

Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное  
учреждение высшего профессионального образования  
**«Томский государственный университет систем управления и  
радиоэлектроники»**

Кафедра комплексной информационной безопасности  
электронно-вычислительных систем (КИБЭВС)

Лабораторная работа № 2  
по дисциплине  
**«Криптографические методы и средства защиты информации»**

Разработчик:  
Доцент каф. КИБЭВС  
канд. техн. наук  
\_\_\_\_\_ О. О. Евсютин  
«\_\_» \_\_\_\_\_ 2014 г.

Томск 2014

## Работа № 2.

### Шифрование диска BitLocker.

#### Цель работы

Целью данной работы является изучение штатного средства шифрования информации в операционных системах Microsoft Windows — технологии шифрования диска BitLocker.

#### Краткие теоретические сведения

Обеспечение конфиденциальности данных, хранимых на носителях информации, посредством организации аутентифицированного доступа к ним является действенным до тех пор, пока носитель информации не попадет в руки злоумышленника, который в этом случае сможет работать с ним напрямую в обход всех механизмов разграничения прав доступа. В такой ситуации обеспечить конфиденциальность можно лишь с помощью шифрования содержимого носителя информации.

В операционных системах Microsoft Windows, начиная с Windows Vista (только в выпусках Enterprise, Ultimate), для этой цели служит технология шифрования диска BitLocker (BitLocker Drive Encryption), позволяющая шифровать информацию как на стационарных, так и на съемных носителях. Для шифрования используется алгоритм AES со 128-битовым ключом.

В отличие от шифрованной файловой системы (Encrypting File System – EFS), позволяющей шифровать отдельные файлы и каталоги, BitLocker шифрует носитель информации полностью. Такое шифрование является прозрачным для пользователей, которые после входа в систему могут работать с файлами как обычно, не испытывая затруднений от наличия данного защитного механизма. Однако злоумышленник, получивший физический доступ к диску, не сможет считать его содержимое.

BitLocker автоматически шифрует все файлы, добавляемые на зашифрованный диск. Если к файлам на зашифрованном диске предоставляется общий доступ, то храниться они будут в зашифрованном виде, но авторизованные пользователи смогут получать к ним доступ обычным образом.

Технология BitLocker предназначена для работы с носителями информации, на которых используются файловые системы exFAT, FAT16, FAT32 или NTFS. Для шифрования диска с операционной системой на нем должна использоваться файловая система NTFS.

Существуют некоторые различия между реализациями технологии BitLocker в операционных системах Windows Vista и Windows 7. Основное различие заключается в том, что в Windows 7 не нужно выполнять специальную разметку дисков. Ранее пользователь должен был для этого использовать утилиту Microsoft BitLocker Disk Preparation Tool, сейчас же достаточно просто указать, какой именно диск должен быть защищен, и система автоматически создаст на диске скрытый загрузочный раздел, используемый BitLocker. Этот загрузочный раздел будет использоваться для запуска компьютера, он хранится в незашифрованном виде (в противном случае загрузка была бы невозможна), раздел же с операционной системой будет зашифрован. По сравнению с Windows Vista, размер загрузочного раздела занимает примерно в десять раз меньше дискового пространства. Дополнительному разделу не присваивается отдельная буква, и он не отображается в списке разделов файлового менеджера.

BitLocker может работать в различных режимах, каждый из которых имеет свои особенности, а также обеспечивает свой уровень безопасности:

- режим с использованием доверенного платформенного модуля;
- режим с использованием доверенного платформенного модуля и USB-устройства;

- режим с использованием доверенного платформенного модуля и персонального идентификационного номера (ПИН-кода);
- режим с использованием USB-устройства, содержащего ключ.

Доверенный платформенный модуль (Trusted Platform Module — TPM) — это специальный криптографический чип, также называемый криптопроцессором, предназначенный для хранения ключевой информации и реализации некоторых криптографических функций. Такая микросхема может быть интегрирована, например, в некоторых моделях ноутбуков, настольных ПК, различных мобильных устройствах и т. д.

Когда защита выполняется исключительно с помощью доверенного платформенного модуля, в процессе включения компьютера на аппаратном уровне происходит сбор данных, которые позволят установить подлинность аппаратного обеспечения. Данная проверка является «прозрачной» и не требует от пользователя никаких действий, в случае успешного прохождения, выполняется загрузка операционной системы в штатном режиме. При обнаружении угрозы BitLocker заблокирует диск с операционной системой. Чтобы разблокировать его, потребуется специальный ключ восстановления BitLocker, который необходимо создать при первом запуске BitLocker. В противном случае доступ к файлам может быть потерян.

### Порядок выполнения работы

Работа выполняется на виртуальной машине с установленной операционной системой Windows 7 Ultimate, для запуска которой используется программа VMware Player. Чтобы выполнить все действия, предусмотренные в данной работе, необходимо подготовить виртуальную машину не менее чем с двумя локальными дисками.

#### *BitLocker To Go*

Для шифрования локальных дисков, не являющихся системными, а также съемных дисков, предназначена функция BitLocker To Go. Чтобы воспользоваться данной функцией, необходимо открыть инструмент «Шифрование диска BitLocker» на «Панели управления» (рис. 2.1).

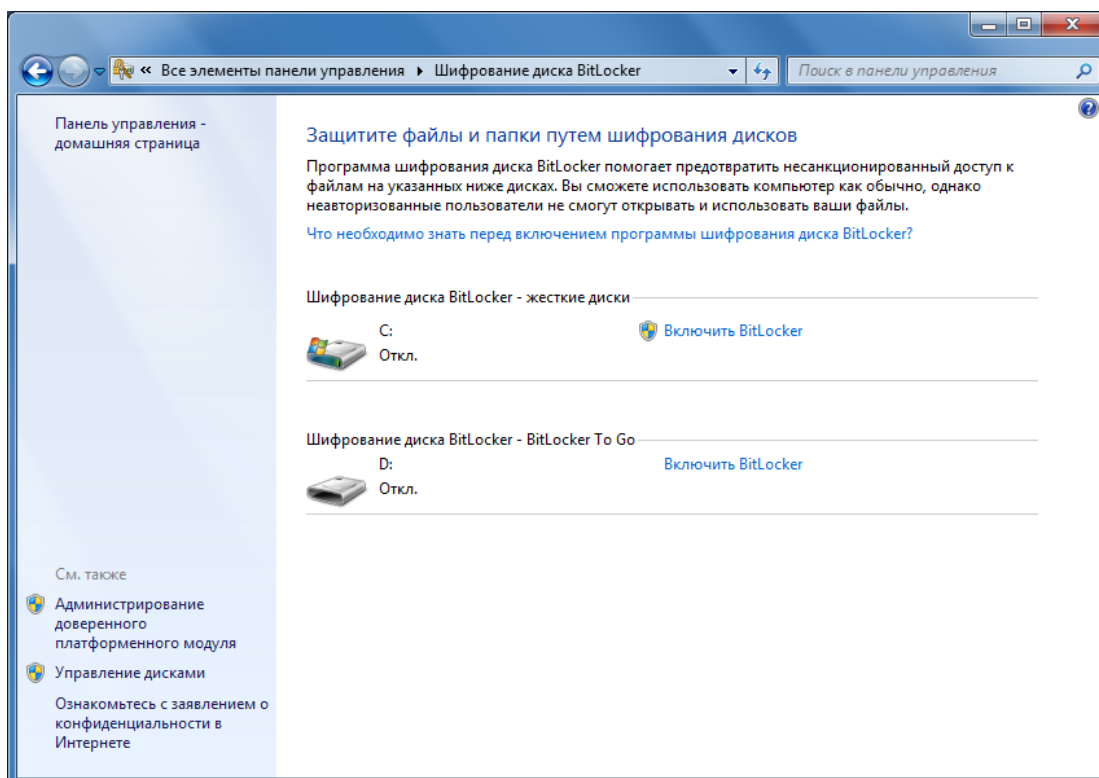
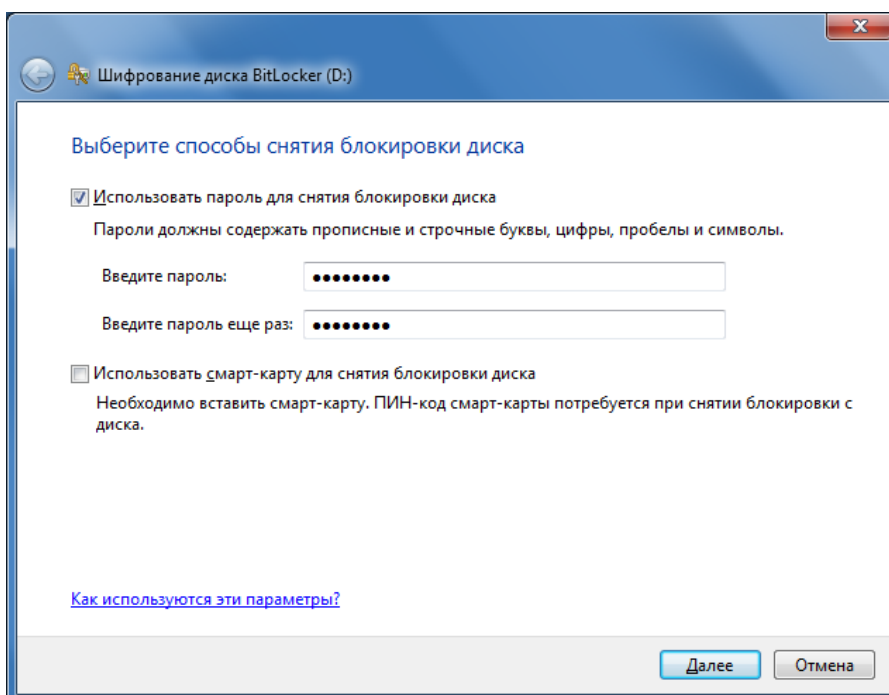


