Руководство по использованию шифрования BitLocker в Windows 10

Безмалый В.Ф.
Windows Insider MVP

Проблема защиты данных в случае физической утраты компьютера или внешнего носителя (флешки) особенно актуальна для мобильных пользователей, число которых непрерывно растет.

С момента выпуска Windows Vista компания Microsoft представила новую функцию безопасности под названием BitLocker Drive Encryption. В составе Windows 7 была представлена **функция BitLocker To Go для портативных устройств хранения,** таких как флэш-накопители и SD-карты.

В случае если вы используете Windows 10, для использования шифрования вам необходимо использовать версию Pro или Enterprise. Почему Microsoft не сделает это стандартной функцией во всех версиях операционной системы, все еще непонятно, учитывая, что шифрование данных является одним из наиболее эффективных способов обеспечения безопасности. Если вы используете Windows 10 Home, вам нужно выполнить Easy Upgrade до Windows 10 Pro, чтобы провести обновление.

Что такое шифрование?

Шифрование — это способ сделать читаемую информацию неузнаваемой для неавторизованных пользователей. Когда вы шифруете свою информацию, она остается пригодной для использования, даже когда вы делитесь ею с другими пользователями. Если вы отправите зашифрованный документ Word другу, ему сначала потребуется его расшифровать. Windows 10 включает в себя различные типы технологий шифрования, **шифрованную файловую систему (EFS)** и шифрование диска BitLocker.

Что вы должны знать и сделать заранее

Шифрование всего вашего жесткого диска может быть долгим процессом. Я настоятельно рекомендую перед включением BitLocker сделать резервную копию всего компьютера . Особо рекомендуется, если у вас нет источника резервного питания, а во время шифрования произойдет его отключение.

Начиная с версии1809 для шифрования используется более безопасный стандарт, которым вы можете воспользоваться. Обратите внимание, что новый стандарт шифрования совместим только с другими системами Windows 10 1809 и выше.

Если вы используете Windows 10 на более старом компьютере без чипа Trusted Platform Module (TPM 1.2), вы не сможете настроить BitLocker. Пожалуйста, помните об этом. Как выйти из этой ситуации мы рассмотрим ниже в этой статье.

Включение шифрования диска BitLocker в Windows 10

Нажмите *Проводник> Этот компьютер*. Затем щелкните правой кнопкой мыши системный диск, на котором установлена Windows 10, затем нажмите «*Включить BitLocker»*.

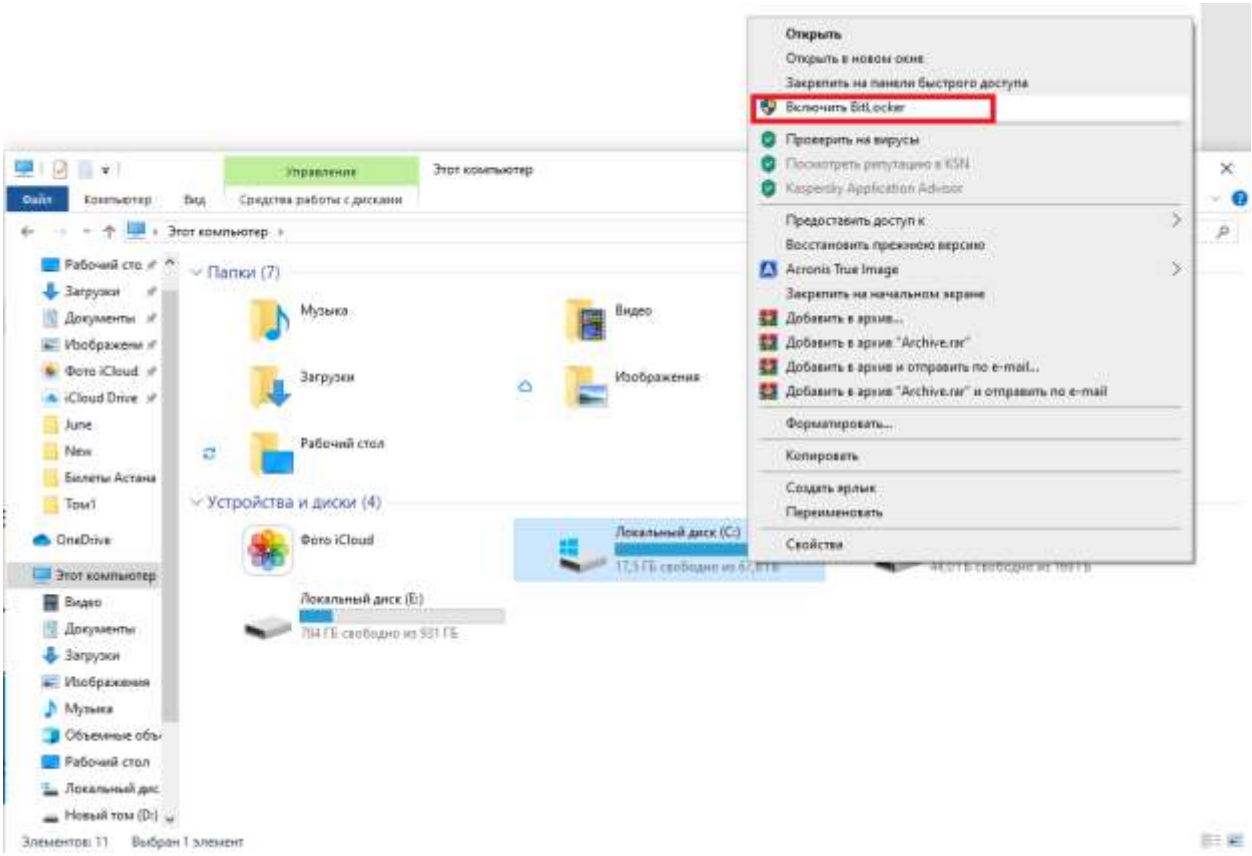
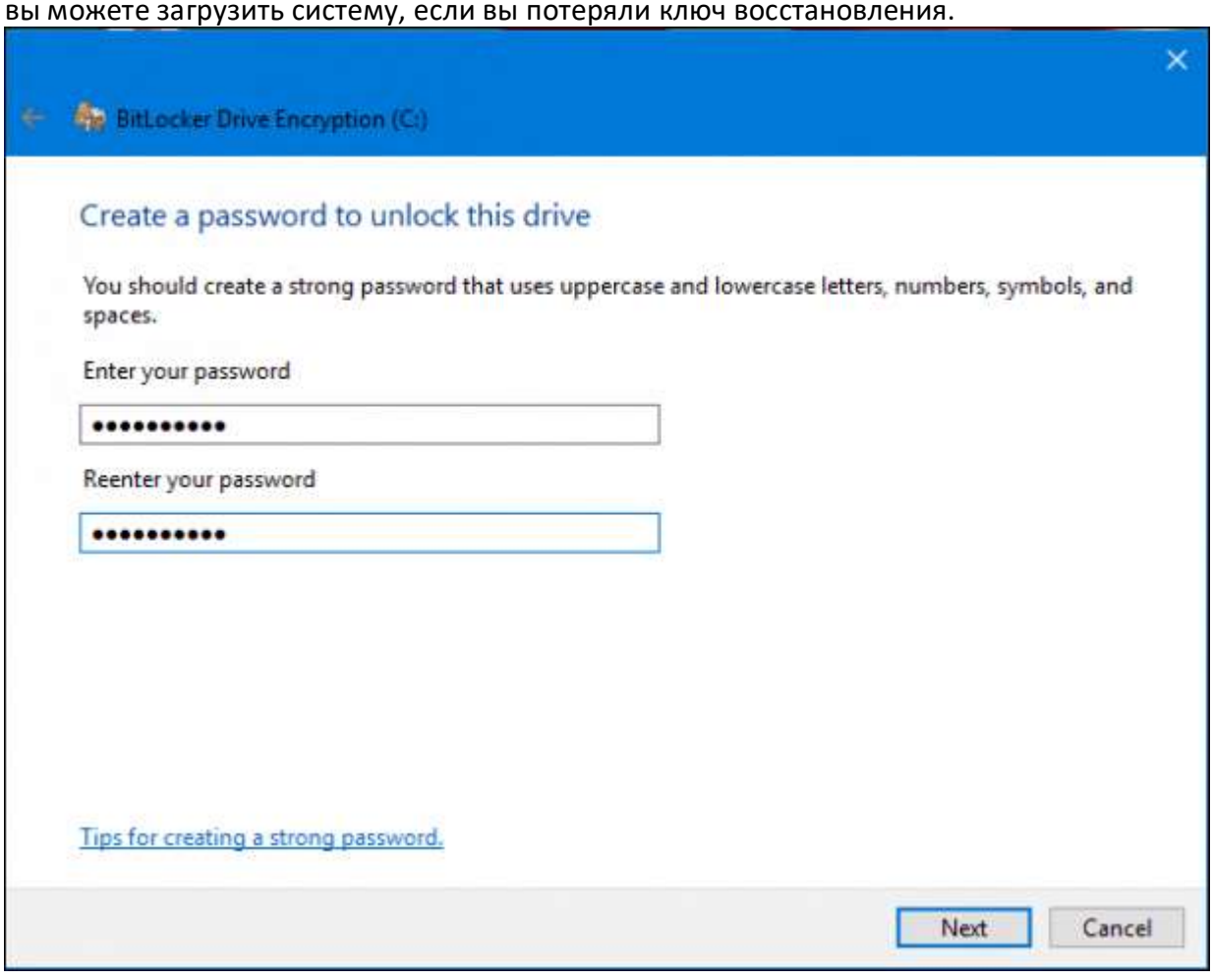


Рисунок 1 Включить BitLocker

Введите пароль, чтобы разблокировать диск; это будет важный тест, чтобы убедиться, что вы можете загрузить систему, если вы потеряли ключ восстановления.



