



Operating Systems & Security

Часть 2

2024

Антонов ДМ





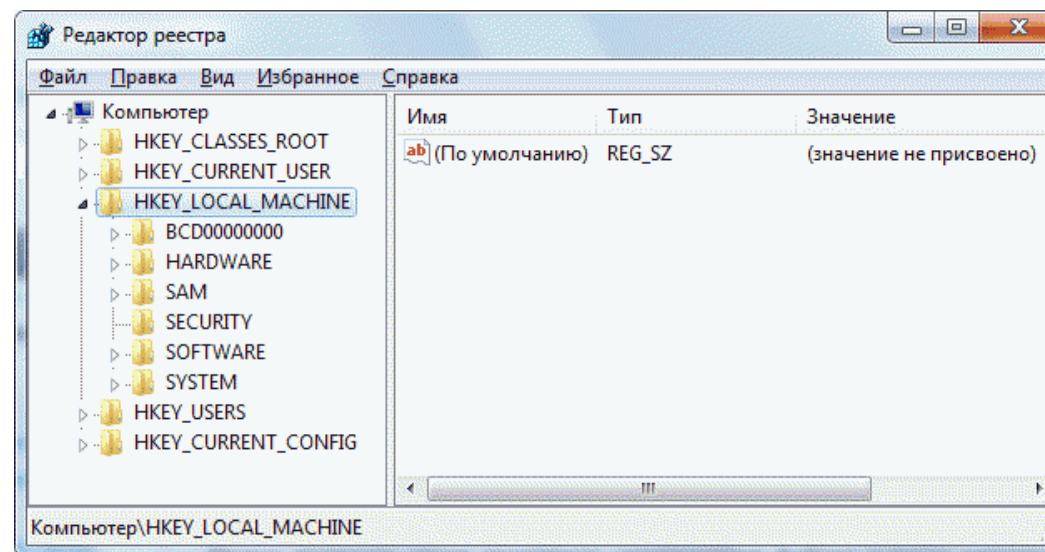
Часть 3.

1. Локальная политика безопасности
2. Восстановление системы
3. Реестр Windows
4. Управление дисками
5. Файловые системы Windows
6. Использование BitLocker



РЕЕСТР WINDOWS

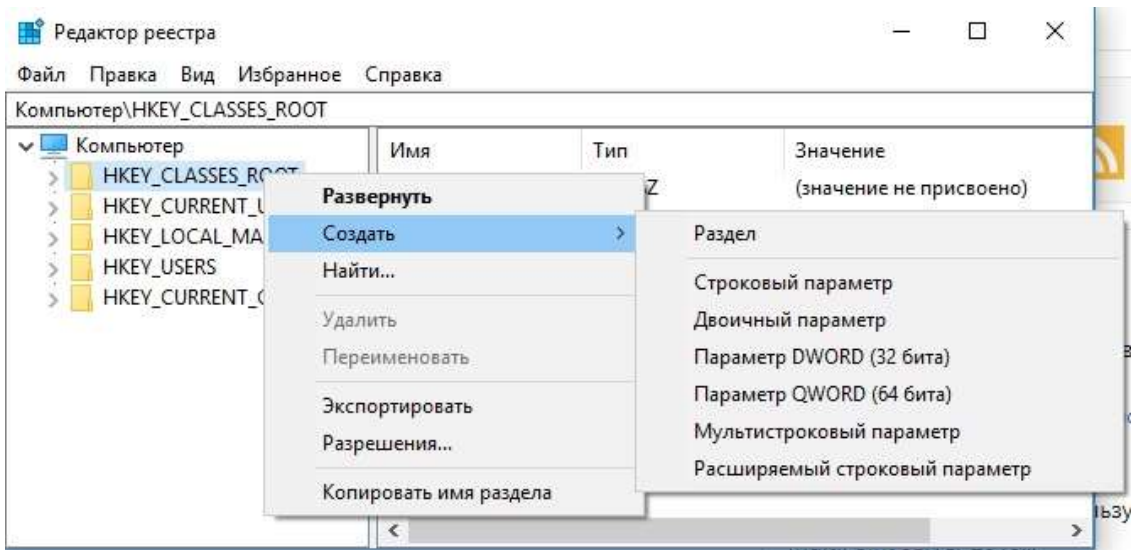
Реестр в ОС Windows – база данных, в которой хранятся в упорядоченном виде все актуальные настройки как встроенных и сторонних программ на ПК, так и всей операционной системы в целом. Во время работы компьютера система постоянно обращается к нему за необходимой информацией.



1. HKEY_CURRENT_USER (HKCU). Этот раздел отвечает за данные пользователя, вошедшего в систему в настоящий момент. Здесь хранятся папки пользователя, фон экрана, значки рабочего стола и т. п.
2. HKEY_USERS (HKU). Здесь содержится информация обо всех профилях на компьютере.
3. HKEY_LOCAL_MACHINE (HKLM). В этом разделе хранится конфигурация аппаратного и программного обеспечения. Некоторые данные подраздела HARDWARE хранятся в ОЗУ, а не на жёстком диске. Это связано с тем, что они временные по своей природе и нужны только при загрузке аппаратного обеспечения, а затем удаляются.
4. HKEY_CLASSES_ROOT (HKCR) содержит сведения о расширениях всех зарегистрированных в системе типов файлов и ассоциациях (отвечает за запуск необходимой программы при открытии файла с помощью «Проводника Windows») и сведения о внедрённых COM-серверах.
5. HKEY_CURRENT_CONFIG. Данный раздел содержит аппаратные параметры, необходимые для загрузки системы.



РЕЕСТР WINDOWS



Компьютер\HKEY_CURRENT_USER\Control Panel\Colors

Имя	Тип	Значение
(По умолчанию)	REG_SZ	(значение не присвоено)
ActiveBorder	REG_SZ	180 180 180
ActiveTitle	REG_SZ	153 180 209
AppWorkspace	REG_SZ	171 171 171
Background	REG_SZ	10 59 118
ButtonAlternate...	REG_SZ	0 0 0
ButtonDkShadow	REG_SZ	105 105 105
ButtonFace	REG_SZ	240 240 240
ButtonHighlight	REG_SZ	255 255 255
ButtonLight	REG_SZ	227 227 227

Изменение строкового параметра

Параметр:

Background

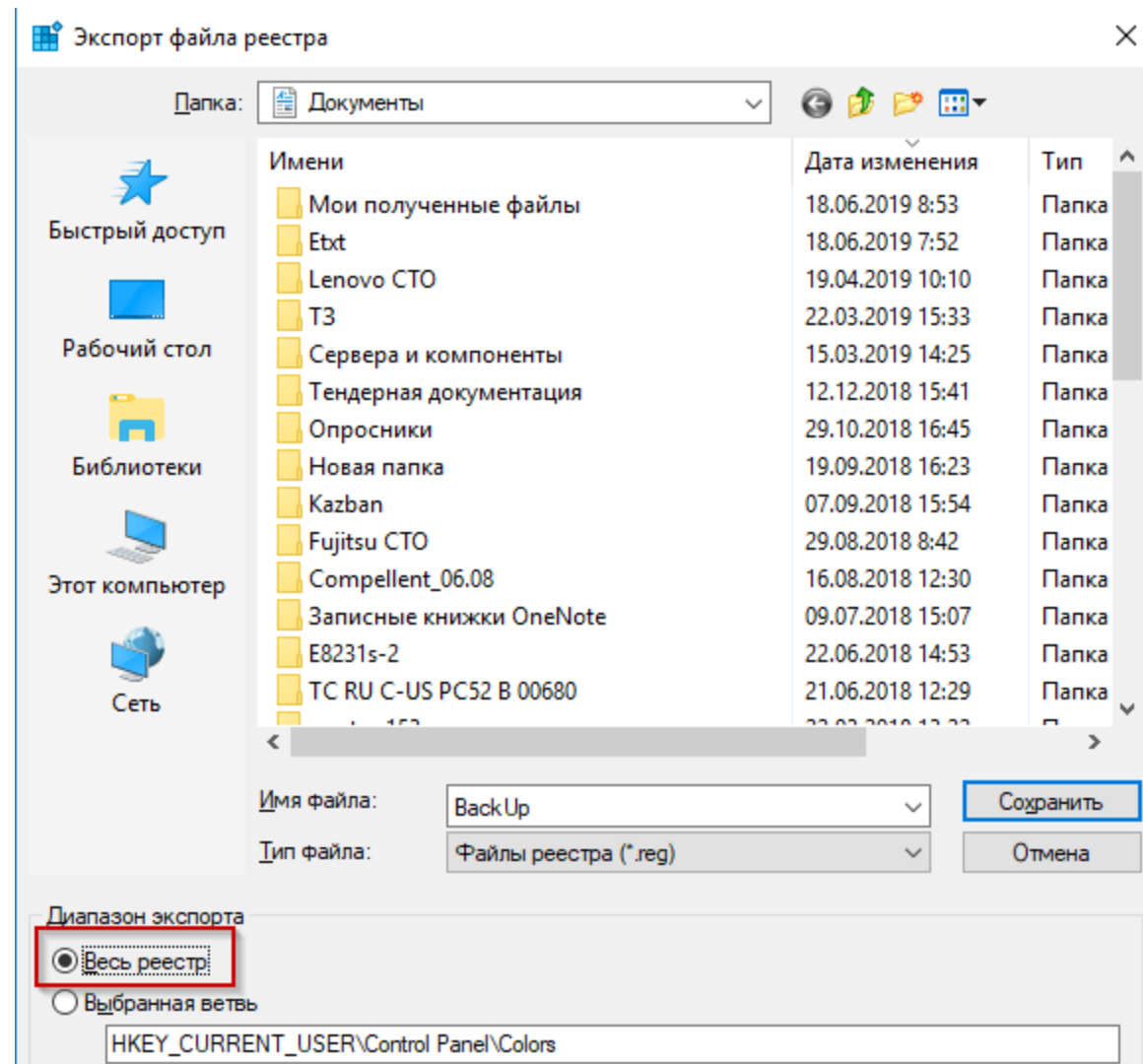
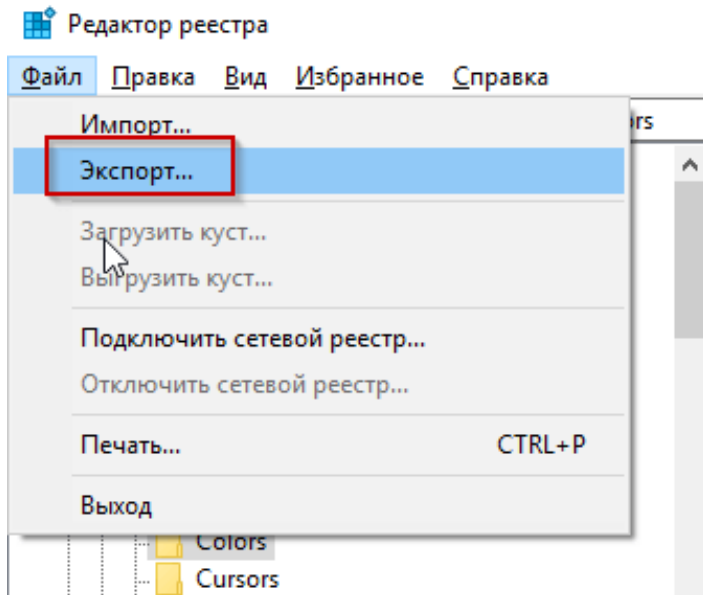
Значение:

10 59 118

OK Отмена



РЕЕСТР WINDOWS





РЕЕСТР WINDOWS

Все версии Windows поддерживают раздел реестра **RunOnce**, который можно использовать для указания команд, которые система будет выполнять один раз, а затем удаляется.

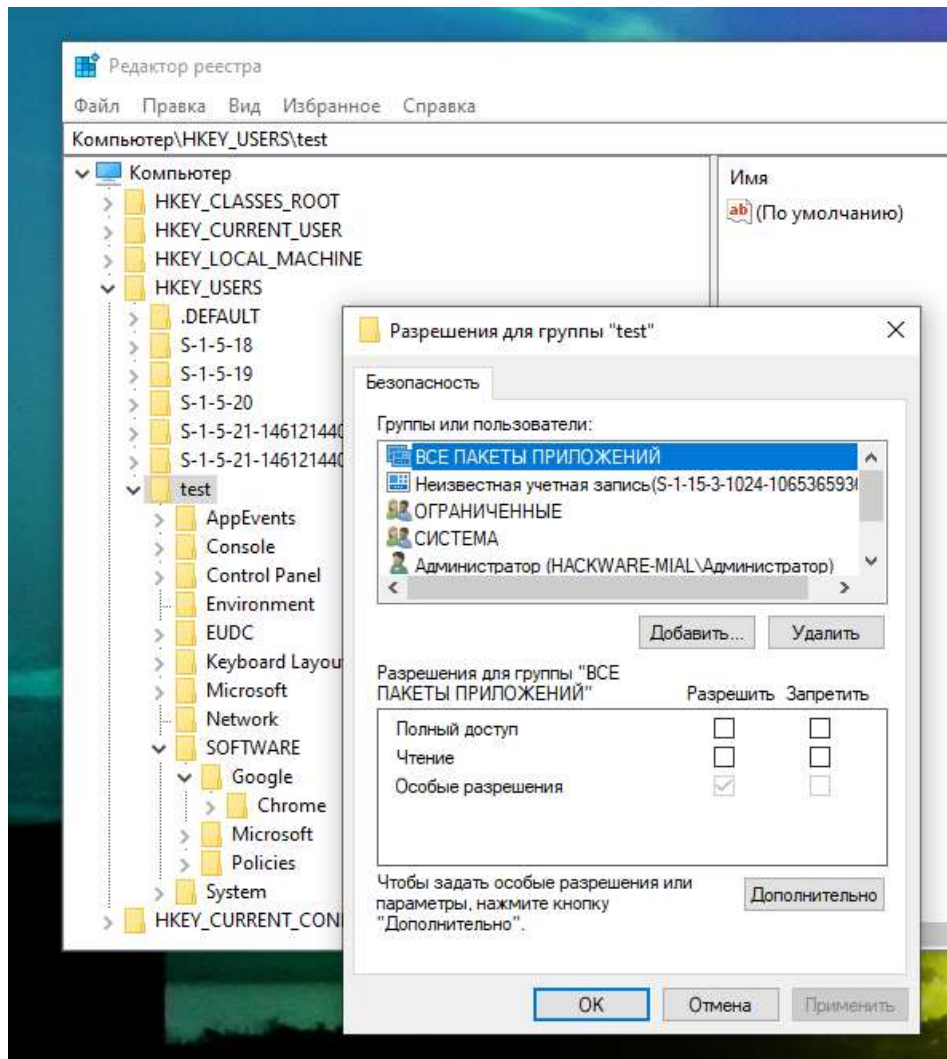
HKLM,

"Software\Microsoft\Windows\CurrentVersion\RunOnce"

1 Способы обеспечения безопасности реестра

- 1.1 Физическая безопасность - запирание дверей
- 1.2 Отключение службы удалённого реестра
- 1.3 Ограничение удалённых пользователей
- 1.4 Цифровая подпись драйверов
- 1.5 Ограничение физического доступа

<https://hackware.ru/?p=14371>





РЕЕСТР WINDOWS

REG <операция> [Список параметров]

1	имя_раздела	КОРЕНЬ\<подраздел>
2	КОРЕНЬ	[НКЛМ НКСУ НКСР НКУ НКСС]
3	подраздел	Полное имя подраздела реестра в одном из выбранных корневых
4		файлов.
5		
6	имя_файла	Имя диска, на который сохраняется файл. Если путь не указан,
7		то файл создается в текущей папке вызывающего процесса.
8		
9	/y	Выполнение замены существующего файла без запроса
10		подтверждения.
11		
12	/re	Указывает, что к разделу реестра следует обращаться с помощью
13		представления для 32-разрядных приложений.
14		
15	/reg:64	Указывает, что к разделу реестра следует обращаться с помощью
16		представления для 64-разрядных приложений.

Типичные операции:

- QUERY
- ADD
- DELETE
- COPY
- SAVE
- LOAD
- UNLOAD
- RESTORE
- COMPARE
- EXPORT
- IMPORT
- FLAGS



РЕЕСТР WINDOWS

Примеры настроек безопасности

Защита от сетевых атак протокола TCP/IP

Для защиты от сетевых атак протокола TCP/IP добавляются параметры, с установкой их значения и изменения значения существующих параметров в ключе реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

Отключение автоматического входа в систему под учетной записью администратора

Отключение автоматического входа в систему под учетной записью администратора обеспечивается установкой параметру «AutoAdminLogon» значения «1,0» в ключе реестра HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon

Отключение клиентов по истечении разрешенного времени входа

Отключение клиентов по истечении разрешенного времени входа обеспечивается установкой параметру «enableforcedlogoff» значения «4,1» в ключе реестра HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters

Использование цифровой подписи для сервера

Использование цифровой подписи (с согласия сервера или всегда) обеспечивается установкой параметру «EnableSecuritySignature» значения «4,1» (с согласия сервера) или параметру «RequireSecuritySignature» значения «4,1» (всегда) в ключе реестра HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters

Шифрование данных безопасного канала

Шифрование данных безопасного канала (при необходимости) обеспечивается назначением параметру «sealsecurechannel» значения «4,1» в ключе реестра HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\setlogon\Parameters

Запрет форматирования и извлечения съемных носителей

Запрет форматирования и извлечения съемных носителей обеспечивается назначением параметру «AllocateDASD» значения «1,0» в ключе реестра HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon



РЕЕСТР WINDOWS

Примеры редакторов

Оба редактора имеют одинаковые основные возможности. С их помощью вы сможете:

- Просматривать в графическом виде древовидную иерархическую структуру
- Просматривать и изменять разделы, подразделы, параметры и значения параметров (в соответствии с имеющимися у вас полномочиями доступа).
- Соединяться с удаленным компьютером (для доступа к которому у вас имеются полномочия) и проверять или даже изменять содержимое Реестра.

Regedt32

- Возможность просмотра и изменения списков контроля доступа (ACLs) для разделов Реестра.
- Возможность аудита разделов, при помощи которого вы можете наблюдать, кто пытался удалять, добавлять или редактировать разделы (или их содержимое) и узнать, были ли эти попытки успешными.
- Поддержку всех типов данных Реестра, описанных ранее. Кроме того, вы можете редактировать значения одних типов при помощи редактора для другого типа (вручную, редактируя значения REG_BINARY).
- Режим «только чтение», в котором вы можете просматривать Реестр, но не можете вносить в него изменения.
- Сохранение и восстановление файлов-ульев или отдельных разделов.
- Используется старый, «многодокументный» интерфейс MDI (multiple documents interface), в котором для каждого корневого раздела применяется свое окно документа.

Regedit

- Поиск (на соответствие некоторой текстовой строке) разделов, имен параметров и содержимого параметров. Эта возможность чрезвычайно ценна и является основной причиной применения Regedit.
- Использование привычного двухпанельного интерфейса в стиле Проводника Windows, помогающего сравнить взаимное расположение двух разделов или параметров. Он содержит и другие возможности в стиле Проводника Windows, такие как контекстные меню, редактирование прямо на месте и удобное управление деревом.
- Импорт и экспорт нужных разделов (и нижележащих в них элементов данных) в пригодные для чтения людьми текстовые файлы, а не только импорт и экспорт разделов в двоичном виде.
- Имеется меню Favorites (Избранное) в которое вы можете добавлять разделы, которые будут, по вашему мнению, редактироваться часто.



РЕЕСТР WINDOWS

РЕЕСТР WINDOWS

ПОСЛЕ УСТАНОВКИ ОС



ЧЕРЕЗ ГОД

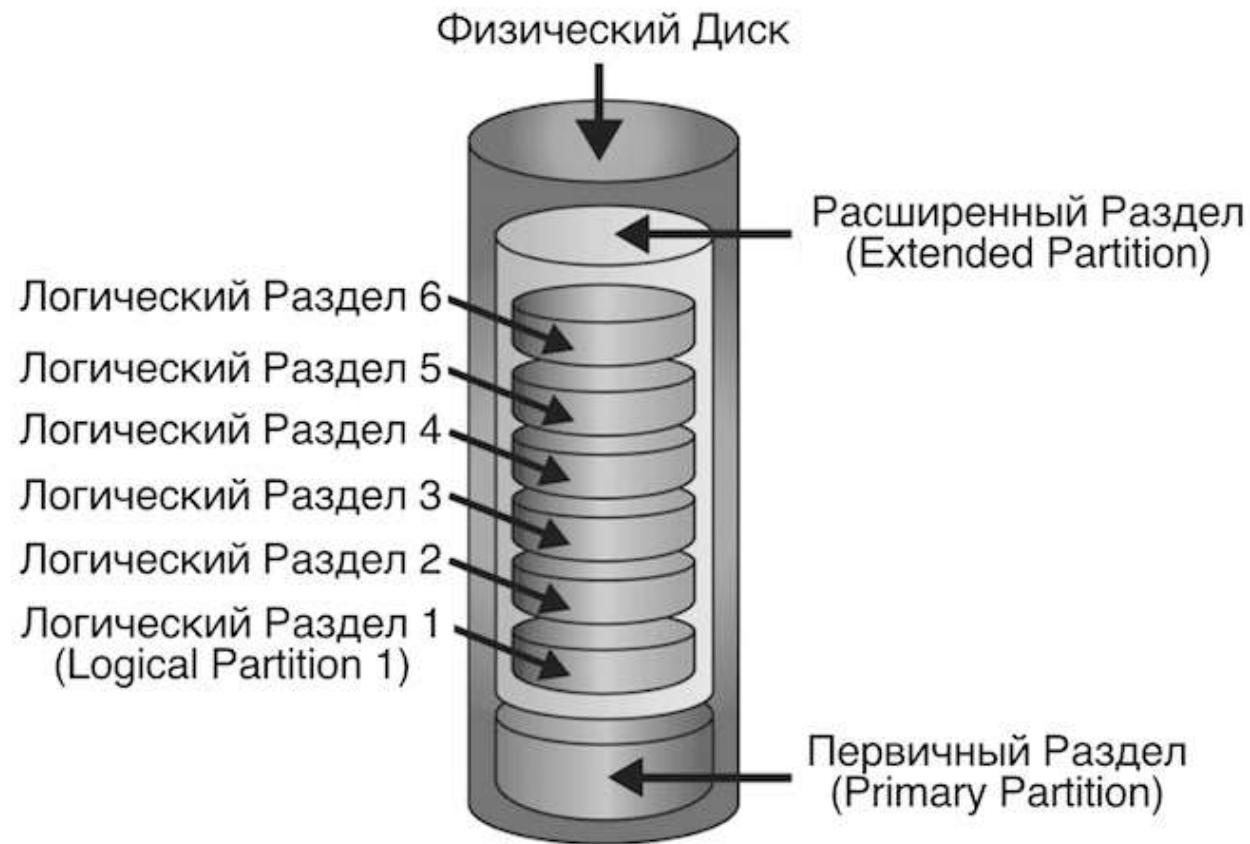




Управление дисками

Настройка дисков производится с помощью утилиты **Управление дисками**. Эта утилита позволяет вам просматривать состав и управлять физическими дисками и томами.

Раздел – это логически выделенная часть пространства на жестком диске. Каждый раздел, созданный под управлением Windows, должен иметь связанную с ним файловую систему. Разделы позволяют одному физическому жесткому диску быть представленным в операционной системе в виде нескольких логических областей, имеющие каждый свою букву для идентификации и использоваться так, как если бы на компьютере было установлено несколько жестких дисков.

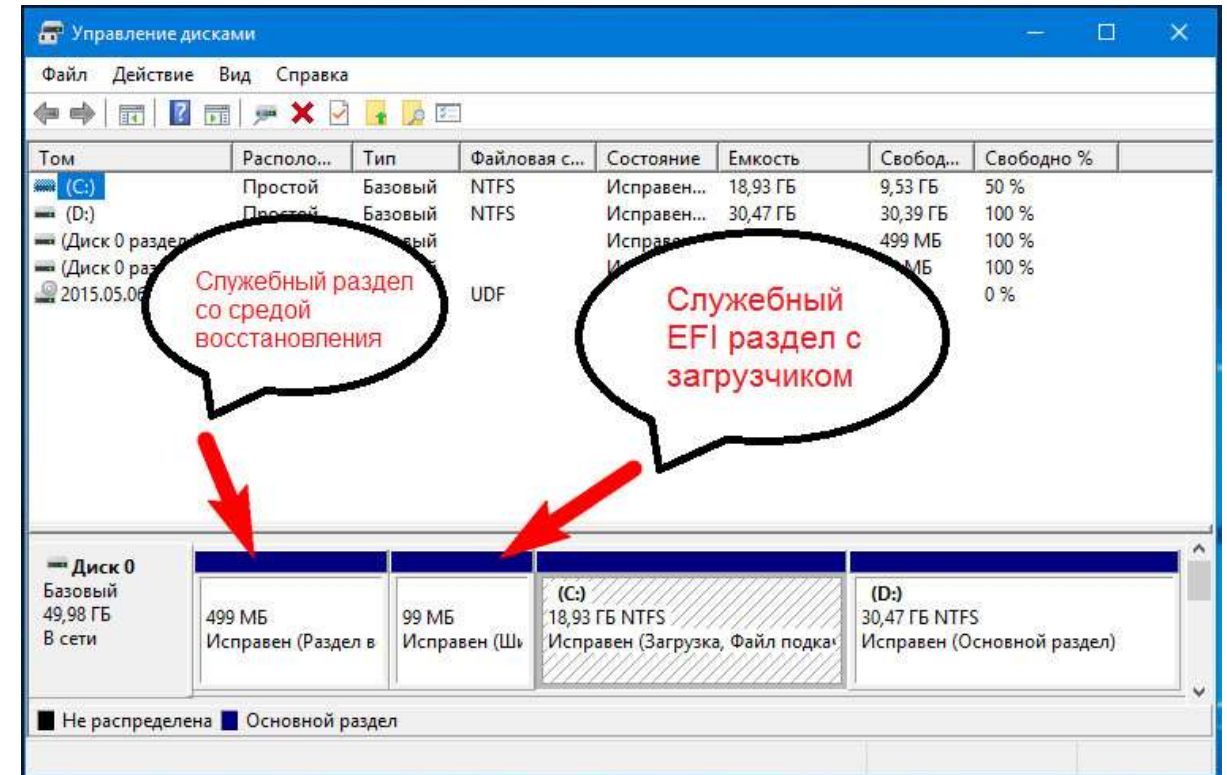




Управление дисками

Файловая система используется для отслеживания хранения файлов на вашем жестком диске таким образом, чтобы этот способ хранения понимался конечными пользователями, но при этом позволял операционной системе получать доступ к файлам в соответствии с запросами.

Рекомендуется использовать файловую систему **NTFS** в Windows 10, потому что это позволит вам использовать такие функции, как локальная безопасность, сжатие файлов и шифрование файлов. Выбрать файловую систему FAT32 рекомендуется только в том случае, если у вас на компьютере уже есть версия Windows, которая не поддерживает NTFS, потому что FAT32 обратно совместима с другими операционными системами. Но в настоящее время это очень маловероятно.





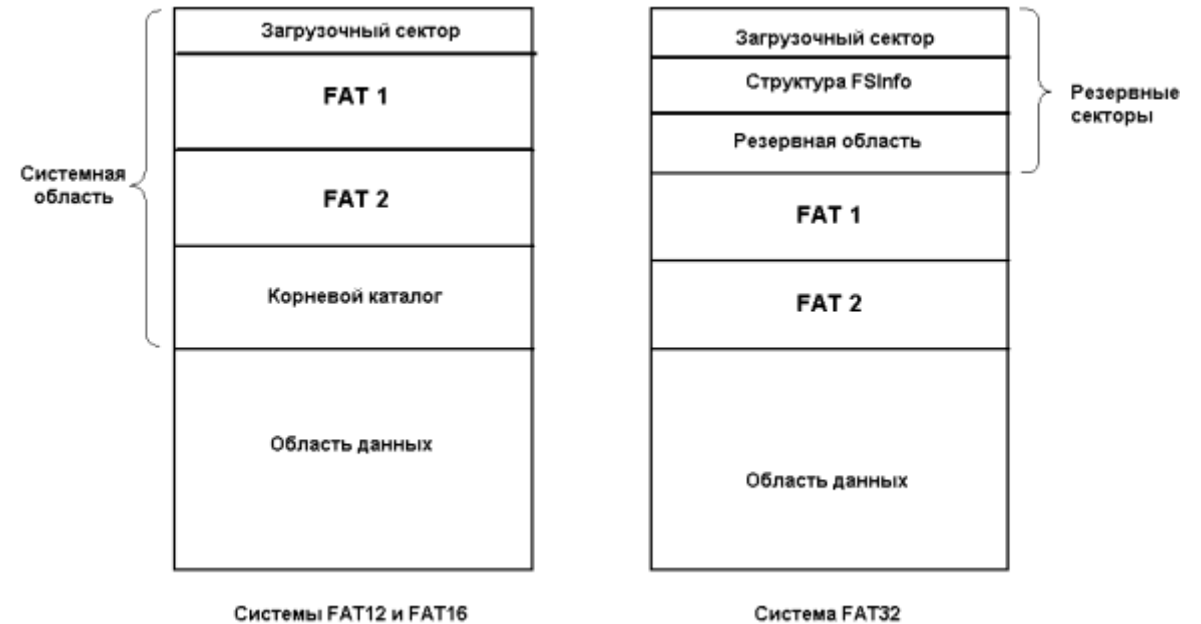
ФАЙЛОВЫЕ СИСТЕМЫ

FAT32

FAT32 – (*File Allocation Table*) это обновленная версия таблицы размещения файлов (FAT). Версия FAT32 была впервые предложена в Windows 95 OSR2 (операционная система Release 2) и может использоваться любой операционной системой Windows по сей день.

