Шифрование BitLocker в Windows8 Developer Preview

Безмалый В.Ф.

MVP Consumer Security

Microsoft Security Trusted Advisor

О необходимости шифрования, а тем более шифрования мобильных компьютеров, написаны горы литературы. Но вместе с тем, увы, приходится констатировать, что шифрование применяют редко. Почему? Не знаю! И практически ежедневно мы получаем все новые и новые данные об утечках.

Приведем примеры.

North Central London, принадлежащий системе NHS, потеряли ноутбук, содержащий 8 млн. 300 тыс. записей, большая часть которых принадлежала онкологическим больным, со ссылкой на западные источники сообщает аналитический центр InfoWatch. За последние несколько лет последовала целая цепочка инцидентов утраты конфиденциальной информации: сотрудники теряли ноутбуки с данными, карты памяти, а в одном случае просто отправили данные об операциях не на тот номер факса.

В Торонто были потеряны 3 незашифрованных CD-ROM с персональными данными клиентов банка Scotiabank. Инцидент, как сообщило руководство, произошёл по недосмотру курьерской службы.

«Пакет с тремя CD пропал при внутренней курьерской пересылке из одного отдела в другой», – сообщил в своем письме Джо Конекни (Joe Konecny), представитель банка по связям с общественностью.

Из дома медицинского работника госпиталя Hull and East Yorkshire Hospitals NHS Trust был украден ноутбук, на котором содержалась персональная информация более тысячи пациентов. Не трудно догадаться, что информация зашифрована не была.

Следует отметить, что инцидент произошел еще в ноябре прошлого(2010) года, но доктор сообщил о пропаже только через несколько недель.

Такие точно истории приключается крайне регулярно. Типичнее просто некуда: украден или потерян ноутбук или флеш-накопитель с конфиденциальной информацией, которая не должна была покидать информационную систему предприятия.

Обширная статистика утечек учит нас, что она никого не учит. Всё равно работники беззаботно сливают служебные документы на мобильные носители, рассчитывая, что "со мной-то такое не случится". Увы, случается.

Руководству предприятий следует подумать не только о наказании провинившегося. Лучше внедрить принудительное шифрование всех носителей, которыми пользуются работники.

Данная статья будет посвящена обзору шифрования BitLocker в операционной системе Windows 8 Developer Preview. Хотелось бы, чтобы читатели понимали тот факт, что все что описано будет в данной статье, относится ТОЛЬКО к данному выпуску. Ведь вполне возможно, что к появлению релиза многие описанные параметры групповой политики будут изменены, а то и удалены, а вместо них могут появиться новые.

Установка BitLocker

Одним из первых, бросающихся в глаза, отличий при установке Windows 8 Developer Preview становится то, что служебный раздел для работы ОС занимает 350Мб (рис.1).

