Yandex Cloud

Fintech ready cloud

Безопасность Yandex Cloud

Концепции безопасности облака

Что мы делаем для безопасности облака

Инструменты безопасности

Соответствие требованиям

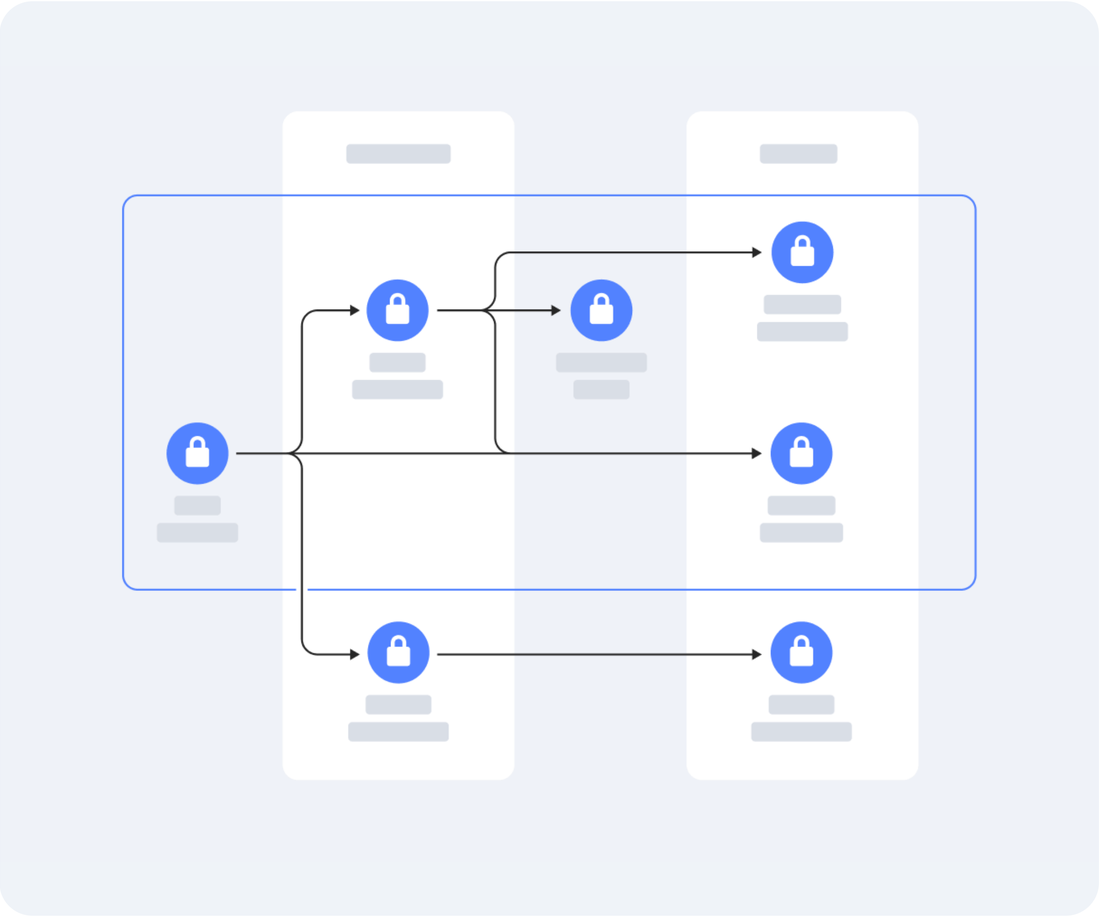
Ресурсы для обеспечения безопасности

Приватность и сохранность данных —
один из приоритетов Yandex Cloud

Соответствие требованиям законодательства

Отдельная команда Privacy

Внедрение принципов Privacy-by-design



Yandex Cloud соответствует международным и национальным стандартам и требованиям

Cloud Security Alliance

Security, Trust, Assurance and Risk (STAR) по уровню Level 1

ГОСТ Р 57580.1-2017

Безопасность финансовых операций

Реестр программного обеспечения

Запись в реестре
№ 9286 от 20.02.2021

152-ФЗ, УЗ-1

Аттестат соответствия по требованиям 21-го приказа ФСТЭК

Стандарты ISO

ISO 27001, ISO 27017, ISO 27018 и ISO 27701

Стандарты PCI

PCI DSS v4 New
Для ЦОД и облачных сервисов, PCI PIN и PCI 3DS

GDPR

Общий регламент о защите данных в Европейской зоне

В инфраструктуре Yandex Cloud представлены 7 слоёв 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
5. Логическая изоляция на уровне учетных записей и прав доступа
6. Разделение сущностей Control Plane и Data Plane
7. Изоляция сервисных компонент инфраструктуры провайдера от пользовательских ресурсов

Подробнее о слоях безопасности в Yandex Cloud

Доступ к данным клиентам строго регулируется

Доступ только с согласия клиентов для помощи

Круглосуточный SOC отслеживает аномальное поведение

Все доступы контролируются на Бастион-сервере (PAM)

Регламенты, least privilege, zero trust, ответственность

Статистика по безопасности самой платформы

(на конец 2023 года)

