tech

Мультиоблако и кибербез: как защищать распределенную инфраструктуру в 2025

Погоржельский Станислав

Технологический евангелист VK Cloud, VK Tech

От чего будем защищать?

Общие тренды ИнфоБез РФ

Безопасность Инфраструктуры из облака всегда выше в сравнении с локальной*

* По мнению технологического евангелиста VK Tech

tech

VMware под Broadcom

License Portability (переносимость лицензий VCF)
Введена переносимость подписок VCF: клиент покупает подписку VCF у Broadcom и может «переносить» её между on-prem и поддерживаемыми облаками.

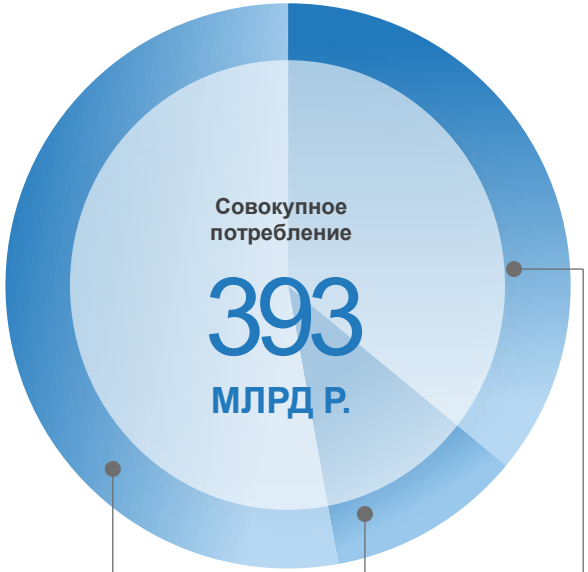
Всё будет как раньше?

*информация из интернета

Закрытие текущей программы VCSP/Advantage
– Broadcom объявляет закрытие Broadcom Advantage Partner Program for VMware Cloud Service Provider (VCSP) 31 октября 2025.
– С 1 ноября 2025 старая VCSP-модель прекращает работу, партнёры не могут увеличивать коммит и привлекать новый бизнес по старой схеме.

Не много аналитики

Совокупное потребление облачных сервисов в РФ (все типы развертывания) в 2024 году по сегментам



SaaS
208 МЛРД Р.
52,8%

PaaS
44 МЛРД Р.
11,2%

IaaS
141 МЛРД Р.
36%

Рыночное и внутреннее потребление облачных сервисов (все типы развертывания) в 2024 году по сегментам

Рыночное потребление

346

МЛРД Р.

* Источник: AHD, 2025

Объем рынка публичных облачных сервисов

Российский рынок публичных облачных сервисов в 2024 году

SaaS
201 МЛРД Р.
66%

PaaS
29 МЛРД Р.
9%

IaaS
74 МЛРД Р.
25%

* Источник: AHD, 2025

Мировой рынок публичных облачных сервисов в 2024 году

SaaS
$483
60%

IaaS
$161
20%

PaaS
$161
20%

Источник: IDC, 2024

Наблюдения по структуре российского рынка

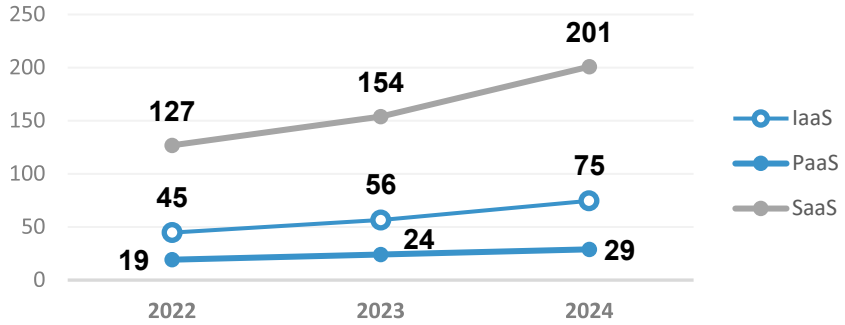
Основную долю российского рынка - 66%, составляет сегмент SaaS.
Это соответствует доле сегмента SaaS на мировом рынке Public cloud.

Сегмент инфраструктуры (IaaS) в РФ более чем вдвое превышает по объему сегмент PaaS, что отличает российский рынок от глобального рынка публичных облачных сервисов, где эти сегменты близки по объему.

Динамика рынка публичных облачных сервисов в 2022-2024

- С 2022 по 2024 год общий объем российского рынка публичных облачных сервисов рос с среднегодовым темпом (CAGR) 26%, увеличившись с 190.7 млрд. руб. в 2022 году до 304.4 млрд. руб. в 2024 году.
- В сегменте IaaS отмечался самый быстрый среднегодовой темп роста – 29%. Доступные мощности ЦОД и развитая инфраструктура связи позволили российским провайдерам в 2022-2023 г. оперативно занять рынок, освободившийся с уходом иностранных провайдеров. Возникшие проблемы с логистикой ИТ-оборудования также способствовали ускорению миграции российских компаний в IaaS.
- Темп роста рынка в сегментах PaaS и SaaS оказался несколько ниже, составив 23% и 26% соответственно. Причиной является уход с российского рынка иностранных поставщиков, занимавших существенную долю рынка в сегментах PaaS и SaaS. Российские поставщики до настоящего времени не смогли предложить качественной замены для многих ведущих продуктов в этих сегментах. Распространение пиратства ПО также сдерживает рост рынка в этих сегментах.

