# Безопасность Windows 7. BitLocker

> Тарас Злонов, CIO-World, 04 марта 2009 года

Основное предназначение технологии BitLocker заключается в предотвращении случайной утечки или преднамеренной кражи информации, хранящейся на жёстких дисках и внешних подключаемых устройствах. По мере роста числа мобильных сотрудников, проблема защиты конфиденциальных данных на используемых ими устройствах становится всё более актуальной. Воровство и потери ноутбуков, а тем более флэш-носителей сегодня, стали повседневной реальностью. Именно поэтому такую широкую популярность получили решения по шифрованию данных. Продукты подобного класса шифруют отдельные файлы, папки, разделы или жёсткие диски целиком.

Однако до недавнего времени в отличие от операционных систем на базе linux в среде microsoft задачи по шифрованию решались только внешними средствами. Технология EFS (Encrypting File System - шифрованная файловая система) так и не получила широкого практического применения. Возможность получения доступа к данным при наличии администраторских прав, отсутствие поддержки смарт-карт для хранения закрытого ключа, используемого в EFS и банальное неудобство использования привели к тому, что многими наличие данной технологии воспринималось лишь как демонстрация того, что “в Windows тоже есть шифрование”.

Впервые представленное в Windows Vista решение BitLocker позволяет защищать важные данные от несанкционированного доступа, а новые возможности, реализованные в Windows 7, решают также проблему защиты внешних устройств и существенно упрощают использование данной технологии. Случаи утраты USB-флэш редко предаются огласке, в отличие от утраты тех же ноутбуков, хотя на практике эти устройства могут содержать ничуть не меньшие объёмы конфиденциальной информации. Вместе с тем, решения по защите данных на этом типе устройств гораздо менее распространены, чем те же решения для жёстких дисков компьютеров. Отказ от использования мобильных устройств для большинства современных компаний не приемлем: обмен информацией с партнёрами, работа дома и многое другое не позволяют полностью отказаться от такого способа переноса информации. Расширение BitLocker To Go предназначено как раз для решения данной проблемы. Данные пользователя, записываемые им на внешнее устройство, защищаются с помощью пароля, критерии сложности которого администратор может задавать в соответствии с требованиями корпоративной политики. Более того, с использованием групповых политик возможен полный запрет на использование незашифрованных мобильных дисков. Помимо парольной аутентификации предусмотрено использование смарт-карт, также возможен *прозрачный* доступ при входе пользователя в домен организации.

В ОС Windows 7 создание шифрованного раздела возможно не только во время установки, но и на работающей системе, для чего достаточно одного нажатия правой кнопки мыши на имени раздела. Именно сложность настройки послужило причиной низкой популярности данной технологии в Windows Vista - сторонние решения, в том числе с использованием открытых кодов были на порядок функциональнее и удобнее.

Для использования шифрования данных в Windows Vista необходимо было вручную изменять таблицу разделов диска, что, очевидно, является не тривиальной задачей для рядовых пользователей. Осознавая эту сложность, Microsoft даже выпустила специальную утилиту BitLocker Drive Preparation Tool, которая теперь является встроенной в Windows 7. Для использования BitLocker желательно наличие TPM (Trusted Platform Nodule - модуль доверенной загрузки), встраивание которого в компьютеры, поставляемые в Российскую Федерацию, имеет ряд ограничений. Дело в том, что данное устройство аппаратно реализует криптографические алгоритмы, а значит, для его ввоза требуются соответствующие лицензии. Сложность с получением этих лицензий таковы, что даже крупные производители деактивируют TPM на комьютерах, поставляемых в Россию, в связи с чем фактически единственным легальным способом использования BitLocker становится хранение ключей шифрования на USB-носителях. Данная опция устанавливается с помощью соответствующей групповой политики. Стоит обратить внимание, что далеко не во всех компьютерах реализована поддержка USB-устройств до старта ОС, а значит, хранение ключей шифрования системного жёсткого диска этих компьютеров на внешних устройствах не возможно.

В процессе шифрования раздела создаётся отдельная скрытая область на жёстком диске размером 200 МБ, после чего стартует шифрование самого раздела с данными. Скорость этой операции зависит от размера жёсткого диска и производительности системы, но так как данная операция выполняется однократно, затрачиваемое время вряд ли является критичным.

После завершения шифрования загрузка ОС Windows 7 будет возможна только при наличии USB-флэш (и/или TPM). При утрате USB-диска потребуется Recovery Key (ключ восстановления) или Recovery Password (пароль восстановления), каждый из которых создаётся ещё в процессе шифрования. Пароль восстановления состоит из 48 цифр, что, в принципе, для определённого круга задач можно признать достаточно безопасным, хотя использование TPM, USB-ключа или смарт-карты, конечно, гораздо надёжнее. Невозможность получения доступа к данным в случае утраченных данных для восстановления требует бережного к ним отношения.

Основное преимущество BitLocker перед конкурентами, т.е продуктам, имеющими сходный функционал, состоит в его “бесплатности”. Вполне возможно, что имея встроенное и полностью интегрированное с Active Directory решение по шифрованию данных, далеко не все пользователи Microsoft будут искать ему замену. Вместе с тем, в нашей стране, в силу рассмотренных выше ограничений на использование TPM, действительное надёжную защиту данных BitLocker обеспечить пока не в состоянии. В борьбе, основными аргументами в которой будут безопасность, стоимость и удобство управления, очевидно должны победить решения по шифрованию данных с централизованным управлением и резервным копированием ключевой информации, использующие высоко надёжные методы аутентификации с применением usb-ключей или смарт-карт, продаваемые по разумной цене. Однако пока на российском рынке подобных решений не наблюдается, что означает только одно: технология BitLocker имеет все шансы на принятие её в качестве корпоративного стандарта для зашиты данных на жёстких дисках и мобильных устройствах.