Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Сыктывкарский государственный университет»
Институт точных наук и информационных технологий
Кафедра информационной безопасности

Методические указания
по выполнению лабораторных работ по дисциплине
«Программно-аппаратная защита информации»

090104 – Комплексная защита объектов информатизации

090900 – Информационная безопасность

Сыктывкар 2013

Лист согласования и утверждения

Методические указания составлены на основании ГОС ВПО и учебного плана специальности 090104 – Комплексная защита объектов информатизации.

Составитель методических указаний:

Старший преподаватель кафедры информационной безопасности

_____ Басенко Алексей Олегович.

Методические указания рассмотрены и одобрены на заседании кафедры информационной безопасности.

Протокол заседания № ___ от «____»_____2013 г.

Заведующий кафедрой, к.ф.-м.н. _____ Носов Леонид Сергеевич.

Аннотация

Методические указания по проведению лабораторных работ по дисциплине «Программно-аппаратная защита информации» предназначены для студентов, обучающихся по специальности 090104 – Комплексная защита объектов информатизации. Также лабораторные работы, описанные в настоящих Методических указаниях, могут применяться в ходе обучения по направлению 090900 – Информационная безопасность в рамках дисциплин «Информационная безопасность автоматизированных систем», «Программно-аппаратные средства защиты информации» и при проведении курсов повышения квалификации.

Содержание

Введение

Методические указания по проведению лабораторных работ по дисциплине «Программно-аппаратная защита информации» предназначены для студентов, обучающихся по специальности 090104 – Комплексная защита объектов информатизации. Также лабораторные работы, описанные в настоящих Методических указаниях, могут применяться в ходе обучения по направлению 090900 – Информационная безопасность в рамках дисциплин «Информационная безопасность автоматизированных систем», «Программно-аппаратные средства защиты информации» и при проведении курсов повышения квалификации.

В соответствии с государственным образовательным стандартом специальности при проведении лабораторных занятий студенты закрепляют навыки в следующих видах деятельности:

экспериментально-исследовательская:

– изучение уязвимостей компьютерных систем, отдельных программных и программно-аппаратных средств защиты информации, проведение анализа их эффективности;

эксплуатационная деятельность:

– настройка, эксплуатация и поддержание в работоспособном состоянии программных и программно-аппаратных средств защиты информации;

– централизованное администрирование программных и программно-аппаратных средств защиты информации в корпоративных сетях;

– проведение контрольных проверок работоспособности и эффективности действующих систем и механизмов защиты информации;

проектно-технологическая:

– изучение и обобщение научно-технической литературы, нормативных и методических материалов по средствам и механизмам защиты информации в компьютерных системах и сетях;

– внедрение комплексных систем и отдельных программных и программно-аппаратных средств защиты информации;

В ходе проведения лабораторных занятий по данной дисциплине происходит закрепление следующих **компетенций**:

– способности к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления (ОК-8);

– способности к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства (ОК-11);

– способности понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах (ПК-2);

– способности принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия (ПК-9);

– способности администрировать подсистемы информационной безопасности объекта (ПК-10);

– способности выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации (ПК-11).

– способности применять программные средства системного, прикладного и специального назначения (ПК-15);

– способностью использовать инструментальные средства для решения профессиональных задач (ПК-16);

– способностью собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности (ПК-18).

– способности применять методы анализа изучаемых явлений, процессов и проектных решений (ПК-20);

– способностью проводить эксперименты по заданной методике, обработку результатов, оценку достоверности их результатов (ПК-22).

– способности осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности (ПК-24)

– способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации (ПК-27).

В результате проведения лабораторных работ студенты должны:

знать:

– основные виды специализированных программных и программно-аппаратных средств защиты информации;

– методы противодействия несанкционированному доступу и иным угрозам в операционных системах;

уметь:

– квалифицированно оценивать область применения конкретных механизмов защиты;

– подбирать под необходимые задачи, осваивать и внедрять распространенные средства защиты информации;

– интегрировать средства защиты информации в имеющиеся компьютерные системы и сети организации, а также обеспечивать их использование совместно с иными применяемыми средствами и системами защиты;

– тестировать эффективность функционирования применяемых средств защиты информации;

владеть:

– профессиональной терминологией в предметной области;

– навыками работы с различными программными средами, оболочками и интерфейсами;

– навыками настройки распространенных программных и программно-аппаратных средств защиты информации;

– навыками централизованного управления применяемыми средствами защиты информации.

