

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

ДИПЛОМНЫЙ ПРОЕКТ

на тему

ЛАБОРАТОРНЫЙ ПРАКТИКУМ ПО ИЗУЧЕНИЮ ФУНКЦИЙ
МОНИТОРИНГА И ЗАЩИТЫ АГЕНТОВ, РЕАЛИЗУЕМЫХ СИСТЕМАМИ
КОНТРОЛЯ И УТЕЧКИ ИНФОРМАЦИИ

Студент Руд Каменьщикова Екатерина Владимировна

Руководитель Р Фатеев А.Г.

Нормоконтролёр Р Фатеев А.Г.

Рецензент инженер по ИТ 2 категории А.О. НПП „Рудин“ Евстигнеев С.А.

Работа допущена к защите (протокол заседания кафедры от 20.06.2016 № 14)

Заведующий кафедрой С.Л. Зефир С.Л. Зефир

Работа защищена с отметкой хорошо (протокол заседания ГЭК
от 24.06.16 № 12)

Секретарь ГЭК А.П. Иванов

Пенза 2016

Проверка ВКР-Тобалов

С.Л. Зефир

РЕФЕРАТ

Отчет о ВКР содержит 105 с., 57 рис., 7 источников, 4 прил.

СИСТЕМА КОНТРОЛЯ И ПРЕДОТВРАЩЕНИЯ УТЕЧКИ ИНФОРМАЦИИ, ПРОГРАММНЫЙ КОМПЛЕКС DEVICE LOCK, ПРОГРАММНЫЙ КОМПЛЕКС ZECURION LOCK, МОНИТОРИНГ СОСТОЯНИЯ АГЕНТОВ, ЗАЩИТА ПРОГРАММНЫХ АГЕНТОВ

Объектом исследований в данном дипломном проекте является лабораторный практикум по изучению функций мониторинга и защиты агентов, реализуемых системами контроля и утечки информации.

Цель ВКР – разработать лабораторный практикум по изучению функций мониторинга и защиты агентов, реализуемых системами контроля и утечки информации.

В процессе работы были подготовлены два лабораторных стенда, используемых при выполнении лабораторного практикума, произведено описание систем контроля и предотвращения утечек информации, используемых при проведении лабораторных работ, разработан порядок выполнения задания к лабораторным работам, входящих, в лабораторный практикум, разработаны контрольные экземпляры отчётов о выполнении лабораторных работ, входящих в лабораторный практикум, определена процедура контроля выполнения задания к лабораторным работам.

В результате выполнения ВКР подготовлено два лабораторных стенда, каждый из которых представляет собой виртуальную локальную сеть, включающую три виртуальных машины, с установленными на них системами контроля и предотвращения утечки информации, а так же подготовлено описание выполнения задания к лабораторный практикуму и разработан контрольный экземпляр отчета о выполнении практикума.

СОДЕРЖАНИЕ

Введение	7
1 Обзор систем контроля по защите информации, реализующих функции мониторинга и защиты агентов	9
1.1 Общая характеристика DLP систем	9
1.2 Каналы утечки информации	9
1.3 Типовые функциональные возможности	10
1.4 Анализ информации при контроле каналов передачи	13
1.5 Функционирование систем контроля и предотвращения утечек информации	14
1.6 Структура и компоненты систем контроля и предотвращения утечек информации	16
1.7 Функции мониторинга защиты агентов	16
1.8 Применение систем контроля и предотвращения утечек информации	17
2 Функции мониторинга и защиты агентов, реализуемые системами контроля и предотвращения утечек информации DeviceLock DLP Suite и Zecurion Zlock (Device Control)	19
2.1 Функции мониторинга и защиты агентов, реализуемые программным комплексом DeviceLock DLP Suite	19
2.1.1 Обзор архитектуры	19
2.1.2 Алгоритм мониторинга	23
2.1.3 Создание и редактирование задачи	24
2.1.4 Просмотрщик журнала мониторинга	32
2.1.5 Настройки журнала мониторинга	33
2.1.6 Фильтр журнала мониторинга	34
2.2 Функции мониторинга и защиты агентов, реализуемые программным комплексом Zecurion Zlock (Device Control)	36
2.2.1 Настройка мониторинга	36

2.2.2Просмотр текущего статуса компьютеров	39
2.2.3Экспорт данных, буфер обмена и просмотр конфигурации	40
3Описание подготовки лабораторных стендов, используемых при проведении лабораторных работ	41
3.1Создание виртуальных машин	41
3.2Создание виртуальных локальных сетей	46
3.2.1Настройка сетевого взаимодействия ВМ	46
3.2.2Настройка службы DNS	48
3.2.3Проверка подключения ВМ друг к другу с использованием утилиты ping	50
3.2.4Установка домена Active Directory	51
3.2.5Проверка правильности установки контроллера домена	53
3.3Установка Device Lock	54
3.4Установка Zecurion Lock	54
3.5Результат подготовки лабораторных стендов	56
4Порядок выполнения лабораторной работы по изучению мониторинга и защиты агентов, реализуемой в программном комплексе DeviceLock DLP Suite	58
4.1Цель и задание к лабораторной работе	58
4.2Порядок выполнения лабораторной работы	58
5Порядок выполнения лабораторной работы по изучению мониторинга и защиты агентов, реализуемой в программном комплексе Zecurion Zlock (Device Control)	77
5.1Цель и задание к лабораторной работе	77
5.2Порядок выполнения лабораторной работы	77
06 Описание порядка выполнения лабораторных работ, входящих в лабораторный практикум и результатов выполнения лабораторных работ	87
7Разработка контрольных экземпляров отчетов о выполнении	88

лабораторных работ, входящих в практикум	
8Определение порядка контроля выполнения задания к лабораторным работам	89
Заключение	91
Список использованных источников	92
Приложение А UML - диаграмма последовательности действий Device Lock	93
Приложение Б UML - диаграмма последовательности действий Zecurion Lock	95
Приложение В Структура и содержание отчета о выполнении практического задания	96
Приложение Г Структура и содержание отчета о выполнении практического задания	102

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

DLP - Data Loss Prevention;

DNS - Domain Name System;

VM - Virtual Machine;

ZL – Zecuron Lock;

БД – база данных;

ВМ – виртуальная машина;

ИТ – информационные технологии;

ИС – информационная система;

ИБ – информационная безопасность;

ОС – операционная система;

ПК – программный комплекс.

ВВЕДЕНИЕ

Для контроля и предотвращения несанкционированных попыток передачи данных за пределы локальной сети предназначены системы защиты от утечек конфиденциальной информации (Data Loss Prevention - DLP). Использование DLP систем наиболее актуально в том случае, когда СЗИ от НСД могут не обеспечивать необходимый уровень безопасности. Например, для контроля действий пользователей при обработке той информации, к которой у них есть доступ. В этом случае пользователи могут воспользоваться своими правами на доступ к информации и осуществить хищение информации посредством несанкционированного копирования на носители информации или передачи по сети.

Актуальность данной работы обусловлена тем, что использование систем контроля и предотвращения утечек информации возрастает, происходит накопление опыта применения. Одной из угроз, которая была выявлена при эксплуатации систем контроля, является несанкционированное воздействие на такой компонент системы контроля утечек, как программный агент, установленный на защищаемый компьютер, на котором работает пользователь. Воздействие на программный агент может заключаться в изменении настроек, режима работы, в отключении и удалении программного агента.

На основе накопленного опыта применения систем контроля утечек информации, был реализован механизм контроля состояния агентов и защиты от несанкционированного воздействия на них. Поэтому администраторы безопасности, применяющие системы контроля, должны обладать знаниями и практическими навыками по использованию такого механизма защиты агентов. Наиболее распространенным способом реализации механизма защиты агентов является механизм мониторинга состояния агентов, восстановления их настроек и защиты агентов от отключения и удаления.

При выполнении ВКР рассматривались две системы контроля и предотвращения утечек информации, реализующие функции мониторинга для защиты агентов от модификации и удаления, которые представлены в двух

лабораторных работах, входящих в состав разрабатываемого лабораторного практикума.

Каждая лабораторная работа применяется для изучения функций мониторинга и защиты агентов, реализуемых системами контроля и предотвращения утечек информации в автоматизированной системе DeviceLock DLP Suite и Zecurion Zlock (Device Control) и получения практических навыков по их настройке и применению.

При выполнении ВКР необходимо было провести обзор систем контроля и предотвращения утечек информации в автоматизированных системах и подготовить описание функций мониторинга и защиты агентов, реализуемые системами контроля и предотвращения утечек информации DeviceLock и Zlock. Выбор рассматриваемых систем обусловлен тем, что каждая имеет действующий сертификат ФСТЭК и по результатам различных обзоров являются одними из наиболее востребованных систем. Затем необходимо было подготовить лабораторные стенды, используемые при проведении лабораторного практикума, разработать задание к практикуму и порядок его выполнения, подготовить контрольные экземпляры отчётов о выполнении каждой лабораторной работы, входящей в лабораторный практикум, определить процедуру контроля выполнения задания к лабораторным работам.

1 Обзор систем контроля по защите информации, реализующих функции мониторинга и защиты агентов

1.1 Общая характеристика DLP систем

Технология DLP (Data Loss Prevention) – 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).[1]

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

1.2 Каналы утечки информации

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

- электронная почта (протоколы SMTP, POP3, IMAP, MAPI, NNTP, S/MIME);
- системы мгновенного обмена сообщений (протоколы OSCAR, MMP, MSN, XMPP, YMSG, HTTPIM, Microsoft Lync, Skype);

- протокол HTTP и его модификации (веб-почта, социальные сети, отправка SMS, контроль поисковых запросов, форумы, видеохостинги (загрузка файлов), фотохостинги (загрузка файлов), файлообменники (загрузка файлов));
- протоколы FTP и P2P;
- туннелирующие протоколы (IP-in-IP, L2TP, PPTP, PPPoE и другие);
- внешние устройства (USB, DVD/CD-ROM, COM, LPT, USB, IrDA, FireWire, модемы, Bluetooth, принтеры, сетевые принтеры, камеры, сканеры и т.д.). Поддерживаются определенные типы устройств. Может быть реализована возможность запретить или разрешить использование устройства, получить тень копию информации, при её передаче на устройство, блокировки копируемой на устройство информации. Могут быть реализованы ограничения доступа в зависимости от типа съемного носителя (производитель, серия, модель, экземпляр). В системах может быть реализована возможность разрешать копирование только на доверенные носители, шифрование файлов на USB-устройствах, контроль беспроводной передачи данных (разрешение, запрет), контроль сетевых подключений (домены, сегменты сети), контроль буфера обмена, контроль запуска процессов;
- мобильные устройства;
- прочие протоколы. К ним относятся дополнительные возможности по контролю и выявлению утечек информации. Например, мониторинг активности на файл-серверах и в общих сетевых папках, контроль файлов, передаваемых отдельными приложениями (iTunes, Dropbox, Яндекс.Диск, uTorrent, GoogleDrive, Evernote), контроль IP-телефонии и др.

1.3 Типовые функциональные возможности

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).

1.4 Анализ информации при контроле каналов передачи

Лингвистический анализ.

Основан на поиске стоп-слов («секретно», «конфиденциально» и т.п.) для выявления сообщений в информационном потоке. Стоп-слова хранятся в специальных словарях. Словари содержат слова, относящиеся к определенной категории или сфере деятельности. Кроме того проводится морфологический анализ, основанный на поиске словоформ, которые могут образовываться от стоп-слов. Анализу подвергается как содержание документа, так и его реквизиты (грифы документы и др.).

Лингвистический анализ использует контекстный анализ (то есть в каком контексте, в сочетании с какими другими словами используется конкретный термин) и семантический анализ текста. Эти технологии работают тем эффективнее, чем больше анализируемый фрагмент.

Использование лингвистических технологий требует обучения систем контроля и предотвращения утечек информации. Например, пополнение словарей стоп-слов, базы категорий слов или корректировка правил для снижения количества ложных срабатываний.

Основным недостатком лингвистических технологий является зависимость от языка, на котором представляется анализируемая информация. Невозможно использовать лингвистический модуль, разработанный для одного языка, в целях анализа другого. Еще одной сложностью при использовании лингвистических технологий для контроля всего спектра конфиденциальной информации является то, что не вся конфиденциальная информация находится в виде текстов. Конфиденциальная информация может быть представлена в виде графических объектов, аудио- и видеофайлов, исходные тексты программ

и т.п. Для лингвистического анализа требуется предварительное преобразование таких файлов.

Статистические методы.

Для обнаружения структурированных данных, которые формируются по определенным правилам, используются регулярные выражения. К таким данным относят например, номера паспортов или кредитных карт.

Также для поиска документов в информационном потоке используют цифровые отпечатки – контрольные значения фиксированной длины, вычисляемые для файлов (документов) по определенным алгоритмам.

Поиск нетипичных сочетаний символов, характерных для случаев простой манипуляции с текстом. Поиск осуществляется при помощи определения шаблонов подмен. Обычно отслеживаются нетипичные для естественного языка пары символов, относящиеся к разным алфавитам.

Статистические методы не зависят от языка текста и нетекстовой информации. Они подходят для защиты статических (мало и редко изменяемых) цифровых объектов любого типа – картинок, аудио/видео, баз данных. Также не требуется категоризация документов.[5]

1.5 Функционирование систем контроля и предотвращения утечек информации

Система контроля и предотвращения утечек информации, как правило, является распределённым программным или программно-аппаратным комплексом, состоящим из нескольких модулей различного назначения. Часть модулей функционирует на выделенных серверах и других компонентах, часть – на рабочих станциях пользователей, часть – на рабочих местах администраторов безопасности.

Выделенные сервера могут потребоваться для таких модулей как база данных и, иногда, для модулей анализа информации. Эти модули, по сути, являются ядром системы контроля и предотвращения утечек информации.

База данных необходима для хранения информации, начиная от правил контроля и подробной информации об инцидентах и заканчивая всеми

документами, попавшими в поле зрения системы за определённый период. В некоторых случаях, система даже может хранить копию всего сетевого трафика компании, перехваченного в течение заданного периода времени. В состав системы контроля и предотвращения утечек информации входит также консоль централизованного управления.

Модули анализа информации отвечают за анализ текстов, извлечённых другими модулями из различных источников: сетевой трафик, документы на любых устройствах хранения информации в пределах компании. В некоторых системах есть возможность извлечения текста из изображений и распознавание перехваченных голосовых сообщений. Все анализируемые тексты сопоставляются с заранее заданными правилами и отмечаются соответствующим образом при обнаружении совпадения.

Для контроля действий сотрудников на их рабочие станции могут быть установлены специальные агенты. Такой агент должен быть защищён от вмешательства пользователя в свою работу (реализовано не во всех системах и обычно требует использования дополнительных средств) и может вести как пассивное наблюдение за его действиями, так и активно препятствовать тем из них, которые пользователю запрещены политикой безопасности компании. Перечень контролируемых действий может ограничиваться входом/выходом пользователя из системы и подключением USB-устройств, а может включать перехват и блокировку сетевых протоколов, теневое копирование документов на любые внешние носители, печать документов на локальные и сетевые принтеры, передачу информации по Wi-Fi и Bluetooth и много другое. Некоторые системы контроля и предотвращения утечек информации способны записывать все нажатия на клавиатуре (keylogging) и сохранять копии экрана.

Обычно, в составе системы контроля и предотвращения утечек информации присутствует модуль управления, предназначенный для мониторинга работы системы и её администрирования. Этот модуль позволяет следить за работоспособностью всех других модулей системы и производить их настройку.

Для удобства анализа и обработки накопленной информации в системы контроля и предотвращения утечек информации может быть реализован отдельный модуль, позволяющий настраивать политику безопасности, отслеживать её нарушения, проводить их детальное расследование и формировать необходимую отчётность. Возможности анализа инцидентов, проведения полноценного расследования и отчетность обычно рассматриваются как ключевая функциональная возможность, которая учитывается при выборе системы.

1.6 Структура и компоненты систем контроля и предотвращения утечек информации

Состав системы контроля и предотвращения утечек информации рассматривается также с точки зрения расположения компонент. Выделяют компоненты (модули) сетевого уровня и компоненты, устанавливаемые на контролируемых узлах сети.

Сетевые компоненты контролируют трафик, пересекающий границы защищенной информационной системы. Обычно они устанавливаются на прокси-серверах, серверах электронной почты, а также в виде отдельных серверов.

Компоненты, устанавливаемые на контролируемых узлах сети, стоят обычно на персональных компьютерах пользователей и контролируют такие каналы, как запись информации на компакт-диски, флэш-накопители и т.п. Эти компоненты также могут отслеживать изменение сетевых настроек, установку программ для туннелирования, стеганографии и другие возможные методы для обхода контроля.

В состав системы контроля и предотвращения утечек информации входит также консоль централизованного управления.

1.7 Функции мониторинга защиты агентов

Мониторинг – функция DLP-систем, позволяющая контролировать текущее состояние агентов на удаленных компьютерах путем периодического опроса.

Функции мониторинга защиты агентов предусматривают:

- контроль работы, целостности, политик агентов;
- защита агента от выключения и удаления;
- маскировка агента в системе;
- возможность в режиме online контролировать клиентские компьютеры;
- возможность настройки реагирования на события.

1.8 Применение систем контроля и предотвращения утечек информации

Использование DLP системы наиболее актуально для организаций, где риск утечки конфиденциальной информации повлечет серьезный финансовый или репутационный ущерб, 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.

На данный момент существует множество систем контроля и предотвращения утечек информации, применяемых для контроля утечек информации, имеющие сертификат ФСТЭК:

- Securion;
- InfoWatch Traffic Monitor Enterprise Edition;
- Symantec;
- SearchInform;
- DeviceLock Endpoint DLP Suite 7.1;

— FalconGaze.[2]

Исходя из данного перечня, для выполнения лабораторного практикума были выбраны продукты DeviceLock и Zlock.

2 Функции мониторинга и защиты агентов, реализуемые системами контроля и предотвращения утечек информации DeviceLock DLP Suite и Zecurion Zlock (Device Control)

2.1 Функции мониторинга и защиты агентов, реализуемые программным комплексом DeviceLock DLP Suite

2.1.1 Обзор архитектуры

Централизованный мониторинг – функция DeviceLock Enterprise Server'a, позволяющая контролировать текущее состояние агентов на удаленных DeviceLock Management Console компьютерах путем периодического опроса. Результат мониторинга отображается в консоли управления в режиме реального времени, а также сохраняется в специальном журнале и позже может быть проанализирован при помощи встроенного просмотрщика журнала мониторинга.

Кроме того, DeviceLock Enterprise Server периодически сравнивает текущие политики безопасности (настройки) агентов на указанных администратором компьютерах с эталонными политиками, и фиксирует информацию о выявленных отклонениях. При этом возможно автоматическое восстановление измененных политик безопасности.

Все действия (опрос компьютеров и DeviceLock Service'ов, проверка целостности политики и т.п.) в мониторинге выполняются задачами.

На одном DeviceLock Enterprise Server'е можно создать любое количество задач. Максимальное количество задач на сервере ограничено только количеством свободной памяти, скоростью процессора и пропускной способностью сети. Необходимо иметь в виду, что сервер должен иметь достаточно ресурсов, чтобы одновременно подключаться как минимум к 10 удаленным компьютерам.

По умолчанию DeviceLock Enterprise Server может выполнять одновременно до 30 задач. Это означает, что при необходимости выполнения, например, 40 задач, и все они запускаются в одно и то же время, то сначала

будут запущены первые 30 задач, а затем, по мере их окончания, по одной будут запускаться оставшиеся 10 задач.

Тем не менее, можно изменить максимальное количество одновременно запускаемых задач. Чтобы поменять это значение, применяется редактор реестра Regedit и вносятся следующие изменения в реестр компьютера, на котором запущен DeviceLock Enterprise Server:

- ключ: HKEY_LOCAL_MACHINE\SOFTWARE\SmartLineVision\DeviceLockEnterpriseServer;
- имя: ConcurrentJobs;
- тип: DWORD;
- значение: <количество_потоков>, где <количество_потоков> должно содержать число от 1 до 1000.

Во время своего выполнения задачи пишут полезную информацию в журнал мониторинга. Эта информация включает в себя текущие состояния компьютеров и DeviceLock Service'ов, а также возможные ошибки, которые возникают в процессе сканирования компьютеров и подключения к DeviceLock Service'ам.

Также задачи отображают списки компьютеров и их текущие состояния в консоли управления. Это позволяет анализировать ситуацию в режиме реального времени.

Чтобы просмотреть список компьютеров для определенной задачи, необходимо выделить эту задачу в дереве консоли в соответствии с рисунком 1.

Чтобы обновить информацию в списке компьютеров, используется Refresh из контекстного меню или соответствующая кнопка на инструментальной панели.

- Computer Name – имя компьютера;
- Status – текущее состояние (статус) компьютера и DeviceLock Service'a.



Рисунок 1 – Просмотр списка компьютеров для определённой задачи

Статус также влияет на картинку (иконку) отображаемую слева от параметра Computer Name. Общее правило для отображения иконки компьютера такое:

- зеленый компьютер – означает, что компьютер и DeviceLock Service работают;
- красный компьютер – означает, что компьютер не работает (либо не найден) или работает, но DeviceLock Service не запущен;
- компьютер с восклицательным знаком – означает, что обнаружены проблемы либо с компьютером, либо с DeviceLock Service'ом.

Выделяется семь различных состояний (статусов):

- Computer is available – этот статус означает, что компьютер работает и DeviceLock Service на нем запущен. Также, если эта задача проверяет целостность политики, то данная проверка прошла без ошибок. Иконка компьютера будет – «зеленый компьютер». Если эта задача восстанавливает измененную политику, иконка компьютера будет - “зеленый компьютер с восклицательным знаком”;
- Computer is unavailable – этот статус означает, что DeviceLock Enterprise Server не может просканировать компьютер. Это DeviceLock Management Console происходит, когда компьютер выключен или соединения

блокируются файрволом, но при этом имя компьютера или его IP-адрес могут быть получены через DNS. Иконка компьютера будет – «красный компьютер»;

— Service is unavailable – этот статус означает, что DeviceLock Enterprise Server не может подсоединиться к DeviceLock Service’у. Это происходит, когда компьютер работает, но DeviceLock Service не запущен на нем. Также это может происходить из-за того, что DeviceLock Service запущен не на том TCP-порту, который указан в настройках задачи, или соединения блокируются файрволом. Иконка компьютера будет – «красный компьютер с восклицательным знаком». За дополнительной информацией относительно проблем соединения, можно обратиться к описанию параметра Service connection settings;

— Settings are corrupted – этот статус означает, что компьютер работает и DeviceLock Service на нем запущен, но процедура проверки целостности политики вернула ошибку. Это происходит, когда эталонная политика, присвоенная данной задаче, отличается от политики, установленной на DeviceLock Service. Иконка компьютера будет – «зеленый компьютер с восклицательным знаком»;

— Unresolved computer address– этот статус означает, что DeviceLock Enterprise Server не может получить имя/адрес компьютера. Это происходит, когда задано имя компьютера не существующее в DNS. Также это может происходить из-за того, что компьютер в данный момент не включен, а в сети нет DNS-сервера. В таком случае статус Unresolved computer address должен трактоваться как Computer is unavailable. Иконка компьютера будет – «красный компьютер с восклицательным знаком»;

— Unsupported service version– этот статус означает, что DeviceLock Enterprise Server пытается получить политику (настройки) из DeviceLock Service’а версии 6.2 и ниже. Проверка целостности политик поддерживается только для версий 6.2.1 и выше. Иконка компьютера будет – «зеленый компьютер с восклицательным знаком»;

— Access is denied— этот статус означает, что DeviceLock Enterprise Server не может подсоединиться к DeviceLock Service'у из-за недостатка привилегий. Это происходит, когда учетная запись, под которой запущена служба DeviceLock Enterprise Server'а, не имеет прав доступа для подключения к DeviceLock Service'у. Иконка компьютера будет – «зеленый компьютер с восклицательным знаком». Дополнительная информация относительно проблем соединения находится в описании параметров Service connection settings.

Также, все те же самые статусы (за исключением Computer is available) записываются в журнал мониторинга и могут быть проанализированы позже.

- Last Scan Time – дата и время последней попытки сканирования;
- Service Uptime – время работы DeviceLock Service'а;
- DeviceLock Management Console;
- Computer Uptime – время работы компьютера;
- Service Version – версия DeviceLock Service'а. Последние пять цифр определяют номер сборки.

2.1.2 Алгоритм мониторинга

Алгоритм, используемый в мониторинге, прост, но эффективен:

— прежде всего DeviceLock Enterprise Server пытается просканировать компьютер и определить, работает он или нет. Если сканирование удалось, то компьютер получает статус «доступен» и мониторинг компьютера продолжается. В противном случае компьютер получает статус «недоступен» и мониторинг компьютера прекращается (происходит запись в журнал);

— затем DeviceLock Enterprise Server пытается подключиться к DeviceLock Service'у. Если подключение удалось, то DeviceLock Service получает статус «доступен» и мониторинг компьютера продолжается. В противном случае DeviceLock Service получает статус «недоступен» и мониторинг компьютера прекращается (происходит запись в журнал);

— если данная задача должна проверять целостность политики, то мониторинг компьютера продолжается. В противном случае мониторинг компьютера прекращается (в журнал ничего не пишется);

— DeviceLock Enterprise Server получает политику из DeviceLock Service'a и сравнивает ее с эталонной политикой, присвоенной данной задаче. Если расхождений в политиках не обнаружено, то мониторинг компьютера прекращается (в журнал ничего не пишется). Если обнаружены различия в двух политиках, то мониторинг компьютера продолжается (происходит запись в журнал);

— если данная задача должна восстанавливать измененную политику, то DeviceLock Enterprise Server заменяет политику на DeviceLock Service на эталонную и мониторинг компьютера прекращается (происходит запись в журнал). В противном случае мониторинг компьютера просто прекращается (в журнал ничего не пишется). Если на каком либо из шагов, описанных выше, происходит ошибка, то в журнал записывается сообщение об этой ошибке. Если ошибка не критичная, то мониторинг компьютера продолжится. Если же ошибка критичная, то мониторинг компьютера прекратится.

Также, некоторые очень критичные ошибки (такие как нехватка памяти) могут вызвать остановку исполнения всей задачи.

2.1.3 Создание и редактирование задачи

Каждая задача содержит свой собственный список компьютеров и набор настроек.

Чтобы создать новую задачу, нужно открыть Создать задачу из контекстного меню, доступного для пункта Мониторинг, согласно рисунку 2.

Чтобы отредактировать существующую задачу, используется Редактировать задачу из контекстного меню.

Для того, что бы навсегда удалить задачу, ее выделяют в дереве консоли и удаляют с помощью Удалить задачу из контекстного меню.

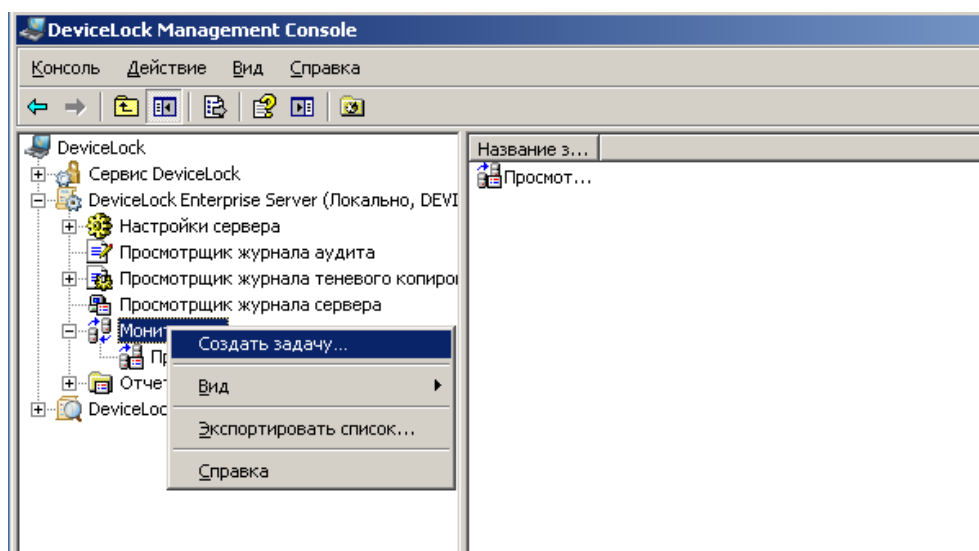


Рисунок 2 – Создание новой задачи

При нажатии на кнопку Редактирование, конфигурируется список, выбранный в Компьютер.

