Лабораторная работа № 3

**Защита конфиденциальных данных и аудит**

Цель работы: Изучить систему защиты конфиденциальных данных. Ознакомиться с основными способами и настройками защиты различных носителей конфиденциальных данных. Изучить основы аудита.

Операционные системы: Windows 8.1, Windows 10

Краткий теоретический материал

BitLocker Drive Encryption — [проприетарная](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%BF%D1%80%D0%B8%D0%B5%D1%82%D0%B0%D1%80%D0%BD%D0%B0%D1%8F_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0) технология, являющаяся частью операционных систем [Microsoft](https://ru.wikipedia.org/wiki/Microsoft) [Windows начиная с версии Vista](https://ru.wikipedia.org/wiki/Windows_Vista) Ultimate.

BitLocker позволяет защищать данные путём полного шифрования диска(ов): логических, карт [SD](https://ru.wikipedia.org/wiki/Secure_Digital) и [USB](https://ru.wikipedia.org/wiki/USB)-флешек. Поддерживаются следующие алгоритмы шифрования:

* [AES](https://ru.wikipedia.org/wiki/Advanced_Encryption_Standard) 128
* [AES](https://ru.wikipedia.org/wiki/Advanced_Encryption_Standard) 128 c Elephant diffuser (используется по умолчанию)
* [AES](https://ru.wikipedia.org/wiki/Advanced_Encryption_Standard) 256
* [AES](https://ru.wikipedia.org/wiki/Advanced_Encryption_Standard) 256 c Elephant diffuser

Trusted Platform Module (TPM) - название спецификации, описывающей [криптопроцессор](https://ru.wikipedia.org/wiki/%D0%91%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D1%8B%D0%B9_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D1%81%D1%81%D0%BE%D1%80), в котором хранятся [криптографические ключи](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F)) для защиты информации.

Сам ключ может храниться в [TPM](https://ru.wikipedia.org/wiki/Trusted_Platform_Module) или на [USB](https://ru.wikipedia.org/wiki/USB)-устройстве, либо же на компьютере. В случае с [TPM](https://ru.wikipedia.org/wiki/Trusted_Platform_Module) при загрузке компьютера ключ может быть получен из него сразу, либо только после аутентификации с помощью USB-ключа или ввода [PIN-кода](https://ru.wikipedia.org/wiki/PIN-%D0%BA%D0%BE%D0%B4) пользователем. Таким образом, возможны следующие комбинации для доступа:

* [TPM](https://ru.wikipedia.org/wiki/Trusted_Platform_Module)
* [TPM](https://ru.wikipedia.org/wiki/Trusted_Platform_Module) + [PIN](https://ru.wikipedia.org/wiki/PIN-%D0%BA%D0%BE%D0%B4)
* [TPM](https://ru.wikipedia.org/wiki/Trusted_Platform_Module) + [PIN](https://ru.wikipedia.org/wiki/PIN-%D0%BA%D0%BE%D0%B4) + [USB](https://ru.wikipedia.org/wiki/USB)-ключ
* [TPM](https://ru.wikipedia.org/wiki/Trusted_Platform_Module) + [USB](https://ru.wikipedia.org/wiki/USB)-ключ
* [USB](https://ru.wikipedia.org/wiki/USB)-ключ (данный режим требует активации через групповые политики)
* Пароль (данный режим доступен начиная с Windows 8, а также требует активации через групповые политики)

BitLocker шифрует том, а не физический диск. Том может занимать часть диска, а может включать в себя массив из нескольких дисков. Для работы BitLocker’у в случае шифрования системного диска потребуется два [NTFS](https://ru.wikipedia.org/wiki/NTFS)-[тома](https://ru.wikipedia.org/wiki/%D0%9B%D0%BE%D0%B3%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9_%D0%B4%D0%B8%D1%81%D0%BA), один для [ОС](https://ru.wikipedia.org/wiki/%D0%9E%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0) и один для загрузочной части. Последний должен быть не менее 1,5 Гб, и не будет зашифрован. Начиная с [Windows Vista](https://ru.wikipedia.org/wiki/Windows_Vista) SP1 появилась возможность шифровать несистемные [тома](https://ru.wikipedia.org/wiki/%D0%9B%D0%BE%D0%B3%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9_%D0%B4%D0%B8%D1%81%D0%BA). После создания разделов необходимо инициализировать [TPM](https://ru.wikipedia.org/wiki/Trusted_Platform_Module)-модуль в ПК, где он есть, и активировать BitLocker. В [Windows 7](https://ru.wikipedia.org/wiki/Windows_7) появился BitLocker To Go, позволяющий шифровать сменные носители, а также снижены требования для загрузочной части, для неё достаточно 100 Мб.