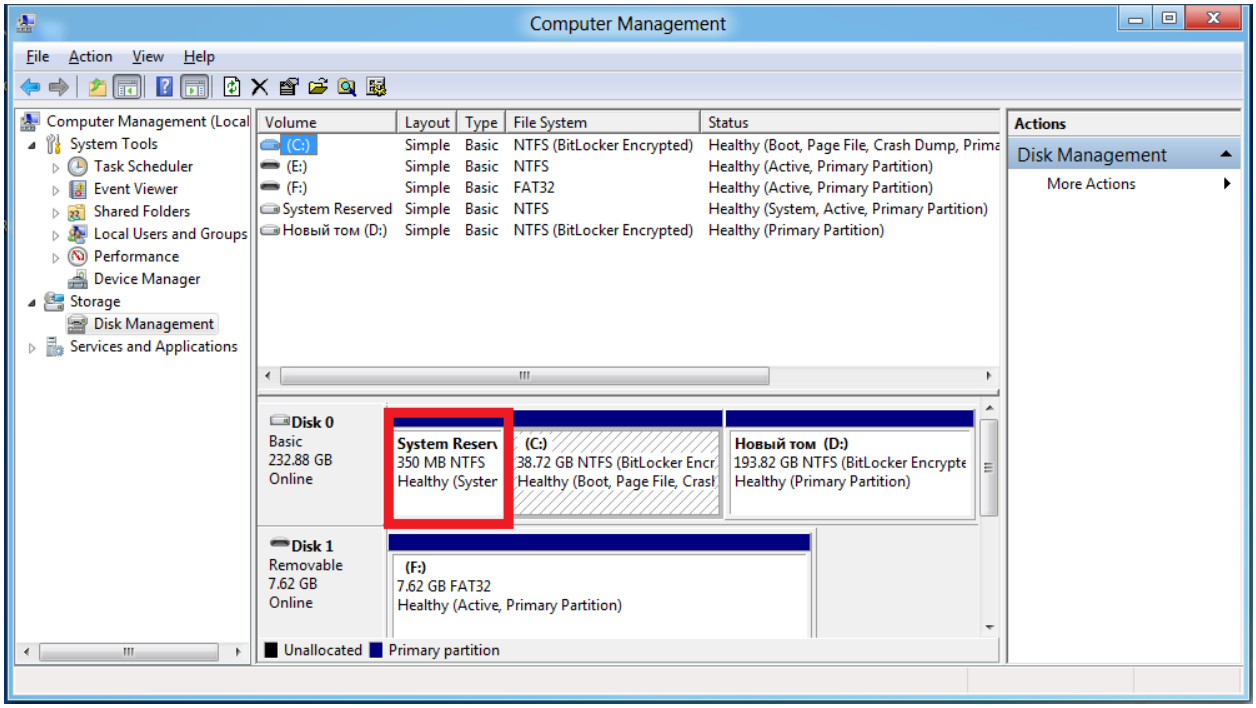

Рисунок 1 Диспетчер дисков. Красным цветом выделен служебный раздел

Еще на этапе установки BitLocker понимаешь, что в данной ОС, так же как и в предыдущей, специалисты Microsoft считают, что на вашем ПК уже по умолчанию установлен Trusted Platform Module (TPM) версии 1.2 (не ниже).

Это на самом деле правильно, но есть одно маленькое но… На просторах СНГ это, увы, не всегда так, поэтому мы с вами начинаем установку BitLocker с изменения параметров групповых политик.

Установка BitLocker без TPM

Для изменения параметров групповой политики необходимо, нажав Win+R вызвать окно Run и набрать команду **cmd**.

В появившемся окне командной строки набрать **gpedit.msc**

Появится окно Local Group Policy Editor (рис.2)

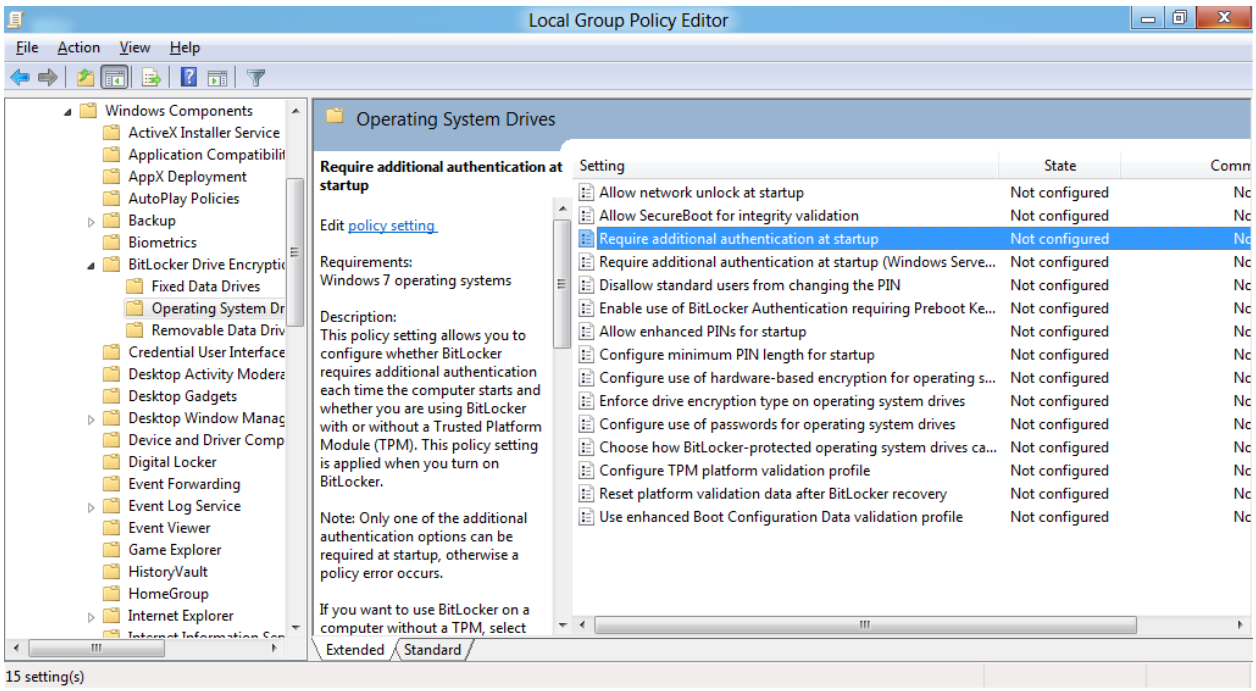

Рисунок 2 Local Group Policy Editor

В появившемся окне выбрать **Local Computer Police – Administrative Templates – Windows Components – BitLocker Drive Encryption – Operation System Drive – Require additional authentication at startup.**