Поддерживаются два типа списков компьютеров.

Первый тип это - Staticlist – все компьютеры задаются в списке по именам и/или IP- адресам, как показано на рисунке 3. Поскольку этот список статический, то даже если какой-либо компьютер больше не существует в сети, он будет контролироваться задачей, пока запись о нем не будет вручную удалена из этого списка.

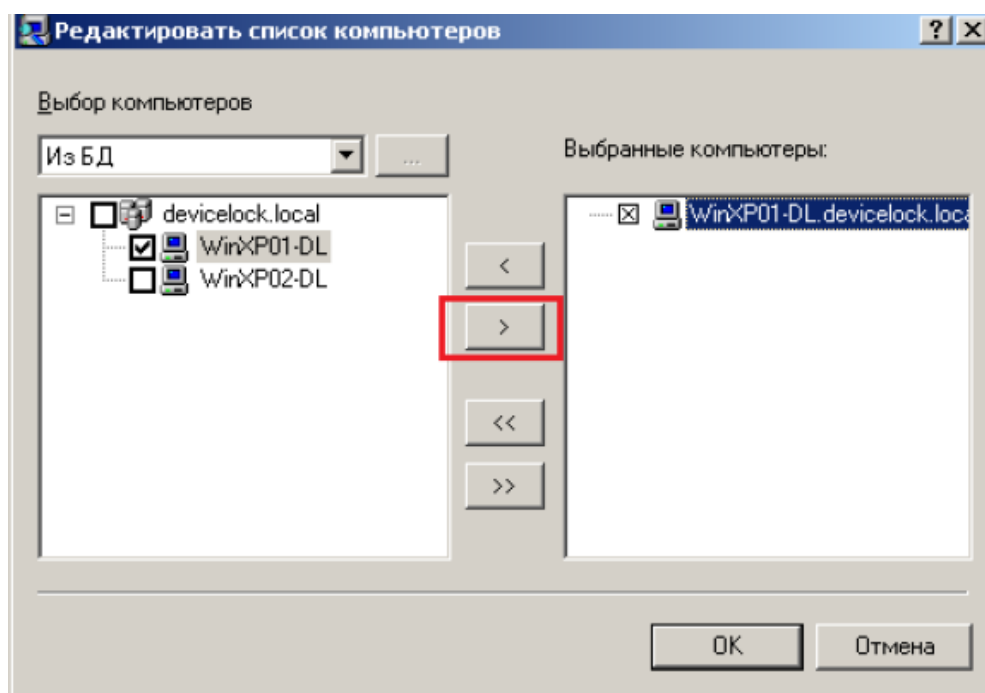


Рисунок 3 – Список компьютеров

Контролируемые компьютеры задаются в правом списке. Необходимые компьютеры выбираются в левом списке и затем перемещаются в правый список путем нажатия на кнопку >. Если необходимо исключить некоторые компьютеры из процесса мониторинга, то они выделяются в правом списке и нажимается кнопка <.Используя кнопки >>и <<, за один раз можно добавлять и удалять все доступные компьютеры (не нужно по отдельности выделять компьютеры в списках).

Есть несколько вариантов выбора компьютеров в левом списке:

- компьютеры – просмотр дерева сети и выбор компьютеров;
- из файла – загрузка заранее подготовленного списка компьютеров из внешнего текстового файла, а затем выбор компьютеры. Чтобы открыть внешний файл, используется кнопка Текстовый файл может содержать имена компьютеров и/или IP-адреса, каждый из которых должен быть записан на отдельной строке, и может быть как в Юникод, так и в не Юникод кодировке;
- ручной ввод – вручную вводятся и выбираются компьютеры. Имена компьютеров и/или IP-адреса должны быть на отдельных строках.

Помимо статического списка существует динамический - Dynamiclist – вместо имен компьютеров или IP-адресов, динамический список содержит путь к контейнеру (например, подразделение) в дереве службы каталогов (такой как Active Directory, Novell eDirectory, OpenLDAP и т.п.). Каждый раз в момент выполнения задачи DeviceLock Enterprise Server получает все компьютеры, которые в настоящий момент времени существуют в контейнере. Таким образом, если некоторый компьютер был удален из службы каталогов или был перемещен в другой контейнер, то он не будет более контролироваться задачей. И наоборот, если появился новый компьютер, который не существовал в контейнере на момент создания/редактирования задачи, а был добавлен туда позже, то этот новый компьютер будет контролироваться в момент выполнения задачи.

Если DeviceLock Enterprise Server работает на Windows NT4, то для использования динамического списка должен быть установлен компонент «Расширение Active Directory для Windows NT 4.0»

Путь к контейнеру, из которого DeviceLock Enterprise Server будет получать все компьютеры в момент выполнения задачи, должен быть указан в поле Путь. Необходимо использовать строку в LDAP-формате. Просмотр дерева службы каталогов и выбор контейнера осуществляется путем нажатия на кнопку Выберите. В этом случае путь к этому контейнеру будет подставлен в поле Путь автоматически.

Есть два режима работы со службой каталогов:

— Active Directory – просмотр дерева Active Directory и выбор нужного контейнера;

Несмотря на то, что дерево Active Directory может отображаться и в режиме LDAP, рекомендуется использовать этот специальный режим Active Directory, т.к. в этом случае DeviceLock Enterprise Server работает со службой каталогов более эффективно и потребляет меньше ресурсов.

Если для доступа к Active Directory требуется задать данные (пользователь и пароль) альтернативной учетной записи, то необходимо нажать на кнопку ... и указать в открывшемся диалоге Credentials необходимое имя пользователя и соответствующий ему пароль.

Если альтернативная учетная запись не задана, то для доступа к Active Directory используется учетная запись, от имени которой запущена служба DeviceLock Enterprise Server'a.

Чтобы разрешить DeviceLock Enterprise Server'у использовать внутренний механизм синхронизации, предоставляемый Active Directory, нужно установить флажок Синхронизация. Использование данного механизма позволяет значительно снизить нагрузку на контроллер домена и быстрее получать компьютеры в момент выполнения задачи.

Чтобы использовать механизм синхронизации, требуется доступ к ActiveDirectory с правами администратора;

— LDAP – просмотр LDAP-дерева (LightweightDirectory AccessProtocol) и выбор нужного контейнера.

Чтобы настроить подключение к LDAP-серверу, необходимо нажать на кнопку ... и открыть диалог LDAP Настройки, как показано на рисунке 4.



Рисунок 4 - Настройка подключения к LDAP-серверу

Хост – имя или IP-адрес LDAP-сервера, к которому выполняется подключение.

Порт – номер порта, по котором LDAP-сервер принимает подключения. По умолчанию это порт 389.

Начало DN – начальная точка для просмотра дерева каталога. Использовать строка в LDAP-формате (например, cn=qa,o=SMARTLINE,c=US). Поле Base DN остаётся пустым для просмотра с корня дерева. При нажатии на кнопку Fetch можно получить все доступные контексты.

Пользователь DN – имя пользователя, под которым выполняется подключение к каталогу. Используется строка в LDAP- формате (например, cn=admin,o=SMARTLINE,c=US).

Если имя пользователя не задано, то для доступа к LDAP-серверу используется учетная запись, от имени которой запущена служба DeviceLock EnterpriseServer'a.

Пароль – пароль пользователя.

Методы обнаружения сетевых ресурсов – различные методы сетевого сканирования используемые для определения статусов (доступен или недоступен) проверяемых компьютеров.

В момент выполнения задачи DeviceLock Enterprise Server использует все выбранные методы сканирования в перечисленном порядке, пока один из них не вернет статус доступен для компьютера. Если ни один из методов не вернул статус доступен, то данный компьютер получает статус недоступен.

Поддерживается три метода сетевого сканирования:

- Ping sweep – DeviceLock Enterprise Server посылает обычный ICMP-пакет (“пинг”) к компьютеру и ждет от него ответа;

- Net BIOS queries– если компонент «Клиент для сетей Microsoft» установлен на компьютере, то этот компьютер ответит на Net BIOS-запрос, посланный DeviceLock Enterprise Server’ом;

- TCP discovery (ports) – DeviceLock Enterprise Server проверяет перечисленные TCP-порты на компьютере и ищет первый открытый порт.

Используя запятую (,) или точку с запятой (;) в качестве разделителя, указывается несколько портов одновременно.

Если на компьютере используется какой-либо фаервол, то он может блокировать отсылку некоторых или всех сетевых пакетов. В таком случае данный компьютер получит статус недоступен, даже если он на самом деле включен и работает.

Чтобы задать дополнительные параметры сканирования, нажимается кнопка Расширенные настройки и открывается диалог Настройка методов сетевого сканирования, как показано на рисунке 5.

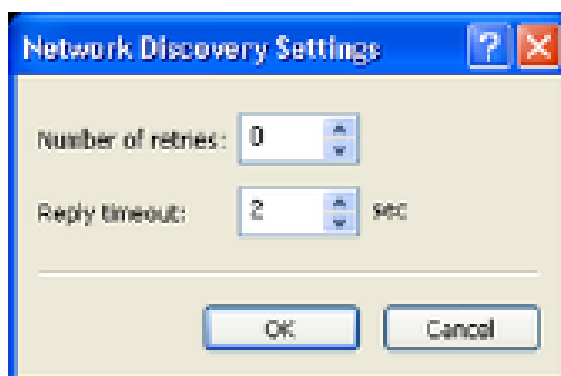


Рисунок 5 – Задание дополнительных параметров сканирования

Число повторных попыток – определяет, какое количество раз DeviceLock EnterpriseServer будет повторно выполнять каждый метод сканирования, когда он возвращает статус недоступен. 0 – означает, что повторных попыток сканирования этим же методом предприниматься не будет (для данного компьютера в данный момент выполнения задачи).

Время ожидания – время в секундах, в течении которого DeviceLock EnterpriseServer ожидает ответ от компьютера для каждого метода сканирования. Если DeviceLock EnterpriseServer работает в медленной или в загруженной сети, то вам, возможно, будет нужно увеличить это значение.

DeviceLock Service может быть настроен на использование либо фиксированного порта, либо динамических портов.

Есть два способа подключения:

- Dynamic ports – для использования DeviceLock Enterprise Server’ом динамических портов при подключении к DeviceLock Service’ам используется данная опция;

- Fixed TCP port– если DeviceLock Service’ы настроены на использование фиксированного TCP-порта, то выбирается эта опцию и указывается номер порта.

Чтобы успешно подключаться к контролируемым сервисам и получать необходимую информацию от них, DeviceLock Enterprise Server должен обладать как минимум правом доступа только на чтение (Read-only) к этим сервисам. Если данная задача также должна перезаписывать настройки

(политики) на контролируемых сервисах, то DeviceLock Enterprise Server должен обладать правом полного доступа (Fullaccess) к этим сервисам.

Для подключения к контролируемым DeviceLock Service'ам используется учетная запись, от имени которой запущена служба DeviceLock Enterprise Server'а. Если секретный ключ установлен, то DeviceLock Enterprise Server может использовать авторизацию по сертификату.

Проверка настроек службы - этот флажок устанавливается, в случае если необходимо проверять целостность политик DeviceLock Service'ов на контролируемых компьютерах.

Файл настройки службы – чтобы назначить задаче эталонную политику, нужно загрузить настройки сервиса из внешнего XML-файла (файл эталонной политики). Этот файл эталонной политики может быть создан в DeviceLock Service Settings Editor'е, DeviceLock Management Console или в DeviceLock Group Policy Manager'е.

В процессе проверки целостности DeviceLock Enterprise Server получает политики из контролируемых DeviceLock Service'ов и сравнивает их с эталонной политикой, присвоенной данной задаче.

Все неопределенные параметры (те, у которых состояние «не определен») в эталонной политике игнорируются в процессе проверки целостности. Эта особенность используется для контроля целостности только отдельных настроек (самых важных) и при этом позволяет изменять остальные параметры без записи уведомления в журнал мониторинга.

Чтобы загрузить файл эталонной политики, используется кнопка Поскольку на данном шаге цифровая подпись не проверяется, этот файл может быть как подписанным, так и неподписанным. Тем не менее, при загрузке подписанного файла, его имя будет отображаться в поле Service Settings file в круглых скобках.

Если редактируется задача и эталонная политика уже назначена ей, можно экспортировать эту политику во внешний XML-файл, путем нажатия на кнопку Сохранить.

Восстановление параметров службы – этот флажок ставится, если необходимо позволить DeviceLock Enterprise Server’у восстанавливать измененную политику на эталонную у контролируемых DeviceLock Service’ов для которых в процессе проверки целостности было выявлено расхождение политик. Используя эту функцию, осуществляется не только пассивный мониторинг целостности отдельных настроек, но и восстанавливаются оригинальные значения настроек в случае их изменения.

Интервал сканирования – время в секундах, которое должно пройти после окончания выполнения задачи и перед началом выполнения этой же задачи снова.

Максимальное количество потоков – это параметр, показывающий количество потоков, которое может быть задействовано данной задачей в процессе своего выполнения. Увеличение этого значения необходимо, чтобы распараллелить процесс сканирования компьютеров. Тем не менее, большее число потоков требует большего количества ресурсов (особенно памяти и сетевого трафика) для DeviceLock Enterprise Server’a.

2.1.4Просмотрщик журнала мониторинга

Этот встроенный просмотрщик позволяет получить список записей из журнала мониторинга. Журнал мониторинга, показанный на рисунке 6, используется задачами для записи информации о контролируемых ими компьютерах и DeviceLock Service’ах.

Столбцы просмотрщика определены следующим образом:

- тип – тип события: успех, информация, предупреждение, ошибка;
- дата/время– дата и время, когда событие произошло;
- событие– номер, идентифицирующий событие;
- название задачи – название задачи, ответственной за это событие.

Может быть пустым, если событие не связано с задачей;

- имя компьютера – имя компьютера, принадлежащего задаче, которая ответственна за это событие. Может быть пустым, если событие не связано с компьютером;

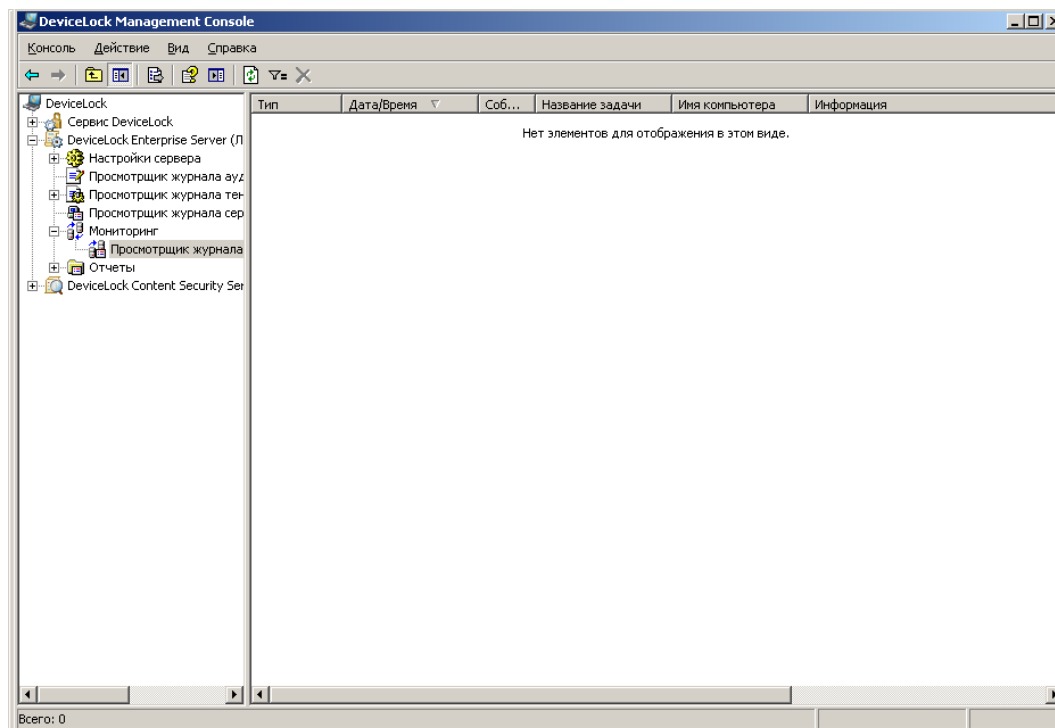


Рисунок 6 – Журнал мониторинга

- информация – иная, специфичная для данного события информация, такая как описание ошибки, предупреждение и т.п.;
- сервер – имя сервера, где событие произошло;
- запись N – номер записи.

Чтобы обновить список, используется Обновить из контекстного меню или соответствующая кнопка на инструментальной панели.

Чтобы полностью очистить этот журнал, используется Очистить из контекстного меню или соответствующая кнопка на инструментальной панели.

2.1.5 Настройки журнала мониторинга

Чтобы определить максимальный размер журнала мониторинга и действия DeviceLock Enterprise Server'а в случае его заполнения, используется Настройки из контекстного меню, доступного по нажатию правой кнопки мыши на элементе Просмотрщик журнала мониторинга, как показано на рисунке 7.

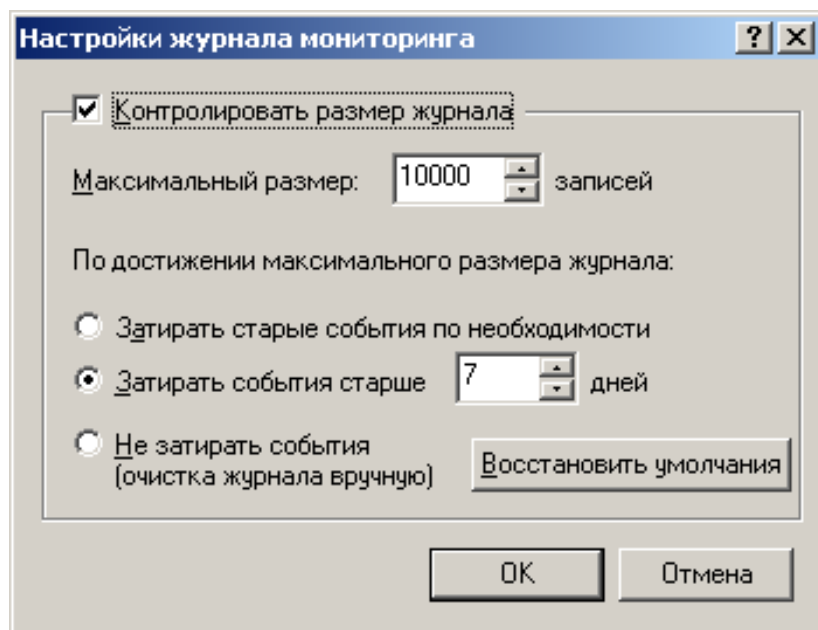


Рисунок 7 – Настройка журнала мониторинга

2.1.6 Фильтр журнала мониторинга

Фильтрация данных в Просмотрщике журнала мониторинга происходит так чтобы только записи, удовлетворяющие заданным условиям, выводились в список.

Чтобы открыть диалог Фильтр (см. рисунок 8), используется Фильтр из контекстного меню, доступного по нажатию правой кнопки мыши на элементе Просмотрщик журнала мониторинга или соответствующая кнопка на инструментальной панели.

Когда фильтр включен, можно определить условия фильтрации, задав необходимые значения в следующих полях:

- успех – флажок, определяющий нужно ли фильтровать записи по типу успех;
- уведомление – флажок, определяющий нужно ли фильтровать записи по типу уведомление;
- предупреждение – флажок, определяющий нужно ли фильтровать записи по типу предупреждение;
- ошибка – флажок, определяющий нужно ли фильтровать записи по типу ошибка;

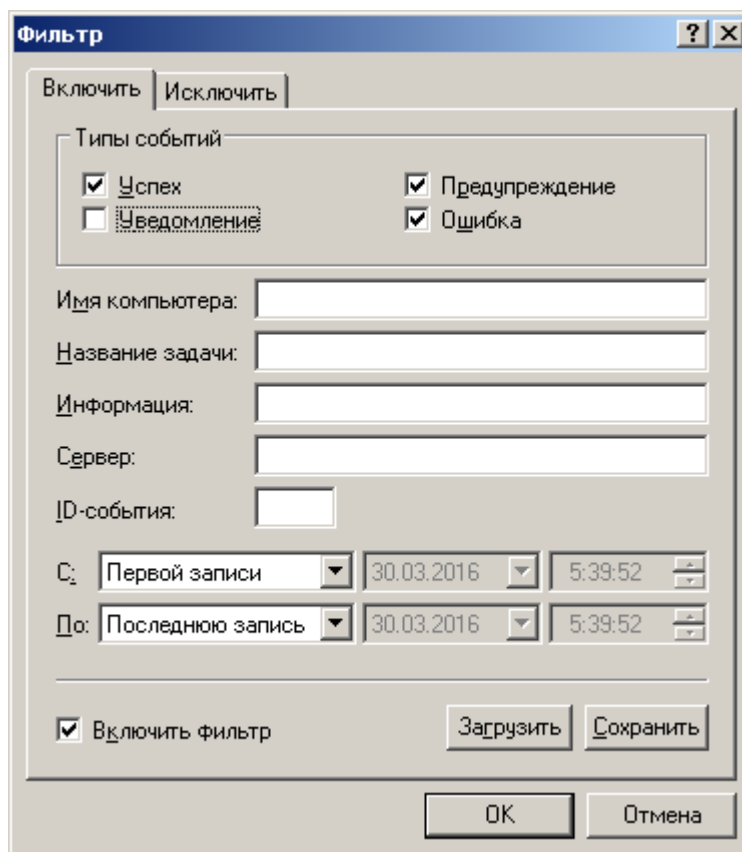


Рисунок 8 – Фильтр журнала мониторинга

— имя компьютера – текст, соответствующий значению столбца имя компьютера в Просмотрщике журнала мониторинга. Это поле нечувствительно к регистру и можно использовать маски. Используя точку с запятой в качестве разделителя, можно задать несколько значений;

— название задачи – текст, соответствующий значению столбца Название задачи в Просмотрщике журнала мониторинга. Это поле нечувствительно к регистру и можно использовать маски. Используя точку с запятой в качестве разделителя, можно задать несколько значений;

— информация – текст, соответствующий значению столбца информация в Monitoring Log Viewer. Это поле нечувствительно к регистру и вы можете использовать маски. Используя точку с запятой в качестве разделителя, можно задать несколько значений;

— сервер – текст, соответствующий значению столбца Сервер в Просмотрщике журнала мониторинга. Это поле нечувствительно к регистру и

можно использовать маски. Используя точку с запятой в качестве разделителя, можно задать несколько значений;

- ID события – число, соответствующее значению столбца Событие в Просмотрщике журнала мониторинга. Используя точку с запятой в качестве разделителя, можно задать несколько значений;

- с – определяет начало временного интервала событий, которые необходимо фильтровать;

- по – определяет конец временного интервала событий, которые фильтруются. [4]

2.2 Функции мониторинга и защиты агентов, реализуемые программным комплексом Zecurion Zlock (Device Control)

2.2.1 Настройка 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 надо:

- открыть в дереве пункт Компьютеры и приложения и выбрать необходимый элемент дерева — компьютер, группу либо домен;

- выбрать пункт Свойства соединения в меню Соединение и перейти на вкладку Мониторинг Zlock, соответственно рисунку 9;

- отметить пункт Включить мониторинг состояния Zlock. Если настройка параметров мониторинга недоступна, необходимо выключить опцию Наследовать настройки мониторинга. Включенная опция Наследовать настройки мониторинга означает, что на данный компьютер распространяются настройки мониторинга группы или домена, к которым он относится;

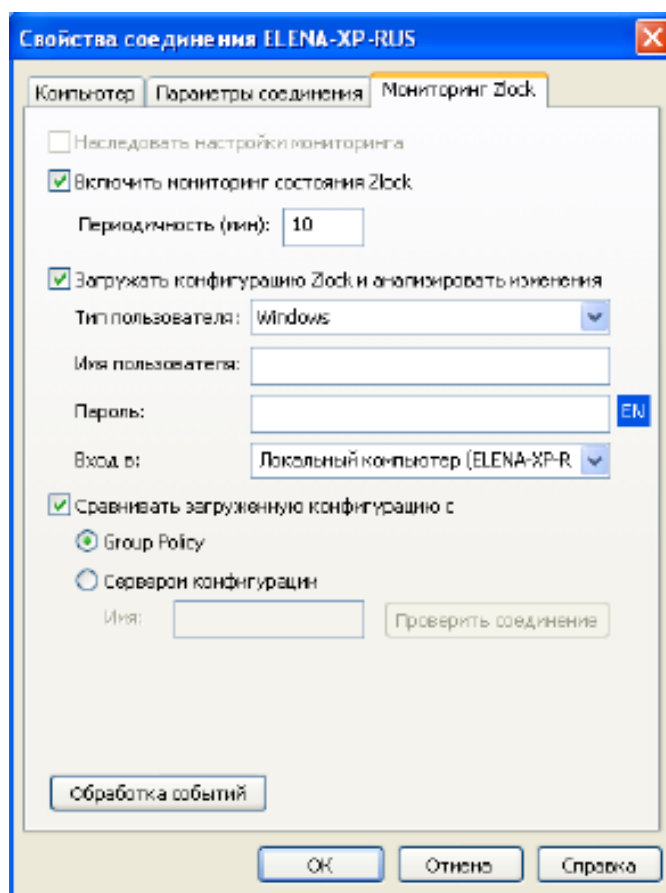


Рисунок 9 – Мониторинг ZLock

— в поле Периодичность указать 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;

— если необходимо, 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: Group Policy или сервер конфигураций. Если сравнение необходимо выполнить с конфигурацией, распространяемой через сервер конфигураций, необходимо указать имя сервера конфигураций и нажать

кнопку Проверить соединение. В отличие от журналирования, при котором выполняется только фиксирование события изменения конфигурации, включение флага Загружать конфигурацию Zlock и анализировать изменения позволяет детально проанализировать, какие именно изменения произведены, а включение флага Сравнивать загруженную конфигурацию с позволяет обнаружить отличия конфигурации удаленного компьютера с распространяемой;

— указать, какие действия нужно выполнить при возникновении каждой ситуации. Для этого нажать на кнопку Обработка событий, как представлено на рисунке 10;

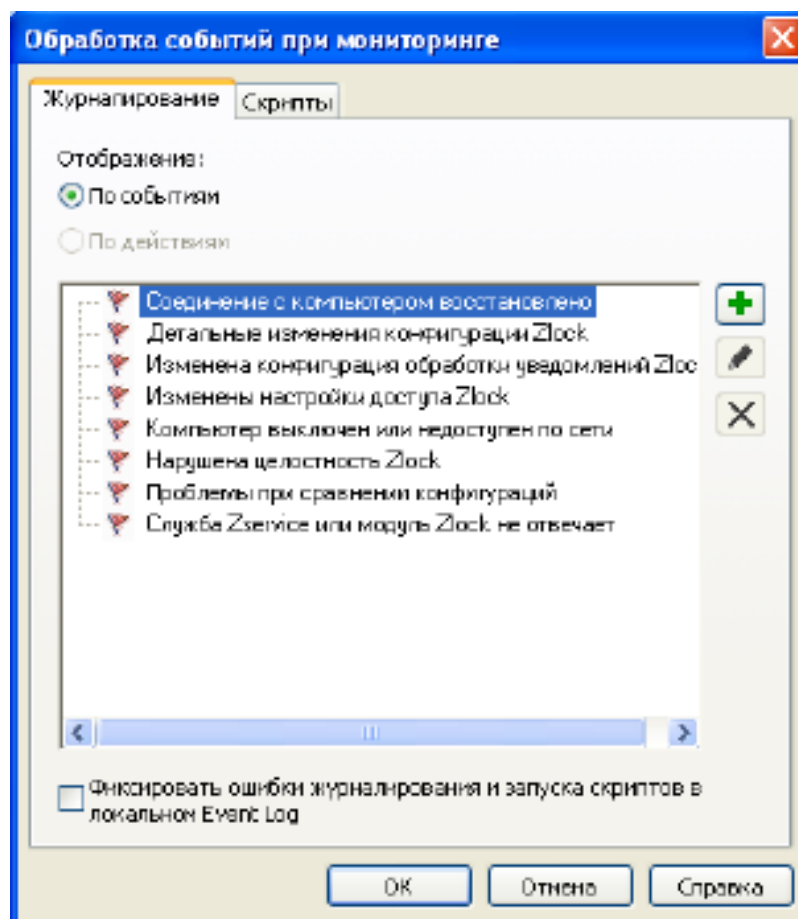


Рисунок 10 – Обработка событий

— 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.

