Управление внешними запоминающими устройствами

Контроль использования информации, перемещаемой за периметр локальной сети компании, — одна из главных задач службы информационной безопасности. С каждым годом эта работа все усложняется. Резко возросло число всевозможных USB-накопителей и их объем (диски в 4 Гбайт уже давно не редкость); переносные MP3-плейеры с жестким диском, фотоаппараты, мобильные телефоны — все они имеют большой объем памяти. Рынок таких устройств демонстрирует экспоненциальный рост, при этом размеры устройств становятся все меньше, а производительность и объем переносимых данных — все больше.

Постоянно увеличиваются инвестиции в межсетевые экраны, разрабатываются все новые способы шифрования данных, различные средства и технологии контроля для защиты данных. Однако не стоит забывать, что все эти меры не способны остановить попытки хищения данных со стороны собственных сотрудников, приносящих на работу флэш-диски и скачивающих на них конфиденциальную информацию. Все эти технологии не в состоянии воспрепятствовать обиженным сотрудникам, которые вполне могут использовать USB-устройства для загрузки вредоносной программы в сеть. Именно поэтому и был разработан целый класс программного обеспечения контроля сменных носителей.

В данной статье мы с вами рассмотрим два возможных способа контроля внешних носителей, желательно без покупки дополнительного программного обеспечения.

Управление внешними запоминающими устройствами в Windows 7

Начиная с операционной системы Windows Vista, компания Microsoft встраивает в операционные системы возможность управлять использованием внешних запоминающих устройств с помощью локальных (групповых) политик. В данном разделе мы попытаемся разобраться, как управлять внешними устройствами с помощью политик Windows 7.

Для использования режима контроля над применением внешних носителей в Windows 7 администратор должен задействовать групповые (локальные) политики. При помощи групповых политик он может указать конкретные устройства, использование которых на данном компьютере разрешено.

Управление с помощью ID устройства

Предположим, что сотруднику приказом выделен флэш-диск A, но из дома он может принести еще и флэш-диск B. Средствами групповых политик в Windows 7 можно сделать так, что флэш-диск A работать будет, а при включении флэш-диска B сотрудник получит сообщение о том, что он нарушает политику безопасности. Давайте рассмотрим подробнее, как это осуществить.

Каждое устройство, использующее USB-порт, обладает так называемым уникальным цифровым идентификатором. То есть для создания списка разрешенных устройств нам вначале нужно получить идентификаторы (ID) этих устройств.

Для получения соответствующего ID устройства подсоедините его к USB-порту, дождитесь, пока система опознает его, и запустите диспетчер устройств Device Manager. В появившемся списке устройств раскройте узел Universal Serial Bus controllers и выберите USB Mass Storage Device. Для вызова контекстного меню нажмите правую клавишу и выберите пункт Properties. Затем выберите Details. В раскрывающемся списке Property укажите пункт Bus relations (см. рис. 1).

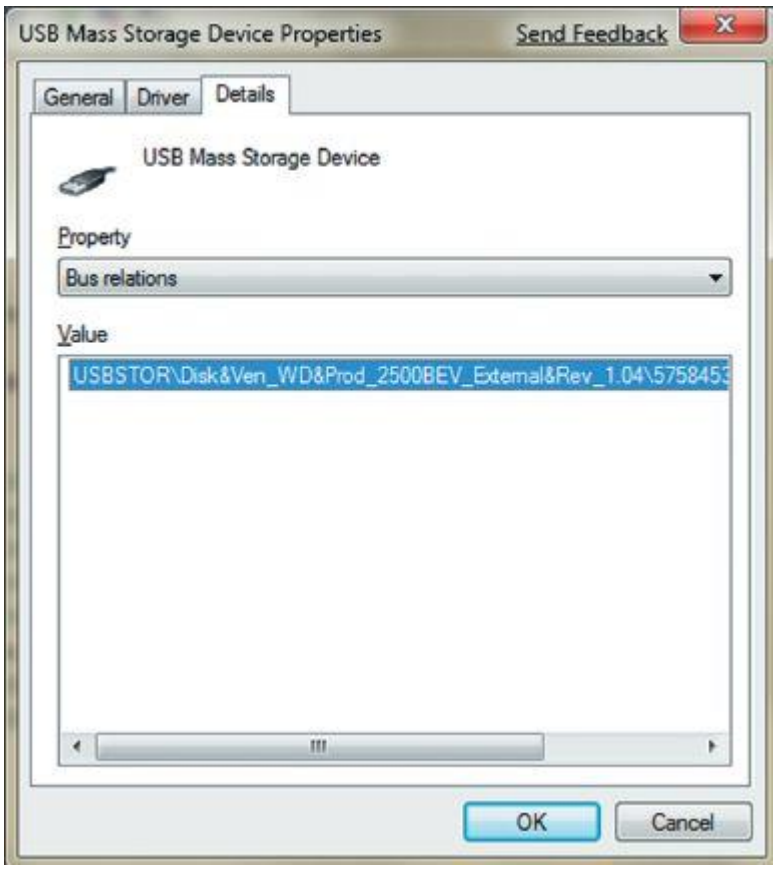

Рисунок 1 USB Mass Storage Device Properties

Скопируйте значение параметра в любой текстовый редактор. Вы получите строку типа USBSTOR\Disk&Ven_WD&Prod_2500BEV_External&Rev_1.04\575845323038443536353234&0.

Из полученной строки нужно выделить подстроку 57584532303844353635323 4 от последнего символа \ до &. Это и будет искомое имя устройства.