Основными недостатками FAT32 по сравнению с NTFS являются:

- ■ отсутствие поддержки больших жестких дисков;
- ■ отсутствие параметров безопасности и встроенной поддержки сжатия и шифрования диска;
- ■ не поддерживает отказоустойчивость;
- ■ сильно быстро деградирует быстродействия при увеличении размера диска (поэтому и ограничение 32 Гб).





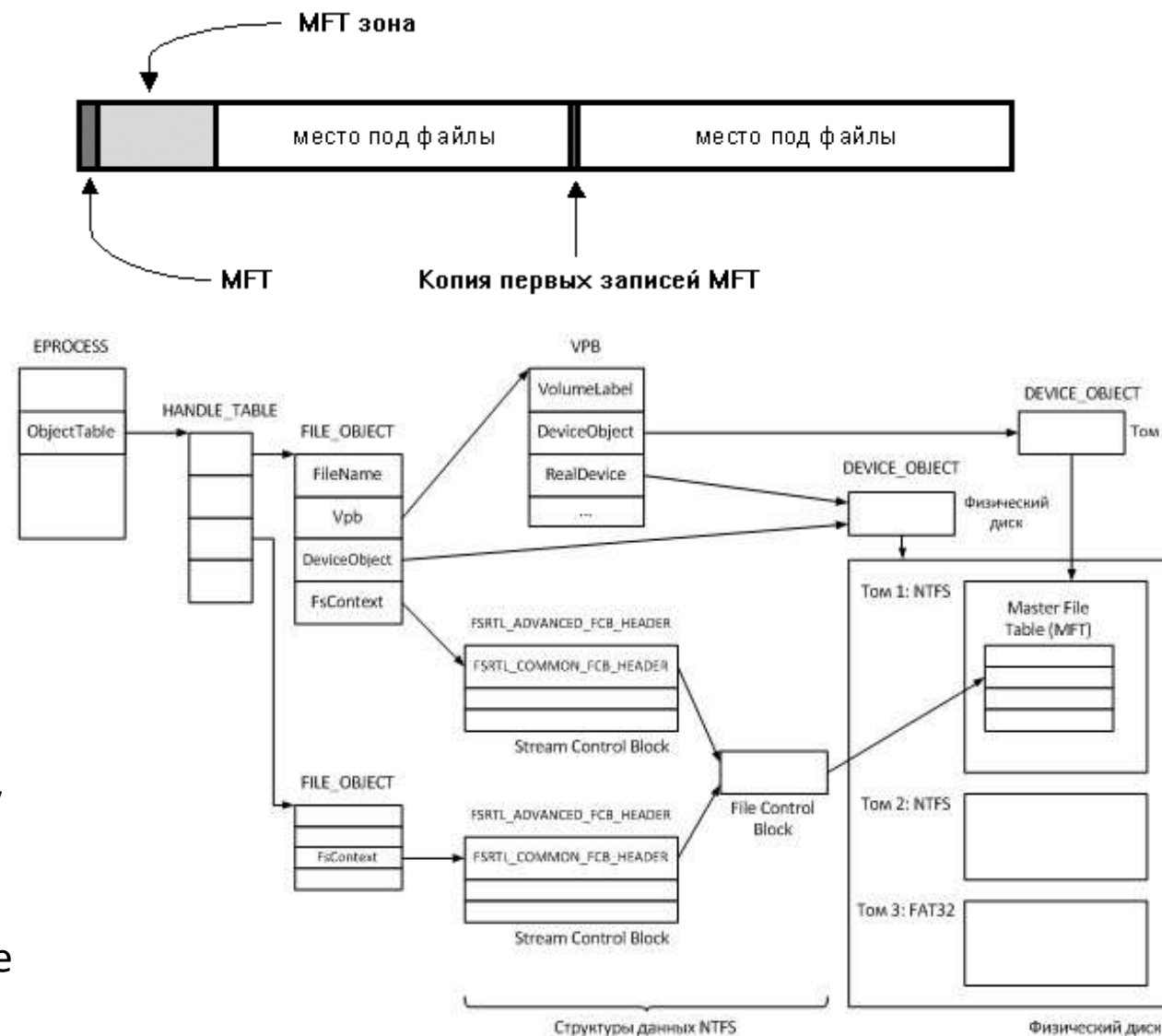
ФАЙЛОВЫЕ СИСТЕМЫ

NTFS

В виде файлов хранятся и административные данные базовой файловой системы – те самые данные, которые в других файловых системах находятся в скрытых областях по фиксированному адресу.

В NTFS нет нужды резервировать какие-то особые области под файловые таблицы, таблицу разделов или журнал транзакций: они хранятся в виде обычных файлов и могут физически располагаться в любом месте тома.

В отличие от других файловых систем, в NTFS нет жёстко заданной структуры. В ней нет, как в FAT, отдельных областей для системных структур, файловых таблиц и собственно данных. В NTFS вся файловая система считается областью данных, поэтому любой файл может быть сохранён в любом секторе тома. Единственным исключением являются загрузочный сектор и загрузочный код, расположенные в первых секторах тома.

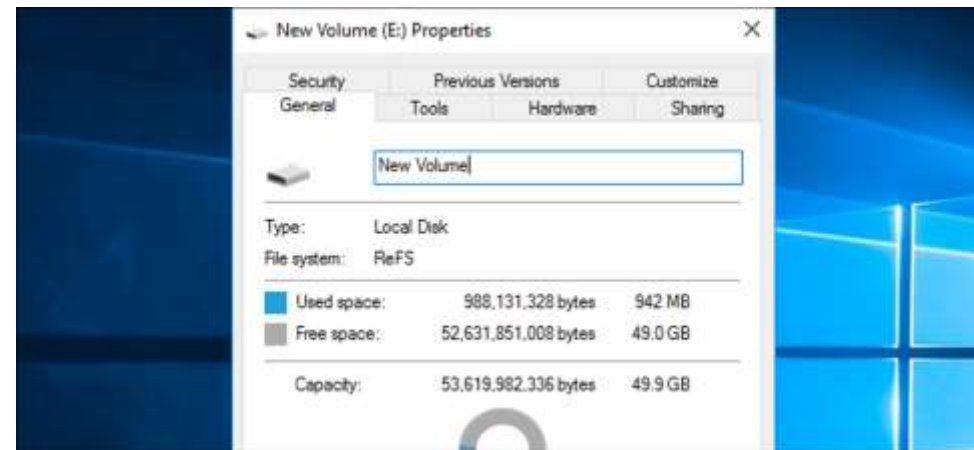


ФАЙЛОВЫЕ СИСТЕМЫ



ReFS

ReFS (Resilient file system) – представляет собой отказоустойчивую технологию, пришедшую на замену NTFS. Призвана устранить недостатки предшественницы и уменьшить количество информации, которая может быть потеряна при различных операциях. Поддерживает работу с файлами большого объема.



Object Table

Object ID	Disk Offset & Checksum
Object ID	Disk Offset & Checksum
Object ID	Disk Offset & Checksum
Object ID	Disk Offset & Checksum

Directory

File Name	File Metadata
File Name	File Metadata
File Name	File Metadata
File Name	File Metadata

File Metadata

Key	Value
Key	Value
Key	Value
Key	Value
Key	Value

File Extents

	Disk Offset & Checksums
0-7894	Disk Offset & Checksums
7895-10000	Disk Offset & Checksums
10001-57742	Disk Offset & Checksums
57743-9002722	Disk Offset & Checksums

ФАЙЛОВЫЕ СИСТЕМЫ



ReFS

- Большая производительность;
 - Улучшение возможностей по проверке носителя на наличие ошибок;
 - Низкая степень потери данных при появлении ошибок файловой системы и bad-блоков;
 - Осуществление шифрования EFS;
 - Функционал дисковых квот;
 - Увеличенный максимальный предел файла до 18,3 Эб;
 - Увеличенное количество хранимых в папке файлов до 18 трлн.;
 - Максимальный объем диска до 402 Эб;
 - Количество символов в имени файла увеличено до 32767.
- Существующие разделы Windows не подлежат для использования ReFS, то есть необходимо использовать только не использованные под систему разделы, например, те, которые предназначены для хранения файлов.
 - Внешние накопители не поддерживаются.
 - Преобразовать NTFS диск в диск ReFS без потери данных невозможно, только форматирование и резервное копирование важных файлов.
 - Не всё программное обеспечение способно распознать эту ФС.

NTFS				REFS			
CrystalDiskMark 5.1.2 x64				CrystalDiskMark 5.1.2 x64			
Файл Настройки Вид Помощь Язык(Language)				Файл Настройки Вид Помощь Язык(Language)			
3 100MB R: 50% (50/99GB)				3 100MB R: 1% (1/99GB)			
All	Read [MB/s]	Write [MB/s]		All	Read [MB/s]	Write [MB/s]	
Seq Q32711	176.9	174.4		Seq Q32711	168.6	165.6	
4K Q32711	1.859	0.926		4K Q32711	1.999	0.951	
Seq	176.7	173.6		Seq	179.5	176.6	
4K	0.691	0.822		4K	0.796	0.941	

NTFS				REFS			
CrystalDiskMark 5.1.2 x64				CrystalDiskMark 5.1.2 x64			
Файл Настройки Вид Помощь Язык(Language)				Файл Настройки Вид Помощь Язык(Language)			
5 2GB V: 0% (0/80GB)				5 2GB V: 1% (1/80GB)			
All	Read [MB/s]	Write [MB/s]		All	Read [MB/s]	Write [MB/s]	
Seq Q32711	99.81	63.70		Seq Q32711	75.75	77.89	
4K Q32711	0.924	0.910		4K Q32711	0.847	1.009	
Seq	100.7	57.88		Seq	32.06	83.47	
4K	0.487	0.539		4K	0.084	0.790	



Управление дисками

Преобразование файловой системы

В Windows 10 вы можете конвертировать разделы FAT32 в NTFS. Преобразование файловой системы – это процесс преобразования одной файловой системы в другую без потери данных. Если вы отформатируете диск, в отличие от его преобразования, все данные на этом диске будут потеряны.

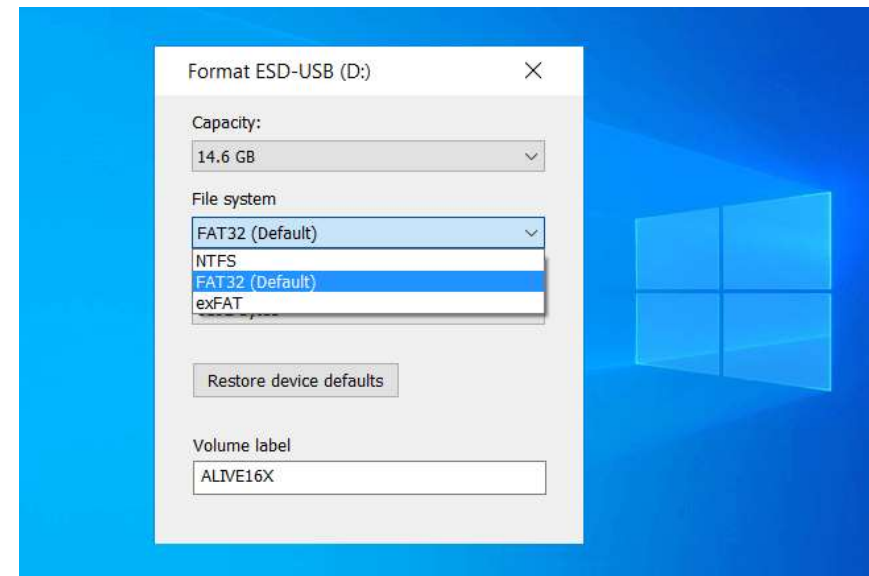
Чтобы преобразовать раздел, можно воспользоваться консольной утилитой Convert. Синтаксис команды Convert следующий:

convert [диск:] / fs: ntfs

Например, если вы хотите преобразовать свой D: диск в NTFS, вы должны ввести следующую команду:

convert D: / fs: ntfs

Windows 10 также поддерживает Compact Disk File System (CDFS). Однако CDFS нельзя управлять. Она используется только для работы с компакт-дисками.



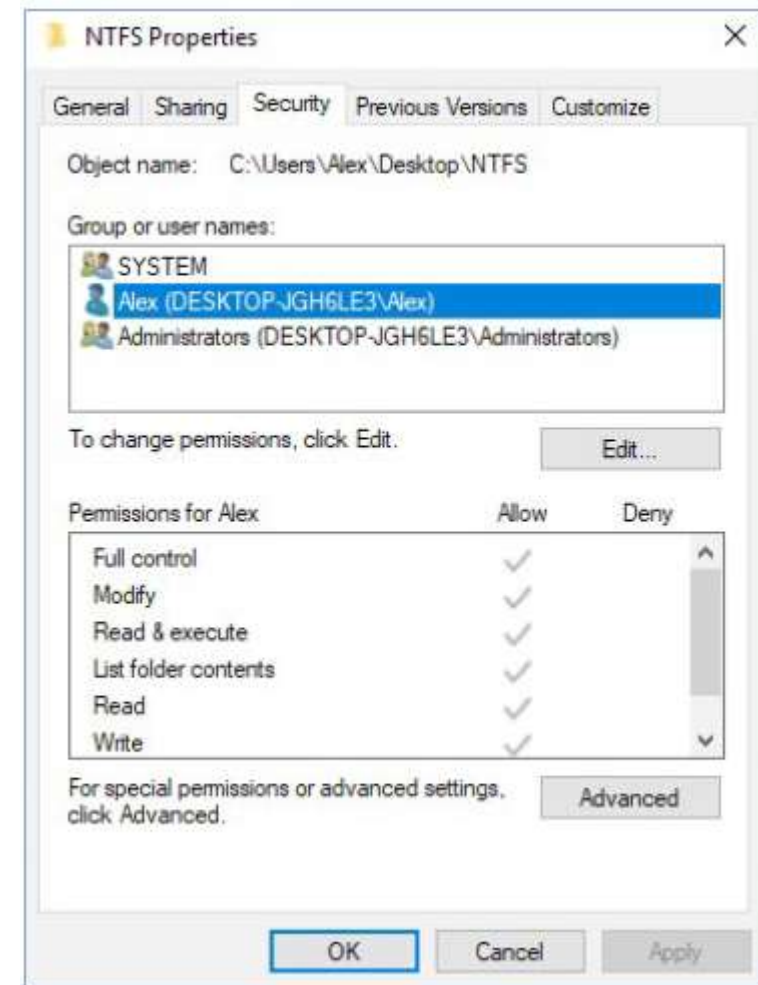


Управление дисками

Безопасность NTFS (NTFS Security)

Одним из главных преимуществ NTFS является **безопасность**. Безопасность NTFS является одним из наиболее важных аспектов работы ИТ-администратора. Преимуществом NTFS безопасности является то, что она может быть применена для отдельных файлов и папок. Не имеет значения, работаете ли вы локально или удаленно, безопасность всегда будет установлена с помощью NTFS.

Разрешение по умолчанию – **Пользователи = чтение** будет устанавливаться для всех новых папок и файлов.





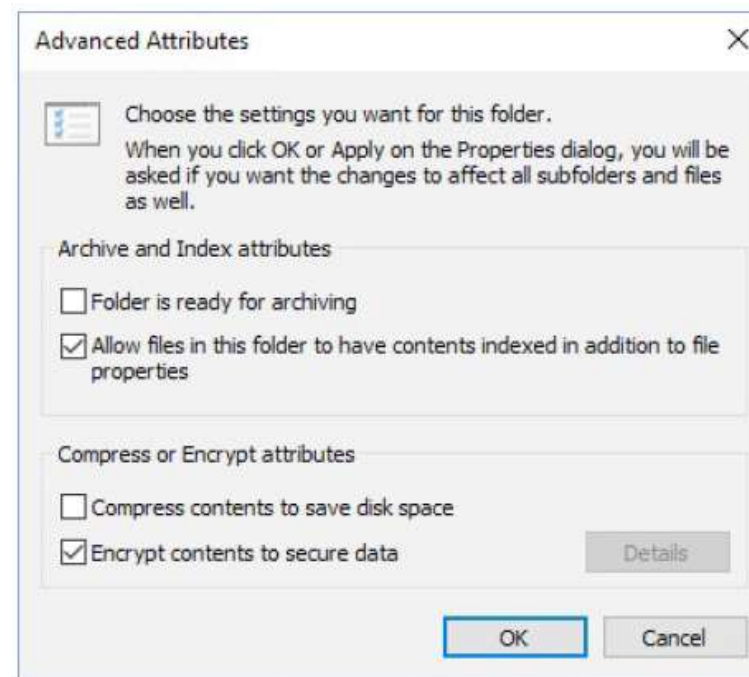
Управление дисками

Сжатие (Compression)

Сжатие позволяет сжимать файлы или папки, что в свою очередь позволяет более эффективно использовать пространство на жестком диске. Например, файл, который обычно занимает 20 МБ пространства, может использовать только 13 МБ после сжатия. Чтобы включить сжатие, просто нажмите кнопку [Другие](#) во вкладке [Общие](#) в свойствах папки и установите флажок [Сжимать содержимое для экономии места на диске](#).

Шифрование (EFS) (Encryption)

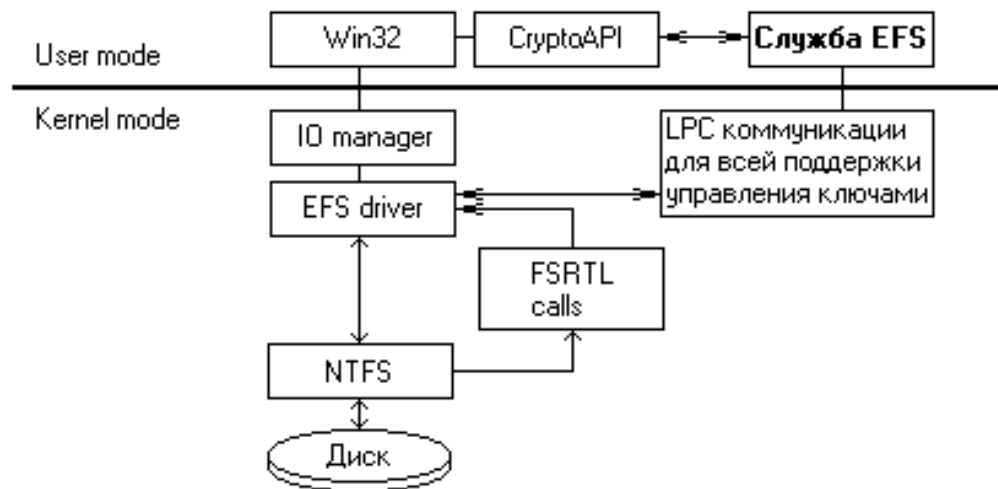
Шифрование позволяет пользователю или администратору защищать файлы или папки с помощью шифрования. Шифрование использует идентификатор безопасности пользователя (SID) для защиты файла или папки. Чтобы реализовать шифрование, откройте диалоговое окно [Другие...](#) для папки и установите флажок [Шифровать содержимое для защиты данных](#)



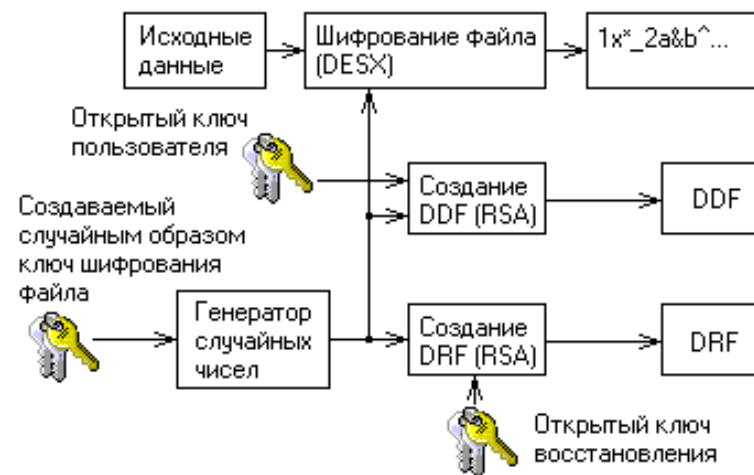


ШИФРУЮЩАЯ ФАЙЛОВАЯ СИСТЕМА

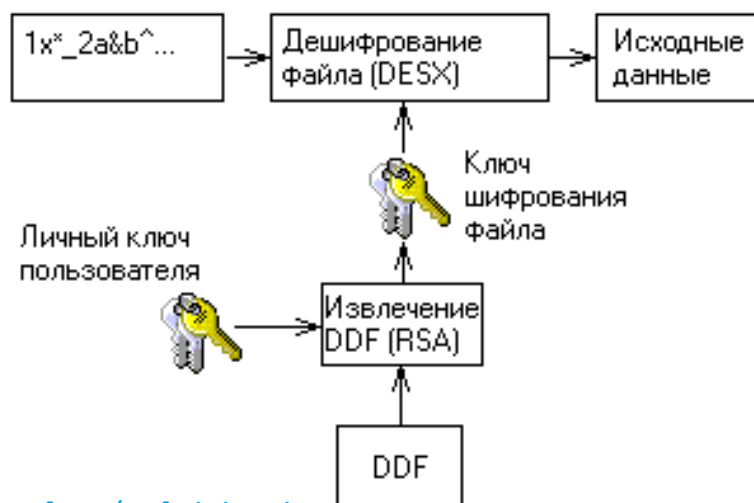
Реализация в Windows



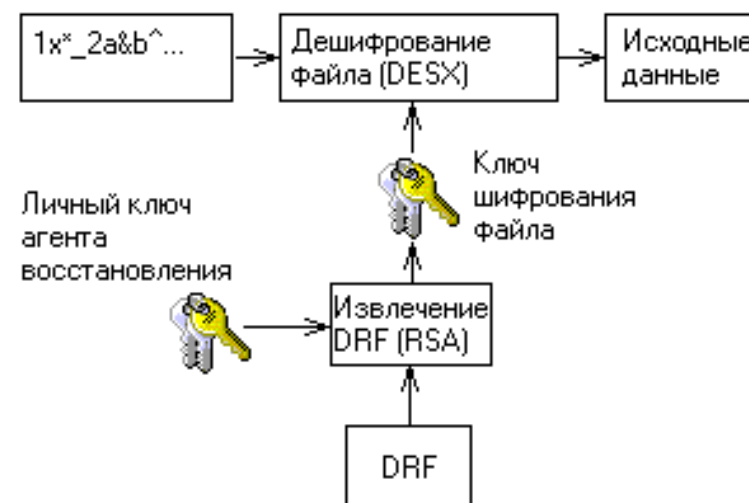
Процесс шифрования



Процесс дешифрования



Процесс восстановления





Управление дисками

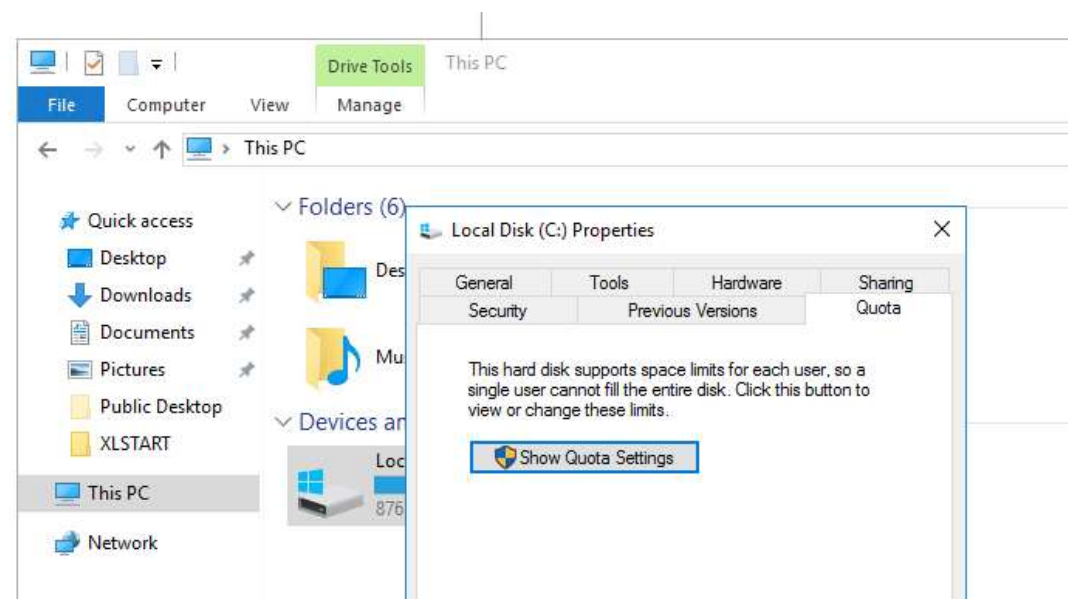
Квоты (Quotas Disk)

Квоты дают администраторам возможность ограничить объем пространства на диске, который пользователь может использовать. У вас есть несколько вариантов, доступных при настройке дисковых квот. Вы можете настроить дисковые квоты на основе томов или пользователей.

Установка квот по объему. Один из способов настройки дисковых квот – это установить квоту по объему на основе значений, которые будут использоваться по-умолчанию. Это означает, что если у вас есть жесткий диск с томами C:, D: и E: вам нужно настроить три отдельных квоты (по одному для каждого тома). Таким образом вы устанавливаете общую квоту диска на основе тома для всех пользователей.

Настройка квот для пользователя. Так же есть возможность настроить квоты на томах индивидуально для каждого пользователя. При этом вы можете индивидуально разрешить пользователям иметь независимые квоты, превышающие общую квоту, настроенную для тома.

Создание шаблонов квот. Шаблоны – это predetermined способы настройки квот. Шаблоны позволяют настраивать дисковые квоты без необходимости создания дисковой квоты с нуля.





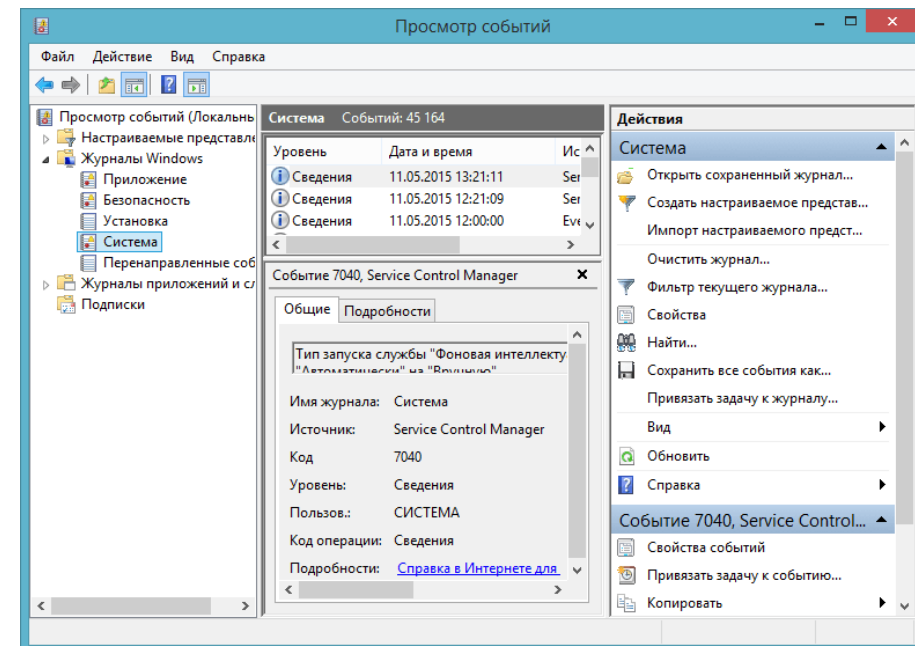
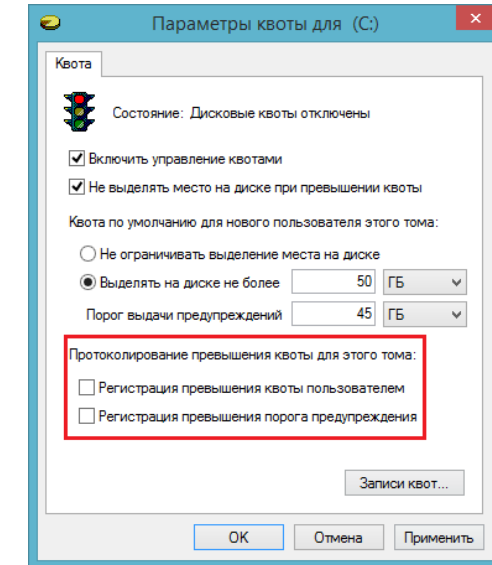
Управление дисками

Квоты (Quotas Disk)

При превышении своей дисковой квоты пользователь увидит сообщение о нехватке места, при этом он больше не сможет записывать новые данные на этот диск до тех пор, пока не освободит дисковое пространство, очистив корзину, удалив ненужные файлы, программы и т.д.