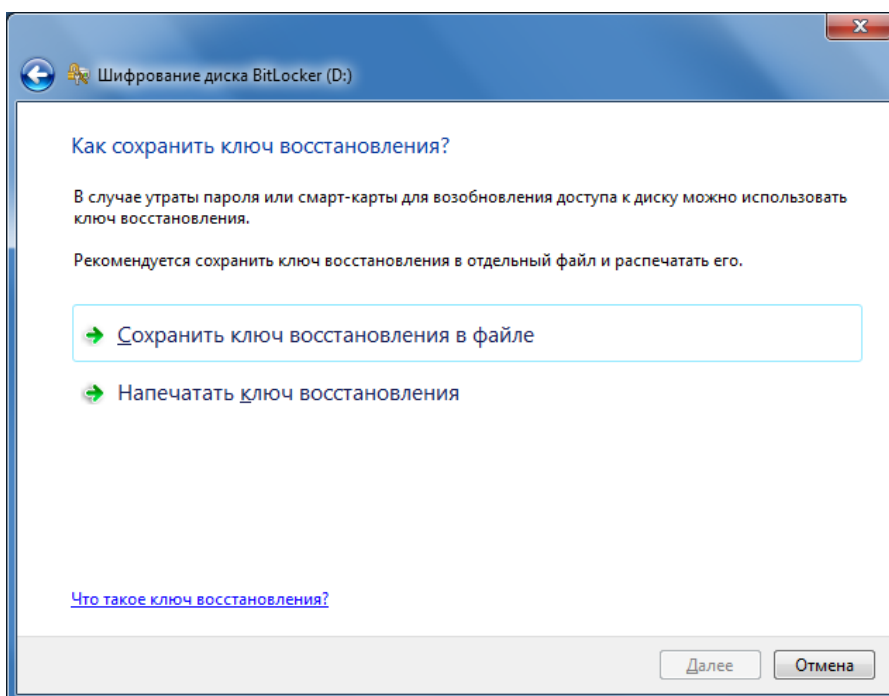
Рис. 2.1. Инструмент Windows «Шифрование диска BitLocker»

Чтобы запустить процедуру шифрования диска D (рис. 2.1), выполните команду «Включить BitLocker». Выберите способ шифрования с использованием пароля, введите произвольный пароль, содержащий не менее 8-ми символов, и нажмите «Далее» (рис. 2.2).



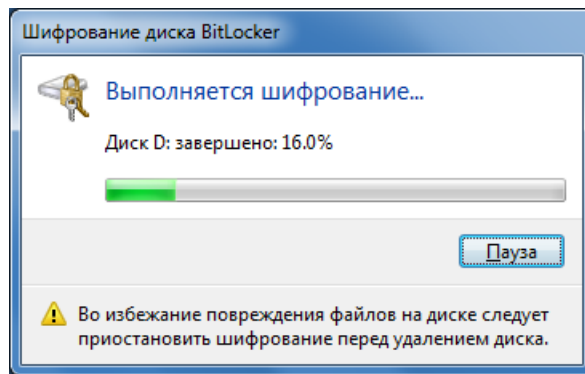
**Рис. 2.2.** Ввод пароля для блокировки диска

В следующем окне выберите пункт «Сохранить ключ восстановления в файле» (рис. 2.3) и указав место сохранения файла, нажмите «Далее».

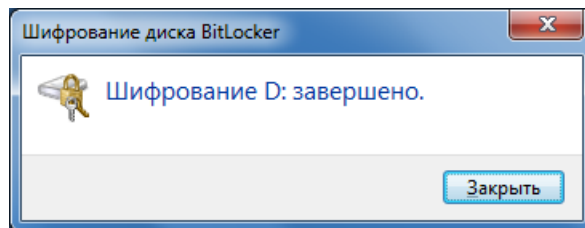


**Рис. 2.3** Сохранение ключа восстановления

Затем запустите процедуру шифрования диска нажатием кнопки «Начать шифрование» (рис. 2.4) и дождитесь, когда диск будет полностью зашифрован (рис. 2.5).

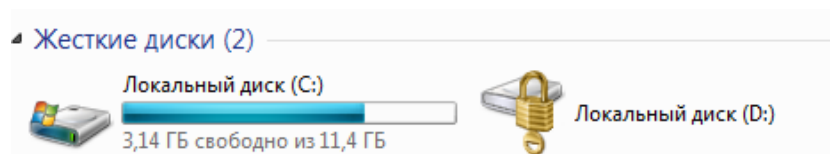


**Рис. 2.4.** Процесс шифрования диска



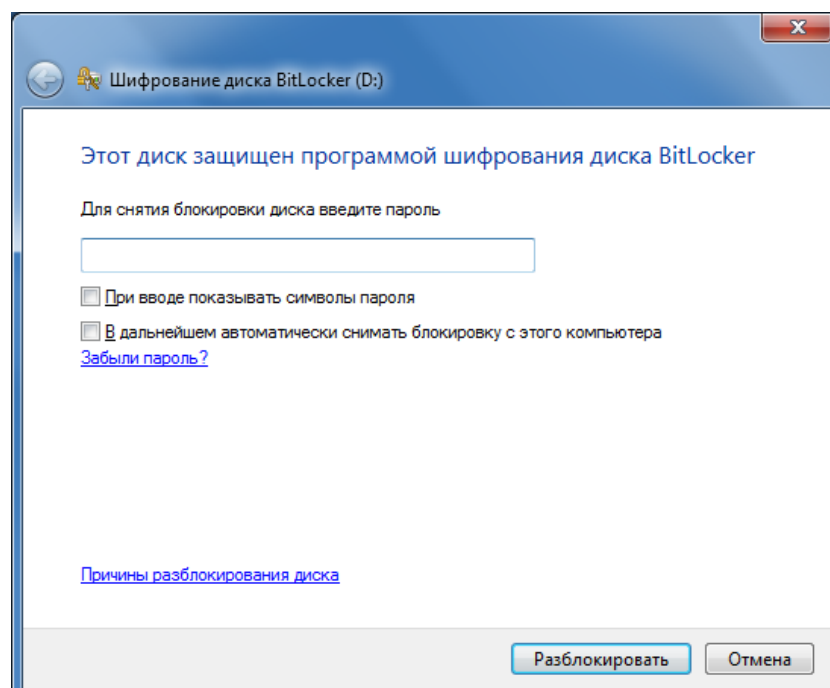
**Рис. 2.5.** Процесс шифрования завершен

Чтобы заблокировать диск, выполните перезагрузку. Теперь значок локального диска D в зашифрованном состоянии отображается с закрытым замком (рис. 2.6).



**Рис. 2.6.** Зашифрованный диск D

При попытке открыть данный диск, появится окно с запросом пароля для разблокировки диска (рис. 2.7).



**Рис. 2.7.** Запрос на ввод пароля для снятия блокировки диска

После ввода верного пароля диск становится доступным, а значок диска изменяется на открытый замок (рисунок 8).



Рисунок 8 – Разблокированный диск D

Таким же способом, применяя функцию «BitLocker To Go», можно зашифровать USB-флеш-накопитель. Прочитать информацию, хранящуюся на зашифрованном USB-флеш-накопителе, можно только при подключении к компьютеру с операционной системой не ниже Windows XP с установленным обновлением KB970401, содержащим программу «BitLocker To Go Reader». При этом отобразится запрос на ввод пароля, установленного при зашифровании, и только после ввода верного пароля информация на USB-флеш-накопителе будет расшифрована.

