



# ПОДКЛЮЧЕНИЕ АСУ ТП СЕТЕЙ К СИСТЕМАМ АНАЛИЗА ТРАФИКА

# МЫ СЕГОДНЯ

**20 ЛЕТ**

в отрасли

**СВЫШЕ 1 МЛРД**

выручка за 2022

**380+**

сотрудников

**3 ОФИСА**

в Москве и Пензе



ЦИФРОВЫЕ РЕШЕНИЯ

## Направления



Телеком  
оборудование



Твердотельные  
накопители



Микросхемы



Аппаратура для  
космоса

# НАША КОМАНДА



## Разработка

Программисты

Разработчики RTL

Схемотехники

Топологи

Конструкторы

Криптографы



## Производство

Входной контроль

Поверхностный монтаж

Визуальный контроль

Финальная сборка

Испытания



## Техническое сопровождение

Проектировщики типовых решений

Наладчики оборудования

Служба технической поддержки



## ВЫПУСКНИКИ ВЕДУЩИХ ТЕХНИЧЕСКИХ ВУЗОВ РОССИИ

МГТУ  
им. Н.Э. Баумана

МИЭТ  
ПГУ

МФТИ

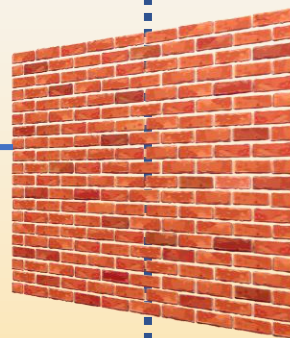
МИФИ

МЭИ

# ИБ СТРОИТСЯ НА КОНТРОЛЕ ПЕРИМЕТРА. ОБЩЕПРИНЯТЫЙ ПОДХОД



ЦИФРОВЫЕ РЕШЕНИЯ



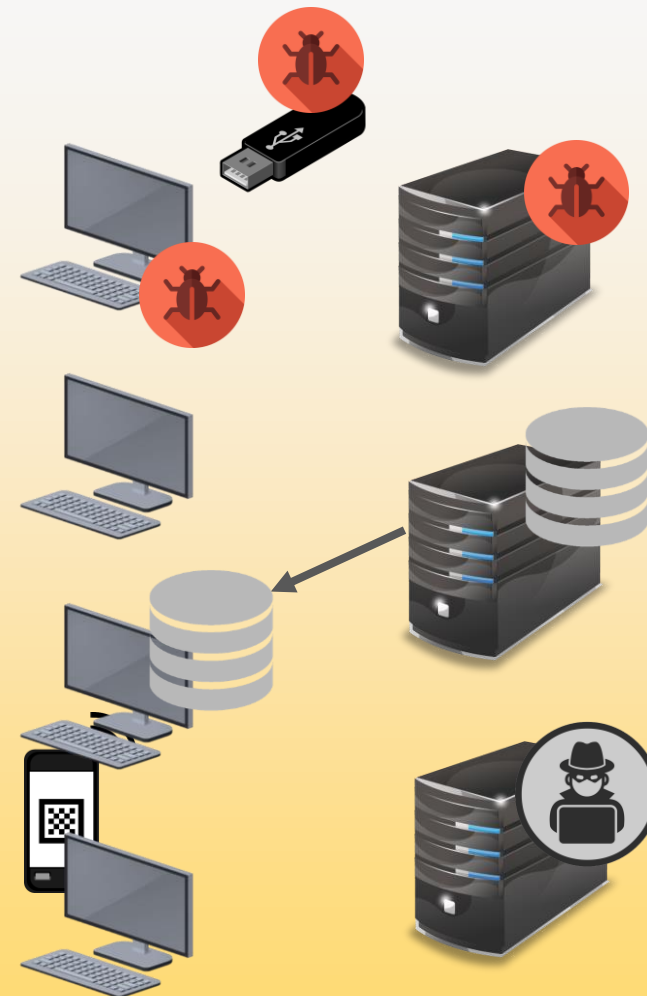
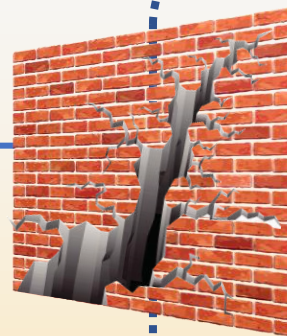
## ИБ ПОСТРОЕНА НА МЭ

- Контроль доступа между сетями с разными уровнями угроз

## НЕДОСТАТКИ

- Нет контроля внутреннего (локального) трафика

# КОНТРОЛЬ ПЕРИМЕТРА. РИСКИ



## РИСКИ ПРИ ИБ НА МЭ

- Зараженные накопители
- Зараженные рабочие станции и сервера
- Несанкционированный доступ к рабочим станциям и серверам
- Подключение рабочей станции к Интернет через мобильный телефон
- Уязвимости в МЭ
- Утечка данных внутри сети