Механизмы расшифровки и их уязвимости

Существует три механизма проверки подлинности, которые можно использовать для реализации Bitlocker шифрования:

* Прозрачный режим работы: Этот режим использует возможности аппаратного обеспечения  [TPM](https://ru.wikipedia.org/wiki/TPM) для предоставления прозрачной работы пользователей. Пользователи входят на [компьютер](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80) с операционной системой Windows, как обычно. Ключ, используемый для шифрования диска, закодирован в чип TPM и он может быть выдан только в коде [загрузчика ОС](https://ru.wikipedia.org/wiki/%D0%97%D0%B0%D0%B3%D1%80%D1%83%D0%B7%D1%87%D0%B8%D0%BA_%D0%BE%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%BE%D0%B9_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B) (если загрузочные файлы, показываются как не измененные). Этот режим уязвим для нападения при холодной загрузке, так как позволяет выключить компьютер и загрузиться злоумышленнику.
* Режим проверки подлинности пользователя: Этот режим предполагает, что [пользователь](https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D1%8C) прошёл некоторую аутентификацию в пред загрузочной среде в виде предварительного ввода PIN-кода. Этот режим уязвим при использовании [буткит-атак](https://ru.wikipedia.org/wiki/%D0%91%D1%83%D1%82%D0%BA%D0%B8%D1%82).
* Режим USB-ключа: Пользователь должен вставить устройство [USB](https://ru.wikipedia.org/wiki/USB) в компьютер, которое содержит ключ запуска, чтобы иметь возможность загрузки в защищенную операционную систему. Обратите внимание, что для этого режима необходимо, чтобы [BIOS](https://ru.wikipedia.org/wiki/BIOS) на компьютере поддерживал чтение устройств USB в загрузочной среде. Этот режим также уязвим к буткит-нападениям.

В Windows 8.1 и Windows 10 BitLocker позволяет пользователям принимать решение зашифровать только свои данные или весь диск целиком. Так же была усилена защита от атаки «грубой силой». При обнаружении данной атаки драйвер BitLocker переводится в защищенный режим. Информация не будет расшифрована, пока пользователь не введет 48- символьный пароль восстановления. Так же может быть ведено условие, чтобы расшифровка диска происходила только из доверительной сети.

Для настройки политик шифрования необходимо перейти по следующему пути:  ***Конфигурация компьютера\ Административные шаблоны\ Компоненты Windows\ Этот параметр политики позволяет выбрать шифрование диска*** *BitLocker* ***.***

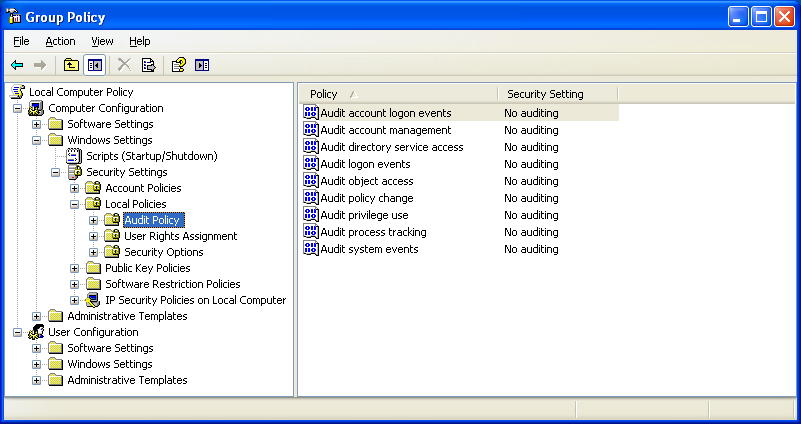
В открывшемся окне возможна настройка BitLocker под различные носители информации.

Для того чтобы непосредственно зашифровать носитель, от необходимо зайти в Панель управления/Система и Безопасность/Шифрование диска BitLocker.

Если при шифровании возникает ошибка в которой содержится данный текст «Это устройство не может использовать доверенный платформенный модель (TRM)..», то смотрите файл «Как включить BitLocker в Windows 8 без TPM.pdf».

