ЦИФРОВЫЕ РЕШЕНИЯ

Российские мультивендорные решения:

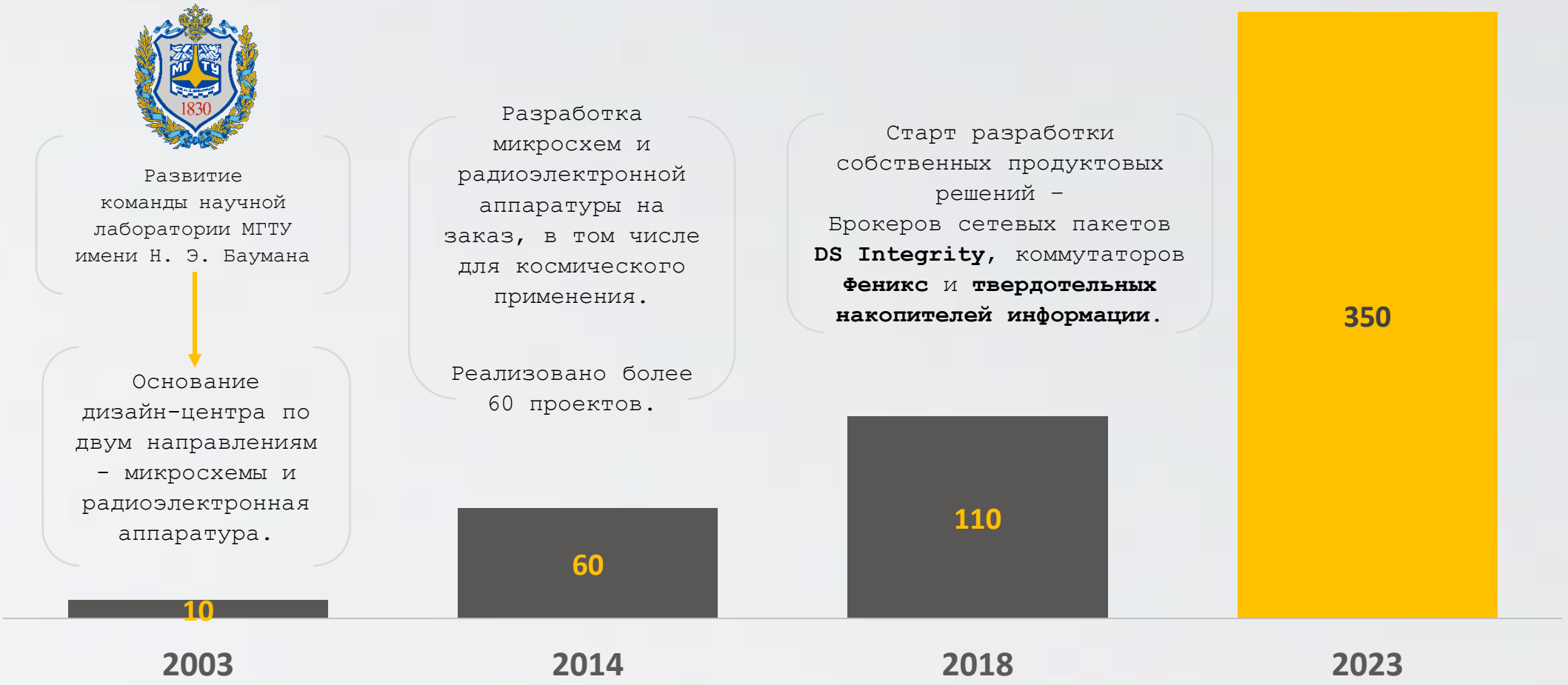
высокопроизводительная кластеризация NGFW и кейсы подключения NTA

Сергей Плотко | Директор по аналитике и интеграции

2023

ИСТОРИЯ

ЦИФРОВЫЕ РЕШЕНИЯ



МЫ СЕГОДНЯ

ЦИФРОВЫЕ РЕШЕНИЯ

НАПРАВЛЕНИЯ

- Телеком оборудование
- Твердотельные накопители
- Микросхемы
- Аппаратура для космоса

350+ СОТРУДНИКОВ

3 ОФИСА И СОБСТВЕННОЕ ПРОИЗВОДСТВО В МОСКВЕ И ПЕНЗЕ

РАЗРАБАТЫВАЕМ И ПРОИЗВОДИМ БОЛЕЕ 19 ЛЕТ

СВЯЗУЮЩЕЕ ЗВЕНО

ЦИФРОВЫЕ РЕШЕНИЯ

ЧТО НУЖНО ИБ ОТ ИТ ?

- Возможность видеть все данные из сети
- Легкий доступ к необходимым данным в любом сегменте сети

ЧТО НУЖНО ИТ ОТ ИБ ?

- Отсутствие взаимного влияния сети и систем ИБ

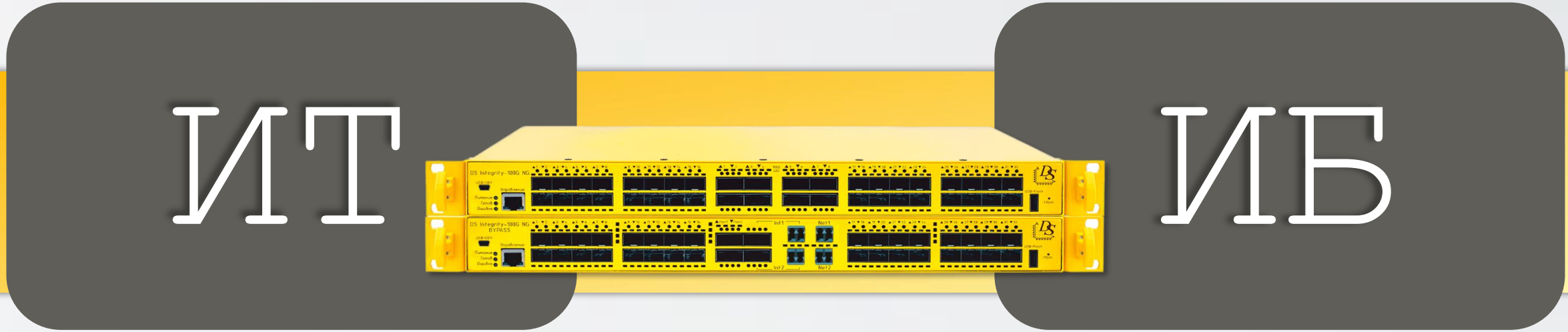
ИТ ? ИБ

СВЯЗУЮЩЕЕ ЗВЕНО

ЦИФРОВЫЕ РЕШЕНИЯ

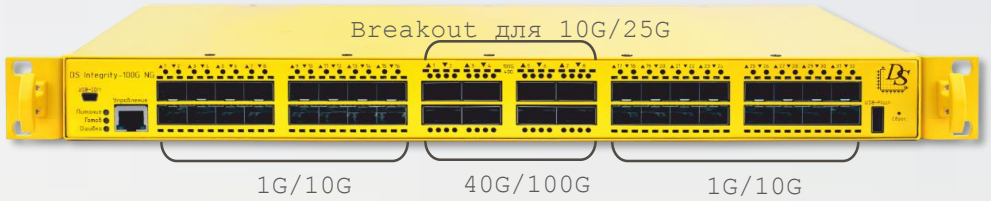
БРОКЕР СЕТЕВЫХ ПАКЕТОВ

- Полная видимость сети для систем ИБ
- Анализ производительности сети и простой траблшутинг для ИТ-подразделений
- Отсутствие влияния систем влияния ИБ на основную инфраструктуру сети
- Легкость масштабирования имеющихся и внедрения новых решений