2.2.2 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, согласно рисунку 11.

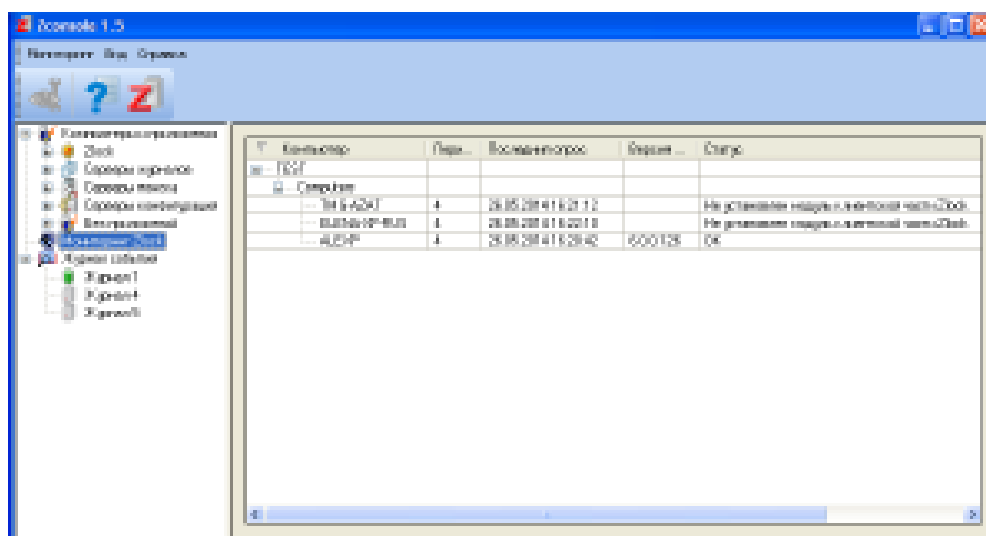


Рисунок 11 – Просмотр статуса удалённых компьютеров

2.2.3 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 либо кнопки .[4]

3 Описание подготовки лабораторных стендов, используемых при проведении лабораторных работ

3.1 Создание виртуальных машин

Для создания образа виртуальных машин был скачан установочный пакет Oracle VM VirtualBox 4.2.16 с официального сайта компании Oracle. Данная программа проста в управлении, имеет весь необходимый функционал, является бесплатной.

Необходимо нажать кнопку «Next» («Далее»), как показано на рисунке 12 и перейти к диалогу выбора устанавливаемых компонентов, оставляя все без изменений и нажать кнопку «Next» (см. рисунок 13).



Рисунок 12 – Установка Oracle VM VirtualBox 4.2.16

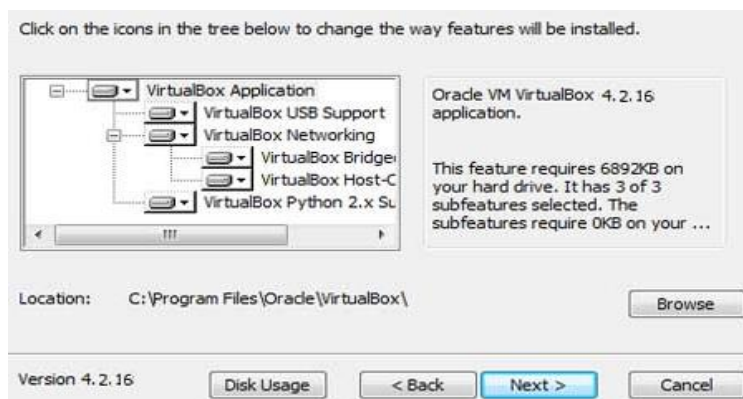


Рисунок 13 – Выбор компонентов

На следующем шаге, установщик предложит выбрать место, где будут созданы ярлыки для запуска программы. По умолчанию ярлыки будут созданы на рабочем столе и на панели быстрого запуска (см. рисунок 14).

После выбора создания ярлыков, нажать кнопку «Next», откроется окно с запросом на установку драйверов сетевых устройств, нажать кнопку «Yes» (см. рисунок 15). Следующий этап – это установка Oracle VM VirtualBox 4.2.16, нажать «Install». Установка VirtualBox была завершена, нажать «Finish» (см. рисунок 16).

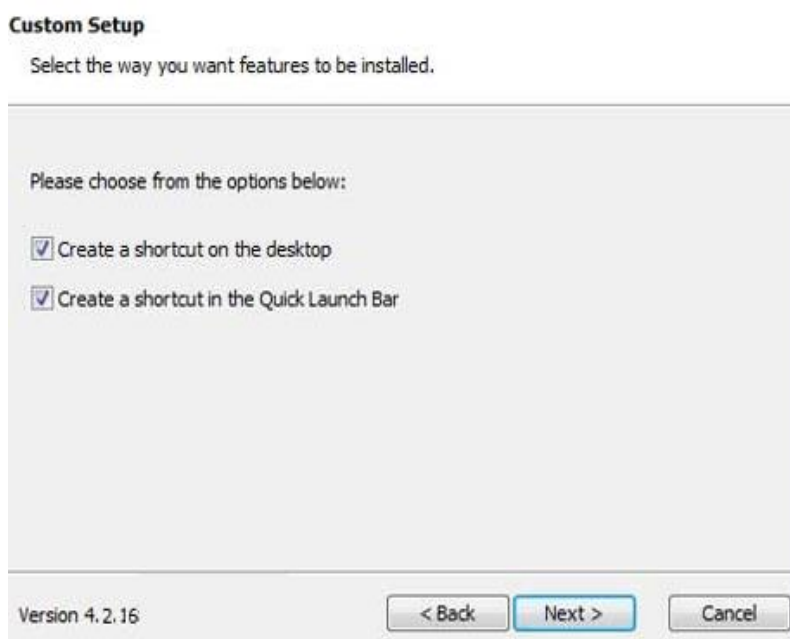


Рисунок 14 – Выбор создания ярлыков



Рисунок 15 – Установка драйверов сетевых устройств



Рисунок 16 – Завершение установки

Сначала был настроен каталог, в котором хранятся конфигурационные файлы. Для того чтобы настроить каталог, необходимо выбрать пункт меню «Файл – Свойства – Общие» или нажать комбинацию клавиш Ctrl+G и выбрать необходимый путь для сохранения конфигурационных файлов.

В VirtualBox необходимо нажать кнопку «Создать» и в появившемся диалоговом окне задать имя виртуальной машины, тип и версию операционной системы и нажать кнопку «Next» (см. рисунок 17).

В следующем окне выбрать объем оперативной памяти, выделяемой виртуальной машине и нажать кнопку «Next» (см. рисунок 18).

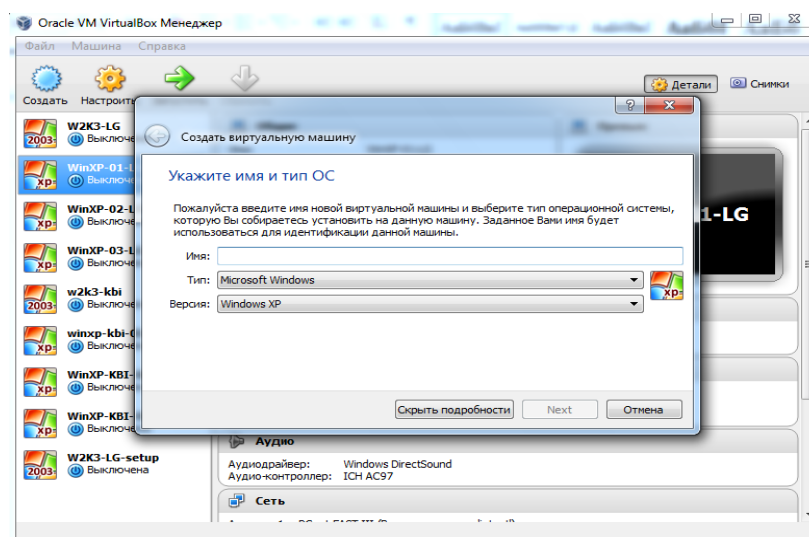


Рисунок 17 – Создание виртуальной машины

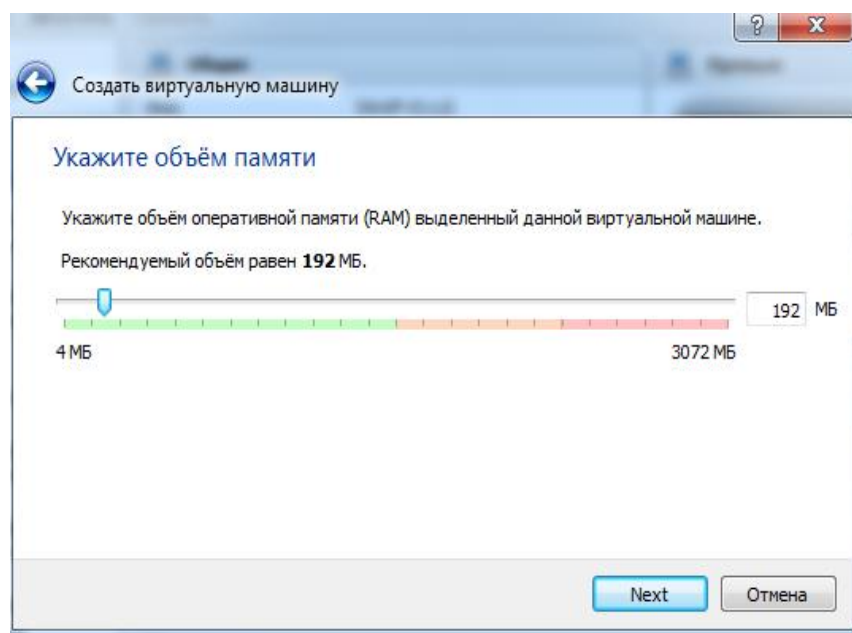


Рисунок 18 – Выбор объема памяти

В открывшемся окне выбрать размер загрузочного жесткого диска для создаваемой виртуальной машины, в данном случае выбрать существующий диск, нажать по иконке папки, выбрать файл с образом диска на компьютере и нажать кнопку «Создать» (см. рисунок 19).

Таким образом, используя заранее созданные образы сервера и трех клиентов, два из которых являются копией первого, были созданы виртуальные машины (см. рисунок 20).

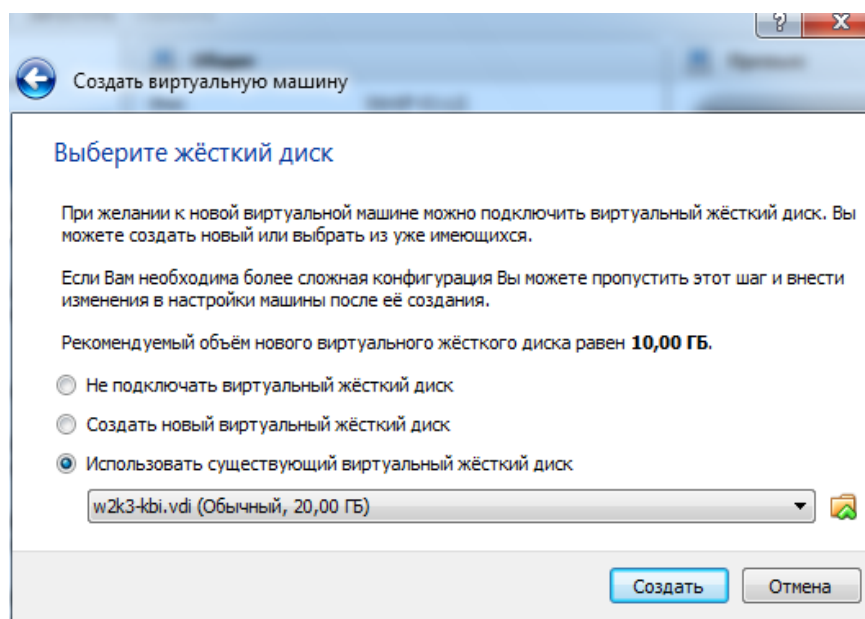


Рисунок 19 – Выбор жесткого диска

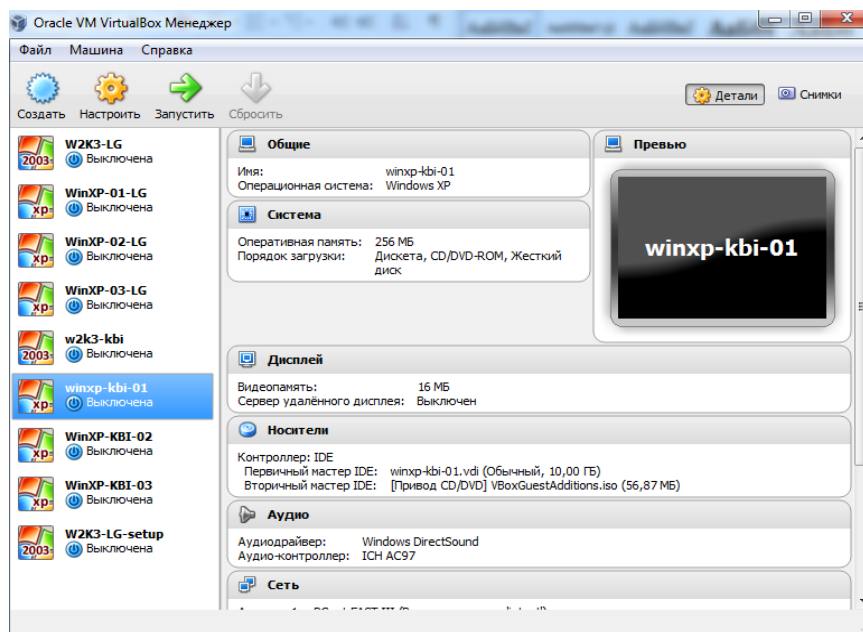


Рисунок 20 – Окно VM VirtualBox

После создания VM необходимо установить гостевую ОС. При создании лабораторного стенда для одной VM в качестве ОС установлена Windows 2003 Server, для двух VM установлена Windows XP. Описанная последовательность действий использовалась при создании каждой VM, входящей в состав лабораторного стенда. Установка гостевой ОС была выполнена в соответствии с порядком установки, определенным разработчиком [3,4].

В результате действий, описанных выше, было создано два виртуальных стенда:

— виртуальный стенд для лабораторной работы с программным комплексом Device Lock, который включает в себя:

- одну VM с установленной гостевой ОС Windows 2003 Server;
- две VM с установленной гостевой ОС Windows XP.

— виртуальный стенд для лабораторной работы с программным комплексом ZLock, который включает в себя:

- одну VM с установленной гостевой ОС Windows 2003 Server;
- две VM с установленной гостевой ОС Windows XP.

3.2 Создание виртуальных локальных сетей

3.2.1 Настройка сетевого взаимодействия VM

После создания VM необходимо настроить сетевое взаимодействие VM, входящих в лабораторный практикум для DeviceLock, а также для ZecurionLock. Каждая сеть состоит из 3 VM. Порядок настройки одинаков для каждого стенда.

Следующим этапом необходимо настроить сеть в виртуальной машине и общую папку. Для этого выбрать необходимую виртуальную машину, нажать правой кнопкой мыши и выбрать пункт свойства, во вкладке «Сеть» установить «Тип подключения: Внутренняя сеть» (см. рисунок 21). Во вкладке «Общие папки» нажать на пиктограмму «Добавить общую папку» и выбрать папку, по которой будет происходить обмен между системой и виртуальной машиной. Выше изложенные настройки проводятся с каждой виртуальной машиной (см. рисунок 22).

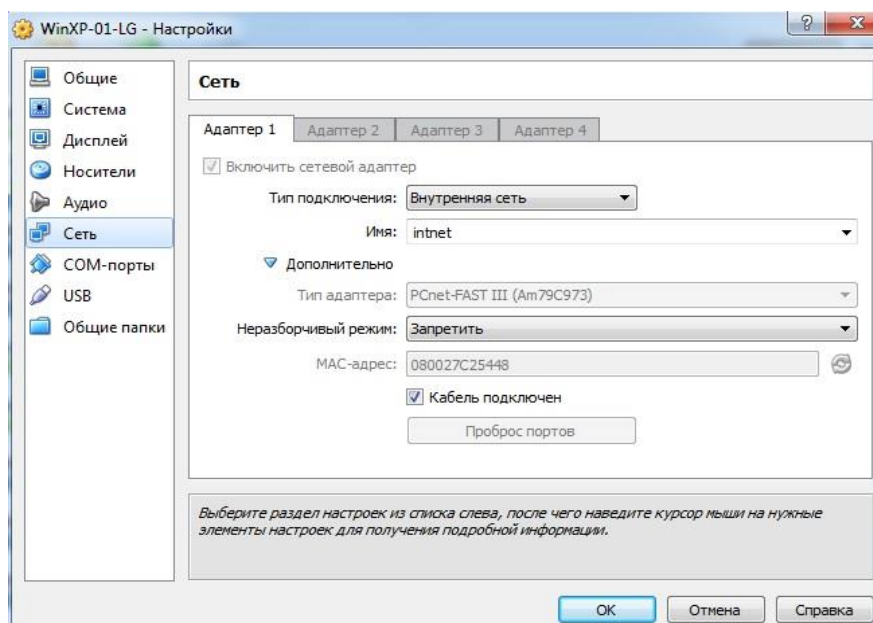


Рисунок 21 – Настройка сети

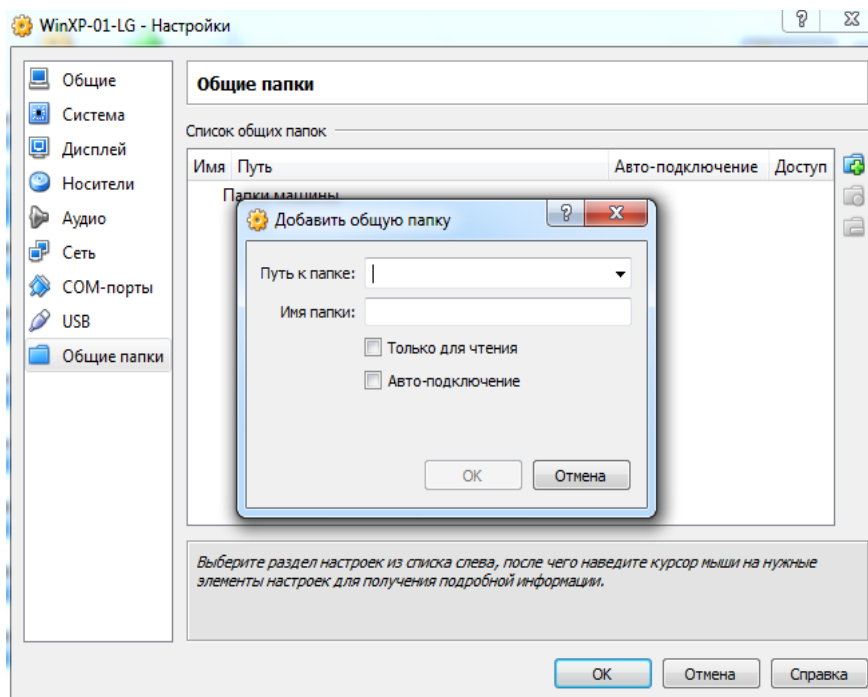


Рисунок 22 – Настройка общей папки

Далее запустить сервер W2K3 - DL и произвести его настройку. Для запуска брандмауэра, перейти по следующему пути «Пуск – Панель управления – Брандмауэр Windows». Во вкладке «Общие» нажать «Откл.» (см. рисунок 23). Отключение брандмауэра позволяет настроить сеть для бесперебойной работы.

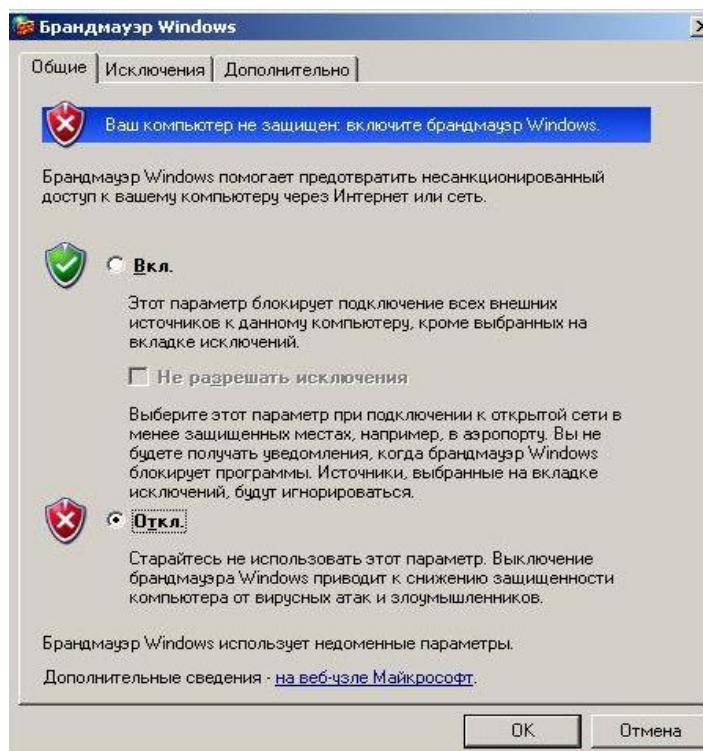


Рисунок 23 – Отключение брандмауэра Windows

Далее перейти на следующую вкладку «Исключения» и в окне «Программы и службы» отметить все программы и службы (см. рисунок 24).

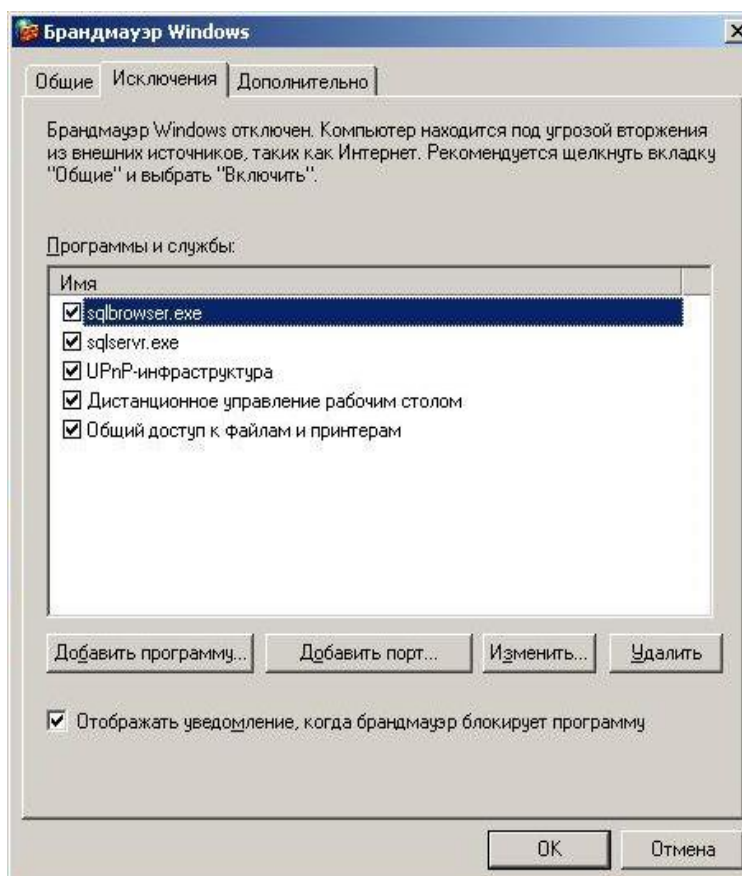


Рисунок 24 – Исключения брандмауэра

Затем перейти на следующую вкладку «Дополнительно – Параметры сетевого подключения – Параметры» и в открывшейся вкладке «Дополнительные параметры» «Службы» отметить все службы из списка, далее перейти на вкладку «ICMP» и отметить все разрешения, нажать кнопку «ОК».

3.2.2 Настройка службы DNS

Настройка DNS на сервере состоит из следующих шагов:

- а) в главном меню выбрать «Панель управления» —> «Сетевые подключения», а затем правой кнопкой мыши щелкнуть по пункту «Подключение по локальной сети»;
- б) из контекстного меню выбрать «Свойства»;
- в) в окне свойств подключения к локальной сети выбрать пункт «Протокол сети Интернет TCP/IP» и нажать на кнопку «Свойства». Откроется окно свойств протокола TCP/IP;

- г) в поле «Предпочитаемый сервер DNS» ввести IP-адрес сервера;
- д) последовательным нажатием на кнопку ОК закрыть все окна;
- е) в меню Пуск нажать правой кнопкой мыши на меню Мой компьютер и выбрать пункт «Свойства»;
- ж) в диалоговом окне «Свойства системы» открыть вкладку «Имя компьютера» и нажать кнопку «Изменить»;
- и) в диалоговом окне смены имени компьютера нажать кнопку «Дополнительно»;
- к) в диалоговом окне «DNS-суффикс и NetBIOS-имя компьютера» ввести в поле «Предпочитаемый DNS-суффикс» имя зоны. Нажатием ОК закрыть окно;
- л) диалоговое окно закрыть нажатием ОК. После этого необходимо перезагрузить компьютер;
- м) после перезагрузки компьютера снова открыть консоль DNS и в левой части окна выбрать зону.

