Полезное

- Изменить часовой пояс из командной строки с помощью TZutil
- Как полностью удалить принтер в Windows, если он не удаляется
- Включение Secure Boot
- Как включить TPM на компьютере или ноутбуке

Изменить часовой пояс из командной строки с помощью TZutil

Для управления часовым поясом в Windows можно использовать встроенную утилиту `tzutil.exe` (Windows Time Zone Utility).

Вывести идентификатор текущего часового пояса (TimeZoneID):

```
tzutil /g
```

```
Russian Standard Time
```

tzutil /g узнать текущий часовой пояс компьютера

Выведите список всех часовых поясов с их параметрами и названиями:

```
tzutil /l
```

tzutil /l список всех часовых поясов

Если вам нужно быстро найти вывести все часовые пояса, с определенным с сдвигом, например UTC +2, выполните команду:

```
tzutil /l | find /I "utc+02"
```

поиск временных зон по UTC смещению

Чтобы изменить текущий часовой часовой пояс (UTC+03:00) Москва, Санкт-Петербург, Волгоград – (Russian Standard Time) на (UTC+04:00) Ижевск, Самара (Russia Time Zone 3), выполните команду:

```
tzutil /s "Russia Time Zone 3"
```

Как полностью удалить принтер в Windows, если он не удаляется

Штатные способы удаления принтера в Windows

Сначала рассмотрим стандартные способы удаления принтеров в Windows, которые нужно обязательно попробовать.

1. Укройте панель управления Settings -> Devices -> Printers and Scanners (или выполните команду быстрого доступа `ms-settings:printers`);
2. Выберите принтер, который вы хотите удалить и нажмите **Remove Device**;
   Удалить принтер в панели Параметры
3. Подтвердите удаление принтера

Если при удалении принтера появляется ошибка “Локальная подсистема печати не выполняется”, проверьте настройки службы spooler согласно инструкции.

Также вы можете удалить принтер из классической Панели управления Windows:

1. Выполните команду `control /name Microsoft.DevicesAndPrinters` ;
2. Выберите принтер в списке и нажмите на кнопку **Remove Device**;

Удалить принтер из классической панели управления Windows

Обратите внимание, что, если в очереди печати принтера есть активные задания печати, вы не сможете удалить его, пока не очистите очередь печати. Чтобы очистить очередь печати, найдите принтер в панели управления и выберите опцию **Open queue**. Выберите опцию Printer -> Cancel All Document.

очистка очереди печати принтера

Попробуйте удалить принтер после очистки очереди печати.

Обратите внимание, что сетевые принтеры могут устанавливаться с помощью групповых политик. В зависимости от настроек GPO, такие принтеры не всегда можно удалить.

Для удаления принтера можно использовать mmc консоль **Print Management** (несколько раз она помогла мне удалить принтер, который не отображался в панели управления Windows).

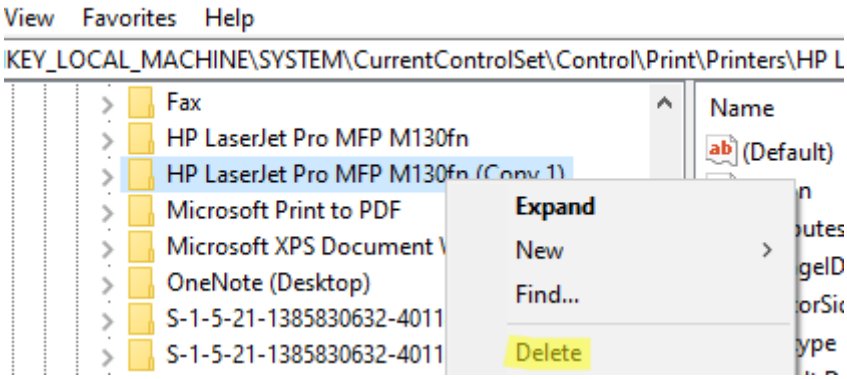
1. Запустите консоль командой `printmanagement.msc` ;
2. Перейдите в раздел Print Manager -> Print Servers -> выберите ваш компьютер -> Printers;
3. Выберите принтер и в контекстном меню нажмите Delete.

   удалить принтер в консоли print management

Принудительное удаление принтера в Windows

Если по каким-то причинам принтер не отображается в панели управления или не удаляется с ошибкой, вы можете принудительно удалить его.

1. Запустите `regedit.exe` ;
2. Перейдите в ветку HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Printers;
3. Найдите раздел с именем вашего принтера (в моем примере это `HP LaserJet Pro MFP M130fn (Copy 1)` ;
4. Удалите ветку реестра принтера;



5. Перезагрузите компьютер и проверьте, что принтер исчез из панели управления. Если он не исчез, но его статус изменился на *Not Connected,* просто удалите его.

