Kripta

Руководство пользователя

Пошаговое шифрование USB-накопителей и разделов с восстановлением пароля через службу поддержки компании.



Версия 1.2 · Windows · macOS · Linux

Ноябрь 2026

Содержание

1 Что такое Kripta — назначение и требования

2 Первый запуск — корпоративная конфигурация и компоненты

3 Главное окно — индикаторы, уведомления, значок

4 Шифрование диска — мастер из 4 шагов

5 Разбиение диска на разделы — зашифрованная и свободная области

6 Работа с зашифрованным диском — разблокировка, открытие, блокировка

7 Смена пароля

8 Я забыл(а) пароль — восстановление через службу поддержки

9 Настройки — язык, конфигурация, обновления

10 Использование диска на других компьютерах

11 Сообщения и устранение неполадок

12 Часто задаваемые вопросы

A Приложение для ИТ-отдела — пакеты, подписанная конфигурация, языки

Обозначения

Тексты на экране (кнопки, заголовки, пункты) записаны так: **Зашифровать диск**. Снимки экрана сделаны в версии для macOS: в Windows и Linux окно такое же, отличаются только имена устройств (например, `E:` или `/dev/sdb1` вместо `/dev/disk4s1`).

1 Что такое Kripta

Kripta защищает данные на ваших **USB-накопителях** и **разделах** внешних дисков с помощью шифрования AES-256. После шифрования содержимое диска может прочитать только тот, кто знает пароль: если вы потеряете накопитель, никто другой не сможет его открыть.

Пошаговое шифрование
Четыре шага: выберите диск, задайте пароль, подтвердите, подождите.

Автоматическая разблокировка
При подключении зашифрованного диска Kripta сразу запрашивает пароль и открывает его.

Работает везде
Один и тот же накопитель открывается в Windows, macOS и Linux (стандартный формат VeraCrypt).

Самостоятельная установка
Kripta сам устанавливает и обновляет VeraCrypt; корпоративная конфигурация импортируется из файла.

Девять языков
Итальянский, английский, французский, испанский, немецкий, русский, арабский, китайский и японский, а также добавленные вами.

Восстановление через службу поддержки
Если вы забудете пароль, служба поддержки поможет задать новый без потери данных.

Что вам понадобится

- Установленная программа **Kripta**. При первом запуске Kripta сам установит **VeraCrypt** — модуль шифрования (в macOS также **FUSE-T**), если его нет: глава 2.
- **Подписанный файл конфигурации** (`.kripta-config`) от службы поддержки, если ИТ-отдел ещё не настроил компьютер.
- **Подключение к корпоративной сети** (или VPN) при шифровании нового диска: ключ восстановления сразу отправляется в службу поддержки. Для разблокировки уже зашифрованного диска сеть не нужна.
- **Учётные данные администратора** компьютера, когда система их запрашивает (см. врезку).

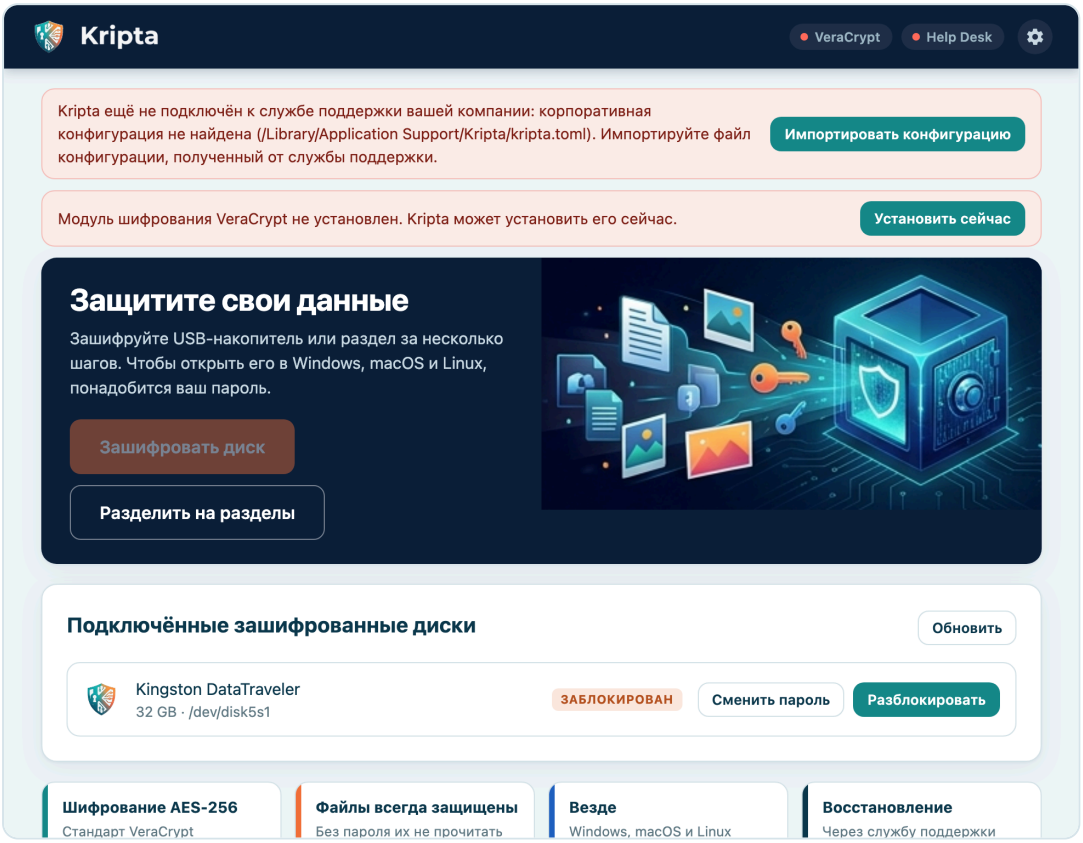
Запросы авторизации
Чтобы читать и записывать данные напрямую на диск, устанавливать компоненты и сохранять конфигурацию, Kripta нужны права администратора. В **Windows** при запуске появляется окно контроля учётных записей. В **macOS** и **Linux** появляется сообщение «Kripta требуется разрешение администратора для завершения операции». Если ИТ-отдел установил системную службу Kripta, эти запросы не появляются.

Кратко о восстановлении

При шифровании Kripta создаёт 48-значный **ключ восстановления**, защищает его и отправляет в архив службы поддержки. Вам не нужно его видеть или хранить. Просмотреть его могут только сотрудники службы поддержки после проверки вашей личности, и каждый просмотр регистрируется.

2 Первый запуск

При первом запуске Kripta проверяет две вещи: подключён ли он к службе поддержки вашей компании и установлен ли VeraCrypt. Если чего-то не хватает, в верхней части окна появляется уведомление с кнопкой для исправления. Всё можно сделать самостоятельно.

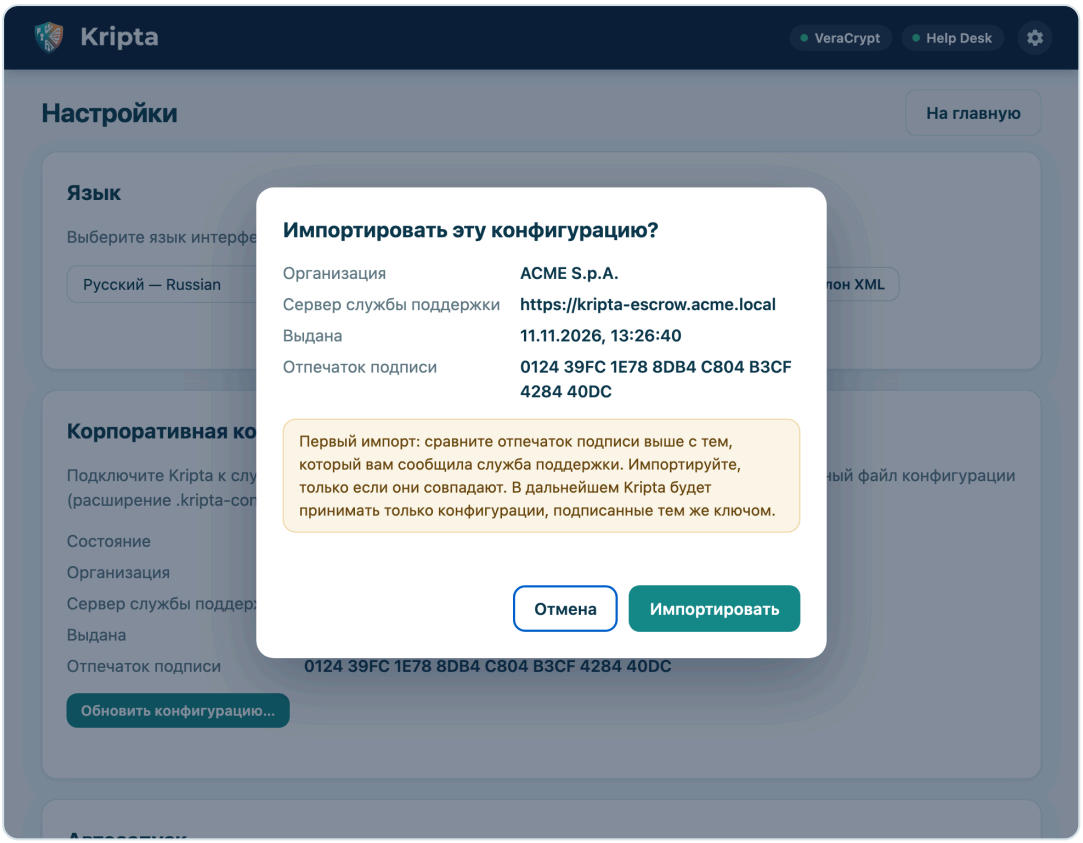


Первый запуск: нужно импортировать конфигурацию и установить VeraCrypt.

Импорт корпоративной конфигурации

Конфигурация сообщает Kripta, в какой архив службы поддержки отправлять ключи восстановления. Служба поддержки выдаёт её в виде файла с расширением `.kripta-config` с цифровой подписью: никто не может изменить его незаметно для Kripta.