Если необходимо, чтобы операционная система записывала каждое событие квот, тогда включите параметры «Регистрация превышения квоты пользователем» и «Регистрация превышения порога предупреждения» в окне «Параметры квоты».

Для того чтобы все сделанные вами настройки были сохранены, нажмите «Применить». Когда Windows попросит вас подтвердить еще раз, что вы действительно хотите включить дисковые квоты, нажмите ОК





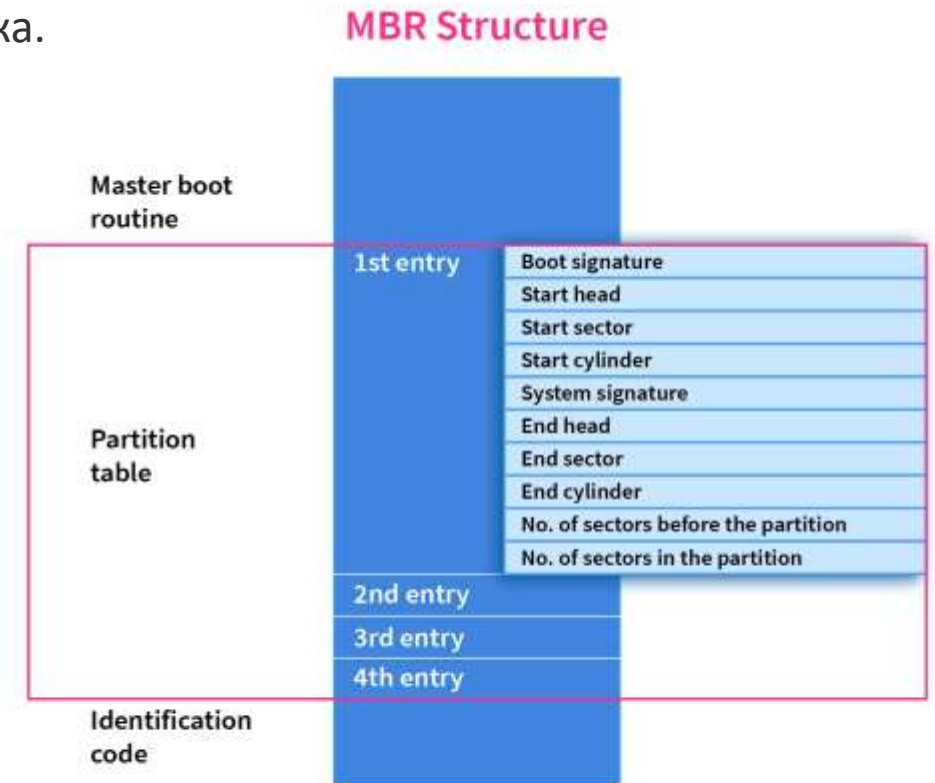
Управление дисками

Прежде чем использовать диск, его необходимо разбить на разделы. **MBR** (*Главная загрузочная запись*) и **GPT** (*Таблица разделов GUID*) представляют собой два различных способа хранения информации о разделах диска.

MBR

Аббревиатура **MBR** расшифровывается как *Главная загрузочная запись*. **MBR** – это специальный загрузочный сектор, расположенный в начале диска. Этот сектор содержит загрузчик для установленной операционной системы, а так же информацию о логических разделах диска. Загрузчик – это небольшой кусок кода, который обычно используется для загрузки большого загрузчика с другого раздела или диска.

MBR работает с дисками объемом до 2 ТБ, но он может справиться и с дисками большего размера. Кроме этого MBR поддерживает не более 4 основных разделов. Если вам нужно больше, придется сделать один из основных разделов *расширенным разделом* и разместить в нем логические разделы.





Типы дисков и стили разделов

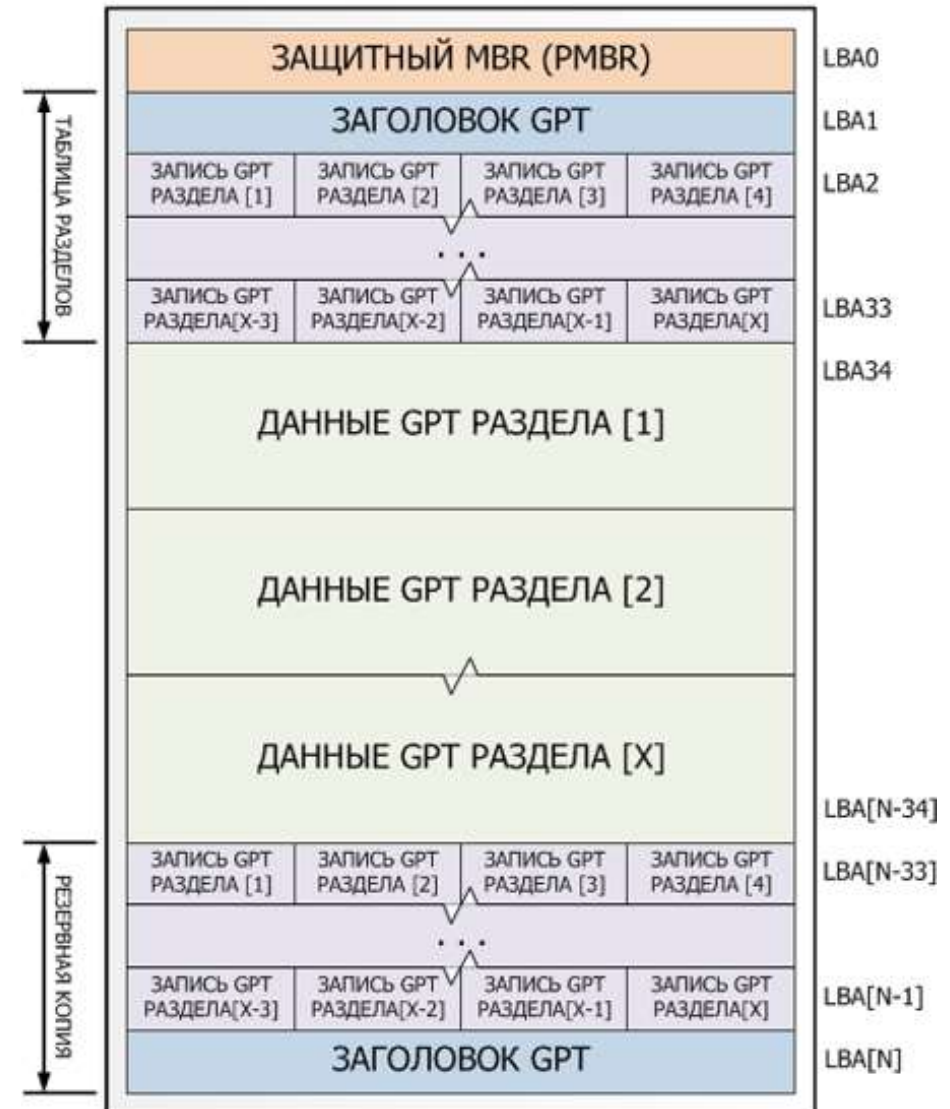
Преимущества GPT

GPT означает *Таблица разделов GUID*. Это новый стандарт, который постепенно приходит на смену MBR.

Он является частью UEFI, а UEFI заменяет старый неудобный BIOS так же, как GPT заменяет MBR на что-то более современное.

Он называется таблицей разделов GUID, поскольку каждому разделу на вашем диске присваивается *уникальный глобальный идентификатор* или **GUID**.

У этой системы нет ограничений в отличие от MBR. Диски могут быть гораздо объемнее, а ограничение на размер будет зависеть от операционной и файловой систем. GPT позволяет создавать практически неограниченное количество разделов



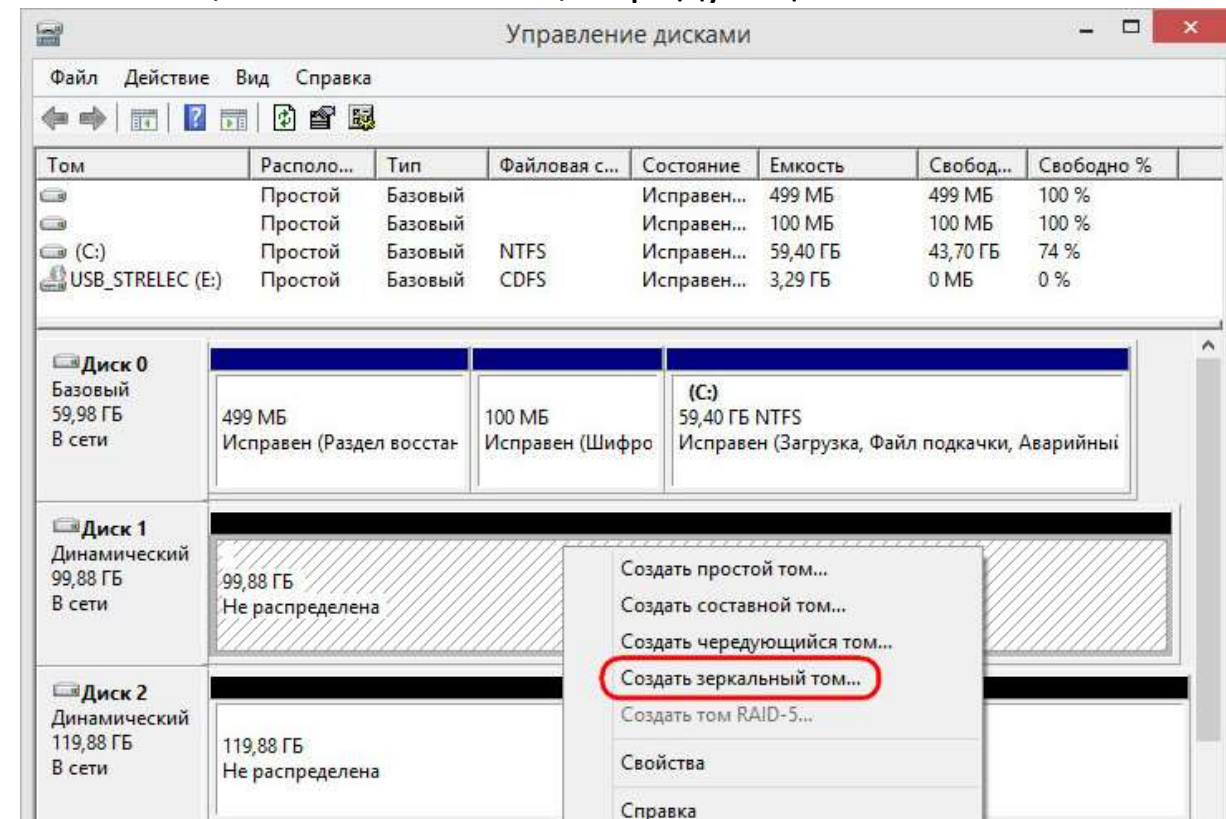


Управление дисками

Динамические диски

Динамическое диски – это возможность Windows, позволяющая на базе динамического диска, создать динамические тома. Динамические тома не могут содержать разделы или логические диски. Динамические диски поддерживают несколько типов динамических томов: простые тома, составные тома, чередующиеся тома и зеркальные тома.

Динамические диски также поддерживает резервный массив независимых дисков (RAID). Чтобы настроить динамическое хранилище, вы конвертируете или обновляете базовый диск до динамического диска. При преобразовании базового диска в динамический, вы не теряете никаких данных. После преобразования диска любые разделы, существующие на базовом диске, преобразуются в динамические простые тома, и затем вы можете создавать любые дополнительные динамические тома, необходимые на динамическом диске. Создать динамические диски можно с помощью оснастки Windows **Управление дисками (Disk Management)**.





Управление дисками

Простые тома

Простой том содержит пространство от одного динамического диска. Это пространство может быть смежным или несмежным. Простые тома используются, когда у вас достаточно места на одном диске для хранения всего тома.

Составные тома

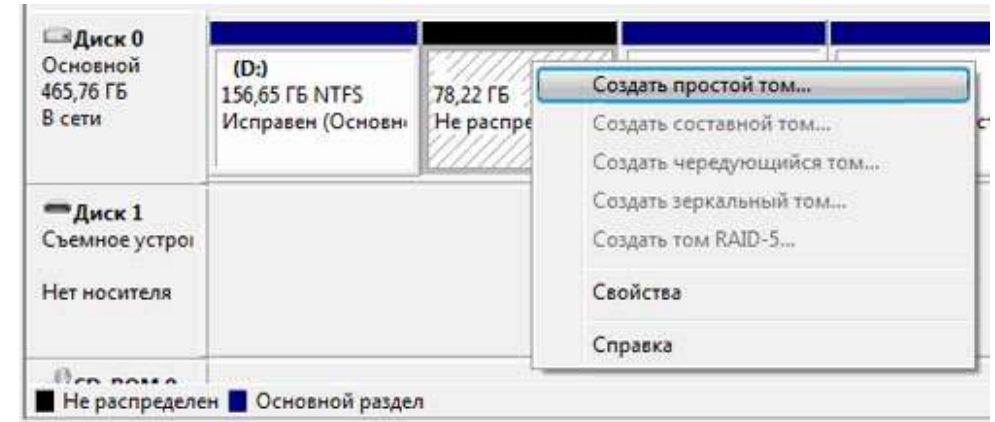
Составной том состоит из дискового пространства на двух или более динамических дисках (максимум до 32 динамических дисков). Составные тома используются для динамического увеличения размера динамического тома. Когда вы используете составной том, данные записываются последовательно, заполняя пространство на одном физическом диске, а затем пространство на следующем физическом диске.

Чередующиеся тома

Чередующийся том хранит данные в равных частях между двумя или более (до 32) динамическими дисками. Поскольку данные записываются поочередно в равных частях на каждый диск, вы можете воспользоваться значительно меньшим временем, затрачиваемым на несколько операций ввода-вывода и увеличить скорость чтения и записи данных.

Зеркальные тома

Том чередующийся с контролем четности





ОБЛАЧНЫЕ ХРАНИЛИЩА

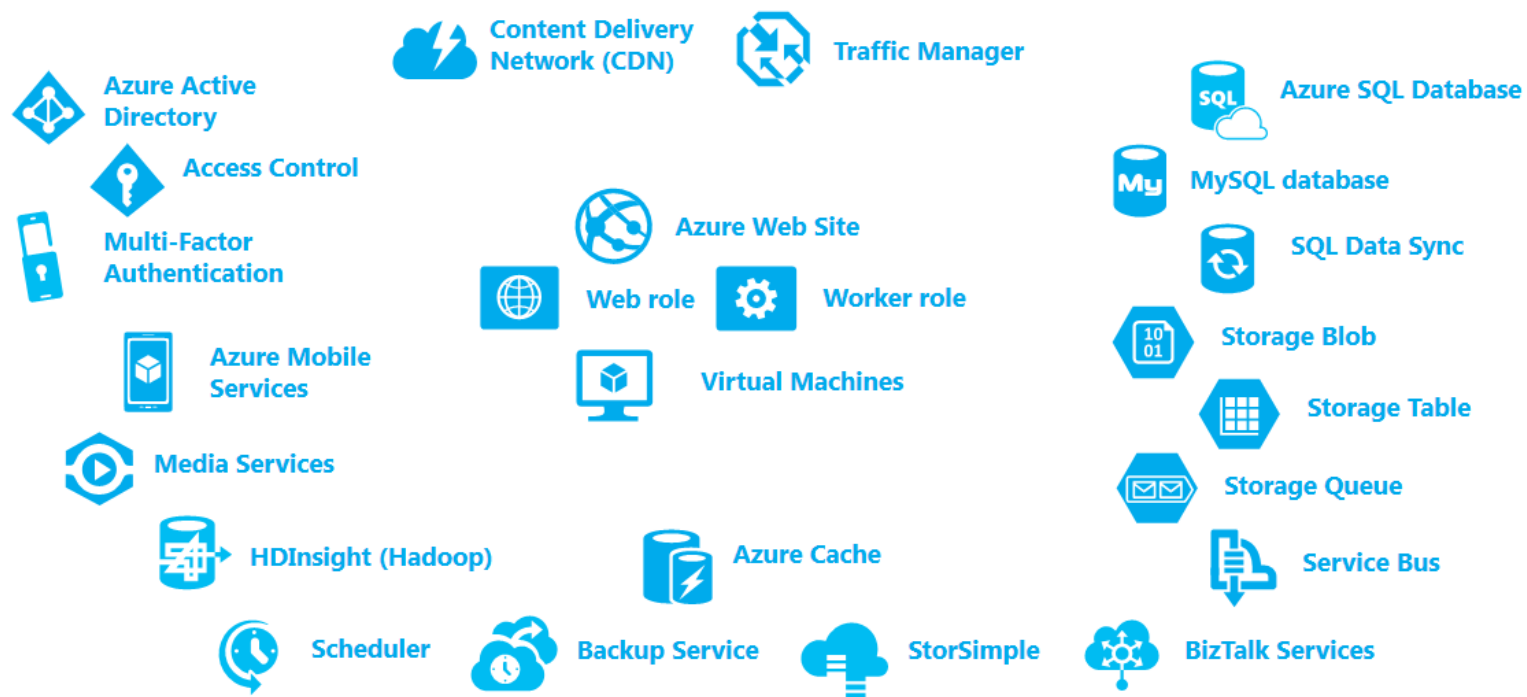
Microsoft Azure и Microsoft OneDrive

Microsoft Azure упрощает хранение документов в облаке, используя портал Azure. Портал – это интерфейс, при помощи которого пользователи и ИТ-специалисты могут контролировать и управлять тем, как данные хранятся в облаке.

Портал Azure позволяет вам выполнить следующие действия:

- загрузка и выгрузка данных в/из Azure;
- запуск отчетов, показывающих фактическое использование каждого файла;
- изменение размеров квот ваших пользователей.

Microsoft Azure Cloud Platform





ОБЛАЧНЫЕ ХРАНИЛИЩА

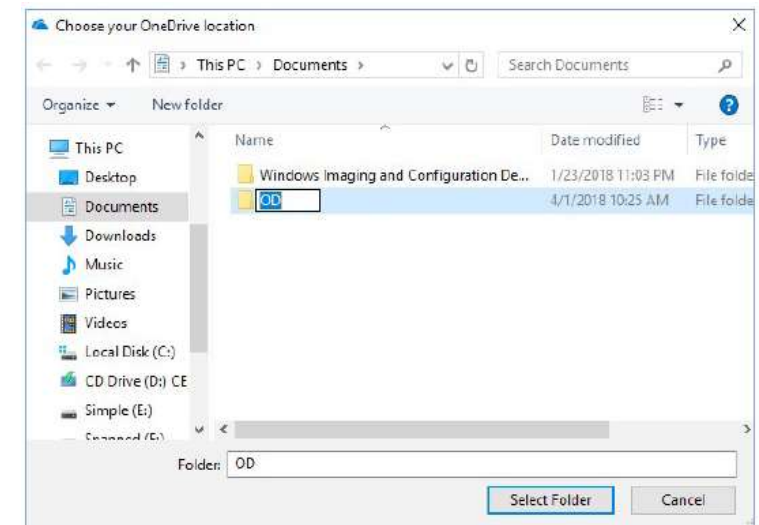
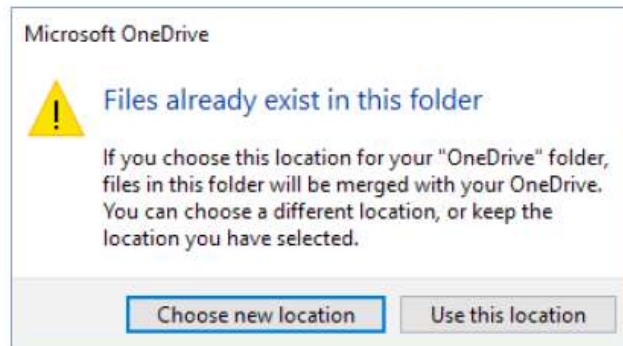
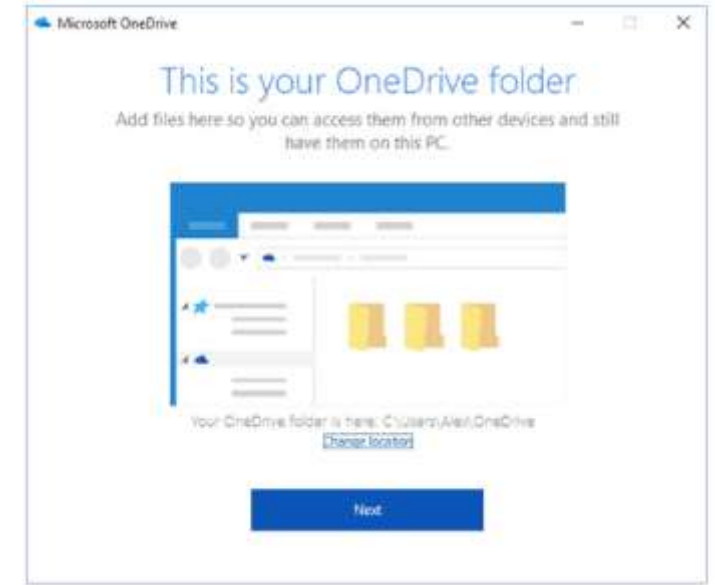
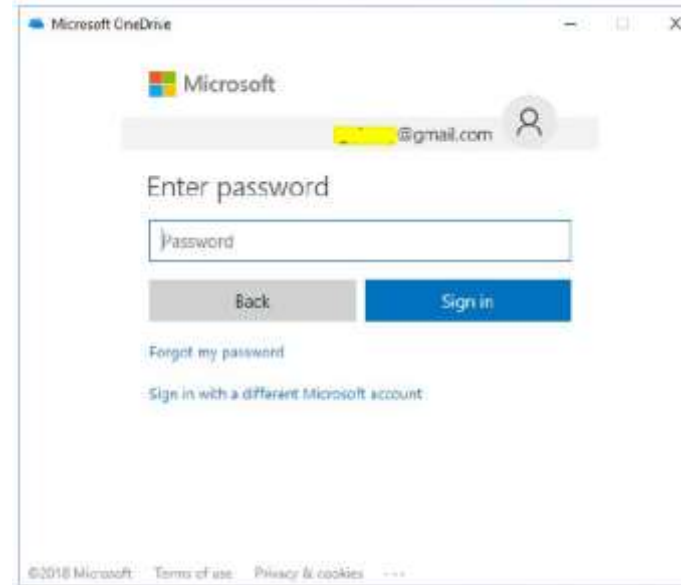
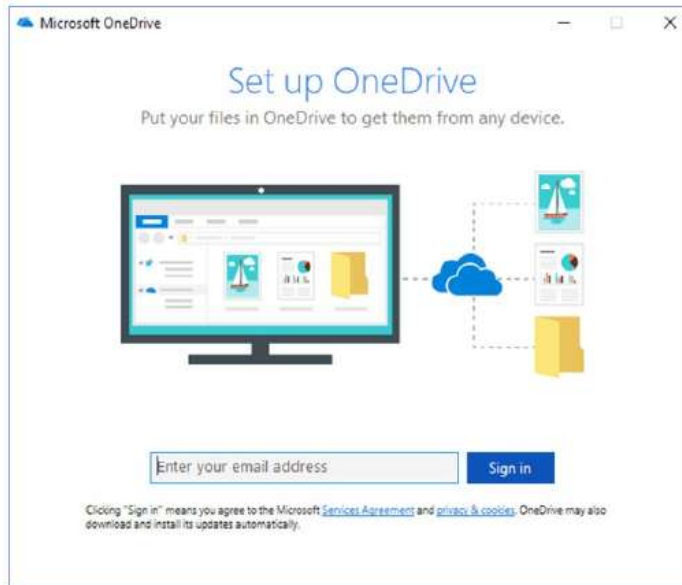
Microsoft OneDrive является облачной подпиской на хранилище, поэтому домашние пользователи могут хранить свои документы, а затем получать доступ к этим документам из любой точки мира.

OneDrive был разработан для среднестатистического домашнего пользователя, который хочет хранить данные в безопасной, защищенной облачной среде. OneDrive, когда он был впервые выпущен, также позиционировался для использования в корпоративных средах, но с появлением Windows Azure, OneDrive стал более **домашним** решением.

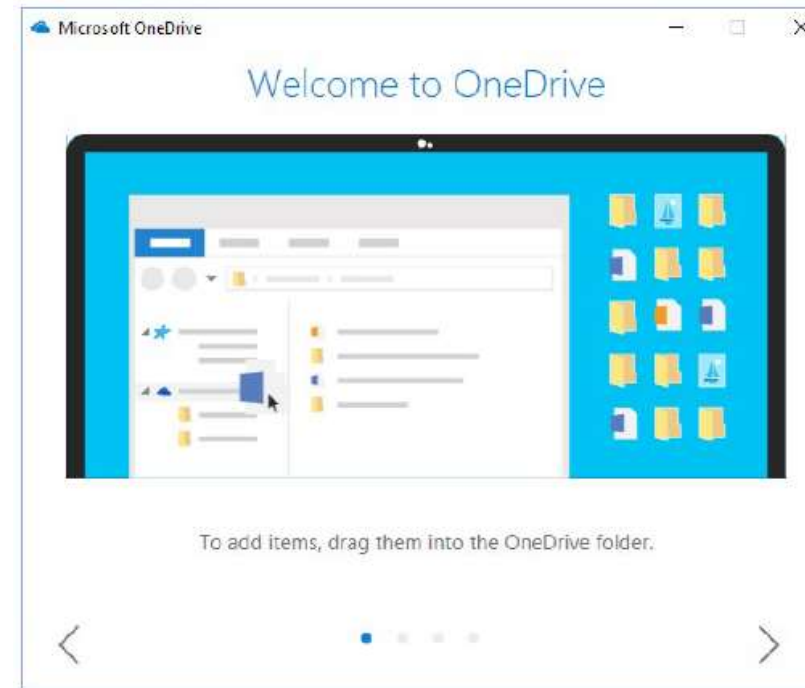
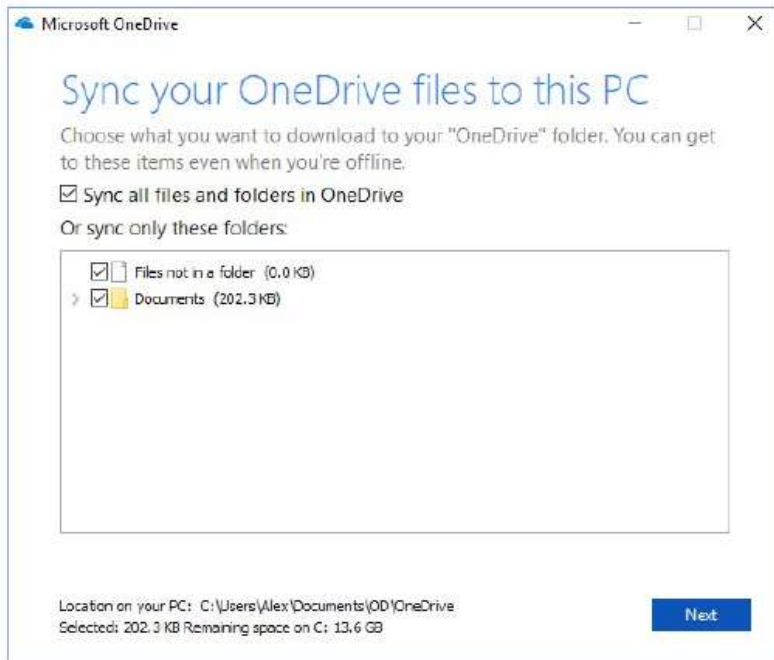
Файлы по требованию (*On-Demand*) — функция безопасности, которая позволяет вам обращаться к файлам без необходимости их загрузки. И поскольку данные хранятся в облаке, OneDrive также работает, как механизм восстановления данных, если ваш ноутбук сломался или был украден/утерян.