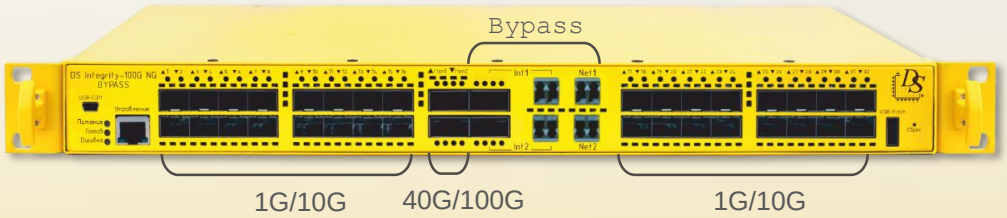


НАШИ РЕШЕНИЯ

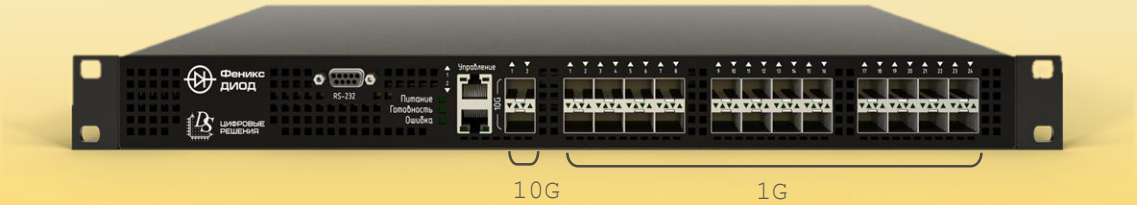
ЦИФРОВЫЕ РЕШЕНИЯ



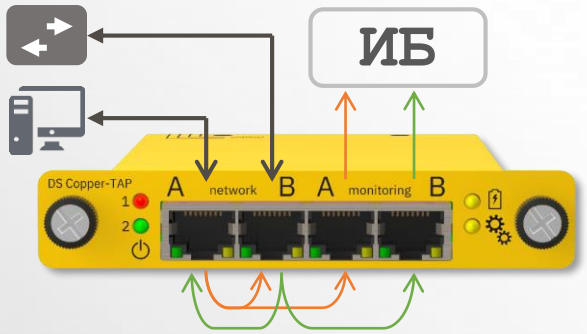
DS INTEGRITY NG



DS INTEGRITY NG BYPASS



ФЕНИКС-ДИОД



DS COPPER-TAP

DS OPTIC-TAP

от 1G до 100G
интерфейсы

до 1,6 Тбит/с
пропускная способность

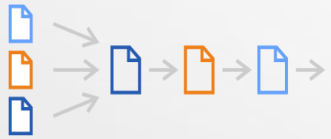
МИНПРОМТОРГ РОССИИ

ФСТЭК
в стадии сертификации по 4 уровню доверия

РЕШАЕМЫЕ ЗАДАЧИ

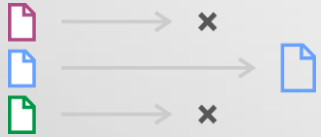
ЦИФРОВЫЕ РЕШЕНИЯ

БАЗОВЫЕ ФУНКЦИИ



АГРЕГАЦИЯ

БАЛАНСИРОВКА



ФИЛЬТРАЦИЯ

ЗЕРКАЛИРОВАНИЕ

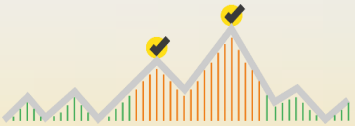
ДОПОЛНИТЕЛЬНЫЕ ФУНКЦИИ

ДЕДУПЛИКАЦИЯ

МОДИФИКАЦИЯ

ТУННЕЛИРОВАНИЕ

РАЗБОР ТУННЕЛЕЙ



ЗАЩИТА ОТ ВСПЛЕСКОВ

ГЕНЕРАЦИЯ sFlow

PORT STAMPING, TIME STAMPING

NGFW

КТО УШЕЛ С РЫНКА

ЦИФРОВЫЕ РЕШЕНИЯ

И другие производители

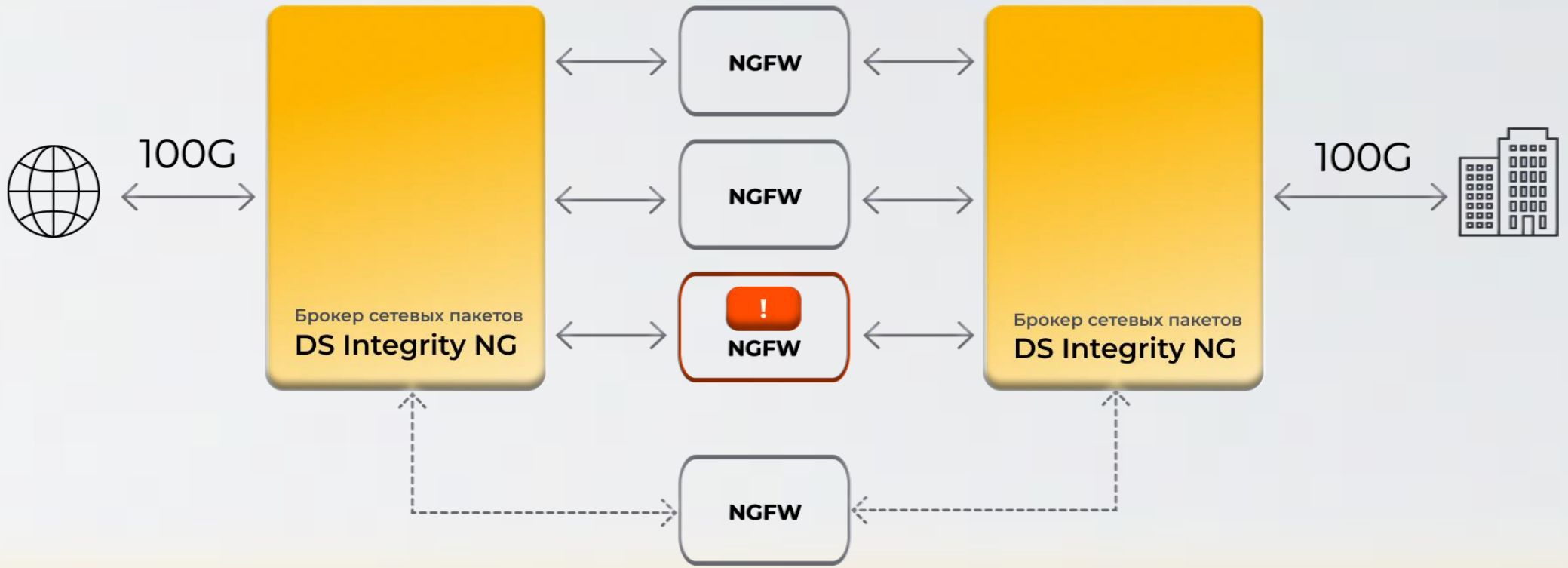
КАК ПОДКЛЮЧИТЬ NGFW?

ЦИФРОВЫЕ РЕШЕНИЯ

ЛЕГКО!