820 млн

общее количество инвестиций

x2

отбитых DDoS атак

6 млн

выплаты bug bounty

10

бюллетеней безопасности

~100

кол-во человек в Security

12

кол-во внешних ИБ аудитов

>1500

кол-во часов Red Team

В Yandex Cloud обрабатываются данные, требующие особой защиты

Персональные данные

Медицинские данные

Коммерческая тайна

Финансовые данные

Концепции безопасности облака

Что мы делаем для безопасности облака

Инструменты безопасности

Соответствие требованиям

Ресурсы для обеспечения безопасности

Инструменты безопасности Yandex Cloud

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

Smart Web Security Preview
Защита веб-приложений

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

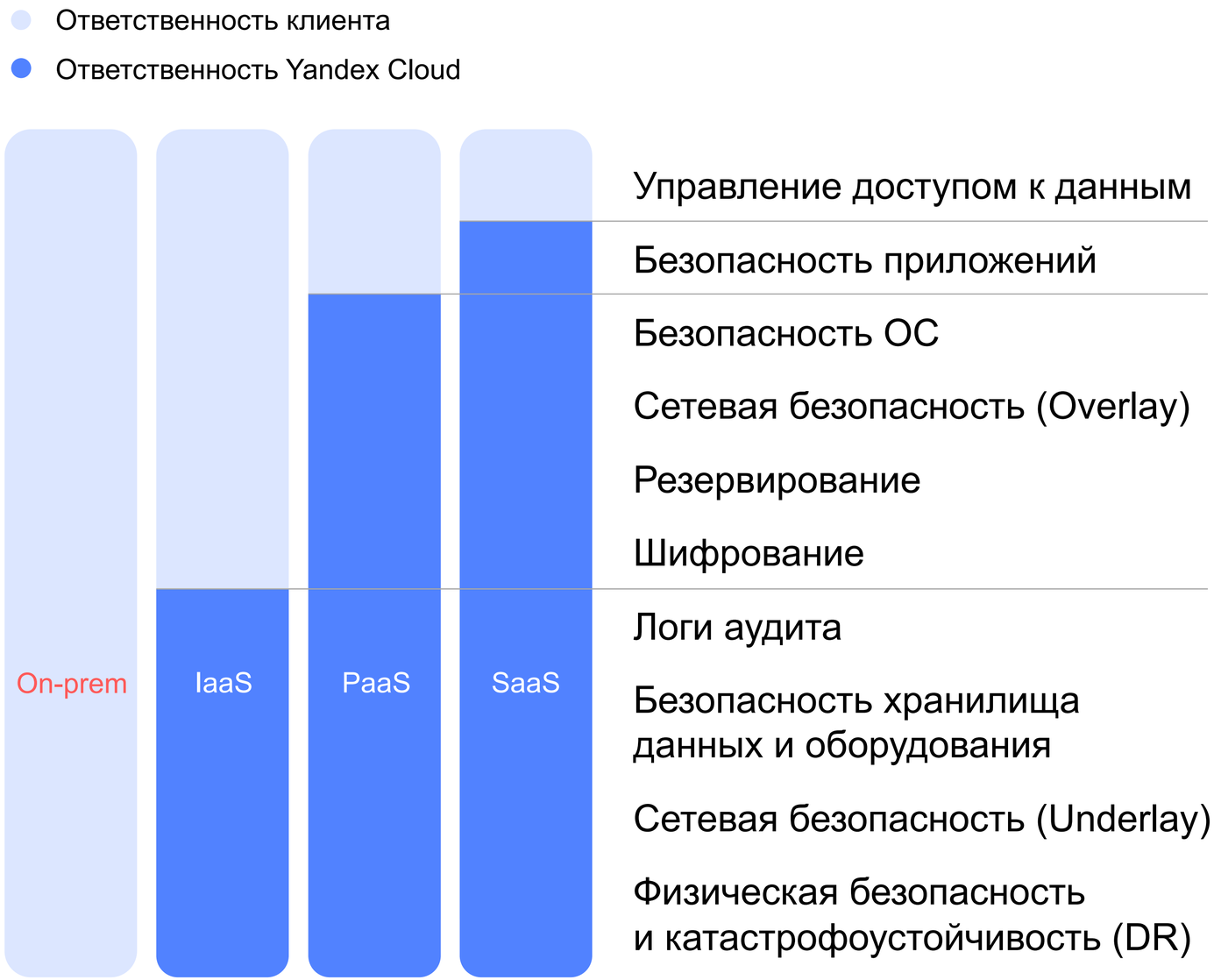
Подробнее

Yandex Cloud Marketplace

Все решения на сайте

Как обеспечивается безопасность в Yandex Cloud

Совместная ответственность между облаком и клиентом

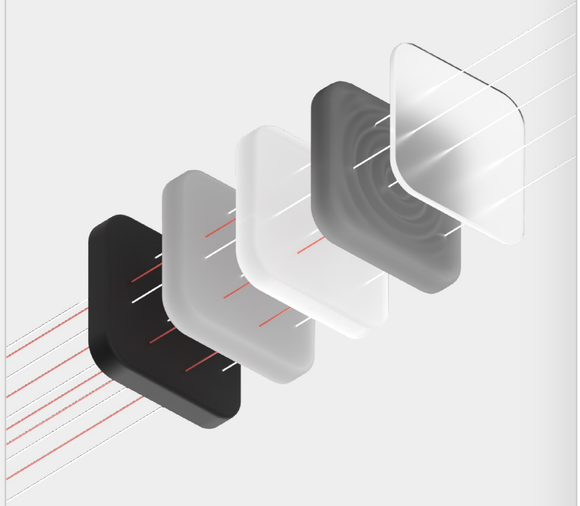


Больше информации

Основные меры по 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

Сервера 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 Control plane сущностей и Data Plane
7. Изоляция сервисных компонент (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 посредством функциональности 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.