Выберите способ резервного копирования ключа восстановления, вы можете использовать свою учетную запись Microsoft, если она у вас есть, сохранить ключ на флэш-накопителе USB, сохранить в другом месте, кроме локального диска, или распечатать копию.

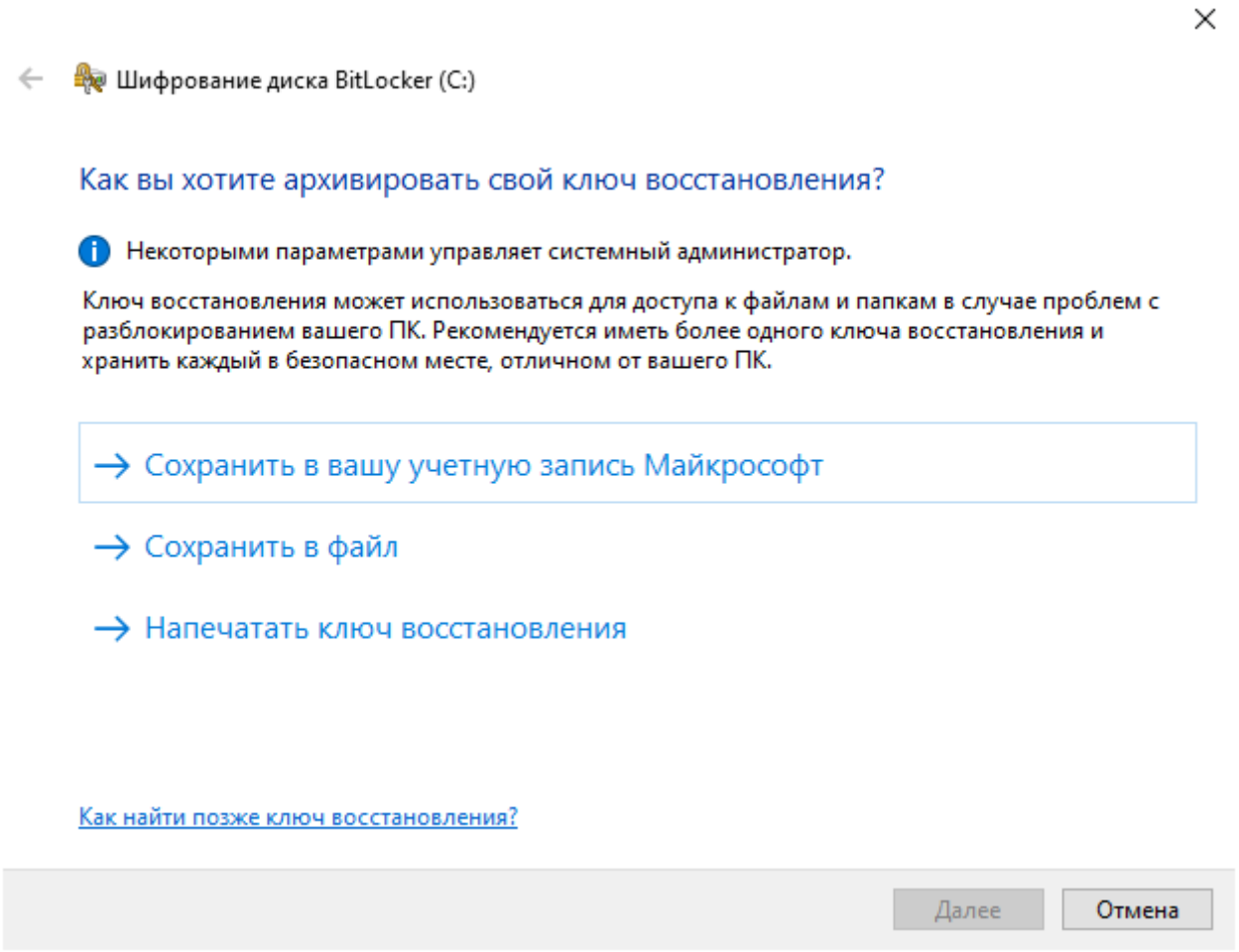


Рисунок 2 Сохранить ключ восстановления

У вас есть два варианта шифрования локального диска, если это новый компьютер, только что извлеченный из коробки, используйте только *Шифровать только используемое место*. Если он уже используется, выберите второй вариант *Зашифровать весь диск* . Поскольку я уже использовал этот компьютер, я пойду со вторым вариантом. Обратите внимание, что это займет некоторое время, особенно если это большой диск. Убедитесь, что ваш компьютер работает от источника бесперебойного питания в случае сбоя электроэнергии.

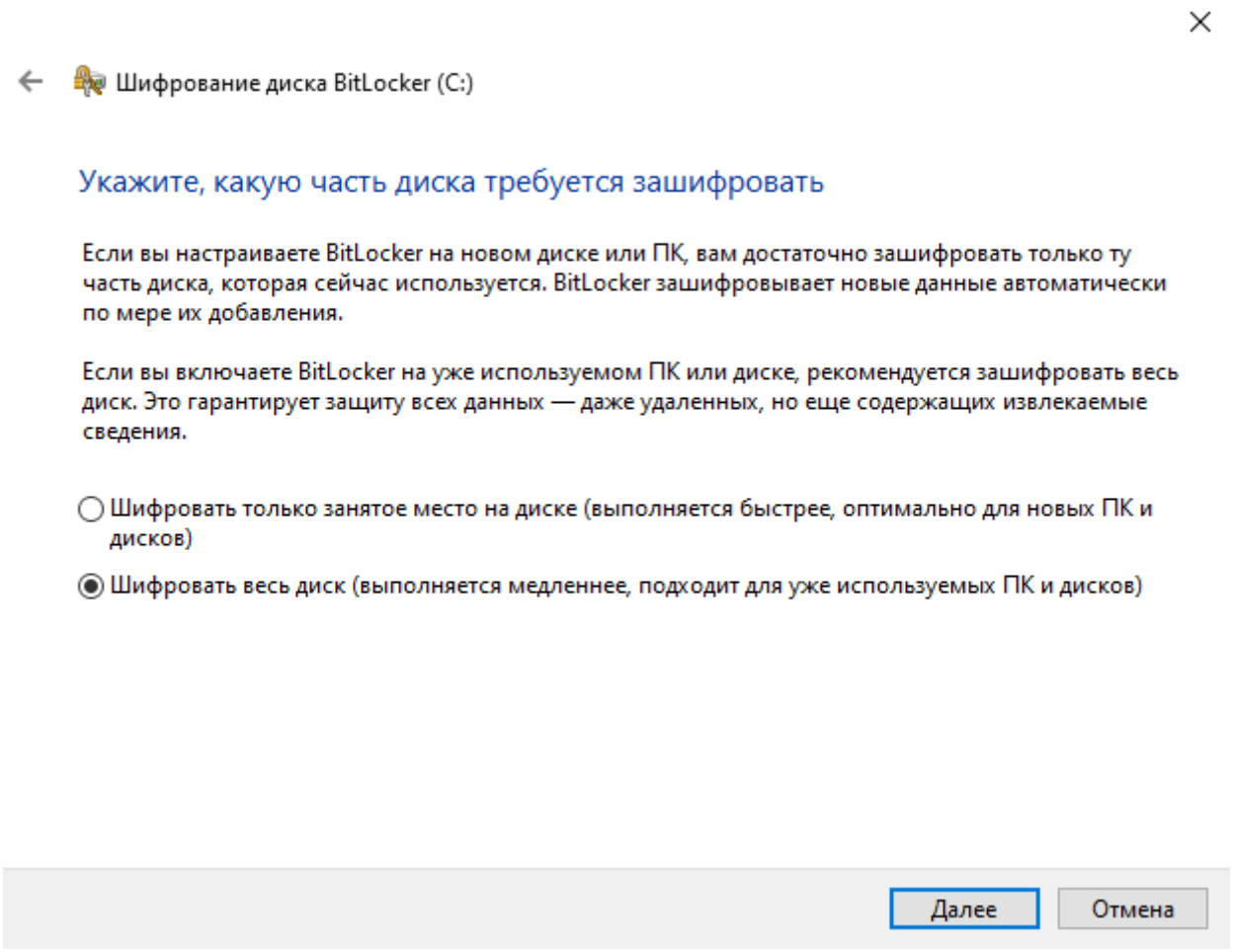


Рисунок 3 Шифровать весь диск

Если вы используете Windows 10 November Update, он включает более надежный режим шифрования под названием XTS-AES, обеспечивающий дополнительную поддержку целостности с улучшенным алгоритмом. Если это жесткий диск, выберите эту опцию.

