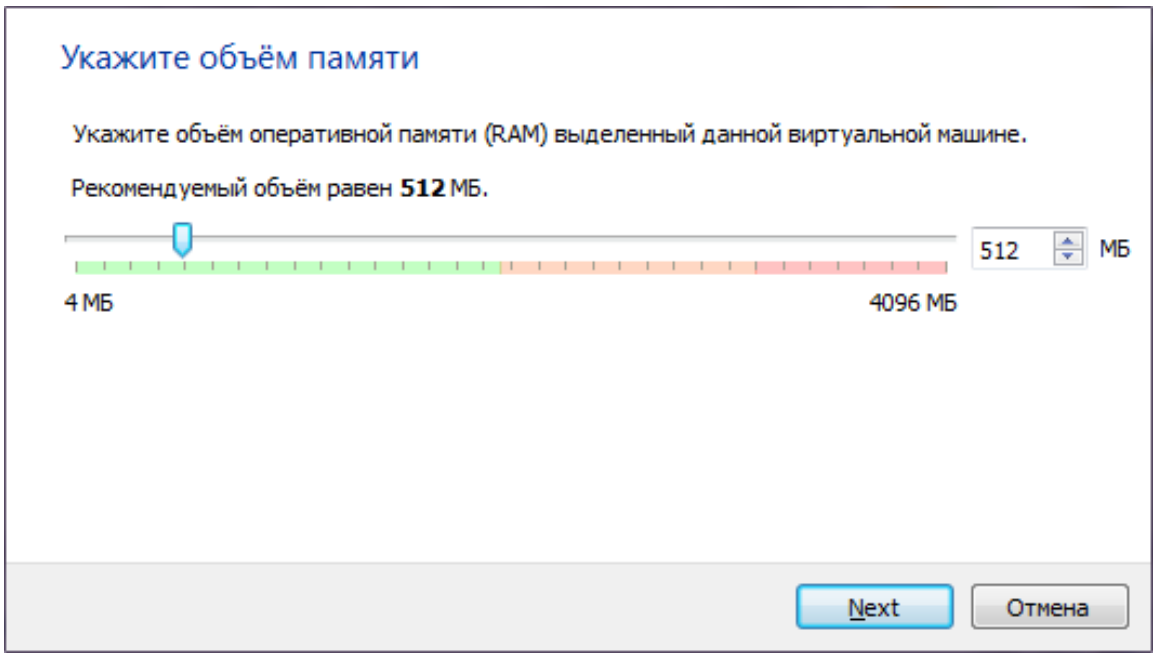

Рисунок 7 – Объем оперативной памяти виртуальной машины

Значение объема оперативной памяти, установленное по умолчанию было оставлено без изменений, т.к. оно является достаточным для функционирования ВМ с установленной гостевой ОС Windows Server 2003.

На следующем шаге требуется подключить новый или уже имеющийся виртуальный жесткий диск к новой виртуальной машине. Был выбран пункт «Создать новый виртуальный диск» - «Создать», как показано на рисунке 8.

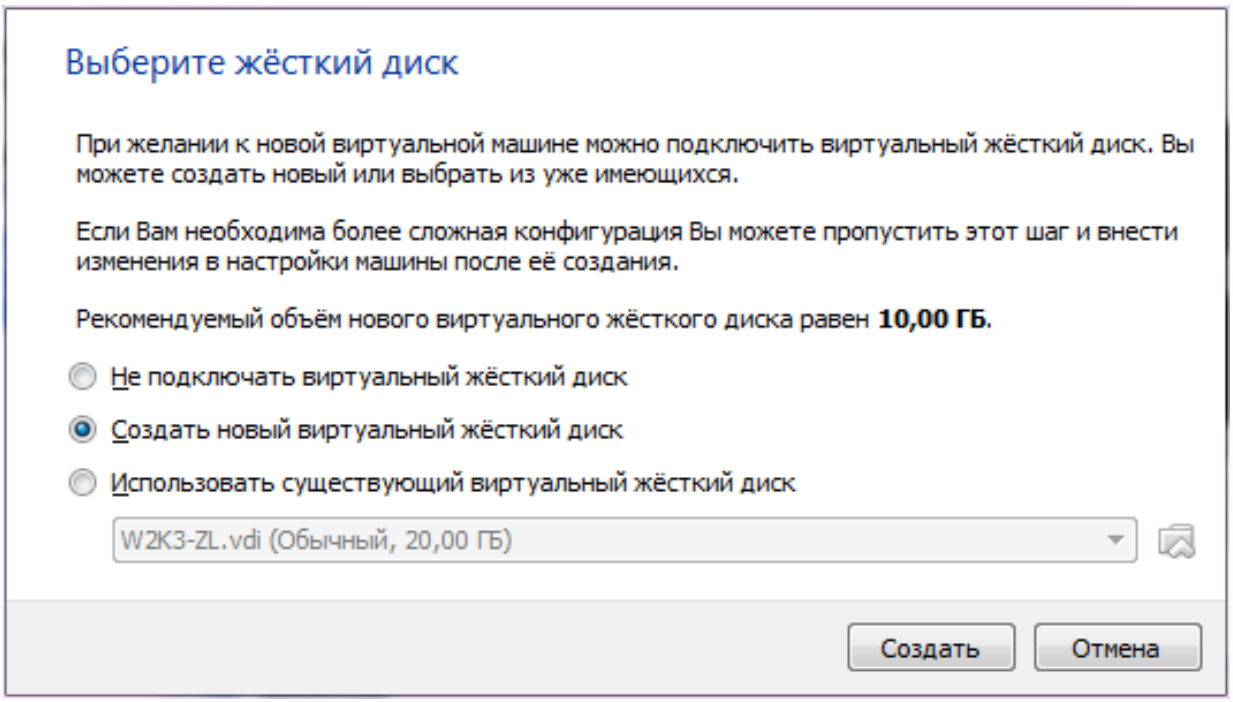

Рисунок 8 – Выбор жесткого диска

VirtualBox использует собственный формат виртуальных дисков — файлы Virtual Disk Image (VDI), данный формат обеспечивает переносимость ВМ с одного компьютера на другой (см. рисунок 9).

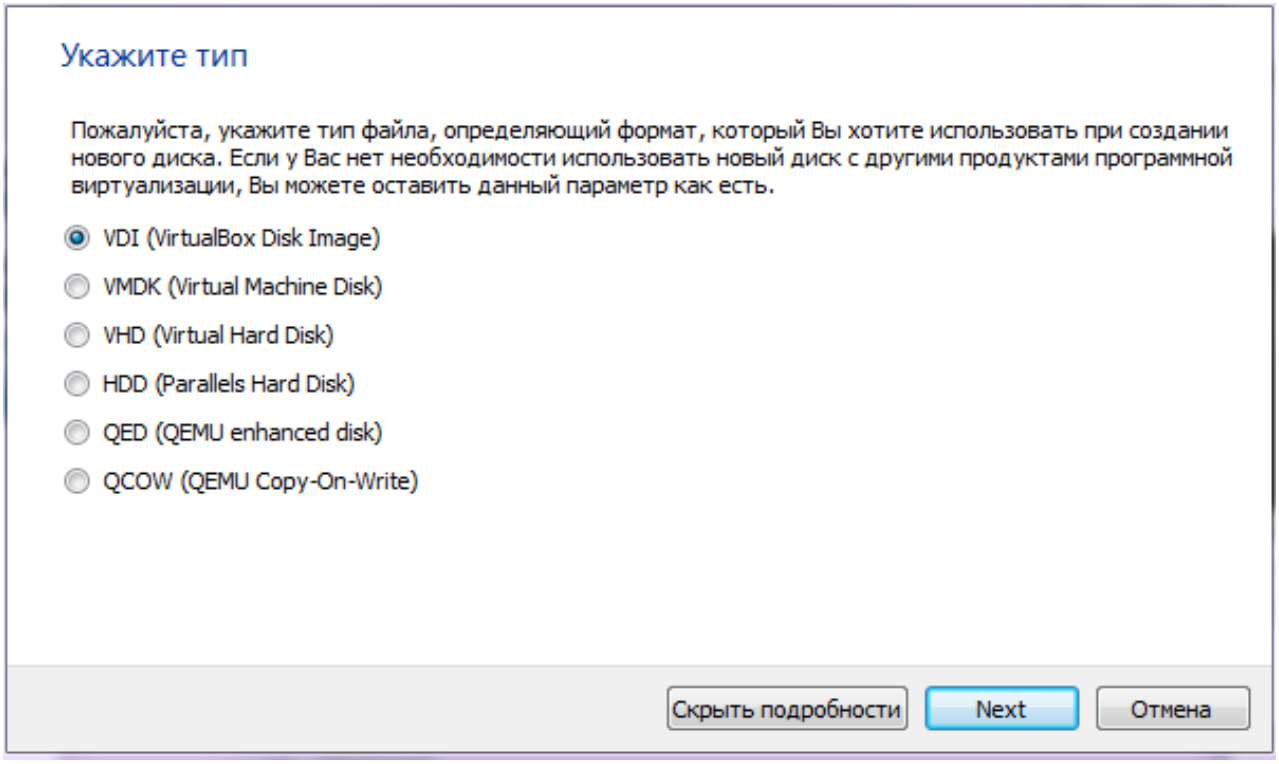

Рисунок 9 – Тип файла

Далее следует выбрать тип виртуального жесткого диска:

– динамический виртуальный жесткий диск – использует место реального носителя по мере заполнения виртуального;

– фиксированный виртуальный жесткий диск – использует фиксированное количество места на реальном жестком диске, однако у такого диска повышено быстродействие.

Был выбран тип «Динамически виртуальный жёсткий диск» (см. рисунок 10), т.к. это позволяет экономить место на жестком диске ПК. Экономия осуществляется за счет того, что при создании ВМ файл с жестким диском ВМ имеет минимальный размер. Размер файла увеличивается по мере заполнения жесткого диска на виртуальной машине.

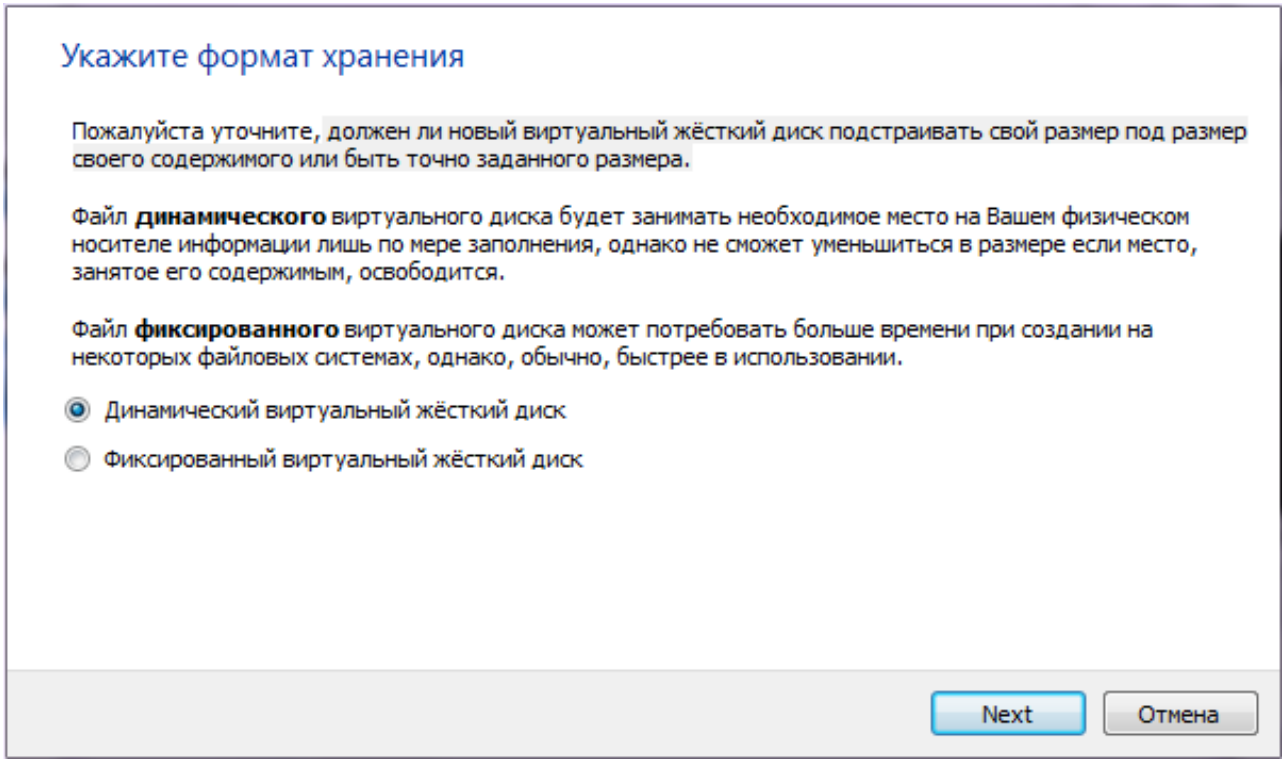

Рисунок 10 – Выбор формата хранения

На следующем шаге требуется указать имя файла виртуального жёсткого диска и его размер. По умолчанию он минимален и равен 20 Гб, именно столько необходимо для нормального функционирования создаваемой ВМ. Также объем был выбран с целью оптимального расходования объема жесткого диска ПЭВМ, которая будет использоваться для развертывания создаваемого стенда. Для завершения была нажата кнопка «Создать».

Таким образом, была создана ВМ со следующими параметрами:

– имя ВМ – W2K3-ZL;

– тип ОС – Windows Server 2003 (32-bit);

– объем ОЗУ – 512 Мб;

– вариант настройки виртуального жесткого диска – «Создать новый виртуальный диск»;

– тип жесткого диска – Динамический виртуальный жесткий диск;

– объем жесткого диска ВМ – 20 Гб.

Аналогичные действия были применены для создания двух других виртуальных машин за исключение некоторых параметров:

– имя ВМ – WinXP01-ZL (WinXP02-ZL);
– тип ОС – Microsoft Windows XP (32-bit);
– объем ОЗУ – 192 Мб;
– тип жесткого диска – динамический виртуальный жесткий диск;
– объем жесткого диска ВМ – 10 Гб.

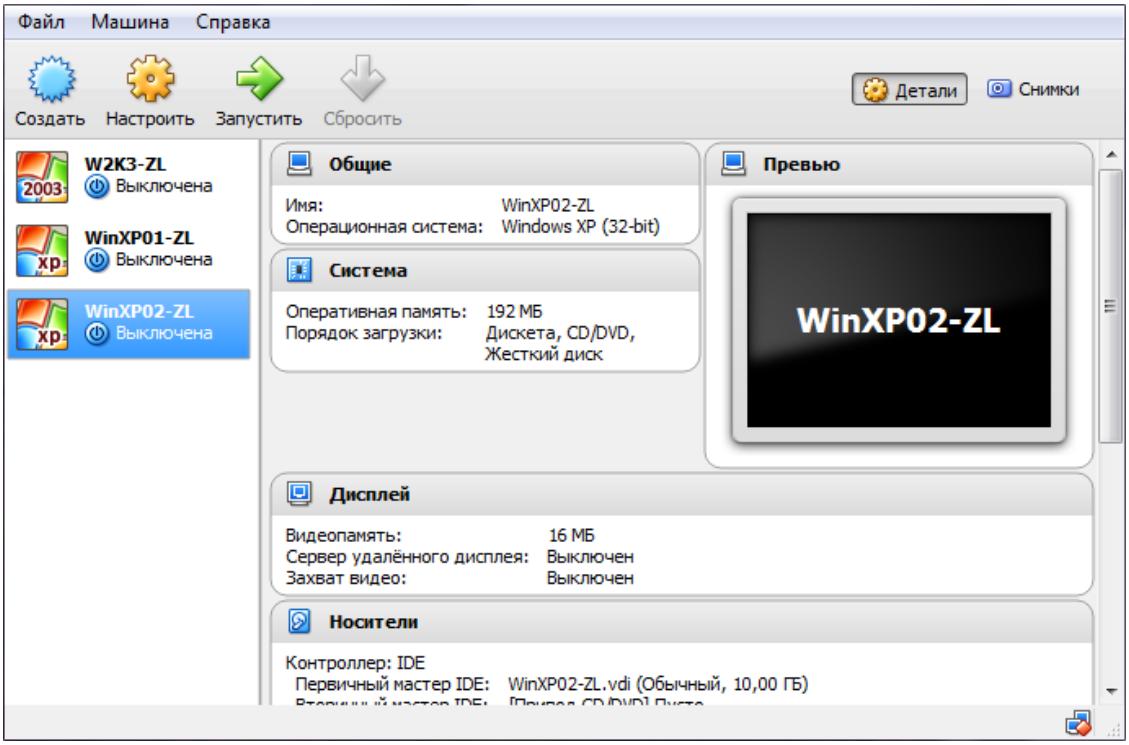

Рисунок 11 – Созданные виртуальные машины

3.3 Установка гостевых ОС

После создания ВМ необходимо установить ОС. При создании лабораторного стенда для одной ВМ в качестве гостевой ОС установлена Windows Server 2003, для двух ВМ установлена Windows XP. Процедура установки производилась в соответствии с документацией разработчиков компании Microsoft. Описанная последовательность действий использовалась при создании каждой ВМ, входящей в состав лабораторного стенда. При завершении установки был определен пароль учетной записи администратора.[5]

3.4 Настройка виртуальной локальной сети

После создания ВМ и установки на них ОС необходимо настроить сетевое взаимодействие для всех созданных ВМ.

Для каждой ВМ следует настроить сеть и общую папку. Выбрав нужную виртуальную машину, нажав правой кнопкой мыши, пункт «Настроить…».

В категории «Общие» на вкладке «Дополнительно» необходимо настроить параметры буфера обмена:

– параметр «Общий буфер обмена» - Двунаправленный;

– параметр «Drag’n’Drop» - Двунаправленный.

Это позволит более удобно пользоваться буфером обмена между ВМ.

В категории «Сеть», на вкладке «Адаптер 1» включен сетевой адаптер и установлен тип подключения «Внутренняя сеть» (имя: intnet). После этого стрелкой вниз было открыто меню «Дополнительно». В нем требуется выбирать тип адаптера «PCnet-FAST III (Am79C973)», для параметра «Неразборчивый режим» выбрано «Разрешить все» (см. рисунок 12).

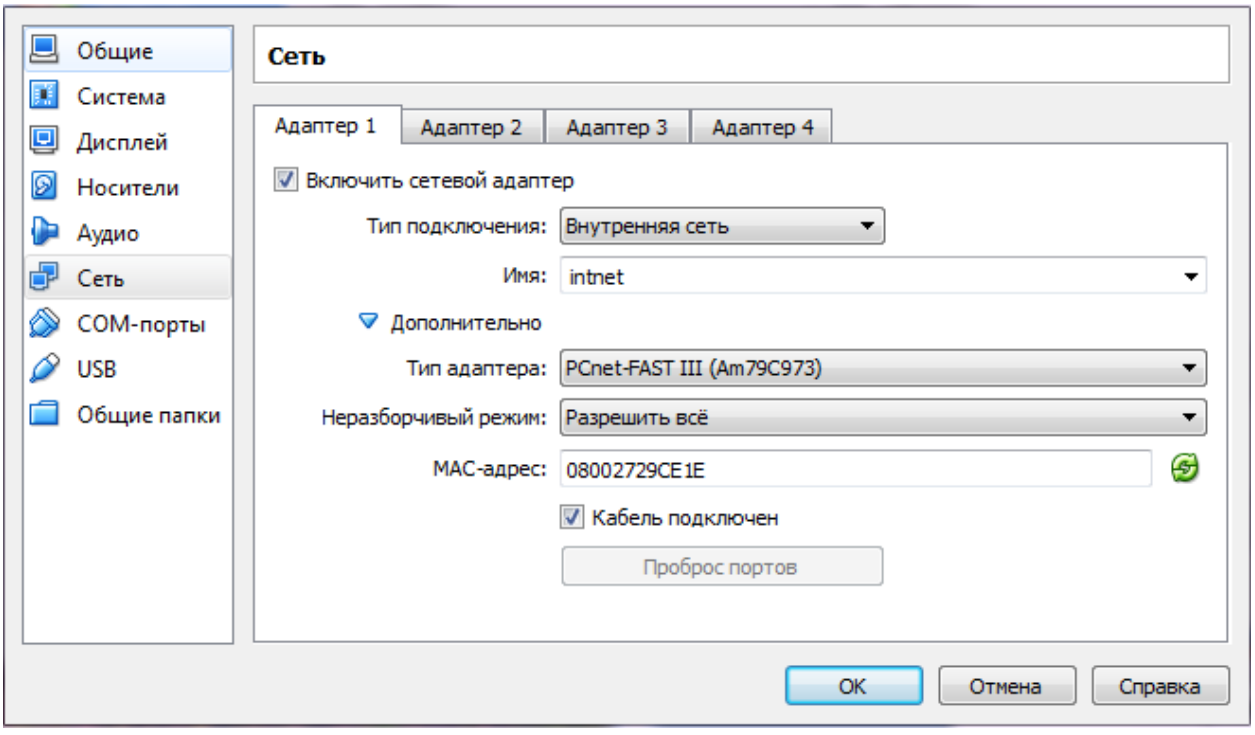

Рисунок 12 – Настройка сети

Далее во вкладке «Общие папки» справа от списка был выбран пункт «Добавить новую общую папку» и указана папка, через которую будет происходить обмен между системой и виртуальной машиной (см. рисунок 13).

