ООО «Базальт СПО»

Российский разработчик
операционных систем «Альт»

basealt.ru

Репозиторий: подходы к организации и метрики доверия

Костригин Николай Александрович

nickel@basealt.ru

Руководитель отдела безопасности разработки программного обеспечения

Репозиторий

Этимология

Слово «репозиторий» происходит от латинского repositorium («хранилище», «гробница»).

Оно образовано от глагола reponere — «класть обратно, возвращать, убирать», состоящего из приставки re- (обратно, снова) и глагола ponere (класть, ставить). В современный русский язык термин пришёл из английского языка (repository — склад, хранилище).

Разновидности репозиториев

Ключевые типы хранилищ в цикле разработки ПО

Реестры контейнеров

Хранение и распространение Docker-образов и других OCI-артефактов для развертывания.

Примеры

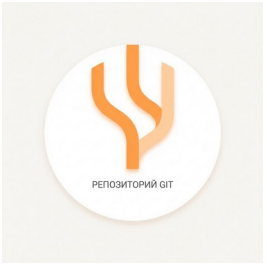
Docker Hub · GHCR · Harbor

Linux дистрибутивы

Коллекции бинарных пакетов (RPM, DEB) и исходных кодов для ОС.

Примеры

ALT Linux Sisyphus · RHEL · Fedora · Debian · Ubuntu

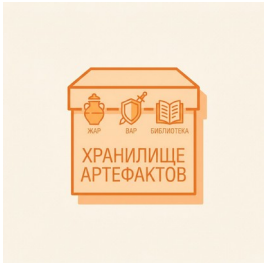


Git проекты

Системы контроля версий для исходного кода апстримных проектов и совместной разработки.

Примеры

GitHub · GitLab · Bitbucket



Хранилища артефактов

Управление зависимостями и собранными библиотеками (JAR, NPM, NuGet).

Примеры

Sonatype Nexus · JFrog Artifactory

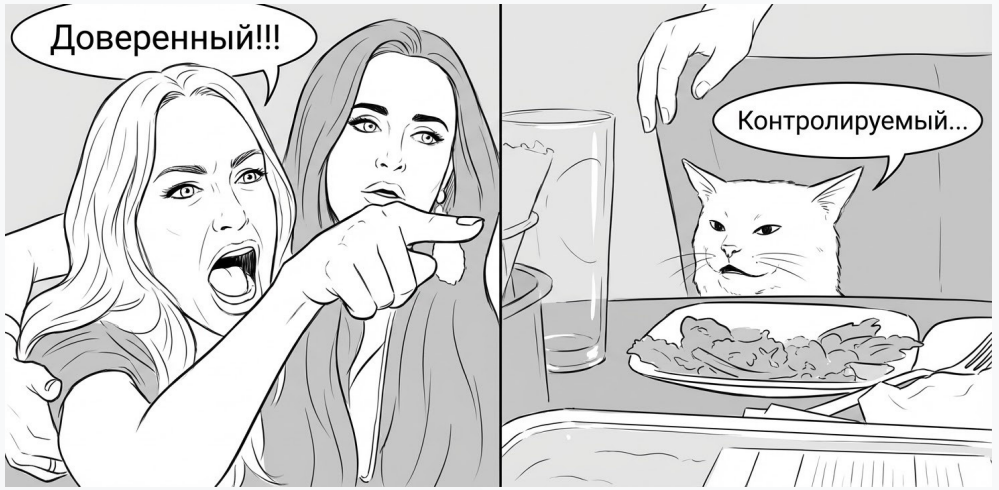
Сравнительный анализ типов репозиториев

Матрица ключевых характеристик для выбора стратегии управления и безопасности.

КРИТЕРИЙ	SOURCE CODE GIT, SVN	BINARY ARTIFACTS ARTIFACTORY, NEXUS	LINUX REPOS APT, YUM/DNF	CONTAINER DOCKER, OCI	LANGUAGE NPM, PYPI, MAVEN
Назначение	Версионирование кода, коллаборация, diffs	Хранение билдов, проксирование зависимостей	Дистрибуция системных пакетов ОС	Хранение и запуск образов приложений	Библиотеки и зависимости языка
Размер Объектов	KB - MB TEXT BASED	MB - GB BINARIES	MB PACKAGES	MB - GB LAYERS	KB - MB ARCHIVES
Безопасность	Commit Signing	Access Control	GPG & TUF	Scanning & Sign	Variable
Метаданные	History, Branches, Tags, Blame	Properties, Build Info, Layouts	Dependencies, Checksums, Signatures	Manifests, Configs, Layers, Labels	Versions, SemVer, Dependencies
Специализация	Разработка	Управление	Стабильность	Развертывание	Экосистема

Репозиторий в цепочке поставок

Уточним термины



Защита информации • Разработка безопасного программного обеспечения

Композиционный анализ программного обеспечения • Общие требования

3.1.9 контролируемый репозиторий:
репозиторий, в отношении содержимого которого выполняются проверки, направленные на повышение безопасности разрабатываемого ПО и предусмотренные регламентами и иными организационно-распорядительными документами организации.

Доверенный

Проверенный

Контролируемый

Безопасный

Метрики доверия: Crypto, TUF, SLSA, ScoreCard

Frameworks

NIST | OpenSSF

Crypto Verification

Базовая проверка целостности и авторства артефакта.

Чем подтверждается

- Хеши (SHA-256) в метаданных и lock-файлах
- Цифровые подписи (GPG, Cosign)
- Цепочка доверия сертификатов (PKI)

Где внедряется

Repository (Storage) | CI Pipeline | Registry Proxy

TUF

The Update Framework. Защита процесса доставки обновлений.

