Безопасность Windows 7. BitLocker To Go

> Тарас Злонов, CIO-World, 06 марта 2009 года

Рассмотренная в предыдущей статье технология BitLocker, защищающая данные на жёстких дисках компьютеров, хорошо известна ещё с предыдущей версии ОС Microsoft - Windows Vista

Определённые нововведения, появившиеся в новой операционной системе, могут повысить популярность данного решения, однако гораздо большие шансы на успех имеет решение для шифрования внешних устройств - BitLocker To Go.

Желание пользователей носить в кармане “зашифрованную флэшку”, похоже, может осуществиться на практике. Технология BitLocker To Go, доступная в Windows 7, конечно, не первая в этом классе. Многие вендоры поставляли вместе с USB-флэш собственные приложения для их криптографической защиты, а практически любое современное ПО для шифрования обязательно поддерживает работу с внешними устройствами или позволяет использовать шифрованные файл-контейнеры, которые могут на них храниться.

Доступные ранее продукты в большей массе своей требовали предварительной установки программного обеспечения на рабочую станцию, к которой подключался зашифрованный USB-диск или другое внешнее устройство хранения данных, что не всегда являлось возможным. Фактически единственным практичным сценарием была возможность работать с зашифрованной USB-флэш на конечном числе специально подготовленных рабочих мест (например, на офисном десктопе, ноутбуке и домашнем компьютере).

Важнейшее преимущество BitLocker To Go состоит в его интеграции в саму операционную систему. Теперь зашифрованное устройство можно будет просто подключать к любому компьютеру, не заботясь о предварительной установке и настройке чего-либо. Решение, давно доступное пользователям Linux, наконец-то приходит и к Windows-пользователям.

Первоначальное шифрование осуществляется достаточно просто. В контекстном меню подключенного USB-устройства достаточно выбрать нужный пункт. Для ограничения доступа к данным можно использовать пароль и/или смарт-карту. Приятно, что даже для компьютера вне домена по умолчанию заданы критерии качества вводимого пароля - желанию пользователей использовать пароль `123` не суждено сбыться.

В ходе дальнейшей настройки есть возможность сохранить в виде файла или распечатать ключ восстановления (recovery key), представляющий собой 48 цифр. Количество различных вариантов ключа восстановления (10 в степени 48) примерно соответствует 159 битам. В качестве алгоритма шифрования по умолчанию используется AES с длиной ключа 128 бит, а при необходимости можно увеличить её до 256 бит. Перед шифрованием данных BitLocker может использовать алгоритм, называемый диффузором (diffuser), основной целью применения которого является получение сильно разнящихся шифрованных данных при незначительно отличающихся исходных. Применение диффузора

существенно затрудняет взлом ключей или дешифровку. Данная опция по умолчанию включена. В целом, обеспечиваемый уровень безопасности даже без дополнительных настроек вполне достаточен не только для защиты личной переписки от любопытных знакомых, но и в корпоративной среде

Время первоначального зашифрования зависит от скорости работы устройства и его полного объёма (но не от количества записанной информации), а после его завершения в контекстном меню появляется пункт для запуска утилиты управления, которая позволяет сменить пароль, зарегистрировать или удалить смарт-карту и повторно сохранить ключ восстановления, а также включить режим кэширования - то есть возможность работы с данным устройством на конкретном компьютере без ввода пароля. Расшифрование устройства возможно только в Панели управления.

Имеющаяся в большинстве решений сторонних разработчиков поддержка файлов-контейнеров позволяет использовать USB-флэш для хранения открытых и шифрованных данных одновременно, для чего достаточно сделать размер этого файла-контейнера меньшим, чем объём памяти самого устройства. BitLocker To Go может шифровать внешние носители только целиком.

Полноценная работа с зашифрованной информацией возможна только в Windows 7, в ОС Windows XP и Vista работа осуществляется с помощью специального приложения BitLocker To Go Reaser, записываемого на USB-флэш. С его помощью, после ввода правильного пароля или предъявления смарт-карты, можно выбрать файл для копирования с зашифрованной области. Интеграция с Windows Explore и прозрачные чтение/запись возможны только после установки соответствующей утилиты. Фактически, зашифрованный внешний USB-диск представляет собой большое количество служебных файлов, большая часть из которых являются скрытыми, а также уже упомянутое приложение, позволяющее считывать данные, но не имеющего функционала записи новых файлов на диск..

Несмотря на некоторые неудобства, присущие, быть может, только текущей версии, BitLocker To Go может найти своё применение в корпоративной среде. Крайне немногие решения по шифрованию данных имеют централизованное управление, а по глубине интеграции вряд ли хоть одно из них может сравниться с решением от Microsoft. Как и остальные компоненты Windows, BitLocker To Go может управляться с помощью групповых политик.

Важнейшая задача централизованного управления при внедрении средств шифрования, а именно - архивирование ключей восстановления, на случай утраты пользователем данных для доступа к зашифрованной информации, успешно решена в Windows 7: эта информация хранится в Active Directory.

Из других интересных возможностей стоит отметить возможность запрета работы с незашифрованными USB-устройствами. При этом пользователю после подключения любого нового устройства будет предлагаться либо зашифровать его, либо работать только в режиме чтения. Записать что-либо на незащищённый внешний носитель будет нельзя.

Возможность использования смарт-карт для аутентификации пользователя при доступе к зашифрованной информации является не только существенным плюсом в плане обеспечиваемого уровня безопасности, но и потенциально способна повысить удобство использования этого решения на практике. Многие производители электронных USB-ключей уже предлагают интегрированные модели,

оснащённые не только специализированным чипом с функционалом смарт-карты, но и дополнительной флэш-памятью. Такие гибридные устройства с использованием технологии BitLocker To Go позволят сочетать высокий уровень безопасности, мобильность и простоту использования.

Подводя итоги, можно порекомендовать использование BitLocker To Go прежде всего в крупных организациях, стандартом ОС на рабочих местах в которых будет Windows 7. Ограниченная поддержка Windows Vista и Windows XP вряд ли будет серьёзной помехой для домашних пользователей Windows 7: принципиальная, пусть и не совсем удобная, возможность работы с зашифрованными данными на любой современной ОС Windows без дополнительных настроек является важным конкурентным преимуществом.

В заключение напомним, что BitLocker планируется сделать доступным только в топовых версиях Windows 7 - Ultimate и Enterprise.

Архивная копия