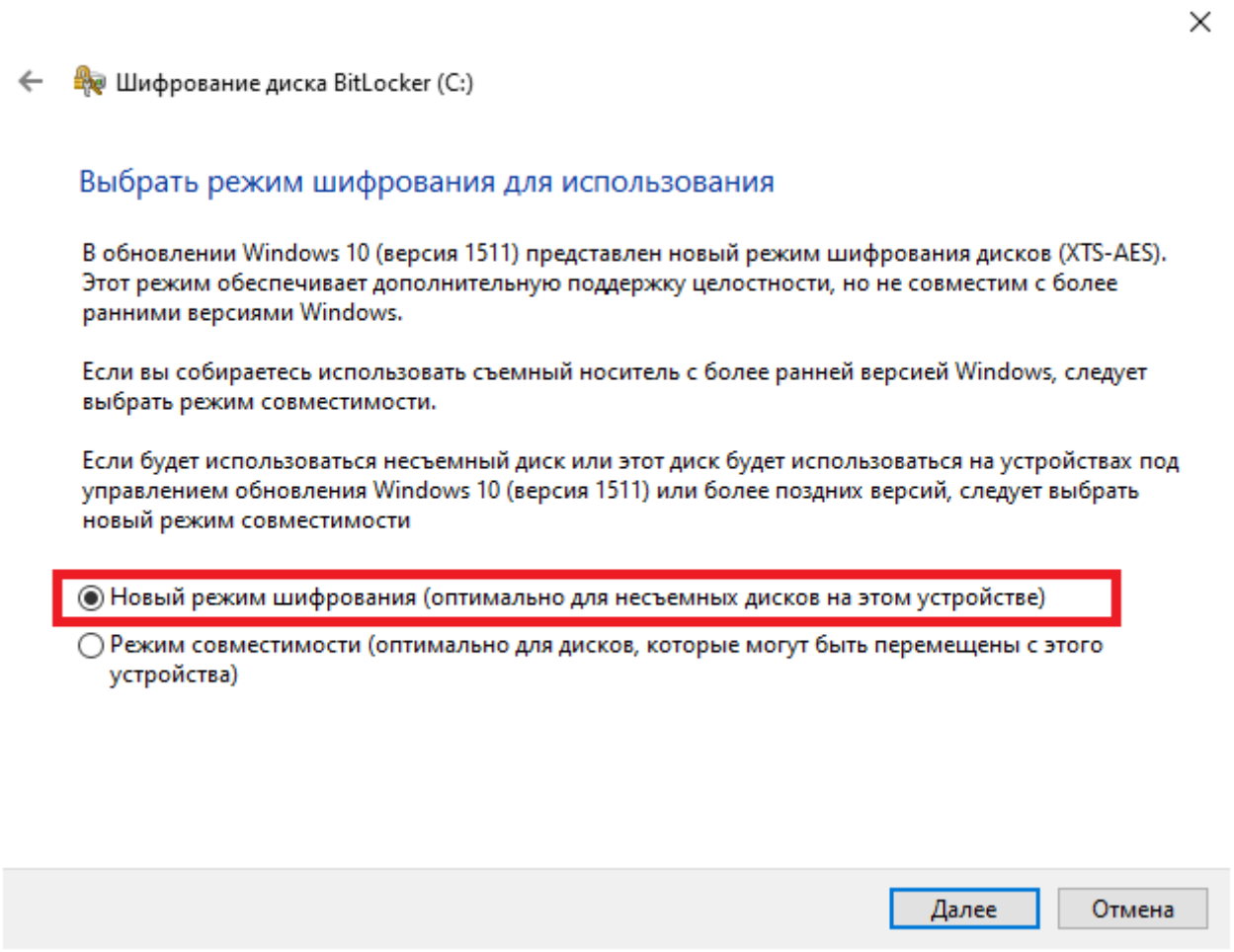


Рисунок 4 Выбор режима шифрования

Когда вы будете готовы к шифрованию, нажмите «Продолжить».

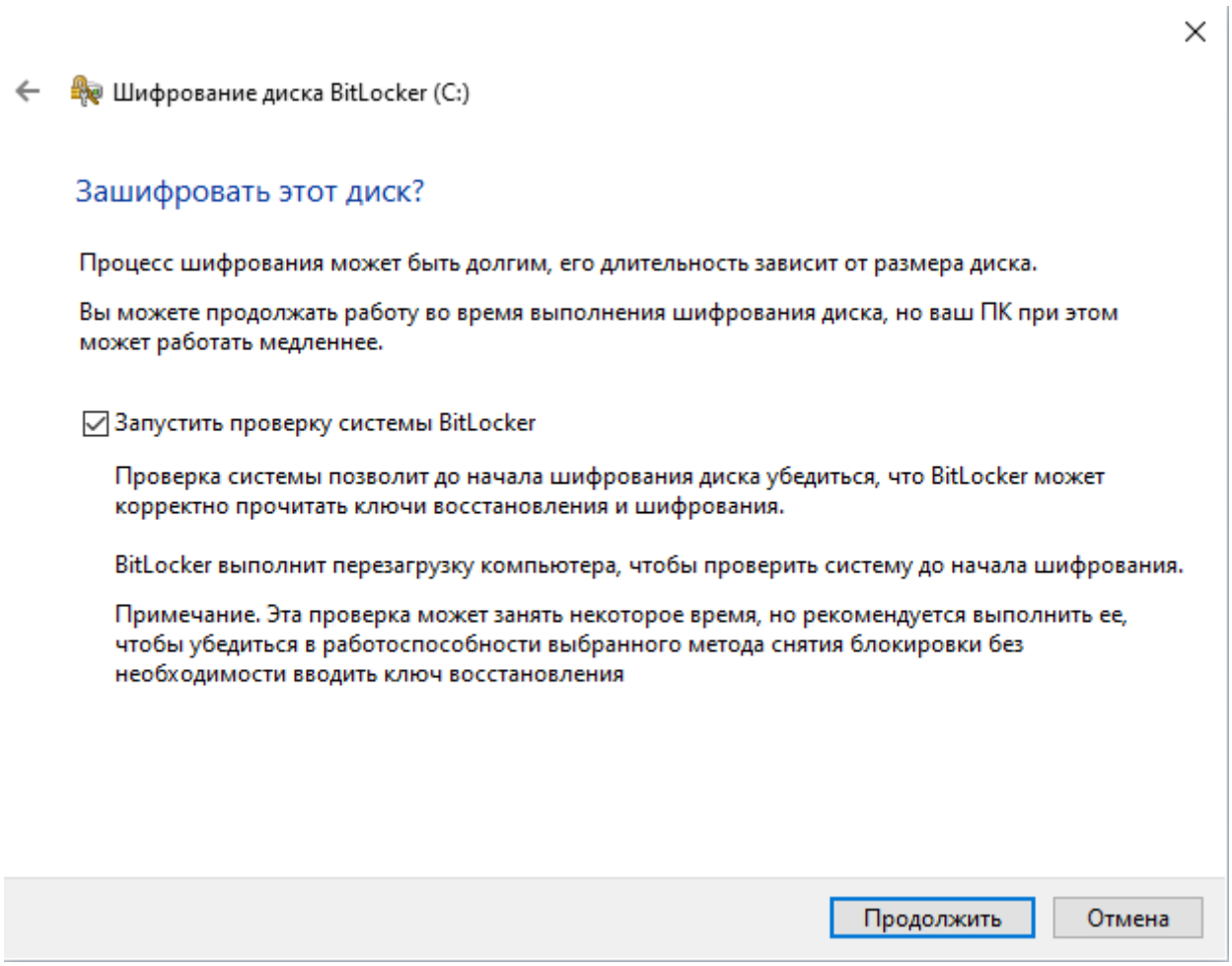


Рисунок 5 Проверка системы до начала шифрования

Перезагрузите компьютер при появлении соответствующего запроса.

Помните тот пароль, который вы создали ранее? Сейчас самое время ввести его.