ЦИФРОВЫЕ РЕШЕНИЯ

кластеризация с помощью брокеров сетевых пакетов DS INTEGRITY NG

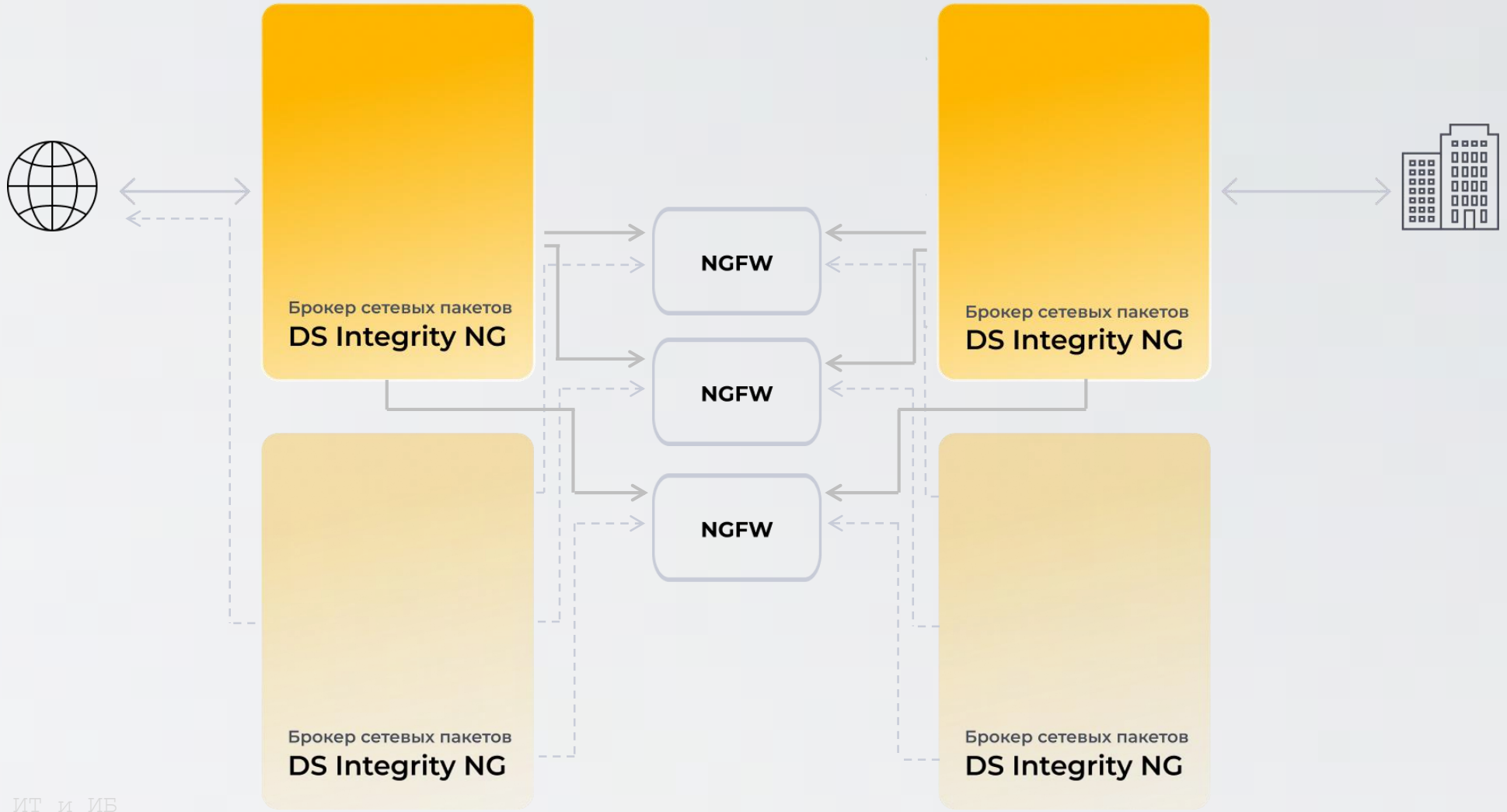


UserGate КОД безопасности ideco

БАЛАНСИРОВКА НАГРУЗКИ

ЦИФРОВЫЕ РЕШЕНИЯ

с использованием отказоустойчивого кластера брокеров



БАЛАНСИРОВКА НАГРУЗКИ

с использованием одного брокера

ЦИФРОВЫЕ РЕШЕНИЯ

БРОКЕРЫ СЕТЕВЫХ ПАКЕТОВ

ЦИФРОВЫЕ РЕШЕНИЯ

КТО УШЕЛ С РЫНКА

Gigamon®

ixia

А также

CGS Tower Networks ltd

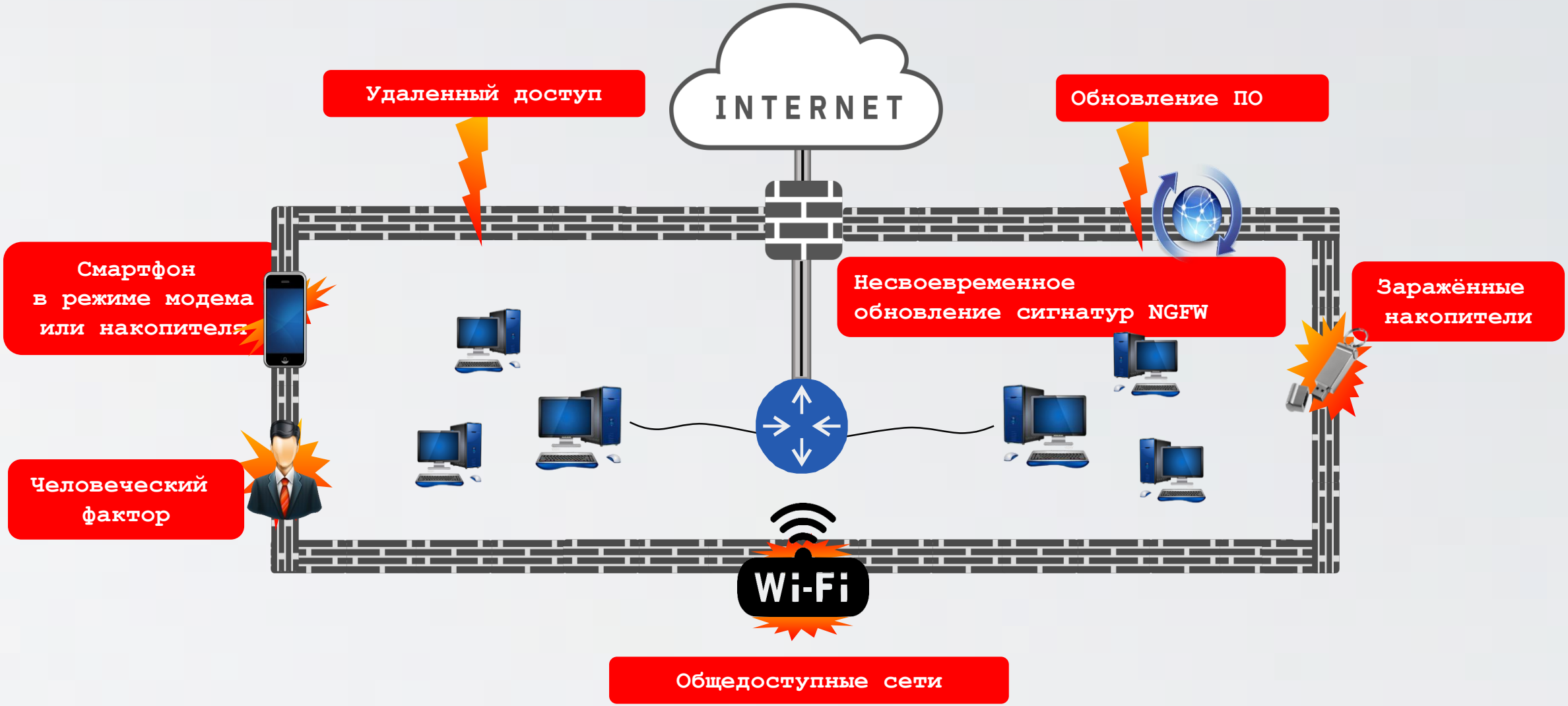
NIAGARA NETWORKS

PROFITAP

КОНТРОЛЬ ПЕРИМЕТРА –

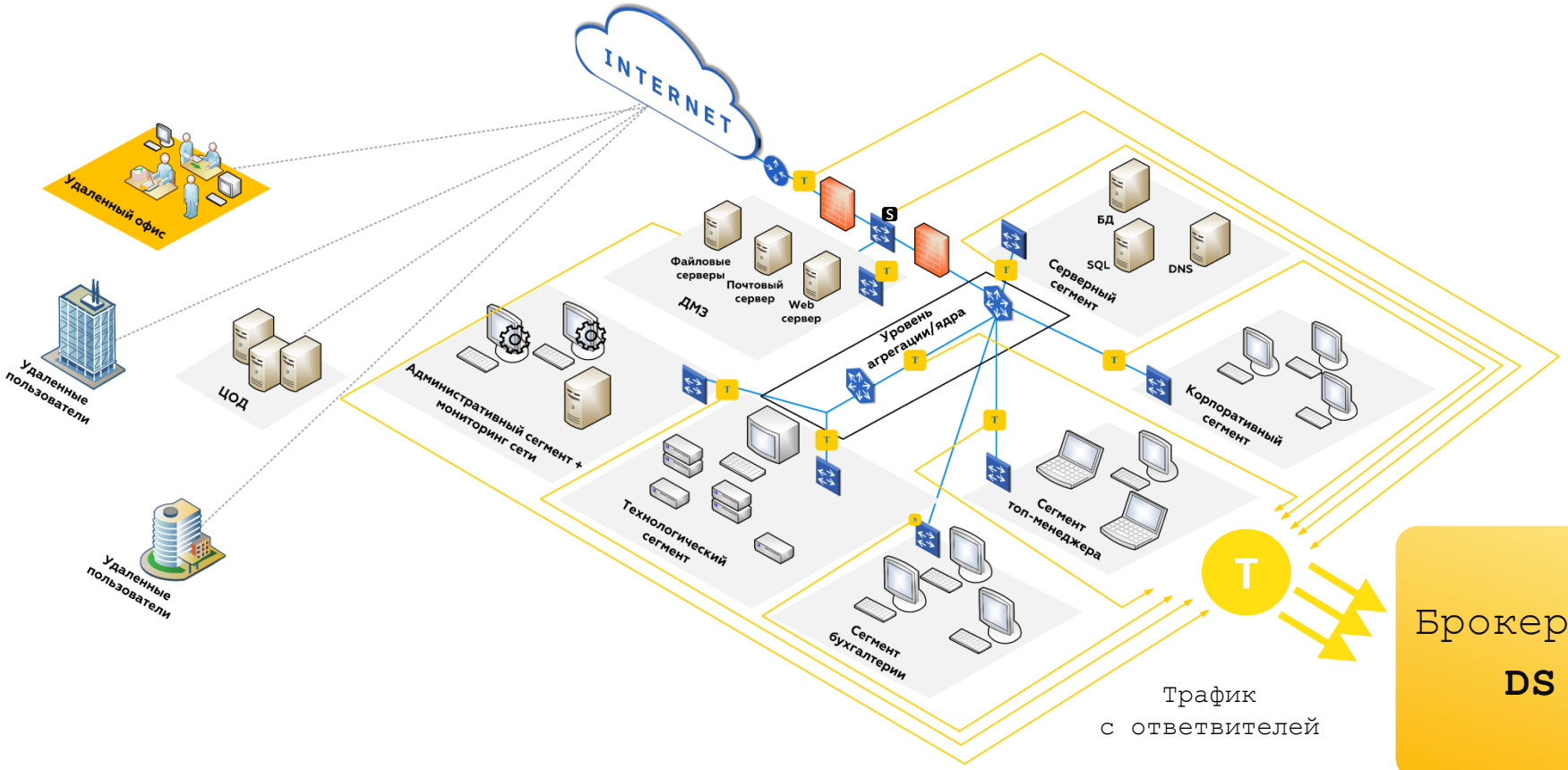
ЭТО ТОЛЬКО НАЧАЛО

ЦИФРОВЫЕ РЕШЕНИЯ