Данный параметр политики позволяет указывать, необходима для дополнительная аутентификация при запуске (перезагрузке) ПК, а так же будете ли вы использовать BitLocker используя TPM или без него.

Внимание! При запуске требуется только одна из возможных опций.

В случае если вы собираетесь использовать BitLocker на компьютере без установленного TPM, необходимо установить флаг **"Allow BitLocker without a compatible TPM"**. В данном режиме для запуска вам потребуется либо пароль либо USB-ключ (обратите внимание, в Windows 7 это был только USB-ключ). Если вы используете USB-ключ, то происходит доступ к диску и дальнейшая загрузка ПК. В случае если USB-ключ (флешка) будет утеряна, вам удет необходимо восстановить доступ к диску, используя один из вариантов восстановления.

В случае если ваш ПК оборудован совместимым TPM, вы сможете использовать четыре метода аутентификации:

1. Только TPM
2. TPM+USB-карта, содержащая ключ
3. TPM+PIN (содержит от 4 до 20 цифр)
4. TPM+USB-ключ+PIN

Внимание! Если Вы хотите использовать PIN +USB-карту, вы должны сконфигурировать настройки BitLocker, используя режим командной строки вместо мастера BitLocker Drive Encryption.

После редактирования данного параметра необходимо применить параметры с помощью команды **gpupdate.exe /force**

Теперь можно приступить непосредственно к шифрованию. Для этого необходимо войти в «Мой компьютер», выбрать диск, содержащий операционную систему (я рекомендую шифровать его первым) и нажав правую клавишу, из контекстного меню выбрать Enable BitLocker (рис.3).