## РЕШЕНИЕ

- Необходим анализ трафика внутри сети

# СВЯЗУЮЩЕЕ ЗВЕНО

## 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 обратного влияния систем ИБ на сеть

**ИТ**

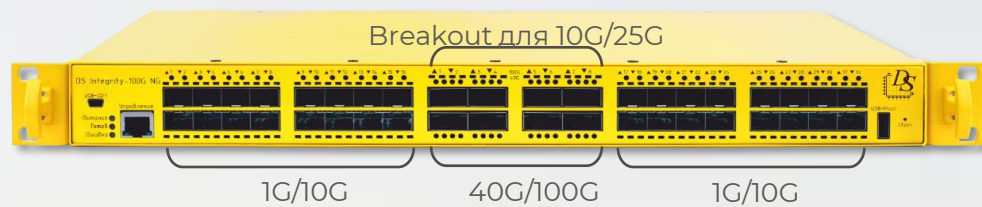
**?**

**ИБ**

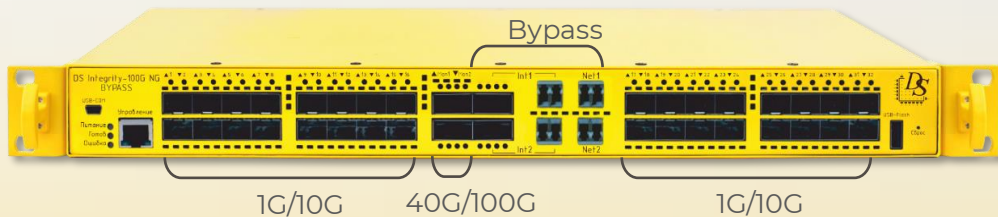
# НАШИ РЕШЕНИЯ



ЦИФРОВЫЕ РЕШЕНИЯ



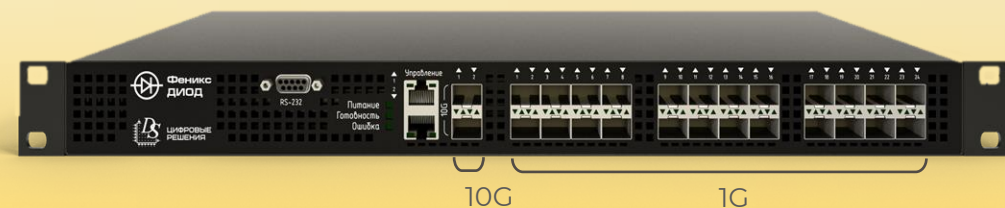
DS INTEGRITY NG



DS INTEGRITY NG BYPASS



DS COPPER-TAP



ФЕНИКС-ДИОД

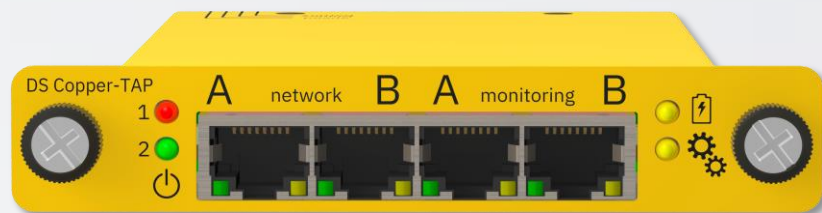


DS OPTIC-TAP

от 1G до 100G  
интерфейсы

до 1,6 Тбит/с  
пропускная способность

# ОТВЕТВИТЕЛИ ТРАФИКА



**DS Copper-TAP**  
Медные ответвители трафика



**DS Optic-TAP**  
Оптические ответвители трафика



# ПОДКЛЮЧЕНИЕ СИСТЕМ NTA



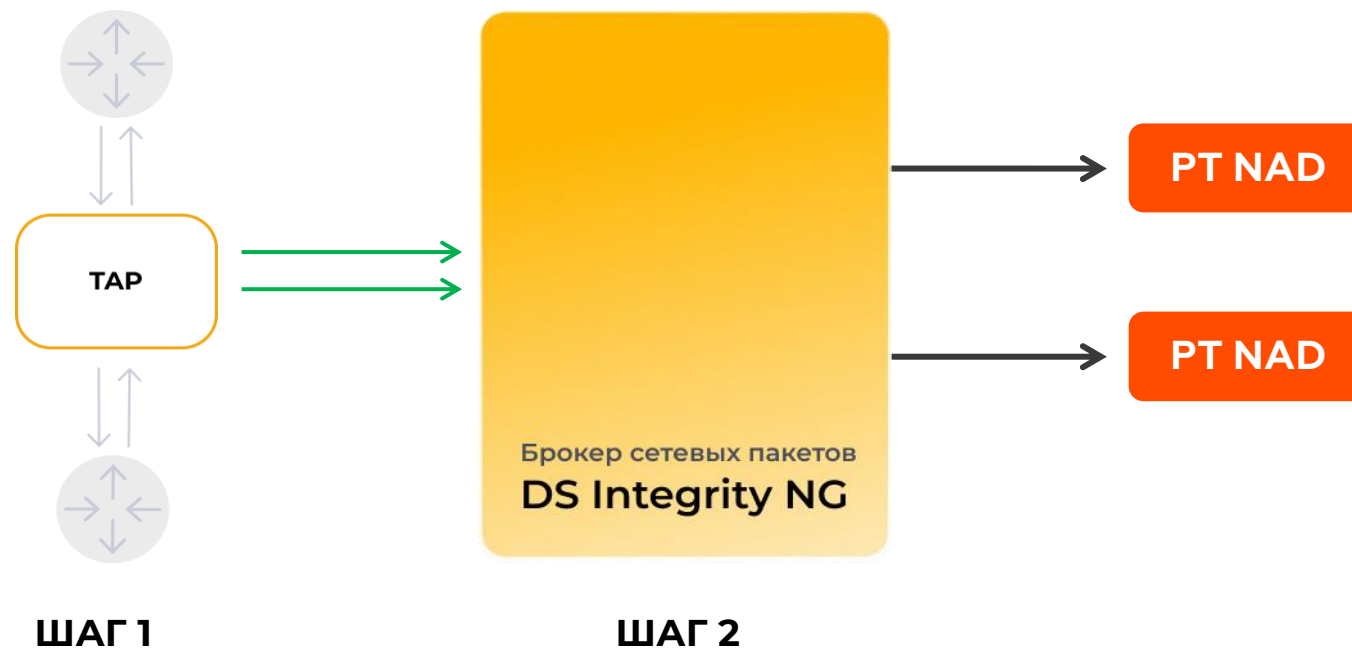
ЦИФРОВЫЕ РЕШЕНИЯ

БЫЛО

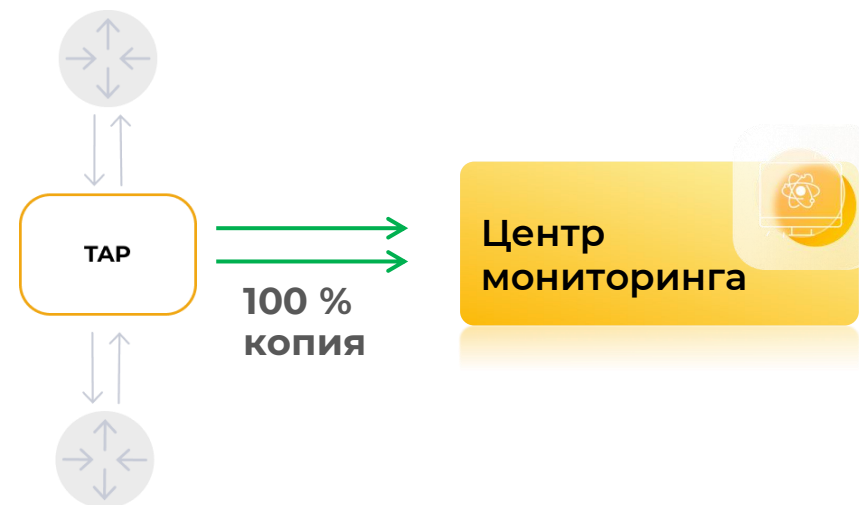
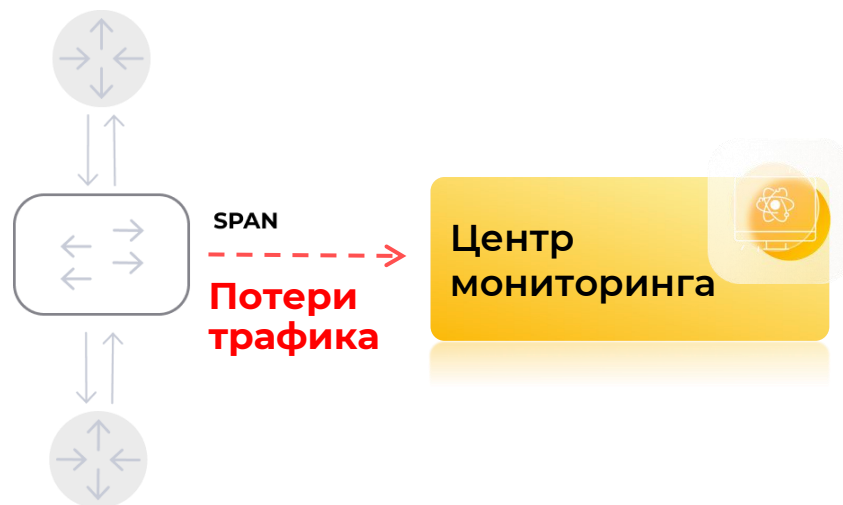


