Kaspersky Industrial Cybersecurity Conference 2023

Коммуникационные и облачные сервисы VK для промышленности: можно ли?

Олег Бойко

Директор по информационной безопасности,
ООО "ВК Цифровые технологии"

kaspersky

Работа в промышленности

tech

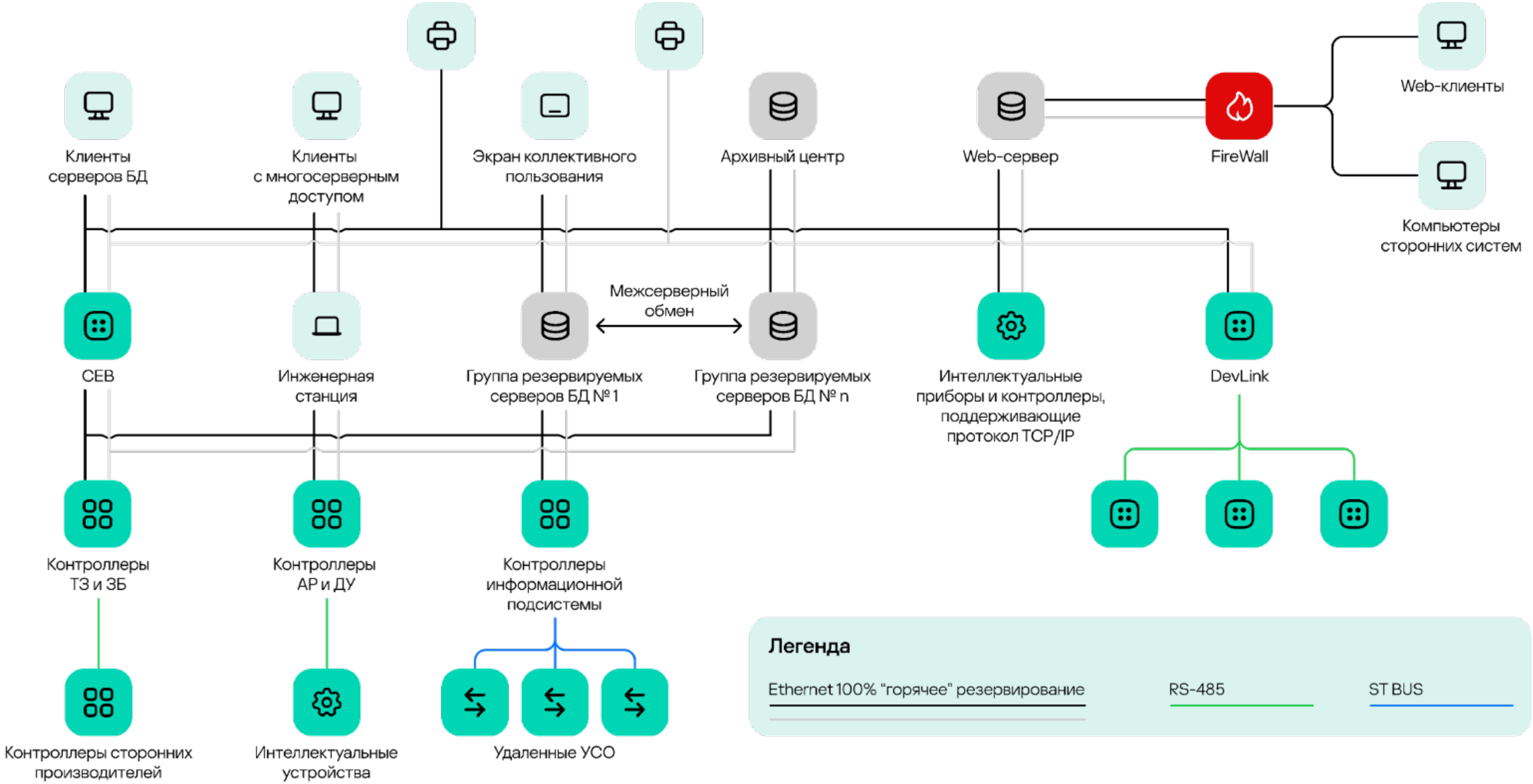
Работа в промышленности

tech

Работа в промышленности

tech

ИТ-ландшафт промышленного предприятия



ИТ-задачи и вызовы

ИТ-инфраструктура как сервис

Объединение вычислительных мощностей организации во внутреннее облако с финансовым контролем по каждому проекту, автоматизированным предоставлением ресурсов и контролем информационной безопасности

ИТ-задачи и вызовы

ИТ-инфраструктура как сервис

Объединение вычислительных мощностей организации во внутреннее облако с финансовым контролем по каждому проекту, автоматизированным предоставлением ресурсов (Pay-as-you-go) и контролем информационной безопасности

Платформа для разработки

Ускорение и стандартизация написания приложений для микросервисной архитектуры с автоматизацией процесса разработки (создание кода, тестирование, интеграция тестовых и продуктивных сред)

ИТ-задачи и вызовы

ИТ-инфраструктура как сервис

Объединение вычислительных мощностей организации во внутреннее облако с финансовым контролем по каждому проекту, автоматизированным предоставлением ресурсов (Pay-as-you-go) и контролем информационной безопасности

Платформа для разработки

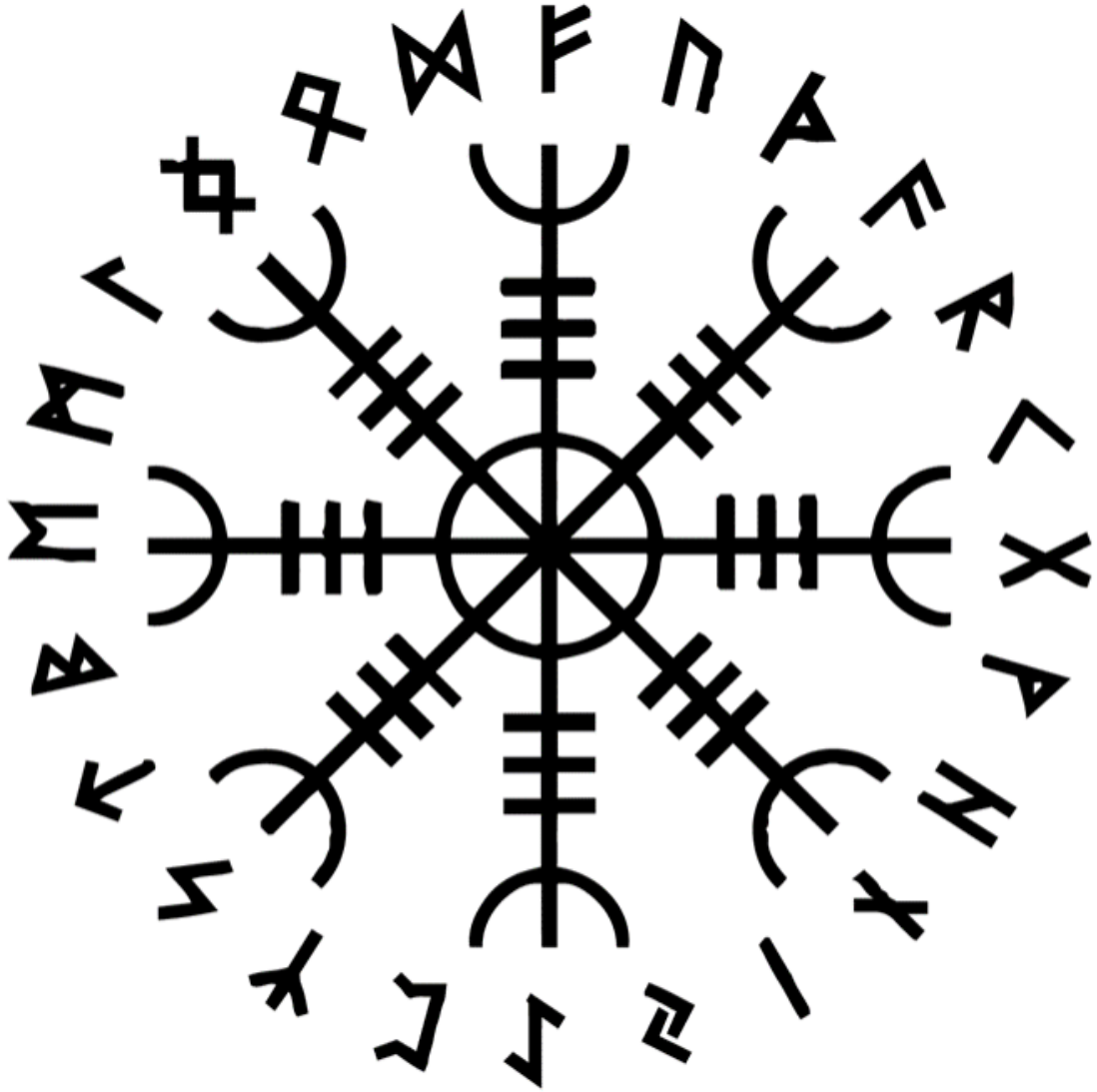
Ускорение и стандартизация написания приложений для микросервисной архитектуры с автоматизацией процесса разработки (создание кода, тестирование, интеграция тестовых и продуктивных сред)

Платформа данных

Объединение данных в организации для анализа и монетизации. Проектирование хранилищ данных, озер данных и витрин данных. Быстрое создание процессов обработки и моделей для предиктивной аналитики