Динамика российского рынка публичных облачных сервисов в 2022–2024 годы, млрд руб.



	2022	2023	2024	CAGR, %
IaaS	44.7	56.5	74.6	29%
PaaS	19.2	24.0	28.9	23%
SaaS	126.8	153.9	200.9	26%
Total:	190.7	234.3	304.4	26%

* Источник: AHD, 2025

Динамика рынка IaaS в 2022-2024 годы

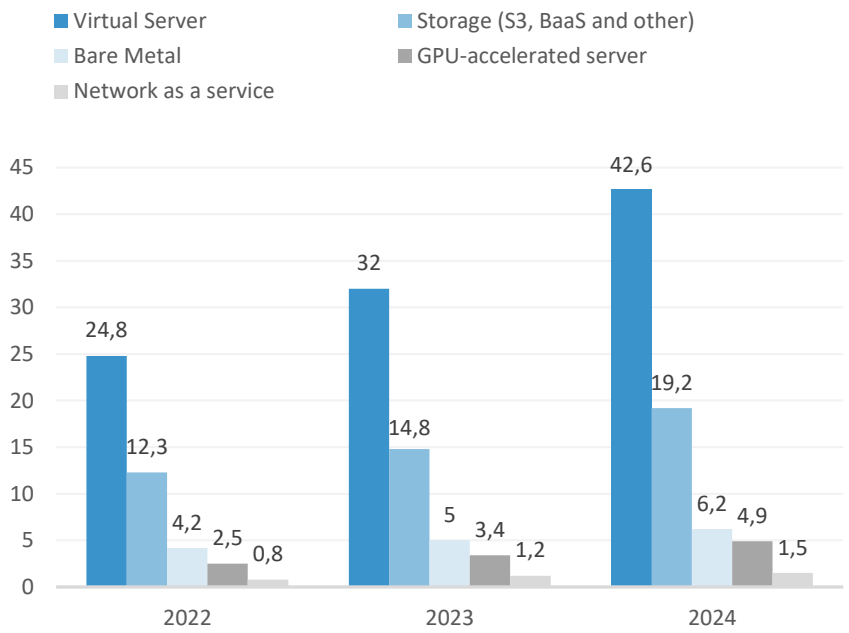
С 2022 по 2024 год российский рынок публичных IaaS рос с среднегодовым темпом (CAGR) 29.2%, увеличившись с 44.6 млрд. руб. в 2022 году до 74.4 млрд руб. в 2024.

Самый быстрый темп роста показал подсегмент GPU-accelerated server, CAGR в период с 2022 по 2024 годы составил 39.3%. Спрос на облачные вычисления с GPU связан с широким внедрением AI / ML сервисов, а также с логистическими сложностями в покупке серверов с GPU.

Вместе с тем нагрузки, требующие серверов с ускорителями, пока не постоянны и часто связаны с этапом разработки и обучения моделей заказчиками.

Высокий темп роста, CAGR более 30%, с 2022 по 2024 годы показал Virtual Server – отчасти благодаря уходу основных поставщиков ИТ оборудования, росту цен и сложности приобретения и поддержки импортного ИТ оборудования.

Динамика российского рынка публичных IaaS в 2022-2024 годы, млрд руб.



* Источник: AHD, 2025

Динамика рынка PaaS в 2022-2024 годы

С 2022 по 2024 год российский рынок публичных PaaS рос с среднегодовым темпом (CAGR) 22.8%, увеличившись с 19.2 в 2022 году до 28.9 млрд руб. в 2024.

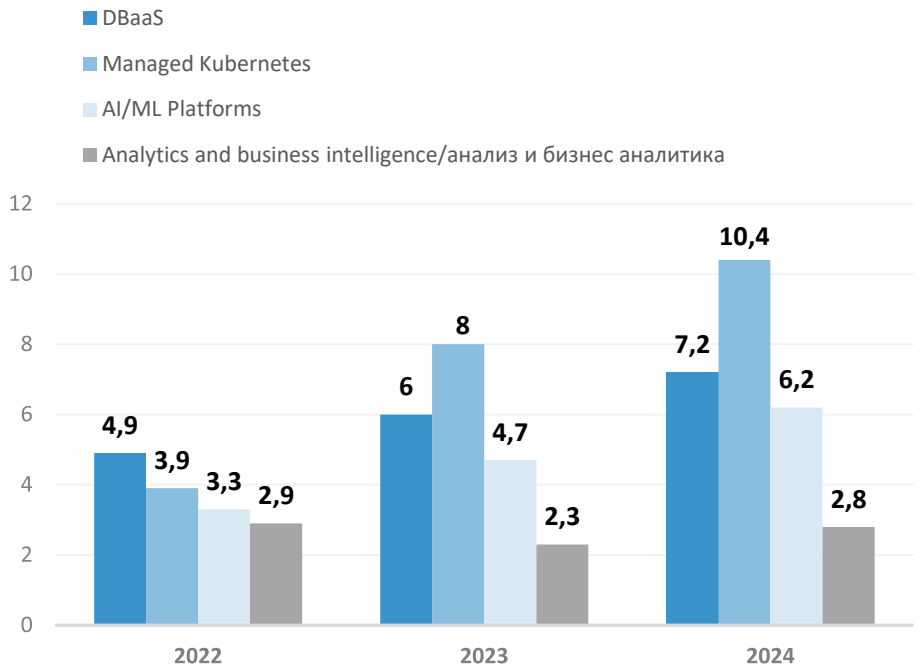
Быстрый темп роста (с низкой базы) показал подсегмент Managed Kubernetes, CAGR в период с 2022 по 2024 годы составил 63%.

