Yandex Cloud

Что проще: безопасная разработка в публичном или приватном облаке

Рами Мулейс,
менеджер группы продуктовой архитектуры
Security & Compliance

Обсудим

1. Преимущества публичного облака
2. Безопасная конфигурация окружения
3. Безопасное приложение и среда разработки
4. Безопасная инфраструктура

Пример приватного облака

Персонал,
аутсорсеры

Приложение

Средства защиты

Наложенные
Самописные инструменты

Базы данных


PostgreSQL


MySQL


MongoDB

CI/CD-система


Jenkins Status


GitLab

K8s


Kubernetes

Портал управления ВМ,
или самописная платформа

Слой виртуализации

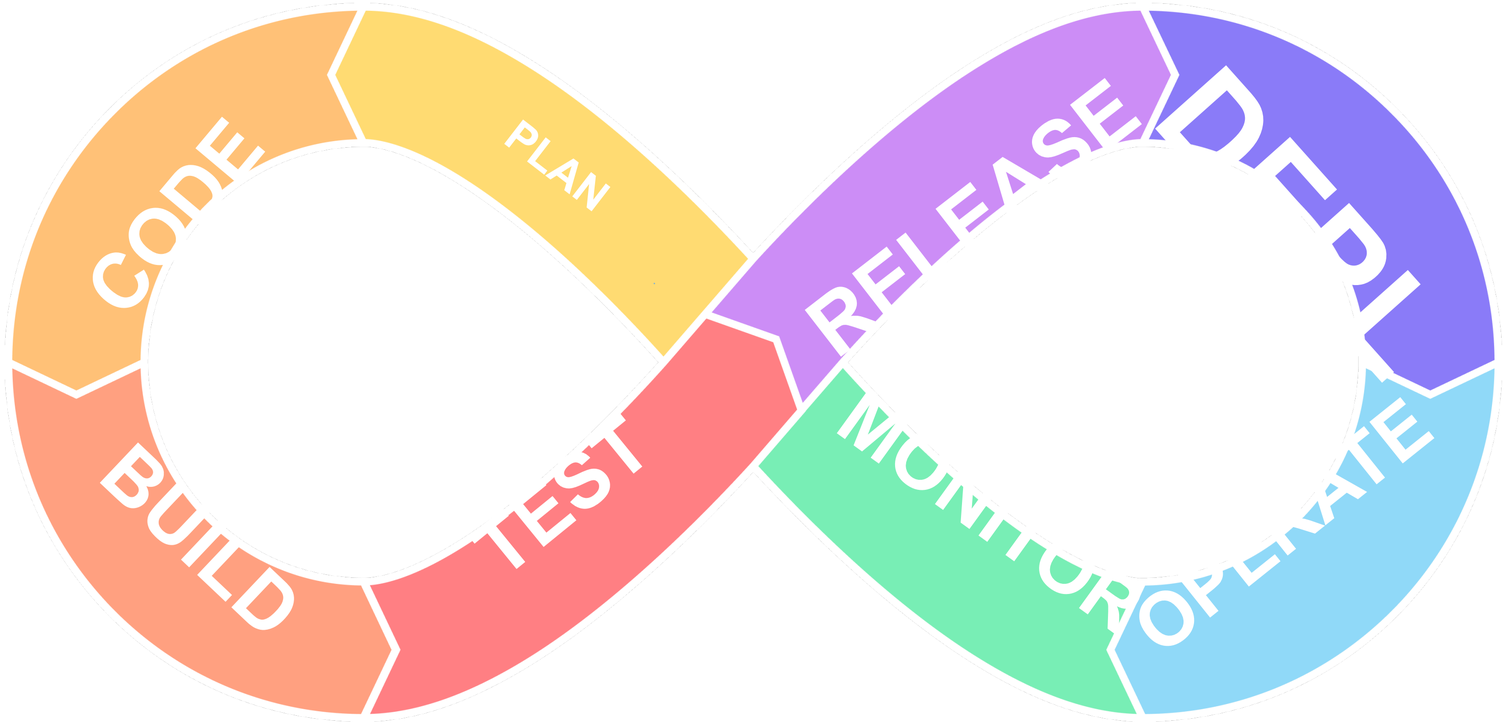