1. Сохраните полученный файл на компьютере (по электронной почте, с корпоративного портала или с накопителя).
2. Нажмите **Импортировать конфигурацию** в уведомлении или откройте **Настройки** (шестерёнка вверху справа) и нажмите **Импортировать подписанную конфигурацию…**.
3. Выберите файл. Kripta проверит подпись и покажет организацию, сервер службы поддержки, дату выдачи и **отпечаток подписи**.
4. При первом импорте **сравните отпечаток** с тем, который сообщила служба поддержки (по телефону, в интранете…). Если он совпадает, нажмите **Импортировать**.
5. Подтвердите запрос авторизации системы. Появится сообщение **Конфигурация импортирована**, а индикатор **Help Desk** станет зелёным.

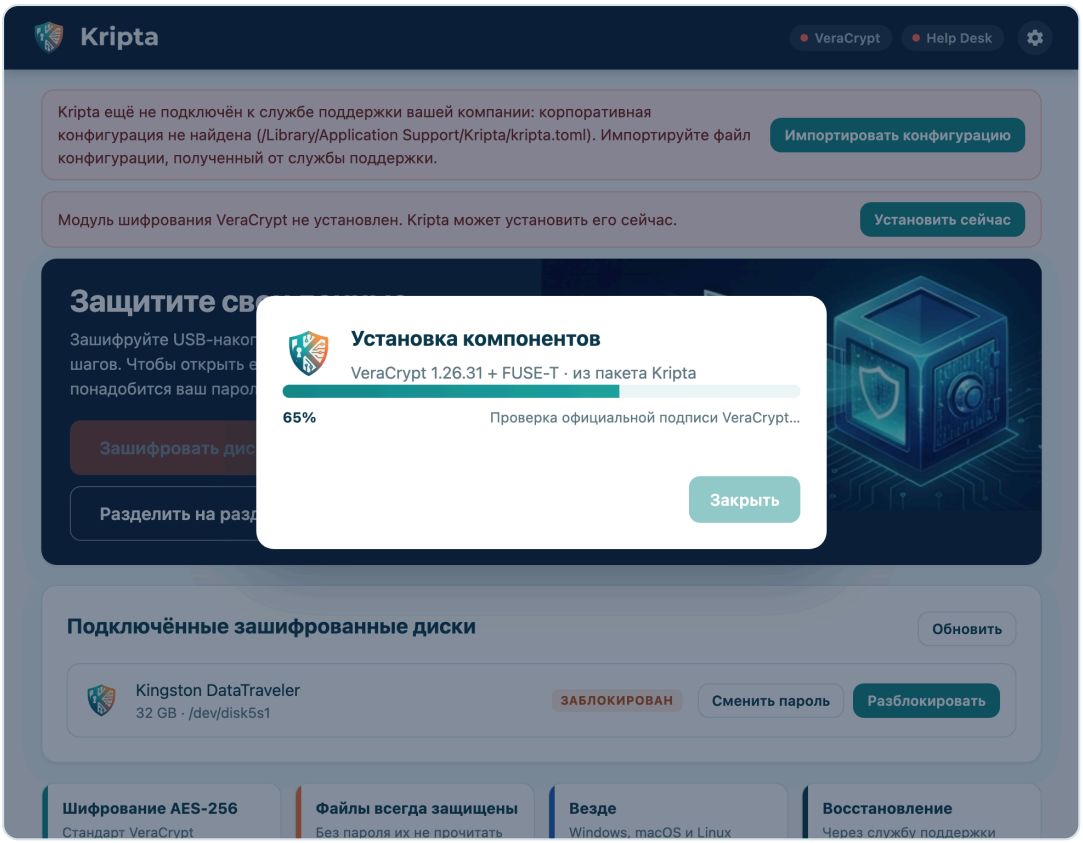


Подтверждение импорта с отпечатком подписи.

> **Если отпечаток не совпадает, не импортируйте**
>
> Файл может быть не от вашей компании. Отмените и обратитесь в службу поддержки. После первого импорта Kripta принимает только обновления, подписанные тем же ключом: поддельный файл отклоняется автоматически.

Установка VeraCrypt

Kripta уже содержит официальный установщик VeraCrypt (и FUSE-T для macOS). Нажмите **Установить сейчас** в уведомлении и подтвердите запрос авторизации: Kripta проверит официальную подпись установщиков и установит их без дополнительных вопросов.

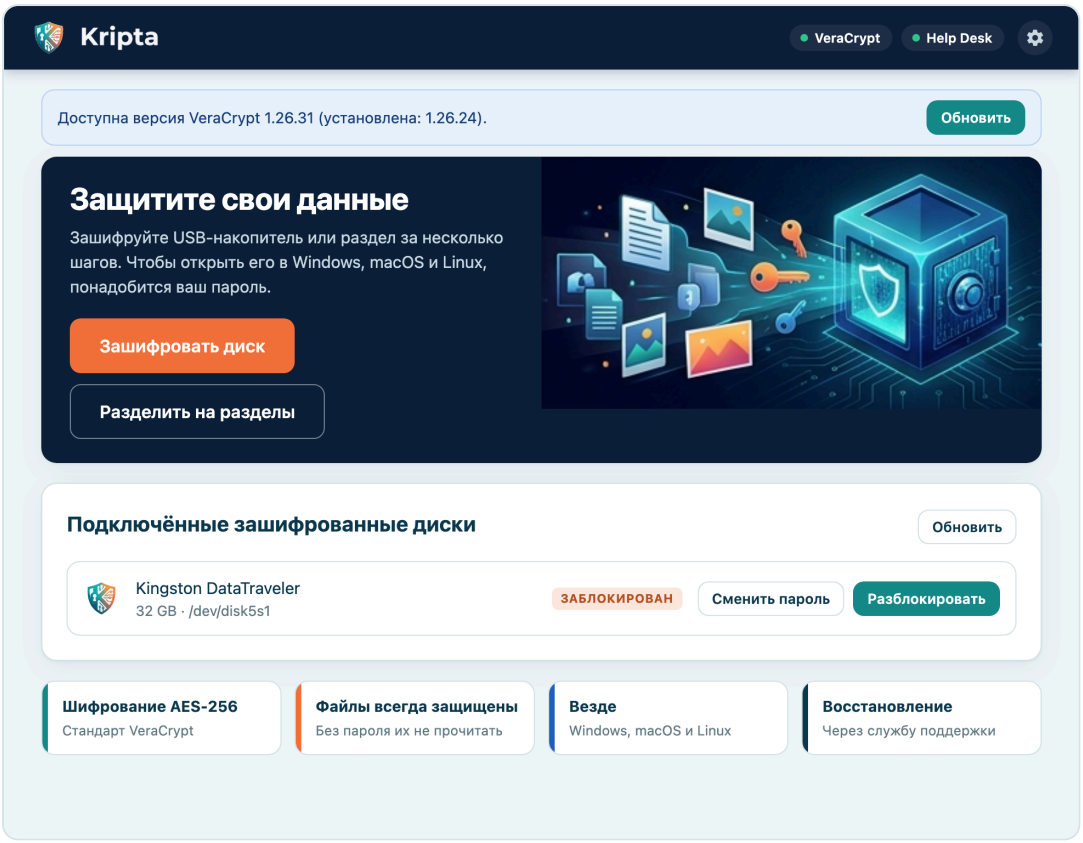


Установка компонентов с проверкой официальной подписи.

По окончании появится сообщение **Установка завершена**. В Windows может потребоваться перезагрузка.

Обновления VeraCrypt

При каждом запуске (а затем раз в день) Kripta проверяет, не вышла ли новая версия VeraCrypt. Если вышла, появляется синее уведомление с кнопкой **Обновить**. Новая версия загружается с официального сайта и устанавливается, только если подпись разработчиков VeraCrypt действительна.



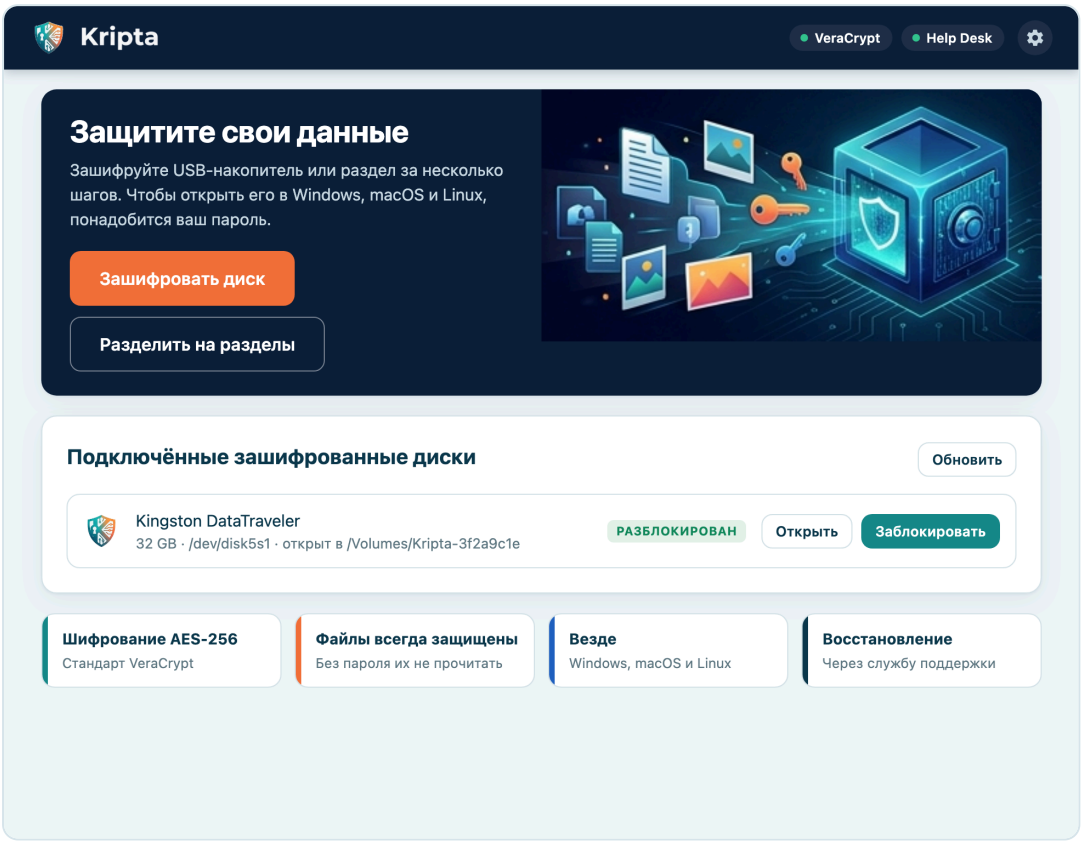
Доступно обновление VeraCrypt.