Среднегодовой темп роста AI/ML платформ в этот период составил 32.2%

Среднегодовой темп роста DBaaS составил 20.4%.

На динамику сегмента PaaS в 2022-2024 годы негативное влияние оказал уход ведущих поставщиков платформ разработки, интеграции, обеспечения качества и управления жизненным циклом ПО. Восстановления на этих функциональных рынках не произошло, поскольку российские провайдеры не смогли предложить функциональных и качественных альтернативных решений.

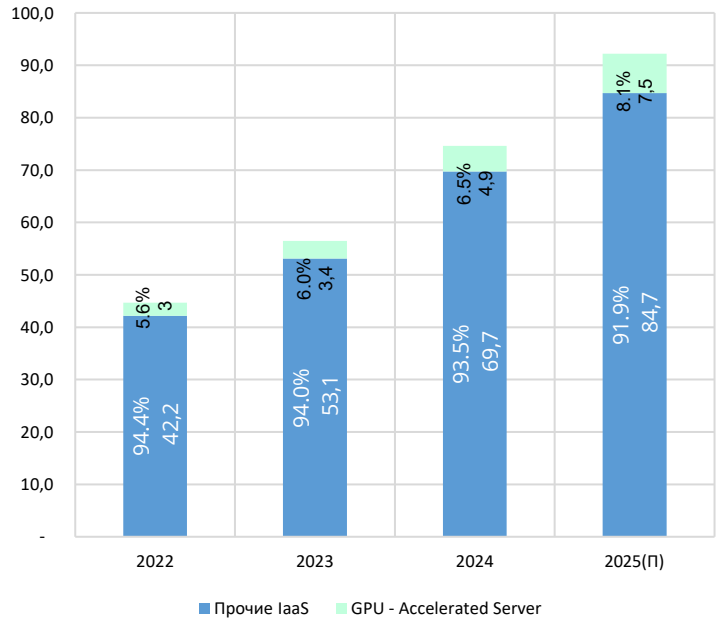
Динамика российского рынка публичных PaaS в 2022-2024 годы, млрд руб.



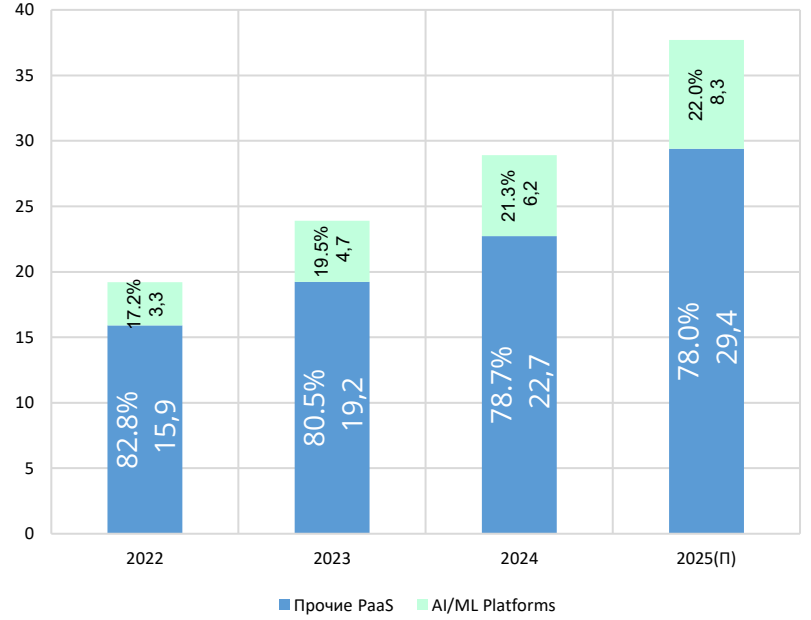
* Источник: AHD, 2025

Влияние AI на рынок публичных облачных сервисов

Объем рынка IaaS в 2022-2024 годы и прогноз на 2025 год, млрд. руб. и доля серверов с GPU, %



Объем рынка PaaS в 2022-2024 годы и прогноз на 2025 год, млрд. руб. и доля AI/ML платформ, %



