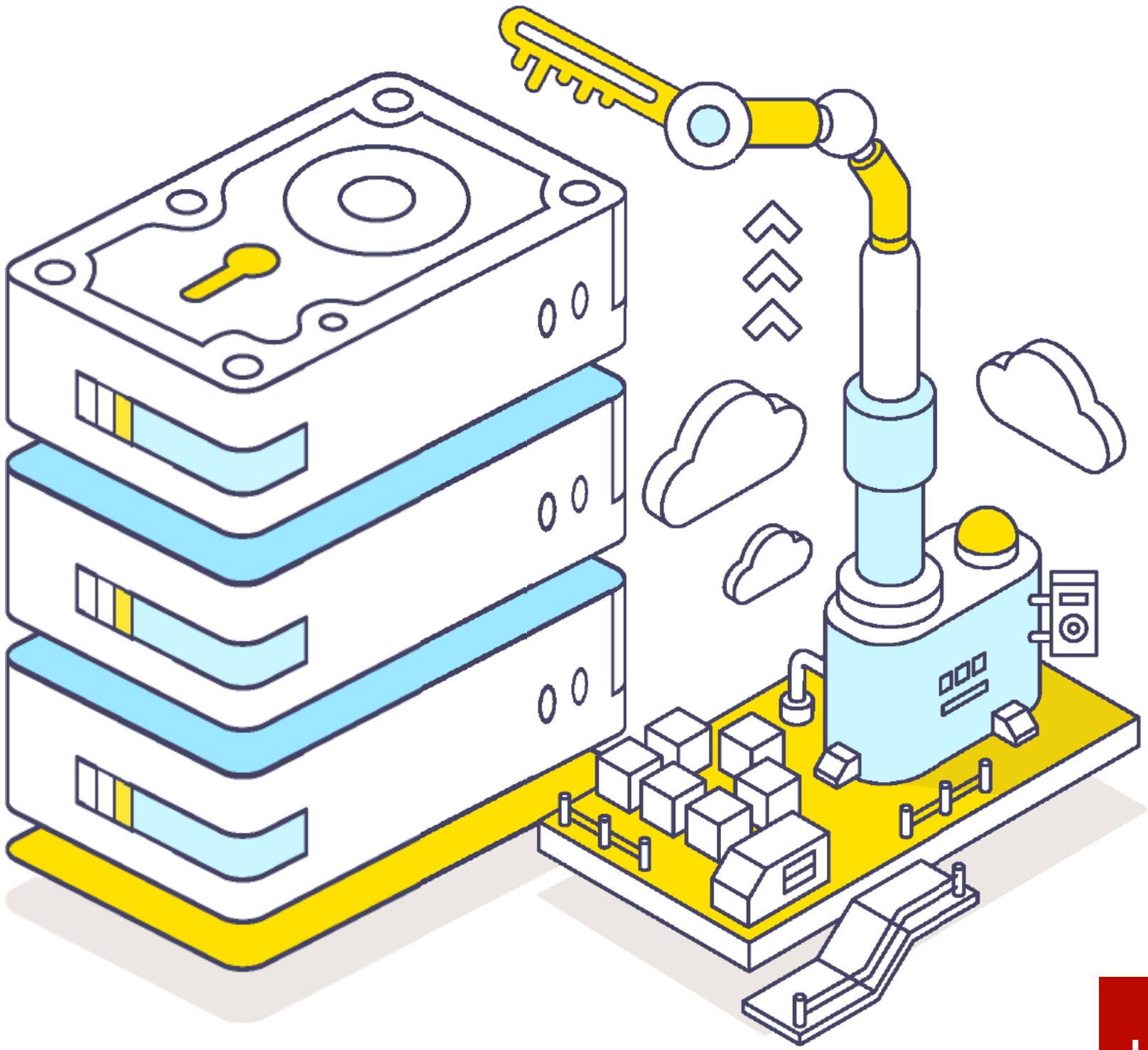
ИЗУЧАЕМ И ВСКРЫВАЕМ BITLOCKER

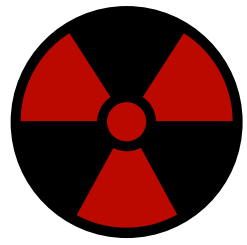
84ckf1r3
84ckf1r3@gmail.com

КАК УСТРОЕНА ЗАЩИТА ДИСКОВ WINDOWS И ЧТО НУЖНО ДЛЯ ЕЕ ВЗЛОМА



ИНТРО

Технология шифрования BitLocker впервые появилась десять лет назад и менялась с каждой версией Windows. Однако далеко не все изменения в ней были призваны повысить криптостойкость. В этой статье мы подробно разберем устройство разных версий BitLocker (включая предустановленные в последние сборки Windows 10) и покажем, как обойти этот встроенный механизм защиты.



WARNING

Статья написана в исследовательских целях. Вся информация в ней носит ознакомительный характер. Она адресована специалистам по безопасности и тем, кто хочет ими стать.

ОФЛАЙНОВЫЕ АТАКИ

Технология BitLocker стала ответом Microsoft на возрастающее число офлайновых атак, которые в отношении компьютеров с Windows выполнялись особенно просто. Любой человек с загрузочной флешкой может почувствовать себя хакером. Он просто выключит ближайший компьютер, а потом загрузит его снова — уже со своей ОС и портативным набором утилит для поиска паролей, конфиденциальных данных и препарирования системы.

В конце рабочего дня с крестовой отверткой и вовсе можно устроить маленький крестовый поход — открыть компы ушедших сотрудников и вытащить из них накопители. Тем же вечером в спокойной домашней обстановке содержимое извлеченных дисков можно анализировать (и даже модифицировать) тысячью и одним способом. На следующий день достаточно прийти пораньше и вернуть все на свои места.

Впрочем, необязательно вскрывать чужие компьютеры прямо на рабочем месте. Много конфиденциальных данных утекает после утилизации старых компов и замены накопителей. На практике безопасное стирание и низкоуровневое форматирование списанных дисков делают единицы. Что же может помешать юным хакерам и сборщикам цифровой падали?

Как пел Булат Окуджава: «Весь мир устроен из ограничений, чтобы от счастья не сойти с ума». Основные ограничения в Windows задаются на уровне прав доступа к объектам NTFS, которые никак не защищают от офлайновых атак. Windows просто сверяет разрешения на чтение и запись, прежде чем обрабатывает любые команды, которые обращаются к файлам или каталогам. Этот метод достаточно эффективен до тех пор, пока все пользователи работают в настроенной админом системе с ограниченными учетными записями. Однако стоит повысить права или загрузиться в другой операционке, как от такой защиты не останется и следа. Пользователь сам себя сделает админом и переназначит права доступа либо просто проигнорирует их, поставив другой драйвер файловой системы.

Есть много взаимодополняющих методов противодействия офлайновым атакам, включая физическую защиту и видеонаблюдение, но наиболее эф-

фективные из них требуют использования стойкой криптографии. Цифровые подписи загрузчиков препятствуют запуску постороннего кода, а единственный способ по-настоящему защитить сами данные на жестком диске — это шифровать их. Почему же полнодисковое шифрование так долго отсутствовало в Windows?

ОТ VISTA ДО WINDOWS 10

В Microsoft работают разные люди, и далеко не все из них кодят задней левой ногой. Увы, окончательные решения в софтверных компаниях давно принимают не программисты, а маркетологи и менеджеры. Единственное, что они действительно учитывают при разработке нового продукта, — это объемы продаж. Чем проще в софте разобраться домохозяйке, тем больше копий этого софта удастся продать.

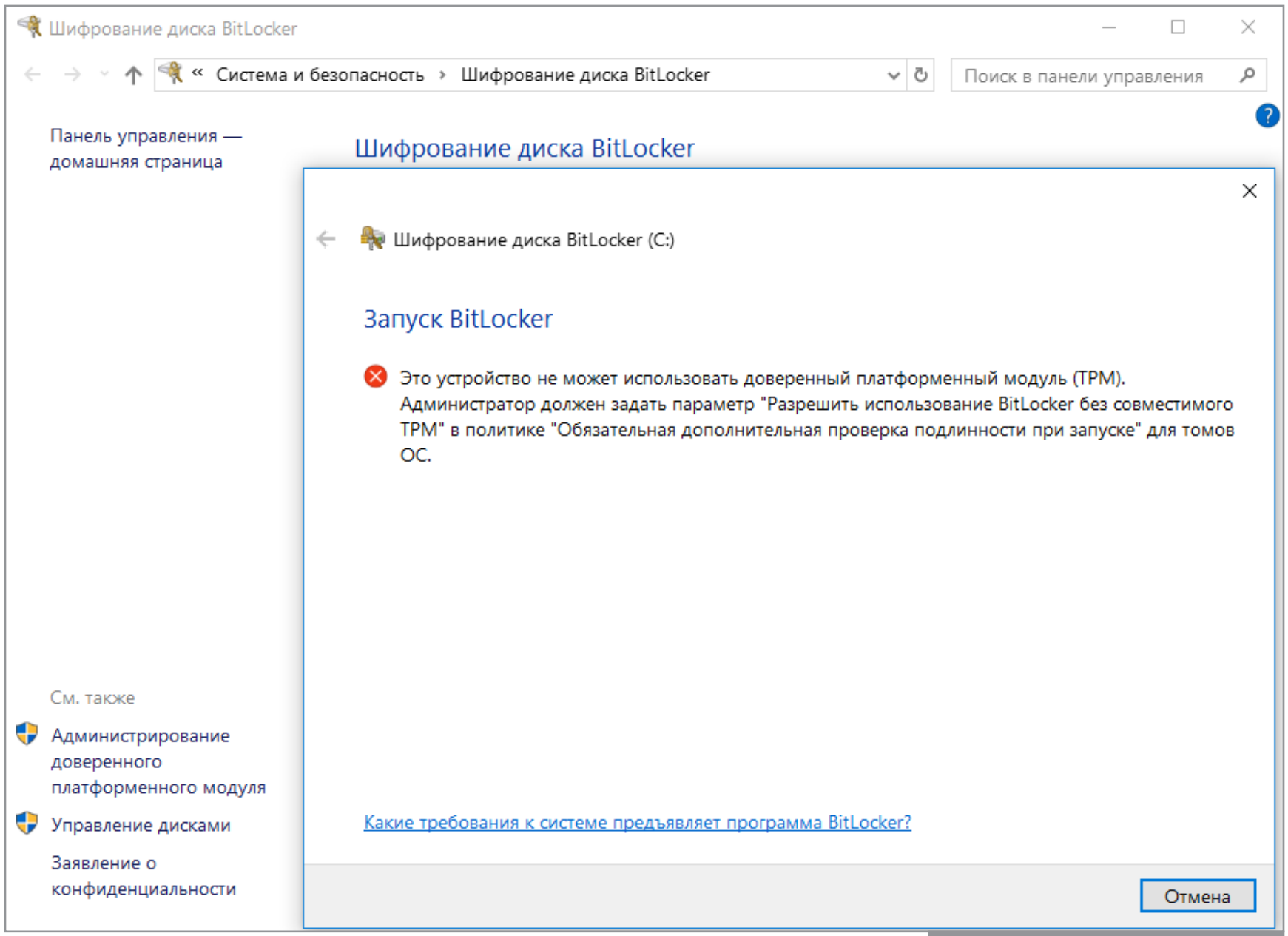
«Подумаешь, полпроцента клиентов озаботились своей безопасностью! Операционная система и так сложный продукт, а вы тут еще шифрованием пугаете целевую аудиторию. Обойдемся без него! Раньше ведь обходились!» — примерно так мог рассуждать топ-менеджмент Microsoft вплоть до того момента, когда XP стала популярной в корпоративном сегменте. Среди админов о безопасности думали уже слишком многие специалисты, чтобы сбрасывать их мнение со счетов. Поэтому в следующей версии Windows появилось долгожданное шифрование тома, но только в изданиях Enterprise и Ultimate, которые ориентированы на корпоративный рынок.

Новая технология получила название BitLocker. Пожалуй, это был единственный хороший компонент Vista. BitLocker шифровал том целиком, делая пользовательские и системные файлы недоступными для чтения в обход установленной ОС. Важные документы, фотки с котиками, реестр, SAM и SECURITY — все оказывалось нечитаемым при выполнении офлайновой атаки любого рода. В терминологии Microsoft «том» (volume) — это не обязательно диск как физическое устройство. Томом может быть виртуальный диск, логический раздел или наоборот — объединение нескольких дисков (составной или чередующийся том). Даже простую флешку можно считать подключаемым томом, для сквозного шифрования которого начиная с Windows 7 есть отдельная реализация — BitLocker To Go (подробнее — во врезке в конце статьи).

С появлением BitLocker сложнее стало загрузить постороннюю ОС, так как все загрузчики получили цифровые подписи. Однако обходной маневр по-прежнему возможен благодаря режиму совместимости. Стоит изменить в BIOS режим загрузки с UEFI на Legacy и отключить функцию Secure Boot, и старая добрая загрузочная флешка снова пригодится.

