



# Полнодисковое шифрование

Максим Петров (Access Now)  
maxim@accessnow.org

- 
- Зачем нужно полное шифрование?
  - Полное шифрование на стационарных компьютерах/ноутбуках.
  - Шифрование данных на мобильных устройствах.
  - Резервное копирование данных.

# Зачем нужно полное шифрование?



Ведь:

- Мне нечего скрывать.
- У меня уже стоит пароль на вход.
- Мое устройство всегда со мной.

# Полнодисковое шифрование на компьютерах

---

Стандартные инструменты:

- BitLocker для Windows

<https://support.microsoft.com/ru-ru/windows/ad5dcf4b-dbe0-2331-228f-7925c2a3012d>

- FileVault для macOS

<https://support.apple.com/ru-ru/guide/mac-help/mh11785/mac>

- DM-Crypt для Linux

<https://losst.ru/shifrovanie-diskov-v-linux>

Стороннее кросс-платформенное решение - VeraCrypt

<https://safe.roskomsvoboda.org/veracrypt>

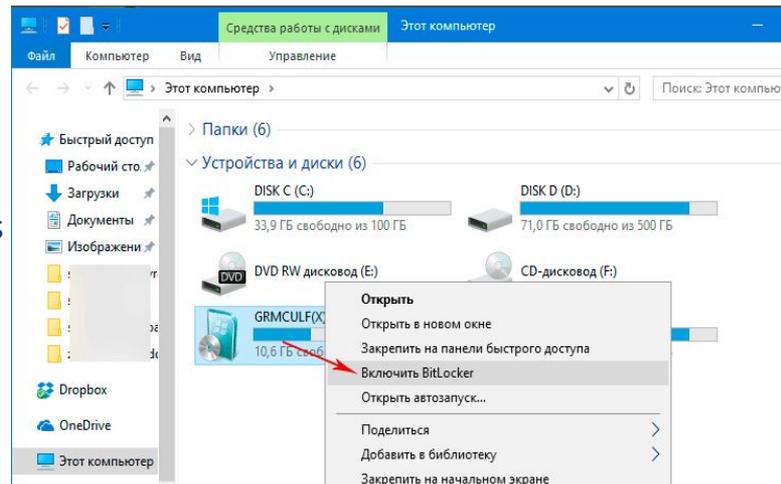
# BitLocker для Windows

- Версии Windows, поддерживающие шифрование BitLocker

- Оборудование с TPM

<https://remontka.pro/bitlocker-without-tpm-windows>

- Включение BitLocker
- Ключ восстановления

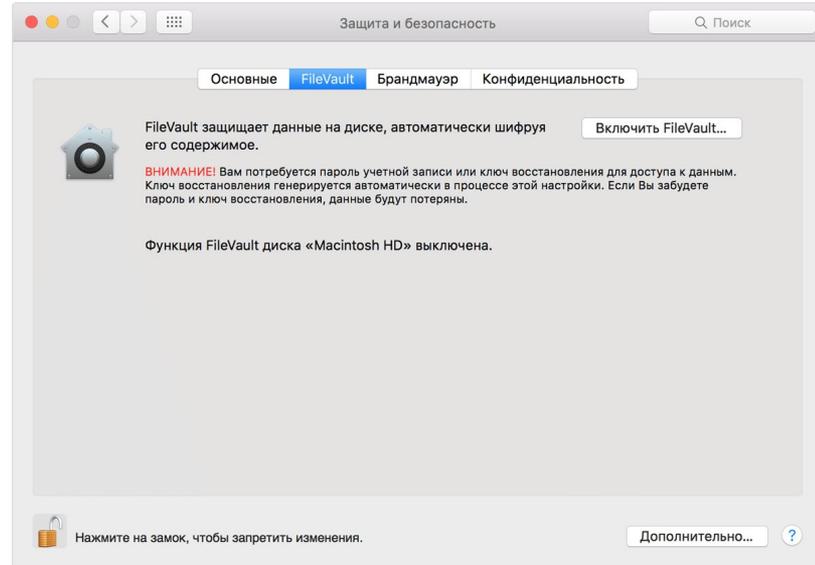


<https://support.microsoft.com/ru-ru/windows/oc453637-bc88-5f74-5105-741561aae838>

# FileVault для macOS

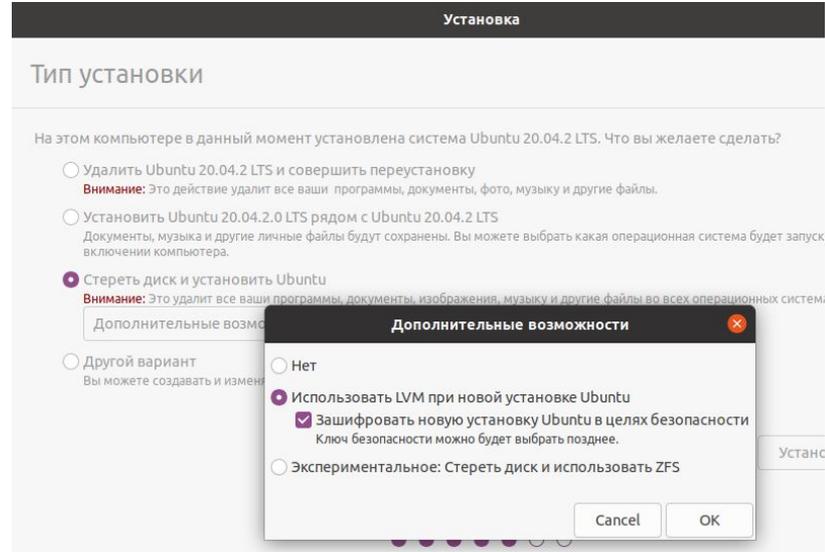
- Версии macOS, поддерживающие шифрование FileVault 2
- Включение FileVault
- Сброс пароля