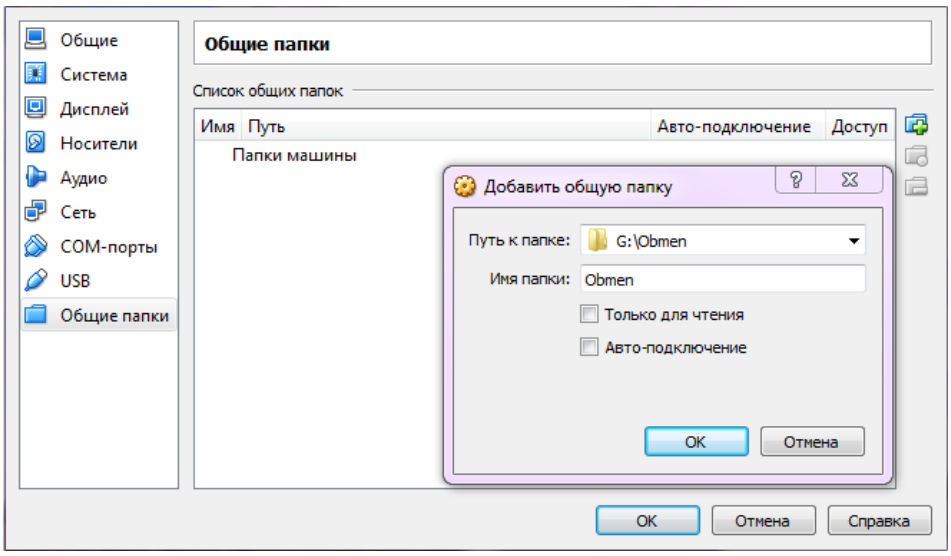

Рисунок 13 – Настройка общей папки

Все вышеперечисленные настройки проводятся с каждой созданной виртуальной машиной.

3.5 Настройка гостевых ОС

Для настройки сетевых подключений необходимо было запустить все ВМ. После этого был осуществлен вход под учетной записью администратора на каждой ВМ.

Далее необходимо узнать IP-адрес, для этого был выполнен ряд действий по следующему пути «Пуск – Панель управления – Сетевые подключения – Подключение по локальной сети». В окне «Состояние Подключение по локальной сети» была выбрана вкладка «Поддержка», где в «Состояние подключения» был найден IP-адрес.

Далее был установлен компонент ОС Windows, реализующий сервис DNS, поскольку в создающемся виртуальном стенде статическая адресация в виду небольшого количества машин.

Для настройки DNS на сервер в главном меню следует выбрать пункт «Панель управления» — «Сетевые подключения», а затем правой кнопкой мыши щелкнув по пункту «Подключение по локальной сети». Из контекстного меню выбрав «Свойства» и в окне свойств подключения к локальной сети выбрав пункт «Протокол сети Интернет TCP/IP», выбрав «Свойства». Откроется окно свойств протокола TCP/IP, в поле «Предпочитаемый сервер

DNS» введен IP-адрес сервера, после чего последовательным нажатием на кнопку «ОК» закрыты все окна.

Для настройки DNS на рабочей станции необходимо зарегистрироваться как «Администратор». В меню, открываемом кнопкой «Пуск», выбрать пункт «Панель управления» — «Сетевые подключения», а затем правой кнопкой мыши щелкнув по пункту «Подключение по локальной сети». Из контекстного меню был выбран пункт «Свойства», в окне «Подключение по локальной сети — свойства» выбран «Протокол сети Интернет», далее «Свойства», в поле «Предпочитаемый DNS-сервер» введен адрес. Затем нажать кнопку «ОК». Диалоговое окно свойств подключения закрыть нажатием кнопки «Закрыть».[6]

Для того чтобы изменения вступили в силу, надо будет перезагрузить компьютер.

Для того, чтобы уточнить сетевой адрес, необходимо открыть диалоговое окно сетевого адаптера.

Далее необходимо узнать имя компьютера, сформированное при установке гостевой ОС. После этого имя по умолчанию необходимо сменить для того чтобы оно соответствовало названию ВМ и указывало на роль ВМ в разрабатываемом стенде. Были установлены следующие имена ВМ:

- для ВМ с ОС Windows Server 2003 R2 на W2K3-ZL;
- для ВМ с ОС Windows XP Professional 2002 на WinXP01-ZL;
- для ВМ с ОС Windows XP Professional 2002 на WinXP02-ZL.

После установки DNS была создана зона прямого просмотра, в которой были включены все ВМ. Имя зоны – study.local.

Для проверки правильности установки DNS была выполнена проверка наличия консоли DNS и наличие следующих локальных служб:

- DNS-сервер(только для серверов);
- DNS-клиент.

После проверки в окне свойств сетевого адаптера было отключено динамическое распределение адресов (DHCP) и указаны параметры для работы для работы служб DNS.

Далее к имени компьютера были дописаны DNS-суффикс study.local. Это делается для добавления компьютера в зону прямого просмотра.

Для того, чтобы все вышеописанные изменения вступили в силу, необходимо перезагрузить ВМ.

Далее необходимо проверить доступность ВМ в локальной сети intnet. Для этого были запущены все клиентские виртуальные машины и виртуальная машина с гостевой ОС Windows Server 2003. На виртуальной машине сервера W2K3-ZL была запущена командная строка и с помощью утилиты командной строки «ping» была проверена сетевая доступность всех ВМ, включенных в локальную сеть (проверка самой машины, а затем каждой клиентской машины) (см. рисунок 14). Аналогичные действия были выполнены на ВМ с гостевой ОС Windows XP. Результат показан на рисунке 14.

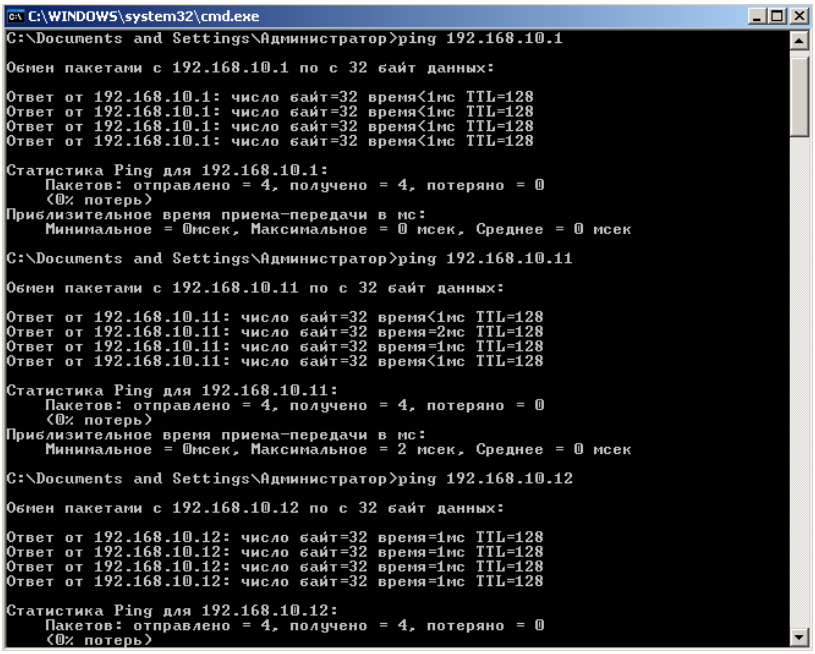

Рисунок 14 – Проверка сетевой доступности

Все выше изложенные настройки позволяют с полной уверенностью говорить, что сеть была полностью настроена для работы виртуальных машин.

Далее было выполнено создание домена и установка служб Active Directory, необходимых для работы домена, веб-сервера IIS, сервера сертификатов Active Directory, а также сервер приложений, сетевые службы, стандартные и служебные программы.

В роли первичного контроллера домена выступает ВМ W2K3-ZL. Именем созданного домена является имя зоны прямого просмотра.

Далее в домен study.local были добавлены ВМ WinZP01-ZL и WinXP02-ZL.

Для проверки работы домена был выполнен вход под учетной записью доменного администратора.

Далее проверяется синхронизация времени между ВМ домена. Это необходимо для обеспечения корректного управления компьютерами домена с сервера.

Результат проверки позволяет сделать вывод, что настройка гостевых ОС завершена.

Далее была произведена настройка сервера W2K3-ZL. Для запуска брандмауэра, перейти по следующему пути «Пуск – Панель управления – Брандмауэр Windows». Во вкладке «Общие» был выбран «Откл». Отключение брандмауэра позволяет настроить сеть для бесперебойной работы.[7]

Далее на следующей вкладке «Исключения», в окне «Программы и службы» были отмечены все программы и службы (см. рисунок 15).

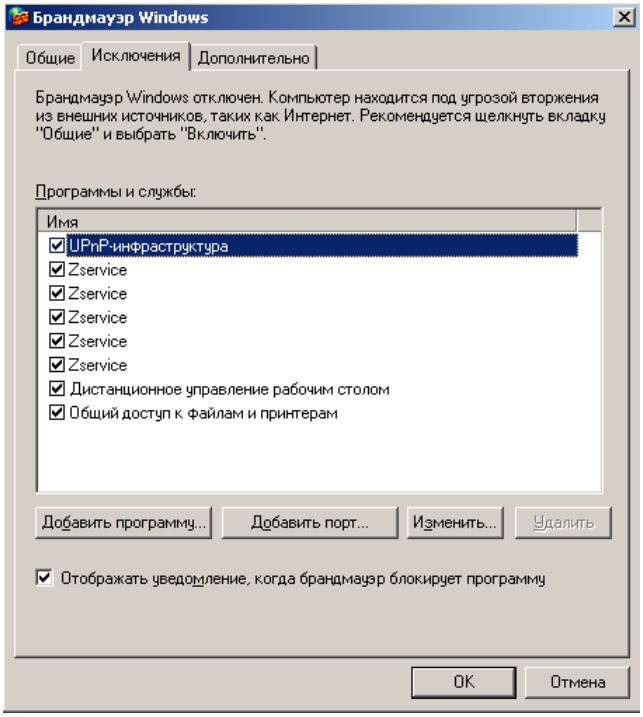

Рисунок 15 – Исключения брандмауэра

Затем на следующей вкладке «Дополнительно – Параметры сетевого подключения – Параметры» и в открывшейся вкладке «Дополнительные параметры» «Службы» были отмечены все службы из списка, далее на вкладке «ICMP» отмечены все разрешения, в завершение нажата кнопка «ОК».

3.6 Установка системы контроля и предотвращения утечек информации Zecurion Zlock

Установка в соответствии с руководством администратора, входящим в установочный компонент.

При установке Zecurion Zlock на ВМ W2K3-ZL была установлена БД Microsoft SQL Express в соответствии с руководством администратора. Эта БД необходима для установки консоли управления Zecurion Zlock, которая нужна для реализации задач мониторинга. Далее на ВМ W2K3-ZL была установлена серверная часть Zecurion Zlock, а так же были установлены компоненты управления Zecurion Zlock. На ВМ с гостевой ОС Windows XP был установлен клиентский модуль Zecurion Zlock, а так же консоль управления.

После установки была проверена работоспособность посредством подключения сервера Zecurion Zlock к сервису. Так же было проверено подключение к СУБД MS SQL. Подключение выполнялось с ОС Windows 2003 Server. Все компоненты установленного программного комплекса работают корректно, сбоев не происходит.

3.7 Результат создания виртуального стенда

В результате описанных в подразделах 3.1-3.6 действий, был разработан виртуальный стенд, включающий следующие ВМ:

– одна ВМ с ОС Windows Server 2003 с именем W2K3-ZL;
– одна ВМ с ОС Windows XP Professional 2002 с именем WinXP01-ZL;
– одна ВМ с ОС Windows XP Professional 2002 с именемWinXP02-ZL.

Каждая ВМ выполняет определенную роль:

– W2K3-ZL – первичный контроллер домена, сервер приложений, веб-сервер, SMTP-сервер, DNS-сервер, рабочее место администратора Zlock;

– WinXP01-ZL – компьютер домена, автоматизированное рабочее место пользователя;

– WinXP02-ZL – компьютер домена, автоматизированное рабочее место пользователя.

Состав виртуального стенда показан в приложении А.

4 Порядок выполнения задания по применению программного комплекса Zecurion Zlock, для выявления и предотвращения утечек информации

4.1 Создание учетных записей пользователей

Создать учетную запись локального пользователя на компьютере WinXP01-ZL (User1). Для этого осуществить вход на компьютер WinXP01-ZL с использованием учетной записи либо локального, либо доменного администратора. Запустить программу «Управление компьютером» создать учетную запись пользователя, нажав правой кнопкой мыши «Новый пользователь».

При создании учетной записи установить следующие параметры учетных записей (см. рисунок 16):

– «Запретить смену пароля пользователем»;

– «Срок действия пароля не ограничен».

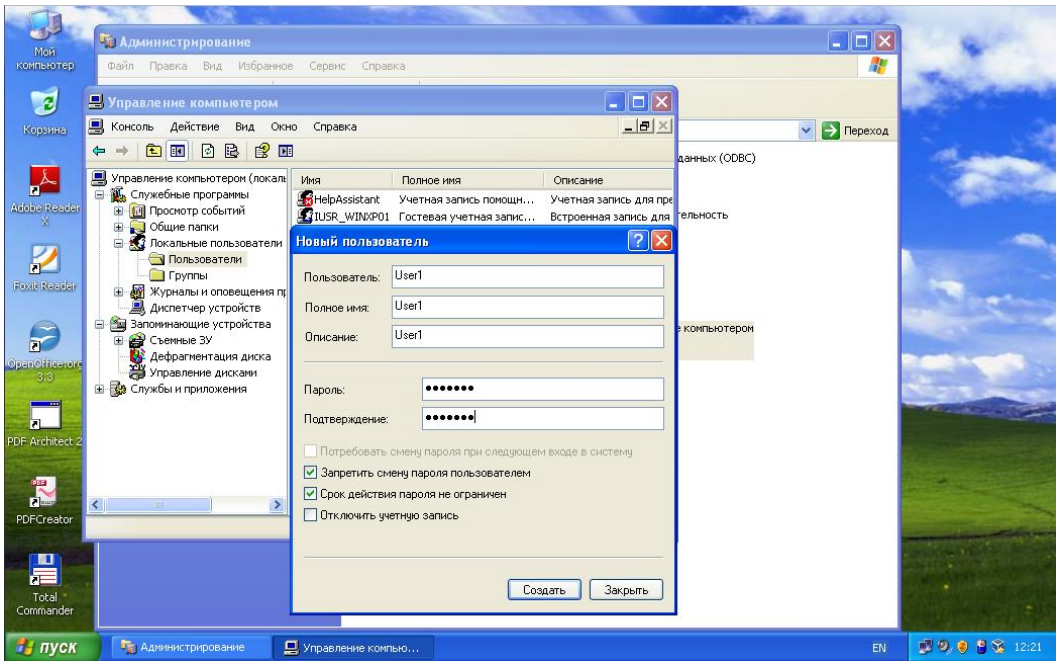

Рисунок 16 – Создание учетной записи пользователя

При установлении пароля необходимо, чтобы он соответствовал доменной политике паролей, определяющей требования сложности пароля. Минимальная длина пароля должна быть 7 символов. Должны использоваться символы как минимум из трех групп символов.

Таким образом, были созданы три учетные записи User1, User2, User3.

4.2 Включение и настройка аудита

На контроллере домена W2K3-ZL осуществить вход, используя учетную запись доменного администратора. Запустить консоль управления Zecurion Zlock. После выполнения запуска консоли управления на экране появится окно, отображающее список загружаемых компонентов (см. рисунок 17).

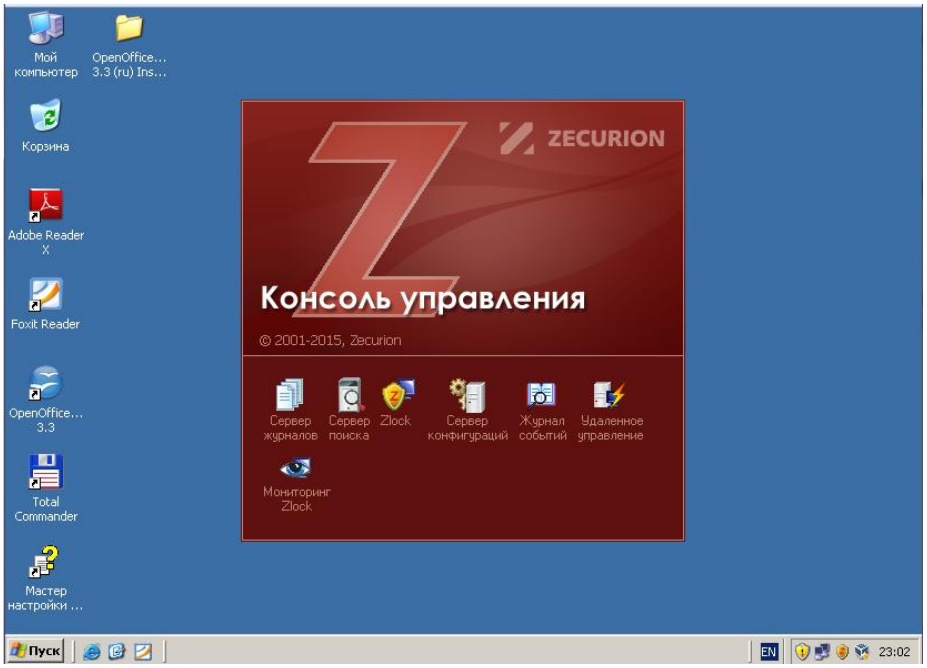

Рисунок 17 – Компоненты управления ZLock

После завершения загрузки компонентов на экране появится консоль управления, основное окно которой отображает в левой и правой частях, список загруженных компонентов (см. рисунок 18).

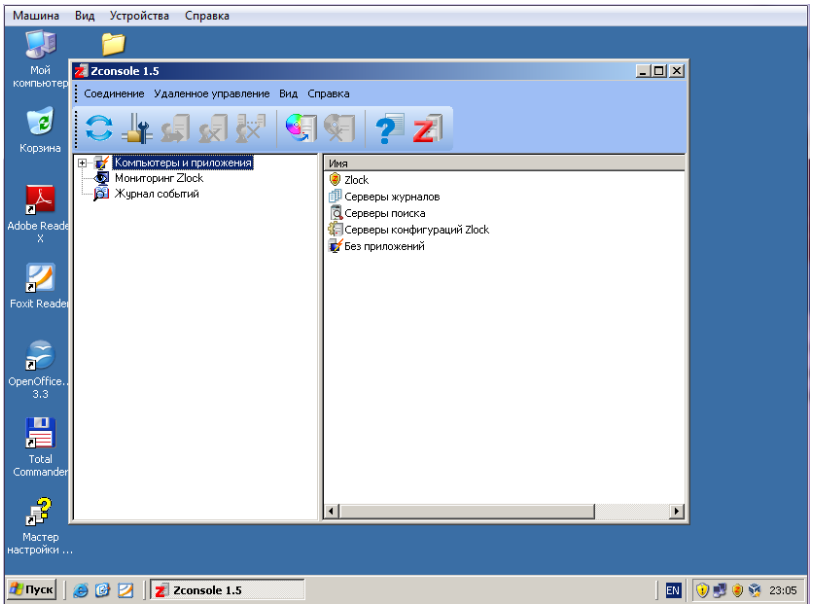

Рисунок 18 – Консоль управления ZLock

Для просмотра списка компьютеров сети, на которых установлен клиентский модуль ZLock, необходимо в левой части окна консоли управления отобразить содержимое раздела «Компьютеры и приложения», щелкнув левой клавишей мыши по знаку «+» слева от названия раздела. Затем отобразить содержимое подраздела ZLock (см. рисунок 19).

