# ГОСТ-подпись и SBoM в НАЙС.ОС — доверие и прозрачность поставок

В НАЙС.ОС реализована целостная система доверия к программному обеспечению, включающая: ГОСТ-подпись всех RPM-пакетов с использованием GnuPG, который уже по умолчанию поддерживает алгоритмы ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012; Хранение SBoM (Software Bill of Materials) в формате SPDX JSON в репозитории, рядом с каждым пакетом; Автоматическая проверка уязвимостей (CVE) на основе NVD JSON 2.0 (NIST) и БДУ ФСТЭК. Пакетный менеджер tdnf при подключении к официальному зеркалу *.niceos.ru автоматически: Проверяет цифровую ГОСТ-подпись каждого RPM-файла перед установкой; Анализирует .sbom.json на предмет уязвимостей и лицензионной прозрачности; Предупреждает о CVE ещё до установки — в CLI или в графической оболочке. Это решение обеспечивает: Прозрачность происхождения каждого пакета и его состава; Воспроизводимость сборки на основе открытых данных; Безопасность поставки и соответствие требованиям нормативных документов.

## 1. Зачем это нужно: доверие к цепочке поставки

Современные ИТ-системы подвержены всё более изощрённым **supply-chain атакам** — внедрение уязвимого или вредоносного кода на этапе сборки, публикации или обновления. Самые громкие случаи:

- **SolarWinds (2020)** — внедрение бэкдора на этапе CI/CD;
- **xz-backdoor (2024)** — вредоносный код в системной библиотеке компрессии, распространявшийся через Linux-дистрибутивы.

В этих условиях особое значение приобретают механизмы доверия к поставляемому ПО:

- **Подписание пакетов** (в НАЙС.ОС — ГОСТ-подпись);
- **Software Bill of Materials (SBOM)** — документ, описывающий состав пакета и его зависимости;
- **Анализ CVE** по открытым базам (NVD JSON 2.0 и БДУ ФСТЭК);
- **Прослеживаемость** от исходников до бинарников.

Кроме того, **сертификационные требования ФСТЭК и Минцифры** обязывают обеспечить:

- ГОСТ-подписанный контент в доверенных хранилищах;
- контроль происхождения компонентов (вплоть до уровня SPDX);
- интеграцию CVE-мониторинга и аудит поставки.

В **НАЙС.ОС** всё это реализовано на системном уровне. Пользователь может:

- Проверить **кем собран пакет** и с какой версией исходников;
- Посмотреть **что входит в состав** через SBOM;
- Убедиться, что **пакет подписан ГОСТ-подписью** из доверенного ключа;
- Узнать, **есть ли уязвимости** (CVE) до установки или обновления.

## 2. Что такое ГОСТ-подпись и как она работает в НАЙС.ОС

В **НАЙС.ОС** каждый пакет проходит цифровую подпись на финальном этапе сборки. В отличие от классических схем с RSA, используется **отечественный ГОСТ-алгоритм** в соответствии с требованиями 63-ФЗ и ФСТЭК:

- **ГОСТ Р 34.10–2012** (эллиптическая подпись, 256 или 512 бит);
- **ГОСТ Р 34.11–2012** (Stribog — криптографический хеш).

Подпись выполняется в формате **Detached Signature** с помощью утилиты `gpg`, которая уже встроена в **НАЙС.ОС** с полной поддержкой ГОСТ. Это значит:

- Подписи хранятся отдельно — файл `package.rpm.sig` рядом с `package.rpm`;
- Или встраиваются в `repodata/repomd.xml.asc` — для проверки целостности всего репозитория;
- Проверка возможна как вручную через `rpm --checksig`, так и автоматически в `tdnf`.

**✒ Почему detached и зачем GPG, если есть rpmkeys?**

Классический `rpmkeys` не поддерживает ГОСТ. Использование **Detached-подписей**

**через GnuPG** позволяет:

- Использовать расширенные ГОСТ-алгоритмы через `libgcrypt`;
- Применять один и тот же ключ для подписей пакетов, ISO и SBoM;
- Проверять подписи в **CI, tdnf, rpm** и сторонних инструментах (например, через `gpgv`);
- Полностью контролировать формат, хеш и OID без привязки к внутренним структурам RPM.