### *Использование BitLocker на компьютере без TPM*

Прежде чем выполнить шифрование системного диска, необходимо внести некоторые изменения в групповую политику, потому что BitLocker изначально использует систему TPM, и при его отсутствии Windows с настройками по умолчанию для системного диска не позволит включить BitLocker. Чтобы использовать BitLocker на компьютере без TPM, выполните следующие действия:

- 1) откройте меню «Пуск», введите в поле поиска «gpedit.msc» и нажмите Enter;
- 2) в появившемся окне «Редактор локальной групповой политики» зайдите в раздел «Конфигурация компьютера», затем в «Административные шаблоны» и в «Компоненты Windows» найдите «Шифрование диска BitLocker» (рис. 2.9);

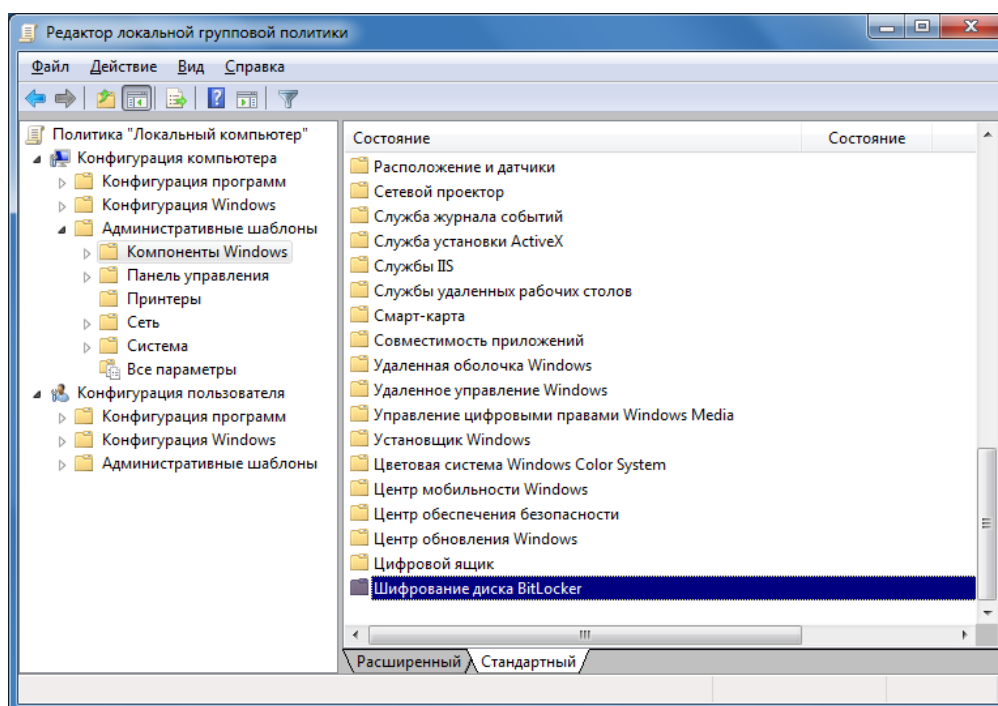
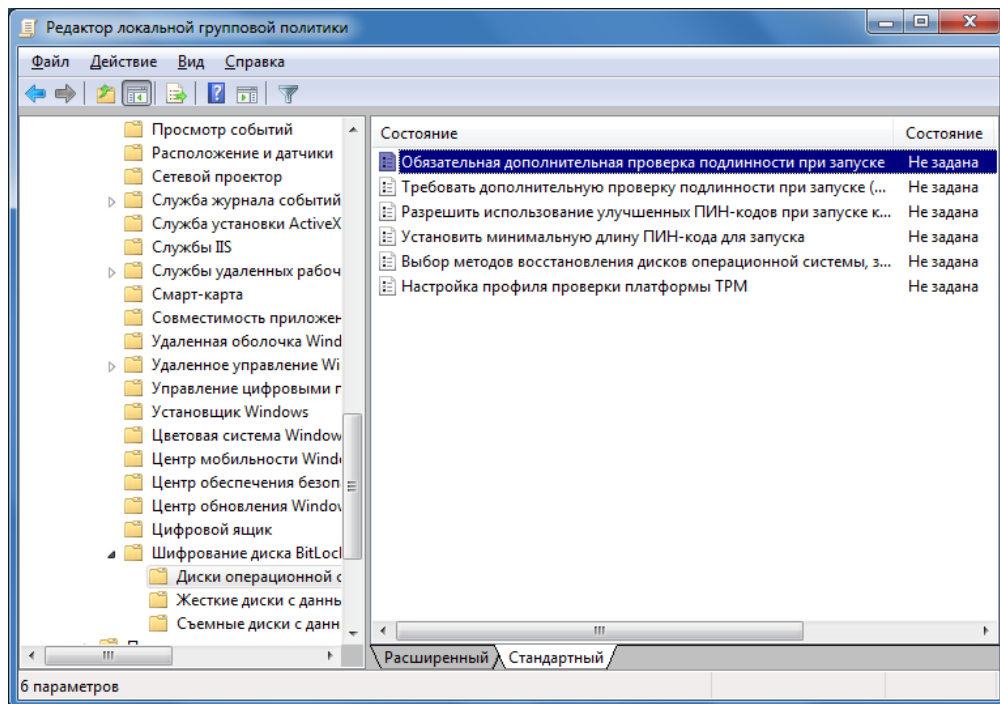


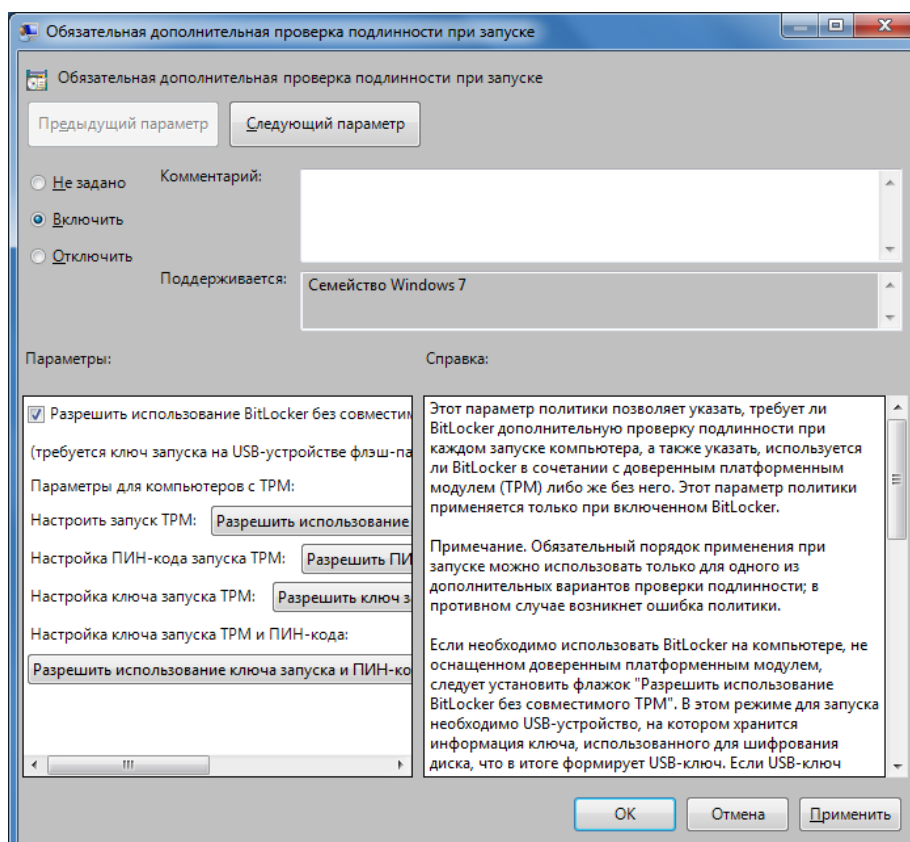
Рис. 2.9. Редактор локальной групповой политики

3) в данном компоненте зайдите в «Диски операционной системы» и откройте настройку «Обязательная дополнительная проверка подлинности при запуске» (рис. 2.10);



**Рис. 2.10.** Настройки BitLocker для системных дисков

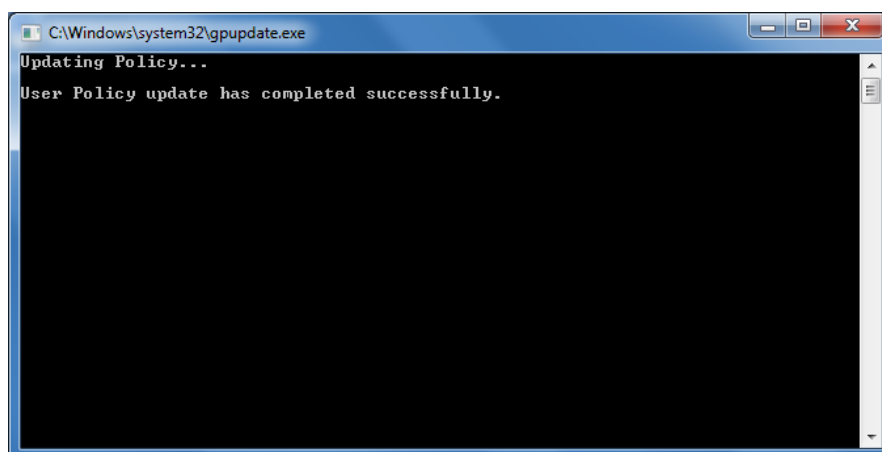
4) в появившемся окне выберите вариант «Включить», установите флажок «Разрешить использование BitLocker без совместимого TPM» и нажмите кнопку «ОК» (рис. 2.11). Теперь вместо TPM можно использовать ключ запуска;



**Рис. 2.11.** Включение использования BitLocker без совместимого TPM

5) закройте редактор локальной групповой политики;

б) чтобы новые настройки групповых политик вступили в силу немедленно, нажмите кнопку «Пуск», введите «gpupdate.exe /force» в поле поиска и нажмите Enter. Дождитесь завершения процесса (рис. 2.12).