ПОДКЛЮЧЕНИЕ СИСТЕМ NTA

ЦИФРОВЫЕ РЕШЕНИЯ



Современная ИБ-инфраструктура помимо защиты периметра включает в себя мониторинг внутренних сегментов

Брокер сетевых пакетов **DS Integrity NG**

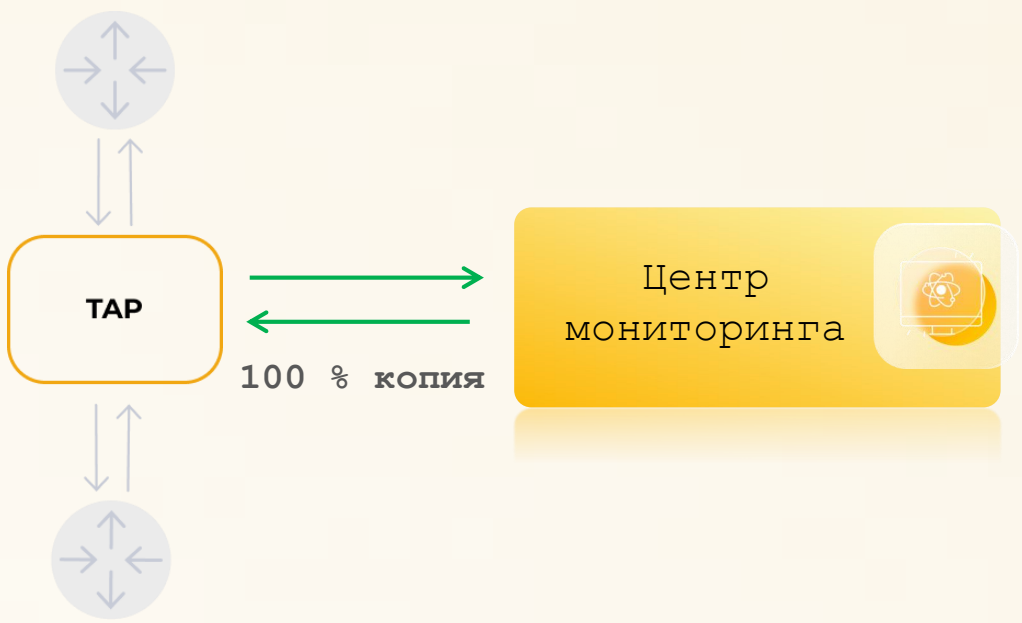
ИТ

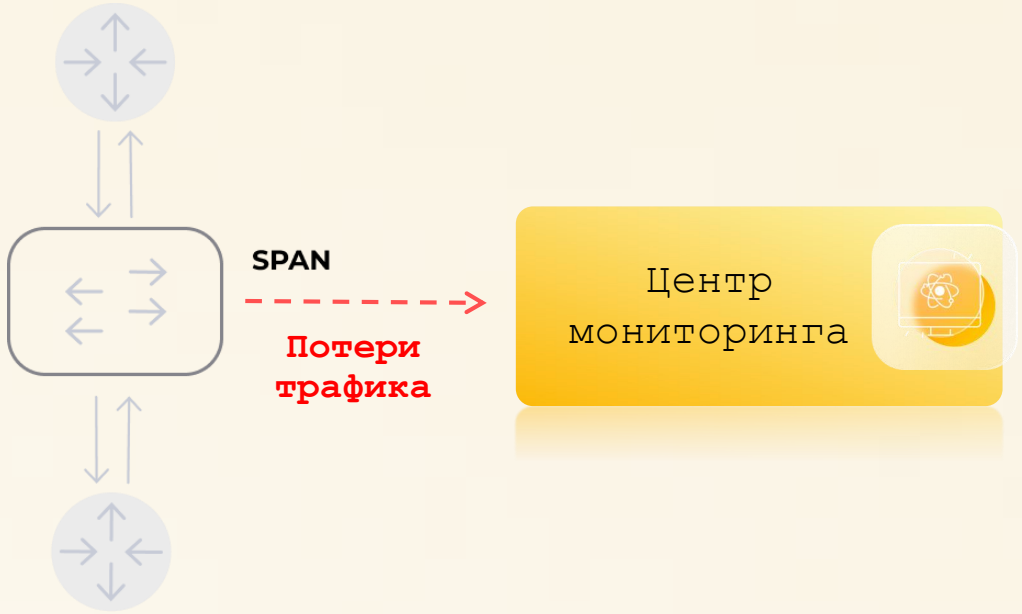
ИБ

positive technologies

МОНИТОРИНГ СЕТИ С TAP ИЛИ SPAN

ЦИФРОВЫЕ РЕШЕНИЯ





Передача трафика через TAP

- Требует установки дополнительного оборудования
- Высокая производительность
- Не подвержены атакам

Передача трафика через SPAN

- Не требует покупки
- Использует порты коммутатора
- Снижает производительность коммутатора