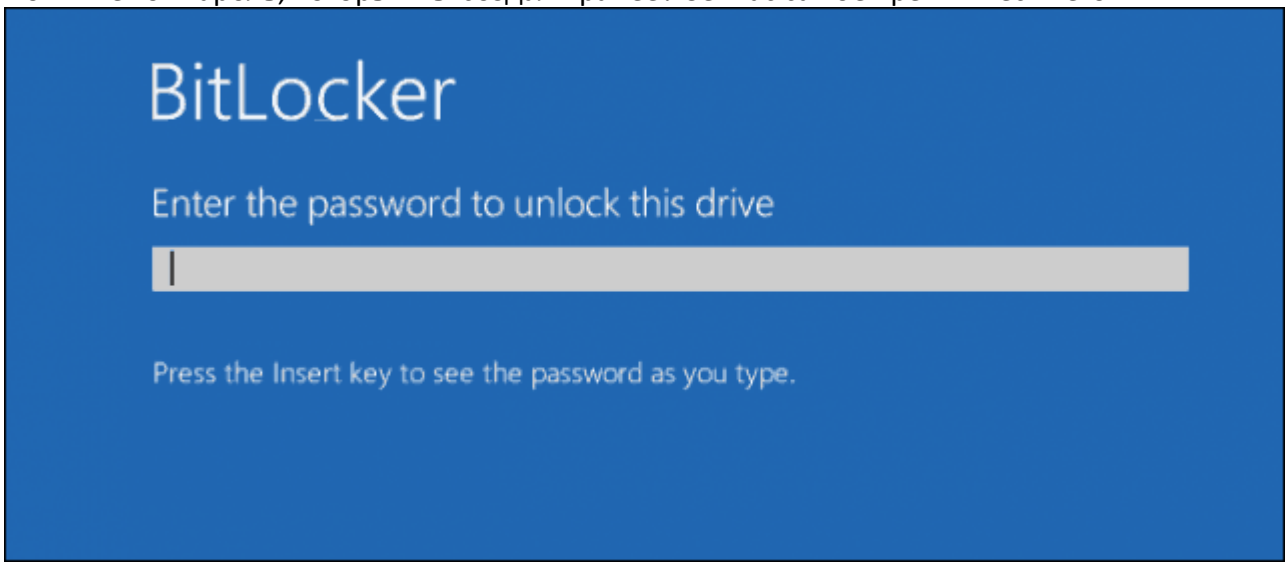
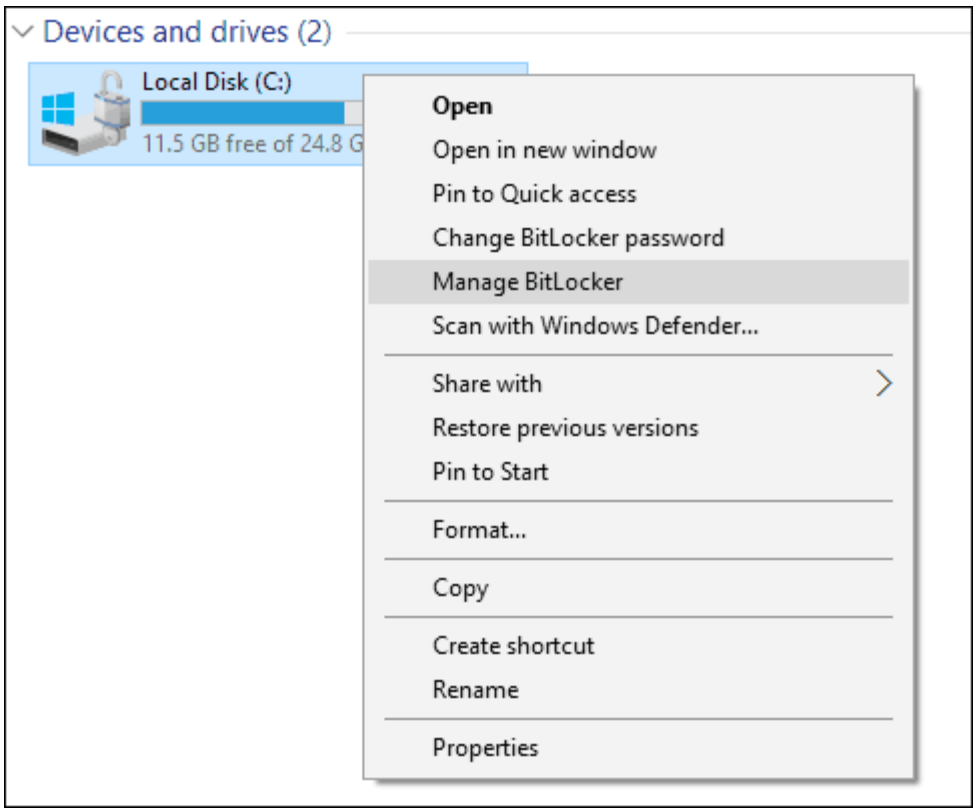


Рисунок 6 Ввод пароля

После входа в Windows 10 вы заметите, что ничего особенного не происходит. Щелкните правой кнопкой мыши на системном диске и выберите «*Управление BitLocker*».



Вы увидите текущее состояние. Это займет некоторое время, поэтому вы можете продолжать пользоваться компьютером, пока шифрование выполняется в фоновом режиме, и вы получите уведомление, когда оно будет завершено.

Когда шифрование BitLocker завершено, вы можете использовать компьютер как обычно. Любой контент, созданный в дополнение к вашим сообщениям, будет защищен.

Если в любой момент вы захотите приостановить шифрование, вы можете сделать это с помощью элемента панели управления шифрованием BitLocker. Нажмите на ссылку *Приостановить* . Данные, созданные в режиме ожидания, не шифруются. Рекомендуется отключить шифрование BitLocker при обновлении Windows, изменении прошивки компьютера или внесении изменений в оборудование.

Устранение неполадок при установке BitLocker

Если при попытке установить BitLocker появляется следующая ошибка, это, вероятно, означает, что ваш компьютер не поддерживает микросхему Trusted Platform Module (1.2).

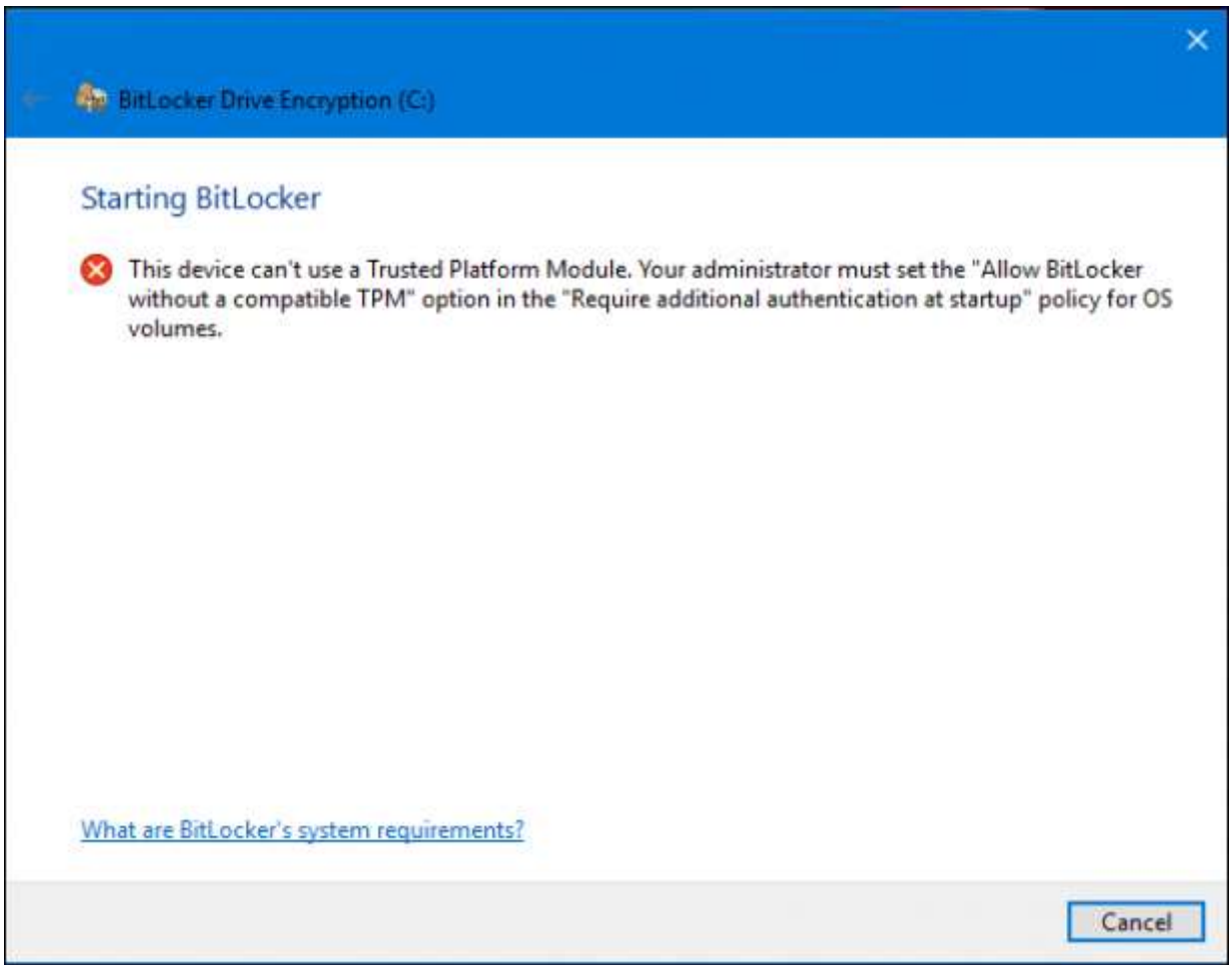
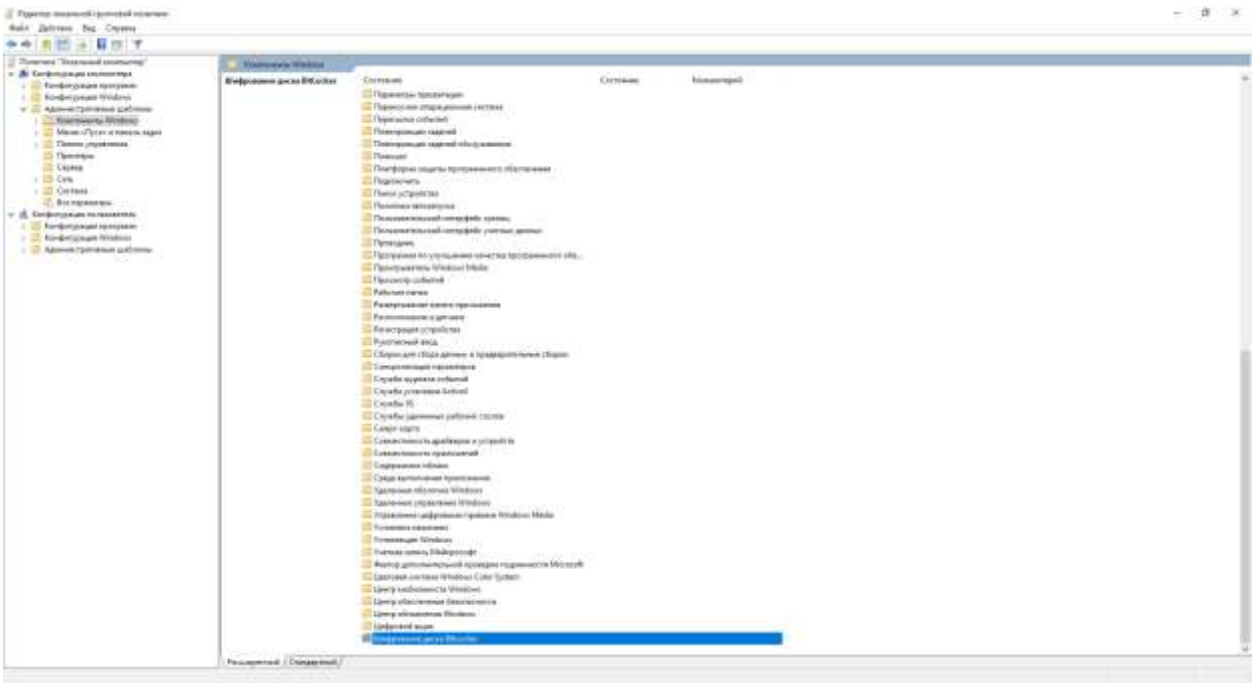


