

Суверенное облако — это юрисдикция, а не география:

как лицензии и право «дотягиваются» до
ваших данных»



Станислав Погоржельский

Технологический Евангелист
VK CLOUD & DATA



Продукты VK Tech

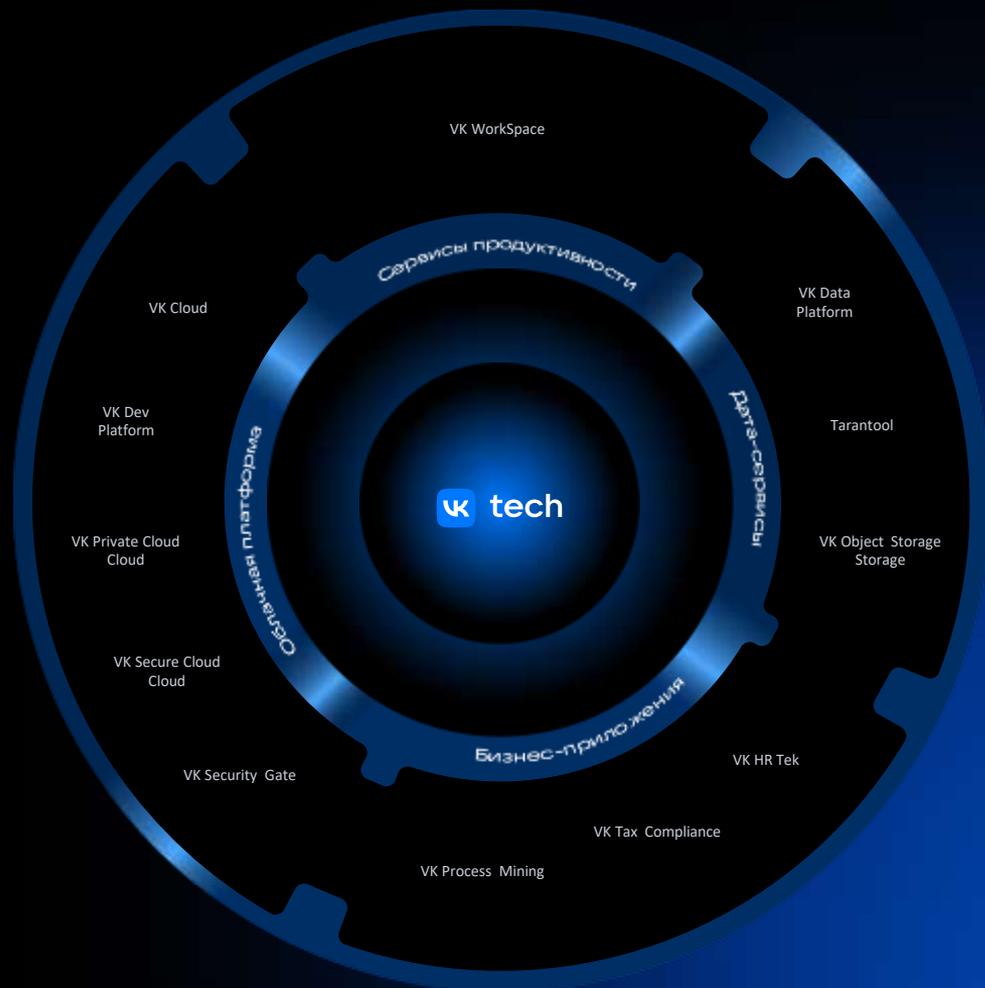
Мультифункциональный портфель VK Tech — это готовая экосистема ИТ-продуктов для повышения эффективности бизнеса

Топ-3

среди производителей отечественного ПО по версии TAdviser

20+

продуктов в реестре отечественного ПО



VK Cloud

Платформа с широким набором облачных сервисов для эффективной разработки и работы с данными для компаний любого масштаба

9 лет

на рынке

VK Cloud является ведущим экспертом в построении облаков в России

01

>8000

компаний

Строят бизнес на решениях VK Cloud

02

400+

инженеров

Участвуют в разработке облачной платформы

03

Цифровой суверенитет — глобальная задача, а не российская особенность



Защита и локализация стали глобальным трендом:

Россия

242-ФЗ 2014 | вступил в силу 2015

требование хранить ПДн граждан РФ на территории России

Китай

Закон о кибербезопасности | 2017

локализация данных операторов критической инфраструктуры и персональных данных

США

Cloud Act | 2018

экстерриториальный доступ к данным американских компаний независимо от страны хранения

Европа

GDPR | вступил в силу 2018

+ суверенные облака Gaia-X (2020) — защита данных и европейская цифровая независимость

Индия

Digital Personal Data Protection Act | 2023

требования к хранению данных граждан на территории страны

Россия

183-ФЗ | 2022

запрет иностранного ПО на КИИ с 01.01.2025

О чем поговорим?



Где теряется контроль

три уровня зависимости
от иностранных технологий



Ключевые риски

от компрометации гипервизора
до санкционных отключений



Community vs Vendor

когда бесплатное ПО с поддержкой сообщества
не гарантирует суверенитет



Чек-лист дорожной карты

что делать прямо сейчас

Три уровня зависимости от иностранных технологий

Юридическая зависимость

Вендор под иностранной юрисдикцией

01

Технологическая зависимость

Закрытый код и обновления под контролем вендора

02

Экономическая зависимость

Вендор диктует цены и условия

03

Уровень 1:

Юридическая зависимость

Риск ли реальная проблема?

Ваша инфраструктура подчиняется законам не той страны, где стоят серверы, а той, где зарегистрирован вендор.

Как это работает на практике

- Cloud Act позволяет США получать данные через провайдера. Например, AWS серверы во Франкфурте — подпадают под Cloud Act
- VMware гипервизор — лицензии активируются из США
- Американские власти могут запросить метаданные, логи, конфигурации — без уведомления клиента

Санкции блокируют доступ к технологиям

- Broadcom прекратила продажи лицензии VMware v8 (февраль 2024)
- Обновления безопасности недоступны
- Лицензии могут быть отозваны по решению правительства США

Российская регуляторика запрещает такие риски

- 87-ФЗ: запрет иностранного ПО на КИИ с 01.01.2025
- Использование VMware после этой даты = нарушение закона
- Штраф и предписания ФСТЭК

Уровень 2: Технологическая зависимость

Суть проблемы

Гипервизор контролирует все виртуальные машины.

Если он скомпрометирован или недоступен для обновления, под угрозой вся инфраструктура.

Критические уязвимости остаются без исправлений

- В 2024-2025 обнаружены критические уязвимости в VMware ESXi и vCenter с оценкой до 9.8 по шкале CVSS.
- Broadcom прекратила поддержку perpetual лицензий.
- Обновления доступны только по платной подписке. Без официального доступа патчинг невозможен.

Закрытый код исключает независимый аудит

- Проприетарный код нельзя проверить на бэкдоры или уязвимости.
- Вся информация о безопасности зависит от заявлений вендора.
- Самостоятельно исправить критическую проблему невозможно.
- Приходится ждать решения от иностранной компании.

Цепочка поставок обновлений под контролем вендора

- Обновления поставляются только через серверы Broadcom в США.
- Процесс сборки, тестирования, подписи находится за пределами российской юрисдикции.
- Риск компрометации на этапе доставки обновлений.

Компрометация гипервизора означает компрометацию всего

- Атакующий получает доступ к памяти, дискам и трафику всех виртуальных машин.
- Файрволы и системы защиты уровня ОС обходятся.
- Одна уязвимость в гипервизоре превращается в доступ ко всей инфраструктуре.

Уровень 3:

Экономическая зависимость

Суть проблемы

Вендор контролирует не только технологии, но и коммерческие условия их использования.

Вы не можете влиять на цены, модель лицензирования или доступность продукта.

Рост стоимости без предупреждения

- Broadcom купила VMware и подняла цены на 300-400%.
- Perpetual лицензии отменили, всех перевели на подписку.
- Модель лицензирования изменилась с сокетов на ядра, стоимость выросла в 2-3 раза.

Уйти сложно и долго

- Миграция на другую платформу занимает 6-18 месяцев.
- Нужно переучивать команду, менять процессы, переносить критичные системы.
- Всё это время вы остаётесь заложником условий вендора

Вендор может изменить всё в любой момент

- Прекращение продаж, изменение условий поддержки, отзыв лицензий.
- Вы узнаете об этом постфактум и вынуждены действовать в условиях дефицита времени.