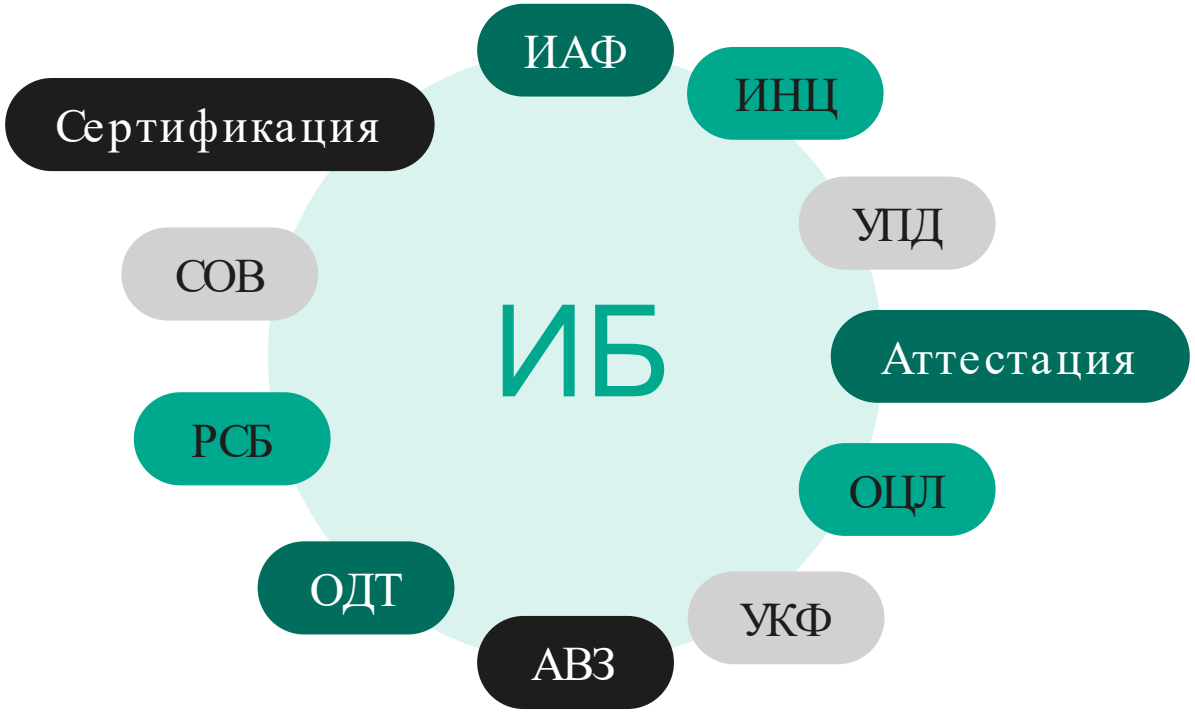
tech

Требования от ИБ

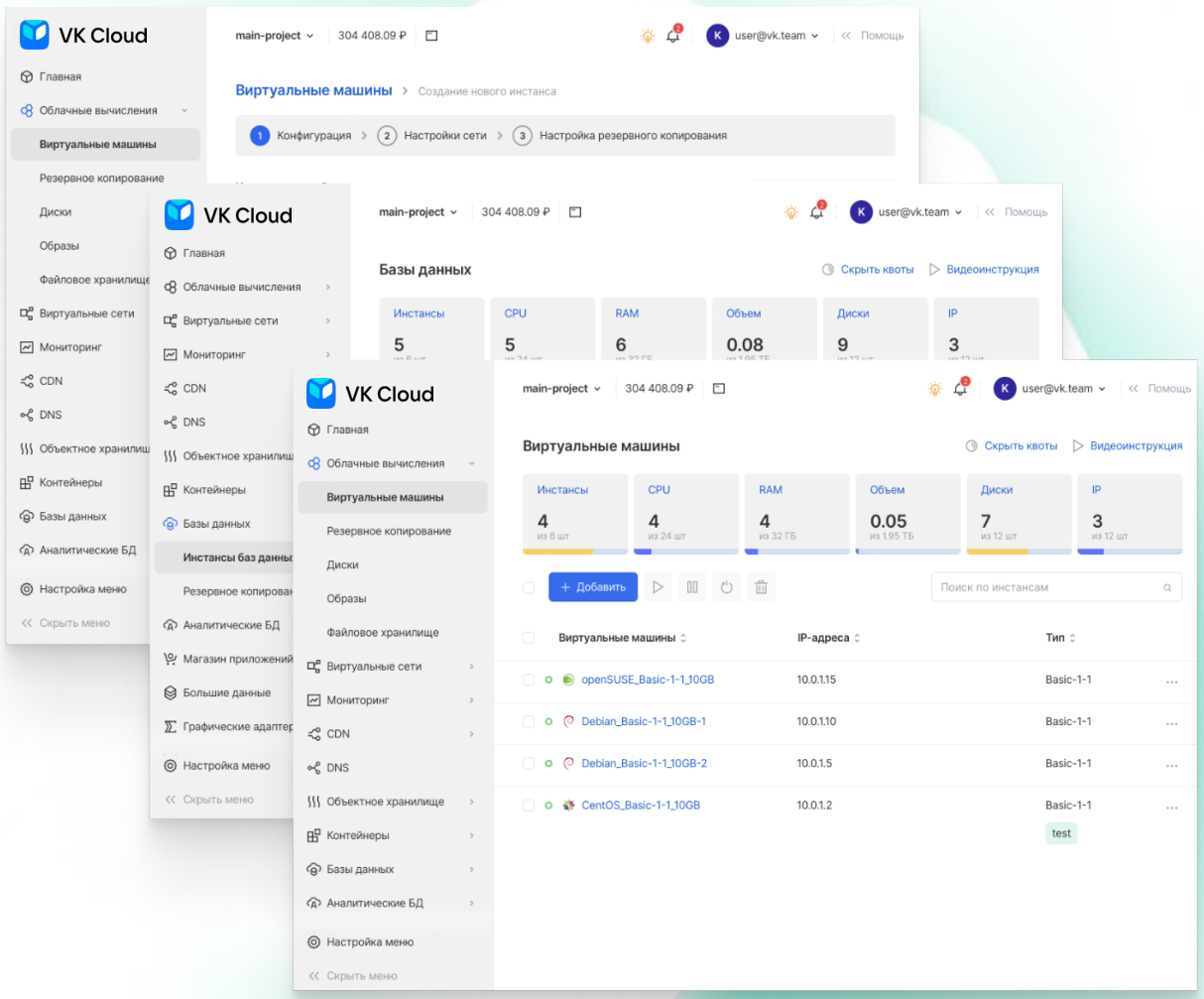


tech

Требования от ИБ



tech



Private Cloud

- Платформа для построения частного облака в ЦОДах заказчиков: крупных компаниях и государственных учреждениях.
- С широким выбором готовых инструментов для ИТ-специалистов, разработчиков, дата-аналитиков, кибербезопасности.
- У продуктов несколько независимых слоев защиты.
- Платформу можно развернуть на серверах компании (On-Premise) или использовать в облаке (SaaS).
- Входят в реестр российского ПО и отвечают требованиям ФЗ-152.

VK Cloud tech

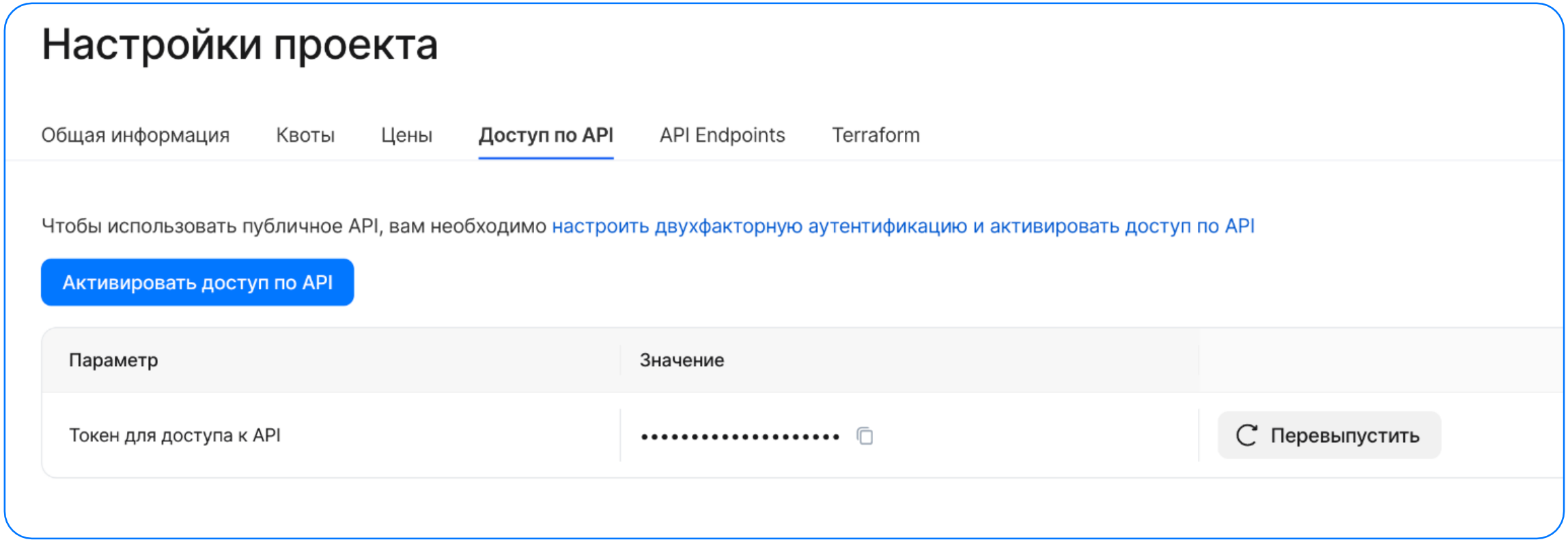
Cloud: идентификация и аутентификация

Внешняя аутентификация через корпоративный LDAP-каталог

Внутренняя аутентификация с помощью Keycloak

А ещё в проекте можно исследовать и реализовать интеграцию с вашим IdP/IdM, прикрутить VPN с 2FA и пр.