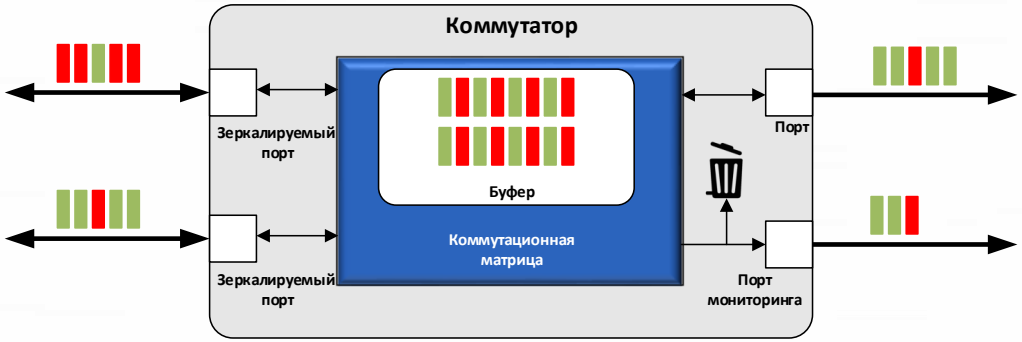
ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ SPAN

ЦИФРОВЫЕ РЕШЕНИЯ

Работа коммутатора без SPAN

- Пакеты копятся в буфере и удаляются после передачи в целевой порт

Потери зеркалируемого трафика

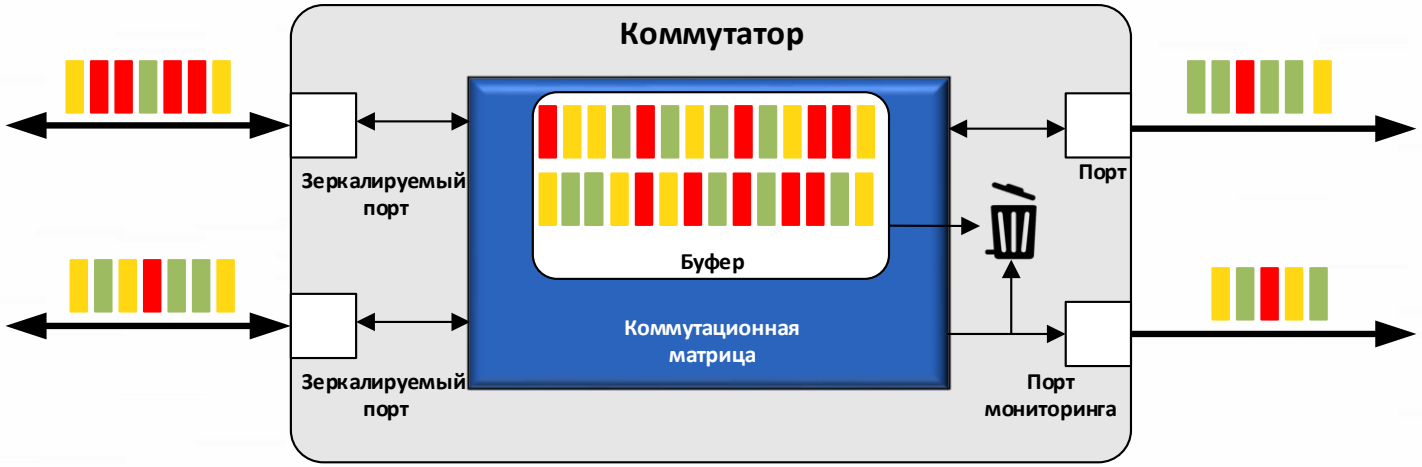


- SPAN порт не может передать весь трафик, циркулирующий по основным портам
- Зеркалируемый трафик отбрасывается

ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ SPAN

ЦИФРОВЫЕ РЕШЕНИЯ

Нарушение работы основной инфраструктуры

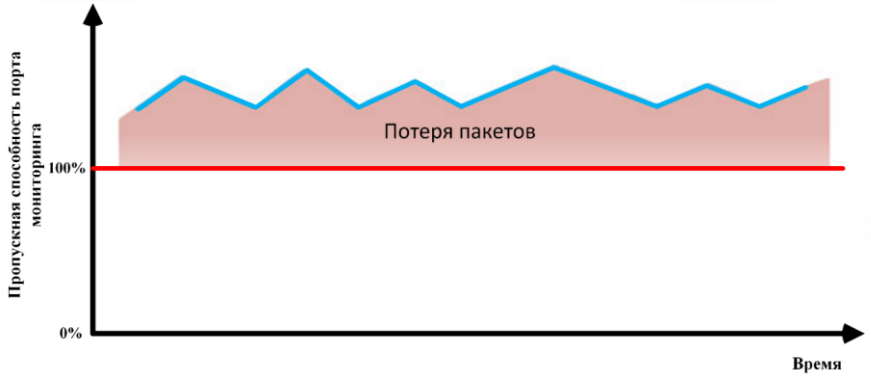


- Заполнение буфера пакетами из-за задержки удаления
- Потери зеркалируемого трафика
- Деградация производительности сети

ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ SPAN

ЦИФРОВЫЕ РЕШЕНИЯ

Поведение SPAN при нагрузке



- Зеркалируемый трафик в разы больше пропускной способности порта мониторинга
- Часть пакетов будет отброшена

Потери трафика при всплесках

- Даже при нагрузке до 10% трафик передается неравномерно
- Совпадение всплесков по нескольким портам приводят к потерям

	ИТ	ИБ
SPAN-порты	Плюсы	
	Функция коммутатора (обычно уже есть)	Не требуют дополнительного бюджета
	Минусы	
	• Требуют периодической проверки настроек • Приводят к потере пакетов и к деградации (или даже нарушению функционирования) сети	• Имеют низкий приоритет, что ведет к потере пакетов • Высокая зависимость от настроек (в том числе в случае взлома) • Не все пакеты зеркалируются • Отсутствует возможность оптимизации трафика
TAP-ответвители	Плюсы	
	• Полная прозрачность для сетевых устройств – не влияют на передачу трафика • Не требуют специальной настройки и обновлений • Зеркалируют служебный трафик, полезный для траблшутинга сети	• 100% копия трафика из инфраструктуры без искажений • Пассивное решение, невозможно вывести из строя путем внешних атак • Легко масштабируются
	Минусы	
	Требуют технологическое окно для установки	Покупается как самостоятельное решение

SPAN В АСУ ТП

ЦИФРОВЫЕ РЕШЕНИЯ

загрузка коммутатора до 5% - низкая вероятность потерь

- Меньше точек отказа
- Уменьшение затрат на оборудование
- Включается без разрыва связи
- Не занимает места

КАКИЕ ПРОБЛЕМЫ ОСТАНУТСЯ?

ЦЕЛОСТНОСТЬ НАСТРОЙКИ *(человеческий и технический фактор)*	СЛУЖЕБНЫЙ ТРАФИК НЕ ЗЕРКАЛИРУЕТСЯ В SPAN	ВОЗНИКНОВЕНИЕ ДУБЛИКАТОВ ПАКЕТОВ	РОСТ ОБЪЕМА ТРАФИКА *(увеличение количества оборудования и атаки хакеров)*
Последствия			
Трафик не поступает на систему анализа или поступает «мусорный» трафик в сеть АСУ ТП	Пропущенная атака хакеров	Повышение нефункциональной нагрузки на NTA	Потеря исходных данных Деградация сети (потеря трафика на основных портах)

ВАЖНОСТЬ ПОЛНОТЫ И ЦЕЛОСТНОСТИ ИСХОДНЫХ ДАННЫХ

ЦИФРОВЫЕ РЕШЕНИЯ

Попробуйте решить.
Легко?

$$\begin{cases} x^2 + y + 2z = 8 \\ x + 2y^2 + 4z = 11 \\ x + 11y^2 + 8z^2 = 0 \end{cases}$$

