# Инструкция по эксплуатации операционной системы Aviacode OS

**Версия 1.0**

# 1. Введение

## 1.1. Назначение документа

Настоящая инструкция определяет порядок эксплуатации операционной системы Aviacode OS после её установки на целевую аппаратную платформу. Документ предназначен для специалистов, осуществляющих настройку, сопровождение и диагностику комплексов на базе Aviacode OS.

## 1.2. Область применения

Инструкция применяется при эксплуатации Aviacode OS в составе комплексов самообслуживания и других устройств, работающих в потоковом режиме. Основные операции включают первоначальную настройку, установку прикладного ПО, диагностику и решение типовых проблем.

## 1.3. Перечень ссылочных документов

- Список совместимого оборудования (Hardware Compatibility List): `https://docs.aviacod.ru/aviacodeos_hardware`
- Список поддерживаемого программного обеспечения (Software Compatibility List): `https://docs.aviacod.ru/aviacodeos_software`

# 2. Подготовка к эксплуатации

## 2.1. Проверка совместимости

Перед началом работ убедитесь, что используемая аппаратная платформа и планируемое к установке прикладное ПО присутствуют в актуальных списках совместимости (см. п. 1.3).

## 2.2. Подготовка аппаратной платформы

Подготовьте одноплатный компьютер согласно руководству производителя. Подключите необходимое периферийное оборудование.

## 2.3. Установка Aviacode OS

Установите предварительно собранный образ Aviacode OS на загрузочный носитель целевого устройства (eMMC или SD-карта). Процесс установки описан в отдельном документе «Инструкция по установке».

# 3. Настройка системы

## 3.1. Подключение и настройка сети

### 3.1.1 Подключение по SSH

**Первоначальное подключение по SSH и настройка безопасности**

После первой загрузки системы и появления приглашения на ввод логина и пароля на локальном мониторе, выполните следующие шаги для настройки безопасного удалённого доступа.

**Подключение по SSH с реквизитами по умолчанию**

- **IP-адрес:** Определите IP-адрес устройства в локальной сети (например, с помощью команды `ip a` на устройстве).
- **Пользователь по умолчанию:** `aviacode`
- **Пароль по умолчанию:** `aviacode` *(Пароль должен быть указан в отдельном документе "Реквизиты по умолчанию". Здесь указан пример.)*
- **Команда для подключения с АРМ:**
- `ssh aviacode@<IP-адрес_устройства>`
- При первом подключении примите fingerprint сервера, введя `yes`.

**Смена пароля пользователя root**

Сразу после первого входа смените пароль `aviacode` на уникальный, сложный пароль, который **не следует записывать или использовать для регулярного доступа**.

```
passwd
```

Введите новый сложный пароль дважды. Этот пароль будет использоваться только для критических административных задач в консоли.

**Создание отдельного пользователя для удалённого доступа**

1. Создайте нового пользователя (например, `admin`):
2. `adduser admin`
3. Задайте для него надёжный пароль и заполните дополнительную информацию (можно пропустить).
4. При необходимости добавьте пользователя в группу `sudo` для выполнения административных команд:
5. `usermod -aG sudo admin`

**Настройка аутентификации по SSH-ключу (отключение парольной аутентификации)**

1. **На АРМ (вашем компьютере)** сгенерируйте пару SSH-ключей, если её ещё нет:

   ```
   ssh-keygen -t ed25519 -C "your_email@example.com"
   ```

2. Ключи по умолчанию сохранятся в `~/.ssh/id_ed25519` (приватный) и `~/.ssh/id_ed25519.pub` (публичный).
3. Скопируйте публичный ключ на устройство с Aviacode OS:

   ```
   ssh-copy-id admin@<IP-адрес_устройства>
   ```

4. Введите пароль пользователя `admin`.
5. **На устройстве Aviacode OS** отредактируйте конфигурационный файл SSH-сервера:

   ```
   sudo nano /etc/ssh/sshd_config
   ```

6. Найдите и измените/добавьте следующие директивы:

   ```
   PasswordAuthentication no PubkeyAuthentication yes PermitRootLogin no
   ```

7. Сохраните файл (`Ctrl+O`, `Enter`) и закройте редактор (`Ctrl+X`).
8. Перезапустите службу SSH для применения изменений:

   ```
   sudo systemctl restart sshd
   ```

9. **Важно:** Не закрывайте текущую SSH-сессию до проверки новой. Откройте новое окно терминала и убедитесь, что подключение под пользователем `admin` работает по ключу, а парольный вход и вход под `root` запрещены.