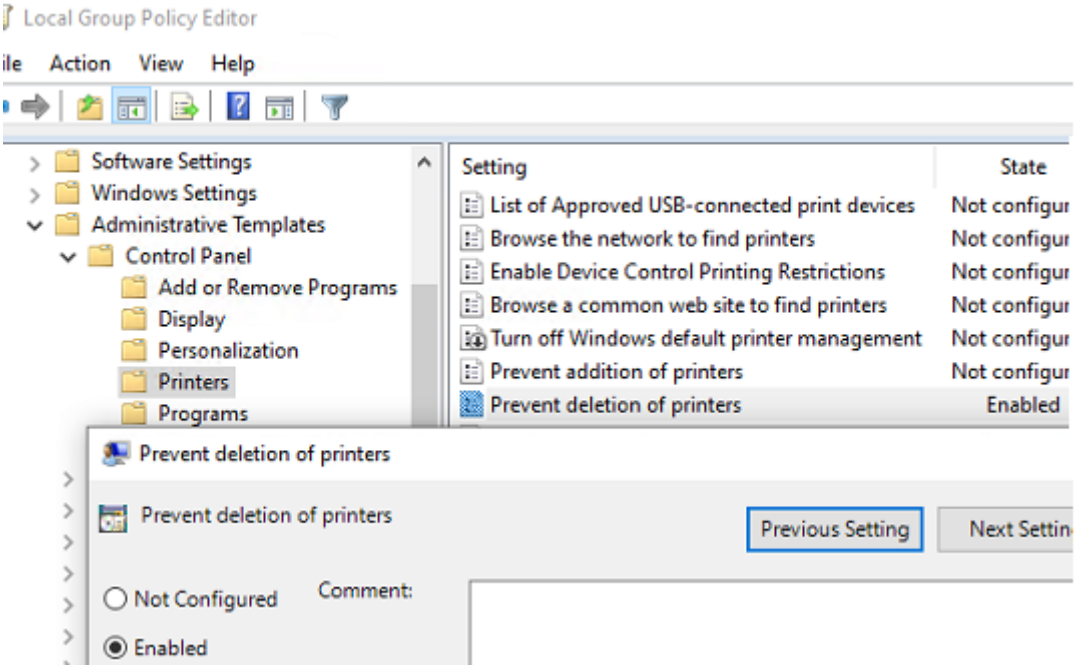
   При удалении принтера может появится ошибка:

> Операция отменена из-за ограничений, действующих на этом компьютере. Обратитесь к системному адми

> This operation has been cancelled due to restrictions in effect on this computer. Please contact your system admir

ошибка удаления принтера - Операция отменена из-за ограничений, действующих на этом кс

В этом случае проверьте, не включена ли параметр групповой политика, запрещающий удалять принтеры. Этот параметр находится в следующем разделе локального редактора GPO (gpedit.msc): User Configuration –> Administrative Templates –> Control Panel –> Printers.



На доменном компьютере проверьте результирующие настройки GPO с помощью утилиты gpresult.

Если политика отключена или не настроена, нужно удалить скрытые принтеры и очереди печати в диспетчере устройств. Такая проблема часто встречается с сетевыми принтерами.

1. Запустите Device Manager (`devmgmt.msc`);
2. Включите опцию **View** -> **Show hidden devices**
3. Разверните секции **Print queues** и **Printers** и удалите ненужные принтеры.
   удаление скрытых принтеров в диспетчере устройств

Удаление драйвера принтера в Windows

При удалении принтера из панели управления, его драйвера остаются в Windows. Если вы удалили принтер из панели управления, и хотите удалить его драйвер печати:

1. Откройте оснастку `services.msc` и перезапустите службу Диспетчер Печати (Print Spooler). Можно перезапустить службу PowerShell командой: Restart-Service spooler -Verbose
2. Откройте оснастку управления печатью `printmanagement.msc` ;
3. Разверните секцию Print Manager -> Print Servers -> выберите ваш компьютер -> Drivers;
4. В списке перечислены все установленные драйвера принтеров;
5. Щелкните правой кнопкой по драйверу, который вы хотите удалить и выберите **Удалить пакет драйвера** (**Remove driver package**)
   .удалитб драйвер принтера в Windows

6. Подтвердите удаление драйвера, его inf файла и всех связанных файлов.
7. удаление пакета драйвера в диспетчере печати

Также вы можете удалить ненужные драйвера в свойствах сервера печати. Для этого выполните команду `printui /s /t2` , выделите драйвер принтера и нажмите кнопку **Delete**.