■ positive technologies

СТАЛО



# ЗЕРКАЛИРОВАНИЕ ТРАФИКА С СЕТИ



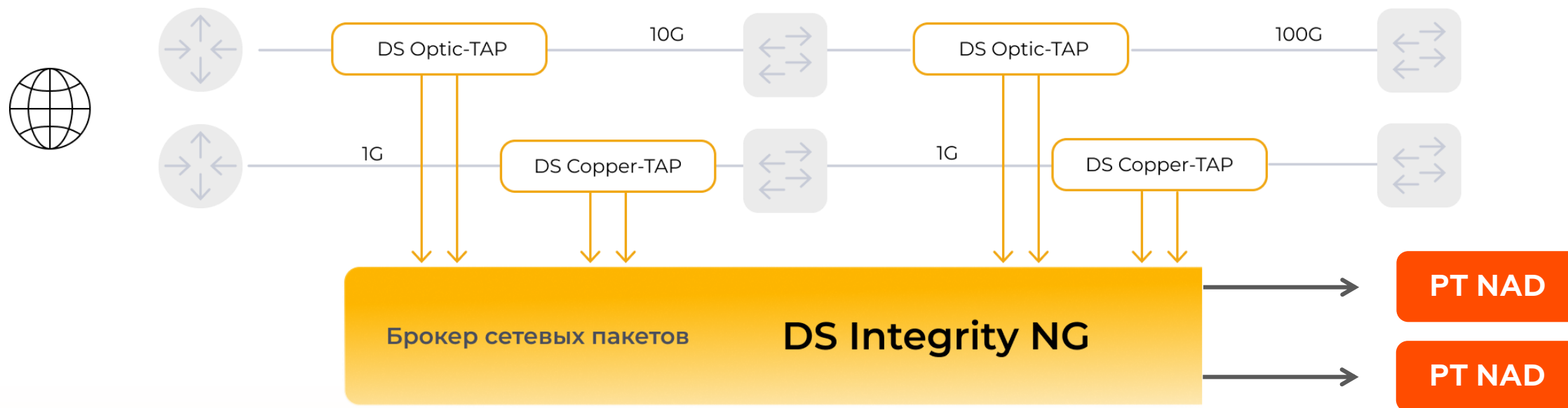
## Передача трафика через SPAN

- Ограничен по производительности
- Расходует порты коммутатора
- Не требует дополнительных расходов

## Передача трафика через TAP

- Высокая производительность
- Не подвержены атакам
- Требуется установка дополнительного оборудования

# ПОДКЛЮЧЕНИЕ СИСТЕМ NTA



# SPAN В АСУ ТП

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

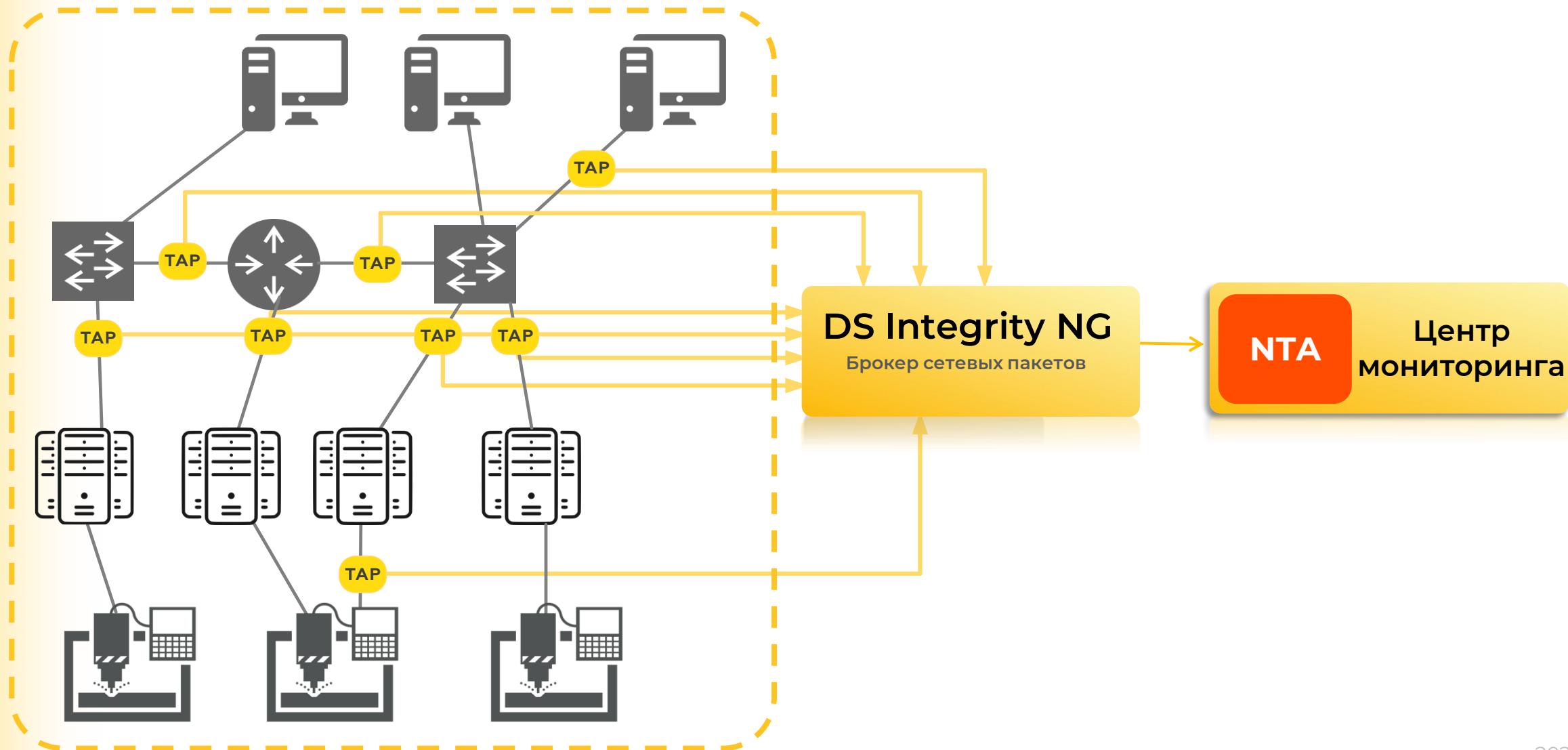
Трафик не поступает на систему анализа или поступает «мусорный» трафик в сеть АСУ ТП