ИБ, которая влияет на большинство!

tech

Основные федеральные законы ПДн

152-ФЗ «О персональных данных» 27.07.2006

Определяет ПДн/оператора/обработку; права субъектов; основания и принципы обработки; трансграничную передачу; уведомление; локализацию баз (ч.5 ст.18)

149-ФЗ «Об информации, ИТ и о защите информации» 27.07.2006

Общие принципы защиты информации и обязанности владельцев/операторов ИС (в т.ч. ИСПДн)

242-ФЗ от 21.07.2014 Поправки про локализацию

Внёс в 152-ФЗ требование локализации при сборе ПДн через интернет (ч.5 ст.18)

572-ФЗ (29.12.2022) — о биометрических ПДн и ЕБС

Устанавливает правила идентификации/аутентификации по биометрии (ЕБС), обработку биометрических ПДн вне ЕБС

187-ФЗ «О безопасности КИИ» 26.07.2017

Требования по обеспечению безопасности для значимых объектов КИИ; распространяется на операторов-субъектов КИИ, если их ИС обрабатывают ПДн

Обработка ПДн и соблюдение 152-ФЗ — с сентября 2025

- Локализация: БД/бекапы/DR — только в РФ
- Согласие — отдельный документ
- Логи и мониторинг — неизменяемое хранение
- Облачный контур — УЗ1/К1 4 УД
- Штрафы (сент. 2025)
  - ИП/юрлица — до 15–20 млн ₽
  - Самозанятые — до 500 тыс ₽

- Обезличивание по приказу РКН №140
  - Передача обезличенных данных в ГИС — по требованию
  - Уведомление об инциденте: 24/72 ч

01.09.2025

tech

Основные инсайты от клиентов

tech

Что говорят клиенты из облака
Ключевые тренды

Базовые сервисы важнее инноваций

Фокус на стабильной
инфраструктуре и платформе

Безопасность
на первом месте

Без сертификатов и защиты не работаем

Гибридная инфраструктура

Управление собственными
серверами и облаком вместе

DevSecOps окупается

Проверка безопасности при каждом изменении
кода экономит миллионы

Финансовый контроль

Отслеживание расходов
в реальном времени

Безопасный инсайт: безопасность определяет выбор провайдера

Изолированные VPC/VLAN

Сегментация сети
для разных уровней данных

WAF + Anti-DDoS

Базовая защита web-приложений

S3 с WORM и Object Lock

Неизменяемые бэкапы
для защиты от ransomware

Резервное копирование

Автоматические бэкапы
с хранением в другом ЦОД

Логирование и аудит

Полная история действий
для расследования инцидентов

Безопасность стала приоритетом №1"
После ужесточения требований регуляторов мы в первую очередь смотрим на compliance-сертификаты провайдера. Наличие услуг на базе решений
с аттестацией ФСТЭК — это уже
не конкурентное преимущество,
а базовое требование для работы с облаком

— CISO федерального ритейлера

Гибридный инсайт: единое управление распределенной инфраструктурой

VMware/OpenStack совместимость

Миграция VM между on-premise и cloud без изменений (MIND/HYSTAX)

Site-to-Site VPN / Direct Connect

Защищенная связность между площадками

Единая консоль управления

Мониторинг и управление всей инфраструктурой

Унифицированный биллинг

Консолидированная отчетность по всем ресурсам

Cross-platform бэкапы

Резервное копирование между on-premise и cloud

Гибридное облако — это не мода, а необходимость

У нас есть системы, которые по закону должны стоять on-premise, но хочется облачную гибкость. Hybrid Cloud Management позволяет управлять всем из одного окна — это критично, когда у тебя 5 ЦОДов и 3 облака

— ИТ-директор производственной компании

Инсайт разработчика: безопасность на каждом этапе разработки

Security Gate

Комплексная проверка кода, зависимостей и конфигураций в CI/CD pipeline

Managed Kubernetes с Falco

Runtime security для обнаружения аномального поведения контейнеров

Aqua/Lantry как K8s дополнение

Сканирование образов, runtime protection, compliance проверки

Cloud-native SAST/DAST

Проверка исходного кода и работающих приложений прямо в облачной среде

DevSecOps экономит миллионы на устранении уязвимостей

Раньше безопасность проверялась перед релизом, теперь — на каждом коммите. Стоимость исправления критической уязвимости на проде в 100 раз выше, чем на этапе разработки. За год сэкономили около 15 млн рублей только на предотвращении инцидентов.

