ЦИФРОВЫЕ РЕШЕНИЯ

# ПОДКЛЮЧЕНИЕ СРЕДСТВ СЕТЕВОЙ БЕЗОПАСНОСТИ К ИНФРАСТРУКТУРЕ АСУ ТП

**Сергей Плотко**

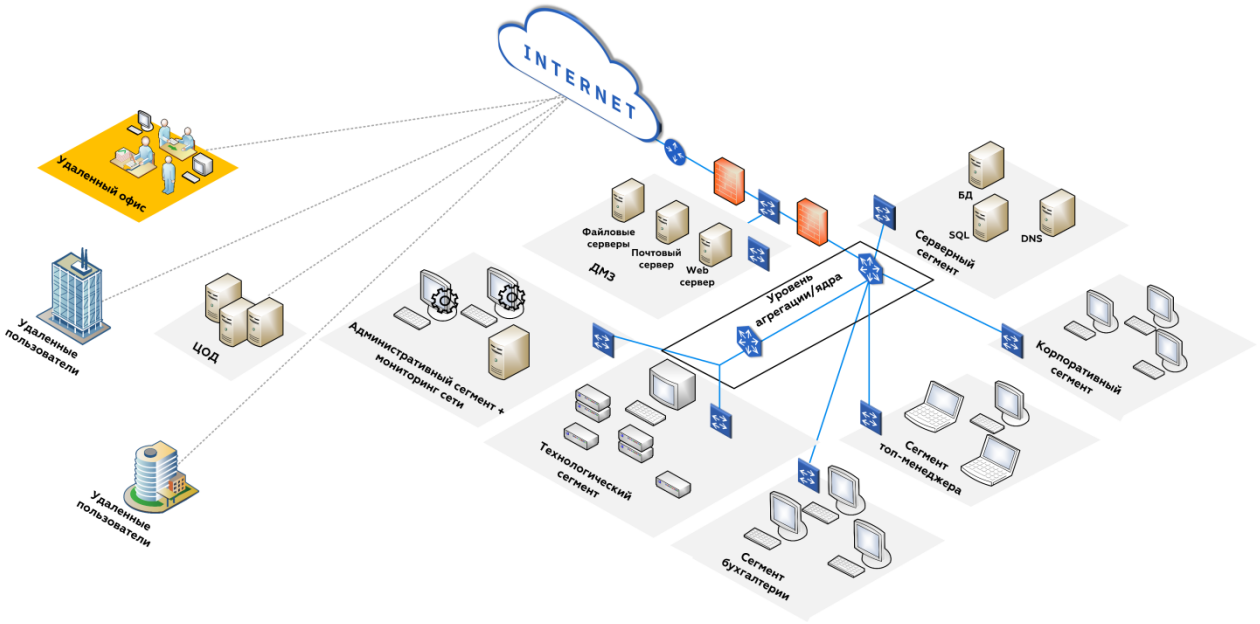
Директор по аналитике и интеграции
АО «НПП «Цифровые решения»

# Проблемы современной ИТ-инфраструктуры

ЦИФРОВЫЕ РЕШЕНИЯ

**20 лет назад**


**Сегодня**




Усложнение ИТ-инфраструктуры, увеличение скоростей и количества проколов передачи данных требует внедрения инструментов анализа и ИБ различных типов.
В свою очередь, такие инструменты имеют ограничения по подключению и производительности, а также свои требования к исходным данным и критичности работы

