Инженерный подход к безопасности NGFW

Марк Коренберг
CTO

ideco

Ideco сегодня

20 лет на рынке, тысячи защищённых компаний и регулярные продуктовые релизы — решения Ideco создаются командой, где более половины сотрудников (150 человек) сосредоточены на разработке.

Мы растём вместе с нашими клиентами, масштабируем решения и поддерживаем безопасность сотен тысяч пользователей по всей стране.

20+
лет на рынке

5500+
компаний под защитой

2400+
участников сообщества

55%
сотрудников в R&D

25000
атак блокируются ежедневно

4
мажорных релиза продукта в год

Инженерный подход к безопасности NGFW

ideco

Проблема

- Реальные инциденты возникают из-за архитектурных и процессных решений.
- Устойчивость NGFW определяется дисциплиной разработки и эксплуатации.

Тезис

Инженерный подход — это формализованные процессы, архитектурные принципы и строгий контроль

Безопасность встроена в жизненный цикл разработки

ideco

Процесс разработки

- 25 формализованных процессов разработки безопасного ПО.
- Охват всего цикла РБПО: архитектура, моделирование угроз, анализ кода, тестирование, сборка, выпуск, сопровождение.
- Внутренние и внешние аудиты.
- Соответствие требованиям ГОСТ.
- Мы не завязаны на поставщиков ПО, а все делаем сами. Базовая ОС обновляется каждый релиз.

Вывод

Безопасность — это не этап, а непрерывный процесс

Все это знают)

Регламенты РБПО по этапам жизненного цикла ПО

ideco

Управление процессами и требованиями

- Процессы РБПО
- Обучение сотрудников РБПО
- Управление требованиями ПО
- Управление конфигурацией ПО
- Управление недостатками ПО

Сборка и защита среды разработки

- Использование безопасной системы сборки
- Безопасность сборочной среды
- Управление доступом и контроль целостности кода
- Обеспечение безопасности секретов

Безопасная разработка

- Оформление исходного кода
- Экспертиза исходного кода
- Статический анализ
- Динамический анализ
- Композиционный анализ
- Контроль цепочек поставок

Архитектура и моделирование угроз

- Анализ архитектуры ПО
- Разработка модели угроз и поверхности атаки

Тестирование

- Функциональное тестирование
- Нагрузочное тестирование
- Тестирование на безопасность

Выпуск и поставка

- Безопасность при выпуске версии
- Безопасная поставка пользователям

Эксплуатация и сопровождение

- Техническая поддержка
- Реагирование на уязвимости
- Поиск уязвимостей при эксплуатации
- Безопасность при выводе из эксплуатации

Статический и динамический анализ

ideco

Статический анализ

- Проводится по модулям поверхности атаки.
- Подтверждённые Critical и Major блокируют релиз.
- Повторный анализ до полного устранения.
- Обязательное кросс-ревью разметки.

Динамический анализ и фаззинг

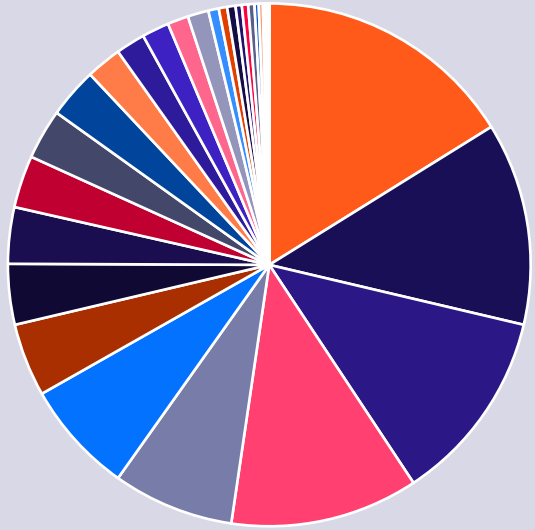
- Перечень модулей формируется по модели угроз.
- Повторный анализ после исправлений.
- Фиксация аварийных завершений и результатов.

Статический и динамический анализ

ideco

Проверено 1062 предупреждений в 40 проектах

Исправлено 88 уязвимостей



На каждый модуль потрачено не менее 50 часов фаззинга. На ядро ~350 часов.

