

# **Информационная безопасность технологических сегментов IP-сети (СКАДА, АСУТП и прочее)**

**управление рисками**



# FOX-IT

## информация о компании

- Миссия: «Разработка инновационных решений для повышения уровня безопасности в обществе!»
- Компания создана в 1999 году
- Более 100 инженеров-разработчиков
  - Все сотрудники лицензированы Правительством Нидерландов
- Штаб-квартира в городе Делфт, Нидерланды, офисы в США и Великобритании
- Партнерская сеть по всему миру



# FOX-IT

## направления деятельности





# SNITEGROUP

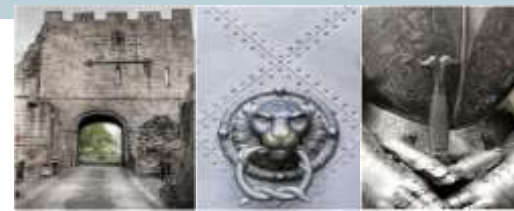
## Информация о компании

- SNITEGROUP – консалтинговая компания
- Экспертиза в области , решений по системам передачи данных, системам учета электроэнергии и информационной безопасности технологических сегментов сетей (SCADA, АСУТП и т.д.)
- Технологические партнеры – в 6 странах мира
- Штаб-квартира - г. Шлирен Швейцария



# Что такое риск?

- Риск – это комбинация вероятности события и его последствий (ISO/IEC Guide 73)
- Любые действия приводят к событиям и последствиям, которые могут представлять собой как потенциальные «положительные» возможности, так и «опасности»



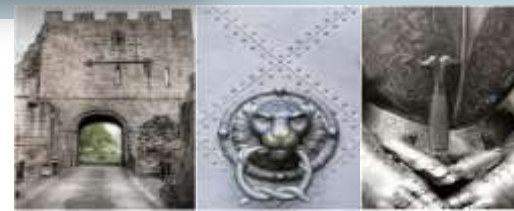
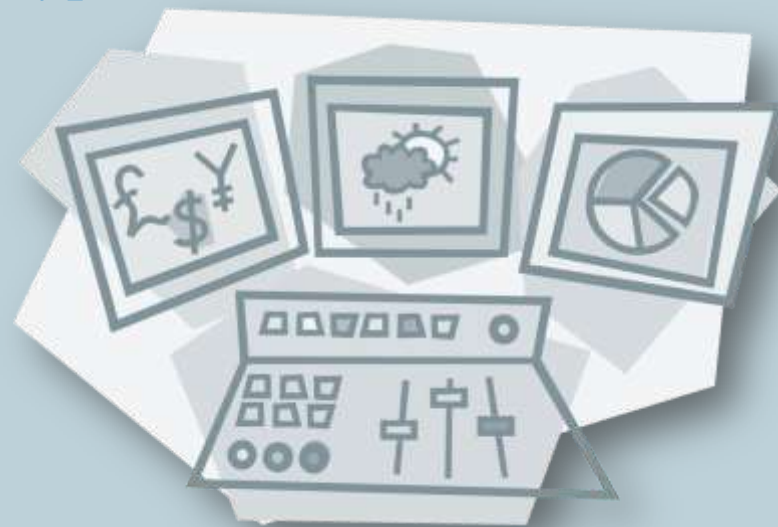
# Перечень рисков

- Ошибки персонала
- Преднамеренные действия по сокрытию (изменению информации)
- Утечка информации
- Качество сервиса
- Ошибки программного обеспечения
- Некорректная работа программно-аппаратных комплексов
- Нарушения методологии работы
- Искажения отчетности



# РИСК: Преднамеренные действия по сокрытию (изменению информации)

- Таблицы баз данных
- Экраны приложений
- Отчеты
- Системные и прикладные журналы событий



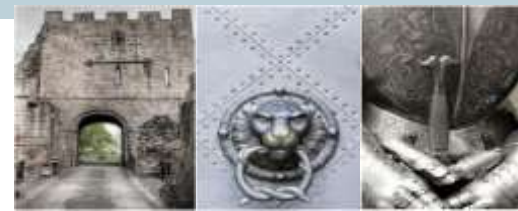
# Как это работает?