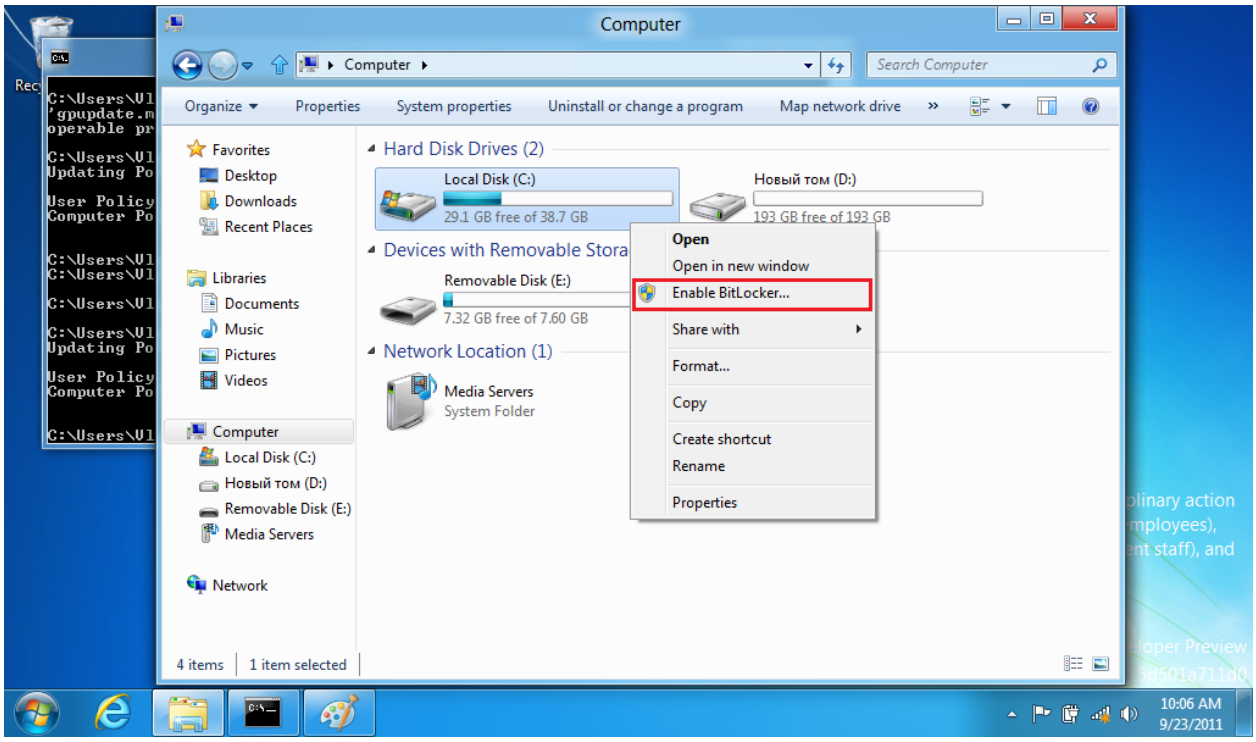

Рисунок 3 Шифрование системного раздела

После этого вам будет предоставлен выбор (рис.4):

1. Использовать USB-флеш для хранения ключа шифрования.
2. Использовать пароль для входа в систему

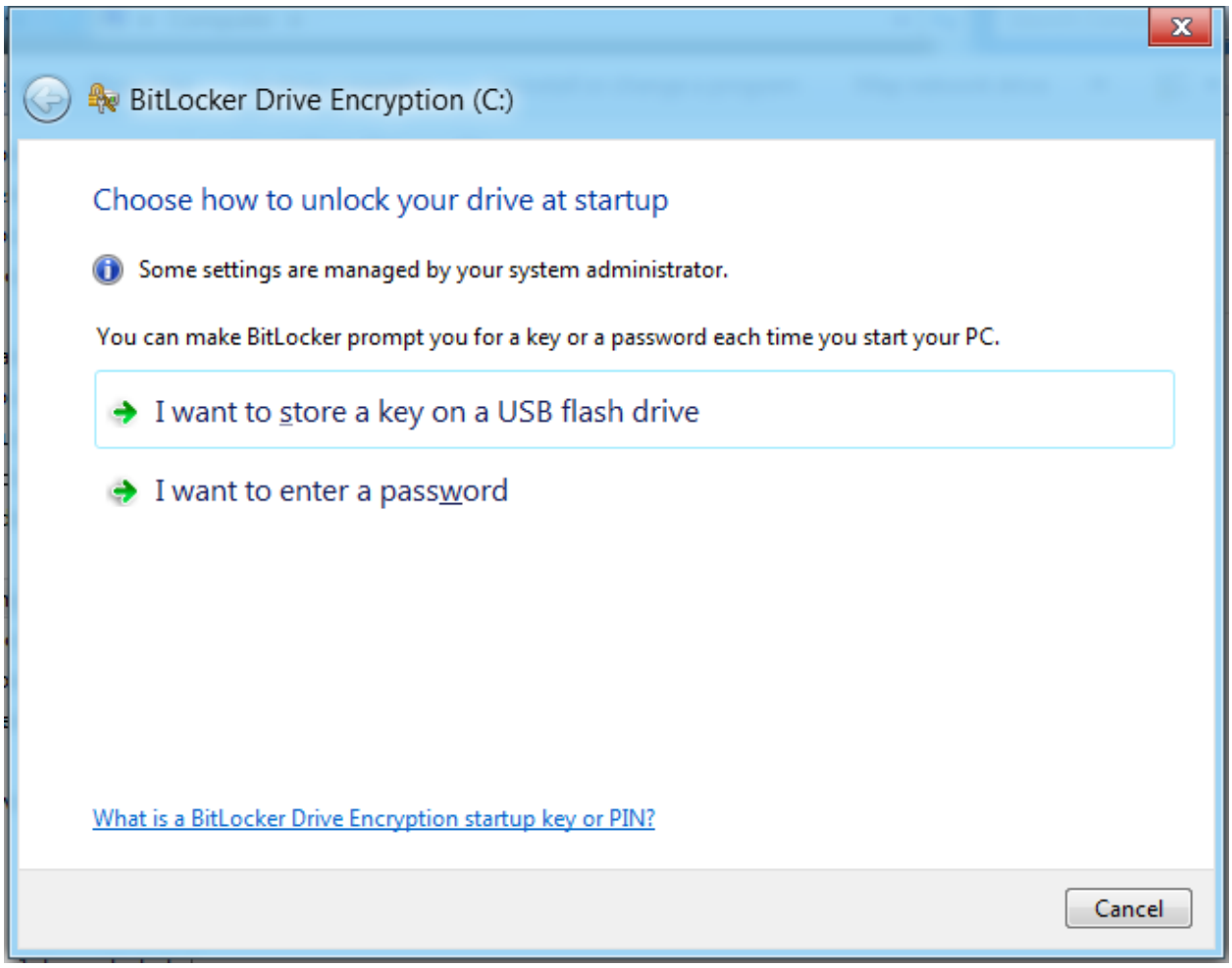

Рисунок 4 Выбор метода доступа к шифрованному разделу

Какой способ лучше? На мой взгляд пароль, если, конечно, это не пароль 1234. Можно выбрать USB-флешку, но, естественно, при этом помнить, что после загрузки, флешку нужно вынуть и положить в карман, а не в ту сумку, в которой вы носите ноутбук.