- техцентр 4
- net-snmp(snmp)
- zabbix
- squid
- netmap-ipfw(kipfw)
- ideco-ad-backend
- ideco-cluster-backend
- ideco-app-backend
- ideco-dns-backend
- ideco-proxy-backend
- frr(bgpd и ospfd)
- fail2ban
- openssh
- dnsmasq
- cerberus
- ideco-routing-backend
- ideco-firewall-backend
- ideco-auth-backend
- ideco-local-menu
- ideco-shaper-backend
- python3
- ideco-acl-helpers
- modsecurity
- nginx
- ideco-app-control-nfq
- ideco-web-backend
- ideco-system-backend
- ideco-backup-backend
- ideco-logs-backend
- kernel
- etcd
- suricata
- unbound
- iptables
- igmpproxy
- ideco-ald-backend
- ideco-user-backend
- ideco-central-console-backend
- ideco-network-backend

Результаты анализа CVE

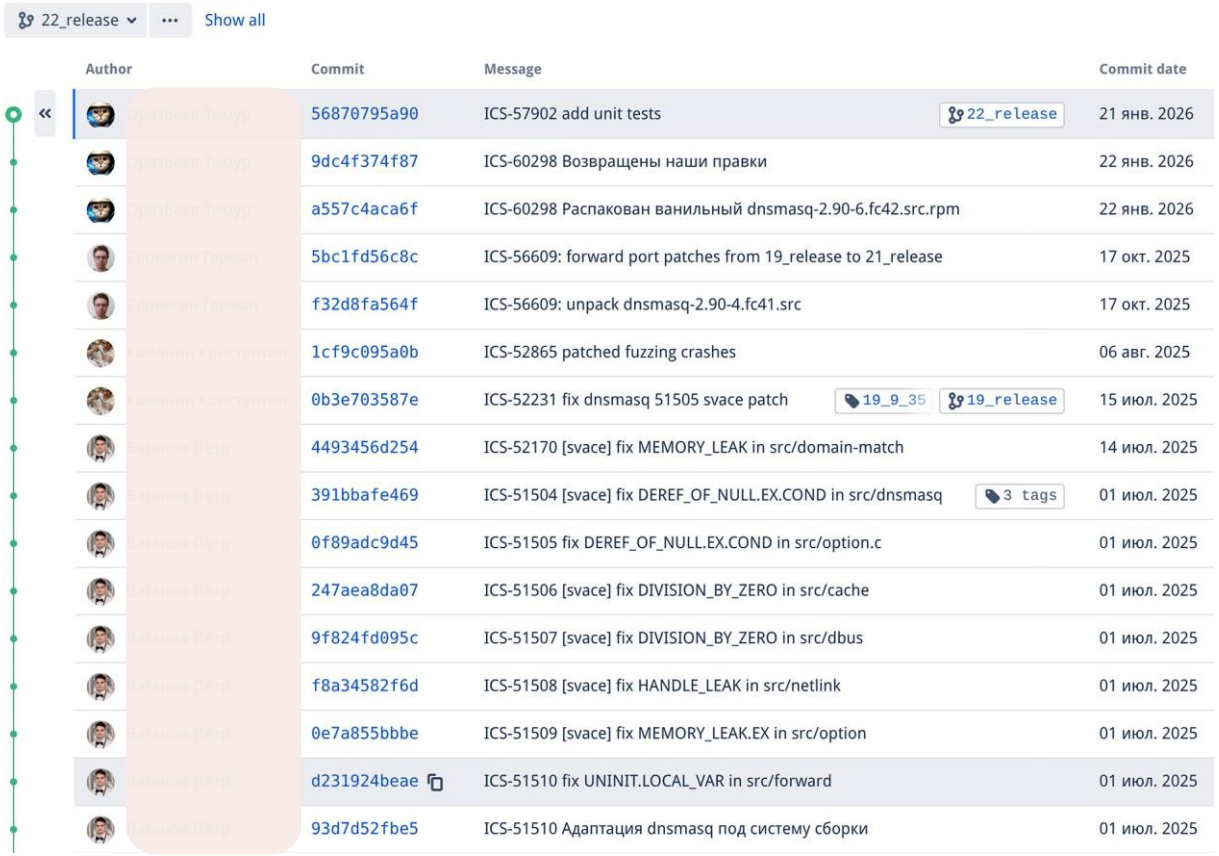
Сравнение веток

Структура найденных CVE

- Основной вклад: golang, dnsmasq, системные библиотеки.
- Часть CVE относится к Windows-only сценариям или неиспользуемым функциям.
- Некоторые CVE являются FP или уже устранены.