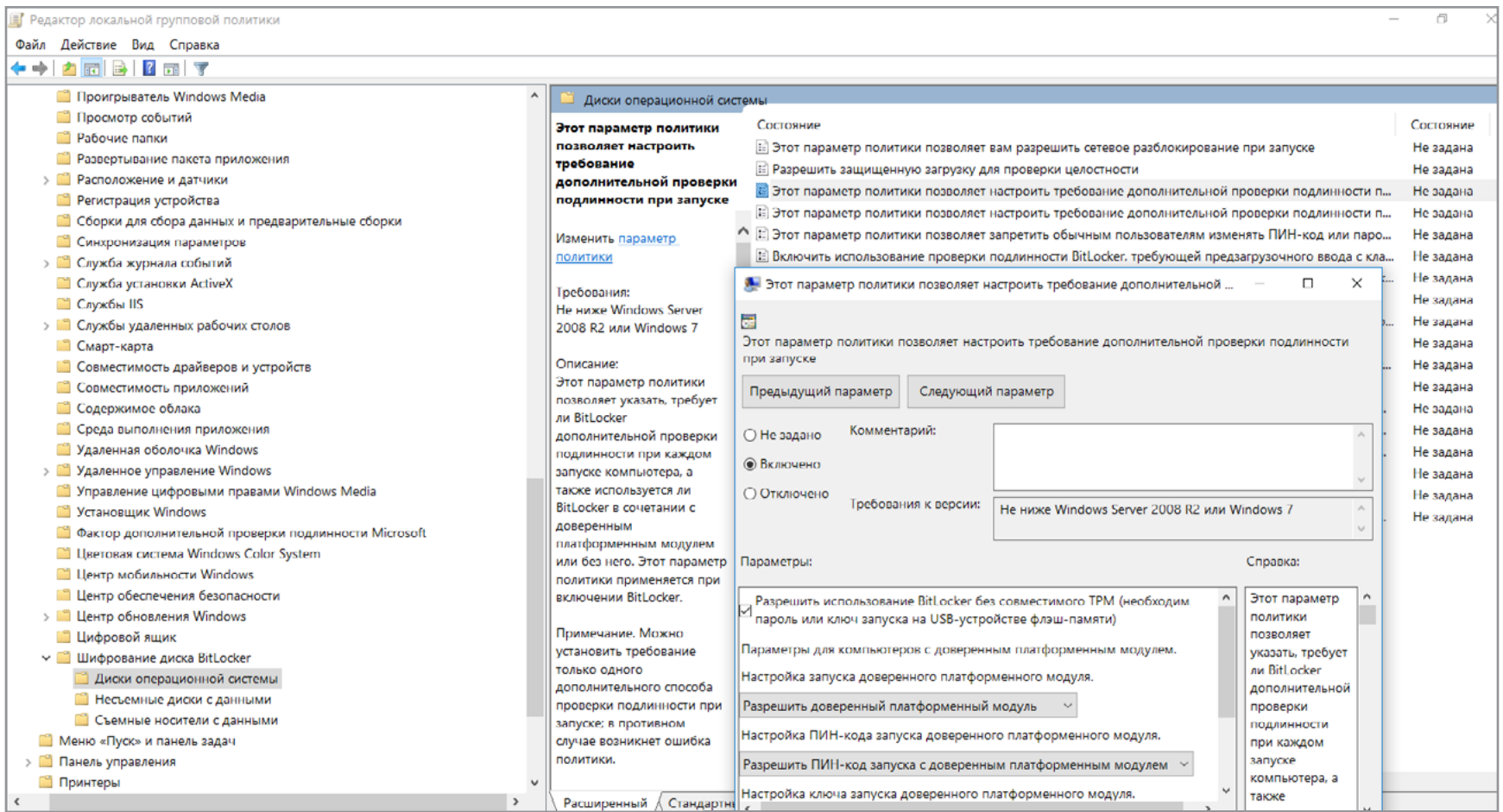
КАК ИСПОЛЬЗОВАТЬ BITLOCKER

Разберем практическую часть на примере Windows 10. В сборке 1607 BitLocker можно включить через панель управления (раздел «Система и безопасность», подраздел «Шифрование диска BitLocker»).



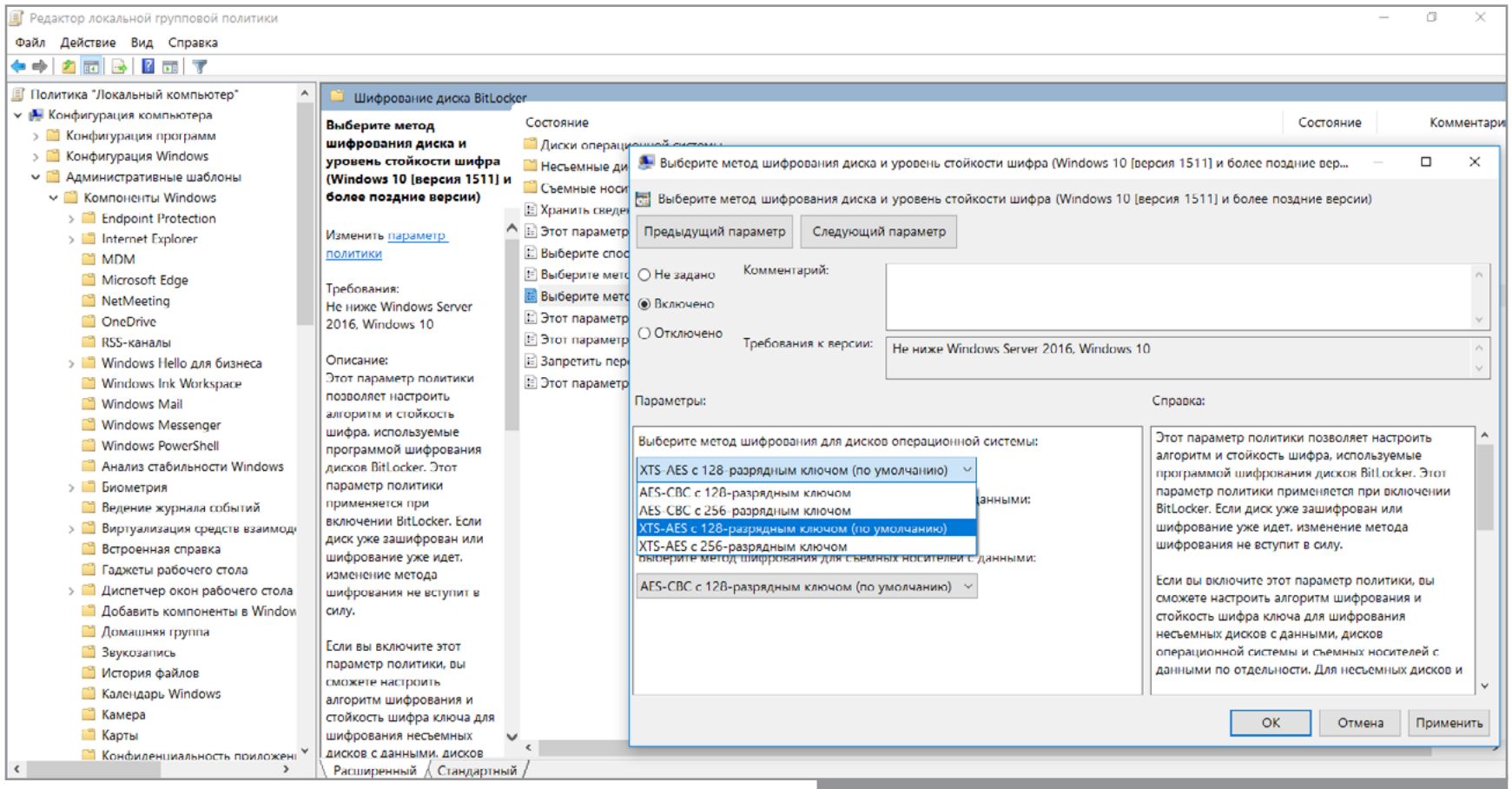
Включение BitLocker

Однако если на материнской плате отсутствует криптопроцессор TPM версии 1.2 или новее, то просто так BitLocker использовать не удастся. Чтобы его активировать, потребуется зайти в редактор локальной групповой политики (gpedit.msc) и раскрыть ветку «Конфигурация компьютера → Административные шаблоны → Компоненты Windows → Шифрование диска BitLocker → Диски операционной системы» до настройки «Этот параметр политики позволяет настроить требование дополнительной проверки подлинности при запуске». В нем необходимо найти настройку «Разрешить использование BitLocker без совместимого TPM...» и включить ее.



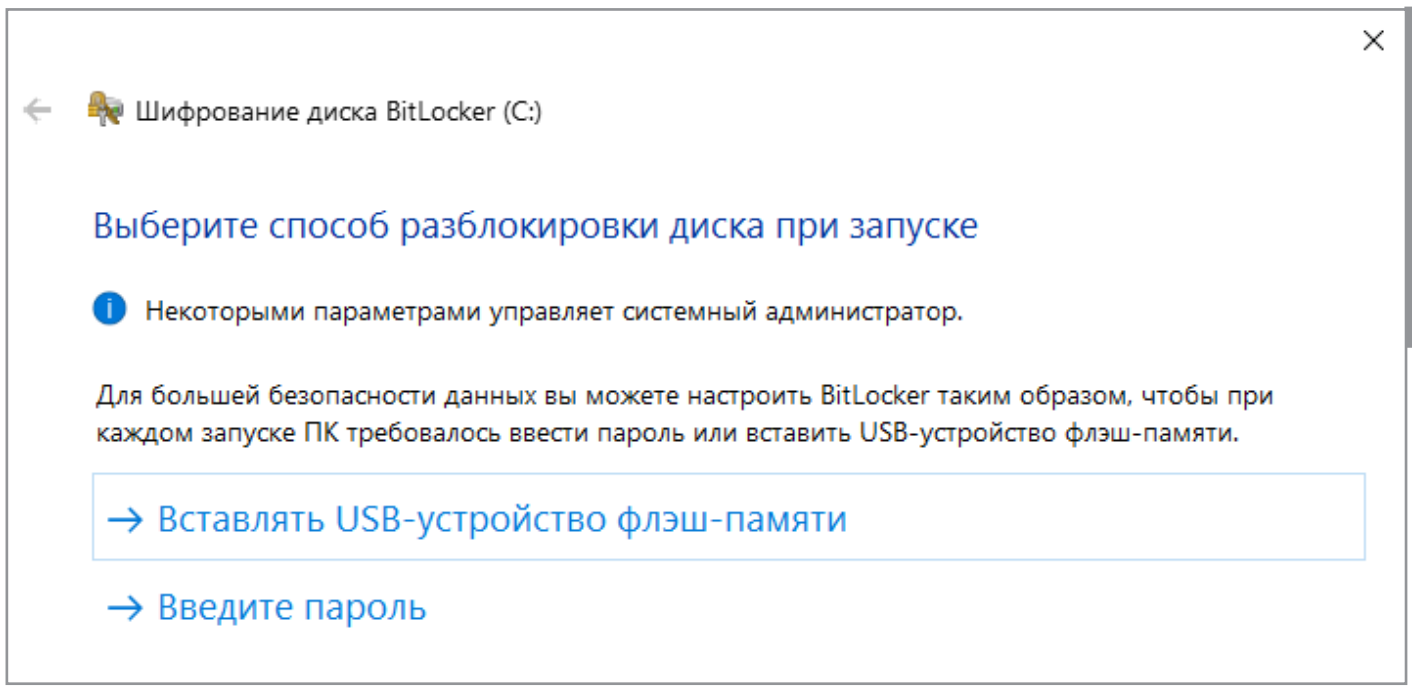
Настройка использования BitLocker без TPM

В соседних секциях локальных политик можно задать дополнительные настрой-ки BitLocker, в том числе длину ключа и режим шифрования по стандарту AES.



Дополнительные настройки BitLocker

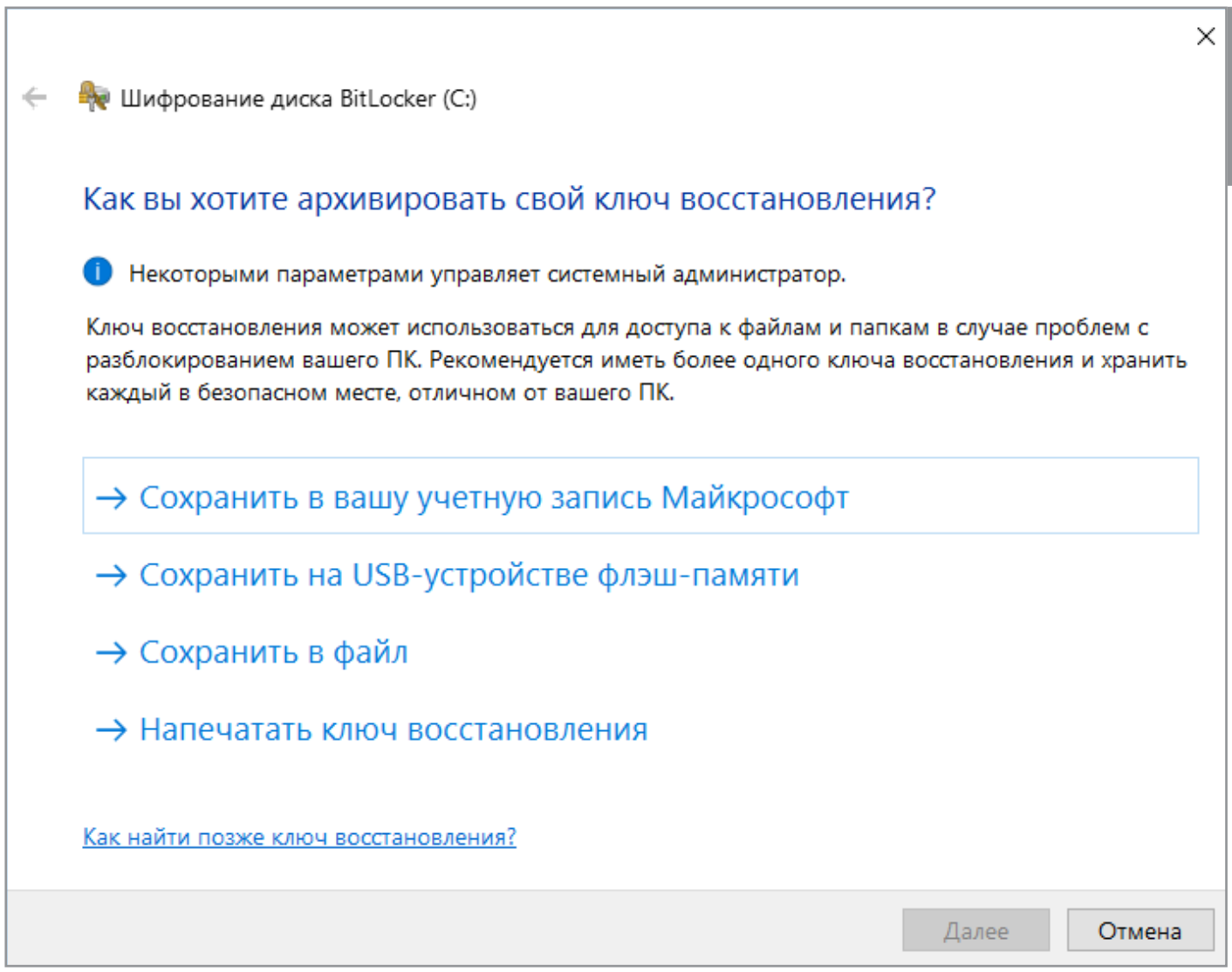
После применения новых политик возвращаемся в панель управления и следуем указаниям мастера настройки шифрования. В качестве дополнительной защиты можно выбрать ввод пароля или подключение определенной USB-флешки.