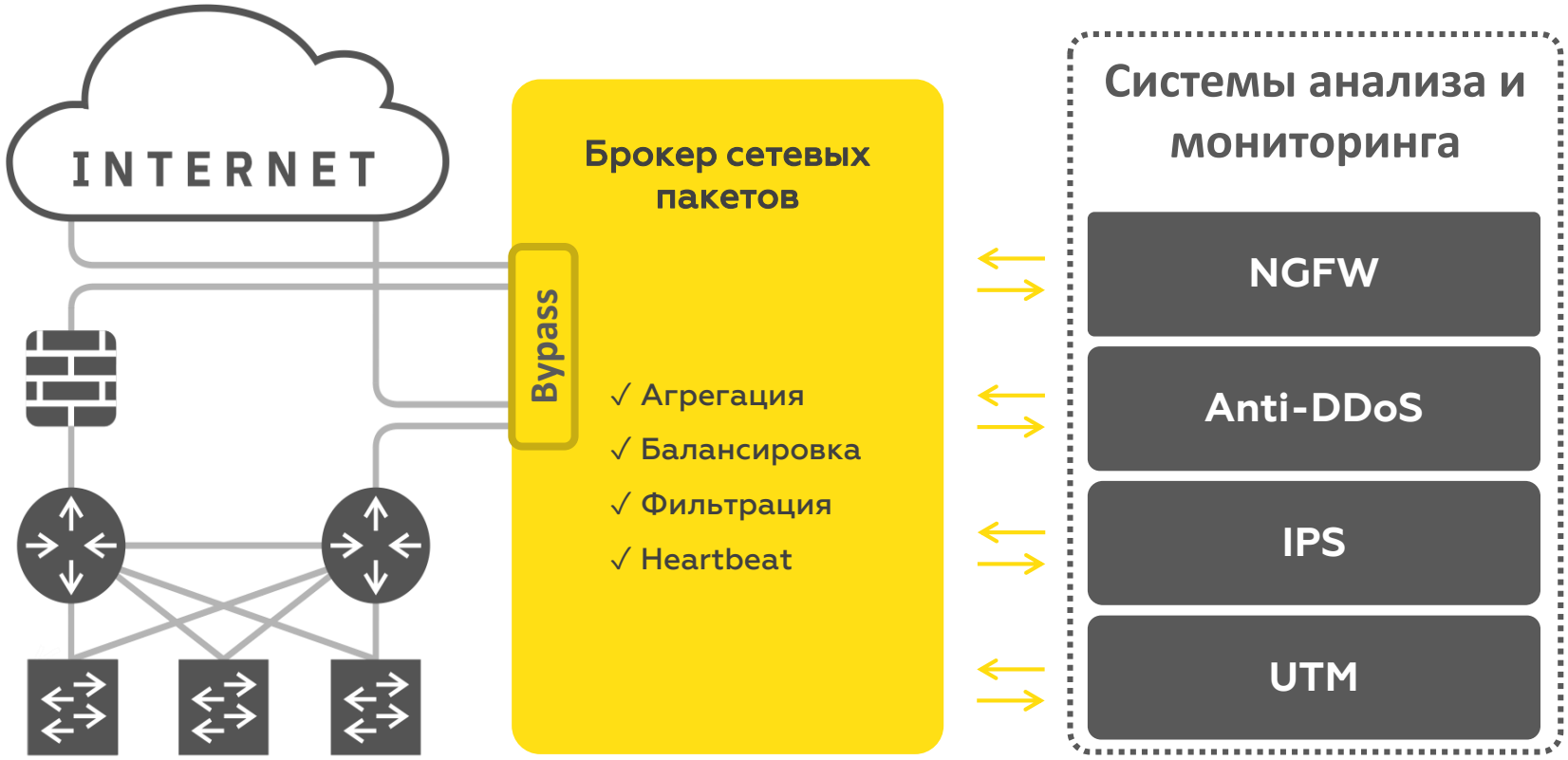
# Связующее звено в ИТ-инфраструктуре

ЦИФРОВЫЕ РЕШЕНИЯ


Брокер сетевых пакетов связывает две ключевых области внутри ИТ-инфраструктуры:

- Помогает организовать эффективную схему взаимодействия оборудования
- Оптимизирует весь трафик перед отправкой на системы мониторинга и ИБ

# Активное подключение средств анализа и ИБ



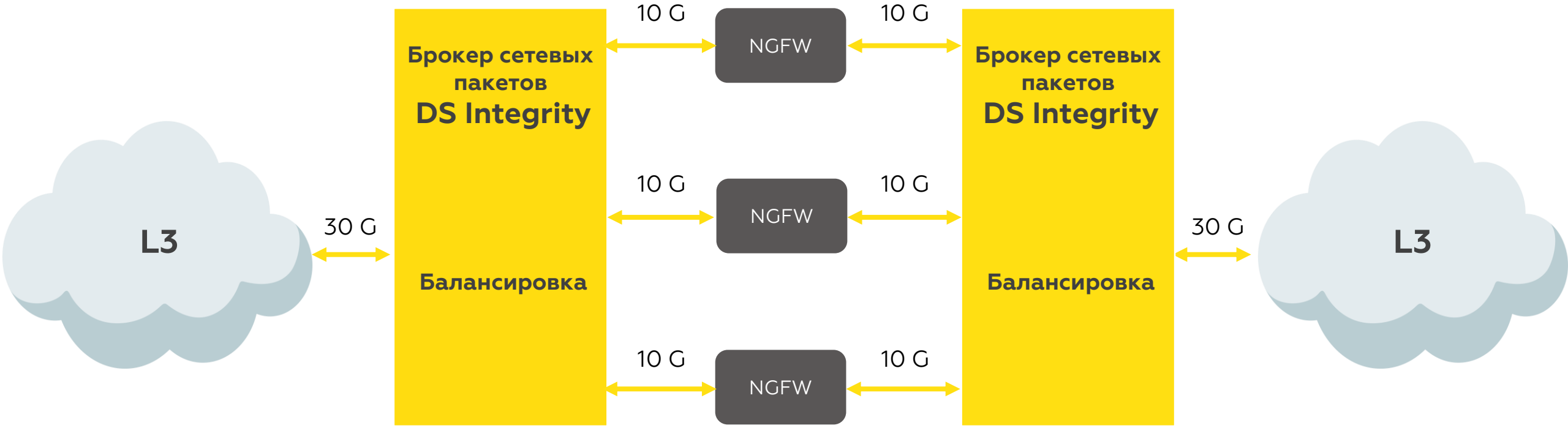

КОД безопасности

UserGate

✓ Технологические партнёры

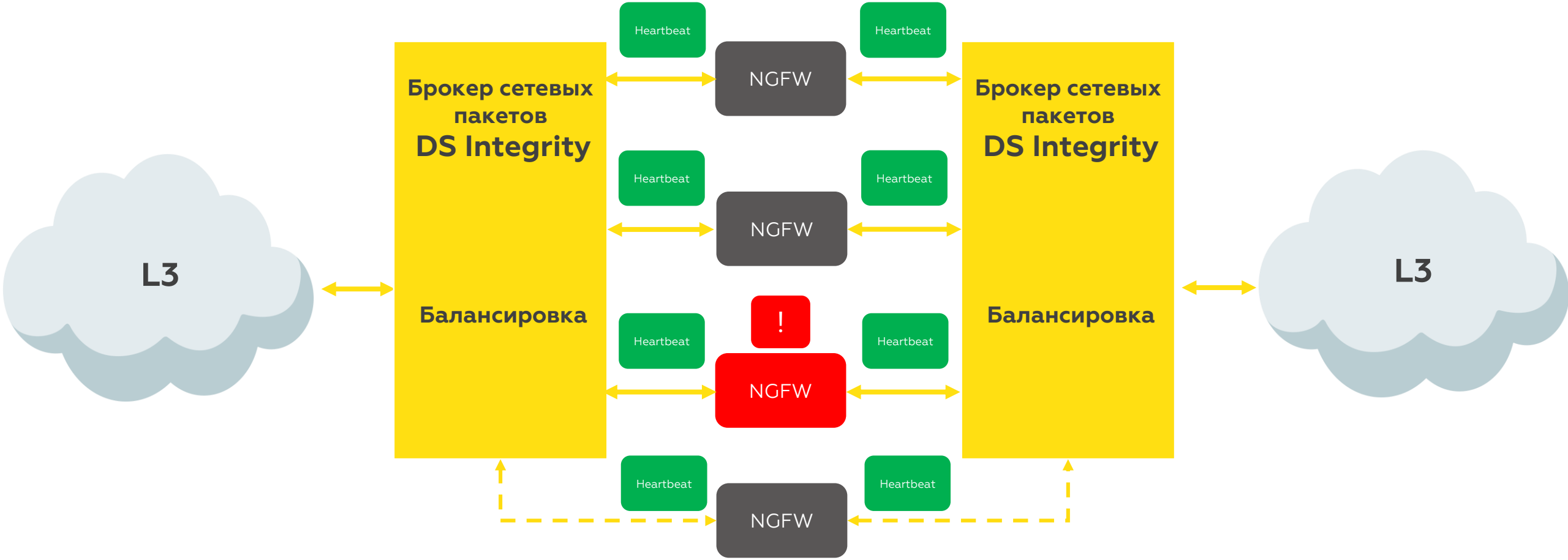
Активное подключение предполагает установку брокера сетевых пакетов **с функцией Bypass** «в разрыв» канала