Перед обновлением

Заблокируйте все открытые зашифрованные диски: Kripta не обновляет VeraCrypt, пока диск разблокирован. Автоматическую проверку можно отключить в настройках (глава 9).

3 Главное окно

При открытии Kripta показывает начальный экран. Здесь можно зашифровать новый диск и управлять подключёнными зашифрованными дисками.

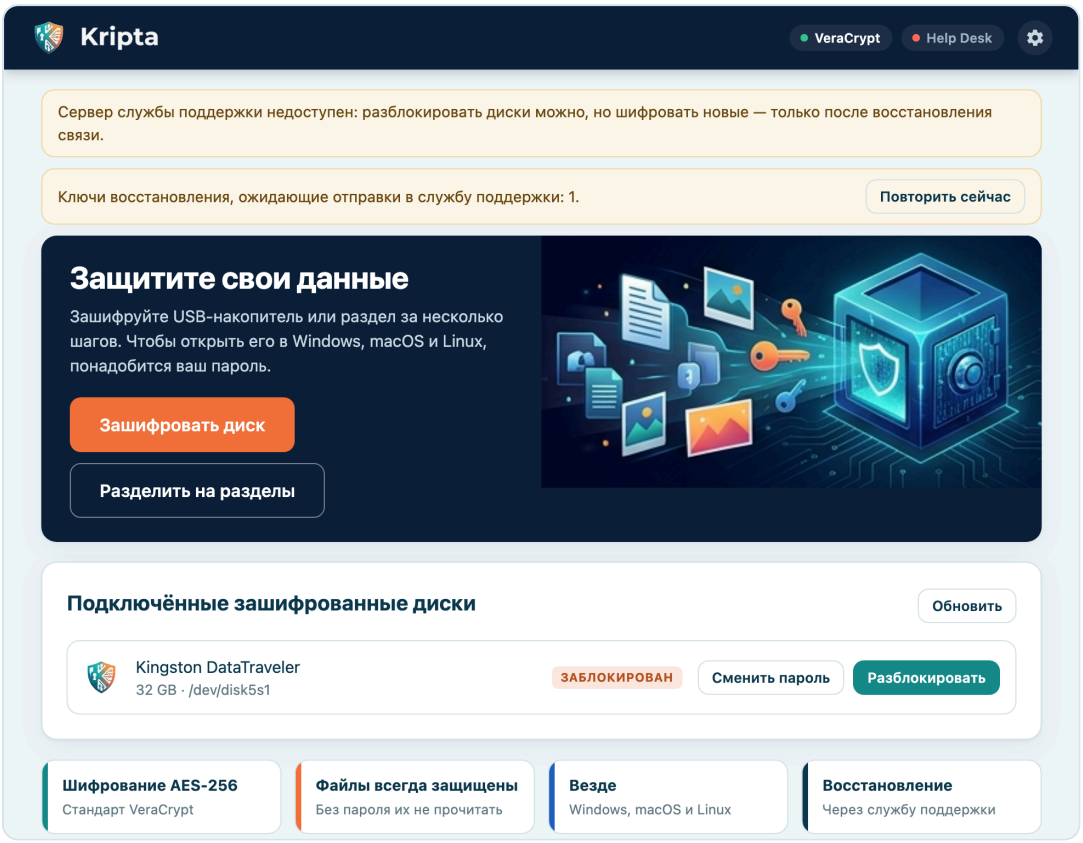


Начальный экран с подключённым и разблокированным зашифрованным диском.

Элемент	Назначение
VeraCrypt	**Зелёная** точка: модуль шифрования установлен. **Красная**: не установлен (глава 2). При наведении видна версия.
Help Desk	Зелёный: архив ключей доступен. Красный: недоступен (нет сети, VPN выключен, нет конфигурации).
Шестерёнка	Открывает **Настройки**: язык, корпоративная конфигурация, компоненты (глава 9).
Зашифровать диск	Запускает мастер (глава 4). Неактивна, если Kripta не настроен или нет VeraCrypt.
Разделить на разделы	Делит USB-накопитель или внешний диск на несколько разделов (глава 5).
Подключённые зашифрованные диски	Подключённые диски Kripta с состоянием **Заблокирован** или **Разблокирован** и кнопками.

Уведомления

В верхней части окна могут появляться цветные блоки с кнопкой для решения проблемы:



Сервер службы поддержки недоступен, один ключ восстановления ожидает отправки.

- **Сервер службы поддержки недоступен:** разблокировать диски можно, шифровать новые — нельзя.
- **Ключи восстановления ожидают отправки:** Kripta повторяет попытки сам; нажмите **Повторить сейчас**, когда снова будете в сети. **Не закрывайте Kripta, пока уведомление не исчезнет.**
- **Kripta ещё не подключён к службе поддержки / VeraCrypt не установлен / доступна версия VeraCrypt…:** см. главу 2.

Значок Kripta: строка меню и область уведомлений

Kripta работает в фоне, чтобы замечать подключение зашифрованных дисков; управление — через значок с эмблемой:

Система	Где находится значок	Полезно знать
macOS	В **строке меню** вверху справа. Kripta **не отображается в Dock**.	На MacBook с вырезом лишние значки скрываются при заполненной строке: уберите ненужные или перетащите их с нажатой клавишей ⌘.
Windows	В **области уведомлений** внизу справа, рядом с часами.	Если он среди скрытых значков, нажмите стрелку ^ и перетащите эмблему на панель.

Система	Где находится значок	Полезно знать
Linux	В **области уведомлений** панели.	В «чистом» GNOME (Fedora, Debian) нужно расширение **AppIndicator and KStatusNotifierItem Support**.

Меню значка содержит пункты **Открыть Kripta**, **Зашифровать диск…**, **Разделить на разделы…**, **Заблокировать все диски**, **Настройки…** и **Выйти из Kripta**. Пункты отображаются на выбранном языке.

> **Закрытие окна не завершает Kripta**
> Kripta продолжает работать в строке меню или области уведомлений. Чтобы снова открыть окно, выберите **Открыть Kripta** или запустите Kripta повторно: откроется уже работающее окно.

Автозапуск

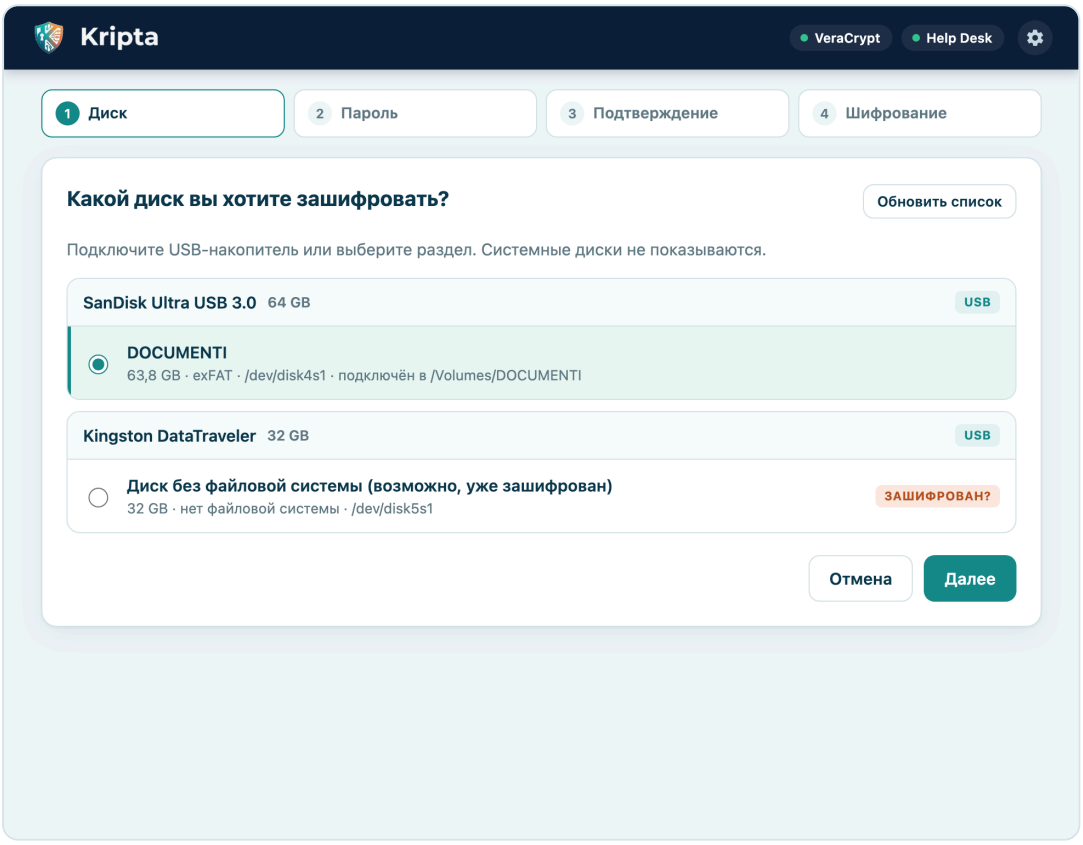
После установки Kripta **запускается сам при каждом входе в систему**, не открывая окно, и постоянно работает в фоне: как только вы подключаете зашифрованный диск, он запрашивает пароль. Отключить это можно в **Настройки › Автозапуск** (глава 9). **Выйти из Kripta** закрывает его до следующего входа.

4 Шифрование диска

> **Шифрование удаляет всё содержимое диска.**
> Перед началом скопируйте нужные файлы в другое место. После шифрования их можно будет скопировать обратно на защищённый диск.

Подключите накопитель, убедитесь, что индикатор **Help Desk** зелёный, и нажмите **Зашифровать диск**.