VMware


Openstack


Hyper-V

Физический слой: помещение,
серверы, стойки

CI/CD



Managed Service for GitLab

Container Registry

Load Testing

Monitoring

Cloud Logging

Tracker

Managed Service for Elasticsearch

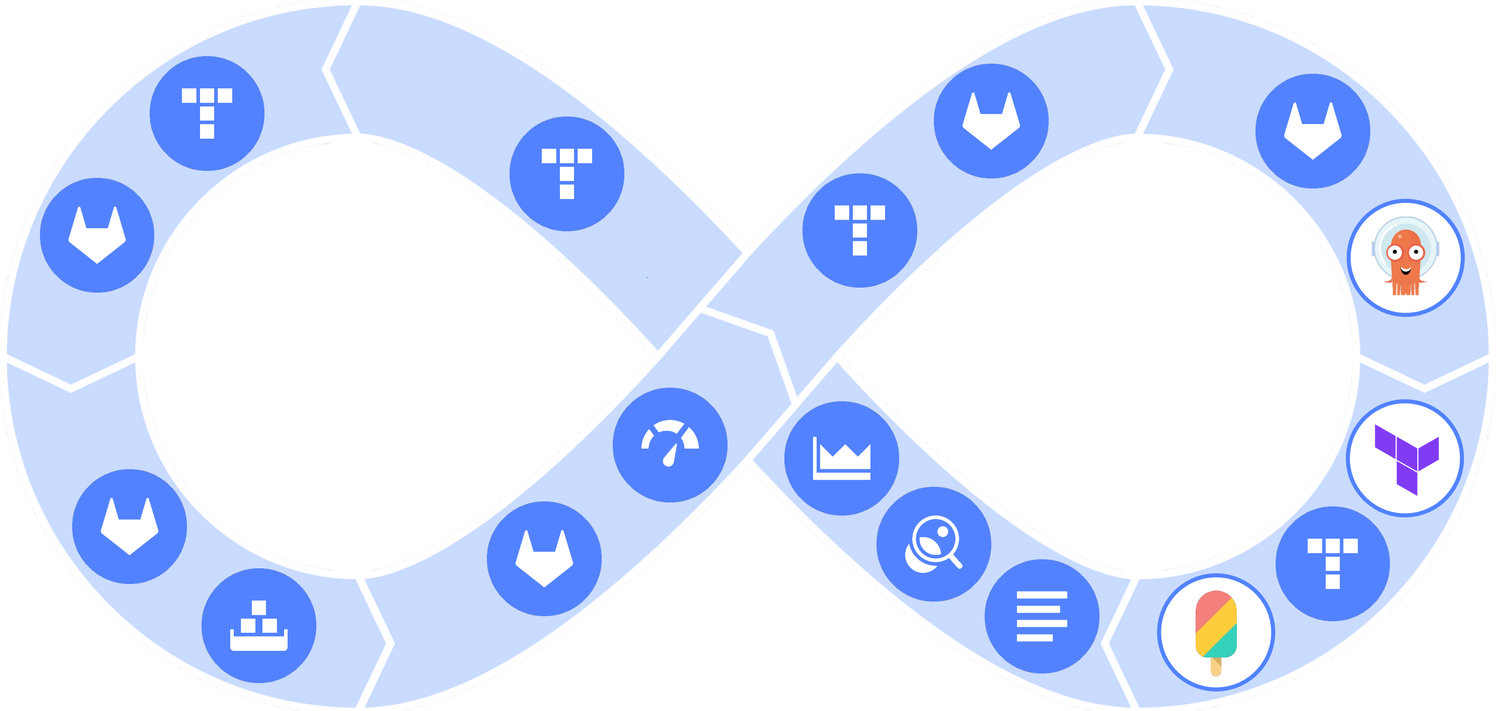
Argo CD

Terraform

Crossplane

Образы в Yandex Cloud Marketplace

CI/CD



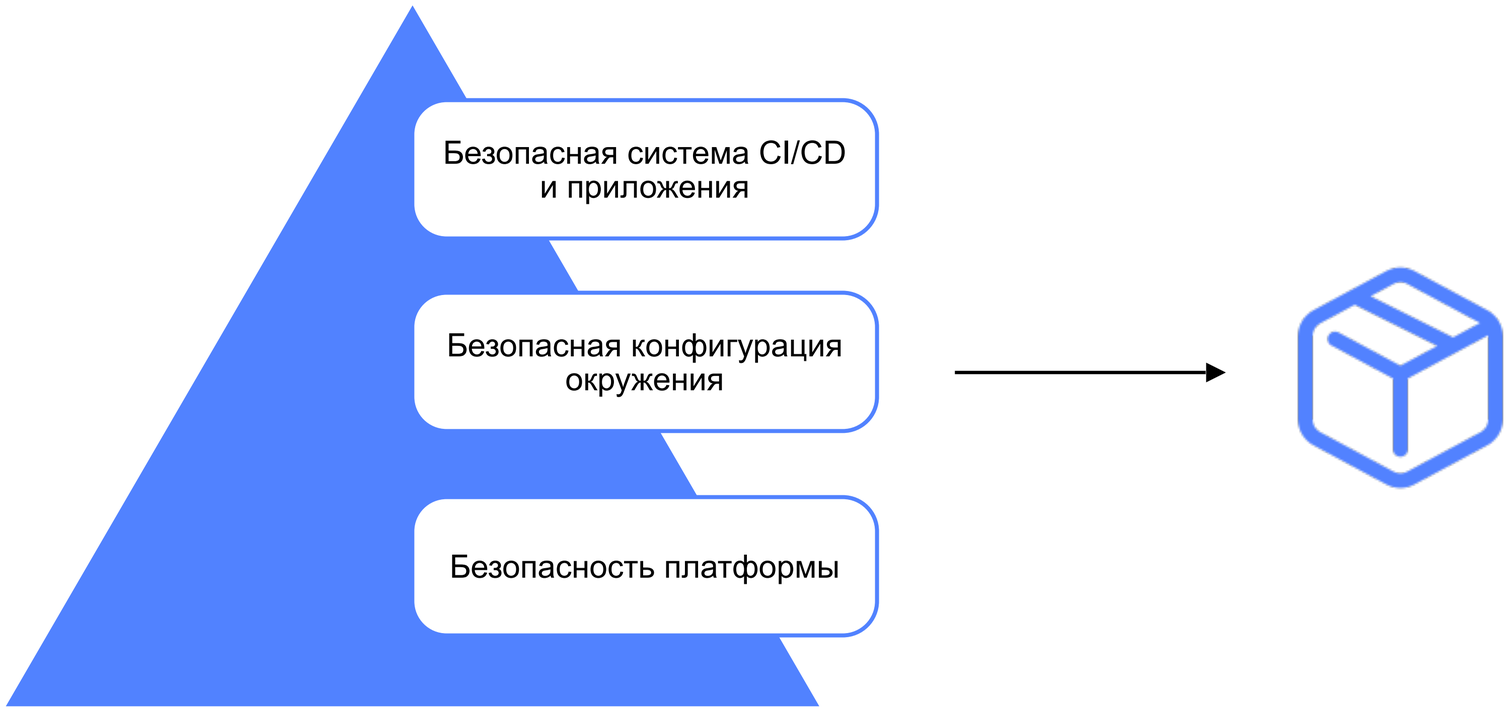
Топ-риски в публичных облаках

Успешная атака на уязвимое приложение клиента
Утечка секретов в публичное пространство

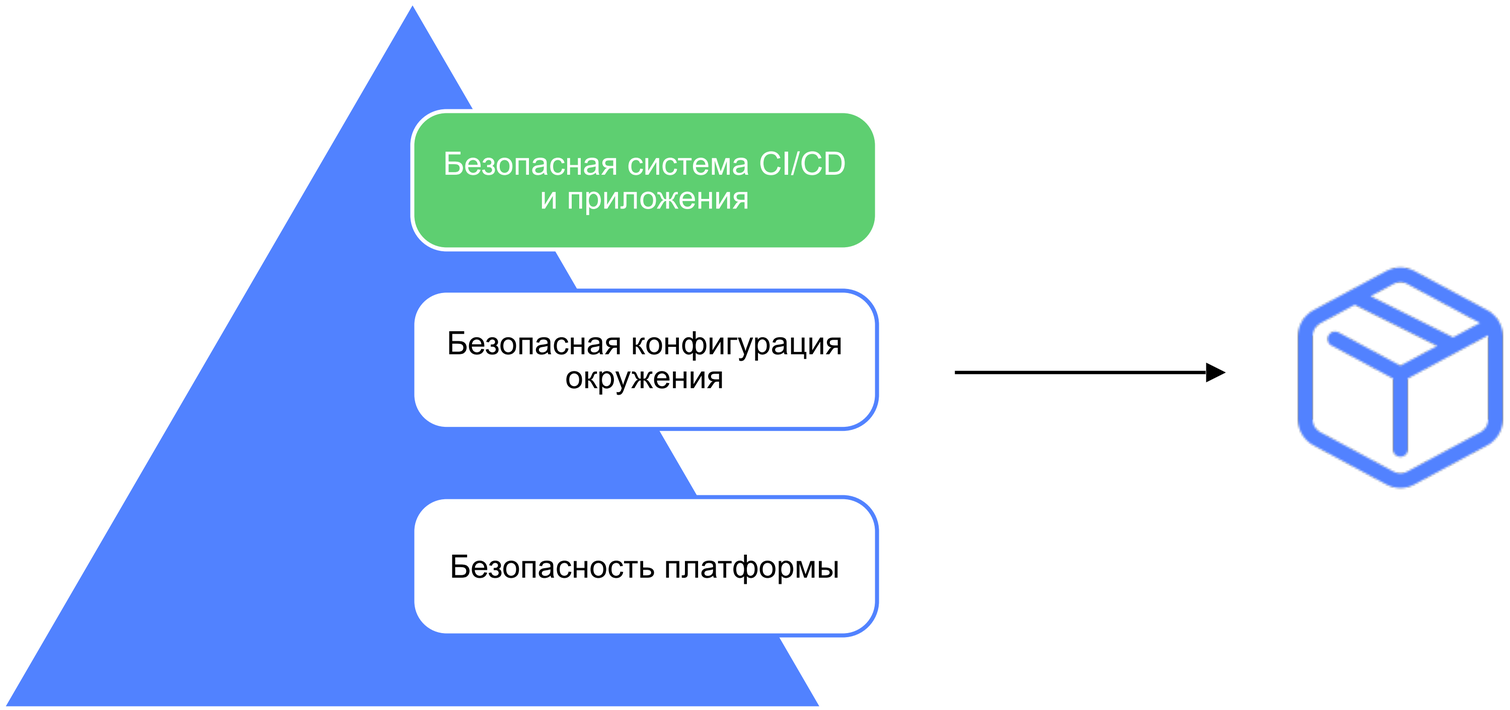
Неавторизованный доступ к объектам:
публичный доступ к S3, MDB и др.