# Распределение трафика



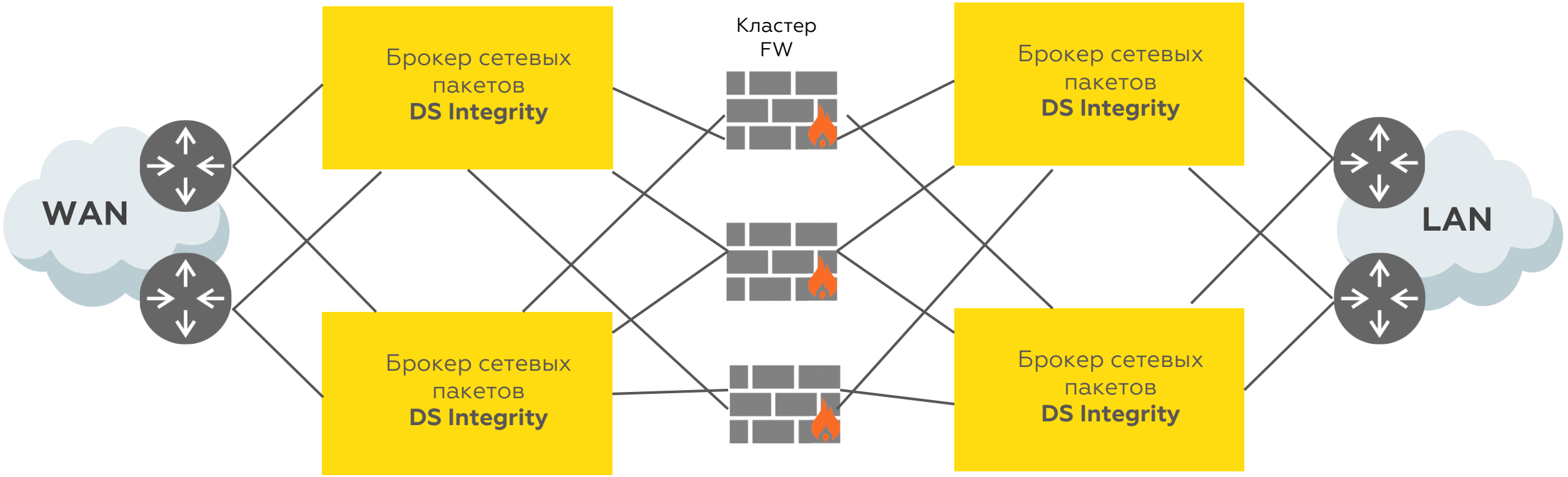

Брокер сетевых пакетов DS Integrity балансирует нагрузку на необходимое количество анализаторов, разделяя потоки трафика с сохранением целостности сессий/потоков

# Резервирование систем и проверка их работоспособности




Для контроля работоспособности отдельных устройств, брокер сетевых пакетов DS Integrity NG добавляет в трафик специальные пакеты (технология Heartbeat).
Если обнаруживается нерабочее устройство, происходит мгновенная перебалансировка трафика между оставшимися в кластере средствами.