Вывод

- В новой версии 21.12 зафиксировано снижение CRITICAL CVE: 13 → 9.
- Отсутствуют HIGH/MEDIUM/LOW уровни.
- Часть CVE классифицирована как Mitigated (3 штуки) или NotAffected (24 штуки).
- Используется автоматизированный анализ на базе NVD (980 831 записей).



Версия 19.17

CRITICAL: 13

HIGH/MEDIUM/LOW: 0

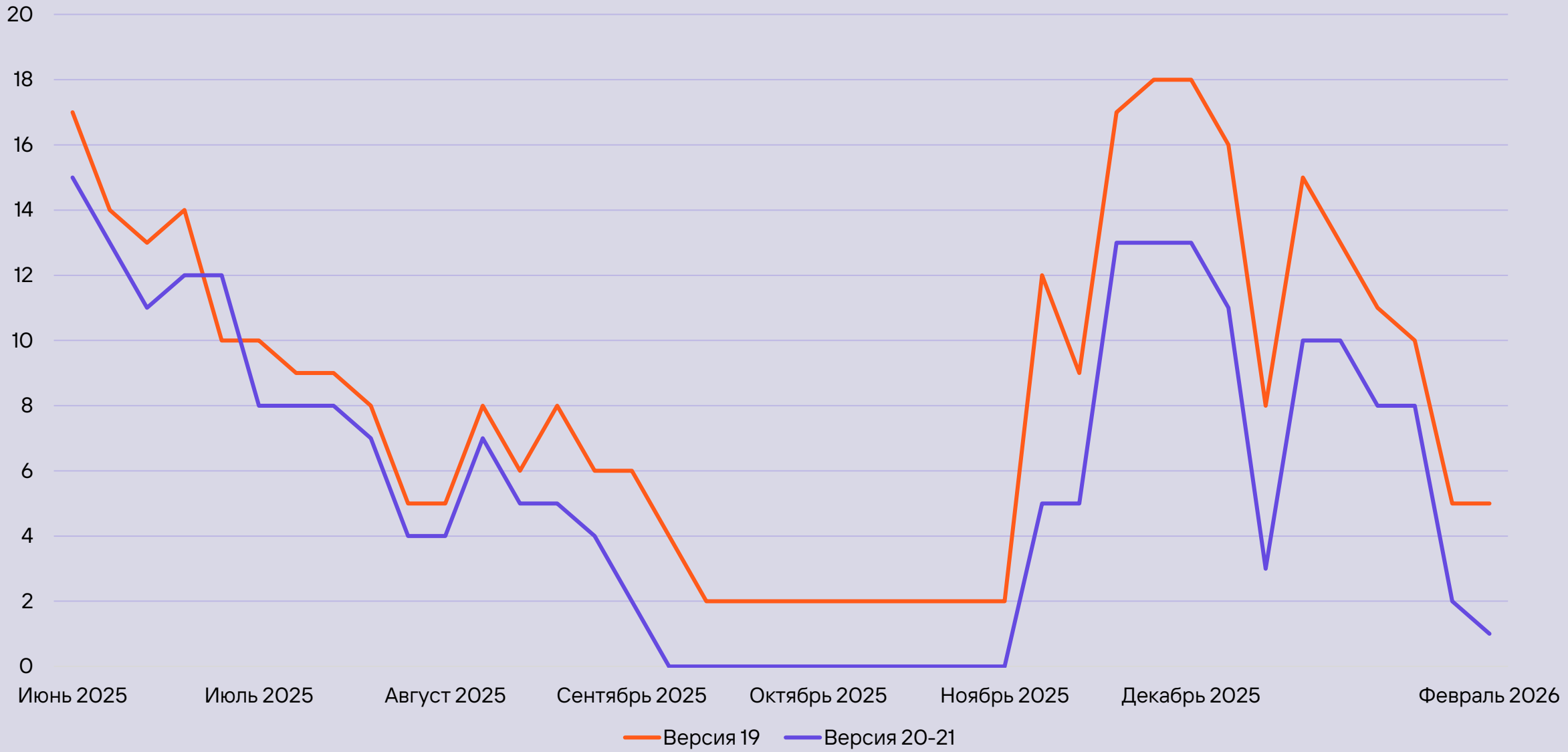
Версия 21.12

CRITICAL: 9 (снижение)

