NICE OS
RU LINUX

ООО «НАЙС СОФТ ГРУПП»
ИНН 5024245440
КПП 502401001
ОГРН 1245000085846

ООО «НАЙС СОФТ ГРУПП»

Документация, содержащая описание функциональных характеристик экземпляра программного обеспечения НАЙС.ОС, предоставленного для проведения экспертной проверки

ООО «НАЙС СОФТ ГРУПП»
ИНН 5024245440
КПП 502401001
ОГРН 1245000085846

ООО «НАЙС СОФТ ГРУПП»
ИНН 5024245440
КПП 502401001
ОГРН 1245000085846

1. Введение

1.1 Назначение документа

Настоящий документ содержит описание функциональных и архитектурных характеристик редакции **НАЙС.ОС CLOUD** — специализированной модификации операционной системы общего назначения НАЙС.ОС, предназначенной для применения в облачных средах, контейнерной инфраструктуре, системах автоматизации и CI/CD-пайплайнах.

Документ разработан с целью:

- формализации архитектурных и функциональных решений, реализованных в редакции CLOUD;
- подтверждения соответствия программного обеспечения требованиям нормативных документов Российской Федерации, включая Постановление Правительства №1236;
- обеспечения полноты и прозрачности сведений, необходимых для включения в **Единый реестр российских программ для электронных вычислительных машин и баз данных**;
- использования в качестве базового описания для сопровождающей документации, технического анализа и проектирования решений на базе редакции CLOUD.

1.2 Основания для разработки

Документ разработан в рамках подготовки редакции **НАЙС.ОС CLOUD** к включению в Единый реестр российского программного обеспечения, на основании следующих оснований:

- Приказ Минцифры России, устанавливающий порядок подачи и рассмотрения заявлений о включении программного обеспечения в Реестр;
- Требования Постановления Правительства Российской Федерации №1236 от 16 ноября 2015 г. (в редакции от 1 января 2024 г.);
- Методические рекомендации и шаблоны, утверждённые ФГИС «Единый реестр отечественного ПО»;
- Требования ГОСТ 19.201–78, ГОСТ 19.101–77, ГОСТ Р ИСО/МЭК 42010–2019 в части оформления и описания архитектурных решений;
- Политика обеспечения импортонезависимости и стратегического развития свободного программного обеспечения;
- Инициатива ООО «НАЙС СОФТ ГРУПП» по разработке воспроизводимой, криптографически защищённой облачной редакции операционной системы.

1.3 Область применения

Редакция **НАЙС.ОС CLOUD** предназначена для следующих сценариев эксплуатации:

- Автоматизированное развёртывание серверов в облачных инфраструктурах IaaS/PaaS/Private Cloud;
- Использование в качестве базового образа в CI/CD-средах, включая GitLab CI, Jenkins, Buildbot и др.;
- Развёртывание в контейнерах (Docker/Podman), кластерах Kubernetes и нативных runtime-средах (systemd-nspawn);
- Интеграция с системами конфигурации и управления инфраструктурой: **Ansible**, **cloud-init**, **kickstart**, **cloud-config**;
- Встраивание в DevOps-пайплайны как минималистичной платформы для кастомизации и расширения;
- Разработка и сопровождение образов в формате OCI, RAW, qcow2, ISO для масштабируемых поставок;
- Сценарии эксплуатации без графического интерфейса (headless-first) с акцентом на CLI-управление и API-интерфейсы.

1.4 Термины и сокращения

Термин/ сокращение	Расшифровка
НАЙС.ОС	Операционная система, разработанная ООО «НАЙС СОФТ ГРУПП»
CLOUD	Облачная редакция без графического интерфейса (headless)
CI/CD	Непрерывная интеграция / непрерывная доставка (Continuous Integration / Continuous Delivery)
OCI	Open Container Initiative — стандарт формата контейнеров
OSTree	Система атомарного управления версиями файловой системы
SPDX	Software Package Data Exchange — стандарт маркировки лицензий

GPG	GNU Privacy Guard — система криптографической подписи и шифрования
ГОСТ	Государственный стандарт Российской Федерации
РР №1236	Постановление Правительства РФ №1236 от 16.11.2015 о запрете закупок иностранного ПО
HEADLESS	Окружение без графического интерфейса
systemd-nspawn	Изолированное выполнение процессов в контейнероподобных средах с systemd
cloud-init	Система автоматической инициализации облачных виртуальных машин

