Deckhouse Stronghold

Реализация поддержки шифрования ГОСТ в Deckhouse Stronghold

Безопасное управление жизненным циклом секретов

Для чего необходимо шифрование ГОСТ

Использование шифрования ГОСТ актуально для российских компаний и государственных организаций, работающих в таких сферах, как:

- топливно-энергетический комплекс
- государственный сектор
- финансовый сектор, банки
- здравоохранение
- связь
- оборонная и ракетно-космическая промышленность

Направления реализации шифрования ГОСТ в Deckhouse Stronghold

В Deckhouse Stronghold поддержка ГОСТ-шифрования реализуется по четырём ключевым направлениям.

Seal wrap

Доступно

Двойное шифрование с использованием комбинации криптоалгоритмов (AES + ГОСТ) при сохранении данных с использованием криптопровайдера или аппаратных модулей безопасности (HSM). В данном случае Deckhouse Stronghold не реализует алгоритмы ГОСТ самостоятельно, а делегирует их внешнему криптопровайдеру: шифрование и расшифровка данных происходят при помощи wrap/unwrap-операций через CSP (например, КриптоПро CSP) или HSM (например, Рутокен ЭЦП 3.0).

TLS

Доступно

Обеспечивает зашифрованный обмен данными между сервером и клиентом.
На данный момент в Deckhouse Stronghold используется встроенный TLS-стек на Go.

PKI с поддержкой ГОСТ

В процессе реализации

Обеспечивает зашифрованный обмен данными между сервером и клиентом.
На данный момент в Deckhouse Stronghold используется встроенный TLS-стек на Go.

Transit secrets engine с поддержкой ГОСТ

В процессе реализации

Позволит пользователям выполнять операции шифрования данных с применением криптоалгоритма ГОСТ по запросу.

Все четыре направления могут быть реализованы с использованием криптопровайдера (например, КриптоПро CSP) или с помощью HSM для вызова библиотеки внешнего вендора (например, Рутокен ЭЦП 3.0).

Дорожная карта реализации поддержки шифрования ГОСТ в Deckhouse Stronghold

Январь – апрель 2025	▪ Поддержка шифрования root-ключа с помощью внешнего HSM (AES, RSA) ▪ Поддержка ГОСТ-шифрования root-ключа с помощью внешнего HSM (Рутокен ЭЦП 3.0)
Май 2025	▪ Выбор решения для реализации шифрования ГОСТ с помощью криптопровайдера
Июнь 2025	▪ Разработка архитектуры решения с учётом требований по интеграции КриптоПро CSP
Июль 2025	▪ Реализация MVP-версии Deckhouse Stronghold с поддержкой КриптоПро CSP
Август 2025	▪ PoC интеграции Deckhouse Stronghold с КриптоПро CSP ▪ Поддержка шифрования ГОСТ методом seal wrap с помощью Рутокен ЭЦП 3.0
Сентябрь 2025	▪ Реализация интеграции Deckhouse Stronghold с КриптоПро CSP ▪ Поддержка шифрования ГОСТ методом seal wrap с помощью КриптоПро CSP
Октябрь 2025	▪ Поддержка ГОСТ-шифрования с помощью TLS 1.3 ▪ Подтверждение технологической совместимости с Рутокен ЭЦП 3.0
Ноябрь – декабрь 2025 Мы находимся здесь	▪ **Релиз Deckhouse Stronghold Enterprise Edition 1.17 с поддержкой ГОСТ (Крипто Про CSP, TLS)** ▪ **Релиз Deckhouse Stronghold Certified Security Edition 1.16 (сертифицированная ФСТЭК России редакция) с поддержкой Рутокен ЭЦП 3.0**
H1'2026	▪ Реализация Transit secrets engine с поддержкой ГОСТ ▪ Релиз Deckhouse Stronghold Certified Security Edition 1.17 с поддержкой ГОСТ (КриптоПро CSP, TLS)
H2'2026	▪ Реализация PKI с поддержкой ГОСТ

Дальнейшие планы

После реализации всех четырёх направлений — seal wrap, TLS, PKI и Transit с поддержкой ГОСТ — мы планируем провести оценку влияния среды функционирования в соответствии с требованиями ПКЗ-2005. Эта процедура направлена на проверку того, как компоненты встроенного средства криптографической защиты информации (СКЗИ) взаимодействуют с компонентами Deckhouse Stronghold.

По результатам оценки влияния мы планируем получить заключение ФСБ России о признании данного решения соответствующим требованиям по эксплуатации СКЗИ.

Нормативная база

Использование криптографических средств защиты является обязательным
при создании систем защиты информации в соответствии с такими нормативными документами, как:

- Приказ ФСБ России от 18 марта 2025 года № 117;
- Приказ ФСБ России от 10 июля 2014 года № 378;
- Приказ ФСБ России от 9 февраля 2005 года № 66.

Приказ ФСБ России от 18 марта 2025 года № 117

Краткий обзор

Приказ устанавливает обновлённые и расширенные требования к защите информации в государственных и смежных информационных системах с обязательным использованием СКЗИ.

Документ предписывает, что информация, передающаяся через коммуникационные каналы, системы внешнего доступа, хранимая в системах, должна быть защищена СКЗИ.

Сферы регулирования

- Государственные информационные системы (ГИС)
- Иные информационные системы государственных органов, унитарных предприятий и учреждений (за исключением систем, обрабатывающих госсекреты, и ряда высших органов)

Приказ ФСБ России от 10 июля 2014 года № 378

Краткий обзор

Этот приказ детализирует организационные и технические меры, которые обязаны применять операторы персональных данных в ИСПДн, особенно когда используются СКЗИ, чтобы соответствовать требованиям защиты данных, установленным Правительством РФ.

Меры группируются по уровням защищённости, и для каждого уровня (1, 2, 3, 4-й) определяются обязательные меры: от простых до наиболее строгих.

В приложении к приказу перечислен состав мер, включая требования к управлению ключами, шифрованию, аудитам и защите каналов связи, контроль доступа и др.

Сферы регулирования

- Операторы персональных данных

Приказ ФСБ России от 9 февраля 2005 года № 66

Краткий обзор

Этот приказ утверждает Положение ПКЗ-2005, которое определяет базовый нормативно-правовой каркас для создания, производства, реализации и эксплуатации СКЗИ с ограниченным доступом, не содержащих сведений, составляющих государственную тайну.

ПКЗ-2005 также устанавливает требования к оценке соответствия, сертификации, контролю безопасности, защите ключей, методам испытаний и процедурам безопасности при эксплуатации СКЗИ.

Рекомендации по стандартизации Р 1323565.1.020-2020 (TLS 1.2) и Р 1323565.1.030-2020 (TLS 1.3)

Краткий обзор

Документы содержат рекомендации, призванные формализовать и регламентировать использование криптографических алгоритмов в TLS 1.2 и TLS 1.3.

Для кого актуально

- Государственный сектор
- Финансовый сектор
- Субъекты КИИ
- Все, кто строит цифровые платформы, взаимодействующие с ГИС