После получения уникального ID устройства можно перейти к настройке групповых политик. Для настройки групповых политик в режиме командной строки запустите команду gpedit.msc. В появившемся окне групповых политик выберите Computer Configuration — Administrative Templates — System — Device Installation (экран 2).

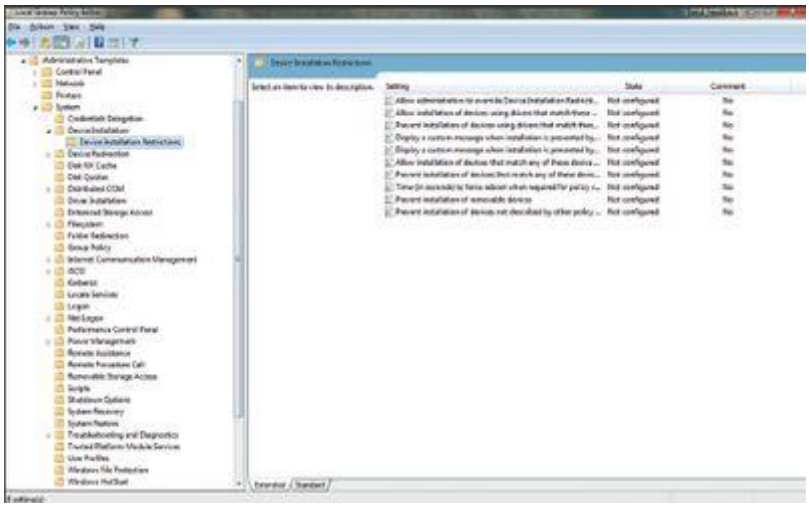

Рисунок 2 Окно групповых политик

Далее выберите настройку Allow installation of devices that mach any of these device IDs () и, чтобы разрешить установку в открывшемся окне, добавьте или удалите ID устройства (экран 3).

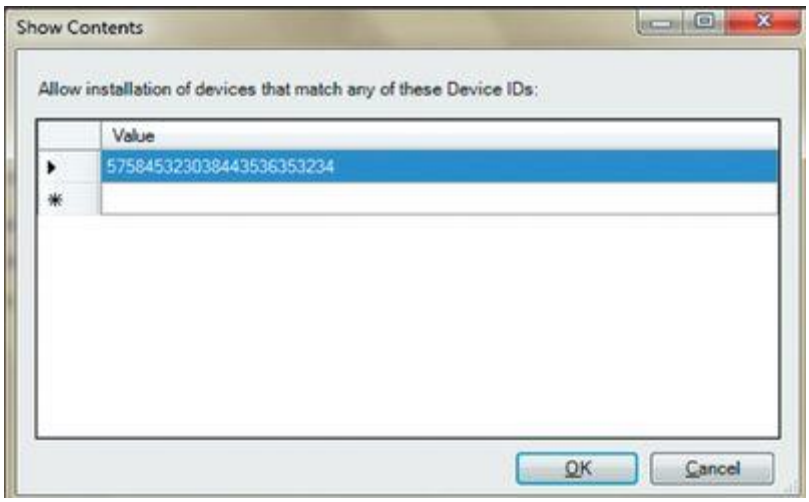

Рисунок 3 ID устройства

После создания списка разрешенных устройств нужно запретить установку всех остальных, включив настройку Prevent installation of devices not described by other policy settings.

Вместе с тем стоит учесть, что теперь вы сможете запретить установку сменных носителей вообще. Для этого служит правило, приведенное на экране 4.

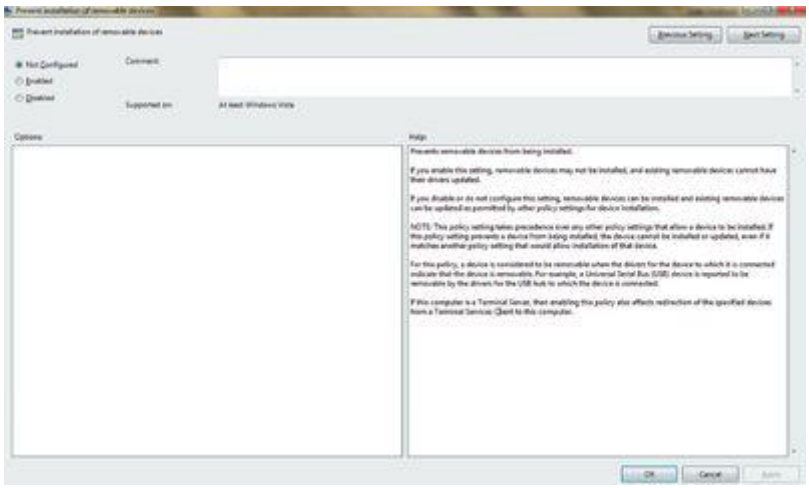

Рисунок 4 Запретить установку сменных носителей вообще

Данное правило политики препятствует установке сменных устройств. Существующие сменные устройства не смогут при этом обновлять свои драйверы. Данное правило имеет приоритет по отношению к любым другим параметрам настройки политики установки сменных устройств. Для этого правила признаком того, что устройство является сменным, служит драйвер устройства, с которым оно связано.

Вместе с тем администратор может создать «черный» список устройств, которые не могут быть установлены на данном компьютере, включив настройку Prevent installation of devices that match any of these devices IDs.

Текст, введенный в окне правила Display a custom message when installation is prevent by policy (balloon text), определяет сообщение, которое пользователь видит в окне уведомления в случае, если политика запрещает установку устройства. Этот текст будет отображен как основной текст сообщения, выводимого Windows всякий раз, когда установка устройства будет запрещаться политикой. Заголовок окна уведомления может быть настроен и с помощью настройки Display a custom message when installation is prevent by policy (balloon title).

