Лабораторная работа 11. Разграничение доступа к устройствам

Цель лабораторной работы: практическое изучение принципов разграничения доступа к устройствам на основе программного продукта DeviceLock.

Задачи лабораторной работы:
1. Настройка DeviceLock Management Console
2. Разграничение доступа к устройствам
3. Белый список устройств
4. Аудит использования устройств
5. Теневое копирование файлов

Задание

Контрольные вопросы

Содержание лабораторной работы:

В данной работе рассмотрены приложения, позволяющие администратору компьютера или домена контролировать доступ пользователей к дисководам, CD/DVD - приводам, другим сменным устройствам, адаптерам WiFi и Bluetooth, а также к USB, FireWire, инфракрасным, COM и LPT-портам.

Контроль доступа может выполняться на двух уровнях: уровне интерфейса (порта) и уровне типа (съёмное устройство, принтеры, жёсткие диски и т.д.). Некоторые устройства проверяются на обоих уровнях, в то время как другие - только на одном: либо на уровне интерфейса (порта), либо на уровне типа.

DeviceLock состоит из трёх частей:

- *агента (DeviceLock Service). Агент устанавливается на каждый компьютер, автоматически запускается и обеспечивает защиту устройств на компьютере-клиенте;*
- *сервера (DeviceLock Enterprise Server). Это дополнительный необязательный компонент, используемый для централизованного сбора и хранения данных теневого копирования и журналов аудита;*
- *консоли управления. Это интерфейс контроля, который системный администратор использует для удалённого управления любой системой, на которой установлен агент.*

Рассматриваемые утилиты и приложения:

- *консоль управления DeviceLock Management Console. С её помощью можно просматривать и изменять разрешения и правила аудита, устанавливать DeviceLock Service, а также просматривать журналы аудита и теневого копирования для отдельных компьютеров.*

1. Настройка DeviceLock Management Console

Войдите под учётной записью «Администратор». Запустите «DeviceLock Management Console»: «Пуск - Программы - DeviceLock» (рис. 1). Доступ к консоли можно также получить через «MMC», добавив оснастку «DeviceLock Management Console».

Подключите консоль «DeviceLock Management Console» к управляемому компьютеру. Для этого в контекстном меню «Сервис DeviceLock» выберите «Подключиться...» (рис. 2). Дополнительно включите настройку «Подключаться к локальному компьютеру при запуске» для автоматического подключения сервиса.

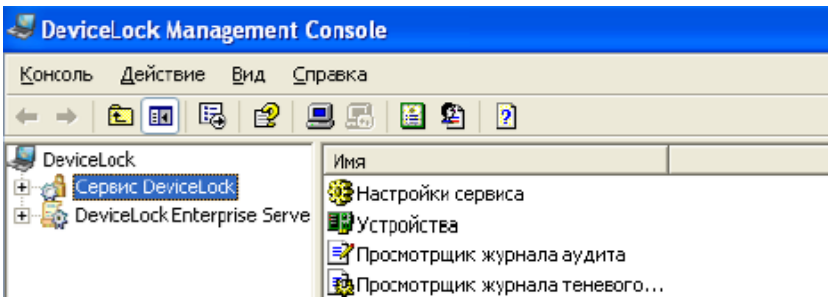

Рис. 1 - «DeviceLock Management Console»

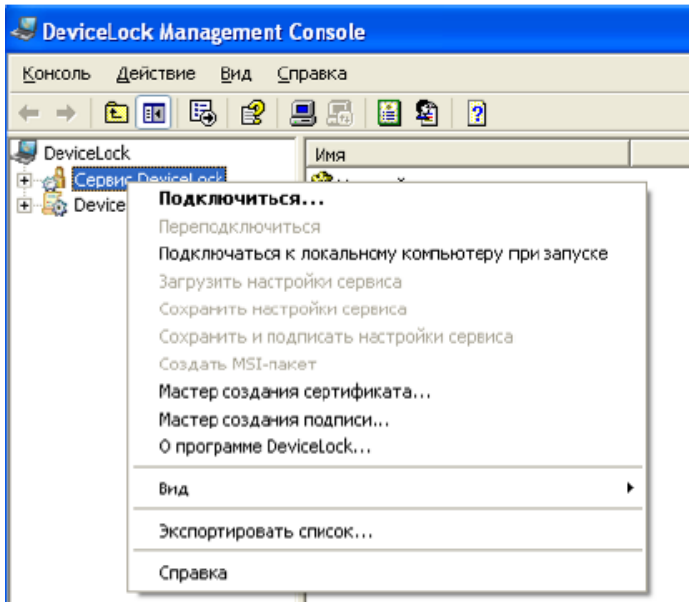

Рис. 2 - Подключение консоли DeviceLock

Перейдите во вкладку «Настройка сервиса - Администраторы DeviceLock». Добавьте в качестве администратора DeviceLock учётную запись «Администратор» (рис. 3). В данной вкладке можно добавить и других пользователей с возможностью ограничения доступа к оснастке (полный доступ, изменение, только чтение). Пользователи, не внесённые в список, не будут иметь доступ к оснастке управления разграничением доступа к устройствам.