Это также соответствует требованиям ФСТЭК к ГОСТ-подписям (профиль ТК-26).

## 3. Что такое SBoM и как он организован

**SBoM (Software Bill of Materials)** — это «инвентаризационная ведомость» программного пакета: она показывает, из каких компонентов он состоит, какие библиотеки использует, какие лицензии применяются, и даже какие уязвимости могут в нём присутствовать.

В **НАЙС.ОС** каждый пакет сопровождается машинно-читаемым **SBoM-документом** в формате SPDX (JSON). Этот файл:

- Автоматически генерируется при сборке пакета с помощью `rpm2spdx` или `syft`;
- Содержит полную информацию о бинарных/исходных зависимостях, лицензиях и хэшах;
- Хранится **рядом с RPM-пакетом** в репозитории, как файл `package.sbom.json`;
- Не устанавливается в систему, но доступен для анализа до инсталляции.

**🥓 Пример: как посмотреть зависимости пакета до установки**

Допустим, вы хотите понять, от чего зависит `nginx` перед установкой. Для этого:

1. Загрузите SBoM-файл: `wget https://repo.niceos.ru/x86_64/nginx-1.24.sbom.json`
2. Откройте его в любом JSON-редакторе или используйте `jq`:
3. `jq '.packages[] | {name: .name, license: .licenseConcluded}' nginx-1.24.sbom.json`

Вы получите список компонентов и лицензий. Это удобно для аудита и соответствия требованиям по открытому ПО.

## 4. Как всё это работает в `tdnf`

Пакетный менеджер `tdnf`, поставляемый с **НАЙС.ОС**, поддерживает расширенную проверку доверия при установке и обновлении пакетов из официальных репозиториев `*.niceos.ru`.

При каждом запросе `tdnf install / update` выполняется следующий цикл проверки:

- ✅ **Проверка цифровой подписи**: каждый RPM-файл проверяется с использованием **отсоединённой ГОСТ-подписи**, подписанной через GnuPG (ГОСТ Р 34.10–2012 + Stribog).
- 🎁 **Загрузка и верификация SBoM**: если для пакета имеется файл `.sbom.json` в формате SPDX, он автоматически загружается и проверяется на корректность.
- 🛡️ **Проверка безопасности**: компоненты из SBoM сопоставляются с базами CVE:
  - NVD JSON 2.0 — база CVE от NIST;
  - БДУ ФСТЭК — российский реестр уязвимостей.

Если найдено совпадение с известной уязвимостью, `tdnf` **предупредит пользователя до установки** — с указанием CVE-идентификатора, уровня опасности и ссылки на описание.

**🔍 Пример**

При установке библиотеки `libxml2` с известной CVE:

```
CVE-2024-12345 detected in libxml2 (critical)
Description: Use-after-free in xmlParseTryOrFinish
Source: NVD / БДУ
Install anyway? [y/N]
```

## 5. Что это даёт пользователю и администратору

Интеграция ГОСТ-подписи, SBoM и CVE-проверки в **НАЙС.ОС** даёт ощутимые преимущества как обычным пользователям, так и системным администраторам, работающим в критичных или регулируемых средах:

- ✅ **Гарантия подлинности:** каждый пакет проверяется на соответствие ГОСТ-подписи. Вы можете быть уверены, что файл действительно из официального репозитория `*.niceos.ru` и не был подменён на промежуточном этапе.

- 🔍 **Прозрачность состава:** SBoM-файлы позволяют проследить:
  - какие исходники использовались при сборке,
  - какие библиотеки входят в состав,
  - какие лицензии применимы — всё в одном JSON-документе формата SPDX.
- 🛡️ **Криптографическая достоверность:** используется строгое ГОСТ-подписание через GnuPG, что соответствует требованиям 63-ФЗ и ФСТЭК (профиль ТК-26). Это важно для организаций, проходящих сертификацию.
- 🚨 **Автоматическое предупреждение об уязвимостях:** CVE-анализ по базам NVD и БДУ выполняется до установки , что позволяет вовремя предотвратить внедрение уязвимого ПО — особенно актуально для серверов, шлюзов, УЦ и других компонентов КИИ.