- **Запись и воспроизведение**
  - Запись всех действий пользователей в контролируемом сегменте сети
  - Полное восстановление экранов пользовательских сессий
- **Анализ содержания экрана**
  - Автоматическое распознавание экранов и полей баз данных
  - Поиск по содержимому экрана (а-ля “Google”), например: кто открывал мнемосхему объекта в определенный период времени?
- **Идентификация действий пользователя**
  - Постоянный анализ действий пользователей
  - Восстановление последовательности действий пользователя, которая может включать в себя, в том числе, несколько экранов и приложений
- **Аналитический процессор**
  - Настраиваемые правила отслеживания и предупреждения действий пользователей в реальном времени
  - Гибкая система изменения правил
  - Управление инцидентами обеспечивает предупреждение аварий и расследование произошедших событий





# Информационные потоки

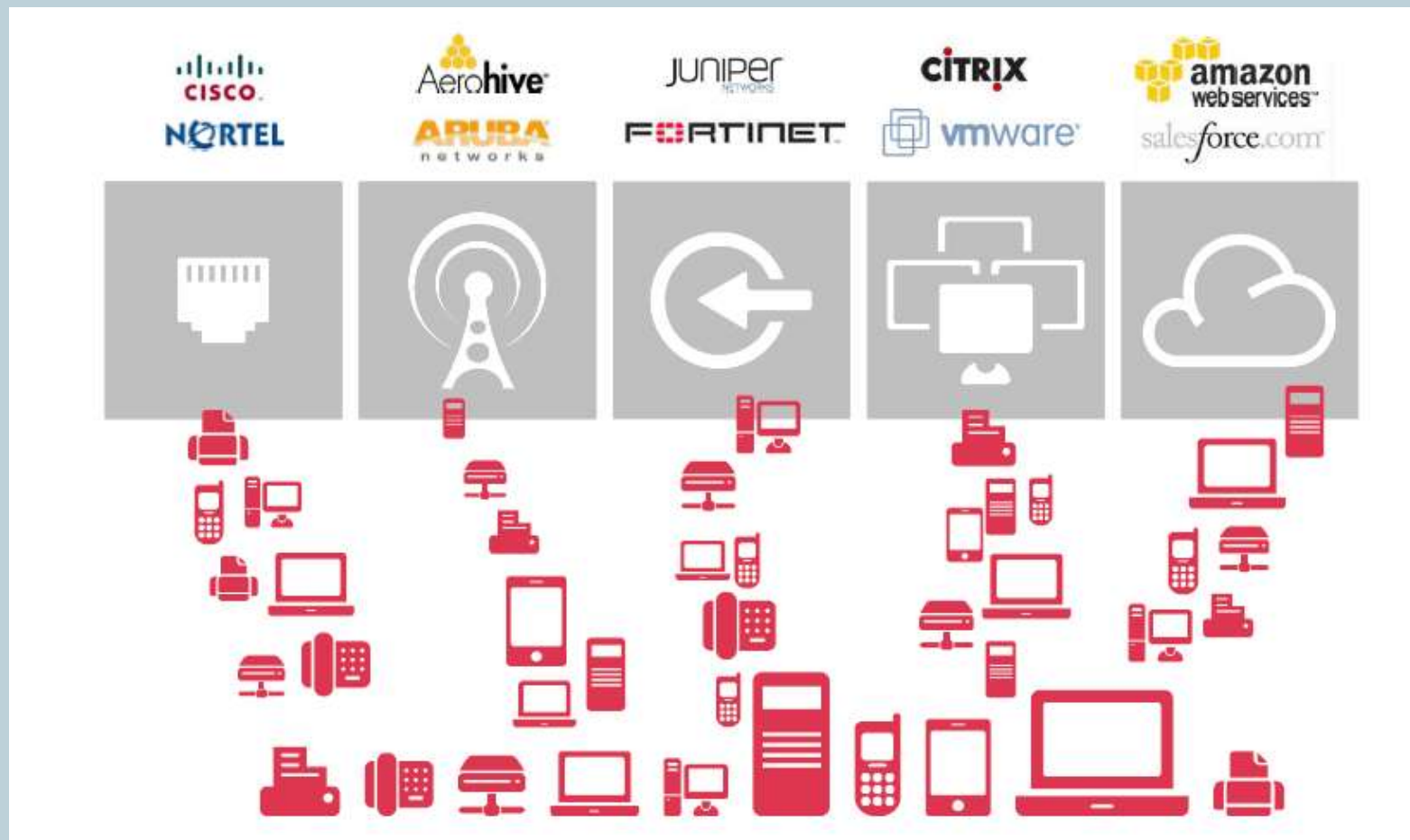


# Риск: Некорректная работа программно-аппаратных комплексов

- Бесконечные сочетания вариантов доступа к сети
- Многочисленные виды устройств, пользователей и услуг



# Схема доступа к сети



# Система управления доступом к сети

- Не требует установки агентов
- Стандартные протоколы (SNMP, SSH, HTTP)
- Интеграция с управляемыми и неуправляемыми устройствами доступа;