# Отказоустойчивая балансировка группы МЭ



# Подключение пассивных средств анализа


positive technologies

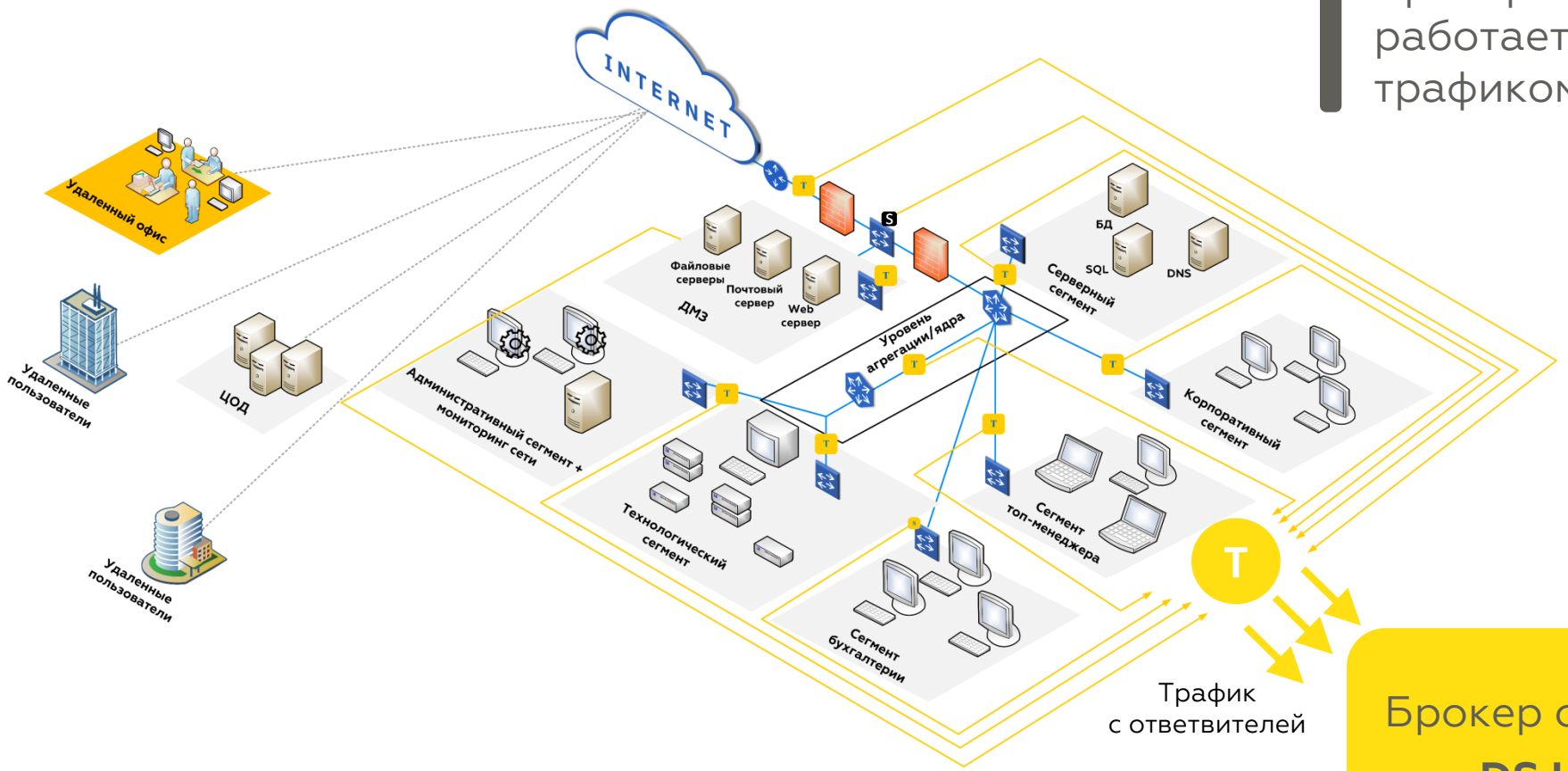
✓ Технологический партнёр

Пассивное подключение брокера сетевых пакетов к ИТ-Инфраструктуре осуществляется через SPAN-порты или ответвители трафика (TAP), например, с помощью ответвителей DS Optic-TAP или DS Copper-TAP

# Подключение пассивных средств анализа

ЦИФРОВЫЕ РЕШЕНИЯ

Брокер сетевых пакетов DS Integrity NG работает как с трафиком от TAP, так и с трафиком со SPAN-портов