Чем подтверждается

- Разделение ролей (Root, Targets, Snapshot, Timestamp)
- Сроки действия метаданных (TTL) против freeze-атак
- Пороговые подписи (Quorum) для критичных операций

Где внедряется

Update Server | Repository Meta

SLSA

Supply-chain Levels for Software Artifacts. Зрелость сборки.

Чем подтверждается

- Уровни зрелости (L1–L3)
- Provenance (происхождение): кто, где, как и из чего собрал
- Герметичность и воспроизводимость сборки

Где внедряется

Build System (CI) | Attestation Store | Admission Controller

Как это работает вместе?

Crypto гарантирует целостность файла. **TUF** гарантирует, что вам не подсунули старую или "злую" версию репозитория. **SLSA** доказывает, что файл был собран доверенной CI-системой из правильного исходного кода.

OpenSSF ScoreCard

OpenSSF Scorecard — оценка репозитория

OpenSSF Scorecard оценивает зрелость практик разработки, а не безопасность кода.

Ключевые параметры:

Code Review и Branch Protection
CI и безопасность GitHub Actions
Подписи коммитов и релизов
Управление зависимостями (pinned versions)
Security policy, лицензия, активность проекта

Результат:
агрегированный score 0–10 (взвешенные проверки)

Независимая разработка

Проект «Сизиф»:

- Все продукты Базальт СПО, включая сертифицированную версию ОС — Альт СП, построены на пакетной базе стабильных ветвей репозитория Сизиф.
- Сизиф один из независимых репозиториев Свободного ПО, вбирает в себя пакеты, разрабатываемые мировым сообществом.
- Основой проекта Сизиф является ALT Linux Team, а поддержку инфраструктуры репозитория обеспечивает ООО «Базальт СПО»
- Многие сотрудники компании являются членам ALT Linux Team

Анализ практик сборки и контроля Sisyphus

01

Политики приёма

Submission tasks

Подача пакетов через систему заданий girar.

Ревью кода

Ручная проверка изменений мейнтейнерами.

02

Воспроизводимые сборки

Изоляция hasher

Сборка в чистом chroot окружении.

Детерминизм

Фиксированные зависимости для повторяемости.

03

Автоматизация процессов

girar-driven CI

Оркестрация интеграции системой girar.

Builder robots

Автоматическое выполнение рутинных операций.

04

Версионирование и хранение

Исходники

git.altlinux.org

Бинарные пакеты

Ftp.altlinux.org; packages.altlinux.org

Трекинг

Bugzilla

Оценка зрелости по метрикам доверия (сторонний наблюдатель, OSINT)

Level 1	Level 2 (Текущий уровень)	Level 3	Level 4	Level 5
Ad-hoc	**Defined (Build L1-L2)**	Automated	Measured	Optimized

Сильные стороны

Изоляция (hasher)
Чистые clean chroot окружения сборки

Автоматизация (girar)
Централизованная сборка роботами

Прозрачный git-workflow
Публичный доступ к истории изменений

Области для улучшения

SBOM-generation
Нестандартизированная генерация SBOM

Provenance-attestations
Отсутствие in-toto аттестаций процессов

Подпись Sigstore/Cosign
Внедрение современных механизмов подписи

Целевые KPIs (Target Metrics)

≥ 80%	≥ 75%	100%	≤ 14дн
пакетов с SBOM	верифицировано	подписано	MTTR Critical CVE

Видимое и скрытое: айсберг SLSA

Баланс между публичной прозрачностью и внутренней безопасностью

Sisyphus Repo

git.alt workflow

Bugzilla Tracker

ПУБЛИЧНЫЙ УРОВЕНЬ (VISIBLE)

Очевидные для внешнего наблюдателя практики (SLSA L1–L2)

SLSA Build L1-L2

ВНУТРЕННИЙ КОНТУР (HIL

Глубинные процессы безопасности (L3)

Dependency Graph

Vuln Management

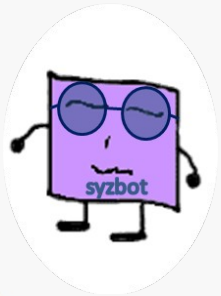
Стратегия прозрачности

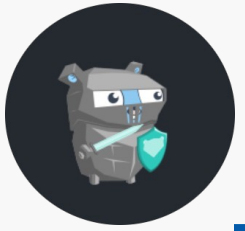
Команда ALT Linux Team работает над публикацией скрытых метрик (SBOM, provenance) во внешний контур там, где это не снижает безопасность инфраструктуры.

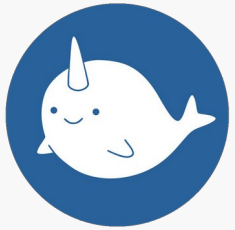
Internal SBOM

Security Ops & L3

Особенности при проведении РБПО-исследований







ИСП РАН

- SnapFuzz
- Hopper
- Nyx
- Go-Fuzz
- AFL++
- LibFuzzer
- Clang Static Analyzer
- Cppcheck
- Clippy
- Svace
- Sydr-fuzz
- Syzkaller
- jazzer

Большое число объектов исследования (>30);
Большое число языков программирования, на которых они написаны;
Необходим большой ассортимент инструментов (>10).

Спасибо за внимание!

OpenSSF

Стандарты безопасности цепочки поставок, гайды и инструменты (Scorecard, Sigstore, SLSA).

openssf.org

ALT Linux Sisyphus

Официальный портал репозитория Сизиф: поиск пакетов, статистика сборок и документация.

packages.altlinux.org

ALT Linux Space

Место для обсуждения, разработки и развития свободных проектов сообщества.

altlinux.space