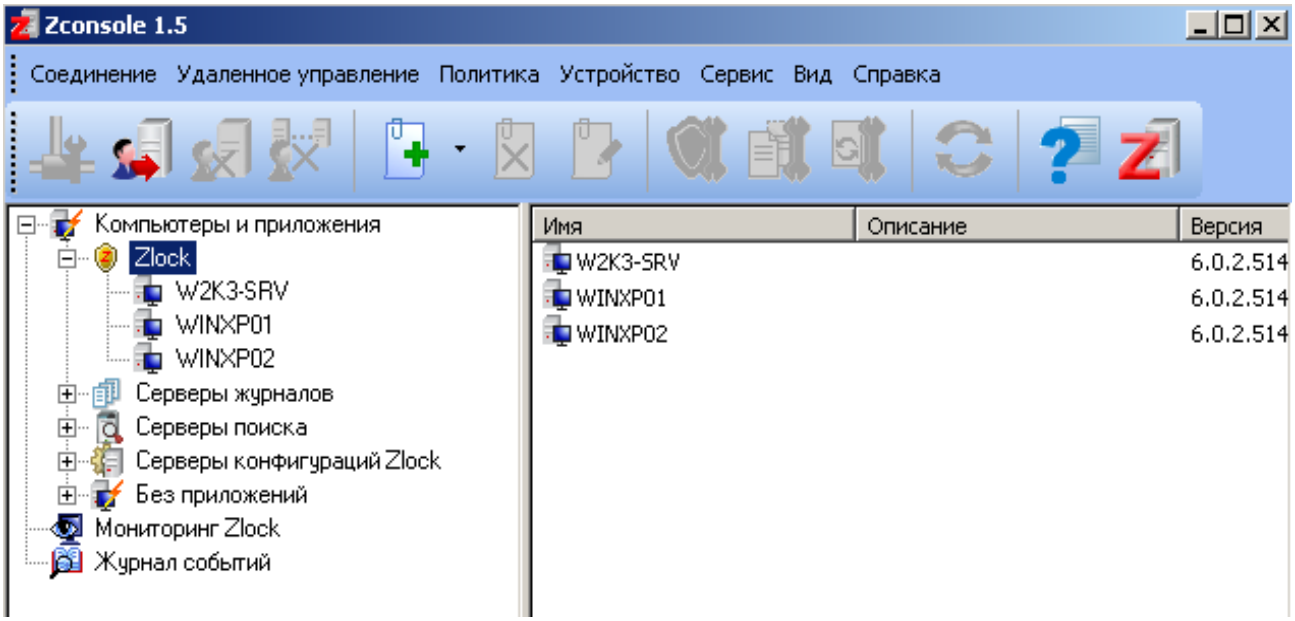

Рисунок 19 – Список компьютеров с установленным ZLock

По умолчанию права доступа клиентского модуля Zlock настроены таким образом, что пользователи, входящие в группу локальных администраторов, имеют полный доступ ко всем функциям системы. В дальнейшем права пользователей можно изменять.

Для соединения с отдельными компьютерами необходимо:

– открыть элемент «Компьютеры и приложения» в древовидном списке консоли Zlock и выбрать компьютер;

– выбрать пункт «Установить соединение» в меню «Соединение».

В консоли управления, так же как и в клиентском модуле, доступен список подключенных устройств к удаленному компьютеру. Для его просмотра необходимо выполнить соединение с удаленным компьютером и в дереве Zlock выбрать «Подключенные устройства». В нижней части экрана отобразится информация о свойствах выбранного устройства (см. рисунок 20).

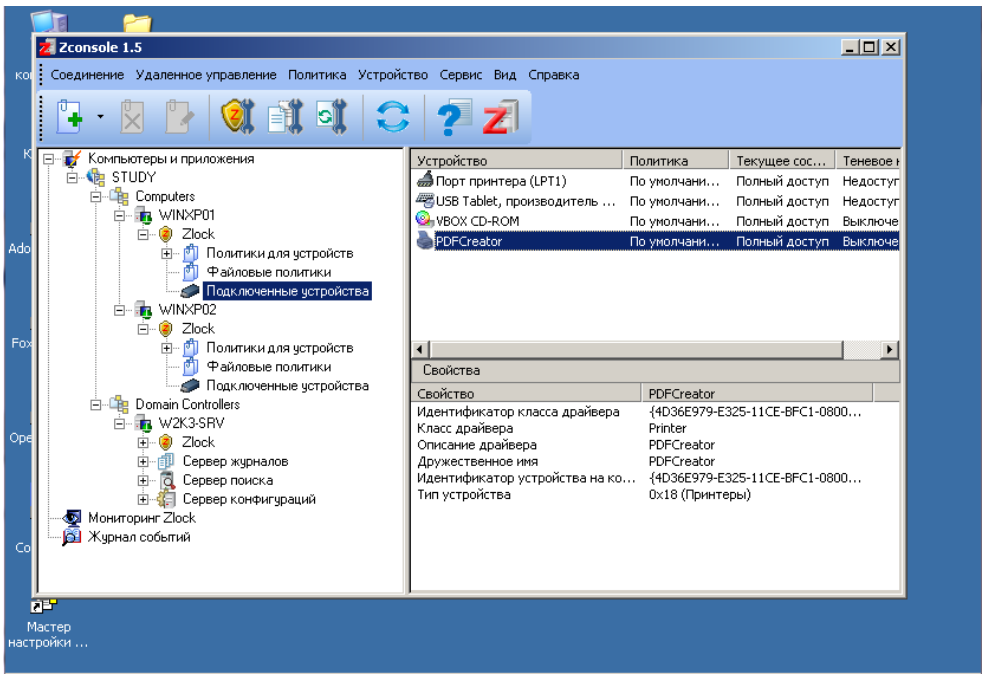

Рисунок 20 – Подключенные устройства

4.3 Создание политики доступа к устройству

Для создания новой политики доступа необходимо выбрать пункт «Политика для устройств» и нажав правой кнопкой мыши выбрать «Политика доступа к устройству» (см. рисунок 21).

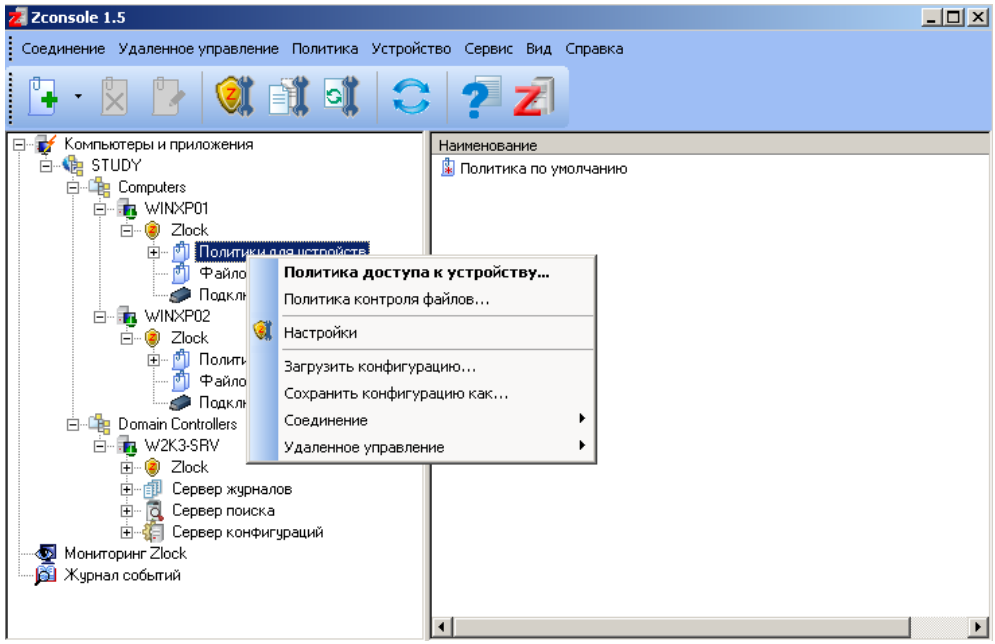

Рисунок 21 – Политика доступа к устройству

В закладке «Доступ» задается имя политики, приоритет политики и права доступа к устройству. Отметить все данные как показано на рисунке 22. При

необходимости можно включить опцию «Постоянная политика». Включенная опция означает, что эта политика не будет удаляться при загрузке политик.

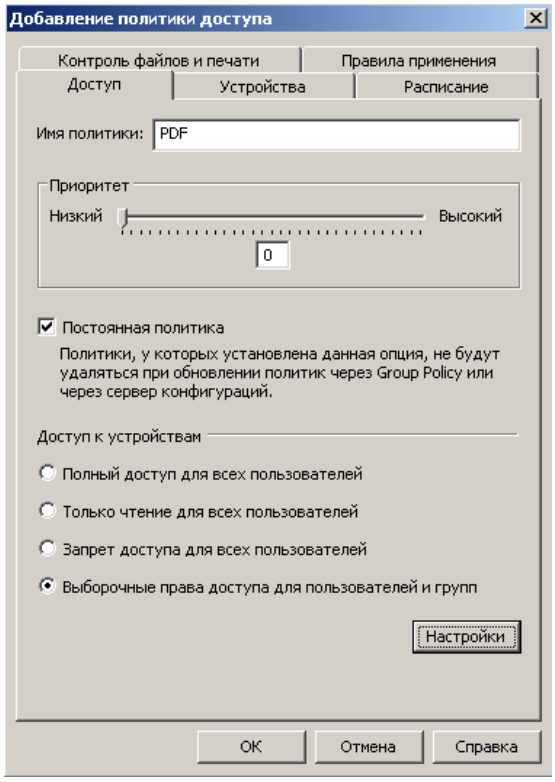

Рисунок 22 – Доступа к устройствам

В нижней части панели нажать кнопку «Настройки». В окне «Доступ» справа выбрать «Добавить» и указать пользователей из данного локального компьютера, как показано на рисунке 23.

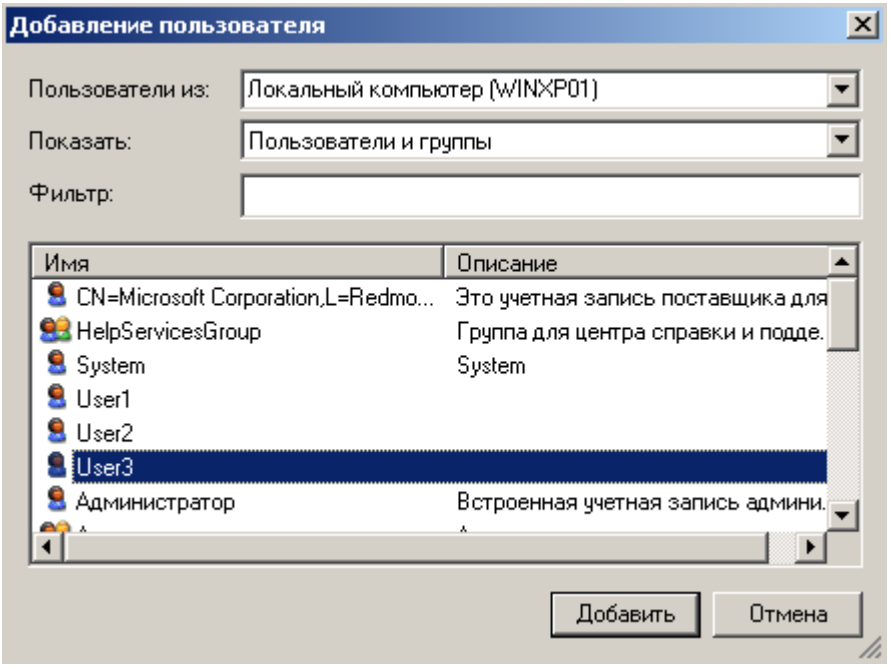

Рисунок 23 – Добавление пользователя

После чего в окне доступа отобразятся добавленные пользователи. Каждому пользователю должны быть присвоены права доступа. Для User1 выбрать полный доступ, для User2 выбрать чтение, а для User3 полный запрет, как показано на рисунке 24.

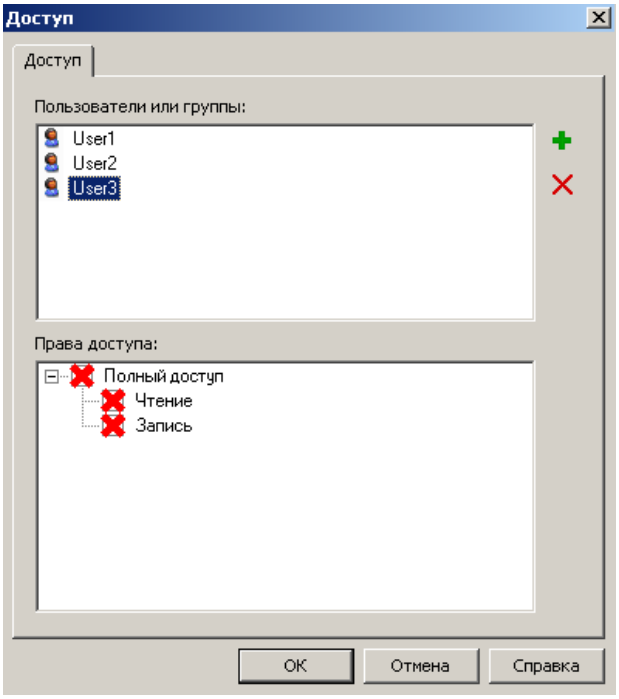

Рисунок 24 – Права доступа пользователей

В закладке «Устройства» нажать справа плюс, после чего необходимо выбрать «Принтер». В окне «Принтеры» указать источник списка устройств и выбрать принтер, как показано на рисунке 25.

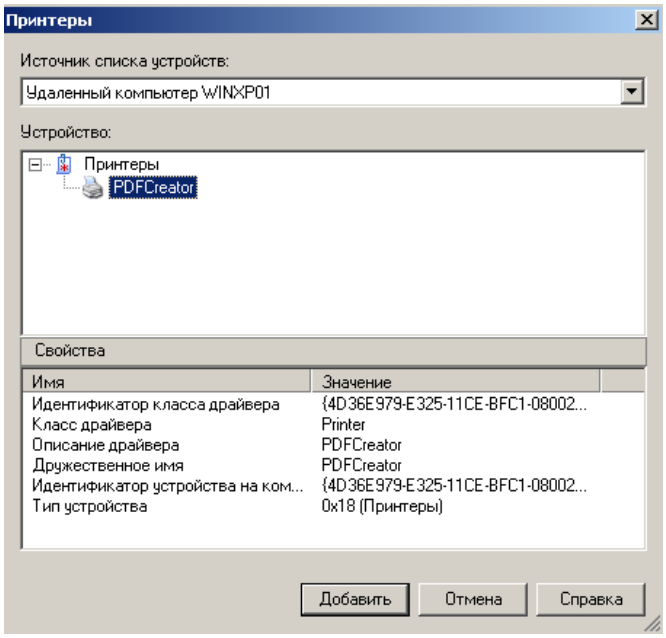

Рисунок 25 – Принтер

После добавления принтера он должен отобразиться в закладке «Устройства», как показано на рисунке 26.

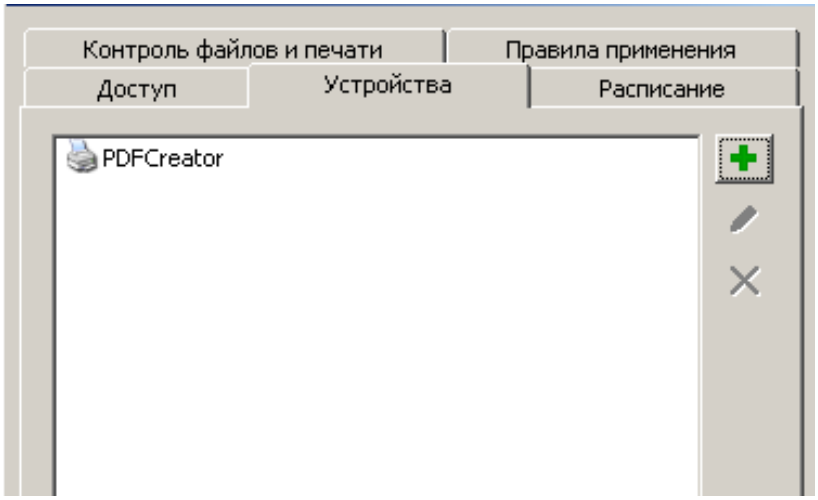

Рисунок 26 – Устройства

Далее выбрать вкладку «Расписание» и выбрать тип расписания политики «Ежедневное». «Срок действия политики» и «Действие политики» оставить без изменения, как показано на рисунке 27.

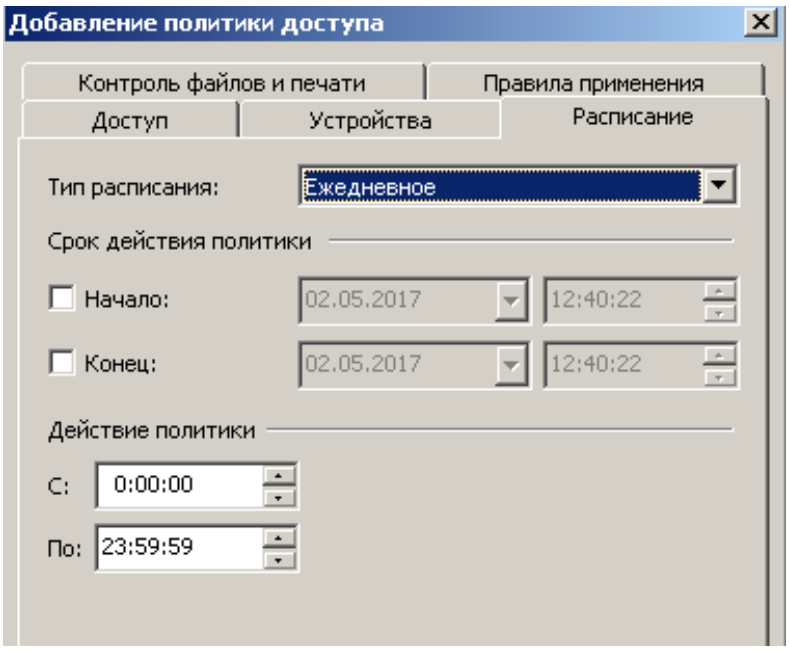

Рисунок 27 – Расписание

Для настройки правил применения политики нужно перейти на вкладку «Правила применения». Политика может применяться в зависимости от доступности домена: домен доступен локально, домен доступен через VPN, домен не доступен. Следует отметить все пункты, как показано на рисунке 28.

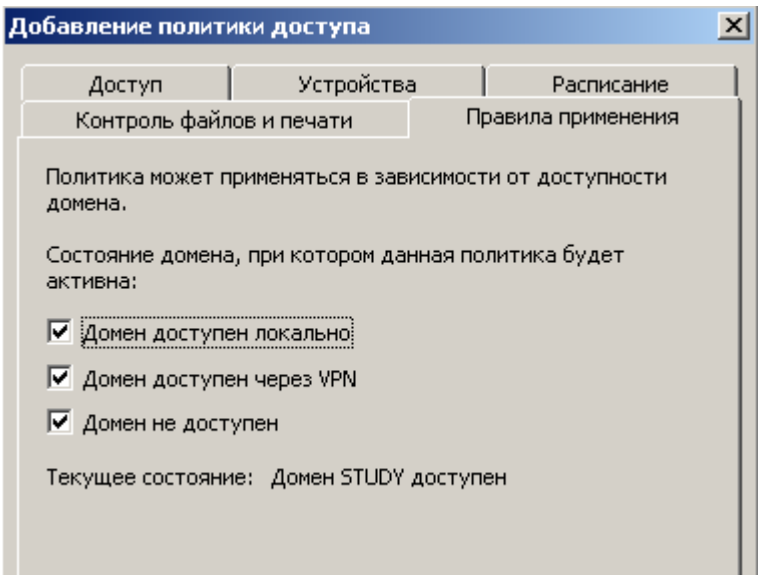

Рисунок 28 – Правила применения политик

Во вкладке «Контроль файлов и печати» выполняются настройки журналирования, обработки файловых операций, шифрования и теневого копирования файлов.

При выборе «Журналирование» перейти к его настройке, используя кнопку «Настройки» соответствующего блока. Нажать кнопку «Добавить действие» для добавления действия при файловых операциях. Выбрать пункт «В файл» и указать папку локального хранилища и формат файла, как показано на рисунке 29. После чего нажать кнопку «Ок».

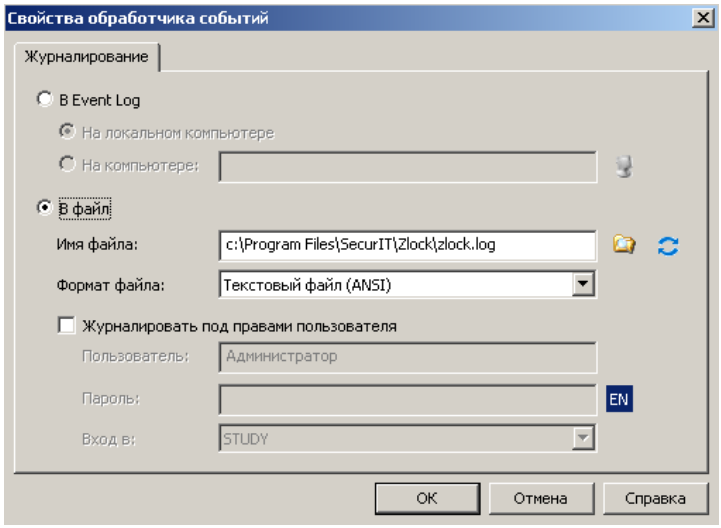

Рисунок 29 – Запись в файл

В окне «Журналирование и обработка файловых операций» оставить все как показано на рисунке 30. Нажать кнопку «Ок».