Шаг 1 — Диск

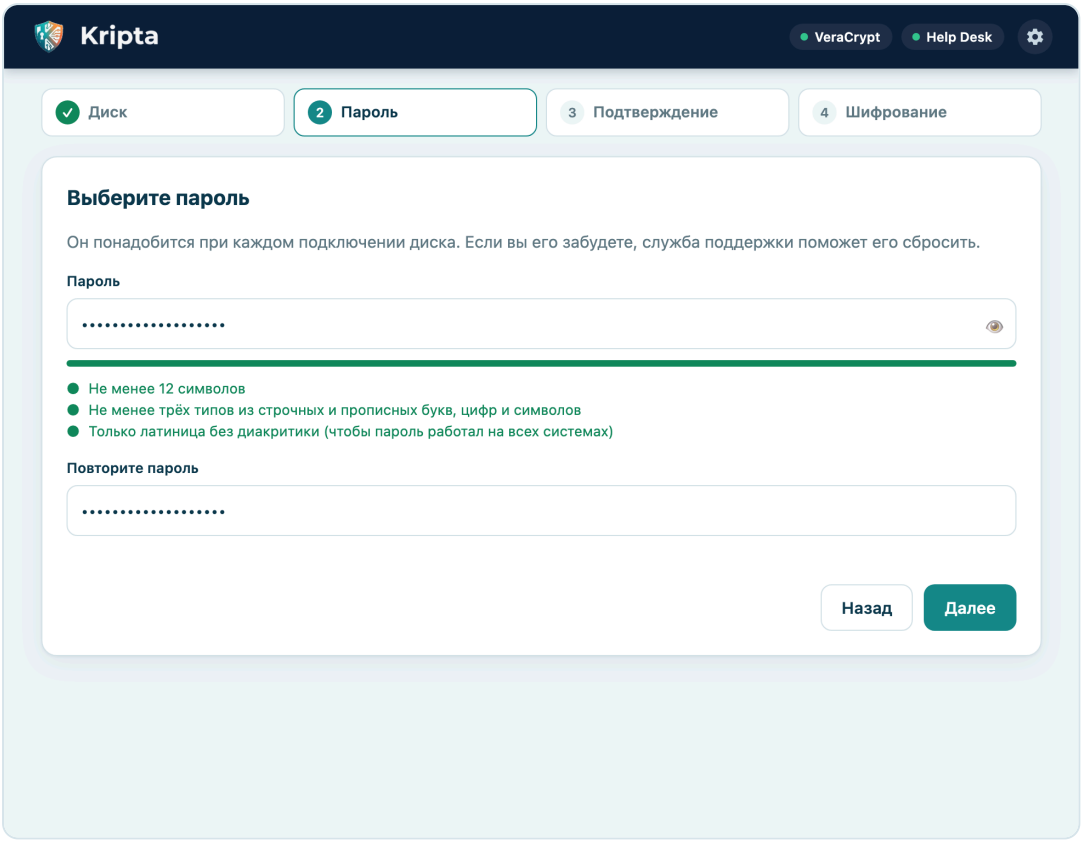


Выбор диска для шифрования.

1. Kripta показывает подключённые устройства, сначала съёмные. **Системные диски никогда не показываются**.
2. Внимательно проверьте **ёмкость и имя**, чтобы выбрать правильный диск.
3. Если накопитель не отображается, переподключите его и нажмите **Обновить список**.
4. Выберите диск и нажмите **Далее**.

> **Метка «Зашифрован?»**
> Так обозначается диск без распознаваемой файловой системы: вероятно, он уже зашифрован. Если зашифровать его снова, текущее содержимое будет потеряно.

Шаг 2 — Пароль

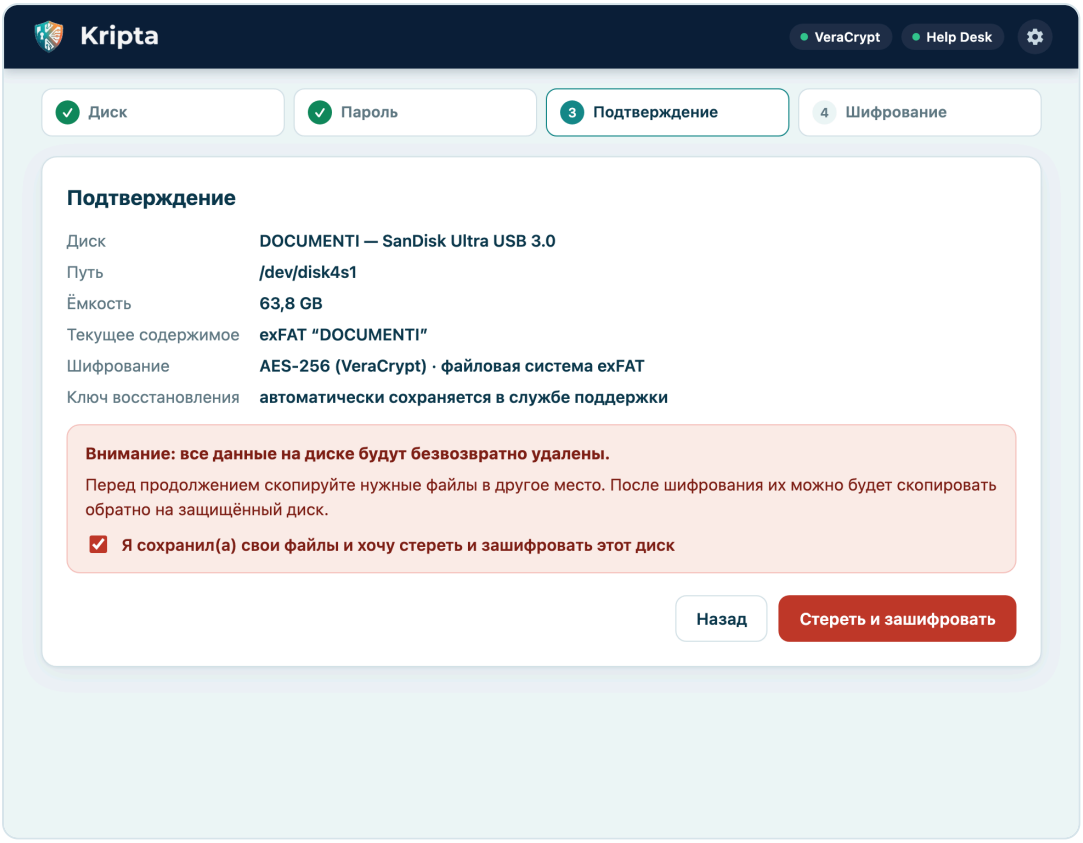


Правила становятся зелёными по мере выполнения.

Пароль должен содержать **не менее 12 символов**, **не менее трёх типов** из строчных и прописных латинских букв, цифр и символов и **только латиницу без диакритики**: кириллицу и буквы вроде é, ü другие системы могут вводить иначе. Цветная полоса показывает надёжность; кнопка 👁 показывает пароль. Повторите его во втором поле и нажмите **Далее**.

> **Совет**
> Фраза из нескольких слов, соединённых символами и цифрами (например, `Poezd-Ozero-Zeleny-47`), надёжна и легко запоминается. Не используйте пароль от корпоративной учётной записи.

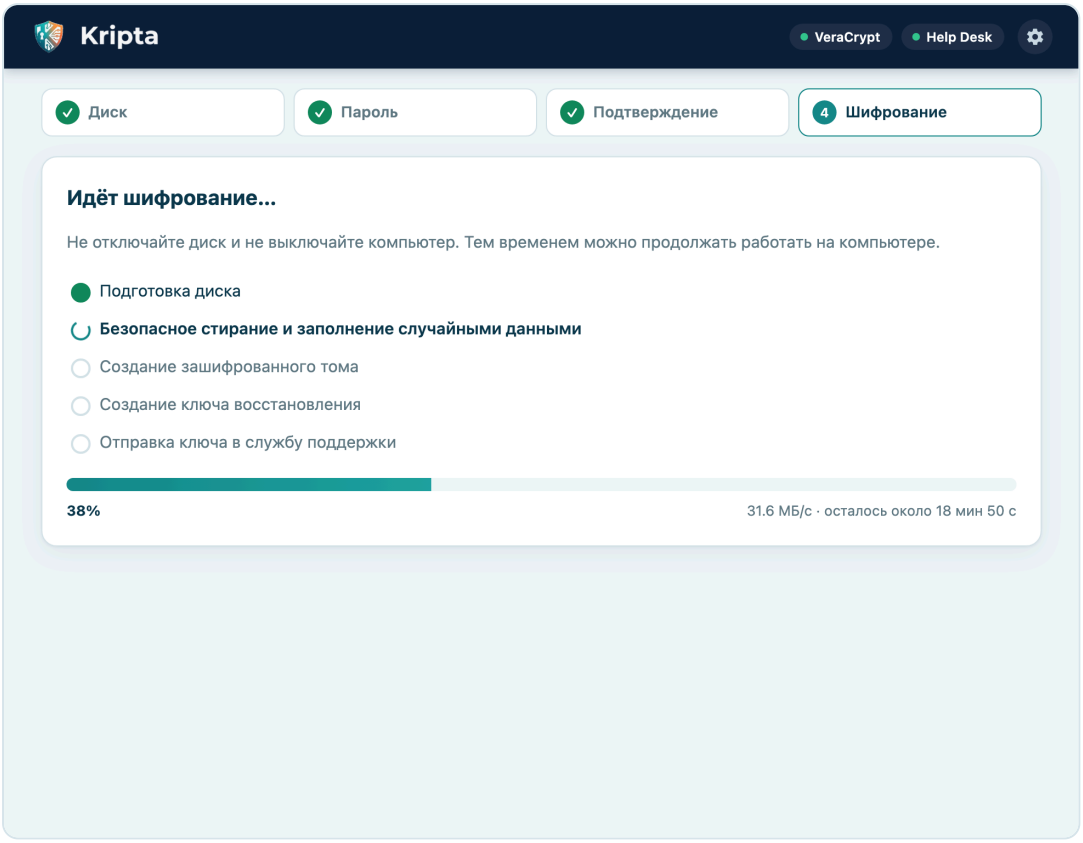
Шаг 3 — Подтверждение



Сводка и подтверждение удаления.

Проверьте сводку, отметьте **Я сохранил(а) свои файлы и хочу стереть и зашифровать этот диск** и нажмите **Стереть и зашифровать**. Система может запросить разрешение администратора.