— CTO финтех-стартапа

Инсайт экономиста: прозрачность расходов меняет подход к бюджетированию

Поминутная тарификация

Оплата только за фактическое использование ресурсов

Биллинг с детализацией

Разбивка затрат по проектам, командам, тегам

Budget Alerts

Уведомления при превышении заданных лимитов расходов

Reserved Instances & Savings Plans

Скидки до 40% при долгосрочных коммитментах

Auto-shutdown policies

Автоматическое выключение dev/test окружений в нерабочее время

Переход на поминутную тарификацию и детальный биллинг сэкономил нам 30% облачного бюджета

Мы видим расходы по каждому сервису в реальном времени и можем мгновенно отключить неэффективные ресурсы. Pay-as-you-go позволяет не платить за простаивающие мощности в ночное время и выходные

— CFO e-commerce платформы

tech

Облако 2025 — практичность побеждает хайп

Главные выводы от клиентов

Безопасность — не опция, а требование

Без сертификатов ФСТЭК, соответствия 152-ФЗ и встроенной защиты провайдер не пройдет даже первичный отбор

Гибрид — новая норма

Enterprise не переходит в облако полностью. Критичные системы остаются on-premise, но управляются через единую консоль с облачными сервисами.

Меньше, но качественнее

Компании отказываются от погони за количеством сервисов

90%

потребностей бизнеса покрывают 5-7 базовых облачных услуг

Автоматизация безопасности окупается быстро

DevSecOps и shift-left подход снижают стоимость устранения уязвимостей в 100 раз. ROI — менее года

Каждая минута на счету

Поминутная тарификация и real-time биллинг меняют экономику облака. Экономия до 30% только за счет выключения неиспользуемых ресурсов.

Bare Metal — когда виртуализация не нужна

Для наших высоконагруженных баз данных виртуализация съедала до 15% производительности. Bare Metal серверы в облаке дали прямой доступ к железу. Развернули Kubernetes прямо на выделенных серверах — worker-ноды работают на полной мощности без оверхеда гипервизора.
При этом получаем все плюсы облака: быстрое масштабирование, оплата помесячно, никакого обслуживания железа

— Техлид маркетплейса

Наша система обработки платежей требует предсказуемой производительности — никаких «шумных соседей». Bare Metal в облаке стал идеальным решением: dedicated серверы с NVMe дисками, при этом можем добавить быстро новую ноду вместо 2 месяцев ожидания поставки железа.
Latency снизился на 40%, а стоимость владения упала вдвое по сравнению с собственным ЦОД

— СТО процессинговой компании

S3 с Object Lock и WORM — защита от ransomware

После атаки шифровальщика на одного из наших партнеров, мы перевели все бэкапы в S3 с Object Lock. Теперь даже если злоумышленник получит полный доступ к инфраструктуре, он физически не сможет удалить или зашифровать наши резервные копии. WORM-политики гарантируют неизменность данных на заданный срок.
За год было 3 попытки атак — все безуспешные, бизнес даже не заметил

— Начальник ИБ производственного холдинга

Версионирование в S3 спасло нас от человеческого фактора уже десятки раз.
Junior-разработчик случайно удалил 500 ГБ продакшн-данных — восстановили за 5 минут из предыдущей версии. Это дешевле и надежнее, чем tape-библиотеки, которые мы использовали раньше

— ИТ-директор аудиторской компании

GPU в облаке — AI доступен каждому

Раньше для обучения наших ML-моделей арендовали физический сервер с GPU за 400 тыс. в месяц, даже когда он простаивал. Сейчас используем GPU в Kubernetes — автоматически скейлимся от 1 до 20 карт в зависимости от задач. **Обучение модели для рекомендательной системы теперь занимает 3 часа вместо 2 дней.** Платим только за фактическое использование — экономия 70% бюджета на инфраструктуру ML

— Head of AI e-commerce платформы

GPU как сервис позволил нам войти в генеративный AI без миллионных инвестиций. Арендуем карты для fine-tuning LLM под наши задачи, и для инференса в проде. **За полгода запустили 5 AI-продуктов, которые генерят 30% новой выручки компании**

— CTO маркетингового агентства

Георепликация СУБД — данные всегда доступны

Межрегиональная репликация PostgreSQL между разными ДЦ дала нам настоящий disaster recovery. Когда в прошлом месяце был инцидент в проекте ДЦ, база автоматически переключилась на резервный регион. **Простой — 0 секунд, потери данных — 0.** Клиенты даже не заметили. При этом не нужно держать свою команду DBA в каждом городе.