   В Windows имеется система **Аудита,** позволяющая отслеживать и журналировать информацию о том, когда, кем и с помощью какой программы были удалены документы. По умолчанию, Аудит не задействован — слежение само по себе требует определённый процент мощности системы, а если записывать всё подряд, то нагрузка станет слишком большой. Тем более, далеко не все действия пользователей могут нас интересовать, поэтому политики Аудита позволяют включить отслеживание только тех событий, что для нас действительно важны. Система Аудита встроена во все операционные системы **Microsoft** **Windows** **NT.**

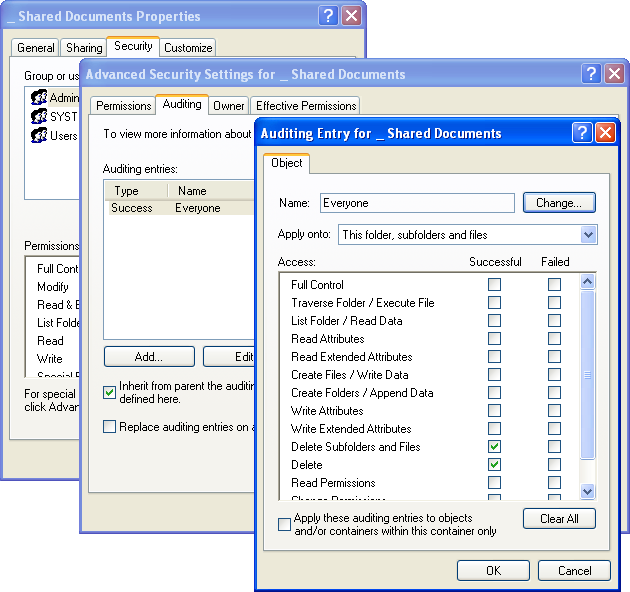
  Для включения аудита зайдите с правами администратора в компьютер, предоставляющий доступ к общим документам, и выполните команду **Start**→**Run**→**gpedit.msc.** В разделе Computer Configuration раскройте папку **Windows Settings → Security Settings → Local Policies → Audit Policies (**локал политика безопасности/локальная политика/политика аудита**):**

****

Дважды щёлкните по политике **Audit object access (Аудит доступа к объектам)** и выберите галочку **Success.** Этот параметр включает механизм слежения за успешным доступом к файлам и реестру. Действительно, ведь нас интересуют только удавшиеся попытки удаления файлов или папок. Включите Аудит только на компьютерах, непосредственно на которых хранятся отслеживаемые объекты.

        Простого включения политики Аудита недостаточно, мы также должны указать, доступ к каким именно папкам требуется отслеживать. Обычно такими объектами являются папки общих (разделяемых) документов и папки с производственными программами или базами данных, то есть, ресурсы, с которыми работают несколько человек.

        Заранее угадать, кто именно удалит файл, невозможно, поэтому слежение и указывается за Всеми (Everyone). Удавшиеся попытки удаления отслеживаемых объектов любым пользователем будут заноситься в журнал. Вызовите свойства требуемой папки (если таких папок несколько, то всех их по очереди) и на закладке **Security (Безопасность) → Advanced (Дополнительно) → Auditing (Аудит)** добавьте слежение за субъектом**Everyone (Все),** его успешными попытками доступа **Delete (Удаление)** и **Delete Subfolders and Files (Удаление подкаталогов и файлов):**



  Событий может журналироваться довольно много, поэтому также следует отрегулировать размер журнала**Security (Безопасность)**, в который они будут записываться.

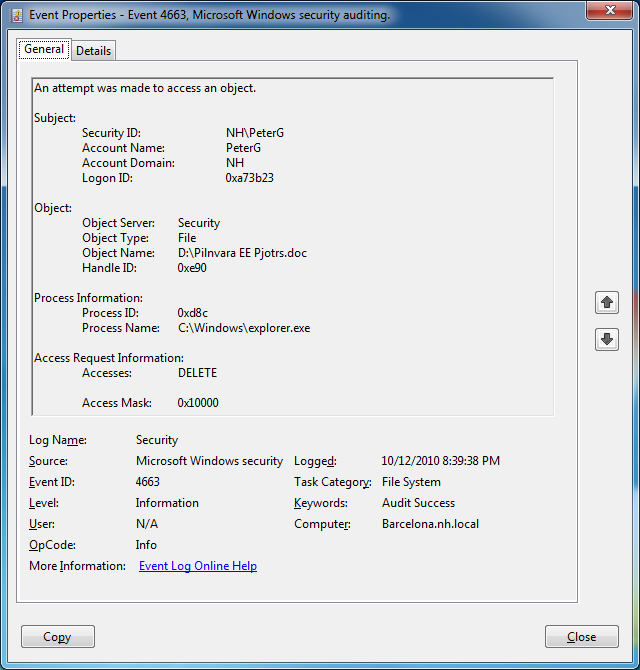
Для этого выполните команду **Start → Run → eventvwr.msc.** В появившемся окне вызовите свойства журнала Security и укажите следующие параметры:

* Maximum Log Size = **65536 KB** (для рабочих станций) или **262144 KB** (для серверов)
* Overwrite events as needed.