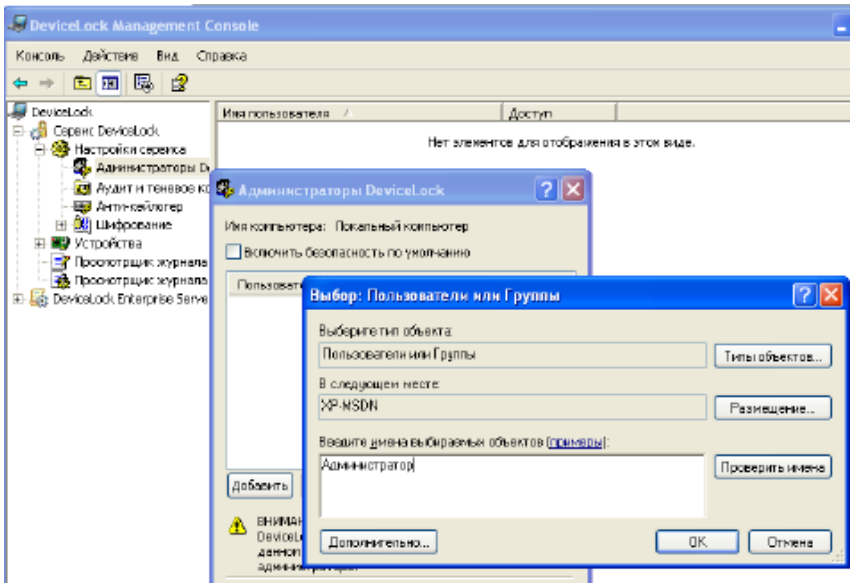

Рис. 3 - Добавление администратора DeviceLock

2. Разграничение доступа к устройствам

Когда пользователь пытается получить доступ к устройству, DeviceLock перехватывает запрос на уровне ядра ОС. В зависимости от типа устройства и интерфейса подключения (например, USB), DeviceLock проверяет права пользователя в соответствующем списке управления доступом (ACL). Если у пользователя отсутствуют права доступа к данному устройству, будет возвращено сообщение об ошибке - «доступ запрещён».

Перейдите в раздел «Устройства - Разрешения» (рис. 4)

Рис. 4 - Разрешения для устройств

Запретите доступ учётной записи «user» к приводу DVD/CD-ROM (рис. 5). Если на ПК установлено несколько CD/DVD-приводов, то можно воспользоваться белым листом устройств, для того чтобы выбрать определённый носитель.

Рис. 5 - Разрешения для DVD/CD-ROM

Войдите под учётной записью «user». Убедитесь, что доступ к CD/DVD - приводу запрещен.

Под учётной записью «Администратор» разрешите пользователю «user» только чтение файлов со съёмных носителей (рис. 6).

Рис. 6 - Разрешения для съемных устройств

Примечания:

- *если пользователь входит в какую-либо группу и у этой группы стоит полный доступ к устройству, то режим только чтение не будет работать (это связано с тем, что разрешения суммируются);*
- *если учётную запись не добавить в разрешения, то доступ ей будет запрещён.*

Войдите под учётной записью «user».

Подключите съёмный носитель и убедитесь, что запись на него невозможна.

DeviceLock предоставляет возможность разграничения доступа к устройствам по дням недели и времени суток.

Войдите под учётной записью «Администратор» и установите пользователю «user» полный доступ к съёмным устройствам в будние дни с 8:00 до 17:00 либо на время занятий (рис. 7).

Рис. 7 - Разграничения доступа к устройствам по дням недели и времени суток

Войдите под учётной записью «user». Подключите съёмный носитель и убедитесь, что доступ к нему разрешён.

Под учётной записью «Администратор» измените системное время на воскресенье.

Войдите под учетной записью «user» и проверьте запрет доступа к съёмному носителю.

3. Белый список устройств

Под учётной записью «Администратор» запретите доступ к USB- порту учётной записи «user» (рис. 8).

В случае с USB-устройствами DeviceLock в первую очередь проверит разрешения на уровне интерфейса (USB-порта), открыт или нет доступ к USB-порту. Затем, поскольку «Windows» определяет USB-флэш как съёмное устройство, DeviceLock также проверит ограничения на уровне типа устройства (съёмное устройство). Под учётной записью «user» проверьте запрет доступа к съёмному носителю.

