

# Инструменты безопасности в Deckhouse Kubernetes Platform

Онлайн-курс | 6 дней

## Аудитория курса

- DevOps-инженеры
- Системные инженеры Kubernetes
- Инженеры по безопасности (Security Engineer) / специалисты по информационной безопасности

## Цели курса

- Получить знания о принципах работы и применении инструментов безопасности в Deckhouse Kubernetes Platform (DKP)
- Приобрести базовые навыки для администрирования и эксплуатации инструментов безопасности в DKP

## Требования к участникам

- Знать Linux на уровне пользователя
- Знать основные понятия и сущности Kubernetes (pod, deployment, service, ingress)
- Уметь работать с утилитой kubectl

## Формат

- Курс состоит из теоретического материала (вводной видеолекции и онлайн-вебинаров с демонстрацией работы в кластере) и практической части с выполнением лабораторных работ на учебном стенде



# План работы

## Инструменты безопасности в Deckhouse Kubernetes Platform

| Тема                                                                               | Структура                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Основы информационной безопасности в Kubernetes и Deckhouse Kubernetes Platform | <p><b>Цель:</b> получить знания об основах безопасности в Kubernetes и DKP, а также о концепции Zero Trust в информационной безопасности.</p> <p><b>Теория:</b></p> <ul style="list-style-type: none"><li>• Стандарты безопасности и модель 4C</li><li>• Процесс обеспечения информационной безопасности (ИБ) информационной системы; модели ИБ</li><li>• Zero Trust для Kubernetes и DKP</li><li>• Проекты, направленные на безопасность Kubernetes</li><li>• Нейтрализация рисков при использовании контейнеризации в DKP</li><li>• Аспекты безопасности кластера DKP на основе модели Zero Trust</li></ul> <p><b>Практика:</b> тестирование по теме.</p>                                                                                                    |
| 2. Безопасность пода                                                               | <p><b>Цель:</b> научиться создавать и применять политики безопасности для подов, а также управлять Admission controllers для ограничения ресурсов в объектах кластера.</p> <p><b>Теория:</b></p> <ul style="list-style-type: none"><li>• Pod Security Standards</li><li>• Параметры безопасности пода (Security Context)</li><li>• Концепция Admission controllers</li><li>• Возможности модуля admission-policy-engine DKP: расширение стандартных политик, операционные и собственные политики</li><li>• Admission controllers: ResourceQuota, LimitRange, PodNodeSelector</li></ul> <p><b>Практика:</b> работа со стандартными политиками безопасности пода, создание собственного ограничения и операционной политики, работа с Admission controllers.</p> |
| 3. Сетевые политики безопасности. Mutual TLS                                       | <p><b>Цель:</b> научиться создавать и применять сетевые политики для пространств имён и других объектов кластера, создавать и применять взаимную достоверную аутентификацию сервисов, а также шифрование сетевого трафика кластера.</p> <p><b>Теория:</b></p> <ul style="list-style-type: none"><li>• CNI, Cilium</li><li>• Network Policy, CiliumNetworkPolicy</li><li>• Примеры сетевых политик</li><li>• mTLS на основе Istio</li><li>• Политики авторизации в Istio</li></ul> <p><b>Практика:</b> создание сетевых политик для различных объектов кластера, шифрование сетевого трафика кластера, создание политик авторизации Istio.</p>                                                                                                                  |
| 4. Управление доступом                                                             | <p><b>Цель:</b> научиться создавать и применять аутентификаторы для доступа в DKP, а также распределять на них права доступа.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

---

**Теория:**

- Аутентификация в кластере DKP: сертификаты X.509, ServiceAccount, OIDC-провайдеры, модуль user-authn DKP
- Текущая ролевая модель
- Экспериментальная ролевая модель

**Практика:** создание пользователя и группы пользователей, защита приложения с помощью DexAuthenticator, применение ролей из различных моделей.

---

## 5. Управление сертификатами и хранение секретов

**Цель:** научиться создавать и применять системы для управления цифровыми сертификатами и хранения секретов в DKP, а также доставлять различные секреты в приложения.

**Теория:**

- Модуль cert-manager DKP
- Deckhouse Stronghold: функциональные характеристики, сферы применения и работа с секретами
- Доставка секретов в приложения
- Механизм секретов PKI
- Механизм для работы с SSH-ключами

**Практика:** работа с сертификатами в DKP, доставка секретов в приложения с помощью Deckhouse Stronghold.

---

## 6. Выявление уязвимостей и аудит безопасности в кластере

**Цель:** научиться проверять пользовательские образы в runtime на известные уязвимости, искать угрозы безопасности в кластере, а также реализовывать правила аудита.

**Теория:**

- Недоверенные репозитории и подмена образов
- Сканирование образов: модуль operator-trivy DKP
- Проверка соответствия кластера требованиям безопасности
- Аудит Kubernetes API
- Модуль runtime-audit-engine DKP. Falco

**Практика:** выявление уязвимостей в подах, защита от уязвимых образов, настройка политики аудита API-сервера и правил аудита Falco.