Требования регуляторов и штрафы за несоблюдение требований

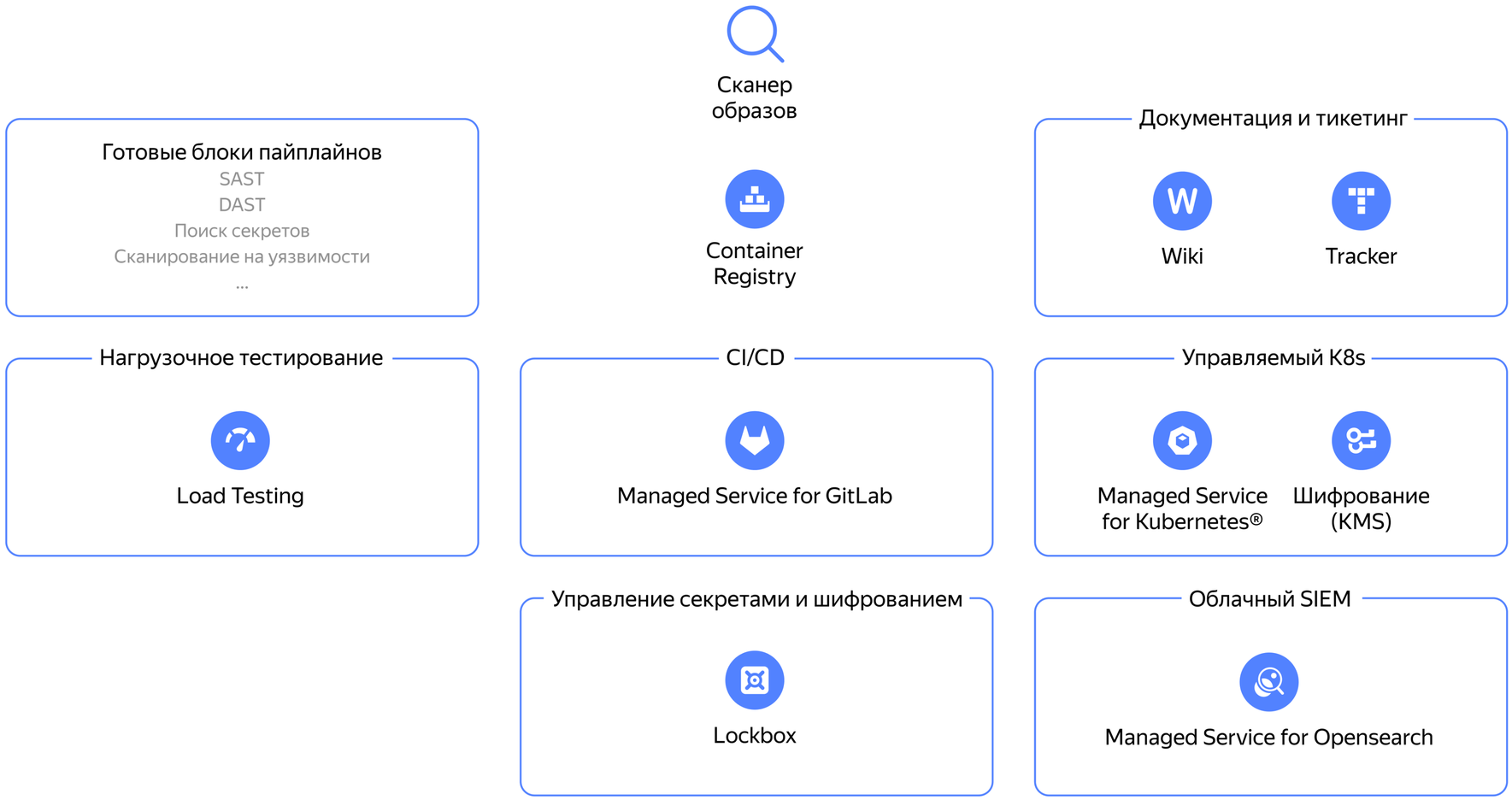
Готовые блоки безопасной разработки «из коробки»



Готовые блоки безопасной разработки «из коробки»