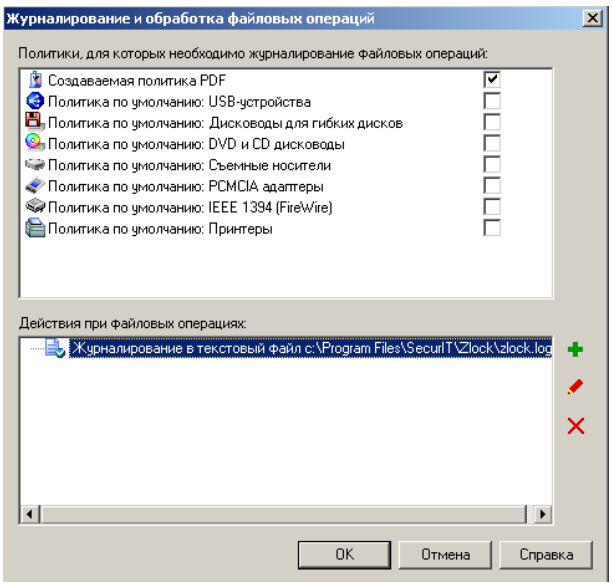

Рисунок 30 – Журналирование

Для настройки теневого копирования необходимо выбрать пункт «Теневое копирование» (см. рисунок 31).

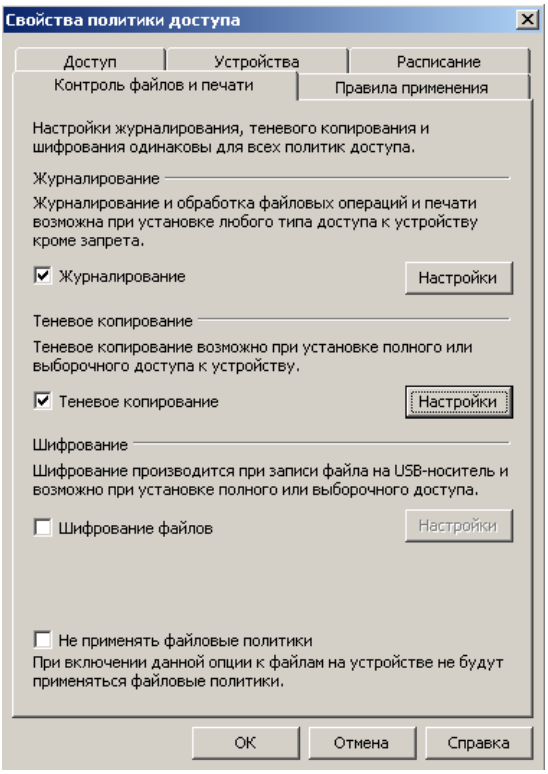

Рисунок 31 – Настройка теневого копирования

На вкладке «Локальное хранилище» окна «Теневое копирование» требуется выполнить настройку параметров хранилища файлов теневых копий и снимков экрана, а также просмотр хранилища на клиентском компьютере до передачи файлов на сервер.

В поле «Каталог» указывается путь к папке локального хранилища, оставить по умолчанию. Максимальный размер каталога локального хранилища задается либо в виде фиксированной величины в мегабайтах, либо в процентах от свободного места на диске. Выбрать фиксированный объем – 3000 МБ.

Если свободного места в каталоге недостаточно для копирования файла или документа, то, в зависимости от настроек, Zlock может:

– перезаписать файлы или документы определенного срока давности (если таких файлов обнаружено не будет, или освободившегося места будет недостаточно для сохранения теневой копии, то запись на носитель или печать будет заблокирована);

– перезаписать самые старые файлы;

– запретить запись до появления свободного места в каталоге;

– запись на носитель или печать без теневого копирования.

Выбрать «Перезапись самых старых файлов», как представлено на рисунке 32.

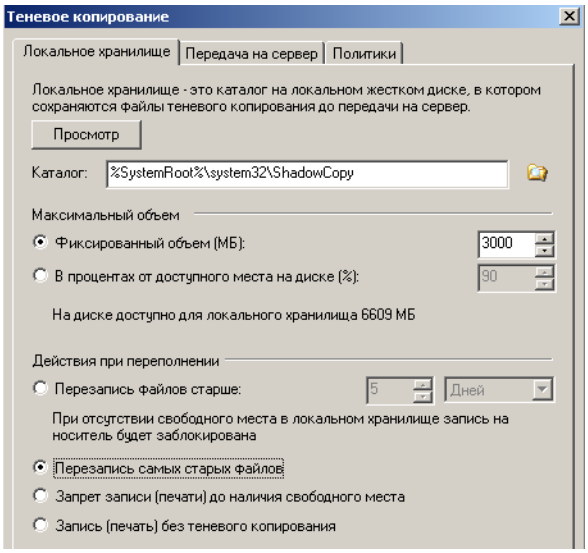

Рисунок 32 – Локальное хранилище

Распечатанные документы сохраняются в формате PDF. Если печать на принтере прошла в нераспознанном формате, то документ сохраняется в бинарном виде с расширением bin. Просмотр документа в этом случае невозможен, но возможно распечатать его на том же принтере. Для этого следует нажать кнопку печати файла, доступную для бинарных файлов.

Для настройки передачи теневых копий на сервер журналов предназначена вкладка «Передача на сервер». Чтобы включить передачу, необходимо отметить опцию «Передавать информацию о теневом копировании и файлы на сервер». Файлы могут передаваться сразу после поступления в локальное хранилище либо с заданной периодичностью. Отметить опцию «Передавать файлы как можно раньше».

При передачи файлов теневых копий на сервер журналов необходимо выбрать соответствующий тип хранилища – Сервер журналов, указать имя сервера журналов выбрав компьютер из списка – W2K3-ZL. Указать сетевую папку для хранения файлов теневого копирования или выбрать ее из списка нажав кнопку справа. Поля «Тип пользователя», «Имя», «Пароль», «Вход в»: предназначены для ввода информации о пользователе, от чьего имени будет происходить передача информации на SQL-сервер или сервер журналов и запись файлов на сетевую папку. При включенной опции «Извлекать текст из изображения» из локального хранилища на указанный сервер будет передаваться как теневая копия графического файла, так и извлеченный из нее текст. Ввести все данные как показано на рисунке 33.

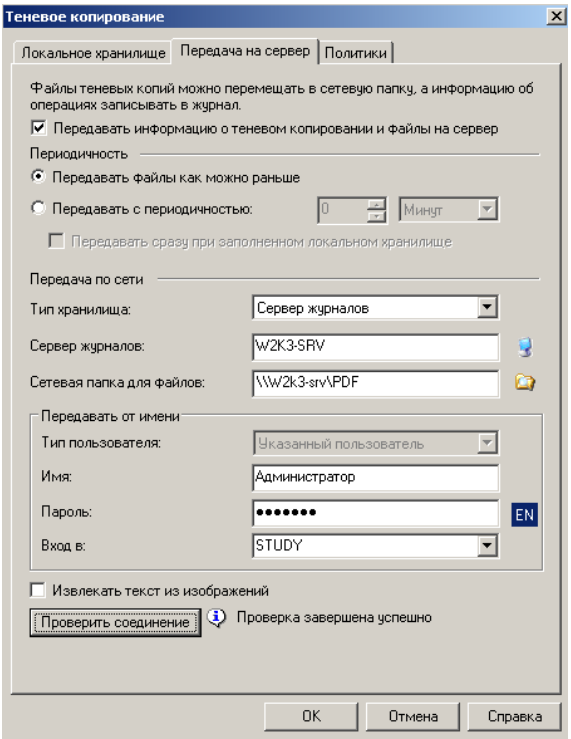

Рисунок 33 – Передача на сервер

На вкладке «Политики» отмечаются политики, для которых производится теневое копирование (см. рисунок 34).

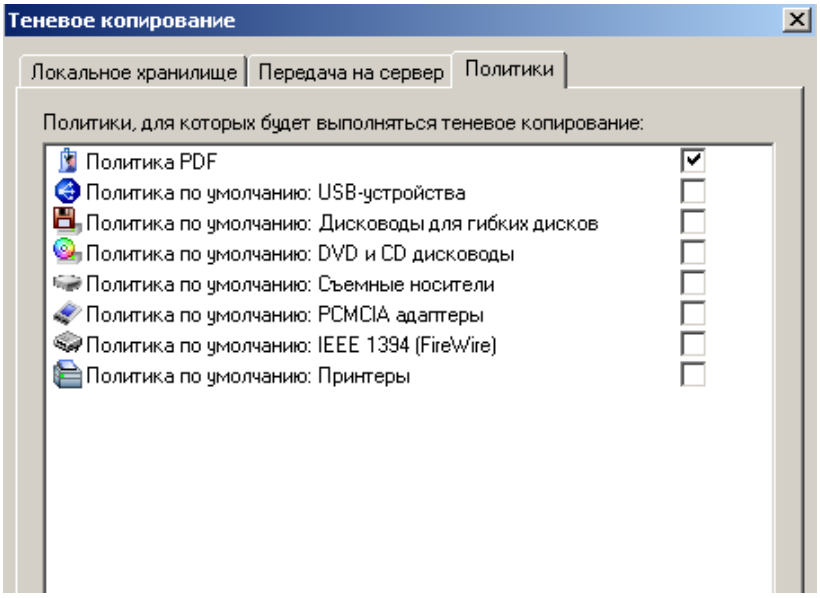

Рисунок 34 – Теневое копирование для политики

После выполнения вышеизложенных действий будет создана политика доступа для принтера «PDF» (см. рисунок 35).

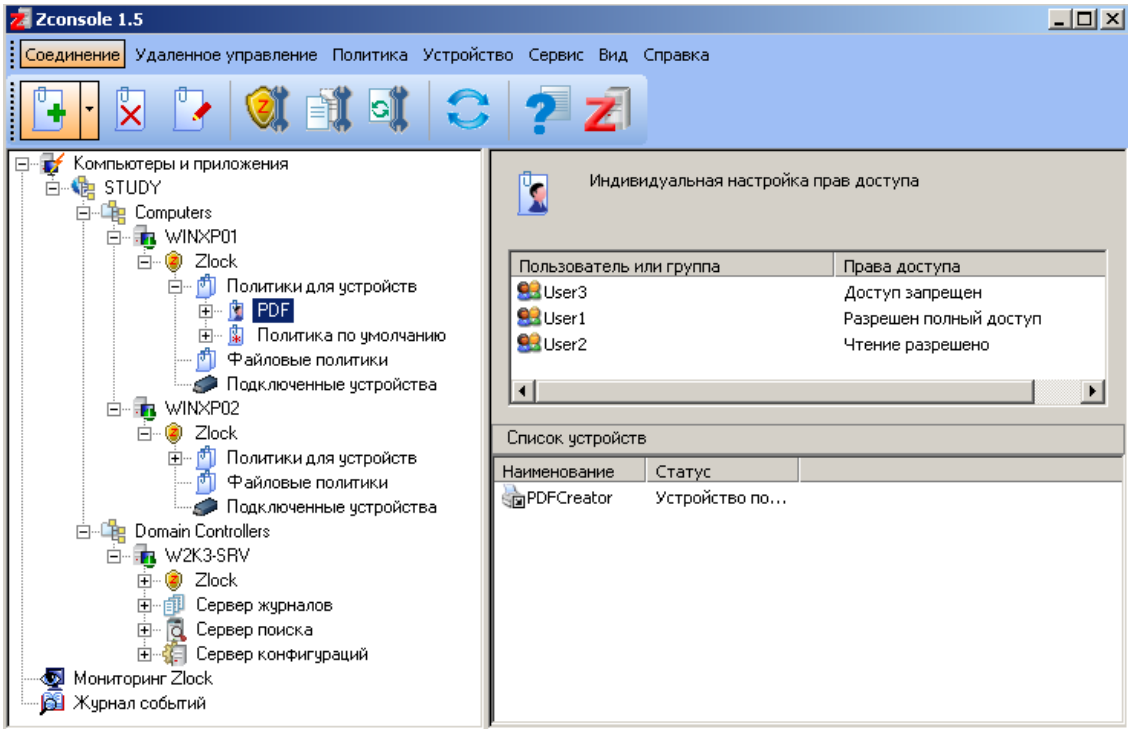

Рисунок 35 – Созданная политика для устройства

Затем на компьютере домена WinXP01-ZL войти под учетной записью каждого пользователя и проверить возможность печати файлов, для этого необходимо открыть любой текстовый файл и попытаться пустить его на

печать. Согласно правам доступа User1 имеет полный доступ к печати файлов, User2 и User3 не имеют доступ печати согласно политики PDF (см.рисунок 36).

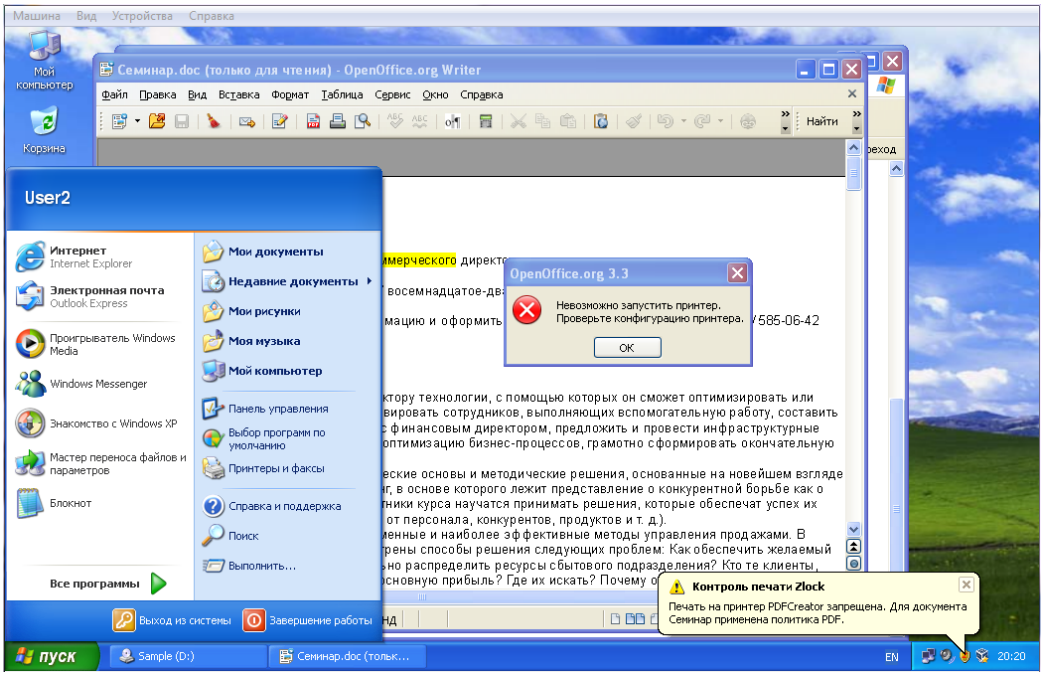

Рисунок 36 – Доступ печати для User2(PDF)

После этого необходимо проверить журналирование событий, открыв файл, который находится по адресу c:\Program Files\SecurIT\Zlock\zlock.log (см. рисунок 37).

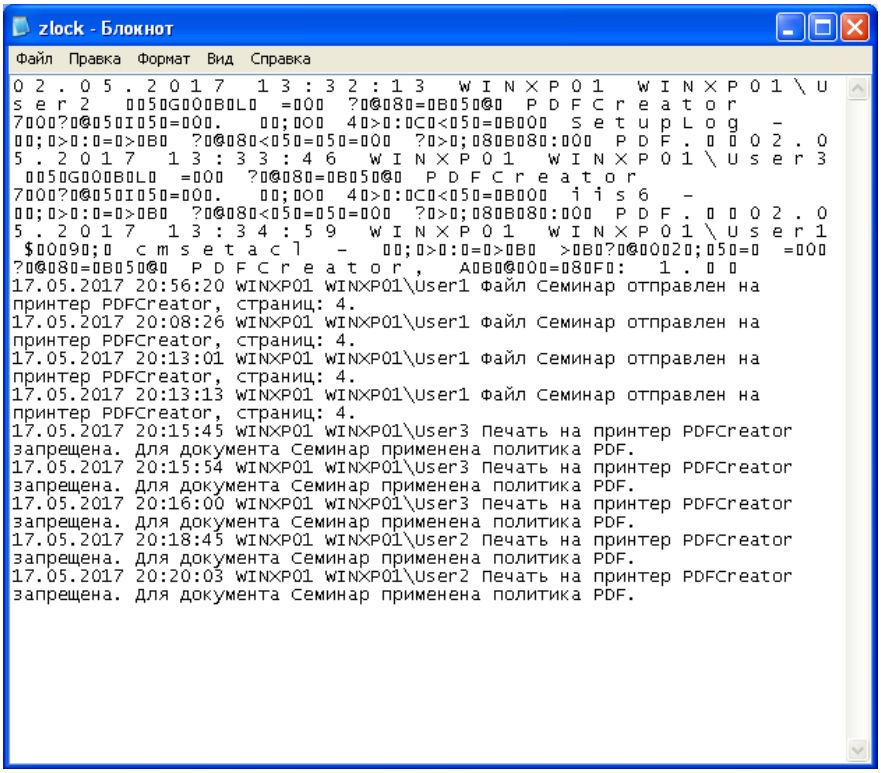

Рисунок 37 – Журналирование событий

Затем создать новую политику доступа FDP согласно вышеизложенным пунктам, изменяя лишь приоритет политики и права доступа к устройству в закладке «Доступ». Приоритет поставить выше, чем у политики доступа PDF. В нижней части панели нажать кнопку «Настройки». В окне «Доступ» справа выбрать «Добавить» и указать тех же пользователей данного локального компьютера, изменяя права доступа. Для User1 выбрать чтение, для User2 выбрать полный запрет, а для User3 полный доступ.

Для проверки действия политик осуществить вход на компьютере WinXP01-ZL, используя учетные записи пользователей. Согласно правам для политики FDP с высшим приоритетом, доступ User3 имеет полный доступ к печати файлов, User1 и User2 не имеют доступ печати (см.рисунок 38).

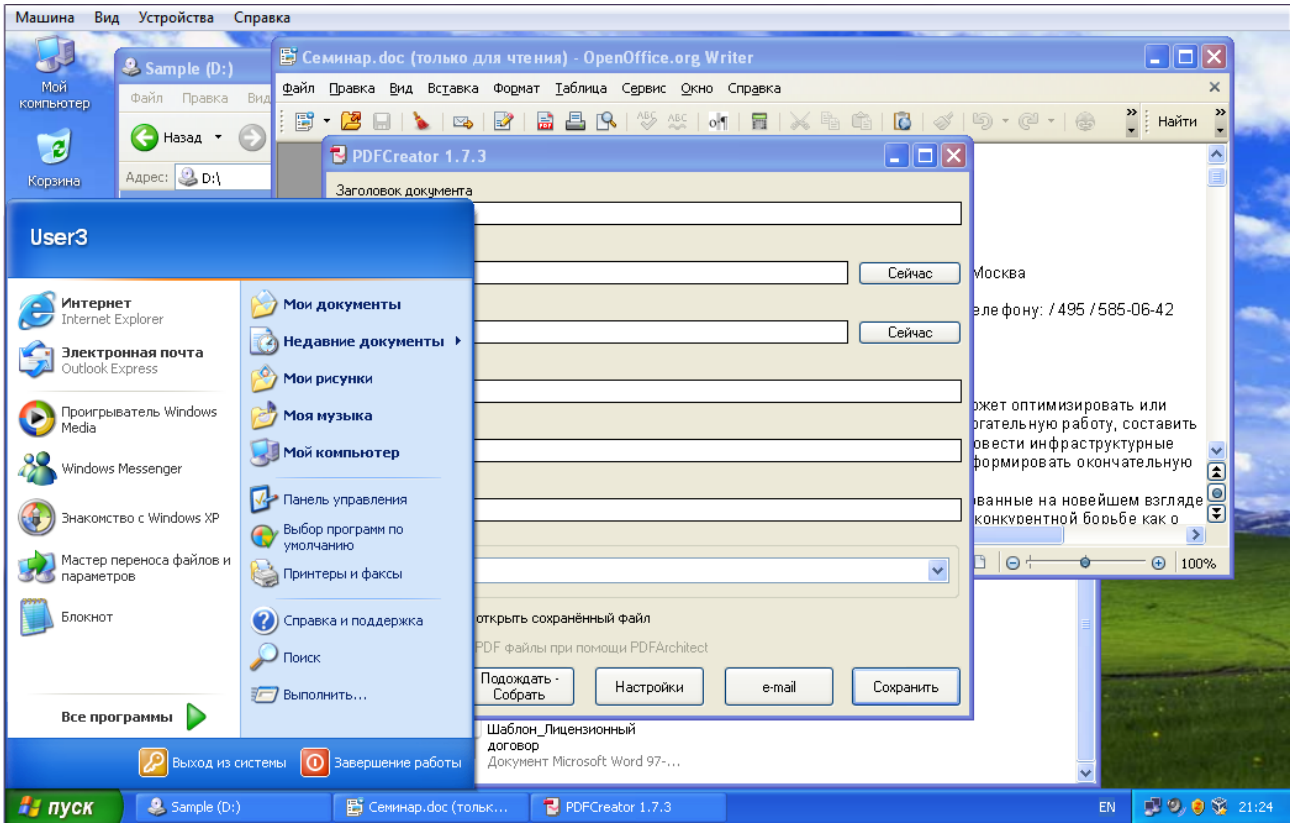

Рисунок 38 – Доступ печати для User3 (FDP)

После выполнения задания необходимо составить отчет, в котором будут представлены результаты выполнения действий в виде снимков экрана, записи файла журналирования, а также вывод, в котором будут описаны навыки, которые были получены при выполнении данного задания.

