

# Исследуем шифрование в ОС «Альт»



Кейс направлен на изучение возможностей шифрования в ОС «Альт» и работе с зашифрованными объектами.

Перед выполнением задания познакомьтесь:

- со Спецификацией для операционной системы «Альт Рабочая станция К» (KDE) — [https://www.basealt.ru/fileadmin/docs/Specification\\_WS-K\\_10.pdf](https://www.basealt.ru/fileadmin/docs/Specification_WS-K_10.pdf)
- с рекомендованными в операционных системах семейства Альт способами повышения прав — [https://www.altlinux.org/Получение\\_прав\\_root](https://www.altlinux.org/Получение_прав_root)
- с разделами документации — <https://docs.altlinux.org/ru-RU/index.html#alt-kworkstation> — об обновлении системы и установке дополнительных пакетов.

Каждый шаг задания необходимо по возможности подтвердить соответствующими скриншотами.

## Инструкция по шифрованию в ОС «Альт Рабочая станция К» (KDE)

### Шаг 1: Установка ОС и разбиение диска

При установке **Альт Рабочая станция К**, ориентируйтесь на Спецификацию продукта и указанные в данном пункте задания настройки.

На этапе разбиения диска выберите **Ручное разбиение**. Создайте следующие разделы:

1. **/boot** – 512-1024 МБ, файловая система **ext4** (без шифрования).
2. **swap** – 128-512 МБ (в зависимости от объема ОЗУ), файловая система **swap**.
3. **/** (корневой раздел) – 30-50 ГБ, файловая система **ext4**. **На этот раздел устанавливается ОС.**
4. **/home** – оставшееся пространство, файловая система **ext4**.
5. **Раздел для шифрования (LUKS)** – 50+ ГБ (по необходимости), файловая система **ext4**, шифруется с помощью **LUKS**.

После настройки разделов завершите установку ОС.

---

## Шаг 2: Установка приложений для шифрования

После установки и загрузки системы установите программы **KGpg**, **SiriKali** и **Partition Manager** через **терминал** или **Центр приложений Discovery** (перед установкой пакетов не забудьте обновить ОС до актуального состояния).

Пакеты: kde5-kpgg, sirikali, partitionmanager.

---

## Шаг 3: Создание файлов и каталога для шифрования

1. Убедитесь, что вы работаете в контексте прав пользователя системы.
  2. Создайте файл 1\_enc\_file.doc в **домашней папке пользователя**.
  3. Создайте каталог 1\_enc\_folder и внутри него файл 2\_enc\_file.doc:
- 

## Шаг 4: Шифрование файла с помощью KGpg

1. Откройте **KGpg** через меню приложений.
  2. При первом запуске создайте пару ключей (если их нет). При необходимости — создайте исполняемый файл GnuPG.
  3. Выберите **Файл** → **Зашифровать файл**.
  4. Выберите 1\_enc\_file.doc, установите параметры шифрования (например, OpenPGP) и подтвердите действие.
  5. Получите зашифрованный файл 1\_enc\_file.doc.pgp.
- 

## Шаг 5: Шифрование каталога с помощью SiriKali

1. Откройте **SiriKali**.
  2. Следует зашифровать каталог 1\_enc\_folder.
  3. Метод шифрования — на ваш выбор (например, gocryptfs или cryfs).
  4. Установите пароль для шифрования.
  5. После создания зашифрованного контейнера, используйте **SiriKali** для его монтирования при необходимости.
- 

## Шаг 6: Создание и открытие документов на зашифрованном разделе

1. Переместите 1\_enc\_file.doc и 1\_enc\_folder на зашифрованный раздел:
2. Откройте зашифрованный раздел в файловом менеджере **Dolphin** и убедитесь, что файлы доступны.
3. После работы безопасно размонтируйте раздел.
4. Закройте зашифрованный раздел

Теперь ваш раздел зашифрован, и данные на нем защищены.

---

## **Шаг 7: Настройка автоматического монтирования через GUI**

1. Установите plasma-vault для управления зашифрованными томами:
  2. Добавьте зашифрованный раздел в Plasma Vault:
    - Откройте Plasma Vault из меню KDE.
    - Нажмите + Добавить хранилище → Существующий LUKS-том → укажите раздел (например, /dev/sda4).
    - Задайте пароль и точку монтирования (например, /mnt/encrypted).
  3. Монтируйте/размонтируйте раздел через иконку Plasma Vault в системном трее.
- 

## **Шаг 8: Работа с файлом в зашифрованном разделе**

1. Откройте Dolphin → перейдите в /mnt/encrypted.
  2. Редактируйте 3\_enc\_file.doc через текстовый редактор (KWrite, Kate).
  3. После работы размонтируйте раздел через Plasma Vault.
- 

Готово! Теперь в вашей системе зашифрованы файлы, папки и раздел диска, обеспечивая безопасность данных.