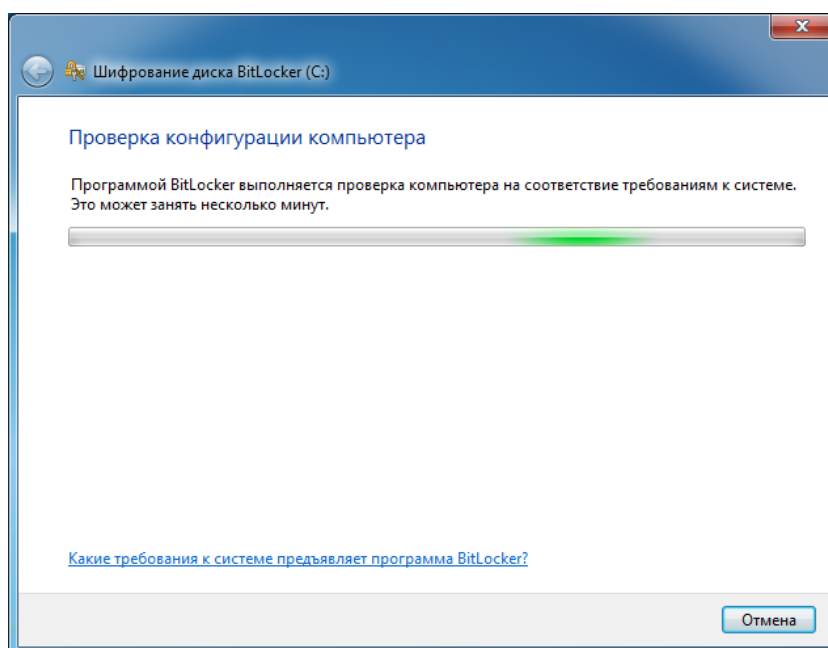


**Рис. 2.12.** Применение новых настроек групповых политик

Теперь можно приступить к шифрованию системного диска без TPM, а с использованием USB-флеш-накопителя.

#### Подготовка системного диска для BitLocker

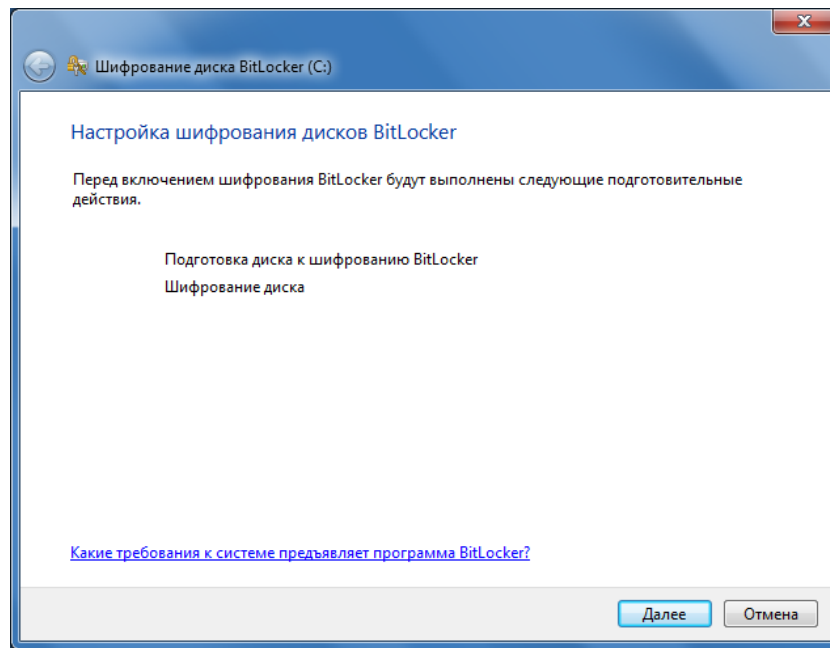
Откройте инструмент «Шифрование диска BitLocker» и выполните команду «Включить BitLocker» для системного диска C. Запустится проверка конфигурации компьютера, время выполнения которой занимает несколько минут (рис. 2.13).



**Рис. 2.13.** Проверка конфигурации компьютера

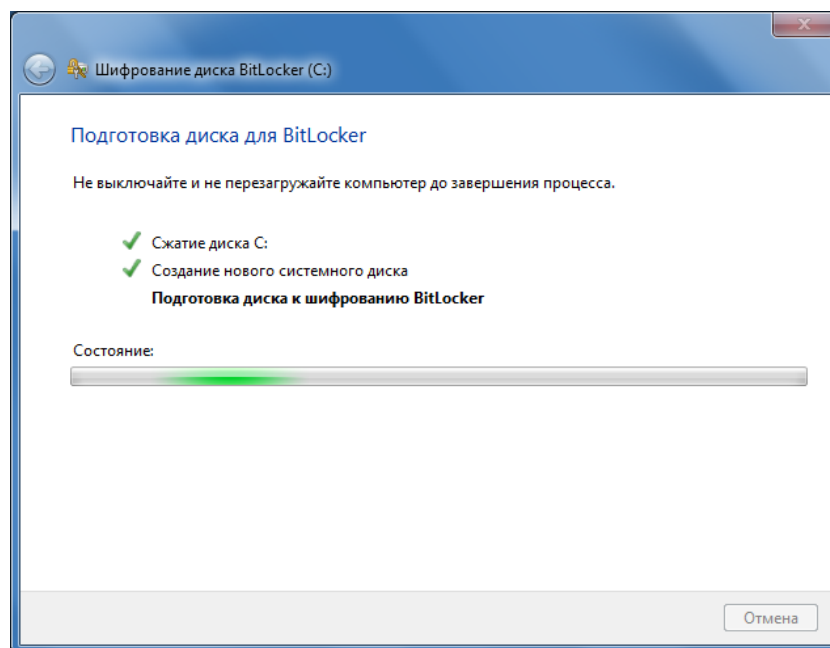
После выполненной проверки конфигурации компьютера отобразится окно с перечнем действий, которые необходимо выполнить для шифрования системного диска (рис. 2.14).





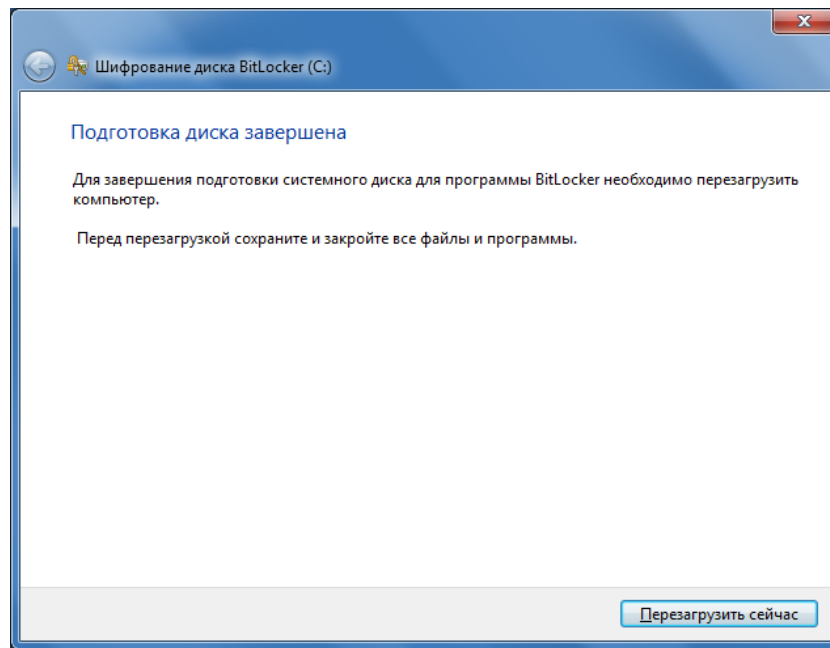
**Рис. 2.14.** Настройка шифрования дисков BitLocker

Нажмите два раза «Далее», начнется подготовка диска для BitLocker (рис. 2.15).



