Шифрование BitLocker в Windows 8 Developer Preview

Владимир Безмалый

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

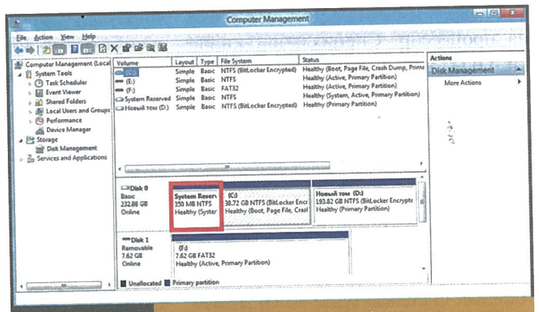
В Торонто было потеряно 3 незашифрованных компакт-диска с персональными данными клиентов банка Scotiabank. Инцидент, как сообщило руководство, произошел по недосмотру курьерской службы. «Пакет с тремя компакт-дисками пропал при внутренней курьерской пересылке из одного отдела в другой», — сообщил в своем письме 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 тысячи с лишним 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.

Подобные истории приключаются регулярно. Типичнейшая картина: украден или потерян ноутбук или флэш-накопитель с конфиденциальной информацией, которая не должна была покидать информационную систему предприятия.

Обширная статистика утечек учит нас, что никого она не учит. Все равно сотрудники беззаботно копируют служебные документы на мобильные носители, рассчитывая, что «со мной-то такого не случится». Увы, случается, и руководству предприятий следует подумать не только о наказании провинившегося. Лучше внедрить принудительное шифрование всех носителей, которыми пользуются сотрудники.

Данная статья посвящена обзору шифрования BitLocker в демонстрационной версии операционной системы Windows 8 Developer Preview. Хотелось бы подчеркнуть, что все сказанное здесь относится ТОЛЬКО к данному выпуску. Ведь вполне возможно, что в официальном релизе некоторые описанные параметры групповой политики будут изменены, а то и удалены, а вместо них могут появиться новые.



Экран 1 Диспетчер дисков (красным цветом выделен служебный раздел)

Установка BitLocker

Одним из первых очевидных отличий при установке Windows 8 Developer Preview оказывается то, что служебный раздел для работы операционной системы занимает 350 Мбайт (см. экран 1). Кроме того, еще на этапе установки BitLocker становится ясно, что в данной операционной системе, как и в предыдущей, специалисты Microsoft исходят из того, что на вашем компьютере уже по умолчанию установлен модуль доверия 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

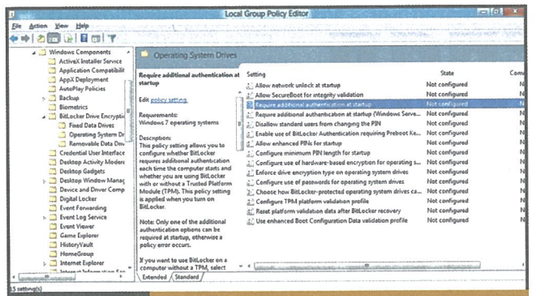
Для изменения параметров групповой политики необходимо, нажав комбинацию клавиш Win+R, вызвать окно Run и набрать команду cmd. В появившемся окне командной строки набрать gpedit.msc. Появится окно Local Group Policy Editor, показанное на экране 2.

В появившемся окне следует раскрыть контейнеры Local Computer Police — Administrative Templates — Windows Components — BitLocker Drive Encryption — Operation System Drive — Require additional authentication at startup. Данный параметр политики позволяет указывать, необходима ли дополнительная аутентификация при запуске (перезагрузке) компьютера, а также будете ли вы использовать BitLocker с TPM или без него. При запуске требуется указать только один из возможных вариантов.

В случае если вы собираетесь использовать BitLocker на компьютере без установленного модуля TPM, необходимо установить флаг Allow BitLocker without a compatible TPM. В данном режиме для запуска вам потребуется задействовать 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 компьютера. Если USB-ключ (флэшка) будет утерян, потребуется восстановить доступ к диску, используя один из вариантов восстановления.

