ЦИФРОВЫЕ РЕШЕНИЯ

# Зеркалирование трафика и безопасное подключение средств мониторинга в АСУ ТП

Алексей Лакаев | Руководитель отдела развития телекоммуникационного оборудования

# О компании

**21 ГОД**
в отрасли

**СВЫШЕ 2,7 МЛРД**
выручка за 2024

**400+**
сотрудников

**СОБСТВЕННОЕ**
производство

**3 ОФИСА**
в Москве и Пензе

ЦИФРОВЫЕ РЕШЕНИЯ

## Направления

- Телеком оборудование
- Твердотельные накопители
- Средства защиты информации
- Микросхемы
- Аппаратура для космоса

# Проблемы мониторинга АСУ ТП

ЦИФРОВЫЕ РЕШЕНИЯ

Физическая нехватка портов на NTA для требуемого охвата

Требование по изоляции сети АСУ ТП

Избыточная нагрузка на средства анализа

Сложность анализа из-за одинаковой адресации в разных сегментах

# SPAN в АСУ ТП

*если есть на коммутаторах*

ЦИФРОВЫЕ РЕШЕНИЯ

## Загрузка коммутатора до 5% - низкая вероятность потерь

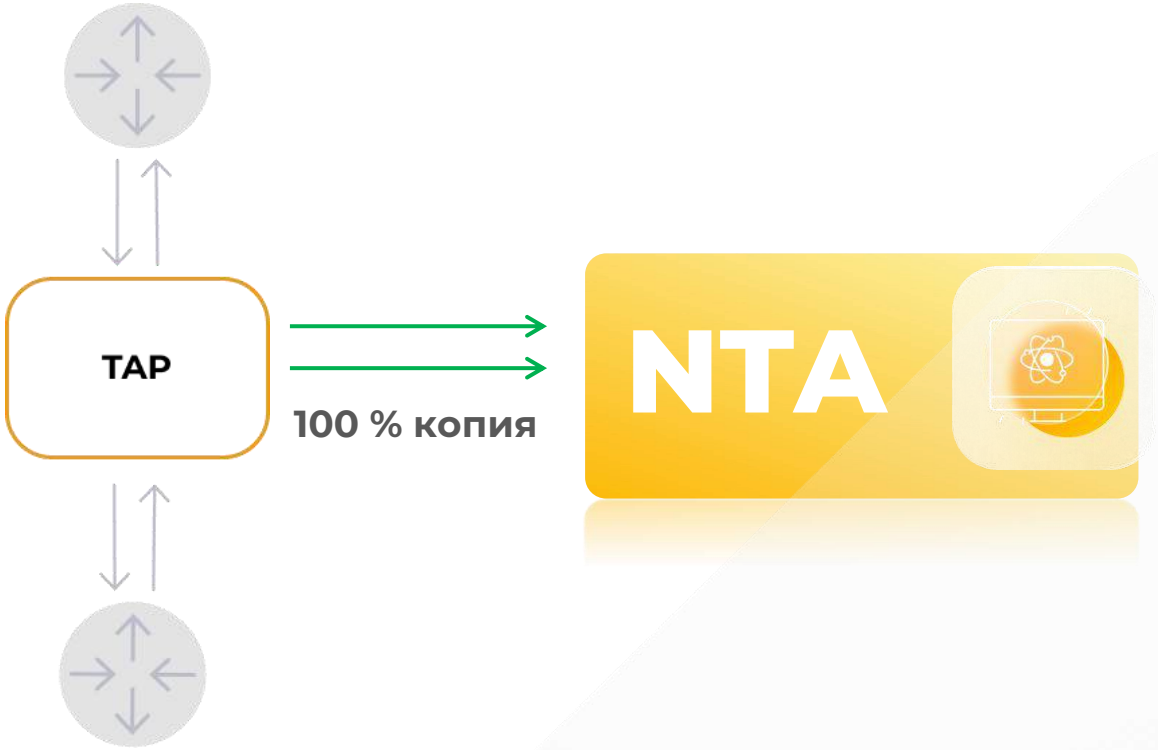
- Меньше точек отказа
- Уменьшение затрат на оборудование
- Включается без разрыва связи
- Не занимает места

## Какие проблемы останутся?

- **Целостность настройки**
  человеческий и технический фактор
  - Трафик не поступает на систему анализа или поступает «мусорный» трафик в сеть АСУ ТП
- **Возникновение дубликатов пакетов**
  - Повышение нефункциональной нагрузки на NTA
- **Рост объема трафика**
  увеличение количества оборудования и атаки хакеров
  - Потеря исходных данных
  - Деградация сети (потеря трафика на основных портах)