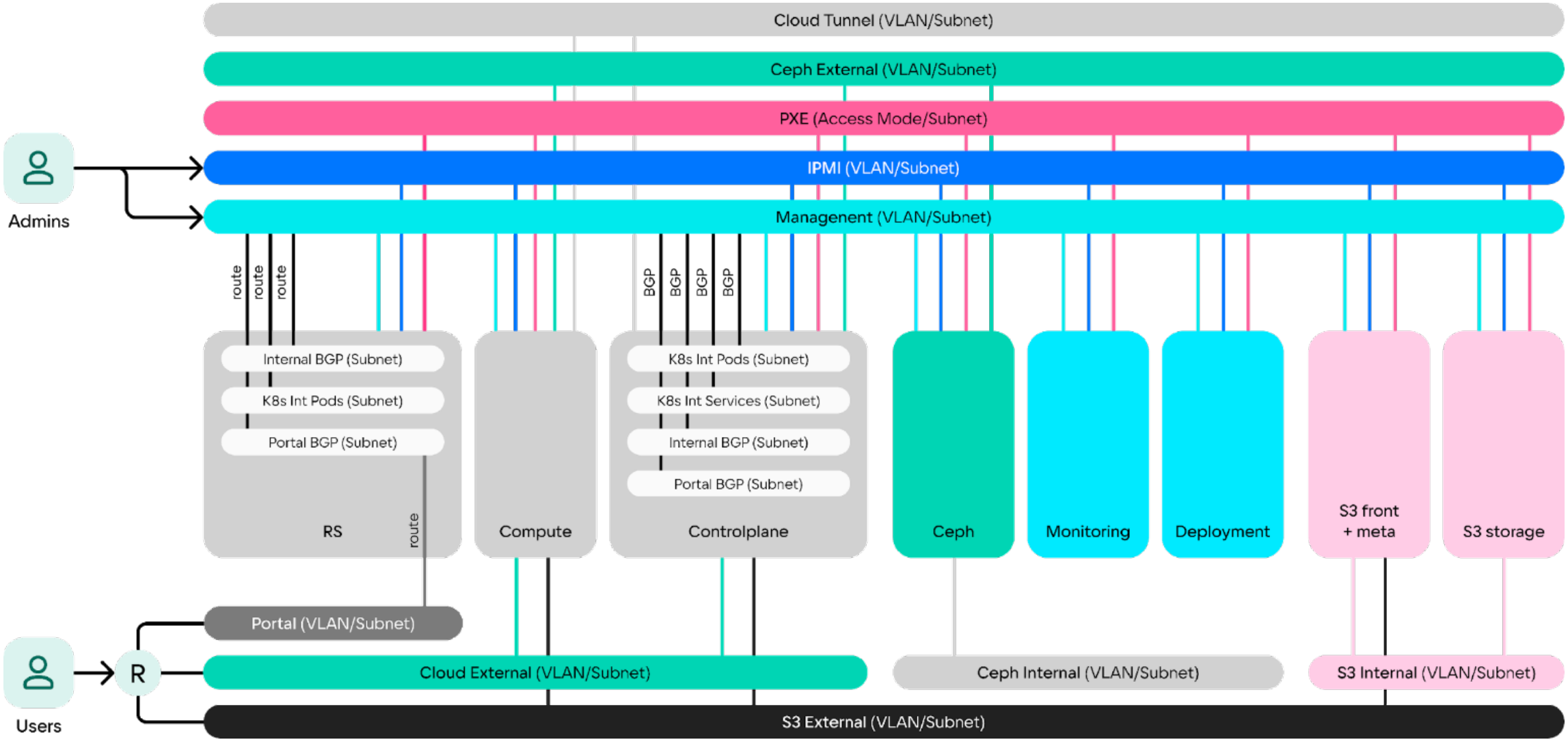
Cloud: идентификация и аутентификация



Cloud: управление доступом

Операции / Роль	Владелец проекта	Суперадминистратор	Администратор проекта	Наблюдатель	Администратор пользователей (IAM)	Администратор биллинга	Администратор виртуальных машин	Администратор сети	Администратор сетевой безопасности	Администратор внутренних сетей	Администратор Kubernetes	Оператор Kubernetes Аудитор Kubernetes
Общее управление												
Пользователи и их роли в проекте RW: добавление / удаление пользователей проекта, назначение им ролей. R: просмотр списка пользователей и их ролей	RW	RW	R	R	RW	–	–	–	–	–	–	–
Баланс и платежи RW: просмотр баланса проекта с детализацией расходов, пополнение баланса. R: просмотр баланса проекта без детализации расходов	RW	RW	R	R	–	RW	–	–	–	–	–	–
Виртуальные машины (Облачные вычисления)												
Виртуальные машины RW: добавление / изменение / удаление / перезагрузка ВМ, подключение ВМ к виртуальной сети, мониторинг ВМ, доступ к логам. R: просмотр и мониторинг ВМ, доступ к логам	RW	RW	RW	R	–	–	RW	–	R	R	–	–
Виртуальные диски RW: добавление / изменение / удаление дисков, монтирование, создание снимков, миграция. R: просмотр дисков	RW	RW	RW	R	–	–	RW	–	R	R	–	–
Образы RW: добавление / изменение / удаление образов ВМ. R: просмотр образов	RW	RW	RW	R	–	–	R	–	R	R	R	–
Сеть (Виртуальные сети и DNS)												
DNS-зоны RW: добавление / изменение / удаление DNS-зон. R: просмотр DNS-зон	RW	RW	RW	R	–	–	R	RW	R	R	R	R
Балансировщики нагрузки RW: добавление / изменение / удаление балансировщиков нагрузки. R: просмотр балансировщиков нагрузки	RW	RW	RW	R	–	–	R	RW	R	R	RW	R
Сети и подсети, IP адреса, маршрутизаторы RW: добавление / изменение / удаление сетей, подсетей, плавающих IP адресов, маршрутизаторов. R: просмотр сетей, подсетей, плавающих IP адресов, маршрутизаторов	RW	RW	RW	R	–	–	R	RW	R	RW	RW	R
VPN RW: добавление / изменение / удаление VPN-туннелей. R: просмотр VPN-туннелей	RW	RW	RW	R	–	–	R	RW	R	R	RW	R
Настройки firewall RW: добавление / изменение / удаление групп правил. R: просмотр групп правил	RW	RW	RW	R	–	–	RW	RW	RW	R	RW	R
Сервисы PaaS												
Контейнеры RW: добавление / изменение / удаление кластеров Kubernetes. R: просмотр кластеров Kubernetes	RW	RW	RW	R	–	–	–	–	–	–	RW	R
Мониторинг RW: добавление / изменение / удаление дашбордов и триггеров. R: просмотр дашбордов и триггеров	RW	RW	RW	R	–	–	RW	–	R	R	–	–

Cloud: изоляция underlay и overlay



Cloud: фильтрация сетевого трафика

Задача:

При интеграции в ЦОД необходимо выбрать вариант реализации функции межсетевого экранирования

Выбор во многом обусловлены требованиями ИБ

Выбор повлияет на эффективность процессов самообслуживания

Варианты решения:

Централизованное управление фильтрацией трафика пользователя

Распределенный межсетевой экран на основе SDN (Security groups)

Вендорские решения для фильтрации трафика в облаке

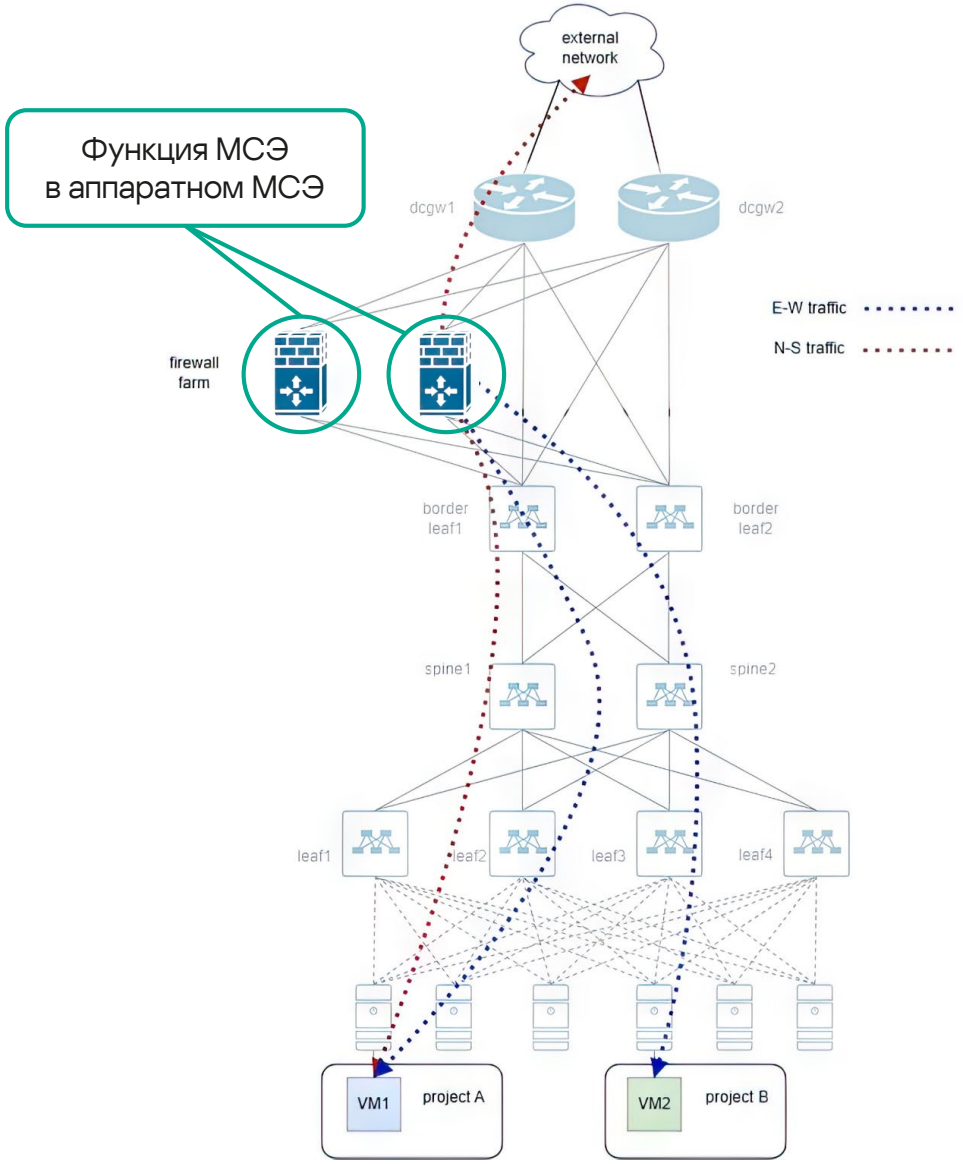
Централизованная фильтрация трафика

Плюсы

- Ферма МСЭ – единая точка фильтрации трафика
- Фильтрация как трафика от ВМ во внешний мир и обратно так и трафика между ВМ (или между проектами)
- Понятная и функциональная аппаратная часть и программное обеспечение фермы МСЭ

Минусы

- Неоптимальный форвардинг
- Плохо масштабируется с ростом облачной нагрузки
- Требуется автоматизация управления фермой МСЭ и синхронизацией с облачной платформой