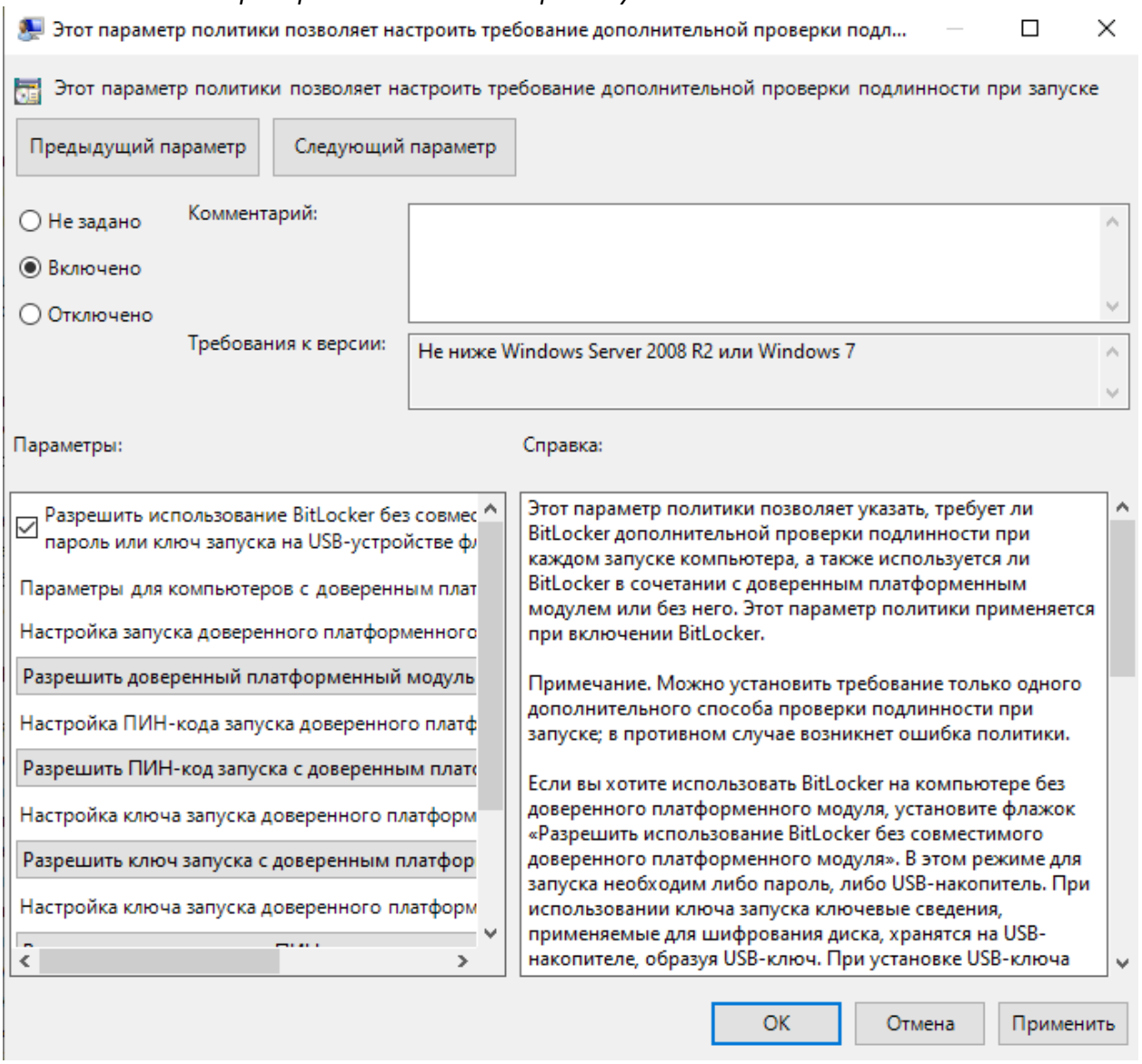
Рисунок 7 Ваш компьютер не оборудован Trusted Platform Module

На самом деле, прежде чем идти дальше в групповые политики, рекомендую вначале зайти в BIOS и проверить, а включена ли там поддержка TPM. В моем случае решение было именно таким.

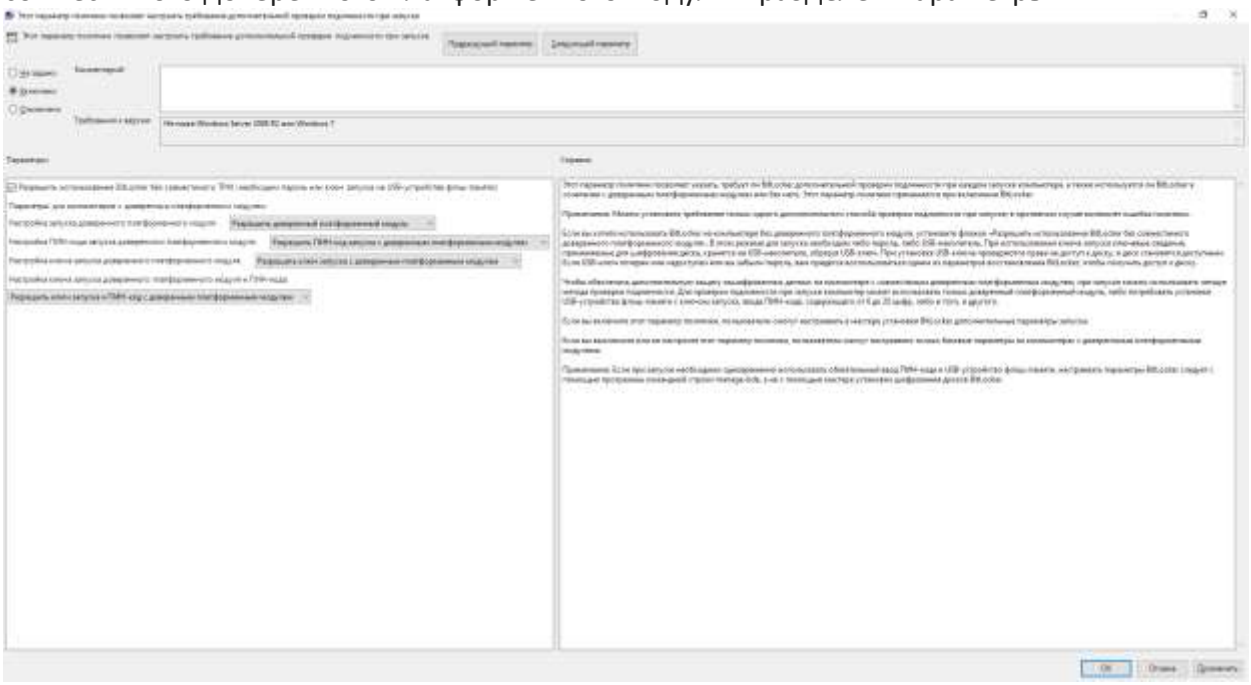
Если же ваш компьютер действительно не оборудован TPM, то в групповой политике вы сможете задать исключение. Для этого нажмите **клавиши Windows+R**, а затем введите gpedit.msc и нажмите Enter. Выберите *Административные шаблоны – Компоненты Windows – Шифрование BitLocker – Диски операционной системы.*