5 Порядок выполнения задания по изучению функций мониторинга и защиты агентов, реализуемых программным комплексом Zecurion Zlock

5.1 Настройка отображения компьютеров домена и параметров соединения с компьютерами домена

На контроллере домена W2K3-ZL осуществить вход, используя учетную запись доменного администратора. Запустить консоль управления ZLock. Для отображения домена и компьютеров домена включая контроллеры необходимо в меню «Вид» установить способ группирования «По компьютерам». Затем в левой части окна консоли выбрать домен STUDY, открыть диалоговое окно его свойств, щелкнув правой клавишей мыши и выбрав в контекстном меню команду «Свойства домена». Для параметра «Загружать список компьютеров» установить значение «Из Active Directory». Дополнительно установить параметры «Использовать группы Active Directory» и «Проверять доступность компьютеров через NetBIOS». Для параметра «Отображать отсутствующие в NetBIOS компьютеры:» установить значение «как недоступные». Установить параметр «Автоматически обновлять список компьютеров».

Для установления соединения с компьютерами домена необходимо настроить параметры соединения. Настройку следует выполнить для домена STUDY и применить установленные параметры для всех компьютеров домена. Для параметров соединения с доменом STUDY установить следующие значения параметров:

- «Порт:» – номер порта 1246 (по умолчанию);
- «Тип аутентификации:» – аутентификация Windows;
- «Тип пользователя:» – указанный пользователь»;
- «Пользователь:» – имя учетной записи доменного администратора;
- «Вход в:» – название домена STUDY.

Для групп компьютеров «Computers» (компьютеры домена) и «Domain Controllers» (контроллеры домена) в свойствах соединения группы установить параметр «Использовать настройки домена STUDY». Затем настроить свойства соединения с каждым компьютером домена отдельно, установив параметр

использования настройки группы компьютеров при установлении соединения с выбранным компьютером домена.

После настройки параметров соединения с компьютерами проверить их действие установив соединение со всеми компьютерами домена. При подключении к первому компьютеру может быть выдан запрос на ввод имени и пароля администратора. Указать имя учетной записи и пароль доменного администратора, для параметра «Вход в:» установить в качестве значения имя домена STUDY». После подключения просмотреть список приложений ZLock, установленных на каждом компьютере, а также отображение подразделов для настройки политик для устройств и файловых политик.

5.2 Настройка сервера конфигураций

Для настройки сервера конфигураций необходимо открыть диалоговое окно настроек используя команду «Настойки» из меню «Сервис».

На вкладке «Общие» проверить путь к каталогу, в котором хранятся файлы конфигураций сервера. Для этого параметра указать каталог с настроенным общим доступом для компьютеров домена, который был создан для хранения конфигураций Zlock. Он должен быть оставлен по умолчанию. В качестве сервера поиска указать имя контроллера домена W2K3-SRV и проверить соединение. Сервер должен быть доступен (см. рисунок 39).

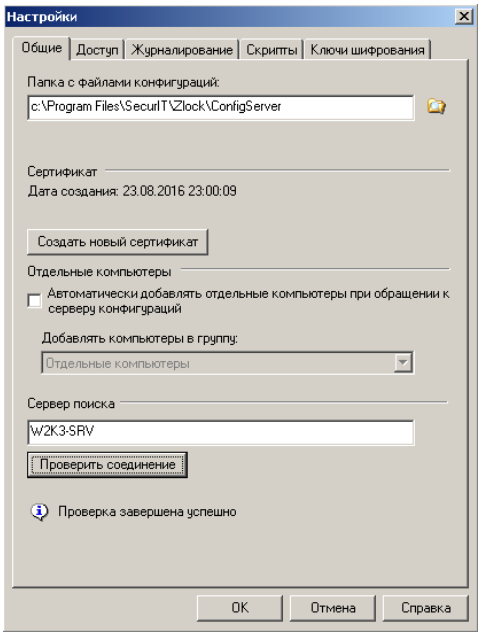

Рисунок 39 – Окно настроек сервера конфигураций

На вкладке «Доступ» нажать кнопку «+», выбрать пункт «Добавить учетную запись или группу Windows». В окне «Добавление пользователя» для параметра «Пользователи из:» установить значение «Домен (STUDY)», для параметра «Показать» – «Пользователи или группы». Для параметра «Фильтр:» значение не указывать. В списке пользователей и групп пользователей выбрать учетную запись доменного администратора и включить его в список контроля доступа. Назначить ему полный доступ (см. рисунок 40).

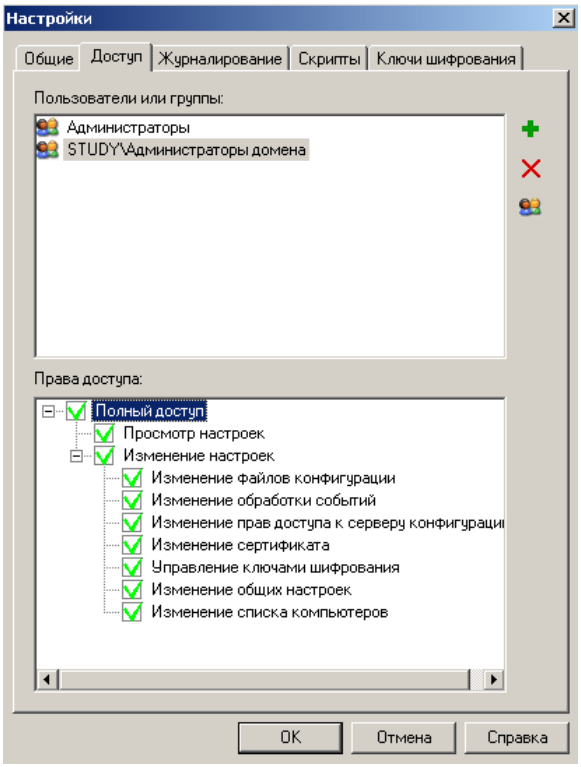

Рисунок 40 –Настройка доступа

Группу «Администраторы», входящую в список контроля доступа по умолчанию, удалить.

На вкладке «Журналирование» нажать кнопку «+» и выбрать команду «Журналирование на сервер». В диалоговом окне «Выбор типа сервера» установить параметр «Сервер журналов» и нажать кнопку «Далее>». В диалоговом окне «Журналирование на сервер журналов» установить следующие значения параметров:

– «Сервер журналов:» – W2K3-SRV. Установка параметра производится с указанием имени сервера вручную;

– «Пользователь:» – имя учетной записи доменного администратора;

– «Пароль:» – пароль учетной записи доменного администратора;

– «Вход в:» – имя домена STUDY.

После настройки требуется нажать кнопку «Проверить соединение». Должно быть выдано сообщение, что проверка завершена успешно (см. рисунок 41).

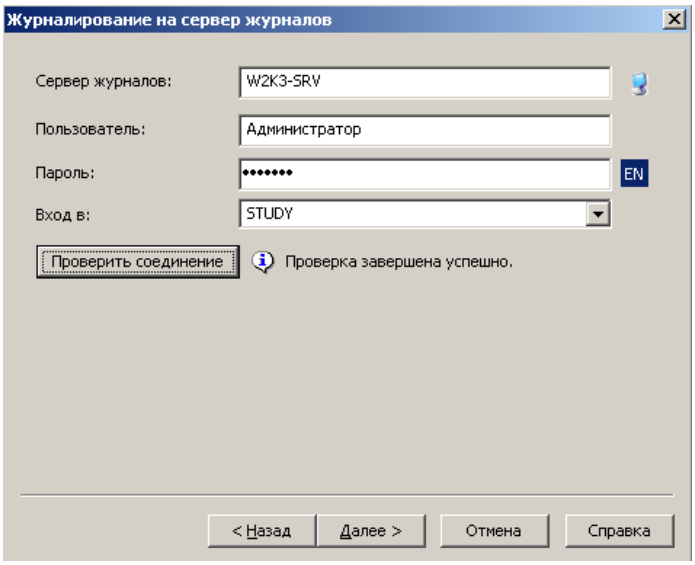

Рисунок 41 – Настройка журналирования

Нажать кнопку «Далее>». В диалоговом окне «Обрабатываемые события» выбрать «Изменение конфигурации», «Изменение настроек доступа», «Изменение общих настроек» и нажать кнопку «Готово» (см рисунок 42).

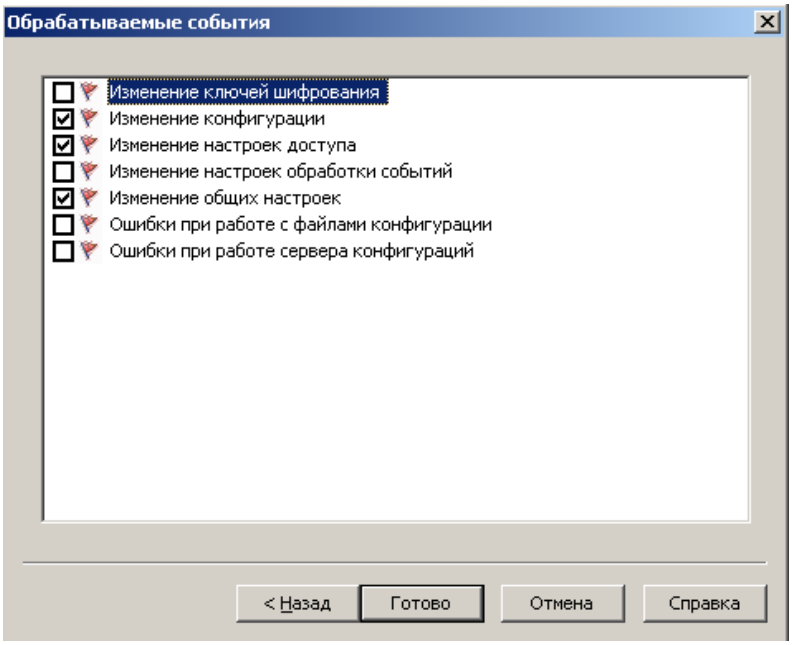

Рисунок 42 – Выбор обрабатываемых событий

Для завершения настроек сервера конфигураций нажать кнопку «ОК».

Для настройки файла конфигураций необходимо отобразить иерархию компьютеров домена в правой части окна консоли управления, выбрать настраиваемый объект и нажать кнопку «…». Для создания конфигурации выбрать группу компьютеров «Computers».

При нажатии кнопки «…» появится диалоговое окно «Конфигурация Zlock», в котором надо нажать кнопку «+». Появится диалоговое окно «Список настроек». В диалоговом окне «Список настроек» указать необходимые настройки для новой конфигурации. Для настройки конфигурации в диалоговом окне «Список настроек» отключить все настройки, кроме настроек «Снимки экрана» и «Теневое копирование на сервер» и нажать кнопку «ОК». В диалоговом окне «Конфигурация Zlock» отобразится вкладка «Прочие настройки». На этой вкладке находится набор параметров для настройки теневого копирования и снимков экрана (см. рисунок 43).

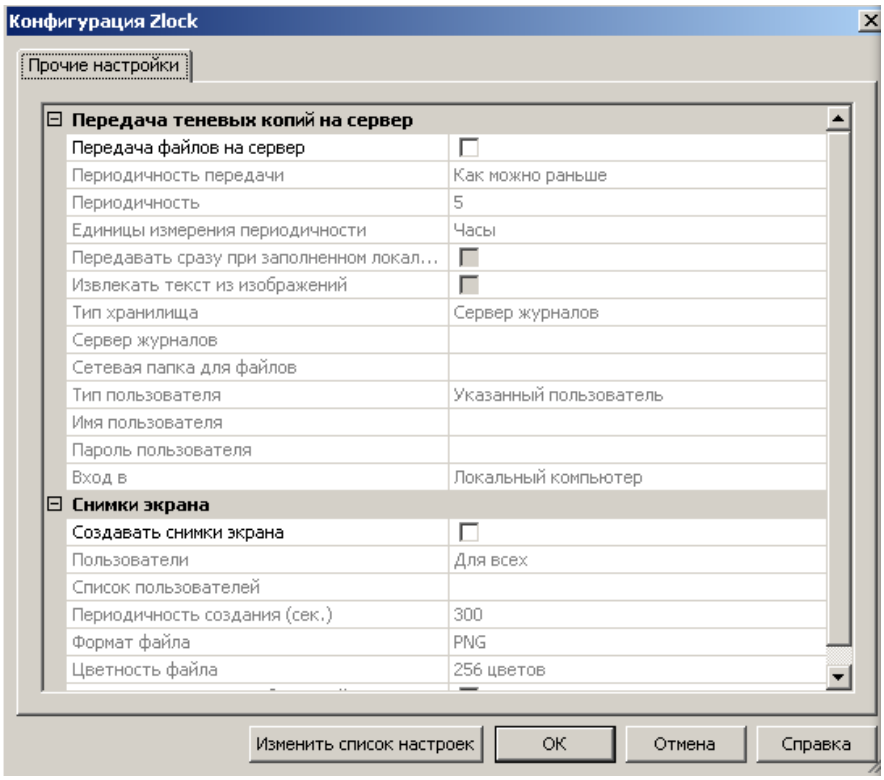

Рисунок 43 – Настройка конфигурации

Для теневого копирования включить параметр «Передача файлов на сервер». Для параметра «Сервер журналов» указать имя сервера – W2K3-SRV. Для параметра «Сетевая папка для файлов» указать сетевой путь к каталогу общего доступа, созданного для хранения теневых копий. Для параметра «Имя

пользователя» указать имя учетной записи доменного администратора. Для ввода пароля администратора нажать кнопку «…», ввести пароль доменного администратора и его подтверждение. Для параметра «Вход в» указать имя домена STUDY. Остальные параметры теневого копирования оставить без изменения.

Для настройки снимков экрана установить параметр «Создавать снимки экрана». Для параметра «Пользователи» установить значение «Для всех». Периодичность создания снимков экрана установить равной 30 секундам. Остальные значения оставить без изменения. После завершения настройки нажать кнопку «ОК».

В диалоговом окне «Сохранение конфигурации» указать имя файла, в котором будет сохранена конфигурация, и нажать кнопку ОК. Созданная конфигурация будет отражена в диалоговом окне «Конфигурация Zlock». Для сохранения настроек нажать кнопку ОК. В правой части окна консоли управления в колонке «Конфигурация», в строке с именем группы компьютеров домена Computers должно отобразиться имя файла, в котором сохранена конфигурация.

Для того чтобы эта конфигурация была применена к компьютеру WinXP01-ZL необходимо выполнить следующие действия. В правой части окна консоли управления в колонке «Наследование» в строке с именем компьютера WinXP01-ZL установить отметку. При этом в колонке «Конфигурация» должно отобразиться имя файла, в котором сохранена конфигурация. Для компьютера WinXP02-ZL наследование конфигурации отключить.

Затем проверить установление соединения с компьютером домена WinXP01-ZL и если необходимо, то установить его. Открыть диалоговое окно настроек приложения Zlock, установленного на этом компьютере. В диалоговом окне настроек перейти на вкладку «Шифрование и загрузка настроек». Для параметра «Управление настройками» установить значение «Загружать настройки с сервера конфигураций». Для параметра «Имя сервера» в группе настроек «Сервер конфигураций» указать имя сервера конфигураций –

W2K3-SRV. Нажать кнопку «Проверить соединение». Проверка должна быть завершена успешно. Результат представить в отчете в виде снимка экрана. После выполнения настройки и проверки соединения с сервером нажать кнопку «ОК».

Далее в левой части окна консоли управления выбрать приложение Zlock, установленного на компьютере WinXP01-ZL. В правой части окна консоли управления в группе параметров «Загрузка настроек» проверить состояние параметра «Синхронизация настроек». Должно быть указано имя сервера конфигураций. В качестве значения параметра «Последняя синхронизация» может быть указано, что синхронизация не проводилась. Статус синхронизации может указывать на то, что конфигурация для компьютера не определена. В качестве сервера поиска также должен быть указан контроллер домена W2K3-SRV. После включения наследования конфигурации становится доступной гиперссылка «синхронизировать» как часть значения параметра «Последняя синхронизация». Для применения конфигурации к компьютеру WinXP01-ZL необходимо щелкнуть по этой гиперссылке и дождаться завершения синхронизации. Значение параметра «Последняя синхронизация» изменится и будет отражать дату и время последней синхронизации. Также изменится значение параметра «Статус синхронизации». Появится еще один параметр отображающий имя файла конфигурации.

Для проверки применения политики на компьютере WinXP01-ZL осуществить вход, используя учетную запись любого локального пользователя, и выполнить действия, имитирующие работу пользователя на компьютере. При имитации действий пользователя необходимо проверять содержимое каталога общего доступа, который создан для хранения теневых копий, для проверки создания снимков экрана. Действие политики должно приводить к созданию графических файлов, которые являются снимками экрана, создаваемыми на компьютере WinXP01-ZL. После проверки применения политики и создания нескольких снимков экрана завершить сеанс работы пользователя.

5.3 Настройка сервера журналов и отображение записей в журнале событий

Для настройки сервера журналов и просмотра записей о применении политик и конфигураций необходимо установить соединение с контроллером домена W2K3-SRV и открыть список установленных приложений. Выбрать сервер журналов, щелкнув правой клавишей мыши по имени приложения и в контекстном меню выбрать команду «Настройки». На вкладке «Хранение журналов» должен быть установлен параметр «Журналирование в файлы формата XML». Параметр «Каталог» указывает полный путь к файлу, используемому для хранения на сервере записей о событиях. Оставить значение параметра без изменений. На вкладке «Доступ» в списке контроля доступа будут указаны группы «Все» и «Администраторы». Добавить в список контроля доступа учетную запись администратора домена и предоставить ему полный доступ к серверу журналов. Группу «Администраторы» удалить. Для группы «Все» должно быть указано разрешение «Добавление в журнал». После настройки параметров сервера журналов применить изменения, нажав кнопку «ОК».

Для просмотра записей в журнале аудита необходимо добавить журнал для просмотра записей, в который они будут загружены из файла, указанного в настройках сервера журналов. Для добавления журнала необходимо в консоли управления выбрать основной узел «Журнал событий» щелкнув правой клавишей мыши и выбрать команду «Добавить» (см. рисунок 44).

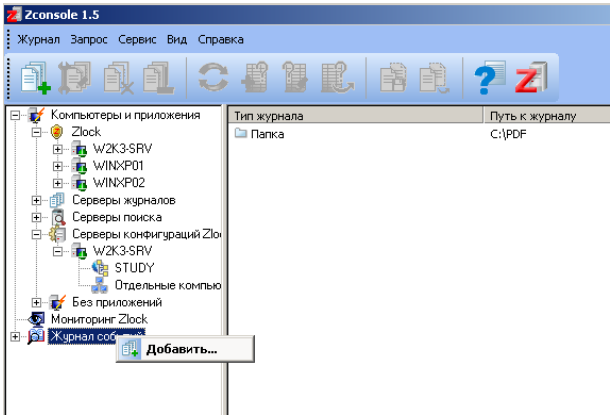

Рисунок 44 – Команда добавления журнала для просмотра событий

В диалоговом окне «Добавление журнала» выбрать тип журнала. Тип журнала выбрать «Сервер журналов» поскольку при настройке сервера конфигураций выбирался способ журналирования на сервер. Также можно выбрать значение «Журналирование в файлы формата XML» поскольку этот способ указан в настройках сервера конфигураций. Выбор одного из этих двух источников отобразит одинаковые записи, так как XML-файл находится на сервере журналов.