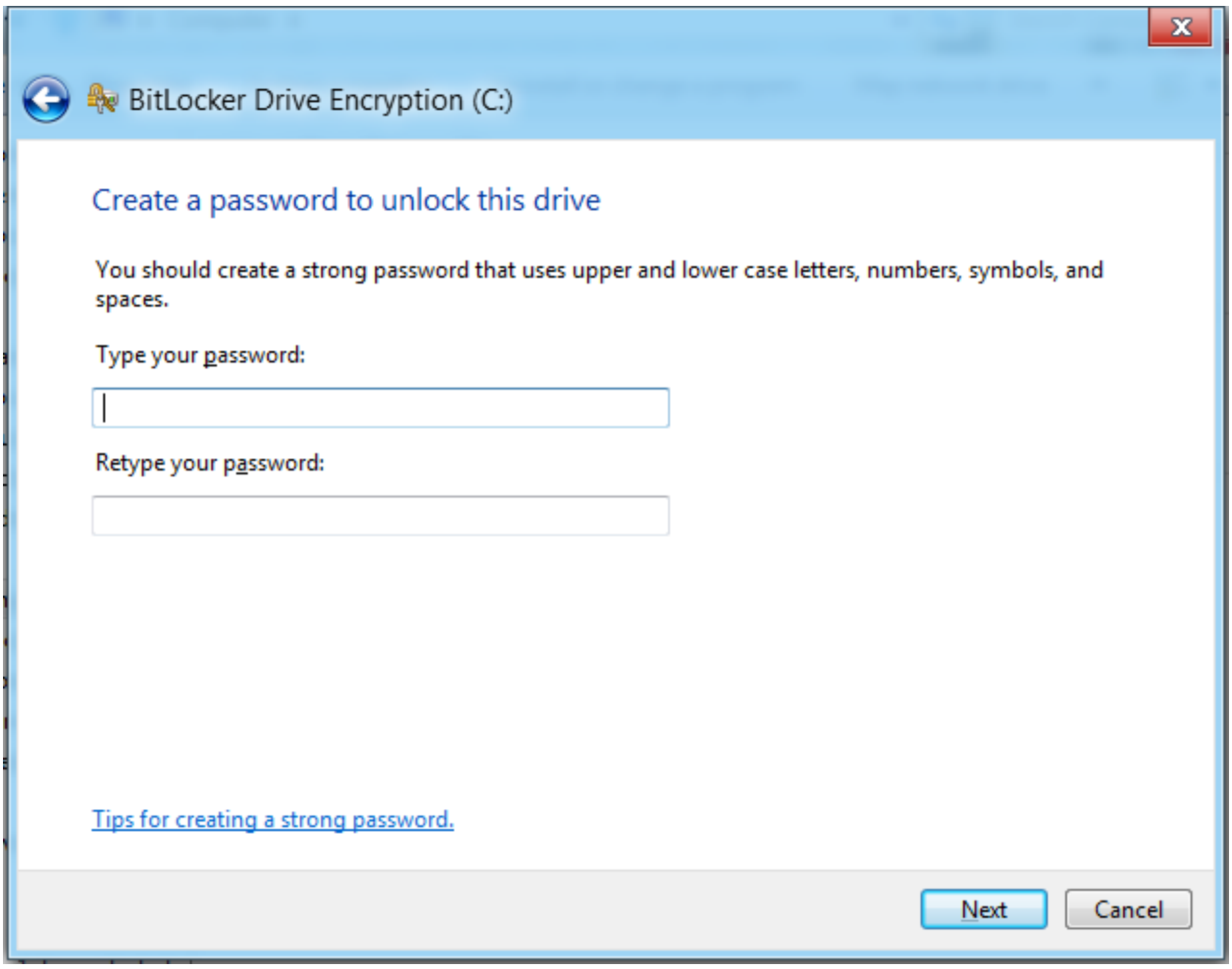

Рисунок 5 Создать пароль для доступа к диску

Естественно, после создания пароля, вам необходимо создать USB-флеш для возможного восстановления системы (рис.6).