tech

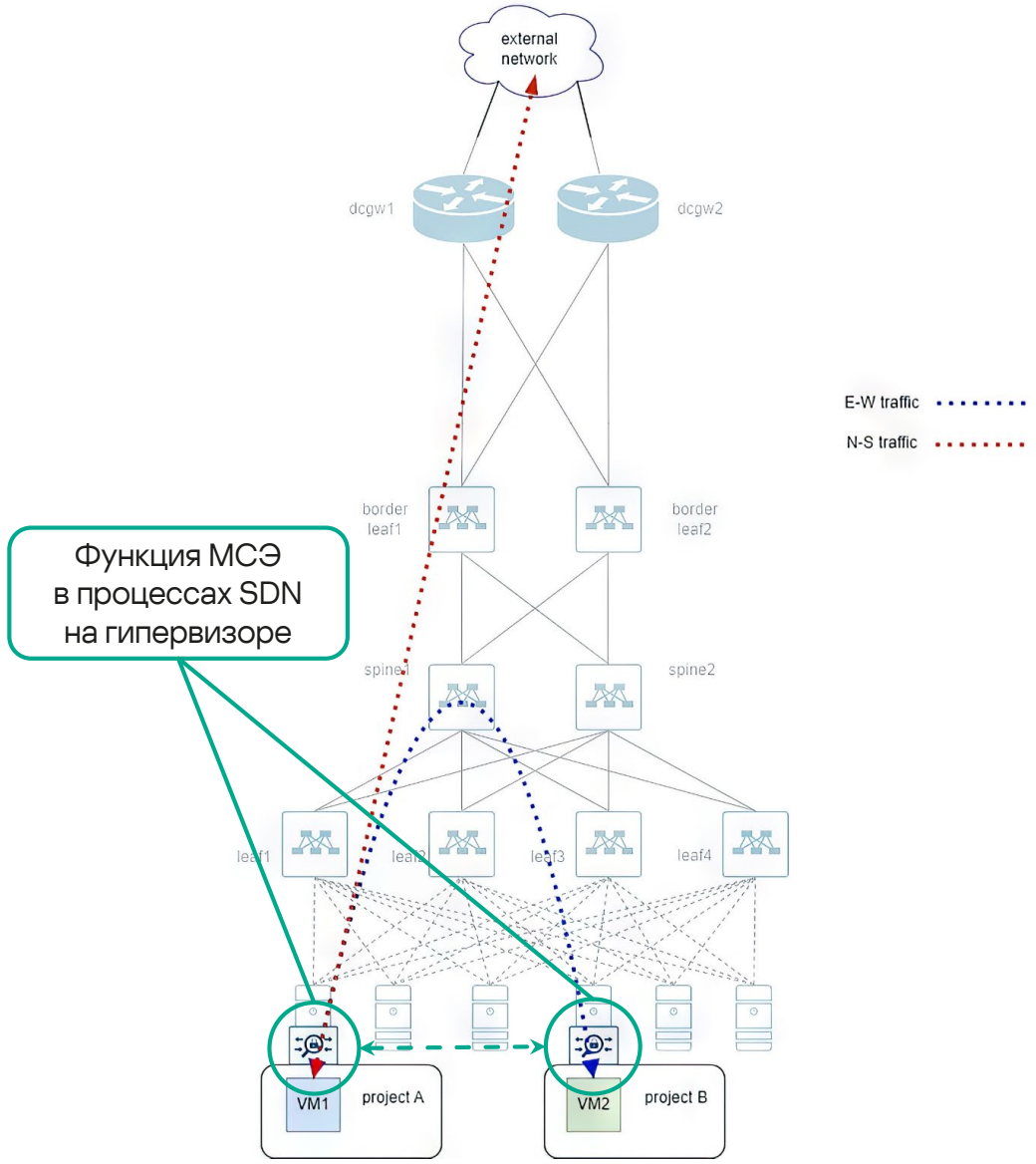
Распределенная фильтрация трафика

Плюсы

- Neutron/Sprut посредством Security Group
- Фильтрация максимально близко к ВМ на гипервизоре
- Оптимальный форвардинг
- Фильтрация трафика как между ВМ,
  так и трафика между ВМ и внешней сетью
- Максимальная интеграция с облачной платформой
- Нет единой точки отказа

Минусы

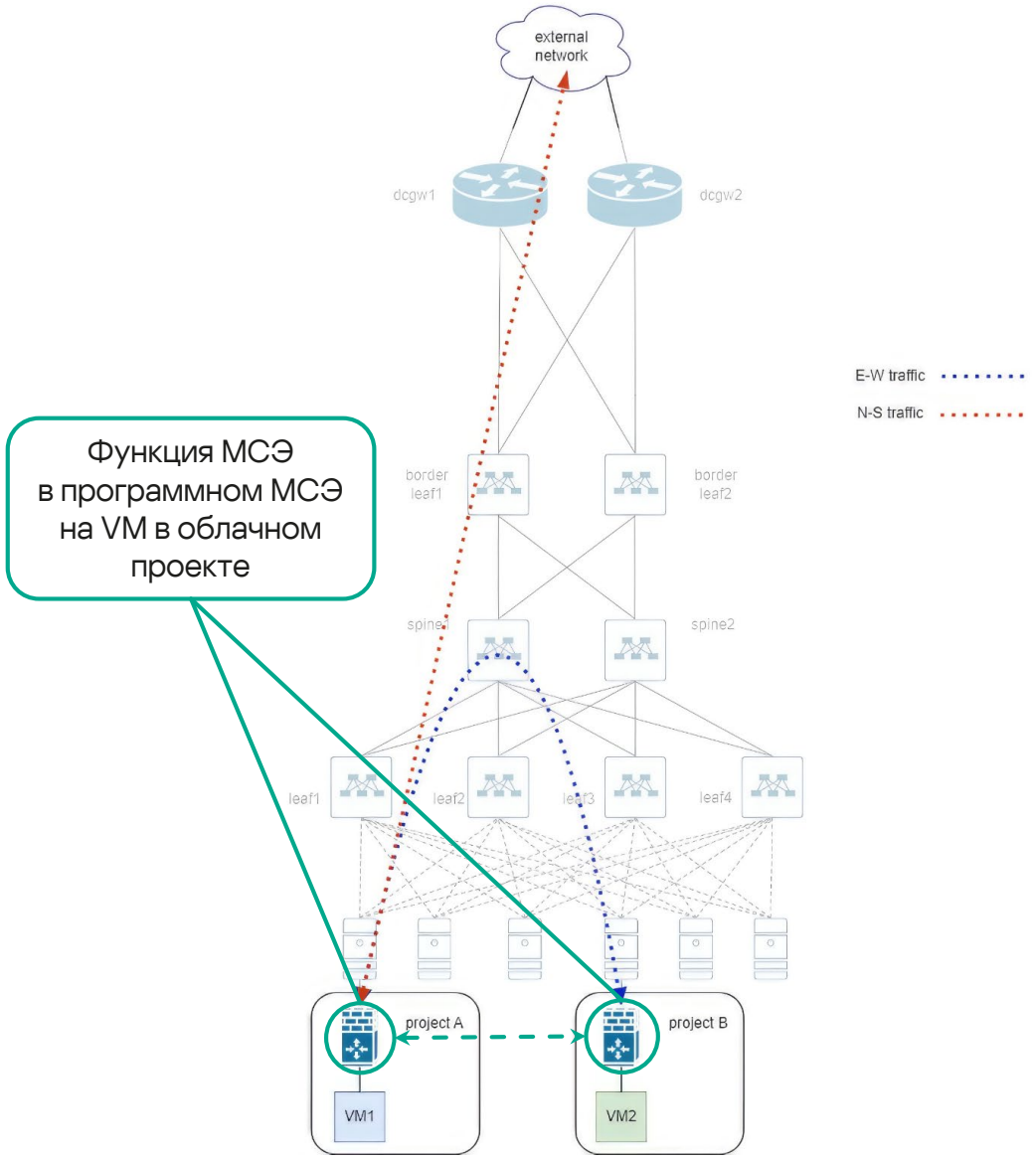
- Существенно меньший функционал
- Команде эксплуатации потребуется адаптироваться



tech

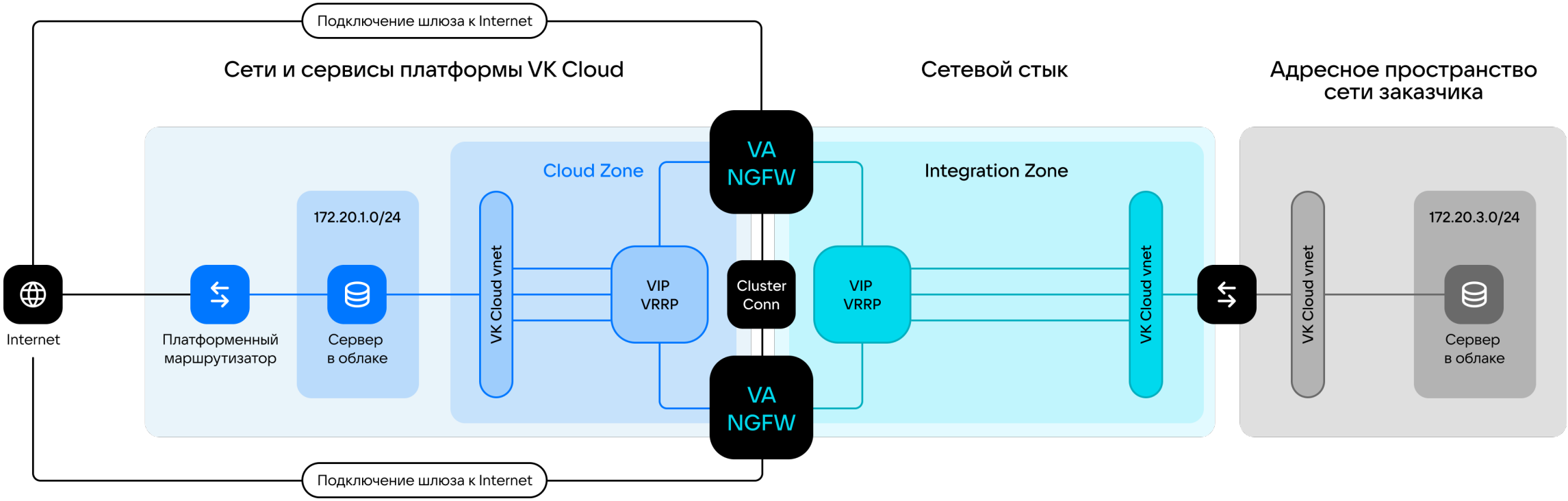
Виртуальные межсетевые экраны

- Размещение виртуального NGFW в проекте клиента
- Влияние на производительность NGFW за счет масштабирования выделенных ресурсов
- Подключение внешних каналов к портам NGFW
- Привычное управление политиками безопасности
- Сегментация внутренней облачной инфраструктуры



tech

Виртуальные межсетевые экраны

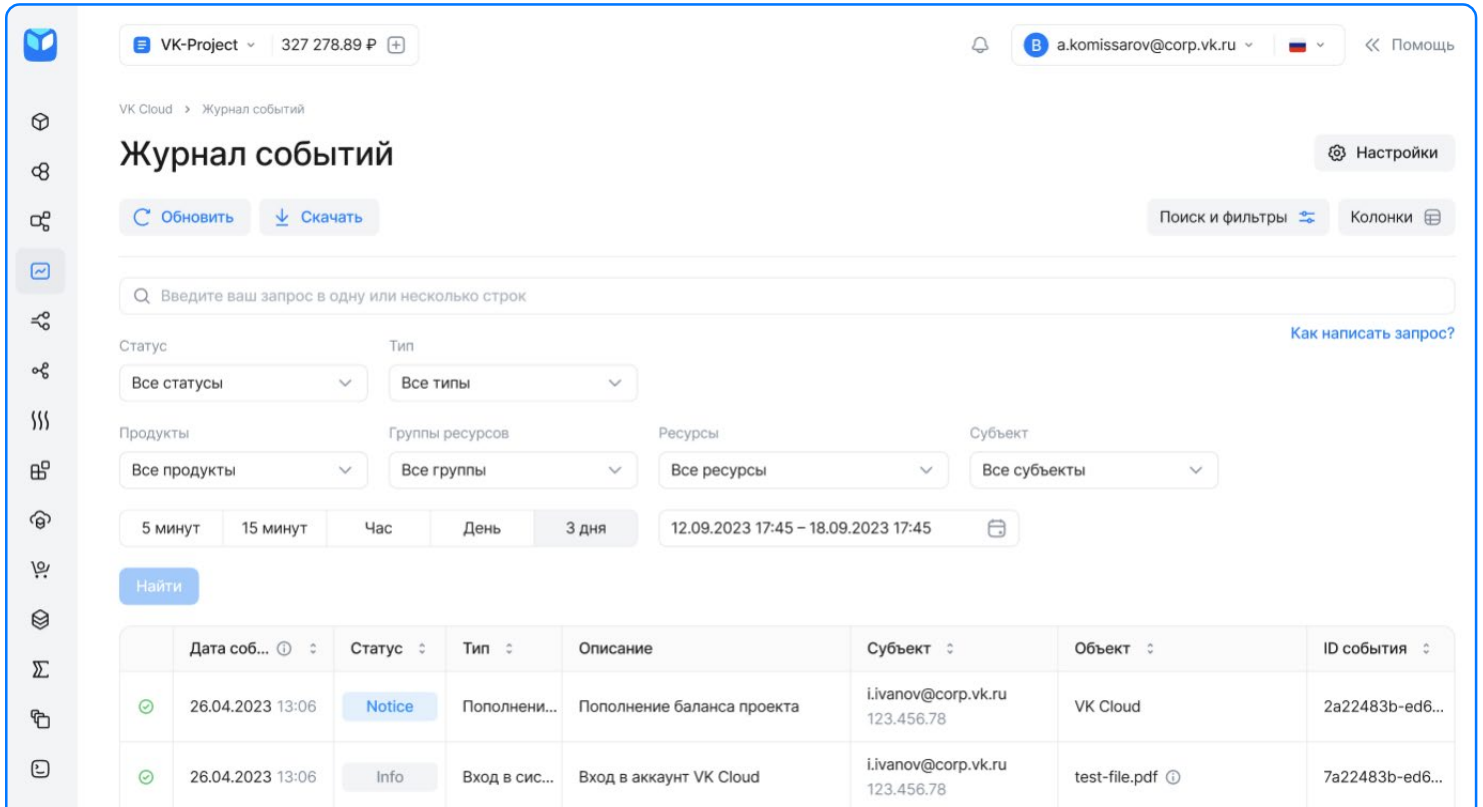


- Привычный интерфейс работы с правилами
- Отказоустойчивость
- Реализация политик фильтрации трафика в соответствии требованиям организации
- Использование статической или динамической маршрутизации