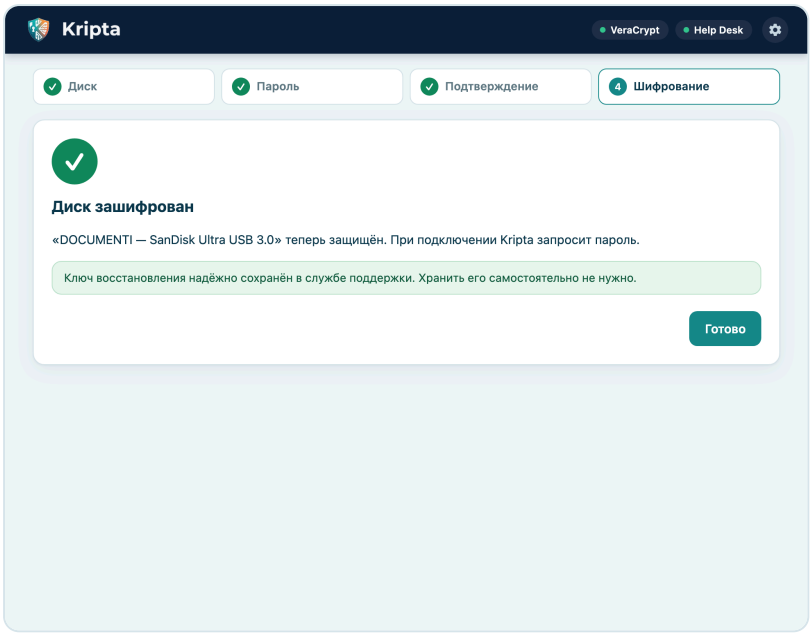
Шаг 4 — Шифрование



Ход выполнения со скоростью и оставшимся временем.

Kripta подготавливает диск, полностью перезаписывает его случайными данными (самый долгий этап), создаёт зашифрованный том exFAT, генерирует ключ восстановления и отправляет его в службу поддержки.

> **Во время шифрования**
> Не отключайте диск, не выключайте компьютер и не переводите его в спящий режим. Накопитель на 64 ГБ шифруется примерно от 15 минут до часа.



Шифрование завершено.

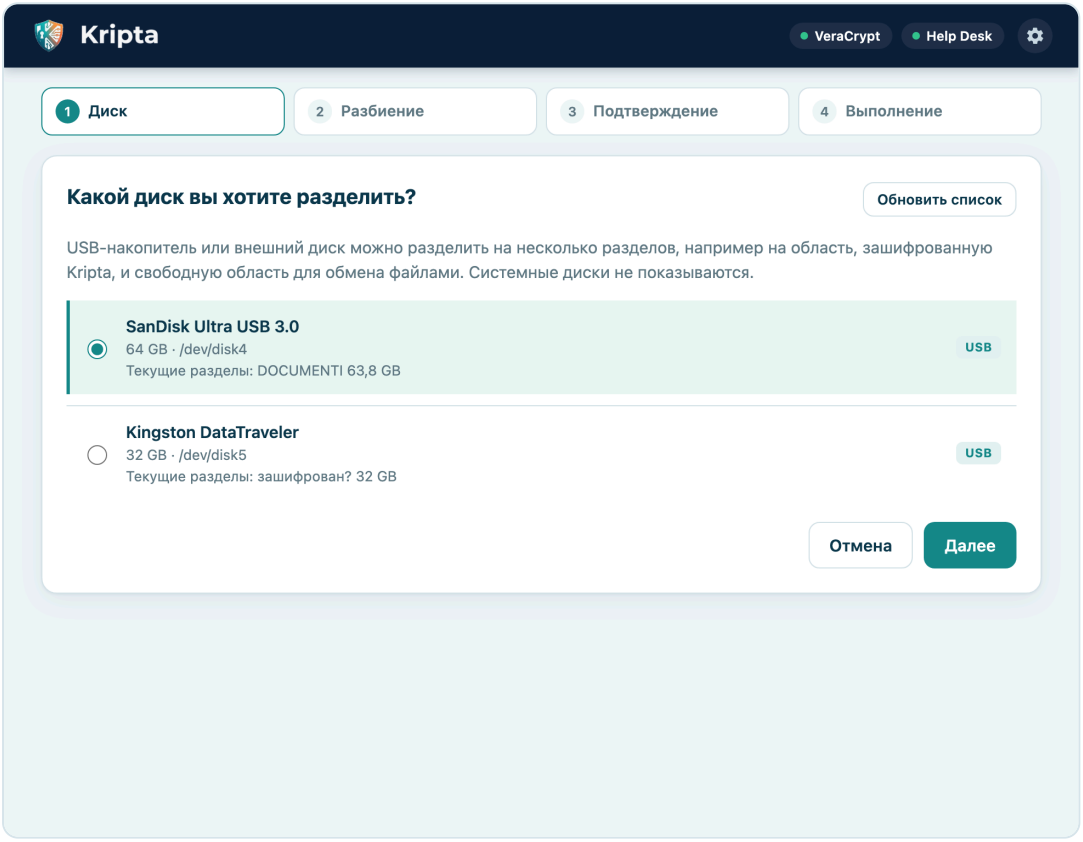
Если появилось сообщение **Ключ восстановления ещё не отправлен**, диск всё равно зашифрован и готов к работе: не закрывайте Kripta и оставайтесь в сети, ключ будет отправлен при первой возможности. Если шифрование не удалось, причина указана в сообщении (глава 11).

5 Разбиение диска на разделы

Функция **Разделить на разделы** делит USB-накопитель или внешний диск на несколько независимых частей, у каждой из которых своё имя и файловая система. Типичный вариант — **зашифрованная область** для конфиденциальных данных и **свободная область** для обмена файлами с компьютерами без Kripta.

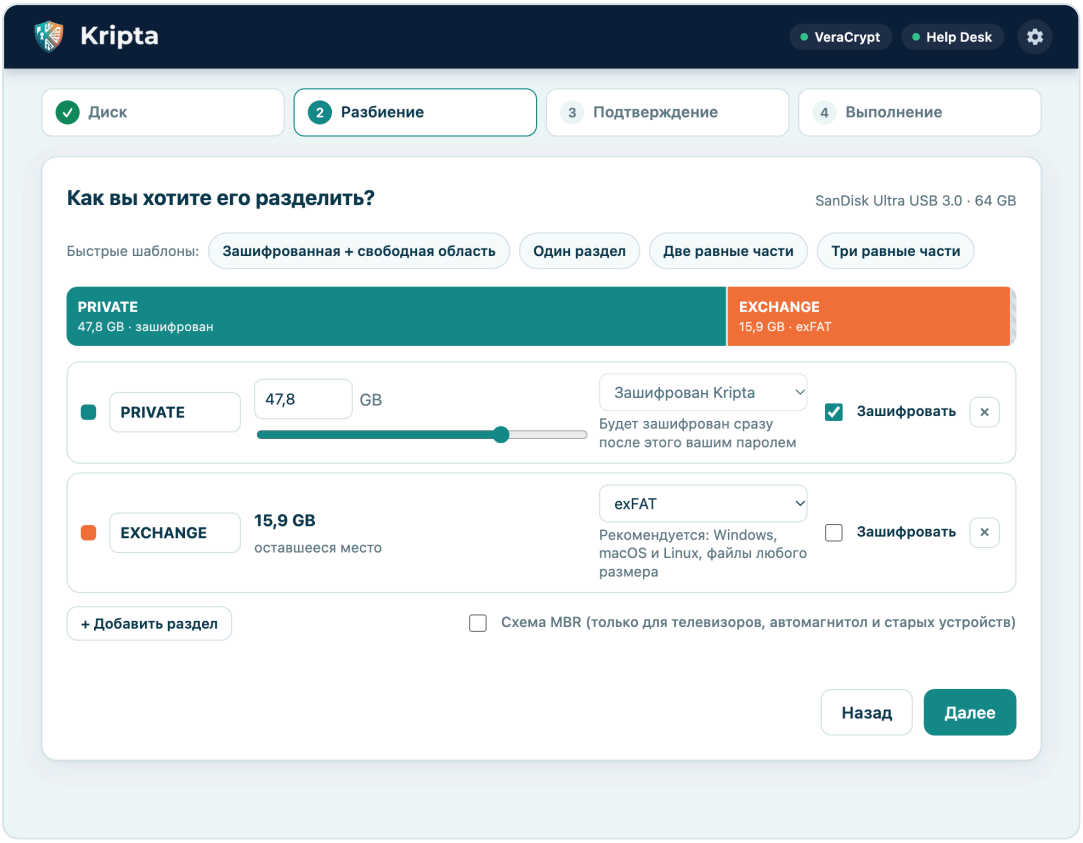
> **Разбиение стирает весь диск**
> , включая существующие разделы и уже зашифрованные диски. Сохраните нужные файлы в другом месте.

Шаг 1 — Диск



Выбор диска с текущими разделами.

Шаг 2 — Разбиение



Цветная полоса показывает разбиение в пропорции.

Шаблон	Результат
Зашифрованная + свободная область	Три четверти диска для шифрования, остальное — свободная область exFAT. Этот шаблон предлагается изначально.
Один раздел	Весь диск в одном разделе.
Две / Три равные части	Диск делится на части одинакового размера.

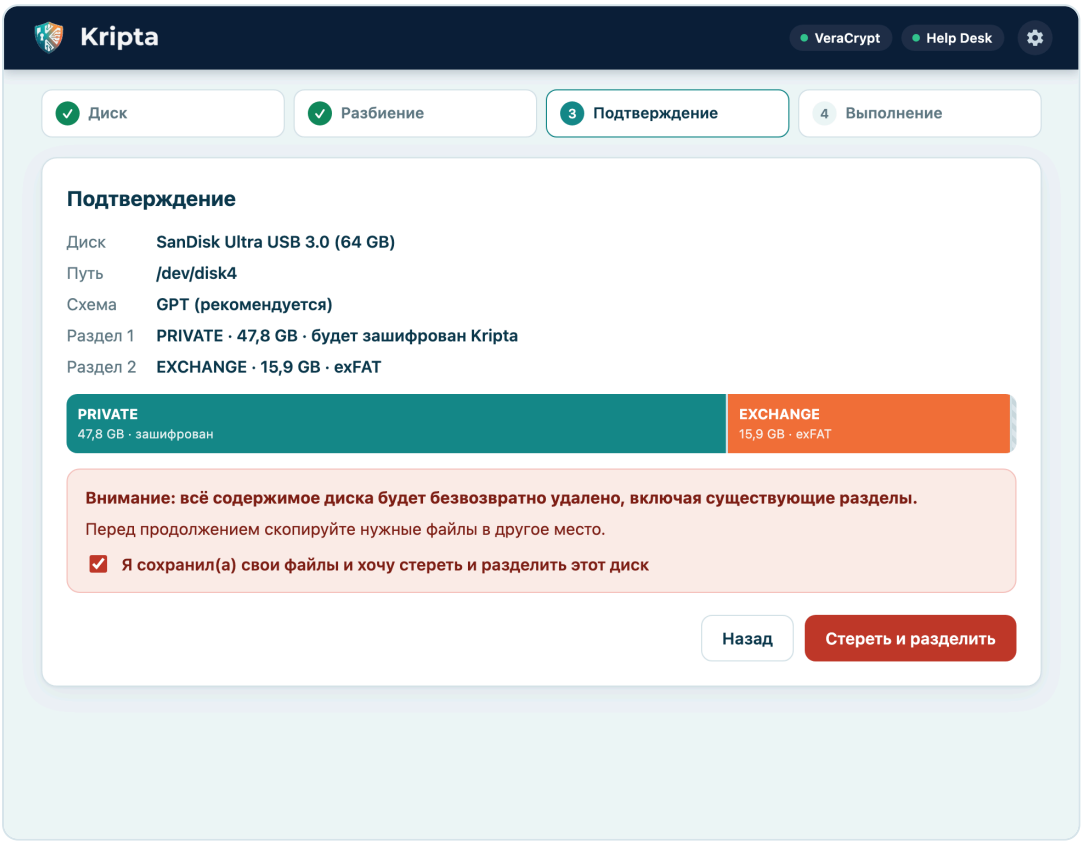
Для каждого раздела задаются **имя** (до 11 символов: латинские буквы, цифры, `_` и `-`), **размер** (последний занимает оставшееся место), **файловая система** и флажок **Зашифровать**. Кнопка **+ Добавить раздел** добавляет ещё один (до 8).