Однако не стоит забывать, что данный способ запрета внешних устройств будет работать только в домене Windows Server 2008R2 клиентский ПК – Windows 7.

Однако, согласитесь, ведь ваши задачи могут не только требовать чтобы на работе сотрудники работали со строго определенными флешками. Т.е. вполне возможен вариант, когда некоторым вашим сотрудникам необходим доступ к USB-флеш по чтению, некоторым запретить совсем, а некоторым (например, администратору ИБ) – полный доступ.

Для решения данной задачи необходимо применять стороннее программное обеспечение.

Рассмотрим, как решить данную задачу с помощью корпоративного антивирусного программного обеспечения от «Лаборатории Касперского» Kaspersky Work Space Security.

Управление внешними запоминающими устройствами с помощью Kaspersky Endpoint Security 8.

С помощью данного ПО вы можете блокировать устройства по типу (сменные носители, CD/DVD, Wi-Fi, портативные устройства (MTP[1]) и др.) или по типу шины.

Для некоторых из устройств можно явно задать время действия запрета, ввести его для отдельных операций или сделать исключение для некоторых пользователей. Это можно сделать для:

- Съемных дисков
- CD/DVD
- Дискет
- Стримеров
- Жестких дисков

Полностью вы можете отключить:

- модемы
- внешние сетевые адаптеры
- WiFi
- Принтеры
- Устройства чтения смарт-карт
- Мультифункциональные устройства
- Windows CE USB ActiveSync устройства
- Портативные устройства (MTP)
- Bluetooth

Сканеры и устройства для обработки изображений можно отключить только полностью отключив шину по которой они подключаются:

- USB (мышь и клавиатуру заблокировать нельзя)
- FireWire
- Infra-Red
- Serial Port
- Parallel Port
- PCMCIA

[1] К портативным устройствам (MTP) относятся мобильные телефоны, iPod, iPad, iPhone

Правила для устройств имеют более высокий приоритет. Т.е. если разрешить использование съемных дисков, то настройка USB-шины значения не имеет, флешка блокироваться не будет.

Для флешек, жестких дисков, дискет, CD/DVD можно задать ограничения на использование:

- Список учетных записей, которым они доступны Выбрать можно либо из доменных, либо локальных учетных записей.
- Типы операций и расписание запрещения (разрешения). Можно независимо управлять чтением и записью. Время задается в виде таблицы с точностью до часа и дня недели. Например, операции чтения с флешек и дисков разрешены в рабочие дни с 8-00 до 20-00, а операции записи могут производить только администраторы и только в рабочее время.

Вместе с тем стоит учесть, что в случае, когда пользователю все же необходимо предоставить пользователю временный доступ к заблокированному устройству, этот доступ можно предоставить.

В случае если пользователь обнаруживает что нужное ему устройство заблокировано, он может сгенерировать, используя локальный интерфейс KES, уникальный ключ и переслать его администратору по электронной почту. В свою очередь администратор, рассмотрев запрос, может выслать пользователю специальный код доступа.

При получении кода доступа пользователь его активирусет.

После этого доступ к выбранному устройству (и только к нему) будет временно открыт на период времени, указанный администратором.

Для того чтобы сформировать запрос, пользователь открывает интерфейс KES на закладке **Центр управления**

