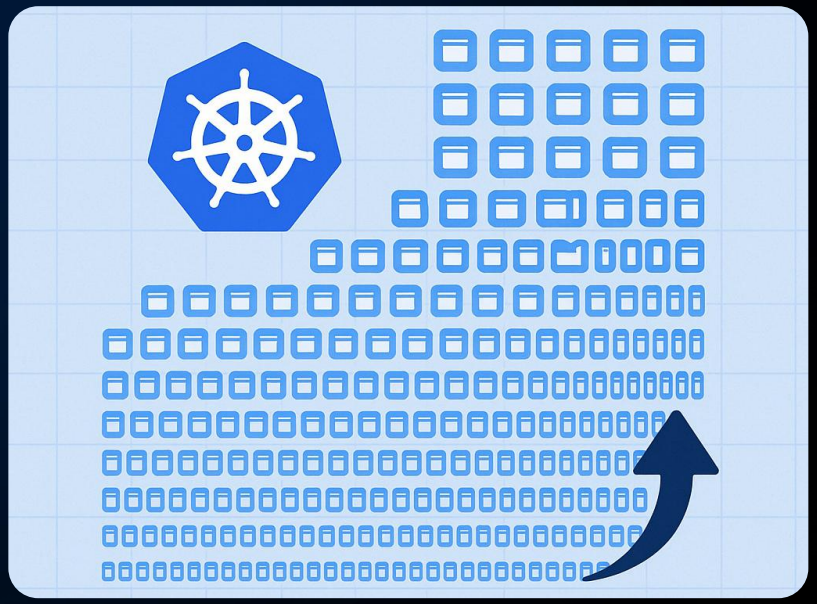
tech

Высоконагруженные инфраструктуры и безопасность данных: практики DevSecOps под требования регуляторов



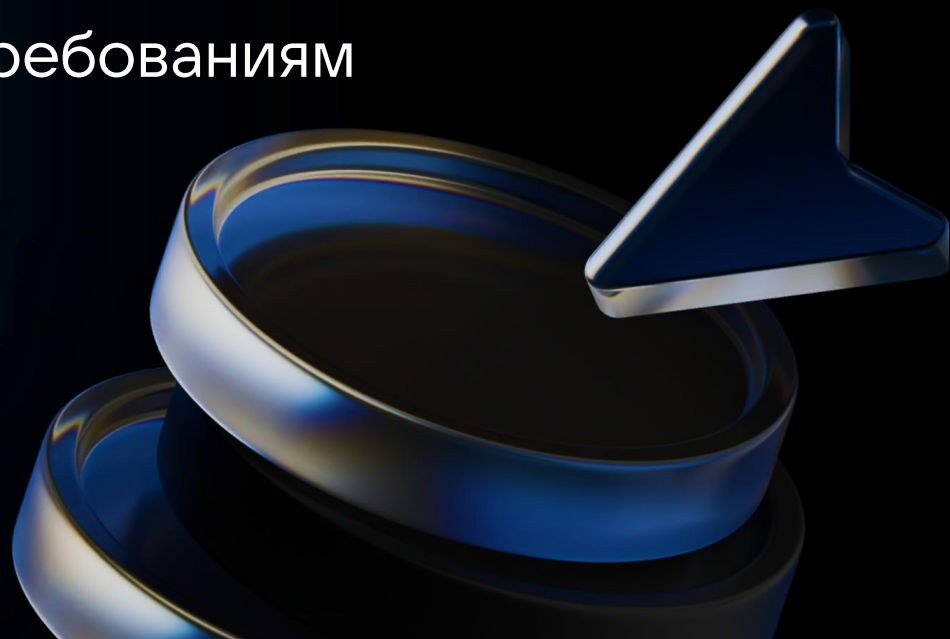
Станислав Погоржельский
Технологический евангелист
VK Cloud&Data

Восстановление после кибератаки — основная задача ИТ/ИБ

- **Атака зашифровала файлы**, что привело к полной недоступности критических данных.
- **Атака на каналы связи нарушила работу веб-сервисов**, блокируя доступ клиентов.
- **Утечка данных** привела к простою, репутационным потерям и штрафам за ПДн.
- **Пожар уничтожил локальное оборудование**, оставив ИТ-инфраструктуру недоступной на недели.
- **Фишинговая атака** на сотрудников позволила получить доступ к учетным записям, скомпрометировав системы.
- **Сбой локального хранилища** из-за отказа оборудования привел к потере данных и остановке операций.

