

### Выберите способы разблокировки диска

- ☒ Использовать пароль для снятия блокировки диска

Пароли должны содержать прописные и строчные буквы, цифры, пробелы и символы.

Введите свой пароль

Введите пароль еще раз


- ☐ Использовать смарт-карту для снятия блокировки диска

Необходимо будет вставить смарт-карту. ПИН-код смарт-карты потребуется при снятии блокировки с диска.

Далее

Отмена

×

←  Шифрование диска BitLocker (D:)

Выберите способы разблокировки диска

☒ Использовать пароль для снятия блокировки диска

Пароли должны содержать прописные и строчные буквы, цифры, пробелы и символы.

Введите свой пароль

Введите пароль еще раз


☐ Использовать смарт-карту для снятия блокировки диска

Необходимо будет вставить смарт-карту. ПИН-код смарт-карты потребуется при снятии блокировки с диска.


Далее

Отмена

×

←  Шифрование диска BitLocker (D:)

Как вы хотите архивировать свой ключ восстановления?

 Ваш ключ восстановления сохранен.

Если вы забыли свой пароль или потеряли смарт-карту, вы можете использовать ключ восстановления для доступа к диску.

→ Сохранить в вашу учетную запись Майкрософт

→ Сохранить в файл

→ Напечатать ключ восстановления

[Как найти позже ключ восстановления?](#)

Далее

Отмена



←  Шифрование диска BitLocker (D:)

### Укажите, какую часть диска требуется зашифровать

Если вы настраиваете BitLocker на новом диске или ПК, вам достаточно зашифровать только ту часть диска, которая сейчас используется. BitLocker зашифровывает новые данные автоматически по мере их добавления.

Если вы включаете BitLocker на уже используемом ПК или диске, рекомендуется зашифровать весь диск. Это гарантирует защиту всех данных — даже удаленных, но еще содержащих извлекаемые сведения.

- ☒ Шифровать только занятое место на диске (выполняется быстрее, оптимально для новых ПК и дисков)
- ☐ Шифровать весь диск (выполняется медленнее, подходит для уже используемых ПК и дисков)

Далее

Отмена

### Выбрать режим шифрования для использования

В обновлении Windows 10 (версия 1511) представлен новый режим шифрования дисков (XTS-AES). Этот режим обеспечивает дополнительную поддержку целостности, но не совместим с более ранними версиями Windows.

Если вы собираетесь использовать съемный носитель с более ранней версией Windows, следует выбрать режим совместимости.

Если будет использоваться несъемный диск или этот диск будет использоваться на устройствах под управлением обновления Windows 10 (версия 1511) или более поздних версий, следует выбрать новый режим совместимости

- ☐ Новый режим шифрования (оптимально для несъемных дисков на этом устройстве)
- ☒ Режим совместимости (оптимально для дисков, которые могут быть перемещены с этого устройства)