Для настройки DNS на рабочей станции необходимо проделать следующие действия:

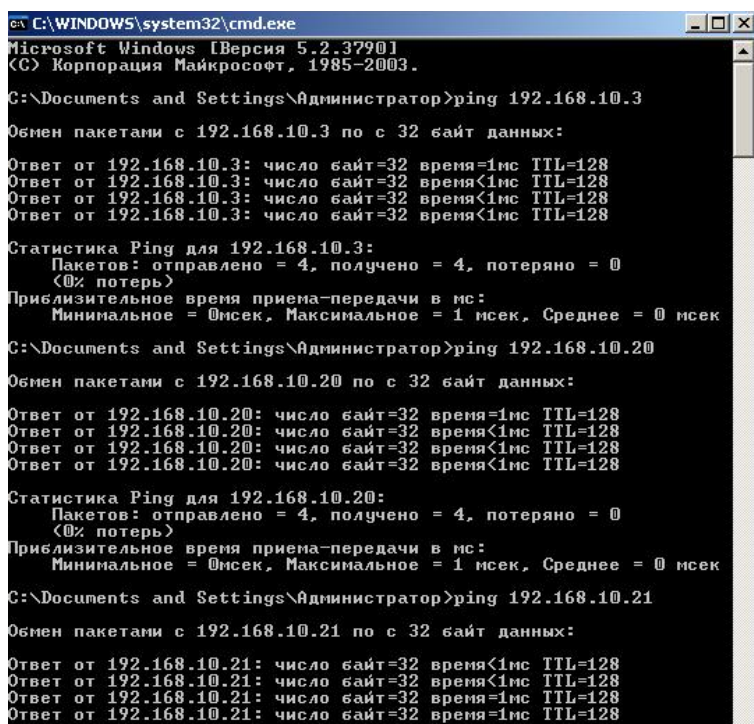
- а) зарегистрироваться на компьютере как «Администратор»;
- б) в главном меню выбрать «Панель управления» —> «Сетевые подключения», а затем правой кнопкой мыши щелкнуть по пункту «Подключение по локальной сети»;
- в) из контекстного меню выбрать «Свойства»;
- г) в окне «Подключение по локальной сети — свойства» выбрать «Протокол сети Интернет», нажать на кнопку «Свойства»;
- д) в поле «Предпочитаемый DNS-сервер» ввести адрес. Затем нажать ОК. Диалоговое окно свойств подключения закрыть нажатием кнопки «Закрыть»;
- е) далее действовать так же, как на сервере (пункты с е по л). Для того, чтобы изменения вступили в силу, надо будет перезагрузить компьютер. Закрыть оба окна и перезагрузить компьютер.

Указанные шаблоны были использованы с настройками Device Lock и ZLock.

3.2.3 Проверка подключения ВМ друг к другу с использованием утилиты ping

Последний этап позволяет проверить соединения в сетях на основе TCP/IP. Для этого необходимо запустить все клиентские виртуальные машины и виртуальную машину сервер. На виртуальной машине сервер запустить командную строку и с помощью команды «ping», пропинговать всю сеть, начиная проверку самой машины, а затем на каждую клиентскую машину (см. рисунок 25). Аналогично сделать для каждой клиентской машины.

Все выше изложенные настройки позволяют с полной уверенностью говорить, что сеть была полностью настроена для работы виртуальных машин. Аналогичные настройки сети необходимо выполнить для всех компьютеров домена и контролера домена.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Версия 5.2.3790.1
(C) Корпорация Майкрософт, 1985-2003.

C:\Documents and Settings\Администратор>ping 192.168.10.3

Обмен пакетами с 192.168.10.3 по с 32 байт данных:

Ответ от 192.168.10.3: число байт=32 время=1мс TTL=128
Ответ от 192.168.10.3: число байт=32 время<1мс TTL=128
Ответ от 192.168.10.3: число байт=32 время<1мс TTL=128
Ответ от 192.168.10.3: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.10.3:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    <0% потерь>
    Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 1 мсек, Среднее = 0 мсек

C:\Documents and Settings\Администратор>ping 192.168.10.20

Обмен пакетами с 192.168.10.20 по с 32 байт данных:

Ответ от 192.168.10.20: число байт=32 время=1мс TTL=128
Ответ от 192.168.10.20: число байт=32 время<1мс TTL=128
Ответ от 192.168.10.20: число байт=32 время<1мс TTL=128
Ответ от 192.168.10.20: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.10.20:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    <0% потерь>
    Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 1 мсек, Среднее = 0 мсек

C:\Documents and Settings\Администратор>ping 192.168.10.21

Обмен пакетами с 192.168.10.21 по с 32 байт данных:

Ответ от 192.168.10.21: число байт=32 время<1мс TTL=128
Ответ от 192.168.10.21: число байт=32 время<1мс TTL=128
Ответ от 192.168.10.21: число байт=32 время=1мс TTL=128
Ответ от 192.168.10.21: число байт=32 время=1мс TTL=128
```

Рисунок 25 – Ping сети

Для выполнения двух лабораторных работ практикума было создано шесть виртуальных машин. Для изучения ПК DeviceLock:

- «WinXP 01-DL» и «WinXP02 – DL» – компьютеры домена, на которых установлена ОС Windows XP SP3;

- «W2K3 – DL» – виртуальная машина, являющаяся сервером. На эту виртуальную машину была установлена ОС Windows 2003 Server.

Для изучения ПК ZLock:

- «WinXP 01-ZL» и «WinXP02 – ZL» – компьютеры домена, на которых установлена ОС Windows XP SP3;

- «W2K3 – ZL» – виртуальная машина, являющаяся сервером. На эту виртуальную машину была установлена ОС Windows 2003 Server.

Перед установкой систем контроля и предотвращения утечек информации в каждой виртуальной сети был настроен контроллер домена и служба Active Directory. Каждой виртуальной машине был присвоен IP – адрес, соответственно:

- «WinXP 01-DL» – 192.168.10.11;

- «WinXP02 – DL» – 192.168.10.12;

- «W2K3 – DL» – 192.168.10.1;

- «WinXP 01-ZL» – 192.168.10.11;

- «WinXP02 – ZL» – 192.168.10.12;

- «W2K3 – ZL» – 192.168.10.2.

Виртуальные машины были разработаны с учетом эксплуатации их на компьютере с основной ОС Windows XP и выше. Именно под Windows XP сконфигурирована их корректная работа, как в сети, так и автономно.

3.2.4 Установка домена Active Directory

Для установки домена Active Directory выполните следующую последовательность действий:

а) зарегистрировать на сервере как Администратор. В командной строке («Пуск» -> «Выполнить», в поле «Открыть» введя cmd ввести команду dsppromo. Она запустит «Мастер установки службы Active Directory». Нажать кнопку «Далее»;

б) прочитать сведения, приведенные в диалоговом окне «Совместимость с ОС», и нажать кнопку «Далее»;

в) в диалоговом окне «Тип контроллера домена» оставить переключатель в положении «Контроллер домена в новом домене» и нажать кнопку «Далее»;

г) в диалоговом окне «Создать новый домен» оставить переключатель в положении «Новый домен в новом лесу» и нажать кнопку «Далее»;

д) в диалоговом окне «Новое имя домена» ввести в поле «Полное DNS-имя» имя нового домена и нажать кнопку «Далее»;

е) в диалоговом окне «NetBIOS-имя домена» оставить имя по умолчанию STUDY и продолжить нажатием кнопки «Далее»;

ж) в диалоговом окне «Папки базы данных и журналов» оставить предложенный путь C:\WINDOWS\NTDS для БД и C:\WINDOWS\NTDS для журнала. Затем нажать «Далее»;

и) в диалоговом окне «Общий доступ к системному тому» оставить предложенный путь C:\WINDOWS\SYSTEMVOLUME32 и нажать «Далее»;

к) теперь сервер произведет поиск зоны DNS по имени, соответствующему заданному имени домена. Если зона будет найдена, отобразится уведомление об успешно проведенной диагностике. Если нет — система предложит ее автоматическую установку и конфигурирование. Прочитав информацию, нажать кнопку «Далее»;

л) в диалоговом окне «Разрешения» отметить пункт «Разрешения, совместимые только с Windows 2000 или Server Windows Server 2003», а затем нажать кнопку «Далее»;

м) в диалоговом окне «Пароль администратора для режима восстановления» задать в поле «Пароль режима восстановления» и в поле «Подтверждение пароля» пароль, который используется при восстановлении БД Active Directory. Затем нажать кнопку «Далее»;

н) в диалоговом окне «Итоговый результат» проверить исправность настройки всех параметров домена Active Directory. В случае выявления каких-

либо ошибок нажатием на кнопку «Назад» вернуться к диалоговому окну и исправить необходимые параметры. Потом нажатием кнопки «Далее» запустить дальнейший процесс установки контроллера домена;

п) по окончании работы «Мастера установки службы Active Directory» нужно перезагрузить компьютер.

3.2.5 Проверка правильности установки контроллера домена

Сервер сейчас управляет и доменом Active Directory. После установки каждого контроллера домена следует провести контроль качества установки:

а) зарегистрироваться на как Администратор (только администратор теперь обладает всеми правами доступа в домене);

б) запустить «Проводник» и убедиться, что существует папка C:\WINDOWS\NTDS с файлами NTDS.DIT (БД Active Directory) и EDB.LOG (файл журнала транзакций). Далее убедиться в существовании папки C:\WINDOWS\SYSVOL;

в) в меню «Пуск» перейти в раздел «Администрирование» и убедиться, что там добавились инструменты для управления доменом: «консоли Active Directory — пользователи и компьютеры», «Active Directory — сети и сервисы» и «Active Directory — домены и доверие». Затем открыть окно консоли «Просмотр событий» и убедиться, что там добавились пункты «Служба каталогов» и «Служба репликации файлов». Выбрать пункт «Служба репликации файлов» и найти событие 13516. Там сообщается, что контроллер домена выполняет свои функции;

г) открыть консоль DNS и убедиться, что в зоне были созданы поддомены _msdcs, _sites, _tcp, _udp, Domain-DnsZones и ForestDnsZones. Первые четыре поддомена очень важны для функционирования домена Active Directory. Они включают в себя т.н. списки SRV (Размещение сервиса — Service location) на основании которых все компьютеры с системами Windows 2000/XP/2003 ориентируются в сети при поиске важных сервисов;

д) в командной строке ввести команду net share. Отобразятся разделяемые папки компьютера, в том числе и папка с сетевым именем

NETLOGON, которое сопоставлено папке C:\WINDOWS\SYSVOL\study.local\SCRIPTS.

После указанных действий было создано два виртуальных стенда:

— виртуальный стенд для лабораторной работы по изучению с программного комплекса Device Lock, который включает в себя:

—одну ВМ с установленной гостевой ОС Windows 2003 Server;

—две ВМ с установленной гостевой ОС Windows XP.

— виртуальный стенд для лабораторной работы по изучению программного комплекса ZLock, который включает в себя:

—одну ВМ с установленной гостевой ОС Windows 2003 Server;

—две ВМ с установленной гостевой ОС Windows XP.

3.3 Установка Device Lock

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

При установке ПК DL на ВМ W2K3-DL была установлена БД Microsoft SQL Express в соответствии с руководством администратора [5]. Эта БД необходима для установки DL Enterprise Server, который нужен для реализации задач мониторинга. Далее на ВМ W2K3-DL была установлена серверная часть DL, а так же были установлены компоненты управления DL. На ВМ с гостевой ОС Windows XP был установлен сервис DL а так же консоль управления.

После установки была проверена работоспособность посредством подключения сервер DL к сервису, для подключения использовалась консоль DL Management console, запускаемая на ВМ с DL 2003 Server. Так же было проверено подключение к СУБД MS SQL. Подключение выполнялось с ОС Windows 2003 Server. Использовалась консоль DL Management console.

В результате всё работает корректно.

3.4 Установка Zecurion Lock

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

При установке ПК ZL на VM W2K3-ZL была установлена БД Microsoft SQL Express в соответствии с руководством администратора [7]. Эта БД необходима для установки ZL Консоль управления, которая нужна для реализации задач мониторинга. Далее на VM W2K3-ZL была установлена серверная часть ZL, а так же были установлены компоненты управления ZL. На VM с гостевой ОС Windows XP был установлен сервис ZL а так же консоль управления.

После установки была проверена работоспособность посредством подключения сервера ZL к сервису. Так же было проверено подключение к СУБД MS SQL. Подключение выполнялось с ОС Windows 2003 Server.

В результате всё работает корректно.

Схема лабораторного стенда по Device Lock представлена на рисунке 26, по Zecrion Lock на рисунке 27.

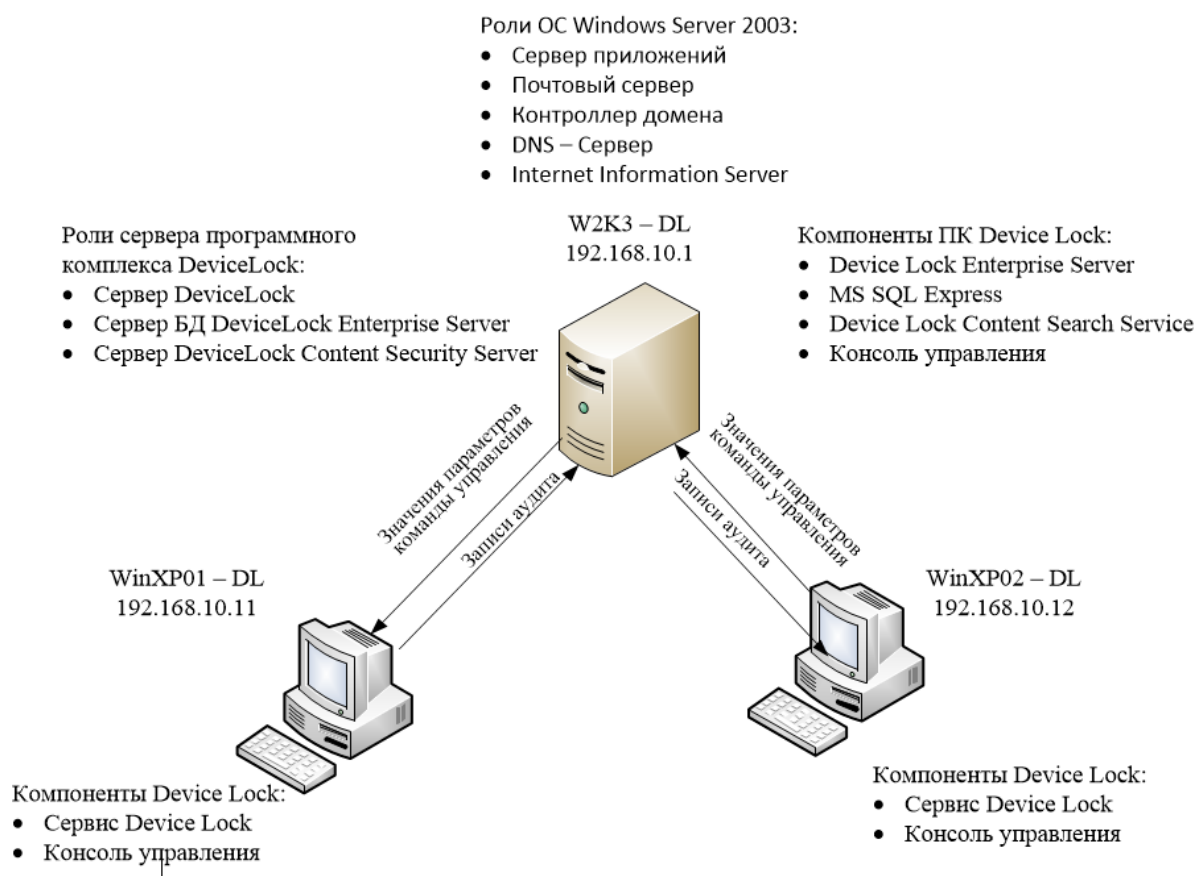


Рисунок 26 – Схема лабораторного стенда Device Lock

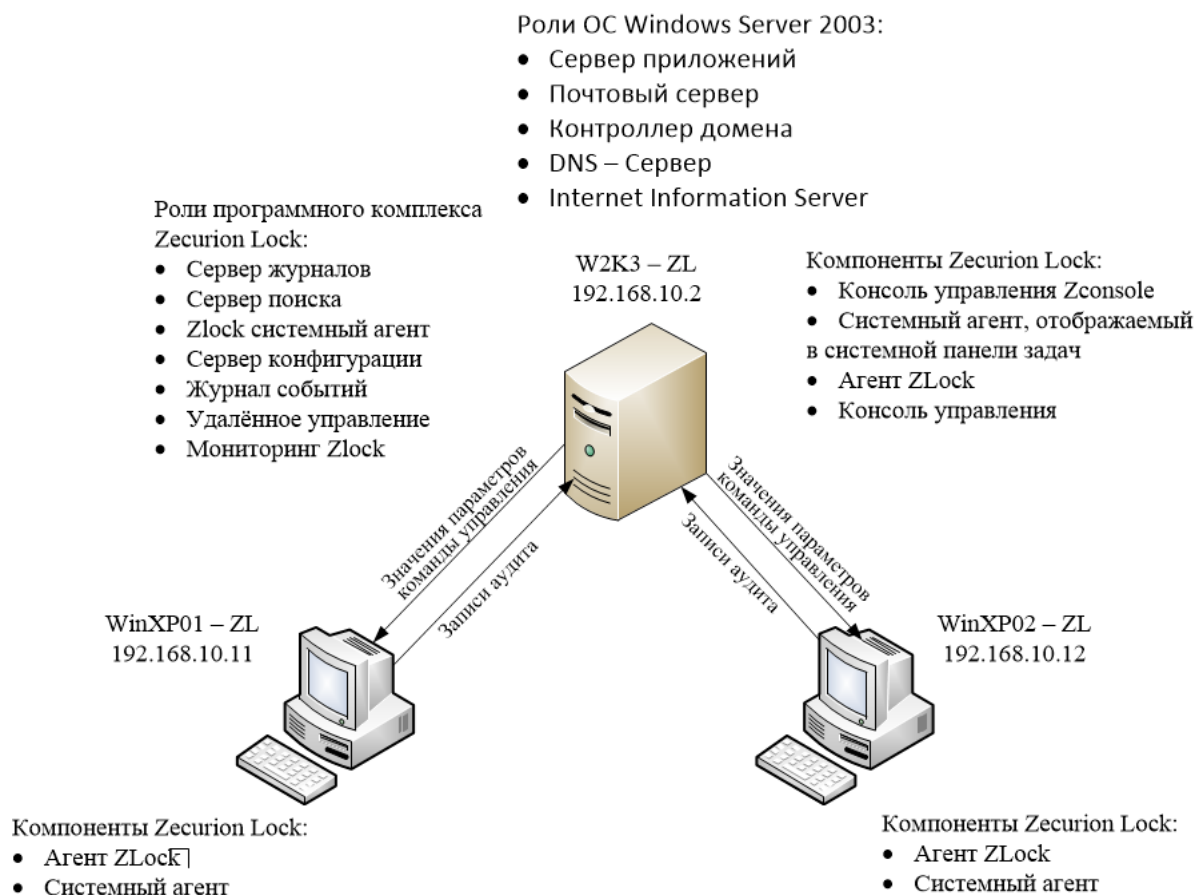


Рисунок 27 – Схема лабораторного стенда Zecurion Lock

3.5 Результат подготовки лабораторных стендов

В результате выполнения действий описанных в подпунктах 3.1-3.5 было подготовлено 2 стенда.

После указанных действий было создано два виртуальных стенда:

— виртуальный стенд для лабораторной работы по изучению ПК Device Lock, который включает в себя:

—одну ВМ с установленной гостевой ОС Windows 2003 Server, которая включает в себя Enterprise Server, сервер приложений, контроллер домена, сервис DL Server, консоль управления, DL Content Search Server;

—две ВМ с установленной гостевой ОС Windows XP, которые включают в себя сервис DL и консоль DL;

— виртуальный стенд для лабораторной работы по изучению ПК ZLock, который включает в себя:

—одну ВМ с установленной гостевой ОС Windows 2003 Server, который включает в себя консоль управления, сервис ZL, контроллер домена;

—две ВМ с установленной гостевой ОС Windows XP, который включает в себя сервис ZL.

4 Порядок выполнения лабораторной работы по изучению мониторинга и защиты агентов, реализуемой в программном комплексе DeviceLock DLP Suite

4.1 Цель и задание к лабораторной работе

Цель работы – получить навыки создания задач мониторинга и применение их для защиты сервиса Device Lock от несанкционированного изменения настроек ,отключения, удаления.

Задание на лабораторную работу включает в себя:

- настройку аудита и теневого копирования для сервиса DeviceLock;
- настройку политики безопасности домена и контроллера домена при регистрации событий;
- создание учётных записей доменных и локальных пользователей;
- создание задач мониторинга;
- имитацию нарушений работы агентов;
- формирование отчётов по журналу регистрации событий;
- вывод по выполненной работе.

4.2 Порядок выполнения лабораторной работы

Включение и настройка аудита.

Осуществить вход на контроллере домена W2K3-DL с использованием учетной записи доменного администратора. Запустить консоль управления DeviceLock Management Console. Подключится к сервису DeviceLock, установленному на компьютере WinXP01-DL. С помощью консоли управления DeviceLock Management Console настроить аудит и теневое копирование для компьютера WinXP01-DL, установив следующие значения параметров:

- «Локальная директория» – оставить значение по умолчанию;
- «Включить локальную квоту» – *включено*;
- «Затирать файлы старше чем (дней)» – 10;
- «Локальная квота (%)» – 50;
- «Сохранять файлы нулевой длины» – *включено*;

- «Запретить передачу данных при ошибках» – включено;
- «Тип журнала аудита» – журнал событий и журнал DeviceLock;
- «Настройка журнала аудита» – 2048 КБайт, затирать старые события по необходимости;
- «Отправлять данные теневого копирования» – отключено.

Состояние подсистемы аудита и теневого копирования после настройки для компьютера WinXP01-DL показано на рисунке 27.

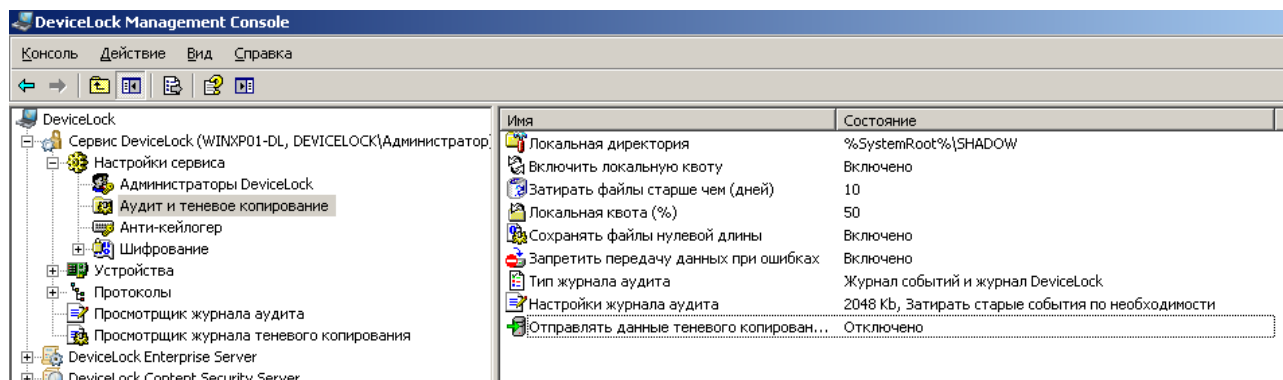


Рисунок 27 – Настройка подсистемы аудита и теневого копирования

Настройка управления программным комплексом DeviceLock

Настроить управление сервисом DeviceLock, установленным на компьютере WinXP01-DL. Для этого необходимо на контроллере домена W2K3-DL запустить консоль управления DeviceLock Management Console и выполнить подключение к сервису DeviceLock, установленному на компьютере WinXP01-DL. Затем перейти к пункту «Администраторы DeviceLock, подраздела «Настройка сервиса». Добавить в список администраторов сервиса DeviceLock только администратора домена и назначить ему полный доступ (см. рисунок 28).

Затем перейти в подраздел «Настройки сервиса» щелкнув по нему левой клавишей мыши. В правой части консоли выбрать пункт DeviceLock Enterprise Server(ы), щелкнув правой клавишей мыши. В появившемся окне ввести имя сервера – W2K3-DL (см. рисунок 29).

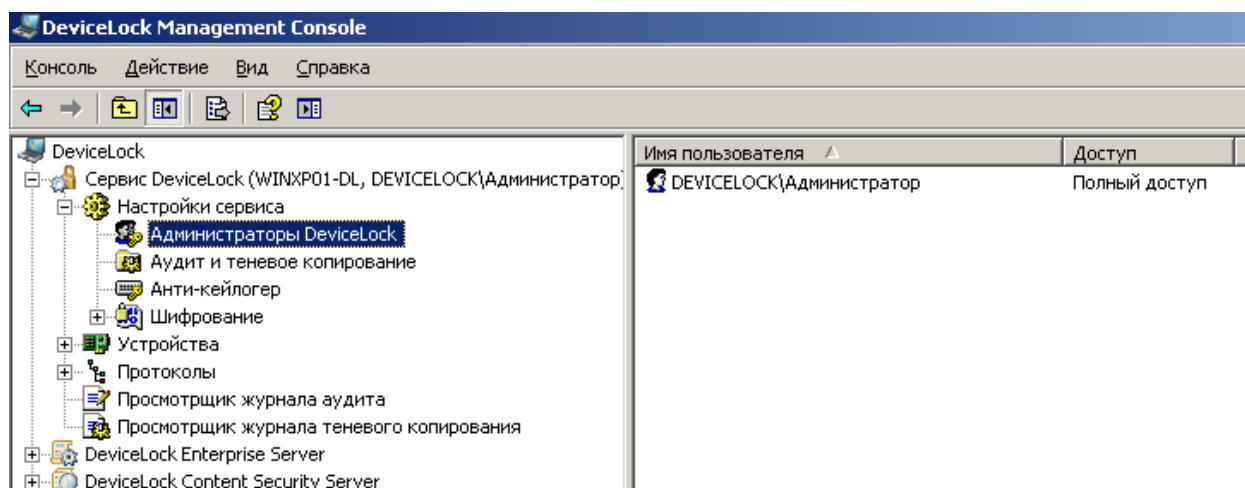


Рисунок 28 – Настройка списка администраторов сервиса DeviceLock, установленного на компьютере WinXP01-DL

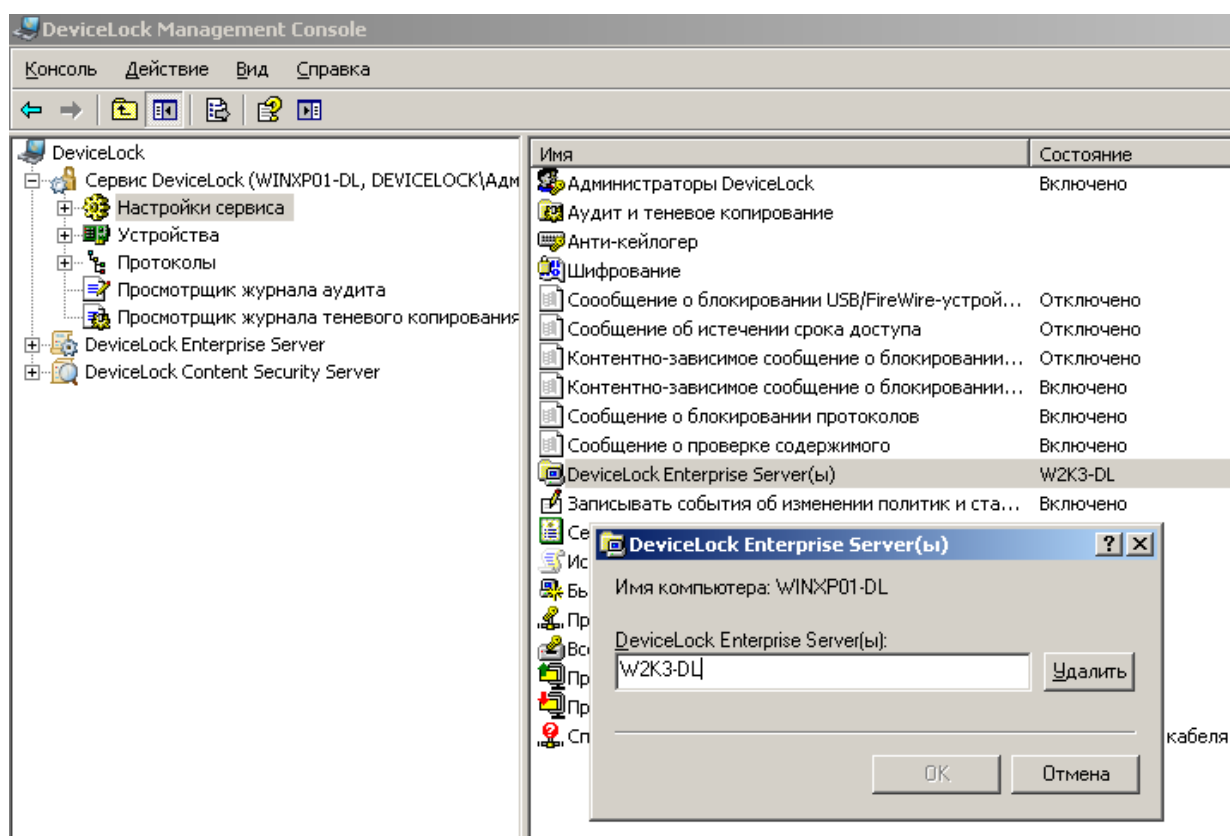


Рисунок 29 – Выбор DeviceLock Enterprise Server

Настроить управление сервером DeviceLock Enterprise Server. Для этого в консоли управления DeviceLock Management Console выбрать раздел DeviceLock Enterprise Server и выполнить подключение к серверу. При подключении в диалоговом окне «Выбор компьютера» указать параметр «Локальным компьютером: (тем, на котором запущена эта консоль)». Затем

открыть раздел DeviceLock Enterprise Server, щелкнув один раз левой клавишей мыши по знаку «+» слева от названия раздела и выбрать подраздел «Настройки сервера». Аналогичным способом открыть содержание этого раздела и выбрать пункт «Администраторы сервера». Добавить в список управления DeviceLock Enterprise Server доменного администратора, предоставив ему полный доступ. Добавление учетной записи доменного администратора для DeviceLock Enterprise Server осуществляется также как и для сервиса DeviceLock (см. рисунок 30).

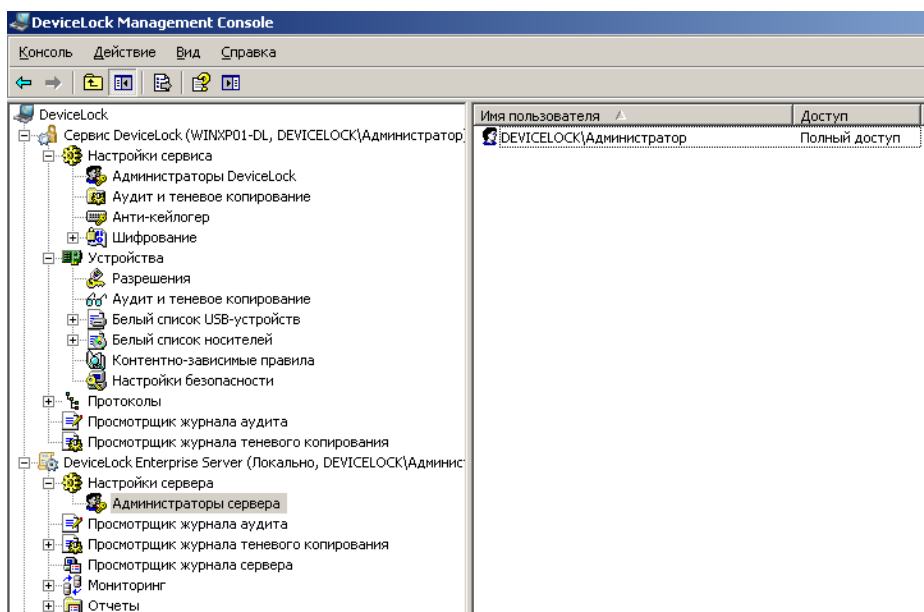


Рисунок 30 – Список администраторов DeviceLock Enterprise Server

Проверить наличие учетной записи доменного администратора в списке администраторов DeviceLock Enterprise Server.

Включение режима отображения устройств.

При настройке и подготовке программного комплекса DeviceLock к применению необходимо настроить режим отображения устройств для защищаемого компьютера WinXP01-DL. Для настройки необходимо на контроллере домена – компьютере W2K3-DL, запустить консоль управления DeviceLock Management Console. Подключиться к сервису DeviceLock, установленному на компьютере WinXP01-DL. Затем выбрать подраздел «Устройства». Щелкнуть по нему правой клавишей мыши и в контекстном

меню выбрать команду «Отображать только доступные устройства» (см. рисунок 31).

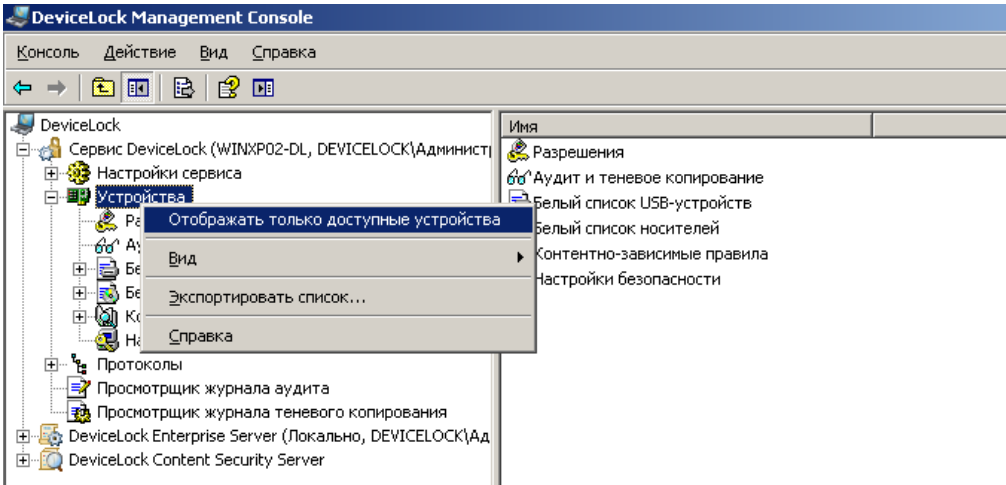


Рисунок 31 – Изменение режима отображения устройств

После выбора команды в списке «Разрешения» отобразятся только те устройства, доступом к которым можно управлять на компьютере с установленным сервисом DeviceLock – WinXP01-DL (см. рисунок 32).

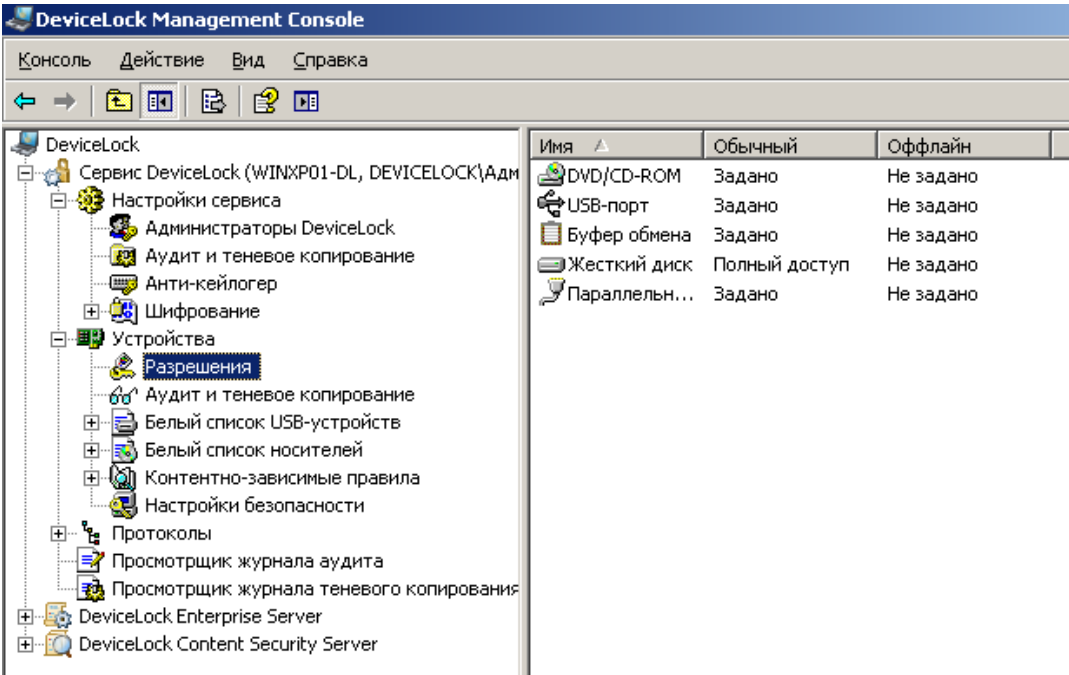


Рисунок 32 – Список доступных устройств для компьютера WinXP01-DL

Создание учетных записей пользователей.

Создать учетную запись локального пользователя на компьютере WinXP01-DL (User01). Для этого осуществить вход на компьютер WinXP01-DL с использованием учетной записи либо локального, либо доменного

администратора. Запустить программу «Управление компьютером» создать учетную запись пользователя. При создании учетной записи установить следующие параметры учетных записей (см. рисунок 33):

- «Запретить смену пароля пользователем»;
- «Срок действия пароля не ограничен».

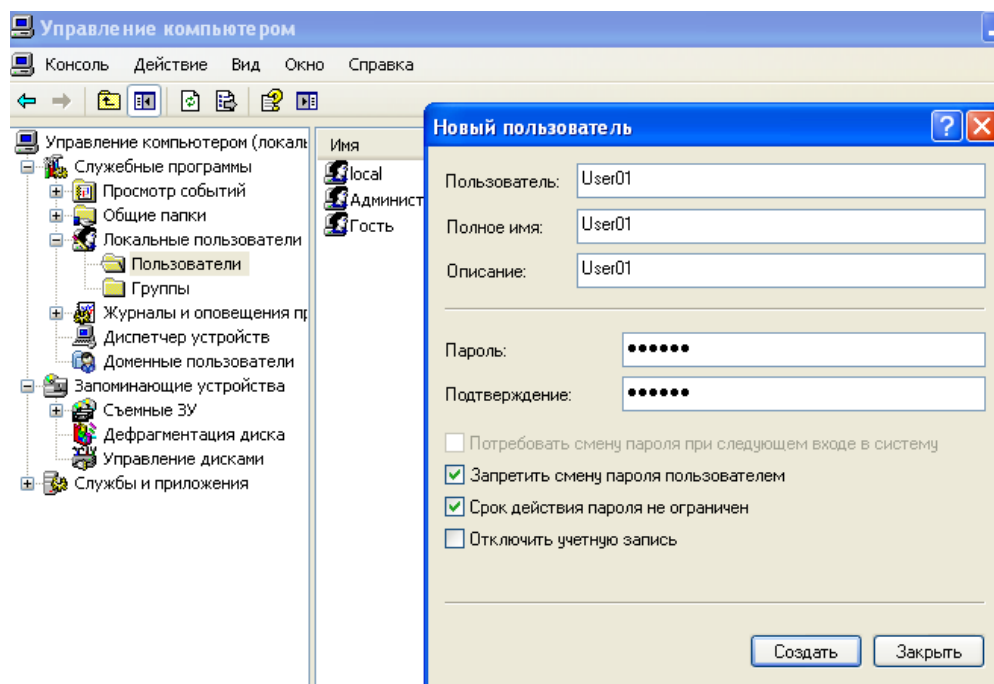


Рисунок 33 – Создание учетной записи пользователя

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.

Настройка прав доступа к жесткому диску компьютера WinXP01-DL.

Предварительно для выполнения практического задания необходимо настроить права доступа локального пользователя к жесткому диску компьютера WinXP01-DL. Для этого осуществить вход, используя учетную запись администратора. Открыть диалоговое окно свойств диска C:\ компьютера WinXP01-DL и перейти на вкладку «Безопасность». Добавить в список контроля доступа учетную запись локального пользователя User01. Предоставить полный доступ к диску C:\ компьютера WinXP01-DL (см. рисунок 34).

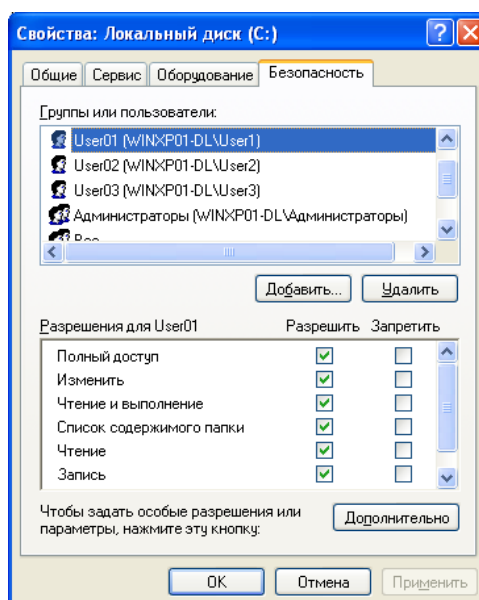


Рисунок 34 – Назначение разрешений для локальных пользователей

Затем в диалоговом окне свойств на вкладке «Безопасность» (см. рисунок 8) нажать кнопку «Дополнительно», в диалоговом выбрать учетную запись пользователя User01 и нажать кнопку «Изменить» (см. рисунок 35).

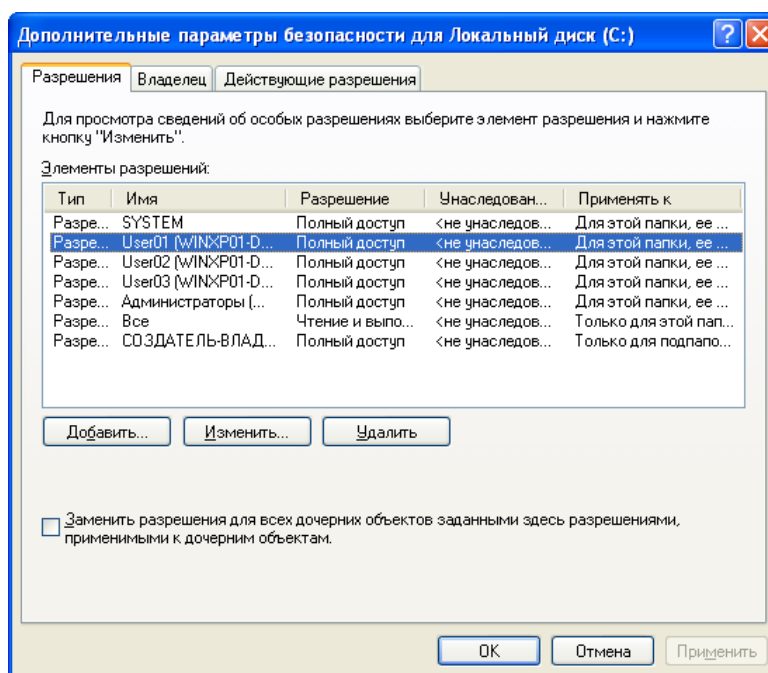


Рисунок 35 – Задание дополнительных параметров прав доступа

В появившемся диалоговом окне (см. рисунок 36) установить способ наследования разрешений, указав для параметра «Применять:» значение «Для этой папки, ее подпапок и файлов».

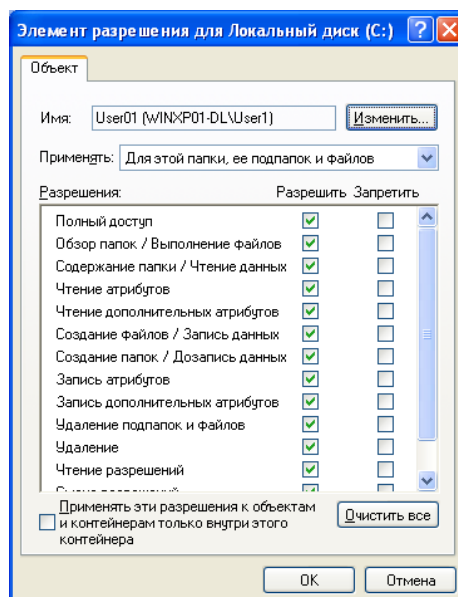


Рисунок 36 – Установка способа наследования прав доступа

Использование консоли DeviceLock Service Settings Editor для настройки сервиса DeviceLock.

В список администраторов сервиса DeviceLock, установленного на компьютере WinXP01-DL, добавить учетную запись локального администратора компьютера, установив для него право на изменение. Затем в подразделе «Разрешения» для устройств выбрать DVD\CD-ROM и добавить в список контроля доступа учетную запись локального пользователя User1 компьютера WinXP01-DL, установив для него разрешение только на чтение. На компьютере WinXP01-DL осуществить вход, используя учетную запись локального пользователя User1. Подключить к ВМ образ оптического диска и выполнить попытку доступа к оптическому диску. Доступ для локального пользователя User1 должен быть разрешен. Завершить сеанс работы пользователя User1.