Рис. 8 - Разрешения для USB-порта

Так как разграничению доступа подвергаются все USB-устройства, возникает необходимость делать исключения для USB-устройств, разрешённых к использованию в организации.

Исключения можно указывать двумя способами:

- *через «Настройки безопасности» (рис. 9);*
- *через «Белый список» на основе идентификации модели или конкретного экземпляра устройства.*

Рис. 9 - Настройки безопасности

Если в «Настройках безопасности» включить настройки управления каким-либо классом устройств, то к устройствам этого класса применяется разграничение доступа. Если настройка отключена, то использовать устройства данного класса могут все пользователи.

При использовании белого списка есть два варианта идентификации устройств:

1) *Device Model - описывает все устройства одной и той же модели. Каждое устройство идентифицируется по комбинации идентификатора производителя (VID) и продукта (PID).*
   Комбинация VID и PID описывает конкретную модель, но не конкретное устройство. Это значит, что все устройства данной модели данного производителя будут распознаны как одно устройство.
2) *Unique Device - описывает конкретное уникальное устройство. Каждое устройство идентифицируется по комбинации идентификатора производителя (VID), продукта (PID) и серийного номера.*

Устройство может быть добавлено в белый список как уникальное устройство только в том случае, если производитель присвоил ему серийный номер на этапе изготовления.

Перед тем как устройство может быть авторизовано через белый список, оно должно быть добавлено в базу данных. Перейдите во вкладку «Устройства - Белый список USB», в контекстном меню выберите «Управление». В появившемся окне (рис. 10) перейдите в «Базу данных USB-устройств».

Рис. 10 - Белый список USB-устройств

Добавьте в «Базу данных устройств» те USB-устройства, к которым необходимо разрешить доступ, выбрав устройство и нажав кнопку «Добавить» (рис. 11).

Рис. 11 - База данных USB-устройств

Разрешите пользователю «user» доступ к USB-устройству из базы данных. Для этого добавьте учётную запись «user» и из «Базы данных USB-устройств» выберите необходимые устройства (рис. 12).

Рис. 12 - Добавление устройства в белый список пользователя

4. Аудит использования устройств

Кроме функции контроля доступа, DeviceLock позволяет осуществлять протоколирование и аудит использования устройств пользователями на локальном компьютере.

Чтобы включить протоколирование действий пользователя, необходимо установить соответствующие права аудита.

1) *Чтение/запись - протоколируются попытки пользователя читать/записывать данные. Для типов устройств «Bluetooth, FireWire- порт, ИК-порт, Параллельный порт, последовательный порт, USB-порт и WiFi».*
2) *Печать - протоколируются попытки пользователя посылать документы на принтеры. Применимо только к типу «Принтер».*
3) *Выполнение - протоколируются попытки пользователя удаленно выполнить код на стороне устройства. Применимо только к типу «Windows Mobile».*
4) *Чтение/запись не файлов - протоколируются попытки пользователя читать/записывать не файловые объекты (календарь, контакты, задачи и т.п.). Применимо только к типам «Windows Mobile» и «Palm».*

Существует возможность протоколировать успешный доступ к устройствам и ошибки доступа:

1) *«Аудит разрешений» - все попытки доступа, которые были разрешены DeviceLock, т.е. пользователю был предоставлен доступ к устройству.*
2) *«Аудит запретов» - все попытки доступа, которые были заблокированы DeviceLock, т.е. пользователю был запрещён доступ к устройству.*

Перейдите в раздел «Устройства - Аудит и теневое копирование». Примените к съёмным устройствам аудит для пользователя «user» (рис. 13).

Рис. 13 - Настройка аудита для съёмных устройств

Убедитесь, что пользователю «user» разрешён доступ к съёмным устройствам. Войдите под учётной записью «user», подключите съёмное устройство и скопируйте на него образцы рисунков «Windows» из каталога «*\Мои документы\Мои рисунки\Образцы рисунков».

Войдите под учётной записью «Администратор».

Доступ к результатам аудита можно получить во вкладке «Просмотрщик журнала аудита» (рис. 14).

Журналы аудита могут храниться как в стандартных журналах ОС «Windows», так и в журналах DeviceLock. Перейдите во вкладку «Настройка сервиса - Аудит и теневое копирование» (рис. 15).

Опция - «Тип журнала аудита» устанавливает вид журнала и может принимать три значения:

- *«Журнал событий» - данные аудита записываются только в стандартный журнал «Windows», хранящийся на локальном компьютере;*
- *«Журнал DeviceLock» - данные аудита записываются только в собственный защищённый журнал, отсылаемый на DeviceLock Enterprise Server для централизованного хранения;*
- *«Журнал событий и DeviceLock» -запись в оба журнала.*

Рис. 14 - Просмотрщик журнала аудита

Рис. 15 - Вкладка «Настройка сервиса - Аудит и теневое копирование»

Для того чтобы просмотреть журнал аудита через стандартный журнал «Windows», запустите консоль управления «Пуск - Выполнить - MMC». В ней добавьте оснастку «Просмотр событий». Вкладка «DeviceLock Log» предоставляет журнал аудита (рис. 16).