- Нет обработки трафика, не требует изменения топологии
- Интеграция с корпоративным каталогом и доменом
- Изменяемый белый список объектов для проверки подлинности
- Интегрируется в текущую сеть и существующую идеологию информационной безопасности



# РИСК: Утечка информации...

- Собственные ОС и протоколы → открытые стандарты
- Централизованные вычисления → распределенные вычисления
- Сегментированные потоки данных → интегрированные потоки данных
- Замкнутые системы → открытые системы

## В чем проблема ?

Если мы присоединены к сети, то более уязвимы



Должны быть отделены от сети



Нет реального времени

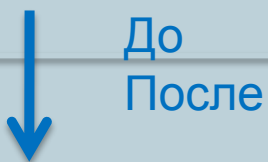
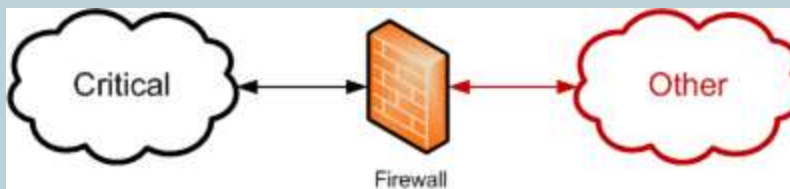


# Варианты присоединения к сети

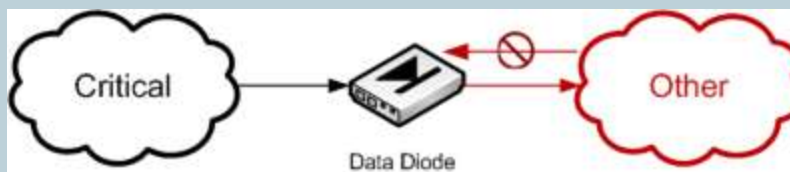
- Air Gaps



- Firewalls



- Data Diodes



# Вариант 1: Отсутствие соединения

- Ручной перенос данных на CD
- Подготовка данных по устным запросам



## Преимущества:

- Нет соединения = нет потери уровня безопасности

## Недостатки:

- Нет реального времени
- Ручной ввод данных
- Потеря информации
- Больше рисков технических ошибок



## Вариант 2: Фаерволлы

- Логическое разделение сетей
  - Блокировка неавторизованного доступа
  - Разрешение на авторизованные потоки данных