DevSecOps для высоконагруженных инфраструктур:

как выстроить безопасность в Kubernetes и при работе с разными СУБД в распределённых ДЦ, обеспечить обезличивание данных и соответствие требованиям регуляторов



tech

Вектора атак

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

tech

Импортозамещение и информационная безопасность

Обработка персональных данных и соблюдение 152-ФЗ — с сентября 2025

Локализация: БД/бекапы/DR — только в РФ

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

Что нового с 1 сентября 2025 года?

Обезличивание — только по утверждённым методам

Что означает: используете лишь методы из приказа № 140; для каждого набора фиксируете параметры метода; перед любым использованием/передачей — проверка невозможности повторной идентификации с протоколом. При смене алгоритмов/моделей — переобезличивание. Это исключает «вольные» техники и снижает риск ре-идентификации.

Раздельное хранение исходных ПДн, обезличённых наборов и ключей соответствия

Что означает: три разных сегмента/хранилища и разные права доступа; единые склады/бэкапы запрещены. Правило распространяется на резервные копии и DR. Идея простая: разнести «сырьё», «обезличку» и «связку», чтобы одним доступом нельзя было восстановить личность.

Реестр и журналирование операций с обезличенными данными

Что означает: ведёте реестр обезличивания (источник, метод, параметры, дата, ответственный, место/срок хранения) и журнал передач (когда, кому, что, на каком основании). Это делает процесс проверяемым и воспроизводимым.

Передача обезличённых данных в ГИС Минцифры — по требованию, в установленном составе, сроках и формате

Что означает: по получении требования вы готовите «состав» и передаёте обезличённые по № 140 данные с контрольными материалами. Чувствительные категории (включая биометрию) включаются только если прямо указано в требовании; иначе — исключаются.

Согласие субъекта — исключительно отдельным документом/экраном

Что означает: текст согласия не прячется в договор/оферту/политику; вы храните доказуемость получения (кто/когда/какую версию принял). Это повышает юридическую стойкость согласий. .

Локализация хранения при сборе — только в РФ

Что означает: БД с ПДн граждан РФ (включая реплики, бэкапы и DR-сайты) — в российских ДЦ; запись/накопление/хранение за рубежом при сборе запрещены. Иностранные регионы и SaaS-аналитика с записью ПДн — под перенос/замену

Процедура уведомления

Куда и как (без учёта НКЦКИ):
Электронная форма РКН «Инциденты» (вход через Госуслуги).

Сроки:

- **До 24 часов** с момента выявления инцидента (кем угодно: вами, РКН, третьим лицом) — первичное уведомление.
- **До 72 часов —** дополнительное уведомление о результатах внутреннего расследования.

Что указать:

