

Подходы и технологии для обеспечения безопасности персональных данных в облаке

Евгений Кондратьев,
Руководитель Cloud Solutions, «Неофлекс»

О КОМПАНИИ

Neoflex создает ИТ-платформы для цифровой трансформации бизнеса, помогая заказчикам получать устойчивые конкурентные преимущества.

Мы фокусируемся на заказной разработке программного обеспечения и внедрении сложных информационных систем, используя передовые технологии и подходы.

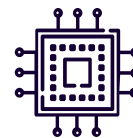
Наш отраслевой опыт и технологическая экспертиза, усиленная собственными акселераторами разработки, позволяют решать бизнес-задачи любого уровня сложности.



ОСНОВАНА
В 2005



1100+
СОТРУДНИКОВ



9 ЦЕНТРОВ
РАЗРАБОТКИ

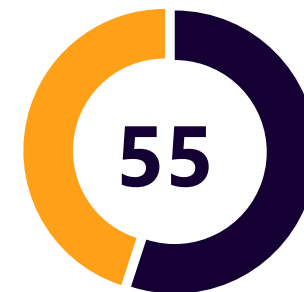
9 из **10**

Заказчиков продолжают сотрудничество с «Неофлекс» после первого проекта



Компаний из рейтинга
РБК ТОП-100

**НАМ
ДОВЕРЯЮТ**



Российских банков
из ТОП-100

ТЕМЫ

- 1 Тренды использования облаков в РФ
- 2 Вызовы хранения и обработки данных в облаках
- 3 Причины и последствия утечек данных
- 4 Как облака помогают защитить персональные данные?
- 5 Автоматизация безопасности, CSPM
- 6 Платформа для защиты облаков