Файловая система	Открывается в	Примечания
exFAT (рекомендуется)	Windows, macOS, Linux	Практически без ограничений на размер файлов.
FAT32	Почти любом устройстве	Файлы до 4 ГБ; в Windows раздел до 32 ГБ.
NTFS	Windows; в macOS только чтение	В Linux требуется `ntfs-3g`.
APFS, **Mac OS Extended**	Только Mac	Доступны только на Mac.

Файловая система	Открывается в	Примечания
ext4	Только Linux	Доступна только в Linux.

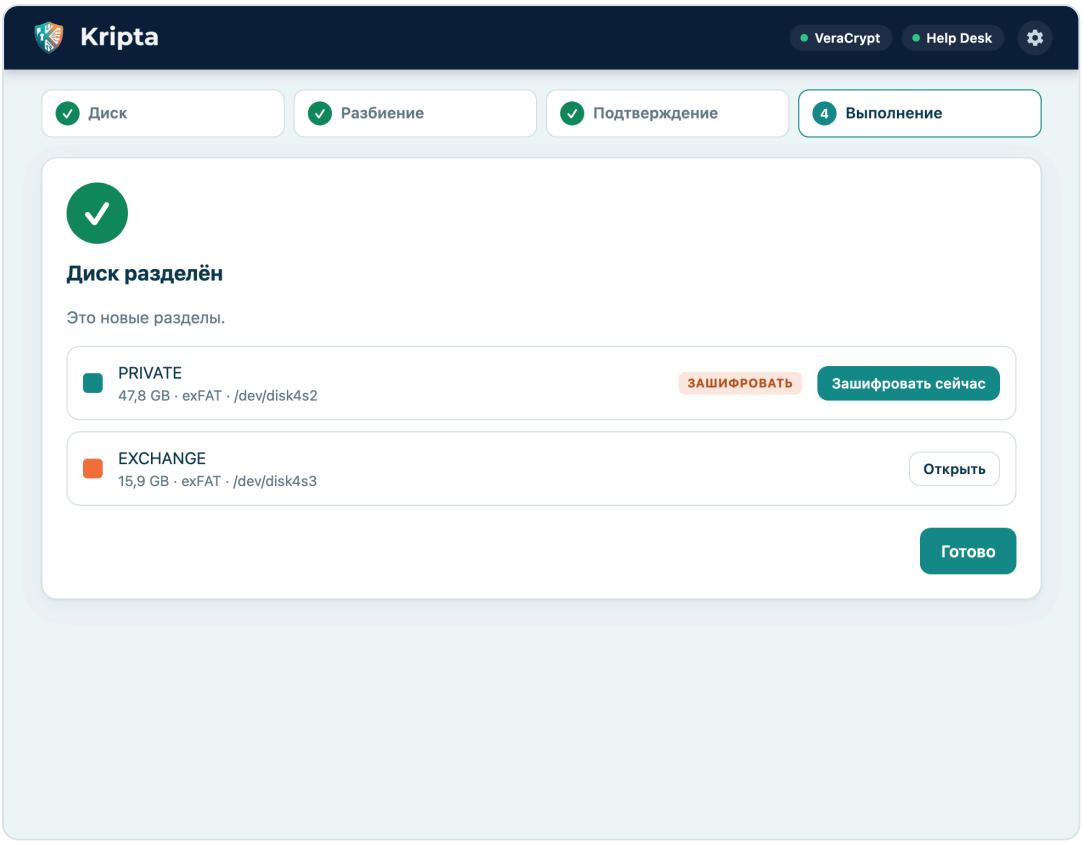
> **Схема MBR**
> Включайте её, только если накопитель должен работать с телевизорами, автомагнитолами или очень старыми компьютерами: максимум 4 раздела и 2 ТБ.

Шаг 3 — Подтверждение и шаг 4 — Выполнение



Сводка перед удалением.

Отметьте флажок подтверждения и нажмите **Стереть и разделить**. Обычно это занимает меньше минуты.



Разделы созданы: у области для шифрования есть кнопка «Зашифровать сейчас».

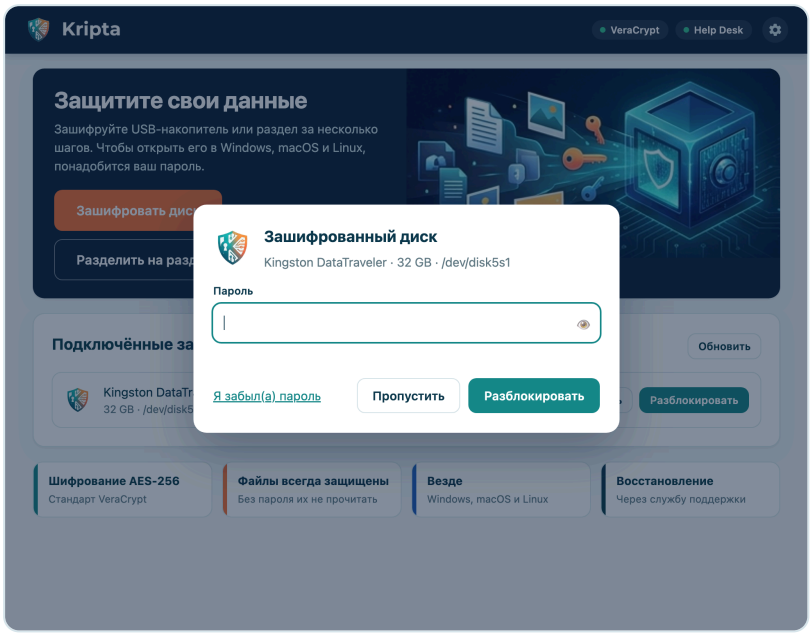
Рядом с разделами для шифрования нажмите **Зашифровать сейчас**: шифрование (глава 4) начнётся с уже выбранным разделом.

> **Пока область «Зашифровать» не зашифрована, она не защищена**
> Не копируйте туда конфиденциальные файлы до завершения шифрования.

6 Работа с зашифрованным диском

Разблокировка

При подключении зашифрованного диска, когда Kripta запущен, автоматически появляется запрос пароля.



Запрос пароля при подключении.

1. Введите пароль и нажмите **Разблокировать** (или Enter).
2. Диск откроется как обычный в Проводнике, Finder или файловом менеджере Linux.
3. Кнопка **Пропустить** позволяет разблокировать его позже из главного окна.

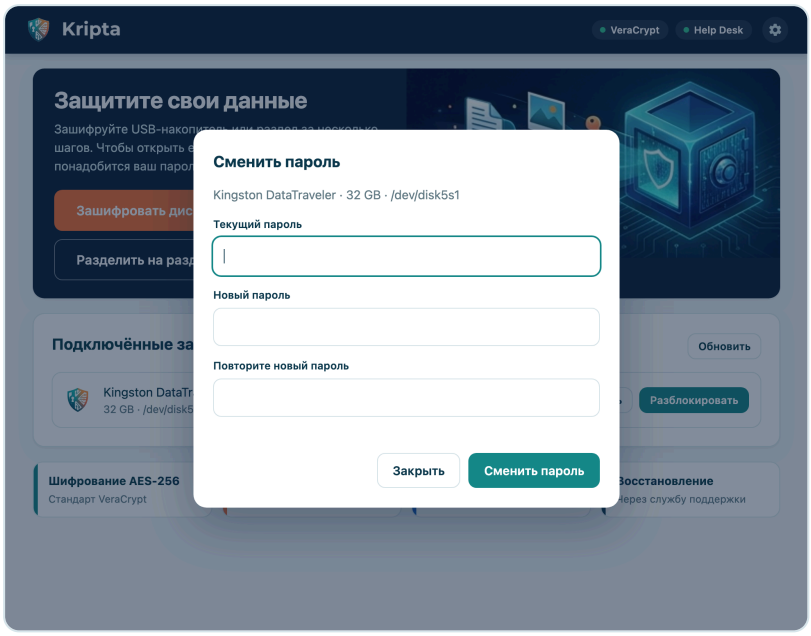
Работа с файлами и блокировка

На разблокированном диске файлы используются как обычно: всё записываемое шифруется прозрачно. Закончив, закройте открытые файлы, нажмите **Заблокировать** и отключите диск.

> **Не отключайте разблокированный диск, не заблокировав его**
> Можно потерять копируемые файлы.

7 Смена пароля

Пароль можно сменить в любой момент, если вы знаете текущий. Данные на диске не затрагиваются.



