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.

Revision #1
Created 20 February 2026 12:29:35 by admin_vy
Updated 20 February 2026 12:30:23 by admin_vy