Настраиваем разблокировку компьютера при включении

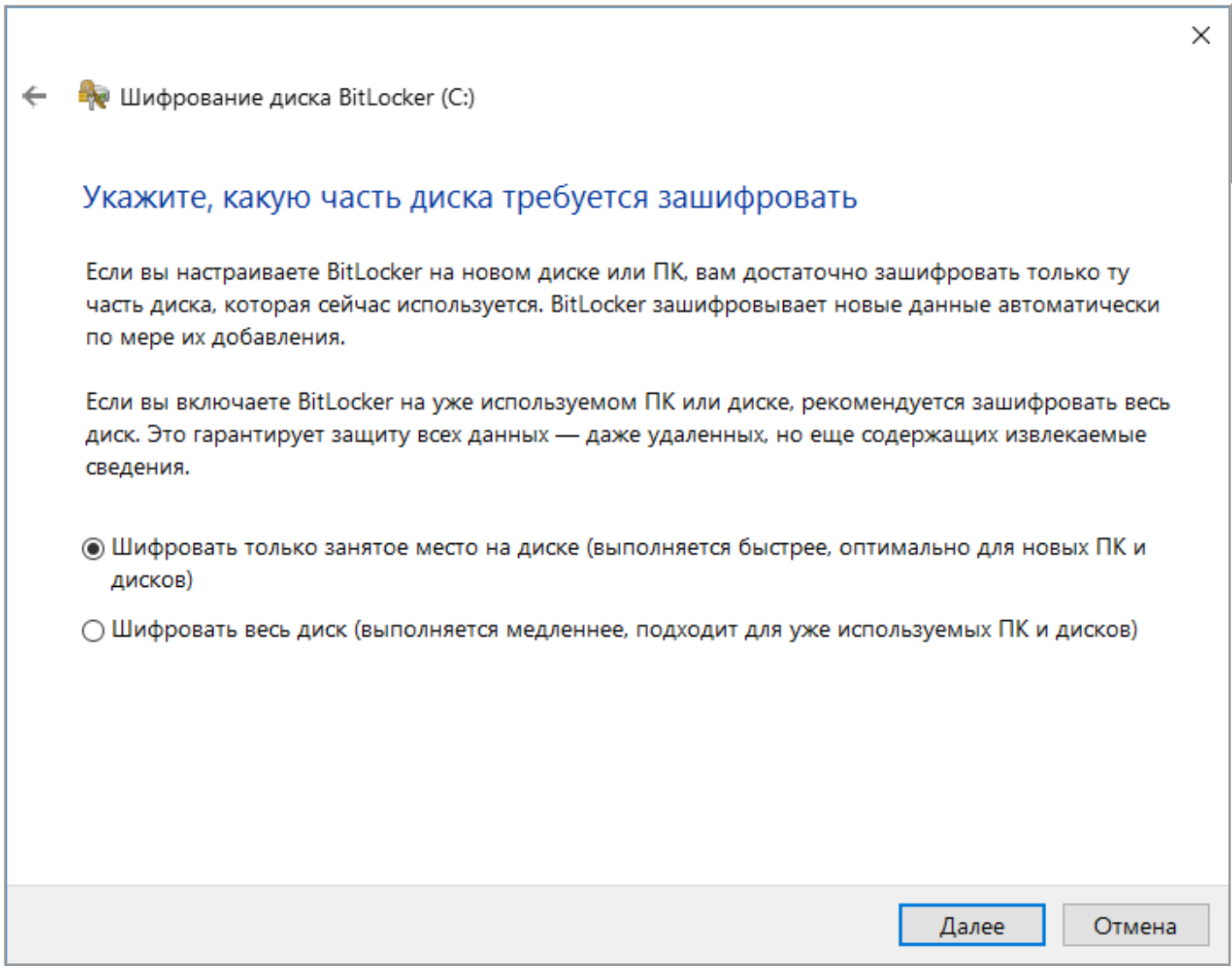
На следующем этапе нам предложат сохранить копию ключа на случай восстановления.

По умолчанию предлагается отправить ее на серверы Microsoft, записать в файл или даже напечатать.



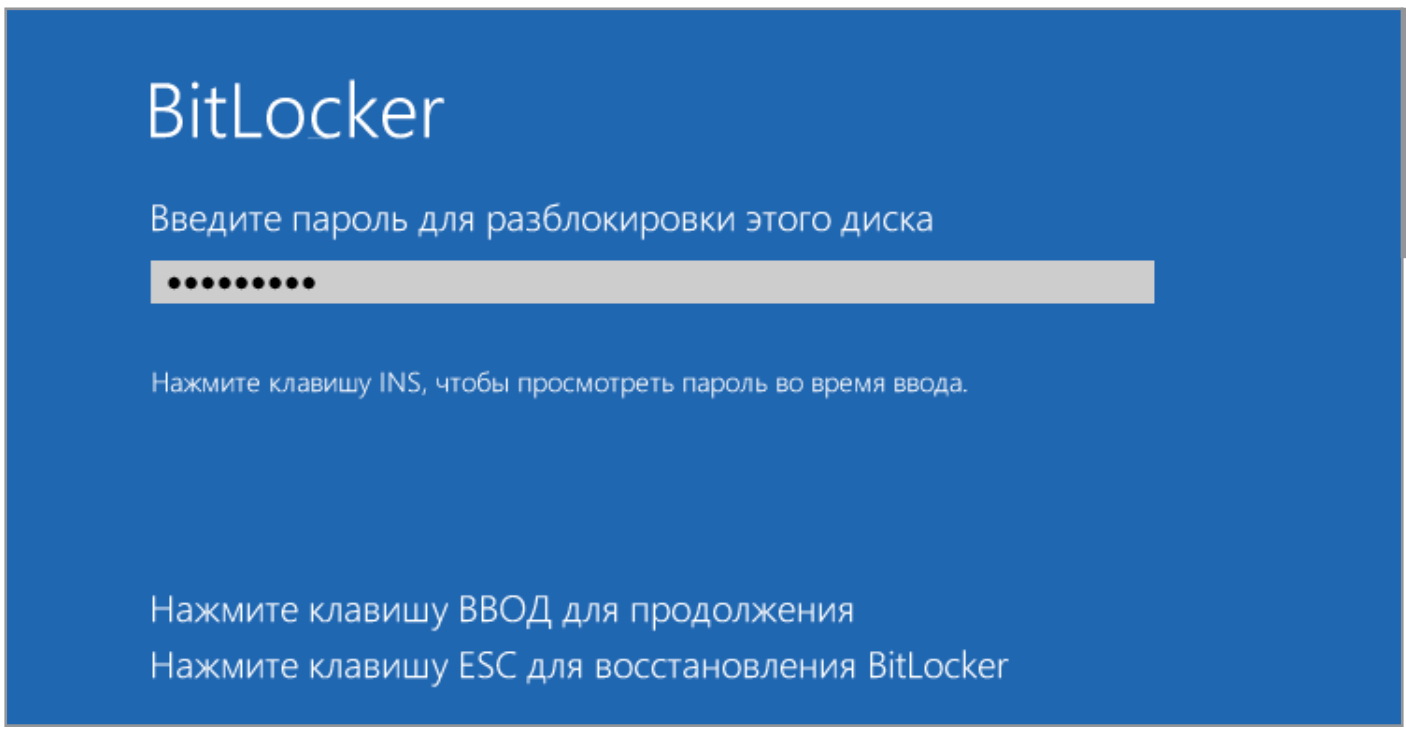
Сохранение ключа восстановления

Хотя BitLocker и считается технологией полнодискового шифрования, она позволяет выполнять частичное шифрование только занятых секторов. Это быстрее, чем шифровать все подряд, но такой способ считается менее надежным. Хотя бы потому, что при этом удаленные, но еще не перезаписанные файлы какое-то время остаются доступными для прямого чтения.



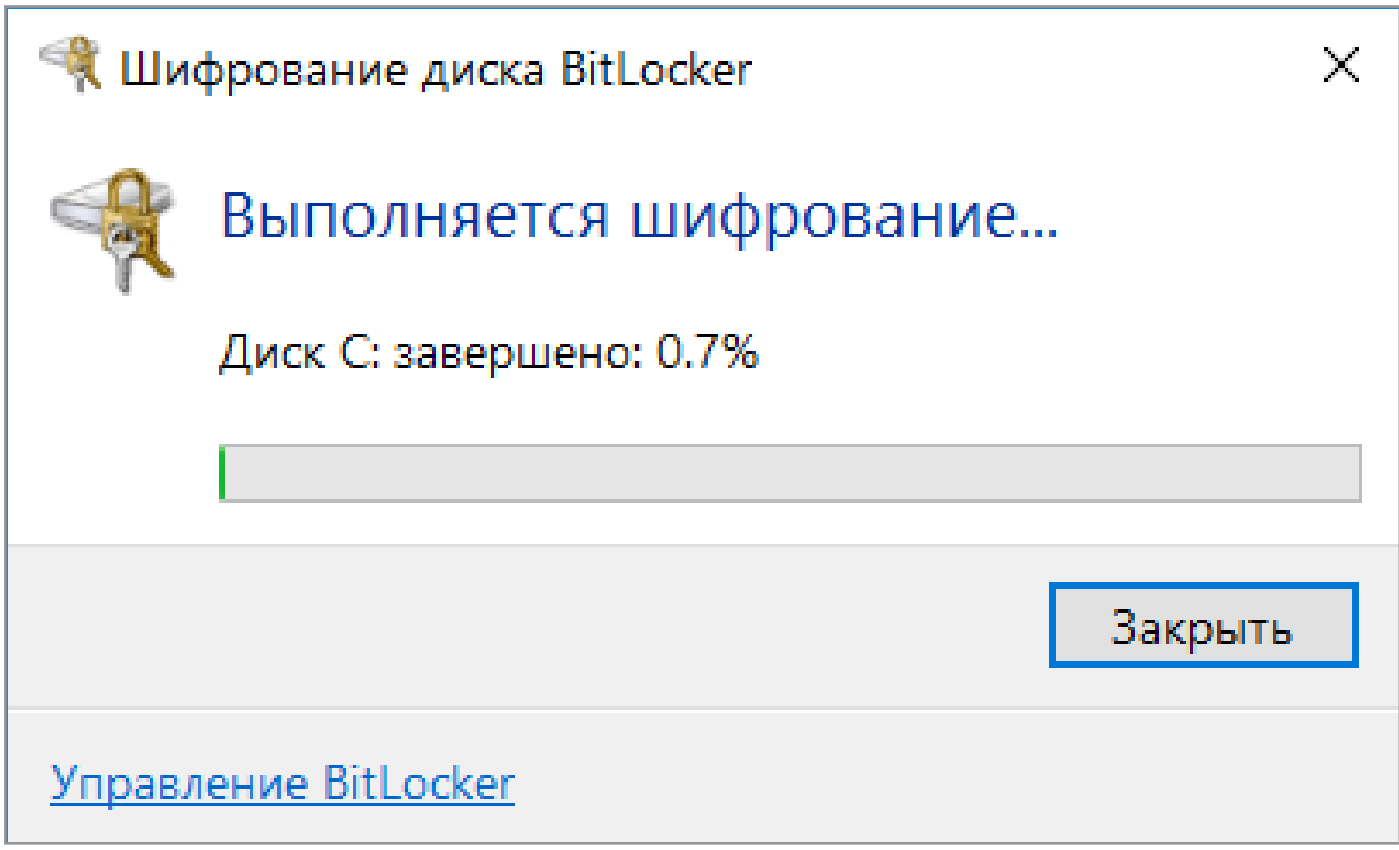
Полное и частичное шифрование

После настройки всех параметров останется выполнить перезагрузку. Windows потребует ввести пароль (или вставить флешку), а затем запустится в обычном режиме и начнет фоновый процесс шифрования тома.



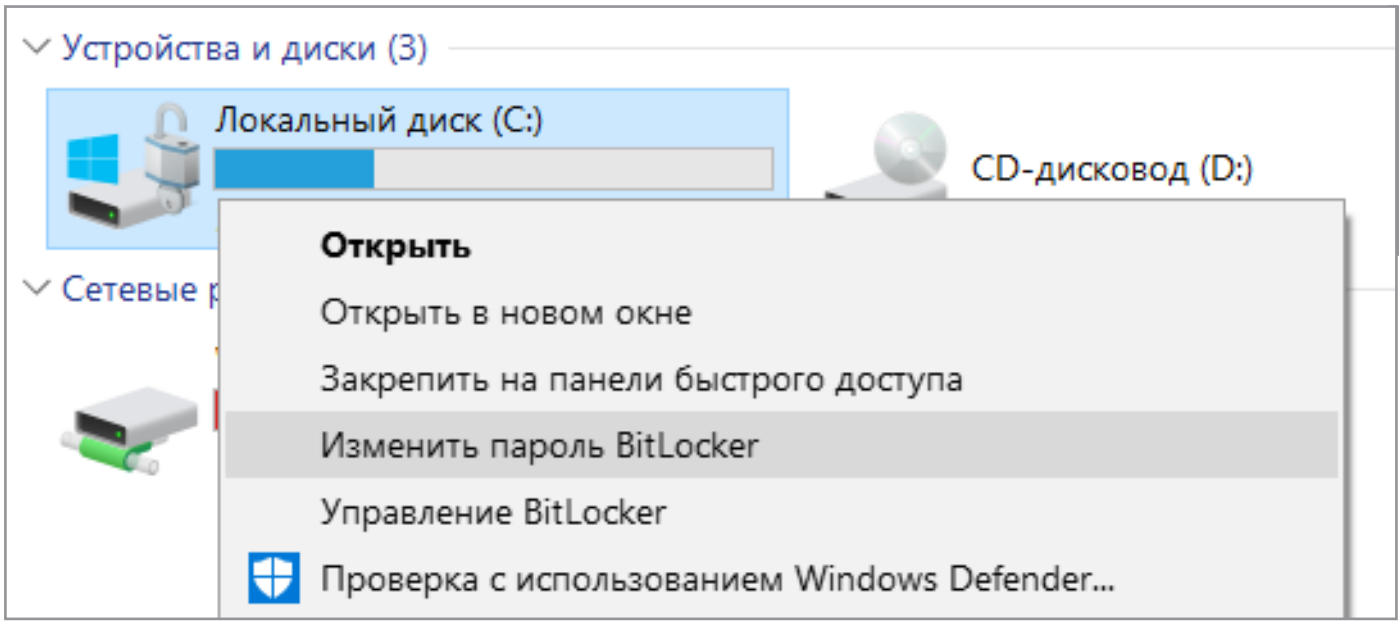
Запрос пароля перед запуском Windows

В зависимости от выбранных настроек, объема диска, частоты процессора и поддержки им отдельных команд AES, шифрование может занять от пары минут до нескольких часов.