удалить драйвер принтера панель управления

Включение Secure Boot

Перед включением убедитесь, что диск переведен в формат GPT. Это можно сделать без потери данных с помощью встроенной утилиты MBR2GPT.

Дальше следуйте пошаговой инструкции:

1. Определите номер системного диска. Откройте «Управление дисками» (командная строка / без кавычек «diskmgmt.msc») и найдите диск с разделом «Зарезервировано системой». Обычно это диск «0». Важно: у системного раздела должно быть не менее 100 МБ — утилита создаст новый EFI-раздел, если старый меньше.
2. Перейдите в среду восстановления Windows. Зажмите «Shift» и выберите «Перезагрузка» / «Поиск и устранение неисправностей» / «Дополнительные параметры» / «Командная строка». После перезагрузки войдите под своей учетной записью.
3. Выполните проверку совместимости диска**.** Введите поочередно: «mbr2gpt /validate /disk:0».
4. Если все в порядке, появится сообщение «Validation completed successfully». Если ошибка — уточните номер диска.
5. Начните преобразование**.** Введите команды: mbr2gpt / convert / disk:0

Через несколько секунд появится отчет об успешной конвертации. После этого «обратной дороги нет» — диск теперь в GPT.

Теперь следует убедиться, что режим загрузки в BIOS установлен в UEFI, а не Legacy, и сама система поддерживает UEFI. В этом можно убедиться, поискав в интернете модель вашей материнской платы и увидев там поддержку UEFI.

Включение Secure Boot

Для того, чтобы включить Secure Boot:

1. Перезагрузите компьютер и войдите в BIOS/UEFI (клавиша Del, F2, F10 или Esc — зависит от модели).
2. Найдите вкладку Boot или Security.
3. Активируйте параметр Secure Boot **/** Enabled.
4. Если система просит установить ключи — выберите Install Default Keys.
5. Сохраните изменения (F10) и перезагрузите ПК.

Помните, что расположение опции на популярных материнских платах разнится:

- ASUS — Boot → Secure Boot → OS Type → Windows UEFI Mode.
- MSI — Settings → Advanced → Windows OS Configuration.
- Gigabyte — BIOS Features → Secure Boot.
- ASRock — Security → Secure Boot.
- Acer / Lenovo / HP — обычно во вкладке Security, иногда требуется установить Supervisor Password.

Частые ошибки и их решения

Система не загружается после включения

Причина — неподписанный загрузчик. Решение: отключите Secure Boot, загрузитесь в Windows, установите обновления и проверьте наличие ключей Microsoft в UEFI.

Secure Boot «Отключено» при активной настройке

Такое бывает, если включен CSM (Compatibility Support Module). Отключите его полностью, иначе UEFI не применит защиту.

Конфликт с BitLocker

BitLocker может запросить ключ восстановления после изменения параметров загрузки. Рекомендуется приостановить шифрование перед изменениями.

Ошибки с Linux

Многие дистрибутивы (Ubuntu, Fedora) поддерживают Secure Boot, но кастомизированные ядра или драйверы требуют подписи. Решение — временно отключить Secure Boot или создать локальный ключ через «mokutil».

Альтернативный путь с переустановкой Windows

Если вы включили Secure Boot, но ничего выше вам не помогло, то можно настроить безопасную загрузку через переустановку системы:

- Используйте программу Rufus для монтирования образа новой Windows.
- При установке переконвертируйте диск в формат GPT.
- В крайних случаях обновите прошивку BIOS/UEFI — старые версии могут работать некорректно с новыми ключами Microsoft.

Как включить TPM на компьютере или ноутбуке

Установка Windows 11, действия, связанные с шифрованием, а в последнее время — некоторое ПО, игры и их модули могут требовать наличия и включения модуля TPM 2.0 (или иной версии) в системе.

В этой простой инструкции несколько примеров включения модуля TPM (Trusted Platform Module) в БИОС/UEFI ноутбуков и компьютеров при его наличии в системе, а также дополнительная информация, которая может пригодиться в контексте рассматриваемой темы.

Проверяем: возможно, TPM уже включён

Прежде чем выполнять далее описываемые действия, рекомендую заглянуть в диспетчер устройств, привожу пример для Windows 11/10:

1. Нажмите правой кнопкой мыши по кнопке Пуск и выберите пункт «Диспетчер устройств» в контекстном меню, либо нажмите клавиши **Win+R** на клавиатуре, введите **devmgmt.msc** и нажмите Enter.
2. В диспетчере устройств обратите внимание на наличие раздела «Устройства безопасности» и на его содержимое.Модуль TPM 2.0 в диспетчере устройств

Если такой раздел есть, а в нем вы видите «Доверенный платформенный модуль», то что-либо включать не требуется, TPM на вашей системе уже включён и, судя по всему, работает.