ТРЕНДЫ ИСПОЛЬЗОВАНИЯ ОБЛАКОВ В РФ

△ **85%**

компаний планируют использовать облачные технологии к 2025 году

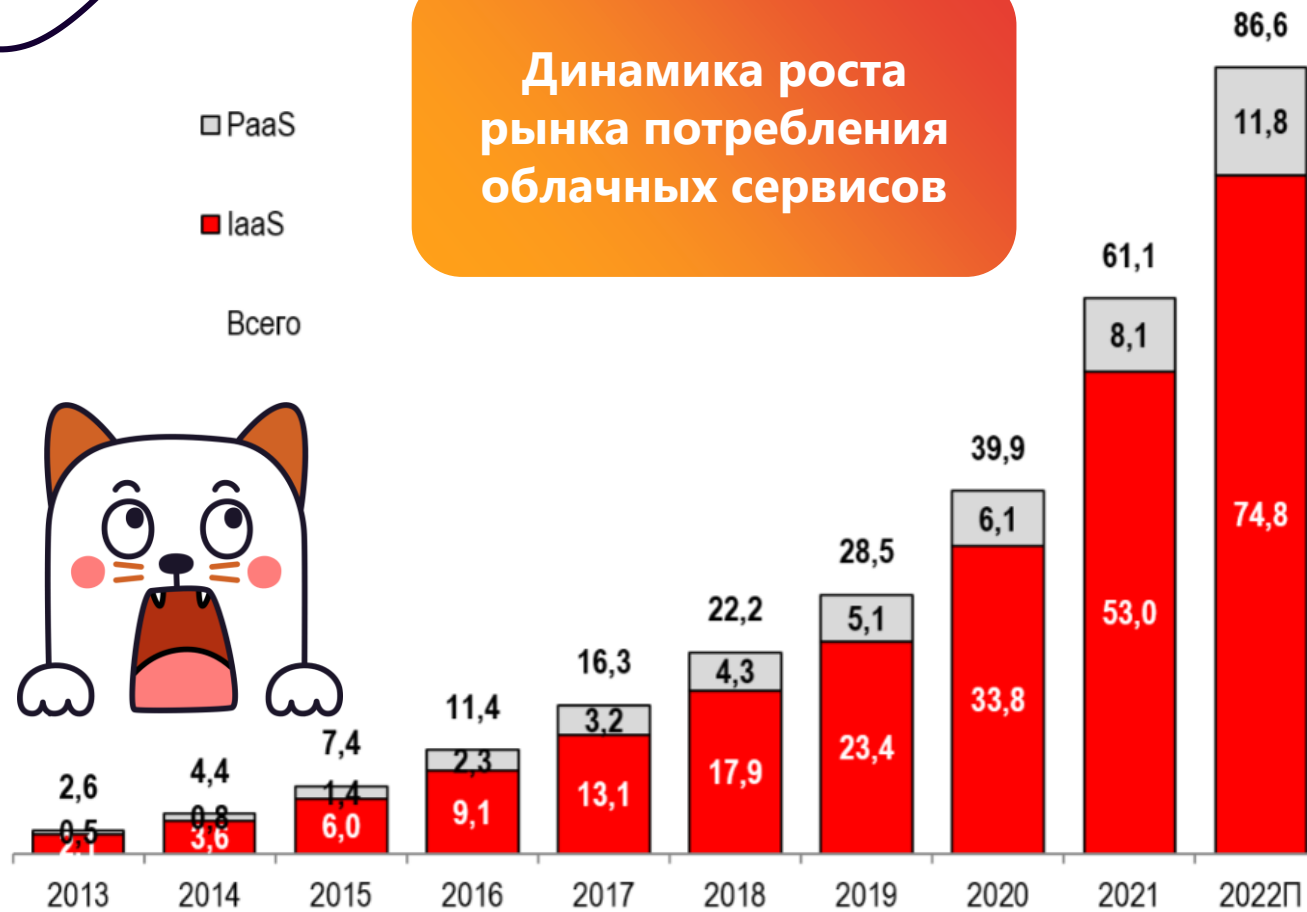
△ **40%**

в год - прогнозный темп роста рынка потребления облаков

△ **2x**




кратный рост выручки ТОП провайдеров за последний год

Динамика роста рынка потребления облачных сервисов



Источник: iKS-Consulting

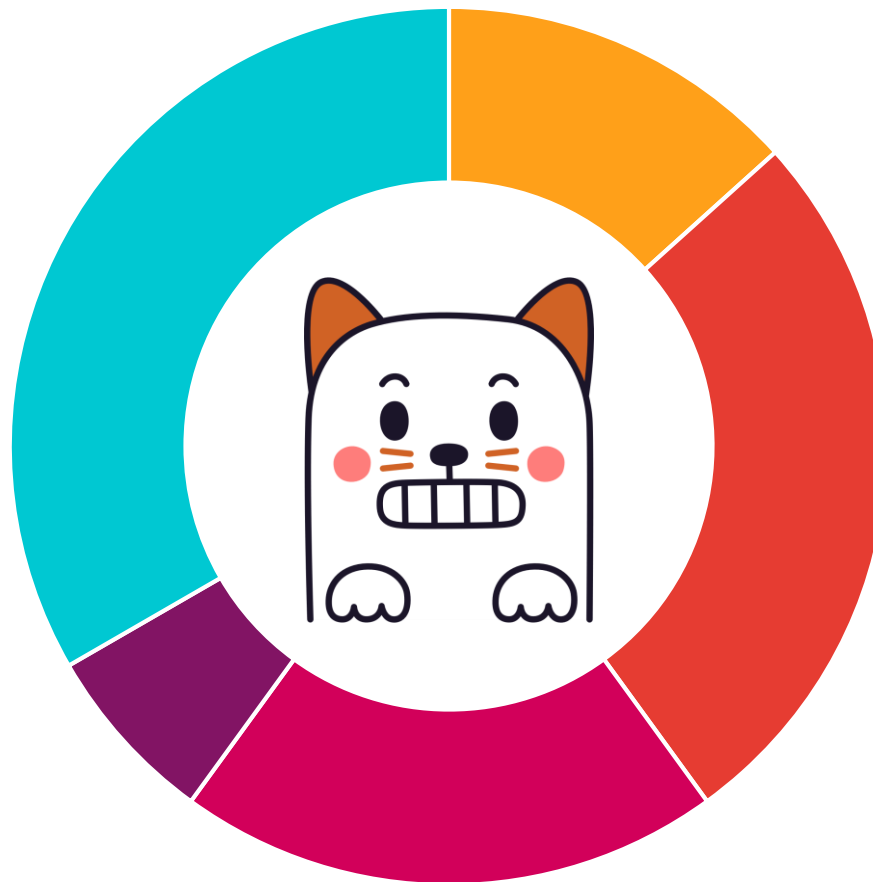
ВЫЗОВЫ ДЛЯ ИБ ПРИ ХРАНЕНИИ И ОБРАБОТКИ ДАННЫХ В ОБЛАКАХ

-  **Публичность** - риски безопасности сервисов, явно или косвенно опубликованных в интернет
-  **Приватность** – хранение данных у провайдера, а также разделение мощностей с другими пользователями
-  **Compliance** - соблюдение требования регуляторов
-  **Мониторинг изменений** – пользователи могут создавать небезопасно-skonфигурированные ресурсы
-  **Контроль доступов** – принцип минимальных привилегий





ОСНОВНЫЕ ПРИЧИНЫ УТЕЧЕК ДАННЫХ



■ Уязвимость ■ Конфигурация ■ Социальная инженерия ■ Нет данных ■ НСД

ПОСЛЕДСТВИЯ УТЕЧКИ ДАННЫХ



Юридические последствия



Урон репутации



Потеря доверия клиентов



Финансовые потери



Санкции регуляторов



ОБЛАКА ПОМОГАЮТ ИБ

1 Шифрование данных при передаче и хранении

2 Контроль и разделение прав доступа