Дисциплина «Программно-аппаратная защита информации» является одной из завершающих в цикле общепрофессиональных дисциплин и основывается на знаниях и навыках, полученных в рамках дисциплин «Операционные системы» и «Безопасность операционных систем». Указанные предшествующие дисциплины должны быть освоены студентами в полном объеме.

Знания и практические навыки, полученные в ходе выполнения лабораторных работ по дисциплине «Программно-аппаратная защита информации» используются обучающимися при прохождении практики, разработке выпускной квалификационной работы, а также непосредственно в дальнейшей профессиональной деятельности.

Содержание лабораторных работ, порядок их выполнения и система оценивания

В рамках дисциплины «Программно-аппаратная защита информация» проводятся лабораторные работы по следующим темам:

- дискреционное и мандатное разграничение доступа
- организация изолированных пользовательских сред
- терминальный доступ
- разрушающие программные воздействия
- гарантированное затирание информации
- контроль за использованием съемных носителей информации
- доверенная загрузка.

Лабораторный практикум состоит из двух этапов. На первом (подготовительном) этапе студенты совместно с преподавателем в интерактивном режиме изучают практические аспекты применения средств защиты информации от несанкционированного доступа, а также иных программных и программно-аппаратных средств защиты, особенности их администрирования и настройки.

В рамках второго этапа студенты индивидуально выполняют задания, приведенные в настоящих методических указаниях, основываясь на теории, полученной в ходе лекционных занятий, и информации с первого подготовительного этапа.

Лабораторные работы предполагают необходимость предварительной подготовки к их сдаче в рамках самостоятельной работы. В ходе самостоятельной работы студентами может применяться вспомогательная литература, приведенная в описании каждого из заданий.

Лабораторные работы сдаются в компьютерном классе. Все действия в рамках каждой из работ должны быть выполнены в полном соответствии с поставленными задачами (в т.ч. с точным соблюдением наименований создаваемых объектов). Перед сдачей лабораторной работы необходимо выполнить самопроверку.

Задание считается выполненным только в случае, если студентом решены все поставленные в рамках лабораторной работы задачи. Исключение составляют отдельные задания, для которых предусмотрено дифференцированное оценивание в зависимости от объема выполненных работ.

За успешное выполнение каждого задания начисляются баллы в зависимости от категории его сложности (задания первой категории – самые простые, третьей – наиболее сложные). Количество баллов, соответствующее каждой категории сложности, определяется преподавателем исходя из применяемой системы оценивания.

Тема 1. Дискреционное и мандатное разграничение доступа

Задание 1.1. СЗИ от НСД «SecretNet 6» – автономный (доступ к ресурсам)

Цель задания:

Изучение особенностей и отработка навыков настройки дискреционного и мандатного разграничения доступа к ресурсам в СЗИ от НСД «SecretNet 6» – автономный.

Начальная моделируемая инфраструктура:

Клиентский компьютер **COMP** (ОС Windows XP SP3 и выше) без подключения к домену. На компьютере присутствует только локальный пользователь **Администратор**. Политики безопасности операционной системы имеют настройки по умолчанию.

Задачи:

1. Установить на клиентский компьютер COMP СЗИ от НСД «SecretNet 6» – автономный.

2. Создать пользователей **USER1** (**уровень доступа – конфиденциально**) и **USER2** (**уровень доступа – секретно**).

3. С использованием мандатного механизма разграничить доступ пользователей**USER1** и **USER2** к трем созданным директориям со следующими метками конфиденциальности: **общедоступно**, **конфиденциально**, **секретно**.