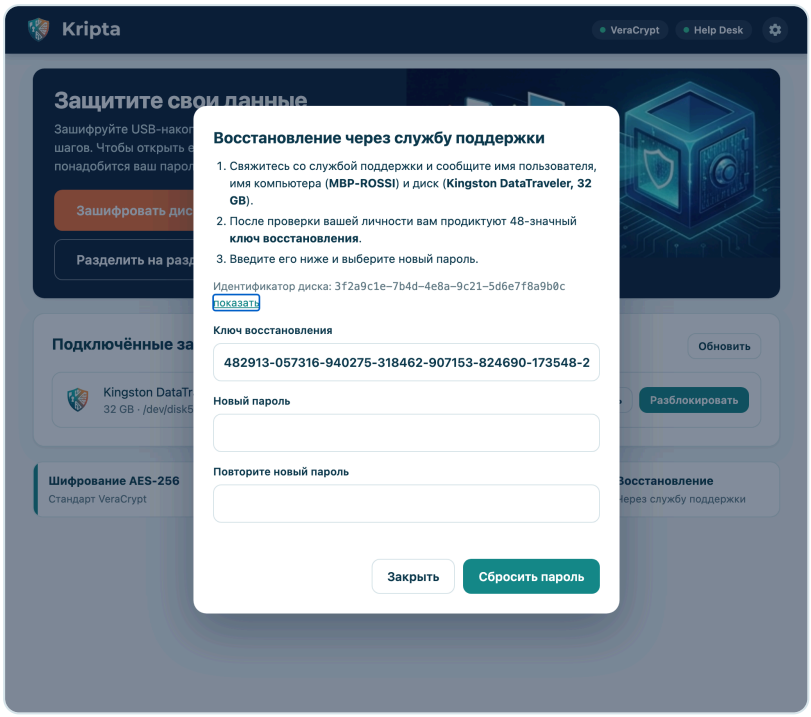
Окно смены пароля.

1. Если диск разблокирован, сначала нажмите **Заблокировать**.
2. Нажмите **Сменить пароль** рядом с диском.
3. Введите текущий пароль и дважды новый (правила те же, что в главе 4), затем подтвердите.

> **А ключ восстановления?**
> Он остаётся действительным: служба поддержки сможет помочь и после смены пароля.

8 Я забыл(а) пароль

Служба поддержки может сообщить ключ восстановления диска: с ним вы зададите новый пароль и вернёте все файлы.



Восстановление через службу поддержки.

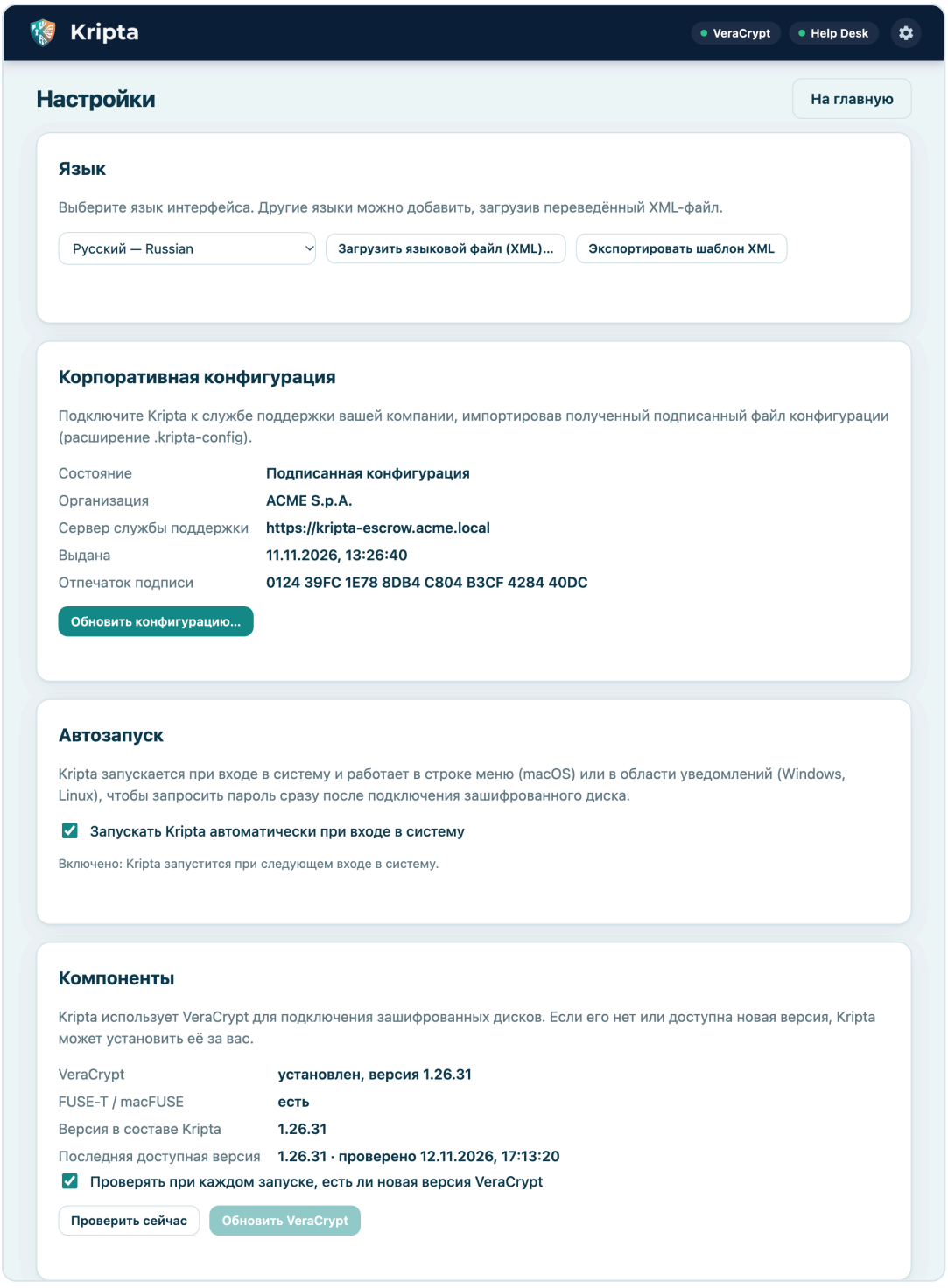
1. В запросе пароля выберите **Я забыл(а) пароль**.
2. В окне указаны имя компьютера и диска; кнопка **показать** выводит также идентификатор диска.
3. **Свяжитесь со службой поддержки** и сообщите эти данные. После проверки вашей личности вам продиктуют **48-значный ключ**.
4. Введите его в поле **Ключ восстановления**, задайте новый пароль и нажмите **Сбросить пароль**.

Один ключ — одно использование
После каждого восстановления Kripta создаёт новый ключ и отправляет его в службу поддержки.

Осторожно, мошенники
Служба поддержки никогда не спросит ваш пароль. Это вы обращаетесь в службу поддержки, а не наоборот.

9 Настройки

Открываются шестерёнкой вверху справа или пунктом **Настройки…** в меню значка.



Настройки: язык, корпоративная конфигурация, компоненты, сведения.

Язык

Выберите язык в списке: интерфейс, меню значка и запросы авторизации сразу переключатся. При выборе **Автоматически** Kripta использует язык системы. Встроенные языки:

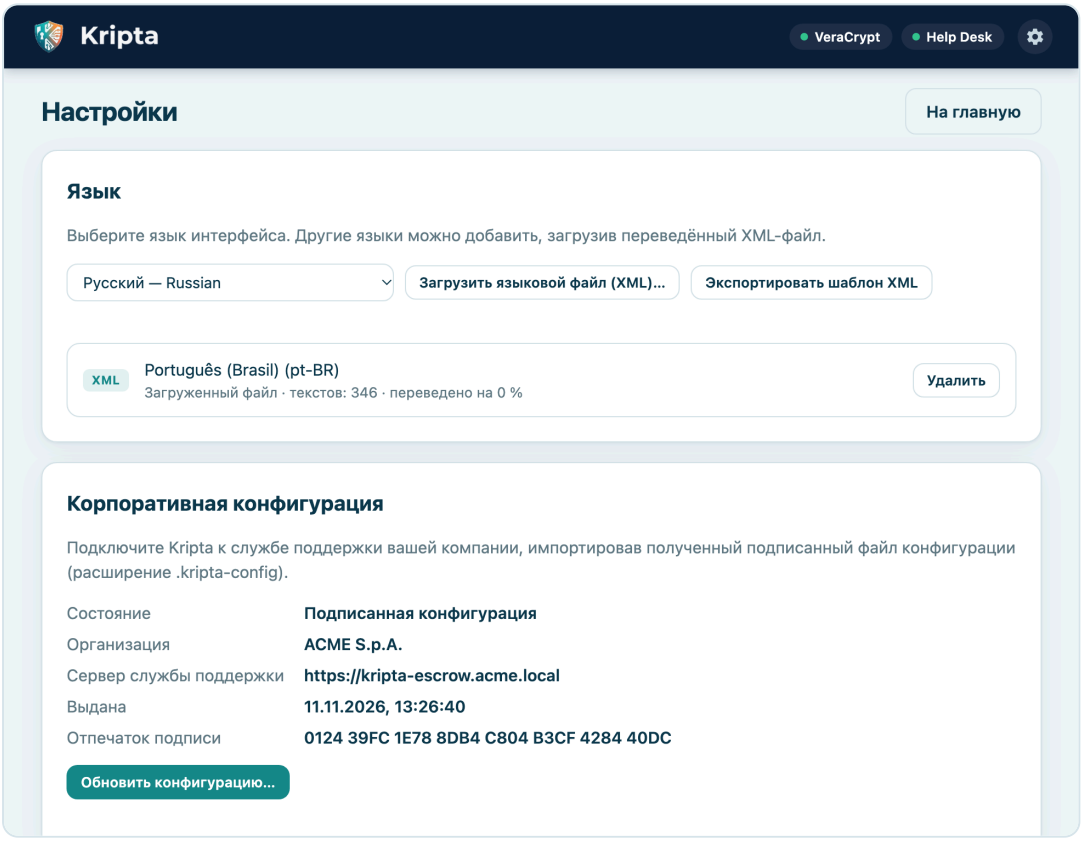
Italiano English Français Español Deutsch Русский العربية 中文 日本語

Добавление языка

Переводы — это простые файлы **XML**, по одному на язык. Чтобы добавить язык:

1. Нажмите **Экспортировать шаблон XML**: файл текущего языка сохранится в папке «Загрузки».
2. Переведите текст каждого элемента `<string>`, не меняя атрибуты `id` и заполнители `{1}`, `{2}`.
3. В начале файла укажите `code` (например, `pt` или `pt-BR`), `name`, `english-name` и `dir` (`rtl` для языков с письмом справа налево).
4. Нажмите **Загрузить языковой файл (XML)…** и выберите файл: язык появится в списке с процентом переведённых текстов. Отсутствующие тексты показываются на английском.

```
<kripta-language format="1" code="pt" name="Português" english-name="Portuguese" dir="ltr">
  <string id="home.title">Proteja os seus dados</string>
  …
</kripta-language>
```



Язык, загруженный из XML-файла, с кнопкой «Удалить».