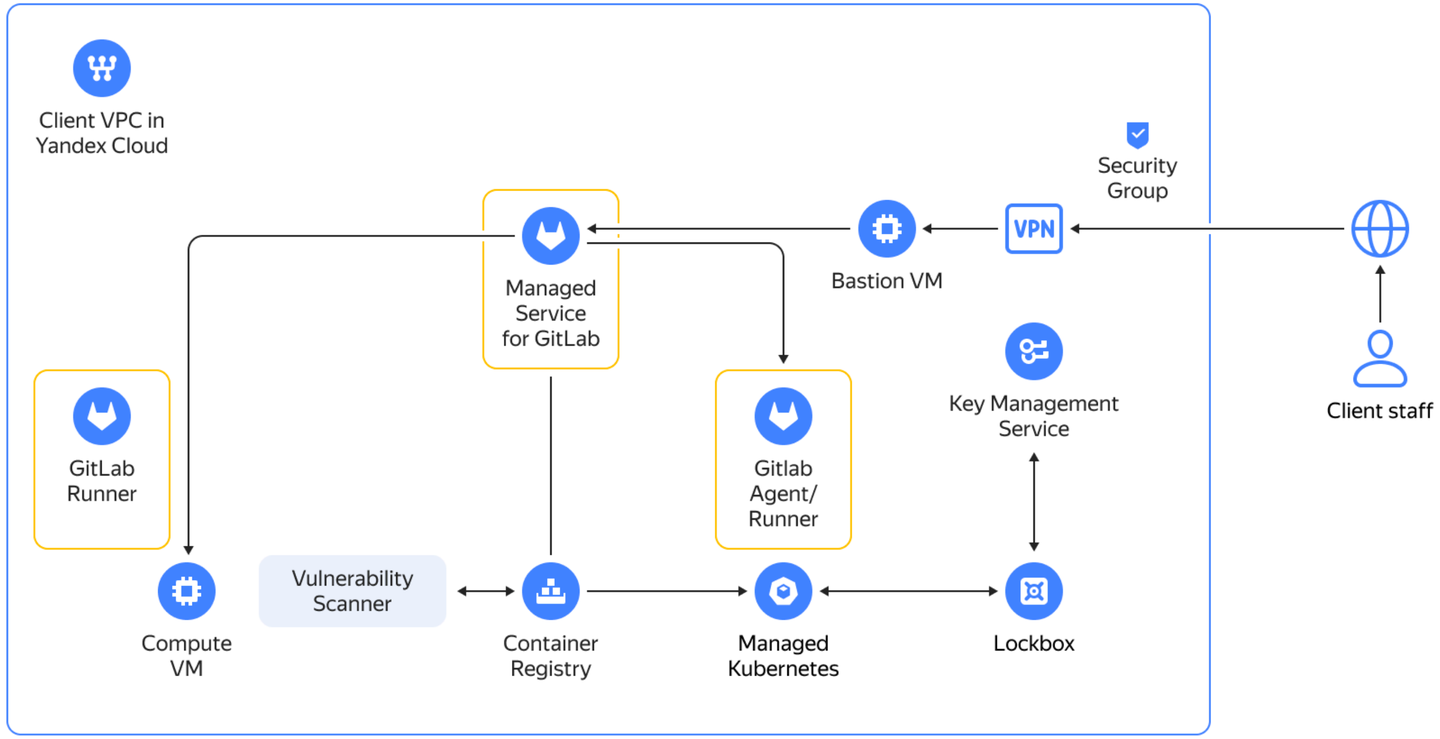


Безопасный CI/CD и приложения



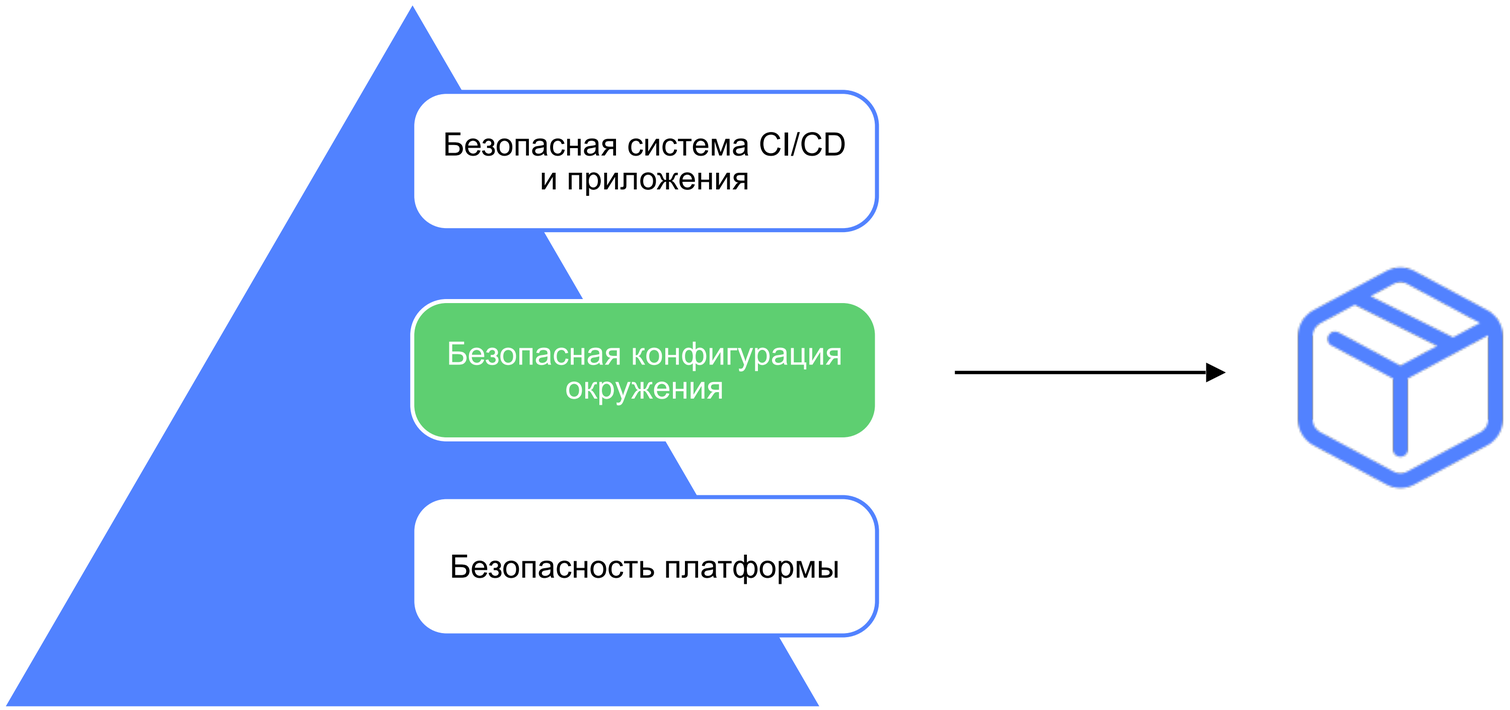
Безопасная разработка

- Безопасная инсталляция
- Автоматическое резервное копирование
- Полностью управляемый сервис
- Встроенные механизмы построения DevSecOps



github.com/yandex-cloud/yc-solution-library-for-security/tree/master/secure_ci_cd/secure_ci_cd_with_webinar

Безопасная конфигурация окружения



Безопасная конфигурация окружения — публичное облако

Инструменты безопасности Yandex Cloud

Cloud Native Сервисы

Identity and Access Management
Идентификация, контроль доступа к ресурсам

Certificate Manager
Управление TLS-сертификатами

Lockbox
Создание и хранение секретов

DDoS Protection
Защита от DDoS-атак

Key Management Service
Управление ключами шифрования

SmartCaptcha
Инструмент верификации запросов

Container Registry Vulnerability Scanner
Поиск уязвимостей в docker-образах

Audit Trails Preview
Сервис сбора и выгрузки аудитных логов

Возможности платформы

- Service Roles
- Bucket Policy
- Security Groups
- Object Storage Encryption with KMS Keys
- SAML Federations
- Automated Backups in MDB
- Container Registry Vulnerability Scanner