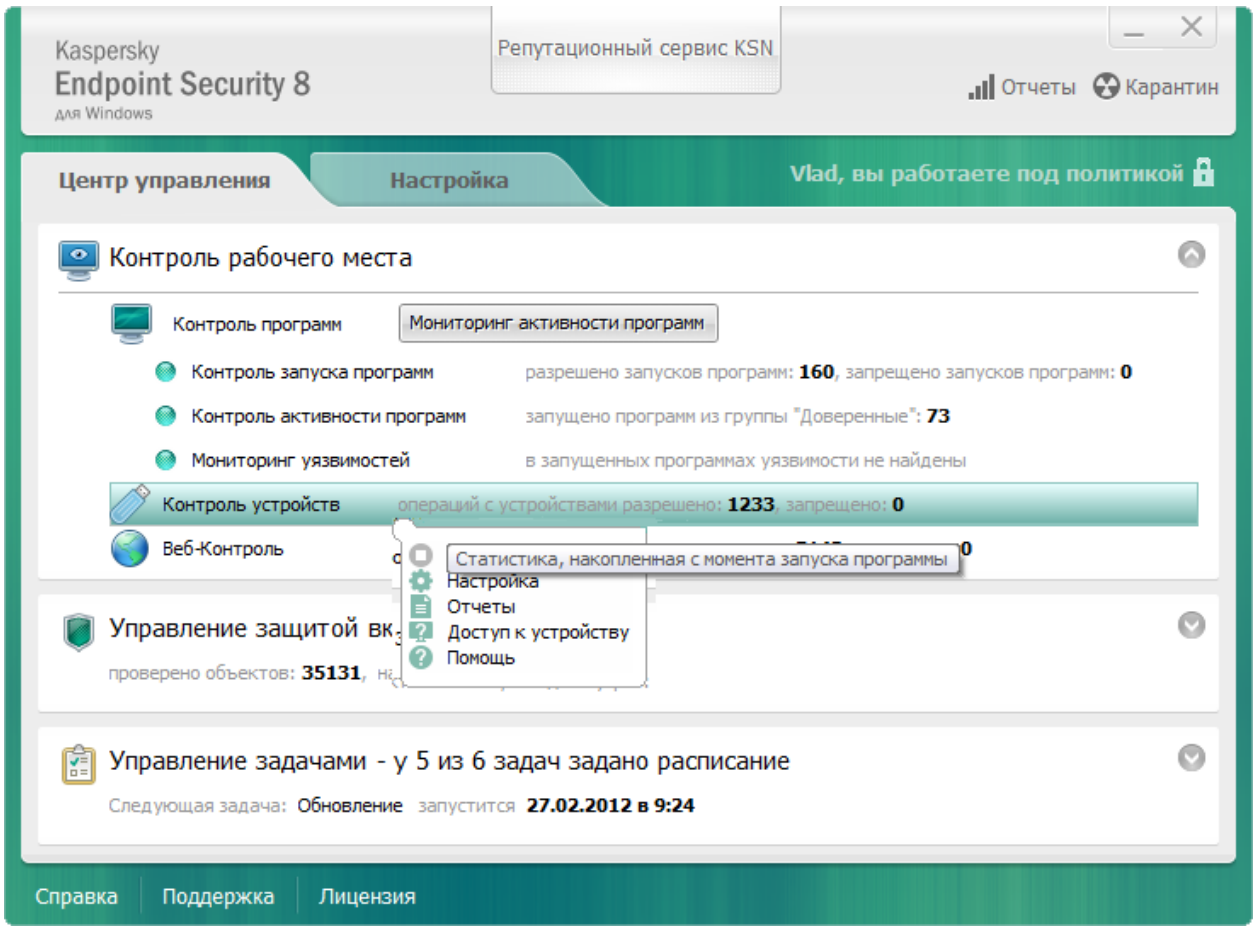

Рисунок 5 Центр управления. Доступ к устройству

В открывшемся окне будут перечислены все устройства, когда-либо получавшие доступ к компьютеру, в том числе заблокированные.

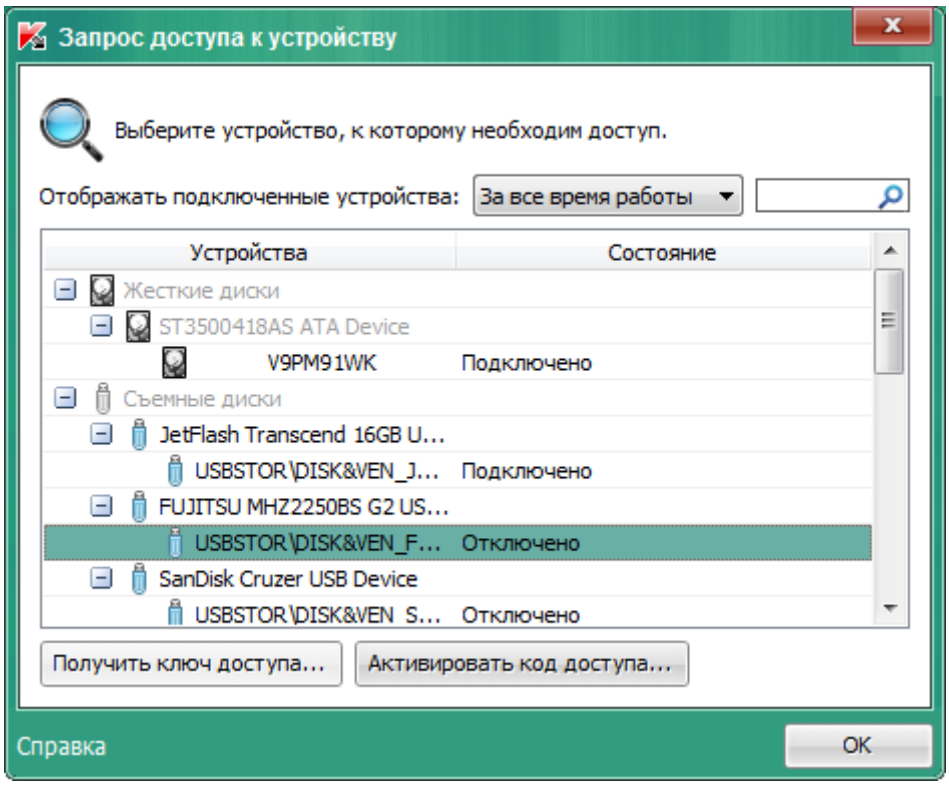

Рисунок 6 Запрос доступа к устройству

Здесь нужно найти то, к которому требуется доступ, выделить его и нажать **Получить ключ доступа.** Единственный настраиваемый параметр – желаемый период времени. По умолчанию – 24 часа.

Ключ, полученный в виде **.acode** файла пользователь должен переслать администратору.

Администратор на основе полученного ключа .acode генерирует ключ (файл ч расширением **.akey**) он пересылается обратно на клиентский ПК. Пользователь в том же окне выбирает кнопку **Активировать код доступа** и вводит полученный **.akey**-файл**.** Перезагрузка не требуется. Устройство доступно сразу же.

Запрет внешних носителей в Windows 8 Consumer Preview

Если вы работаете под управлением Windows 8 Consumer Previev, то для того чтобы разрешить работу лишь с определенными внешними носителями, вам придется провести весь цикл работ аналогично Windows 7.

Т.е. вначале с помощью диспетчера устройств выбрать ID разрешенного устройства (рис.7).