3 Организация хранения секретов

4 Защита внешних ресурсов

5 Прозрачность и контроль изменений

6 Резервное копирование

7 Управление конфигурациями и уязвимостями

Облачные сервисы (на примере YC)

- Встроенные сервисы шифрования данных
- Key Management Service
- Certificate Manager

- IAM

- LockBox
- Vault

- Security Groups
- Anti DDoS
- WAF

- Audit Logs
- Cloud Monitoring

- Cloud Backup

- CSPM
- Cloud Protection Platform



ОБЛАКА ПРЕДОСТАВЛЯЮТ ТЕХНИЧЕСКИЕ СТАНДАРТЫ БЕЗОПАСНОСТИ

Стандарт по защите облачной инфраструктуры Yandex Cloud 1.1

Статья создана  Yandex Cloud

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.

Структура стандарта

Стандарт описывает рекомендации для следующих задач обеспечения безопасности:

- Аутентификация и управление доступом.
- Сетевая безопасность.
- Безопасная конфигурация виртуальной среды.
- Шифрование данных и управление ключами.
- Сбор, мониторинг и анализ аудитных логов.
- Управление уязвимостями.
- Резервное копирование.
- Физическая безопасность.
- Защита приложений.

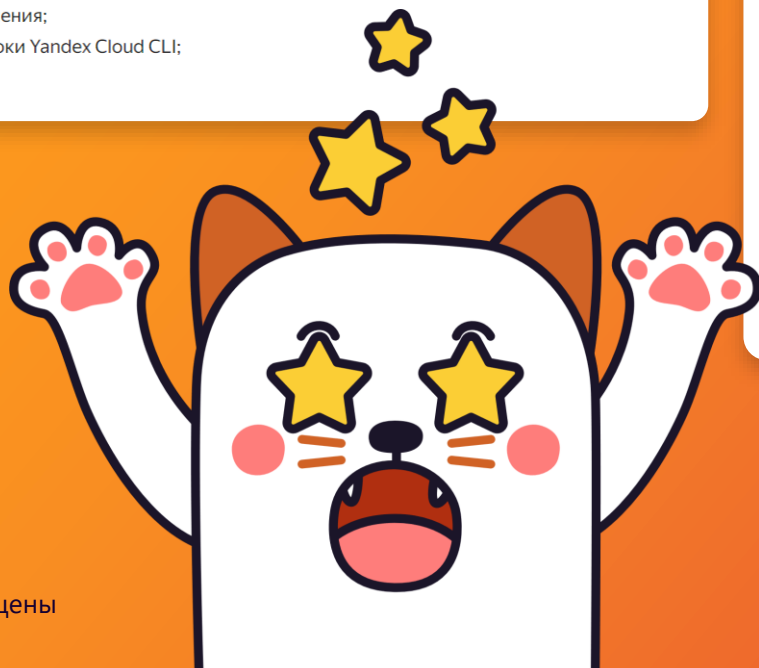
Требования и подготовка

Для проверок убедитесь, что

- установлен и настроен YC CLI по [инструкции](#);
- вы вошли в [консоль управления](#);
- установлена утилита jq.