Security Solution Library

Библиотека готовых решений на GitHub

Подробнее

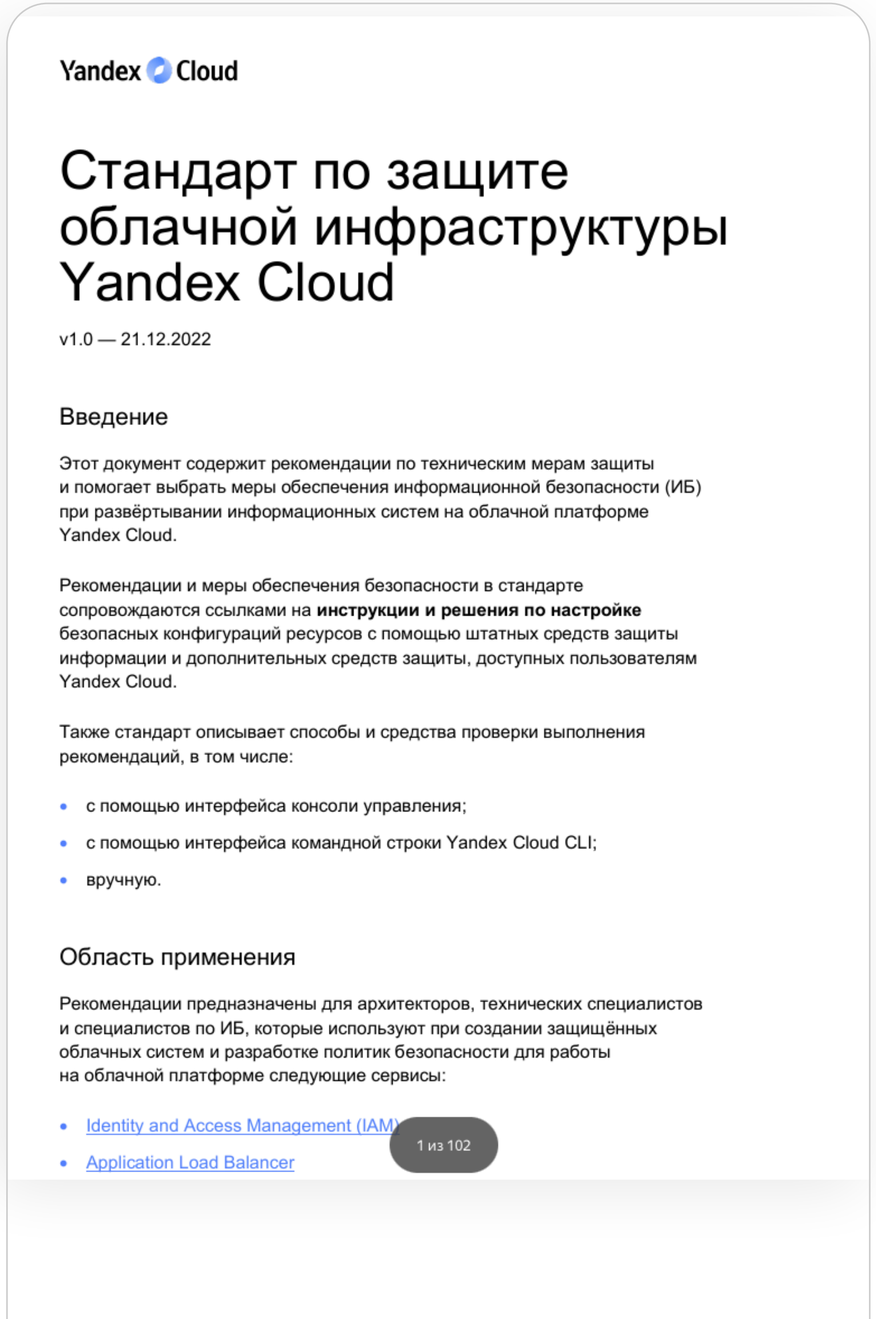
Yandex Cloud Marketplace

Все решения на сайте

Стандарт по защите облачной инфраструктуры Yandex Cloud 1.0

- Основан на практическом опыте и на наших гайдах
- Инструмент для аудита контролей безопасности в облаке
- Учитывает основные риски, связанные с облаком
- Можно автоматизировать

clck.ru/33Yyyj



Yandex Cloud

Стандарт по защите облачной инфраструктуры Yandex Cloud

v1.0 — 21.12.2022

Введение

Этот документ содержит рекомендации по техническим мерам защиты и помогает выбрать меры обеспечения информационной безопасности (ИБ) при развёртывании информационных систем на облачной платформе Yandex Cloud.

Рекомендации и меры обеспечения безопасности в стандарте сопровождаются ссылками на **инструкции и решения по настройке** безопасных конфигураций ресурсов с помощью штатных средств защиты информации и дополнительных средств защиты, доступных пользователям Yandex Cloud.

Также стандарт описывает способы и средства проверки выполнения рекомендаций, в том числе:

- с помощью интерфейса консоли управления;
- с помощью интерфейса командной строки Yandex Cloud CLI;
- вручную.