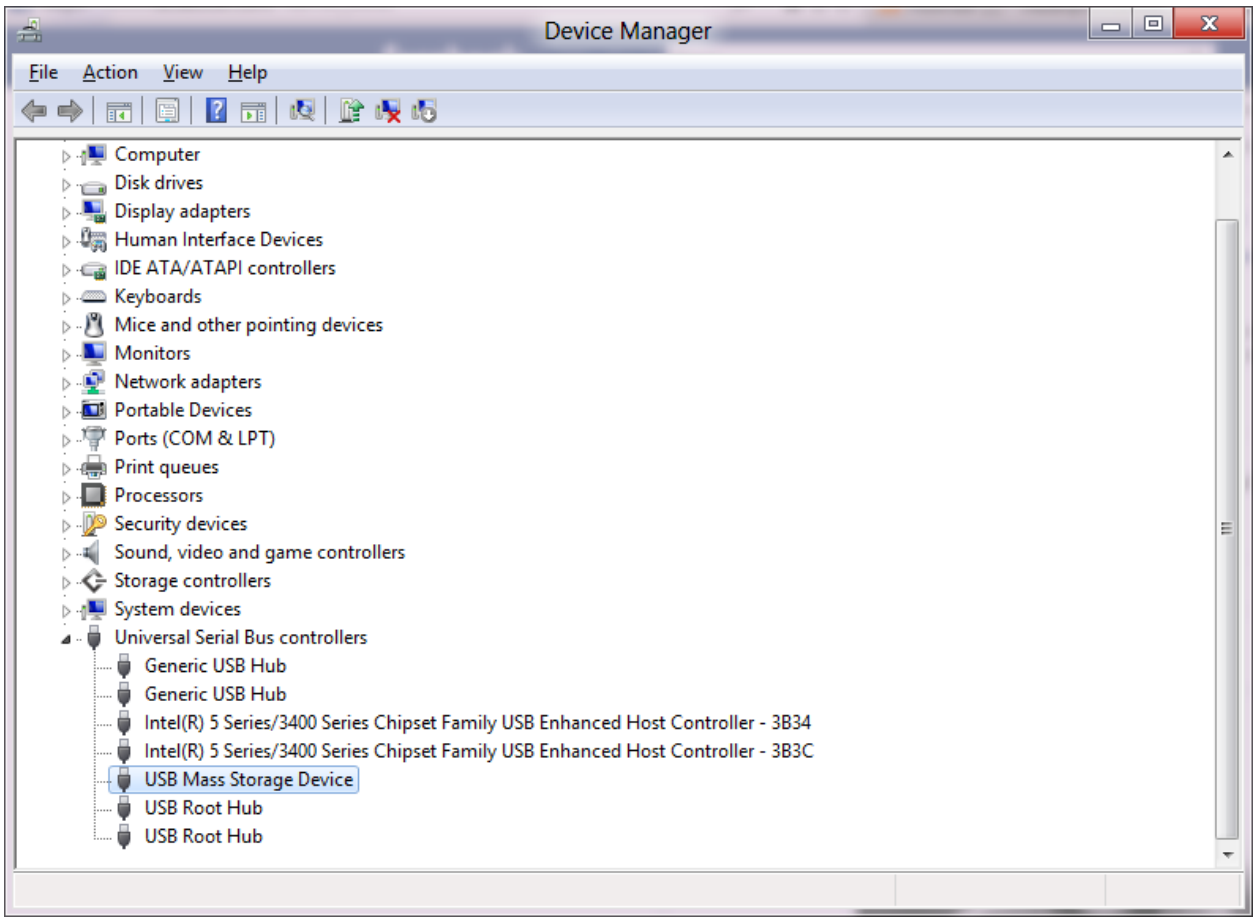

Рисунок 7 Диспетчер устройств

В данном случае выбрать USB Mass Storage Device и нажав правую клавишу на выбранном устройстве из меню выбрать свойства этого устройства (рис.8)