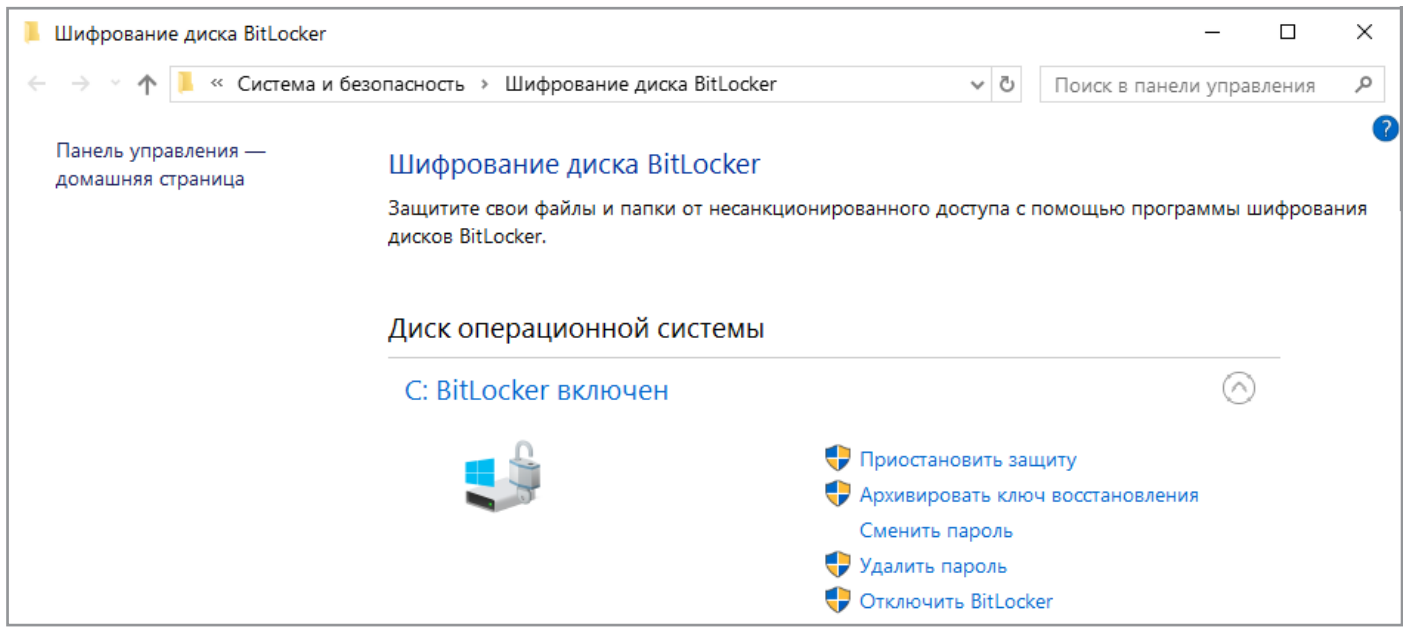
Шифрование BitLocker

После завершения этого процесса в контекстном меню «Проводника» появятся новые пункты: изменение пароля и быстрый переход к настройкам BitLocker.



Интеграция BitLocker в контекстное меню

Обрати внимание, что для всех действий, кроме смены пароля, требуются права администратора. Логика здесь простая: раз ты успешно вошел в систему, значит, знаешь пароль и имеешь право его сменить. Насколько это разумно? Скоро выясним!



BitLocker в панели управления

КАК УСТРОЕН BITLOCKER

О надежности BitLocker не следует судить по репутации AES. Популярный стандарт шифрования может и не иметь откровенно слабых мест, а вот его реализации в конкретных криптографических продуктах ими часто изобилуют. Полный код технологии BitLocker компания Microsoft не раскрывает. Известно лишь, что в разных версиях Windows она базировалась на разных схемах, а изменения никак не комментировались. Более того, в сборке 10586 Windows 10 он просто исчез, а спустя два билда появился вновь. Впрочем, обо всем по порядку.

Первая версия BitLocker использовала режим сцепления блоков шифртекста (CBC). Уже тогда были очевидны его недостатки: легкость атаки по известному тексту, слабая стойкость к атакам по типу подмены и так далее. Поэтому в Microsoft сразу решили усилить защиту. Уже в Vista к схеме AES-CBC был добавлен алгоритм Elephant Diffuser, затрудняющий прямое сравнение блоков шифртекста. С ним одинаковое содержимое двух секторов давало после шифрования одним ключом совершенно разный результат, что усложняло вычисление общего паттерна. Однако сам ключ по умолчанию использовался короткий — 128 бит. Через административные политики его можно удлинить до 256 бит, но стоит ли это делать?

Для пользователей после изменения ключа внешне ничего не изменится — ни длина вводимых паролей, ни субъективная скорость выполнения операций. Как и большинство систем полнодискового шифрования, BitLocker использует несколько ключей... и ни один из них пользователи не видят. Вот принципиальная схема BitLocker.

1. При активации BitLocker с помощью генератора псевдослучайных чисел создается главная битовая последовательность. Это ключ шифрования тома — FVEK (full volume encryption key). Именно им отныне шифруется содержимое каждого сектора.
2. В свою очередь, FVEK шифруется при помощи другого ключа — VMK (volume master key) — и сохраняется в зашифрованном виде среди метаданных тома.

3. Сам VMK тоже шифруется, но уже разными способами по выбору пользователя.
4. На новых материнских платах ключ VMK по умолчанию шифруется с помощью ключа SRK (storage root key), который хранится в отдельном криптопроцессоре — доверенном модуле (TPM, trusted platform module). У пользователя нет доступа к содержимому TPM, и оно уникально для каждого компьютера.
5. Если отдельного чипа TPM на плате нет, то вместо SRK для шифрования ключа VMK используется вводимый пользователем пин-код или подключаемый по запросу USB-Flash-накопитель с предварительно записанной на нем ключевой информацией.
6. Дополнительно к TPM или флешке можно защитить ключ VMK паролем.

Такая общая схема работы BitLocker сохранялась и в последующих выпусках Windows вплоть до настоящего времени. Однако способы генерации ключей и режимы шифрования в BitLocker менялись. Так, в октябре 2014 года Microsoft по-тихому убрала дополнительный алгоритм Elephant Diffuser, оставив только схему AES-CBC с ее известными недостатками. Поначалу об этом не было сделано никаких официальных заявлений. Людям просто выдали ослабленную технологию шифрования с прежним названием под видом обновления. Туманные объяснения этого шага последовали уже после того, как упрощения в BitLocker заметили независимые исследователи.

Формально отказ от Elephant Diffuser потребовался для обеспечения соответствия Windows требованиям федеральных стандартов обработки информации США (FIPS), однако один аргумент опровергает эту версию: Vista и Windows 7, в которых использовался Elephant Diffuser, без проблем продавались в Америке.

Еще одна мнимая причина отказа от дополнительного алгоритма — это отсутствие аппаратного ускорения для Elephant Diffuser и потеря в скорости при его использовании. Однако в прежние годы, когда процессоры были медленнее, скорость шифрования почему-то устраивала. Да и тот же AES широко применялся еще до того, как появились отдельные наборы команд и специализированные чипы для его ускорения. Со временем можно было сделать аппаратное ускорение и для Elephant Diffuser или хотя бы предоставить клиентам выбор между скоростью и безопасностью.

Более реалистичной выглядит другая, неофициальная версия. «Слон» мешал сотрудникам АНБ, которым хотелось тратить меньше усилий при расшифровке очередного диска, а Microsoft охотно взаимодействует с органами власти даже в тех случаях, когда их запросы не вполне законны. Косвенно подтверждает теорию заговора и тот факт, что до Windows 8 при создании ключей шифрования в BitLocker применялся встроенный в Windows генератор псев-

дослучайных чисел. Во многих (если не во всех) выпусках Windows это был Dual_EC_DRBG — «криптографически стойкий ГПСЧ», разработанный Агентством национальной безопасности США и содержащий ряд изначально заложенных в него уязвимостей.

Разумеется, тайное ослабление встроенного шифрования вызвало мощную волну критики. Под ее давлением Microsoft вновь переписала BitLocker, заменив в новых выпусках Windows ГПСЧ на CTR_DRBG. Дополнительно в Windows 10 (начиная со сборки 1511) схемой шифрования по умолчанию стала AES-XTS, иммунная к манипуляциям с блоками шифртекста. В последних сборках «десятки» были устранены и другие известные недочеты BitLocker, но главная проблема по-прежнему осталась. Она настолько абсурдна, что делает бессмысленными остальные нововведения. Речь идет о принципах управления ключами.

Лос-аламосский принцип

Задачу дешифрования дисков BitLocker упрощает еще и то, что в Microsoft активно продвигают альтернативный метод восстановления доступа к данным через Data Recovery Agent. Смысл «Агента» в том, что он шифрует ключи шифрования всех накопителей в пределах сети предприятия единым ключом доступа. Заполучив его, можно расшифровать любой ключ, а значит, и любой диск, используемый в той же компании. Удобно? Да, особенно для взлома.
Идея использовать один ключ для всех замков уже скомпрометировала себя многократно, однако к ней продолжают возвращаться в той или иной форме ради удобства. Вот как записал Ральф Лейтон воспоминания Ричарда Фейнмана об одном характерном эпизоде его работы над проектом «Манхэттен» в Лос-Аламосской лаборатории: «...я открыл три сейфа — и все три одной комбинацией. <...> Я уделал всех их: открыл сейфы со всеми секретами атомной бомбы — технологией получения плутония, описанием процесса очистки, сведениями о том, сколько нужно материала, как работает бомба, как получаются нейтроны, как устроена бомба, каковы ее размеры, — словом, все, о чем знали в Лос-Аламосе, всю кухню!»

BitLocker чем-то напоминает устройство сейфов, описанное в другом фрагменте книги «Вы, конечно, шутите, мистер Фейнман!». Самый внушительный сейф сверхсекретной лаборатории имел ту же самую уязвимость, что и простой шкафчик для документов. «...Это был полковник, и у него был гораздо более хитрый, двухдверный сейф с большими ручками, которые вытаскивали из рамы четыре стальных стержня толщиной три четверти дюйма. <...> Я осмо-

трел заднюю сторону одной из внушительных бронзовых дверей и обнаружил, что цифровой лимб соединен с маленьким замочком, который выглядел точно так же, как и замок моего шкафа в Лос-Аламосе. <...> Было очевидно, что система рычагов зависит от того же маленького стержня, который запирал шкафы для документов. <...>. Изображая некую деятельность, я принялся наугад крутить лимб. <...> Через две минуты — щелк! — сейф открылся. <...> Когда дверь сейфа или верхний ящик шкафа для документов открыты, очень легко найти комбинацию. Именно это я проделал, когда Вы читали мой отчет, только для того, чтобы продемонстрировать Вам опасность».

Криптоконтейнеры BitLocker сами по себе достаточно надежны. Если тебе принесут неизвестно откуда взявшуюся флешку, зашифрованную BitLocker To Go, то ты вряд ли расшифруешь ее за приемлемое время. Однако в реальном сценарии использования зашифрованных дисков и съемных носителей полно уязвимостей, которые легко использовать для обхода BitLocker.

ПОТЕНЦИАЛЬНЫЕ УЯЗВИМОСТИ

Наверняка ты заметил, что при первой активации BitLocker приходится долго ждать. Это неудивительно — процесс посекторного шифрования может занять несколько часов, ведь даже прочитать все блоки терабайтных HDD быстрее не удается. Однако отключение BitLocker происходит практически мгновенно — как же так?

Дело в том, что при отключении BitLocker не выполняет расшифровку данных. Все секторы так и останутся зашифрованными ключом FVEK. Просто доступ к этому ключу больше никак не будет ограничиваться. Все проверки отключатся, а VMK останется записанным среди метаданных в открытом виде. При каждом включении компьютера загрузчик ОС будет считывать VMK (уже без проверки TPM, запроса ключа на флешке или пароля), автоматически расшифровывать им FVEK, а затем и все файлы по мере обращения к ним. Для пользователя все будет выглядеть как полное отсутствие шифрования, но самые внимательные могут заметить незначительное снижение быстродействия дисковой подсистемы. Точнее — отсутствие прибавки в скорости после отключения шифрования.

Интересно в этой схеме и другое. Несмотря на название (технология полнодискового шифрования), часть данных при использовании BitLocker все равно остается незашифрованной. В открытом виде остаются MBR и BS (если только диск не был проинициализирован в GPT), поврежденные секторы и метаданные. Открытый загрузчик дает простор фантазии. В псевдосбойных секторах удобно прятать руткиты и прочую малварь, а метаданные содержат много все-

го интересного, в том числе копии ключей. Если BitLocker активен, то они будут зашифрованы (но слабее, чем FVEK шифрует содержимое секторов), а если деактивирован, то просто будут лежать в открытом виде. Это всё потенциальные векторы атаки. Потенциальные они потому, что, помимо них, есть куда более простые и универсальные.

Ключ восстановления

Помимо FVEK, VMK и SRK, в BitLocker используется еще один тип ключей, создаваемый «на всякий случай». Это ключи восстановления, с которыми связан еще один популярный вектор атаки. Пользователи боятся забыть свой пароль и потерять доступ к системе, а Windows сама рекомендует им сделать аварийный вход. Для этого мастер шифрования BitLocker на последнем этапе предлагает создать ключ восстановления. Отказ от его создания не предусмотрен. Можно только выбрать один из вариантов экспорта ключа, каждый из которых очень уязвим.

В настройках по умолчанию ключ экспортируется как простой текстовый файл с узнаваемым именем: «Ключ восстановления BitLocker #», где вместо # пишется идентификатор компьютера (да, прямо в имени файла!). Сам ключ выглядит так.

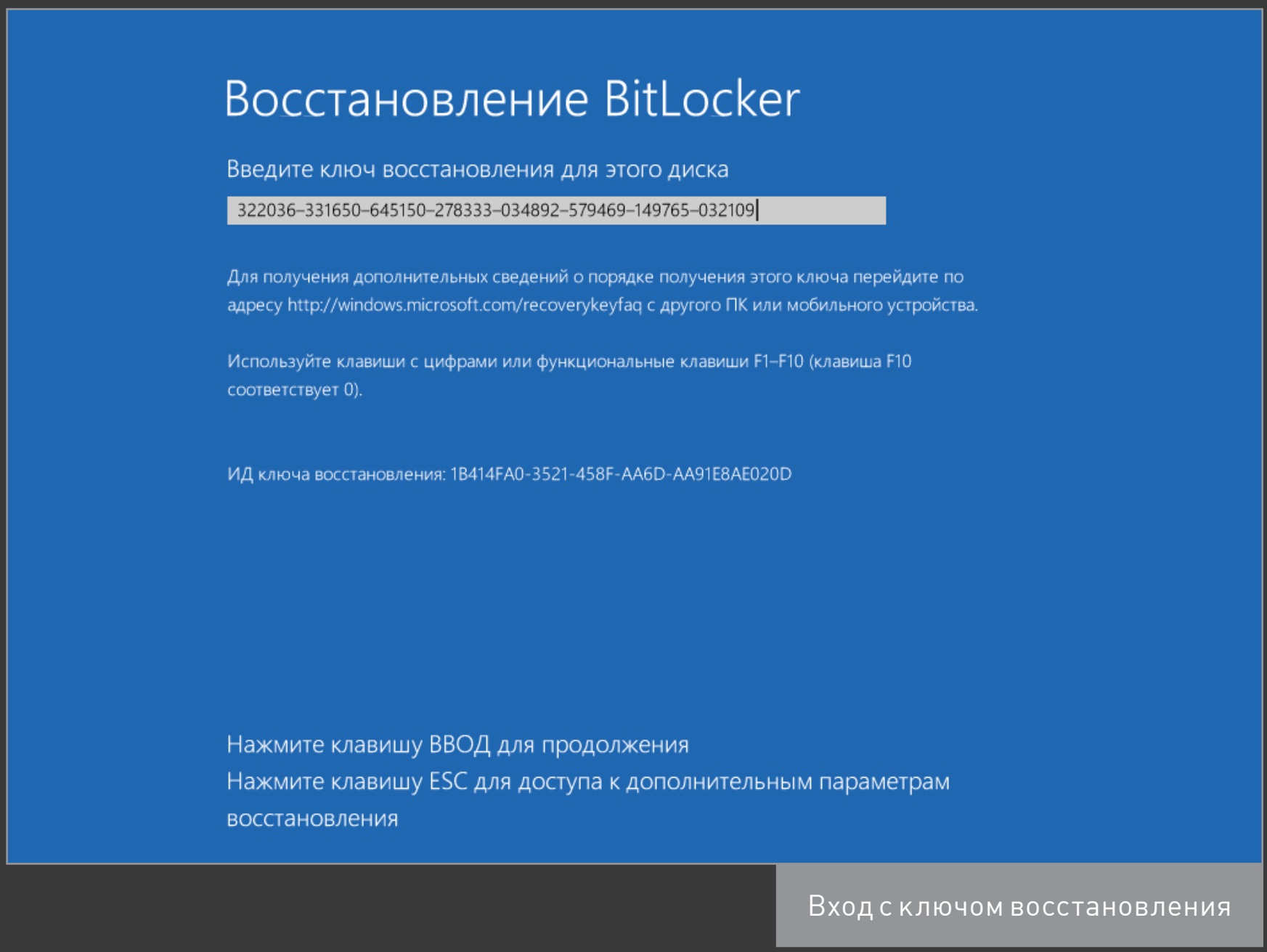
Lister - [f:\Ключ восстановления BitLocker 1B414FA0-3521-458F-AA6D-AA91E8AE020D.TXT]