2. Общая характеристика архитектуры

2.1 Архитектурный подход: *headless-first*, минимальное окружение выполнения

Редакция **НАЙС.ОС CLOUD** разрабатывается в соответствии с принципом **headless-first** — исключено наличие графического интерфейса пользователя, все взаимодействие осуществляется через CLI, API и системы удалённой конфигурации. Такой подход позволяет:

- минимизировать поверхность атаки и объём устанавливаемого ПО;
- повысить скорость и предсказуемость развёртывания;
- снизить требования к ресурсам (RAM, диск, CPU);
- упростить встраивание в контейнеризированные и облачные среды.

ООО «НАЙС СОФТ ГРУПП»
ИНН 5024245440
КПП 502401001
ОГРН 1245000085846

Архитектура операционной системы ориентирована на **минимальное окружение выполнения (minimal runtime)** с заранее определённым набором компонентов, необходимых для выполнения задач CI/CD, контейнеризации, автоматизации и конфигурации.

2.2 Основные принципы: воспроизводимость, криптозащита, автоматизация

В архитектурную основу **НАЙС.ОС CLOUD** заложены следующие принципы:

- **Воспроизводимость (reproducible builds):**
  - использование переменных среды (`SOURCE_DATE_EPOCH`, `BUILD_PATH_PREFIX_MAP`);
  - фиксация всех зависимостей и параметров сборки;
  - детерминированная упаковка (tar, gzip, ostree с отключёнными метками времени);
  - автоматическая верификация хешей и бинарной идентичности (diffoscope, rebuilderd).
- **Интеграция криптографии ГОСТ:**
  - встроенная поддержка ГОСТ-алгоритмов в OpenSSL, GnuTLS, GPG, Nettle, OpenVPN;
  - системная генерация и валидация подписей с применением ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012;

- обязательная подпись всех релизов и пакетов, включая `.sig`, `.asc`, detached hash.

- **Автоматизация жизненного цикла:**
  - cloud-init и cloud-config для конфигурирования виртуальных машин и контейнеров;
  - ansible-совместимые роли и сценарии начальной настройки;
  - стандартные инструменты автоматизации: systemd timers, kickstart, REST-интерфейсы и D-Bus.

Применение этих принципов обеспечивает стабильность, предсказуемость и соответствие современным требованиям к защищённым инфраструктурным ОС.

2.3 Уровни архитектуры: логический / программный / виртуальный

Архитектура **НАЙС.ОС CLOUD** представлена в виде трёх основных уровней:

Уровень	Описание
Логический	Включает компонентную модель операционной системы, описание ролей (init, system, networking, security), модули и зависимости между ними, а также логику взаимодействия компонентов
Программный	Отражает структуру ПО: ядро Linux, systemd-окружение, системные службы, CLI-интерфейсы, криптобиблиотеки, инструменты контейнеризации, модули cloud-init, Ansible и DevOps-агенты
Виртуальный	Определяет возможные среды развёртывания: образы OCI, системы на базе Kubernetes, контейнеры в Podman/systemd-nspawn, виртуальные машины в QEMU/KVM, образцы в формате ISO, RAW и qcow2

ООО «НАЙС СОФТ ГРУПП»
ИНН 5024245440
КПП 502401001
ОГРН 1245000085846

Каждый уровень проектируется с учётом расширяемости, независимости модулей, минимального окружения и обеспечения безопасности при автоматизированной доставке ПО.

3. Компонентная архитектура

3.1 Модули и сервисы: сетевые, инфраструктурные и криптографические

Редакция **НАЙС.ОС CLOUD** строится на строго определённом наборе компонент, предназначенных исключительно для работы в автоматизированных, безголовых (headless) средах. В состав входят:

- **Сетевые компоненты:**
  - `systemd-networkd`, `resolved`, `nftables`, `iproute2`, `dhcpcd`;
  - поддержка туннелирования (WireGuard, OpenVPN ГОСТ), IPv6, VLAN и bridge-режимов.
- **Инфраструктурные службы:**
  - `systemd`, `journald`, `logind` (в режиме headless);
  - `machine-id`, `hostname`, `localectl`, `timedatectl` — минимальные компоненты инициализации хоста.
- **Криптографическая база:**

ООО «НАЙС СОФТ ГРУПП»
ИНН 5024245440
КПП 502401001
ОГРН 1245000085846

- `libcrypto` с интеграцией ГОСТ-алгоритмов (OpenSSL/gost-engine, GnuTLS, Nettle);
- `gpg`, `gpg-agent` с поддержкой ГОСТ в `libgcrypt` и `libksba`;
- модули валидации подписей, генерации ключей, работы с сертификатами и контуром доверия.