tech

Cloud: регистрация событий безопасности

- Гарантии записи сообщения
- Хранение событий до 365 дней*
- Выгрузка отчётов в файл
- Быстрый отклик поисковой выдачи
- Подключение SIEM систем клиента
- RBAC модель доступа к событиям
- Язык поисковых запросов
- Сбор данных уровня Control Plane и Data Plane*
- Обогащение информации о событии из смежных систем
- Шифрование буфера обогащённых событий



Cloud: регистрация событий безопасности

Сервис позволяет подключать SIEM систему, как целевую для передачи в неё сохранённых событий

Поддерживаемые форматы Syslog: RAW, CEF

События передаются в обогащённом виде

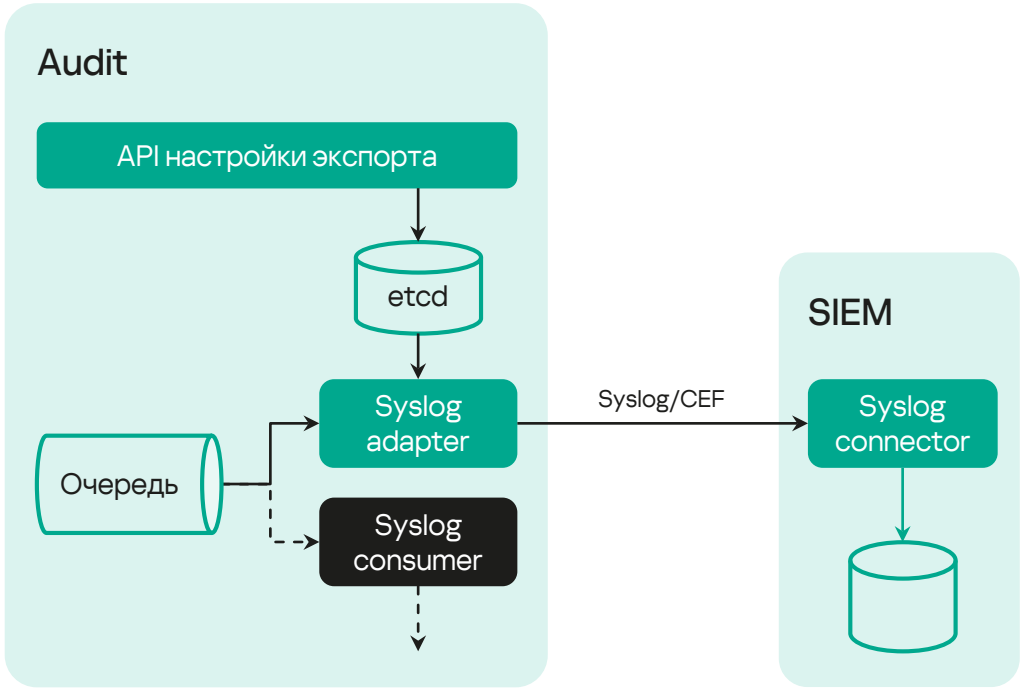
Подключение к SIEM системе должно поддерживать TLS шифрование

Сервис аудита позволяет подключать к себе множество SIEM систем

Подключение SIEM системы может происходить на разных уровнях:

- Super Admin: может создать подключение для выгрузки данных в SYSLOG со всей системы Аудита
- Project Admin: имеет право подключить SIEM систему на уровне проекта и выгружать туда данные конкретного проекта

Право подключать SIEM системы будет указано в ролевой модели сервиса Аудита



Cloud: резервное копирование

Сервис Karboii (собственная разработка)

- Встроен в личный кабинет

Резервное копирование

- Виртуальных машин
- Баз данных (Платформенного сервиса DBaaS (кроме Trantool))

Автоматические и ручные бэкапы

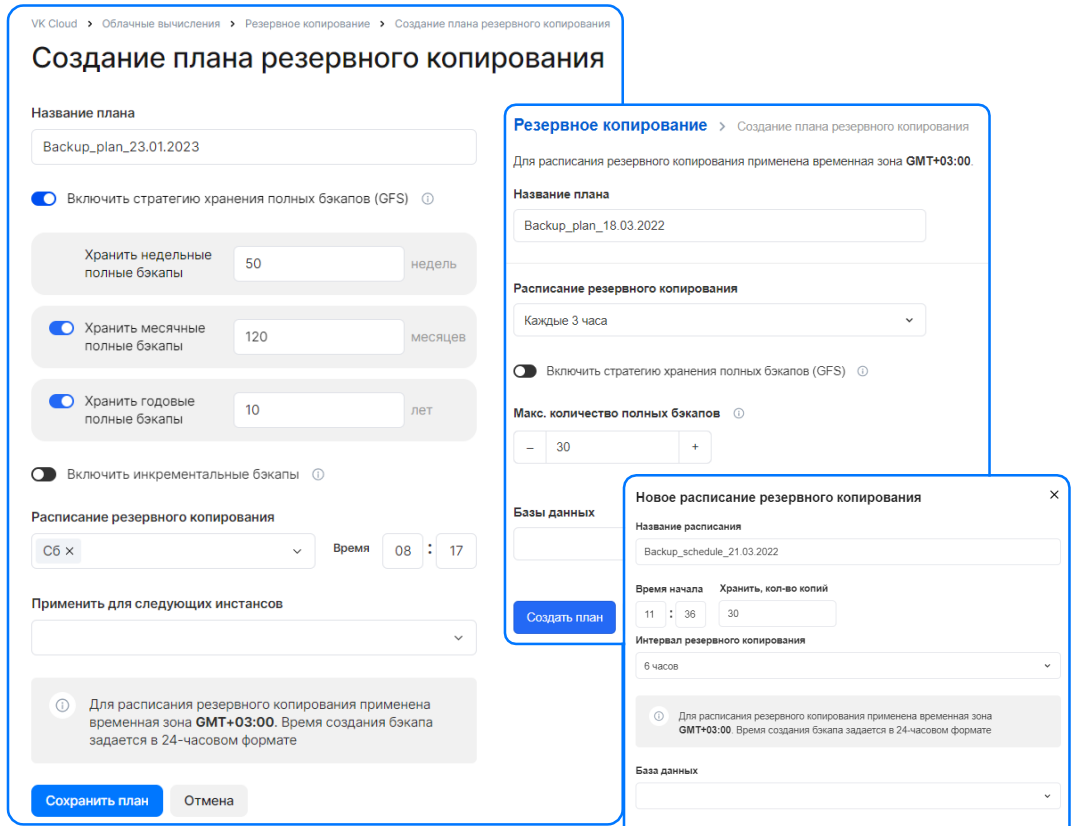
- Запуск плана в указанное время
- Недельные полные бекапы
- Ежедневные инкрементальные бекапы
- Forward Incremental Backup Retention Policy
- GFS retention policy
- Поддержка нескольких инстансов в одном плане

Восстановление

- Диска ВМ
- В исходную ВМ
- В новый инстанс

Point-in-time recovery (Postgre SQL)

Хранение в объектном S3 хранилище



Публичное облако VK Cloud

Аттестация

- 152-ФЗ УЗ1

Сертификация

- ГОСТ Р 57580.1-2017
- PCI DSS 3.2.1
- ИСО 27001, 27017, 27018 – 2Н2023

А также:

SLA 99,95%
с финансовыми гарантиями

24/7
«IT-служба одного окна»

ЦОДы Tier III,
расположение в РФ

tech

VK WorkSpace

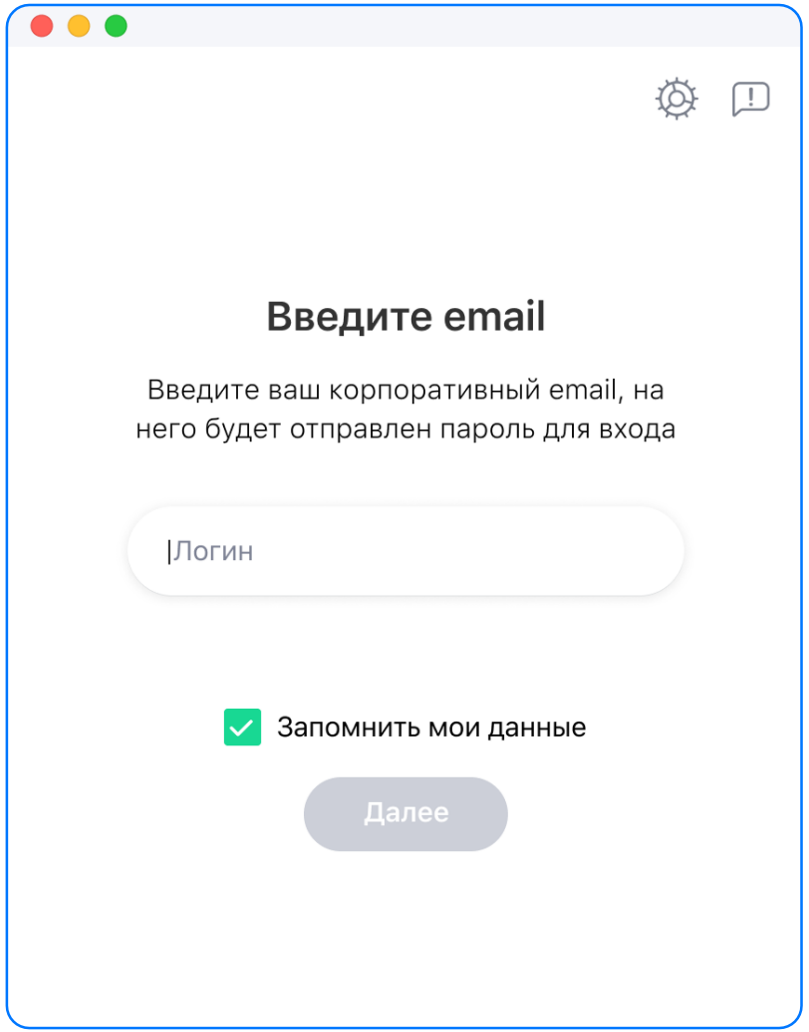
Коммуникационная платформа для бизнеса от VK включает:

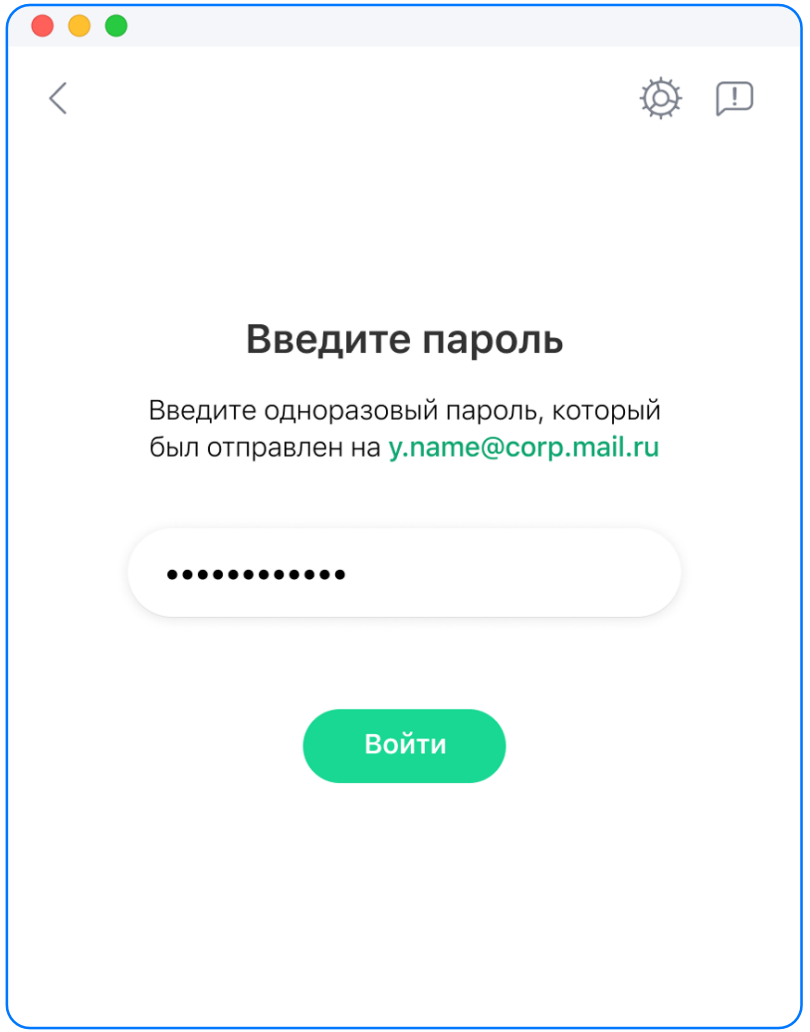
- Корпоративную почту VK WorkMail с календарем и адресной книгой.
- Мессенджер VK Teams с аудио- и видеозвонками.
- Файловое хранилище VK WorkDisk со встроенным редактором документов.

- Все сервисы находятся в едином пространстве, доступны в режиме одного окна и управляются из общей административной панели.
- У продуктов несколько независимых слоев защиты.
- Платформу можно развернуть на серверах компании (On-Premise) или использовать в облаке (SaaS).
- Входят в реестр российского ПО и отвечают требованиям ФЗ-152.

tech

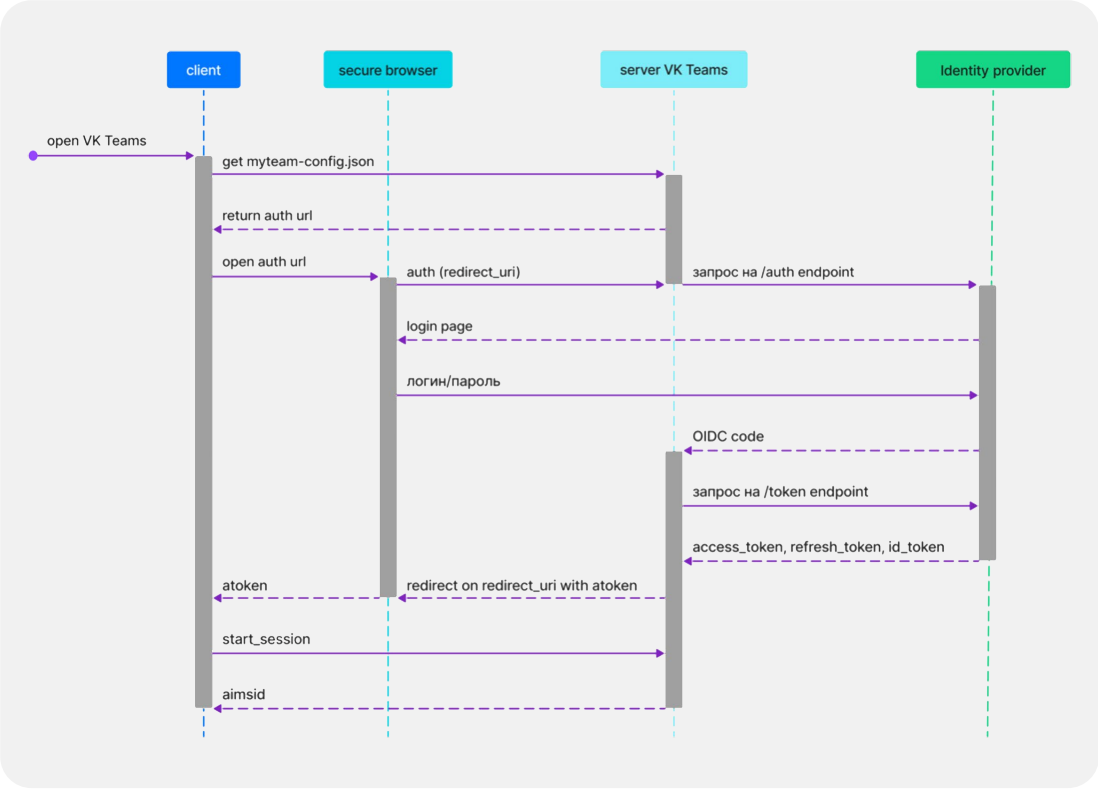
VK WorkSpace (Teams): идентификация и аутентификация





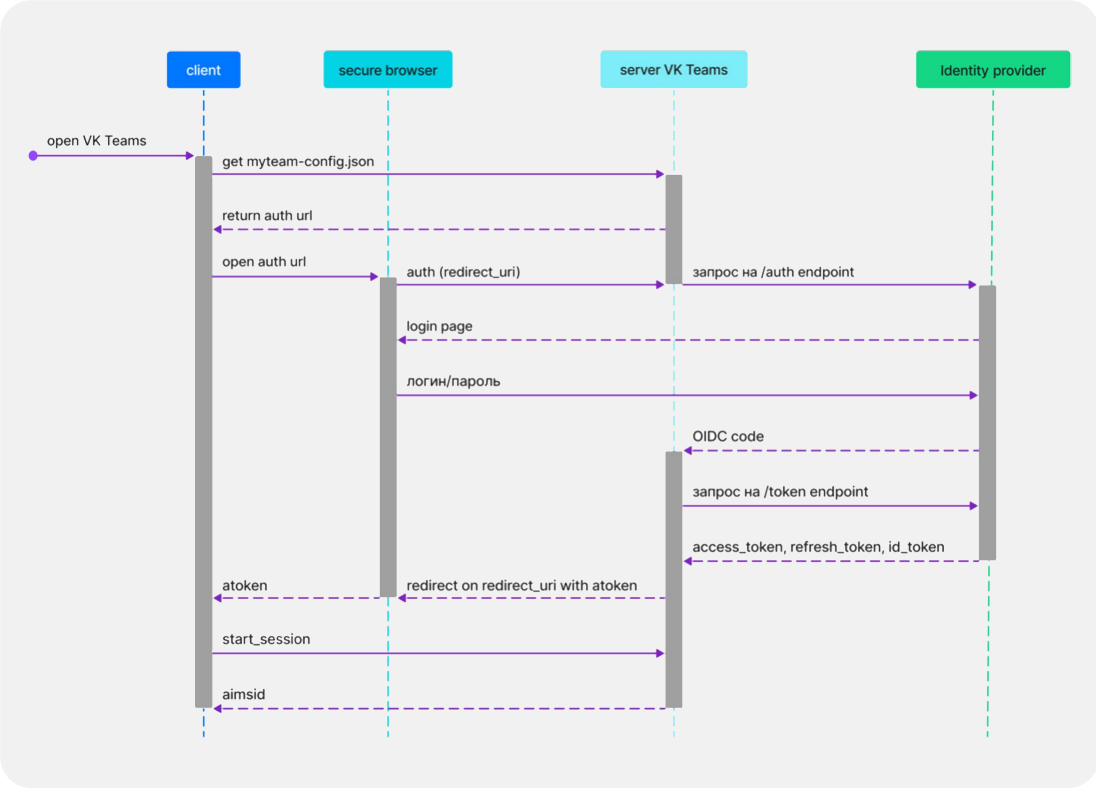
VK WorkSpace (Teams): идентификация и аутентификация