Установка OneDrive



Установка OneDrive



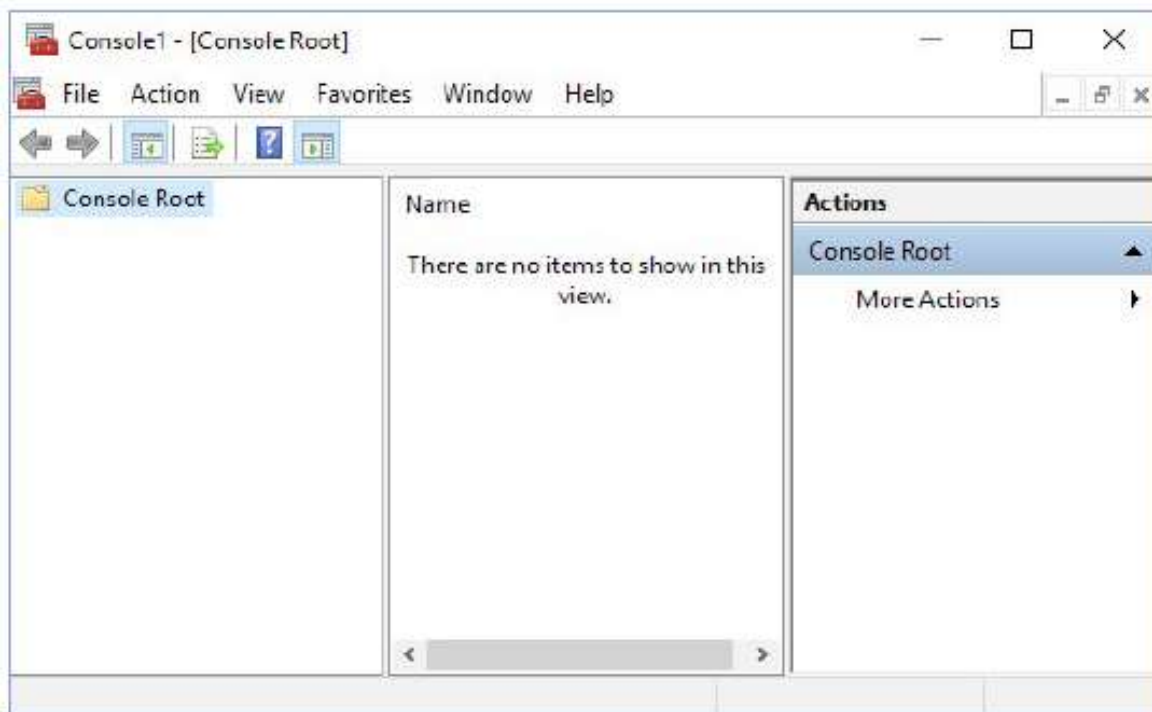
Documents

3/31/2018 12:24 PM File folder



консоль управления Microsoft

Консоль управления Microsoft (MMC) – это консольная среда для управления приложениями. MMC обеспечивает общую среду для оснасток. **Оснастки (Snap-ins)** – это административные инструменты, разработанные Microsoft или сторонними поставщиками. Примеры оснасток MMC, которые вы можете использовать, – это [Управление компьютером](#), [Управление печатью](#) и т. д.



MMC предлагает множество преимуществ:

- ■ MMC очень настраиваема – вы добавляете только оснастки, которые вам нужны;
- ■ оснастки используют стандартный интуитивно понятный интерфейс, поэтому они проще в использовании, чем предыдущие версии административных утилит;
- ■ вы можете сохранить настроенные MMC и поделиться ими с другими администраторами;
- ■ вы можете настроить разрешения, чтобы MMC работал в авторском режиме, который дает административные права на управление оснасткой, или в пользовательском режиме, который ограничивает возможности пользователей;
- ■ вы можете использовать большинство оснасток для удаленного управления компьютером.



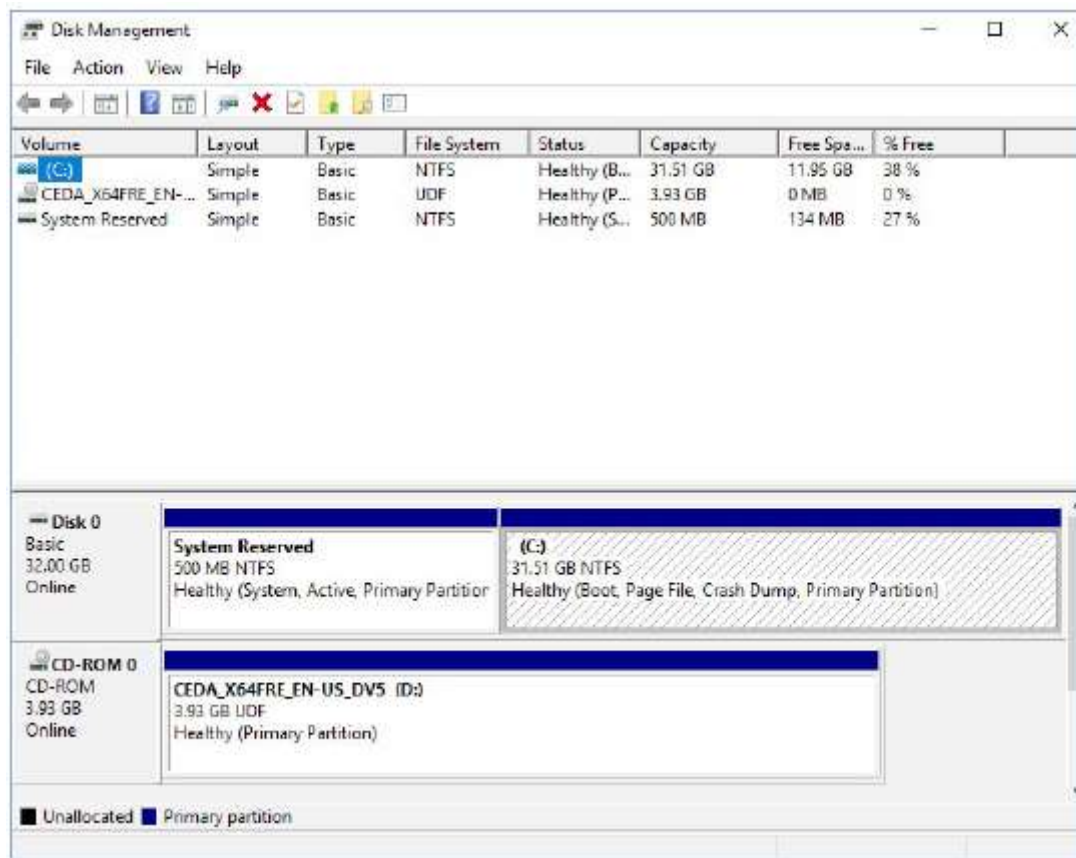
консоль управления Microsoft

Настройка режимов MMC

РЕЖИМ КОНСОЛИ	ОПИСАНИЕ
Авторский режим	Позволяет использовать все функции без ограничений
Пользовательский: полный доступ	Не позволяет пользователю добавлять или удалять оснастки или изменять свойства консоли. Пользователи имеют полный доступ к дереву
Пользовательский: ограниченный, многооконный	Предотвращает доступ пользователей к участкам дерева, не видимым в окне консоли оснастки
Пользовательский: ограниченный, однооконный	Открывает консоль в режиме одного окна и предотвращает доступ пользователей к участкам дерева, не видимым в окне консоли ос-

Возможно настроить MMC для запуска в авторском режиме для полного доступа к функциям MMC или в одном из трех пользовательских режимов, которые имеют более ограниченный доступ к функциям MMC. Чтобы настроить консольный режим, в редакторе MMC выберите [Параметры файла](#), чтобы открыть диалоговое окно [Параметры](#). В этом диалоговом окне вы можете выбрать из режимов консоли

Управление дисками



Открыв оснастку **Управление дисками**, вы получите доступ к следующей информации:

- тома, которые инициализированы компьютером;
- тип диска, базовый или динамический;
- тип файловой системы, используемой каждым разделом;
- состояние раздела и содержит ли он системный или загрузочный раздел;
- емкость (объем пространства), выделенная для раздела;
- объем оставшегося свободного места, после создания разделов или томов;
- объем служебных данных, связанных с разделом.



Управление дисками

Windows 10 также включает в себя консольную утилиту **Diskpart**, которая может использоваться как альтернатива графической утилите [Управление дисками](#).

Вы можете просмотреть все параметры, связанные с утилитой Diskpart, набрав Diskpart в командной строке, запущенной от имени администратора и затем набрав ? В приглашении Diskpart

```
Administrator: Command Prompt - diskpart
C:\Windows\system32>diskpart

Microsoft DiskPart version 10.0.15063.0

Copyright (C) Microsoft Corporation.
On computer: DESKTOP-JGH6LE3

DISKPART> ?

Microsoft DiskPart version 10.0.15063.0

ACTIVE          - Mark the selected partition as active.
ADD             - Add a mirror to a simple volume.
ASSIGN          - Assign a drive letter or mount point to the selected volume.
ATTRIBUTES      - Manipulate volume or disk attributes.
ATTACH          - Attaches a virtual disk file.
AUTOMOUNT       - Enable and disable automatic mounting of basic volumes.
BREAK          - Break a mirror set.
CLEAN           - Clean the configuration information, or all information, off the
                  disk.
COMPACT         - Attempts to reduce the physical size of the file.
CONVERT         - Convert between different disk formats.
CREATE          - Create a volume, partition or virtual disk.
DELETE         - Delete an object.
DETAIL         - Provide details about an object.
DETACH         - Detaches a virtual disk file.
EXIT           - Exit DiskPart.
EXTEND         - Extend a volume.
EXPAND         - Expands the maximum size available on a virtual disk.
FILESYSTEMS     - Display current and supported file systems on the volume.
FORMAT         - Format the volume or partition.
GPT            - Assign attributes to the selected GPT partition.
HELP           - Display a list of commands.
IMPORT         - Import a disk group.
INACTIVE       - Mark the selected partition as inactive.
LIST           - Display a list of objects.
MERGE         - Merges a child disk with its parents.
ONLINE        - Online an object that is currently marked as offline.
OFFLINE       - Offline an object that is currently marked as online.
RECOVER       - Refreshes the state of all disks in the selected pack.
                  Attempts recovery on disks in the invalid pack, and
                  resynchronizes mirrored volumes and RAID5 volumes
                  that have stale plex or parity data.
REM           - Does nothing. This is used to comment scripts.
REMOVE        - Remove a drive letter or mount point assignment.
REPAIR        - Repair a RAID-5 volume with a failed member.
RESCAN       - Rescan the computer looking for disks and volumes.
RETAIN       - Place a retained partition under a simple volume.
SAM          - Display or set the SAM policy for the currently booted OS.
SELECT       - Shift the focus to an object.
SETID        - Change the partition type.
SHRINK       - Reduce the size of the selected volume.
UNIQUEID     - Displays or sets the GUID partition table (GPT) identifier or
                  master boot record (MBR) signature of a disk.
```




Управление дисками

Процесс создания раздела на базовом диске.

Для получения списка дисков используется команда: **list disk** В результате получаем список дисков, присутствующих в системе:

```
Administrator: Command Prompt - diskpart
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Windows\system32>diskpart

Microsoft DiskPart version 10.0.15063.0

Copyright (C) Microsoft Corporation.
On computer: DESKTOP-JGH6LE3

DISKPART> list disk

Disk ###  Status       Size       Free       Dyn  Gpt
-----  -
Disk 0    Online      32 GB      0 B
Disk 1    Online      500 MB     498 MB
Disk 2    Online      500 MB     498 MB

DISKPART>
```

Для выбора какого-либо из них для дальнейших операций, используется команда SELECT: **select disk 1** – выбрать второй диск. В списке объектов (в данном случае – дисков), получаемом по команде LIST, выбранный объект отмечается звездочкой.

```
Administrator: Command Prompt - diskpart

DISKPART> select disk 1

Disk 1 is now the selected disk.

DISKPART> detail disk

VBOX HARDDISK
Disk ID: 67105416
Type   : SATA
Status : Online
Path   : 2
Target : 0
LUN ID : 0
Location Path : PCIR00T(0)#PCI(0D00)#ATA(C02T00L00)
Current Read-only State : No
Read-only   : No
Boot Disk   : No
Pagefile Disk : No
Hibernation File Disk : No
Crashdump Disk : No
Clustered Disk : No

There are no volumes.

DISKPART> _
```



Управление дисками

Управление административными задачами жесткого диска

Утилита управления дисками позволяет выполнять различные административные задачи для жесткого диска:

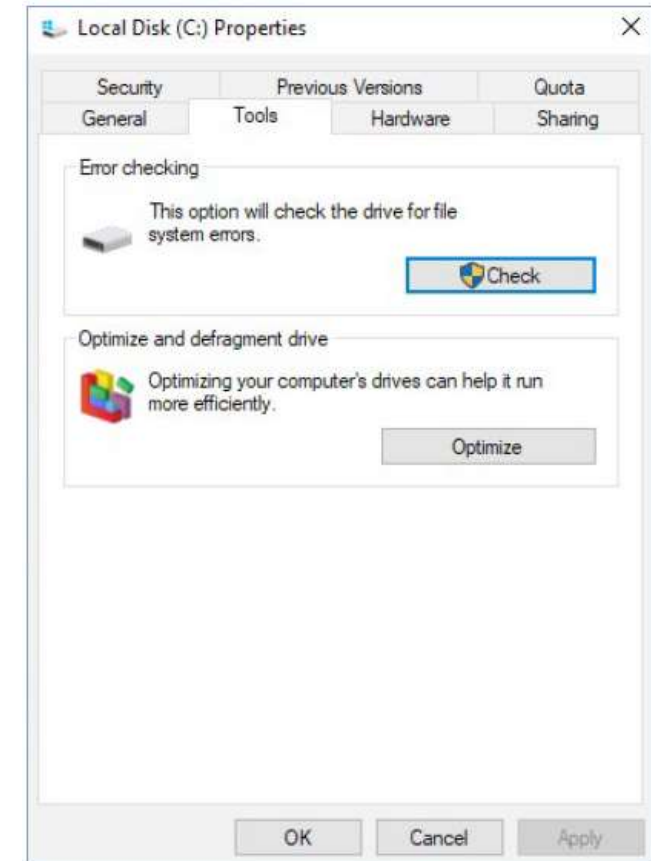
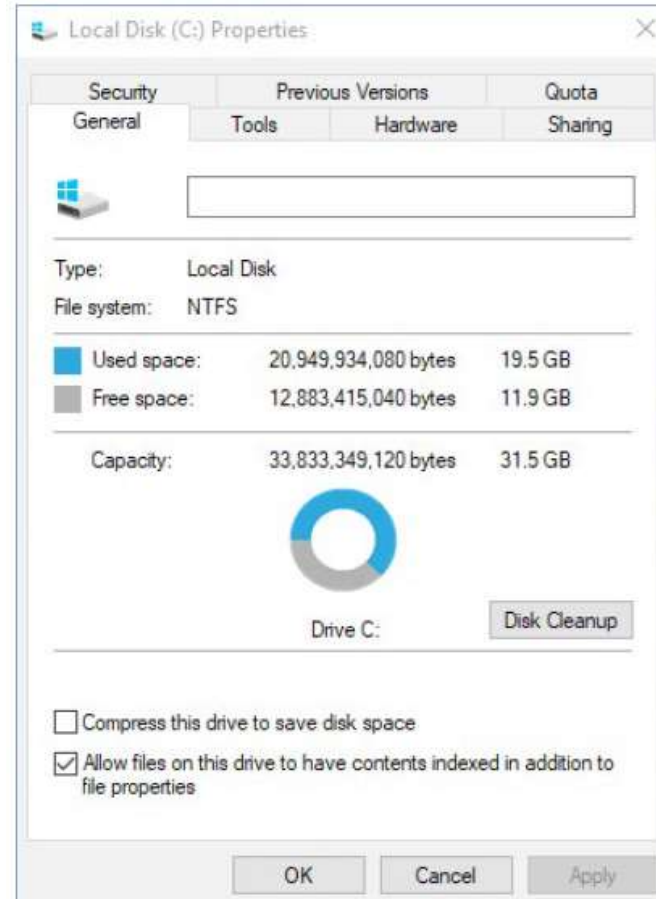
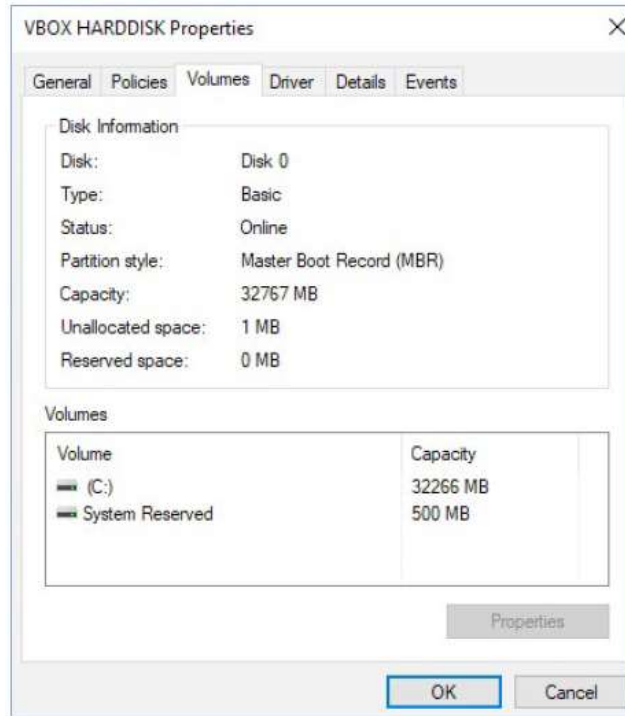
- просмотр свойств диска;
- просмотр свойств томов и разделов;
- добавление нового диска;
- создание разделов и томов;
- преобразование базового диска в динамический или GPT-диск;
- изменение буквы диска;
- изменение размера тома или раздела;
- удаление раздела или тома.

Просмотр свойств диска

Чтобы просмотреть свойства диска, щелкните правой кнопкой мыши номер диска на нижней панели главного окна **Управление дисками** и выберите **Свойства** в контекстном меню. Появится диалоговое окно **Свойства диска**. Перейдите на вкладку **Тома**, чтобы просмотреть список томов связанных с диском.

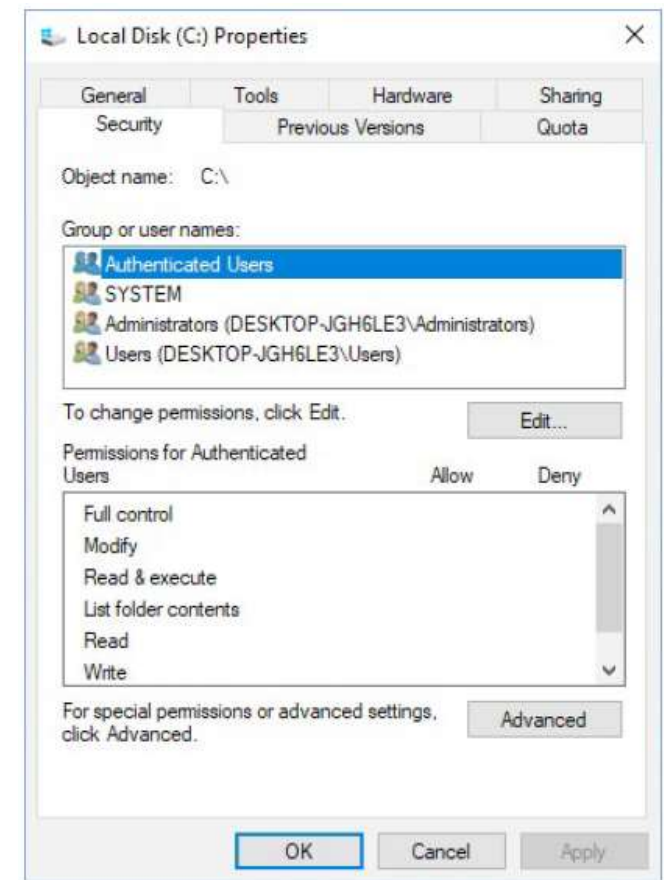
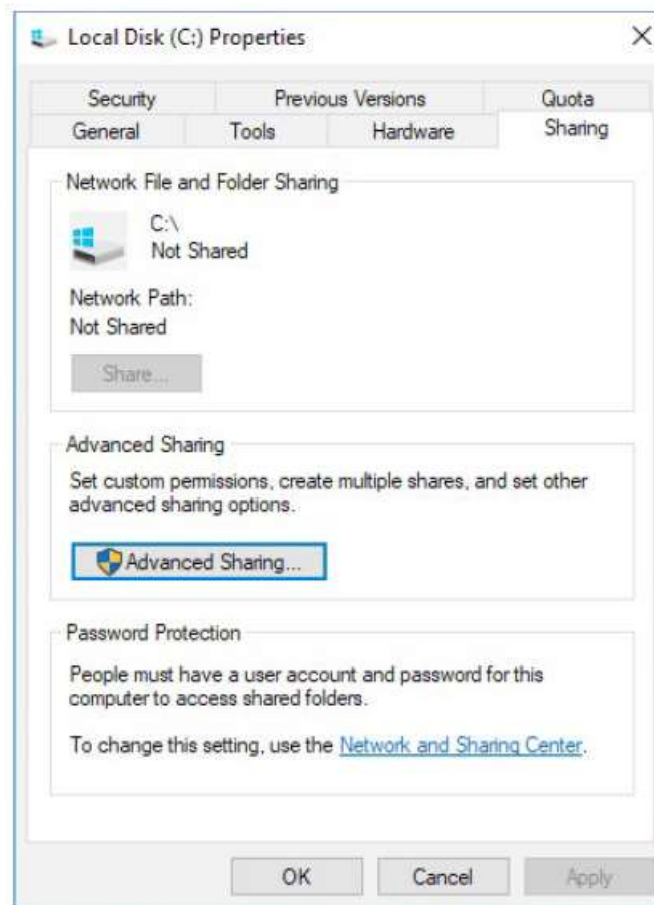
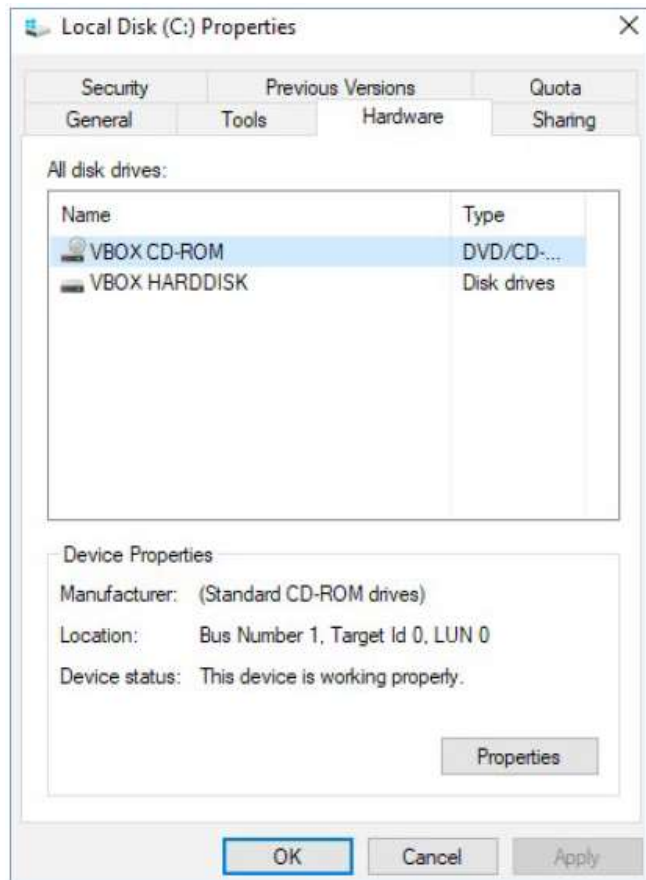
- номер диска;
- тип диска (базовый, динамический, CD-ROM, съемный, DVD или неизвестный);
- состояние диска (онлайн или офлайн);
- стиль раздела;
- емкость диска;
- объем нераспределенного пространства на диске;
- объем свободного места на диске;
- логические тома, определенные на физическом диске.

Управление дисками





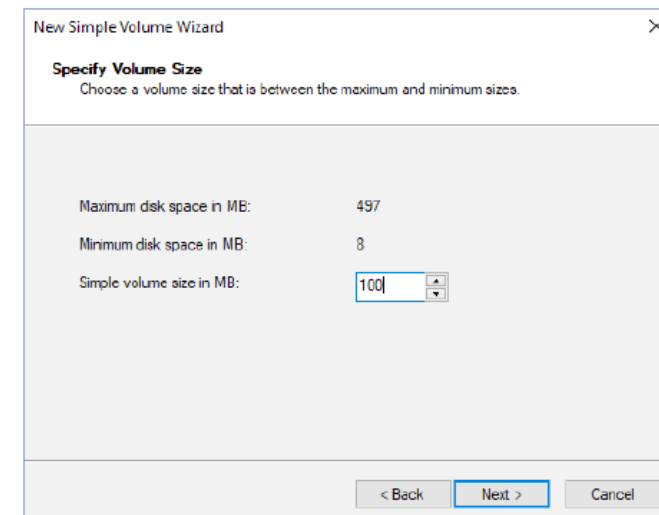
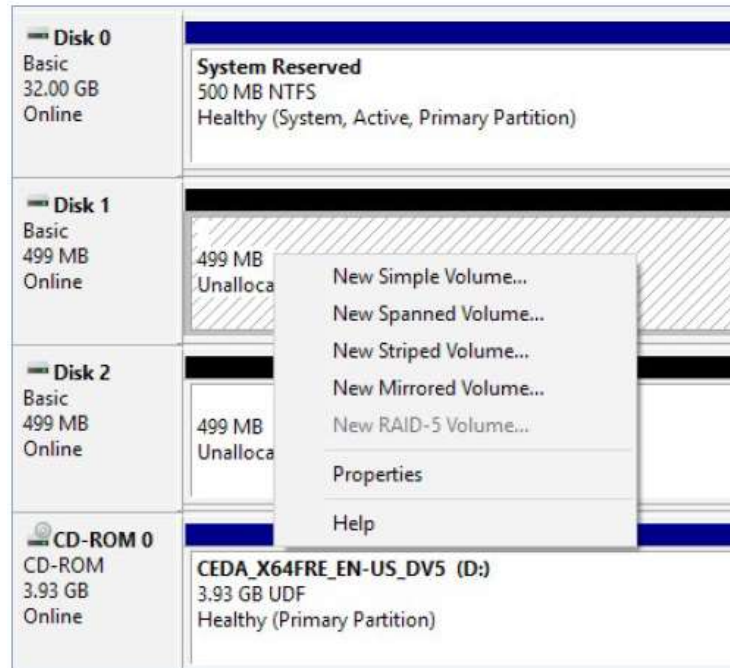
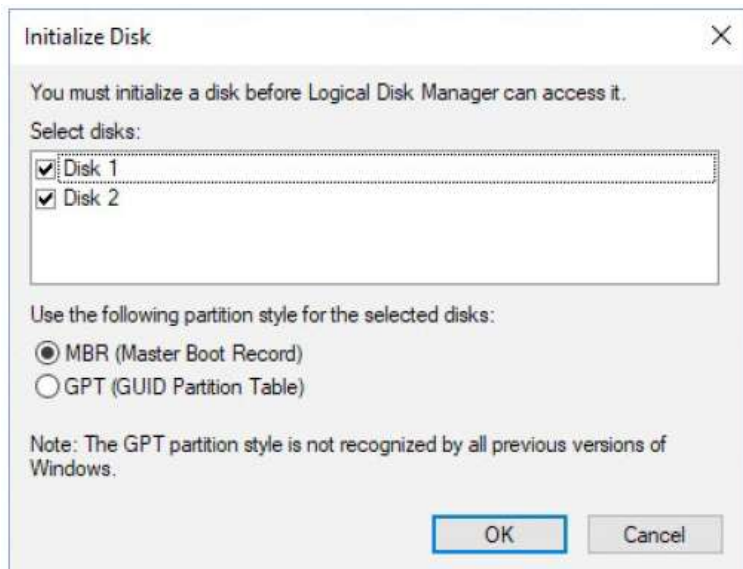
Управление дисками



Управление дисками



Создание разделов и томов





Управление дисками

Обновление базового диска на динамическом или GPT-диске

New Simple Volume Wizard




Assign Drive Letter or Path
For easier access, you can assign a drive letter or drive path to your partition.

☒ Assign the following drive letter: E

☐ Mount in the following empty NTFS folder: Browse...

☐ Do not assign a drive letter or drive path

< Back Next > Cancel

 Disk 0 Basic 32.00 GB Online	System Reserved 500 MB NTFS Healthy (System, Active, Primary Partition)	
 Disk 1 Basic 499 MB Online	New Volume (E:) 100 MB NTFS Healthy (Primary Partition)	399 MB Unallocated
 Disk 2 Basic 499 MB Online	499 MB Unallocated	

New Simple Volume Wizard

Format Partition
To store data on this partition, you must format it first.

Choose whether you want to format this volume, and if so, what settings you want to use.