Файл с тем же кодом, что у встроенного языка, заменяет его (удобно для исправления термина); кнопка **Удалить** возвращает оригинал. Файлы девяти встроенных языков находятся рядом с этим руководством, в папке `lang`.

Корпоративная конфигурация

Показывает организацию, сервер службы поддержки, дату и отпечаток установленной конфигурации. **Обновить конфигурацию…** импортирует новый файл от службы поддержки (глава 2).

Компоненты

Показывает установленную версию VeraCrypt, версию в составе Kripta и последнюю доступную. **Проверить сейчас** выполняет проверку сразу, **Установить** / **Обновить VeraCrypt** запускает установку. Флажок **Проверять при каждом запуске…** включает или отключает автоматическую проверку.

Автозапуск

Флажок **Запускать Kripta автоматически при входе в систему** включён по умолчанию. Под ним показано, зарегистрирован ли автозапуск в системе. Если его снять, Kripta не будет обнаруживать зашифрованные диски, пока вы его не откроете.

10 Использование диска на других компьютерах

Диски, зашифрованные Kripta, используют стандартный формат **VeraCrypt** с файловой системой **exFAT**: они открываются в Windows, macOS и Linux.

Компьютер	Что происходит при подключении диска
С настроенным Kripta	Появляется запрос пароля: всё автоматически.
С установленным Kripta, но **без корпоративной конфигурации** (например, дома)	Запрос пароля всё равно появляется, и диск разблокируется. Если нет VeraCrypt, Kripta предложит **Установить сейчас**. Без конфигурации нельзя шифровать новые диски и восстанавливать пароль.
Только с VeraCrypt	Откройте VeraCrypt, выберите свободный слот, **Выбрать устройство**, раздел накопителя, затем **Смонтировать** и введите пароль.
Без Kripta и VeraCrypt	Запрос не появится: операционные системы не запускают программы с USB-накопителей. Система может предложить **отформатировать** диск: **всегда отказывайтесь**. Установите Kripta (с корпоративного сайта) и подключите диск снова.

Права администратора

Чтобы открыть зашифрованный диск на любом компьютере, нужны права администратора, поскольку VeraCrypt использует системный драйвер. На компьютере, учётных данных которого у вас нет, диск открыть невозможно.

Свободная область для обмена

Если вы часто работаете на компьютерах без Kripta, разделите накопитель по шаблону **Зашифрованная + свободная область** (глава 5): в свободную область можно скопировать и установщик Kripta.

11 Сообщения и устранение неполадок

Сообщение или ситуация	Что делать
Kripta ещё не подключён к службе поддержки вашей компании	Импортируйте файл `.kripta-config`, полученный от службы поддержки (глава 2).
Подпись пакета недействительна	Файл изменён или повреждён: запросите его в службе поддержки повторно.
Пакет подписан другим / неодобренным ключом	Файл не от вашей компании. Не используйте его и обратитесь в службу поддержки.
Конфигурацией управляет ИТ-отдел, её нельзя заменить	Компьютер настроен централизованно: импортировать ничего не нужно.
Модуль шифрования VeraCrypt не установлен	Нажмите **Установить сейчас**. Если кнопки нет, обратитесь в службу поддержки.
Официальная подпись VeraCrypt недействительна / файл не совпадает с подписанной версией	Загрузка изменена или неполна: установка отменена. Повторите позже.
Перед обновлением VeraCrypt заблокируйте все зашифрованные диски	Нажмите **Заблокировать** у открытых дисков и повторите обновление.
Перезагрузите компьютер, чтобы завершить обновление (Windows)	Сохраните работу и перезагрузите компьютер.
Сервер службы поддержки недоступен. Шифрование не начато.	Подключитесь к корпоративной сети или VPN и повторите попытку. Данные на диске не изменены.
Ключи восстановления ожидают отправки	Подключитесь к сети и нажмите **Повторить сейчас**. Не закрывайте Kripta, пока уведомление не исчезнет.
Нет доступных дисков	Переподключите накопитель (попробуйте другой USB-порт) и нажмите **Обновить список**.
Авторизация администратора отменена / Истекло время ожидания	Повторите операцию и подтвердите запрос системы.
Не удаётся отключить / заблокировать том	Закройте документы и окна, открытые с диска, и повторите попытку.
Неверный пароль	Проверьте Caps Lock и раскладку клавиатуры. Если вы его забыли, см. главу 8.
Неверный ключ восстановления	Сверьте цифры с сотрудником: нужен **самый последний** ключ.
На диске есть разблокированный диск Kripta	Заблокируйте его на начальном экране и повторите разбиение.

Сообщение или ситуация	Что делать
Система не обнаружила новые разделы	Отключите и снова подключите диск.
Языковой файл не является корректным XML / недопустимый элемент	Исправьте указанный файл: допускаются только элементы `<string>` с простым текстом.
Окно разблокировки не появляется при подключении	Убедитесь, что Kripta запущен (значок на панели), и нажмите **Разблокировать** в главном окне.

12 Часто задаваемые вопросы

Можно ли зашифровать накопитель с файлами, не потеряв их?

Нет. Шифрование стирает диск. Скопируйте файлы в другое место, зашифруйте диск и скопируйте их обратно.

Можно ли зашифровать внутренний диск компьютера?

Нет. Kripta предназначен для накопителей и внешних дисков; системные диски не показываются.

Может ли служба поддержки прочитать мои файлы?

Служба поддержки хранит только ключ восстановления и может просмотреть его лишь по вашему запросу; каждый доступ регистрируется.

Нужно ли записывать ключ восстановления?

Нет. Вы его никогда не видите и не должны хранить: он хранится в службе поддержки.

Устанавливает ли Kripta программы на мой компьютер?

Только VeraCrypt (и FUSE-T в macOS), после вашего подтверждения и только при действительной официальной подписи разработчиков.

Можно ли использовать накопитель на домашнем компьютере?

Да, установив Kripta или VeraCrypt (глава 10). Соблюдайте правила компании об использовании данных вне офиса.

Нужного языка нет. Что делать?

Можно перевести шаблон XML и загрузить его в настройках (глава 9) или попросить ИТ-отдел распространить перевод.

Почему в пароле нельзя использовать кириллицу и буквы с диакритикой?

Windows, macOS и Linux могут кодировать их по-разному: тот же пароль, введённый в другой системе, может быть не распознан.

Сколько места занимает шифрование?

Очень мало: несколько сотен килобайт на заголовки тома.

A Приложение для ИТ-отдела

Пакеты

Система	Пакет	Примечания
Windows 10/11 (x64)	`Kripta_1.2.0_x64-setup.exe`	Содержит официальные MSI VeraCrypt (x64 и ARM64). Приложение запускается с правами администратора.
macOS 11+	`Kripta_1.2.0_universal.dmg`	Содержит VeraCrypt (сборки для FUSE-T и macFUSE) и FUSE-T, не требующий расширений ядра.
Debian / Ubuntu	`Kripta_1.2.0_amd64.deb`	Содержит VeraCrypt для Ubuntu 22.04/24.04 и Debian 12/13; для других версий Kripta загружает проверенный пакет.
Fedora / RHEL	`Kripta-1.2.0-1.x86_64.rpm`	Содержит VeraCrypt для Fedora 44; установите также `exfatprogs`.
Другие дистрибутивы	`Kripta_1.2.0_amd64.AppImage`	Переносимый исполняемый файл.

Подписанная конфигурация

На сервере escrow один раз создайте ключ подписи, затем подпишите клиентскую конфигурацию (шаблон в `deploy/client/kripta.toml.example`):

```
kripta-escrow keygen-sign            # закрытый ключ (хранить офлайн) + открытый + отпечаток
kripta-escrow sign-config client.toml signing.key "ACME" acme.kripta-config
```

Распространите `acme.kripta-config` среди пользователей и опубликуйте **отпечаток** по надёжному каналу (интранет, телефон службы поддержки). Kripta сохраняет конфигурацию в системном расположении (`%ProgramData%\Kripta`, `/Library/Application Support/Kripta`, `/etc/kripta`) через привилегированный процесс вместе с ключом подписавшего: последующие обновления должны иметь ту же подпись. Чтобы не зависеть от проверки отпечатка пользователем, соберите Kripta с `KRIPTA_PROVISIONING_KEYS=<открытый ключ>`: будут приниматься только эти ключи. Конфигурацию, скопированную ИТ-отделом вручную (без подписи), нельзя заменить пакетом.

Установка и обновление VeraCrypt

- Встроенные установщики подготавливаются при сборке скриптом `scripts/fetch-veracrypt.py`.
- Перед установкой привилегированный процесс проверяет подпись OpenPGP официального списка SHA-256 встроенным ключом IDRIX (отпечаток `5069 A233 D55A 0EEB 174A 5FC3 821A CD02 680D 16DE`) и хеш файла.
- Параметры в `kripta.toml`: `veracrypt_update_check = false` отключает проверку обновлений; `veracrypt_release_api = "https://mirror.internal/…"` задаёт внутреннее зеркало в формате

API GitHub.

Языки

XML-файлы языков находятся в `app/ui/lang/` (включены в приложение) и в `docs/manuale/lang/`. Языки, загруженные пользователями, сохраняются в папке данных пользователя (`languages/`). Чтобы распространить новый язык для всех, добавьте файл в `app/ui/lang/`, а его код — в список в `app/ui/i18n.js`.

Дополнительные компоненты

- **Запуск при входе** в строке меню / области уведомлений (`kripta --background`): **автоматически**. Kripta регистрирует его при каждом запуске (macOS: `~/Library/LaunchAgents/com.kripta.agent.plist`, перезапуск при аварийном завершении; Windows: задача планировщика «Kripta» при входе с наивысшими правами, создаётся также установщиком и удаляется при удалении; Linux: `/etc/xdg/autostart/kripta.desktop` из пакетов .deb/.rpm, `~/.config/autostart/kripta.desktop` для AppImage). Отключается в настройках.
- **Привилегированный помощник** как служба (без запросов пароля): `deploy/macos/com.kripta.helper.plist`, `deploy/linux/kripta-helper.service`.