4. С использованием дискреционного механизма разграничить доступ пользователей **USER1** и **USER2** к данным директориям следующим образом:

- **общедоступная папка** – полный доступ **USER1**, доступ только на чтение (выполнение запрещено) **USER2**;
- **конфиденциальная папка** – полный доступ (кроме возможности удалить саму папку) **USER1** и **USER2**;
- **секретная папка** – нет доступа **USER1**, полный доступ (кроме возможности удалить саму папку) **USER2.**

При этом на данные папки **другие пользователи не должны иметь никаких прав доступа**, группа **SYSTEM** и **Администраторы** должны иметь полные права по доступу. Пользователь **USER** не должен иметь возможности изменять предоставленные ему полномочия.

Самопроверка:

1. Разместить в каждой из созданных директорий любой текстовый документ и исполняемый файл. Проверить возможность открытия и изменения текстового документа, а также запуска исполняемого файла в каждой из директорий согласно поставленной задаче.
2. Проверить наличие в журнале СЗИ событий входа пользователей в систему, а также событий обращения к созданным директориям и файлам, размещенным в них.

Вспомогательная литература и иные источники:

1. Комплект документации на СЗИ от НСД «SecretNet 6» – автономный.

Категория сложности № 1.

Задание 1.2. СЗИ от НСД «DallasLock 8.0-C» (доступ к ресурсам)

Цель задания:

Изучение особенностей и отработка навыков настройки дискреционного разграничения доступа к ресурсам, а также настройки регистрации событий в СЗИ от НСД «DallasLock 8.0-C».

Начальная моделируемая инфраструктура:

Клиентский компьютер **COMP** (ОС Windows XP SP3 и выше) без подключения к домену. На компьютере присутствует только локальный пользователь **Администратор**. Политики безопасности операционной системы имеют настройки по умолчанию.

Задачи:

1. Установить на клиентский компьютер COMP СЗИ от НСД «DallasLock 8.0-C».

2. Создать пользователей **USER1** (**уровень доступа – конфиденциально**) и **USER2** (**уровень доступа – секретно**).

3. С использованием мандатного механизма разграничить доступ пользователей **USER1** и **USER2** к двум созданным директориям DIR1 и DIR2 со следующими метками конфиденциальности: **конфиденциально**, **секретно**.

4. С использованием дискреционного механизма СЗИ разграничить доступ пользователей **USER1** и **USER2** к двум созданным директориям следующим образом:

- **DIR1** – полный доступ (без прав на выполнение) **USER1**, доступ только на чтение (без прав на выполнение) **USER2**;
- **DIR2** – нет доступа **USER1**, доступ на чтение и выполнение **USER2.**

При этом на данные папки **другие пользователи не должны иметь никаких прав доступа**, группа **SYSTEM** и **Администраторы** должны иметь полные права по доступу. Пользователь **USER** не должен иметь возможности изменять предоставленные ему полномочия.

5. Настроить средствами СЗИ аудит доступа для данных директорий, обеспечив регистрацию **только событий удаления, записи данных и изменения разрешений.** Также должны регистрироваться события входа пользователей и изменения политик (как средствами ОС, так и средствами СЗИ).

Самопроверка:

1. Разместить в каждой из созданных директорий любой текстовый документ и исполняемый файл. Проверить возможность открытия и изменения текстового документа, а также запуска исполняемого файла в каждой из директорий согласно поставленной задаче.
2. Проверить наличие в журнале СЗИ событий входа пользователей в систему, а также событий обращения к созданным директориям и файлам, размещенным в них.

Вспомогательная литература и иные источники:

1. Комплект документации на СЗИ от НСД «DallasLock 8.0-C».

Категория сложности № 1.

Тема 2. Организация изолированных пользовательских сред

Задание 2.1. СЗИ от НСД «SecretNet 6» – автономный (замкнутая программная среда)

Цель задания:

Изучение особенностей и отработка навыков настройки замкнутой программной среды в СЗИ от НСД «SecretNet 6» – автономный.

Начальная моделируемая инфраструктура:

Клиентский компьютер **COMP** (ОС Windows XP SP3 и выше) без подключения к домену. На компьютере присутствует только локальный пользователь **Администратор**. Политики безопасности операционной системы имеют настройки по умолчанию.

Задачи:

1. Установить на клиентский компьютер COMP СЗИ от НСД «SecretNet 6» – автономный.