☐ Do not format this volume

☒ Format this volume with the following settings:

File system: NTFS

Allocation unit size: Default

Volume label: New Volume

☒ Perform a quick format

☐ Enable file and folder compression

< Back Next > Cancel

Disk 0 Basic 32.00 GB Online	System Reserved 500 MB NTFS	(C:) 31.51 GB NTFS Healthy (Boot, Page File)
CD-ROM CD-ROM 3.93 GB Online		
Unallocated		

New Spanned Volume...
New Striped Volume...
New Mirrored Volume...
New RAID-5 Volume...
Convert to Dynamic Disk...
Convert to GPT Disk
Offline
Properties
Help

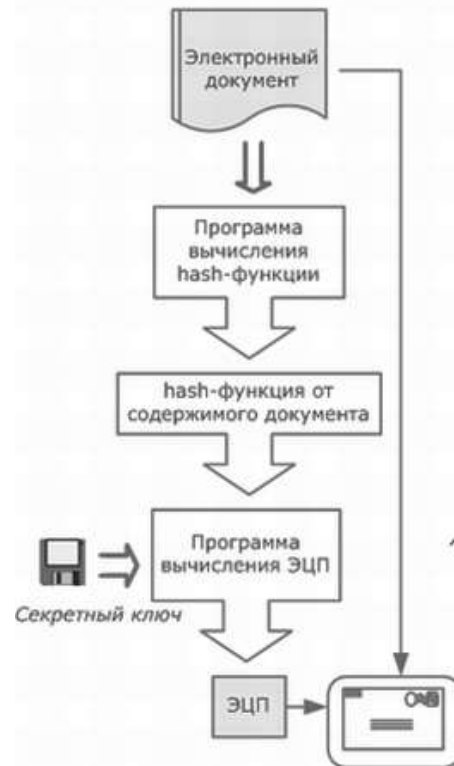
РАБОТА С ЭЛЕКТРОННОЙ ПОДПИСЬЮ



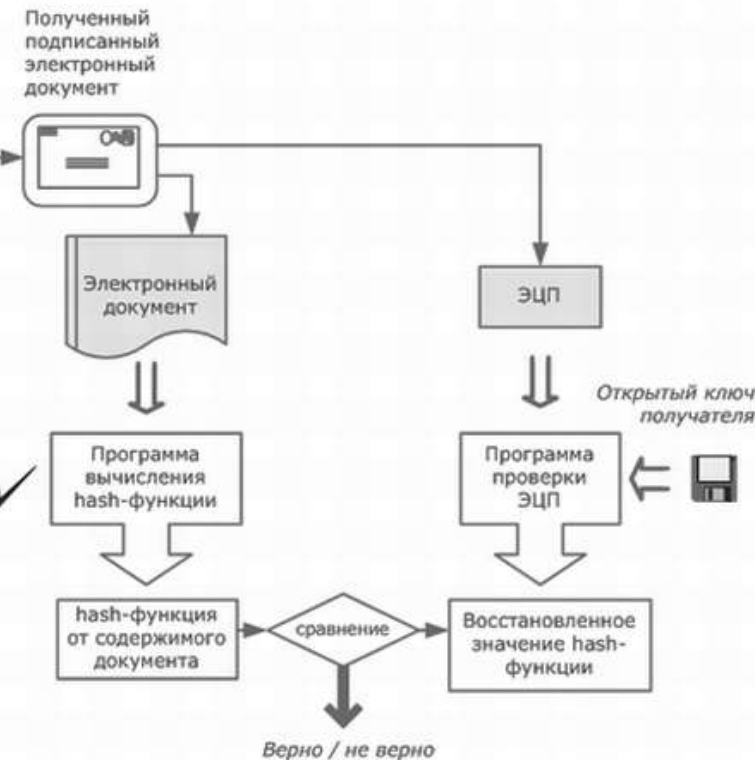
Этап 1. Подготовка ключей



Этап 2. Подписывание документа



Этап 3. Проверка подписи на документе



Есть ли в этом процессе уязвимые/слабые места?



РАБОТА с СЕРТИФИКАТАМИ

Понятие сертификата

Сертификат в общем смысле, применимо не только к компьютерам – это обычно документ, который подтверждает подлинность чего-либо, либо принадлежность объекта какому-то конкретному владельцу.

Сертификаты функционально связаны с криптографией. С точки зрения криптографии сертификат - цифровой документ, подтверждающий соответствие между открытым ключом и информацией, идентифицирующей владельца ключа. Сертификат содержит информацию о владельце ключа, сведения об открытом ключе, его назначении и области применения, название центра сертификации и т. д. Открытый ключ (сертификат) может быть использован для организации защищенного канала связи с владельцем двумя способами:

- для проверки подписи владельца (аутентификация)
- для шифрования посылаемых ему данных (конфиденциальность)



Существует две модели организации инфраструктуры сертификатов: централизованная (PKI), децентрализованная (PGP).

В централизованной модели существуют корневые центры сертификации, подписям которых обязан доверять каждый пользователь. В децентрализованной модели каждый пользователь самостоятельно выбирает, каким сертификатам он доверяет и в какой степени.



РАБОТА с СЕРТИФИКАТАМИ

В основу PGP положен стандарт [OpenPGP](#), который содержит:

- сведения о владельце сертификата;
- открытый ключ владельца сертификата;
- ЭЦП владельца сертификата;
- период действия сертификата;
- предпочтительный алгоритм шифрования.

В основу PKI положен стандарт X.509, который содержит:

- открытый ключ владельца сертификата;
- серийный номер сертификата;
- уникальное имя владельца;
- период действия сертификата;
- уникальное имя издателя;
- ЭЦП издателя и идентификатор алгоритма подписи.

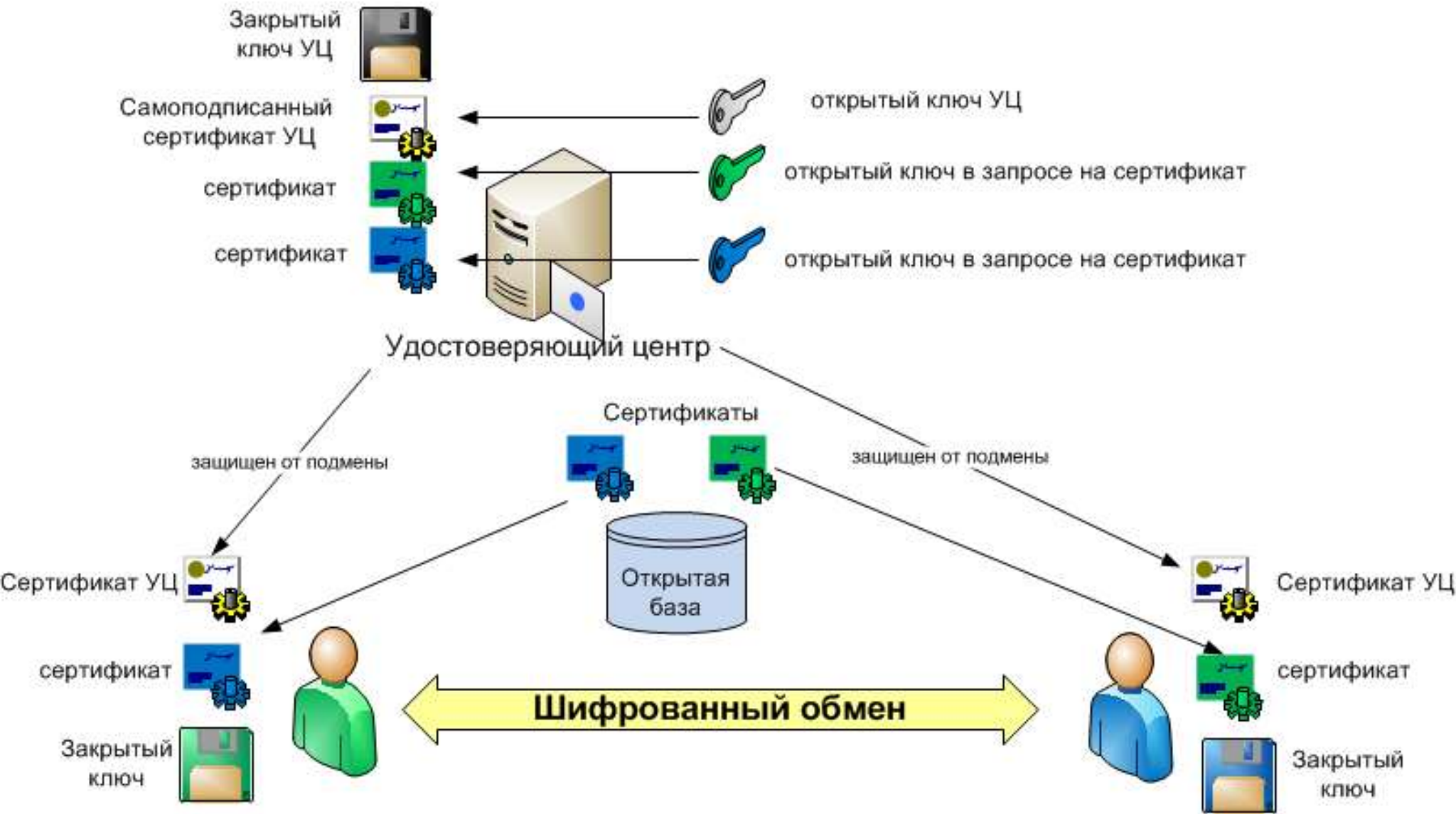
Несмотря на наличие множества версий формата X.509, существует ряд фундаментальных различий между форматами сертификатов X.509 и PGP:

сертификат PGP создается только лично (самоподписанный сертификат), сертификат X.509 может получаться от центра сертификации, а также быть самоподписанным;

сертификат X.509 содержит только одно имя владельца сертификата;

сертификат X.509 содержит только одну ЭЦП, подтверждающую подлинность сертификата.

РАБОТА С СЕРТИФИКАТАМИ





РАБОТА с СЕРТИФИКАТАМИ

Криптография с открытыми ключами основывается на:

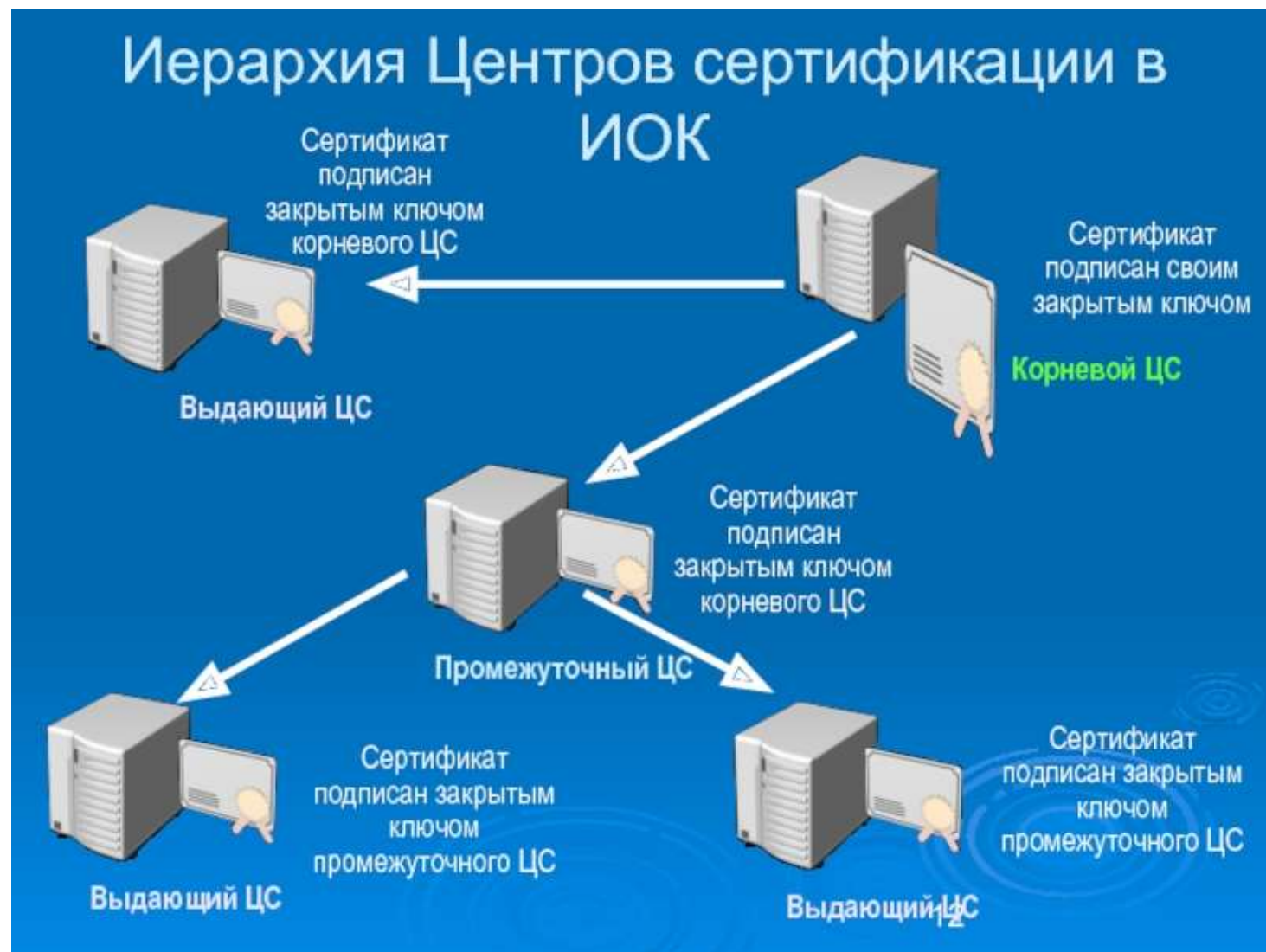
владении своим личным Секретным ключом и владении Открытым ключом получателем

Получатели используют Открытый ключ отправителя секретным ключом (для проверки)

Проблема: Как получатель может быть уверен, что открытый ключ действительно принадлежит отправителю?

Решение: Использование доверенного третьего лица для заверения Открытого ключа.

Третье лицо является Центром Сертификации или Доверенным Центром. Заверенный этим центром открытый ключ является сертификатом

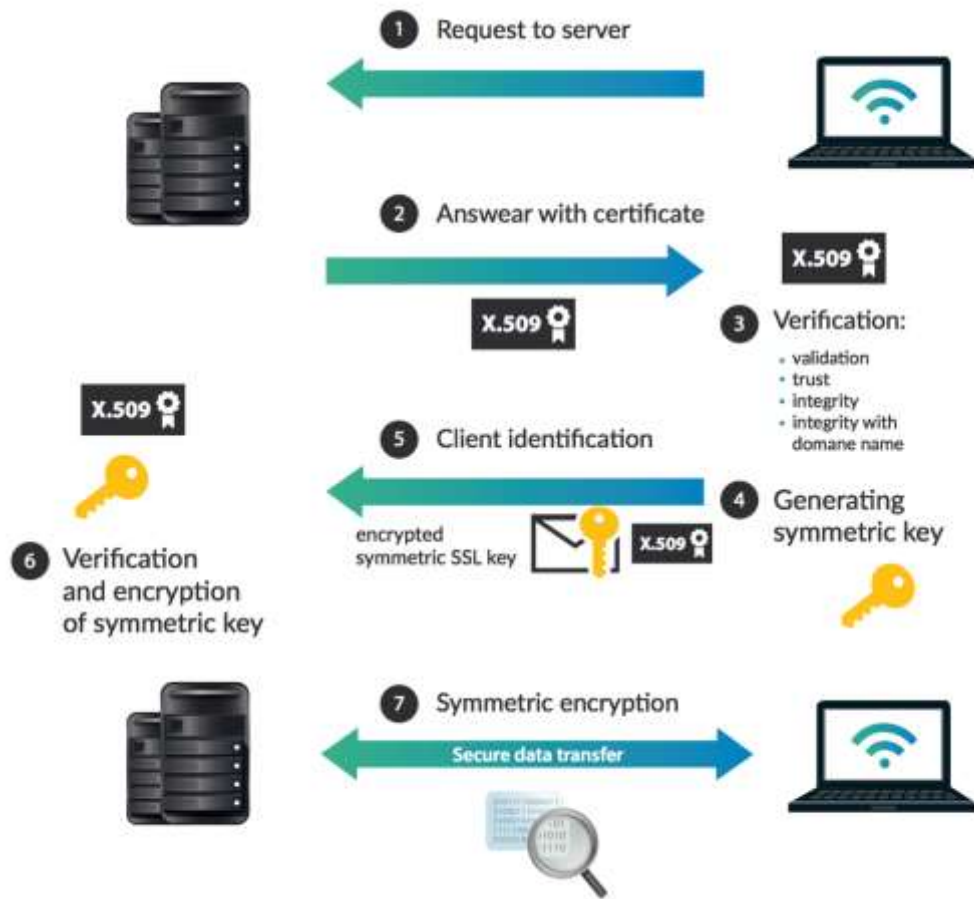


РАБОТА с СЕРТИФИКАТАМИ



SSL сертификаты

SSL (*Secure Sockets Layer* — уровень защищённых [сокетов](#)) — криптографический протокол, который подразумевает безопасную связь. Он использует асимметричную криптографию для аутентификации ключей обмена, симметричное шифрование для сохранения конфиденциальности, коды аутентификации сообщений для целостности сообщений.



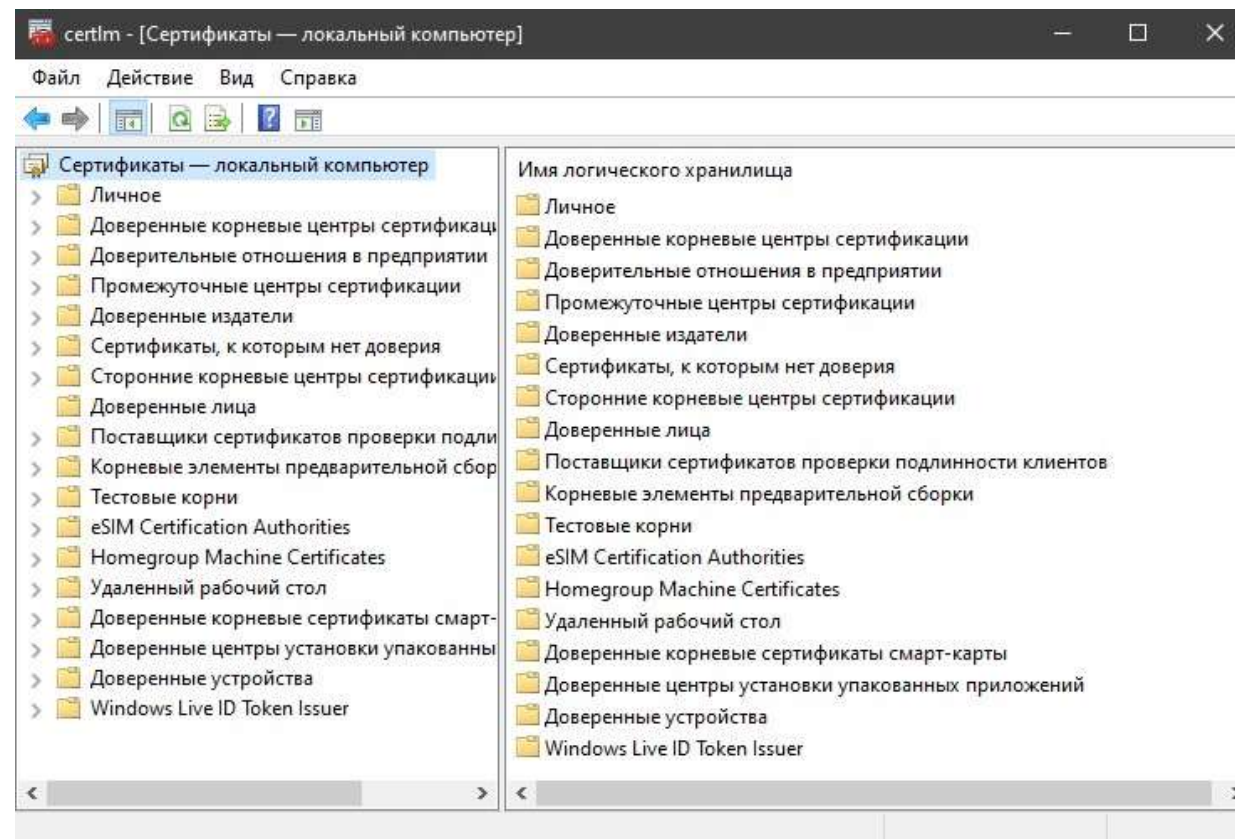
1. Браузер или сервер пытается подключиться к веб-сайту (веб-серверу), защищенному с помощью SSL.
2. Браузер или сервер запрашивает идентификацию у веб-сервера.
3. В ответ веб-сервер отправляет браузеру или серверу копию своего SSL-сертификата.
4. Браузер или сервер проверяет, является ли этот SSL-сертификат доверенным. Если это так, он сообщает об этом веб-серверу.
5. Затем веб-сервер возвращает подтверждение с цифровой подписью и начинает сеанс, зашифрованный с использованием SSL.
6. Зашифрованные данные используются совместно браузером или сервером и веб-сервером.



РАБОТА с СЕРТИФИКАТАМИ В ОС

Certmgr.msc является оснасткой консоли управления Microsoft, тогда как Certmgr.exe является утилитой командной строки.

Используя диспетчер сертификатов, вы можете запросить новый сертификат с тем же ключом или другим ключом. Вы также можете экспортировать или импортировать сертификат. Чтобы выполнить какое-либо действие, выберите сертификат, щелкните меню «Действие» > «Все задачи», а затем щелкните нужную команду действия. Вы также можете щелкнуть правой кнопкой мыши контекстное меню, чтобы выполнить эти действия.



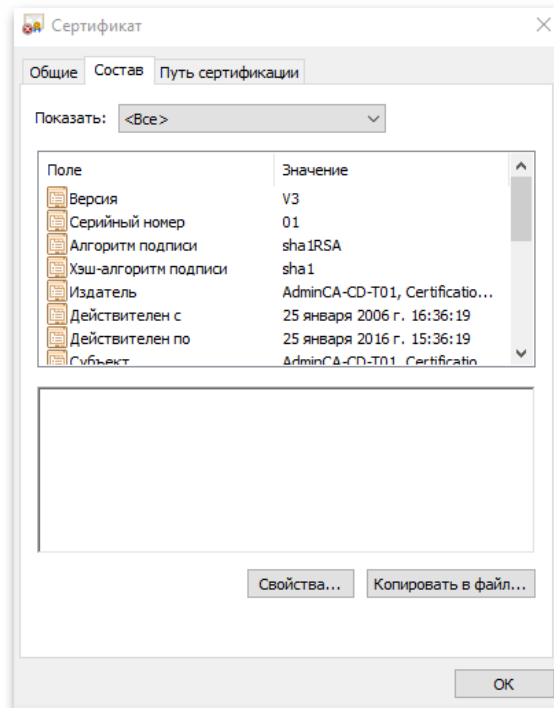
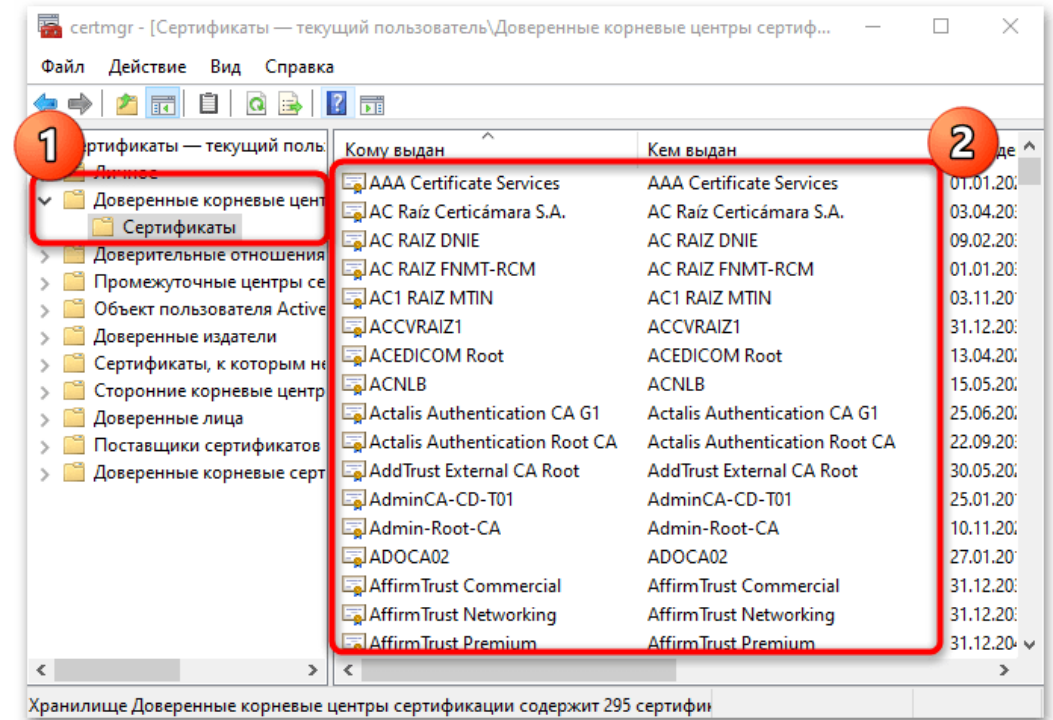
Диспетчер сертификатов (Certmgr.exe) предназначен для управления сертификатами, списками доверия сертификатов (CTL) и списками отзыва сертификатов (CRL).

<https://learn.microsoft.com/ru-ru/dotnet/framework/wcf/feature-details/working-with-certificates>



РАБОТА с СЕРТИФИКАТАМИ В ОС

В каталоге «Личное» по умолчанию сертификатов нет, поскольку пользователь самостоятельно их устанавливает с токена или делает импорт данных. «Доверенные корневые центры сертификации» позволяют посмотреть данные от крупнейших издательств, которые представлены во внушительном списке. Благодаря им используемый браузер доверяет сертификатам большинства сайтов. Это обеспечивает безопасное пребывание в сети.

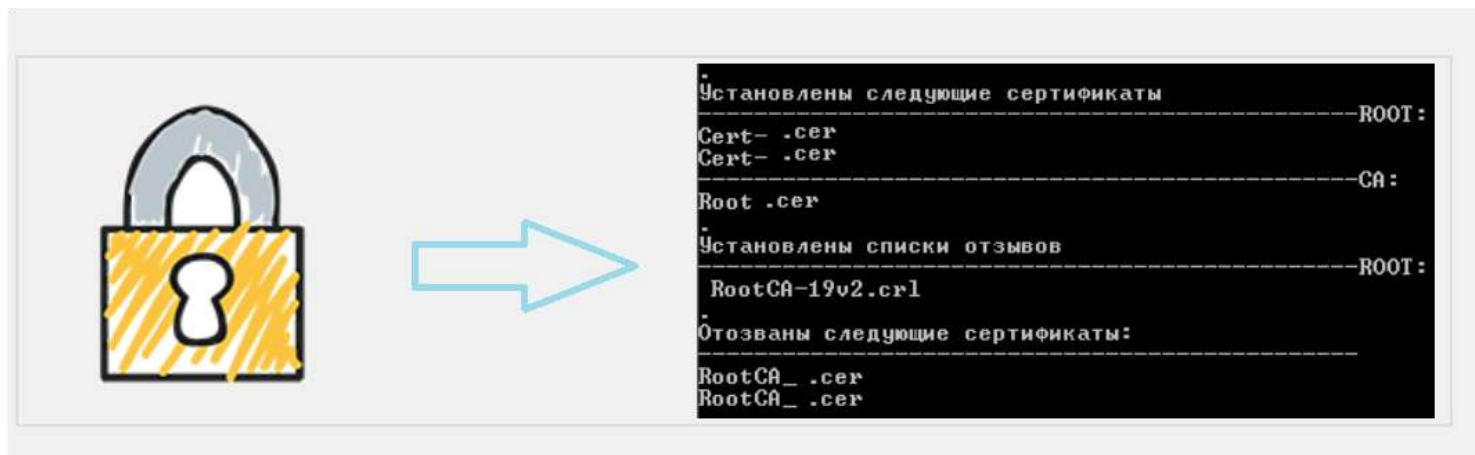


Чтобы посмотреть содержимое корневого сертификата, дважды щелкните левой кнопкой мыши по его названию. В дополнительном окне есть общая информация, подробный состав и свойства каждого элемента, а также путь сертификации.



РАБОТА с СЕРТИФИКАТАМИ

Основные функции программы **Certmgr.exe**. Отображение сведений о сертификатах, CTL и CRL на консоли. Добавляет сертификаты, CTL и CRL в хранилище сертификатов. Удаляет сертификаты, CTL и CRL из хранилища сертификатов. Сохраняет в файл сертификат X.509, CTL или CRL из хранилища сертификатов.



Программа **Certmgr.exe** работает с двумя типами хранилищ сертификатов: системным и StoreFile. Указывать тип хранилища необязательно, поскольку программа Cedrtmgr.exe может автоматически определить тип хранилища и выполнить соответствующие действия. При запуске программы Certmgr.exe без параметров выполняется оснастка «certmgr.msc» с графическим интерфейсом пользователя, облегчающим управление сертификатами, что также можно сделать из командной строки. В графическом интерфейсе пользователя имеется мастер импорта, копирующий сертификаты, CTL и CRL с диска в хранилище сертификатов.