Брокер сетевых пакетов **DS Integrity NG**

ИТ

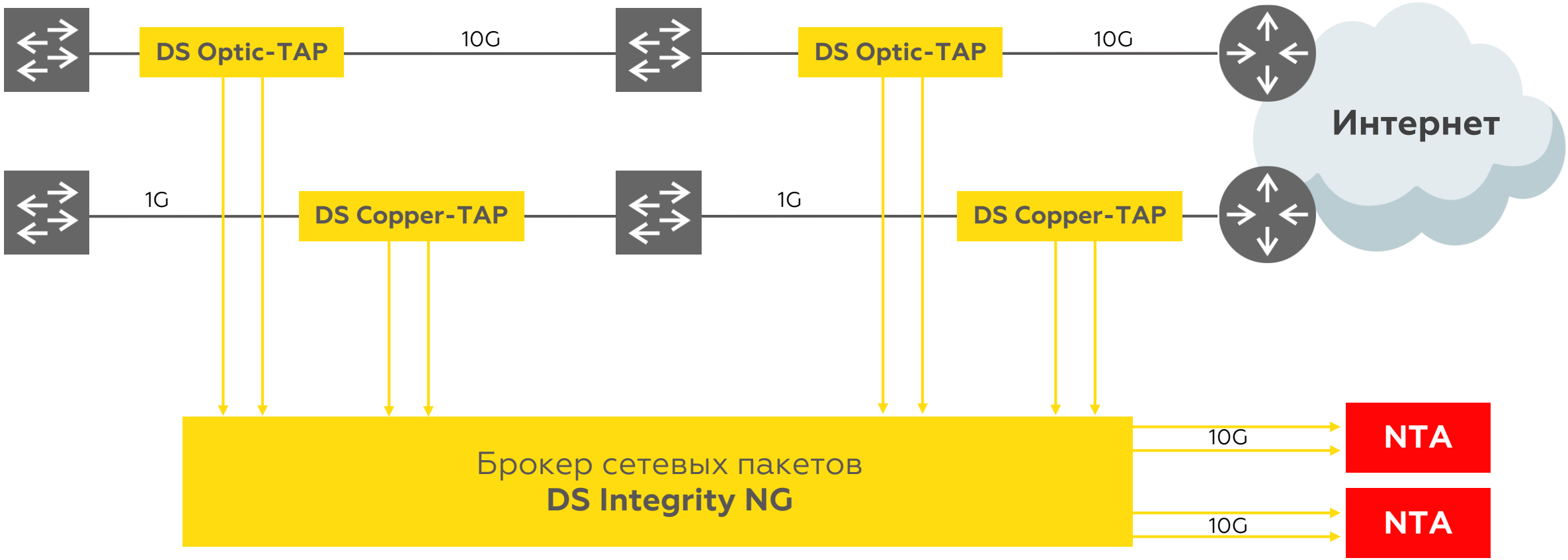
ИБ

# Сравнение пассивного подключения через SPAN и TAP

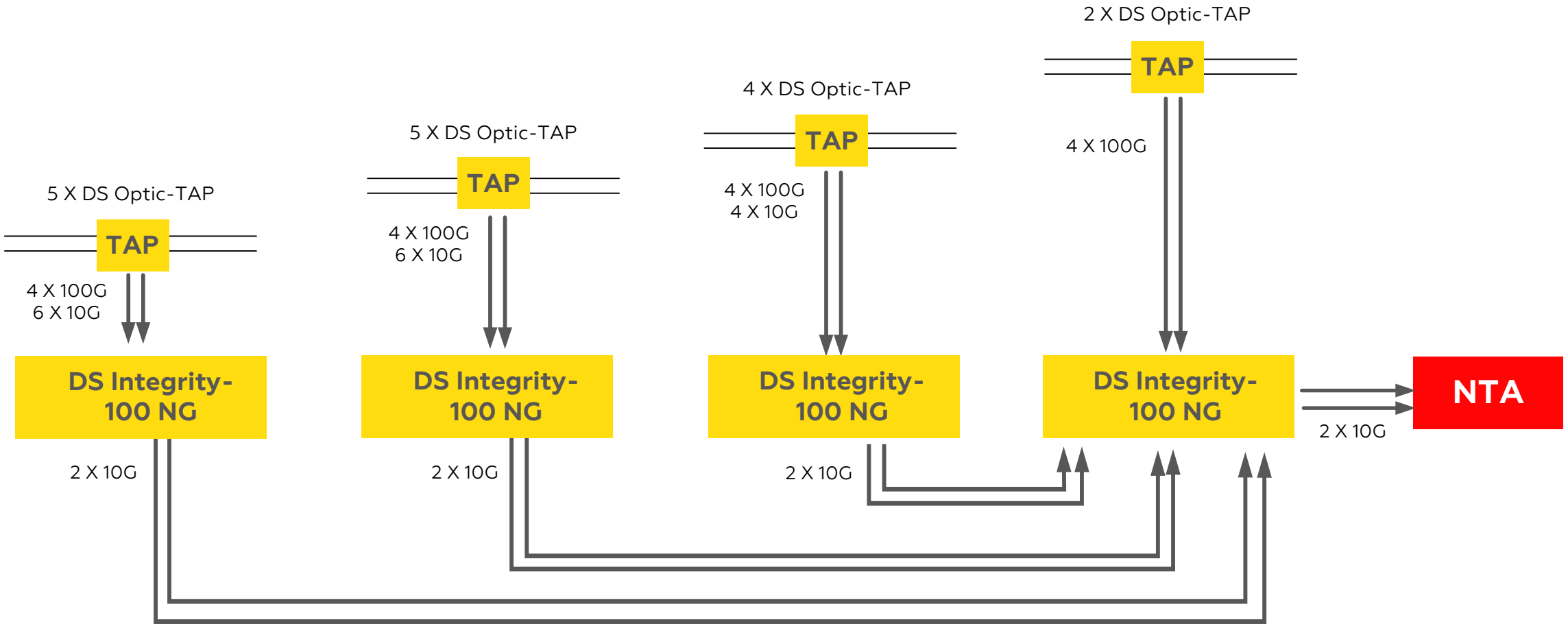
ЦИФРОВЫЕ РЕШЕНИЯ

| | ИТ | ИБ |
|---|---|---|
| **SPAN-порт коммутатора** | + Функция коммутатора обычно уже встроена<br>— Требуется периодическая проверка настроек<br>— Приводит к потере пакетов, к деградации или даже к нарушению функционирования сети | + Не требует дополнительных расходов<br>— Имеет низкий приоритет, что ведет к потере пакетов<br>— Высокая зависимость от настроек (в т.ч. в случае взлома)<br>— Не все пакеты зеркалируются<br>— Отсутствует возможность оптимизации трафика |
| **TAP ответвители** | + Полная прозрачность для сетевых устройств (нет влияния на передачу трафика)<br>+ Не требуют специальной настройки и обновлений<br>+ Зеркалируют служебный трафик, полезный для траблшутинга сети<br>— Требуют технологическое окно для установки | + Снимают 100% копию трафика без искажений<br>+ Пассивное решение, которое невозможно вывести из строя внешними атаками<br>+ Легко масштабируется<br>— Приобретается как самостоятельное решение |