2. Создать ЗПС для пользователя **USER** со следующими доступными задачами: **Acrobat Reader**, **Windows Movie Maker**. Запуск иных задач (кроме тех, что расположены в c:\windows\) должен быть запрещен. Запуск встроенных игр (Сапер, Косынка и т.д.) должен быть запрещен.

Самопроверка:

1. Проверить корректность применения настроек СЗИ от НСД, реализующих ЗПС под пользователем USER на клиентском компьютере COMP, проверив возможность запуска только разрешенных программ в соответствии с заданием.

Вспомогательная литература и иные источники:

1. Комплект документации на СЗИ от НСД «SecretNet 6» – автономный.

Категория сложности № 2.

Задание 2.2. СЗИ от НСД «Dallas Lock 8.0-C» (замкнутая программная среда)

Цель задания:

Изучение особенностей и отработка навыков настройки замкнутой программной среды в СЗИ от НСД «DallasLock 8.0-C».

Начальная моделируемая инфраструктура:

Клиентский компьютер **COMP** (ОС Windows XP SP3 и выше), подключенный к домену test.local. Сервер **WIN2008** (ОС Windows 2008 R2) с добавленной ролью контроллера домена (домен **test.local**). Сервер WIN2003R2 (ОС Windows 2003 R2), подключенный к домену test.local. На компьютере и серверах присутствуют только локальные пользователи **Администратор**. Политики безопасности операционных систем имеют настройки по умолчанию.

Задачи:

1. Развернуть на сервере WIN2003R2 сервер управления DallasLock.

2. С использованием возможностей сервера управления провести удаленную установку DallasLock на клиентский компьютер COMP.

3. Создать ЗПС, которая будет применяться на доменного пользователя **USER** при включении его в доменную группу **ZPS**, со следующими доступными задачами: **WordPad**, **Windows Movie Maker**. Запуск иных задач (кроме тех, что расположены в c:\windows\) должен быть запрещен. Запуск встроенных игр (Сапер, Косынка и т.д.) должен быть запрещен.

Самопроверка:

1. Проверить корректность настроек сети, выполнив команду ping win2008.test.local и ping win2003r2.test.local с клиентского компьютера COMP,а также ping comp.test.localc сервера win2003r2.

2. Проверить корректность установки СЗИ от НСД на клиентский компьютер, проанализировав журнал системных событий операционной системы.

3. Проверить корректность применения настроек сервера управления, реализующих ЗПС под пользователем USER на клиентском компьютере COMP, проверив возможность запуска только разрешенных программ в соответствии с заданием.

Вспомогательная литература и иные источники:

1. Комплект документации на СЗИ от НСД «DallasLock 8.0-C».

2. Служба Active Directory. Ресурсы Windows Server 2008 (Windows Server 2008 Active Directory Resource Kit). Стэн Раймер, Конан Кезема, Майк Малкер, Байрон Райт.

Категория сложности № 3.

Тема 3. Терминальный доступ

Задание 3.1. Active Directory (терминальные службы)

Цель задания:

Изучение и отработка навыков развертывания терминального сервера, а также разграничения прав пользователей при работе на нем, изучение особенностей применения групповых политик.

Начальная моделируемая инфраструктура:

Клиентский компьютер **COMP** (ОС Windows XP SP3 и выше) без подключения к домену. Сервер WIN2008 (ОС Windows 2008 R2) с добавленной ролью контроллера домена (домен **test.local**). На компьютере и сервере присутствуют только локальные пользователи **Администратор**. Политики безопасности операционных систем имеют настройки по умолчанию.

Задачи:

1. Включить клиентский компьютер COMP в домен.
2. Развернуть на сервере WIN2008 **терминальный сервер.**
3. Создать доменного пользователя **USER.**
4. Групповыми политиками **настроить автоматический запуск WordPad** при входе пользователя USER на терминальный сервер, **при этом пользователь не должен иметь возможности работать на сервере терминалов с иным ПО и не должен иметь доступ на запись в любые директории кроме своего собственного профиля или временных папок.** Работа с иным ПО ограничивается через политики ограниченного использования программ, при этом **ограничения не должны применяться локально на компьютере COMP пользователя или на каких-либо других пользователей.**

Самопроверка:

1. Проверить корректность настроек сети, выполнив команду ping win2008.test.local с клиентского компьютера COMP.
2. Проверить возможность входа пользователя USER на терминальный сервер.
3. Проверить корректность прав доступа к файловым ресурсам, а также возможность запуска только разрешенных программ в соответствии с заданием.
4. Проверить отсутствие ограничений на запуск программ для пользователя USER на компьютере COMP.