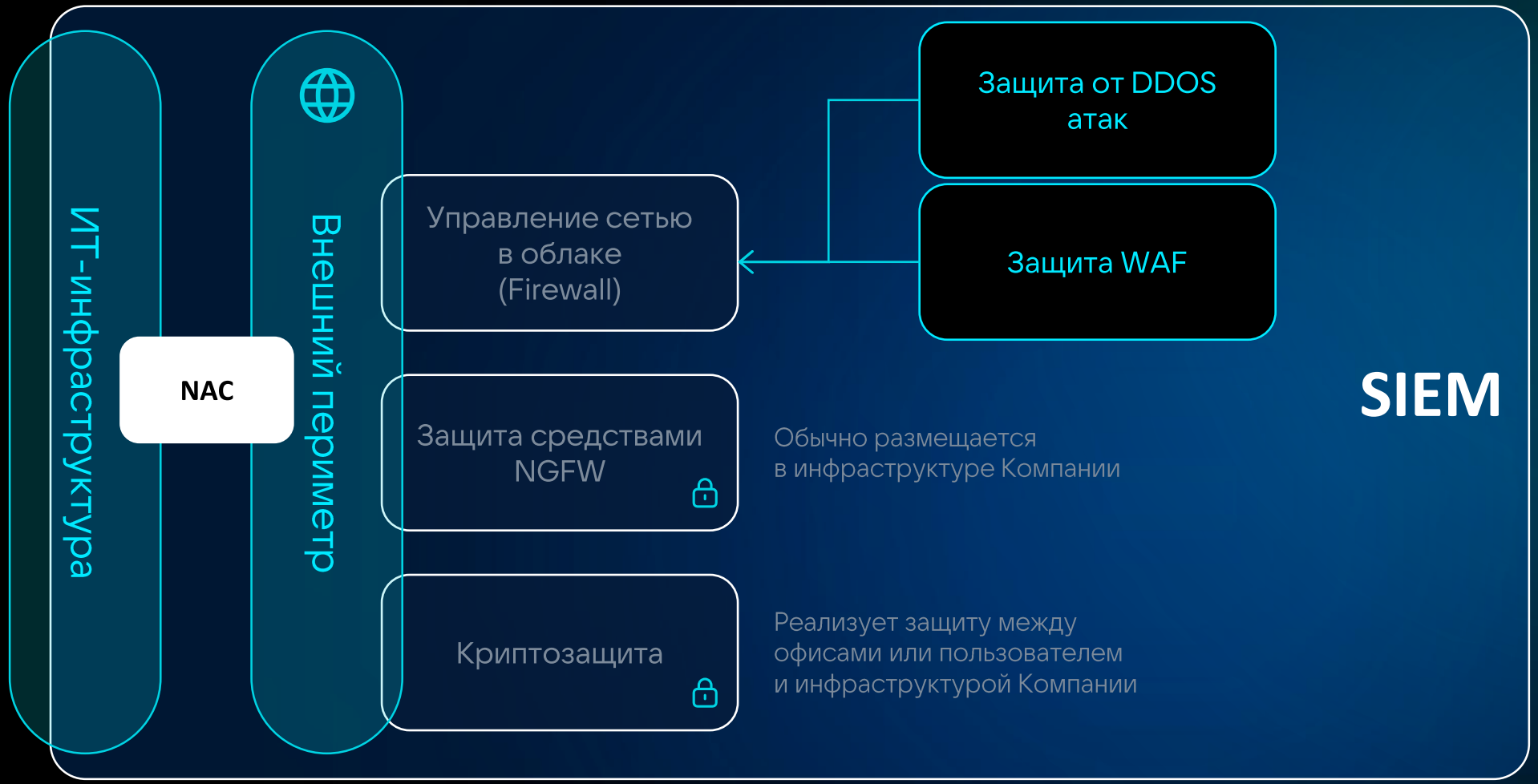
- **В 24 часа:** что произошло, предполагаемые причины, возможный вред субъектам, принятые меры, контакт уполномоченного лица.
- **В 72 часа:** итог расследования (масштаб, категории данных, канал утечки), сведения о причинивших инцидент (если установлены), дополнительные меры.

Нюанс: 24/72 — это календарные часы, а не «рабочие дни»
Если РКН сам выявил утечку и прислал требование, вы всё равно отправляете первичное/дополнительное уведомления в те же сроки.

tech

Архитектура

Почти идеальная инфраструктура



tech

k8s

Безопасность в Kubernetes

Network Policies — микросегментация трафика между подами. Аналогия: как противопожарные двери в здании — локализуют проблему в одной зоне

Pod Security Standards (замена PSP):
•Контроль привилегий (запрет root, read-only filesystem)