Осуществить вход на компьютере WinXP01-DL, используя учетную запись локального администратора. Запустить на компьютере WinXP01-DL консоль управления DeviceLock Management Console и выполнить подключение к сервису DeviceLock, установленному на компьютере WinXP01-DL. При выборе компьютера указать локальное подключение. После подключения перейти в раздел «Устройства», подраздел «Разрешения». В правой части окна

консоли отобразится список устройств. Выбрать DVD\CD-ROM щелкнув один раз правой мыши и в контекстном меню выбрать команду «Разрешения». В списке контроля доступа выбрать учетную запись локального пользователя User1 и отключить установленное для него разрешение на чтение. Применить сделанные настройки.

Затем на контроллере домена W2K3-DL осуществить вход, используя учетную запись доменного администратора, запустить консоль управления DeviceLock Management Console и выполнить подключение к компьютеру WinXP01-DL. Перейти в подраздел «Разрешения» раздела параметров «Устройства» и для устройства DVD\CD-ROM проверить список контроля доступа. Для локального пользователя User1 компьютера WinXP01-DL разрешение на чтение должно быть отключено. На компьютере WinXP01-DL осуществить вход, используя учетную запись локального пользователя User1. Выполнить попытку доступа к DVD\CD-ROM. Доступ должен быть запрещен.

Затем на контроллере домена W2K3-DL осуществить вход, используя учетную запись доменного администратора, запустить консоль управления DeviceLock Management Console и выполнить подключение к компьютеру WinXP01-DL. Для локального администратора компьютера WinXP01-DL установить право только чтение. На компьютере WinXP01-DL осуществить вход, используя учетную запись локального администратора. Подключиться к сервису DeviceLock и выполнить попытку изменить разрешения для локального пользователя User1. Изменение прав доступа будет заблокировано.

На компьютере WinXP01-DL завершить сеанс работы локального администратора и осуществить вход, используя учетную запись доменного администратора, запустить консоль управления DeviceLock Management Console и выполнить подключение к сервису DeviceLock. При подключении выбрать локальное подключение к компьютеру WinXP01-DL. Проверить текущие настройки разрешений для DVD\CD-ROM и отразить их в виде снимка экрана.

Затем запустить консоль DeviceLock Service Settings Editor (см. рисунок 37).

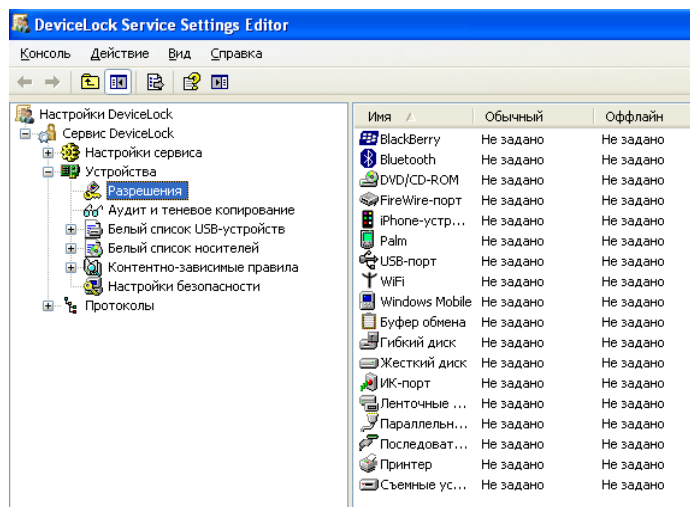


Рисунок 37 – Консоль DeviceLock Service Settings Editor

Выбрать подраздел «Разрешения» в разделе «Устройства». В правой части отобразится список всех устройств, которые поддерживает DeviceLock. Выбрать DVD\CD-ROM щелкнув правой клавишей мыши и в контекстном меню выбрать команду «Установить разрешения» (см. рисунок 38).

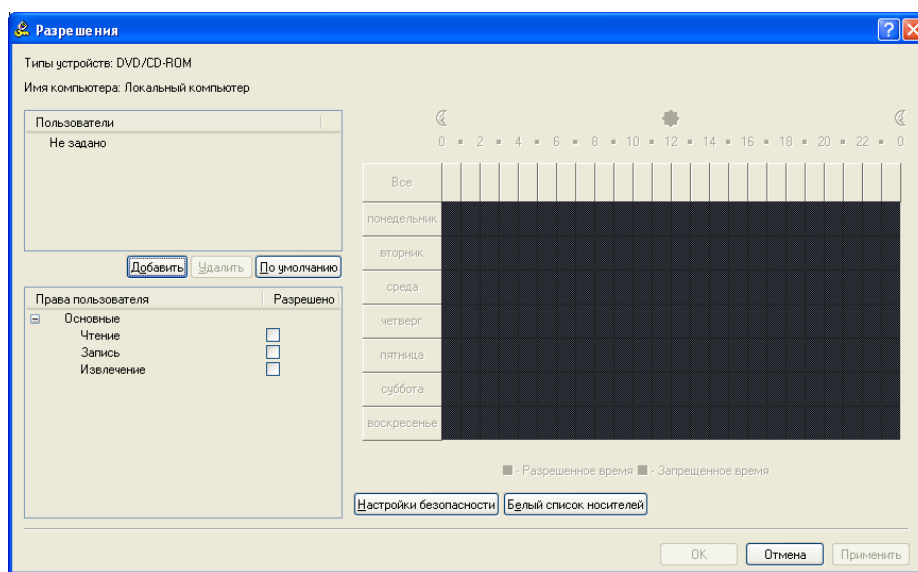


Рисунок 38 – Список контроля доступа для DVD\CD-ROM в консоли DeviceLock Service Settings Editor

Добавить в список контроля доступа учетные записи локального пользователя User1 и локального администратора. При добавлении учетных записей в диалоговом окне «Выбор: Пользователи или группы» изменить размещение базы данных учетных записей, нажав кнопку «Размещение». В

окне запроса пароля доменного администратора нажать кнопку «Отмена». В диалоговом окне «Размещение» выбрать компьютер WinXP01-DL. Для отображения списка учетных записей нажать кнопки «Дополнительно» затем «Поиск». Выбрать учетные записи локального пользователя User1 и локального администратора. Для каждого пользователя установить разрешение только на чтение. Сохранить сделанные настройки. Затем установить разрешения на доступ к жесткому диску для пользователя User1, разрешив чтение и запись, отключив форматирование. Настроить аудит и теневое копирование для DVD\CD-ROM, включив в список контроля учетные записи локального пользователя User1 и локального администратора. Включить аудит успехов и аудит отказов, а также аудит чтения и записи для всех пользователей. Результаты настроек разрешений для DVD\CD-ROM и жесткого диска, а также аудита, отразить в виде снимков экрана.

Установленные настройки сервиса DeviceLock необходимо сохранить в файл настроек. Для сохранения сделанных настроек необходимо в окне консоли DeviceLock Service Settings Editor выбрать сервис DeviceLock щелкнув один раз правой клавишей мыши. В контекстном меню выбрать команду «Сохранить настройки сервиса» (см. рисунок 39).

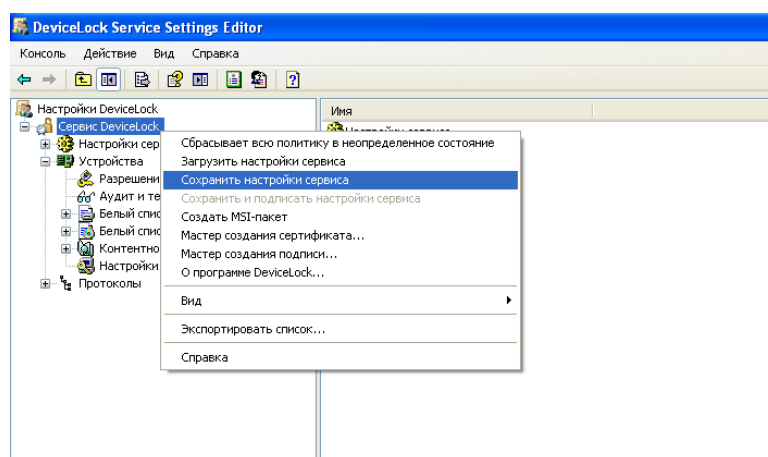


Рисунок 39 – Сохранение настроек в файл настроек сервиса DeviceLock

В диалоговом окне сохранения файла необходимо ввести имя файла WinXP01_Service_Settings и сохранить его в каталог Settings на диске C:\ компьютера WinXP01-DL. Расширение файла – dls. После сохранения файла

настроить для каталога Settings возможность общего доступа (в диалоговом окне свойств каталога, на вкладке «Доступ»). Разрешения и другие параметры доступа оставить без изменения. Закрывать консоль DeviceLock Service Settings и завершить сеанс работы доменного администратора на компьютере WinXP01-DL.

На контроллере домена W2K3-DL открыть консоль управления DeviceLock Management Console. Выполнить подключение к сервису DeviceLock, установленному на компьютере WinXP01-DL. Перейти в подраздел «Администраторы DeviceLock» раздела «Настройки сервиса». Для локального администратора компьютера WinXP01-DL установить право изменения настроек сервиса (привилегия «Изменение»). Затем необходимо применить настройки сервиса DeviceLock, сохраненные в файл настроек WinXP01_Service_Settings.dls. Для применения настроек необходимо щелкнуть один раз правой клавишей мыши по строке «Сервис DeviceLock» и в контекстном меню выбрать команду «Загрузить настройки сервиса» (см. рисунок 40).

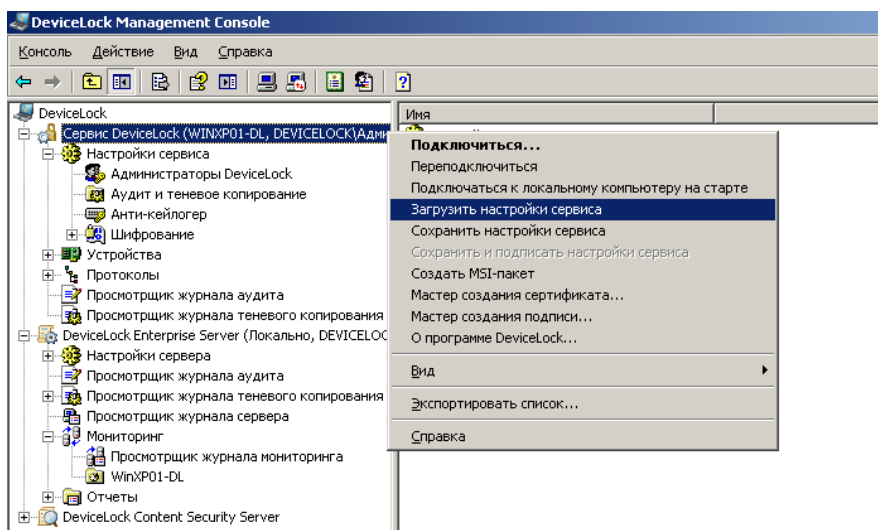


Рисунок 40 – Загрузка настроек сервиса DeviceLock из файла настроек

В диалоговом окне открытия файла выбрать раздел «Сетевое окружение» и далее – «Вся сеть», «Microsoft Windows Network», «Devicelock». В списке компьютеров домена выбрать компьютер WinXP01-DL и открыть каталог Settings с установленным общим доступом. Выбрать файл настроек

WinXP01_Service_Settings.dls. После выполнения команды открытия файла будет выдан запрос на подтверждение выполнения операции загрузки настроек из файла (см. рисунок 41).

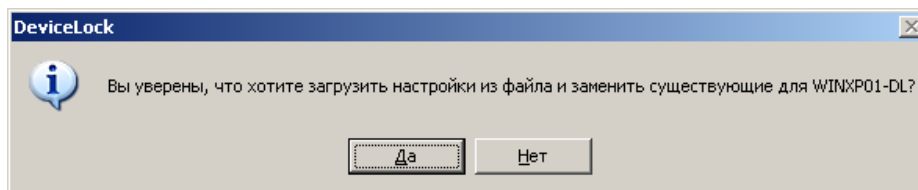


Рисунок 41 – Запрос подтверждения загрузки параметров сервиса DeviceLock из файла настроек

После подтверждения загрузки настроек будут применены настройки, сохраненные в файле. После применения настроек проверить список контроля доступа для DVD\CD-ROM и жесткого диска и разрешения на доступ к устройствам. Они должны соответствовать настройкам, установленным на компьютере WinXP01-DL локально, с использованием консоли DeviceLock Service Settings Editor. Также проверить параметры аудита и теневого копирования для DVD\CD-ROM. Отобразить примененные настройки в виде снимка экрана.

После загрузки настроек из файла осуществить вход на компьютере WinXP01-DL, с использованием учетной записи локального администратора, открыть консоль управления DeviceLock Management Console. Выполнить подключение к сервису DeviceLock, установленному на компьютере WinXP01-DL (локально). Открыть список контроля доступа для DVD\CD-ROM и отключить все разрешения для пользователя User1. Сохранить сделанные изменения. Завершить сеанс работы локального администратора. Осуществить вход на компьютере WinXP01-DL, с использованием учетной записи локального пользователя User1. Подключить образ оптического диска и выполнить попытку доступа к нему пользователя User1. Доступ должен быть запрещен. Результат попытки доступа пользователя User1 к DVD\CD-ROM отразить в виде снимка экрана. Завершить сеанс работы пользователя User1.

Создание задач мониторинга.

На контроллере домена W2K3-DL открыть консоль управления DeviceLock Management Console. Выполнить подключение к сервису DeviceLock, установленному на компьютере WinXP01-DL. Затем подключиться к серверу DeviceLock Enterprise Server, указав локальное подключение. Перейти в раздел «Мониторинг». В этом разделе будет отображен подраздел «Просмотрщик журнала мониторинга». Для защиты агента DeviceLock от санкционированного отключения необходимо создать задачу мониторинга состояния агента. Для создания задачи мониторинга необходимо щелкнуть правой клавишей мыши по названию раздела «Мониторинг» и выбрать в контекстном меню команду «Создать задачу» (см. рисунок 42).

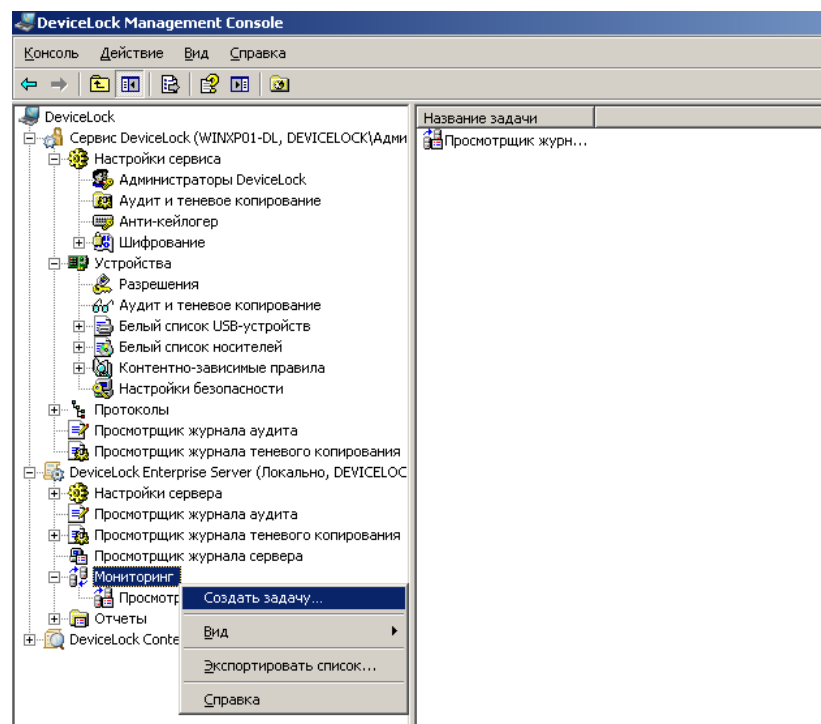


Рисунок 42 – Команда создания задачи мониторинга

После выбора команды на экране будет отображено диалоговое окно создания задачи мониторинга (см. рисунок 43).

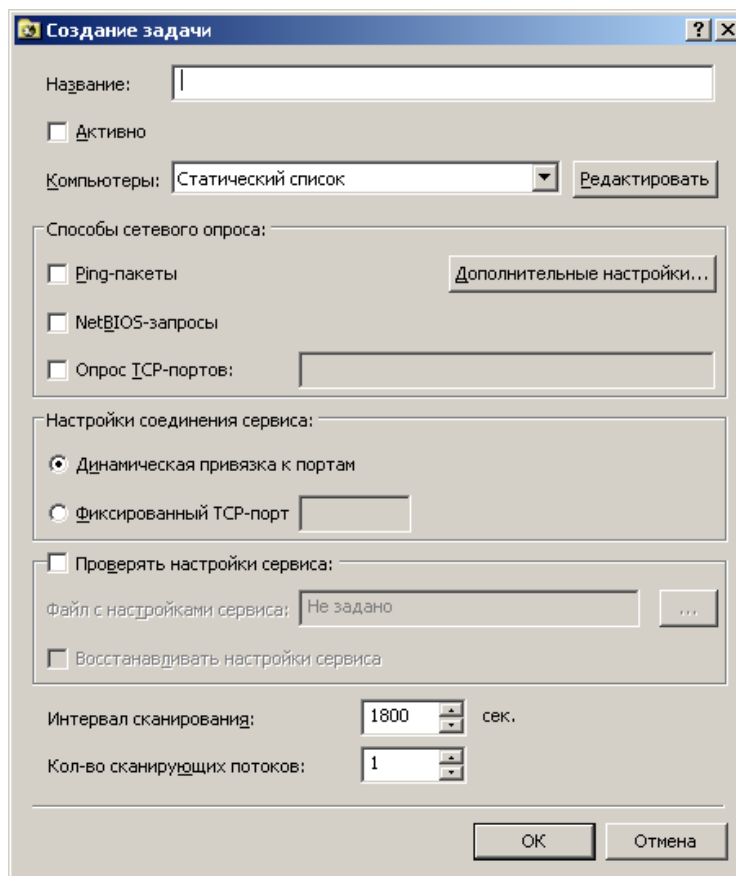


Рисунок 43 – Диалоговое окно настройки задачи мониторинга

В поле «Название» необходимо указать название создаваемой задачи. Параметр «Активно» необходимо включить для того, чтобы DeviceLock Enterprise Server выполнял созданную задачу. В поле «Компьютеры» необходимо указать значение «Статический список» для включения компьютера домена в список объектов задачи по его имени. В список контролируемых компьютеров добавить компьютер WinXP01-DL. Для добавления компьютера нажать кнопку «Редактировать». В диалоговом окне «Редактирование статического списка» установить для параметра «Выбор компьютеров» значение «Компьютеры». В разделе «Microsoft Windows Network» открыть список компьютеров домена DeviceLock и выбрать компьютер WinXP01-DL. Затем нажать кнопку добавления компьютера в список выбранных компьютеров. В этом списке также отметить выбранный компьютер (см. рисунок 44).

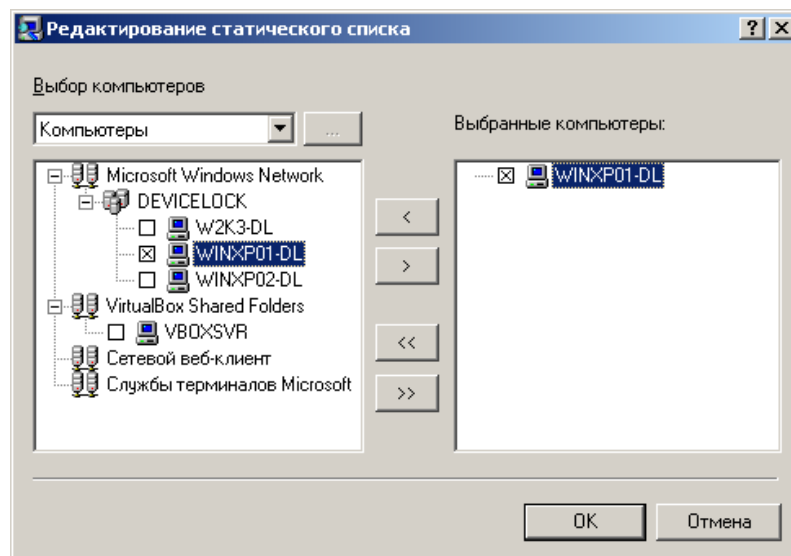


Рисунок 44 – Выбор компьютера WinXP01-DL для построения отчета

После выбора компьютера нажать кнопку ОК.

В разделе параметров «Методы сетевого опроса» включить способы опроса Ping-пакеты и NetBIOS-запросы. Затем нажать кнопку «Дополнительные настройки» и в диалоговом окне настроек указать для параметра «Количество повторов» значение 2, для параметра «Ожидание ответа» значение оставить без изменения.

В разделе «Настройки соединения сервиса» оставить значение «Динамическая привязка к портам».

Установить параметр «Проверять настройки сервиса» для контроля неизменности настроек сервиса DeviceLock на контролируемых компьютерах. Установить параметр «Восстанавливать настройки сервиса» для включения сопоставления текущих настроек с эталонными (хранящимися в файле конфигурации) и восстановления настроек сервиса DeviceLock при их изменении. Далее необходимо указать файл, содержащий эталонные настройки. Для этого надо щелкнуть кнопку открытия диалогового окна выбора файла рядом со строкой «Файл с настройками сервиса» и в диалоговом окне перейти в сетевой каталог Settings (с общим доступом), расположенный на компьютере WinXP01-DL. Выбрать файл WinXP01_Service_Settings.dls. После выбора в строке отобразится полный путь к этому файлу. Если параметры «Проверять

настройки сервиса», «Восстанавливать настройки сервиса», а также файл настроек не будут установлены, то будет проверяться только доступность контролируемого компьютера и работа сервиса DeviceLock на нем.

Параметры «Интервал сканирования» и «Количество сканирующих потоков» оставить без изменения. После настройки результат создания задачи мониторинга отобразить в отчете в виде снимка экрана. Для завершения создания задачи нажать ОК. После создания задачи ее имя отобразится в разделе «Мониторинг» для DeviceLock Enterprise Server. При выборе задачи в правой части окна консоли DeviceLock Management Console отобразится состояние задачи: имя контролируемого компьютера, его статус, время последнего сканирования и др.

После создания задачи мониторинга для сервиса DeviceLock, установленного на компьютере WinXP01-DL, необходимо в консоли управления DeviceLock Management Console подключиться к сервису DeviceLock. Затем загрузить настройки сервиса из файла WinXP01_Service_Settings.dls. После загрузки настроек необходимо проверить применение настроек просмотрев список контроля доступа для DVD\CD-ROM и жесткого диска, а также проверить настройки аудита и теневого копирования для DVD\CD-ROM. Проверить установку разрешения на изменение настроек для локального администратора компьютера WinXP01-DL. Проверить статус компьютера WinXP01-DL в задаче мониторинга. Иконка должна быть зеленого цвета. Результат проверки отразить в виде снимка экрана.

Выполнить вход на компьютере WinXP01-DL, используя учетную запись локального администратора. Запустить консоль управления DeviceLock Management Console и подключиться к сервису DeviceLock локально. Просмотреть список контроля доступа для DVD\CD-ROM. Настройки должны соответствовать настройкам, сохраненным в файле, и разрешать доступ на чтение к DVD\CD-ROM для пользователя User1 и локального администратора. Изменить установленные разрешения на доступ к DVD\CD-ROM для

пользователя User1 и локального администратора. Изменения отразить в виде снимка экрана. Сохранить сделанные изменения.

На контроллере домена W2K3-DL открыть консоль управления DeviceLock Management Console. Проверить подключение к сервису DeviceLock, установленному на компьютере WinXP01-DL. Проверить подключение к серверу DeviceLock Enterprise Server. Перейти в раздел «Мониторинг». Выбрать созданную задачу мониторинга для компьютера WinXP01-DL, щелкнув правой клавишей мыши по ее названию и в контекстном меню выбрать команду «Запустить сейчас» (см. рисунок 45).

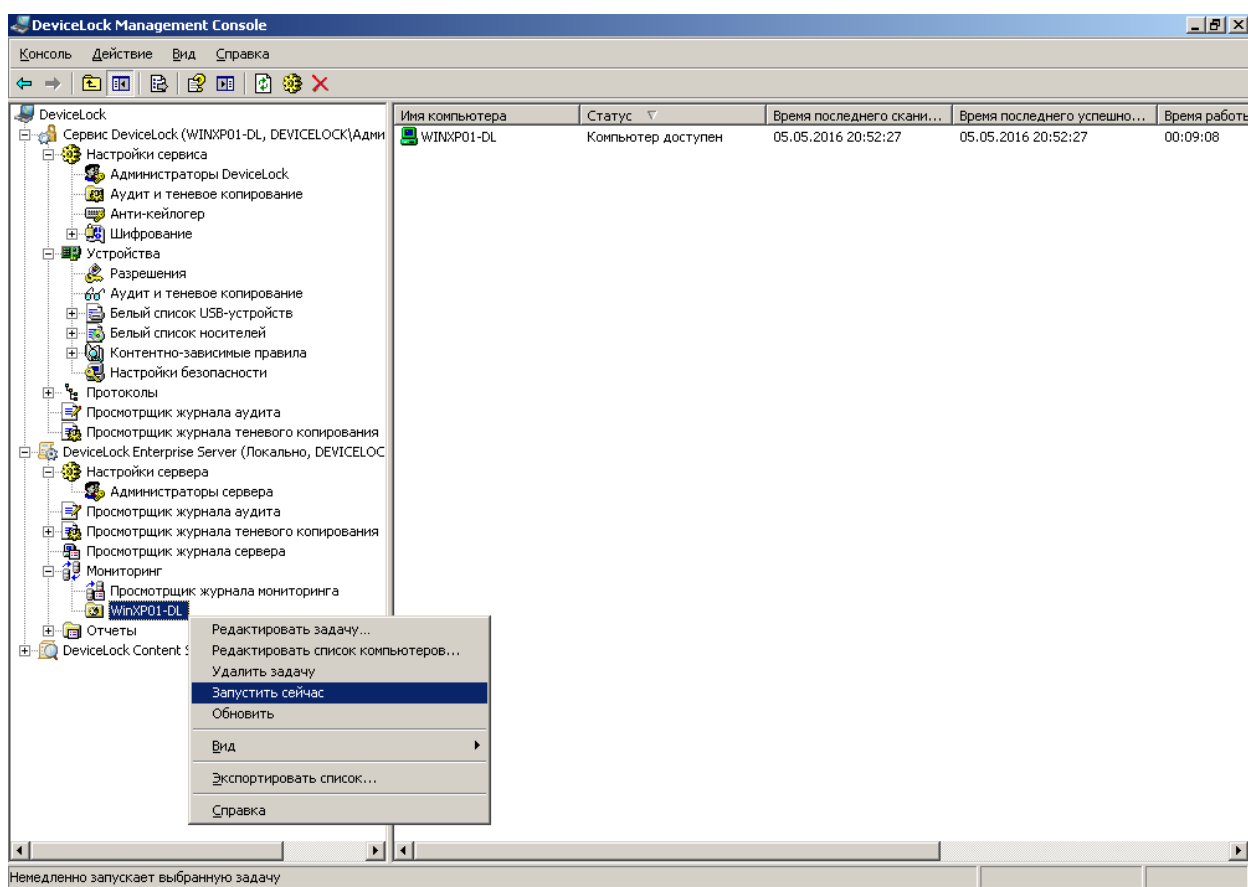


Рисунок 45 – Запуск задачи мониторинга

После запуска задачи мониторинга изменится иконка контролируемого компьютера, на которой отобразится восклицательный знак. Перейти в подраздел «Просмотрщик журнала мониторинга» и найти записи о событиях запуска задачи и событиях контроля настроек сервиса DeviceLock. Сохранить записи в файл и включить их в отчет. Затем еще раз запустить задачу мониторинга на выполнение. Иконка компьютера должна измениться – будет

удален восклицательный знак. Изменения статуса компьютера отразить в виде снимков экрана.

Затем проверить изменение настроек на компьютере WinXP01-DL. После запуска задачи мониторинга они должны быть восстановлены из файла. Для проверки восстановления настроек в консоли управления DeviceLock Management Console в разделе «Устройства» перейти в подраздел «Разрешения» и выбрать DVD\CD-ROM. Открыть список контроля доступа и проверить восстановление настроек. Результат отразить в виде снимка экрана.

После выполнения проверки восстановления настроек сервиса DeviceLock на компьютере WinXP01-DL проверить возможность отключения сервиса DeviceLock, остановки службы, удаления и переименования файла агента. Запустить диспетчер задач и в списке процессов найти процесс DLService.exe, запущенный от имени пользователя SYSTEM. Выполнить попытку завершить процесс. Результат представить в виде снимка экрана.

Затем в Панели управления на компьютере WinXP01-DL открыть раздел «Администрирование» и запустить консоль «Службы». Найти службу DeviceLock Service в списке локальных служб и выполнить попытку ее остановки, изменив тип запуска. После проверки возможности остановки службы DeviceLock 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-DL подключиться к серверу DeviceLock Enterprise Server и перейти к подразделу «Просмотрщик журнала мониторинга». Найти все события, связанные с работой созданной задачи мониторинга – запуск и завершение задачи, проверка и восстановление настроек сервиса DeviceLock, установленного на компьютере WinXP01-DL, а также сообщения об изменениях настроек. Примеры записей о событиях из журнала мониторинга включить в отчет о выполнении практического задания.

5 Порядок выполнения лабораторной работы по изучению мониторинга и защиты агентов, реализуемой в программном комплексе Zecurion Zlock (Device Control)

5.1 Цель и задание к лабораторной работе

Цель работы – получить навыки создания задач мониторинга и применение их для защиты сервиса Zecurion Lock от несанкционированного изменения настроек ,отключения, удаления.

Задание на лабораторную работу включает в себя:

- настройку аудита и теневого копирования для сервиса Zecurion Lock;
- настройку политики безопасности домена и контроллера домена при регистрации событий;
- создание учётных записей доменных и локальных пользователей;
- создание задач мониторинга;
- имитацию нарушений работы агентов;
- формирование отчётов по журналу регистрации событий;
- вывод по выполненной работе.

5.2 Порядок выполнения лабораторной работы

Включение и настройка аудита.

Для начала работы с клиентской частью необходимо установить соединение с удалённым компьютером. Для этого необходимо щёлкнуть правой кнопкой мыши на нужном компьютере в группе Zlock и выполнить команду меню "Установить соединение", после чего будет создана и применена к этому компьютеру политика по умолчанию (рисунок 46)

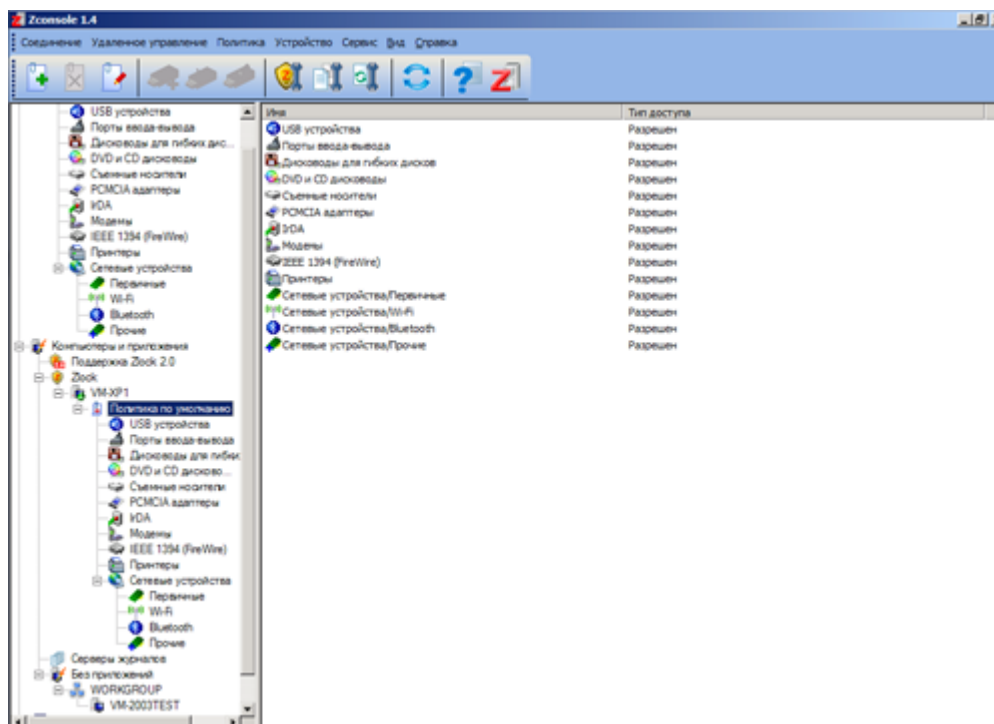


Рисунок 46 – Установка политики по умолчанию