Вспомогательная литература и иные источники:

1. Служба Active Directory. Ресурсы Windows Server 2008 (Windows Server 2008 Active Directory Resource Kit). Стэн Раймер, Конан Кезема, Майк Малкер, Байрон Райт.

2. Групповая политика Windows. Ресурсы Windows Server 2008, Windows Vista, Windows XP, Windows Server 2003 (Windows Group Policy Resource Kit: Windows Server 2008 and Windows Vista). Дерек Мелбер.

3. http://technet.microsoft.com/

Категория сложности № 3 (№ 1 в случае, если вместо задачи № 4 организовывается только возможность входа пользователя с использованием терминальных служб).

Тема 4. Разрушающие программные воздействия

Задание 4.1. Kaspersky Administration Kit

Цель задания:

Изучение и отработка навыков развертывания сервера централизованного управления антивирусными средствами, а также особенностей его интеграции в доменную инфраструктуру.

Начальная моделируемая инфраструктура:

Клиентский компьютер **COMP** (ОС Windows XP SP3 и выше), подключенный к домену test.local. Сервер WIN2008 (ОС Windows 2008 R2) с добавленной ролью контроллера домена (домен **test.local**). На компьютере и сервере присутствуют только локальные пользователи **Администратор**. Политики безопасности операционных систем имеют настройки по умолчанию.

Задачи:

1. Развернуть сервер централизованного управления антивирусами на сервере WIN2008.

2. **С использованием возможности сервера управления установить антивирусное ПО** на клиентский компьютер COMP.

3. Произвести **настройки антивируса с использованием политик**, организовав применение разных наборов политик в зависимости от наличия подключения клиентского компьютера к локальной сети.

4. Организовать **возможность прозрачного подключения доменного пользователя USER** через специализированную консоль, установленную на клиентском компьютере, к серверу централизованного управления **с различными правами**, зависящими от членства пользователя в определенной доменной группе.

Самопроверка:

1. Проверить корректность настроек сети, выполнив команду ping win2008.test.local с клиентского компьютера COMP.

2. Проверить изменение настроек антивируса на клиентском компьютере при отключении сетевого адаптера.

3. Проверить возможность подключения пользователя USER к серверу управления с компьютера COMP.

Вспомогательная литература и иные источники:

1. Комплект документации на Kaspersky Administration Kit.

2. Служба Active Directory. Ресурсы Windows Server 2008 (Windows Server 2008 Active Directory Resource Kit). Стэн Раймер, Конан Кезема, Майк Малкер, Байрон Райт.

Категория сложности № 3 (№ 2 без выполнения задачи № 4).

Задание 4.2. Устранение заражения вредоносным ПО

Цель задания:

Изучение и отработка различных способов устранения заражения компьютера вредоносным программным обеспечением, изучение способов настройки компьютеров, позволяющих снизить риск заражения.

Начальная моделируемая инфраструктура:

Клиентский компьютер **COMP** (ОС Windows XP SP3 и выше). На компьютере присутствуют локальные пользователи **Администратор и USER**. Политики безопасности операционных систем имеют настройки по умолчанию. На компьютере размещается модель вредоносного ПО (тип – Winlocker). Инструментарий: загрузочный диск с антивирусным средством, загрузочный диск с ERD Commander.

Задачи:

1. Запустить файл, моделирующий вредоносное ПО.

2. Провести **ручное удаление вредоносного ПО** с клиентского компьютера с использованием предоставленных средств и отчитаться за выполнение у преподавателя.

3. Вернуться операционную систему в начальное состояние. Произвести **настройку** клиентского компьютера, **предотвращающую возможность повторного заражения.**

Самопроверка:

1. Проверить полную работоспособность компьютера после лечения (отсутствие баннера при загрузке, работоспособность безопасного режима работы и т.д.).