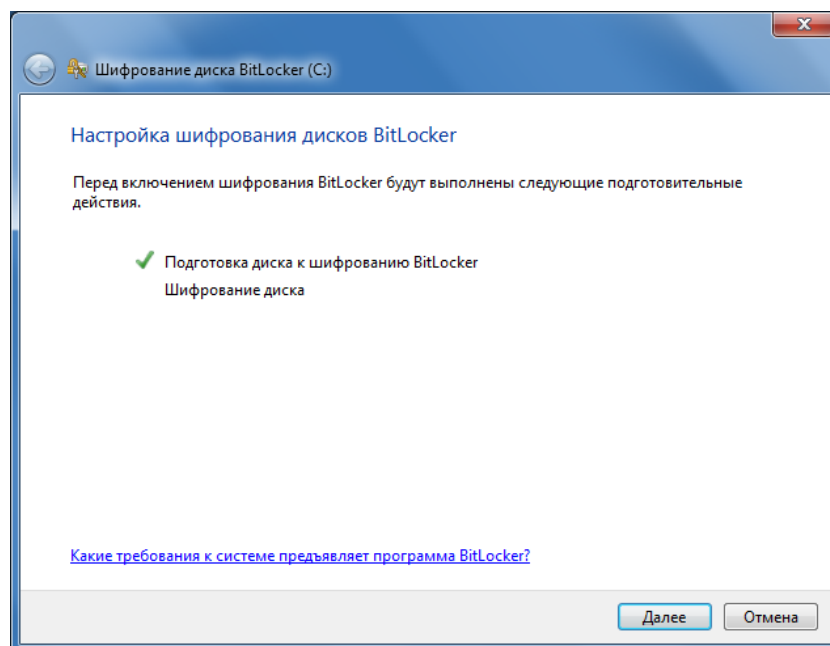
**Рис. 2.15.** Подготовка диска для BitLocker

После подготовки диска для BitLocker отобразится запрос на перезагрузку (рис. 2.16), выполните перезагрузку системы.



**Рис. 2.16.** Запрос на перезагрузку системы

После перезагрузки возобновится процедура шифрования системного диска с сообщением о том, что подготовка диска к BitLocker завершена и можно приступить к самому шифрованию (рис. 2.17).



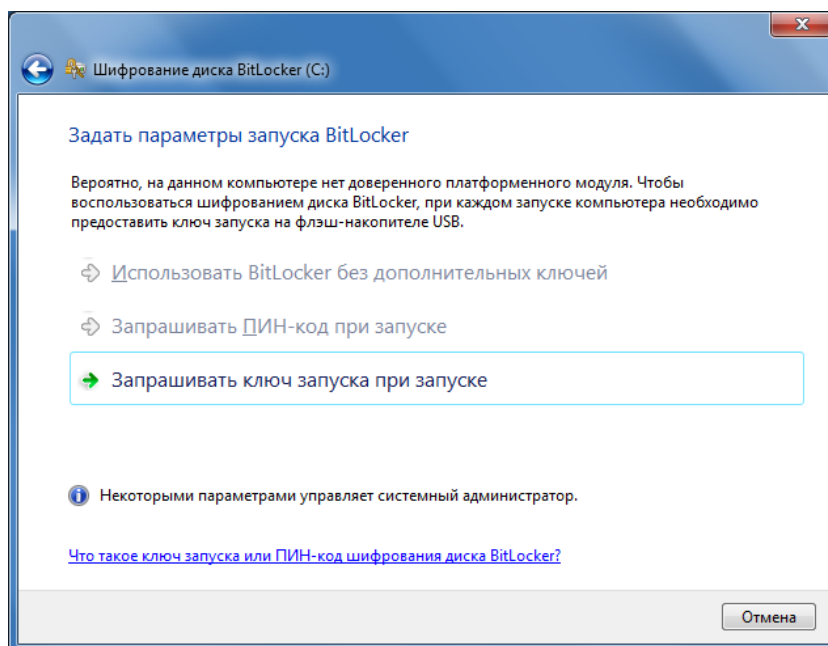
**Рис. 2.17.** Переход к шифрованию системного диска

Данный способ шифрования системного диска с использованием USB-флеш-накопителя в качестве носителя ключа запуска можно использовать только на компьютере, BIOS которого поддерживает чтение USB-устройств в загрузочной среде. Также необходимо, чтобы BIOS был настроен на загрузку сначала с жесткого диска, а затем с USB-устройства. Поэтому его применение на виртуальной машине VMWare Player невозможно (VMWare Player не поддерживает загрузку с USB-устройства). Далее представлено описание действий, выполнение которых приведет к зашифрованию системного диска на реальной системе (не на виртуальной машине).

### Шифрование системного диска на реальной системе (**ДЛЯ ОЗНАКОМЛЕНИЯ**)

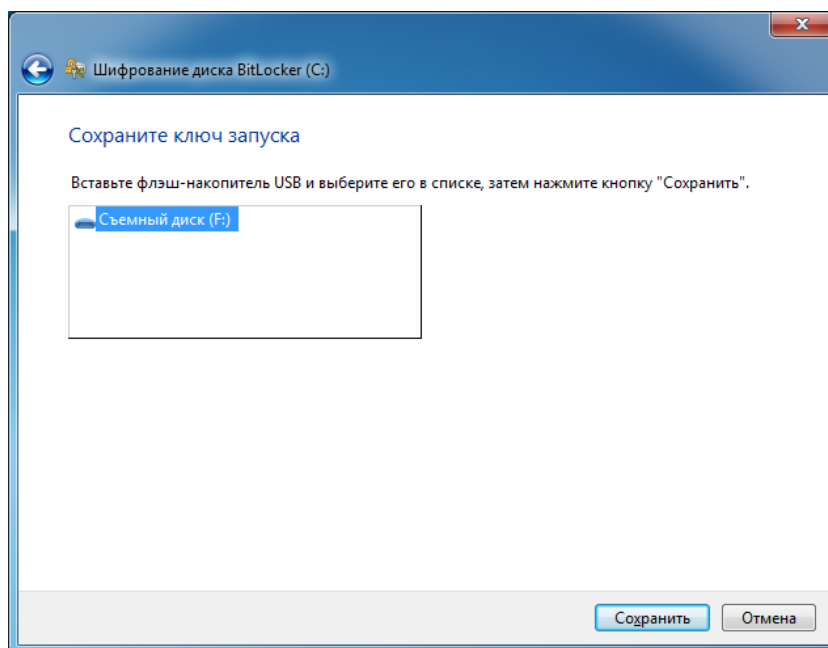
Для продолжения процедуры шифрования необходимо нажать кнопку «Далее».

Без TPM шифрование доступно только единственным способом – запрос ключа запуска при запуске системы (рисунок 18).



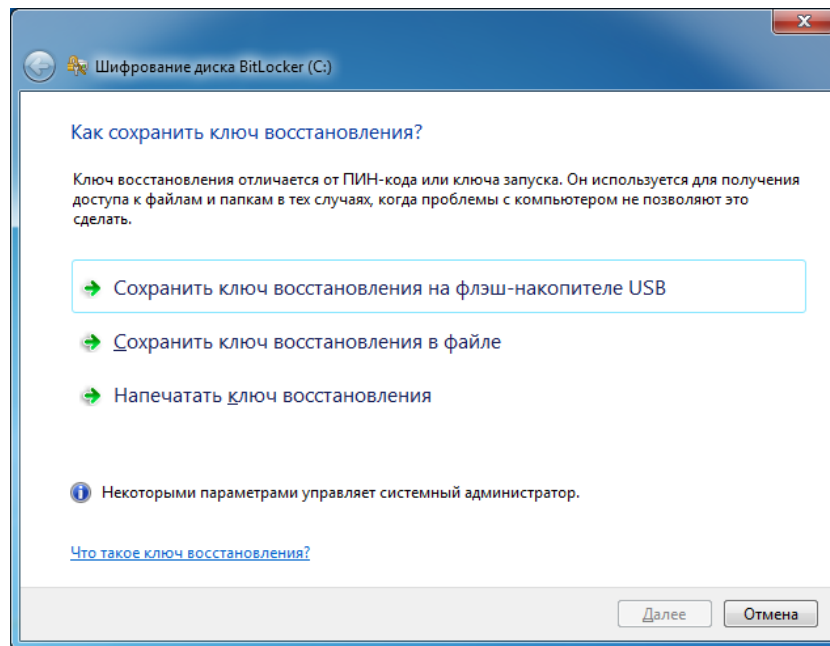
**Рис. 2.18.** Выбор параметров шифрования

Для сохранения ключа записи необходим USB-флеш-накопитель (рис. 2.19).



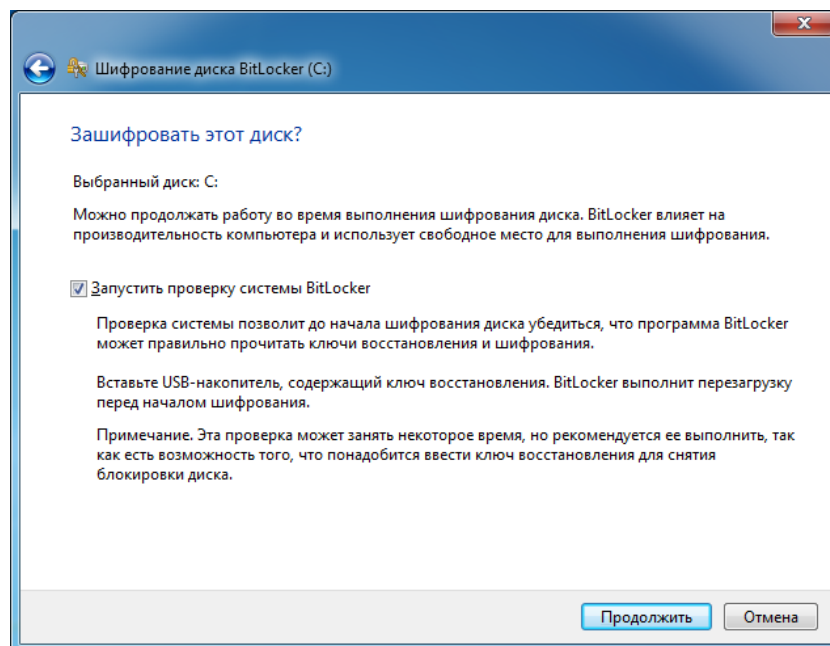
**Рис. 2.19.** Сохранение ключа на USB-флеш-накопителе

Затем будет предложен выбор способа сохранения ключа восстановления, необходимого для получения доступа к системному диску в случае утери USB-флеш-накопителя с ключом запуска (рис. 2.20).