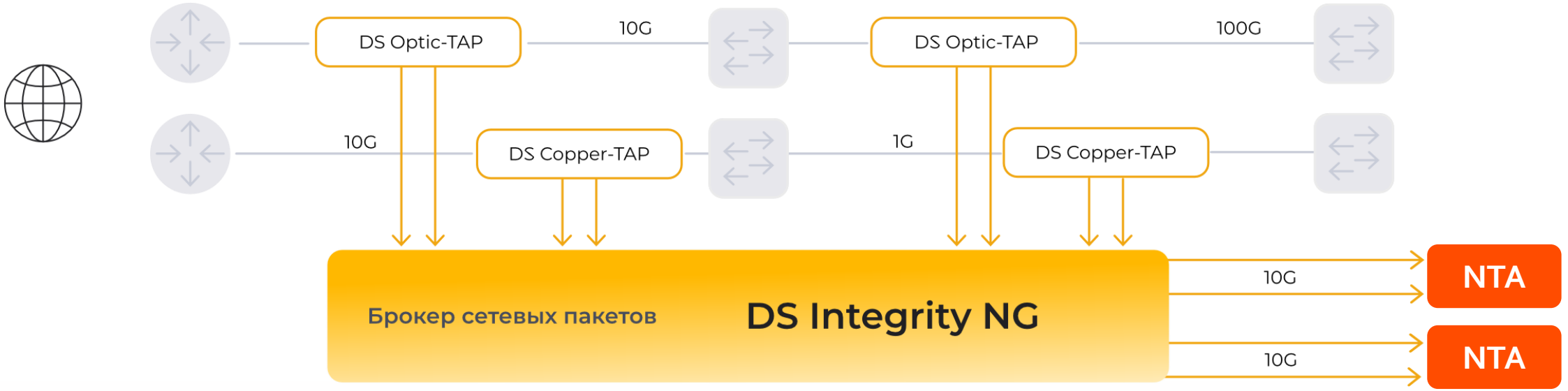
А так?

$$\begin{cases} x^2 + y + 2z = 8 \\ ? + 2y^2 + 4z = 11 \\ x + 11y^2 + 8z^2 = 0 \end{cases}$$

1 Мегабайт переданных данных ~ 700 пакетов
Потеря даже одного из них делает сессию "невидимой"