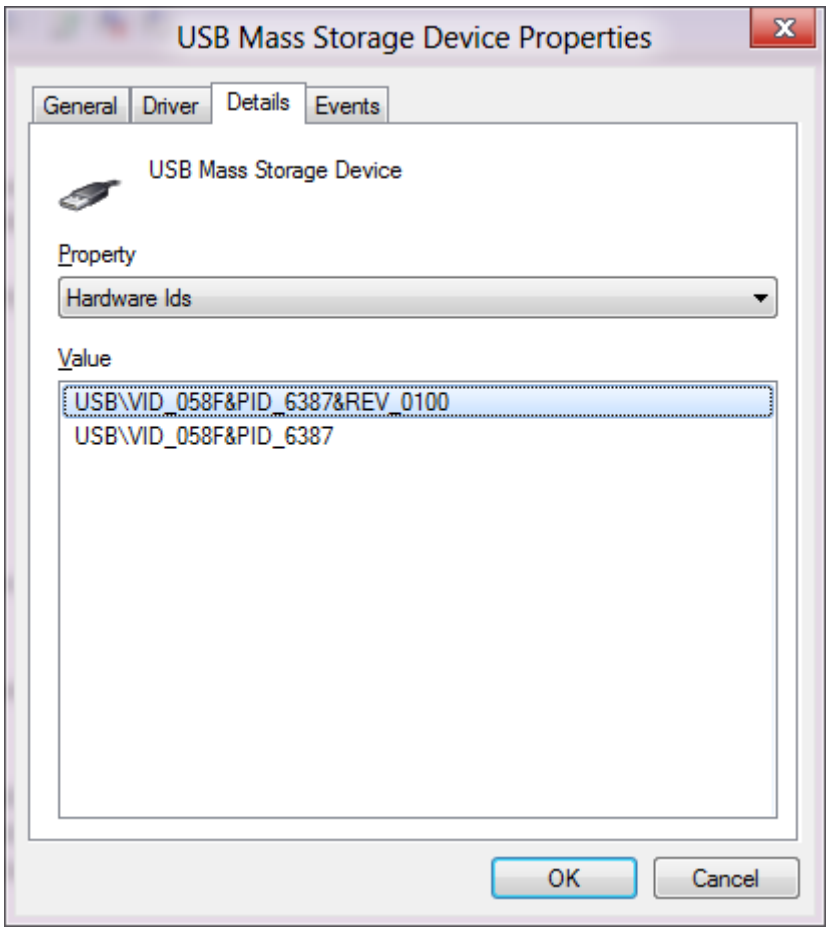

Рисунок 8 USB Mass Storage Device Properties

Выберите в строке Property значение Bus relations и скопируйте его в текстовый редактор. В нашем случае это USB\VID_058F&PID_6387&REV_0100

После этого необходимо перейти к настройке с помощью групповых политик.

Для этого наберите в командной строке gpedit.msc

В появившемся окне настройки параметров групповой политики (рис.9) выберите Computer Configuration — Administrative Templates — System — Device Installation — Device Installation Restrictions

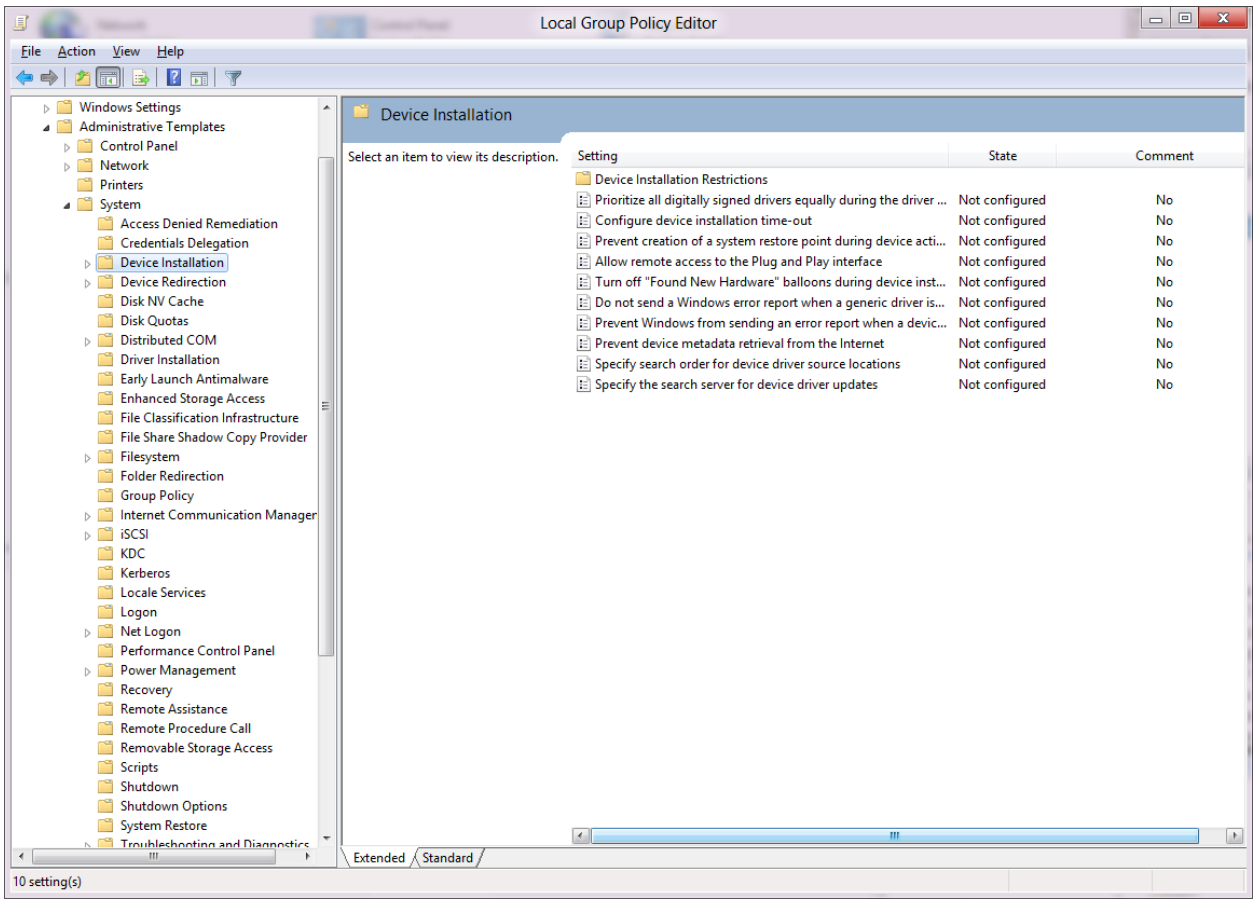

Рисунок 9 Локальный редактор групповой политики

Выберите параметр групповой политики Allow installation of devices that match any of these device IDs (рис.10).