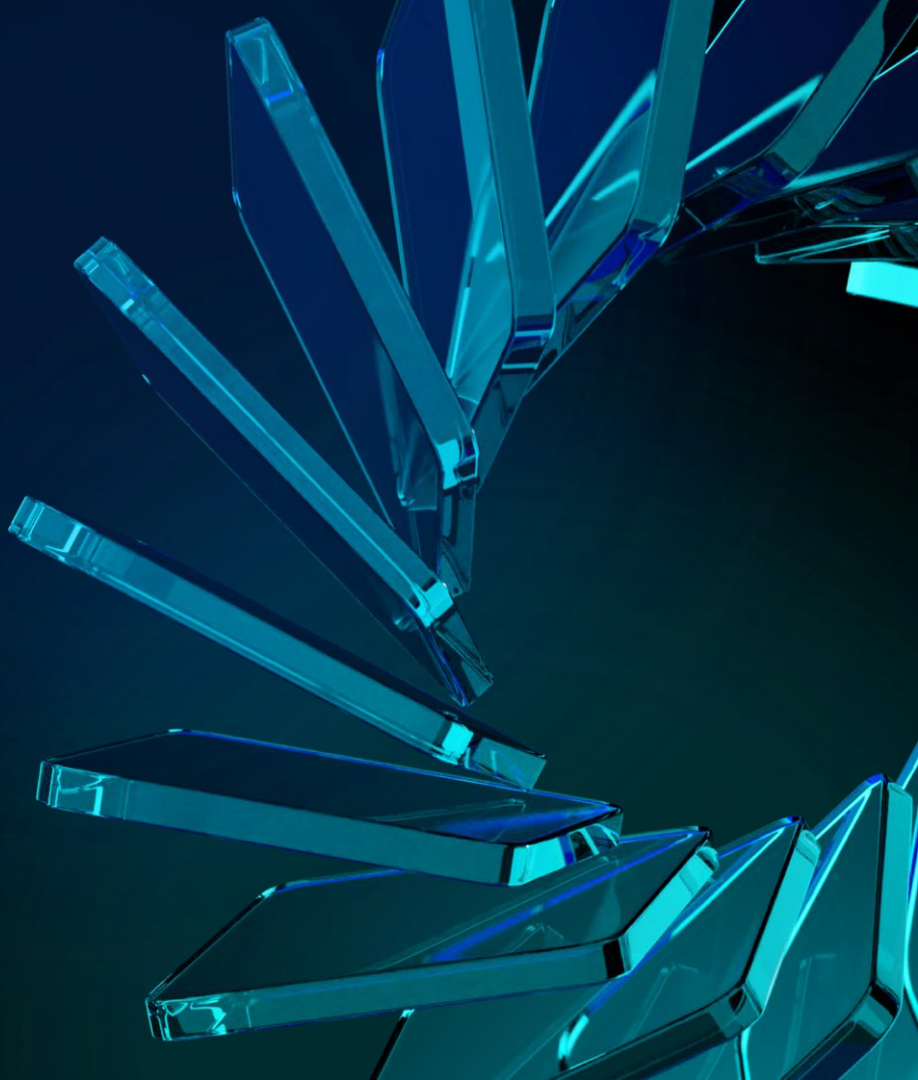
— СТО федерального банка

Наш интернет-магазин работает по всей России. Раньше все запросы шли в один ДЦ и был риск по нагрузке и не хватке места на диске. Развернули дополнительные read-реплики MySQL в разных ДЦ — теперь риски минимализированы. **Управляется все это через одну консоль, как будто это одна база.**

— Технический директор маркетплейса

VK Cloud

Сетевая безопасность в облаке



tech

Категория угроз/сценариев	Пассивная защита	Активная защита
DDoS-атаки	Гео- и IP-фильтрация, rate limiting	Анти-DDoS (scrubbing, mitigation на сетевом/транспортном уровне)
Веб-приложения	Статическая сигнатурная фильтрация	WAF с поведенческим анализом и автообновлением правил
Подозрительный трафик	Логи/алерты без реакции в реальном времени	NGFW с DPI и динамическим блокированием
Атаки нулевого дня	Ограничение экспонирования сервисов	IPS/IDS, NGFW с ML/AI детекцией аномалий
Неавторизованный доступ	ACL, сегментация сети	Интеграция NGFW с IAM, адаптивный контроль доступа
Сканирование и разведка (recon)	Скрывательство портов, фейковые ответы	Honeypots, активное реагирование и блокировка
Управление доступом и маршрутизацией	Встроенный облачный фаервол: SNAT/DNAT, открытие портов, статика	Динамическая настройка политик через API, автоприменение по контексту угроз
Правовое соответствие (РФ)	Облако с аттестацией по 152-ФЗ, К1, выполнение требований ФСТЭК и аттестованного гипервизора	Использование СКЗИ, сертифицированных ФСТЭК, настройка/управление на стороне клиента

Управление сетью (firewalls)

Системы предотвращения вторжений (Intrusion Prevention Systems, IPS)

Системы обнаружения вторжений (Intrusion Detection Systems, IDS)

Виртуальные частные сети (Virtual Private Networks, VPN)

ДДоС-защита (Distributed Denial of Service protection)