- **Преимущества:**

- Проверенная технология
- Автоматизированное и гибкое решение

- **Недостатки:**

- Нет гарантии от ошибок пользователей, хакеров и недобросовестных пользователей





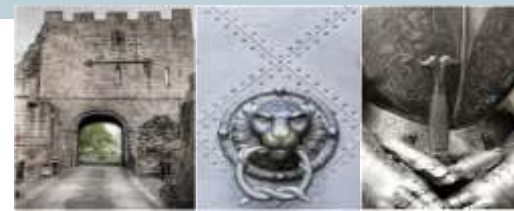
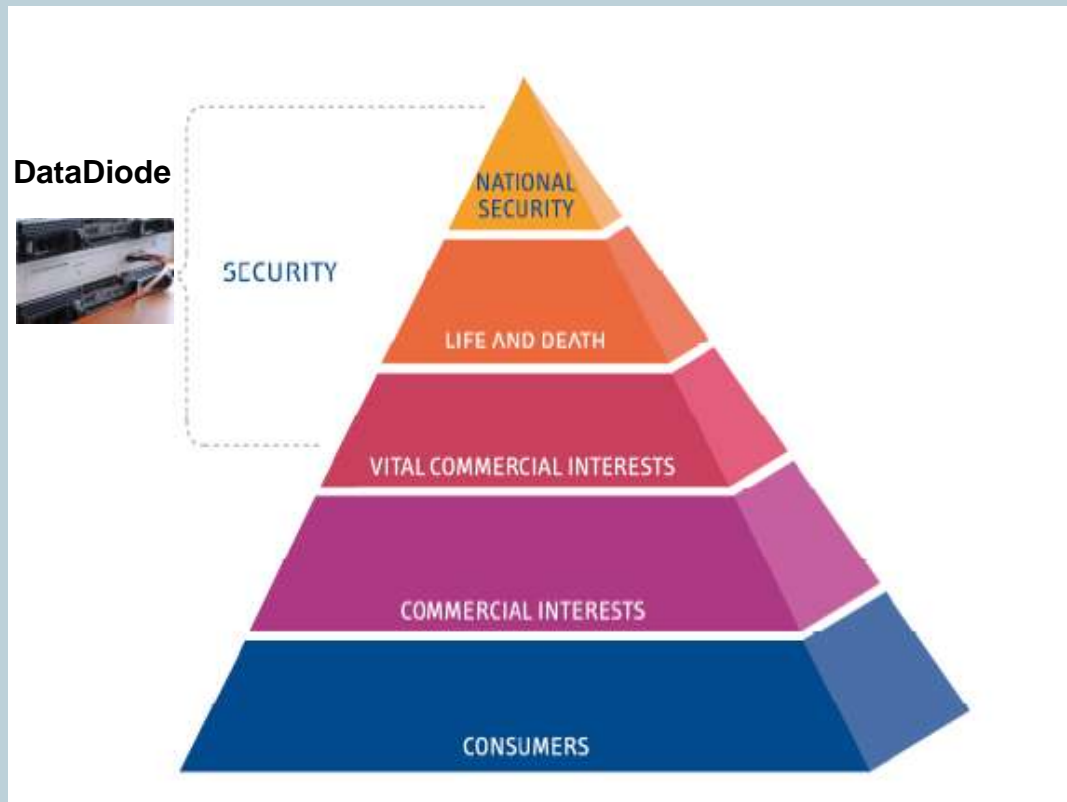
## Вариант 3: ДатаДиоды

- Однонаправленное на физическом уровне, соединение сегментов сетей
- **Преимущества:**
  - Автоматическое и гибкое решение
  - Однонаправленное соединение
  - Взлом не возможен,
  - Нет возможности онлайн-атак и потерь данных 100% защита !
- **Недостатки:**
  - Однонаправленное соединение