Перейти в закладку Расписание (рисунок 47). Задать ежедневное расписание применения политики с 7:59:59 до 19:00.

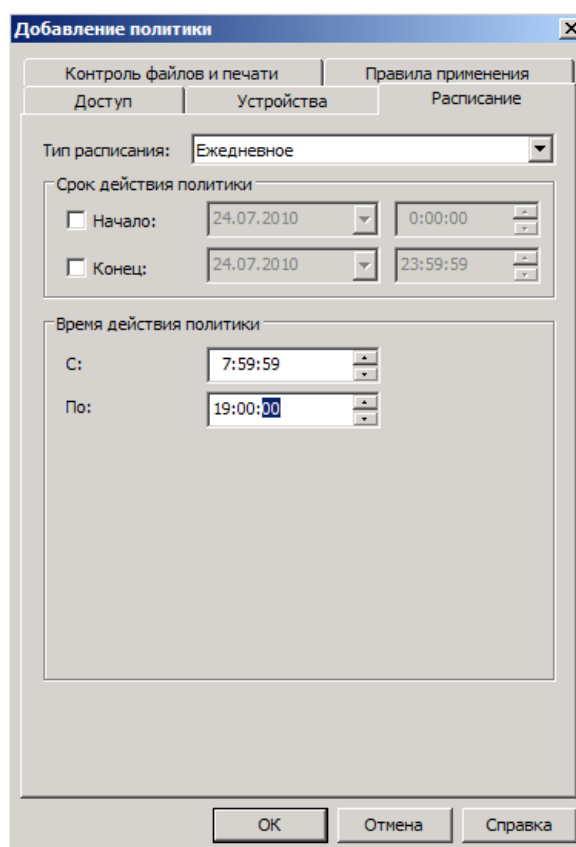


Рисунок 47 – Создание расписания действия политики

Перейти в закладку «Правила применения» (рисунок 48). Политика может применяться в зависимости от доступности домена – домен доступен локально, домен доступен через VPN, домен не доступен. Следует указать, при каком состоянии домена политика будет активна. Тут же отображается текущее состояние рабочей станции.

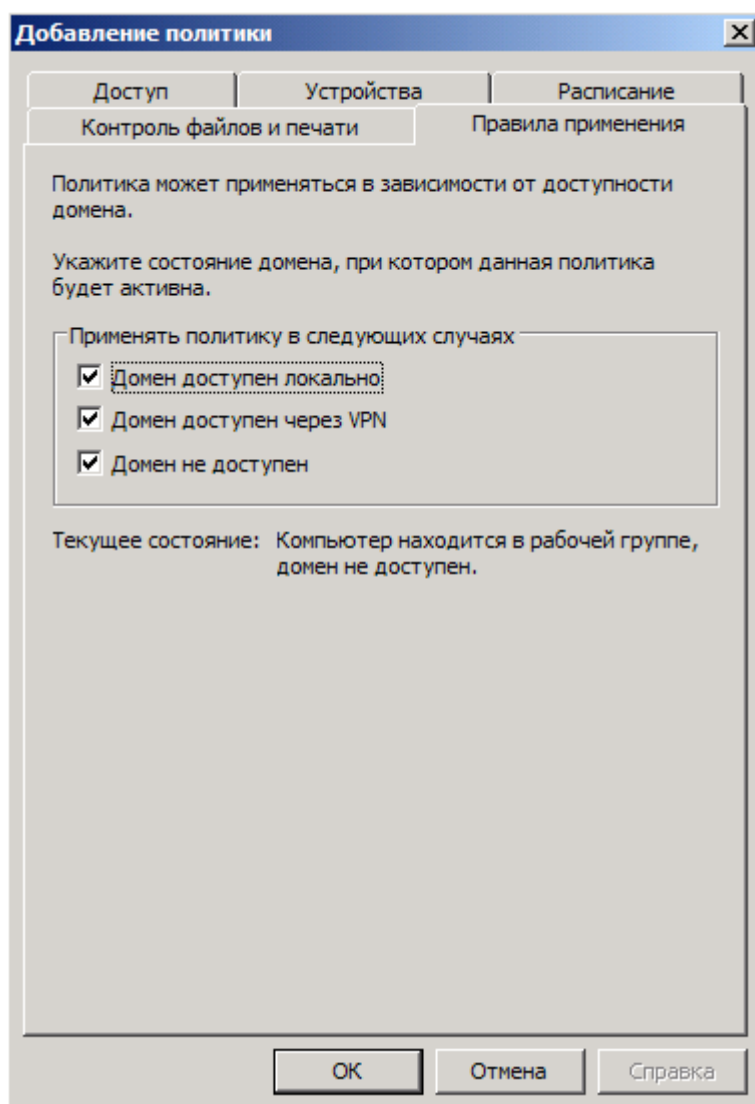


Рисунок 48 – Правила применения политики

Перейти в Закладку «Контроль файлов и печати». Можно настроить журналирование и обработку файловых операций, а также функцию теневого копирования файлов.

Условия, при которых доступны эти опции, видны на рисунке 49.

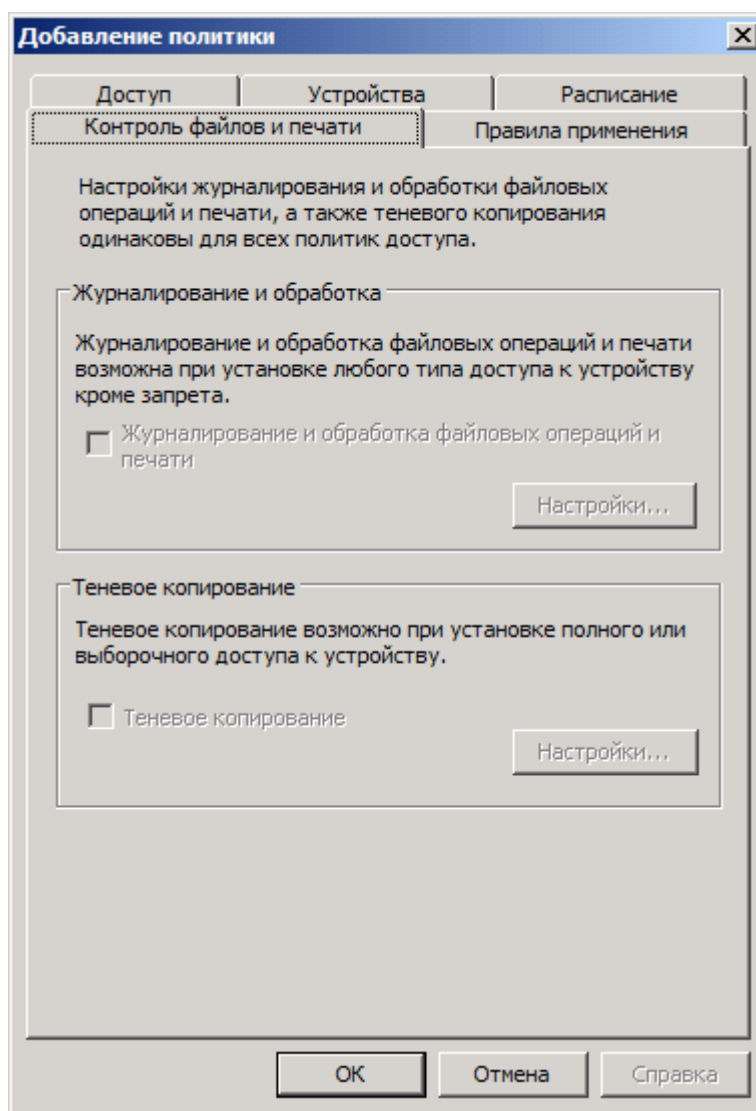


Рисунок 49 – Контроль файлов и печати

Настройку теневого копирования можно произвести, открыв меню Сервис и выполнив там команду Теневое Копирование (рисунок 50).

На вкладке «Политики» отмечаются политики, для которых производится теневое копирование (рисунок 51).

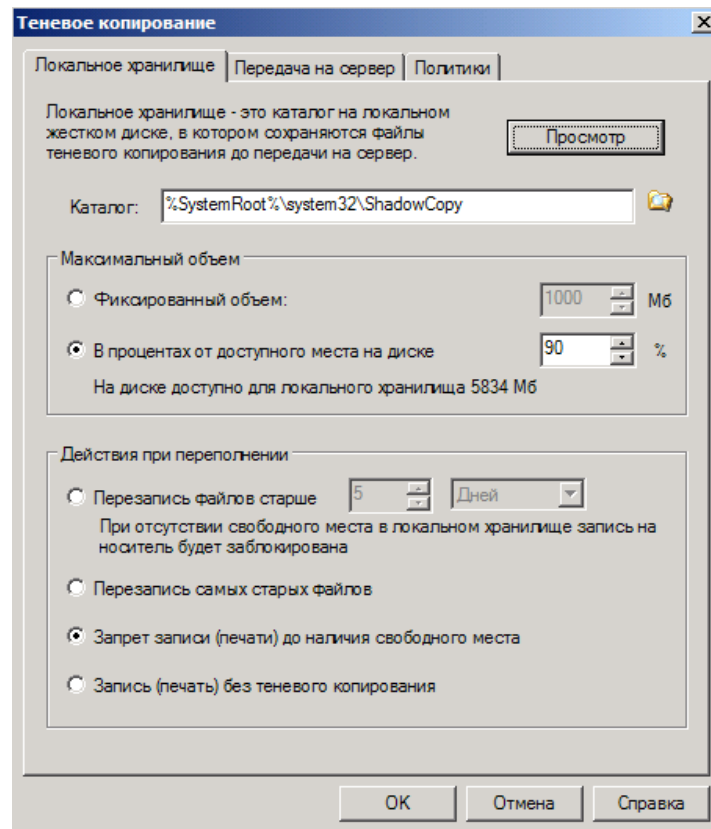


Рисунок 50 – Настройка теневого копирования

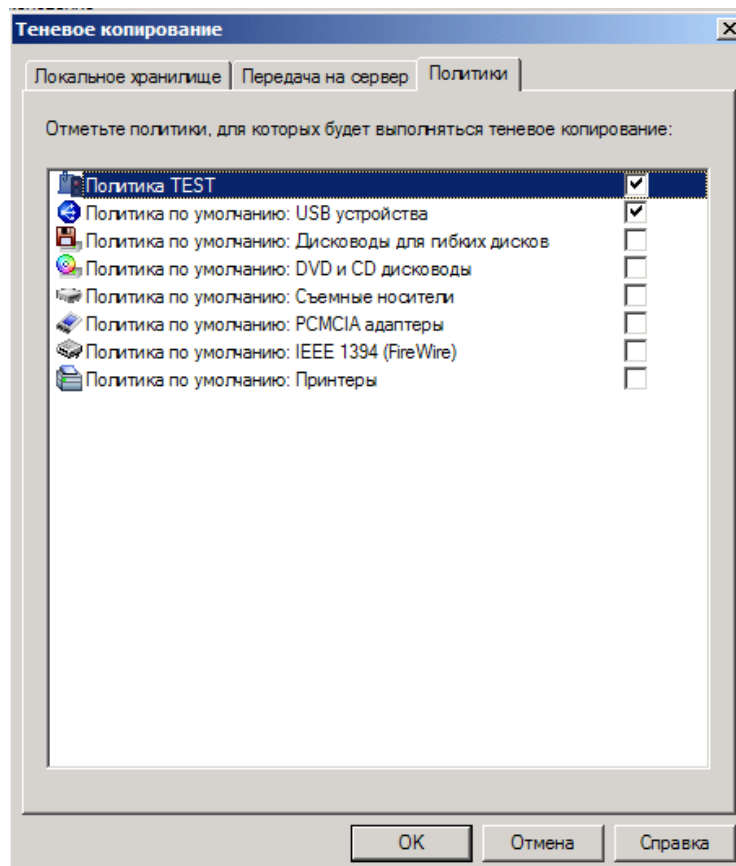


Рисунок 51 – Настройка теневого копирования

Перейти на вкладку «Хранение журналов». При получении информации от клиентской части системы сервер журналов может сохранять ее на локальном компьютере в XML-файле либо в базе данных на SQL-сервере.

Перейти на вкладку «Доступ», назначить Администратору все права, пользователям – запретить (см. рисунок 52).

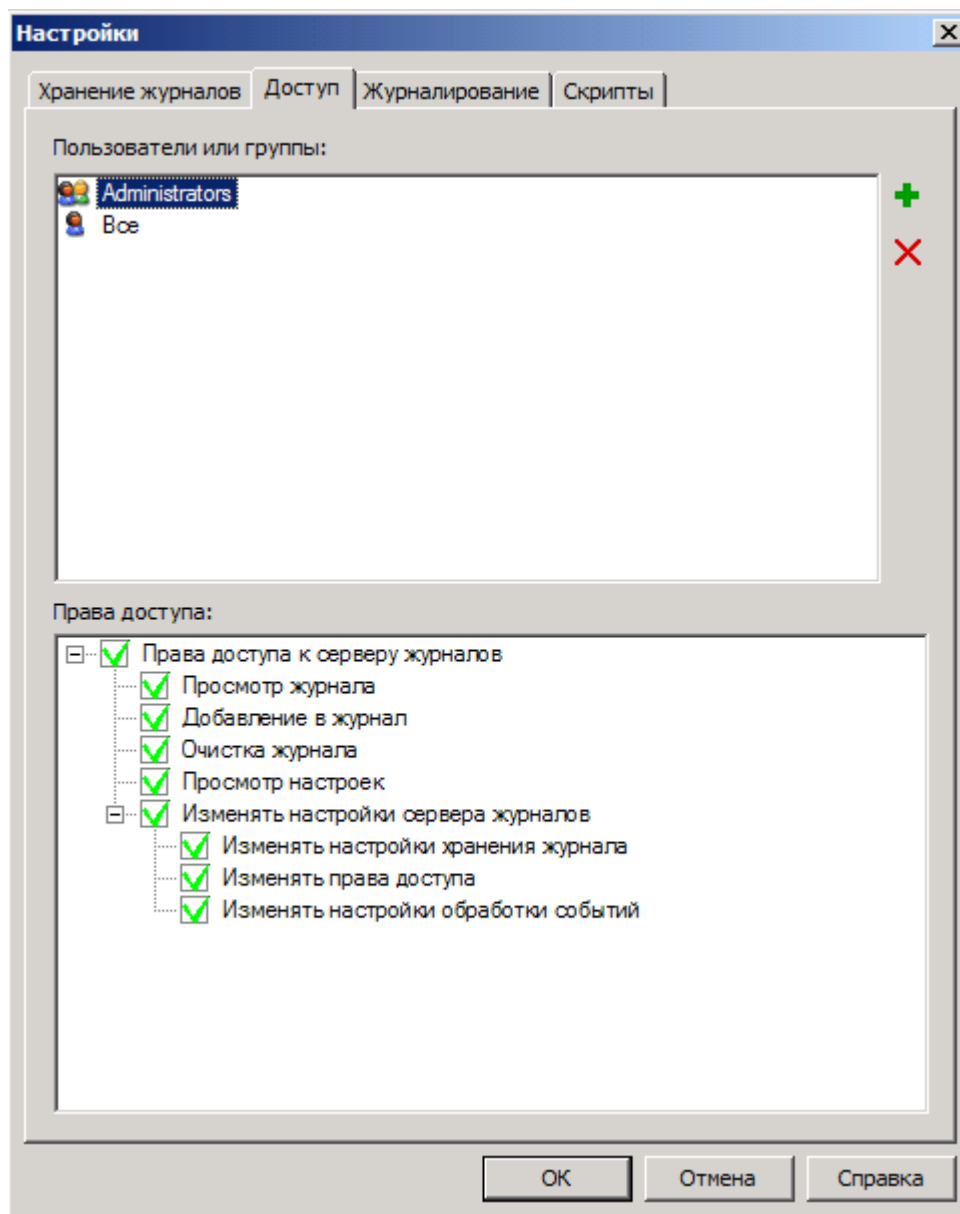


Рисунок 52 – Настройка прав доступа к сервису журналов

Создание учетных записей пользователей

Создать учетную запись локального пользователя на компьютере WinXP01-ZL (User01). 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. При создании учетной записи установить следующие параметры учетных записей (см. рисунок 53):

- «Запретить смену пароля пользователем»;
- «Срок действия пароля не ограничен».

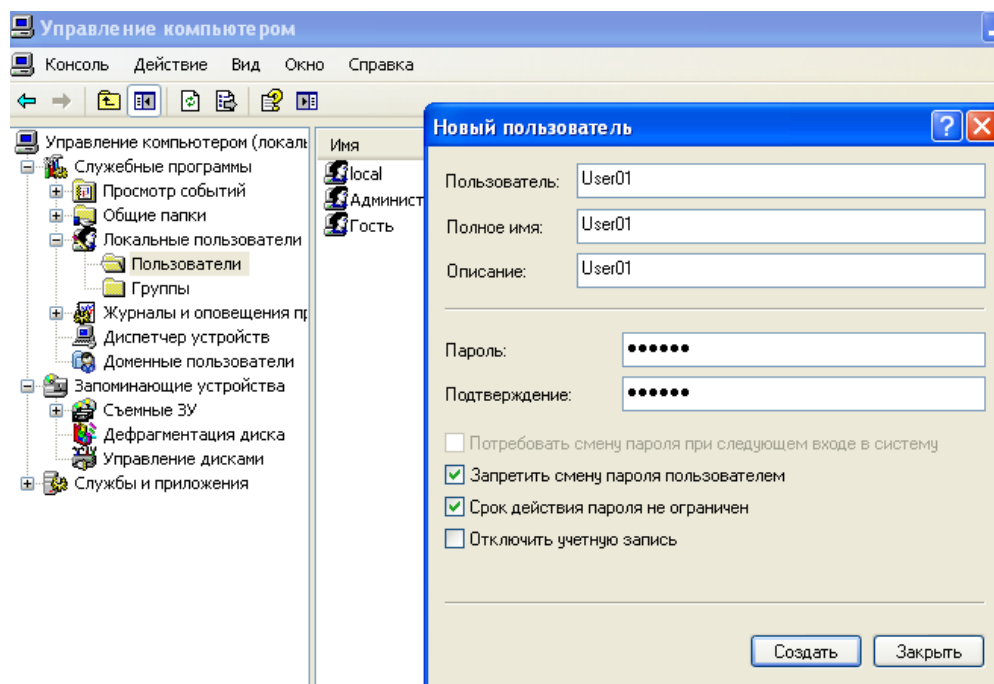


Рисунок 53 – Создание учетной записи пользователя

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.

Настройка прав доступа к жесткому диску компьютера WinXP01-ZL

Предварительно для выполнения практического задания необходимо настроить права доступа локального пользователя к жесткому диску компьютера WinXP01-ZL. Для этого осуществить вход, используя учетную запись администратора. Открыть диалоговое окно свойств диска C:\ компьютера WinXP01-ZL и перейти на вкладку «Безопасность». Добавить в список контроля доступа учетную запись локального пользователя User01. Предоставить полный доступ к диску C:\ компьютера WinXP01-ZL (см. рисунок 54).

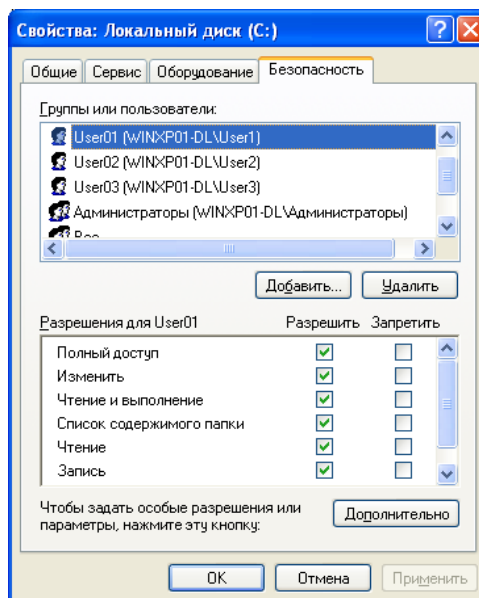


Рисунок 54 – Назначение разрешений для локальных пользователей

Затем в диалоговом окне свойств на вкладке «Безопасность» (см. рисунок 8) нажать кнопку «Дополнительно», в диалоговом выбрать учетную запись пользователя User01 и нажать кнопку «Изменить» (см. рисунок 55).

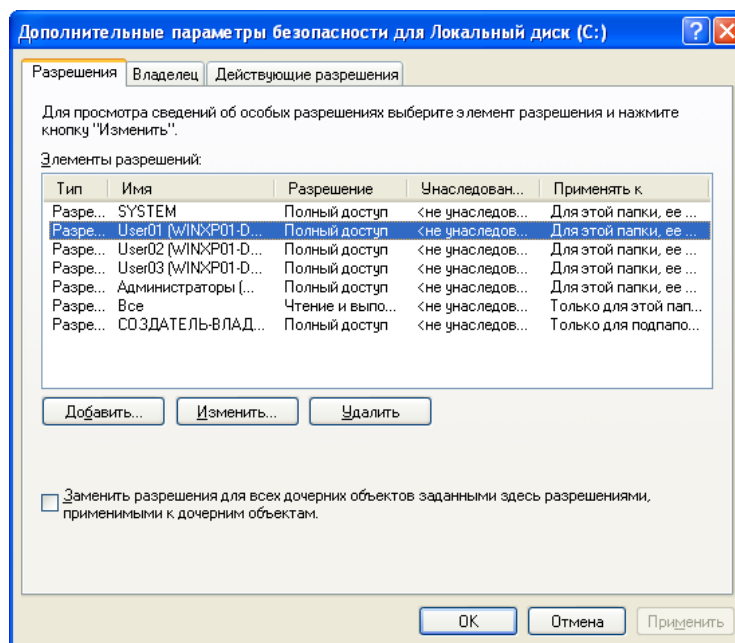


Рисунок 55 – Задание дополнительных параметров прав доступа

В появившемся диалоговом окне (см. рисунок 56) установить способ наследования разрешений, указав для параметра «Применять:» значение «Для этой папки, ее подпапок и файлов».

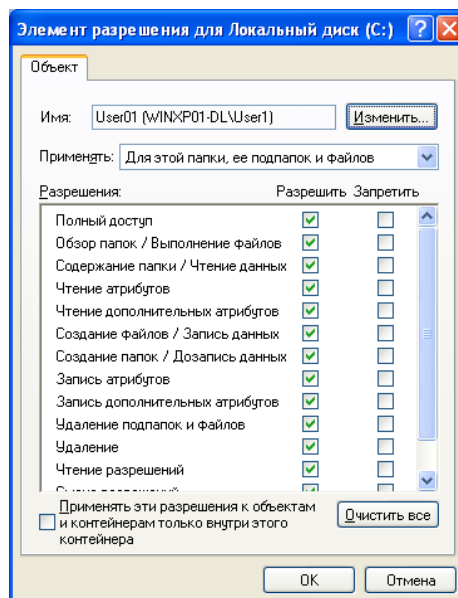


Рисунок 56 – Установка способа наследования прав доступа

Создание задач мониторинга. Система Zlock позволяет вести мониторинг состояния удаленных рабочих станций для выявления каких-либо несанкционированных действий с системой. Через определенные промежутки времени специальный модуль службы Zservice, установленный совместно с консолью администратора, производит опрос рабочих станций.

Для того чтобы включить мониторинг рабочей станции, группы, или домена надо открыть в дереве пункт «Компьютеры и приложения» и выбрать необходимый элемент дерева – рабочую станцию, группу либо домен. Далее выбрать пункт «Свойства соединения» в меню «Соединение» и перейти на вкладку «Мониторинг Zlock» (рисунок 57).

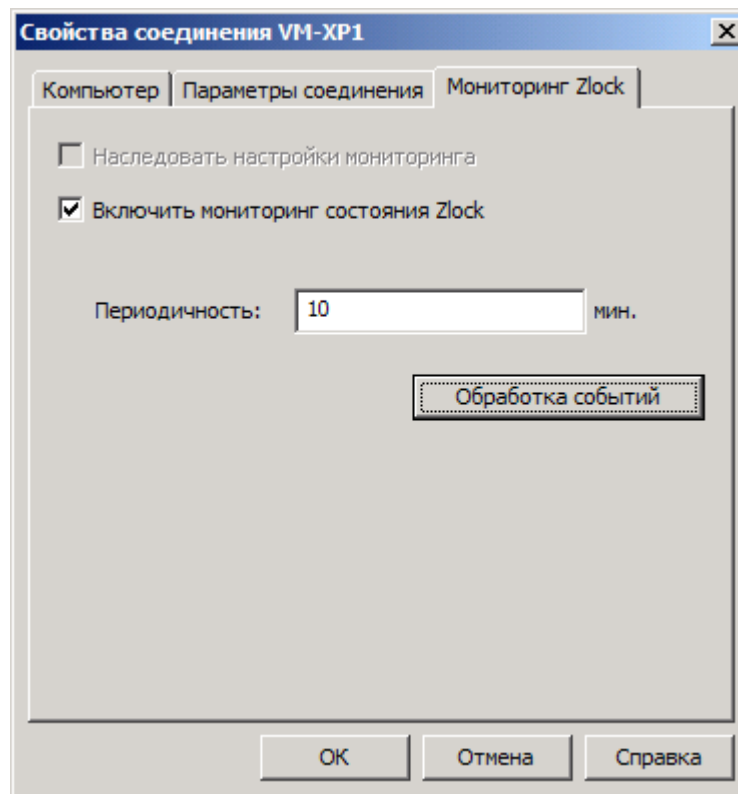


Рисунок 57 – Включение мониторинга

Затем в Панели управления на компьютере WinXP01-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 Lock 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.

6 Описание порядка выполнения лабораторных работ, входящих в лабораторный практикум и результатов выполнения лабораторных работ

Выполнение каждой лабораторной работы, входящей в состав практикума, включает в себя следующие действия:

а) ознакомление с изучаемой системой контроля и предотвращения утечек информации;

б) выполнение задания к лабораторной работе (см. разделы 4, 5);

в) подготовка результатов выполнения лабораторной работы для включения в отчёт о выполнении лабораторной работы. Результаты включают в себя :

— снимки экрана;

— отчёты по журналам регистрации событий.

г) подготовка отчёта о выполнении лабораторной работы. Оформление отчёта о выполнении лабораторной работы в соответствии с требованиями, приведенными в соответствии с разделом 7;

д) защита отчёта, заключающаяся в ответе на контрольные вопросы по теоретическому материалу и заданию к лабораторной работе.

7 Разработка контрольных экземпляров отчетов о выполнении лабораторных работ, входящих в практикум

Результаты выполнения лабораторных работ, входящих в практикум, оформляются в виде отчетов. Содержание выполнения каждой лабораторной работы включает в себя:

- создание снимков экранов;
- записи из журнала событий;
- показ выполнения пунктов задания и отчетов.

Снимки экранов студентам необходимо делать по ходу 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.

Выбранные записи журналов регистрации событий в конце каждой работы экспортируются и после студентам необходимо вставить их в отчет.

Общая структура отчета о выполнении лабораторных работ, а также содержание контрольных экземпляров отчетов приведены в приложении А.

8 Определение порядка контроля выполнения задания к лабораторным работам

Порядок контроля выполнения задания к лабораторным работам, входящим в лабораторный практикум, включает в себя проверку:

- полноты выполнения лабораторной работы;
- соответствия созданных снимков экрана пунктам задания;
- сформированных отчётов.

После выполнения задания к лабораторной работе результаты работы предоставляются для проверки. Предъявляются снимки экранов с указанием того пункта задания, при выполнении которого они формировались. Затем предоставляется сформированный отчёт по журналу регистрации событий, при этом проверяется временная шкала на записях, отображение выполненных действий, достаточность записей о событиях.

После проверки правильности результатов должен быть оформлен отчёт о выполнении задания. До защиты отчёта он также проверяется. Если отчёт выполнен по требованиям, то он допускается к защите, если нет – отправляется на доработку.

Приведённый порядок проверки применяется для контроля выполнения к каждой лабораторной работе.

ЗАКЛЮЧЕНИЕ

В результате дипломного проектирования был разработан лабораторный практикум по изучению функций мониторинга и защиты агентов, реализуемый системами контроля и предотвращения утечек информации, с использованием виртуальных машин, состоящий из двух лабораторных работ. Первая лабораторная работа посвящена изучению и настройке функций мониторинга и защиты агентов, реализуемых системой контроля и предотвращения утечек информации в программном комплексе Device Lock. Вторая лабораторная работа посвящена изучению и настройке функций мониторинга и защиты агентов, реализуемых системой контроля и предотвращения утечек информации в программном комплексе Zecurion Lock

В ходе дипломного проектирования были подготовлены два лабораторных стенда, используемых при выполнении лабораторного практикума, произведено описание систем контроля и предотвращения утечек информации, используемых при проведении лабораторных работ, разработан порядок выполнения задания к лабораторным работам, входящих, в лабораторный практикум, разработаны контрольные экземпляры отчётов о выполнении лабораторных работ, входящих в лабораторный практикум, определена процедура контроля выполнения задания к лабораторным работам.

В первом разделе ВКР был произведен обзор систем контроля по защите информации, реализующих функции мониторинга и защиты агентов..

Во втором разделе ВКР описаны функции мониторинга и защиты агентов, реализуемые системами контроля и предотвращения утечек информации Device Lock и Zecurion Lock.

В третьем разделе было произведено описание подготовки лабораторных стендов, используемых при проведении лабораторных работ.

В четвертом разделе описан порядок выполнения лабораторной работы по изучению функций мониторинга и защиты агентов, реализуемой в программной комплексе DeviceLock DLP Suite.

В пятом разделе описан порядок выполнения лабораторной работы по изучению функций мониторинга и защиты агентов, реализуемой в программной комплексе Zecurion Zlock (Device Control).

В шестом разделе приведено описание выполнения лабораторных работ, входящих в лабораторный практикум и результатов выполнения лабораторных работ..

В седьмом разделе описана разработка контрольных экземпляров отчетов о выполнении лабораторных работ, входящих в лабораторный практикум.

В восьмом разделе определён порядок контроля выполнения задания к лабораторным работам.

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

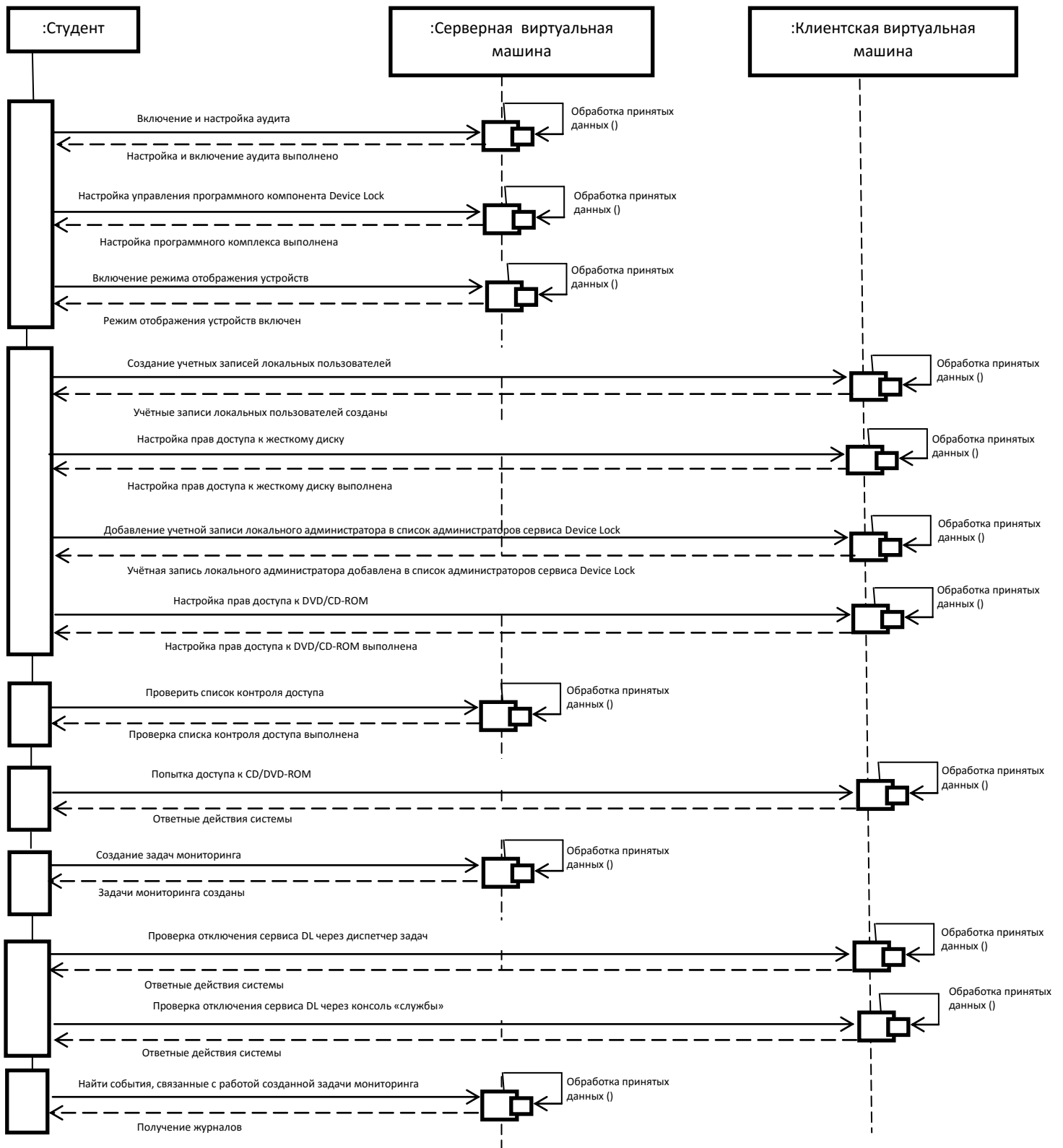
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

- 1 Обзор DLP – систем на мировом и российском рынке[электронный ресурс] - IT – сообщество, Аналитика, Анализ технологий. – 2014. – Режим доступа - https://www.anti-malware.ru/analytics/Technology_Analysis/DLP_market_overview_2014, свободный. – Загл.с экрана.
- 2 Установка Windows Server 2003 [Электронный ресурс] - IT – сообщество, Операционные системы, Windows, Установка Windows Server 2003, 2013. – Режим доступа: <http://perscom.ru/index.php/os/151-windows/780-ustanovka-ws3>, свободный. – Загл.с экрана.
- 3 Компьютерная грамота [Электронный ресурс] – IT – сообщество, Установка операционной системы Windows XP, 2016. – Режим доступа: <http://pc-ramota.com/ustanovka-operacionnoy-sistemy-windows-xp>, свободный. – Загл.с экрана.
- 4 DeviceLock Руководство пользователя Версия продукта 7.1 – 09.08.2011г.
- 5 ZLock Версия 6.0 Система разграничения доступа к ресурсам компьютера. Руководство администратора. 2002-2014 г.
- 6 Как работают DLP – системы [Электронный ресурс] – IT – сообщество, Admin, 2011/ - Режим доступа: <https://xakep.ru/2011/05/04/55604/>, свободный. – Загл.с экрана.
- 7 Предотвращение утечек информации [Электронный ресурс] : Википедия, свободная энциклопедия. – 2016. – Режим доступа: https://ru.wikipedia.org/wiki/Предотвращение_утечек_информации, свободный. – Загл. с экрана.

ПРИЛОЖЕНИЕ А

(обязательное)

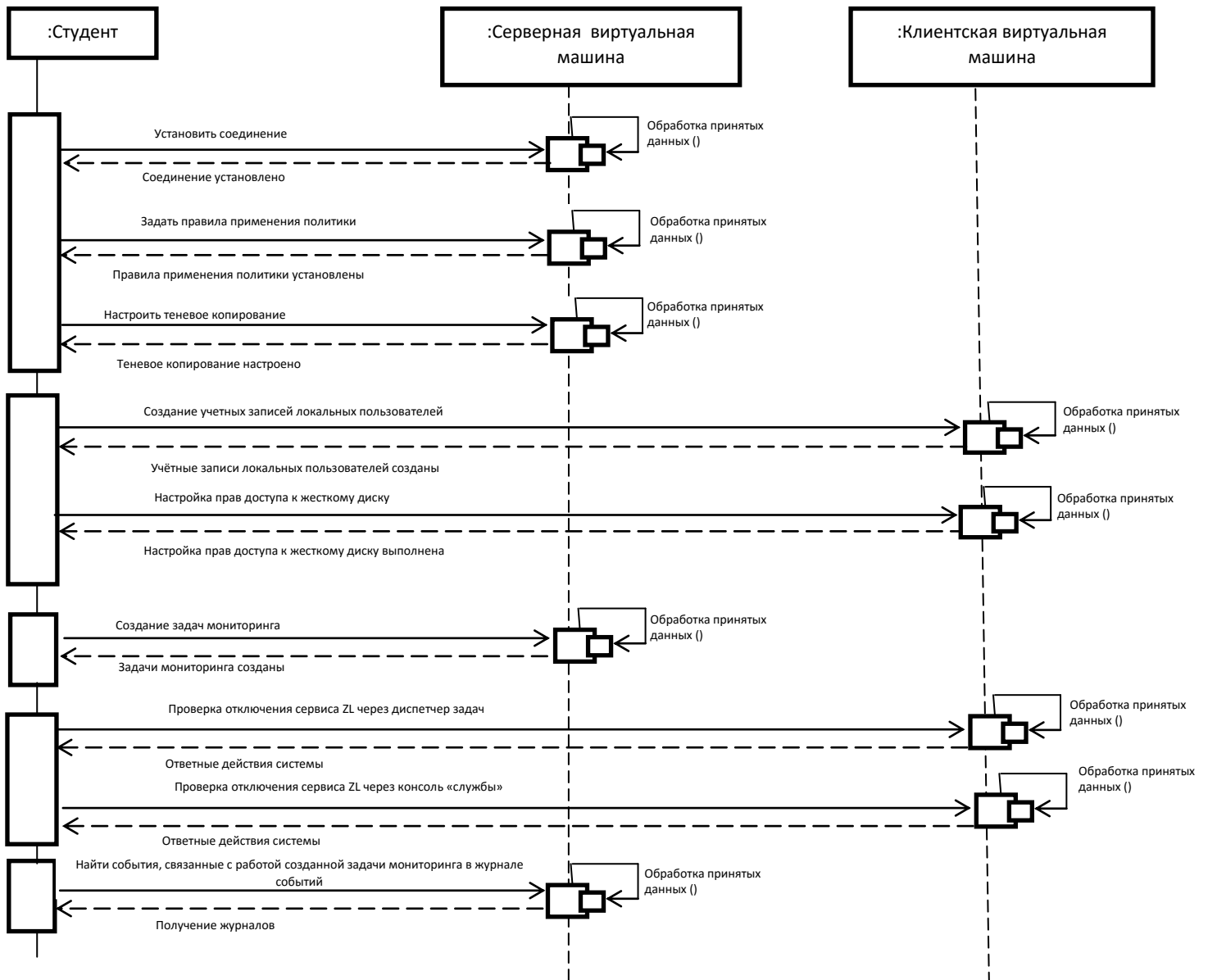
UML - диаграмма последовательности действий Device Lock



ПРИЛОЖЕНИЕ Б

(обязательное)

UML - диаграмма последовательности действий Zecurion Lock



ПРИЛОЖЕНИЕ В

(обязательное)

Структура и содержание отчета о выполнении практического задания

Министерство образования и науки РФ
ФГБОУ ВПО ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Кафедра «Информационная безопасность систем и технологий»

ОТЧЕТ

о выполнении практического задания № 5 «Защита программного агента
DeviceLock от несанкционированного изменения параметров и удаления»

Выполнил: Иванов И.И.

Проверил: Петров П.П.

Пенза, 2016

Цель задания – получить навыки настройки параметров сервиса DeviceLock с использованием редактора настроек и применения функции мониторинга для защиты программного агента DeviceLock от несанкционированного изменения параметров и удаления.

Задание к практическому занятию включает в себя:

- настройку аудита и теневого копирования для сервиса DeviceLock;
- настройку управления сервисом DeviceLock на защищаемых компьютерах;
- настройку управления сервером DeviceLock Enterprise Server;
- настройку режима отображения устройств для сервиса DeviceLock;
- создание учетных записей локальных пользователей;
- настройку прав доступа к жесткому диску защищаемого компьютера;
- создание и применение файла настроек сервиса DeviceLock с использованием консоли DeviceLock Service Settings Editor;
- создание задач мониторинга для контроля состояния программного агента DeviceLock;
- применение задач мониторинга для контроля состояния программного агента DeviceLock и выявления изменения настроек;
- применение задач мониторинга для восстановления настроек программного агента DeviceLock;
- анализ записей журнала мониторинга и формирование отчета;
- вывод по выполненной работе.

Порядок выполнения работы

1 Использование консоли DeviceLock Service Settings Editor для настройки сервиса DeviceLock

1.1 Показать в виде снимков экрана результаты проверки текущих настроек доступа к DVD\CD-ROM на компьютере WinXP01-DL после попыток изменения настроек локальным администратором.

1.2 Показать в виде снимков экрана настройки доступа к DVD\CD-ROM и аудита на компьютере WinXP01-DL, установленные с помощью консоли DeviceLock Service Settings Editor.

1.3 Показать в виде снимков экрана результаты применения файла настроек сервиса DeviceLock на компьютере WinXP01-DL.

1.4 Показать в виде снимков экрана результаты изменения настроек доступа пользователя User1 к DVD\CD-ROM на компьютере WinXP01-DL.

2 Создание задач мониторинга

2.1 Показать в виде снимков экрана настройки задачи мониторинга агента DeviceLock на компьютере WinXP01-DL.

2.2 Показать в виде снимков экрана результаты проверки статуса сервиса DeviceLock и компьютера WinXP01-DL после загрузки файла настроек.

2.3 Показать в виде снимков экрана изменение разрешений на доступ к DVD\CD-ROM на компьютере WinXP01-DL.

2.4 Показать в виде снимков экрана изменение статуса компьютера WinXP01-DL в консоли DeviceLock Management Console после изменения настроек и запуска задачи мониторинга, а также после повторного запуска задачи мониторинга для восстановления настроек сервиса DeviceLock на компьютере WinXP01-DL.

2.5 Показать в виде снимков экрана результаты настройки доступа к DVD\CD-ROM в консоли DeviceLock Management Console на компьютере WinXP01-DL.

2.6 Показать в виде снимков экрана результаты попыток останова сервиса DeviceLock на компьютере WinXP01-DL и удаления файла агента.

3 Формирование отчета

Показать в виде снимков экрана записи журнала мониторинга, отражающие попытки изменения настроек сервиса и запуска задачи мониторинга для проверки статуса компьютера и сервиса DeviceLock, а также запуска задачи мониторинга для восстановления настроек сервиса DeviceLock.

Вывод:

ПРИЛОЖЕНИЕ Г

(обязательное)

Структура и содержание отчета о выполнении практического задания

Министерство образования и науки РФ

ФГБОУ ВПО ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Кафедра «Информационная безопасность систем и технологий»

ОТЧЕТ

о выполнении практического задания № 5 «Защита программного агента
Zecurion Lock от несанкционированного изменения параметров и удаления»

Выполнил: Иванов И.И.

Проверил: Петров П.П.

Пенза, 2016

Цель задания – получить навыки настройки параметров сервиса Zecurion Lock с использованием редактора настроек и применения функции мониторинга для защиты программного агента Zecurion Lock от несанкционированного изменения параметров и удаления.

Задание к практическому занятию включает в себя:

- настройку аудита и теневого копирования для сервиса Zecurion Lock;
- настройку управления сервисом Zecurion Lock на защищаемых компьютерах;
- настройку режима отображения устройств для сервиса Zecurion Lock;
- создание учетных записей локальных пользователей;
- настройку прав доступа к жесткому диску защищаемого компьютера;
- создание задач мониторинга для контроля состояния программного агента Zecurion Lock ;
- применение задач мониторинга для контроля состояния программного агента Zecurion Lock и выявления изменения настроек;
- применение задач мониторинга для восстановления настроек программного агента Zecurion Lock;
- анализ записей журнала мониторинга и формирование отчета;
- вывод по выполненной работе.

Порядок выполнения работы

1 Использование консоли Zecurion Lock для настройки сервиса

1.1 Показать в виде снимков экрана результаты проверки текущих настроек доступа к DVD\CD-ROM на компьютере WinXP01-ZL после попыток изменения настроек локальным администратором.

1.2 Показать в виде снимков экрана настройки доступа к DVD\CD-ROM и аудита на компьютере WinXP01-ZL, установленные с помощью консоли Zecurion Lock.

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

1.4 Показать в виде снимков экрана результаты изменения настроек доступа пользователя User1 к DVD\CD-ROM на компьютере WinXP01-ZL.