OIDC

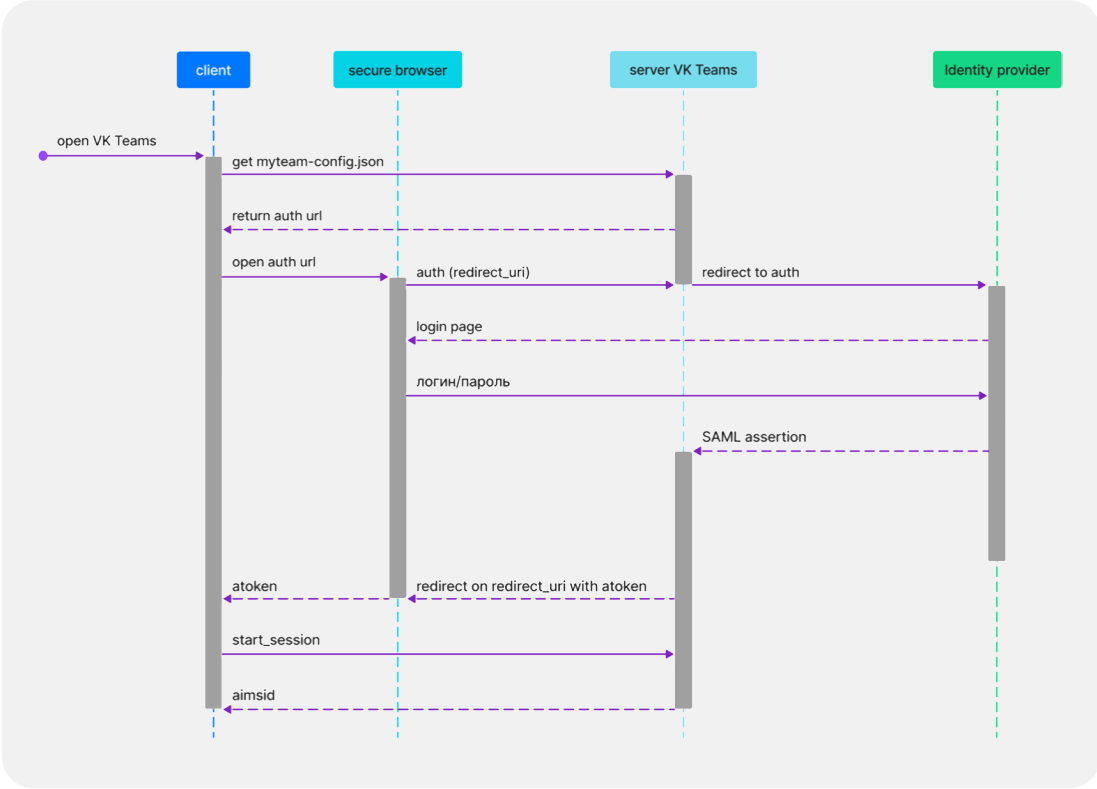


VK WorkSpace (Teams): идентификация и аутентификация

OIDC

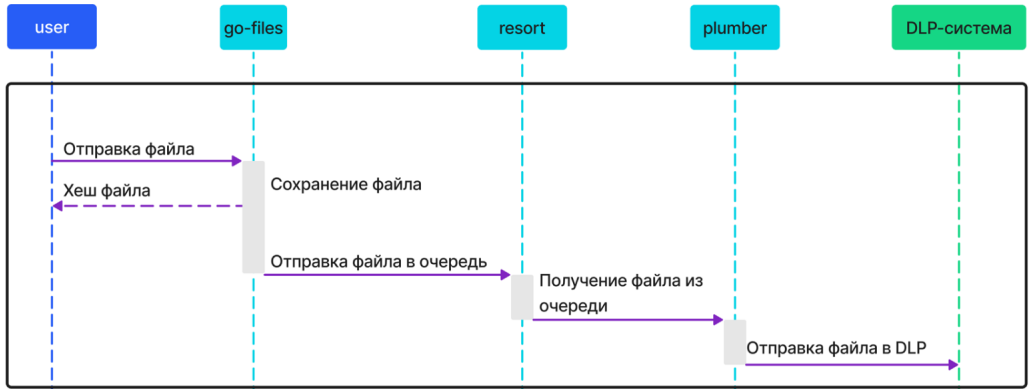


SAML

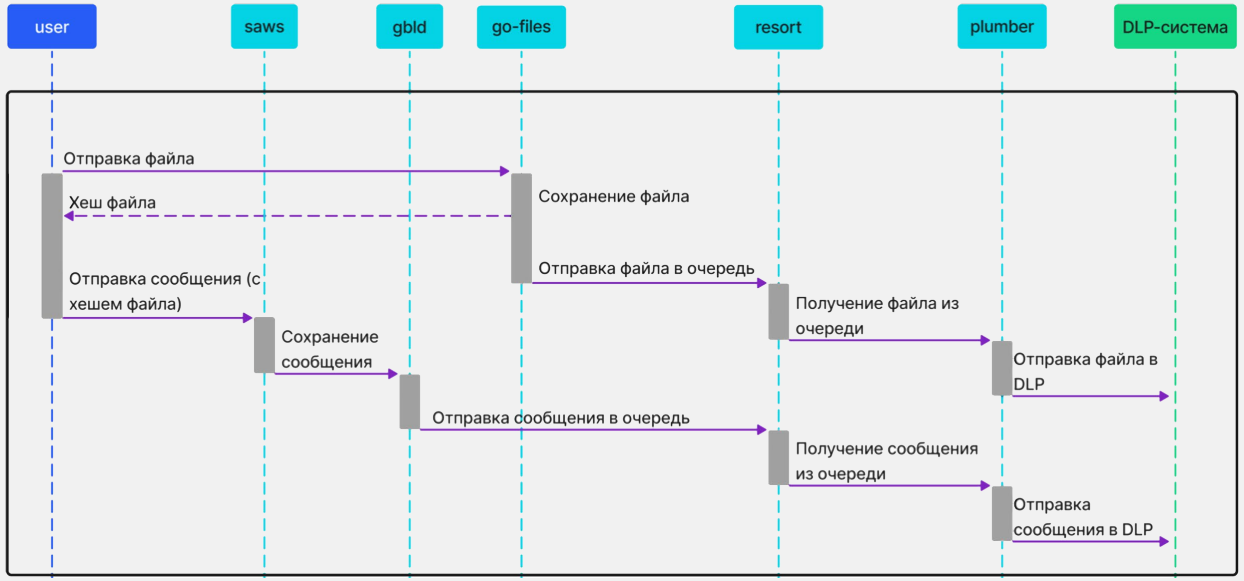


VK WorkSpace (Teams): DLP

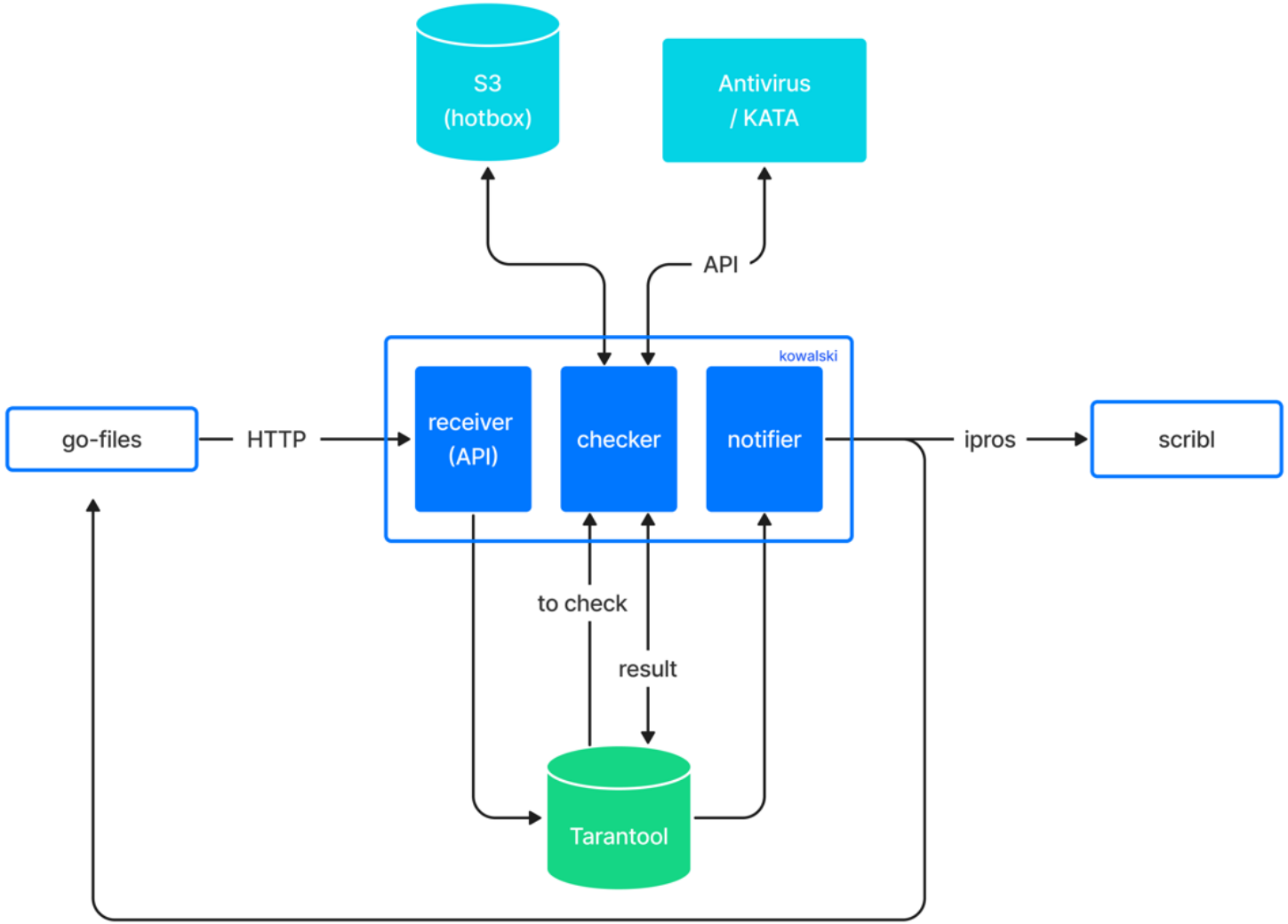
Файл



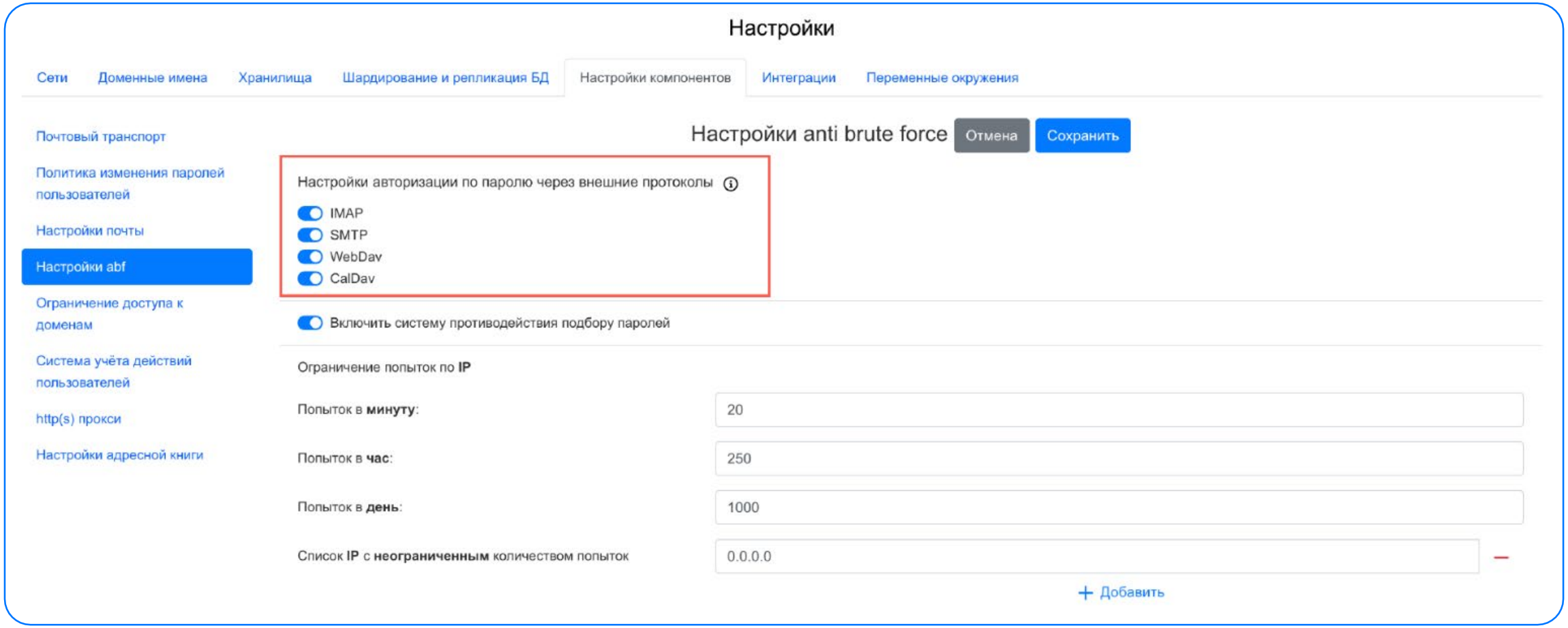
Сообщения с прикрепленным файлом



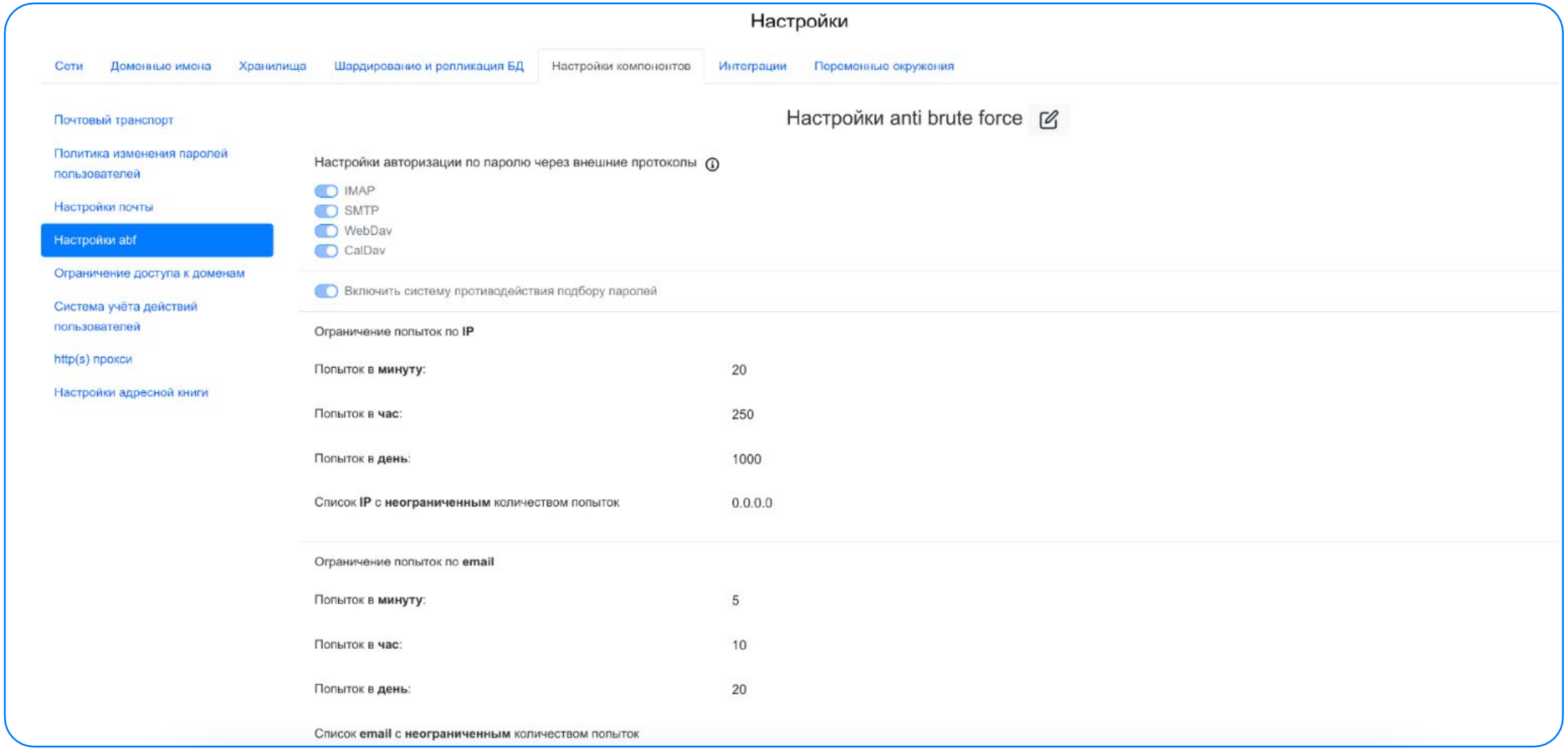
VK WorkSpace (Teams): интеграция с антивирусом



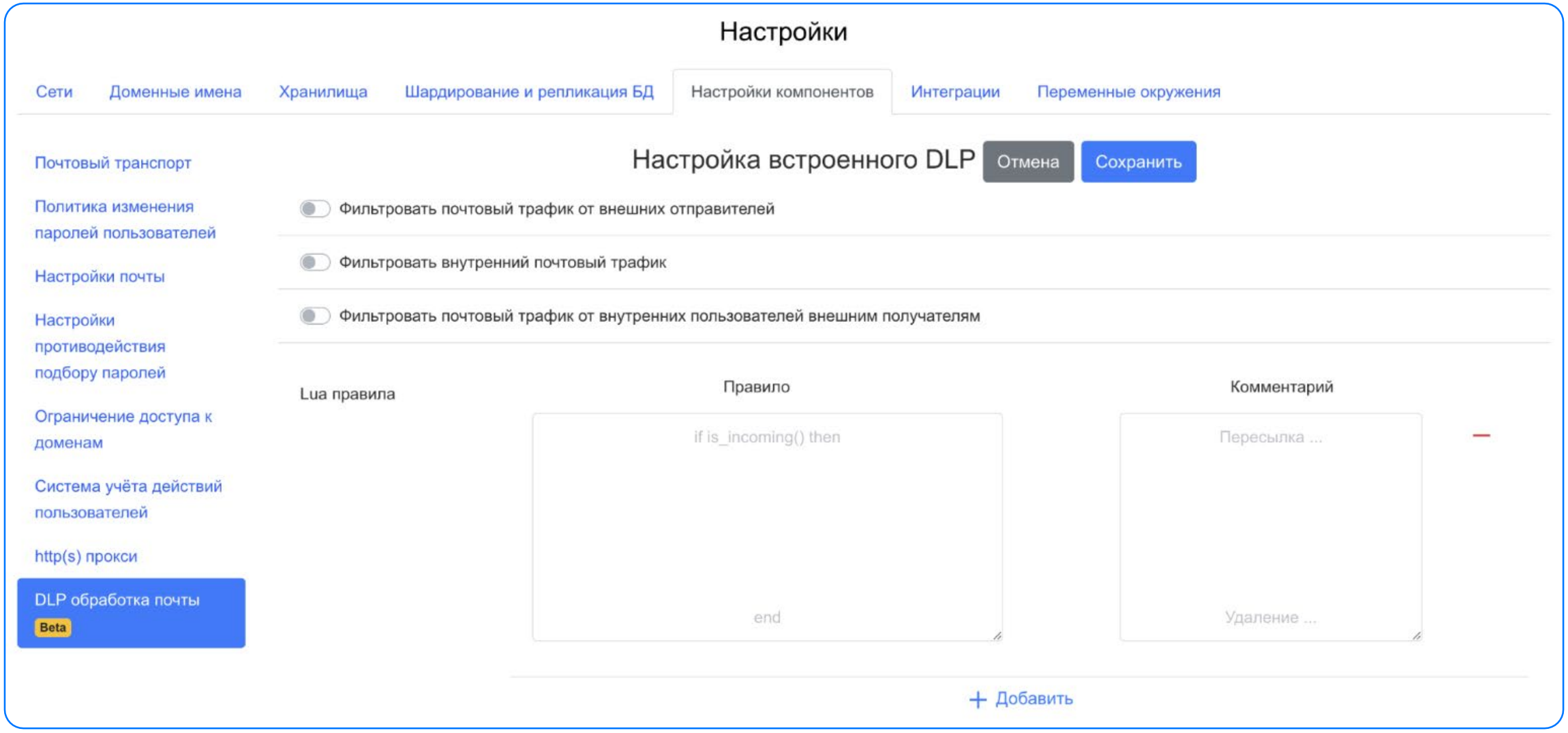
VK WorkSpace (WorkMail): идентификация и аутентификация



VK WorkSpace (WorkMail): идентификация и аутентификация



VK WorkSpace (WorkMail): DLP



VK WorkSpace (WorkMail):

Регистрация событий безопасности

Отслеживаются входы в почтовый ящик и действия, выполняемые владельцем ящика.

Записи об активности пользователей попадают в выделенное хранилище

Трассировка почтовых сообщений предусмотрена на уровне журналов journald по набору ID, присваиваемых сообщению

tech

VK WorkSpace (WorkMail): Рекомендации

VK WorkMail Security Compliance

Перечень параметров и настроек
для безопасной конфигурации

tech

tech

Сертификация

tech

Сертификация

VK Tech сертифицирует:

- ПО Tarantool Data Grid по ТУ и УД4
- ПО VK Cloud по ТУ и УД4

VK Tech готовит к сертификации :

- Объектовое хранилище S3
- Корпоративный мессенджер VK Teams
- Корпоративная почта и календарь VK WorkMail

АВТОВАЗ

Private Cloud:

Перестроили IT – ландшафт
за 3 месяца и заменили
180 приложений

Технологии:

- Managed K8s, DBaaS
- Big Data
- Load Balancing

Результаты внедрения

Миграция всех информационных систем повышенной критичности в приватное облако