Графические, мультимедийные и пользовательские компоненты полностью исключены.

3.2 Взаимодействие: D-Bus, journald, REST, systemctl

Компоненты ОС взаимодействуют друг с другом исключительно по стандартным, надёжным интерфейсам:

- **D-Bus (system/host session):** транспорт событий, запросов конфигурации и контроля служб;
- **journald:** централизованное логирование действий, в том числе CI/CD-агентов, сетевых демонов, systemd-юнитов;
- **REST API:** модули, предоставляющие веб-интерфейсы управления и автоконфигурации (через `cloud-init`, webhooks и конфигурационные агенты);
- **`systemctl`/`loginctl`/`hostnamectl` и другие средства CLI:** основа для автоматизированного управления в сценариях конфигурации, деплоя и DevOps-интеграции.

ООО «НАЙС СОФТ ГРУПП»
ИНН 5024245440
КПП 502401001
ОГРН 1245000085846

Все взаимодействия производятся без участия пользователя, по строго определённым протоколам и в изолированных окружениях.

3.3 Зависимости и слои: минимальная связанность, роль образа

Компоненты организованы в **многослойную структуру**, каждая часть которой независима и воспроизводима:

- **Базовый слой (runtime):** ядро, системные библиотеки, cryptobase;
- **Слой сервисов:** службы инициализации, управления сетью, ключами, логами;
- **Роль/образ (role container):** настроенные поверх базового слоя слои с ansible/kickstart-контентом;
- **Персистентные данные:** тома или конфигурации, загружаемые через `cloud-init`, `Ignition`, `Ansible-push`.

Каждый слой создаётся и проверяется отдельно, что обеспечивает детерминированность, воспроизводимость и модульность.

3.4 Расширяемость: cloud-init, Ansible, kickstart, OSTree

Для конфигурирования и масштабируемого расширения среды предусмотрены стандартные инструменты:

- **`cloud-init`:** начальная настройка облачного хоста, установка ключей, пакетов, параметров сети и пользователей;

ООО «НАЙС СОФТ ГРУПП»
ИНН 5024245440
КПП 502401001
ОГРН 1245000085846

- **`Ansible:`** применение готовых ролей и сценариев (`ansible-pull` и `ansible-playbook`), в том числе с поддержкой SELinux/Firewalld;
- **`kickstart:`** автоматизация начальной установки, генерация кастомизированных образов;
- **`OSTree:`** дельта-обновления, версионирование, откат и атомарное применение изменений.

Механизм расширения не требует пересборки базового образа и может быть интегрирован в CI/CD пайплайн или систему централизованного управления инфраструктурой.

4. Программная архитектура

4.1 Ядро: Linux LTS/hardened + PIE/RELRO

Редакция **НАЙС.ОС CLOUD** использует защищённое и модифицированное ядро Linux в вариантах:

- **LTS-ветка:** стабильная версия с длительной поддержкой;
- **Сборка с флагами безопасности:**
  - `CONFIG_STACKPROTECTOR_STRONG`, `CONFIG_RANDOMIZE_BASE`, `CONFIG_KALLSYMS_HIDE`, `CONFIG_STATIC_USERMODEHELPER`;
  - поддержка ASLR, NX-бит, сегментной изоляции и hardened-загрузки.

Все исполняемые файлы и библиотеки собираются с флагами безопасности:

ООО «НАЙС СОФТ ГРУПП»
ИНН 5024245440
КПП 502401001
ОГРН 1245000085846

- `-fPIE`, `-pie` — только PIE-бинарники;
- `-Wl,-z,relro,-z,now` — жёсткая защита от модификации GOT;
- `-D_FORTIFY_SOURCE=2`, `-fstack-protector-strong`, `-O2` — упрочнение системных и пользовательских утилит.

