Экосистема контейнеров НАЙС.ОС

Экосистема контейнеров НАЙС.ОС

Мы построили собственную экосистему для сборки контейнерных образов, основанную на принципах прозрачной цепочки поставки, воспроизводимости и строгой безопасности. Наши образы собираются из официальных репозиториев НАЙС.ОС, метаданные формируются автоматически, а процессы адаптированы под требования предприятий и регуляторов.

Прозрачная цепочка поставки Воспроизводимые сборки Жёсткая безопасность Готово к enterprise OCI-метаданные Air-gapped

Зачем и почему мы это сделали

- — Нужна **проверяемая** поставка ПО без «серых» скачиваний и чужих архивов.
- — Требуются **детерминированные** и воспроизводимые образы для масштабной эксплуатации.
- — Важно **соответствие требованиям** ИБ и регуляторов (включая ГОСТ-криптографию).
- — Нужна **универсальность**: одинаково работать с Docker, Podman, nerdctl и в закрытых контурах.

Для кого это подходит

DevOps / Платформенные команды

Стабильные базовые образы, единая версияционная модель, предсказуемые обновления и автоматические OCI-лейблы для каталогов образов и GitOps-процессов.

- Консистентная база НАЙС.ОС
- Готовность к Kubernetes/Openshift

- Удобный lifecycle: build attest push deploy

SecOps / Комплаенс / Гос-сектор

Отслеживаемое происхождение, отключение SUID/SGID по умолчанию, генерируемые SBOM и возможность подписи/аттестаций.

- Подпись образов и аттестации (опционально)
- Экспорт SBOM (SPDX/CycloneDX)
- Поддержка отечественной криптографии

Продуктовые команды

Именование образов по пакету, тег — из версии RPM, возможность выпуска специализированных образов «одним движением».

- Схема тегов: `niceos/<pkg>:<version>` (+ `latest` по политике)
- Пресеты для популярных стеков (по желанию)
- Минимальная поверхность атаки и быстрый cold start

Инфраструктура с ограниченным доступом

Сборка и публикация в полностью изолированных контурах без внешних загрузок; одинаковые процессы для online/offline сценариев.

- Air-gapped friendly
- Кэшируемые артефакты и журналы сборок
- Единая методика для разных регистри

Чем хорош подход наших образов

1. Прозрачная цепочка поставки

Все файлы в образе происходят из официальных RPM-пакетов НАЙС.ОС, установленных в изолированное *installroot*. Подписи RPM проверяются системными ключами — вы всегда знаете «кто и откуда».

- • Единый источник истины — репозитории НАЙС.ОС
- • Полный перечень установленных пакетов для аудита
- • Отсутствие «серых» бинарных артефактов

2. Воспроизводимость и детерминизм

Образы собираются с фиксированными параметрами архивации и одинаковой минимальной базой. При одинаковых входных данные совпадают бит-в-бит.

- • Фиксированные метки времени и сортировка при упаковке
- • Минимум слоёв — быстрый pull и предсказуемые diffs
- • Полезно для отладки, кэширования и доверенной сборки

3. Строгая безопасность по умолчанию

Поверхность атаки сокращается: лишние данные не попадают в образ, SUID/SGID-биты снимаются, логи и кэши очищаются. При желании включается non-root политика запусков.

- • `nodocs`, чистка кэшей и логов
- • Удаление SUID/SGID в rootfs
- • Опциональные профили запуска без root

4. Правильные метаданные и теги

Образы снабжаются OCI-лейблами и переменными окружения. Теги формируются из версий RPM — никакой рассинхронизации между пакетом и образом.

- • `org.opencontainers.image.*`: vendor, created, title, version, description
- • Схема имен: `niceos/<пакет>:<версия>` (+`latest` по политике)
- • Готово к каталогам образов и политикам допуска

5. Совместимость и универсальность

Процессы идентичны для Docker, Podman и nerdctl. Поддерживается работа как в открытом интернете, так и в полностью закрытых сегментах.

- • Единый pipeline для разных CLI
- • Air-gapped сборка и публикация
- • Интеграция с корпоративными реестрами

6. Готовность к комплаенсу

Экспорт SBOM, возможность криптографической подписи образов и аттестаций сборок. Поддержка отечественных алгоритмов шифрования.

- • SBOM (SPDX/CycloneDX) и список RPM в образе
- • Подписи и attestations для доверенной доставки
- • Поддержка ГОСТ-криптографии в экосистеме

Как мы готовим образы (в общих чертах)

1) Изоляция и установка из репозиториев НАЙС.ОС

Создаём изолированный *installroot*, устанавливаем минимальную базу и нужный пакет(ы) через менеджер пакетов. На выходе — чистая файловая система для упаковки без лишних слоёв и артефактов.

2) Минимизация, харденинг и упаковка

Очищаем кэши и логи, снимаем SUID/SGID-биты, контролируем метаданные архива. Упаковываем в единый слой — быстрые загрузки и предсказуемые диффы.

3) OCI-метаданные, теги и публикация

Проставляем лейблы `org.opencontainers.image.*`, формируем теги из версий RPM, генерируем SBOM и журналы сборки. Публикуем в корпоративные реестры или размещаем в изолированных контурах.

Итог: образы, которым можно доверять

Контейнерные образы НАЙС.ОС — это управляемая, воспроизводимая и безопасная основа для ваших приложений. Единая методика сборки и строгая дисциплина

метаданных дают предсказуемость на всех этапах — от разработки до эксплуатации.

- **Контроль происхождения** и проверяемость каждого файла.
- **Стабильность и повторяемость** релизов.
- **Готовность к комплаенсу** и требованиям ИБ.
- **Гибкость** для любых CICD и сред (от облаков до air-gapped).

Что дальше

1. Выберите базовый образ НАЙС.ОС или пакет под задачу.
2. Определите политику тегов и метаданных в вашем реестре.
3. Включите SBOM и подписи для усиления доверия.
4. Интегрируйте в ваш CI/CD — и масштабируйте без сюрпризов.