РАБОТА с СЕРТИФИКАТАМИ

Для хранения сертификатов используются специальные **хранилища**.

В системе они представлены обычно 2-мя типами:

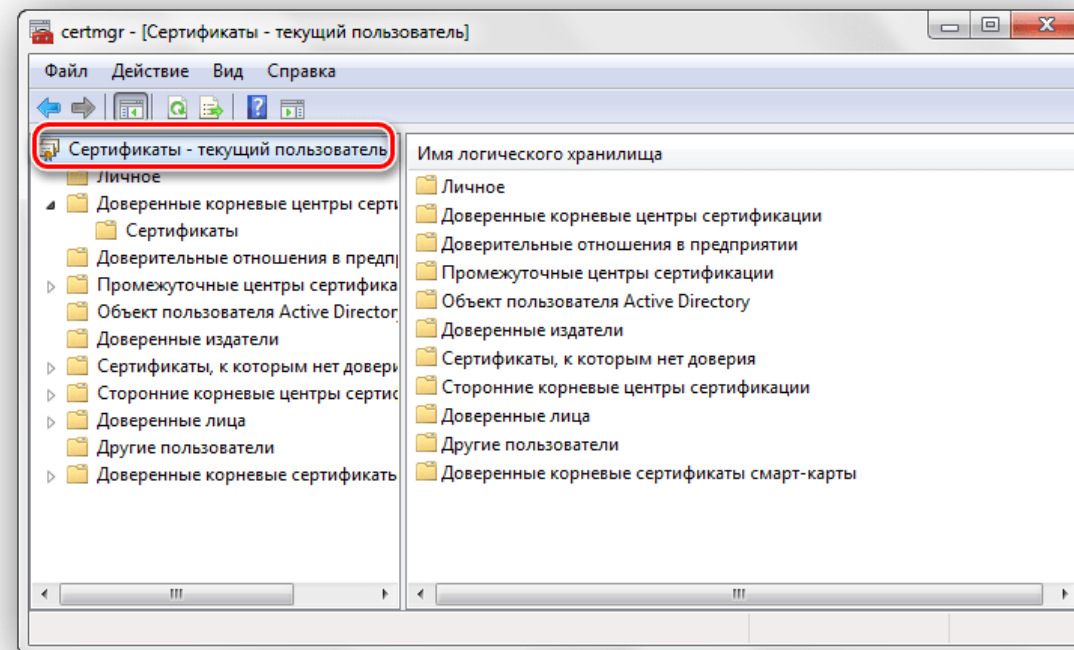
- ☐ хранилище локального компьютера
- ☐ хранилище текущего пользователя.

Пользователь с правами администратора имеет возможность просмотра всех хранилищ. Обычные пользователи, не обладающие правами администратора, имеют доступ лишь ко второму типу.

В хранилище локального компьютера содержатся сертификаты глобальные для всех пользователей, а в хранилище текущего пользователя находятся сертификаты для конкретной учетной записи.

В свою очередь хранилища внутри разделяются на вложенные хранилища, т.е. сертификаты группируются в зависимости от назначения сертификата.

Сертификаты для текущего пользователя наследуют содержимое хранилищ с сертификатами локального компьютера.

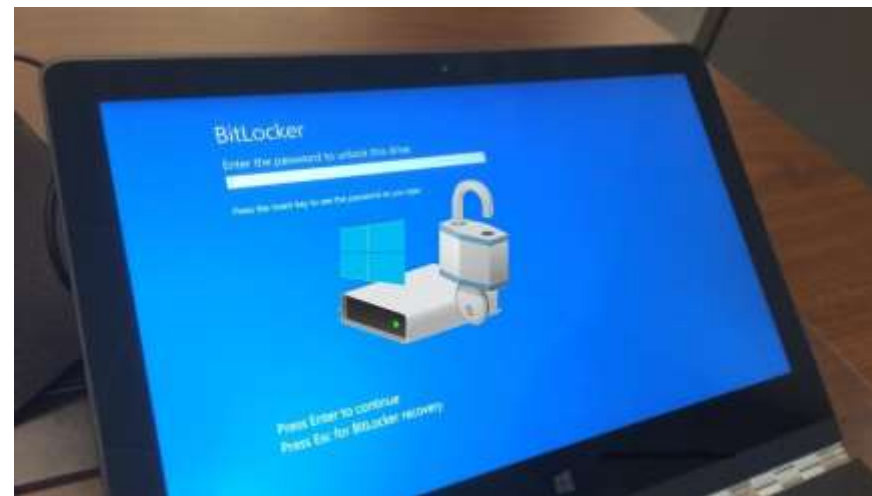




ИСПОЛЬЗОВАНИЕ BitLocker

Шифрование диска BitLocker — это функция защиты данных, которая интегрируется в операционную систему, для закрытия информации на потерянных, украденных или неправильно выведенных из эксплуатации компьютерах.

Предотвращает угрозы хищения данных BitLocker обеспечивает максимальную защиту при использовании с доверенным платформенным модулем (TPM) версии 1.2 или более поздней. Доверенный платформенный модуль — это аппаратный компонент, который производители устанавливают на многих новых компьютерах. Совместно с BitLocker он обеспечивает защиту данных пользователей и предотвращает несанкционированный доступ к компьютеру, пока система находится вне сети.

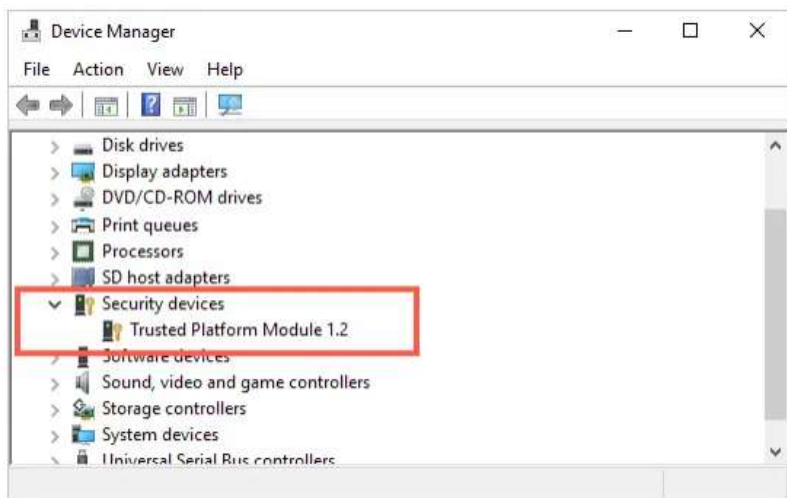


<https://learn.microsoft.com/ru-ru/windows/security/information-protection/bitlocker/bitlocker-device-encryption-overview-windows-10>



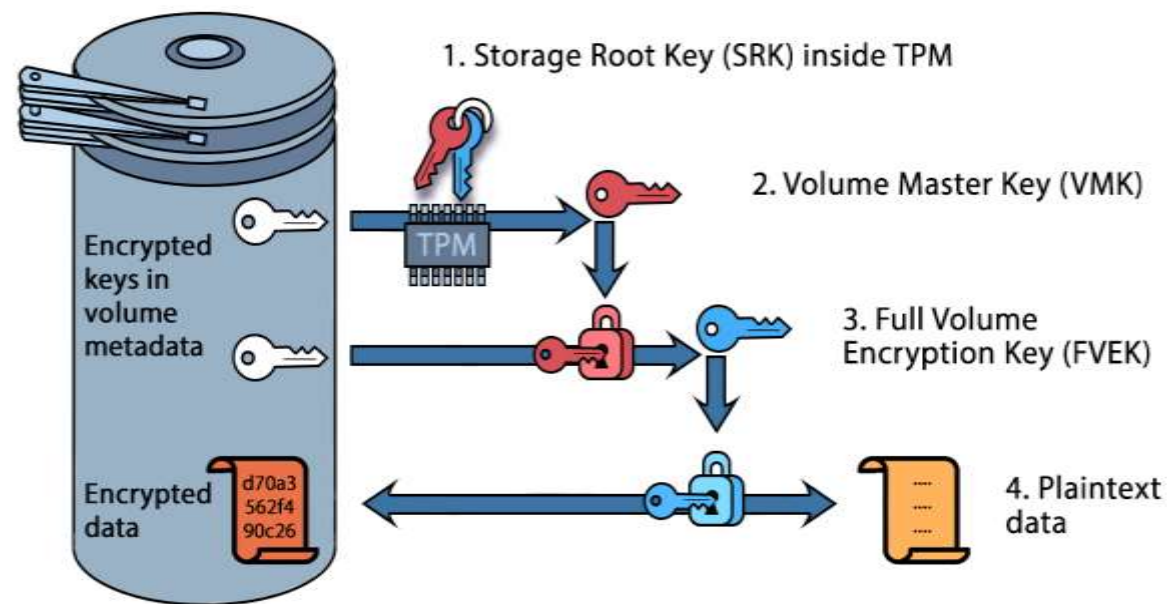
ИСПОЛЬЗОВАНИЕ BitLocker

Важно убедиться, что на вашем компьютере есть микросхема TPM для поддержки такой расширенной настройки безопасности.



Шифрование всего диска действительно скажется на производительности системы, в частности, на скорости чтения/записи данных. Тесты различных пользователей показывают, что на относительно современном железе падение скорости на [SSD](#) — не более 10%, у [жестких дисков](#) падения могут быть больше.

BitLocker Keys



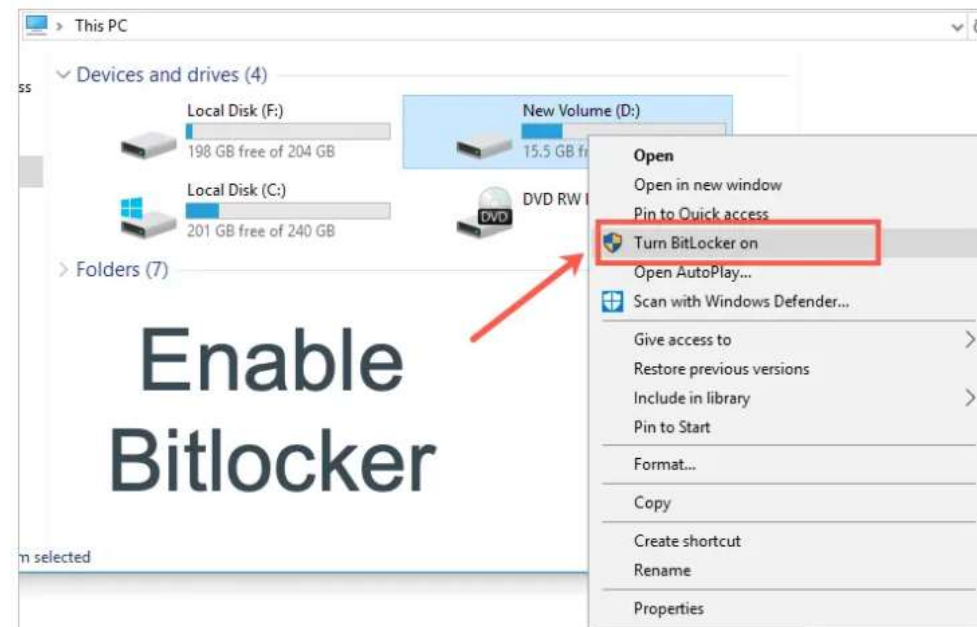
ИСПОЛЬЗОВАНИЕ BitLocker



Включение шифрования диска BitLocker в Windows 10

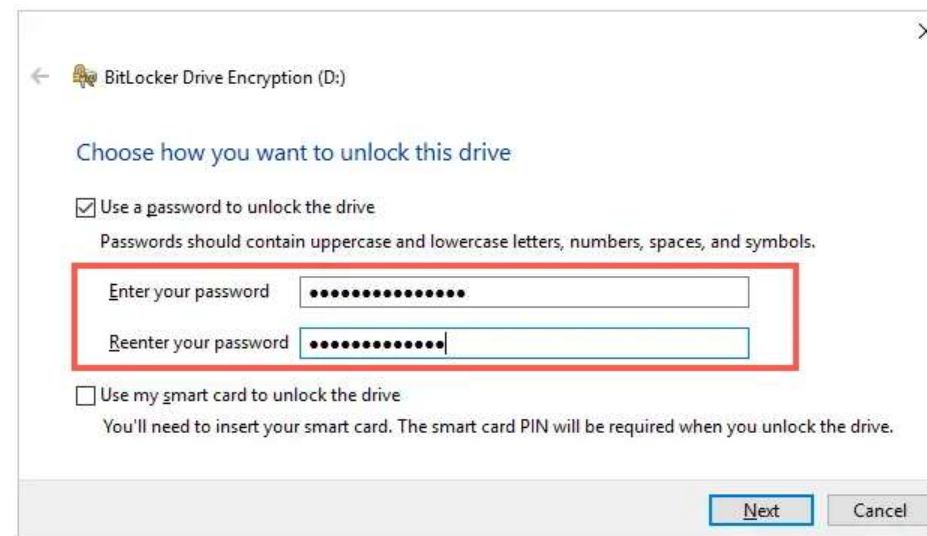
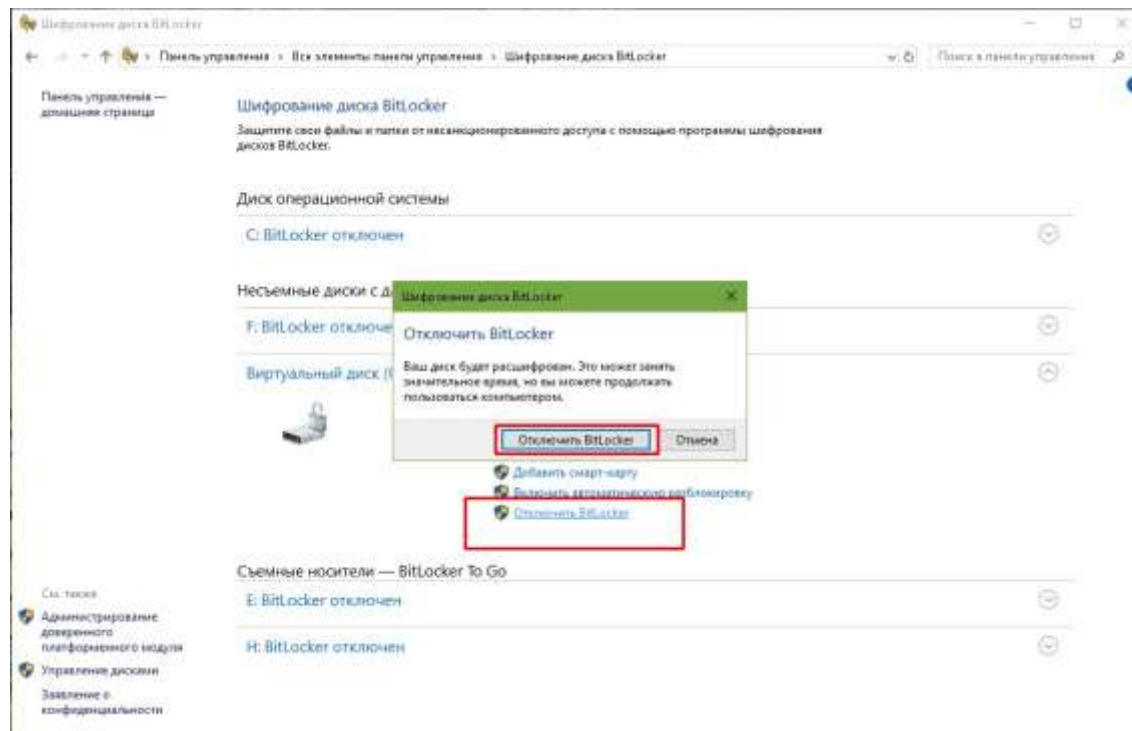
Требования и ограничения шифрования BitLocker

1. BitLocker доступен в версиях Windows 10 Enterprise и Pro, поэтому он может быть бесполезен для пользователей версии Home.
2. ПК с TPM (Trusted Platform Module), микрочипом, поддерживающим расширенные функции безопасности. Однако вы можете использовать менее эффективный вариант программного шифрования для компьютеров, на которых отсутствует микросхема TPM.
3. Bios, поддерживающий TPM или USB-устройства при запуске.
4. Жесткий диск как минимум с двумя разделами с файловой системой NTFS.
5. Шифрование диска BitLocker может занять некоторое время, поэтому ваш компьютер должен быть подключен к источнику питания и не должен прерываться.



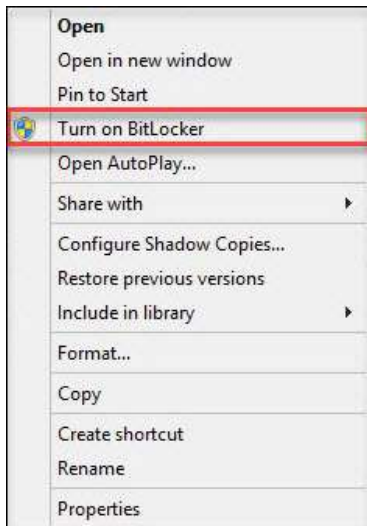


ИСПОЛЬЗОВАНИЕ BitLocker





ИСПОЛЬЗОВАНИЕ BitLocker

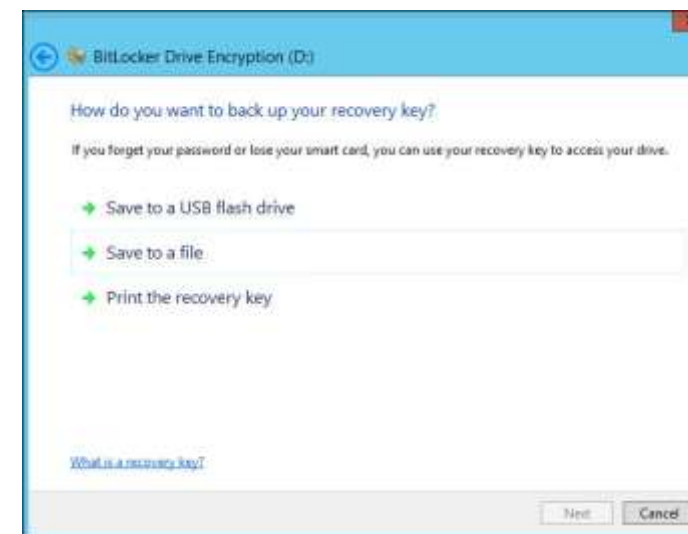
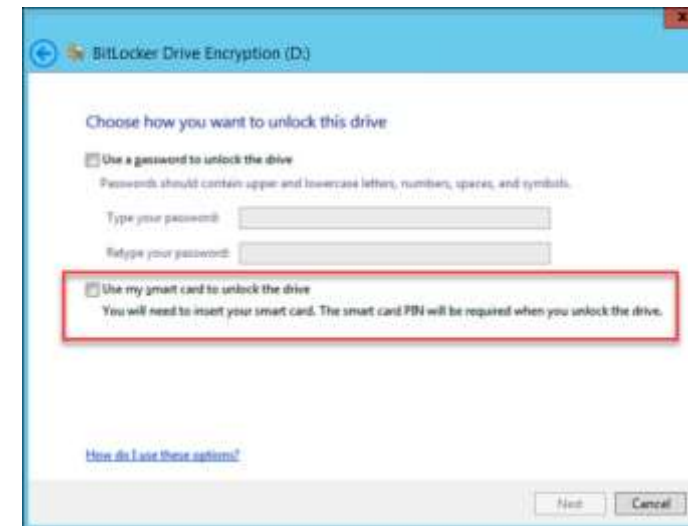
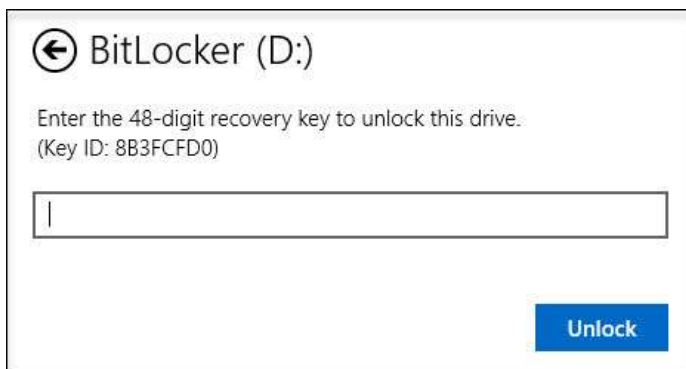


Для использования токена или смарт-карты в BitLocker, на них должны находиться ключи RSA 2048 и сертификат.

Если вы пользуетесь службой Certificate Authority в домене Windows, то в шаблоне сертификата должна присутствовать область применения сертификата «Disk Encryption».

Если нет домена или вы не можете изменить политику выдачи сертификатов, то можно воспользоваться запасным путем, с помощью самоподписанного сертификата.

Если вы хотите открыть зашифрованные данные в Windows для этого понадобится ключ восстановления, который мы распечатали ранее. Просто вводим его в соответствующее поле и зашифрованный раздел откроется.





АУДИТ В WINDOWS

Аудит безопасности Windows - это технические средства и мероприятия, направленные на регистрацию и систематический регулярный анализ событий, влияющих на безопасность информационных систем предприятия. Технически, аудит безопасности в Windows реализуется через настройку политик аудита и настройку аудита объектов. Политика аудита определяет какие события и для каких объектов будут генерироваться в журнал событий Безопасность.

Регулярный анализ данных журнала безопасности относится к организационным мерам, для поддержки которых может применяться различное программное обеспечение. В самом простом случае можно обходиться приложением Просмотр событий. Для автоматизации задач анализа событий безопасности могут применяться более продвинутые программы и системы управления событиями безопасности (SIEM), обеспечивающие постоянный контроль журналов безопасности, обнаружение новых событий, их классификацию, оповещение специалистов при обнаружении критических событий.



АУДИТ В WINDOWS



Хранение журналов

Большинство действий пользователя в системе попадают в журнал событий операционной системы. Файлы журнала сохраняются на системном диске по пути: C:\Windows\System32\winevt\Logs.

Файлы журналы событий Windows хранятся в каталог %SystemRoot%\System32\Winevt\Logs\ в виде файлов с расширением .EVTX. Обратите внимание, что для каждого журнала используется собственный файл. Соответственно, вы можете управлять размерами только того лога Windows, который вам нужен и оставить остальные значения по-умолчанию.

Текущие лимиты на все включенные журналы событий в Windows можно вывести с помощью PowerShell:
Get-Eventlog -List












Organize

New

Open

Select

s PC > Local Disk (C:) > Windows > System32 > winevt > Logs

Name	Date modified	Type	Size
 Security.evtx	11/22/2022 2:16 PM	Event Log	20,484 KB
 System.evtx	11/22/2022 4:40 PM	Event Log	20,484 KB
 Microsoft-Windows-Store%4Operational...	11/21/2022 6:00 PM	Event Log	17,476 KB
 Microsoft-Windows-PowerShell%4Opera...	11/21/2022 10:07 AM	Event Log	15,364 KB
 PowerShellCore%4Operational.evtx	11/15/2022 5:38 PM	Event Log	14,404 KB
 Application.evtx	11/22/2022 2:17 PM	Event Log	10,308 KB
 Microsoft-Windows-TaskScheduler%4Op...	11/22/2022 2:04 PM	Event Log	10,244 KB
 Microsoft-Windows-Storage-Storport%4...	11/22/2022 1:47 PM	Event Log	7,236 KB
 Microsoft-Windows-Storage-ClassPnP%	11/18/2022 7:03 PM	Event Log	6,148 KB
 Microsoft-Windows-SmbClient%4Conne...	11/22/2022 10:01 AM	Event Log	5,188 KB
 Windows PowerShell.evtx	11/16/2022 7:15 PM	Event Log	5,188 KB

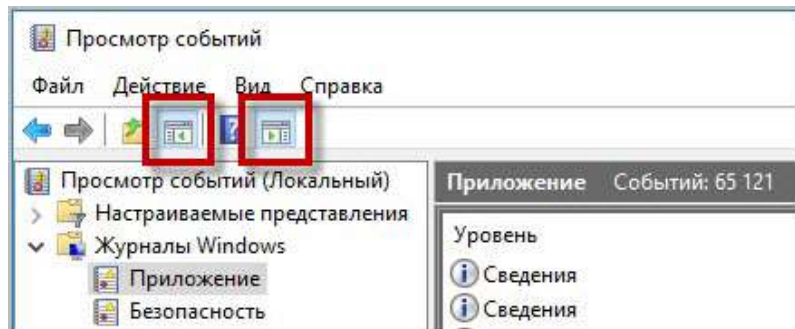
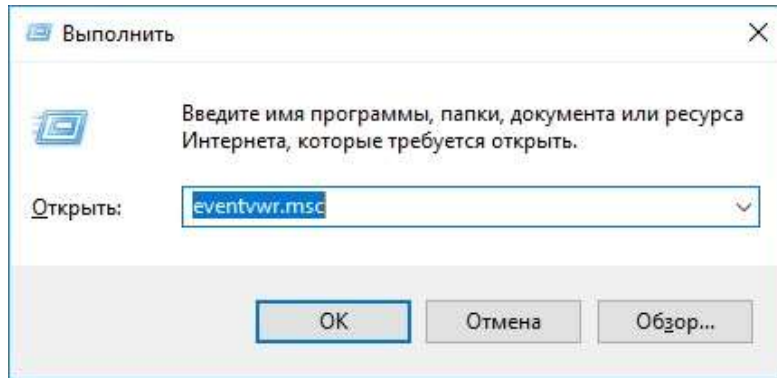
```
PS C:\WINDOWS\system32> Get-Eventlog -List
```

Max(K)	Retain	OverflowAction	Entries	Log
512	7	OverwriteOlder	290	ACEEventLog
20,480	0	OverwriteAsNeeded	18,336	Application
8,192	0	OverwriteAsNeeded	0	Doctor Web
20,480	0	OverwriteAsNeeded	0	HardwareEvents
512	7	OverwriteOlder	0	Internet Explorer
20,480	0	OverwriteAsNeeded	0	Key Management Service
128	0	OverwriteAsNeeded	458	OAAlerts
20,480	0	OverwriteAsNeeded	34,922	Security
20,480	0	OverwriteAsNeeded	42,741	System
15,360	0	OverwriteAsNeeded	3,013	Windows PowerShell

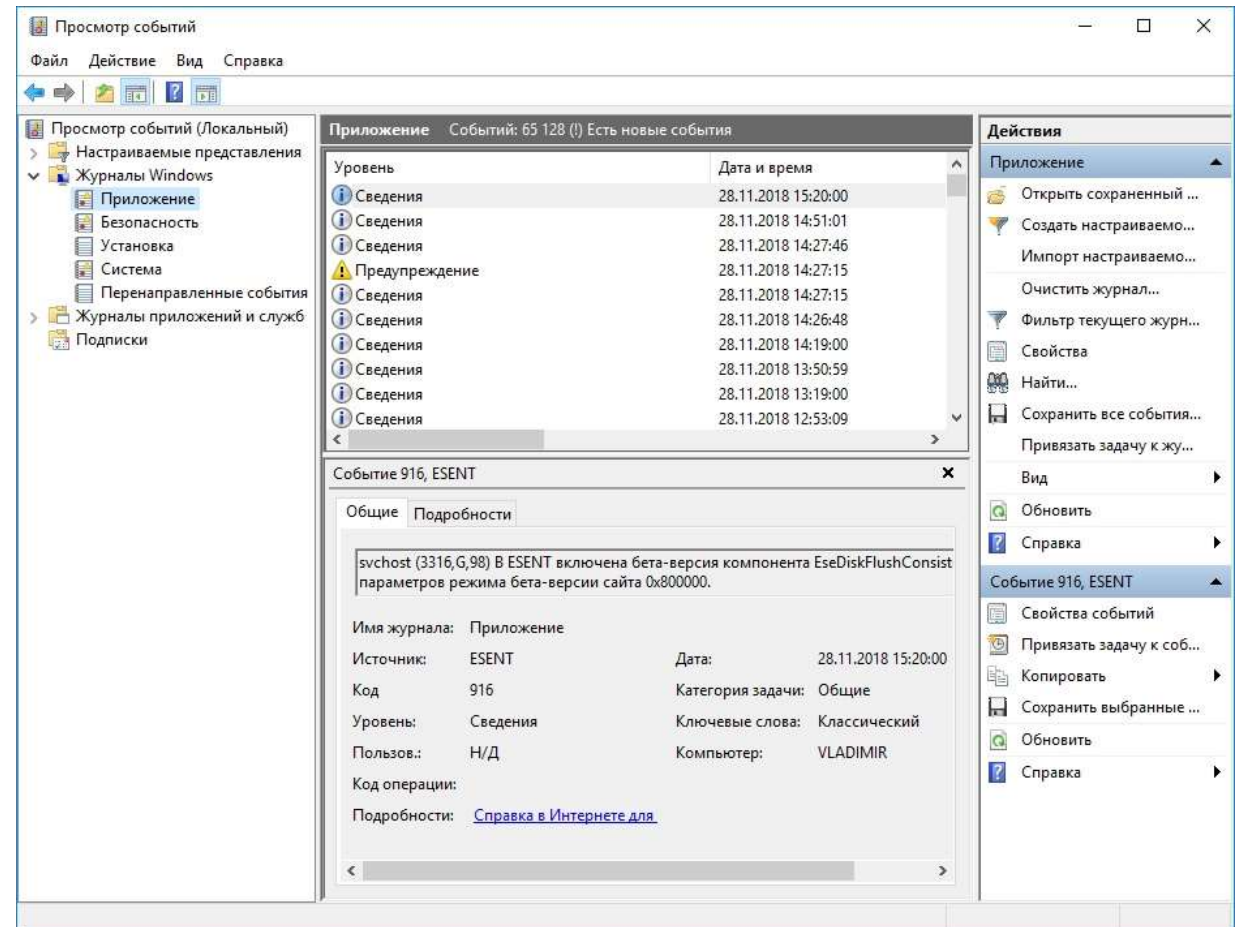


АУДИТ В WINDOWS

Нажать на клавиатуре сочетание клавиш Win+R – в открывшемся окошке ввести eventvwr.msc и нажать ОК