ПОДКЛЮЧЕНИЕ СИСТЕМ NTA

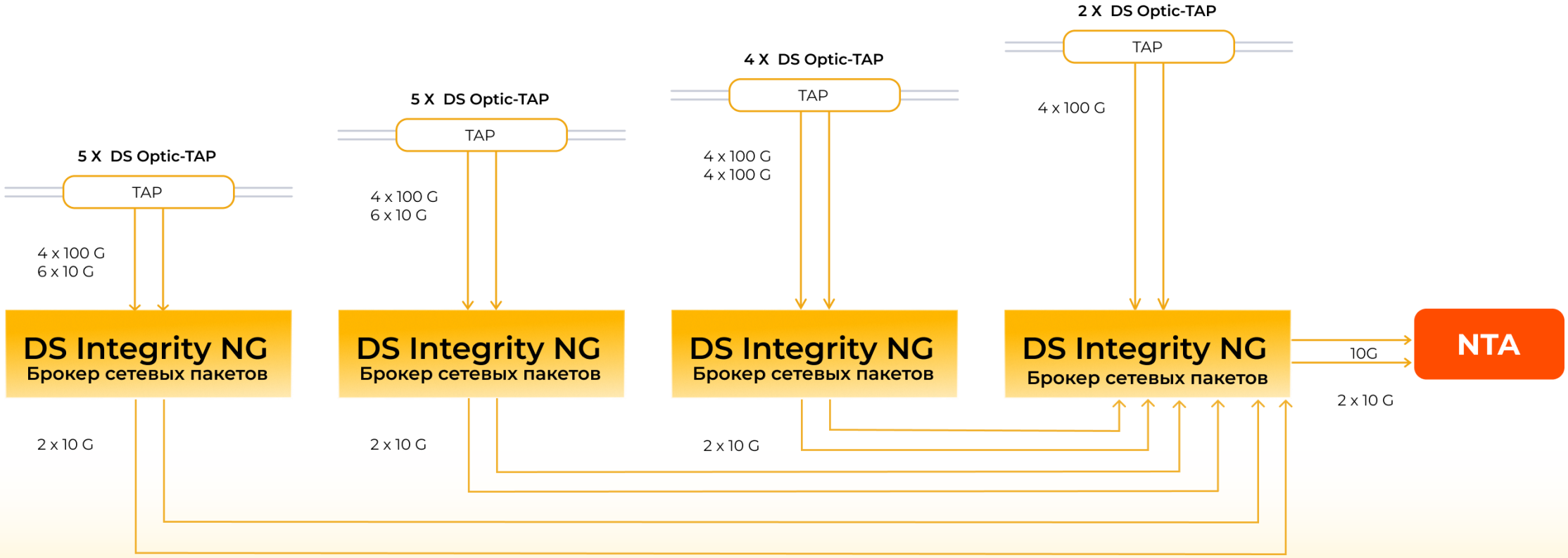
ЦИФРОВЫЕ РЕШЕНИЯ



positive technologies

КАСКАДИРОВАНИЕ ПАКЕТНЫХ БРОКЕРОВ

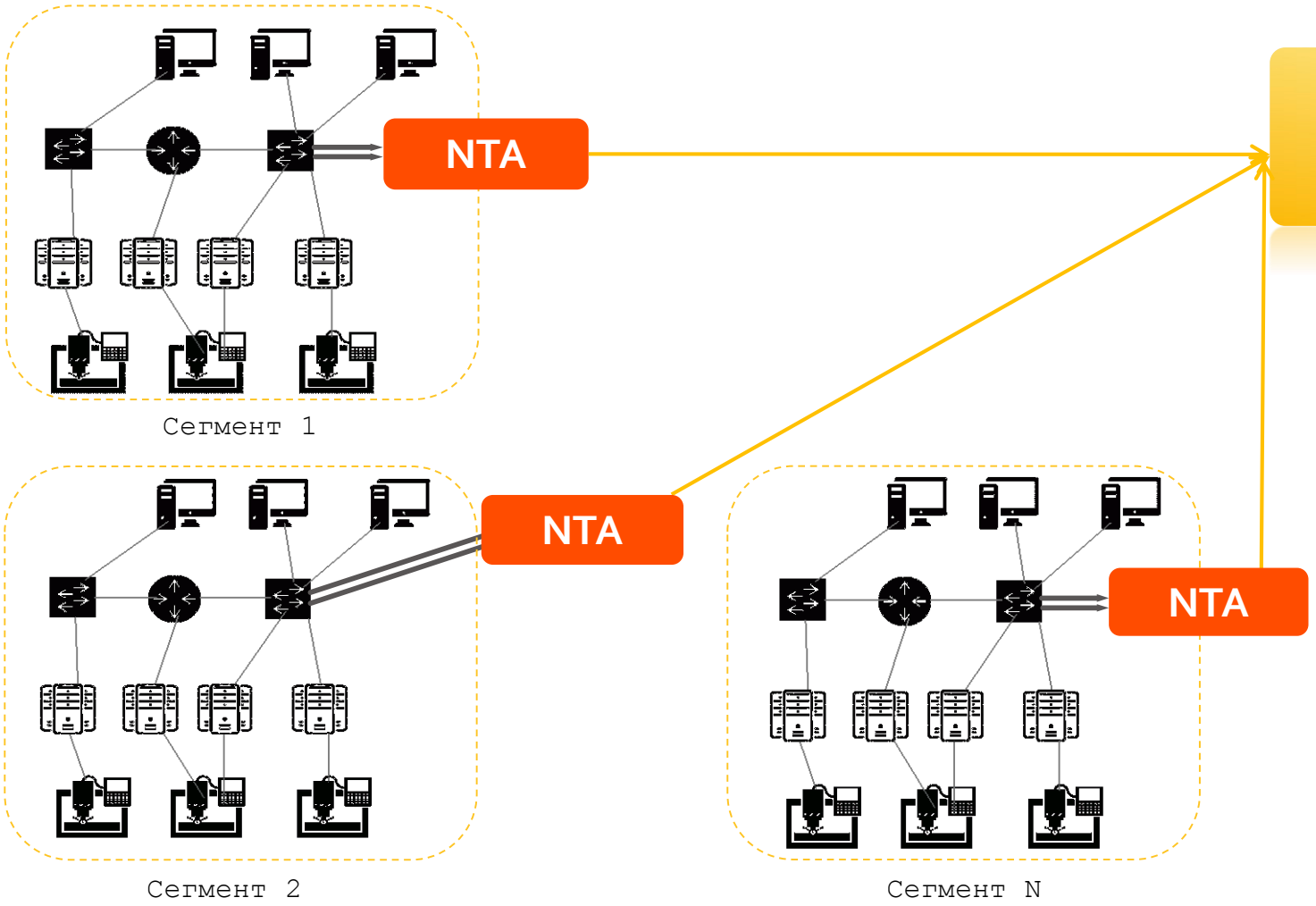
ЦИФРОВЫЕ РЕШЕНИЯ



positive technologies

ПОДКЛЮЧЕНИЕ СЕТЕЙ АСУ ТП

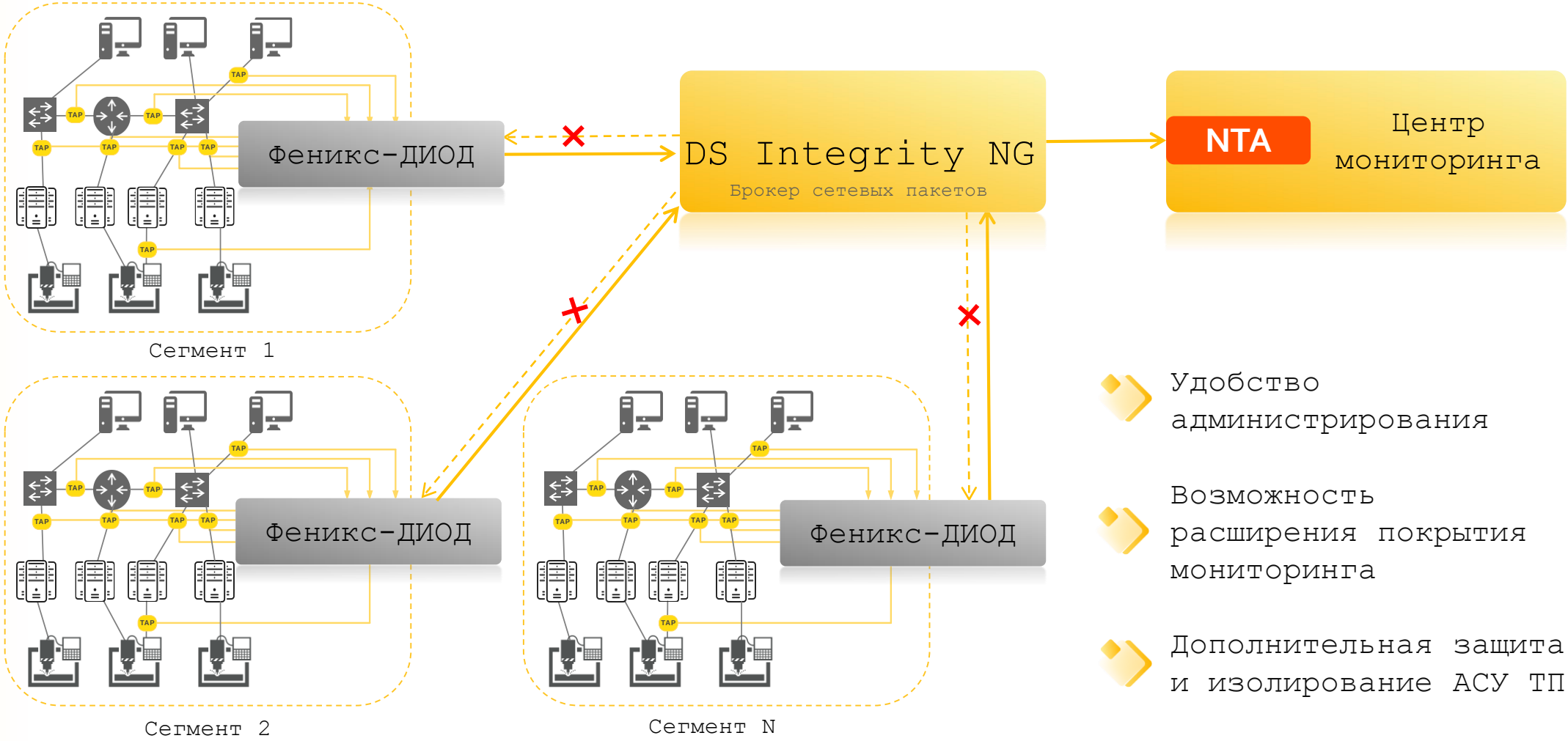
ЦИФРОВЫЕ РЕШЕНИЯ



- Усложнение администрирования
- Ограничение масштабирования
- Риски воздействия средств мониторинга на АСУ ТП

ПОДКЛЮЧЕНИЕ СЕТЕЙ АСУ ТП

ЦИФРОВЫЕ РЕШЕНИЯ

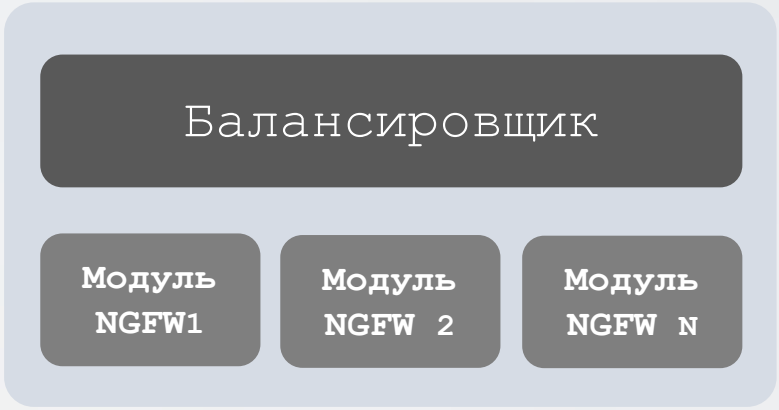


- Удобство администрирования
- Возможность расширения покрытия мониторинга
- Дополнительная защита и изолирование АСУ ТП