<https://support.apple.com/ru-ru/HT204837>



# Dm-crypt в Linux

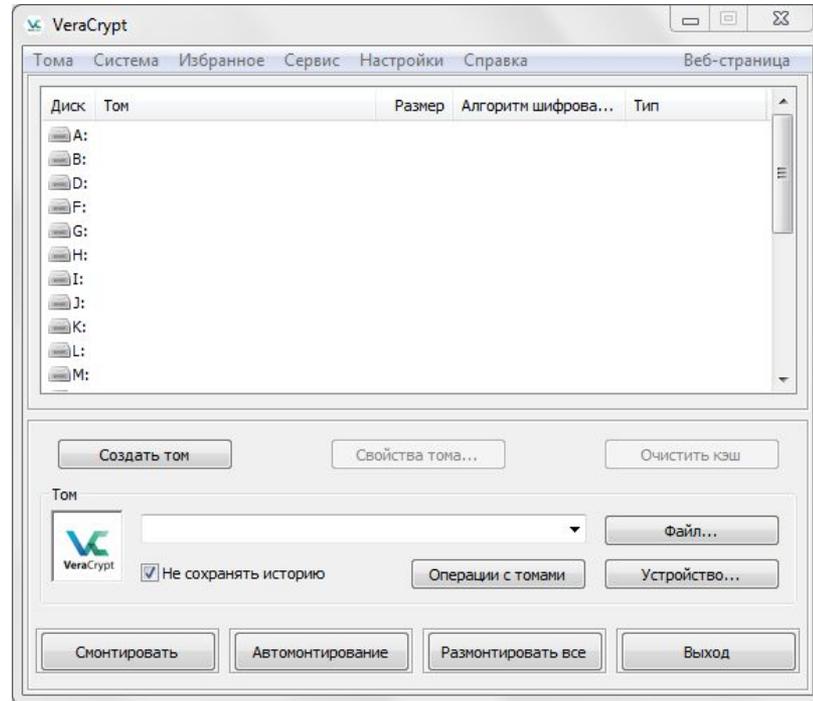
- Что такое dm-crypt?
- Утилита Cryptsetup
- Шифрование при установке Ubuntu



# VeraCrypt

- Совместимость с операционными системами
- Возможности VeraCrypt
  - Создание зашифрованного контейнера
  - Создание скрытого тома
  - Шифрование диска

<https://veracrypt.fr/en/Home.html>



# Шифрование данных на мобильных устройствах



- Шифрование в iOS
- Шифрование в Android

# Шифрование данных в iOS

---

- Настройка шифрования  
<https://support.apple.com/ru-ru/guide/iphone/iph14a867ae/ios>
- Эффективность шифрования, исключения.
- Шифрование резервных копий (iCloud и iTunes)  
<https://support.apple.com/ru-ru/HT205220>  
<https://support.apple.com/ru-ru/HT202303>  
<https://support.apple.com/ru-ru/HT203977>

# Шифрование данных в Android

- FDE (Full Disk Encryption) или FBE (File Based Encryption)?

<https://play.google.com/store/apps/details?id=com.termux>

```
$ getprop ro.crypto.type  
file  
block  
$
```

FBE

FDE

- Как защитить смартфон на Android?

<https://blog.elcomsoft.ru/2019/07/antikriminalistika-kak-zashhitit-smartfon-na-android/>

# Рекомендации по настройкам Android устройств

- Используйте надежный код блокировки (не короче 6 цифр),
- Отключите отладку по USB,
- Не используйте телефон с разблокированным загрузчиком,
- Установить режим по умолчанию при подключении к компьютеру - "Только зарядка",
- Обновляйте Android, или замените телефон на актуальную модель,
- Отключите SmartLock (разблокировка по лицу, в знакомом месте, bluetooth и т.д.),
- Отключите задержку блокировки телефона,
- Не разрешайте установку из неизвестных источников,
- Запретите лишним приложениям разрешение "Draw over other apps" (снимки экрана),
- Проверьте пункт Device admin apps (удаленно заблокировать устройство),
- Опасайтесь встроенных производителями backdoors,
- Обращайте внимание на разрешения приложений,
- Не храните пароль от аккаунта Google в браузере,
- Включите двухфакторную аутентификацию,
- Предосторожность в путешествии.

# Резервное копирование данных

---

- Windows (локальное и OneDrive)

<https://support.microsoft.com/ru-ru/windows/352091d2-bb9d-3ea3-ed18-52ef2b88cbef>

<https://support.microsoft.com/ru-ru/office/93efdc74-424e-4d56-97ce-84125e5ce87f>

- Mac OS (локальное и iCloud Drive)

<https://support.apple.com/ru-ru/HT201250>

<https://support.apple.com/ru-ru/HT204025>

- iOS (iTunes и iCloud)

<https://support.apple.com/ru-ru/guide/iphone/iph3ecf67d29/ios>

- Android (локальное и Google Диск)

<https://support.google.com/android/answer/2819582>

- Сторонние поставщики облачного хранения данных

<https://mega.io/>

<https://www.backblaze.com/>

# Вопросы