# Мониторинг сети с помощью TAP

ЦИФРОВЫЕ РЕШЕНИЯ




## ДЛЯ НАДЕЖНОСТИ

- Не оказывают влияния на оборудование

## ДЛЯ БЕЗОПАСНОСТИ

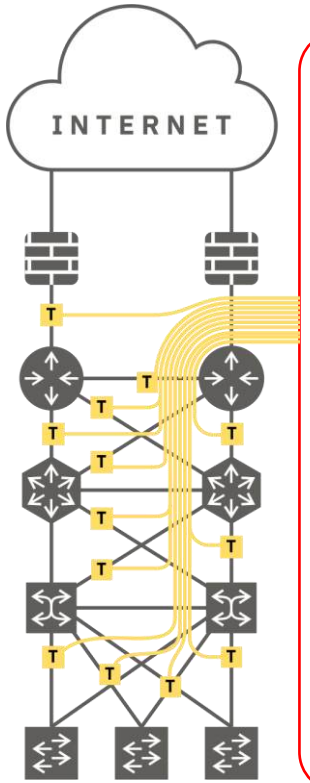
- Гарантируют передачу 100% копии трафика
- Не подвержены атакам

# Сняли трафик

что же дальше?

ЦИФРОВЫЕ РЕШЕНИЯ

?




- Что делать с нехваткой входов в анализаторе
- Как убрать лишние пакеты и лишние сессии
- Как подать один и тот же трафик на несколько систем
- Как поделить большой поток на несколько анализаторов

**Industrial NTA**

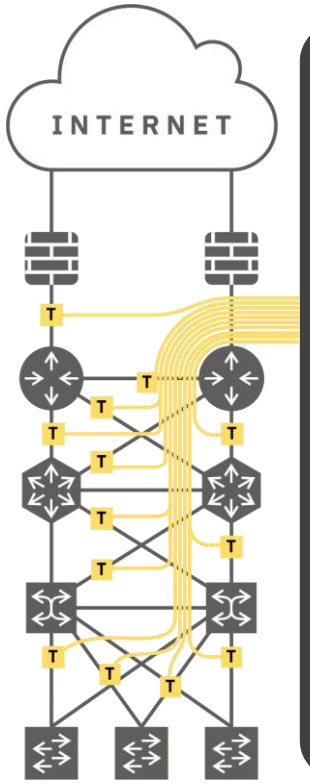
**DLP**

**Troubleshooting**

# Физическая защита трафика

ЦИФРОВЫЕ РЕШЕНИЯ

подача на анализаторы только необходимого трафика




**Агрегатор с однонаправленной передачей**

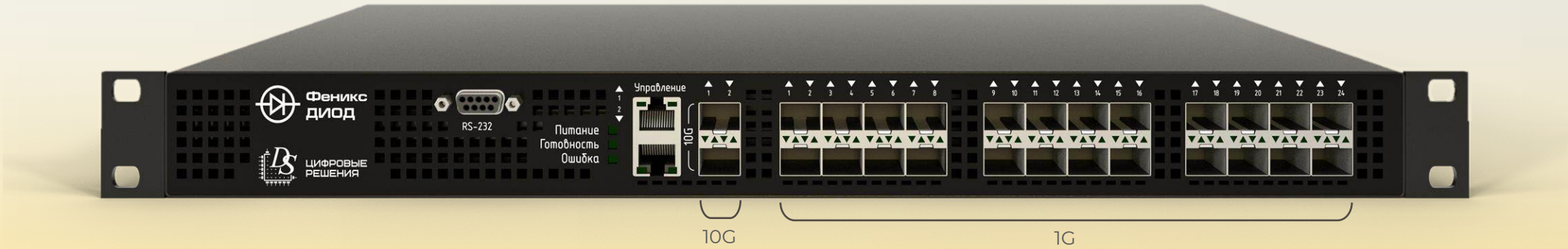
**Феникс - ДИОД**

- Агрегация
- Фильтрация
- Тэгирование трафика (VLAN)
- Балансировка
- Физическая изоляция сегментов

- **Industrial NTA**
- **DLP**
- **Troubleshooting**

# Агрегатор с однонаправленной передачей даных

ЦИФРОВЫЕ РЕШЕНИЯ




**Феникс-ДИОД**

**Однонаправленные агрегаторы** применяются для сбора и передачи данных из сетей АСУ ТП на внешние системы информационной безопасности. Данное оборудование позволяет на аппаратном уровне изолировать сеть АСУ ТП от воздействия со стороны средств мониторинга.