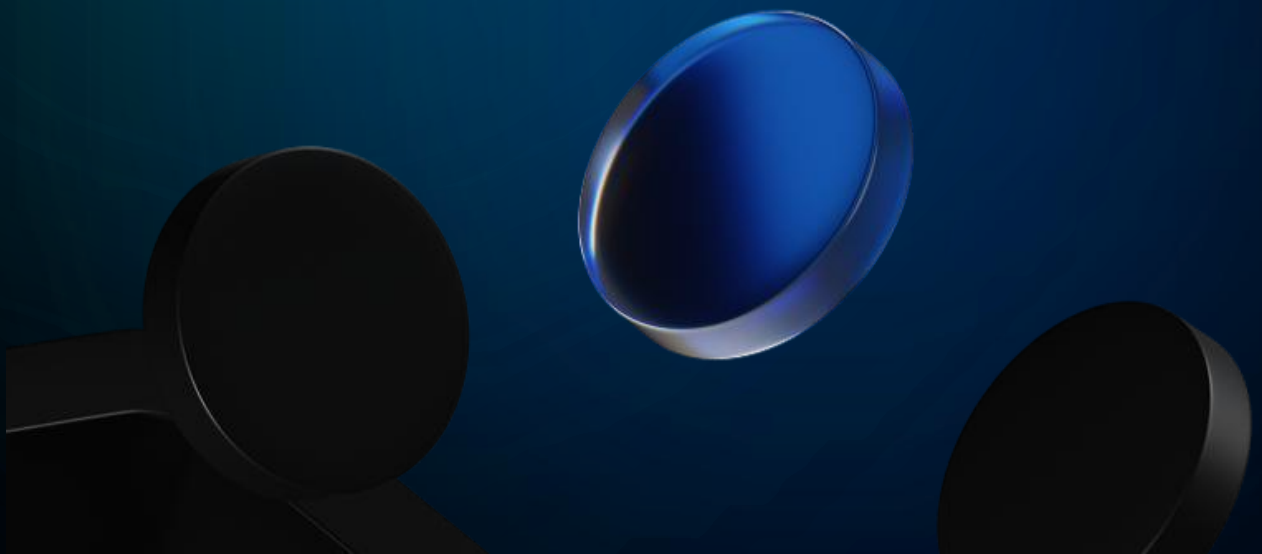
Secrets Management:
•Ротация ключей каждые 90 дней (требование регуляторов)

Runtime Security:
•Falco для детекции аномального поведения
•Пример: обнаружение попытки запуска shell в production-контейнере

Подход	Плюсы	Минусы	Для кого
Встроенные K8s меры	Нативность, низкий overhead	Базовый уровень защиты	Стартапы, dev-окружения
Service Mesh (Istio)	mTLS из коробки, детальный контроль	Сложность, ресурсоёмкость	Enterprise, микросервисы
Специализированные решения (Aqua, Prisma)	Глубокая защита, compliance	Стоимость	Финтех, гостайна

Сегодня все меняется
слишком быстро

K8s должен решать проблемы:



Медленная разработка

Развертывание сред занимает
дни или недели

Пиковые нагрузки

Сервисы падают во время рекламных
акций или всплеска трафика

Высокие затраты

Вы платите за неиспользуемые мощности
и сложное администрирование

Сложность управления

Команда тратит время на поддержку
Kubernetes, а не на развитие продукта

Что такое «экстремальная нагрузка» для кластера

Pod churn

Создание и удаление подов десятками и сотнями в секунду

01

Mass scheduling

Тысячные очереди Pending, bursts-манифестов и Job’ов

02

Image pressure

Валовые imagePull, холодные кэши, ограниченный pull-throughput

03

Control-plane pressure

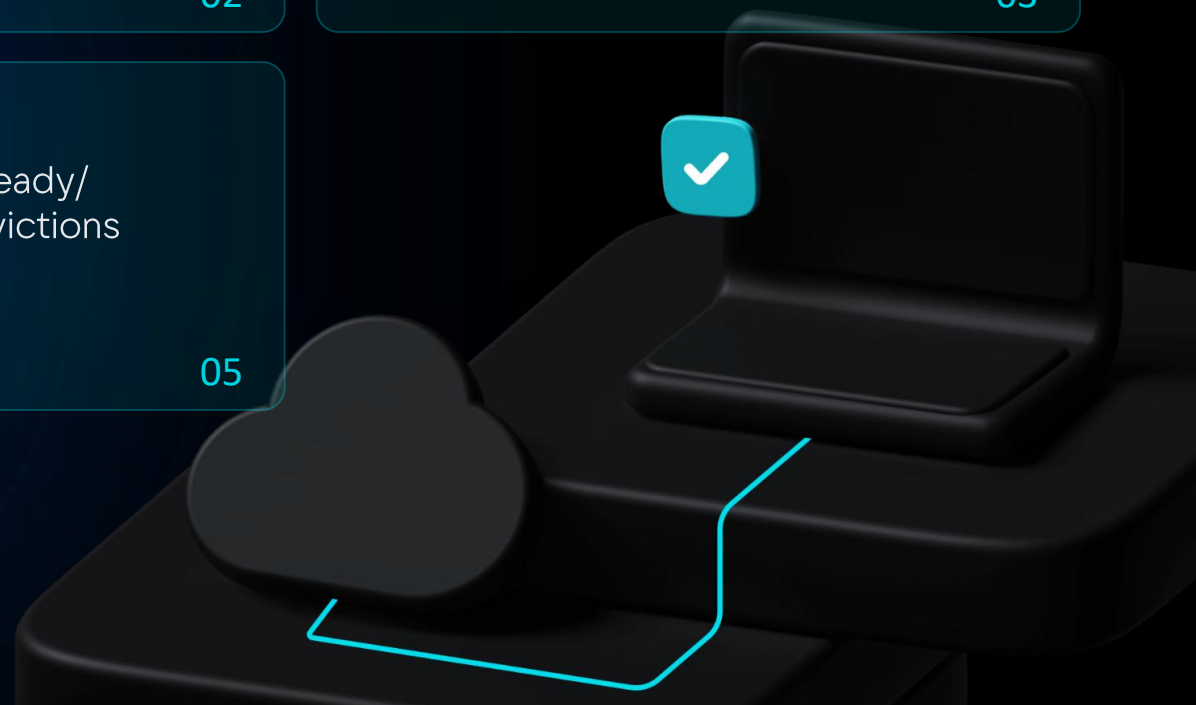
QPS и конкурентные запросы к kube-apiserver, всплеск watch’ей и листингов