Вы можете автоматизировать аудит выполнения всех рекомендаций с помощью доступных решений наших партнёров:

- [Neocat](#) — продукт для управления безопасностью в облаке от компании Неофлекс. Устанавливается изолированно в периметре облака пользователя без необходимости выдачи административных прав.





Как выявить риски ИБ в облачной инфраструктуре?

Проводить периодический аудит

Анализировать параметры конфигураций вручную

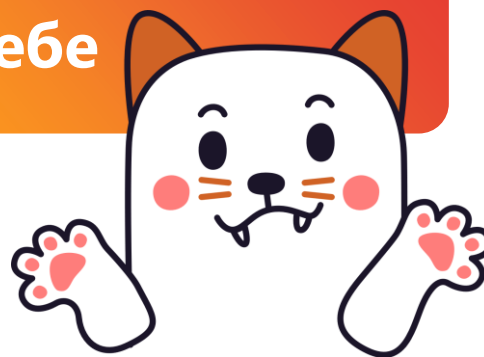
Нет!



Использовать IaC-подход

Проверять код инфраструктуры перед развёртыванием, сверяясь со стандартами

Такое себе



Использовать современные технологии и продукты

Автоматизировать управление безопасностью

Да!





CSPM

Cloud security posture management

Это упреждающий подход к обеспечению ИБ путём автоматического анализа ресурсов в облаках

- Непрерывное выявление и приоритизация рисков
- Обеспечение соответствия инфраструктуры требованиям и стандартам безопасности, таким как:

Yandex Cloud Security

152-ФЗ

PCI DSS

CIS

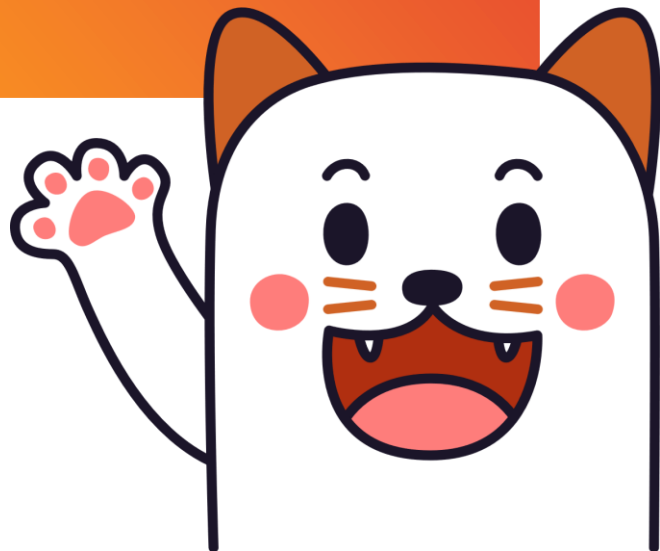
и т. д.



Область действия

- Аутентификация и управление доступом
- Сетевая безопасность
- Безопасная конфигурация ресурсов
- Шифрование данных и управление ключами
- Аудит критических событий ИБ
- Управление уязвимостями
- Резервное копирование

ЗАРУБЕЖНЫЕ ВЕНДОРЫ CSPM



Google Cloud

PRISMA[®]
BY PALO ALTO NETWORKS

Check Point
CloudGuard

Azure

TREND
MICRO

aqua

orca
security

aws

NEOCAT CLOUD PROTECTION PLATFORM

Intelligence Security

NeoCAT позволяет комплексно защищать облачную инфраструктуру и приложения в режиме единого окна