File Edit Options Encoding Help

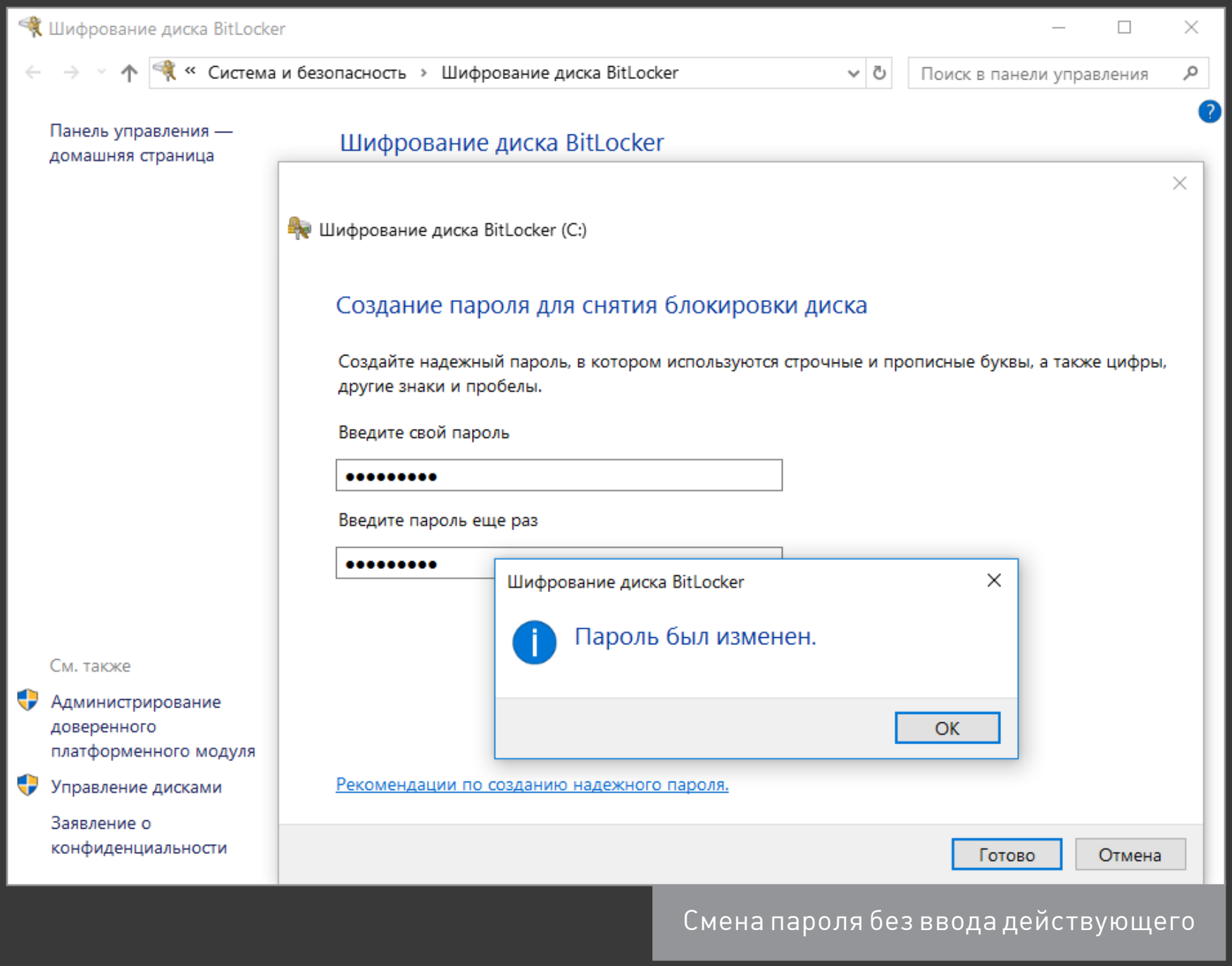
```
Ключ восстановления шифрования диска BitLocker

Чтобы проверить правильность ключа восстановления, сравните начало следующего
идентификатора со значением идентификатора, отображаемым на вашем компьютере.

Идентификатор:

        1B414FA0-3521-458F-AA6D-AA91E8AE020D

Если указанный выше идентификатор совпадает с отображаемым на компьютере,
используйте следующий ключ для разблокировки диска.

Ключ восстановления:

        322036-331650-645150-278333-034892-579469-149765-032109

Если идентификаторы не совпадают, этот ключ не подходит для разблокировки вашего
диска.
Попробуйте другой ключ восстановления или обратитесь за помощью на сайт
http://go.microsoft.com/fwlink/?LinkID=260589.
```

Аварийный вход в BitLocker

Если ты забыл (или никогда не знал) заданный в BitLocker пароль, то просто поищи файл с ключом восстановления. Наверняка он будет сохранен среди документов текущего пользователя или на его флешке. Может быть, он даже напечатан на листочке, как это рекомендует сделать Microsoft. Просто дождись, пока коллега уйдет на перерыв (как всегда, забыв заблокировать свой комп) и приступай к поискам.



Для быстрого обнаружения ключа восстановления удобно ограничить поиск по расширению (txt), дате создания (если представляешь, когда примерно могли включить BitLocker) и размеру файла (1388 байт, если файл не редактировали). Найдя ключ восстановления, скопируй его. С ним ты сможешь в любой момент обойти стандартную авторизацию в BitLocker. Для этого достаточно нажать **Esc** и ввести ключ восстановления. Ты залогинишься без проблем и даже сможешь сменить пароль в BitLocker на произвольный, не указывая старый! Это уже напоминает проделки из рубрики «Западлостроение».



Смена пароля без ввода действующего

ВСКРЫВАЕМ BITLOCKER

Реальная криптографическая система — это компромисс между удобством, скоростью и надежностью. В ней надо предусмотреть процедуры прозрачного шифрования с дешифровкой на лету, методы восстановления забытых паролей и удобной работы с ключами. Все это ослабляет любую систему, на каких бы стойких алгоритмах она ни базировалась. Поэтому необязательно искать уязвимости непосредственно в алгоритме Rijndael или в разных схемах стандарта AES. Гораздо проще их обнаружить именно в специфике конкретной реализации.

В случае Microsoft такой «специфики» хватает. Например, копии ключей BitLocker по умолчанию отправляются в SkyDrive и депонируются в Active Directory. Зачем? Ну, вдруг ты их потеряешь... или агент Смит спросит. Клиента неудобно заставлять ждать, а уж агента — тем более.

По этой причине сравнение криптостойкости AES-XTS и AES-CBC с Elephant Diffuser отходит на второй план, как и рекомендации увеличить длину ключа. Каким бы длинным он ни был, атакующий легко получит его в незашифрованном виде.

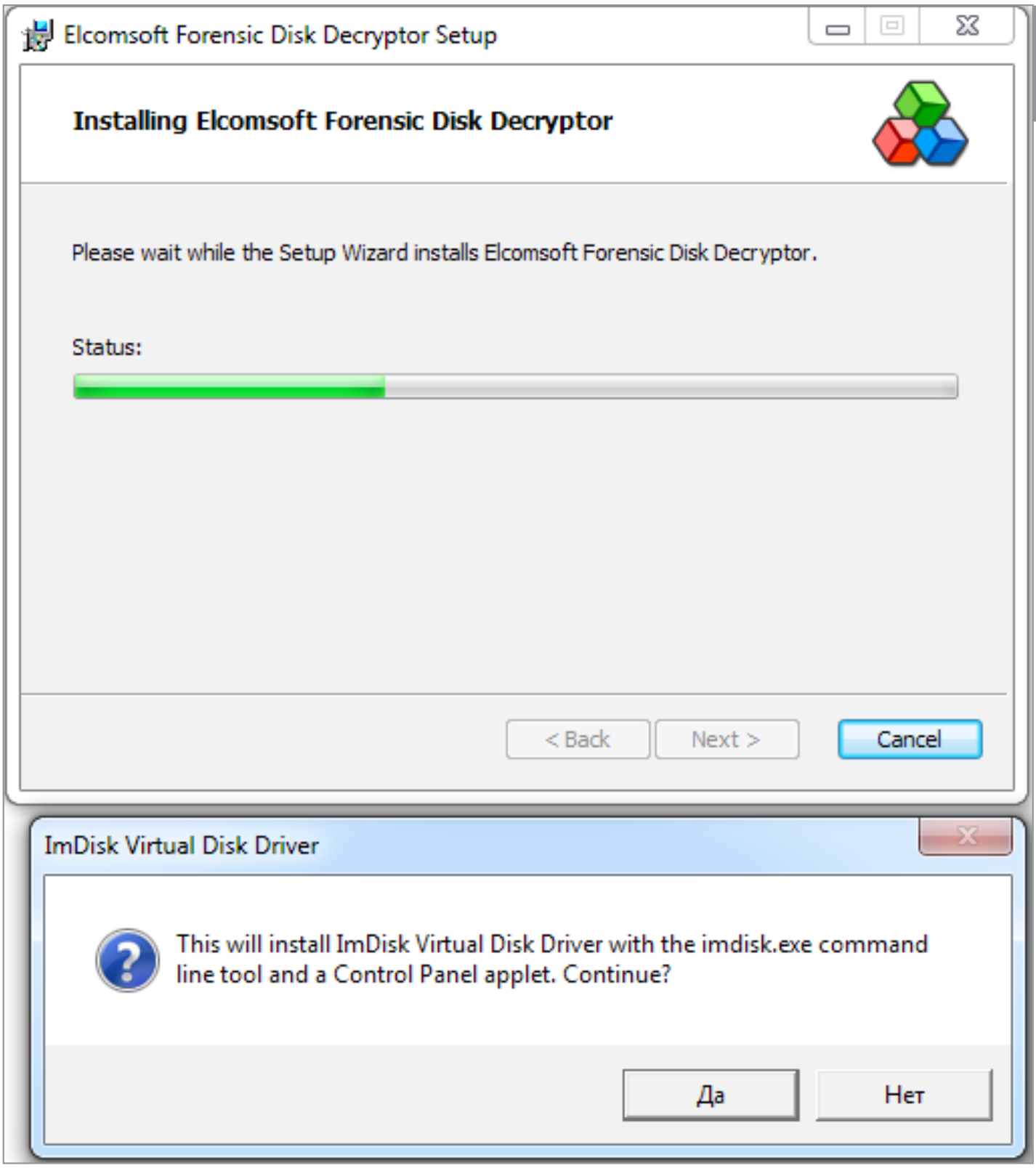
Получение депонированных ключей из учетной записи Microsoft или AD — основной способ вскрытия BitLocker. Если же пользователь не регистрировал учетку в облаке Microsoft, а его компьютер не находится в домене, то все равно найдутся способы извлечь ключи шифрования. В ходе обычной работы их открытые копии всегда сохраняются в оперативной памяти (иначе не было бы «прозрачного шифрования»). Это значит, что они доступны в ее дампе и файле гибернации.

Почему они вообще там хранятся? Как это ни смешно — для удобства. BitLocker разрабатывался для защиты только от офлайновых атак. Они всегда сопровождаются перезагрузкой и подключением диска в другой ОС, что приводит к очистке оперативной памяти. Однако в настройках по умолчанию ОС выполняет дамп оперативки при возникновении сбоя (который можно спровоцировать) и записывает все ее содержимое в файл гибернации при каждом переходе компьютера в глубокий сон. Поэтому, если в Windows с активированным BitLocker недавно выполнялся вход, есть хороший шанс получить копию ключа VMK в расшифрованном виде, а с его помощью расшифровать FVEK и затем сами данные по цепочке. Проверим?