**ФСТЭК**
Сертификация ФСТЭК России
по 4 уровню доверия

в реестре
**Минпромторг России**

# Отличия Феникс-ДИОД от диодов данных

ЦИФРОВЫЕ РЕШЕНИЯ

| | Феникс-ДИОД | InfoDiode |
|---|---|---|
| Однонаправленная передача данных | ✓ | ✓ |
| Количество входов | **24 x 1G** | 1 x 1G |
| Количество выходов | **2 x 10G** | 1 x 1G |
| Проксирование двусторонних протоколов | ✗ | ✓ |
| Агрегация потоков | ✓ | ✗ |
| Фильтрация трафика | ✓ | ✗ |
| Тегирование VLAN | ✓ | ✗ |
| Сертификация ФСТЭК | ✓ | ✓ |

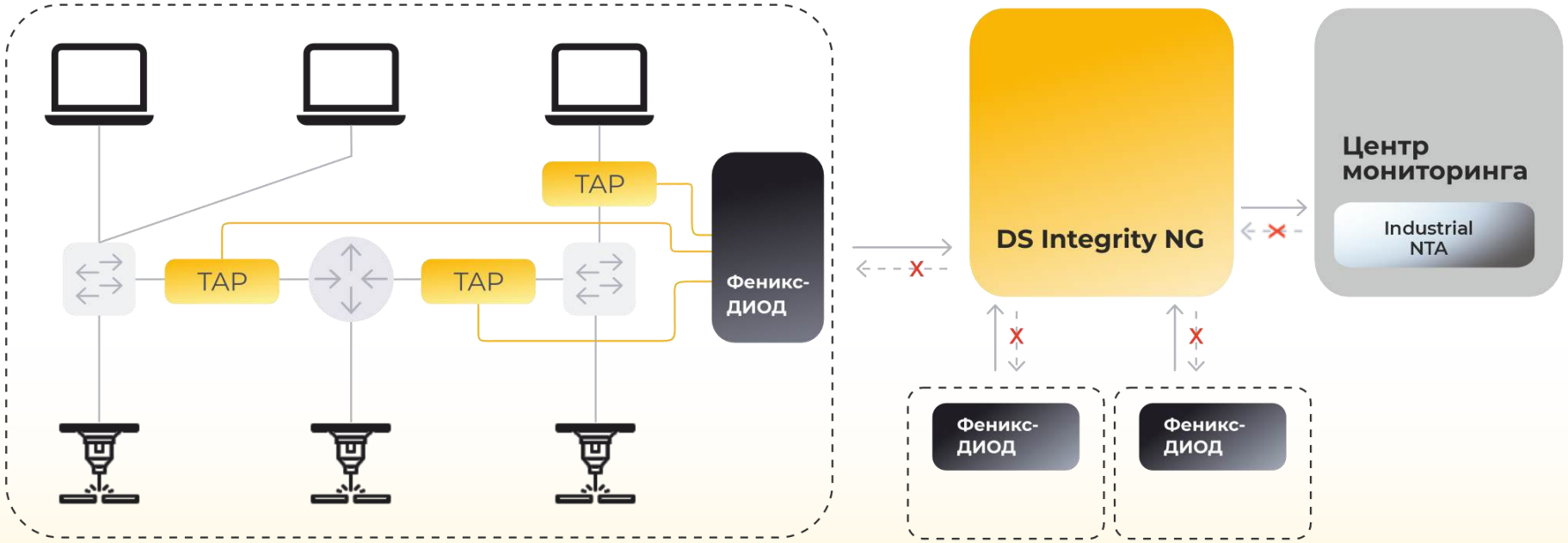
# 3 эшелона защиты сети

ЦИФРОВЫЕ РЕШЕНИЯ

- Оптический однонаправленный сигнал
- Физический разрыв на печатной плате
- Отсутствие логической связи в коммутационной матрице на ПЛИС

# Подключение сетей АСУ ТП

ЦИФРОВЫЕ РЕШЕНИЯ




## ДЛЯ НАДЕЖНОСТИ

- Гарантированное отсутствие воздействия средств ИБ на АСУ ТП
- Правильные настройки «по-умолчанию»

## ДЛЯ БЕЗОПАСНОСТИ

- Широкие возможности по масштабированию
- Легкость администрирования

# Сценарии зеркалирования в АСУ ТП

ЦИФРОВЫЕ РЕШЕНИЯ

TAP

**KICS for Networks / PT ISIM**

\+ Передача 100% копии трафика
Отсутствие влияния на работу сети
Исключение человеческого фактора