04

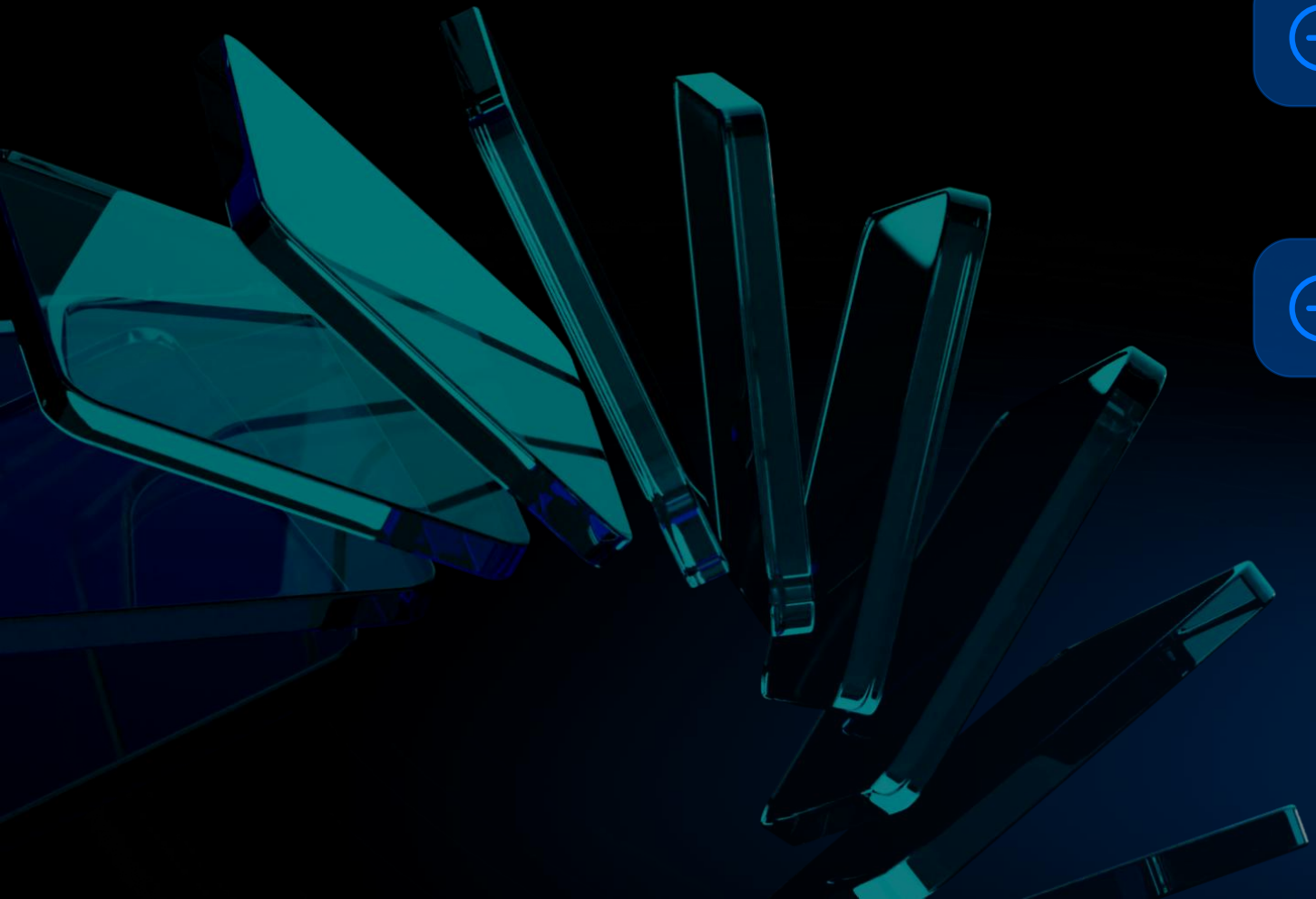
Node pressure

Дефицит CPU/IOPS, NotReady/ Unreachable, массовые evictions

05



Self-healing
для рабочих нод

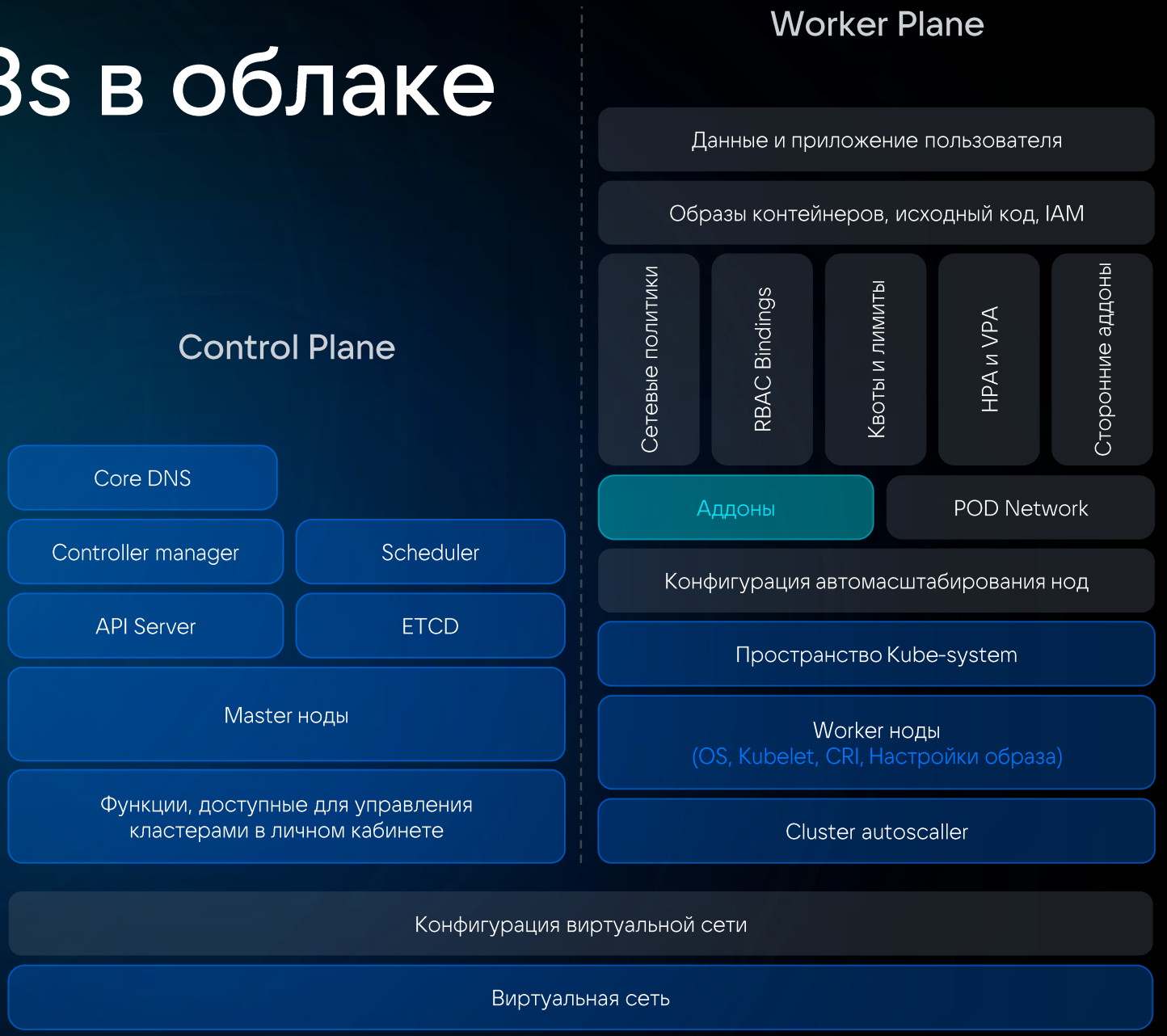


- Компоненты ноды и системных сервисов находятся под контролем сервиса
- При возникшей неисправности сервис автоматически предпринимает действия по восстановлению работы ноды

Перезапуск системного компонента

Пересоздание ноды кластера

Схема k8s в облаке



tech

Безопасность при работе с СУБД в распределённых ДЦ

Безопасность при работе с СУБД в распределённых ДЦ

Шифрование на разных уровнях:

•At rest — transparent data encryption (TDE) для PostgreSQL, MySQL
•In transit — обязательный TLS 1.3 между ДЦ
•End-to-end — шифрование на уровне приложения для особо чувствительных данных