В случае если ваш компьютер оборудован совместимым модулем TPM, вы можете использовать четыре метода аутентификации:

- только TPM;



Экран 2 Local Group Policy Editor

- TPM+USB-накопитель, содержащий ключ;
- TPM+PIN (содержит от 4 до 20 цифр);
- TPM+USB-ключ+PIN.

Если вы хотите использовать вариант PIN +USB-накопитель, необходимо выполнить настройки BitLocker, используя режим командной строки вместо мастера BitLocker Drive Encryption.

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

Далее можно приступить непосредственно к шифрованию. Для этого нужно открыть окно «Мой компьютер», выбрать диск, содержащий операционную систему (я рекомендую шифровать его первым) и, нажав правую клавишу, из контекстного меню выбрать Enable BitLocker (экран 3).

После этого вам будет предложен выбор:

- использовать USB-накопитель для хранения ключа шифрования;
- применять пароль для регистрации в системе.

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

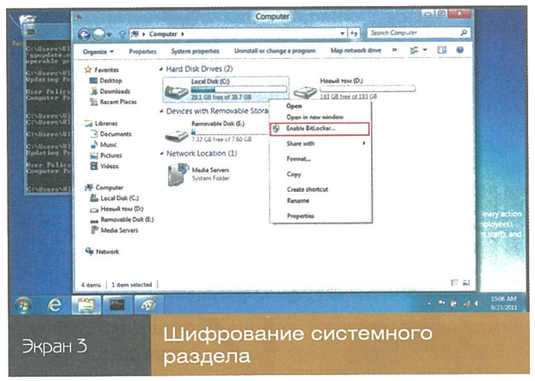
Естественно, после создания пароля необходимо подготовить USB-диск для возможного восстановления системы. Для восстановления вам будет предложено три возможных сценария.

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

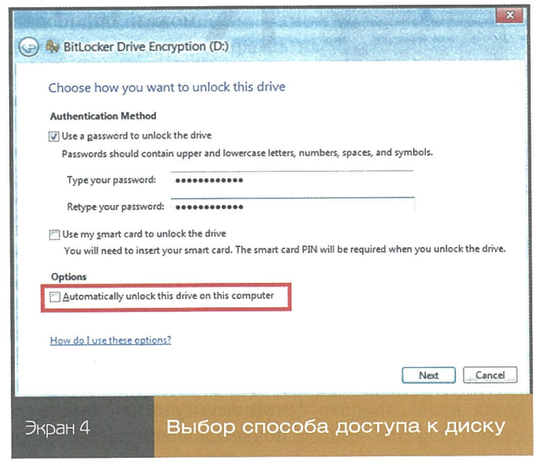
Учтите, что ваш принтер должен быть доступен до того, как вы решите распечатать ключ! После того как вы сохранили ключ, вам будет предложено два варианта шифрования (этого не было в Windows Vista/7):

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

Следует учесть, что первый способ значительно быстрее, однако позволяет злоумышленнику оценить, как много информации на вашем жестком диске. Вместе с тем необходимо помнить, что если вы выбрали первый вариант, то при копировании файлов на диск (создании новых файлов) они будут шифроваться автоматически. После этого ваш компьютер будет перезагружен и автоматически начнется шифрование системного раздела.



Экран 3 Шифрование системного раздела



Экран 4 Выбор способа доступа к диску

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 задать автоматическое открытие диска данных на этом компьютере (экран 4).

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

Итак, как видите, процесс шифрования в готовящейся операционной системе предельно прост и понятен. Естественно, не забудьте позаботиться о хранении копии ключей для расшифровки, чтобы не пожалеть о решении шифровать.

Владимир Безмалый (vladb@windowslive.com) — специалист по обеспечению безопасности, имеет звания MVP Consumer Security, Microsoft Security Trusted Advisor