4.2 Службы: systemd-networkd, journald, sshd, VPN

Сервисный уровень состоит исключительно из инфраструктурных и сетевых служб:

- **Сетевые службы:**
  - `systemd-networkd` — конфигурация сетевых интерфейсов, поддержка bridge/VLAN;
  - `systemd-resolved` — DNS и MDNS;
  - `iptables`/`nftables` — сетевые политики доступа;
  - поддержка OpenVPN с ГОСТ, WireGuard, туннелирование и split-routing.
- **Логирование и мониторинг:**
  - `systemd-journald` — центральный журнал событий;
  - поддержка удалённой агрегации логов, сигнатур хешей и ретроспективного аудита.
- **Управление доступом:**

ООО «НАЙС СОФТ ГРУПП»
ИНН 5024245440
КПП 502401001
ОГРН 1245000085846

- `sshd` — безопасный вход по SSH с обязательной проверкой ключей и 2FA;
- `pam_limits`, `pam_faillock`, `login.defs` — ограничение и аудит доступа.

4.3 Среда CLI: TTY, SSH, tmux, без GUI

В редакции **CLOUD** полностью исключено графическое окружение:

- **Взаимодействие только через CLI:**
  - `TTY`, `getty`, `bash/dash` — базовая консоль;
  - `SSH` — основной канал удалённого доступа;
  - `tmux`, `screen` — мультиплексоры терминалов;
  - `micro`, `nano`, `vim` — текстовые редакторы (опционально).
- Среда запуска изолирована, все интерфейсы доступны только по IP/UNIX-сокетам, поддерживается ведение командной истории с логированием.

4.4 Cloud tooling: cloud-init, dbus-run-session, curl, podman

Для развёртывания и автоматизации используются стандартные и расширяемые инструменты:

- **`cloud-init`:**
  - поддержка всех поставщиков метаданных (NoCloud, OpenStack, EC2, Hetzner, Azure и др.);

ООО «НАЙС СОФТ ГРУПП»
ИНН 5024245440
КПП 502401001
ОГРН 1245000085846

- автоматическая настройка ключей, имени хоста, сети, sshd, пользователей.

- **`dbus-run-session`:**
  - безопасное выполнение сервисов с D-Bus в headless-режиме (например, для конфигурационных агентов);

- **`curl`, `wget`, `ca-certificates`:**
  - базовые утилиты обмена с REST API, webhook-интеграций, скачивания конфигураций;

- **`podman`, `buildah`:**
  - бездемонное выполнение и сборка контейнеров;
  - поддержка rootless-контейнеризации, OCI-образов и systemd-юнитов внутри контейнеров.

Весь инструментарий совместим с DevOps/CI-инфраструктурами и может быть встроен в пайплайны развёртывания и обновления инфраструктуры.

5. Аппаратная совместимость

5.1 Поддерживаемые архитектуры и платформы

Операционная система **НАЙС.ОС CLOUD** ориентирована на развертывание в современных облачных и серверных средах. Поддерживаются следующие аппаратные архитектуры:

ООО «НАЙС СОФТ ГРУПП»
ИНН 5024245440
КПП 502401001
ОГРН 1245000085846

- **x86_64 (amd64):** основная целевая архитектура с полной поддержкой всех функций, включая аппаратное ускорение виртуализации (Intel VT-x, AMD-V), SSE4, AVX и TPM 2.0;
- **ARM64 (AArch64):** в планах расширения — экспериментальная поддержка платформ на базе Ampere, HiSilicon, Rockchip и Raspberry Pi CM4;
- Совместимость как с **BIOS**, так и с **UEFI** прошивками, включая гибридные режимы загрузки (CSM/UEFI mixed).

5.2 Целевые среды выполнения

Редакция **CLOUD** ориентирована на безэкранные среды исполнения с возможностью масштабируемого развёртывания. Поддерживаются следующие гипервизоры и контейнерные технологии:

- **KVM/QEMU** — основная среда виртуализации; поддержка UEFI Secure Boot через `OVMF`;
- **systemd-nspawn** — lightweight контейнеризация для изолированного развертывания сервисов и отладки;
- **OCI-compatible runtime:** полностью поддерживаются `podman`, `crun`, `runc`, что позволяет использовать систему в роли базового образа (base image) в Kubernetes, Docker, OpenShift и аналогичных средах;
- Поддержка UEFI Secure Boot:
    - загрузка через `shim + GRUB` с проверкой подписей;

ООО «НАЙС СОФТ ГРУПП»
ИНН 5024245440
КПП 502401001
ОГРН 1245000085846

- возможна интеграция с корпоративными ключами;
- создание собственных ключей и инфраструктуры подписания загрузчиков.