Пропущенная атака хакеров

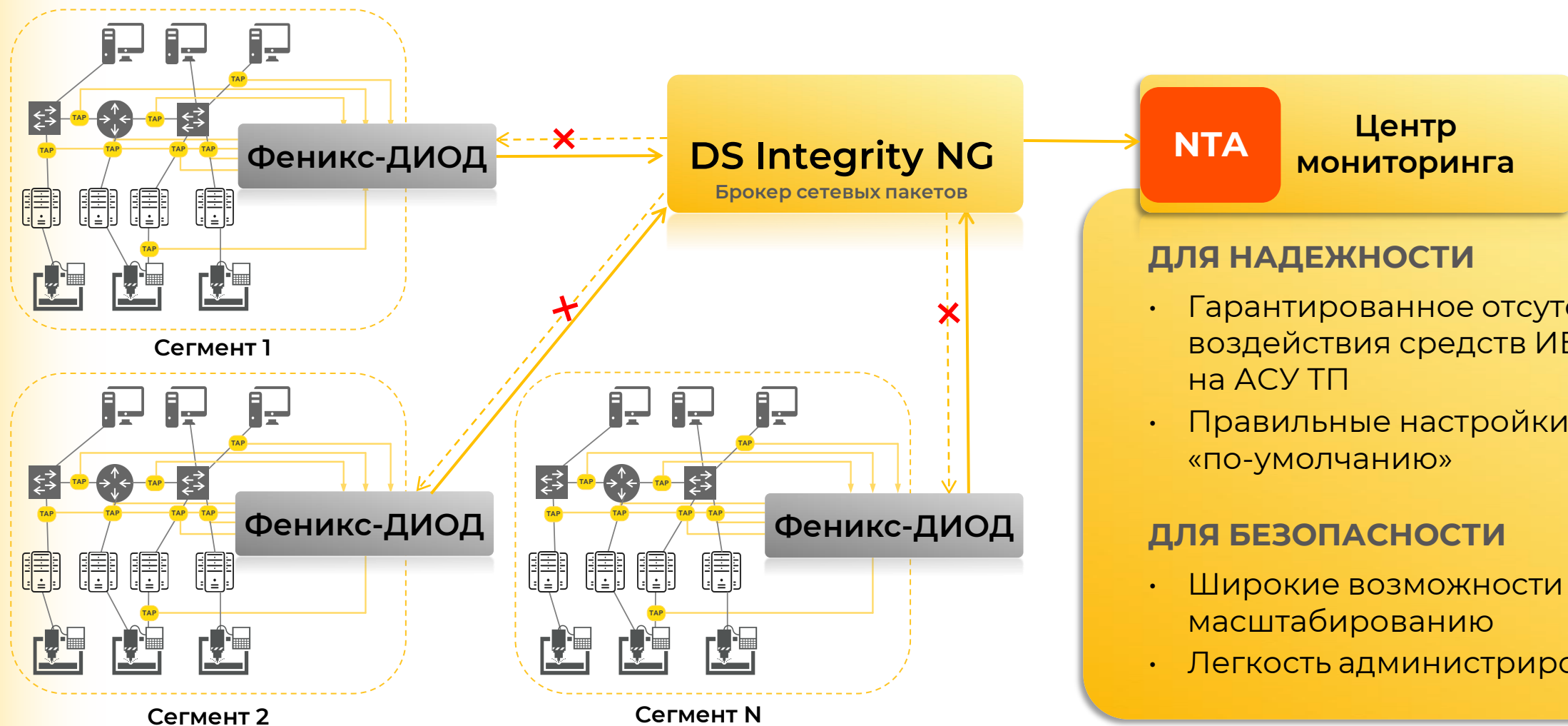
Повышение нефункциональной нагрузки на NTA

Потеря исходных данных  
Деградация сети (потеря трафика на основных портах)