HIGH/MEDIUM/LOW: 0

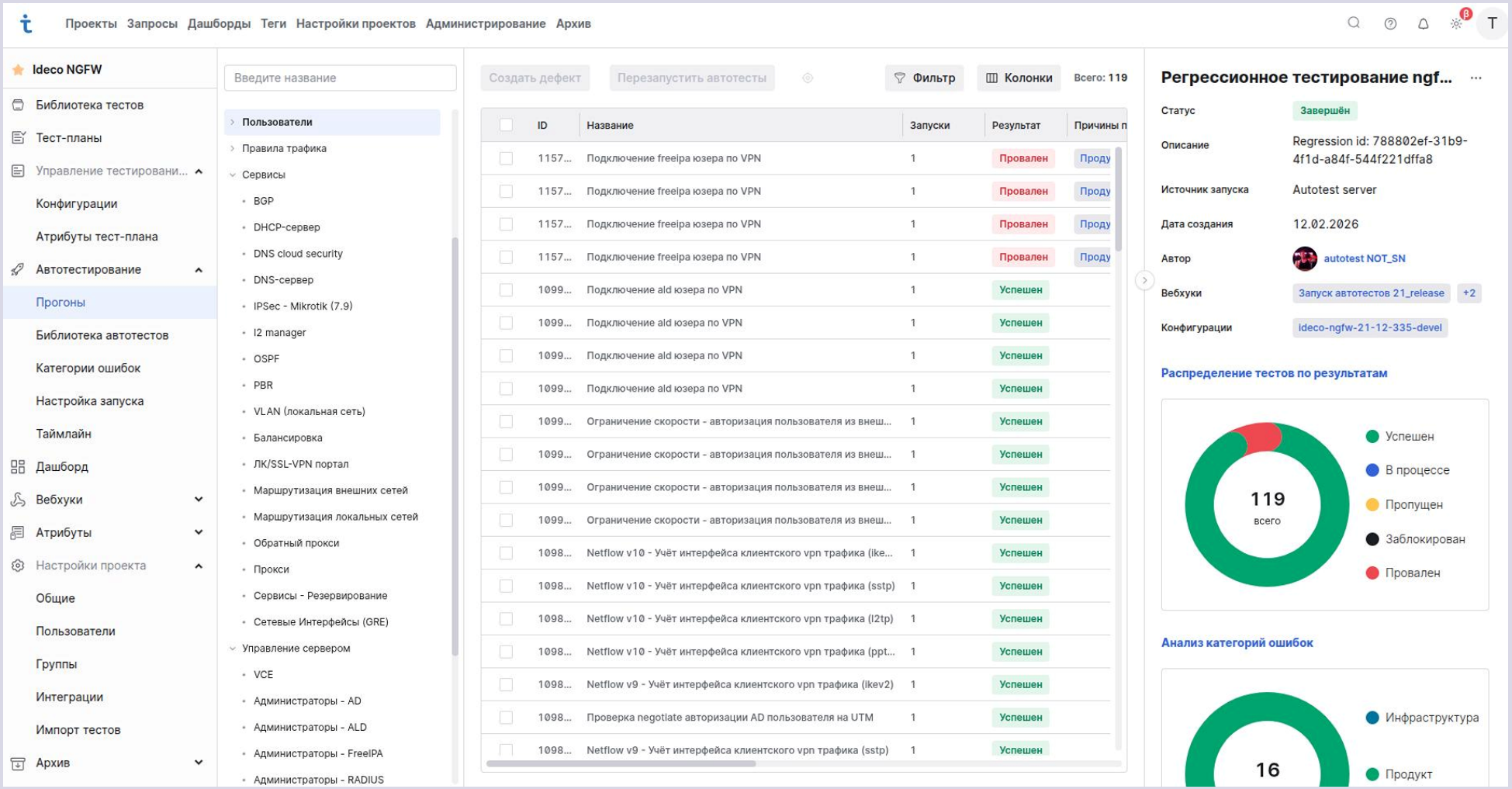
Medium/low уязвимости

ideco



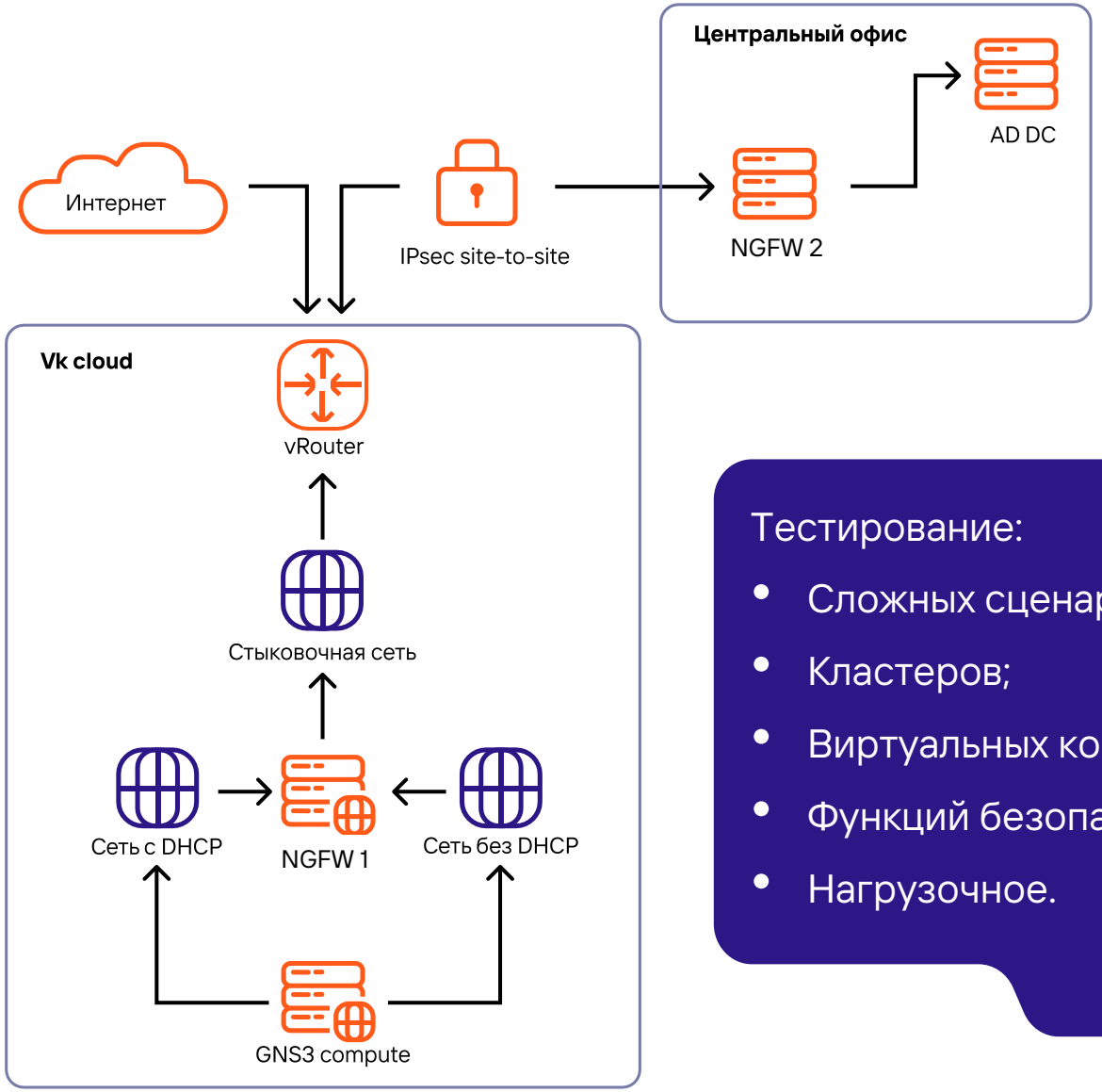
Автотесты

ideco



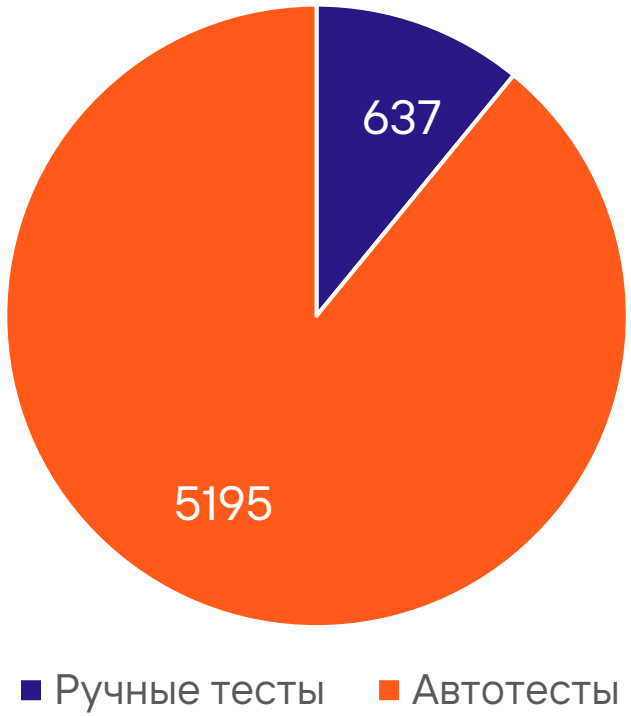
- 300 ВМ
- 45 потоков
- 3,5–4 часа

Тестирование



Тестирование:

- Сложных сценариев;
- Кластеров;
- Виртуальных контекстов;
- Функций безопасности;
- Нагрузочное.



Не только теория, но и практика

ideco

Пилоты у заказчиков

Кейсы технической поддержки

Инциденты и аварийные сценарии

Ограничения по ресурсам
и компетенциям заказчика

Иногда архитектура усложняется внутри, чтобы снизить риски и ошибки в эксплуатации.

Сертифицированное решение Ideco