Запущенная утилита “Просмотр событий” имеет следующий вид:



АУДИТ В WINDOWS

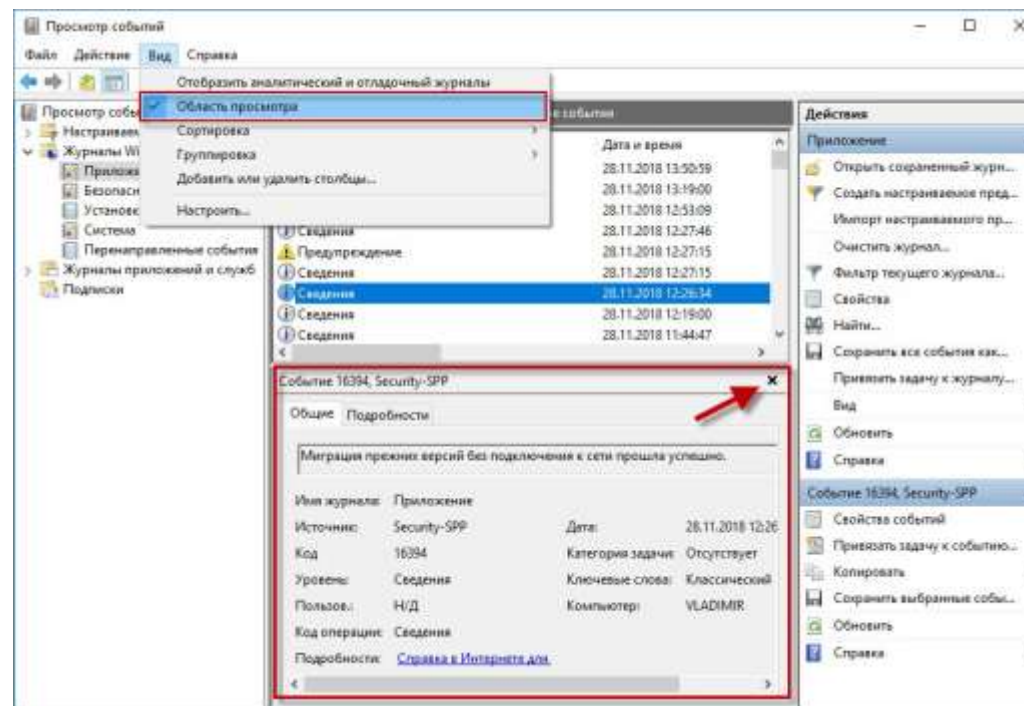
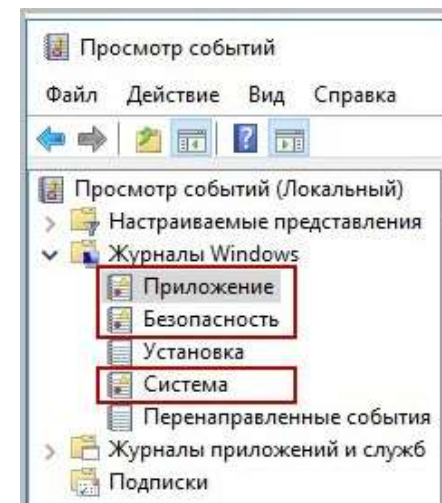


Данный раздел включает три основные и две дополнительные категории: **основные** – это Приложение, Система, **Безопасность**; **дополнительные** – Установка и Перенаправленные события.

Приложение – хранит важные события, связанные с конкретным приложением. Эти данные помогут системному администратору установить причину отказа той или иной программы.

Система – хранит события операционной системы или ее компонентов (например, неудачи при запусках служб или инициализации драйверов; общесистемные сообщения и прочие сообщения, относящиеся к системе в целом).

Безопасность – хранит события, связанные с безопасностью (такие как: вход/выход из системы, управление учётными записями, изменение разрешений и прав доступа к файлам и папкам). В утилите “Просмотр событий” предусмотрена возможность поиска и **фильтрации событий**





АУДИТ В WINDOWS

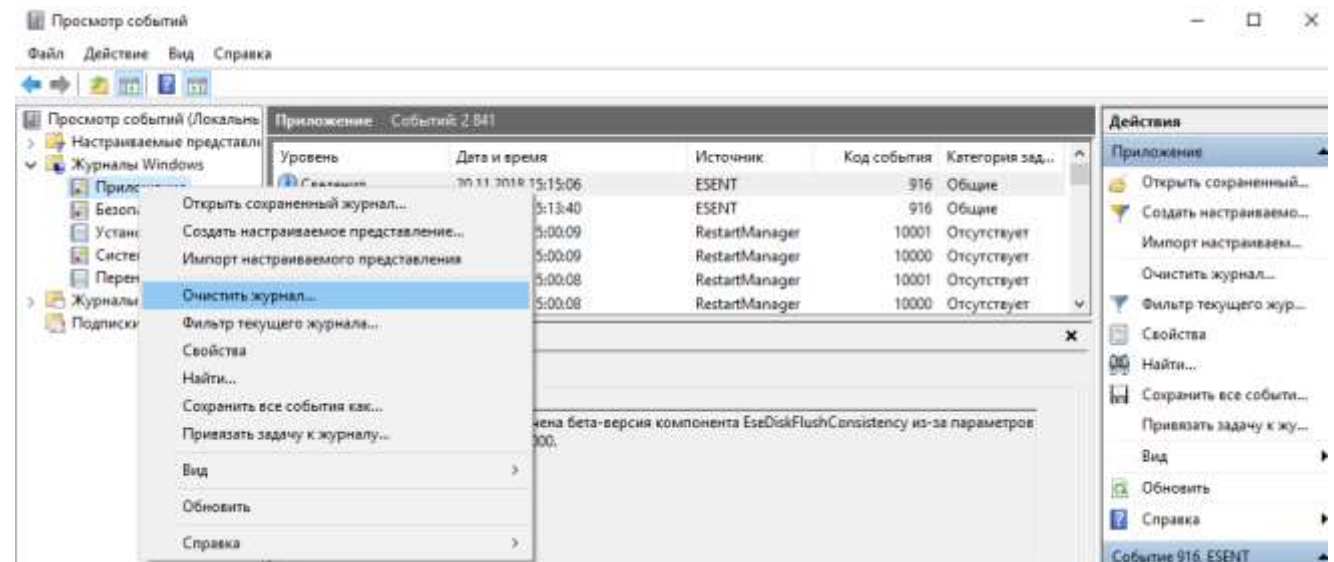
Большинство действий пользователя в системе попадают в журнал событий операционной системы. Файлы журнала сохраняются на системном диске по пути: C:\Windows\System32\winevt\Logs.

C:\Windows\System32\winevt\Logs				
Имя	Размер	Дата	Время	
..	Вверх	10.03.22	14:14	
Application	evt	20 М	01.12.22	11:49
System	evt	20 М	01.12.22	11:45
Security	evt	20 М	01.12.22	10:32
Microsoft-Windows-WMI-Activity%4Operational	evt	1028 К	01.12.22	10:31
Microsoft-Windows-SmbClient%4Connectivity	evt	8196 К	01.12.22	10:31
Microsoft-Windows-StateRepository%4Operational	evt	5124 К	01.12.22	10:31

Как очистить журнал событий в Windows 10

Очистить журнал событий в Windows 10 можно несколькими эффективными способами. До таких способов отнесем выполнение одной команды в командной строке или же в оболочке Windows PowerShell, а также простое удаление событий прямо с журнала.

После открытия журнала достаточно нажать правой кнопкой мыши на категорию, журнал которой необходимо очистить и в контекстном меню выбираем пункт **Очистить журнал...** В открывшемся окне подтверждаем очистку журнала нажав кнопку **Очистить**.



АУДИТ В WINDOWS



Фильтровать текущий журнал

Фильтр XML

Дата: Последние 24 часа

Уровень события: ☒ Критическое ☐ Предупреждение ☐ Подробности
☒ Ошибка ☐ Сведения

☒ По журналу Журналы событий: Приложение
☐ По источнику Источники событий:

Включение или исключение кодов событий. Введите коды событий или диапазоны кодов, разделяя их запятыми. Для исключения условия введите знак минус. Например: 1,3,5-99,-76

<Все коды событий>

Категория задачи:

Ключевые слова:

Подпользователь: <Все пользователи>

Компьютеры: <Все компьютеры>

Очистить

OK Отмена

Управление компьютером

Файл Действие Вид Справка

Управление компьютером (локальным)

- Служебные программы
- Планировщик заданий
- Просмотр событий
 - Настраиваемые представления
 - Журналы Windows
 - Приложение
 - Security
 - Установка
 - Система
 - Перенаправленные события
 - Журналы приложений и служб
 - Подписки
- Общие папки
- Локальные пользователи и группы
- Производительность
- Диспетчер устройств
- Запоминающие устройства
- Управление дисками
- Службы и приложения

Уровень	Дата и время	Источник	Код со...	Категория за...
Сведения	01.12.2022 12:04:21	Windows Err...	1001	Отсутствует
Сведения	01.12.2022 12:02:15	Windows Err...	1001	Отсутствует
Сведения	01.12.2022 12:00:09	Windows Err...	1001	Отсутствует
Сведения	01.12.2022 11:57:58	Windows Err...	1001	Отсутствует
Сведения	01.12.2022 11:55:52	Windows Err...	1001	Отсутствует
Сведения	01.12.2022 11:53:42	Windows Err...	1001	Отсутствует
Сведения	01.12.2022 11:51:36	Windows Err...	1001	Отсутствует
Сведения	01.12.2022 11:49:29	Windows Err...	1001	Отсутствует
Сведения	01.12.2022 11:47:23	Windows Err...	1001	Отсутствует
Сведения	01.12.2022 11:45:17	Windows Err...	1001	Отсутствует
Сведения	01.12.2022 11:43:10	Windows Err...	1001	Отсутствует
Сведения	01.12.2022 11:41:04	Windows Err...	1001	Отсутствует
Сведения	01.12.2022 11:38:58	Windows Err...	1001	Отсутствует
Предупреж...	01.12.2022 11:37:35	Group Policy ...	4098 (2)	
Предупреж...	01.12.2022 11:37:29	Group Policy ...	4098 (2)	
Сведения	01.12.2022 11:36:52	Windows Err...	1001	Отсутствует
Сведения	01.12.2022 11:34:45	Windows Err...	1001	Отсутствует

Событие 4098, Group Policy Shortcuts

Общие Подробности

Элемент предпочтения пользователь "SED" в объекте групповой политики "RF-USR-WWW-Shortcuts (A1745F97-B3F5-4890-AEEF-F3C07D9116A8)" не применен по причине ошибки с кодом '0x80070002 Не удается найти указанный файл'. Эта ошибка была отключена.

Имя журнала: Приложение

Источник: Group Policy Shortcuts Дата: 01.12.2022 11:37:35

Код: 4098 Категория задачи: (2)

Уровни: Предупреждение Ключевые слова: Классический

Подпользов.: СИСТЕМА Компьютер: W0100-PLAN00084.rf.rshbank.ru

Код операции:

Подробности: [Справка в Интернете для...](#)

Действия

- Приложение
- Открыть сохраненный журнал...
- Создать настраиваемое представ...
- Импорт настраиваемого предств...
- Очистить журнал...
- Фильтр текущего журнала...
- Свойства
- Найти...
- Сохранить все события как...
- Привязать задачу к журналу...
- Вид
- Обновить
- Справка
- Событие 4098, Group Policy Shortcuts
- Свойства событий
- Привязать задачу к событию...
- Копировать
- Сохранить выбранные события...
- Обновить
- Справка

Windows Security Log Events. Все события аудита Windows

<https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx>

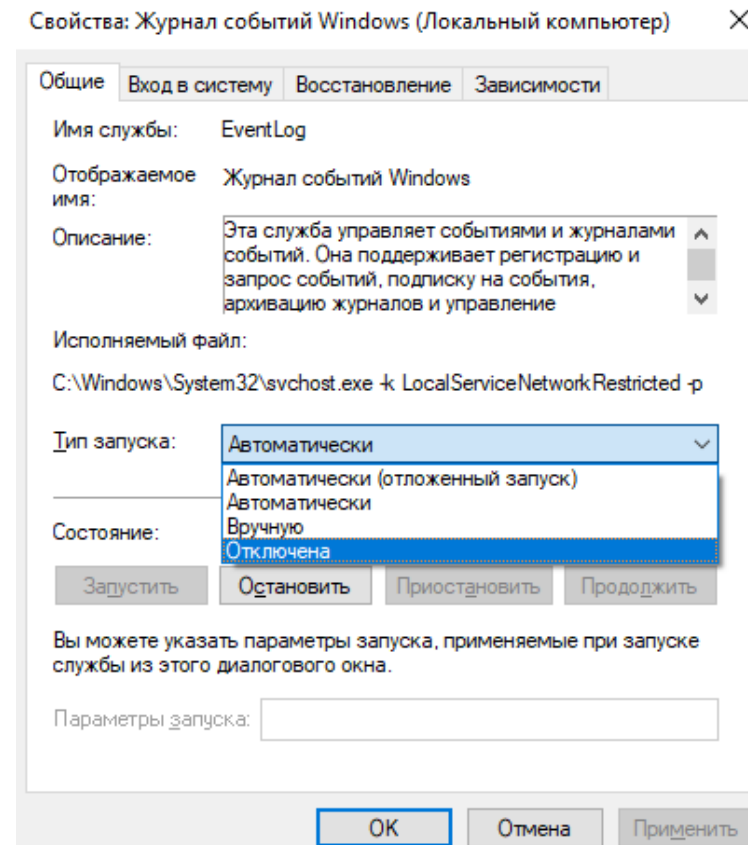


АУДИТ В WINDOWS

Как отключить журнал событий Windows 10

[как открыть службы в Windows 10](#). Есть возможность отключить службу журнала событий Windows 10. И тогда уже после перезагрузки компьютера данные не будут записываться в журнал и пользователь не сможет посмотреть журнал событий в будущем. Поэтому отключать журнал событий не рекомендуется, хотя такая возможность и есть.

- 1.Открываем окно служб выполнив команду **services.msc** в окне **Win+R**.
- 2.Среди списка доступных служб находим **Журнал событий Windows** и в контекстном меню которого выбираем **Свойства**.
- 3.В открывшемся окне изменяем типу запуска службы EventLog на **Отключена** и нажмимте **ОК**.

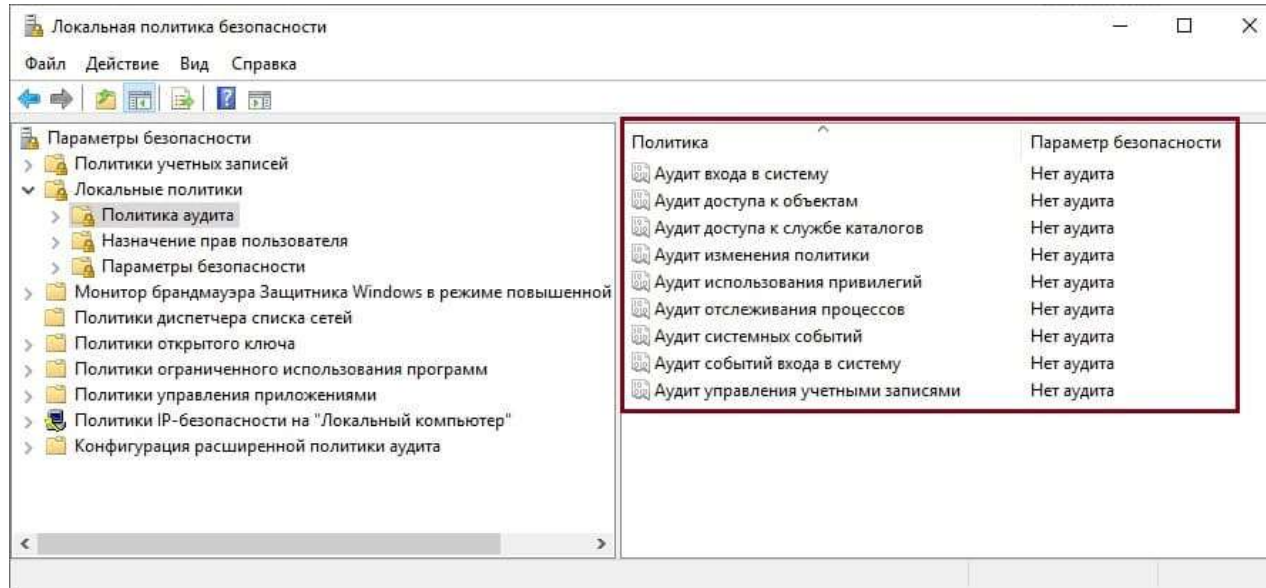


<https://windd.ru/kak-posmotret-zhurnal-sobytij-v-windows-10/>

АУДИТ В WINDOWS



Политика аудита



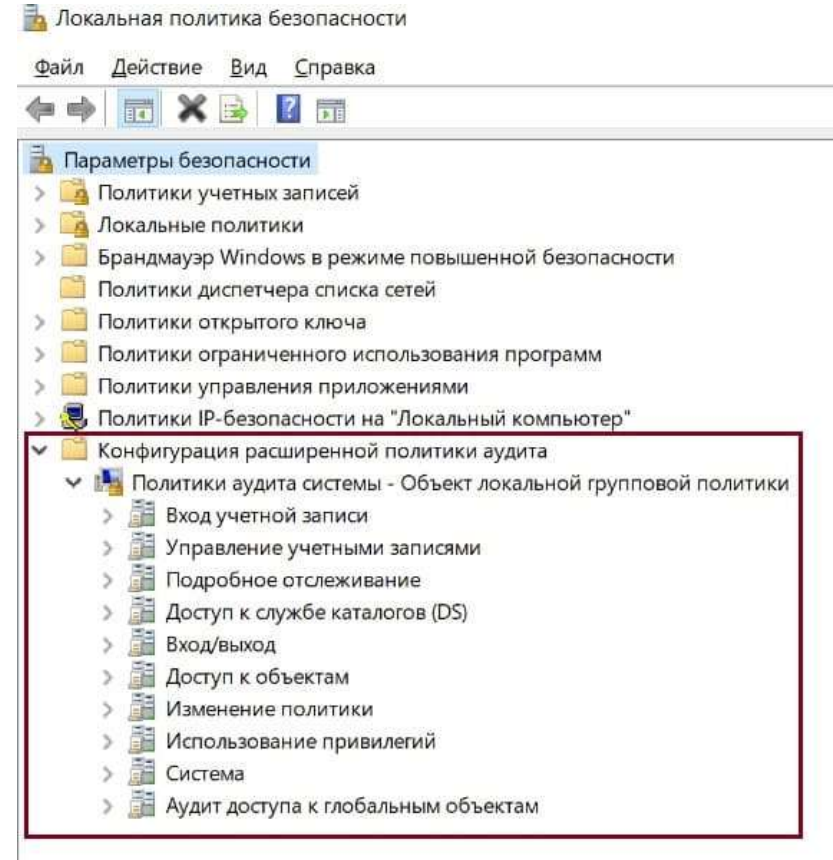
[Базовые политики аудита безопасности](#)

Перед внедрением аудита необходимо выбрать политику аудита. Базовая политика аудита определяет категории событий, связанных с безопасностью, которые требуется выполнить аудит. При первой установке этой версии Windows все категории аудита будут отключены. Включив различные категории событий аудита, можно реализовать политику аудита, которая соответствует требованиям безопасности вашей организации.

[Расширенные политики аудита безопасности](#)

Параметры расширенной политики аудита безопасности находятся в **разделе Параметры безопасности\Конфигурация расширенной политики аудита\Политики аудита системы** и, как представляется, перекрываются с основными политиками аудита безопасности, но они записываются и применяются по-разному.

Расширенная политика аудита



ИНСТРУМЕНТЫ



Windows 10 позволяет легко подключаться к сети и интернету с помощью проводного или беспроводного соединения. Тем не менее, иногда приходится что-то настраивать вручную или устранять проблемы с подключением, и именно тогда вам могут пригодиться многие встроенные инструменты командной строки.

IPConfig

Инструмент ipconfig (Internet Protocol configuration) является одним из наиболее распространенных и позволяет запрашивать и показывать текущую конфигурацию сети TCP/IP (Transmission Control Protocol/Internet Protocol). Команда также включает в себя опции для выполнения таких действий, как обновление параметров протокола динамической конфигурации хоста (DHCP) и Системы доменных имен (DNS).

Ping

Ping — еще один важный сетевой инструмент. Он позволяет отправлять сообщения эхо-запроса ICMP (Internet Control Message Protocol) для проверки IP-соединения с другими устройствами, будь то другой компьютер в сети или интернет-сервис.

Tracert

В Windows 10 также есть инструмент tracert (Trace Route) — он позволяет определить сетевой путь к месту назначения с помощью серии эхо-запросов ICMP. Однако, в отличие от команды ping, каждый запрос включает в себя значение TTL (Time to Live) — каждый раз оно увеличивается на единицу, позволяя отображать список пройденных маршрутов и продолжительности запросов.



ИНСТРУМЕНТЫ

Инструмент: отчет о беспроводной сети

Описание: В этом отчете показаны последние три дня Wi-Fi событий с компьютера. Этот отчет представляет собой HTML-файл, который можно открыть в любом удобном веб-браузере. При составлении отчета о беспроводной сети также создаются CAB-файлы с информацией о подключении. Специалисты службы поддержки могут использовать эти файлы для выявления и решения проблем с беспроводной сетью.

Создание отчета о беспроводной сети

В поле поиска на панели задач введите **Командная строка**, щелкните правой кнопкой мыши (либо нажмите и удерживайте) пункт **Командная строка**, а затем выберите **Запуск от имени администратора** > **Да**.

В командной строке введите **netsh wlan show wlanreport**.



ИНСТРУМЕНТЫ

Вы можете использовать монитор производительности следующим образом.

■ ■ Системный Монитор ActiveX (Performance Monitor ActiveX Control)

Монитор производительности Windows 10 – это элемент управления ActiveX, который можно разместить в других приложениях. Примерами приложений, которые могут взаимодействовать с системным монитором, являются веб-браузеры и клиентские программы, такие как Microsoft Word и Microsoft Excel. Эта функциональность может упростить разработчикам приложений и системным администраторам включение монитора производительности в свои собственные инструменты и приложения.

■ ■ Производительность MMC (Performance Monitor MMC)

Для более общих задач контроля производительности вы можете использовать встроенную оснастку MMC – Производительность (Performance).

■ ■ Группы сборщика данных (Data Collector Sets)

Монитор производительности Windows 10 включает в себя группы сборщиков данных. Этот инструмент работает с журналами производительности, сообщает монитору производительности, где хранятся журналы и когда журналирование должно запускаться. Группы сборщиков данных также определяют учетные данные, используемые для запуска набора.

Чтобы получить доступ к MMC монитора производительности, в панели управления открываете [Администрирование](#) и в нем выбираете элемент [Производительность](#) (Performance). Открывается оснастка MMC Производительность и загружает и инициализирует монитор производительности, включающий несколько счетчиков по умолчанию.

ИНСТРУМЕНТЫ



Системный монитор (Performance Monitor)

Все статистические данные о производительности подразделяются на три основные категории, из которых вы можете выбрать:

1. Объекты производительности (*Performance Objects*)

Объект производительности в системном мониторе представляет собой набор различных статистических данных о производительности, которые вы можете контролировать. Объекты производительности основаны на различных областях системных ресурсов. Например, есть объекты производительности для процессора и памяти, а также для конкретных служб.

2. Счетчики (*Counters*)

Счетчики – это фактические параметры, измеренные системным монитором. Это конкретные элементы, сгруппированные по объектам производительности. Например, в объекте Performance Processor есть счетчик для% Processor Time. Этот счетчик отображает один тип подробной информации об объекте производительности процессора (в частности, количество общего времени процессора, которое используются всеми процессами в системе). Другой набор счетчиков, которые вы можете использовать, позволит вам контролировать, например, серверы печати.

3. Экземпляры (*Instances*)

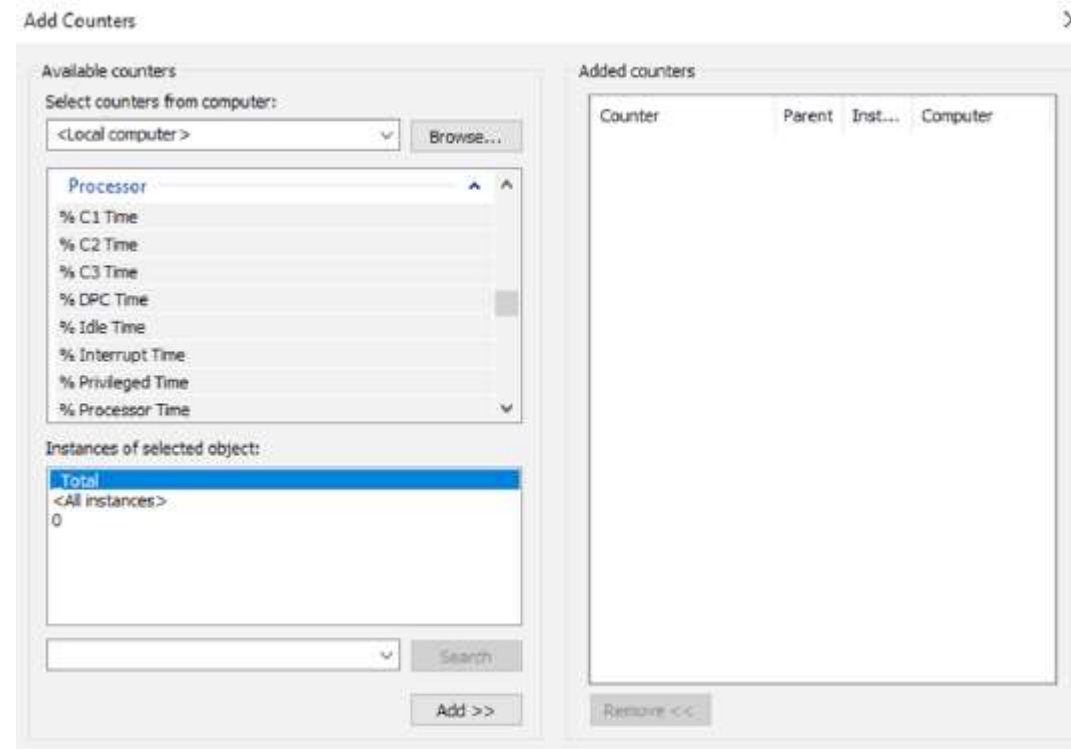
Некоторые счетчики будут иметь экземпляры. Экземпляр далее определяет, какой параметр производительности измеряет счетчик. Простым примером является сервер с двумя процессорами. Если вы решите, что хотите контро-



ИНСТРУМЕНТЫ

Чтобы указать, какие объекты производительности, счетчики и экземпляры вы хотите контролировать, добавьте их в мониторе производительности с помощью диалогового окна **Добавить счетчики (Add Counters)**. На рисунке 33 показаны различные параметры, доступные при добавлении новых счетчиков для мониторинга с использованием системного монитора.

Элементы, которые вы сможете отслеживать, будут основываться на конфигурации вашего оборудования и программного обеспечения. Например, если вы не установили и не настроили Hyper-V, параметры, доступные в объекте производительности Hyper-V Server, будут недоступны. Или, если в системе Windows 10 имеется несколько сетевых адаптеров или процессоров, у вас будет возможность просматривать каждый экземпляр отдельно или как часть общего значения.