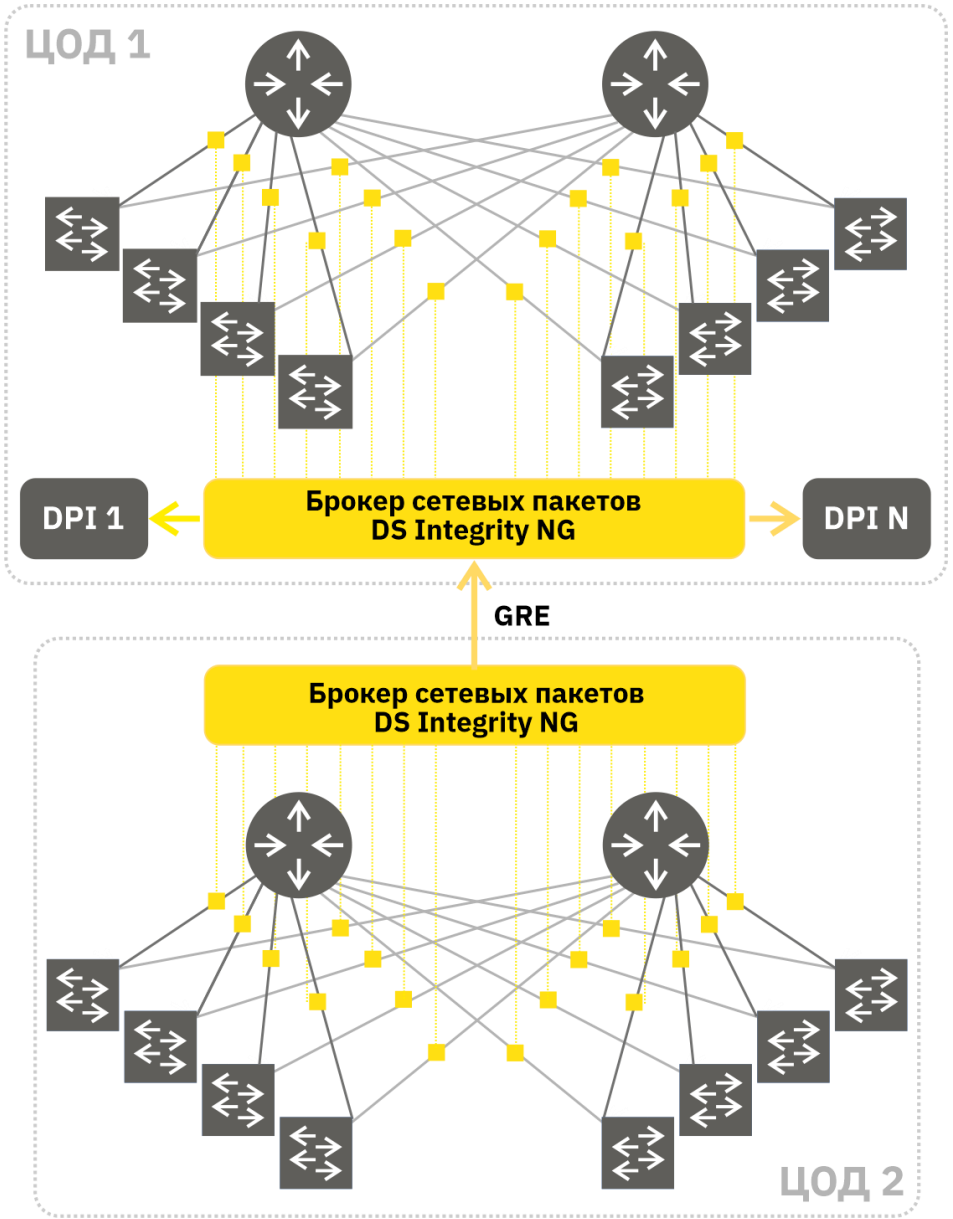
# Подключение систем NTA



# Каскадирование пакетных брокеров

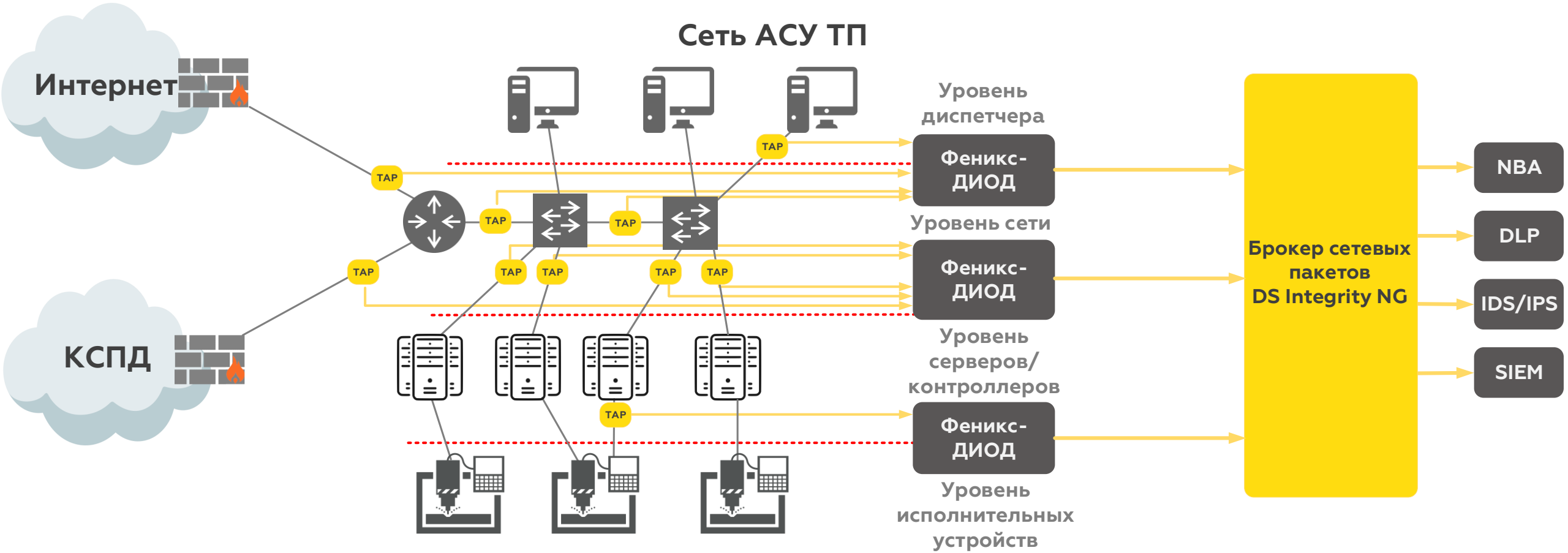


# Передача трафика между ЦОД




- Сбор полной копии трафика и обеспечение одновременной работы нескольких систем анализа и мониторинга, требующих получения идентичного трафика
- Формирование для каждой из систем анализа и мониторинга потока необходимых для их работы данных
- Инкапсуляция трафика в туннель GRE для передачи между несколькими офисами или центрами обработки данных
- Группирование портов и фильтрация трафика для сегментации сеть и разделения анализа по географическому или структурному принципу