Аудит и мониторинг:

•Логирование всех обращений к критичным таблицам
•Алертинг на аномальные паттерны (внезапно 10000 SELECT вместо обычных 100)

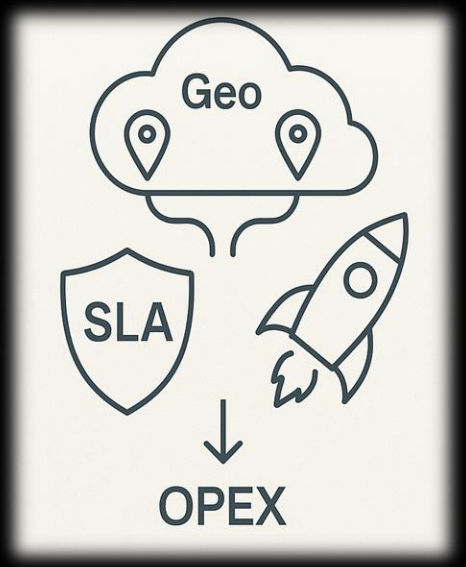
Распределённая репликация:

•Как обеспечить consistency при geo-репликации без потери производительности
•Пример: PostgreSQL с Patroni + WAL-G для async-репликации между МСК и СПБ с RPO < 5 секунд

Backup-стратегии:

•3-2-1 правило: 3 копии, 2 носителя, 1 оффсайт
•Immutable backups против ransomware
•Регулярное тестирование восстановления (раз в квартал)

Георезервирование



Георезервирование снижает риски простоя с типичных 99.9% SLA (8.76 часов простоя в год) до 99.99% (52 минуты в год) — экономия до $2.5 млн в год на предотвращённых инцидентах для среднего бизнеса.