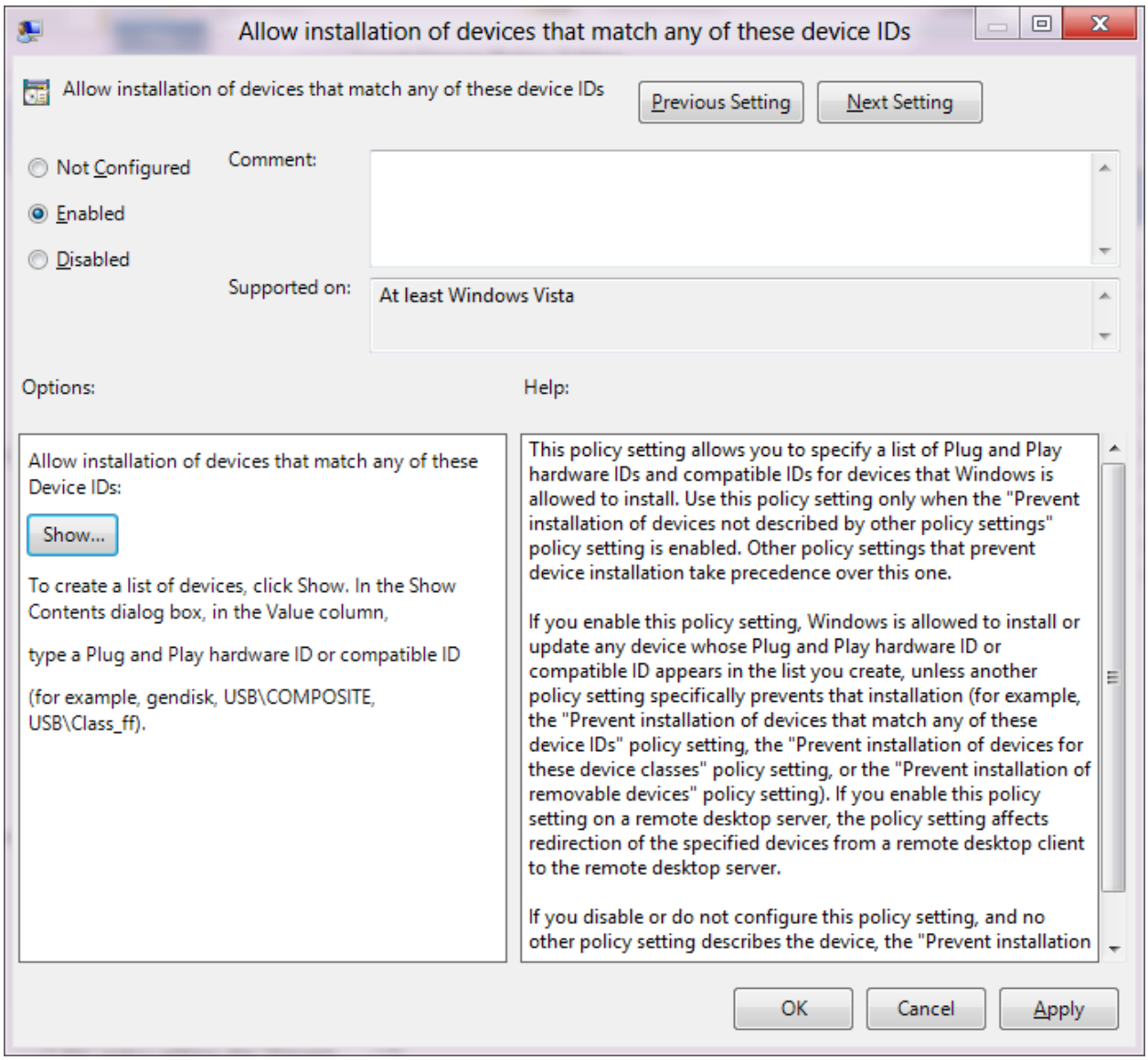

Рисунок 10 Allow installation of devices that match any of these device IDs

Выберите Enable - Show и в полученном окне (рис.11) введите hardware ID.

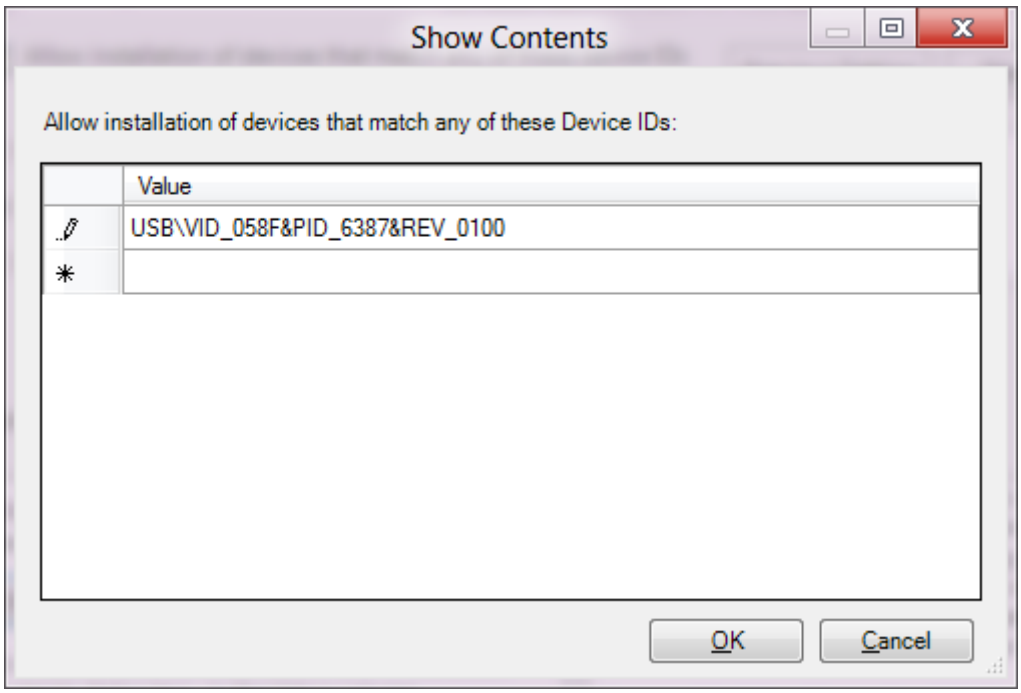

Рисунок 11 Device IDs

После того как вы внесете все разрешенные вами накопители в этот список, вы можете запретить установку всех остальных (рис.12)