Системы авторизации и аутентификации

Системы мониторинга безопасности

AIM, ролевая модель

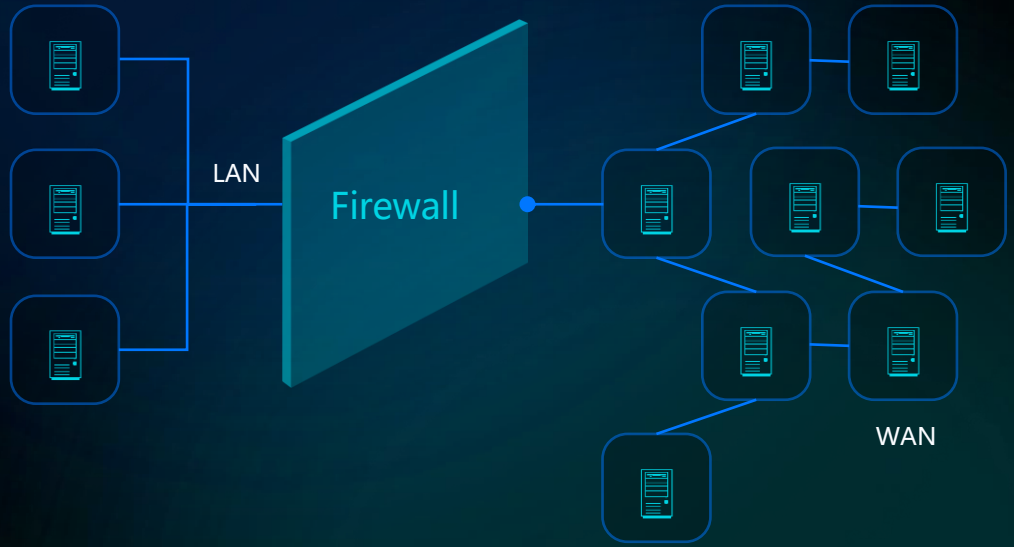
ИТ-инфраструктура

Внешний периметр

Управление сетью в облаке (Firewall)

Основные функции

- Фильтрация трафика
- Мониторинг сетевой активности
- Управление доступом
- VPN-шифрование
- Управление портами
- Управление доступа к сайтам



VK Cloud

схема

VK Cloud

Уровень	Функции	PDU	Примеры
7. Прикладной	Некоторое высокоуровневое API	Данные	HTTP, FTP
6. Представительский	Представление данных между сетевым сервисом и приложением	Данные	ASCII, EBCDIC, JPEG
5. Сеансовый	Управление сеансами: продолжительный обмен информацией в виде множества передач между нодами	Данные	RPC, PAP
4. Транспортный	Надёжная передача сегментов между двумя нодами в сети	Сегменты/ Датаграммы	TCP, UDP
3. Сетевой	Структуризация и управление множеством нод в сети	Пакеты	IPv4, IPv6
2. Канальный	Надёжная передача датафреймов между двумя нодами соединённых физическим уровнем	Фреймы	PPP, IEEE 802.2, Ethernet
1. Физический	Передача и приём потока байтов через физическое устройство	Биты	USB, витая пара

Последствия для бизнеса могут измеряться значительным ущербом в виде потери позиций на рынке, прибыли и репутации

Финансовые потери:

Gartner

Простой онлайн-сервиса на 1 час обходится компаниям в среднем в $300 000

Репутационный ущерб:

Ponemon Institute

72% клиентов теряют доверие к компаниям после киберинцидентов

Потеря рыночных позиций:

Forbes

В 2023 году 34% компаний малого бизнеса, подвергшихся DDoS-атакам, прекратили работу в течение года

VK Cloud

VK Cloud

Защита от DDOS атак

(от англ. Distributed Denial of Services - Распределенный отказ в обслуживании) – сетевая атака, заключающаяся в большом количестве одновременных запросов на сервера компании с целью доведения системы до отказа.

tech

От чего нужно защищаться:

- Атаки на уровне OSI-модели
- Атаки на уровне приложений и протоколов
- Управление доступом
- Атаки на уровне пакетов

Это тип кибератаки, при которой злоумышленник перегружает целевую систему или сеть путем отправки потоков данных с множества источников одновременно. Целью атаки является приведение к отказу в обслуживании,
что приводит к недоступности ресурса для обычных пользователей.

Примеры

- HTTP flood атаки: направленные на перегрузку сервера запросами HTTP
- DNS атаки
- SNMP атаки: использование отраженного трафика SNMP (Simple Network Management Protocol)
- Slowloris атаки: направленные на исчерпание ресурсов сервера путем отправки медленных и неполных
HTTP-запросов
- И т.д.

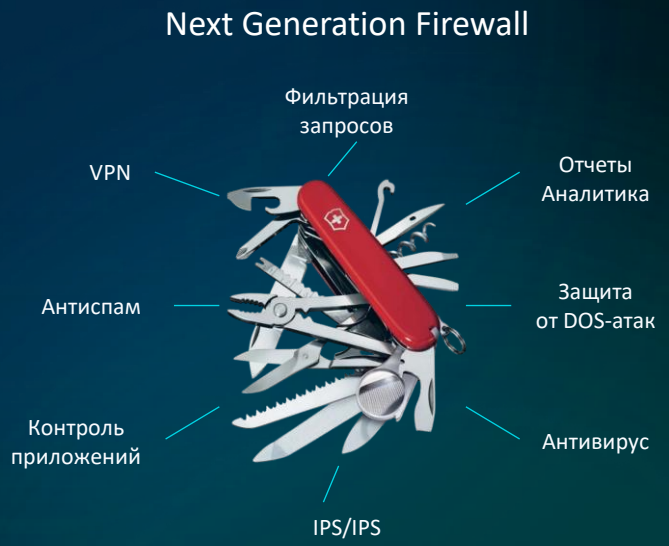
VK Cloud

NGFW

NGFW (Next-Generation Firewall) — это интеллектуальная система сетевой защиты, сочетающая классическую фильтрацию трафика на уровнях L3/L4 с глубоким анализом пакетов, контекстной инспекцией и функциями предотвращения атак, что позволяет не просто контролировать доступ, а проактивно выявлять и блокировать сложные угрозы на границе периметра.