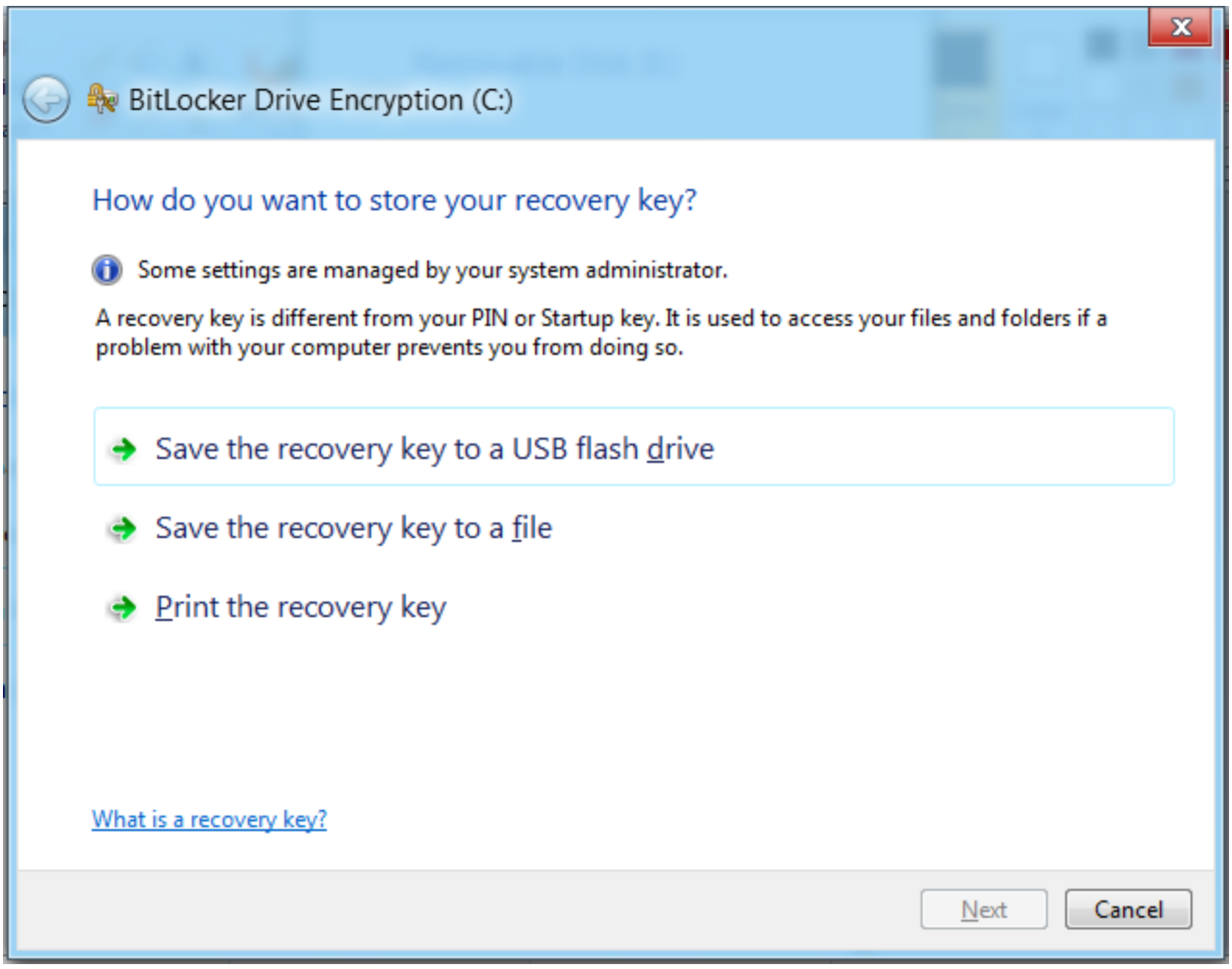

Рисунок 6 Сохраните ваш ключ восстановления

Для восстановления вам будет предложено три возможных сценария:

1. Сохранить ключ восстановления на USB-диске
2. Сохранить ключ восстановления в файле
3. Распечатать ключ восстановления

Учтите, ваш принтер должен быть доступен до того как вы решите распечатать ключ!

После того как вы сохранили ключ, вам будет предложено два варианта восстановления (этого не было в Windows Vista/7) (рис.7).