Экономическая проблема становится операционной

- Нет доступа к обновлениям безопасности.
- Рост цен заставляет экстренно мигрировать с повышенными рисками.
- Невозможно планировать ИТ-бюджет на перспективу.

Экономика: собственный ЦОД vs облако



Экономика: собственный ЦОД или суверенное облако

Выбор модели инфраструктуры — это не только технологии, но и экономика.

- Собственный ЦОД требует капитальных затрат: серверы, СХД, сеть, команда 24/7, лицензии, электричество, обновление железа каждые 3-5 лет.

Все расходы сразу, независимо от загрузки.

①

- Суверенное облако переносит расходы в операционные: платите за потребляемые ресурсы, масштабируетесь за минуты, не содержите команду для поддержки железа. Предсказуемый ежемесячный платёж.

Ключевой вопрос: какой сценарий использования?

- Для стабильной предсказуемой нагрузки собственный ЦОД может быть выгоднее.
- Для переменной нагрузки, dev/test окружений, быстрого масштабирования облако экономичнее.

ТСО нужно считать честно: не только железо, но и зарплаты, риски простоя, время команды.

①

Матрица выбора решений

Матрица выбора: где жить вашим системам

	Собственный ЦОД (иностраный стек)	Облако в РФ на иностранном гипервизоре	Собственный ЦОД (суверенный стек)	Суверенное облако
Юридические риски	Cloud Act, санкции. Штрафы 300-500 тыс. ₽ за нарушение 187-ФЗ	Риск несоответствия для КИИ сейчас или после миграции провайдера. Ответственность на арендаторе	Соответствие 187-ФЗ, контроль юрисдикции	Соответствие 187-ФЗ и 152-ФЗ. Проверьте аттестат ФСТЭК (категория КИИ, класс защищённости, область действия)
Технологические риски	Уязвимости без патчей, supply chain под США	Провайдер не может патчить без доступа к обновлениям	Контроль патчинга, требует экспертизы	Патчинг на провайдере, SLA безопасности
Экономика	Рост цен +300%, легальное использование невозможно	Провайдер переносит растущие расходы на клиентов	Капитальные затраты, команда 24/7, обновление железа	Операционные расходы, масштабирование по требованию
Команда	Эксплуатация запрещённого ПО	Зависимость от провайдера с проблемным стеком	Экспертиза: KVM, OpenStack, мониторинг, патчинг	Фокус на приложения
Скорость	Миграция неизбежна, 6-18 месяцев	Провайдер мигрирует сам, клиенты заложники	Миграция 6-18 месяцев, обучение команды	Запуск за дни, миграция поэтапная

Когда open source не гарантирует суверенитет

Юрисдикция community ≠ юрисдикция заказчика

- Проект живёт в правовом поле страны мейнтейнеров, а не в российской юрисдикции.
- Санкции, экспортные ограничения и политика компании-правообладателя напрямую влияют на доступ к обновлениям и сборкам, даже если код открыт.



Пример: изменение лицензии и политики распространения в MinIO без учета интересов отдельных стран.

Управляемость и продуктовая политика

- Даже при открытом коде владелец бренда определяет, что будет в community-редакции, а что только в коммерческой версии.
- FreeNAS был объединён с линейкой TrueNAS, где продвинутые функции и поддержка доступны в платной редакции; community-ветка развивается с иными приоритетами.



У популярных open source-маршрутизаторов и firewall-проектов часть функциональности, сертификации и SLA концентрируется в коммерческой версии, а не в «бесплатной прошивке».