Для типа журнала «Сервер журналов» необходимо указать имя журнала, которое будет отображаться в консоли управления. Также необходимо определить параметры подключения к серверу журналов. Они должны иметь следующие значения:

- «Сервер журналов:» – W2K3-SRV;
- «Тип пользователя:» – указанный пользователь;
- «Пользователь:» – имя учетной записи доменного администратора;
- «Пароль:» – пароль учетной записи доменного администратора;
- «Вход в:» – имя домена STUDY.

После настройки параметров нажать кнопку «Проверить соединение». Для завершения настройки нажать кнопку ОК. После настройки журнала его имя должно отобразиться в узле основного уровня «Журнал событий».

Для просмотра записей необходимо в левой части окна консоли выбрать имя журнала щелкнув левой клавишей мыши. В правой части окна консоли будет отображено окно для вывода записей о событиях. Для отображения и просмотра записей из журнала сначала следует создать новый запрос или использовать встроенный. Для создания запроса необходимо выбрать в выпадающем списке «Запрос» пункт «<Добавить запрос>». Появится список встроенных запросов (см. рисунок 45).

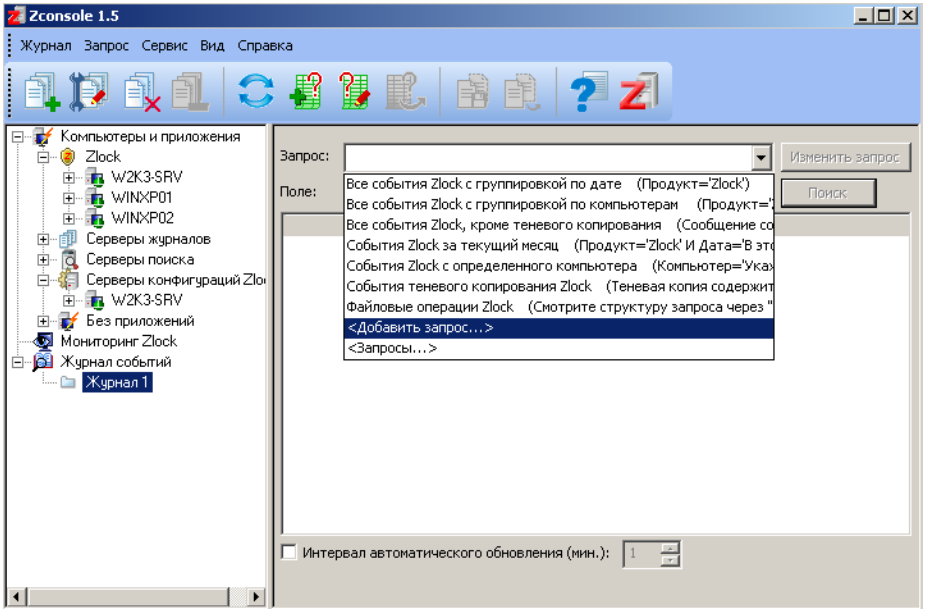

Рисунок 45 – Выбор запроса для отображения записей в журнале

Необходимо ввести имя запроса, выбрав один из встроенных, либо создать запрос, изменив условия для запроса в поле «Условия». Для отображения всех записей накопленных при выполнении задания необходимо выбрать запрос «Все события Zlock с группировкой по дате». Для параметра «Поле:» по умолчанию устанавливается значение «Время».

Для выбора необходимых записей требуется построить запрос, определяющий критерии выбора. Можно использовать один из встроенных запросов. Например, для выбора записей о событиях на компьютере WinXP01-ZL, можно использовать запрос «Все события Zlock с группировкой по компьютерам». События будут сгруппированы по каждому компьютеру домена, на котором события зафиксированы.

Также можно изменить встроенный запрос. Например, если требуется вывести записи о событиях, произошедших на определенном компьютере без использования группировки. Для выбора соответствующих записей следует использовать запрос «События Zlock с определенного компьютера», выбрав его в выпадающем списке «Запрос:». Затем нажать кнопку «Изменить запрос» (см. рисунок 38). Будет выдано диалоговое окно «Запрос» (см. рисунок 46).

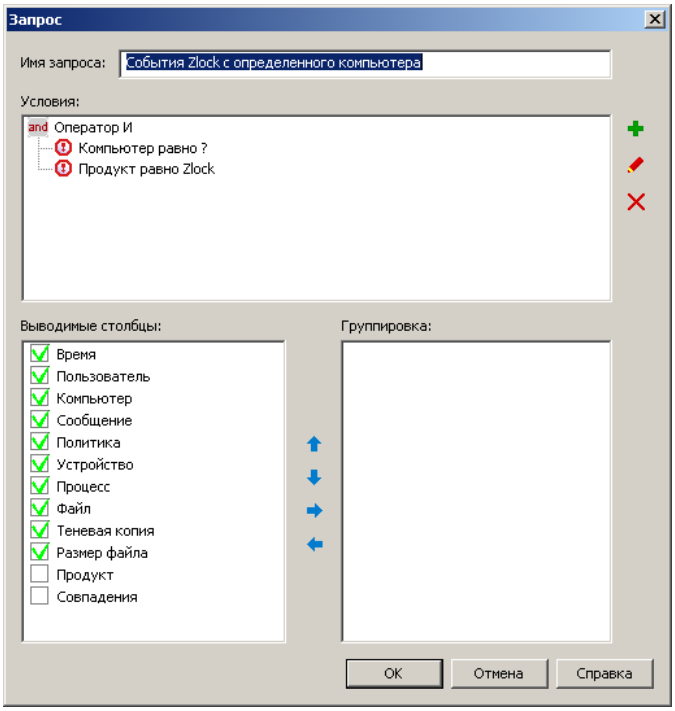

Рисунок 46 – Изменение параметров запроса

В этом окне отображается имя запроса, логический оператор, используемый для объединения условий, условия запроса, столбцы, содержащие сведения о событии и их возможная группировка. Для вывода всех записей о событиях, которые произошли на компьютере WinXP01-ZL необходимо выбрать условие «Компьютер …» и нажать кнопку редактирования «Изменить». В диалоговом окне «Условие» надо указать значение условие «Поле» запроса, логический оператор и значение, поиск которого будет осуществляться по запросу (см. рисунок 47).

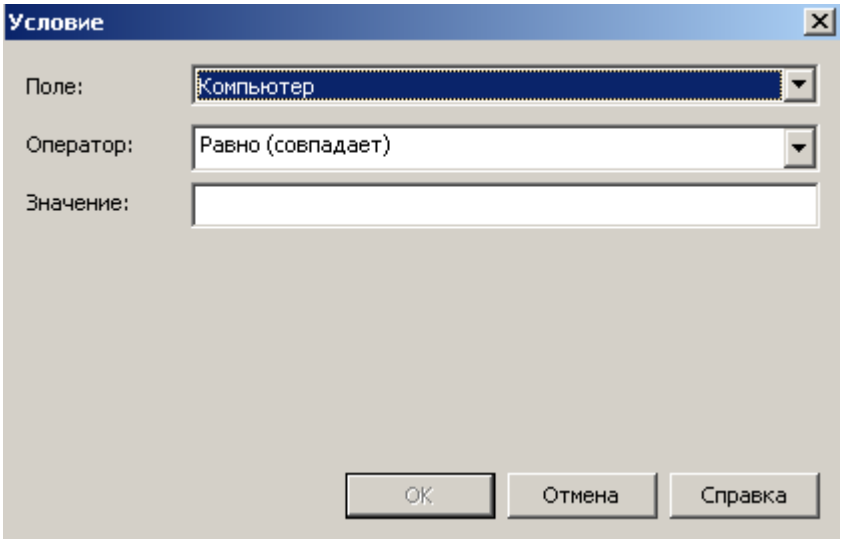

Рисунок 47 – Формирование условий запроса

Для выбора записей необходимо указать для условия «Поле» значение «Компьютер». Оператор выбрать «Равно (совпадает)». В качестве значения указать имя компьютера, отображаемое в домене – WINXP02. В диалоговом окне «Запрос» должно отобразиться имя компьютера как условие поиска. Порядок и группировку выводимых столбцов не менять. После настройки запроса сохранить его параметры в виде снимка экрана. Для завершения настройки нажать кнопку ОК. В правой части окна консоли управления должны быть отображены записи обо всех событиях, которые произошли на компьютере WinXP02-ZL.

Аналогично можно сформировать запросы для вывода записей о действиях определенных пользователей. Например, для вывода сведений о действиях доменного администратора при настройке Zlock потребуется создать новый запрос, поскольку встроенный запрос для пользователей, отсутствует. Для создания нового запроса необходимо нажать кнопку «Добавить запрос» на панели инструментов. В диалоговом окне «Запрос» необходимо определить имя запрос и его условия. Для добавления условий надо нажать кнопку «+». В диалоговом окне «Условия» для параметра «Поле:» установить значение «Пользователь», для параметра «Оператор:» – «Равно (совпадает)». В качестве значения параметра «Значение:» указать имя учетной записи доменного администратора – STUDY\Администратор. Нажать кнопку «ОК» для завершения настроек условий. Для запроса о действиях администратор необходимо добавить еще одно условие, указывающее на компонент Zlock, с которым работал администратор. Для добавления второго условия надо выполнить аналогичные действия. Указать следующие значения параметров условий:

- для параметра «Поле:» установить значение «Продукт»;
- для параметра «Оператор:» – «Равно (совпадает)»;
- для параметра «Значение:» – Zlock.

После настройки второго условия нажать кнопку «ОК». Будет выдан запрос о том, какой логический оператор использовать для объединения условий. Выбрать оператор «И».

В списке выводимых столбцов в диалоговом окне «Запрос» указать столбцы – «Время», «Пользователь», «Компьютер», «Сообщение» и «Продукт». После завершения настройки запроса нажать кнопку «ОК». В правой части окна консоли управления будут отображены записи, соответствующие условиям запроса. При необходимости запрос можно отредактировать, выбрав его в списке и нажав кнопку «Изменить запрос».

По выводимым записям можно осуществлять поиск. Для этого необходимо выбрать поле, по которому будет производиться поиск в раскрывающемся списке параметра «Поле». Ввести в строку поиска информацию, которую необходимо найти и нажать кнопку «Поиск». Будут отображены те записи, которые соответствуют установленному запросу и содержат введенную строку поиска. Для отмены результатов поиска нажать кнопку «Отмена».

Записи, выбранные в результате применения запроса можно сохранить в файл. В качестве формата используется HTML. Для сохранения записей необходимо после применения запроса в меню «Сервис» выбрать команду «Запрос» - «Экспорт в HTML…».

В диалоговом окне «Экспорт сообщений» указать имя файла отчета и каталог, в котором будет сохранен файл. Все отчеты, построенные с использованием созданных поисковых запросов экспортировать в файл.

5.4 Настройка задач мониторинга

Настройка параметров мониторинга производится как для отдельного компьютера, так и для группы, либо домена в целом. При этом отдельный компьютер может либо наследовать настройки от объекта-родителя (группы или домена), либо иметь индивидуальные настройки, в зависимости от состояния указываемой при настройке опции «Наследовать настройки мониторинга».

Чтобы включить мониторинг компьютера, группы, или домена нужно открыть в дереве пункт «Компьютеры и приложения» и выбрать необходимый элемент дерева — компьютер, группу либо домен.

Выбрать пункт «Свойства соединения» и перейти на вкладку «Мониторинг Zlock». Отметить пункт «Включить мониторинг состояния Zlock». В поле «Периодичность» оставить по умолчанию, где указан минимальный интервал опроса данного объекта. В зависимости от загрузки сети, числа одновременно опрашиваемых компьютеров и других факторов, реальное значение периодичности опроса может быть больше, чем заданное.

Отметить пункт «Загружать конфигурацию Zlock и анализировать изменения», указать учетную запись пользователя для запроса информации с удаленного компьютера. В случае обнаружения несанкционированных изменений настроек Zlock выполнит заранее указанные действия.

Загруженную конфигурацию можно сравнить с той, которая распространялась с сервера конфигураций или через групповые политики. Для этого необходимо выбрать пункт «Сравнивать загруженную конфигурацию с» и указать источник сравнения «Сервером конфигурации» (см. рисунок 48).

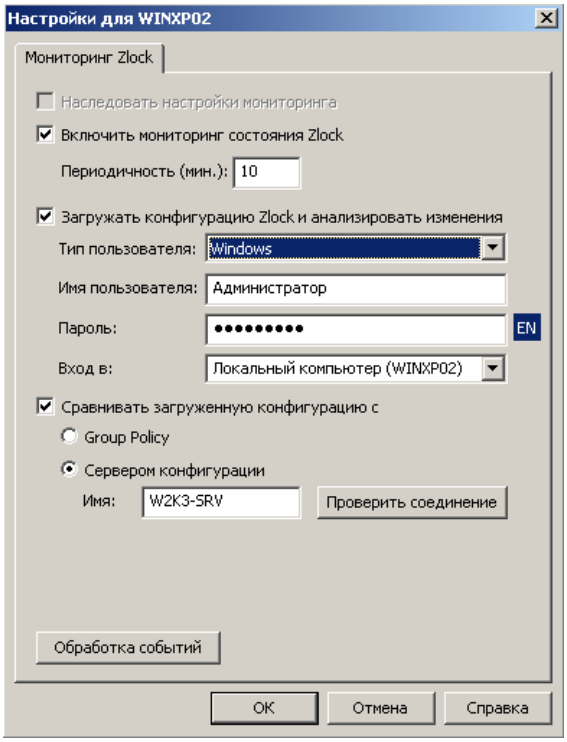

Рисунок 48 – Свойства соединения

Указать, какие действия нужно выполнить при возникновении каждой ситуации. Для этого нажать на кнопку «Обработка событий» (см. рисунок 49).

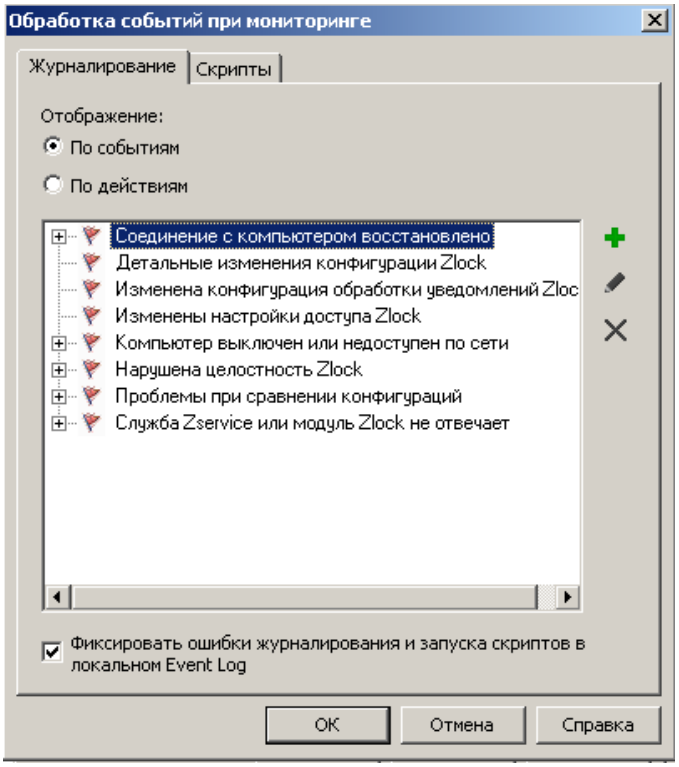

Рисунок 49 – Обработка событий

Изменения вступают в силу после закрытия окна «Свойства соединения» кнопкой «ОК».

Мониторинг компьютеров осуществляется в фоновом режиме, независимо от запущенной консоли управления и сеанса пользователя.

Затем в Панели управления на компьютере WinXP02-ZL открыть раздел «Администрирование» и запустить консоль «Службы». Найти службу Zlock Service в списке локальных служб и выполнить попытку ее останова, изменив тип запуска. После проверки возможности останова службы Zlock Service найти исполняемый файл, соответствующий этой службе и выполнить попытки его удаления и переименования. Результаты отразить в виде снимков экрана.

После выполнения проверок на контроллере домена W2K3-ZL подключиться к серверу Zecurion Zlock и перейти к подразделу «Журнал событий». Найти все события, связанные с работой созданной задачи мониторинга – запуск и завершение задачи, проверка и восстановление настроек сервиса Zlock, установленного на компьютере WinXP01-ZL, а также

сообщения об изменениях настроек. Примеры записей о событиях из журнала мониторинга включить в отчет о выполнении практического задания.

5.5 Просмотр текущего статуса компьютеров

Через заданные промежутки времени модуль мониторинга производит опрос клиентских модулей и отображает статус опрашиваемых компьютеров. При мониторинге отслеживаются следующие ситуации:

– изменена конфигурация Zlock — это означает, что имело место несанкционированное изменение политик Zlock непосредственно на удаленной машине или с использованием удаленного управления (изменение политик с той же консоли администратора, где работает мониторинг, считается санкционированным);

– изменена конфигурация обработки уведомлений Zlock — это означает, что имело место несанкционированное изменение обработки событий (журналирования) Zlock как непосредственно на удаленной машине, так и с какой-либо другой удаленной консоли администратора (изменение настроек обработки событий с той же консоли администратора, где работает мониторинг, считается санкционированным);

– изменены настройки безопасности Zlock — имело место несанкционированное изменение прав доступа к управлению системой Zlock или изменение сертификата, такое изменение могло произойти как непосредственно на удаленной машине, так и с какой-либо другой удаленной консоли администратора (изменение настроек доступа с той же консоли администратора, где работает мониторинг, считается санкционированным);

– нарушена целостность Zlock — это означает, что проверка наличия и целостности всех необходимых модулей, драйверов, записей в реестре выявила нарушение целостности Zlock;

– компьютер выключен или недоступен по сети — это означает, что компьютер отсоединен от сети или выключен;

– соединение с компьютером восстановлено — это значит, что Zlock функционирует нормально после, например, перезагрузки удаленного компьютера;

– служба Zservice или модуль Zlock не отвечает — удаленный компьютер доступен по сети, но служба Zservice или модуль Zlock на нем не отвечают;

– проблемы при сравнении конфигураций — не удалось загрузить конфигурацию с клиентской части или с сервера конфигураций для сравнения.

Для просмотра статуса удаленных компьютеров необходимо выбрать узел «Мониторинг Zlock». Настройка отображения результатов мониторинга выполняется через меню «Вид».

5.6 Изменение конфигурации

Для того чтобы на сервере конфигураций назначить, отредактировать или удалить существующую или создать новую конфигурацию необходимо в правой части консоли в сервере конфигураций выбрать объект. В окне «Конфигурация Zlock» выбрать из списка существующую конфигурацию.

В открывшемся окне «Список настроек» указать необходимые настройки для редактирования выбранной конфигурации.

Нажав кнопку «Изменить список настроек» можно вернуться в окно «Список настроек» и добавить или удалить настройки из списка.

Указать имя создаваемой конфигурации и нажать «Ок». Выбрать в окне «Конфигурации Zlock» конфигурацию и назначить ее объекту, нажав на «ОК».

5.7 Экспорт данных, буфер обмена и просмотр конфигурации

Результаты мониторинга можно экспортировать в файл формата XML или выгружать в буфер обмена для создания отчетов и анализа возникавших ситуаций.

Для этого необходимо выбрать в меню «Мониторинг» пункт «Экспорт данных» или пункт «Скопировать в буфер обмена».

Пункт меню «Просмотр конфигурации» открывает окно для просмотра конфигурации, назначенной данному компьютеру.

Настройки мониторинга каждого компьютера из списка можно вызвать с помощью пункта «Свойства» в меню «Мониторинг».

После выполнения задания необходимо составить отчет, в котором будут представлены результаты выполнения действий в виде снимков экрана, записи файла журналирования и журналов на сервере, а также вывод, в котором будут описаны навыки, которые были получены при выполнении данного задания.

6 Описание порядка выполнения заданий практикума и результатов выполнения

6.1 Порядок выполнения заданий практикума

Выполнение задания практикума предполагает следующую последовательность действий:

– изучение теоретического материала, приведенного в методических указаниях 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.

6.2 Порядок выполнения практического задания по применению программного комплекса Zecurion Zlock для выявления и предотвращения утечек информации

6.2.1 Начало выполнения задания практикума

6.2.1.1 Создание учетных записей локальных пользователей на компьютере WinXP01-ZL.

6.2.1.2 Осуществить вход на контроллере домена W2K3-DL с использованием учетной записи доменного администратора.

6.2.1.3 С помощью консоли управления выполнить настройку аудита и теневого копирования для сервиса Zecurion Zlock.

6.2.1.4 С помощью консоли управления выполнить настройку управления сервисом Zecurion Zlock.

6.2.1.5 Выполнить настройку режима отображения устройств для сервиса Zecurion Zlock.

6.2.1.6 Установить соединение с удаленными компьютерами.

6.2.1.7 Просмотр списка подключенных устройств.

6.2.2 Создание политики доступа к устройству

6.2.2.1 С помощью консоли управления выполнить создание политики доступа к устройству на компьютере WinXP01.