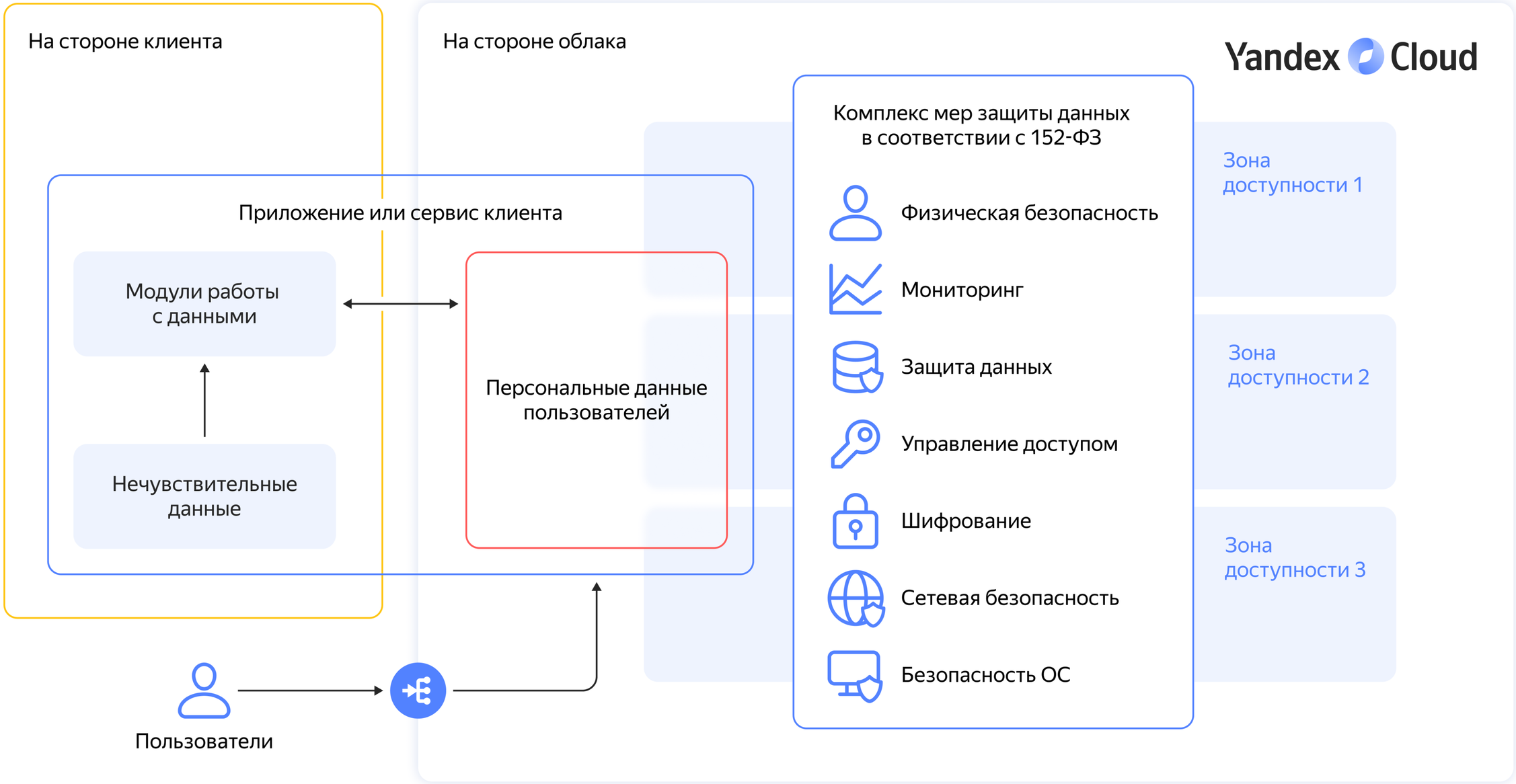
Концепции безопасности облака

Что мы делаем для безопасности облака

Инструменты безопасности

Соответствие требованиям

Ресурсы для обеспечения безопасности


На стороне клиента
На стороне облака
Yandex Cloud
Комплекс мер защиты данных
в соответствии с 152-ФЗ
Физическая безопасность
Мониторинг
Защита данных
Управление доступом
Шифрование
Сетевая безопасность
Безопасность ОС
Зона
доступности 1
Зона
доступности 2
Зона
доступности 3
Приложение или сервис клиента
Модули работы
с данными
Нечувствительные
данные
Персональные данные
пользователей
Пользователи

Соответствие ФЗ-152

Платформа Yandex Cloud имеет аттестат соответствия ИСПДн требованиям ФЗ-152 (УЗ-1), постановления правительства №1119 и Приказа ФСТЭК №21