5.3 Хранилища и форматы образов

Операционная система распространяется в формате готовых к развёртыванию образов, соответствующих стандартам облачных провайдеров:

- **Образы:**
  - `RAW` — для универсальной записи на диски или развёртывания через dd/virt-install;
  - `qcow2` — для интеграции с libvirt/KVM;
  - `OCI` — для контейнеризации и публикации в реестры;
  - `ISO` (опционально) — для автономной установки и тестирования;
- **Шифрование:**
  - Поддержка установки на LUKS 2 (с ключами в TPM или passphrase);
  - Интеграция с TPM 2.0 через `clevis`, `tpm2-tools` и `systemd-cryptenroll`;
  - Возможность автозагрузки зашифрованных разделов при наличии TPM или через cloud-init config;
- **Форматы метаданных:**

ООО «НАЙС СОФТ ГРУПП»
ИНН 5024245440
КПП 502401001
ОГРН 1245000085846

- `buildinfo`, `.manifest`, `.sig` — для проверки целостности и происхождения;
- SHA256 и ГОСТ Р 34.11-2012 хеши, OpenPGP-подписи;
- Поддержка `systemd-repart` для создания и верификации подписанных образов.

6. Сетевая архитектура

6.1 Минимальный сетевой стек

В редакции **НАЙС.ОС CLOUD** реализован минималистичный, но полнофункциональный сетевой стек, ориентированный на автоматическое развертывание и защищённую эксплуатацию в облачных средах. Поддерживаются:

- **IPv4 и IPv6:** конфигурация осуществляется через DHCP, SLAAC или вручную (static);
- **WireGuard:** встроенная поддержка шифрованных одноранговых соединений с использованием минимальной конфигурации, пригодной для автоматизации;
- **OpenVPN ГОСТ:** включена поддержка OpenVPN с патчами для алгоритмов ГОСТ Р 34.10/34.11, TLS-GOST 1.2 и защищённого канального взаимодействия по ГОСТ;

ООО «НАЙС СОФТ ГРУПП»
ИНН 5024245440
КПП 502401001
ОГРН 1245000085846

Доступна полная настройка всех протоколов через CLI, `cloud-init`, `networkd` и внешние системы управления.

6.2 Поддерживаемые протоколы и механизмы

Система предоставляет поддержку современных и безопасных протоколов, необходимых для эксплуатации в DevOps- и CI/CD-средах:

- **SSH (OpenSSH):** основное средство удалённого доступа и управления;
- **HTTPS (cURL, wget):** TLS-соединения с проверкой цепочки доверия и поддержкой ГОСТ-сертификатов;
- **DNS:** разрешение имён через `systemd-resolved` или статически заданные адреса;
- **cloud-init + DHCP:** автоматическая настройка при первом запуске (first boot), в том числе получение конфигурации сети, ключей SSH, метаданных и маршрутов.

6.3 Сетевые службы

Следующие компоненты используются для настройки, управления и фильтрации сетевого взаимодействия:

- **systemd-networkd:** основной компонент настройки сетевых интерфейсов и маршрутов;
- **systemd-resolved:** DNS-резолвер с поддержкой split-DNS и fallback;
- **firewalld:** динамическое управление зонами безопасности и правилами доступа;

ООО «НАЙС СОФТ ГРУПП»
ИНН 5024245440
КПП 502401001
ОГРН 1245000085846

- **nftables:** современный подсистемный firewall, обеспечивающий фильтрацию трафика на уровне ядра;

Все службы настроены на работу в headless-среде и могут быть управляемы через `systemctl`, `dbus`, `networkctl` и интерфейсы конфигурации.

6.4 Безопасность и автоматизация конфигурации сети

Для обеспечения воспроизводимой и безопасной конфигурации применяются следующие подходы:

- **cloud-config:** автоматическая настройка сети при запуске виртуальной машины или контейнера, включая прокси, VPN, маршруты и ключи;
- **ansible:** поддерживаются ansible-роли для настройки сетевых интерфейсов, NAT, VPN-туннелей, параметров безопасности (firewalld, nftables);
- **минимальные привилегии:** все службы работают в изолированных namespaces, с systemd-сервисами в режиме `DynamicUser`, `ProtectSystem`, `ProtectHome`;
- **логирование:** все сетевые события фиксируются через `journald`, доступен экспорт в централизованные системы аудита.