Развертывание
и запуск < 15 мин



Непрерывный мониторинг новых
угроз безопасности



Анализ рисков всех слоёв
инфраструктуры и сервисов



Контроль пользовательских
привилегий



Обнаружение и анализ новых
ресурсов в облаке



Приведение облака в соответствие
с требованиями регуляторов



NeoCAT

**УПРАВЛЯЙТЕ
БЕЗОПАСНОСТЬЮ ОБЛАКА**

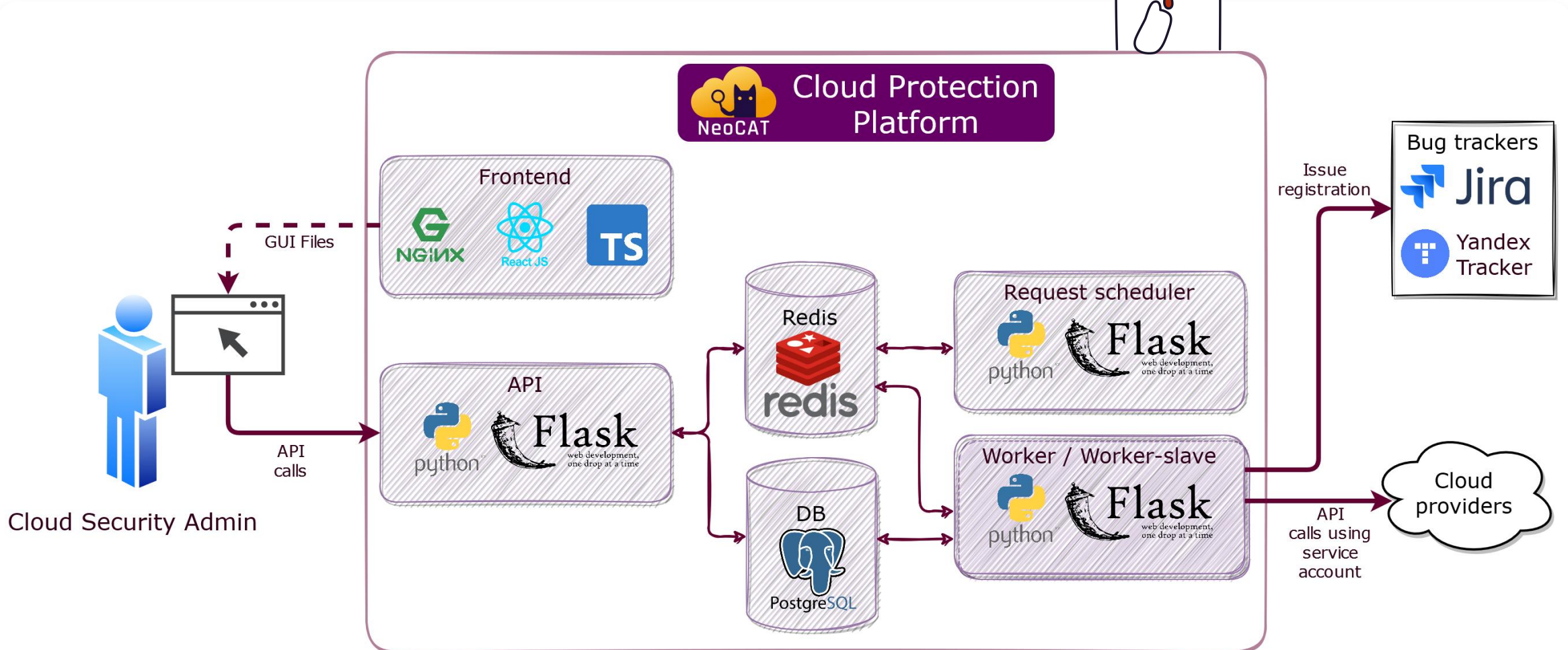
- ВЫЯВЛЕНИЕ РИСКОВ
- ПРИОРИТИЗАЦИЯ
- УСТРАНЕНИЕ
- ПРЕДОТВРАЩЕНИЕ

БИЗНЕС-ЗАДАЧИ, РЕШАЕМЫЕ НЕОСАТ

- ✓ Снижение рисков простоя бизнеса в связи с отказом работы инфраструктуры либо её уничтожением
- ✓ Предотвращение репутационных и финансовых рисков в связи с утечкой данных
- ✓ Соблюдение требований законодательства и регуляторов в части безопасности
- ✓ Устранение рисков нарушения коммерческой тайны и кражи интеллектуальной собственности