2. Проверить невозможность повторного заражения после применения настроек.

Вспомогательная литература и иные источники:

1. Интернет-ресурсы производителей антивирусных средств.

Категория сложности № 1 в случае использования кода разблокировки, № 2 в случае использования разгрузочного диска с антивирусным средством, № 3 в случае использования загрузочного диска с ERD Commander.

Тема 5. Гарантированное затирание информации

Задание 5.1. СГУ-2

Цель задания:

Изучение особенностей удаления информации штатными средствами операционной системы, возможностей восстановления удаленной информации, отработка навыков гарантированного затирания ранее удаленной информации с использованием специализированных программных средств.

Начальная моделируемая инфраструктура:

Клиентский компьютер **COMP** (ОС Windows XP SP3 и выше). На компьютере присутствует только локальный пользователь **Администратор**. Политики безопасности операционных систем имеют настройки по умолчанию. Жесткий диск разбит на 2 тома C:\ и D:\. На диск D:\ был записан и удален штатными средствами ОС файл, содержащий ответы на тест по ПАЗИ, также на диске находится ряд других файлов.

Задачи:

1. С использованием **Winhex** просмотреть содержимое секторов диска D:\, найти и восстановить файл, содержащий ответы на тест по ПАЗИ, на Рабочий стол. Сделать скриншот, демонстрирующий содержимое секторов, которые занимал удаленный файл.

2. Установить на **COMP** СГУ-2 и с его помощью обеспечить невозможность восстановления файла с диска D:\ (иная информация на диске должна остаться в неизменном виде).

Самопроверка:

1. Проверить, что восстановленный файл открывается без сбоев.
2. Проверить результаты выполнения задачи № 2, сравнив данные из Winhex о содержимом секторов диска после применения СГУ-2 с аналогичными данными на скриншоте.

Вспомогательная литература и иные источники:

1. Комплект документации на СГУ-2 и Winhex.

Категория сложности № 1.

Задание 5.2. Гарантированное затирание информации средствами СЗИ от НСД

Цель задания:

Изучение особенностей удаления информации штатными средствами операционной системы, отработка навыков администрирования и тестирования работоспособности СЗИ от НСД в части механизмов гарантированного затирания информации.

Начальная моделируемая инфраструктура:

Клиентский компьютер **COMP** (ОС Windows XP SP3 и выше). На компьютере присутствует только локальный пользователь **Администратор**. Политики безопасности операционных систем имеют настройки по умолчанию. Жесткий диск разбит на 2 тома C:\ и D:\.

Задачи:

1. Установить на клиентский компьютер **COMP** СЗИ от НСД «SecretNet 6» – автономный.
2. Создать пользователя **USER** (уровень допуска – конфиденциально).
3. Создать на диске D:\ каталог **«Конфиденциально»** и разграничить доступ пользователей к нему с использованием мандатного механизма.
4. Настроить СЗИ от НСД «SecretNet 6» на затирание данных только в каталогах, содержащих конфиденциальную информацию.
5. Протестировать работоспособность механизма гарантированного затирания информации СЗИ от НСД «SecretNet 6» с использованием Winhex (файлы удаляются под пользователем USER).

Самопроверка:

1. Создать файлы в каталоге «Конфиденциально» и в корне диска D:\. С использованием Winhex просмотреть содержимое секторов диска D:\, занимаемых файлами, и сделать соответствующие скриншоты.
2. Удалить созданный файлы под пользователем USER и сверить под пользователем Администратор данные из Winhex о содержимом секторов диска после применения гарантированного затирания с аналогичными данными на скриншотах, сделав вывод об эффективности затирания и корректности настроек.

Вспомогательная литература и иные источники:

1. Комплект документации на СЗИ от НСД «SecretNet 6» – автономный.
2. Комплект документации на Winhex.

Категория сложности № 1.

Тема 6. Контроль за использованием съемных носителей информации

Задание 6.1. DeviceLock с централизованным управлением

Цель задания:

Изучение и отработка навыков развертывания системы ограничения и контроля доступа к портам и устройствам ввода-вывода информации, а также особенностей ее интеграции в доменную инфраструктуру, закрепление навыков администрирования Windows Server 2008.

