Сценарий 1. Включение шифрования диска BitLocker на диске операционной системы (Windows 7)

Обновлено: Август 2010 г.

Назначение: Windows 7

В этом разделе приведены указания по включению защиты шифрования диска BitLocker на диске операционной системы компьютера с доверенным платформенным модулем TPM. После шифрования диска пользователи могут входить на компьютер как обычно.

Действия перед началом работы

Необходимые условия для выполнения указаний этого руководства:

- Необходимо наличие учетных данных администратора.
- Для печати ключа восстановления необходимо настроить принтер.
- Компьютер должен соответствовать требованиям BitLocker. Дополнительные сведения см. в разделе "Требования для шифрования диска BitLocker" в пошаговом руководстве Шифрование диска с помощью BitLocker в Windows 7: пошаговое руководство.

Включение шифрования диска BitLocker на диске операционной системы

1. Нажмите кнопку **Пуск**, последовательно выберите пункты **Панель управления** и **Система и безопасность**, а затем щелкните элемент **Шифрование диска BitLocker**.
2. Щелкните элемент **Включить BitLocker** для диска операционной системы. BitLocker проверит компьютер на соответствие системным требованиям. Если компьютер соответствует требованиям, то BitLocker выведет сведения о дальнейших действиях, необходимых для включения BitLocker (подготовка диска, включение модуля TPM и шифрование диска).

   Если диск операционной системы имеет один раздел, то BitLocker подготовит диск путем его сжатия и создания нового раздела операционной системы, используемого для системных файлов, которые необходимы для запуска или восстановления операционной системы и не подлежат шифрованию. Этот диск не будет иметь буквы, чтобы предотвратить случайное сохранение файлов на нем. После подготовки диска необходимо перезапустить компьютер.

   Если модуль TPM не инициализирован, то мастер настройки BitLocker выведет запрос на отключение всех CD-, DVD- и USB-дисков от компьютера и его перезапуск для начала включения модуля TPM. Запрос на включение модуля TPM будет выведен перед загрузкой системы, но в некоторых случаях потребуется перейти в параметры BIOS и включить модуль TPM вручную. Это зависит от модуля компьютера BIOS. После подтверждения необходимости включения модуля TPM запустится операционная система и отобразится индикатор **Инициализация оборудования безопасности для доверенного платформенного модуля**.

   Если компьютер не оборудован модулем TPM, BitLocker может использоваться, но при этом будет использоваться метод проверки подлинности **Только ключ запуска**. Все необходимые сведения о ключе шифрования хранятся на USB-устройстве флэш-памяти, которое должно быть подключено к компьютеру пользователем в процессе загрузки системы. Ключ, хранящийся на USB-устройстве флэш-памяти, используется для разблокировки компьютера. Использование модуля TPM настоятельно рекомендуется, поскольку этот модуль позволяет защититься от атак на критически важный процесс загрузки компьютера. При использовании метода **Только ключ запуска** обеспечивается только шифрование диска; при этом не обеспечивается проверка компонентов ранней загрузки или защита от подмены оборудования. Для использования данного метода компьютер должен поддерживать чтение USB-устройств до загрузки операционной системы, также необходимо включить этот метод проверки подлинности, установив флажок политики **Разрешить использование BitLocker без совместимого TPM** в параметре групповой политики **Обязательная дополнительная проверка подлинности при запуске**, расположенном в следующей области редактора локальных групповых политик: **Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Защита диска BitLocker\Диски операционной системы**.

Примечание
Если параметры групповой политики организации указывают на необходимость резервного копирования сведений о восстановлении BitLocker и модуля TPM в доменные службы Active Directory® (AD DS), то для выполнения этого действия компьютер должен подключиться к домену.

3. После инициализации модуля TPM мастер настройки BitLocker выведет запрос на выбор метода хранения ключа восстановления. Возможны следующие варианты:
   - **Сохранить ключ восстановления на флэш-накопителе USB**. Сохраняет ключ восстановления на флэш-накопителе USB.
   - **Сохранить ключ восстановления в файле**. Сохраняет ключ восстановления на сетевом диске или в другом расположении.
   - **Напечатать ключ восстановления**. Печатает ключ восстановления.

   Используйте один или несколько вариантов сохранения ключа восстановления. Для каждого пункта необходимо выполнить действия мастера по указанию расположения для сохранения или печати ключа восстановления. Когда ключ восстановления будет сохранен, нажмите кнопку **Далее**.

Важно
Ключ восстановления необходим при перемещении зашифрованного диска на другой компьютер или при внесении изменений в сведения по загрузке системы. Ключ восстановления является очень важным компонентом, поэтому рекомендуется сделать его дополнительные копии и хранить их в надежном месте, чтобы иметь возможность обратиться к ним при необходимости восстановления доступа к диску. Ключ

восстановления необходим для разблокировки зашифрованных данных при переходе BitLocker в заблокированное состояние. Ключ восстановления уникален для каждого диска. Ключ не подходит для восстановления зашифрованных данных с другого диска с защитой BitLocker.

Для дополнительной безопасности необходимо хранить ключи восстановления отдельно от компьютера.

4. Мастер настройки BitLocker выводит запрос о готовности к шифрованию диска. Убедитесь в том, что флажок **Запустить проверку системы BitLocker** установлен, а затем нажмите кнопку **Продолжить**.

5. Подтвердите перезагрузку компьютера, нажав кнопку **Перезагрузить сейчас**. После этого компьютер перезагрузится, а BitLocker проверит его совместимость с BitLocker и готовность к шифрованию. Если компьютер не готов, то после входа в систему отобразится сообщение об ошибке.

6. Если компьютер готов к шифрованию, то отображается строка состояния **Шифрование** с ходом выполнения шифрования. Чтобы проверить состояние шифрования диска, наведите указатель мыши на значок **Шифрование диска BitLocker** в области уведомлений у правого края панели задач. Шифрование диска займет некоторое время. Работа на компьютере во время шифрования возможна, но производительность будет ниже, чем обычно. После завершения шифрования отобразится сообщение об успешном выполнении операции.

После выполнения действий этого раздела будет выполнено шифрование диска операционной системы и создан уникальный ключ восстановления диска. При следующем входе в систему изменения не будут заметны. При изменении доверенного платформенного модуля или его недоступности, при изменении в ключевых файлах системы или при попытке загрузить компьютер с диска для обхода загрузки операционной системы компьютер перейдет в режим восстановления, а запуск Windows будет невозможен.

Добавления сообщества

© 2016 Microsoft