2 Создание задач мониторинга

2.1 Показать в виде снимков экрана настройки задачи мониторинга агента Zecurion Lock на компьютере WinXP01-ZL.

2.2 Показать в виде снимков экрана результаты проверки статуса сервиса Zecurion Lock и компьютера WinXP01-ZL после загрузки файла настроек.

2.3 Показать в виде снимков экрана изменение разрешений на доступ к DVD\CD-ROM на компьютере WinXP01-ZL.

2.4 Показать в виде снимков экрана изменение статуса компьютера WinXP01-ZL в консоли Zecurion Lock после изменения настроек и запуска задачи мониторинга, а также после повторного запуска задачи мониторинга для восстановления настроек сервиса Zecurion Lock на компьютере WinXP01-ZL.

2.5 Показать в виде снимков экрана результаты настройки доступа к DVD\CD-ROM в консоли Zecurion Lock на компьютере WinXP01-ZL.

2.6 Показать в виде снимков экрана результаты попыток останова сервиса Zecurion Lock на компьютере WinXP01-ZL и удаления файла агента.

3 Формирование отчета

Показать в виде снимков экрана записи журнала мониторинга, отражающие попытки изменения настроек сервиса и запуска задачи мониторинга для проверки статуса компьютера и сервиса Zecurion Lock, а также запуска задачи мониторинга для восстановления настроек сервиса Zecurion Lock.

Вывод:

МИНОБРНАУКИ России
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования

ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УДК 004.056

Политехнический институт
Факультет приборостроения,
информационных технологий и
электроники
Выпускающая кафедра:
Информационная безопасность систем
и технологий
Учебная группа 11ПИ1

УТВЕРЖДАЮ
Зав. кафедрой ИБСТ
к.т.н., доцент С.Л. Зефирова
«27» 04 2016 г.

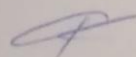
ТЕХНИЧЕСКОЕ ЗАДАНИЕ НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ

студента группы 11ПИ1 Каменьщиковой Екатерины Владимировны
Специальность 100503 – Информационная безопасность
автоматизированных систем

Тема дипломного проекта:

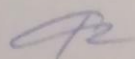
Лабораторный практикум по изучению функций мониторинга и защиты
агентов, реализуемых системами контроля и утечки информации

Руководитель ВКР
к.т.н., доцент кафедры ИБСТ



А.Г. Фатеев

Нормоконтролер
к.т.н., доцент кафедры ИБСТ



А.Г. Фатеев

1 Цели и задачи ВКР

Цель работы – разработать лабораторный практикум по изучению функций мониторинга и защиты агентов, реализуемых системами контроля и утечки информации.

Лабораторный практикум предназначен для изучения функций мониторинга и защиты агентов, реализуемых системами контроля и утечки информации и предотвращения утечек информации в автоматизированной системе DeviceLock DLP Suite и Zecurion Zlock (Device Control) и получения практических навыков по настройке и применению.

2 Тактико – технические требования к выполнению ВКР

Лабораторный практикум включает в себя:

- два лабораторных стенда;
- установленный порядок выполнения задания к каждой лабораторной работе;
- контрольные экземпляры отчётов о выполнении задания к каждой лабораторной работе;
- порядок проверки выполнения задания к каждой лабораторной работе.

Технические требования:

- лабораторный практикум должен включать две лабораторные работы:
 - мониторинг и защита агентов, реализуемая в программном комплексе DeviceLock DLP Suite;
 - мониторинг и защита агентов, реализуемая в программном комплексе Zecurion Zlock (Device Control);
- должны быть подготовлены лабораторные стенды, состоящие из виртуальных машин (ВМ), используемые при проведении лабораторных работ;
- каждый лабораторный стенд должен включать:

– ВМ с установленной операционной системой (ОС) Windows 2003 Server, имитирующую рабочее место администратора;

– ВМ с установленной ОС Windows XP, имитирующую контролируемый компьютер – автоматизированное рабочее место пользователя;

– в лабораторном практикуме должны использоваться системы контроля и предотвращения утечек информации DeviceLock DLP Suite и Zecurion Zlock (Device Control);

– при разработке лабораторного практикума должно применяться средство виртуализации Oracle VirtualBox версии не ниже 4.0;

– должен быть разработан порядок выполнения лабораторных работ, включающий в себя настройку изучаемой системы контроля, имитацию действий пользователей, направленных на реализацию воздействия на программный агент, анализ полученных результатов для определения корректных настроек, обеспечивающих защиту агентов, подготовку отчёта о выполнении лабораторной работы;

– должны быть подготовлены контрольные экземпляры отчетов о выполнении лабораторных работ, входящих в практикум, включающие описание выполнения задания, которое иллюстрируется снимками экрана, показывающими настройки системы и действия систем при имитации нарушений, и отчёты по журналам регистрации событий, формируемых системами контроля и предотвращения утечек информации;

– должен быть определен порядок контроля выполнения задания к лабораторным работам, включающий в себя порядок действий, направленных на проверку правильности выполнения задания к лабораторным работам и отчёт по журналу событий.

В ВКР должны быть рассмотрены следующие вопросы:

– обзор систем контроля и предотвращения утечек информации в автоматизированных системах;

– функции мониторинга и защиты агентов, реализуемые системами контроля и предотвращения утечек информации DeviceLock DLP Suite и Zecurion Zlock (Device Control);

– описание подготовки лабораторных стендов, используемых при проведении лабораторных работ;

– порядок выполнения лабораторной работы по изучению мониторинга и защиты агентов, реализуемой в программном комплексе DeviceLock DLP Suite;

– порядок выполнения лабораторной работы по изучению мониторинга и защиты агентов, реализуемой в программном комплексе Zecurion Zlock (Device Control);

– описание порядка выполнения лабораторных работ, входящих в лабораторный практикум и результатов выполнения лабораторных работ;

– разработка контрольных экземпляров отчетов о выполнении лабораторных работ, входящих в практикум;

– определение порядка контроля выполнения задания к лабораторным работам.

3 Требования к разрабатываемой документации

Отчет по ВКР выполняется в соответствии с требованиями ГОСТ 7.32.

Перечень и содержание графической части ВКР:

– порядок настройки системы контроля и предотвращения утечек информации DeviceLock DLP Suite – 1 л., ф. А1 (плакат);

– порядок настройки системы контроля и предотвращения утечек информации Zecurion Zlock (Device Control) – 1 л., ф. А1 (плакат);

– структура стендов, используемых для проведения лабораторного практикума – 1 л., ф. А1 (плакат);

– состав и содержание отчета о выполнении задания к лабораторному практикуму – 1 л., ф. А1 (плакат);

– UML – диаграмма последовательности действий выполнения лабораторной работы по применению системы контроля и предотвращения утечек информации DeviceLock DLP Suite – 1 л., ф. А1 (плакат);

– UML – диаграмма последовательности действий выполнения лабораторной работы по применению системы контроля и предотвращения утечек информации Zecurion Zlock (Device Control) – 1 л., ф. А1 (плакат);

– демонстрация выполнения лабораторной работы по изучению функции мониторинга и защиты агентов, реализуемой в программном комплексе DeviceLock DLP Suite.

Электронная копия отчета и графической части ВКР должна быть представлена на магнитном или оптическом носителе.

4 Сроки выполнения ВКР

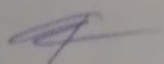
Тема утверждена приказом ректора ПГУ № 491а/о от 25 «04» 2016 г.

Дата выдачи задания « 7 » февраля 2016 г.

Время дипломного проектирования с 18 апреля 2016 г. по 10 июля 2016 г.

Задание к исполнению принял « 7 » февраля 2016 г.

Исполнитель ВКР Вас - Каменьщикова Е.В.



Ректору Пензенского
государственного университета
А. Д. Гулякову
студентки 5 курса ФПИТЭ
очной формы обучения
Каменьщиковой Екатерины Владимировны

заявление.

Я, Каменьщикова Екатерина Владимировна, студентка 5 курса очной формы обучения специальности 10.05.03 – «Информационная безопасность автоматизированных систем», прошу провести проверку с использованием системы «Антиплагиат» дипломного проекта на тему «Лабораторный практикум по изучению функций мониторинга и защиты агентов, реализуемых системами контроля и утечки информации», выполненной мной самостоятельно, на содержание элементов плагиата.

Все прямые заимствования из печатных и электронных источников, а также из защищенных ранее выпускных квалификационных работ, кандидатских и докторских диссертаций имеют соответствующие ссылки.

Я ознакомлена с действующим Стандартом университета «Выпускная квалификационная работа обучающихся по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры», согласно которому обнаружение плагиата является основанием для недопуска ВКР к защите и отчисления из университета.

Подпись /Е.В.Каменьщикова/
27.05.2016 г.

ВКР представлена на проверку 01.06.2016 г.

Руководитель ВКР Подпись /А.Г.Фатеев/

Протокол

проверки на оригинальность в системе «Антиплагиат.ВУЗ» выпускной квалификационной работы на тему «Лабораторный практикум по изучению функций мониторинга и защиты агентов, реализуемых системами контроля и утечки информации» студента 5 курса Е.В.Каменьщиковой специальности 10.05.03 – «Информационная безопасность автоматизированных систем».

Руководитель ВКР к.т.н., доцент кафедры ИБСТ Фатеев Алексей Григорьевич.

Отчет о проверке № 1

ФИО: Иванов Алексей Петрович
дата отправки: 10.06.2016 19:54:43
пользователь: [aa_kamenyshkova@yandex.ru](#) / ID: 1267386
отчет предоставлен сервисом «Антиплагиат»
на сайте: <http://www.antiplagiat.ru>

Информация о документе

ID документа: 42
Имя исходного файла: ВКР_Каменьщикова_ЕВ_11ПИ1.docx
Размер текста: 2927 кБ
Тип документа: не указано
Символов в тексте: 115652
Слов в тексте: 14351
Число предложений: 615

Информация об отчете

Дата: Отчет от 10.06.2016 19:54:43 - Последний готовый отчет
Комментарий: не указан
Оценка оригинальности: 94,47%
Занимательность: 1,57%
Цитирование: 0%



Оригинальность: 94,47%
Занимательность: 1,57%
Цитирование: 0%

08.06.2016 г.

Секретарь ГЭК

А.Г.Фатеев

А.П.Иванов

ОТЗЫВ

на дипломный проект студентки
ФГБОУ ВО Пензенский государственный университет
Каменьщиковой Екатерины Владимировны

Тема проекта: Лабораторный практикум по изучению функций мониторинга и защиты агентов, реализуемых системами контроля и утечки информации.

Одной составляющих подготовки специалистов по защите информации (ЗИ) является изучение программно-аппаратных средств, применяемых для обеспечения информационной безопасности (ИБ), которое включает получение практических навыков по их настройке и применению. В настоящее время применяется большое количество различных средств защиты информации (СЗИ), отличающихся своим назначением и функциональностью. В их числе стали широко использоваться системы контроля и предотвращения утечек информации (СКиПУИ) как отдельный вид СЗИ. Они обладают рядом особенностей, отличающих их от других СЗИ, и требуют навыков по настройке, которая обеспечивает их корректное функционирование. Одной из важных функций СКИПУИ является функция защиты программных агентов, устанавливаемых на контролируемые компьютеры от несанкционированного изменения настроек и удаления агента. Она реализуется как функция мониторинга состояния агента и обеспечивает выявление попыток выполнения подобных действий. Для обеспечения корректного применения СКИПУИ и применения функции мониторинга необходимо подготовить практикум по применению СКИПУИ и применению функции мониторинга, который позволит при его выполнении получить необходимые практические навыки.

Дипломный проект Каменьщиковой Е.В. посвящен разработке лабораторного практикума по изучению функций мониторинга и защиты агентов, реализуемых системами контроля и утечки информации. При выполнении проекта дипломником был разработан лабораторный практикум, включающий две ла-

лабораторных работы. Одна из работ посвящена изучению функций мониторинга и защиты агентов, реализуемых программным комплексом DeviceLock DLP Suite. Вторая работа посвящена изучению функций мониторинга и защиты агентов, реализуемых программным комплексом Zecurion Zlock (Device Control). Для каждой лабораторной работы был подготовлен лабораторный стенд, состоящий из нескольких виртуальных машин с установленными на них изучаемыми СКИПУИ, и объединенных в виртуальную локальную сеть. Подготовлено описание порядка выполнения каждой работы, входящей в лабораторный практикум, устанавливающий основные этапы каждой работы и последовательность их выполнения. Также подготовлены контрольные экземпляры отчетов о выполнении лабораторных работ, определяющие структуру и содержание отчета о выполнении. Следует отметить разработанное описание процесса развертывания лабораторного стенда, что позволяет сократить временные затраты на подготовку к проведению лабораторных работ.

Результатом дипломного проекта Каменьщиковой Е.В. является полностью законченный лабораторный практикум, выполнение которого позволит получить практические навыки по применению функций мониторинга и защиты агентов, реализуемых системами контроля и утечки информации.

Таким образом, техническое задание на дипломный проект выполнено полностью. Все поставленные задачи детально проработаны и успешно решены. При выполнении дипломного проекта Каменьщикова Е.В. показала высокий уровень знаний, способность применять их при самостоятельной работе и самостоятельно решать сложные задачи. Материал, представленный в отчете о ВКР, изложен грамотно, графический и презентационный материал является наглядным и позволяет сформировать представление о содержании и актуальности проекта.

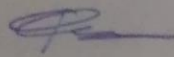
Результаты выполнения ВКР – лабораторный стенд и описание порядка выполнения заданий к лабораторному практикуму планируется использовать при разработке лабораторных работ и практических занятий для студентов специальностей 100502 «Информационная безопасность телекоммуникационных систем» и 100503 «Информационная безопасность автоматизированных сис-

тем», изучающих дисциплины «Современные системы контроля и предотвращения утечек информации» и «Программно-аппаратные средства обеспечения информационной безопасности».

Дипломный проект Каменьщиковой Е.В. выполнен на высоком уровне, соответствует специальности 100503 «Информационная безопасность автоматизированных систем» и может быть допущен к защите в ГЭК.

Дипломный проект Каменьщиковой Е.В. оценивается в 15 баллов.

Руководитель ВКР,
к.т.н., доцент кафедры «ИБСТ»



А.Г. Фатеев

МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

РЕЦЕНЗИЯ

на выпускную квалификационную работу

Каменьщиковой Екатерины Владимировны
(фамилия, имя, отчество)

Тема дипломного проекта: Лабораторный практикум по изучению функций мониторинга и защиты агентов, реализуемых системами контроля и утечки информации.

На рецензию представлена выпускная квалификационная работа, содержащая пояснительную записку в объеме 117 с., 57 рис., 7 источников и 6 приложений.

Целью дипломного проектирования является разработка лабораторного практикума по изучению функций мониторинга и защиты агентов, реализуемых системами контроля и утечки информации.

Дипломный проект посвящен актуальной проблеме: правильной настройке и проверке работоспособности программных агентов, как ключевого звена DLP систем, а также получению практических навыков использования механизмов контроля состояния агентов и защиты от несанкционированного воздействия на них.

Дано обоснование актуальности исследуемой темы, достигнуты поставленная цель и задачи по созданию лабораторного практикума по изучению функций мониторинга и защиты агентов на примере систем контроля и предотвращения утечки информации DeviceLock DLP Suite и Zecurion Zlock (Device Control).

Произведено детальное описание установки и настройки виртуальных машин, для выполнения лабораторного практикума. Последовательно и

доступно описаны порядок выполнения заданий, настройка и мониторинг агентов DeviceLock DLP Suite и Zecurion Zlock, а также имитация нарушений работы агентов и оформление результатов лабораторных работ.

В качестве недостатка следует отметить использование в лабораторном практикуме операционных систем Windows 2003 Server и Windows XP, как не самых актуальных для использования и снятых с поддержки компанией производителем.

Учитывая то, что все пункты технического задания были выполнены, считаю, что выпускная квалификационная работа может быть допущена к защите в ГАК, а Каменьщикова Е.В. достойна присвоения квалификации специалист по защите информации по специальности 100503 «Информационная безопасность автоматизированных систем». С учетом актуальности, достоверности результатов ВКР, общая оценка ВКР составляет 9 баллов.

Рецензент:

Инженер по защите информации

2 категории отдела 5800

АО «НПП «Рубин»

С.А. Евстигнеев