Когда open source не гарантирует суверенитет

Что даёт суверенитет на самом деле

Суверенитет

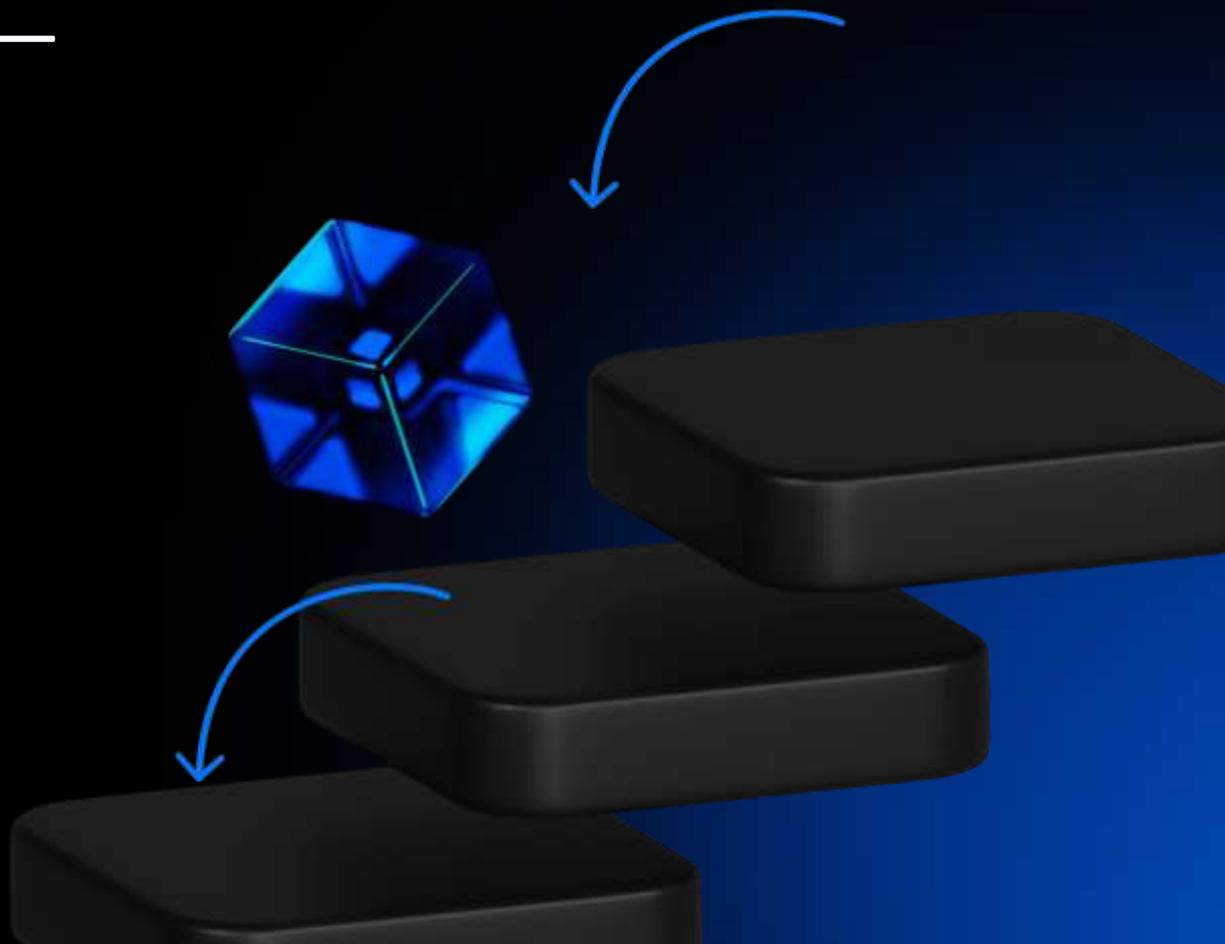
— это не «репозиторий на GitHub»,
а контролируемый стек: локальный правообладатель,
понятная дорожная карта, аудит кода, аттестаты ФСТЭК и
ответственность, закреплённая в договоре.



Для КИИ важен не только open source, но и наличие вендора в
российской юрисдикции, который
обязуется соблюдать требования 187-ФЗ.