— Отсутствие агрегации, фильтрации и гарантированной однонаправленности

SPAN | TAP

Агрегатор Феникс-ДИОД

**KICS for Networks / PT ISIM**

\+ Агрегация, базовая фильтрация
Гарантированная однонаправленная передача

— Отсутствие расширенной фильтрации, дедупликации повторяющихся пакетов, а также туннелирования трафика

SPAN | TAP

Агрегатор DS Diod

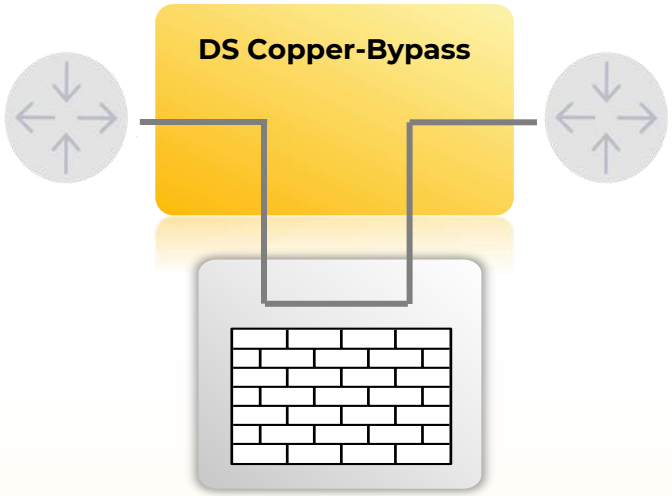
Брокер DS Integrity

**KICS for Networks / PT ISIM**

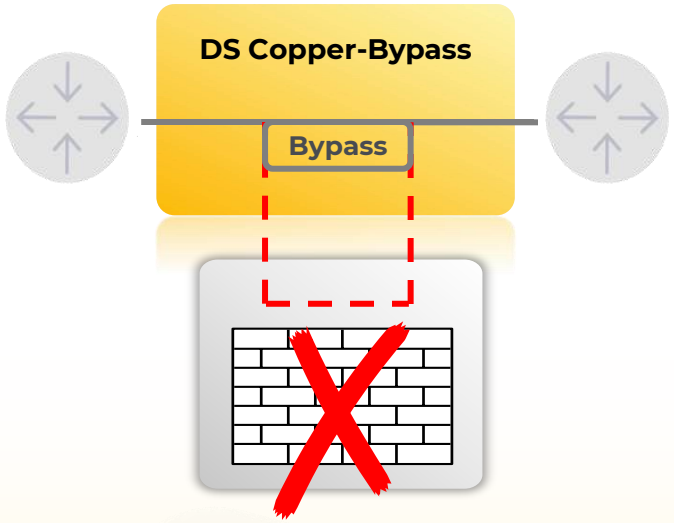
\+ Агрегация, расширенная фильтрация, балансировка на несколько анализаторов, дедупликация повторяющихся пакетов, туннелирование трафика, гарантированная однонаправленная передача данных

# Подключение NGFW через Bypass

ЦИФРОВЫЕ РЕШЕНИЯ




Штатный режим работы




Режим байпас и сохранение линка

**Импортозамещение в АСУ ТП**

✗ NIAGARA Networks ✗ Profitap ✗ IXIA

# Линейки оборудования

ЦИФРОВЫЕ РЕШЕНИЯ

**Зеркалирование и оптимизация трафика для ИБ**

**Сетевые Bypass**

**Аппаратная балансировка нагрузки**

DS Integrity EVO

DS Integrity NG

Феникс-ДИОД

DS Optic-TAP и DS Copper-TAP

DS Copper-Bypass

DS Integrity NG Bypass

DS Proxima

- **Российские аппаратные платформы**
- **Пропускная способность более 2 Тбит/с**
- **Подтвержденная совместимость с российскими производителями средств ИБ**

в реестре **Минпромторг России**

**ФСТЭК** сертификация по 4 уровню доверия

**РЕЕСТР ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ**

# Почему оборудование от Цифровых решений?

ЦИФРОВЫЕ РЕШЕНИЯ

Используется в инфраструктуре субъектов КИИ с 2020 года

Простота интеграции и надежность работы средств мониторинга ИБ, простота расширения в будущем

Реальный опыт адаптации оборудования под индивидуальные требования Заказчика

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

lakaev@dsol.ru | Алексей Лакаев
Руководитель отдела развития
телекоммуникационного оборудования

habr

# СПАСИБО ЗА ВНИМАНИЕ!