Далее

Отмена

### Зашифровать этот диск?

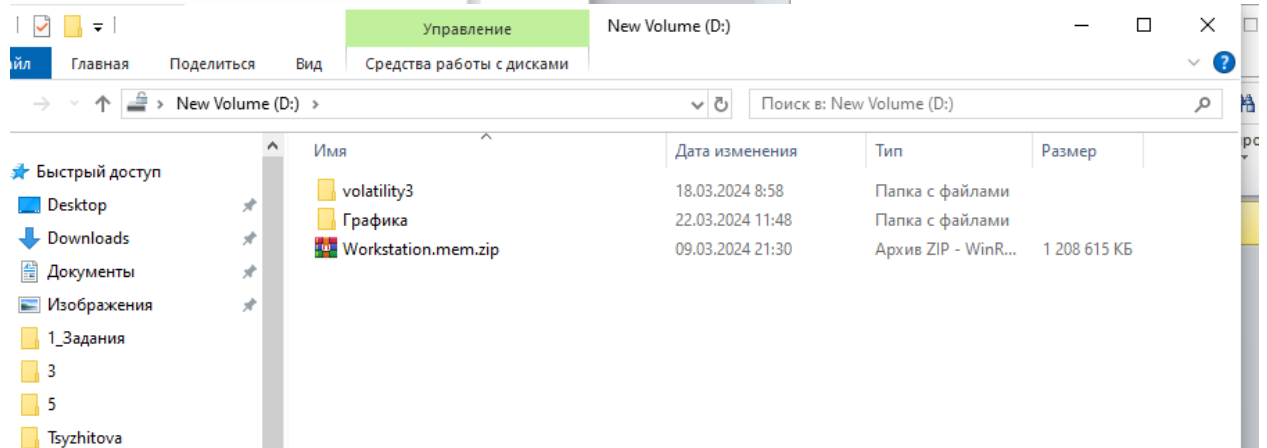
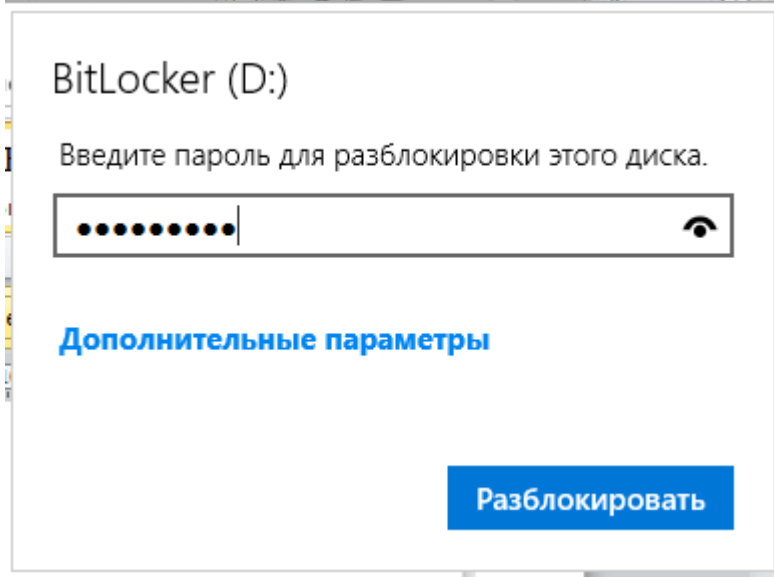
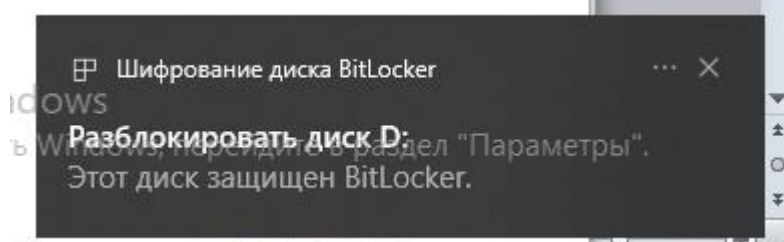
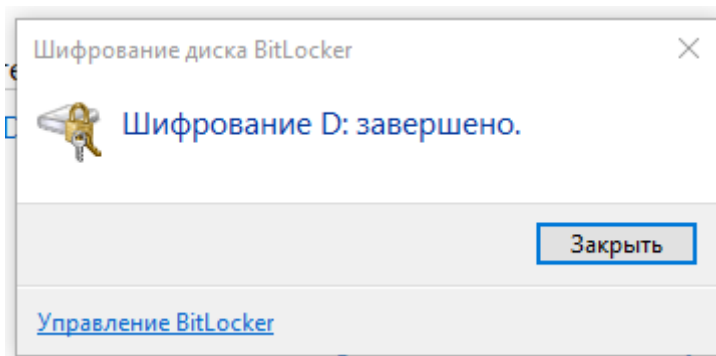
Вы сможете разблокировать этот диск с помощью пароля.

Процесс шифрования может быть долгим, его длительность зависит от размера диска.

До завершения шифрования защита файлов не обеспечивается.

Начать шифрование

Отмена



## New Volume (D:) BitLocker включен



[Архивировать ключ восстановления](#)

[Сменить пароль](#)

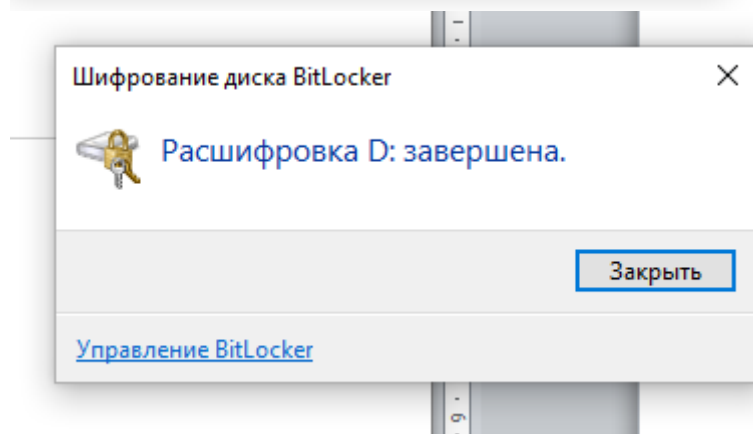
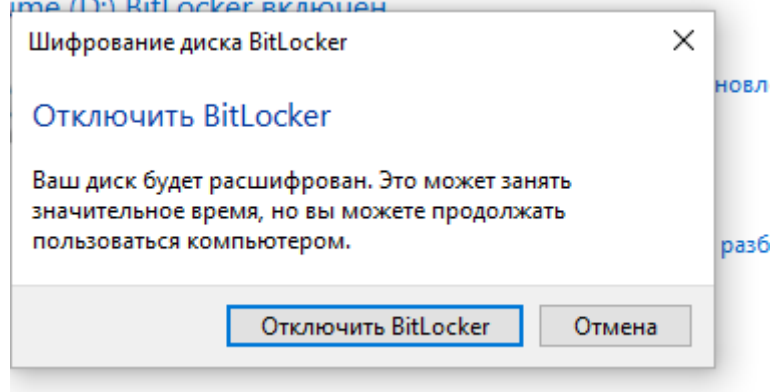
[Удалить пароль](#)

[Добавить смарт-карту](#)

[Включить автоматическую разблокировку](#)

[Отключить BitLocker](#)

## New Volume (D:) BitLocker включен



## New Volume (D:) BitLocker отключен



[Включить BitLocker](#)