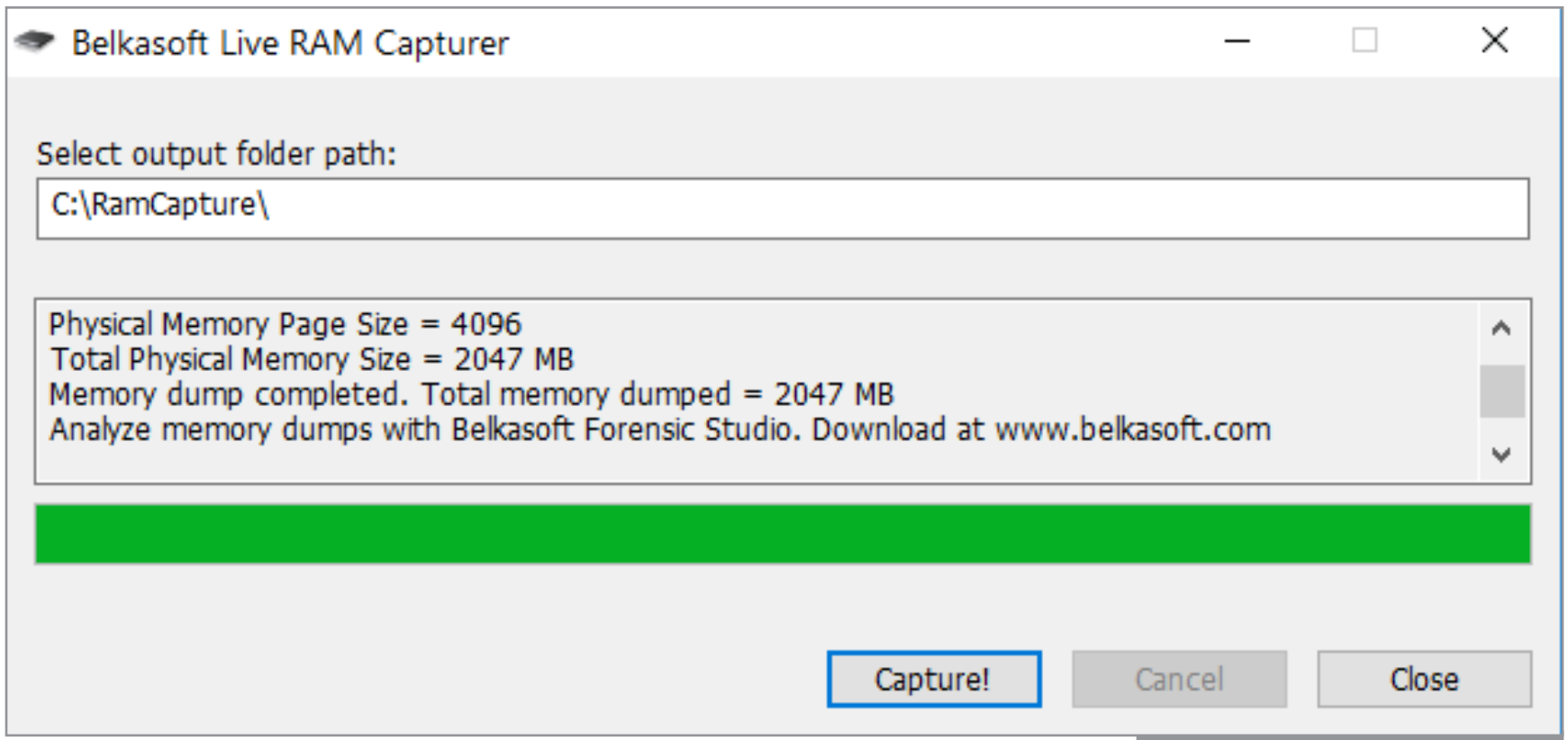
Все описанные выше методы взлома BitLocker собраны в одной программе — Forensic Disk Decryptor, разработанной в отечественной компании «Элкомсофт». Она умеет автоматически извлекать ключи шифрования и монтировать зашифрованные тома как виртуальные диски, выполняя их расшифровку на лету.

Дополнительно в EFDD реализован еще один нетривиальный способ получения ключей — атакой через порт FireWire, которую целесообразно использовать в том случае, когда нет возможности запускать свой софт на атакуемом компьютере. Саму программу EFDD мы всегда устанавливаем на свой компьютер, а на взламываемом стараемся обойтись минимально необходимыми действиями.

Установка EFDD



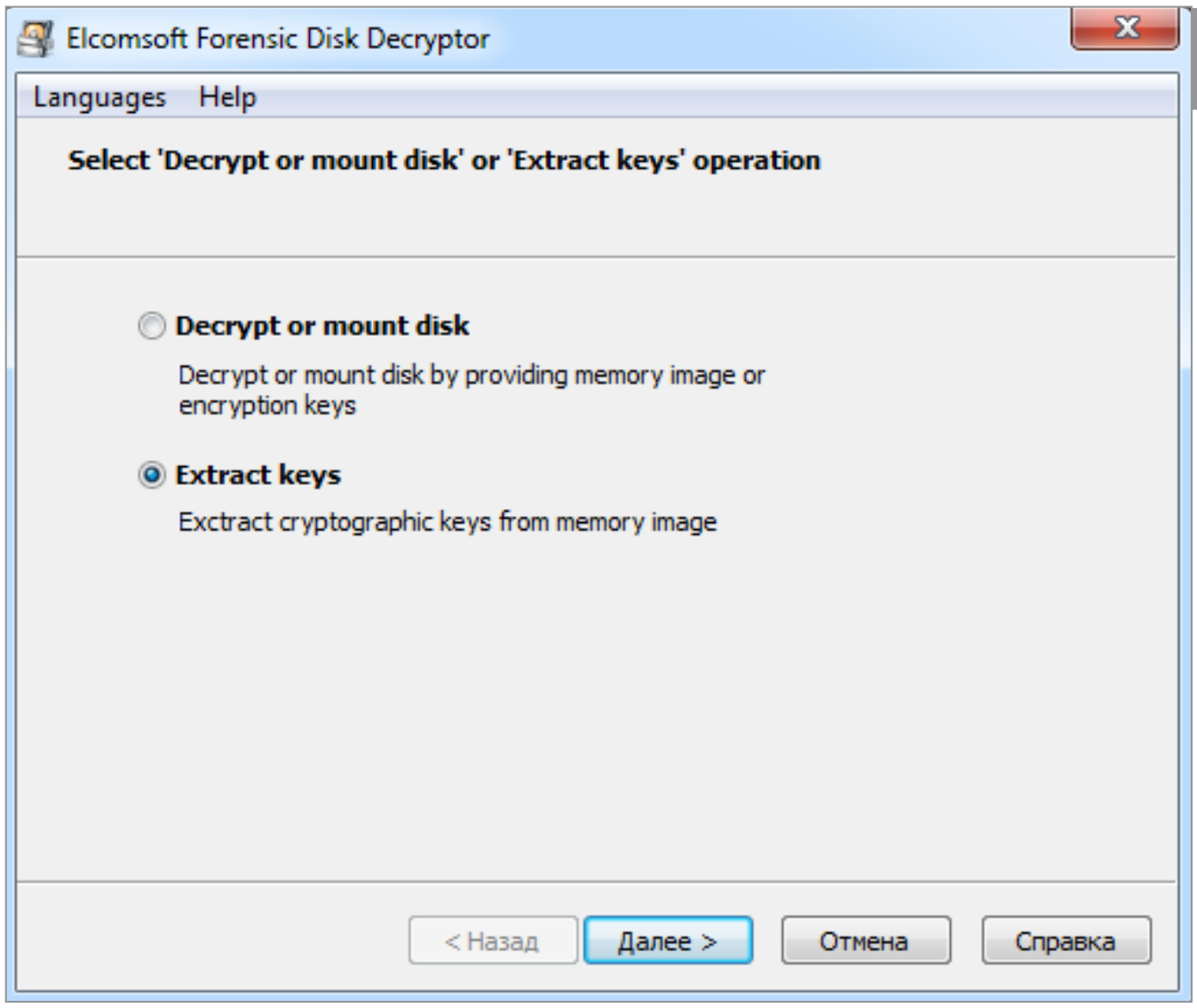
Для примера просто запустим тестовую систему с активным BitLocker и «незаметно» сделаем дамп памяти. Так мы смоделируем ситуацию, в которой коллега вышел на обед и не заблокировал свой компьютер. Запускаем RAM Capture и меньше чем через минуту получаем полный дамп в файле с расширением .mem и размером, соответствующим объему оперативки, установленной на компьютере жертвы.



Делаем дамп памяти

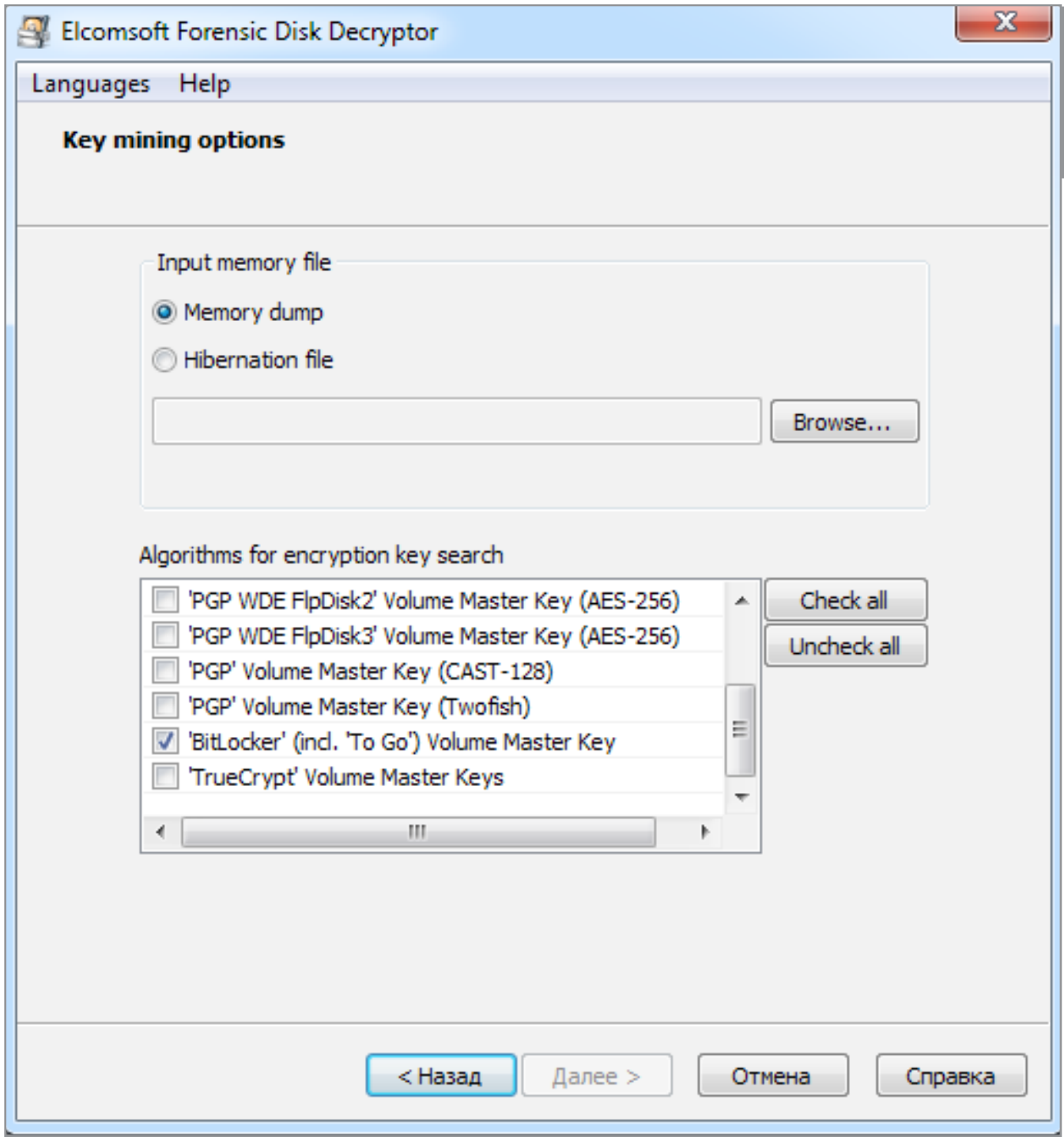
Чем делать дамп — по большому счету без разницы. Независимо от расширения это получится бинарный файл, который дальше будет автоматически проанализирован EFDD в поисках ключей.

Записываем дамп на флешку или передаем его по сети, после чего садимся за свой компьютер и запускаем EFDD.



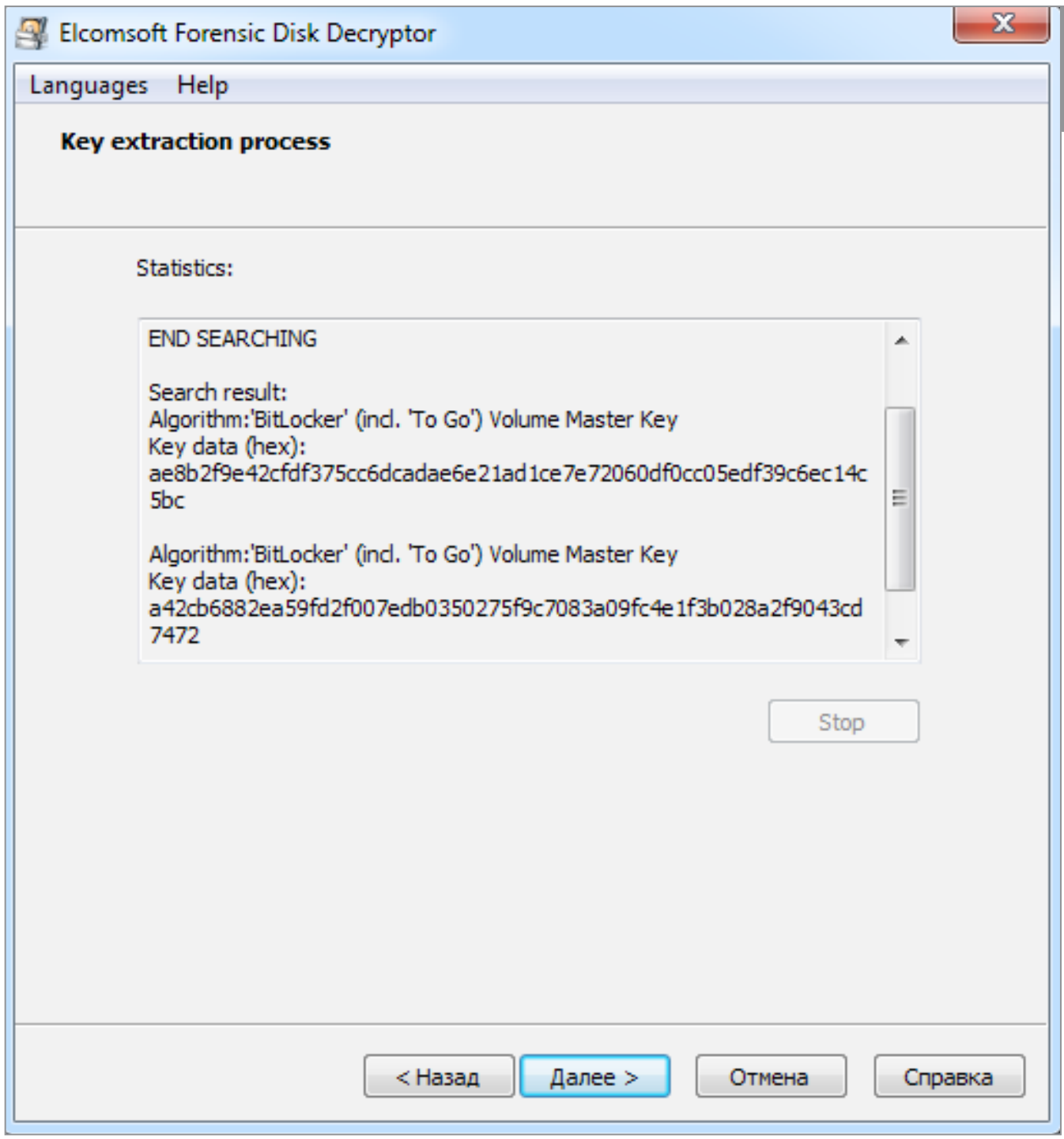
Запуск EFDD

Выбираем опцию «Извлечь ключи» и в качестве источника ключей вводим путь до файла с дампом памяти.