**Рис. 2.20.** Выбор способа сохранения ключа восстановления

После сохранения ключа восстановления будет предложено запустить проверку системы BitLocker (рис. 2.21), для этого система выполнит перезагрузку. Данную проверку желательно произвести, чтобы потом не возникли ошибки после зашифрования системного диска.



**Рис. 2.21.** Запуск проверки системы BitLocker

Если BIOS компьютера поддерживает чтение USB-устройств в загрузочной среде, то запустится процедура шифрования системного диска (рис. 2.22). В противном случае (например, если выполнять данные действия на виртуальной машине) отобразится ошибка, и процедура шифрования будет отменена (рис. 2.23).

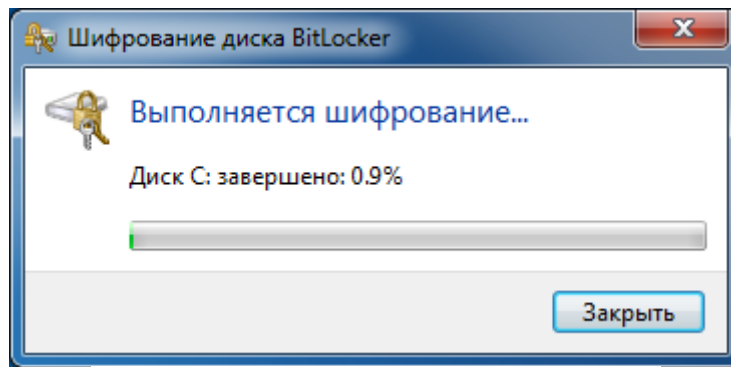


Рис. 2.22. Шифрование системного диска

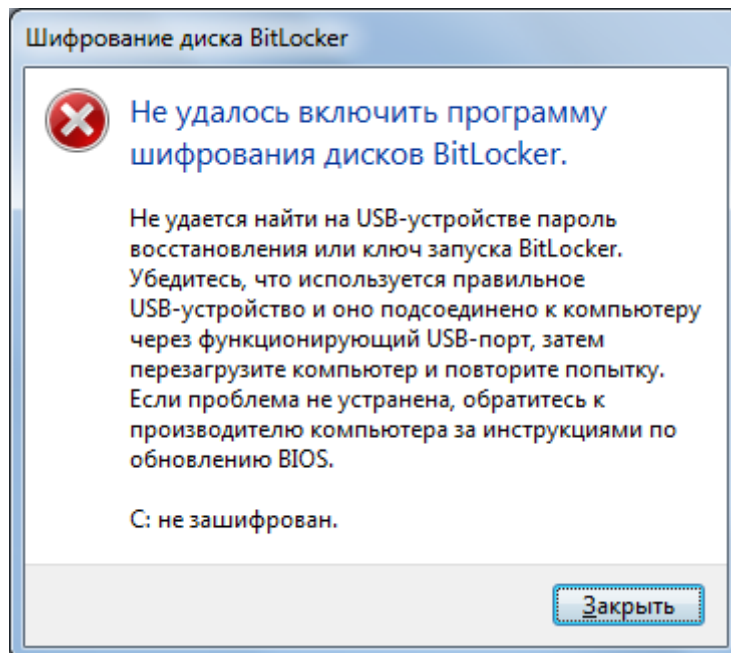


Рис. 2.23. Ошибка при выполнении проверки системы BitLocker

После зашифрования системного диска операционная система будет загружаться только при наличии вставленного USB-флеш-накопителя с ключом запуска во время загрузки системы (рис. 2.24).

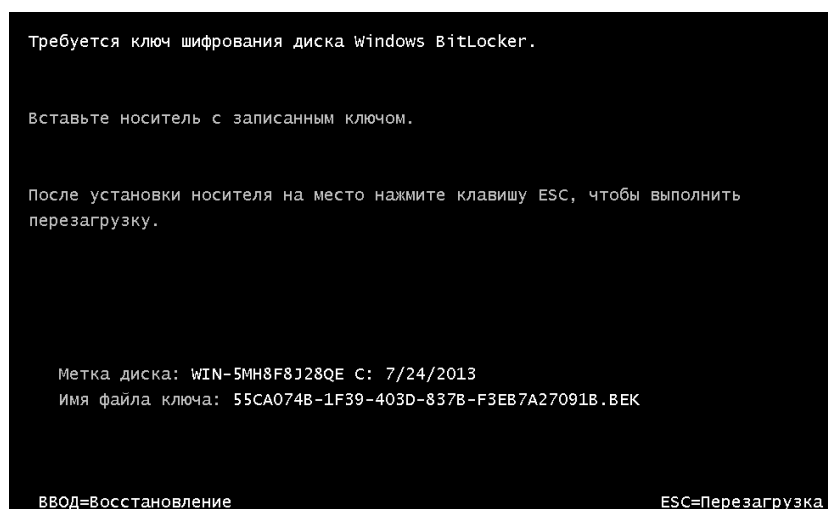
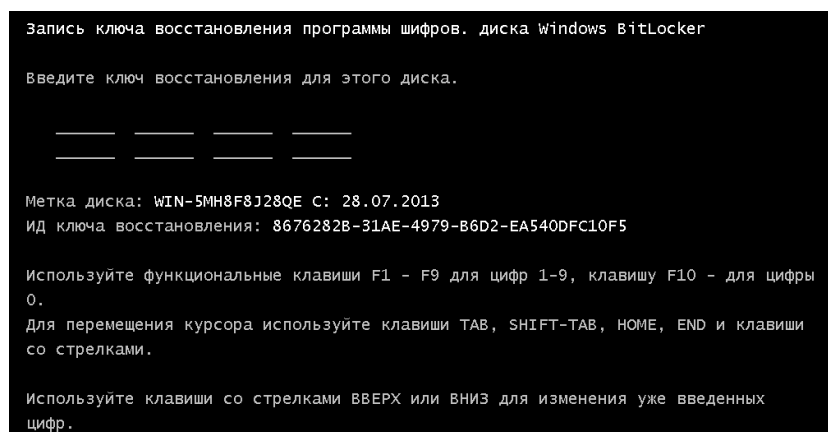


Рис. 2.24. Накопитель с ключом запуска не обнаружен

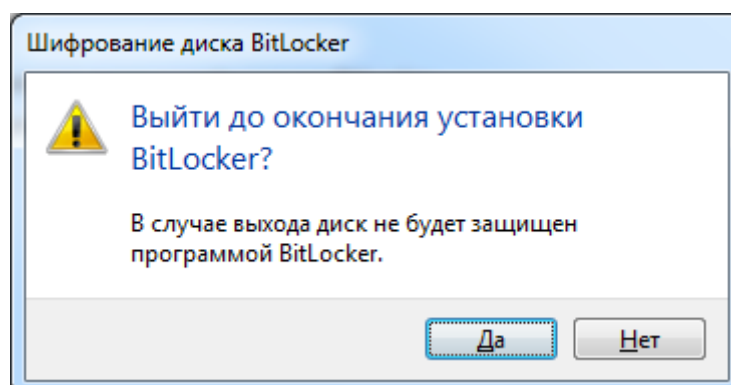
Если ключ запуска был по какой-либо причине утерян, то для загрузки системы можно воспользоваться ручным вводом 48-ми значного ключа восстановления (рис. 2.25).



**Рис. 2.25.** Ввод ключа восстановления

### *Шифрование системного диска на виртуальной машине*

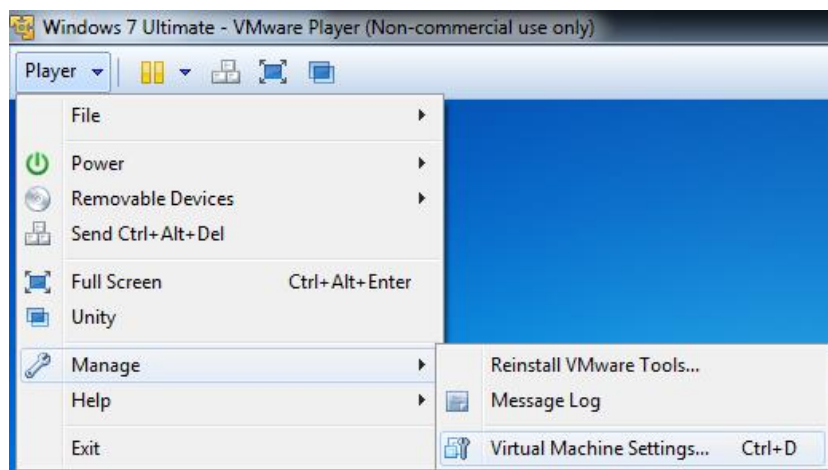
Так как BIOS на виртуальной машине в VMWare Player не поддерживает чтение USB-устройств в загрузочной среде, то продолжение действий процедуры шифрования после выполнения подготовки диска не приведет к положительному результату (отобразится ошибка). Поэтому просто отмените продолжение процедуры шифрования системного диска (рис. 2.26).