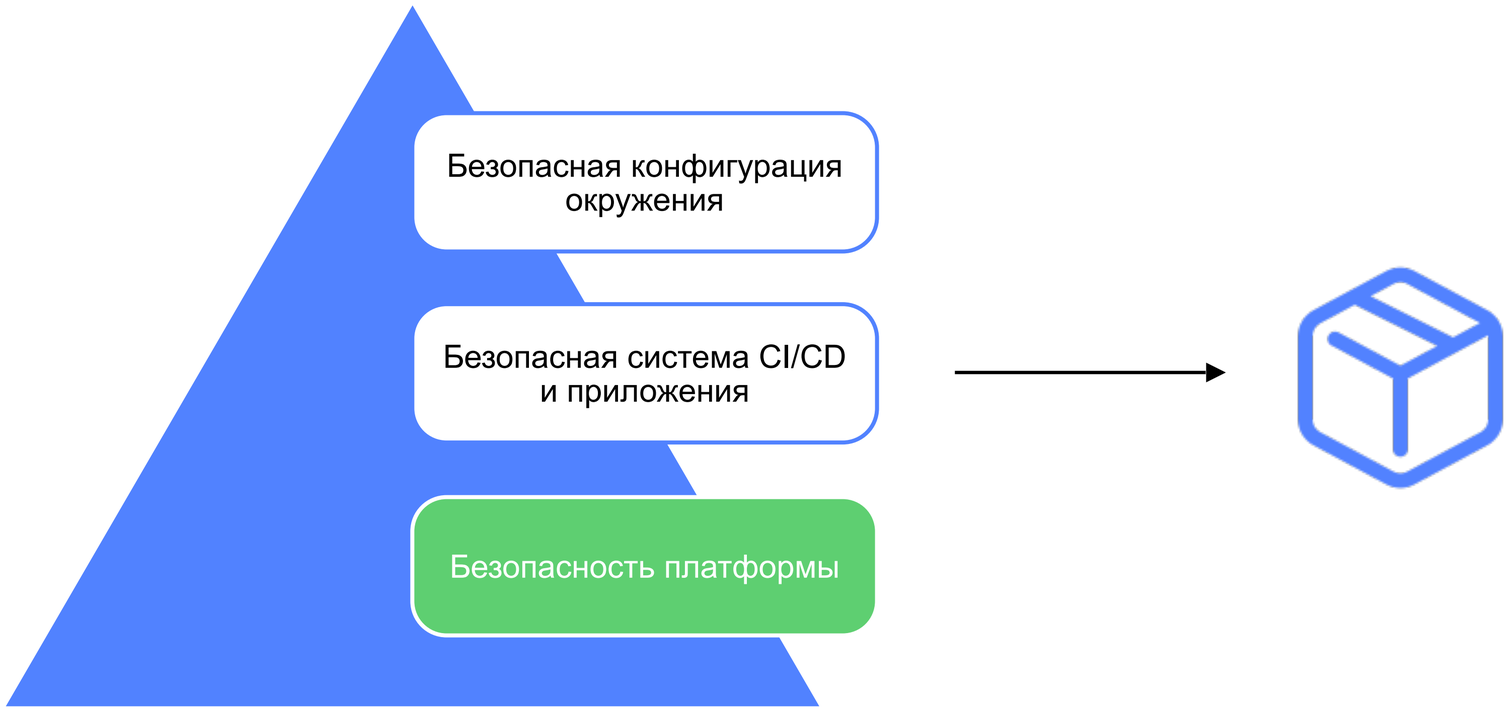
Область применения

Рекомендации предназначены для архитекторов, технических специалистов и специалистов по ИБ, которые используют при создании защищённых облачных систем и разработке политик безопасности для работы на облачной платформе следующие сервисы:

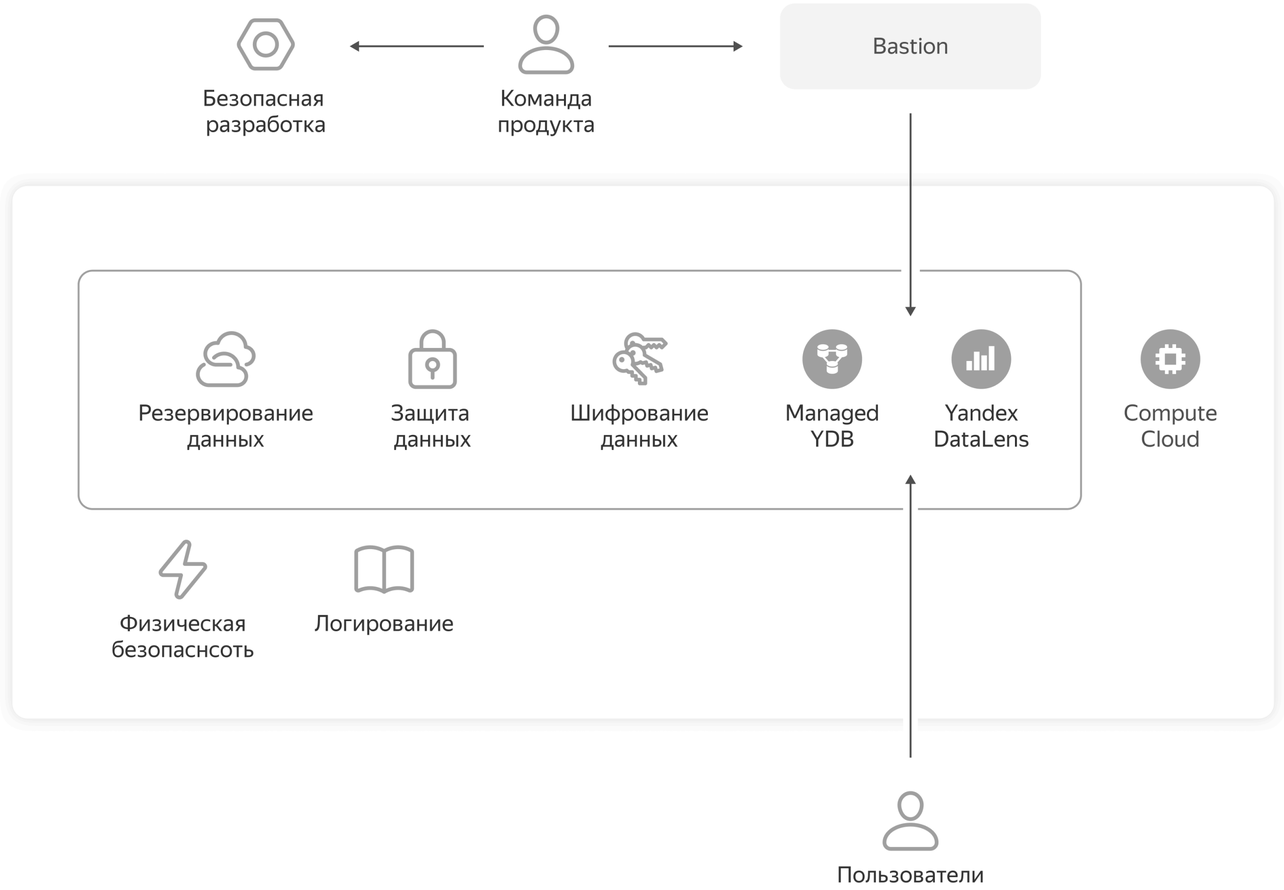
- Identity and Access Management (IAM)
- Application Load Balancer