ИНСТРУМЕНТЫ



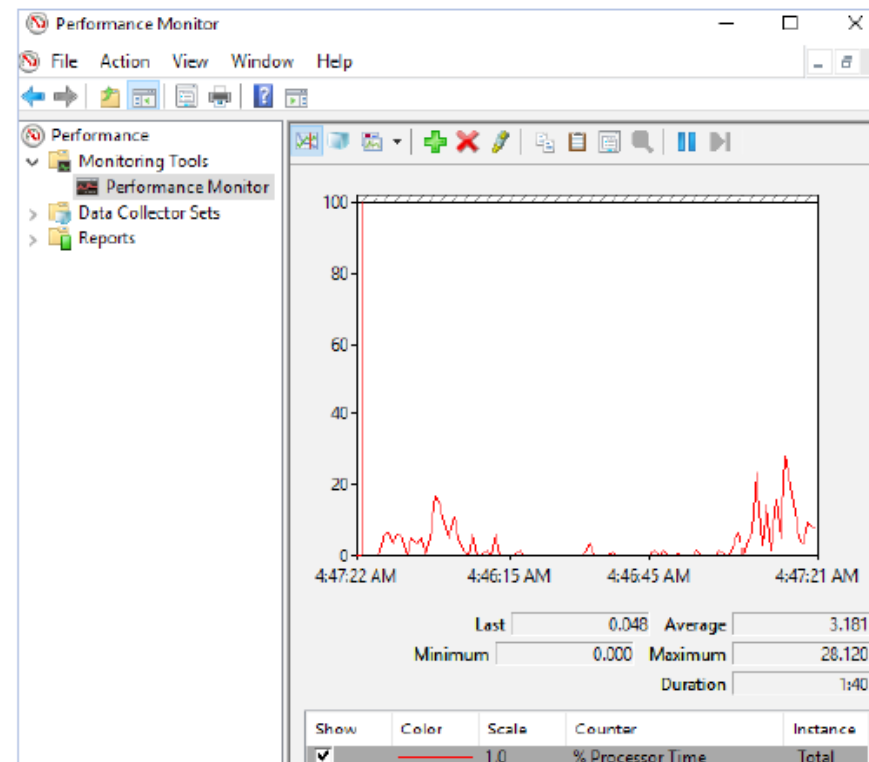
Просмотр информации о производительности

Системный монитор Windows 10 был разработан для отображения информации в ясном и понятном формате. Объекты производительности, счетчики и экземпляры могут отображаться в одном из трех видов. Эта гибкость позволяет системным администраторам быстро и легко определять информацию, которую они хотят увидеть, а затем выбирать, как она будет отображаться на основе конкретных потребностей.

Вы можете использовать следующие основные виды для просмотра статистики и информации об эффективности:

■ ■ Строка (*Graph View*)

Просмотр в режиме **Строка** представляет собой дисплей по умолчанию, который отображается при первом доступе к системному монитору Windows 10. На диаграмме отображаются значения с использованием вертикальной оси и времени с использованием горизонтальной оси. Это представление полезно, если вы хотите отображать значения в течение определенного периода времени или видеть изменения этих значений за этот период времени. Каждая точка, построенная на графике, основана на среднем значении, вычисленном во время интервала выборки для измерения.





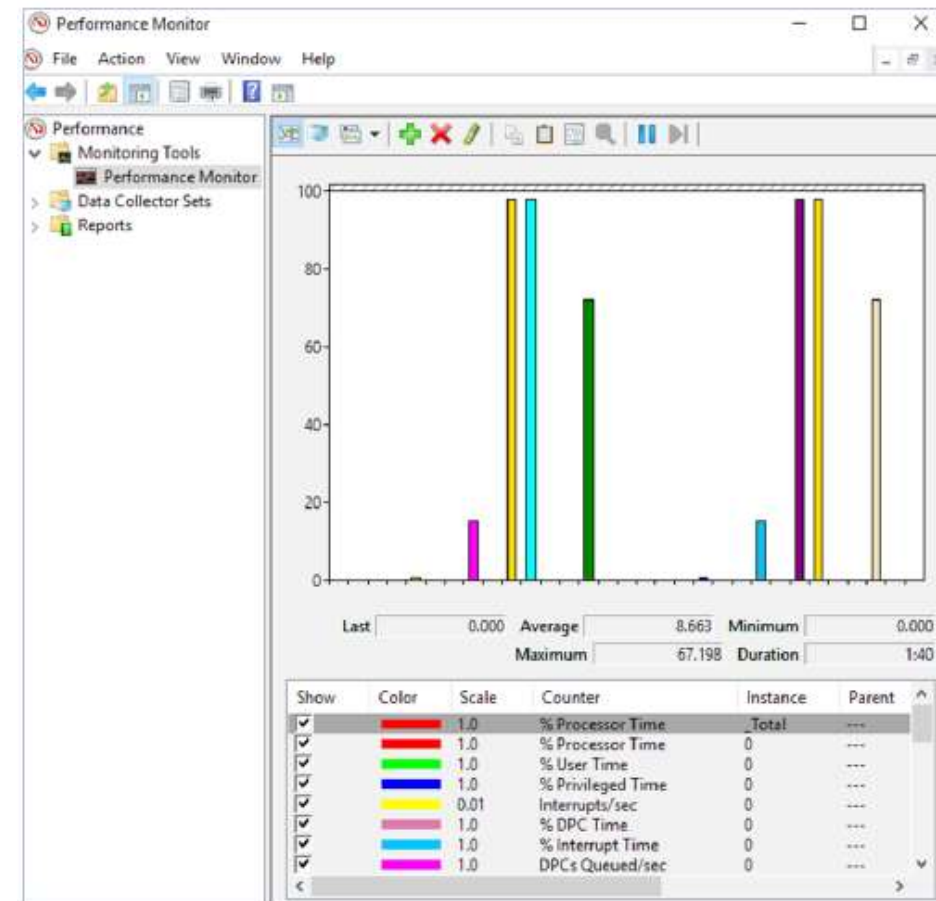
ИНСТРУМЕНТЫ

■ ■ Гистограмма (*Histogram View*)

В окне гистограммы отображается статистика производительности и информация с использованием набора относительных гистограмм. Это представление полезно, если вы хотите увидеть моментальный снимок последнего значения для данного счетчика.

■ ■ Отчет (*Report View*)

Как и в виде гистограммы, в представлении **Отчет** отображаются статистические данные о производительности, основанные на последних измерениях. Вы можете видеть среднее измерение, а также минимальные и максимальные пороговые значения. Это представление наиболее полезно для определения точных значений, поскольку оно предоставляет информацию в виде чисел, тогда как представления строки и гистограммы предоставляют информацию графически. На рисунке приведен пример типа информации, которую вы увидите в представлении **Отчет**.

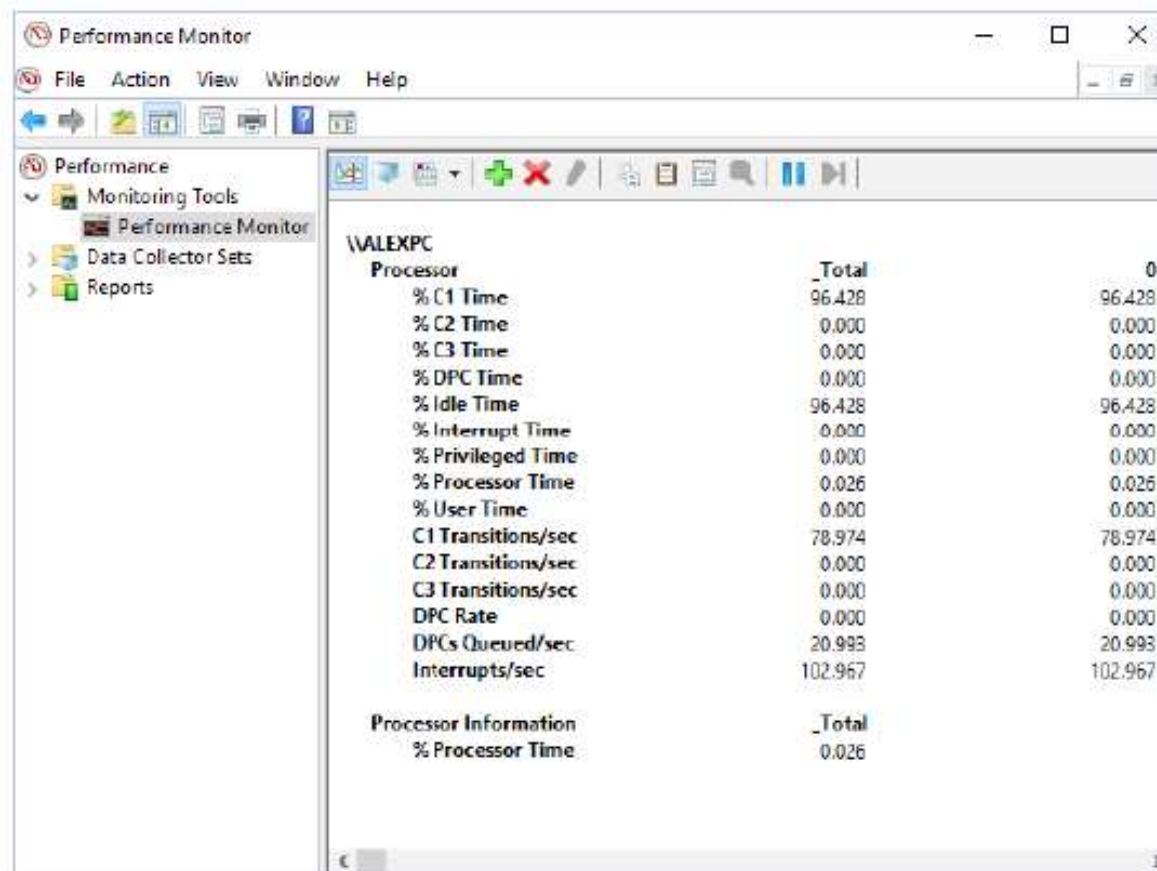




ИНСТРУМЕНТЫ

Управление свойствами системного монитора

Вы можете указать дополнительные параметры для просмотра информации о производительности в свойствах системного монитора. Вы можете получить доступ к этим параметрам, нажав кнопку **Свойства** на панели задач или щелкнув правой кнопкой мыши на экране **Системный монитор** и выбрав **Свойства**.



ИНСТРУМЕНТЫ



Вкладка «Общие» (General)

Performance Monitor Properties

General | Source | Data | Graph | Appearance

Display elements

☒ Legend ☒ Value bar ☒ Toolbar

Report and histogram data

☒ Default ☐ Minimum ☐ Average

☐ Current ☐ Maximum

☒ Sample automatically

Graph elements

Sample every seconds

Duration: seconds

Performance Monitor Properties

General | Source | Data | Graph | Appearance

Data source

☒ Current activity

☐ Log files:

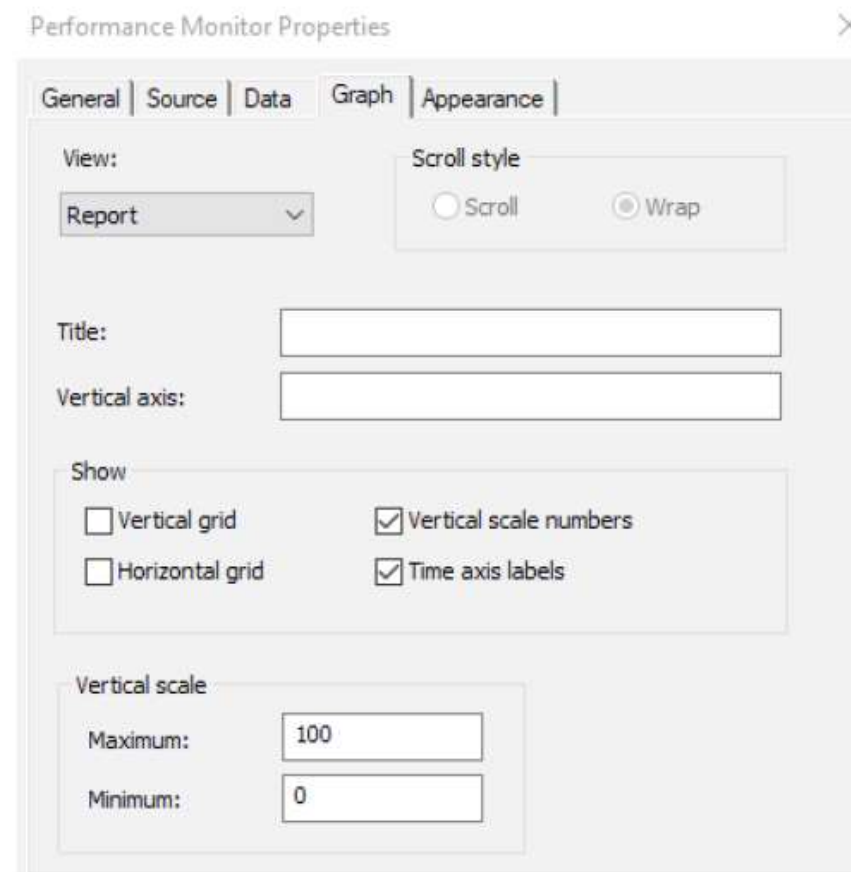
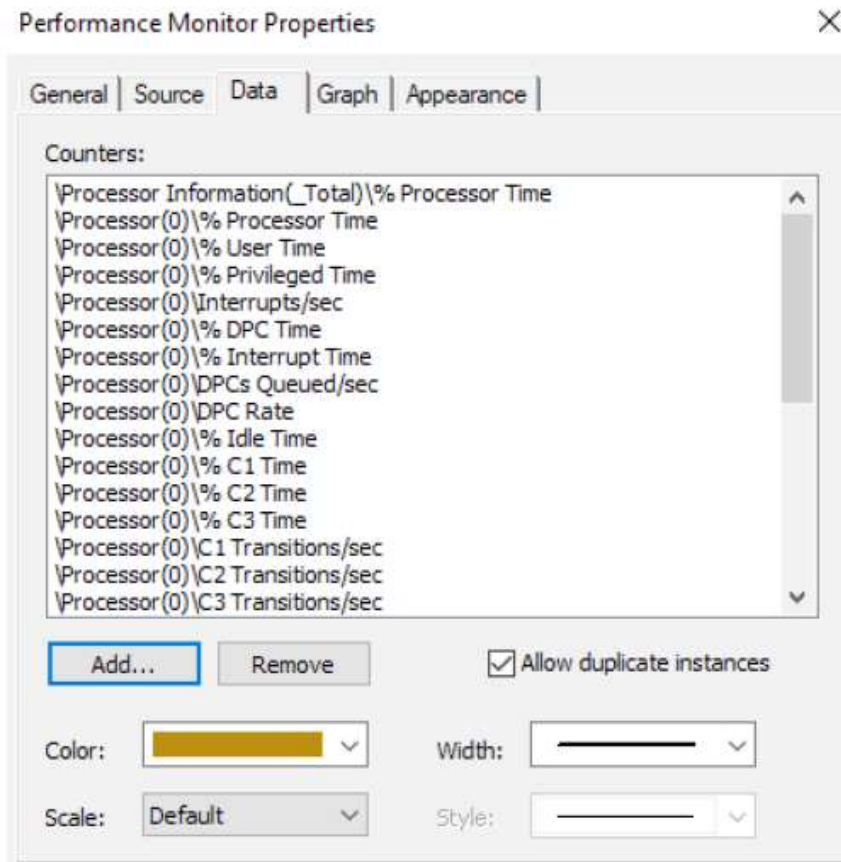
☐ Database:

System DSN:

Log set:



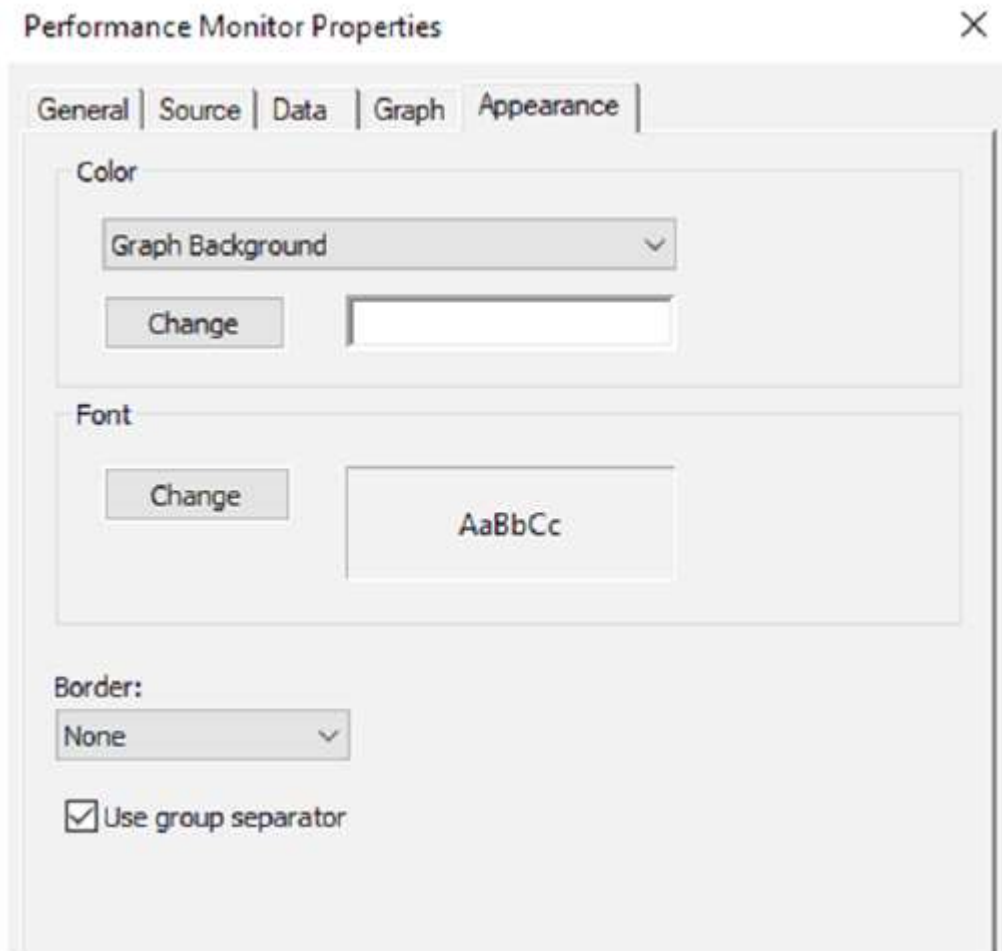
ИНСТРУМЕНТЫ





ИНСТРУМЕНТЫ

Просмотр событий



Используя вкладку **Оформление**, вы можете указать цвета для областей отображения, например фона и переднего плана. Вы также можете указать шрифты, которые используются для отображения значений счетчика в представлениях системного монитора. Вы можете изменить настройки, чтобы найти подходящий баланс между читабельностью и количеством информации, отображаемой на одном экране. Наконец, вы можете настроить свойства для рамки.



ИНСТРУМЕНТЫ

Сохранение и анализ данных в журналах оповещений и производительности

При просмотре информации в системном мониторе у вас есть две основные опции в отношении отображаемых данных:

1. Просмотр текущей активности (*View Current Activity*)

При первом открытии оснастки [Производительность](#) из папки [Администрирование](#) по умолчанию используется просмотр данных, полученных из текущей системной информации. Этот метод просмотра измеряет и отображает различные статистические данные в реальном времени о производительности системы.

2. Просмотр данных файла журнала (*View Log File Data*)

Этот параметр позволяет вам просматривать информацию, которая ранее была сохранена в файле журнала. Хотя объекты производительности, счетчики и экземпляры могут казаться такими же, как и просмотренные с помощью параметра [Просмотреть текущую активность](#), сама информация была записана в предыдущий момент времени и сохранена в файле журнала.

Файлы журналов для параметра [Просмотр данных файла журнала](#) создаются в разделе [Журналы оповещения производительности](#) в инструменте [Производительность](#).

ИНСТРУМЕНТЫ



Три элемента позволяют настраивать способ сбора данных в файлах журнала:

1. Журналы счетчиков (*Counter Logs*)

Регистрируется статистика производительности на основе различных объектов производительности, счетчиков и экземпляров, доступных в Системном мониторе. Значения обновляются на основе установки временного интервала и сохраняются в файле для последующего анализа.

2. Циклическое ведение журнала (*Circular Logging*)

При циклическом протоколировании данные, хранящиеся в файле, перезаписываются при вводе новых данных в журнал. Это полезный метод ведения журнала, если вы хотите записывать информацию только на определенный период времени (например, за последние четыре часа). Циклический журнал также позволяет сохранить дисковое пространство, гарантируя, что файл журнала производительности не будет продолжать расти по мере добавления новых данных.

3. Линейное ведение журнала (*Linear Logging*)

В режиме линейного ведения журнала данные никогда не удаляются из файлов журнала, а новая информация добавляется в конец файла журнала. Результатом является файл журнала, который постоянно растет. Выгода заключается в том, что вся накопленная информация сохраняется.



ИНСТРУМЕНТЫ

Использование других инструментов контроля производительности

Системный монитор позволяет отслеживать различные параметры операционной системы Windows 10 и связанных с ней сервисов и приложений. Тем не менее, вы также можете использовать три других инструмента для мониторинга производительности в Windows 10.

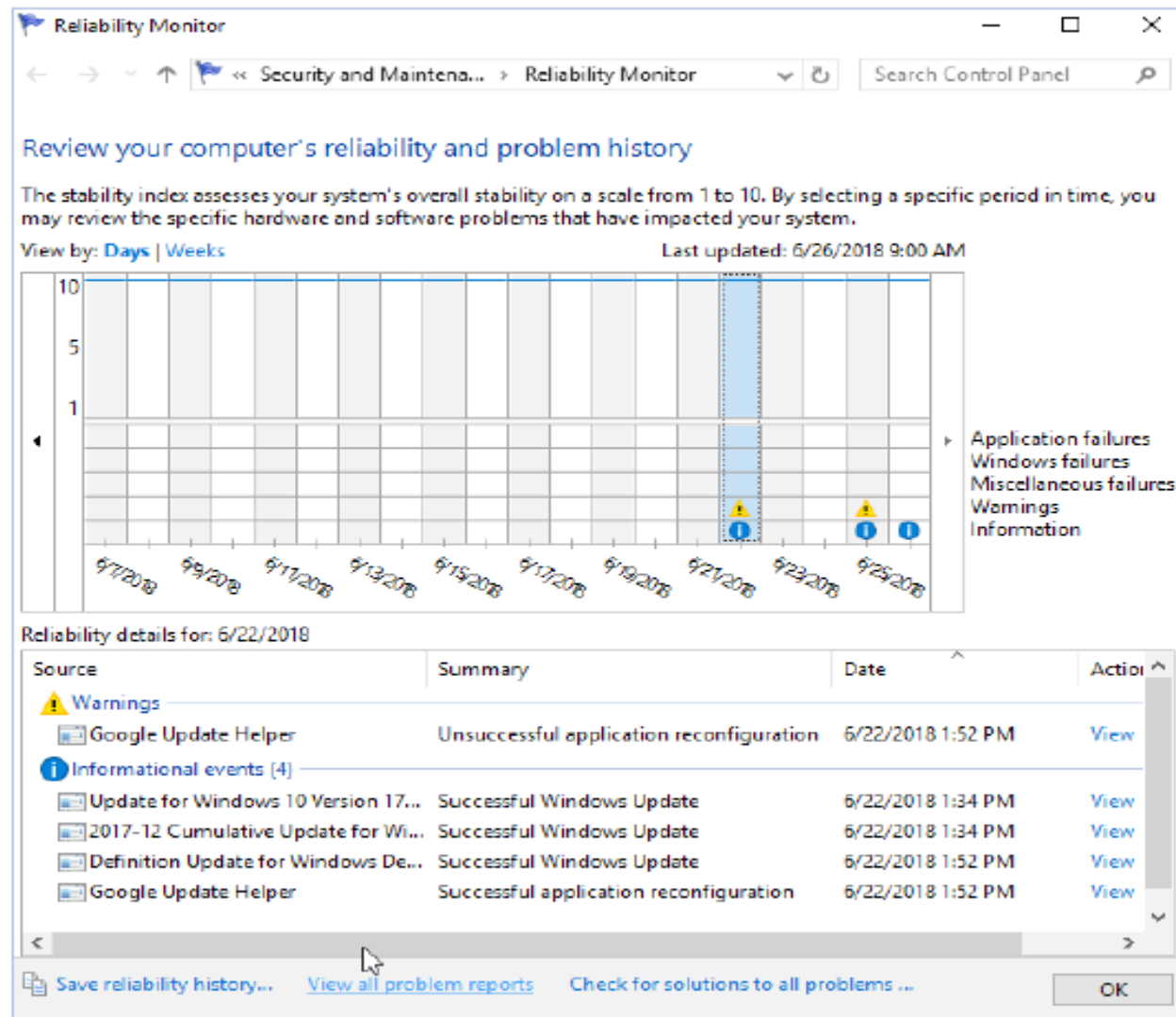
Это – [Монитор стабильности системы](#) (*Reliability Monitor*), [Диспетчер задач](#) (*Task Manager*) и [Просмотр событий](#) (*Event Viewer*). Все три из этих инструментов полезны для мониторинга различных областей общей производительности системы и для изучения деталей, связанных с конкретными системными событиями. В следующих разделах мы рассмотрим эти инструменты и то, как их лучше всего использовать.

ИНСТРУМЕНТЫ



Монитор стабильности системы

Монитор стабильности системы Windows 10 является частью оснастки **Мониторинг надежности и производительности Windows** для Microsoft Management Console (MMC). Самый простой способ доступа к монитору надежности – ввести «надежность» (*reliability*) в поле **Поиск** и выбрать **Просмотр журнала надежности...** (*View reliability history...*) в появившихся результатах.

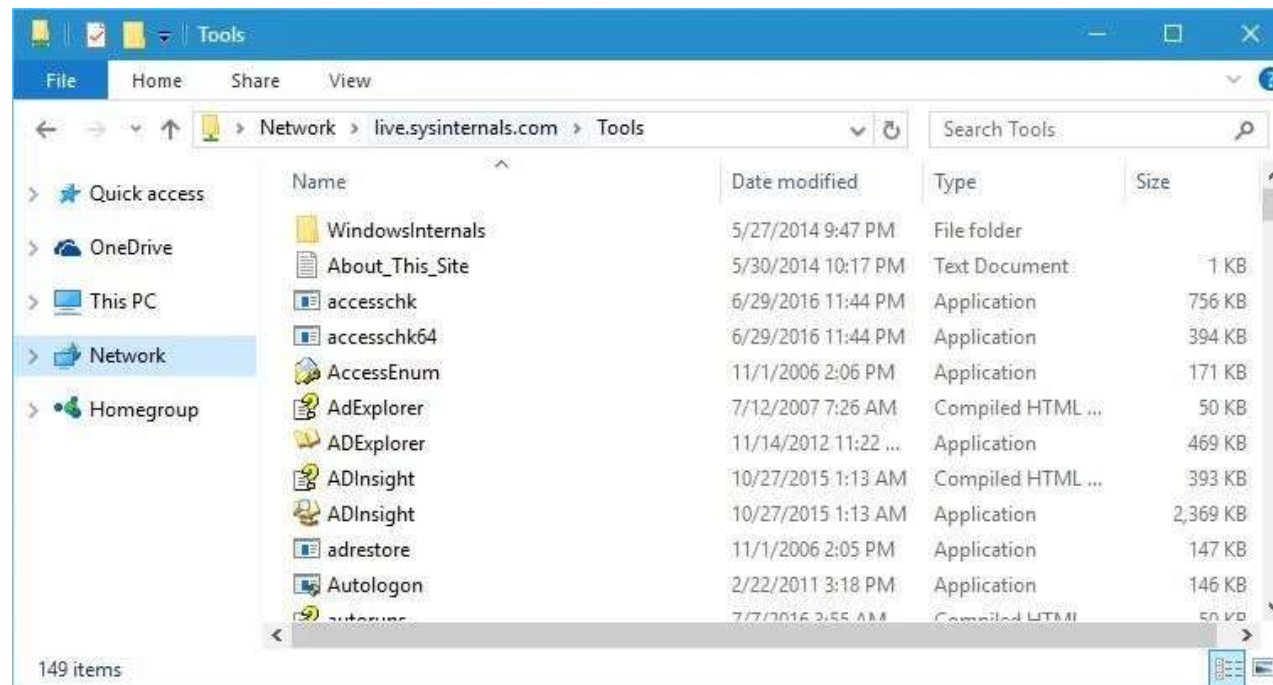


ИНСТРУМЕНТЫ



Sysinternals Utilities

Коллекция системных утилит, разработанная для того, чтобы помочь пользователям диагностировать и устранить проблемы с приложениями и службами Windows. Так как Windows является самой распространенной операционной системой, многие программы должны быть совместимы с ее функциями во избежание ошибок.



Перед тем, как программа может быть представлена конечным пользователям, она должна быть протестирована и проанализирована. Некоторые приложения как раз предназначены для этой цели и являются полезными инструментами для разработчиков. Решение включает более 70 утилит, предназначенных для обнаружения и исправления ошибок, связанных с дисковой подсистемой, сетью и проблемами безопасности, а также для предоставления информации о процессах и системе.

<https://learn.microsoft.com/en-us/sysinternals/downloads/?source=recommendations>