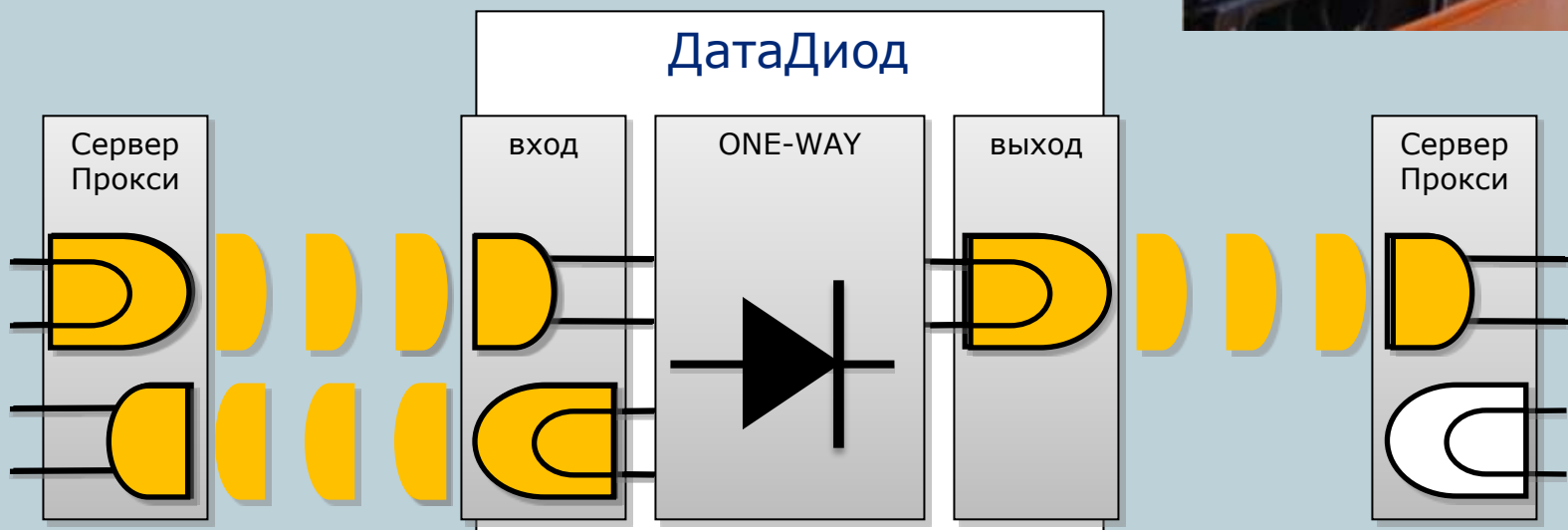


# История создания ДатаДиода

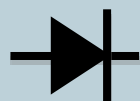
- ДатаДиод первоначально был разработан для использования в государственных организациях EU
- Однако со временем нашел широкое применение также в промышленности и коммерческой сфере