ООО «НАЙС СОФТ ГРУПП»
ИНН 5024245440
КПП 502401001
ОГРН 1245000085846

7. Архитектура безопасности

7.1 Основные принципы

В редакции **НАЙС.ОС CLOUD** реализована архитектура «безопасность по умолчанию», основанная на следующих принципах:

- **Минимальные привилегии (Principle of Least Privilege):** все службы и процессы запускаются с максимально ограниченными правами, без root-доступа, с ограничениями на файловую и сетевую подсистему;
- **Криптографическая верификация:** каждый артефакт (бинарный пакет, образ, метаданные) проверяется по цифровой подписи, верифицируется по хешу и сопровождается метаинформацией;
- **Полная прозрачность цепочек поставки:** в рамках CI/CD-процессов обеспечена трассируемость сборки, подписи, загрузки и установки.

7.2 Механизмы изоляции

Для обеспечения защиты на уровне ядра и окружения исполнения используются следующие технологии:

- **Namespaces:** каждый процесс выполняется в собственном пространстве имён (PID, UTS, MNT, NET, IPC), что исключает доступ к другим контейнерам или хосту;
- **Systemd sandboxing:** все сервисы конфигурируются с использованием `ProtectSystem`, `ProtectHome`, `ReadOnlyPaths`, `NoNewPrivileges` и `DynamicUser`;

ООО «НАЙС СОФТ ГРУПП»
ИНН 5024245440
КПП 502401001
ОГРН 1245000085846

- **Cgroups v2:** применяется для ограничения ресурсов (CPU, RAM, IO), а также для контроля и приоритезации сервисов в рамках контейнеров и VM;
- **Без GUI:** исключение всех графических подсистем и X11 исключает целый класс атак и упрощает доверенную поверхность.

7.3 Интеграция ГОСТ-криптографии

Вся криптографическая инфраструктура в редакции **НАЙС.ОС CLOUD** дополнена и переориентирована на использование отечественных алгоритмов:

- **OpenSSL + gost-engine:** полная поддержка алгоритмов ГОСТ Р 34.10-2012, 34.11-2012, 34.13-2015 для TLS, PKI и хеширования;
- **GnuTLS (patched):** дополнена поддержка TLS-GOST 1.2, шифров и ключевых обменов на основе ГОСТ;
- **GnuPG + libgcrypt (ГОСТ):** поддержка подписей и шифрования с использованием ГОСТ-алгоритмов и сертифицированных ключей;
- **OpenVPN ГОСТ:** используется патчированный OpenVPN с полным TLS-1.2-GOST стеком;
- **libksba (CMS):** реализация ГОСТ-подписей и шифрования в формате CMS (Cryptographic Message Syntax);
- **Nettle:** базовая криптобиблиотека, включающая алгоритмы ГОСТ (через патчи или кастомные билды);

ООО «НАЙС СОФТ ГРУПП»
ИНН 5024245440
КПП 502401001
ОГРН 1245000085846

Использование ГОСТ в криптосреде является обязательным для всех компонентов, участвующих в передаче, хранении и верификации данных.

7.4 Подписи и доверие

Целостность и подлинность всех компонентов гарантируется следующими механизмами:

- **GPG/PGP:** все пакеты и образы подписываются ключами, прошедшими верификацию через внутренний PKI;
- **.sig/.asc:** каждая сборка сопровождается отсоединённой подписью (`.sig`, `.asc`) для проверки пользователем или CI-инфраструктурой;
- **SHA256, ГОСТ Р 34.11-2012:** применяется для формирования контрольных сумм и построения hash chain;
- **manifest/.buildinfo:** каждое хранилище содержит контрольную информацию о составе, времени, авторе сборки, параметрах компиляции и подписи.