        На самом деле, указанные цифры не являются гарантированно точными, а подбираются опытным путём для каждого конкретного случая.

Для проверки журнала нажмите **Start → Run → eventvwr.msc** и откройте для просмотра журнал **Security (Безопасность).** Журнал может быть заполнен событиями, прямого отношения к проблеме не имеющими. Щёлкнув правой кнопкой по журналу Security, выберите  команду **View → Filter** и отфильтруйте просмотр по следующим критериям:

* Event Source:     Security;
* Category:         Object Access;
* Event Types:      Success Audit;
* Event ID:         4663;



Не спешите интерпретировать все удаления как злонамеренные. Эта функция зачастую используется при обычной работе программ — например, исполненяя команду **Save (Сохранить),**  программы пакета **MicrosoftOffice** сначала создают новый временный файл, сохраняют в него документ, после чего удаляют предыдущую версию файла. Аналогично, многие приложения баз данных при запуске сначала создают временный файл блокировок **(.lck),** затем удаляют его при выходе из программы.

Задание

Если вы не разбили диск в прошлой лабораторной работе, то сделайте это сейчас. (<http://remontka.pro/razbit-hdd/> - разметить диск)

*Перед выполнением работы сделайте снимок текущего состояния виртуальной машины, чтобы в случае ошибки откатиться на стартовую позицию.*

Перейдя по пути который указан в «Краткий теоретический материал» необходимо настроить BitLocker в общем плане и отдельно для каждого носителя в соответствии с пунктами ниже.

1. Выбрать метод шифрования AES с 256
2. Съемные носители
   1. Включить для съемных носителей;
   2. Включить использование программного шифрация, а не аппаратное;
   3. Шифрование только занятого места;
   4. Установить требования сложности пароля для шифрования 8 символов;
   5. Включить восстановление съемного носителя;
3. Несъемные носители
   1. Запретить запись данных на незащищенные BitLocker носители;
   2. Использовать программное шифрование;
   3. Полное шифрование диска;
   4. Установить обязательный сложный пароль 8 символов;
   5. Включить восстановление диска с помощью 48 битного ключа;
4. Диск операционной системы:
   1. Разрешить загрузку и проверка целостности;
   2. Установить минимальную длину пин-кода 5 символов;
   3. Использовать только программного шифрования;
   4. Разрешить пользователю выбирать тип шифрования;
   5. Поставить сложный пароль длиной 8 символов
   6. Установить метод восстановления диска. Ключ 48-бит;

После необходимой настройки переходим к непосредственному шифрованию различных носителей информации.

Тут я рекомендую сделать еще снимок виртуальной машины, так как будет необходимо шифровать один и тот же логический том различными способами с различными средствами расшифровки.

При выполнении следующих пунктов необходимо будет проделать и зафиксировать этапы шифрования (выбор необходимых условий) носителей, этапы расшифровки носителей при предоставления пароля доступа, usb устройства и пароля восстановления.

1. Зашифровать диск с ОС (если вылетает ошибка см. pdf файлы)
   1. Сделать чтобы при запуске системы(расшифровки) требовал пароль;
      1. Сохранить пароль восстановления на флэшке;
      2. Сохранить на USB-устройстве флэш памяти;
   2. Сделать чтобы при запуске системы требовалось USB устройство;
2. Зашифровать торой том
   1. Сделать, чтобы при расшифровки диска требовался пароль;
   2. Сохранить ключ восстановления в файле;
3. Зашифровать USB флэшку
   1. Сделать, чтобы при расшифровки носителя требовался пароль;
   2. Сохранить в файл пароль восстановления;

Необходимо настроить политику аудита, как было показано в пункте в ***«***Краткий теоретический материал» и в соответствии с заданием ниже. (<https://technet.microsoft.com/ru-ru/library/dd408940(v=ws.10).aspx)>

Для набора файлов и папок, что создавались в 1-ой лабораторной работе, настроить проверку на удаления. Один из пользователей «студент 1» должен удалить файл ф1. Нужно показать процесс настройка политики аудита. В журнале Аудита продемонстрировать успешный вход «студента 1» и удаление им файла ф1. Так же для пользователя «гость» показать в журнале неудачную попытку доступа к папке п1.