6.2.2.2 Выполнить добавление и настройку прав доступа для созданных пользователей.

6.2.2.3 Происходит выбор источника списка устройств и само устройство.

6.2.2.4 Происходит выбор типа расписания и времени действия политики.

6.2.2.5 Настройка правил применения, где выбирается состояние домена, при котором данная политика будет активна.

6.2.2.6 Настройка журналирования и обработки файловых операций и печати.

6.2.2.7 Настройка теневого копирования для данного устройства.

6.2.3 Проверка настроек политики доступа на защищаемом компьютере

6.2.3.1 На компьютере домена WinXP01 осуществить вход под учетными записями пользователей и имитировать попытки доступа включая попытки НСД.

6.2.3.2 Осуществить анализ записей событий файла журналирования.

6.2.3.3 Формирование отчета по событиям файла журналирования.

6.2.4 Порядок выполнения задания в виде UML-диаграммы

Порядок выполнения задания по применению программного комплекса Zecurion Zlock для выявления и предотвращения утечек информации представлен в виде UML-диаграммы в приложении Б.

6.3 Порядок выполнения практического задания по изучению функций мониторинга и защиты агентов, реализуемых программным комплексом Zecurion Zlock

6.3.1 Начало выполнения задания практикума

6.3.1.1 На компьютере домена WinXP01-ZL осуществить вход, используя учетную запись доменного или локального администратора, и создать три учетных записи локальных пользователей.

6.3.1.2 На контроллере домена W2K3-ZL осуществить вход, используя учетную запись доменного администратора.

6.3.1.3 Выполнить настройку параметров соединения с компьютерами домена.

6.3.1.4 Выполнить подготовку каталогов, необходимых для создания и применения конфигураций.

6.3.1.5 Настроить отображение компьютеров, управляемых сервером конфигураций.

6.3.2 Настройка сервера конфигураций

6.3.2.1 С помощью диалогового окна настроек консоли управления Zlock проверить путь к каталогу с файлами конфигурации.

6.3.2.2 Добавить учетную запись доменного администратора в список контроля доступа с назначением полного доступа.

6.3.2.3 Выполнить настройку журналирования на сервер журналов.

6.3.2.4 Настроить обрабатываемые события.

6.3.2.5 Выполнить настройку файла конфигурации.

6.3.2.6 Выполнить настройку передачи теневых копий на сервере и снимков экрана.

6.3.2.7 Применение конфигурации, созданной на сервере конфигураций, к компьютерам домена.

6.3.2.8 Проверка применения к компьютерам домена конфигурации, созданной на сервере конфигураций.

6.3.2.9 Контроль состояния компьютеров при удалении конфигурации.

6.3.2.10 Настроить сервер журналов.

6.3.2.11 Добавление журнала для просмотра записей, сохраненных на сервере журналов.

6.3.2.12 Формирование запросов для построения отчетов по записям, сохраненным на сервере журналов.

6.3.2.13 Экспорт записей, выбранных с использованием запросов в HTML-файл.

6.3.2.14 Просмотр событий для просмотра перехваченных снимков экрана.

6.3.3 Создание задач мониторинга

6.3.3.1 Создание мониторинга для контроля состояния программного агента Zecurion Zlock.

6.3.3.2 Применение задач мониторинга для контроля состояния программного агента Zecurion ZLock и выявления изменения настроек.

6.3.3.3 Применение задач мониторинга для восстановления настроек программного агента Zecurion Zlock.

6.3.3.4 Анализ записей по файлу журналирования и записям на сервере конфигураций.

6.3.4 Порядок выполнения задания в виде UML-диаграммы

Порядок выполнения задания по изучению функций мониторинга и защиты агентов, реализуемых программным комплексом Zecurion Zlock представлен в виде UML-диаграммы в приложении В.

7 Описание структуры и содержания отчета о выполнении практических заданий

7.1 Общий перечень данных, содержащихся в отчете

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

- цель задания;
- содержание задания;
- описание выполнения задания, иллюстрируемое снимками экрана;
- представление файлов журналирования и отчетов;
- вывод.

Снимки экранов необходимо делать в процессе выполнения лабораторной работы 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.

7.2 Структура отчета по выполнению задания по применению функциональных возможностей программного средства защиты Zecurion Zlock для контроля и предотвращения утечек информации

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:
  - описание подготовительных действий для начала выполнения задания;
  - настройка политики доступа к устройству;

– описание проверки настроек политики на защищаемом компьютере;

– просмотр файла журналирования;

– 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.

7.3 Структура отчета по выполнению задания по изучению функций мониторинга и защиты агентов, реализуемых программным комплексом Zecurion Zlock

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:

– описание подготовительных действий для начала выполнения задания;

– описание процедуры настройки сервера конфигураций;

– описание процедуры настройки сервера журналов;

– описание процедуры создания задач мониторинга для контроля состояния Zecurion Zlock;

– изменение конфигурации;

– экспорт данных;

– проверка состояния;

– 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.

8 Определение порядка контроля выполнения практического задания

8.1 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;

– полноты сформированных отчетов по файлам журналирования и журналам на сервере событий в ходе выполнения заданий 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 журналирования событий и журналам 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.

8.2 Порядок контроля практического задания по применению программного комплекса Zecurion Zlock для выявления и предотвращения утечек информации

Должны быть показаны в виде снимков экрана:

– результаты проверки текущих настроек доступа на компьютере WinXP01-ZL после попыток изменения настроек локальным администратором;

– результат настройки доступа к принтеру и аудита на компьютере WinXP01-ZL, установленные с помощью консоли Zecurion ZLock;

– результаты применения файла настроек сервиса Zecurion ZLock на компьютере WinXP01-ZL;

– результаты изменения настроек доступа пользователя User1 к принтеру на компьютере WinXP01-ZL;

– результаты проверки действия политики доступа к устройству с имитацией попыток НСД.

8.3 Порядок контроля практического задания по изучению функций мониторинга и защиты агентов, реализуемых программным комплексом Zecurion Zlock

Должны быть показаны в виде снимков экрана:

– результаты настройки журнала и проверки подключения к серверу журналов;

– результаты настройки запроса для выбора записей о событиях, произошедших на компьютере WinXP02-ZL;

– результаты настройки запроса для выбора записей, содержащих сведения о действиях доменного администратора по созданию конфигурации;

– результаты настройки запросов для выбора записей, содержащих сведения о действиях локальных пользователей на компьютере WinXP02-ZL и создании снимков экрана при выполнении этих действий;

– результаты просмотра сведений о событиях, возникших при применении конфигурации и создании снимков экрана, а также просмотра созданных снимков экрана;

– результаты настройки задачи мониторинга агента Zecurion Zlock на компьютере

– результаты проверки статуса сервиса Zecurion Zlock и компьютера WinXP02-ZL после загрузки файла настроек;

– результаты изменения разрешений на доступ к принтеру на компьютере WinXP02-ZL;

– результаты изменения статуса компьютера WinXP02-ZL в консоли после изменения настроек и запуска задачи мониторинга, а также после

повторного запуска задачи мониторинга для восстановления настроек сервиса Zecurion Zlock на компьютере WinXP02-ZL;

– результаты настройки доступа к принтеру в консоли на компьютере WinXP01-ZL;

– результаты попыток останова сервиса Zecurion Zlock на компьютере WinXP01-ZL и удаления файла агента.

9 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:

- виртуальный жесткий диск;
- видеоадаптер;
- сетевой адаптер;
- виртуальный привод оптического диска.

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.

ЗАКЛЮЧЕНИЕ

В результате выполнения ВКР был разработан практикум по применению функциональных возможностей программного средства защиты Zecurion Zlock для контроля и предотвращения утечек информации. Первое задание практикума посвящено применению программного комплекса Zecurion Zlock для выявления и предотвращения утечек информации. Второе задание практикума посвящено изучению функций мониторинга и защиты агентов, реализуемых программным комплексом Zecurion Zlock.

В ходе дипломного проектирования был произведен обзор систем контроля и предотвращения утечек информации, а также функций, реализуемые программным комплексом Zecurion Zlock, были созданы виртуальные машины, которые использованы для построения лабораторного стенда. Были созданы командные файлы для автоматизированного развертывания ВМ на компьютере, 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 и разработаны сценарии для развертывания ВМ.

В результате выполнения заданий практикума студенты получают навыки по применению функциональных возможностей программного средства защиты Zecurion Zlock для контроля и предотвращения утечек информации.

Таким образом, все пункты технического задания на выпускную квалификационную работу выполнены полностью.

Результаты ВКР были представлены на IV Ежегодной межвузовской научно-практической конференции «Информационные технологии в науке и образовании. Проблемы и перспективы» (МНПК – 2017) в секции «Информационная безопасность систем и технологий». Публикации, содержащие представленные результаты, включены в сборник статей [8] конференции, находящийся в издании.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. DATA LOSS PREVENTION Защита от утечек информации [Электронный ресурс]. – Режим доступа: http://www.zecurion.ru/downloads/brochures/Zecurion_DLP.pdf, свободный. – Загл. с экрана.

2. ZECURION Защита информации от утечек (DLP-системы) [Электронный ресурс]. – Режим доступа: http://www.zecurion.ru/, свободный. – Загл. с экрана.

3. DLP-системы и способы их обойти [Электронный ресурс]. – Режим доступа: http://helg82.livejournal.com/128094.html, свободный. – Загл. с экрана.

4. Загрузить VirtualBox – Oracle [Электронный ресурс]. Режим доступа: http://www.oracle.com/technetwork/ru/servers-storage/virtualbox/downloads/index.html, свободный. – Загл. с экрана.

5. MICROSOFT Центр загрузки [Электронный ресурс]. – Режим доступа: https://www.microsoft.com/ru-ru/download/, свободный. – Загл. с экрана.

6. Как настроить DNS [Электронный ресурс]. – Режим доступа: http://compfixer.info/dns-setup/, свободный. – Загл. с экрана.

7. Как настроить брандмауэр Windows [Электронный ресурс]. – Режим доступа: https://sonikelf.ru/kak-nastroit-brandmauer-windows/, свободный. – Загл.с экрана.

8. Фатеев А.Г., Забирова А.А. Механизмы обеспечения безопасности компонентов, реализуемые системами контроля и предотвращения утечек информации. Информационные технологии в науке и образовании. Проблемы и перспективы : сб. науч. ст. IV Ежегод. межвуз. науч.-практ. конф. (г. Пенза, 15 марта 2017 года) / под. ред. Л.Р. Фионовой, А.В. Дурина (в печати).

ПРИЛОЖЕНИЕ А

(обязательное)

Состав виртуального стенда, используемого при выполнении практикума

W2K3-ZL
192.168.10.2
ОС: Windows Server 2003
Роли:
- первичный контроллер домена;
- сервер приложений;
- веб-сервер;
- DNS-сервер;
- SMTP-сервер;
- рабочее место администратора Zlock.
Компоненты:
- службы Active Directory;
- компоненты DNS;
- компоненты IIS.
Приложения программного комплекса ZLock:
- сервер журналов;
- сервер поиска;
- клиентский модуль Zlock;
- журнал событий.
WinXP01-ZL
192.168.10.11
ОС: Windows XP
Компоненты:
- DNS-клиент;
- службы IIS.
Роли:
- компьютер домена;
- автоматизированное рабочее место пользователя.
Установлен клиентский модуль Zlock.
WinXP02-ZL
192.168.10.12
ОС: Windows XP
Компоненты:
- DNS-клиент;
- службы IIS.
Роли:
- компьютер домена;
- автоматизированное рабочее место пользователя.
Установлен клиентский модуль Zlock.

Рисунок А.1

ПРИЛОЖЕНИЕ Б

(обязательное)

UML-диаграмма последовательности действий выполнения задания по применению программного комплекса Zecurion Zlock для выявления и предотвращения утечек информации

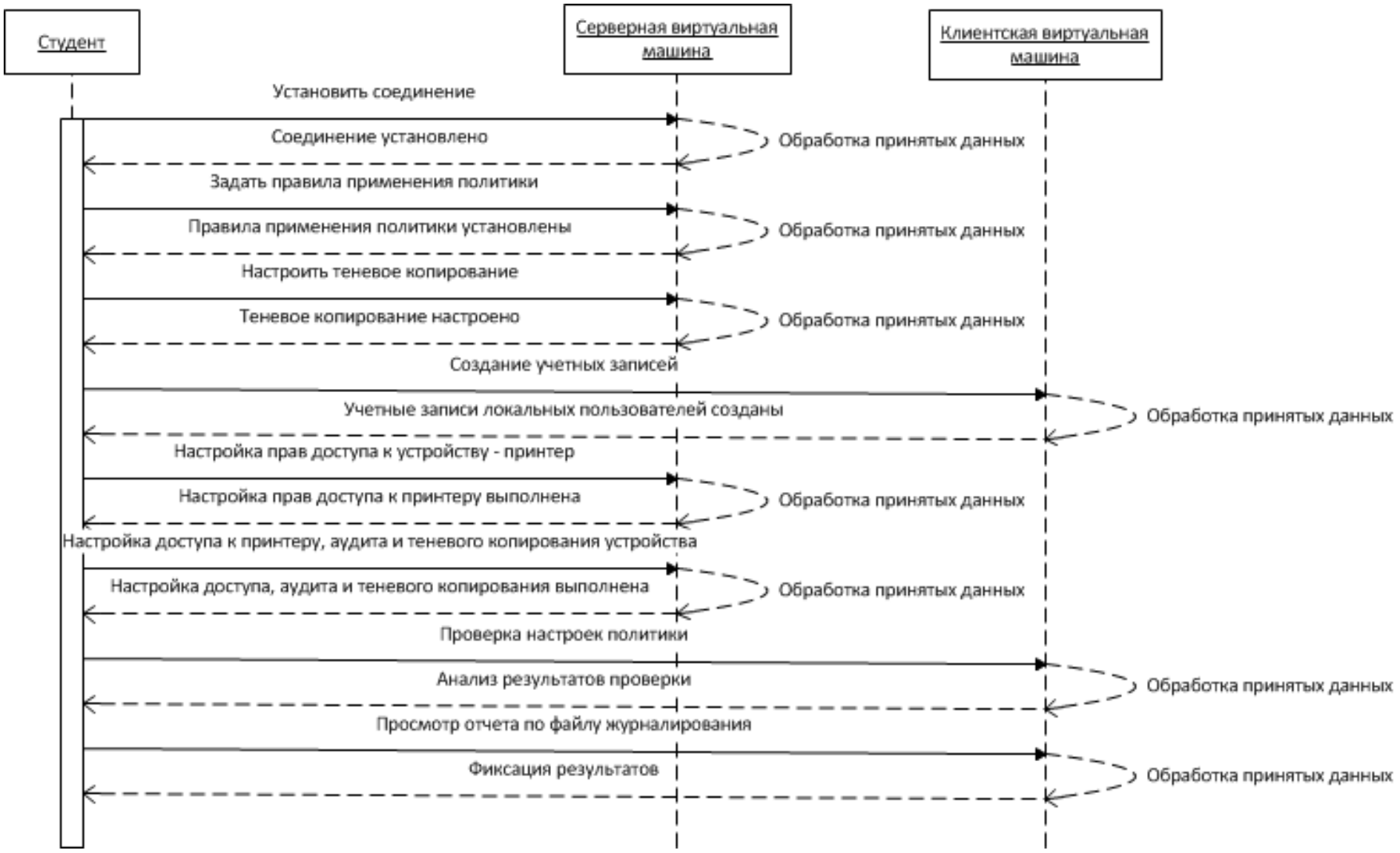
Студент
Серверная виртуальная машина
Клиентская виртуальная машина
Установить соединение
Соединение установлено
Обработка принятых данных
Задать правила применения политики
Правила применения политики установлены
Обработка принятых данных
Настроить теневое копирование
Теневое копирование настроено
Обработка принятых данных
Создание учетных записей
Учетные записи локальных пользователей созданы
Обработка принятых данных
Настройка прав доступа к устройству - принтер
Настройка прав доступа к принтеру выполнена
Обработка принятых данных
Настройка доступа к принтеру, аудита и теневого копирования устройства
Настройка доступа, аудита и теневого копирования выполнена
Обработка принятых данных
Проверка настроек политики
Анализ результатов проверки
Обработка принятых данных
Просмотр отчета по файлу журналирования
Фиксация результатов
Обработка принятых данных

Рисунок Б.1

ПРИЛОЖЕНИЕ В

(обязательное)

UML-диаграмма последовательности действий выполнения задания по изучению функций мониторинга и защиты агентов, реализуемых программным комплексом Zecurion Zlock

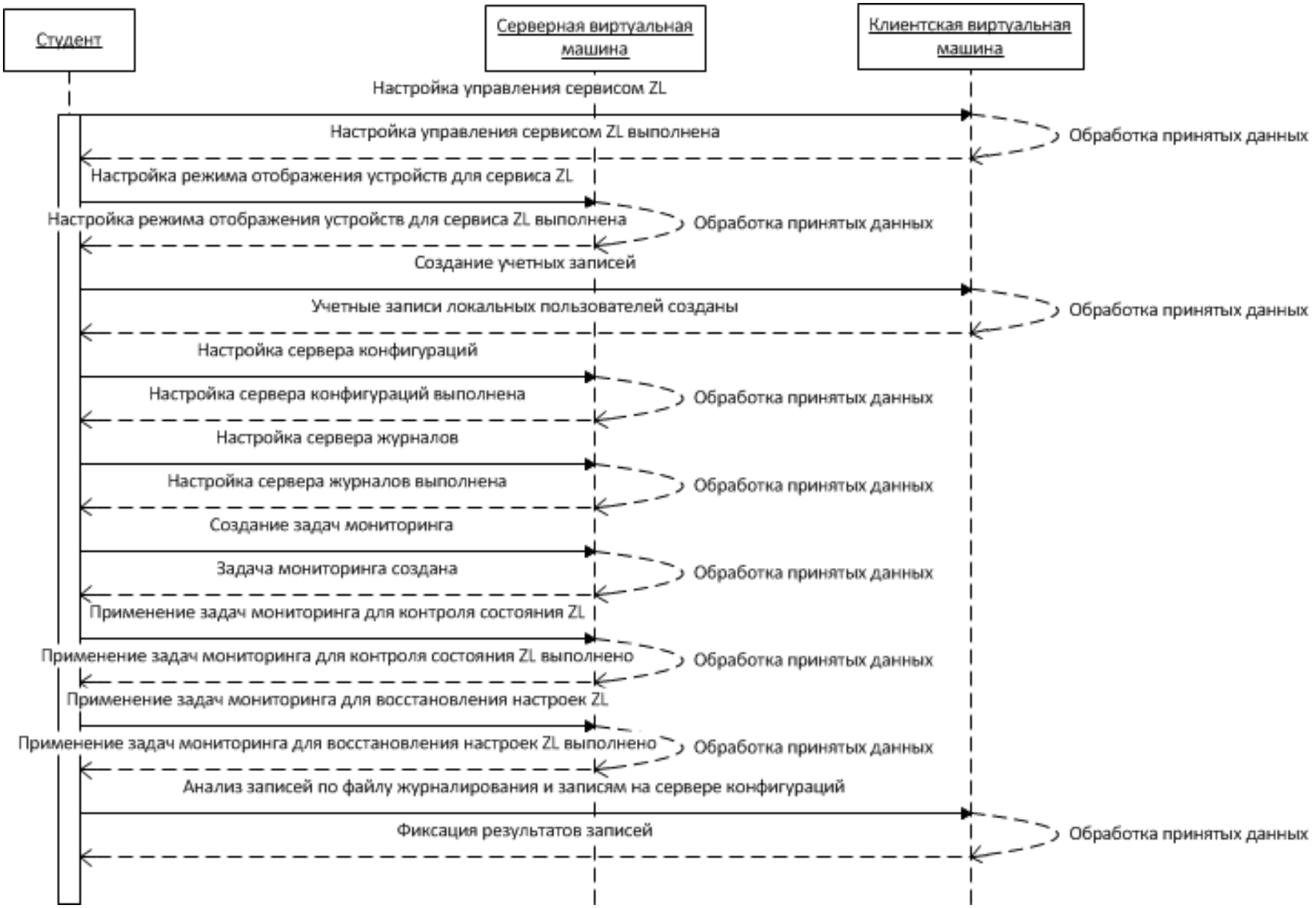
Студент
Серверная виртуальная машина
Клиентская виртуальная машина
Настройка управления сервисом ZL
Настройка управления сервисом ZL выполнена
Обработка принятых данных
Настройка режима отображения устройств для сервиса ZL
Настройка режима отображения устройств для сервиса ZL выполнена
Обработка принятых данных
Создание учетных записей
Учетные записи локальных пользователей созданы
Обработка принятых данных
Настройка сервера конфигураций
Настройка сервера конфигураций выполнена
Обработка принятых данных
Настройка сервера журналов
Настройка сервера журналов выполнена
Обработка принятых данных
Создание задач мониторинга
Задача мониторинга создана
Обработка принятых данных
Применение задач мониторинга для контроля состояния ZL
Применение задач мониторинга для контроля состояния ZL выполнено
Обработка принятых данных
Применение задач мониторинга для восстановления настроек ZL
Применение задач мониторинга для восстановления настроек ZL выполнено
Обработка принятых данных
Анализ записей по файлу журналирования и записям на сервере конфигураций
Фиксация результатов записей
Обработка принятых данных