### 3.1.2 Настройка сети

**Настройка статического IP-адреса через netplan (рекомендуемый способ)**

Aviacode OS, основанная на кодовой базе Debian, может использовать `netplan` для управления сетью.

1. Отредактируйте конфигурационный файл (имя файла может отличаться):

   ```
   sudo nano /etc/netplan/01-netcfg.yaml
   ```

2. Приведите конфигурацию к виду (пример для интерфейса `eth0`):

```
network:
  version: 2
  renderer: networkd
  ethernets:
```

```
enP4p65s0:
  addresses:
    -  192.168.1.100/24
  routes:
    - to: default
      via: 192.168.1.1
  nameservers:
    addresses:
      - 77.88.8.8
```

3. Примените конфигурацию:

```
sudo netplan apply
```

### *3.1.3 Проверка корректности разрешения DNS и доступности сетевых ресурсов*

**Проверка разрешения имён (DNS):**

```
getent hosts docs.aviacod.ru
```

*Имя “docs.aviacod.ru” приведено для примера, необходимо проверить разрешение тех имён, которые требуются для работы прикладных приложений, планируемых к использованию.*

Убедитесь, что команда возвращает IP-адрес.

**Проверка доступности сетевого ресурса (ping):**

```
ping -c 4 77.88.8.8          # Проверка доступности внешнего IP

ping -c 4 docs.aviacod.ru  # Проверка доступности по имени (проверяет и DNS, и сеть)
```

*Адрес 77.88.8.8 приведен для примера, необходимо проверить доступность сетевого шлюза и тех адресов, которые требуются для работы прикладных приложений, планируемых к использованию*

**Проверка доступности конкретного порта (например, HTTPS для репозитория):**

```
timeout 5 bash -c 'cat < /dev/null > /dev/tcp/docs.aviacod.ru/443' && echo "Port is open" || echo "Port is closed"
```

### *3.3. Работа с репозиторием пакетов*

Перед установкой ПО критически важно проверить доступность и целостность репозитория.

**Проверка репозитория (на основе чек-листа):**

- Проверить в каталоге /usr/share/keyrings/ наличие GPG ключа aviacode-os.gpg  и при необходимости скачать или обновить ключ по URL https://repo.aviacod.ru/aviacode-os.gpg.
- Проверить наличие публичного ключа aviacode-os.crt и закрытого ключа aviacode-os.key в каталоге /etc/ssl/private/aviacode/ для обеспечение mTLS. При отсутствии обратиться в техническую поддержку производителя операционной системы.
- Проверить наличие репозитория Aviacode в файле /etc/apt/sources.list.d/aviacode.list.
- Проверить наличие файла конфигурации apt для репозитория Aviacode, в файле /etc/apt/apt.conf.d/90aviacode
- Выполните команду `sudo apt update`. Процесс должен завершиться успешно, без ошибок верификации подписи.
- Система **не должна** принимать обновления из репозитория, не подписанного доверенным ключом, при отсутствии ключей для mTLS, или с повреждённой подписью.

## 4. Установка и управление прикладным программным обеспечением

### *4.1. Установка пакетов ПО самообслуживания*

1. После успешного выполнения `apt update` установите необходимые пакеты: `sudo apt install <имя_пакета_прикладного_ПО>`.
2. Убедитесь, что в процессе установки не возникает ошибок проверки подписи пакетов.

### *4.2. Особенности установки ПО для инференса нейросетей (RKNN)*

Для пакетов, использующих RKNN Runtime, убедитесь, что целевая платформа (SoC с NPU) поддерживается и в системе присутствуют необходимые библиотеки (`librknnrt.so`). Проверьте соответствие версий RKNN Runtime и моделей.

### *4.3. Управление сервисами*

- Запуск сервиса: `sudo systemctl start <имя_сервиса>`
- Автозагрузка: `sudo systemctl enable <имя_сервиса>`
- Проверка статуса: `sudo systemctl status <имя_сервиса>`
- Остановка сервиса: `sudo systemctl stop <имя_сервиса>`
- Перезапуск сервиса: `sudo systemctl restart <имя_сервиса>`
- Отключение: `sudo systemctl disable <имя_сервиса>`

## 5. Диагностика и мониторинг

### *5.1. Проверка корректности работы*

После настройки и установки ПО выполните базовую проверку:

- Сетевые интерфейсы активны.
- Все целевые системные сервисы работают (`systemctl --all`).
- Прикладное ПО запускается и функционирует в целевом сценарии.