Бесшовно мигрировали данные из зарубежных облаков и начали переход на новые приложения без нарушения бизнес-процессов за 3 месяца

Развернули одну зону доступности и планируем построить вторую, идентичную по мощности и набору софта для обеспечения отказоустойчивости. Это защитит информационные системы от последствий потенциальных сбоев и позволит расширить внутренний ИТ-ландшафт.

Private Cloud:

Импортонезависимый ЦОД
и среда разработки

Технологии:

- Виртуальные машины и сети
- Managed K8s, DBaaS
- СХД
- S3

Результаты внедрения

Полная импортонезависимость ЦОДа, все компоненты собраны из отечественных решений: сеть Eltex, серверы Yadro, софт Private Cloud от VK

Единый ландшафт инфраструктуры для разработки

Сокращено время на получение ИТ-ресурсов для запуска MVP с помощью Infrastructure as a Code

Оптимизировано использование мощностей за счет виртуальных машин с гиперконвергентными узлами

Разработчик-интегратор
для атомной отрасли

Private Cloud:

Защищенное облако для всех дочерних компаний с учетом специфики ядерной отрасли

Технологии:

- IaaS
- PaaS

Результаты внедрения

2 дата-центра,
создано более 150 виртуальных машин

Облачные инструменты для хранения чувствительной информации и размещения критических информационных систем, а также для разработки цифровых продуктов

Заказчик получил возможность быстро разворачивать инфраструктуру под задачи разных подразделений, обеспечивать их необходимыми инструментами и значительно экономить ресурсы

tech

Коммуникационные и облачные сервисы VK для промышленности

Можно ли?

tech

Коммуникационные и облачные сервисы VK для промышленности

Можно

tech