Начальная моделируемая инфраструктура:

Сервер **WIN2008** (ОС Windows 2008 R2) с добавленной ролью контроллера домена (домен **test.local**) и установленным SQL сервером **SQLExpress**. Клиентский компьютер **COMP** (ОС Windows XP SP3 и выше), подключенный к домену test.local. На компьютере и сервере присутствуют только локальные пользователи **Администратор**. Политики безопасности операционных систем имеют настройки по умолчанию.

Задачи:

1. Развернуть **сервер DeviceLock** на сервере WIN2008.

2. С **использованием возможностей групповых политик** удаленно установить сервис DeviceLock на клиентском компьютере COMP.

3. Создать в домене группу **DeviceLockAdmins** и пользователя **DLAdmin** (входит в группы Пользователи домена и DeviceLockAdmins). Организовать возможность администрирования сервера и сервиса DeviceLock только пользователями из локальной группы Администраторы и группы DeviceLockAdmins.

4. Войти под пользователем DLAdmin на сервер WIN2008. Удаленно настроить на компьютере COMP для всех пользователей аудит событий успехов и отказов использования USB, Floppy и DVD-ROM. Настроить централизованный сбор журналов указанных событий на сервере DeviceLock.

Самопроверка:

1. Проверить корректность настроек сети, выполнив команду ping win2008.test.local с клиентского компьютера COMP, а также ping comp.test.local с сервера win2008.

2. Проверить корректность удаленной установки сервиса DeviceLock на клиентском компьютере, проанализировав журнал системных событий операционной системы.
3. Проверить корректность предоставления доступа к серверу и сервису DeviceLock, попробовав подключиться к ним под пользователем DLAdmins.
4. Проверить настройки аудита, проанализировав на сервере DeviceLock журнал событий на предмет наличия в нем необходимых данных с клиентского компьютера COMP.

Вспомогательная литература и иные источники:

1. Комплект документации на DeviceLock.
2. Служба Active Directory. Ресурсы Windows Server 2008 (Windows Server 2008 Active Directory Resource Kit). Стэн Раймер, Конан Кезема, Майк Малкер, Байрон Райт.

Категория сложности № 3 (№ 2 без выполнения задачи № 3).

Задание 6.2. DeviceLock + BitLocker

Цель задания:

Изучение и отработка навыков настройки системы ограничения и контроля доступа к портам и устройствам ввода-вывода информации, а также особенностей ее интеграции в доменную инфраструктуру, изучение способов повышения защищенности передаваемых на носителях данных за счет использования прозрачного шифрования.

Начальная моделируемая инфраструктура:

Сервер **WIN2008** (ОС Windows 2008 R2) с добавленной ролью контроллера домена (домен **test.local**). Клиентский компьютер **COMP2** (ОС Windows7 и выше), подключенный к домену test.local. На компьютере и сервере присутствуют только локальные пользователи **Администратор**. Политики безопасности операционных систем имеют настройки по умолчанию. Жесткие диски разбиты на 2 тома C:\ и D:**. 2 флеш-накопителя.**

Задачи:

1. Обеспечить возможность использования **BitLocker** на сервере WIN2008 и зашифровать с его помощью один из флеш-накопителей (для ускорения процесса шифрования рекомендуется использовать носитель малой емкости)
2. Установить сервис DeviceLock на клиентском компьютере COMP.
3. Создать в домене пользователей **USER1** и **USER2.**
4. С использованием групповых политик ограничить **только для USER1** возможность записи на нешифрованные носители информации.
5. С использованием DeviceLock ограничить доступ пользователей к USB, Floppy и DVD-ROM следующим образом.

USER1: Floppy, DVD-ROM – только чтение, USB – чтение и запись.
USER2: Floppy, DVD-ROM – запрет использования, USB – чтение и запись только на шифрованные носители информации.
При этом пользователям разрешено использовать только 2конкретныхфлеш-накопителя.

Самопроверка:

1. Проверить корректность настроек сети, выполнив команду ping win2008.test.local с клиентского компьютера COMP, а также ping comp.test.local с сервера win2008.

2. Проверить возможность записи данных только на шифрованных носитель под пользователями USER1 и USER2.