### *5.2. Диагностика состояния системы*

- **Загрузка:** При проблемах с загрузкой анализируйте последовательность (см. блок-схему в контексте): SoC -> Инициализация DDR -> Загрузочная среда (U-Boot) -> FIT-образ (проверка целостности) -> BL31 -> Ядро ОС. Используйте консоль отладки (UART).
- **Журналы:** Основные логи находятся в `/var/log/`. Используйте `journalctl` для просмотра журналов systemd.
- **Диагностические команды:** `dmesg`, `lsblk`, `ip a`, `apt-cache policy`.

### *5.3. Диагностика целостности загрузки*

В соответствии с архитектурой, FIT-образ содержит механизм **проверки целостности компонентов** (Trusted Firmware BL31, Device Tree) перед передачей управления. Нарушение целостности приведёт к остановке загрузки. В этом случае необходимо восстановить или перепрошить загрузочный образ.

## 6. Решение типовых проблем

### *6.1. Проблемы с загрузкой*

- **Симптом:** Устройство не выходит за этап U-Boot.
- **Действие:** Проверьте целостность загрузочного носителя. Убедитесь, что FIT-образ собран корректно для данной платформы. Проверьте консоль UART для сообщений об ошибках.

### *6.2. Ошибки при работе с репозиторием (`apt update`)*

- **Ошибка подписи:** Убедитесь, что в системе установлен актуальный GPG ключ. Проверьте дату и срок действия подписи репозитория.
- **"Невозможно получить доступ к репозиторию":** Проверьте сетевое подключение, доступность URL и корректность DNS, а также наличие публичного и закрытого ключа mTLS и файла конфигурации apt для подключения к репозиторию Aviacode.

### *6.3. Периферийные устройства не работают*

- Убедитесь, что устройство в списке совместимости.
- Проверьте, загружен ли соответствующий драйвер (`lsmod | grep <драйвер>`).

- Проверьте физическое подключение и настройки (IP-адрес принтера).

## 7. Безопасность

### *7.1. Базовая настройка безопасности*

- Своевременно обновляйте систему только из доверенного подписанного репозитория (`sudo apt upgrade`).
- Отключите неиспользуемые сетевые службы.
- Установите и настройте брандмауэр (`ufw` или `nftables`).

### *7.2. Гарантии целостности*

Эксплуатационная среда гарантирует:

- Невозможность установки неподписанных пакетов из официального репозитория.
- Проверку целостности загрузочной цепи (FIT-образ).
- Использование production-сборок, не содержащих debug-компонентов.

## 8. Дополнительные возможности

### *8.1. Поддержка нового оборудования/ПО*

Для запроса на добавление нового оборудования или программного обеспечения в списки совместимости обратитесь по адресу: **office@aviacod.ru**.

### *8.2. Автоматизация подготовки комплекса*

Aviacode OS поставляется с преднастроенной базовой конфигурацией, что позволяет автоматически разворачивать целевые сервисы после установки. Корректность работы в целевом сценарии проверяется внутренними чек-листами.

**Приложение А. Чек-лист первоначальной настройки**

1. [ ] Проверено наличие оборудования в HCL.
2. [ ] Установлен FIT-образ Aviacode OS.
3. [ ] Настроено сетевое подключение, проверен DNS.
4. [ ] Выполнена проверка доступности и подписи репозитория (`apt update`).
5. [ ] Установлено необходимое прикладное ПО.
6. [ ] Целевые сервисы запущены и добавлены в автозагрузку.
7. [ ] Проведено тестовое функционирование в целевом сценарии.

**Приложение Б. Глоссарий**

- **SoC (System on Chip):** Интегральная схема, содержащая все компоненты вычислительной системы.
- **NPU (Neural Processing Unit):** Процессор для ускорения нейронных сетей.

- **RKNN:** Runtime-окружение для выполнения нейросетевых моделей на NPU Rockchip.
- **FIT-образ (Floppyless Image Tree):** Единый образ, содержащий ядро, Device Tree и initramfs, с поддержкой проверки целостности.
- **Device Tree:** Структура данных, описывающая аппаратную конфигурацию системы для ядра ОС.