Шаг 1 Определите тип данных и процессы работы

Шаг 2 Выберите инструменты защиты данных

Шаг 3 Подготовьтесь к оценке соответствия 152-ФЗ

Требования ФЗ-152 и разделение ответственности: clck.ru/32rnNR

Концепции безопасности облака

Что мы делаем для безопасности облака

Инструменты безопасности

Соответствие требованиям

Ресурсы для обеспечения безопасности

Доступные инструменты обеспечения безопасности

Руководства и гайды

Стандарт по защите облачной инфраструктуры Yandex Cloud

Документация и чеклисты

Бюллетени безопасности

Security Solution Library

Готовые сценарии и примеры

Решения на базе сервисов облака

Решения с использованием сторонних средств защиты

Углублённое обучение

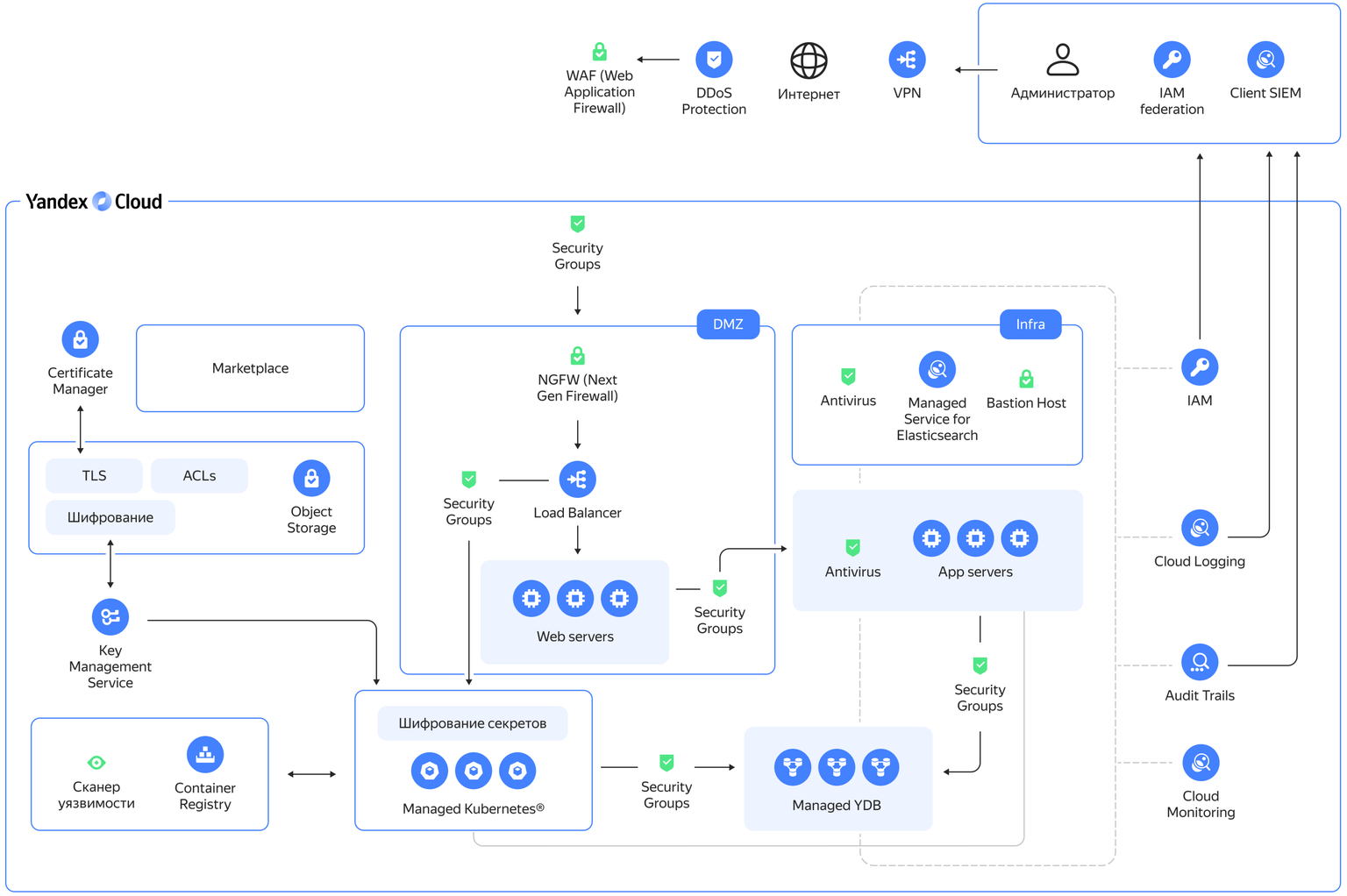
Курсы по безопасности облачных платформ

Стандарт по защите облачной инфраструктуры Yandex Cloud

Практические рекомендации по защите облачной инфраструктуры

cloud.yandex.ru/docs/security/standard/all

Референсная архитектура ИБ для клиента

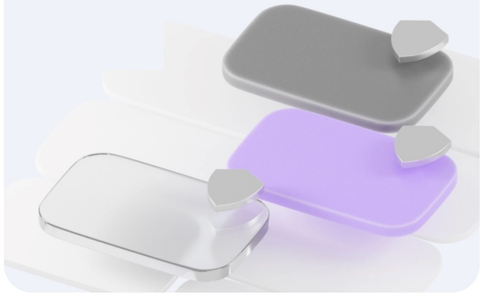


https://github.com/yandex-cloud-examples/yc-security-solutions-library - обратная-связь-и-пожелания

Курсы по облачной безопасности