Рис. 16 - Вкладка «Devicelock Log»

5. Теневое копирование файлов

Теневое копирование позволяет сохранять копии всех файлов, которые пользователь копирует на съёмные носители или отправляет на печать. Сохранённые файлы могут быть в дальнейшем проанализированы на предмет наличия в них конфиденциальной информации.

Перейдите в раздел DeviceLock «Устройства - Аудит и теневое копирование». Включите для пользователя «user» теневое копирование файлов на съёмные устройства (рис. 17).

Рис. 17 - Включение теневого копирования для съёмных устройств

Под учётной записью «user» подключите съёмное устройство и скопируйте на него текстовый или графический файл.

Под учётной записью «Администратор» откройте раздел DeviceLock «Просмотрщик журнала теневого копирования» (рис. 18).

Рис. 18 - Просмотрщик журнала теневого копирования

Откройте появившуюся в журнале запись. Это позволит увидеть содержимое файла, скопированного пользователем «user» на съёмное устройство.

Выбор места хранения теневых копий файлов возможен в разделе «Настройки сервиса - Аудит и теневое копирование - Локальная директория» (рис. 19).

Рис. 19 - Каталог хранения для теневого копирования

Задание

Учётной записи «user» установите разрешения в соответствии с вариантом.

Вариант 1

DVD/CD-ROM	Принтер	Жёсткий диск
Только чтение. Добавьте один носитель в белый список. Полный доступ к виртуальным приводам	Доступ по будням. Аудит печати и запретов доступа	Полный доступ. Аудит чтения и записи

Вариант 2

Съёмные устройства	USB-порт	WIFI
Чтение и извлечение	Аудит всех событий	Доступ по будням

Вариант 3

Съёмные устройства	USB-порт	DVD/CD-ROM
Чтение и извлечение	Запрет доступа к сканерам, принтерам, устройствам хранения usb. Добавьте 3 устройства в белый список	Доступ только по будням с 17 до 19 часов. Аудит записи и разрешений

Вариант 4

WindowsMobile	Съёмные устройства	USB-порт
Только чтение. Аудит всех событий	Запрет доступа вне рабочего времени	Только чтение. Добавить в белый список 2 устройства

Вариант 5

Параллельный порт	Жёсткий диск	Съёмные устройства
Запрет доступа.	Доступ по будням с 8 до 20 часов.	Чтение и извлечение. Аудит всех событий.

Вариант 6

DVD/CD-ROM	WindowsMobile	Съёмные устройства
Только чтение. Аудит всех событий.	Доступ без ограничений. Аудит всех событий.	Чтение и извлечение. Аудит всех событий вне рабочего времени.

Вариант 7

Последовательный порт	USB-порт	Принтер
Запрет доступа вне рабочего времени. Доступ к модемам, подключаемым через данный порт, без ограничений.	Запрет доступа. Добавить 4 устройства в белый список.	Доступ с 8 до 18 часов. Аудит всех событий.

Вариант 8

Bluetooth	Параллельный порт	WindowsMobile
Доступ без ограничений.	Доступ по будням.	Доступ без ограничений. Аудит записи.

Вариант 9

DVD/CD-ROM	USB-порт	Жёсткий диск
Только чтение.	Чтение, извлечение.	Аудит всех событий.

	Добавить в белый список 3 устройства.	

Вариант 10

FireWire-порт	WIFI	Съёмные устройства
Только чтение. Аудит записи и запретов.	Доступ в рабочее время. Аудит чтения и записи.	Запрет доступа. Аудит запретов.

Контрольные вопросы

1. Существует ли возможность разграничения доступа к управлению приложением DeviceLock?
2. В чём отличие уровня интерфейса от уровня типа устройств?
3. Какие функции разграничения доступа к ресурсам предоставляет DeviceLock?
4. Каким образом можно исключить классы USB-устройств (например, мыши, клавиатуры и т.п.) из механизма разграничения доступа?
5. Для чего используются белые списки?
6. К каким классам устройств могут быть созданы белые списки?
7. Какие варианты идентификации устройства применяются в белом списке?
8. Для чего используется база данных устройств?
9. Где могут храниться журналы аудита работы с устройствами?
10. Для чего используется теневое копирование файлов?

Задание

Отчет по лабораторной работе выполняется по стандарту, описанному в методических указаниях