# ПОДКЛЮЧЕНИЕ АСУ ТП СЕТИ К СИСТЕМАМ АНАЛИЗА



# ПОДКЛЮЧЕНИЕ НЕСКОЛЬКИХ АСУ ТП СЕТЕЙ



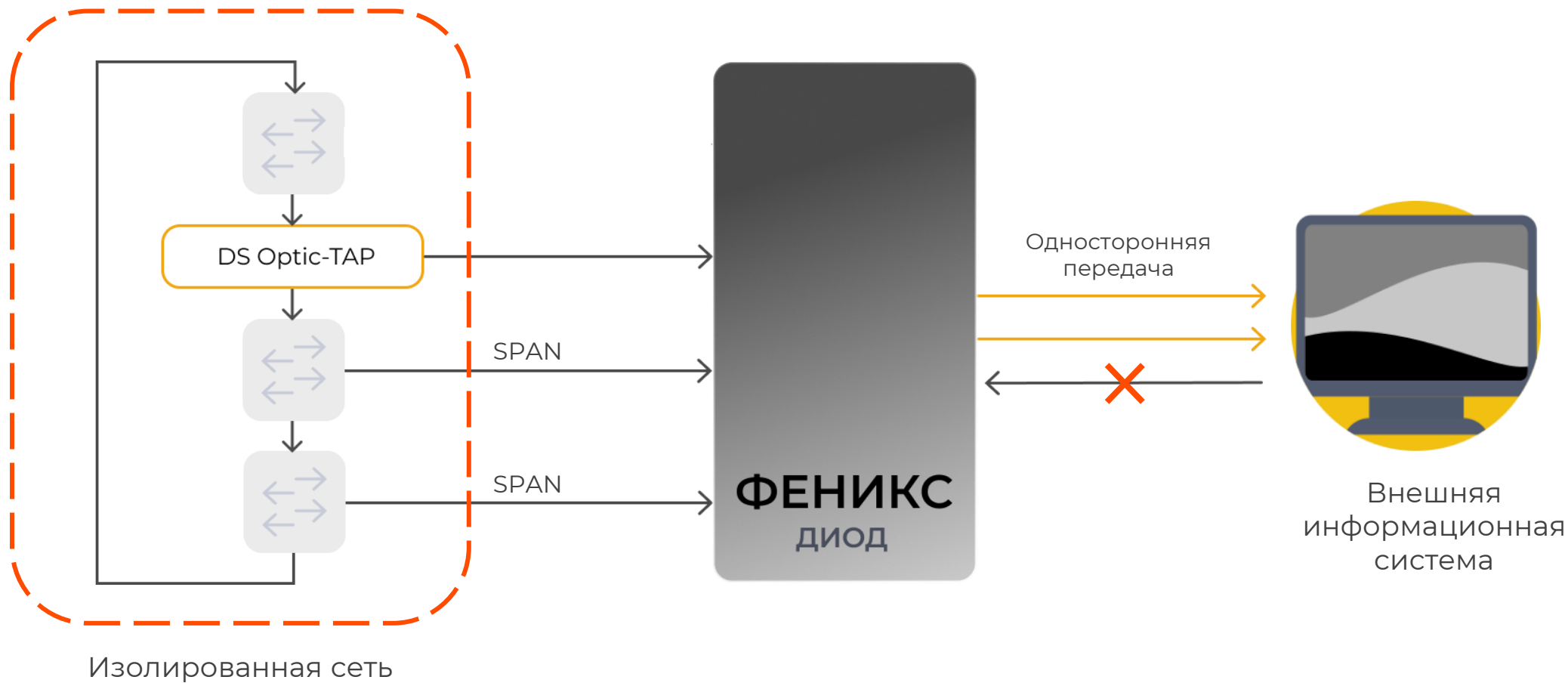
## ДЛЯ НАДЕЖНОСТИ

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

## ДЛЯ БЕЗОПАСНОСТИ

- Широкие возможности по масштабированию
- Легкость администрирования

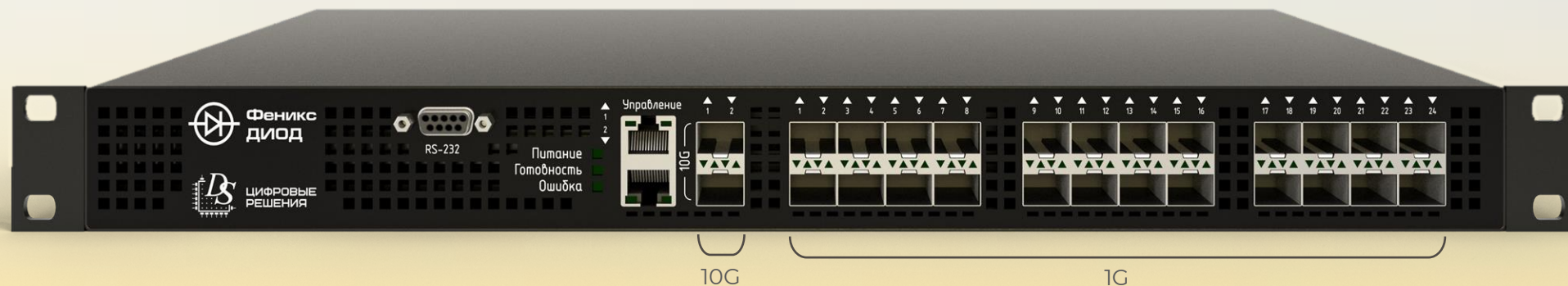
# РАБОТА ФЕНИКС-ДИОД



# АГРЕГИРУЮЩИЙ ОДНОНАПРАВЛЕННЫЙ ШЛЮЗ



ЦИФРОВЫЕ РЕШЕНИЯ



Феникс-ДИОД

**Однонаправленный шлюз** применяются для передачи данных из сетей АСУ ТП на системы информационной безопасности. Данное оборудование позволяет на аппаратном уровне изолировать сеть АСУ ТП от воздействия со стороны средств мониторинга.



**ФСТЭК**  
в стадии сертификации  
по 4 уровню доверия



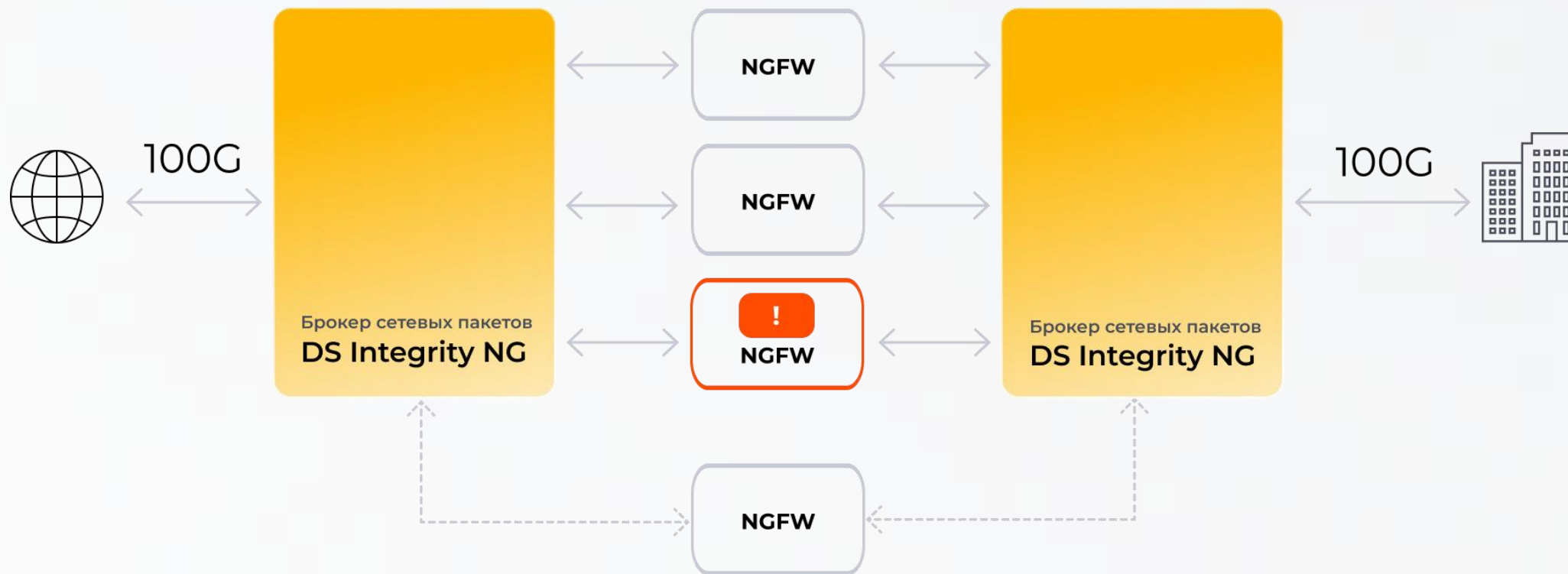
**МИНПРОМТОРГ  
РОССИИ**



# КЛАСТЕРИЗАЦИЯ МЭ С ПОМОЩЬЮ БРОКЕРОВ СЕТЕВЫХ ПАКЕТОВ DS INTEGRITY NG



ЦИФРОВЫЕ РЕШЕНИЯ



# DS INTEGRITY NG В ИНФРАСТРУКТУРАХ



11

Министерств и госслужб



7

Компаний  
промышленного сектора



9

Российских  
банков из ТОП-25



5

Энергетических  
компаний



5

Логистических  
и транспортных  
компаний из ТОП-100



8

Российских IT-компаний  
из ТОП-100

## 1 ПОВЫШЕНИЕ КАЧЕСТВА И СНИЖЕНИЕ ЗАТРАТ

- снижение риска пропуска инцидентов ИБ
- снижение требований к производительности систем ИБ
- ликвидация влияния на ИТ-инфраструктуру
- снижение требований к сотрудникам эксплуатации



## 2 ПРОСТОТА ЭКСПЛУАТАЦИИ

- упрощение администрирования подключения средств ИБ
- интуитивно понятный интерфейс
- совместимость с любыми средствами систем ИБ



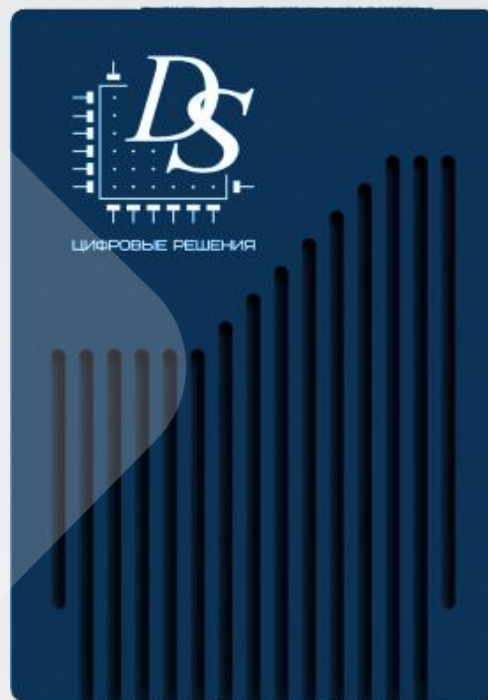
## 3 НАША ПОДДЕРЖКА

- сопровождение внедрения и обучение
- разработка и производство в России
- говорим на вашем языке, всегда на связи