Чек-лист дорожной карты — что делать прямо сейчас



Практические шаги для перехода на суверенный стек — от аудита до требований регуляторики

Инвентаризация и риски

- Какие системы работают на иностранных гипервизорах
- Какие попадают под 187-ФЗ (объекты КИИ, значимые объекты)
- Оценка штрафов: 300-500 тыс. руб. за несоответствие

01

Выбор платформы

- Юрисдикция разработчика и правообладателя
- Аттестат ФСТЭК: категория КИИ и класс защищённости
- Локальная поддержка и готовность команды к эксплуатации

02

Сценарий миграции

- Lift & shift — быстро для совместимых систем
- Рефакторинг — дольше, с оптимизацией под новую платформу
- Гибридная модель — поэтапный переход

03

Регуляtorика

- Соответствие 187-ФЗ закреплено в договоре
- SLA и ответственность провайдера за защиту КИИ
- Документирование процессов для аудитов ФСТЭК

04

Надежность VK CLOUD



ЦОД TIER III

Единая отказоустойчивая архитектура с резервированием

SLA 99,95%

С финансовыми гарантиями

Соответствие требованиям регуляторов

Аттестованная облачная инфраструктура в соответствии с 152-ФЗ

24/7

Ваша «IT-служба одного окна»

IaaS / PaaS

Простое подключение сервисов

Решения VK Cloud



Виртуальные серверы

Конфигурации необходимой мощности внешними IP и безлимитным трафиком 1 Гбит/с



Виртуальные сети

Объединение серверов в локальных сетях, публичный и приватный DNS, VPN, балансировка и фильтрация трафика



Объектное хранилище

Быстрое S3-совместимое объектное хранилище с надежной защитой данных и масштабированием под любые объемы



Графические адаптеры

Высокопроизводительные вычисления в облаке и обучение нейросетей с NVIDIA® Tesla®



VK Data Platform

Платформа больших данных для уменьшения TCO и TTM на базе архитектуры нового поколения и собственного S3-хранилища Object Storage



Базы данных в облаке

Полностью управляемые и масштабируемые базы данных MySQL, PostgreSQL, MongoDB, Redis, ClickHouse, OpenSearch



Кластеры Kubernetes

Автомасштабирование ресурсов и ускорение доставки приложений с Kubernetes как сервисом



Машинное обучение

Платформа для полного цикла ML-разработки и совместной работы Data-команд. API компьютерного зрения и платформа распознавания и синтеза речи

Больше возможностей



CDN

Географически распределенная сеть для быстрой доставки контента



AntiDDoS

Защита AntiDDoS уровней L2–L7



Cloud Backup

Резервное копирование облачных серверов и баз данных



Disaster Recovery

Аварийное восстановление инфраструктуры, в том числе для кластеров ADB



Marketplace

Магазин приложений и ИТ-услуг для бизнеса и разработчиков от ведущих вендоров



Secure Cloud

Аттестованное защищенное облако для ГИС и ИС



Cloud Migration

Автоматическая миграция инфраструктуры в облако



Professional Services

Команда инженеров для развития проекта в облаке VK Cloud



VK Private Cloud

Платформа для построения частного облака на оборудовании аказчика

Cloud Desktop: собственная разработка VK Cloud

Клиентские приложения

- Нативная поддержка Windows 10/11
- Нативная реализация MacOS (BigSur и позднее)
- WebRTC клиент (поддержка Google Chrome, «Яндекс Браузера», Microsoft Edge и других Chromium-клиентов)
- Поддержка Linux через WebRTC



Качество стриминга

- Проприетарный запатентованный протокол №2732786 с минимальными задержками
- Устойчивость картинки в нестабильных сетях (WiFi, LTE)
- Поддержка 60 FPS (до 120 FPS с мощными видеокартами)
- Поддержка разрешения до 4K
- Алгоритм адаптивного битрейта
- Поддержка аппаратных ускорителей



Поддержка GPU

- Использование аппаратного кодирования на GPU
- Уменьшение времени ожидания за счет использования GPU ресурсов
- Поддержка NVIDIA и AMD
- Поддержка кодеков h.264 и h.265