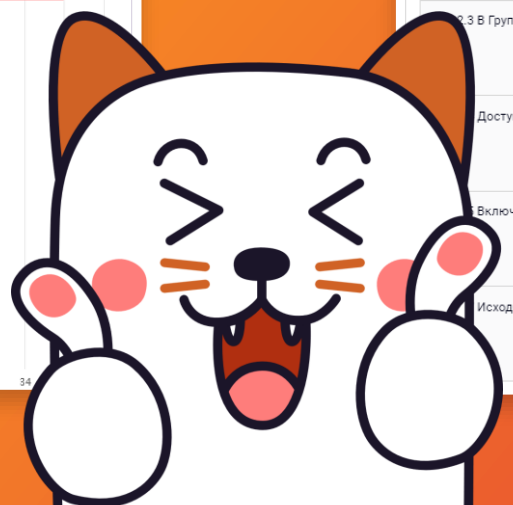
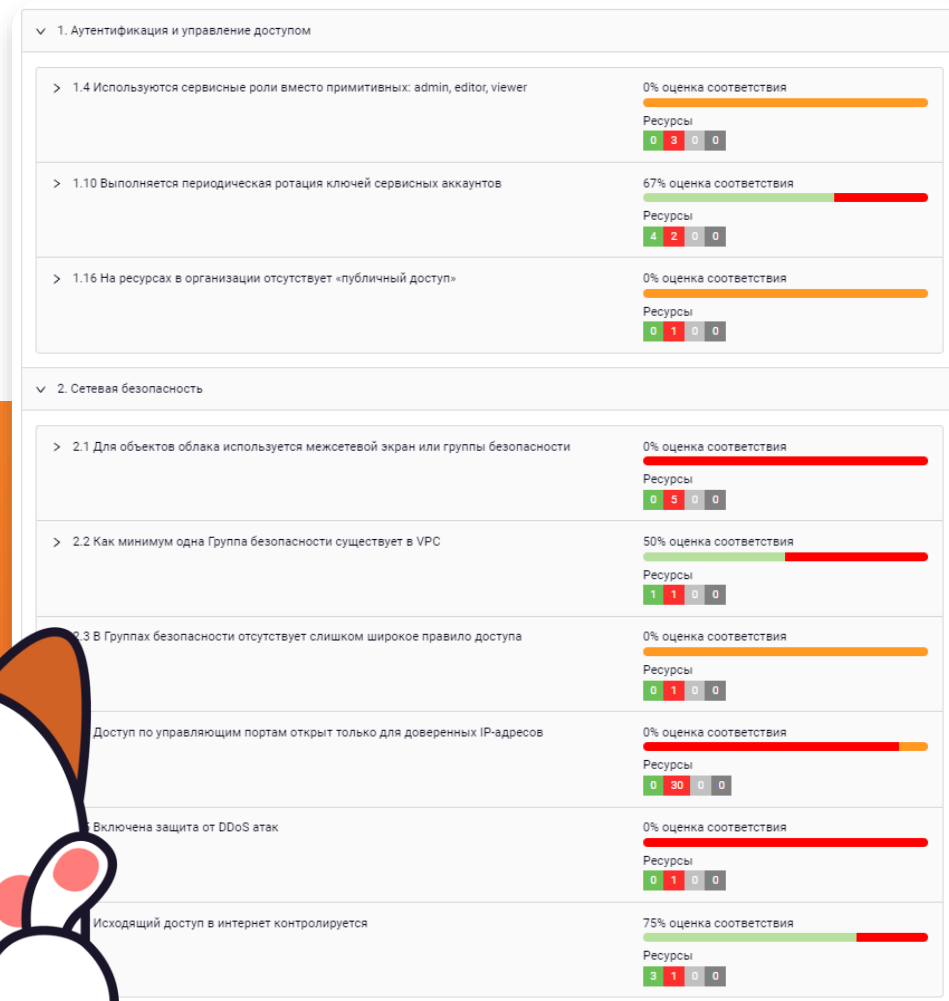
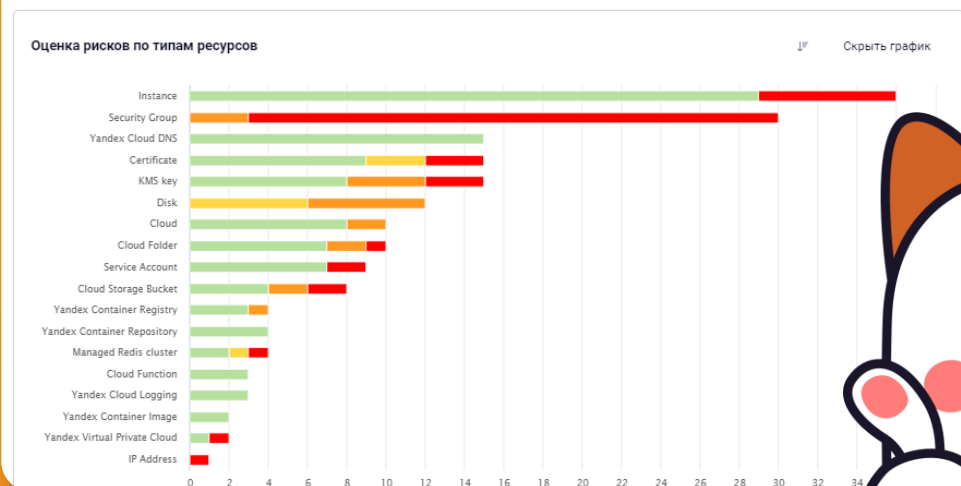