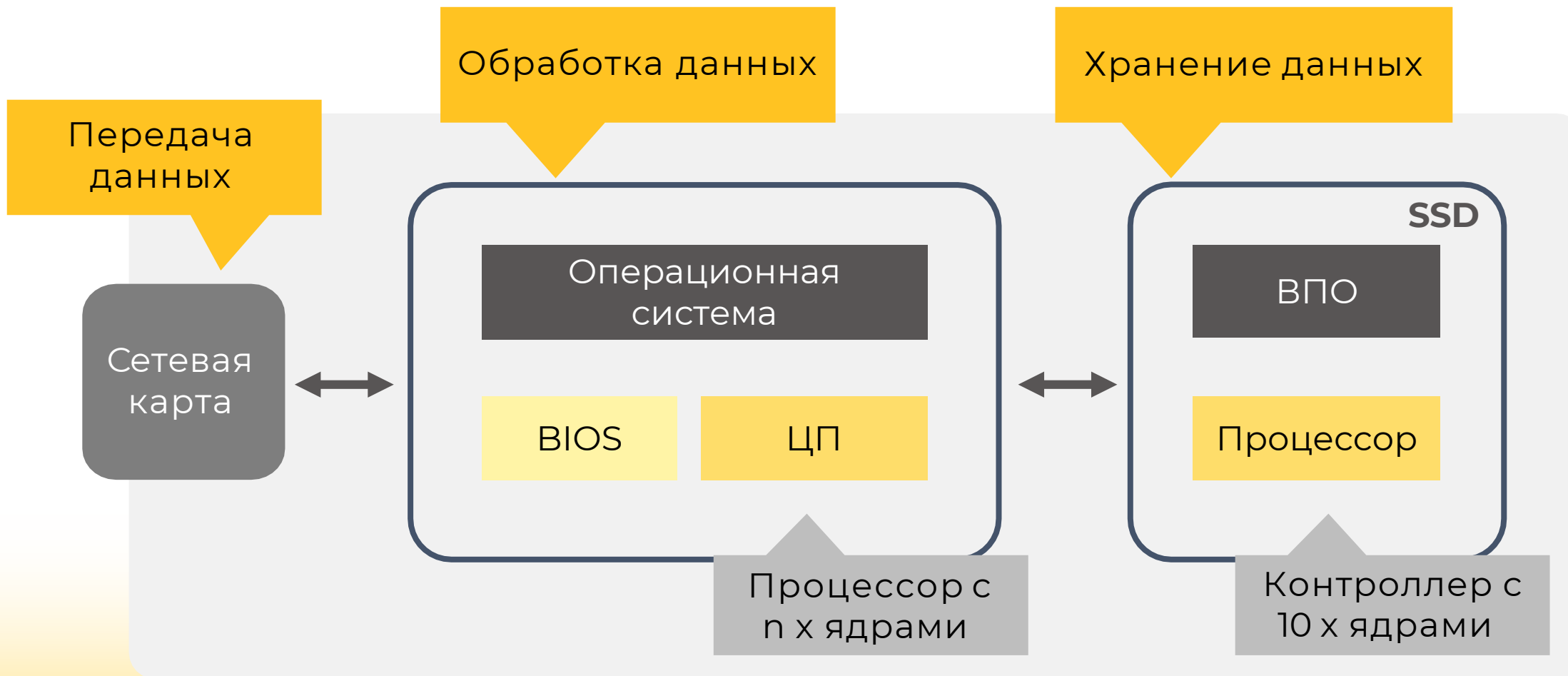
ЦИФРОВЫЕ РЕШЕНИЯ



# ДОВЕРЕННЫЕ И ВЫСОКОНАДЕЖНЫЕ ТВЕРДОТЕЛЬНЫЕ НАКОПИТЕЛИ С ИНТЕРФЕЙСАМИ SATA И USB

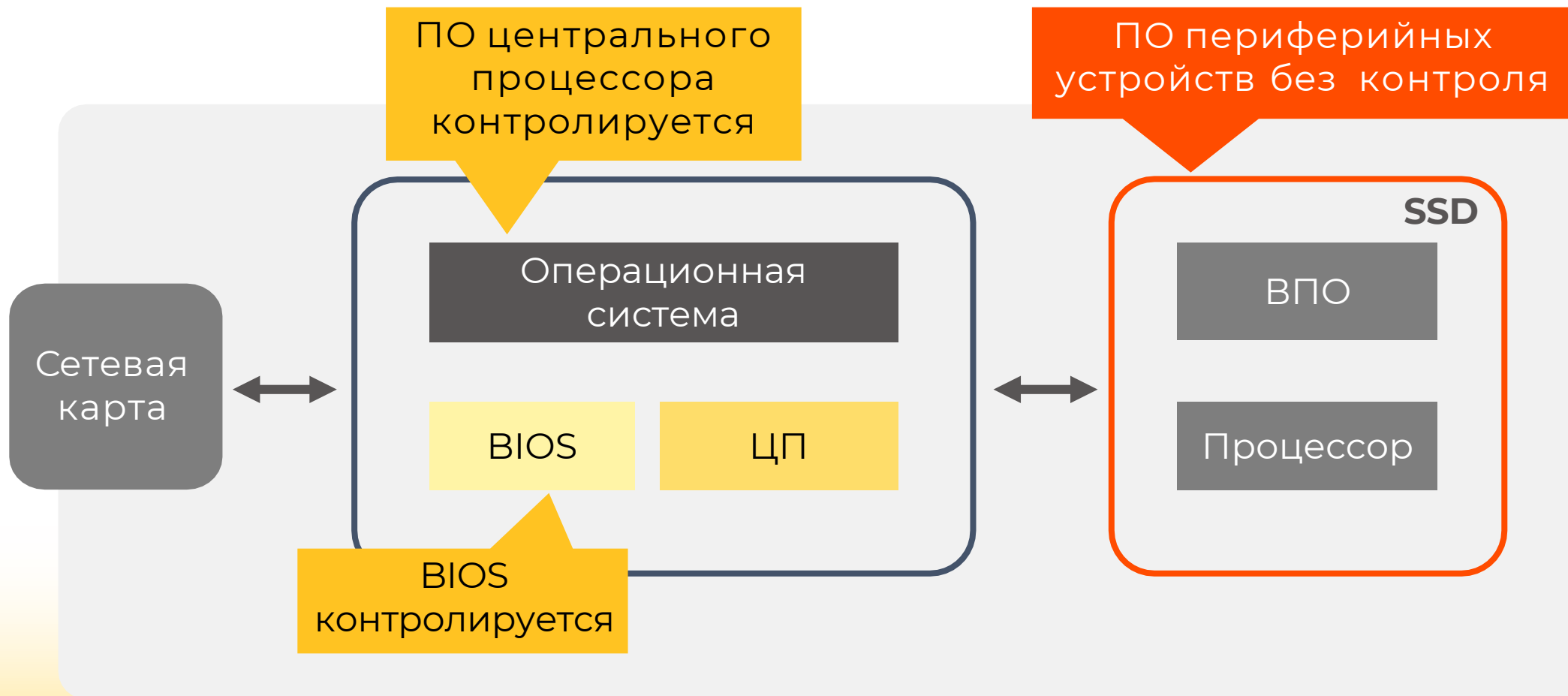
Евгений Шкляев | Менеджер продукта

# АРХИТЕКТУРА ТИПОВОЙ ПЭВМ



Все понимают, что в ПЭВМ есть центральный процессор и функционирующее на нем программное обеспечение. При этом мало кто задумывается, что в современном SSD установлен контроллер, содержащий до 10 процессорных ядер и на нем также функционирует своё программное обеспечение.

# ПОТЕНЦИАЛЬНЫЕ УГРОЗЫ ОТ КОМПОНЕНТОВ ЗАЩИЩЕННОГО АРМ



При анализе угроз информационной безопасности ПЭВМ уделяется внимание программному обеспечению BIOS и центрального процессора, при этом периферийные устройства не контролируются.