8. Интеграция и расширение

8.1 Поддержка автоматизации: Ansible, cloud-init, REST API

Редакция **НАЙС.ОС CLOUD** проектируется как полностью автоматизируемая и управляемая система, включающая:

- **Ansible:** поддержка ролей и плейбуков для развертывания, настройки, обновления компонентов. Включает типовые роли для настройки сети, пользователей, служб, TLS/SSH и пр.;

- **cloud-init:** полная поддержка декларативной инициализации виртуальных машин и образов. Поддерживаются user-data, meta-data и cloud-config форматы, включая автообновление SSH-ключей, запуск скриптов, настройку сети и пр.;

- **REST API (D-Bus bridge):** поддержка вызовов через D-Bus с возможностью обёртывания в REST-интерфейсы для автоматизированного управления (через cockpit или кастомные решения).

8.2 CI/CD-интеграция и контейнеризация

Редакция **НАЙС.ОС CLOUD** включает полный набор средств для использования в CI/CD пайплайнах как базового слоя:

- **Контейнеризация:** образ может быть использован как `base image` в Docker/Podman для сборки и тестирования ПО, с минимальным набором зависимостей;

- **Инфраструктура сборки:** поддержка использования в GitLab CI, GitHub Actions, BuildKit, а также в офлайн-сценариях сборки (`buildah`, `rpmbuild`);

- **Изоляция:** каждый этап CI/CD может запускаться в отдельном контейнере или namespace на базе образа `niceos-cloud`, что упрощает повторяемость и безопасное выполнение задач.

ООО «НАЙС СОФТ ГРУПП»
ИНН 5024245440
КПП 502401001
ОГРН 1245000085846

8.3 Развёртывание и оркестрация

НАЙС.ОС CLOUD совместим с широким спектром платформ для автоматизированного развёртывания:

- **Kubernetes (K8s):** OCI-совместимые образы могут быть использованы как базовые слои для подов и контейнеров с возможностью настройки через ConfigMap/Secret;
- **Podman:** развёртывание контейнеров с использованием rootless-режима и systemd-интеграции (`podman generate systemd`);
- **systemd-nspawn:** запуск как изолированных системных контейнеров, поддерживающих полную инициализацию через `systemd` и автозагрузку;
- **Kickstart/OSTree:** поддержка массовой установки и обновления через автоматизированные конфигурационные шаблоны.

8.4 Интеграция с DevOps-инструментами

НАЙС.ОС CLOUD предоставляет интерфейсы и механизмы взаимодействия с экосистемой DevOps, включая:

- **Интеграция с внешними API:** поддержка инструментов Terraform, Packer, cloud-provider SDKs (через REST и CLI-интерфейсы);
- **Инструменты контроля состояния:** совместимость с Prometheus, Grafana, journald-forwarding, syslog-ng;
- **Журналирование и аудит:** полная совместимость с системами аудита и логирования (journald, auditd, in-toto);

ООО «НАЙС СОФТ ГРУПП»
ИНН 5024245440
КПП 502401001
ОГРН 1245000085846

- **Готовность к внешней автоматизации:** управление пользователями, службами, хранилищами через systemd и D-Bus без необходимости GUI-интерфейсов.

9. Репозитории и доставка

9.1 Репозиторий исходного кода: Gitea с RBAC и подписью коммитов

Исходный код **НАЙС.ОС CLOUD** размещён в собственном инстансе Gitea на сервере организации-разработчика. Инфраструктура репозитория реализует следующие механизмы:

- **Управление доступом:** применяется разграничение ролей (RBAC) с типами: `reader`, `developer`, `maintainer`, `reviewer`;
- **Подписи коммитов:** все изменения исходного кода фиксируются с обязательной GPG-подписью (`git commit -S`), верификация осуществляется автоматически при CI-сборке;
- **Аудит и история:** включена полная трассировка изменений, журналирование всех операций через WebHook/Matrix и внешние системы.

9.2 CI/CD: формирование и подпись артефактов

Автоматизированные процессы сборки и публикации выполняются в изолированных CI/CD-агентах, без доступа к root и сети, с выпуском следующих сопроводительных материалов:

ООО «НАЙС СОФТ ГРУПП»
ИНН 5024245440
КПП 502401001
ОГРН 1245000085846

- **.manifest** — перечень включённых пакетов, хешей, флагов сборки и путей;
- **.buildinfo** — информация о версии компилятора, времени, окружении, переменных среды;
- **Подписи:** все бинарные и метаданные артефакты сопровождаются цифровой подписью (OpenPGP GOST, `.sig`/`.asc`), с возможностью проверки независимо от CI.

Каждому артефакту сопоставляется идентификатор версии `niceos-cloud-X.Y.Z-rN`, реализован контроль воспроизводимости (Reproducible Builds).