Это означает, что установка пакета в НАЙС.ОС — это не просто «копирование файлов», а **процедура с гарантией происхождения, криптографической подлинности и безопасности содержимого** .

# 6. Для разработчиков и интеграторов

**НАЙС.ОС** предоставляет инструменты и практики, которые позволяют разработчикам и DevOps-инженерам создавать надёжные, воспроизводимые и прозрачные пакеты:

- 🔄 **Интеграция SBoM в CI:** при сборке пакета в CI-среде (например, GitHub Actions, GitLab CI, Jenkins) автоматически генерируется файл SBoM в формате `SPDX JSON` с помощью утилит `syft` или `rpm2spdx` . Он публикуется рядом с `.rpm` в репозитории.
- 🔐 **ГОСТ-подпись для стороннего ПО:** сторонние пакеты могут быть подписаны теми же инструментами (через `gpg --detach-sign` с ГОСТ-ключом), что и официальные. Это обеспечивает совместимость с `tdnf` и системой верификации НАЙС.ОС.
- 🌐 **Экосистема:** возможно размещение SBoM и detached-подписи в собственном зеркале или в репозитории проекта с соблюдением тех же требований, что и у официальных пакетов.

### 🥪 Рецепт reproducible и auditable пакета за 4 команды

```
# 1. Собираем пакет
rpmbuild -ba mypkg.spec

# 2. Генерируем SBoM
syft mypkg.rpm -o spdx-json > mypkg.sbom.json
```

```
# 3. Подписываем GPG (ГОСТ-ключ)
gpg --detach-sign --armor mypkg.rpm

# 4. Публикуем в репозиторий
cp mypkg.rpm mypkg.sbom.json mypkg.rpm.asc /var/www/html/repo/
```

Всё — ваш пакет прозрачен, воспроизводим и проверяем tdnf'ом из коробки.

## 7. Поддержка и автоматизация CVE-мониторинга

В **НАЙС.ОС** реализована встроенная система **автоматического анализа уязвимостей (CVE)** , основанная на машинно-читаемых базах данных и тесно интегрированная с механизмами SBoM.

- 📚 **Источники уязвимостей:**
  - **NVD JSON 2.0** — официальная база уязвимостей от NIST;
  - **БДУ ФСТЭК** — российский государственный реестр угроз безопасности.
- 🔎 **Идентификация по имени и версии пакета:** сопоставление идёт по модели `PackageName@Version` — данные берутся из `.sbom.json` , сгенерированного при сборке.
- ⚠️ **Встроенный анализатор** в tdnf сопоставляет зависимости с CVE и **выдаёт предупреждение до установки** , если уязвимость найдена. Это снижает риск установки уязвимого ПО.

Мониторинг CVE выполняется как для официальных пакетов, так и для любых сторонних, если они сопровождаются валидным SBoM.

Это особенно важно при развёртывании критической инфраструктуры, шлюзов, серверов в ИСПДн и системах с требованиями ФСТЭК.

## Заключение

**ГОСТ-подпись** и **SBoM** — это не просто формальности. Это базовые механизмы, на которых строится доверие к программному обеспечению и устойчивость всей экосистемы.

**НАЙС.ОС** реализует эти практики **из коробки** :

- Каждый RPM-файл подписан ГОСТ-ключом через GnuPG;
- Каждому пакету соответствует машинно-читаемый `.sbom.json` ;

- tdnf проверяет подпись, состав и уязвимости до установки.

Для разработчиков и DevOps-инженеров **поддержка этих механизмов не требует особых усилий** — все инструменты (подпись, генерация SPDX, CI-интеграция) доступны и стандартизированы.

Это решение — не только о **безопасности** , но и о **зрелости дистрибутива** : прозрачность, проверяемость, соответствие требованиям ФСТЭК и международной практики.

**НАЙС.ОС** даёт вам в руки верифицируемую и управляемую платформу — используйте её осознанно.