защищает сетевой периметр организаций

ФГУП «ВНИИ «Центр»

АО «Таганрогский завод «Прибой»

АО «Конструкторское бюро
промышленной автоматики»

Внутренняя инфраструктура компании

ideco

Безопасность инфраструктуры напрямую влияет на безопасность продукта

Защищаемся не только от третьих лиц, но и **от атак внутри** за счет:

- Для всех сервисов используется SSO+2FA
- Доступ по API сделан по отзываемым токенам (без использования логина и пароля)
- Сканирование безопасности внутренних сервисов проводится ежедневно (с использованием SIEM)
- SLA исправления критических уязвимостей во внутренних сервисов составляет – 24 часа
- Около 300 сервисов

Разделение Control Plane и Data Plane

ideco

1

Архитектурный принцип

- Управляющий и пользовательский трафик имеют разные модели угроз.
- Изоляция плоскостей — обязательное требование.

2

Реализация

- Контейнерная модель.
- Раздельные ресурсы и изоляция процессов.
- Сохранение управляемости при атаке на Data Plane.

3

Результат

Диагностика и изменение конфигурации возможны
под нагрузкой или атакой.

Виртуальные контексты VCE

ideco

Что такое VCE

- Изолированная среда со своей адресацией, маршрутами, политиками, правилами журналирования.
- Разделение зон безопасности внутри одного устройства.
- Привязка VCE к аппаратным ресурсам