1 из 102

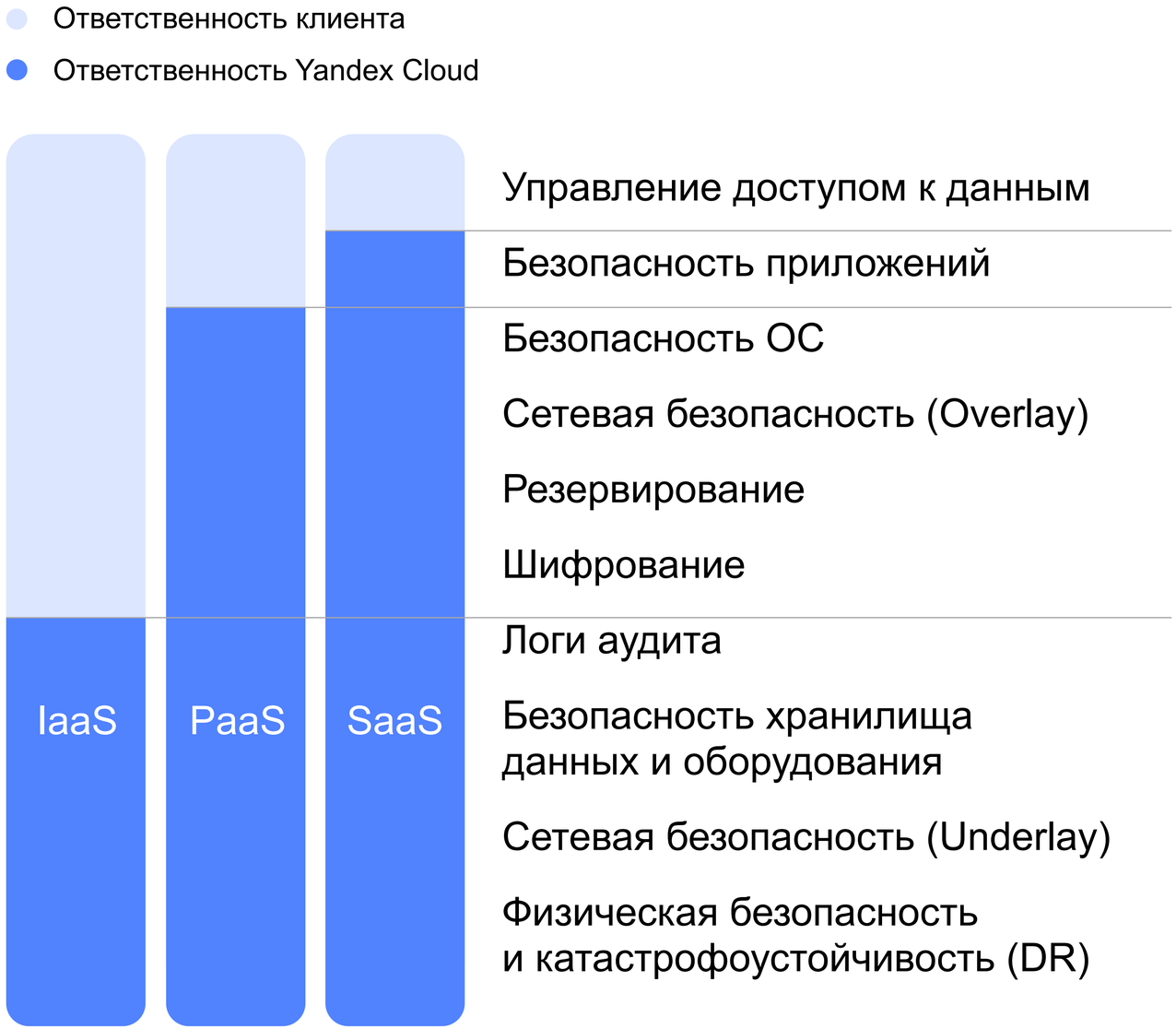
Готовые блоки безопасной разработки «из коробки»



Разделение ответственности между облаком и клиентом



Разделение ответственности между облаком и клиентом



Отвечаем требованиям 152-ФЗ и индустриальных стандартов

152-ФЗ, УЗ-1

Аттестат соответствия
по требованиям 21-го
приказа ФСТЭК

Стандарты ISO

ISO 27001, ISO 27017, ISO 27018
и ISO 27701 (new)

Реестр программного обеспечения

Запись в реестре
№ 9286 от 20.02.2021

PCI

PCI DSS/PCI PIN/PCI 3DS
Для ЦОД и облачных сервисов

GDPR

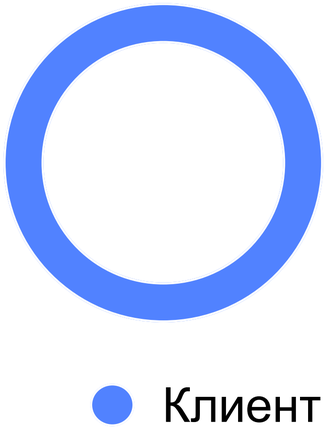
Общий регламент о защите
данных в Европейской зоне

ГОСТ Р 57580.1-2017

Безопасность
финансовых операций

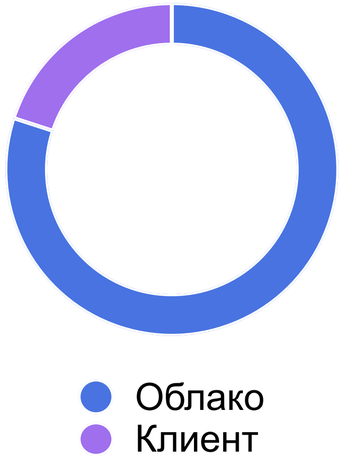
Действия для прохождения аудита

- Построить инфраструктуру, которая соответствует требованиям на всех уровнях, начиная с физического
- Понять, что делать с защитой среды виртуализации
- Провести аудит



- Изучить матрицу ответственности между клиентом и облаком
- Выполнить требования в зоне ответственности клиента

  С помощью готовых блоков
- Провести аудит

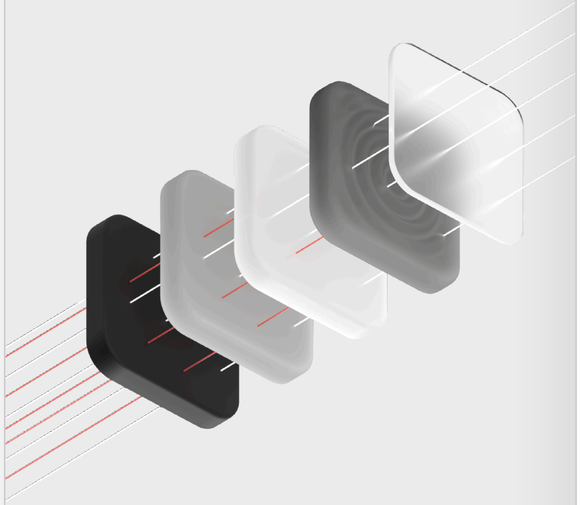


Больше информации

Основные меры информационной безопасности

Изоляция данных в Yandex Cloud

Основные меры по информационной безопасности, применяемые в компании Yandex Cloud



Yandex Cloud 2022

Yandex Cloud

Изоляция данных в Yandex Cloud

Серверы Yandex Cloud находятся в отдельных зонах внутри дата-центров и изолированы от других сервисов Яндекса на уровне оборудования. В таких зонах действуют особые правила доступа, а физическая сеть платформы изолирована по периметру межсетевым экранированием.

В инфраструктуре IaaS/PaaS провайдера представлены следующие слои изоляции:

1. Логическая изоляция на уровне гипервизора
2. Логическая изоляция на уровне управляемых сервисов
3. Изоляция управляющей сети провайдера от виртуальных сетей облачных пользователей
4. Изоляция трафика разных виртуальных сетей
   В том числе виртуальных сетей одного клиента
5. Логическая изоляция на уровне учётных записей и прав доступа
6. Разделение сущностей Control Plane и Data Plane
7. Изоляция сервисных компонентов (виртуальные машины, контейнеры, базы данных) инфраструктуры провайдера от ресурсов пользователей
   - а. На уровне физических хостов
   - б. На уровне сети