ВПО SSD имеет полный доступ к данным. С учётом производительности контроллера SSD требования к защите ВПО SSD должны быть даже выше, чем у BIOS.

# РИСКИ И УГРОЗЫ ДЛЯ ХРАНЕНИЯ ДАННЫХ



1

Внесение изменений в данные

2

Удаление данных

3

Дистанционная передача данных

4

Вредоносное воздействие на АРМ

# ХРАНЕНИЕ ДАННЫХ

Находятся в стадии  
получения категории  
качества ВП

 МИНПРОМТОРГ  
РОССИИ



**USB 3.0  
Аметист**

**USB 2.0  
Аметист-Б**

Находятся в стадии  
получения категории  
качества ВП

 МИНПРОМТОРГ  
РОССИИ

 МИНПРОМТОРГ  
РОССИИ



**SSD SATA 6 Гбит/с  
ТИТАН-К**

**SSD SATA 6 Гбит/с  
ТИТАН**

**SSD SATA 6 Гбит/с  
ТИТАН М.2**

Заклучение ФСБ России  
по требованиям РД НДВ  
по 2 уровню контроля

Находятся в стадии  
сертификации

**Российские контроллеры  
собственной разработки**

**Защита  
от подмены  
ВПО и УИН**

**TBW  
до 14 800 Тбайт**

**От -40 до +70 °С  
рабочая температура**



# ДОВЕРЕННЫЙ НАКОПИТЕЛЬ USB 3.0 АМЕТИСТ



ЦИФРОВЫЕ РЕШЕНИЯ



**Аметист**

**Защита:** подсистема защиты от записи

**Безопасность:**

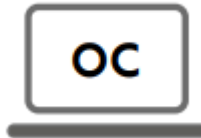
- защита встроенного ПО от модификации
- уникальный идентификатор

**Отказоустойчивость:**

- защита от внезапного отключения питания
- контроль температуры



**TBW**  
**217 Тбайт**



**Windows, Linux,**  
**Android, MCBC,**  
**Эльбрус, ЗОСРВ**  
**«Нейтрино»**



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



**Сертифицирован**

**Заключение ПП РФ №719**

Находится в стадии присвоения  
категории качества «ВП»

- **Интерфейс:** USB 3.0 (USB 3.2 Gen 1 с поддержкой USB 2.0, USB 1.1)
- **Форм-фактор:** USB-stick
- **Срок хранения информации:** не менее 10 лет (при 10% износе памяти)
- **Ёмкость:** 19 Гбайт
- **Скорость чтения/записи:** до 50/59 Мбайт/с
- **Энергопотребление:** не более 1,5 Вт

# НАКОПИТЕЛЬ USB 2.0 ДЛЯ ФИКСАЦИИ ДАННЫХ АМЕТИСТ-Б



ЦИФРОВЫЕ РЕШЕНИЯ



**Аметист-Б**



Находится в стадии  
сертификации

## Фиксация данных:

после перевода в режим «только чтение», ВПО контроллера обеспечивает гарантированную невозможность модификации и удаления данных с накопителя

## Безопасность:

- защита встроенного ПО от модификации
- уникальный идентификатор
- низкий уровень побочных излучений

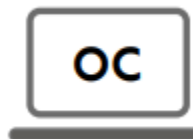
## Отказоустойчивость:

- защита от внезапного отключения питания
- контроль температуры



## Блокировка записи

Необратимый  
запрет изменения  
данных



**Windows, Linux,  
Android, MCBC,  
Эльбрус, ЗОСРВ  
«Нейтрино»**



**от 0 до +50°C**  
Рабочая  
температура

- **Интерфейс:** USB 2.0 (с поддержкой USB 1.1)
- **Форм-фактор:** USB-stick
- **Срок хранения информации:** не менее 10 лет (при 10% износе памяти)

- **Ёмкость:** 19 Гбайт
- **Скорость чтения/записи:** до 35/35 Мбайт/с
- **Энергопотребление:** не более 1,5 Вт

# ДОВЕРЕННЫЙ НАКОПИТЕЛЬ SSD SATA 6 ГБИТ/С ТИТАН-К



ЦИФРОВЫЕ РЕШЕНИЯ



## Титан-К

Заключение ПП РФ №719



Находится в стадии  
сертификации

### Безопасность:

- уникальный идентификатор
- защита встроенного ПО от модификации
- низкий уровень побочных излучений

### Отказоустойчивость :

- защита от внезапного отключения питания
- контроль температуры



**TBW**  
**29 600 Тбайт**



**Windows, Linux,  
Android, MCBC,  
Эльбрус, ЗОСРВ  
«Нейтрино»**



**от 0 до +50°C**  
Рабочая  
температура

- **Интерфейс:** SATA 6 Гбит/с (совм. с SATA 3Гбит/с и SATA 1.5 Гбит/с)
- **Форм-фактор:** 2.5"
- **Срок хранения информации:** не менее 10 лет (при 10% износе памяти)

- **Ёмкость:** до 2400 Гбайт
- **Скорость чтения/записи:** до 470/440 Мбайт/с
- **Энергопотребление:** не более 4 Вт

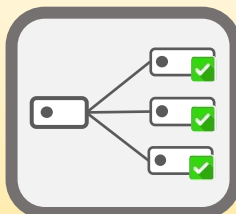
# ПРИМЕНЕНИЕ ДОВЕРЕННЫХ НАКОПИТЕЛЕЙ

Загрузочные  
устройства



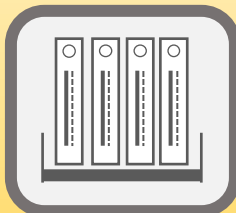
Накопитель для доверенных СВТ  
(тонкие клиенты, моноблоки,  
ПК, ноутбуки)

Универсальное  
переносное устройство



Передача сведений в "чужую"  
автоматизированную систему

Носитель служебных данных  
(Журналы, архивы, лицензии)



Длительное энергонезависимое  
хранение информации

Носитель  
ключевой информации

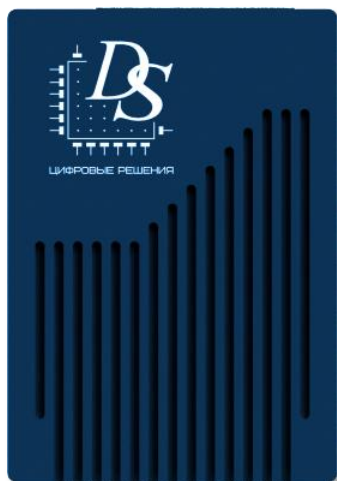


Совместное использование  
с DLP системами

# ВЫСОКОНАДЕЖНЫЙ НАКОПИТЕЛЬ SSD SATA 6 ГБИТ/С ТИТАН



ЦИФРОВЫЕ РЕШЕНИЯ



## Титан Титан М.2

Заключение ПП РФ №719

Находится в стадии присвоения  
категории качества «ВП»

### Надёжность:

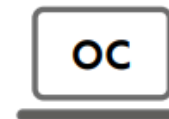
- прочный металлический корпус
- защита от внезапного отключения питания
- контроль температуры
- конформное покрытие

### Безопасность:

защита встроенного ПО от модификации



**TBW**  
до 14 800 Тбайт



**Windows, Linux,  
Android, МСВС,  
Эльбрус, ЗОСРВ  
«Нейтрино»**



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

- **Интерфейс:** SATA 6 Гбит/с (совм. с SATA 3Гбит/с и SATA 1.5 Гбит/с)
- **Форм-фактор:** 2.5", М.2
- **Срок хранения информации:** не менее 10 лет (при 10% износе памяти)