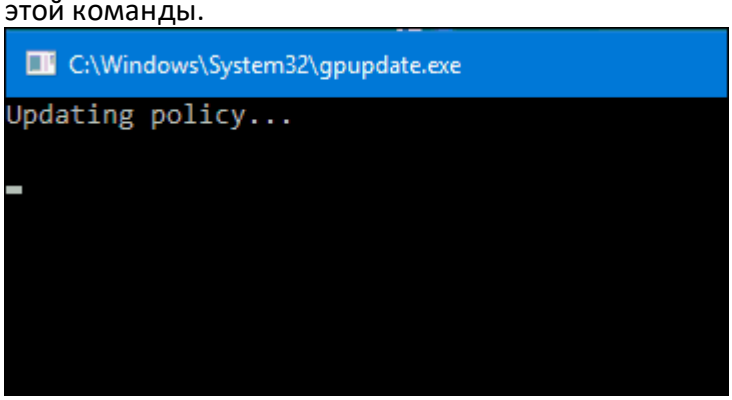
Выберите параметр *«Этот параметр позволяет настроить требование дополнительной проверки подлинности при запуске»*



Щелкните правой кнопкой мыши «*Требовать дополнительную аутентификацию при запуске» и* нажмите «*Изменить».*
Выберите «*Включено»,* а затем установите флажок, чтобы разрешить BitLocker без совместимого доверенного платформенного модуля в разделе «Параметры».

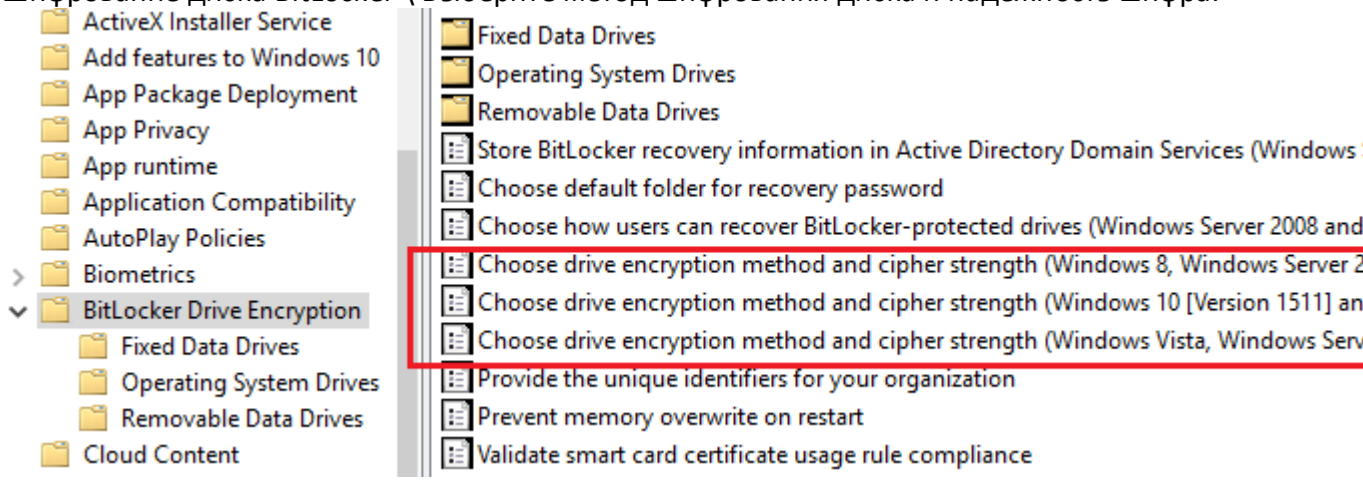


Подтвердите изменения
Нажмите Пуск, затем **введите:** *gpforce.exe / update,* чтобы убедиться, что изменения вступили в силу. Я также рекомендовал бы перезагрузить компьютер после выполнения этой команды.

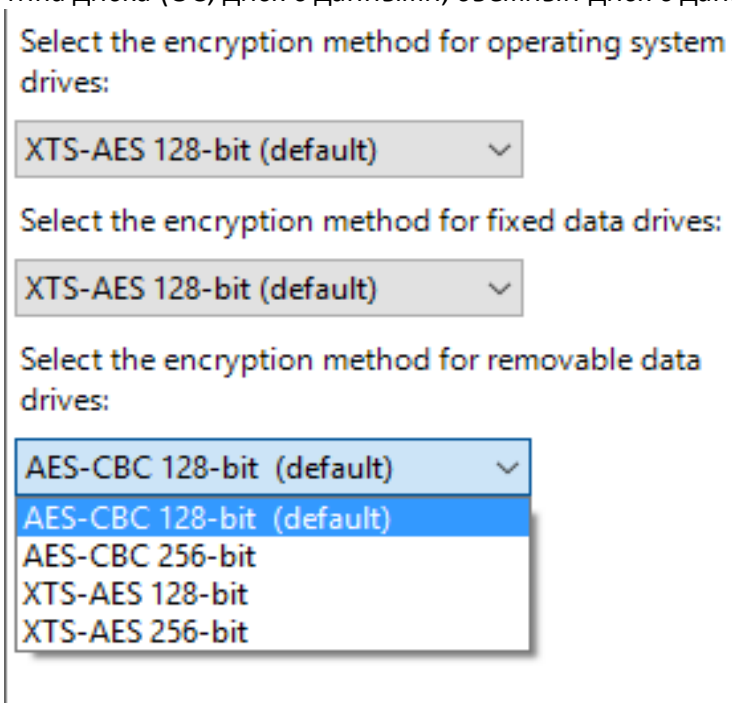


Помните, что вы также можете шифровать флэш-диски и SD-диски.
BitLocker: AES-XTS (новый тип шифрования)
Bitlocker использует AES **(Advanced Encryption Standard)** для шифрования данных на дисках. **AES - это блочный шифр** (в отличие от потокового шифра), который делит простой текст на блоки одинакового размера и затем шифрует каждый блок отдельно. Если данные больше, чем размер блока, они должны быть разделены. Проще всего, данные разделяются на отдельные блоки, а последний блок расширяется битами заполнения. Это самый простой метод преобразования, называемый режимом электронной кодовой книги (ECB), который можно легко перевернуть (одинаковые блоки открытого текста всегда генерируют одинаковые зашифрованные блоки).
Вот почему математики разработали несколько других, более безопасных и менее предсказуемых блочных режимов, называемых «режимами работы блочного шифра», таких как CBC, XTS, LRW, CFB, CCM, OFB и OCB. Общая концепция этих режимов состоит в том, чтобы ввести рандомизацию незашифрованных данных на основе дополнительного ввода (вектора инициализации).