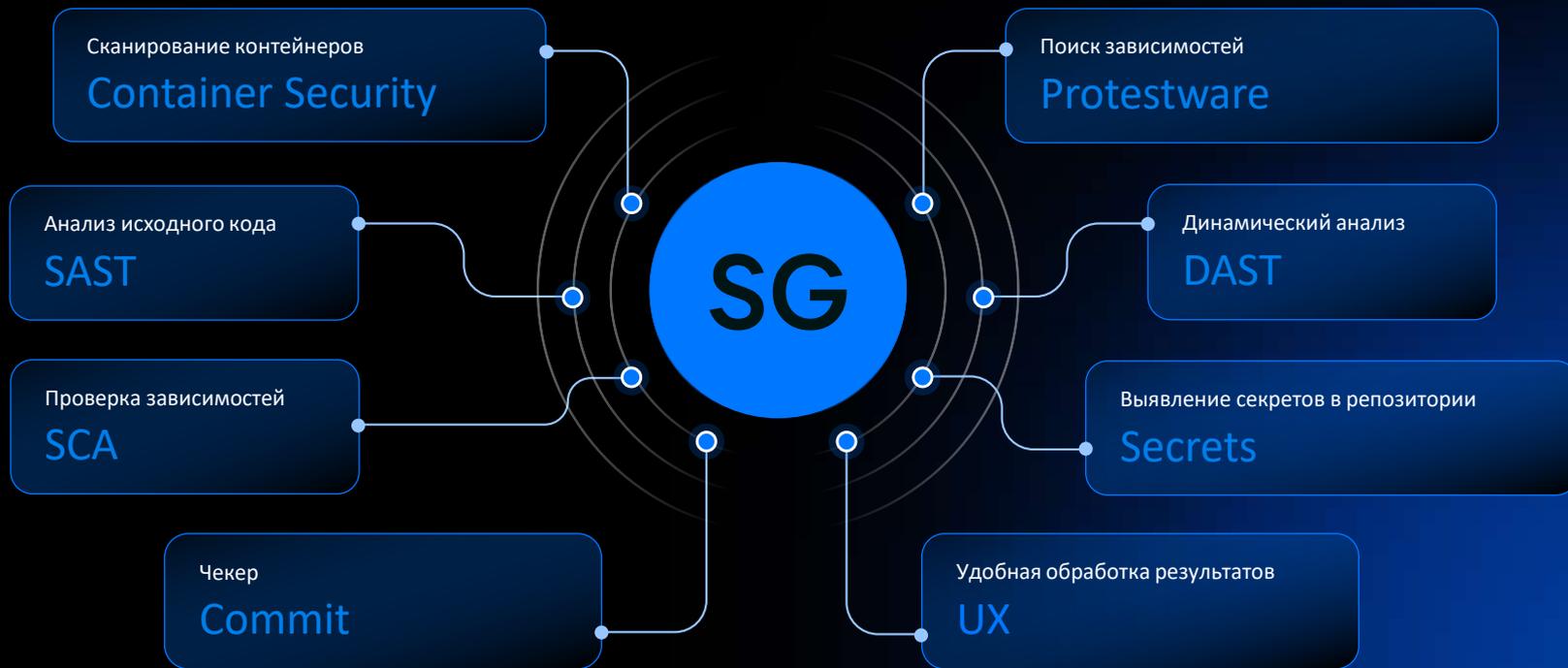


Безопасность

- Сертифицировано в реестре российского программного обеспечения
- Соответствует требованиям ФСТЭК для защиты данных