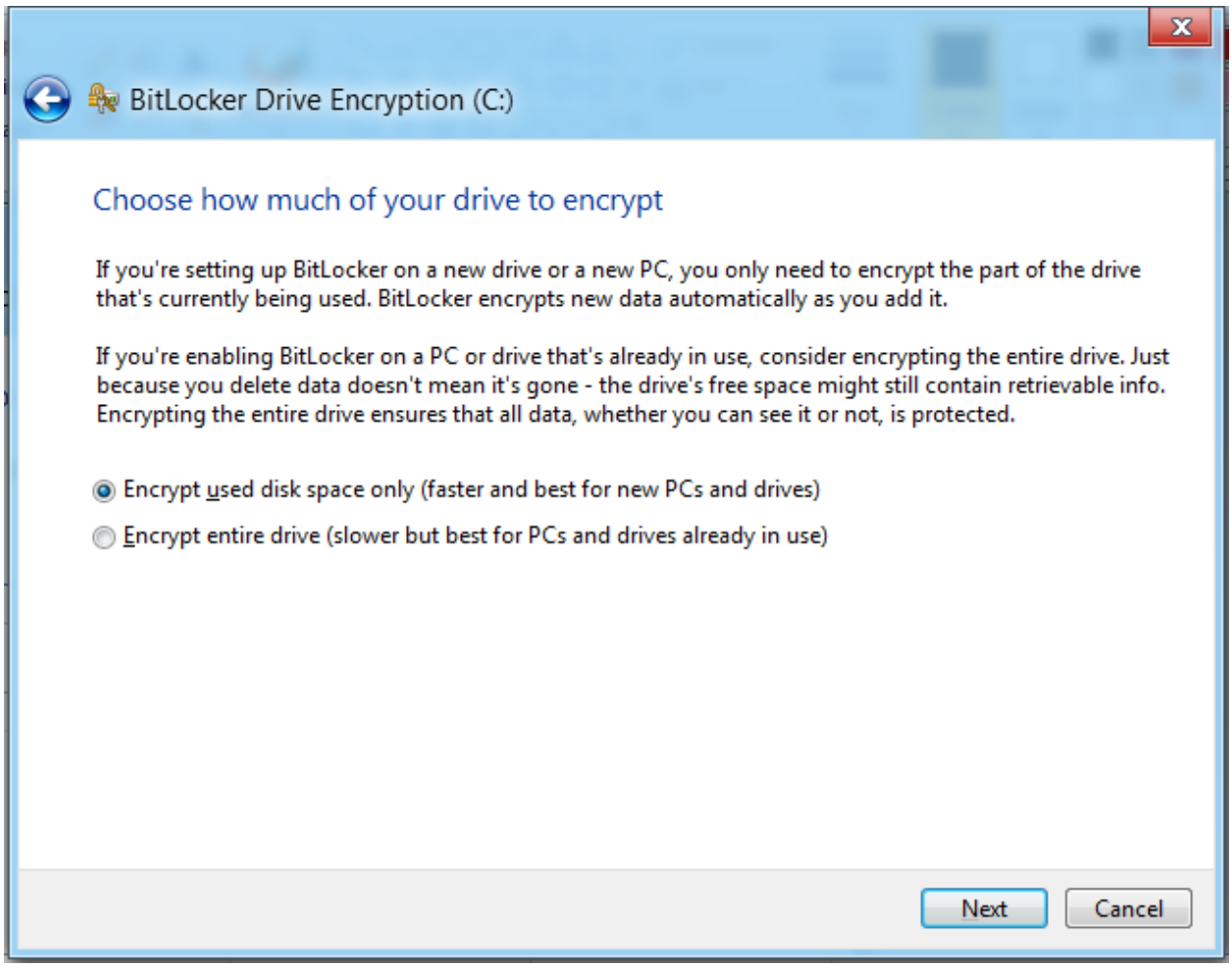

Рисунок 7 Выбор вариантов шифрования

Вам будет предложено 2 варианта шифрования:

1. Шифровать только занятое пространство (быстрее, рекомендуется для новых ПК и дисков)
2. Шифровать весь диск (медленнее, рекомендуется для ПК и дисков, которые использовались до шифрования)

Следует учесть, что способ 1 значительно быстрее, однако позволяет оценить злоумышленнику, насколько много информации на вашем жестком диске. Вместе с тем необходимо помнить, что если вы выбрали первый вариант, то при копировании (создании) новых файлов на диск, они будут шифроваться автоматически.

После этого ваш ПК будет перезагружен и автоматически начнется шифрование системного раздела.