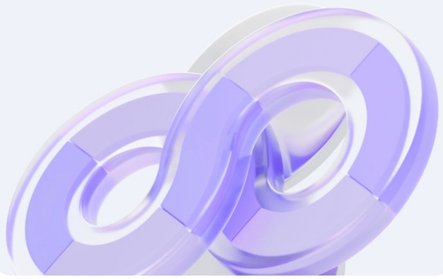
Защита облачной инфраструктуры

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



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.

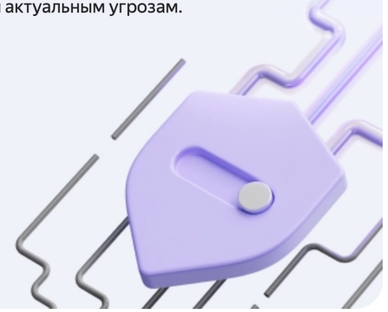


Аутентификация и управление доступами

На курсе вы познакомитесь с механизмами аутентификации и управления доступом и научитесь работать с облачными ресурсами в приложении.

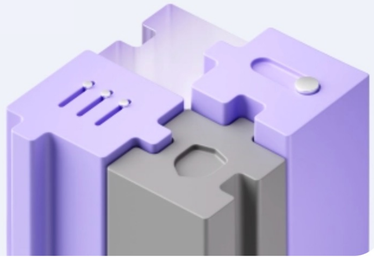
Погружение в сетевую безопасность

На курсе вы настроите защиту облачной инфраструктуры и познакомитесь с облачными инструментами и методами противодействия самым актуальным угрозам.



Compliance в облачной инфраструктуре

На курсе вы узнаете, как применяются требования регуляторов и стандартов в контексте облака и как соответствовать этим требованиям на практике.



Скоро появятся

- Шифрование данных и управление ключами
- Безопасная конфигурация инфраструктуры
- Управление уязвимостями
- Безопасность с Terraform
- Сбор, мониторинг и анализ логов аудита

clck.ru/35WuNv

Спасибо!
Вопросы?

Лев Шумский
Директор по развитию практик безопасности
largeshu@yandex-team.ru

Security-чат
в Telegram

t.me/YandexCloudSecurity