9.3 Форматы доставки и публикации

Собранные артефакты распространяются в нескольких форматах, ориентированных на разные сценарии применения:

- **RPM** — пакеты для установки и обновления компонентов внутри системы;
- **OCI-образы** — контейнерные образы для Docker/Podman/Kubernetes;
- **OSTree** — атомарная поставка системы в виде дерева объектов, поддержка rollback;
- **qcow2 / RAW** — виртуальные образы для запуска в QEMU/KVM и аналогичных средах;
- **ISO** — установочные и Live-образы для развертывания с физических/виртуальных носителей.

ООО «НАЙС СОФТ ГРУПП»
ИНН 5024245440
КПП 502401001
ОГРН 1245000085846

Каждый тип доставки сопровождается сигнатурами, проверяемыми средствами rpm, ostree, podman и др.

9.4 Резервное копирование и контроль версий

Инфраструктура хранения и доставки включает надёжные механизмы защиты данных:

- **borgbackup** — используется для ежедневного резервного копирования всех артефактов, репозиториев, конфигураций;
- **snapshots** — применяются точечные снимки (OSTree, Btrfs) на уровне версий;
- **WORM-хранилище** — поддерживается архивирование в неизменяемые разделы для длительного хранения;
- **каталоги ISO-архивов** — периодически публикуются релизные сборки в формате `.iso`, зафиксированные и подписанные.

Все резервные копии проходят регулярную проверку контрольных сумм и хранятся на нескольких физических площадках.

10. Выводы

10.1 Соответствие требованиям ГОСТ и Постановления Правительства № 1236

Редакция **НАЙС.ОС CLOUD** полностью соответствует требованиям следующих нормативных документов:

- ГОСТ 19.201–78 — в части структуры архитектурного описания;
- ГОСТ Р ИСО/МЭК 42010–2022 — по модели представления архитектуры программных систем;
- Методических рекомендаций Минцифры для включения в **Единый реестр российского ПО**;
- Постановления Правительства РФ № 1236 от 16 ноября 2015 г. — по критериям отечественного происхождения и исключительного права на программное обеспечение.

Архитектура, средства разработки, а также процессы поставки и поддержки соответствуют установленным требованиям для регистрации программных средств в официальных федеральных системах.

10.2 Готовность к реестровой экспертизе

Документационный пакет и технические средства сопровождения **НАЙС.ОС CLOUD** обеспечивают:

- наличие полной цепочки доверия: от исходных кодов до финальных артефактов;
- открытость исходного кода, подтверждённую GPG-подписями и схемой SPDX;
- воспроизводимость сборок и контроль идентичности бинарных выпусков;
- наличие структурированных описаний, отражающих назначение, архитектуру и состав ПО.

Это гарантирует готовность редакции к прохождению технической, правовой и лингвистической экспертизы при подаче заявки в Единый реестр отечественного ПО.

10.3 Перспективы развития

В рамках перспективных направлений развития **НАЙС.ОС CLOUD** планируется:

- **Интеграция eBPF** — для повышения контроля за сетевыми потоками и безопасностью в контейнерных средах;
- **Поддержка архитектур Elbrus и RISC-V** — с акцентом на импортонезависимость и совместимость с отечественными аппаратными платформами;
- **Разработка защищённой редакции** — с реализацией требований по безопасности согласно регламентам ФСТЭК и ФСБ.

Кроме того, приоритетной целью остаётся совершенствование DevSecOps-инфраструктуры, упрощение масштабируемого развёртывания и интеграция в корпоративные облака.

10.4 Подтверждение зрелости и импортонезависимости

Редакция **НАЙС.ОС CLOUD** демонстрирует высокую степень архитектурной зрелости, включающую:

- компонентную модульность и возможность расширения без изменения базового слоя;

ООО «НАЙС СОФТ ГРУПП»
ИНН 5024245440
КПП 502401001
ОГРН 1245000085846

- независимость от зарубежных коммерческих платформ;
- реализацию всех критических компонентов — от ядра до криптографии — исключительно на открытом программном обеспечении с возможностью независимой верификации;
- готовность к промышленному использованию в средах DevOps, CI/CD и облачных провайдеров.

Таким образом, система соответствует современным требованиям суверенной цифровой инфраструктуры Российской Федерации.