3. Проверить, что групповая политика применяется только на пользователя USER1, выполнив команду gpresult под пользователем USER2.

Вспомогательная литература и иные источники:

1. Комплект документации на DeviceLock.
2. Служба Active Directory. Ресурсы Windows Server 2008 (Windows Server 2008 Active Directory Resource Kit). Стэн Раймер, Конан Кезема, Майк Малкер, Байрон Райт.

Категория сложности № 3 (№ 1 без выполнения задачи № 1).

Тема 7. Доверенная загрузка

Задание 7.1. Организация доверенной загрузки с использованием СЗИ от НСД

Цель задания:

Изучение возможности обеспечения доверенной загрузки операционной системы с использованием исключительно программных механизмов СЗИ от НСД.

Начальная моделируемая инфраструктура:

Клиентский компьютер **COMP** (ОС Windows XP SP3 и выше). На компьютере присутствует только локальный пользователь **Администратор**. Политики безопасности операционных систем имеют настройки по умолчанию.

Задачи:

1. Установить на клиентский компьютер COMP СЗИ от НСД «DallasLock 8.0-C».
2. Обеспечить доверенную загрузку операционной системы с использованием возможностей СЗИ от НСД «DallasLock 8.0-C», выполнив преобразование диска с применением алгоритма XOR32. Область для преобразования выбрать самостоятельно.
3. Загрузиться с загрузочного диска и попробовать получить доступ к содержимому жесткого диска операционной системы. Объяснить результат в зависимости от выбранной области для преобразования.

Самопроверка:

1. Проверить наличие запроса на ввод PIN-кода перед началом штатной процедуры загрузки операционной системы.
2. Проверить невозможность просмотреть содержимое жесткого диска операционной системы при загрузке с внешнего носителя информации.

Вспомогательная литература и иные источники:

1. Комплект документации на СЗИ от НСД «DallasLock 8.0-C».

Категория сложности № 2.

Библиографический список

1. Дерек Мелбер. Групповая политика Windows. Ресурсы Windows Server 2008, Windows Vista, Windows XP, Windows Server 2003, М.: Русская Редакция, 2009.

2. Дэн Холме. Эффективное администрирование. Ресурсы Windows Server 2008, Windows Vista, Windows XP, Windows Server 2003 – СПб.: БХВ-Петербург, 2009.

3. Митч Таллоч, Тони Нортроп, Джерри Ханикатт, Эд Вилсон. Ресурсы Windows 7 – СПб.: БХВ-Петербург, 2011.

4. СтэнРаймер, КонанКезема, МайкМалкер, БайронРайт. Служба Active Directory. Ресурсы Windows Server 2008 – СПб.: Питер, 2009.

5. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. – М.: Гостехкомиссия, 1992.

6. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. – М.: Гостехкомиссия, 1992.

7. Средство защиты информации Secret Net 6. Руководство администратора. Управление. Основные механизмы защиты [Электронный ресурс] URL: http://www.securitycode.ru/_upload/editor_files/documentation/SN_6/Secret_Net_6_Admin_Guide.pdf (дата обращения: 15.10.2013).

8. Система защиты информации от несанкционированного доступа Dallas Lock 8.0. Руководство по эксплуатации [Электронный ресурс] URL: http://service.confident.spb.ru/_clients/Dallas/Full/files/DallasLock80C.zip (дата обращения: 15.10.2013).

9. Kaspersky Security Center. Руководство администратора. Версия программы: 10.0 [Электронный ресурс] URL: http://docs.kaspersky-labs.com/russian/kasp10.0_sc_admguideru.pdf (дата обращения: 15.10.2013).

10. DeviceLock Endpoint DLP Suite. Руководство пользователя. Версия продукта 7.3 [Электронный ресурс] URL: http://devicelock.com/ru/dl/DeviceLock%20Manual_ru.pdf (дата обращения: 15.10.2013).

11. Система гарантированного уничтожения информации на машинных носителях. СГУ - 2. Руководство системного программиста [Электронный ресурс] URL: http://www.cobra.ru/sites/default/files/prod/sgu2/sgu2-admin.doc (дата обращения: 15.10.2013).