**Рис. 2.26.** Отмена процедуры шифрования системного диска

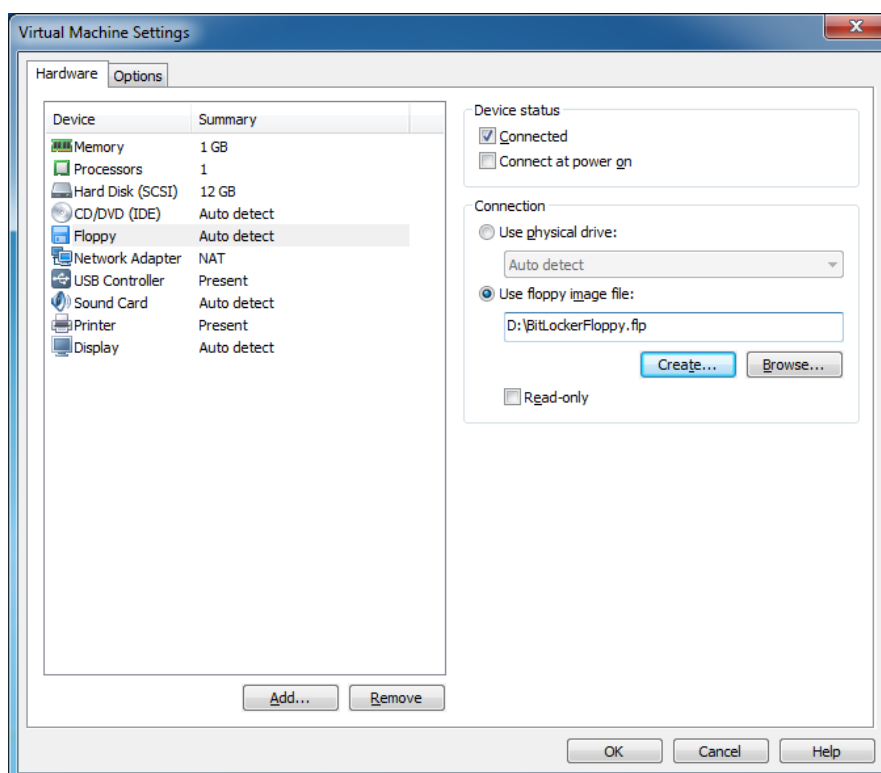
Чтобы зашифровать системный диск на виртуальной машине для сохранения ключа воспользуемся носителем другого типа, нежели USB-накопитель. Для этого необходимо сделать носителем, хранящим ключ запуска операционной системы, обычную дискету (загрузка с дискеты поддерживается на виртуальной машине). Чтобы осуществить это используем непосредственно командную строку, а не инструмент «Шифрование диска BitLocker». Также необходимо, чтобы BIOS был настроен на загрузку сначала с жесткого диска, а затем с дискеты.

Для того чтобы создать образ дискеты откройте меню программы VMWare Player, нажав кнопку «Player», и откройте настройки виртуальной машины, выполнив команду «Manage/Virtual Machine Settings...» (рис. 2.27).



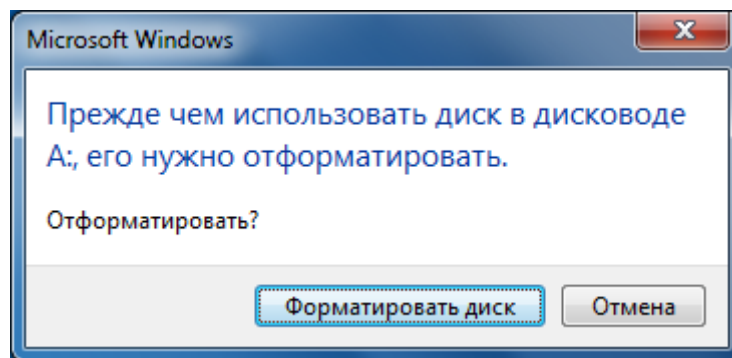
**Рис. 2.27.** Настройки виртуальной машины

В открывшемся окне настроек виртуальной машины перейдите во вкладке «Hardware» на пункт «Floppy». Отметьте пункт «Use floppy image drive» и создайте образ дискеты, нажав кнопку «Create...». Также отметьте пункт «Connected», чтобы подключить созданную дискету к виртуальной машине (рис. 2.28). Нажмите кнопку «OK».



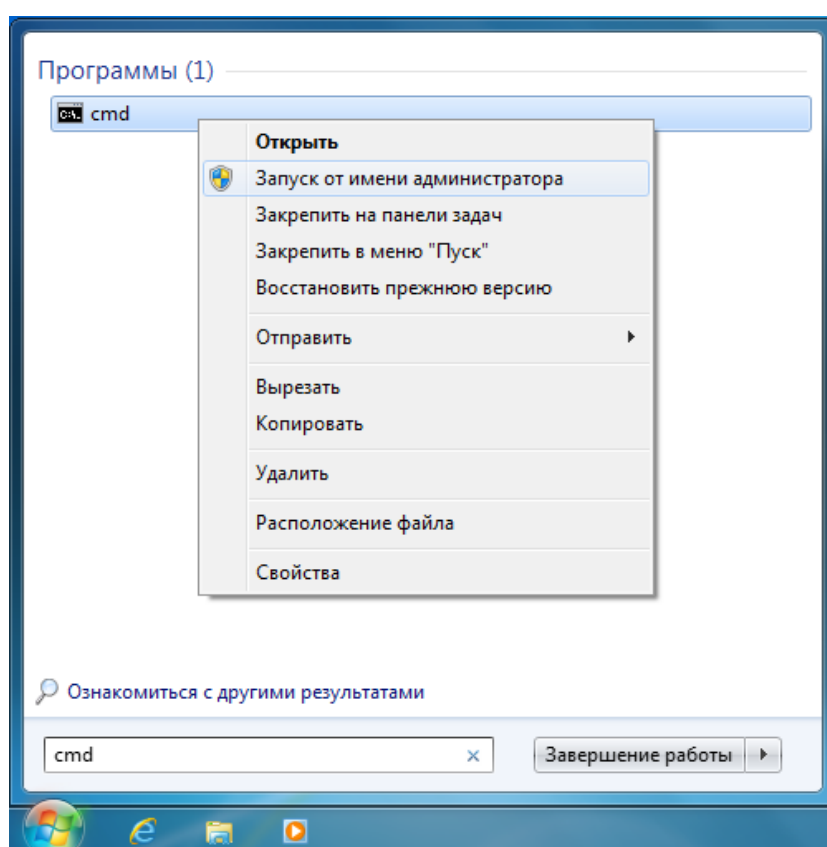
**Рис. 2.28.** Создание образа дискеты

После откройте дисковод A и отформатируйте дискету (рис. 2.29).



**Рис. 2.29.** Форматирование дискеты

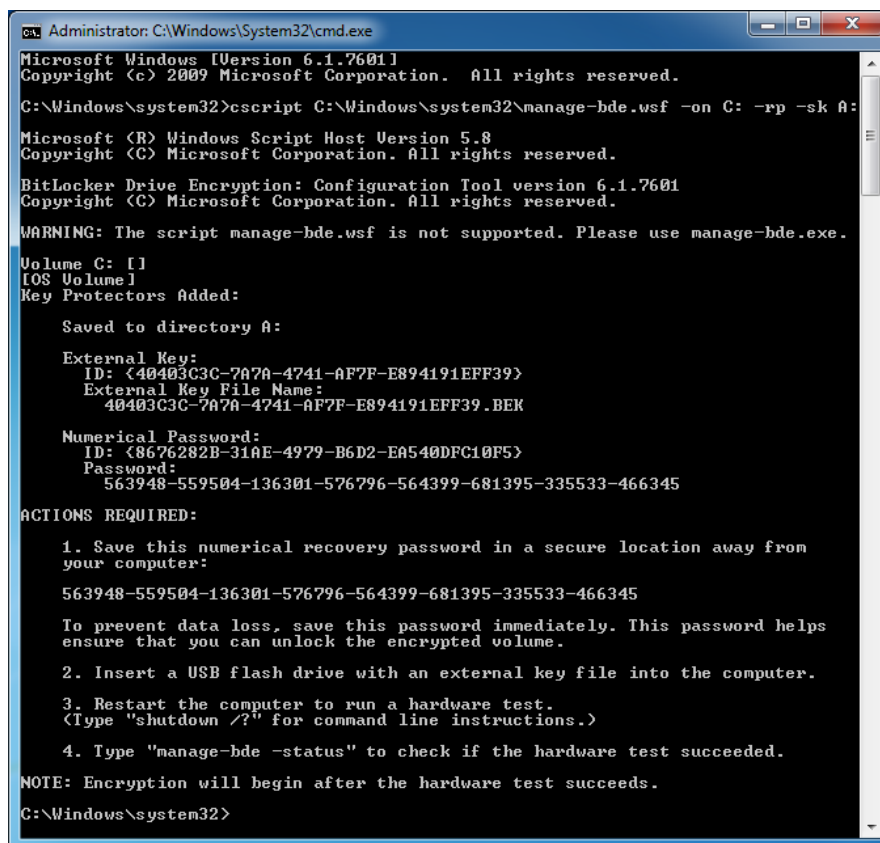
Теперь можно приступить к шифрованию системного диска. Откройте меню «Пуск», в поле поиска введите «cmd». Запустите командную строку от имени администратора (рис. 2.30).