tech

- Межсетевое экранирование
- Обнаружение и предотвращение атак (в т.ч. атаки на веб-приложения)
- Антиспам
- Потоковый антивирус
- Контроль приложений
- Фильтрация интернет-запросов пользователей
- VPN
- Анализ событий/формирование отчетов



VK Cloud

VK Cloud

Криптозащита

это использование сертифицированных средств криптографической защиты информации (СКЗИ), предназначенных для обеспечения конфиденциальности, целостности, подлинности и неотказуемости при передаче и хранении данных, в том числе персональных.

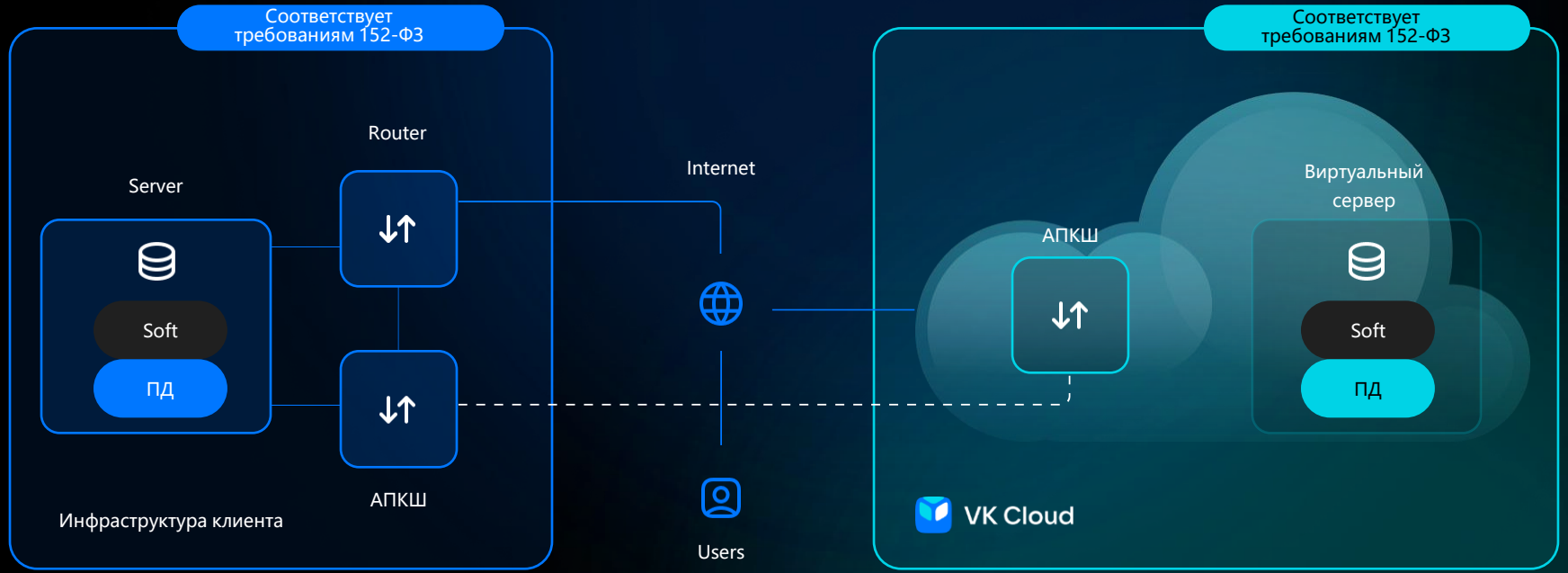
tech

Для кого:

- >300 Тб данных в проекте
- Ограничения ИБ по использованию публичных сетей
- Требуется большая скорость
- Закрываем вопрос ИБ - трафик идет по приватным каналам

VK Cloud

Передача персональных данных в VK Cloud



VK Cloud

Выводы: что важно для клиентов облачных провайдеров

Надежность важнее новизны

Компании выбирают проверенные решения

Защита данных обязательна

Работаем только с сертифицированными провайдерами

Смешанная инфраструктура

Оцените высокий уровень защищенности инфраструктуры и соответствие стандартам

Автоматическая проверка кода

Находим уязвимости до запуска в работу

Прозрачные расходы

Платим за фактическое использование по минутам

Российские решения растут

Миграция с западных платформ ускоряется

Искусственный интеллект для всех

Аренда мощностей вместо покупки оборудования

Выводы – самое главное

Публичное или приватное облако с поддержкой вендора – нужно заново выбирать

Публичные облака – как неизбежность сложных серверов, например, кубер

Требования к разработке ИИ, в частности время – только публичные облако это обеспечат

tech

Следите за нашими новостями в канале

Погоржельский Станислав

Технологический евангелист VK Cloud, VK Tech