# Агрегация трафика из сети АСУ ТП



# Дополнительные возможности

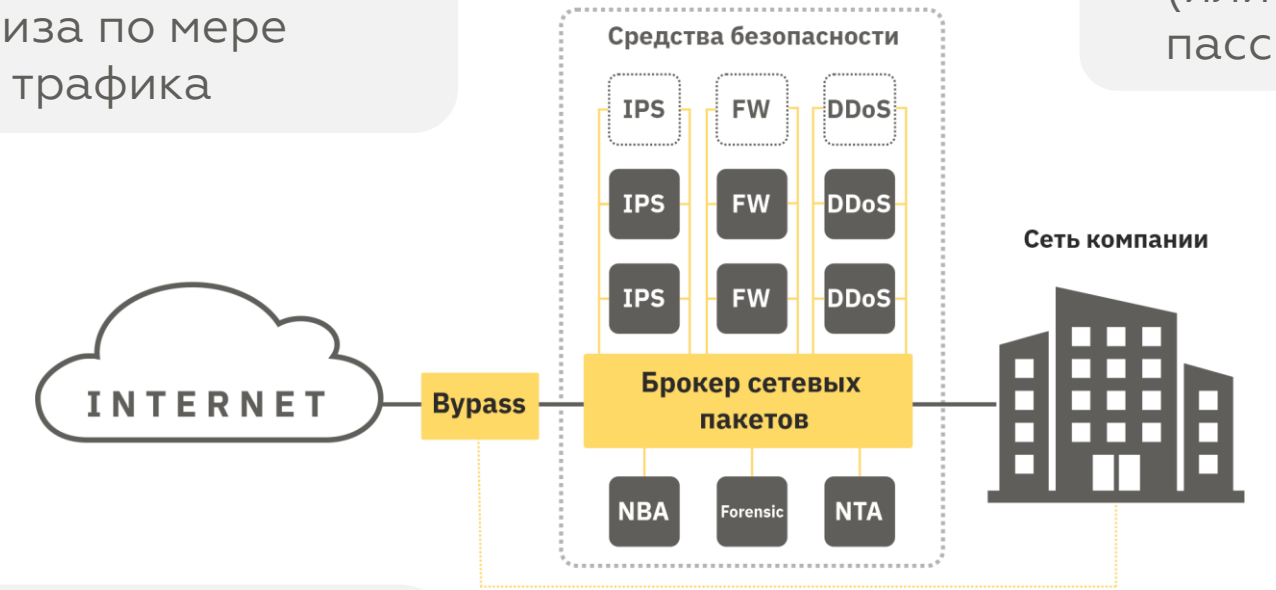
ЦИФРОВЫЕ РЕШЕНИЯ

**1**

Постепенное добавление дополнительных единиц средства анализа по мере роста потоков трафика

**2**

Зеркалирование всего (или части) трафика на пассивные средства анализа




**3**

Подключение активных средств анализа других типов (например, antiDDOS) с независимой балансировкой и резервированием

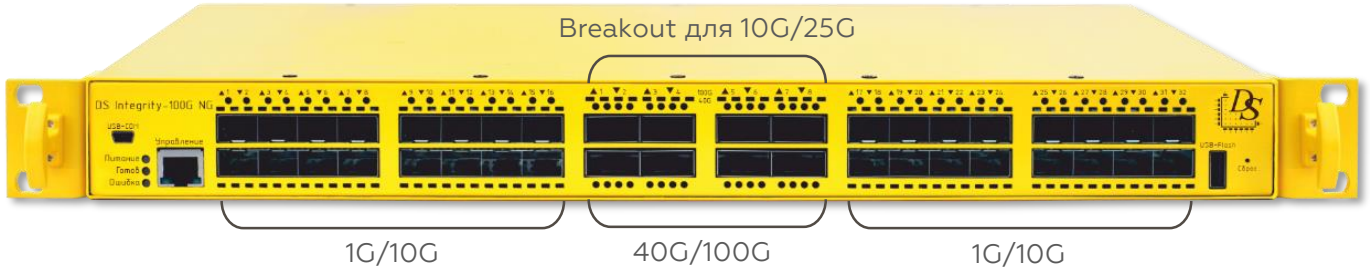
**4**

Оптимизация нагрузки за счёт настройки правил фильтрации (отбрасывание или пропуск мимо межсетевого экрана)

# Брокеры сетевых пакетов DS Integrity NG и ответвители трафика DS TAP

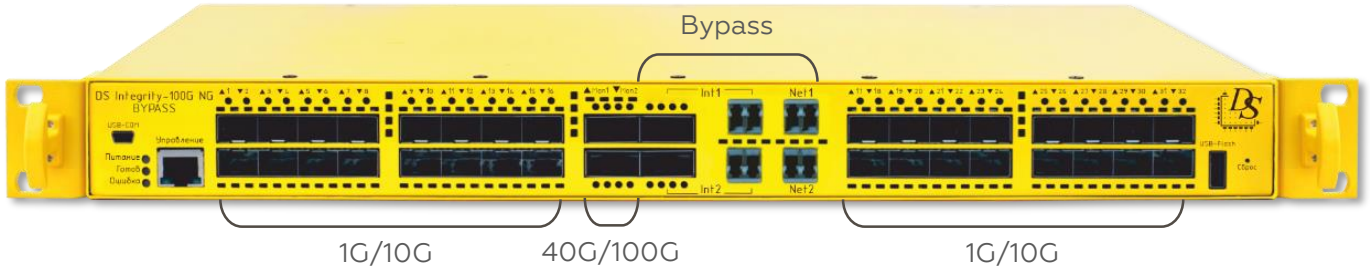
ЦИФРОВЫЕ РЕШЕНИЯ

Включены в реестры
Минпромторга и Минцифры



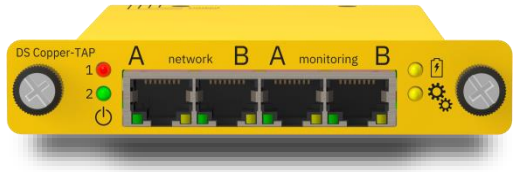

## DS INTEGRITY NG

- до 4 интерфейсов 100G Ethernet
- до 8 интерфейсов 40G Ethernet
- до 32 интерфейсов 25G Ethernet
- до 48 интерфейсов 10G Ethernet
- до 32 интерфейсов 1G Ethernet
- Производительность до 800 Гбит/с