В **BitLocker** AES работает в 2 режимах:
CBC - цепочка зашифрованных блоков (CBC) - в этом режиме открытый текст текущего блока передается XOR с зашифрованным текстом предыдущего блока перед шифрованием. Это дает уверенность в том, что одни и те же данные в разных секторах будут давать разные результаты после шифрования. Первый блок в этом режиме получит случайный вектор инициализации (IV). Режим CBC для Bitlocker **был введен в Windows Vista.**
XTS - основанный на XEX режим твик-кодовой книги - в этом режиме мы по-прежнему выполняем функцию XOR между блоками, но также добавляем дополнительный твик-ключ для улучшения перестановки. Этот ключ настройки может быть адресом сектора или комбинацией адреса сектора и его индекса. Режим XTS для Bitlocker **был введен в Windows 10 (сборка 1511).**
Оба режима поддерживают длину ключа 128 и 256 бит.
Выбор этих двух может быть контроллером через объект групповой политики в разделе **Конфигурация компьютера** \ Административные шаблоны \ Компоненты Windows \ Шифрование диска BitLocker \ Выберите метод шифрования диска и надежность шифра:



Для версии Windows 10 1511 и выше мы можем выбрать разные алгоритмы для каждого типа диска (ОС, диск с данными, съемный диск с данными):



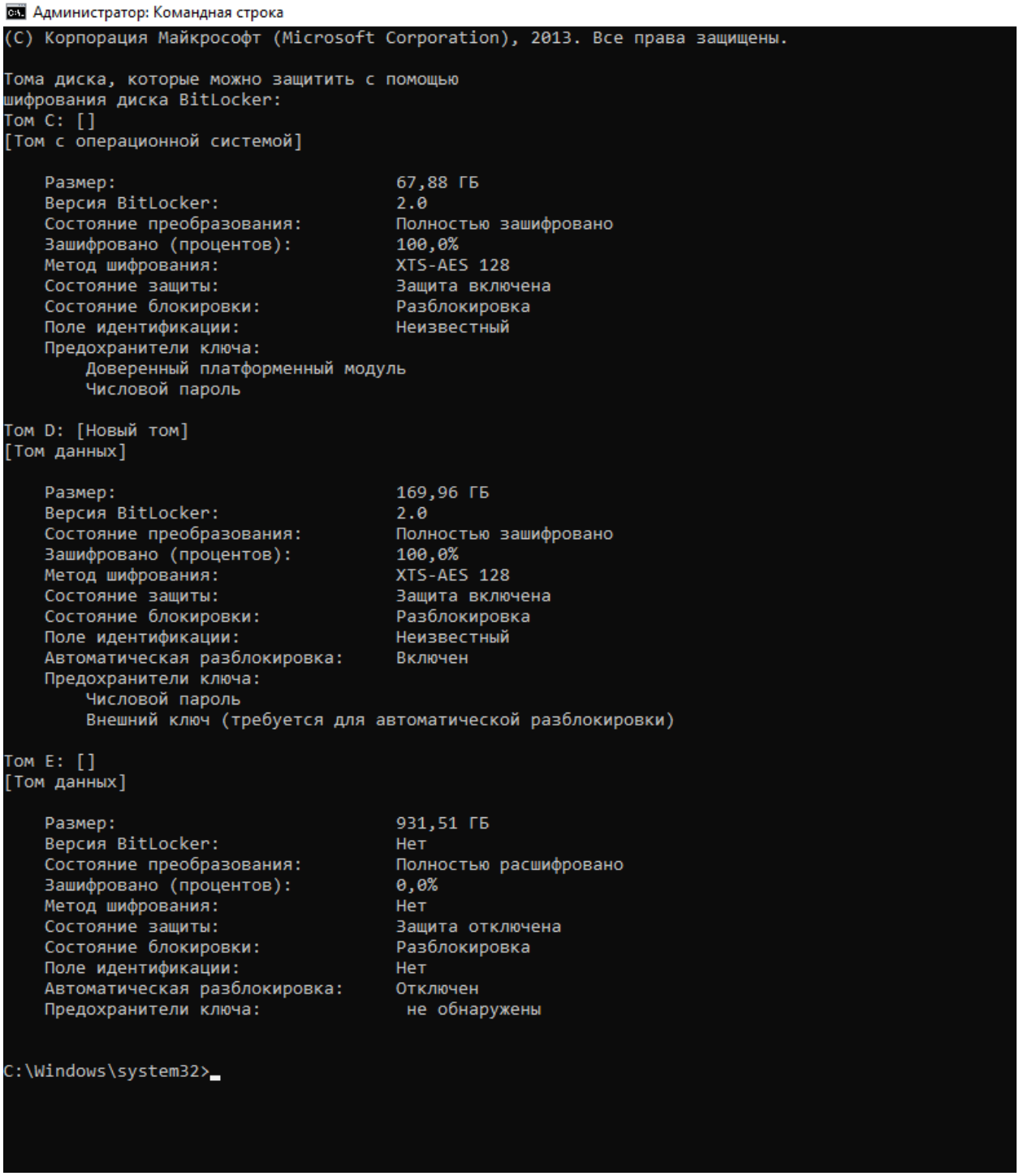
Примечание: в Windows 7 был также AES CBC с Elephant Diffuser, который был удален в Windows 8.
Вышеуказанная конфигурация алгоритмов для Windows 10 (сборка 1511) хранится как **REG_DWORD** с:
HKLM \ SOFTWARE \ Policies \ Microsoft \ FVE
Диски с операционной системой: EncryptionMethodWithXtsOs
Фиксированные диски данных: EncryptionMethodWithXtsFdv
Съемные диски с данными: EncryptionMethodWithXtsRdv
Возможные значения:
AES-CBC 128bit - значение 3
AES-CBC 128bit - значение 4
AES-XTS 128bit - значение 6
AES-XTS 256 бит - значение 7
Тип шифрования для Windows 8 и Windows 10 (ранее 1511) сохраняется как **REG_DWORD** в:
HKLM \ SOFTWARE \ Policies \ Microsoft \ FVE
EncryptionMethodNoDiffuser
AES CBC 128 бит - значение 3
AES CBC 256bit - значение 4

Тип шифрования для Windows Vista и Windows 7 сохраняется как **REG_DWORD** в:
HKLM \ SOFTWARE \ Policies \ Microsoft \ FVE
EncryptionMethod
AES CBC 128 бит - значение 3
AES CBC 256bit - значение 4
AES CBC 128 бит с рассеивателем - значение 1
AES CBC 256 бит с диффузором - значение 2
Так в чем же режим безопасности XTS лучше, чем CBC? Если мы говорим о Bitlocker, мы ясно видим преимущество в производительности:
Начальное время шифрования тома 10 ГБ

Режим AES:	**время шифрования:**
CBC 128bit	11м 49с
CBC 256bit	11м 44с
XTS 128bit	11 м 15 с
XTS 256bit	11м 16с

Ваш индивидуальный тест может отличаться, поскольку производительность шифрования Bitlocker зависит от нескольких факторов, таких как: тип диска (SSD / HDD), прошивка, рабочая нагрузка и многое другое ...
Вместе с тем необходимо отметить, что далеко не всегда вы можете доверять **BitLocker** для шифрования вашего SSD в Windows 10. Почему? Увы, причина достаточно проста. Некоторые SSD объявляют о поддержке «аппаратного шифрования». Если вы включите BitLocker в Windows, Microsoft доверяет вашему SSD и ничего не делает. Но исследователи обнаружили, что многие твердотельные накопители выполняют шифрование просто ужасно, а это означает, что BitLocker не обеспечивает безопасное шифрование.
Microsoft выпустила уведомление по безопасности об этой проблеме. И сегодня для того чтобы проверить используете ли вы аппаратное или программное шифрование вам необходимо сделать следующее:
Запустите файл **manage-bde.exe -status** из командной строки с повышенными привилегиями.

Если ни один из перечисленных дисков не отображает «Аппаратное шифрование» для поля «Метод шифрования», то это устройство использует программное шифрование и не подвержено уязвимостям, связанным с самошифрованием вашего диска.



Для дисков, которые зашифрованы с использованием уязвимой формы аппаратного шифрования, вы можете уменьшить уязвимость, переключившись на программное шифрование с помощью Bitlocker с групповой политикой.

Примечание . После того, как диск был зашифрован с использованием аппаратного шифрования, для переключения на программное шифрование на этом диске потребуется сначала его дешифрование, а затем повторное шифрование с использованием программного шифрования. Если вы используете шифрование диска BitLocker, изменение значения групповой политики для принудительного использования только программного шифрования недостаточно для повторного шифрования существующих данных.

Увы, но многие твердотельные накопители не выполняют шифрование должным образом
Это вывод из новой статьи исследователей из Radbound University. Они пересмотрели микропрограммы многих твердотельных накопителей и обнаружили множество проблем с «аппаратным шифрованием», обнаруженным во многих твердотельных накопителях.
Исследователи протестировали диски Crucial и Samsung, но нет гарантии, что у других производителей нет серьезных проблем с шифрованием.
Например, Crucial MX300 по умолчанию содержит пустой мастер-пароль. Да, все верно - у него мастер-пароль не установлен, и этот пустой пароль дает доступ к ключу шифрования, который шифрует ваши файлы.
Как заставить BitLocker использовать только программное шифрование?
Конфигурация компьютера \ Административные шаблоны \ Компоненты Windows \ Шифрование диска BitLocker \ Фиксированные диски с данными
Дважды щелкните параметр «Этот параметр политики позволяет настроить использование аппаратного шифрования для несъемных дисков с данными» на правой панели.