Шифрование раздела данных

В случае шифрования раздела данных все намного проще. Единственное что хотелось бы рекомендовать – если уж решили шифровать раздел данных – шифруйте вначале системный раздел, а потом диск данных!

Единственное отличие состоит в том, что вы можете указать – автоматически открывать диск данных на этом ПК (рис.8).

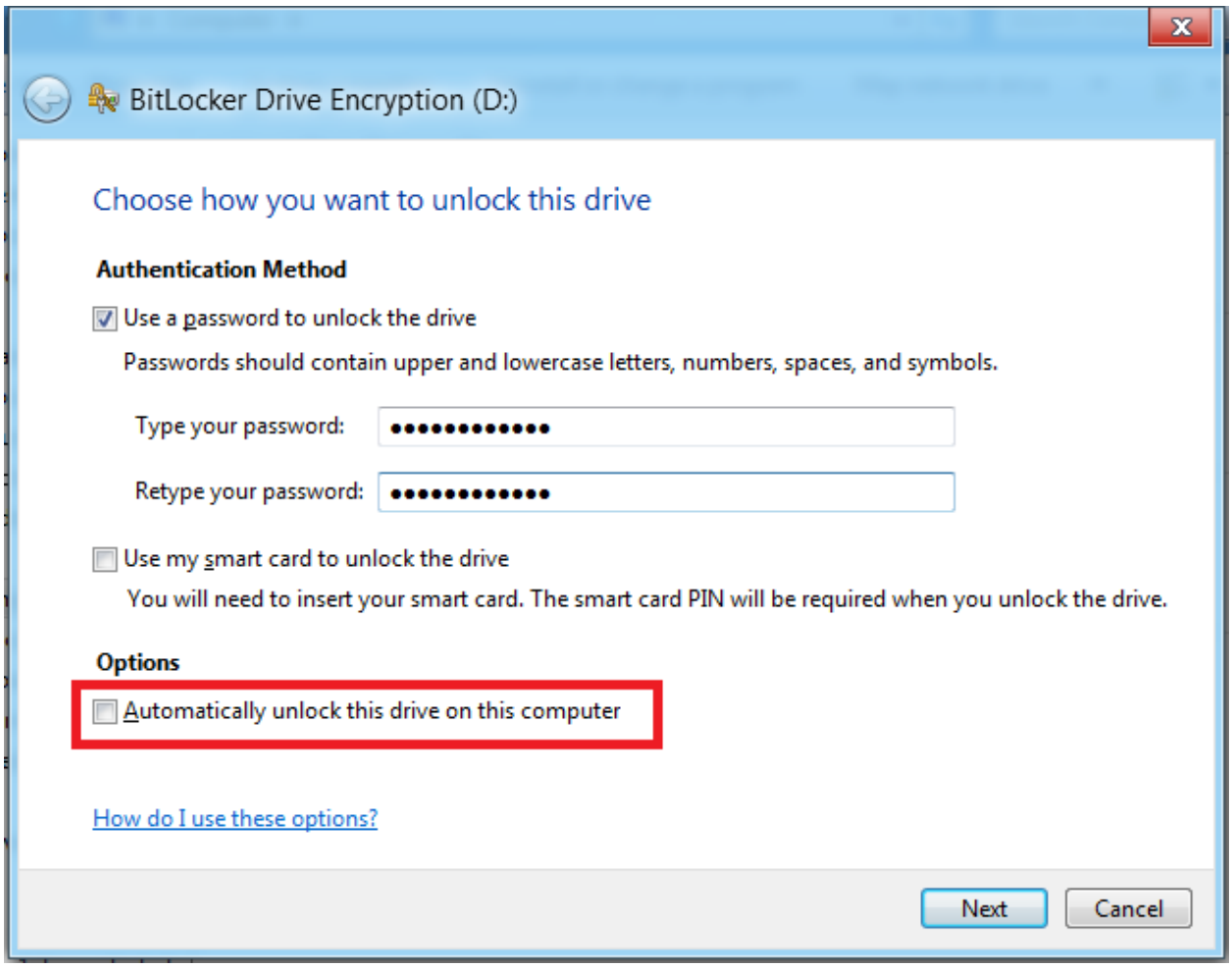

Рисунок 8 Выбор способа доступа к данному диску

Естественно, данную опцию вы можете выбрать только в том случае, если системный раздел предварительно зашифрован.

Давайте рассмотрим подробнее параметры групповой политики, относящиеся к шифрованию BitLocker.

Параметры локальной групповой политики, относящиеся к шифрованию BitLocker