## DS INTEGRITY NG BYPASS

- до 4 интерфейсов 100G/40G Ethernet
- до 32 интерфейсов 10G/1G Ethernet
- Производительность до 720 Гбит/с
- Контроль состояния средства мониторинга (Heartbeat)



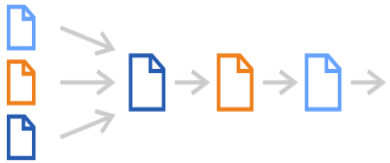

**DS COPPER-TAP**
Медные ответвители трафика

**DS OPTIC-TAP**
Оптические ответвители трафика

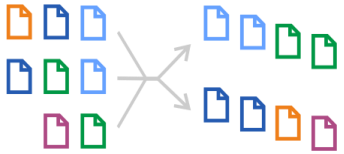
# Функционал DS Integrity

ЦИФРОВЫЕ РЕШЕНИЯ

## БАЗОВЫЕ ФУНКЦИИ



АГРЕГАЦИЯ

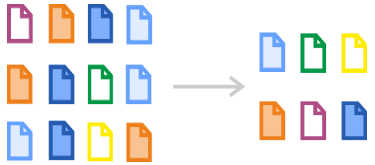


БАЛАНСИРОВКА

ФИЛЬТРАЦИЯ

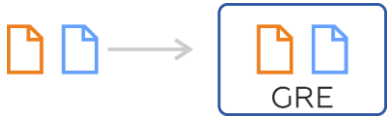
ЗЕРКАЛИРОВАНИЕ

## ДОПОЛНИТЕЛЬНЫЕ ФУНКЦИИ

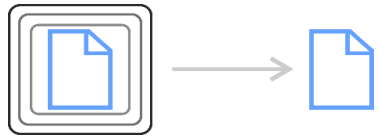


ДЕДУПЛИКАЦИЯ

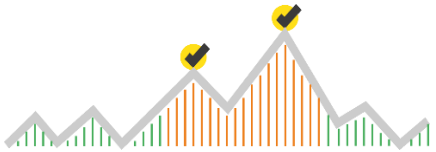
МОДИФИКАЦИЯ




ТУННЕЛИРОВАНИЕ

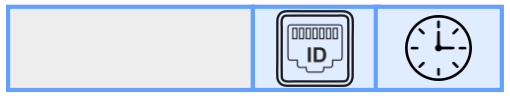


РАЗБОР ТУННЕЛЕЙ



ЗАЩИТА ОТ ВСПЛЕСКОВ

ГЕНЕРАЦИЯ sFlow




PORT STAMPING, TIME STAMPING

# Устройство однонаправленной передачи данных Феникс-1/10G-ДИОД


**Феникс-1/10G-ДИОД** — российское устройство однонаправленной передачи данных для подключения сетей АСУ ТП к системам информационной безопасности

Включен в Единый реестр российской радиоэлектронной продукции

Встроенное программное обеспечение включено в Единый реестр российских программ для электронных вычислительных машин и баз данных

- Входные порты: 24 x 10/100/1000 SFP
- Однонаправленные выходные порты: 2 x 10G SFP+
- Агрегация, балансировка, фильтрация трафика
- Два сменных блока питания с возможностью горячей замены (AC и/или DC)
- 4 блока вентиляторов с возможностью горячей замены (резервирование 3+1)
- Форм-фактор 1U, 305x440x44 мм

# Почему DS Integrity NG и Феникс-ДИОД?

ЦИФРОВЫЕ РЕШЕНИЯ

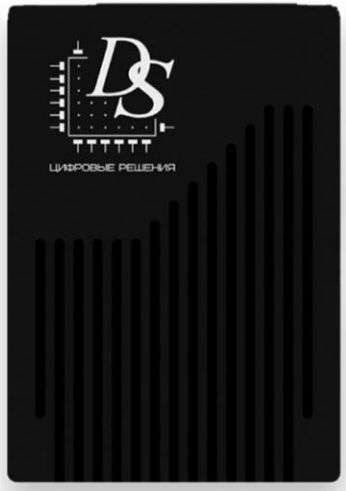
- **Аппаратная реализация базовых и дополнительных функций**
  отсутствие снижения производительности и потерь трафика
- **Создание единой высокопроизводительной системы из мультивендорных решений**
- **Обеспечение полного набора функций работы с туннелированным и фрагментированным трафиком**
- **Российская разработка и производство**

# Доверенные накопители

ЦИФРОВЫЕ РЕШЕНИЯ


**USB 3.0**
**Аметист**


**USB 3.0**
**Аметист-Б**




**SSD SATA 6GB/S**
**Оникс**

**Российский контроллер**
Собственной разработки

**Защита от подмены ВПО и УИН**

**до 40 000**
Количество циклов перезаписи

**Сертифицировано**

**Находятся в стадии сертификации**

# Высоконадёжные накопители

ЦИФРОВЫЕ РЕШЕНИЯ

**USB 3.0**
**УРАН**


**SSD SATA 6GB/S**
**ТИТАН**

**Российский контроллер**
Собственной разработки

**Защита от подмены ВПО и УИН**

**до 40 000**
Количество циклов перезаписи

**от -40 до +70 °C**
Рабочая температура

ИБ АСУ ТП КВО

ЦИФРОВЫЕ РЕШЕНИЯ

# СПАСИБО ЗА ВНИМАНИЕ!


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

8 (495) 978-28-70 (116)

sales@dsol.ru


habr