Эволюция архитектуры

До 2025 года

Managment plane и data plane не разделены

С 2025 года

Элементы managment plane внутри VCE

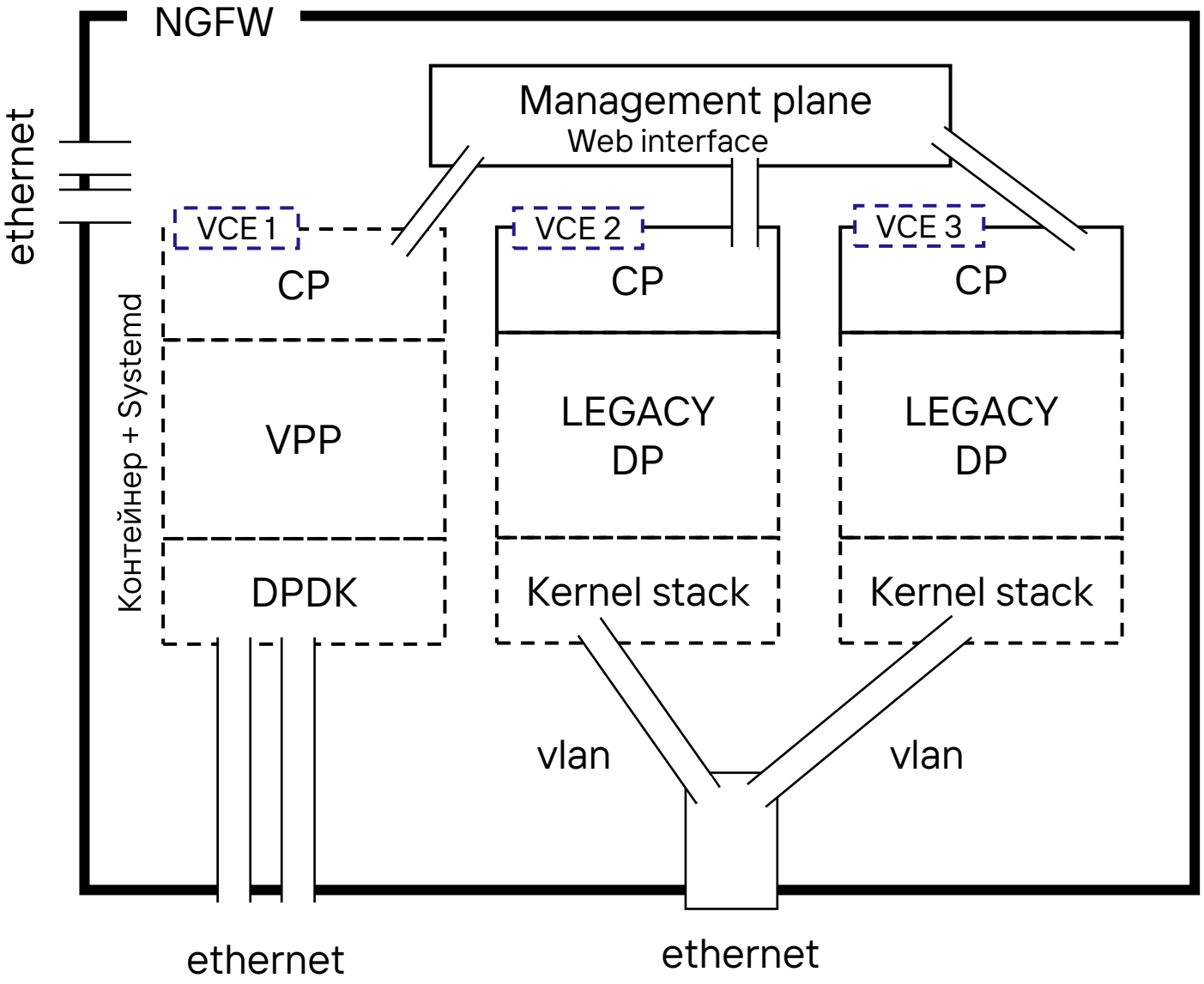
В 2026 году

Обработка трафика только в VCE.
Hardening служб

Архитектура NGFW с контекстами

ideco

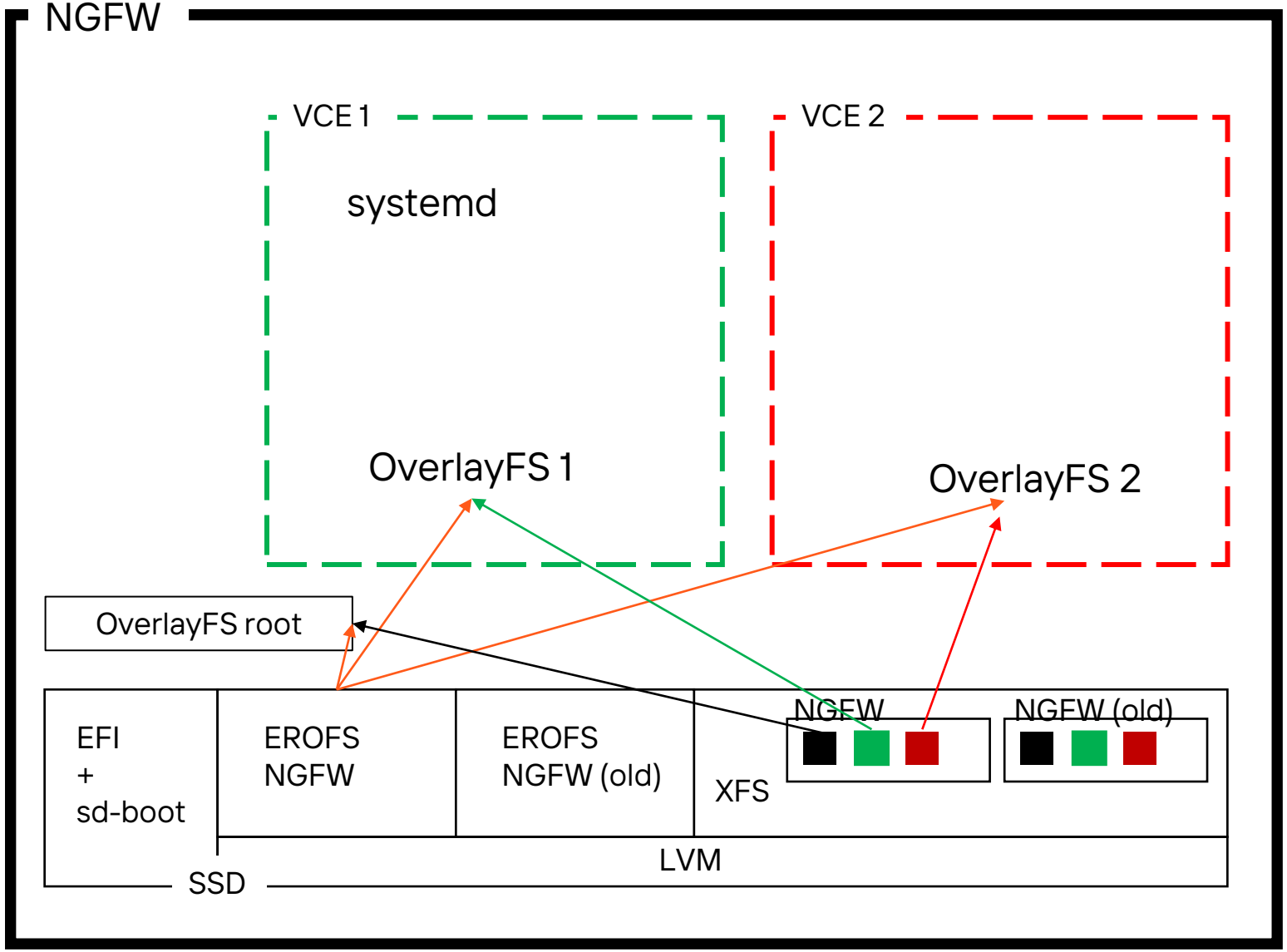
- Management plane — общий
- Несколько VCE — независимые
- Разные типы data plane (VPP/DPDK и legacy)



Файловая система: EROFS + OverlayFS + LVM

ideco

- Общий read-only EROFS
- OverlayFS для каждого VCE
- Нет отдельных контейнерных образов
- Лёгкие обновления, быстрые откаты.



ideco

Зрелый NGFW — это продукт, который строится по процессам РБПО, где качество обеспечено архитектурой, процессами и строгим контролем.

Это дополняет быстрое развитие сетевых функций, ФБ, а так же производительности продукта.

На защите ваших ценностей!

8 800 555 33 40

expert@ideco.ru

ideco.ru

ideco