**Рис. 2.30.** Запуск командной строки от имени администратора

В командной строке введите следующую команду (рис. 2.31):  
cscript C:\Windows\system32\manage-bde.wsf -on C: -rp -sk A:





```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cscript C:\Windows\system32\manage-bde.wsf -on C: -rp -sk A:

Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

BitLocker Drive Encryption: Configuration Tool version 6.1.7601
Copyright (C) Microsoft Corporation. All rights reserved.

WARNING: The script manage-bde.wsf is not supported. Please use manage-bde.exe.

Volume C: [I]
[OS Volume]
Key Protectors Added:

    Saved to directory A:

    External Key:
    ID: {40403C3C-7A7A-4741-AF7F-E894191EFF39}
    External Key File Name:
    40403C3C-7A7A-4741-AF7F-E894191EFF39.BEK

    Numerical Password:
    ID: {8676282B-31AE-4979-B6D2-EA540DFC10F5}
    Password:
    563948-559504-136301-576796-564399-681395-335533-466345

ACTIONS REQUIRED:

    1. Save this numerical recovery password in a secure location away from
    your computer:

    563948-559504-136301-576796-564399-681395-335533-466345

    To prevent data loss, save this password immediately. This password helps
    ensure that you can unlock the encrypted volume.

    2. Insert a USB flash drive with an external key file into the computer.

    3. Restart the computer to run a hardware test.
    (Type "shutdown /?" for command line instructions.)

    4. Type "manage-bde -status" to check if the hardware test succeeded.

NOTE: Encryption will begin after the hardware test succeeds.

C:\Windows\system32>
```

Рис. 2.31. Ввод команды на создание ключа запуска на диске

Запишите полученный 48-мизначный ключ восстановления (recovery password) в любом месте, кроме жесткого диска виртуальной машины! Лучше всего записать его либо на бумаге, либо сохранить на жестком диске системы, из которой производится запуск виртуальной машины.

После выполнения команды появится запрос на перезагрузку компьютера для начала шифрования BitLocker (рис. 2.32). Выполните перезагрузку системы.

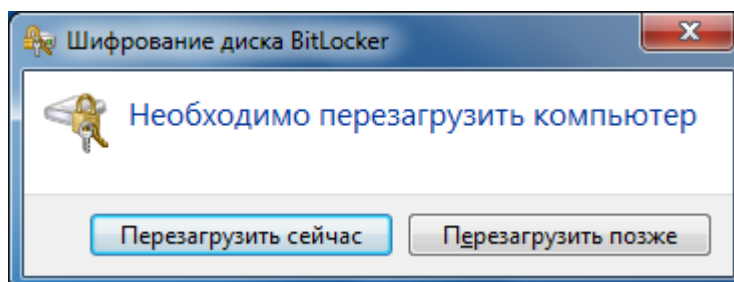
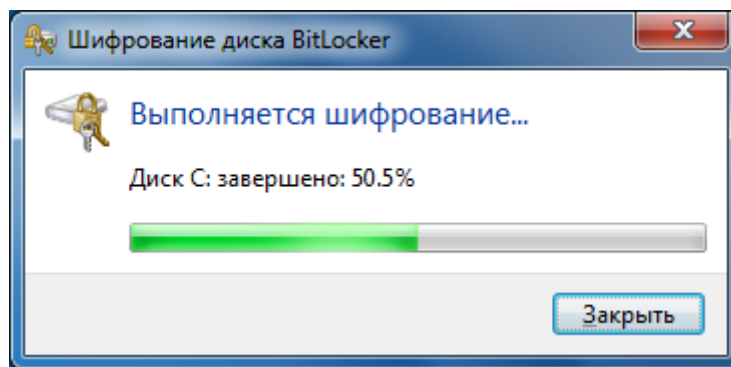


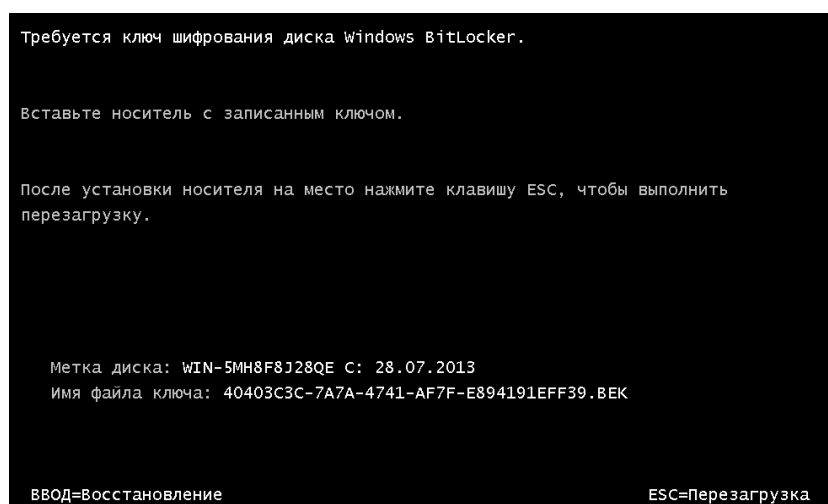
Рис. 2.32. Запрос на перезагрузку для начала шифрования BitLocker

Шифрование системного диска начнется сразу же после загрузки системы (рис. 2.33). Процесс шифрования занимает некоторое время, зависящее от объема диска.



**Рис. 2.33.** Шифрование системного диска

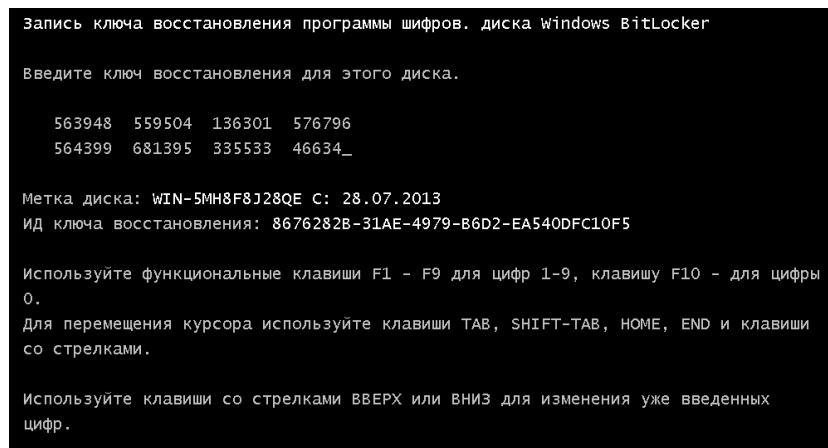
После завершения процедуры шифрования проверьте работу зашифрованной системы. Отсоедините дискету с ключом запуска. Для этого снова откройте настройки виртуальной машины и снимите отметку с пункта «Connected» для дискеты. Далее выполните перезагрузку системы. При начале загрузки системы отобразится сообщение о том, что не был подключен накопитель с ключом запуска (рис. 2.34).



**Рис. 2.34.** Запрос на подключение носителя с ключом запуска

Подсоедините дискету и нажмите Esc. Операционная система запустится.

Если же по какой-либо причине был утерян ключ запуска или сам носитель с ключом запуска, то можно воспользоваться ключом восстановления. Для этого снова отсоедините дискету и перезагрузите систему. В окне запроса носителя с ключом запуска нажмите Enter, откроется окно с вводом ключа восстановления. Введите 48-мизначный ключ восстановления, указанный системой до выполнения шифрования системного диска (рис. 2.35). После ввода правильного ключа восстановления выполнится запуск операционной системы.



**Рис. 2.35.** Запрос на ввод ключа восстановления

**Контрольные вопросы:**

- 1) В каких версиях Windows присутствует технология шифрования дисков BitLocker?
- 2) В чем отличие BitLocker от EFS?
- 3) Какой алгоритм шифрования применяется в BitLocker?
- 4) Для чего используется функция BitLocker To Go?
- 5) Какие режимы работы системы шифрования возможны для шифрования системных дисков?
- 6) Что такое TPM?