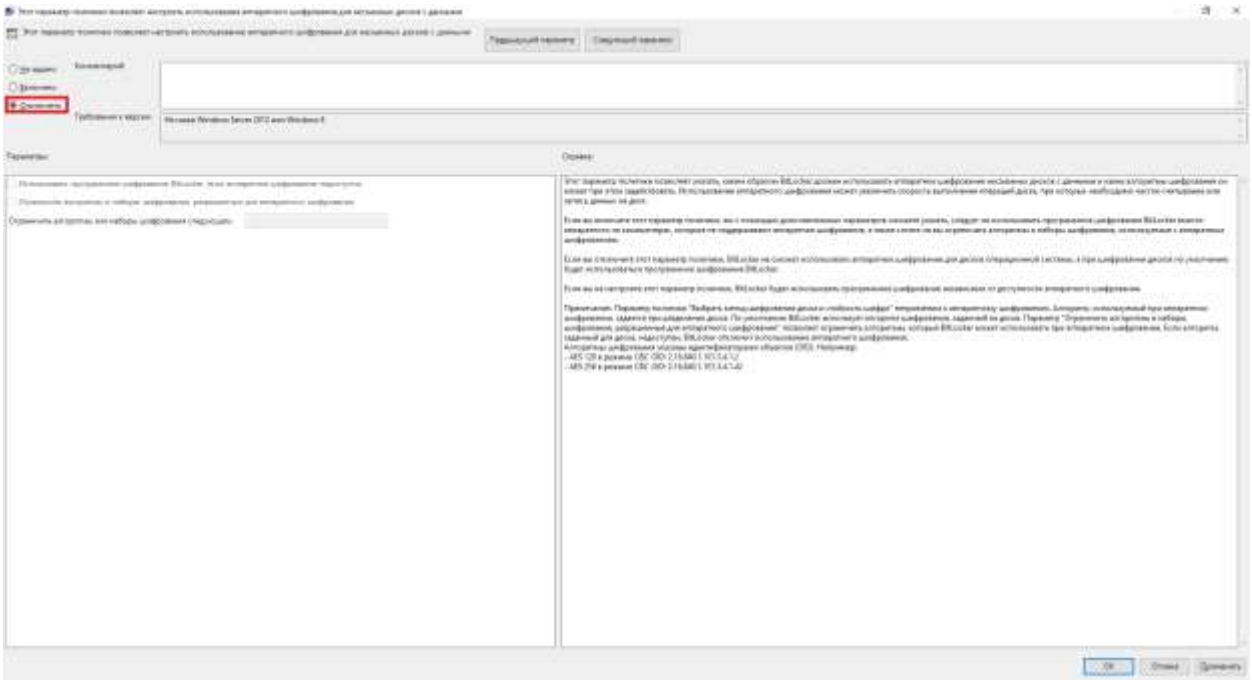


Рисунок 8 Установка программного шифрования
Выберите опцию «Отключено» и нажмите «ОК».
Если у вас использовалось аппаратное шифрование, то вы должны расшифровать и повторно зашифровать диск после того, как это изменение вступит в силу.
Почему BitLocker доверяет твердотельным накопителям?
При наличии аппаратного шифрования, процесс шифрования может происходить быстрее, чем используя программное шифрование. Таким образом, если SSD имеет надежную аппаратную технологию шифрования, использование SSD приведет к повышению производительности.
К сожалению, оказывается, что многим производителям твердотельных накопителей нельзя доверять. Мы не можем быть уверены в правильной реализации шифрования.
В идеальном мире аппаратно-ускоренное шифрование безусловно лучше. Это одна из причин, почему Apple включает чип безопасности T2 на своих новых Mac. Чип T2 использует аппаратно-ускоренный механизм шифрования для быстрого шифрования и дешифрования данных, хранящихся на внутреннем SSD Mac.

Но ваш ПК с Windows не использует подобную технологию - у него есть SSD от производителя, который, вероятно, не слишком много думал о безопасности. И это не плохо.

Еще один часто задаваемый вопрос, а не является ли нарушением приватности хранение ключей шифрования BitLocker в облаке?

В последнее время масса публикаций о конфиденциальности в Windows 10 заполонила Интернет. Microsoft обвиняют в нарушении конфиденциальности, в хранении в облаке ключей шифрования, в отслеживании географических координат нахождения смартфона (планшета) и т. д. Проблема же главным образом в том, что пользователи не читают документацию и тем более не готовы настраивать параметры конфиденциальности. Хотя есть данные, что Windows 10 может отправлять в Microsoft некоторые сведения о пользователе и при включенном в настройках конфиденциальности запрете.

Для сравнения, iOS пока позволяет только частично управлять приватностью, а Android вообще шлёт всё, не учитывая пожелания пользователей на этот счёт (не считая варианта «не пользоваться», конечно).

Что касается ключей шифрования BitLocker, то на самом деле в облаке Microsoft хранятся не ключи шифрования, а ключ для расшифровки в том случае, если по какой-то причине вы не можете расшифровать диск стандартным способом. Единственный сценарий, для которого этот ключ понадобится, это если вас остановят на границе и потребуют расшифровать ваш диск. Если вы подозреваете Microsoft в краже ваших данных, то BitLocker от такого сценария не спасёт в любом случае, ведь когда ОС включена, он ничего не защищает.

При шифровании вам предлагают:

Сохранить резервный ключ в облаке.

Сохранить резервный ключ в файле на другом носителе.

Распечатать резервный ключ.

Запомните, вы сами выбираете что вы будете делать! Единственное — помните, что вы должны его не потерять, следовательно, наиболее оптимальным является сохранить его в нескольких местах.

Учтите: при сохранении файла с ключом на OneDrive вы не видите данный файл при просмотре облака. Он не виден при просмотре файлов и папок. Для того чтобы увидеть данный файл, вы должны перейти по ссылке https://onedrive.live.com/recoverykey .

Запомните: существует несколько мест, в которых может храниться ключ восстановления BitLocker. Вот что нужно проверить:

Подключенную к Интернету учетную запись Microsoft. Это возможно только на компьютерах, не входящих в домен. Чтобы получить ключ восстановления, перейдите на страницу Ключи восстановления BitLocker.

Сохраненную копию ключа восстановления. Возможно, копия ключа восстановления BitLocker сохранена в файле, на USB-флэшке либо имеется печатная бумажная копия.

Если ключ сохранен в файл или напечатан, найдите эту копию, следуйте инструкциям на заблокированном компьютере и введите ключ при отображении запроса.

Если ключ сохранен на флэшке, вставьте ее и следуйте инструкциям на экране компьютера. Если ключ восстановления сохранен в качестве файла на флэшке, потребуется открыть файл и ввести ключ вручную.

Что же касается того, что некоторые пользователи считают, что хранение ключа BitLocker в облаке является нарушением закона о персональных данных, спешу их огорчить и порекомендовать прочесть ФЗ «О персональных данных».

Согласно п.1 ст.3 152-ФЗ «персональные данные — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту

персональных данных)», а ключ расшифрования BitLocker относится в первую очередь к ПК, а не к его пользователю.

Использование ключа восстановления BitLocker

В ходе использования шифрования BitLocker ключевым вопросом является хранение ключа восстановления. В Windows 7 ключ восстановления мы могли хранить либо в текстовом файле на внешнем носителе, либо распечатать его и хранить на бумаге. И тот и другой способ были явно недостаточно безопасны. Безусловно, у вас мог быть и третий путь – хранить файл с ключом восстановления в облаке. Но снова-таки, этот файл нужно было бы заархивировать с паролем. А пароли пользователи имеют обыкновение просто забывать. Итак, круг замкнулся. Для того, чтобы не забыть – нужно хранить. Для того чтобы хранить – нужно зашифровать с паролем. Для того чтобы зашифровать – нужно не забыть. Короче – замкнутый круг.

В Windows 10 пользователям при использовании BitLocker на не доменном компьютере предложили другой вариант. Хранить ключ восстановления в облаке. Этот вариант можно использовать наряду с традиционным распечатыванием или хранением в файле на внешнем носителе.

Вариант хранить ключ восстановления в файле на том же жестком диске не рассматривается ввиду явной небезопасности.

Если вы решите включить шифрование, то вам предложат создать ключ восстановления Безусловно, лучше хранить ключ восстановления в нескольких местах.

Итак, мы выбираем «Сохранить в вашу учетную запись Майкрософт». При этом в вашем облачном хранилище будет создан текстовый файл, содержащий ваш ключ восстановления. Стоит отметить, что, просматривая ваш OneDrive, вы не увидите этот файл. То есть дать общий доступ к файлу ключа восстановления невозможно ни случайно, ни специально.

Для того чтобы получить доступ к файлу восстановления, который вам может потребоваться в экстренной ситуации, вы можете войти в вашу учетную запись Microsoft на любом другом ПК (планшете, смартфоне) и выбрать ссылку Ключ восстановления BitLocker.

Эту информацию вы можете скопировать в файл и затем использовать для расшифровывания ключ восстановления.

Для многих из моих читателей, как и для некоторых экспертов, написавших вот это, такой способ хранения ключа восстановления оказался новостью. Почему? Не знаю.

Да. Если вы так храните ваши ключи восстановления, вам нужно позаботиться о надежности вашего пароля к учетной записи Microsoft. Я рекомендую использовать 2FA (2 factor authentication – двухэтапную аутентификацию). Но об этом я уже говорил. Но все же хранить ключи восстановления таким образом гораздо удобнее, что я вам и рекомендую.