- **Ёмкость:** 300, 600, 900, 1200 Гбайт
- **Скорость чтения/записи:** до 470/440 Мбайт/с
- **Энергопотребление:** не более 4 Вт

# ПРИМЕНЕНИЕ ПРОМЫШЛЕННЫХ НАКОПИТЕЛЕЙ



ЦИФРОВЫЕ РЕШЕНИЯ

- БЛА
- Ноутбуки, планшеты, компьютеры
- Станции управления (НСУ)
- Бортовое оборудование
- Тренажерные системы

**ВПК**

- Аппараты УЗИ, МРТ
- Мониторинг дыхания
- Мониторинг состояния пациента
- Измерительное оборудование

**МЕДИЦИНСКОЕ  
ОБОРУДОВАНИЕ**

- Системы сбора данных
- Контрольно-измерительное оборудование
- Встраиваемые панельные компьютеры
- Роботизированные системы
- Граничные вычисления
- Машинное зрение
- IoT

**ПРОМЫШЛЕННОСТЬ**

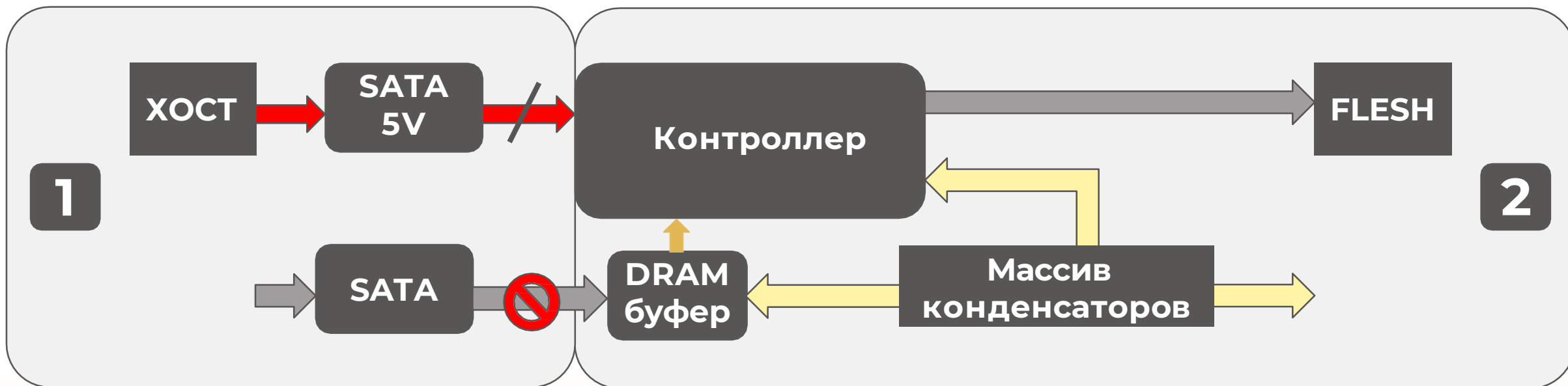
- Бортовые компьютеры
- Регистраторы данных
- Беспилотные решения
- Навигационные терминалы
- Тренажерные системы

**ТРАНСПОРТ**

# ЗАЩИТА ОТ СКАЧКОВ И ПОТЕРИ ПИТАНИЯ

**1** После срабатывания детектора напряжения, контроллер прекращает принимать новые команды от хоста

**2** ВПО контроллера выполняет запись FTL из **DRAM** буфера в **NAND**

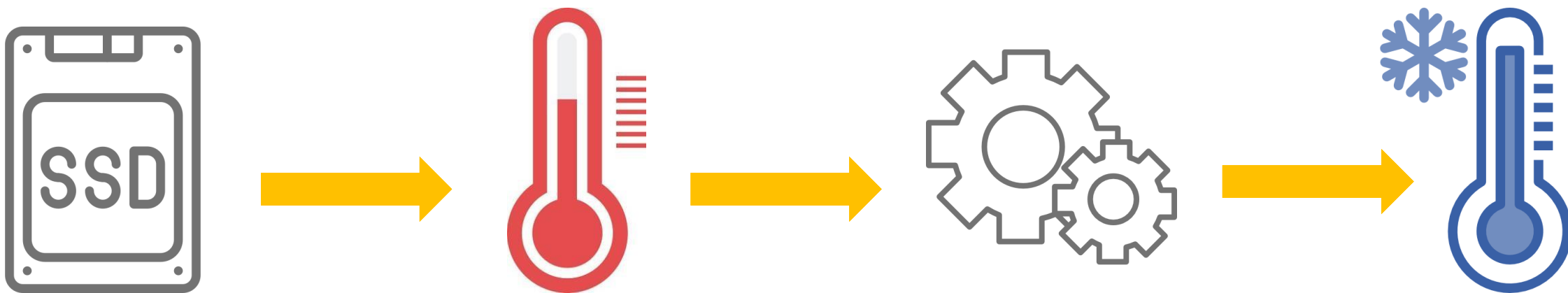


Данные технологии позволяют обеспечить целостность данных и минимизации риска повреждения в ответственных применениях

# ТЕПЛОВОЕ РЕГУЛИРОВАНИЕ



- +70°C - включение терморегулирования
- +85°C - отключение накопителя
- +60°C - переход в штатный режим работы



Наличие механизма терморегулирования позволяет оптимизировать производительность, продлить срок службы и повысить целостность данных



# ПОЧЕМУ НАКОПИТЕЛИ ОТ ЦИФРОВЫХ РЕШЕНИЙ?



ЦИФРОВЫЕ РЕШЕНИЯ

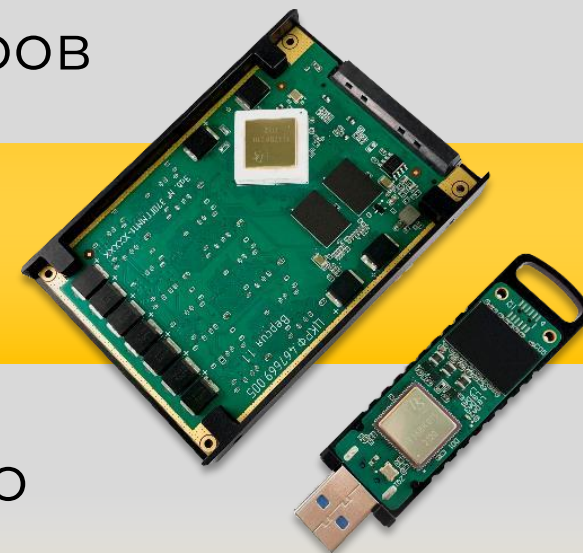
Дополнительные механизмы обеспечения надежности

Защита от подмены ПО и идентификаторов

Российский контроллер

Российская разработка и производство

Комплексная русскоговорящая техническая поддержка по проектам





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



habr



8 (919) 998-11-63 | Куренков Павел  
Инженер по продукту

8 (985) 176-84-26 | Шкляев Евгений  
Менеджер продукта

# СПАСИБО ЗА ВНИМАНИЕ!

Связаться с нами: [sales@dsol.ru](mailto:sales@dsol.ru)