Указываем источник ключей

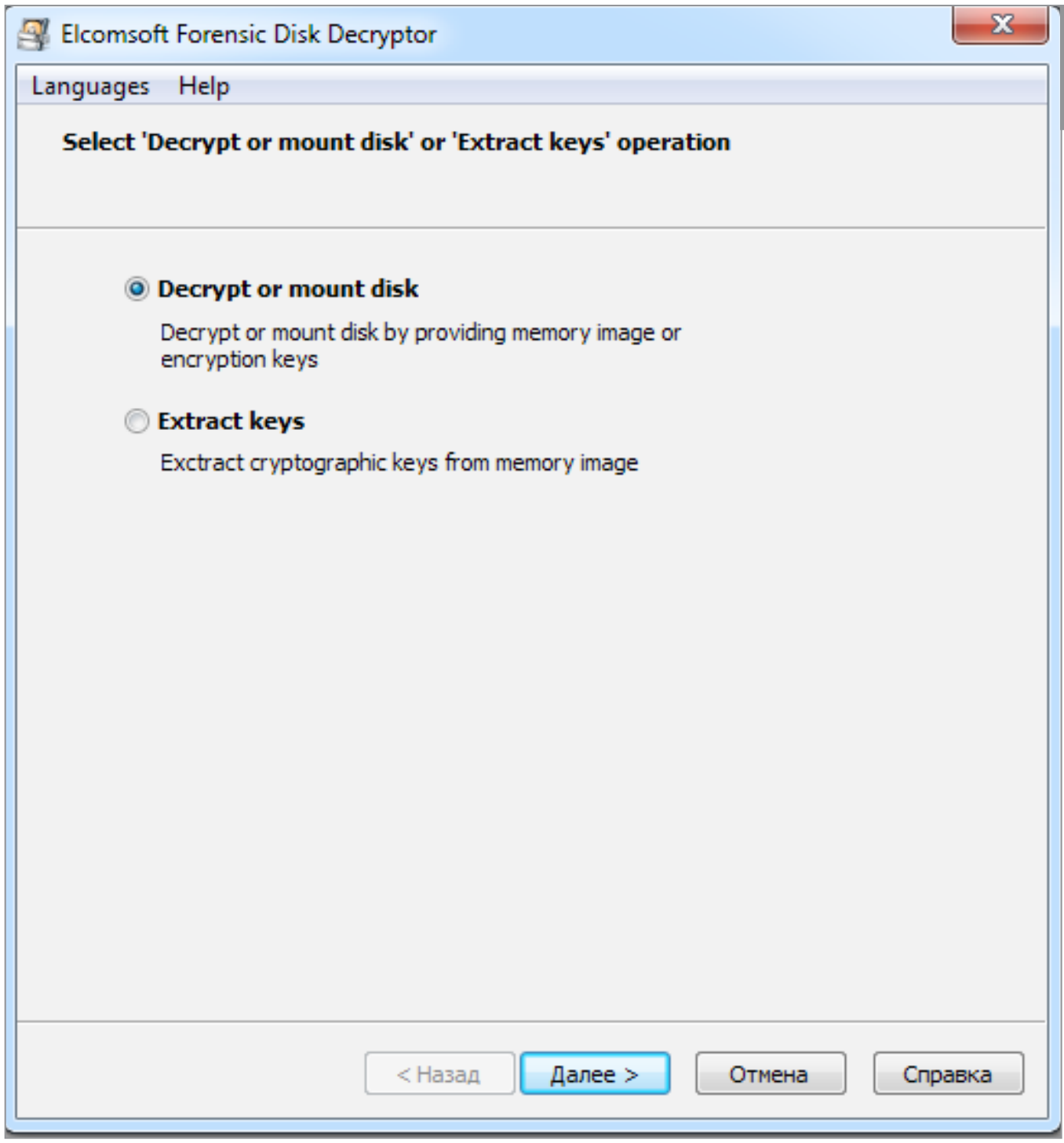
BitLocker — типичный криптоконтейнер, вроде PGP Disk или TrueCrypt. Эти контейнеры получились достаточно надежными сами по себе, но вот клиентские приложения для работы с ними под Windows мусорят ключами шифрования в оперативной памяти. Поэтому в EFDD реализован сценарий универсальной атаки. Программа мгновенно отыскивает ключи шифрования от всех трех видов популярных криптоконтейнеров. Поэтому можно оставить отмеченными все пункты — вдруг жертва тайком использует TrueCrypt или PGP!



EFDD нашла ключи

Спустя несколько секунд Elcomsoft Forensic Disk Decryptor показывает все найденные ключи в своем окне. Для удобства их можно сохранить в файл — это пригодится в дальнейшем.

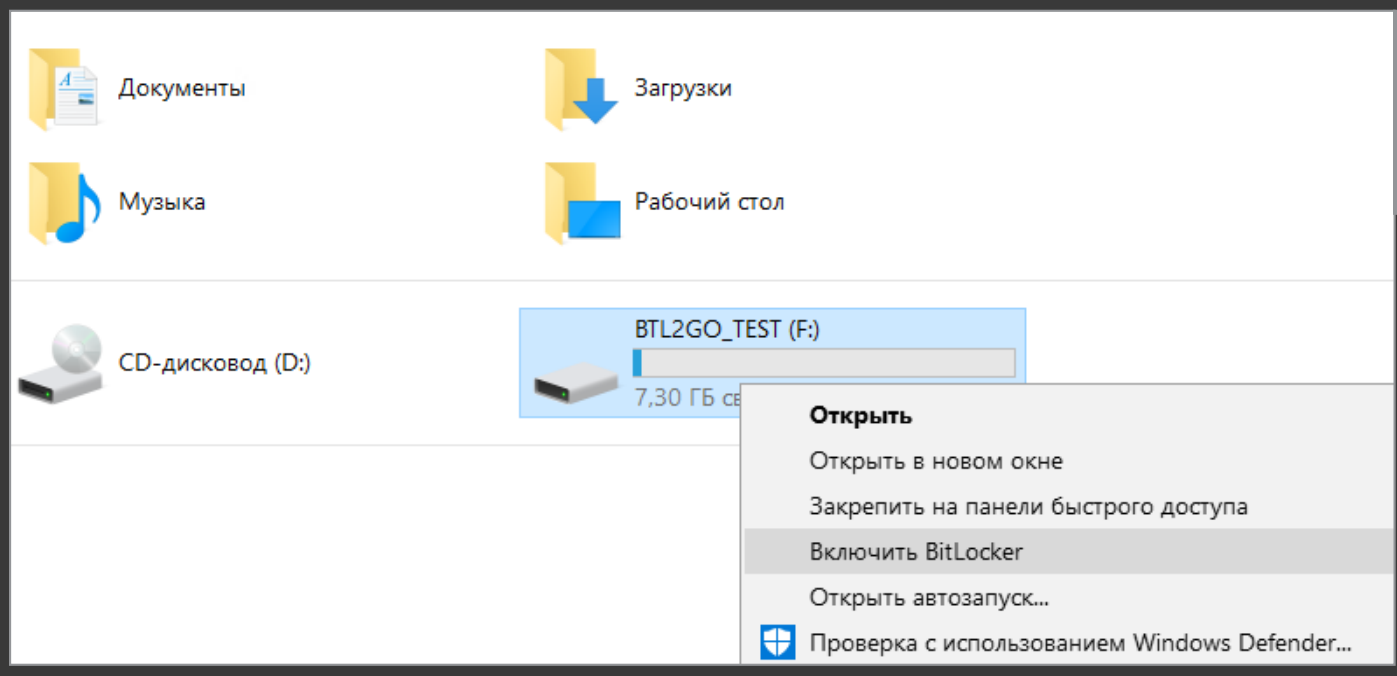
Теперь BitLocker больше не помеха! Можно провести классическую офлайновую атаку — например, вытащить жесткий диск коллеги и скопировать его содержимое. Для этого просто подключи его к своему компьютеру и запусти EFDD в режиме «расшифровать или смонтировать диск».



После указания пути до файлов с сохраненными ключами EFDD на твой выбор выполнит полную расшифровку тома либо сразу откроет его как виртуальный диск. В последнем случае файлы расшифровываются по мере обращения к ним. В любом варианте никаких изменений в оригинальный том не вносится, так что на следующий день можешь вернуть его как ни в чем не бывало. Работа с EFDD происходит бесследно и только с копиями данных, а потому остается незаметной.

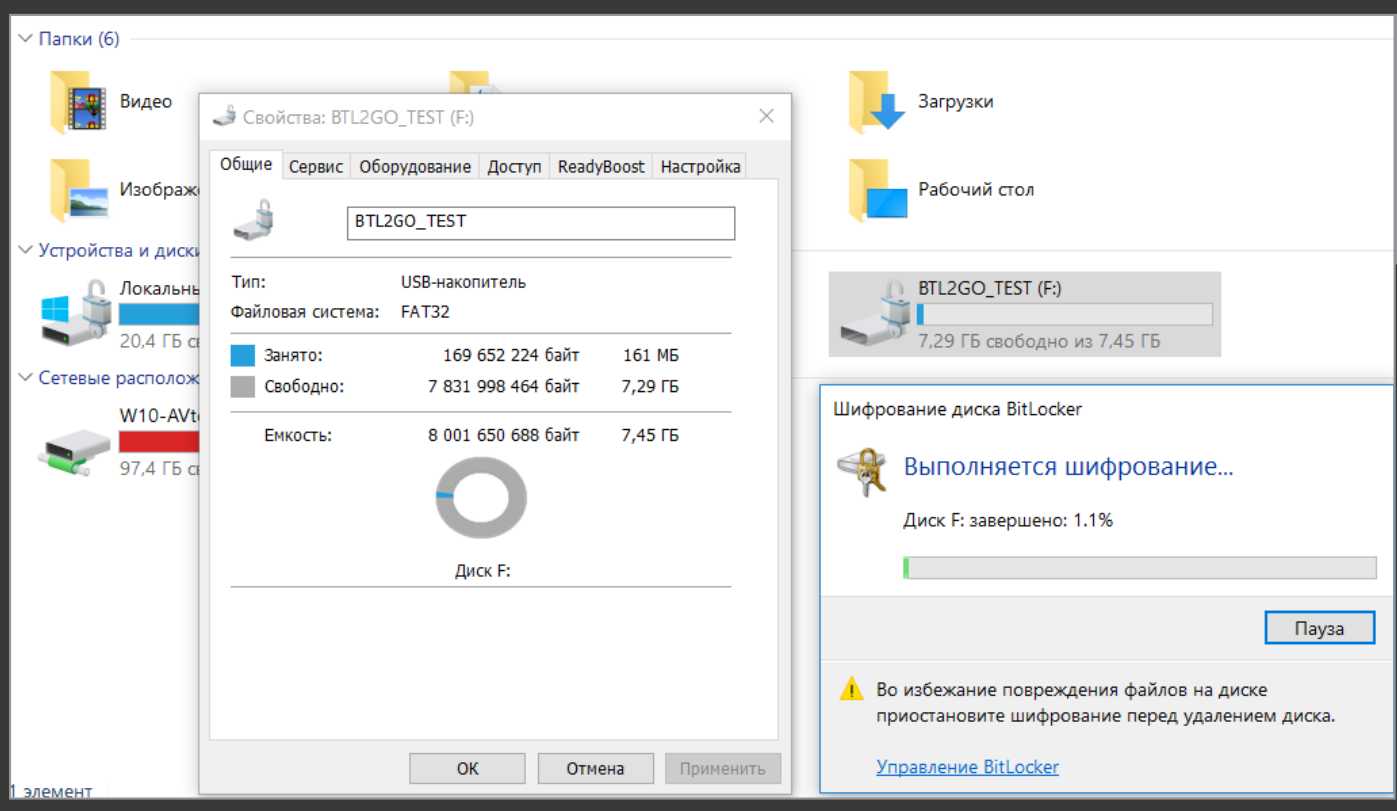
BitLocker To Go

Начиная с «семерки» в Windows появилась возможность шифровать флешки, USB-HDD и прочие внешние носители. Технология под названием BitLocker To Go шифрует съемные накопители точно так же, как и локальные диски. Шифрование включается соответствующим пунктом в контекстном меню «Проводника».



Включаем шифрование на флешке

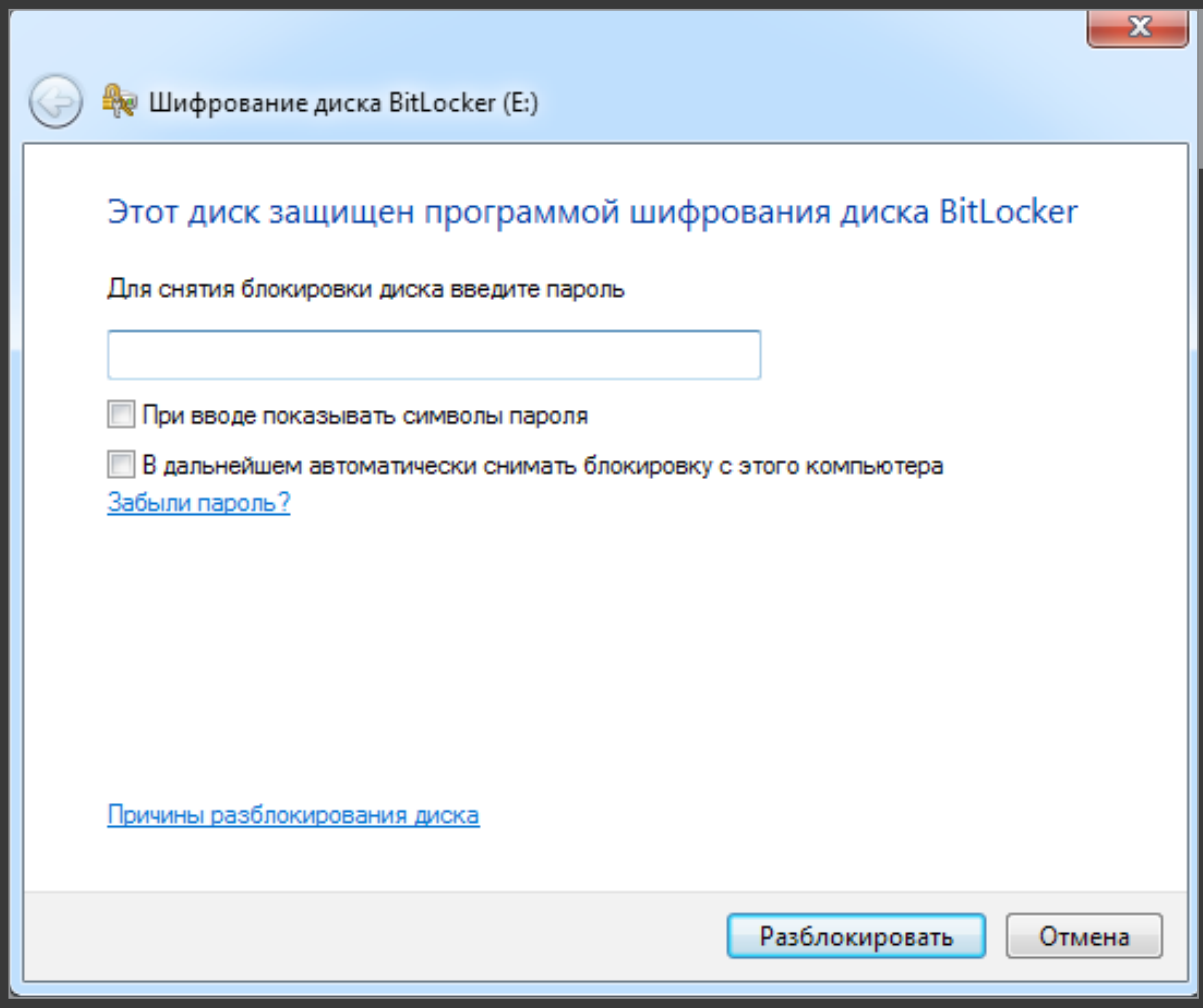
Для новых накопителей можно использовать шифрование только занятой области — все равно свободное место раздела забито нулями и скрывать там нечего. Если же накопитель уже использовался, то рекомендуется включить на нем полное шифрование. Иначе место, помеченное как свободное, останется незашифрованным. Оно может содержать в открытом виде недавно удаленные файлы, которые еще не были перезаписаны.