Логическая изоляция на уровне гипервизора

1

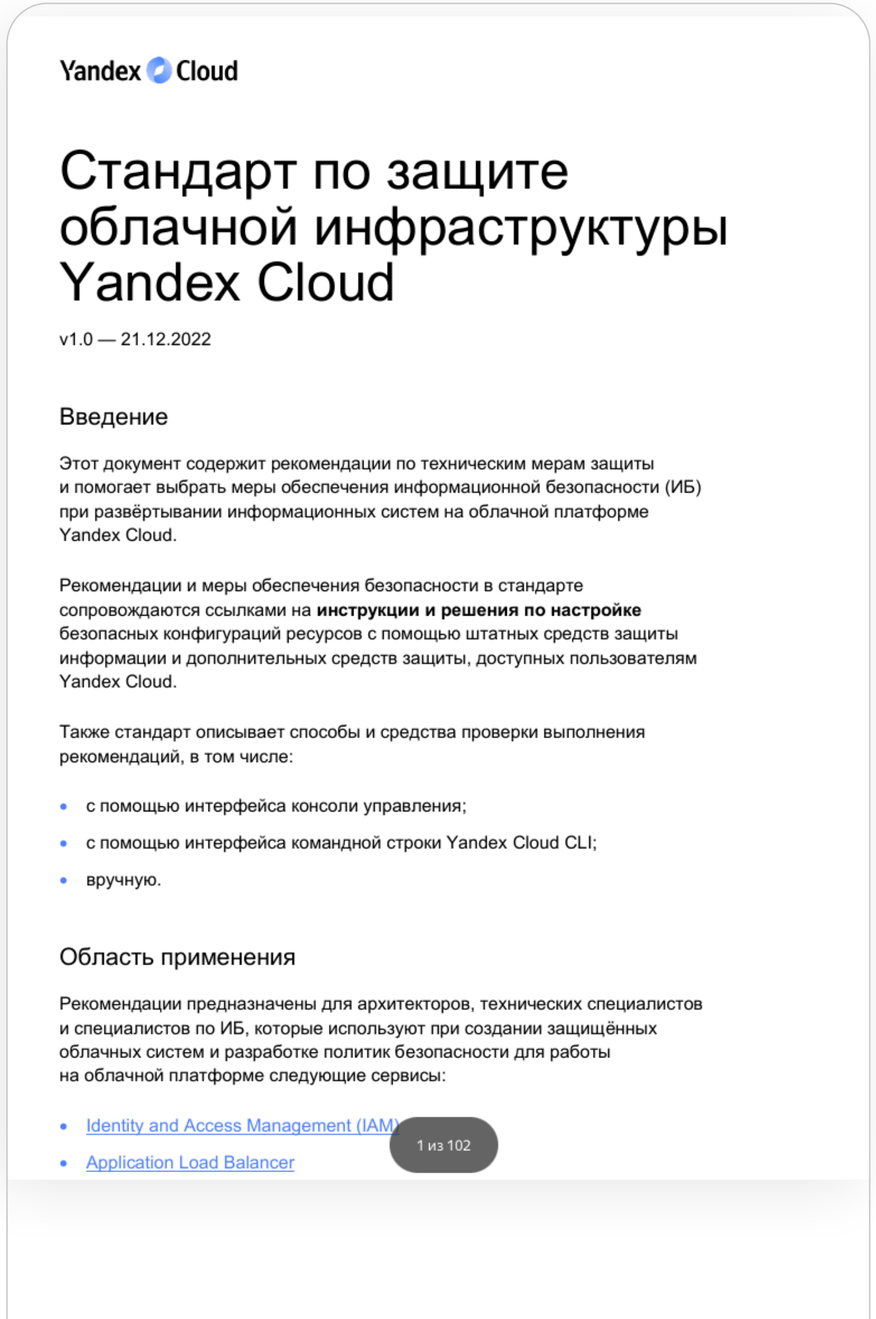
Реализация классической изоляции через функциональность гипервизора. Архитектура гипервизора и средства управления виртуальной средой обеспечивают изоляцию одной виртуальной машины (ВМ) от другой в соответствии с их архитектурой. В Yandex Cloud используется аппаратная виртуализация, реализованная при помощи набора команд Intel VT-x. Взаимодействие таких ВМ можно организовать только с помощью коммутатора L3 между ВМ, при этом не важно, на одном или разных физических хостах они размещены.

Подведём итоги

Стандарт по защите облачной инфраструктуры Yandex Cloud 1.0

- Основан на практическом опыте и на наших гайдах
- Инструмент для аудита контролей безопасности в облаке
- Учитывает основные риски, связанные с облаком
- Можно автоматизировать

clck.ru/33Yyyj



Yandex Cloud

Стандарт по защите облачной инфраструктуры Yandex Cloud

v1.0 — 21.12.2022

Введение

Этот документ содержит рекомендации по техническим мерам защиты и помогает выбрать меры обеспечения информационной безопасности (ИБ) при развёртывании информационных систем на облачной платформе Yandex Cloud.

Рекомендации и меры обеспечения безопасности в стандарте сопровождаются ссылками на **инструкции и решения по настройке** безопасных конфигураций ресурсов с помощью штатных средств защиты информации и дополнительных средств защиты, доступных пользователям Yandex Cloud.

Также стандарт описывает способы и средства проверки выполнения рекомендаций, в том числе:

- с помощью интерфейса консоли управления;
- с помощью интерфейса командной строки Yandex Cloud CLI;
- вручную.

Область применения

Рекомендации предназначены для архитекторов, технических специалистов и специалистов по ИБ, которые используют при создании защищённых облачных систем и разработке политик безопасности для работы на облачной платформе следующие сервисы:

- Identity and Access Management (IAM)
- Application Load Balancer

1 из 102

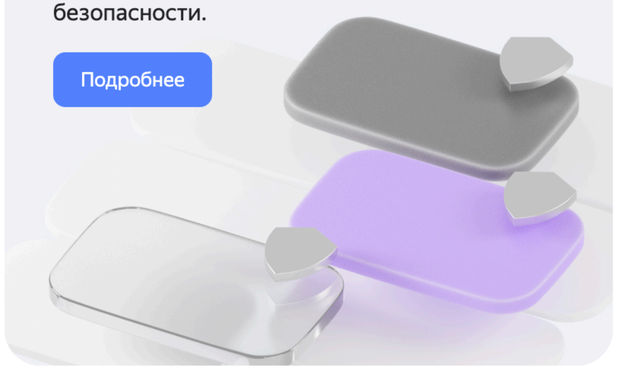
Углублённое обучение

Курсы для Security

Защита облачной инфраструктуры

Познакомьтесь с ключевыми концепциями обеспечения безопасности облачной инфраструктуры. Узнайте, как настроить и поддерживать необходимый уровень безопасности.

Подробнее



DevSecOps в облачном CI/CD

На практике узнаете, что такое DevSecOps, зачем он нужен и как усовершенствовать существующие DevOps-пайплайны, чтобы обеспечить безопасность разрабатываемых приложений.

Подробнее

Скоро появятся

- Аутентификация и управление доступами
- Погружение в сетевую безопасность
- Шифрование данных и управление ключами
- Безопасная конфигурация инфраструктуры
- Управление уязвимостями
- Безопасность с Terraform
- Сбор, мониторинг и анализ логов аудита
- Compliance

Подписаться

cloud.yandex.ru/training/training-pro

Буду рад продолжить общение

Рами Мулейс
Менеджер группы продуктовой архитектуры Security & Compliance

Телеграм-чат
t.me/YandexCloudSecurity