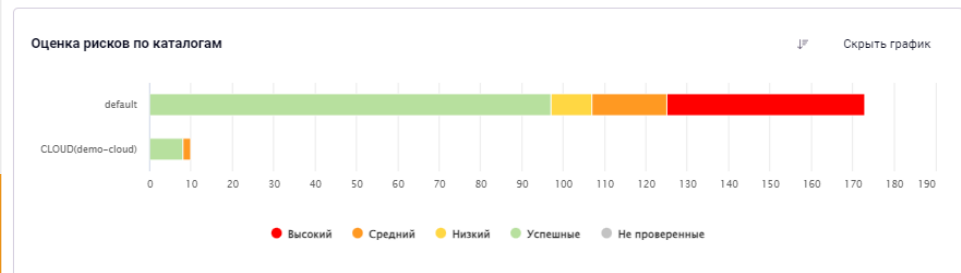
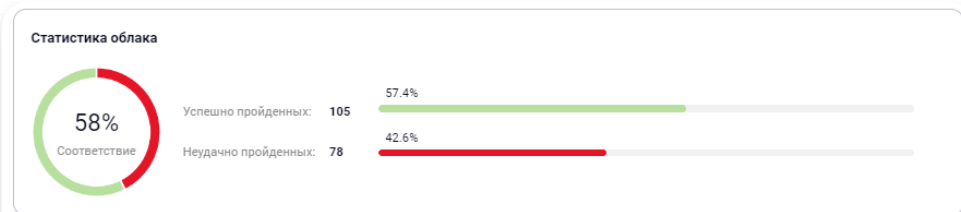