Дополнительно вы можете:

1. Использовать команду **get-tpm** в PowerShell (от имени Администратора) чтобы получить сведения о модуле TPM.Статус TPM в PowerShell
2. Нажать клавиши **Win+R** и ввести **tpm.msc** для перехода в консоль управления TPM, где также присутствуют сведения о его готовности к работе. На скриншоте — пример отображения, когда модуль TPM 2.0 или 1.2 включен (иначе вы получите сообщение о его отсутствии):
   Просмотр состояния и настройка модуля TPM в оснастке tpm.msc

В случае, когда доверенного платформенного модуля TPM не наблюдается, но вы уверены, что на вашем ноутбуке или ПК он в наличии, вероятнее всего, он отключен в БИОС и его можно включить.

Включение модуля TPM в БИОС/UEFI

В зависимости от производителя материнской платы или ноутбука, включение модуля TPM 2.0 (или иной версии) может располагаться в разных разделах настроек БИОС, как правило — в Security, Advanced, в подразделах, связанных с Trusted Computer или Trusted Platform Module (TPM).

Во всех случаях сначала нужно зайти в БИОС/UEFI, а после нахождения нужного раздела настроек — убедиться, что Trusted Platform Module (TPM и другие обозначения, примеры будут приведены далее) включён (Enabled). Если нужный пункт отсутствует, есть вероятность, что ваша система не оснащена этим устройством.

Далее — несколько распространённых примеров опции включения доверенного платформенного модуля на различных ПК и ноутбуках и её наименования, по аналогии можно будет найти нужный пункт и в других версиях БИОС (UEFI):

- На ПК **с процессорами Intel** вместо TPM может присутствовать опция включения PTT — что, по сути, то же самое, но речь идёт не о дискретном модуле TPM, а о встроенном, обычно на уровне процессора:Включение Intel PTT
- На ПК **с процессорами AMD** также возможен вариант иного обозначения для «программного» модуля TPM — fTPM (Firmware TPM). Также на скриншоте вы можете увидеть опцию «Route to SPI TPM» — переключение на дискретный модуль TPM при его наличии:Включение fTPM в БИОС/UEFI
- В некоторых вариантах интерфейса можно встретить переключение между dTPM (отдельный модуль TPM) и Firmaware TPM (fTPM, PPT):Выбор между fTPM и dTPM
- На материнских платах **ASUS** обычно требуется зайти в Advanced — Trusted Computing и переключить TPM Support и TPM State в Enabled.Включение TPM на Asus
- На ноутбуках **HP** загляните в раздел Security, TPM Device должно быть установлено в «Available», TPM State — «Enable».Включить TPM на HP

- На ноутбуках **Lenovo** обратите на раздел Security, а в нём — подраздел «Security Chip», он должен быть Active.
- На **MSI** в разделе Advanced следует найти Trusted Computing и убедиться, что Security Device Support установлено в Enabled.
- На некоторых ноутбуках **Dell** — раздел Security, в подразделе TPM 2.0 включаем пункт TPM On и Enabled.Включить TPM на ноутбуке Dell
- На **Gigabyte** — возможен вариант размещения в разделе Advanced, подразделе Trusted Computing.

Большинство современных устройств оснащаются либо дискретным модулем TPM либо имеют возможность включения Firmware TPM — опцию обычно сравнительно легко найти, используя примеры, приведённые выше.

Дополнительная информация

На многих современных материнских платах ПК также присутствует разъём для подключения дискретного доверенного платформенного модуля, который можно приобрести отдельно:

Дискретный модуль TPM 2.0

Обычно для рядового пользователя это не требуется, но если вы решите установить такой модуль, ознакомьтесь с документацией о совместимости конкретно для вашей материнской платы в инструкции к ней: могут отличаться не только разъёмы подключения, но и присутствовать требования к конкретным совместимым модулям TPM 2.0.

Частый вопрос пользователей — взаимосвязь модуля TPM 2.0 и функции безопасной загрузки Secure Boot. Они не являются взаимозависимыми: то есть доверенный платформенный модуль может функционировать без безопасной загрузки, а она — без модуля TPM. Однако, при одновременном использовании они работают совместно, например Secure Boot может использовать ключи из TPM для проверки целостности процесса загрузки. При этом некоторое ПО может требовать включения обоих элементов безопасности.

В случае, если ваше устройство не оснащено модулем TPM 2.0, а цель включения — установка Windows 11 или обновление до её новой версии, не торопитесь менять компьютер, не исключено что доверенный платформенный модуль вам не потребуется, для установки есть самые различные способы, например — такой. При необходимости включения шифрования BitLocker без доверенного платформенного модуля используйте инструкцию Как включить BitLocker без TPM.