Рисунок В.1

ПРИЛОЖЕНИЕ Г

(обязательное)

Структура отчета о выполнении заданий практикума

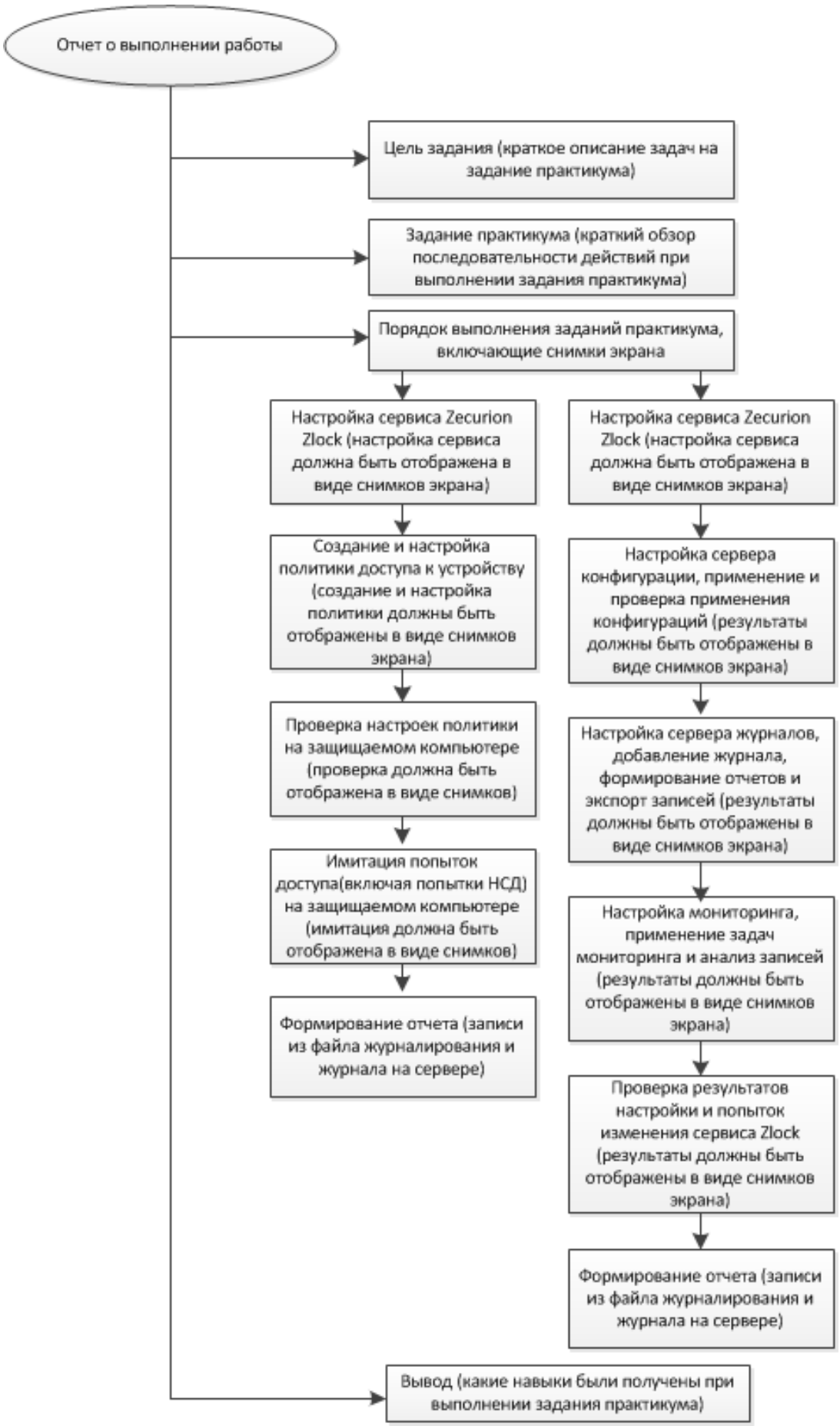
Отчет о выполнении работы
Цель задания (краткое описание задач на задание практикума)
Задание практикума (краткий обзор последовательности действий при выполнении задания практикума)
Порядок выполнения заданий практикума, включающие снимки экрана
Настройка сервиса Zecurion Zlock (настройка сервиса должна быть отображена в виде снимков экрана)
Создание и настройка политики доступа к устройству (создание и настройка политики должны быть отображены в виде снимков экрана)
Проверка настроек политики на защищаемом компьютере (проверка должна быть отображена в виде снимков)
Имитация попыток доступа(включая попытки НСД) на защищаемом компьютере (имитация должна быть отображена в виде снимков)
Формирование отчета (записи из файла журналирования и журнала на сервере)
Настройка сервиса Zecurion Zlock (настройка сервиса должна быть отображена в виде снимков экрана)
Настройка сервера конфигурации, применение и проверка применения конфигураций (результаты должны быть отображены в виде снимков экрана)
Настройка сервера журналов, добавление журнала, формирование отчетов и экспорт записей (результаты должны быть отображены в виде снимков экрана)
Настройка мониторинга, применение задач мониторинга и анализ записей (результаты должны быть отображены в виде снимков экрана)
Проверка результатов настройки и попыток изменения сервиса Zlock (результаты должны быть отображены в виде снимков экрана)
Формирование отчета (записи из файла журналирования и журнала на сервере)
Вывод (какие навыки были получены при выполнении задания практикума)

Рисунок Г.1

ПРИЛОЖЕНИЕ Д

(обязательное)

Контрольный экземпляр отчета по выполнению задания по применению программного комплекса Zecurion Zlock для выявления и предотвращения утечек информации

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

ОТЧЕТ

о выполнении лабораторной работы

«Применение программного комплекса Zecurion Zlock для выявления и предотвращения утечек информации»

Дисциплина:

Группа:

Выполнил: А.А. Забирова

Количество баллов:

Дата сдачи:

Принял: А.Г. Фатеев

Пенза, 2017

Цель практического задания – получить навыки по применению программного комплекса Zecurion Zlock для выявления и предотвращения утечек информации.

Задание включает:

– настройку аудита и теневого копирования для сервиса Zecurion Zlock;

– настройку управления сервисом Zecurion Zlock на защищаемых компьютерах;

– настройку управления сервером Zecurion Zlock;

– настройку режима отображения устройств для сервиса Zecurion Zlock;

– создание учетных записей локальных пользователей;

– настройку прав доступа к принтеру защищаемого компьютера;

– настройку доступа к принтеру и настройка аудита и теневого копирования для данного устройства;

– создание правил для пользователей;

– проверку настроек политики на защищаемом компьютере;

– анализ записей событий файла журналирования;

– формирование отчета по событиям файла журналирования;

– вывод по результатам практического задания.

Порядок выполнения задания

Показать в виде снимков экрана результаты проверки текущих настроек доступа на компьютере WinXP01-ZL после попыток изменения настроек локальным администратором.

Показать в виде снимков экрана результат настройки доступа к принтеру и аудита на компьютере WinXP01-ZL, установленные с помощью консоли Zecurion Zlock.

Показать в виде снимков экрана результаты применения файла настроек сервиса Zecurion ZLock на компьютере WinXP01-ZL.

Показать в виде снимков экрана результаты изменения настроек доступа пользователя User1 к принтеру на компьютере WinXP01-ZL.

Вывод:

ПРИЛОЖЕНИЕ Е

(обязательное)

Контрольный экземпляр отчета по выполнению задания по изучению функций мониторинга и защиты агентов, реализуемых программным комплексом Zecurion Zlock

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

ОТЧЕТ

о выполнении лабораторной работы

«Изучение функций мониторинга и защиты агентов, реализуемых программным комплексом Zecurion Zlock»

Дисциплина:

Группа:

Выполнил: А.А. Забирова

Количество баллов:

Дата сдачи:

Принял: А.Г. Фатеев

Пенза, 2017

Цель практического задания – получить навыки создания файлов конфигураций Zlock, а также настройки сервера конфигураций и применения его для распространения конфигураций Zlock на компьютеры домена и настройки мониторинга и защиты агентов.

Задание включает:

– создание учетных записей локальных пользователей;

– настройку отображения компьютеров домена в консоли управления;

– настройку параметров соединения с компьютерами домена;

– подготовку каталогов, необходимых для создания и применения конфигураций;

– настройку отображения компьютеров, управляемых серверов конфигураций;

– настройку сервера конфигураций;

– создание конфигураций на сервере конфигураций;

– применения конфигурации, созданной на сервере конфигураций, к компьютерам домена;

– проверку применения к компьютерам домена конфигурации, созданной на сервере конфигураций;

– контроль состояния компьютеров при удалении конфигурации;

– настройку сервера журналов;

– добавление журнала для просмотра записей, сохраненных на сервере журналов;

– формирование запросов для построения отчетов по записям, сохраненным на сервере журналов;

– экспорт записей, выбранных с использованием запросов в HTML-файл;

– просмотр событий для просмотра перехваченных снимков экрана;

– создание мониторинга для контроля состояния программного агента Zecurion ZLock;

– применение задач мониторинга для контроля состояния программного агента Zecurion ZLock и выявления изменения настроек;

– применение задач мониторинга для восстановления настроек программного агента Zecurion ZLock;

– анализ записей по файлу журналирования и записям на сервере конфигураций;

– вывод по результатам выполнения практического задания.

Порядок выполнения задания

Показать в виде снимков экрана результаты настройки журнала и проверки подключения к серверу журналов.

Показать в виде снимков экрана результаты настройки запроса для выбора записей о событиях, произошедших на компьютере WinXP02-ZL.

Показать в виде снимков экрана результаты настройки запроса для выбора записей, содержащих сведения о действиях доменного администратора по созданию конфигурации.

Показать в виде снимков экрана результаты настройки запросов для выбора записей, содержащих сведения о действиях локальных пользователей на компьютере WinXP02-ZL и создании снимков экрана при выполнении этих действий.

Показать в виде снимков экрана результаты просмотра сведений о событиях, возникших при применении конфигурации и создании снимков экрана, а также просмотра созданных снимков экрана.

Показать в виде снимков экрана результаты настройки задачи мониторинга агента Zecurion Zlock на компьютере.

Показать в виде снимков экрана результаты проверки статуса сервиса Zecurion Zlock и компьютера WinXP02-ZL после загрузки файла настроек.

Показать в виде снимков экрана результаты изменения разрешений на доступ к принтеру на компьютере WinXP02-ZL.

Показать в виде снимков экрана результаты изменения статуса компьютера WinXP01-ZL в консоли после изменения настроек и запуска задачи

мониторинга, а также после повторного запуска задачи мониторинга для восстановления настроек сервиса Zecurion Zlock на компьютере WinXP02-ZL.

Показать в виде снимков экрана результаты настройки доступа к принтеру в консоли на компьютере WinXP02-ZL.

Показать в виде снимков экрана результаты попыток останова сервиса Zecurion Zlock на компьютере WinXP02-ZL и удаления файла агента.

Вывод:

ПРИЛОЖЕНИЕ Ж

(обязательное)

Порядок проверки выполнения заданий практикума

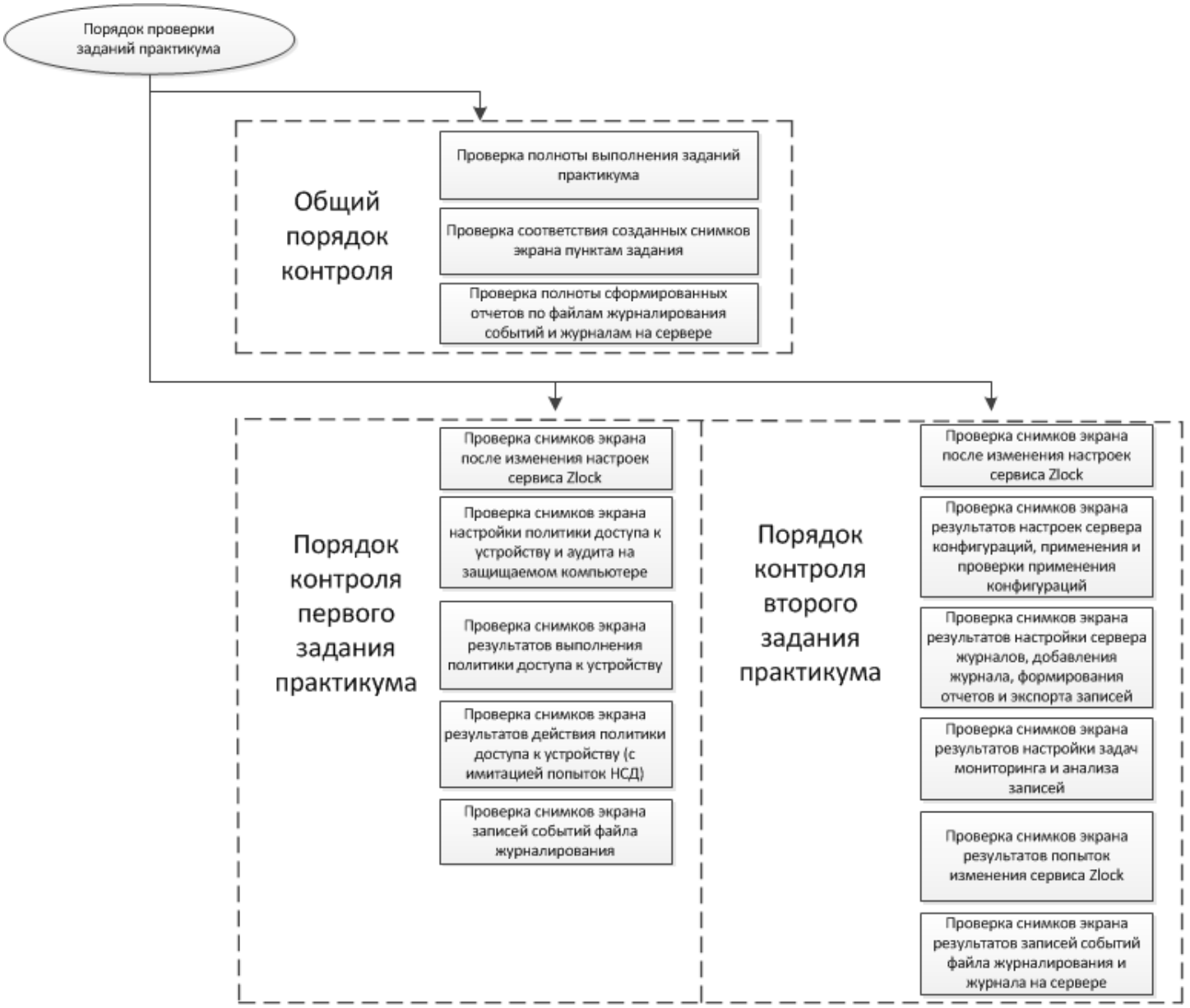
Порядок проверки заданий практикума
Общий порядок контроля
Проверка полноты выполнения заданий практикума
Проверка соответствия созданных снимков экрана пунктам задания
Проверка полноты сформированных отчетов по файлам журналирования событий и журналам на сервере
Порядок контроля первого задания практикума
Проверка снимков экрана после изменения настроек сервиса Zlock
Проверка снимков экрана настройки политики доступа к устройству и аудита на защищаемом компьютере
Проверка снимков экрана результатов выполнения политики доступа к устройству
Проверка снимков экрана результатов действия политики доступа к устройству (с имитацией попыток НСД)
Проверка снимков экрана записей событий файла журналирования
Порядок контроля второго задания практикума
Проверка снимков экрана после изменения настроек сервиса Zlock
Проверка снимков экрана результатов настроек сервера конфигураций, применения и проверки применения конфигураций
Проверка снимков экрана результатов настройки сервера журналов, добавления журнала, формирования отчетов и экспорта записей
Проверка снимков экрана результатов настройки задач мониторинга и анализа записей
Проверка снимков экрана результатов попыток изменения сервиса Zlock
Проверка снимков экрана результатов записей событий файла журналирования и журнала на сервере

Рисунок Ж.1

ПРИЛОЖЕНИЕ И

(обязательное)

Сценарии для автоматизированного развертывания ВМ

И.1 Сценарий для развертывания ВМ W2K3-Zl

```
@echo off
rem *****************************************************
rem Universal script for VMs
rem *****************************************************
set VHDTYPE="immutable"
set VHDPATH="c:\W2K3-ZL.vdi"

set VMNAME="W2K3-ZL"
set OS_TYPE="Windows2003"
REM set OS_TYPE="Windows"

set MEMORY="512"
set _ACPI="on"
set _IOAPIC="off"
set _PAE="on"
set _HWVIRTEX="on"
set _VTXVID="on"
set netadapter="PCnet-FAST ??? (Am79C973)"
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% storagectl %VMNAME% --add floppy --name "Floppy Controller"
%VBOXM% storageattach  %VMNAME% --storagectl PIIX4 --port 0 --device 0 --
type hdd --medium %VHDPATH% --mtype %VHDTYPE%
%VBOXM% storageattach %VMNAME% --storagectl "Floppy Controller" --port 0 -
-device 0 --type fdd
```

%VBOXM% modifyvm %VMNAME% --memory %MEMORY% --vram 16 --acpi %_ACPI% --ioapic %_IOAPIC% --pae %_PAE% --hwvirtex %_HWVIRTEX% --vtxvpid %_VTXVID% --audio none --floppy empty

%VBOXM% modifyvm %VMNAME% --nic1 intnet
if not %SHAREPATH%=="0" %VBOXM% sharedfolder add %VMNAME% --name share --hostpath %SHAREPATH%
@pause

И.2 Сценарий для развертывания ВМ WinXp01-ZL

```
@echo off
rem *****************************************************
rem Universal script for VMs
rem *****************************************************
set VHDTYPE="immutable"
set VHDPATH="c:\WinXP01-ZL.vdi"

set VMNAME="WinXP01-ZL"
set OS_TYPE="WindowsXP"
REM set OS_TYPE="Windows"

set MEMORY="192"
set _ACPI="on"
set _IOAPIC="off"
set _PAE="on"
set _HWVIRTEX="on"
set _VTXVID="on"
set netadapter="PCnet-FAST ??? (Am79C973)"
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% storagectl %VMNAME% --add floppy --name "Floppy Controller"
%VBOXM% storageattach  %VMNAME% --storagectl PIIX4 --port 0 --device 0 --
type hdd --medium %VHDPATH% --mtype %VHDTYPE%
%VBOXM% storageattach %VMNAME% --storagectl "Floppy Controller" --port 0 -
-device 0 --type fdd
```

%VBOXM% modifyvm %VMNAME% --memory %MEMORY% --vram 16 --acpi %_ACPI% --ioapic %_IOAPIC% --pae %_PAE% --hwvirtex %_HWVIRTEX% --vtxvpid %_VTXVID% --audio none --floppy empty

%VBOXM% modifyvm %VMNAME% --nic1 intnet
if not %SHAREPATH%=="0" %VBOXM% sharedfolder add %VMNAME% --name share --hostpath %SHAREPATH%
@pause

И.3 Сценарий для развертывания ВМ WinXp02-ZL

```
@echo off
rem *****************************************************
rem Universal script for VMs
rem *****************************************************
set VHDTYPE="immutable"
set VHDPATH="c:\WinXP02-ZL.vdi"

set VMNAME="WinXP02-ZL"
set OS_TYPE="WindowsXP"
REM set OS_TYPE="Windows"

set MEMORY="192"
set _ACPI="on"
set _IOAPIC="off"
set _PAE="on"
set _HWVIRTEX="on"
set _VTXVID="on"
set netadapter="PCnet-FAST ??? (Am79C973)"
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% storagectl %VMNAME% --add floppy --name "Floppy Controller"
%VBOXM% storageattach  %VMNAME% --storagectl PIIX4 --port 0 --device 0 --
type hdd --medium %VHDPATH% --mtype %VHDTYPE%
%VBOXM% storageattach %VMNAME% --storagectl "Floppy Controller" --port 0 -
-device 0 --type fdd
```

%VBOXM% modifyvm %VMNAME% --memory %MEMORY% --vram 16 --acpi %_ACPI% --ioapic %_IOAPIC% --pae %_PAE% --hwvirtex %_HWVIRTEX% --vtxvpid %_VTXVID% --audio none --floppy empty

%VBOXM% modifyvm %VMNAME% --nic1 intnet
if not %SHAREPATH%=="0" %VBOXM% sharedfolder add %VMNAME% --name share --hostpath %SHAREPATH%
@pause