АРХИТЕКТУРА NEOCAT





НЕОСАТ ПОДДЕРЖИВАЕТ СТАНДАРТ YANDEX CLOUD SECURITY

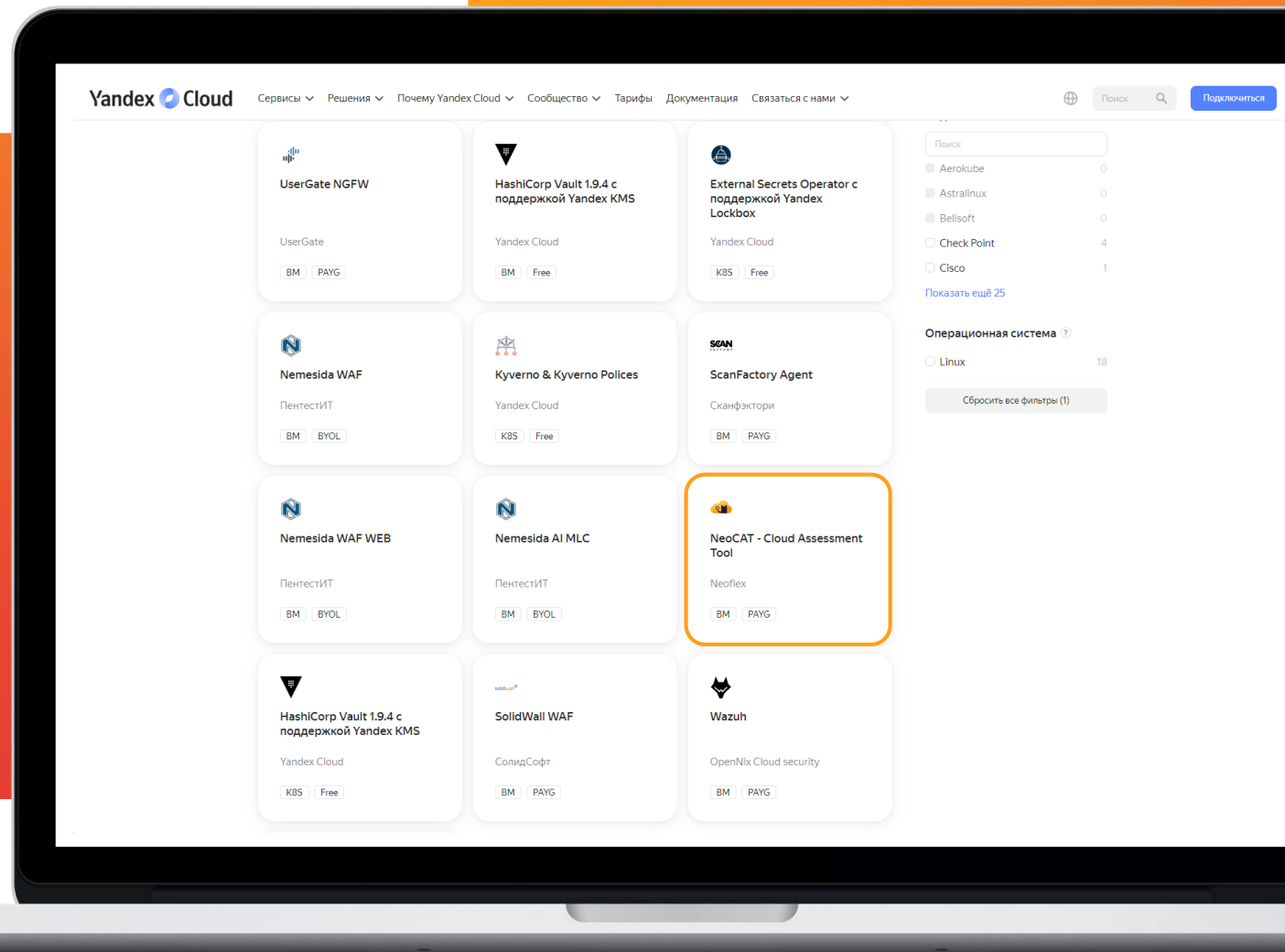


ЛЕГКО И БЕЗОПАСНО ЗАПУСКАЕТСЯ В ВАШЕМ ОБЛАКЕ



НеоСАТ разворачивается за 10 мин из маркетплейса Yandex Cloud

- Устанавливается на отдельную VM
- Не требует стороннего ПО
- Не требует лицензий
- Не передаёт ваши данные за пределы облака
- Не требует установки агентов
- Нет необходимости заключать договор с вендором

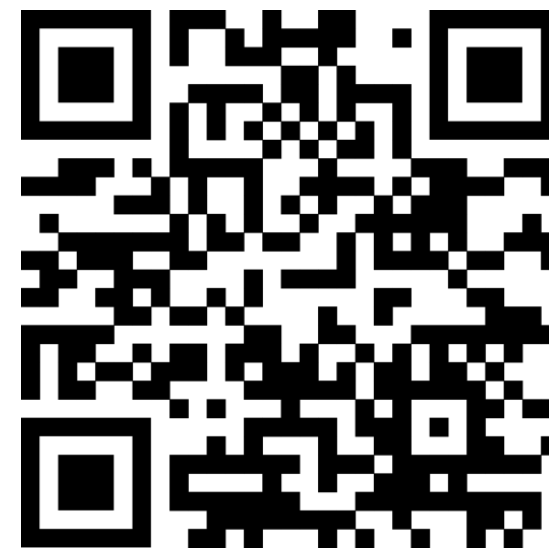




NeoCAT

БОНУС ПЕРВЫМ 10 УЧАСТНИКАМ

**Бесплатная помощь в устранении
рисков, выявленных NeoCAT**



neocat.cloud

**СПАСИБО
ЗА ВНИМАНИЕ!**



Кондратьев Евгений

Лидер продукта NeoCAT

ekondratev@neoflex.ru