Пример: После внедрения георезервирования DBaaS, крупны ритейлер снизил RTO с 4 часов до 15 минут, что критично для обработки 14 млн чеков ежедневно.

Сравниваем два подхода:
Self-Managed — разворачиваем и поддерживаем PostgreSQL своими силами
DBaaS VK Cloud — используем управляемый сервис с георезервированием

Зоны ответственности и скрытые затраты

Самые трудозатратные зоны в Self-Managed: инфраструктура и резервное копирование съедают 280 человеко-часов ежемесячно — это 1.75 полных ставки специалистов.

Зона ответственности	Self-Managed	DBaaS VK Cloud	Экономия времени в облаке
Инфраструктура	Заказ серверов, настройка сети между ЦОД, управление ресурсами 160 ч/мес	Автоматическое предоставление, включая резервный регион 0 часов	160 часов/мес
Обновления и патчи	Команда выполняет вручную с простоем 40 ч/квартал	Провайдер обновляет автоматически без простоя 0 часов	40 часов/квартал
Резервное копирование	Настройка, тестирование восстановления, ротация 80 ч/мес	Автобэкапы с проверкой целостности 2 часа на контроль	78 часов/мес
Мониторинг	Развёртывание стека, настройка алертов для двух площадок 40 ч/мес	Встроенные метрики и алерты 1 час настройки	39 часов/мес
Безопасность	VPN между ЦОД, шифрование, ротация ключей, аудит 60 ч/мес	Шифрование «из коробки», журналы аудита 0 часов	60 часов/мес
Соответствие 152-ФЗ	Процедуры и контроль силами заказчика	Сертифицированная инфраструктура	Снятие рисков

tech

Обезличивание данных (Data Masking)

Маскирование

Процесс необратимого преобразования персональных данных для предотвращения идентификации субъекта

Статическое маскирование — для тестовых баз:
•Замена: Иванов → Петров (из справочника)
•Shuffling: перемешиваем телефоны между записями
•Генерация: создаём синтетические email через Faker

Динамическое маскирование — в runtime:
•Role-based: оператор видит +7***123-45-67, админ видит полный номер
•Реализация через database proxy (ProxySQL для MySQL)

Кейс: Банк снизил риски утечки ПДн на 87% после внедрения маскирования в dev/test средах. До этого — полная копия продакшена с реальными данными клиентов

tech

Выводы

Бесплатные инструменты ИБ в k8s и не только

Инструмент	Назначение	Этап (тип)	Основные ограничения
Semgrep	Статический анализ кода (поиск паттернов уязвимостей)	SAST	Ограниченные встроенные правила, ручная настройка YAML
SonarQube Community	Анализ качества и безопасности кода	SAST	Нет branch analysis, нет PR-комментариев, только main ветка
OWASP Dependency-Check	Анализ зависимостей на известные CVE	SCA	Медленная первая загрузка, устаревшие базы CVE без обновления
Snyk Free	Проверка зависимостей и контейнеров	SCA / Container	Лимит сканов в месяц, нет SLA
Gitleaks	Поиск секретов и токенов в коде	Secret Scan	Нет GUI, требует CLI и конфигурации
TruffleHog	Глубокий поиск утечек в истории Git	Secret Scan	Медленный анализ больших репозиториев
OWASP ZAP	Динамическое тестирование веб-приложений	DAST	Нет headless API-интеграций, требует ручной настройки правил
Nikto	Сканирование веб-серверов	DAST	Старый интерфейс, ограниченные шаблоны
Trivy	Проверка контейнеров и IaC на уязвимости	Container / IaC	Может пропускать кастомные образы, нет глубокой интеграции
Checkov	Анализ Terraform, Kubernetes, CloudFormation	IaC Security	False positives, нет отчётности для менеджмента
Terrascan	Анализ инфраструктурного кода	IaC Security	Небольшое комьюнити, слабая документация

tech

Цена ошибки на этапе разработки – 1 у.е.

Цена ошибки на этапе прода – 100 у.е + репутация, штрафы и риски существования далее бизнеса

Станислав Погоржельский
Технологический евангелист VK Cloud&Data