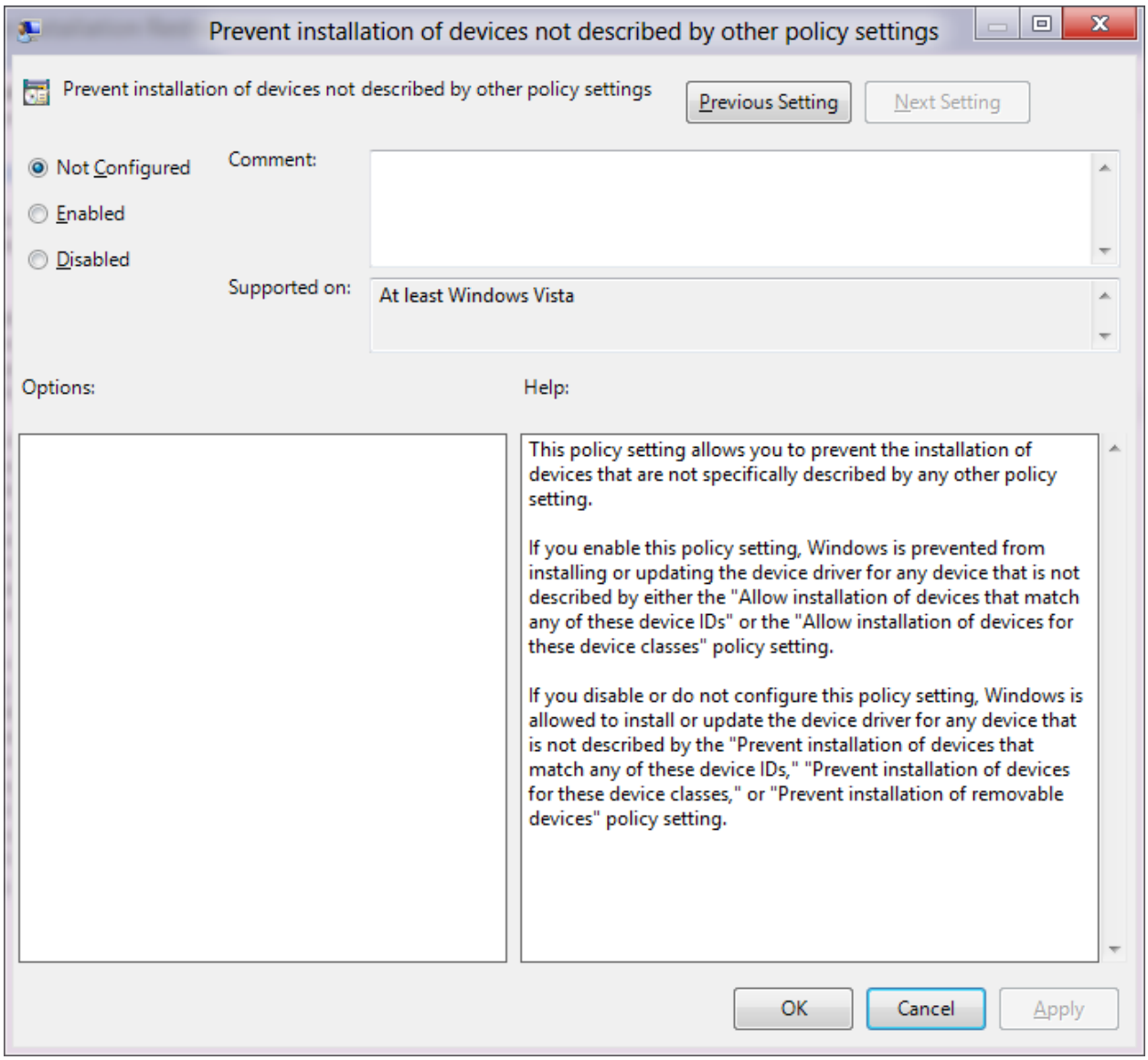

Рисунок 12 Запретить подключение внешних устройств, явно не описанных в групповой политике.

Рассмотрим дополнительно некоторые параметры групповой политики Windows 8, которые относятся к управлению внешними устройствами

Allow installation of devices using drivers that match these device setup classes

Данный параметр позволяет управлять подключением устройств, руководствуясь не ID устройства а его классом. Т.е. вы можете указать какие классы устройств можно подключать к данному ПК.

Prevent installation of devices using drivers that match these device setup classes

Данный параметр позволяет указать какие устройства (по классам) нельзя подключить к данному ПК.

Display a custom message when installation is prevented by a policy setting

Данный параметр политики позволяет создать сообщение (не более 128 символов), которое будет высвечено пользователю в том случае если установка соответствующего устройства запрещена политикой.

Prevent installation of devices that match any of these device IDs

Запретить установку устройств со следующими ID.

Вывод

Таким образом, можно сделать вывод, что на сегодня существует масса разнообразного ПО для решения задач, связанных с управлением внешними устройствами. Вам выбирать какое вы захотите использовать. Однако стоит понимать, что данная задача должна быть решена в целях обеспечения безопасности.