Процесс шифрования съемного накопителя

Даже быстрое шифрование только занятой области занимает от нескольких минут до нескольких часов. Это время зависит от объема данных, пропускной способности интерфейса, характеристик накопителя и скорости криптографических вычислений процессора. Поскольку шифрование сопровождается сжатием, свободное место на зашифрованном диске обычно немного увеличивается.

При следующем подключении зашифрованной флешки к любому компьютеру с Windows 7 и выше автоматически вызовется мастер BitLocker для разблокировки диска. В «Проводнике» же до разблокировки она будет отображаться как диск, закрытый на замок.

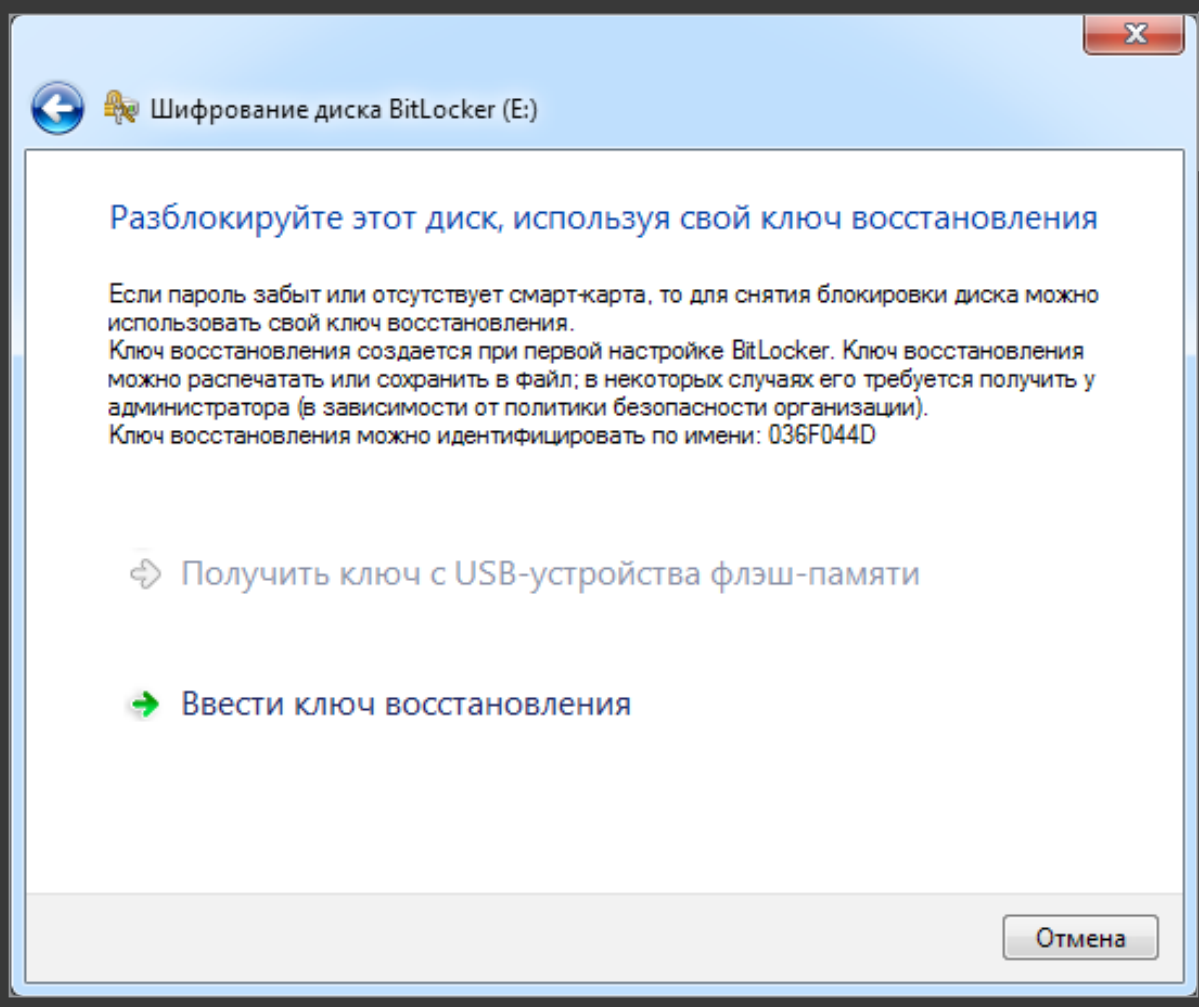


Запрос пароля BitLocker2Go

Здесь можно использовать как уже рассмотренные варианты обхода BitLocker (например, поиск ключа VMK в дампе памяти или файле гибернации), так и новые, связанные с ключами восстановления.

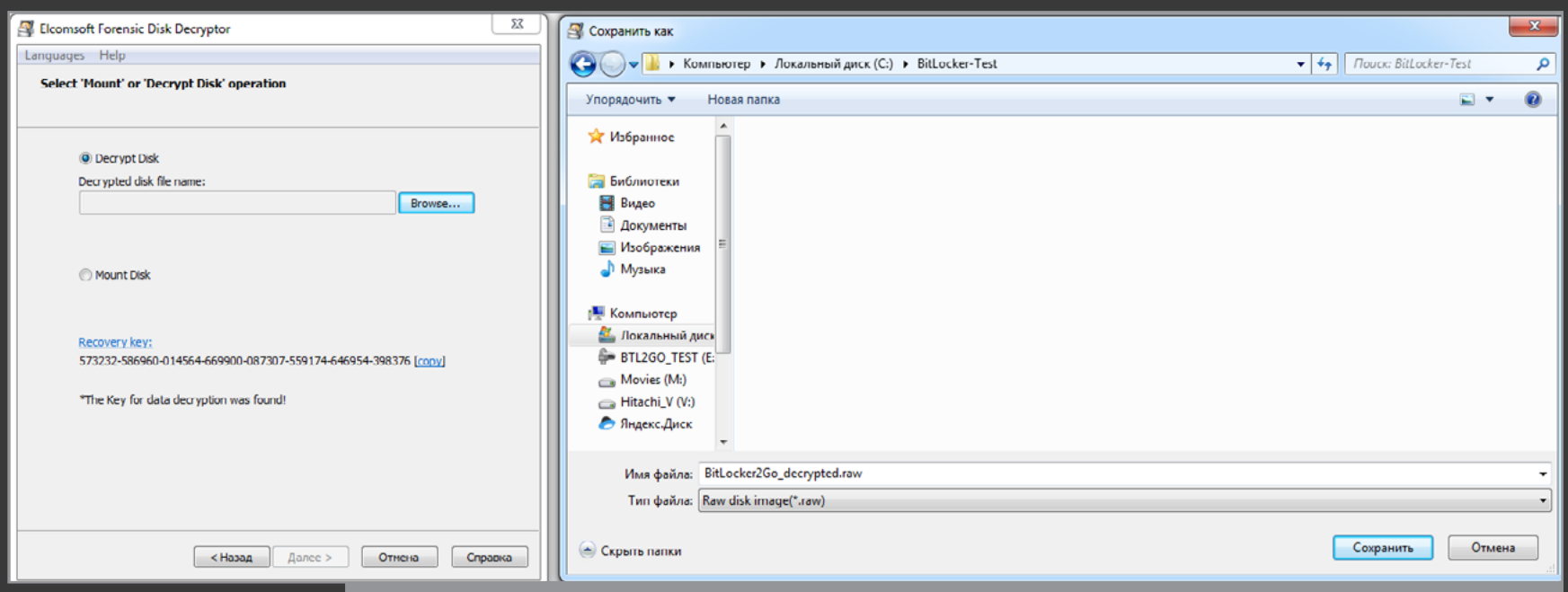
Если ты не знаешь пароль, но тебе удалось найти один из ключей (вручную или с помощью EFDD), то для доступа к зашифрованной флешке есть два основных варианта:

- использовать встроенный мастер BitLocker для непосредственной работы с флешкой;
- использовать EFDD для полной расшифровки флешки и создания ее посекторного образа.



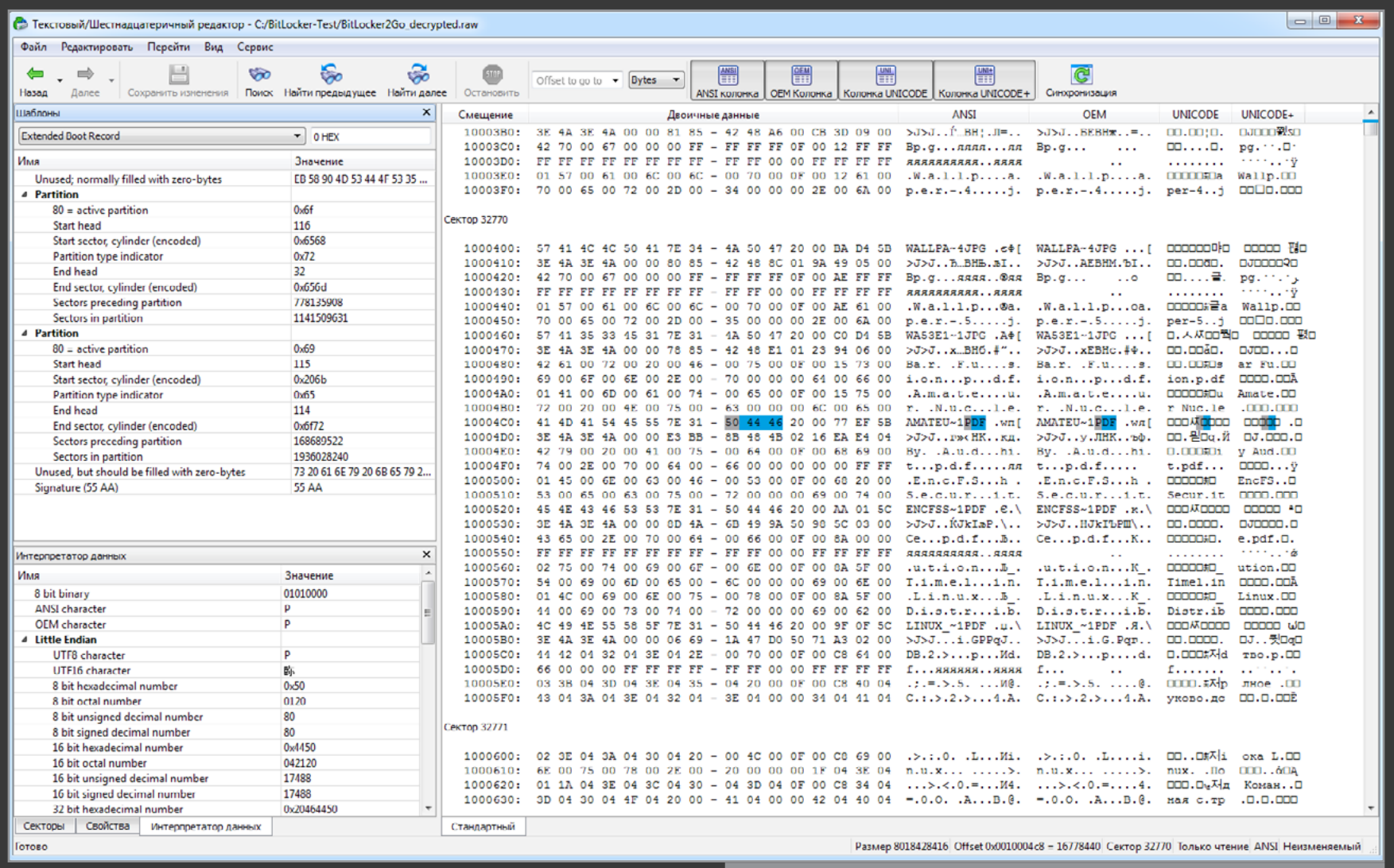
Открываем флешку ключом восстановления

Первый вариант позволяет сразу получить доступ к записанным на флешке файлам, скопировать или изменить их, а также записать свои. Второй вариант выполняется гораздо дольше (от получаса), однако имеет свои преимущества. Расшифрованный посекторный образ позволяет в дальнейшем выполнять более тонкий анализ файловой системы на уровне криминалистической лаборатории. При этом сама флешка уже не нужна и может быть возвращена без изменений.



Расшифровываем флешку в EFDD и записываем посекторный образ

Полученный образ можно открыть сразу в любой программе, поддерживающей формат IMA, или сначала конвертировать в другой формат (например, с помощью UltraISO).



Анализ образа расшифрованного диска

Разумеется, помимо обнаружения ключа восстановления для BitLocker2Go, в EFDD поддерживаются и все остальные методы обхода BitLocker. Просто перебирай все доступные варианты подряд, пока не найдешь ключ любого типа. Остальные (вплоть до FVEK) сами будут расшифрованы по цепочке, и ты получишь полный доступ к диску.

выводы

Технология полнодискового шифрования BitLocker отличается в разных версиях Windows. После адекватной настройки она позволяет создавать криптоконтейнеры, теоретически сравнимые по стойкости с TrueCrypt или PGP. Однако встроенный в Windows механизм работы с ключами сводит на нет все алгоритмические ухищрения. В частности, ключ VMK, используемый для дешифровки основного ключа в BitLocker, восстанавливается с помощью EFDD за несколь-

ко секунд из депонированного дубликата, дампа памяти, файла гибернации или атакой на порт FireWire. Получив ключ, можно выполнить классическую офлайновую атаку, незаметно скопировать и автоматически расшифровать все данные на «защищенном» диске. Поэтому BitLocker целесообразно использовать только вместе с другими средствами защиты: шифрованной файловой системой (EFS), службой управления правами (RMS), контролем запуска программ, контролем установки и подключения устройств, а также более жесткими локальными политиками и общими мерами безопасности.

WWW

BitLocker в Windows 10

RAM Capture

Elcomsoft Forensic Disk Decryptor