ОТ МОНОВЕНДОРНЫХ РЕШЕНИЙ К КОМПЛЕКСНОЙ СИСТЕМЕ

ЦИФРОВЫЕ РЕШЕНИЯ

ЕДИНОЕ РЕШЕНИЕ



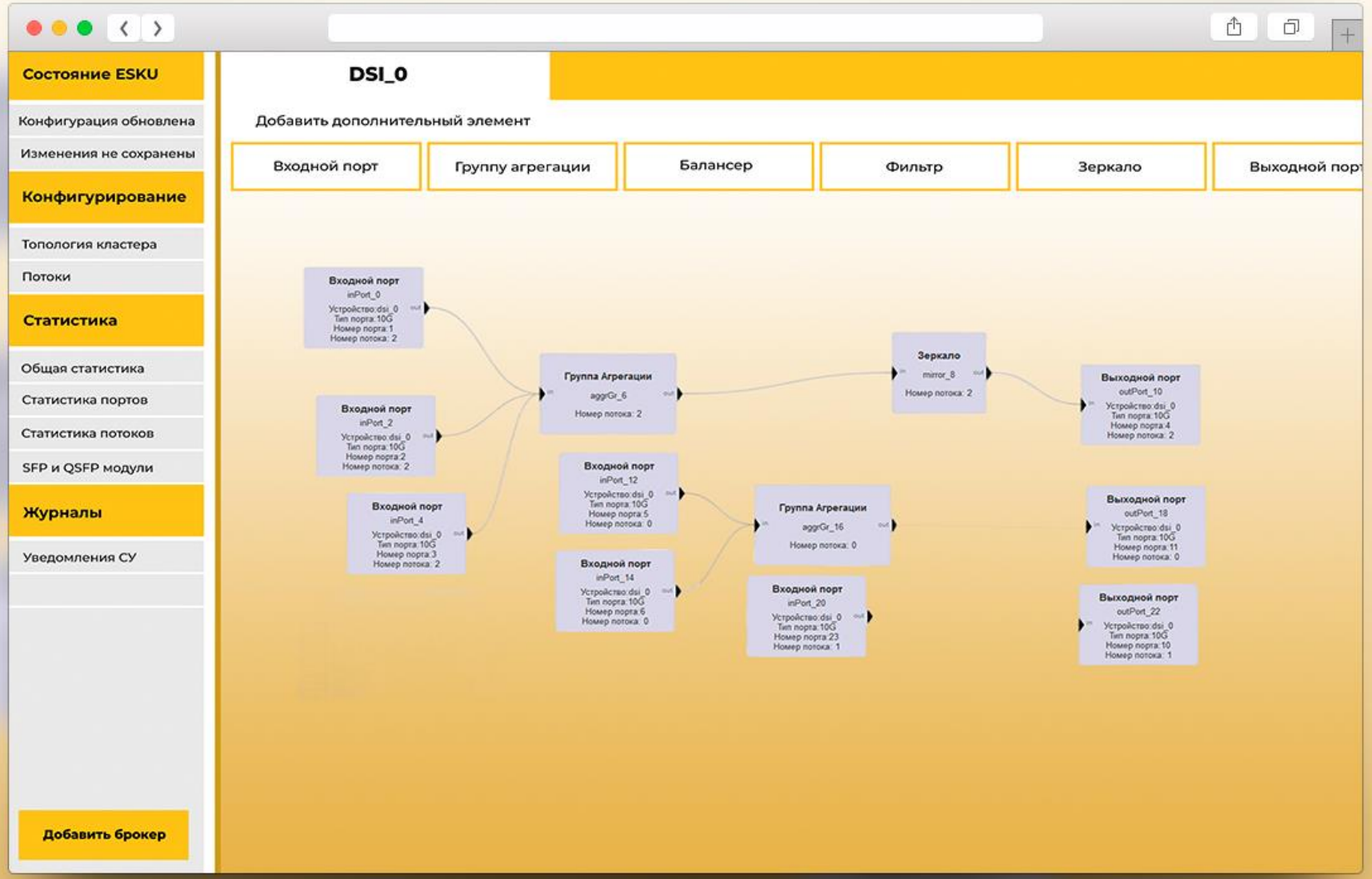
+ Простая настройка
- Сложности при масштабировании архитектуры и внедрении новых систем

ЕДИНАЯ СИСТЕМА

+ Дополнительные возможности по конфигурации и предобработке трафика
- Нетипичная первоначальная инициализация

ЕДИНАЯ СИСТЕМА УПРАВЛЕНИЯ

ЦИФРОВЫЕ РЕШЕНИЯ



- Кластеризация брокеров сетевых пакетов с расширением портовой емкости
- Централизованное управление брокерами сетевых пакетов
- Интуитивно понятный интерфейс

Удаленный доступ

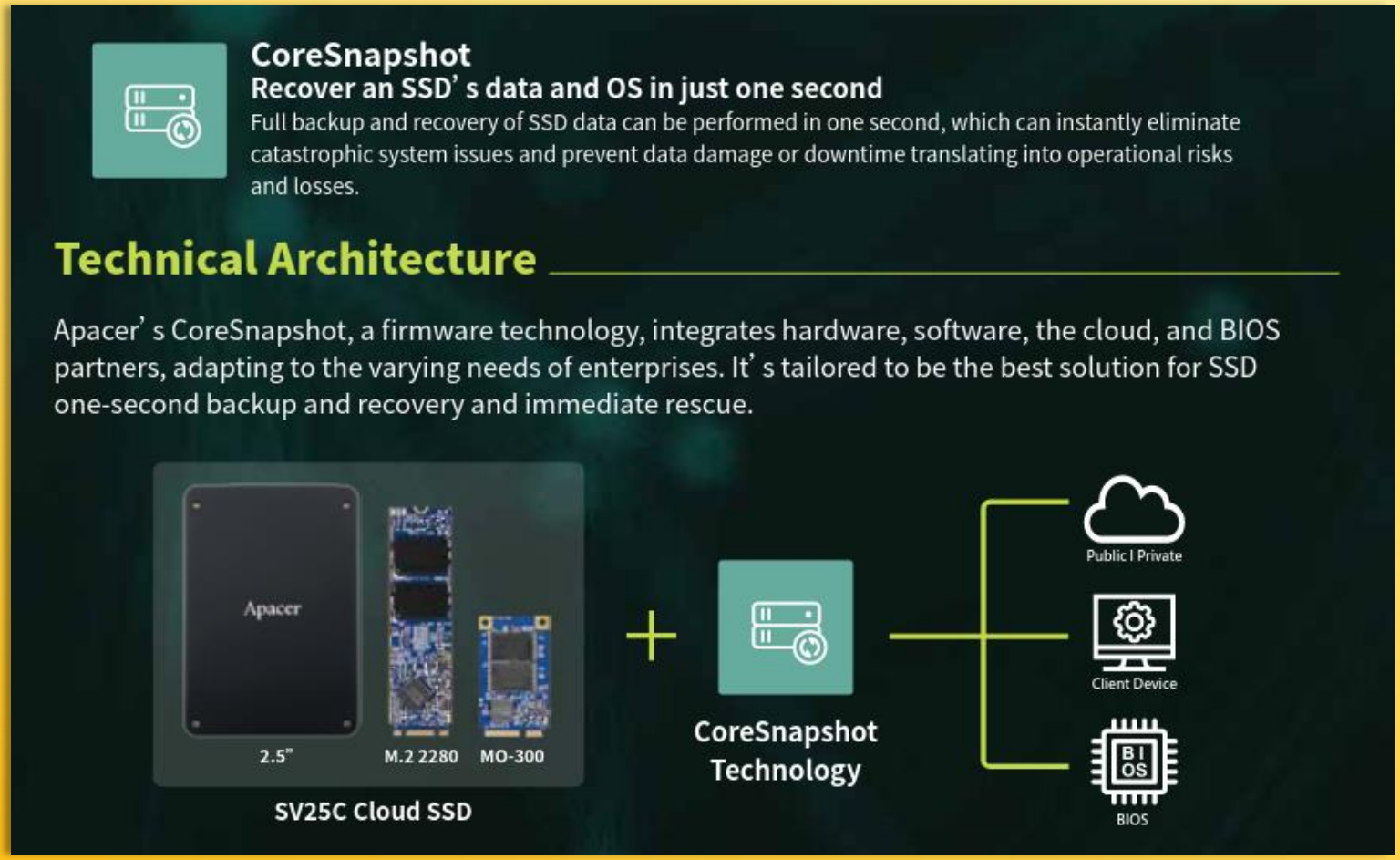
ЦИФРОВЫЕ РЕШЕНИЯ

- Возможность удаленного доступа к SSD от Innodisk описана как штатный и удобный функционал покупного диска
- Другие диски могут иметь тот же функционал как скрытую недекларируемую возможность

Удаленный доступ к SSD Apacer

ЦИФРОВЫЕ РЕШЕНИЯ

Пример из документации



НАКОПИТЕЛИ

ЦИФРОВЫЕ РЕШЕНИЯ

USB 3.0
УРАН

USB 3.0
Аметист

USB 2.0
Аметист-Б

SSD SATA 6GB/S
Оникс

SSD SATA 6GB/S
ТИТАН

Сертифицировано

Находятся в стадии сертификации

Российский контроллер собственной разработки

Защита от подмены ВПО и УИН

До 25 000 количество циклов перезаписи

От -40 до +70 °С рабочая температура

г. Москва, проезд Завода Серп и Молот,
д. 10, БЦ Интеграл

habr

8 (926) 207-27-02 | Сергей Плотко
Директор по аналитике и интеграции

8 (916) 032-23-23 | Вячеслав Пальчиков
Руководитель отдела по работе с партнерами

СПАСИБО ЗА ВНИМАНИЕ!

Связаться с нами: sales@dsol.ru