Security Gate



Security Gate отвечает на запросы ИТ и безопасности

Компании с большим количеством
in-house разработки



Компании в процессе внедрения
практик DevSecOps



Сложности в масштабировании
практик безопасной разработки во
всех проектах



Запрос на внешнюю экспертизу,
методологии, лучшие практики



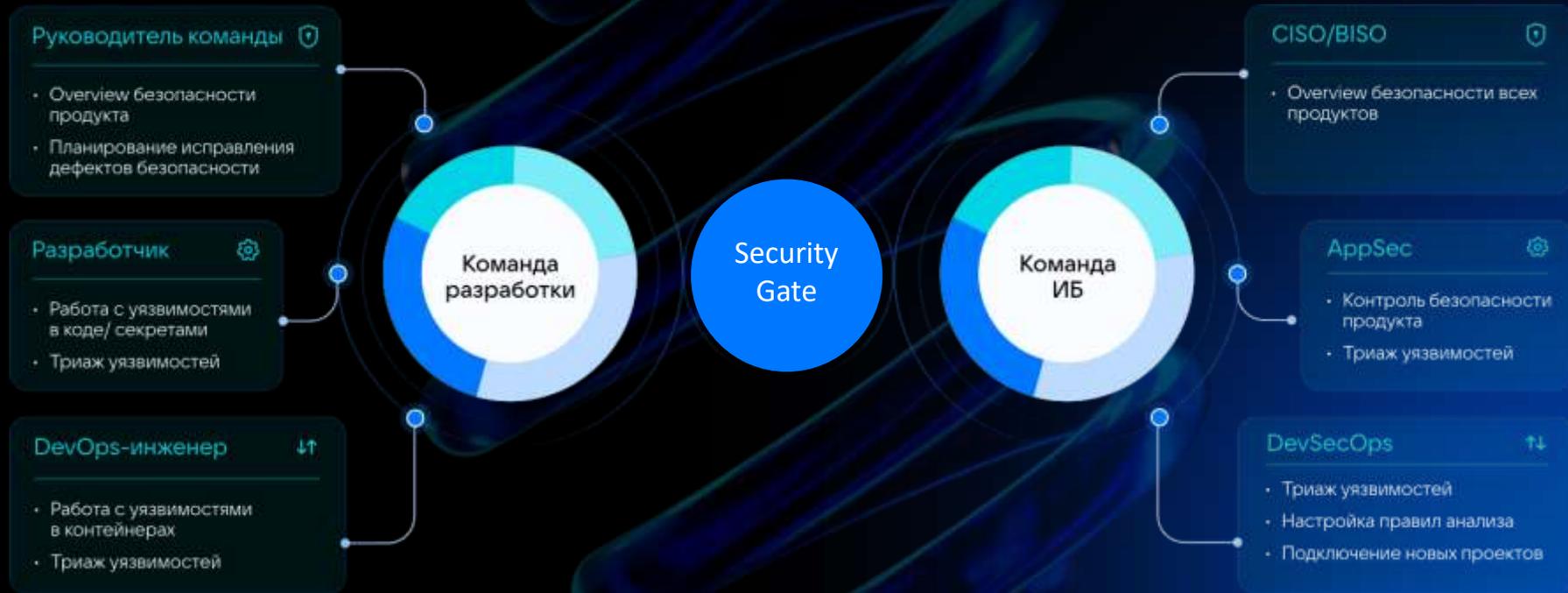
Необходим выбор инструментов
для разнородной кодовой базы



Рассматривается привлечение
продуктовых команд
совместной с ИБ работе
над безопасностью кода



Типовые потребности команд



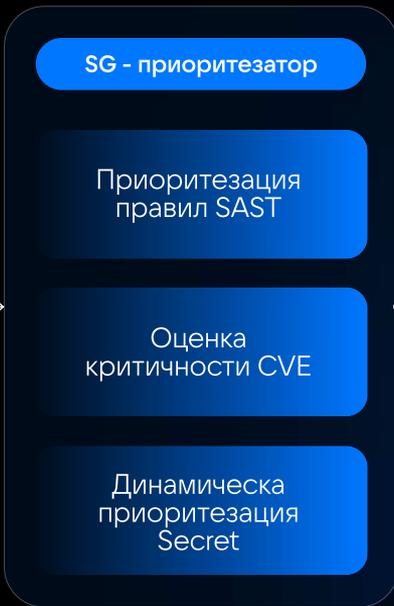
Приоритезация уязвимостей



Множество анализаторов переоценивают критичность обнаруженных дефектов в коде. Это приводит к проблеме «мусорных» сработок на уровнях High+ и скрывает наиболее значимые результаты

Первоначальные результаты

	Crit	High	Medium	Low
SAST	40	56	70	1
SCA	250	472	355	10
Secret	47	35	10	2



Итоговые результаты

	Crit	High	Medium	Low
SAST	10	22	100	35
SCA	16	37	702	322
Secret	12	10	70	2

Нам доверяют

INVITRO

X5Group

ИВИ

1С-БИТРИКС

WESTWING

PHILIP MORRIS
INTERNATIONAL

ЛУКОЙЛ

АВТОВАЗ

BURGER
KING

1c

ГАЗПРОМ
НЕФТЬ

ШАН



РОСАТОМ

Schneider
Electric

amoCRM.



VK Cloud



Станислав Погоржельский

Технологический Евангелист
VK CLOUD & DATA

 TG @Cloudgrad

Спасибо
за внимание!