# Как это работает?

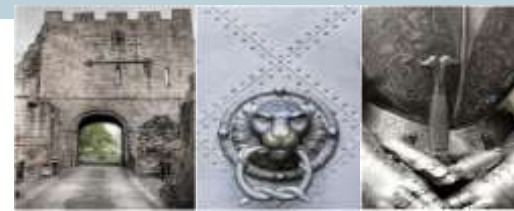


Световой  
передатчик

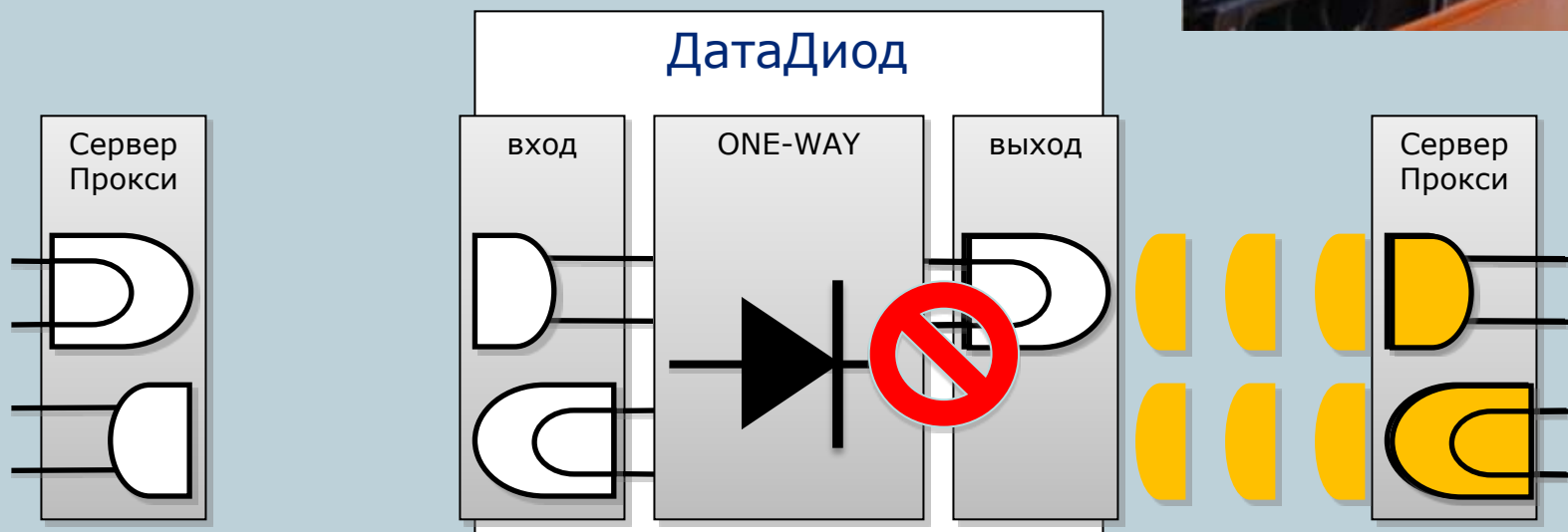


Световой  
приемник

Допустимо



# Как это работает?



Световой передатчик



← Невозможно

Световой приемник



# ДатаДиод



Однонаправленное коммуникационное устройство:

- аппаратная реализация (нет ПО, прошивок)
- сертифицировано
- не может быть взломано
- большое количество внедрений по всему миру

Более 300 поддерживаемых протоколов,  
например:



# Сертификация решения



- Сертификаты
  - Common Criteria **EAL 7+** (Европейский союз)
  - Национальные стандарты
    - NL-NCSA (Голландия)
    - BSI (Германия)
  - NATO Secret (NS)
  - ФСТЭК (Россия)
- NERC (US)  
(North American Electric Reliability Corporation)



# Внедрения



- Правительственные структуры
- Службы безопасности
- Армия
- Полиция
- NASA
- НАТО
- Банки
- Промышленность
- Телекоммуникации



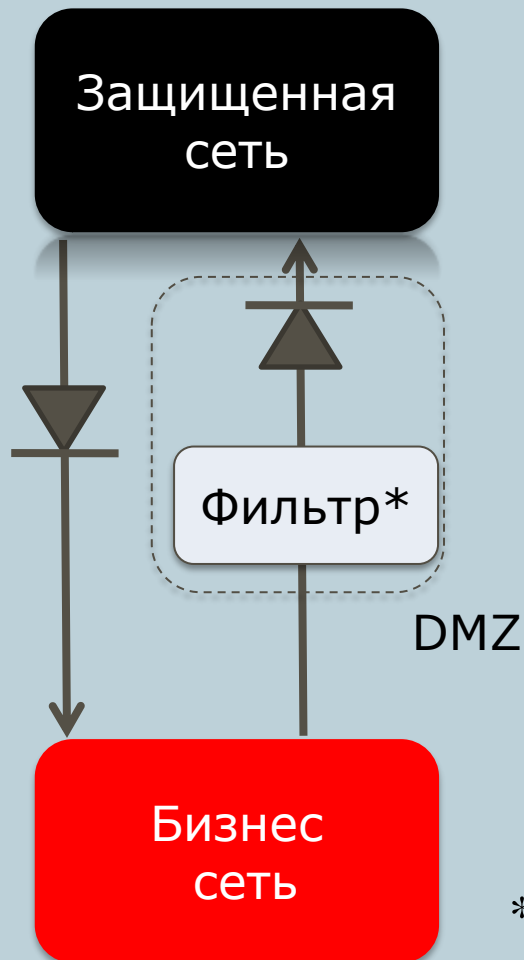
# Типичные приложения



- Передача данных СКАДА/Process Control Security
- Передача файлов (FTP/CIFS/SMB)
- Работа с электронной почтой (SMTP)
- Аудио/Видео поток (UDP)
- Удаленная печать
- Репликации баз данных: Oracle, mysql, MSSQL, etc
- Синхронизация LDAP/Active Directory
- Синхронизация данных
- Сервис обновления Windows Server (WSUS)
- Обновление антивирусов: McAfee, Symantec etc...
- Синхронизация веб-страниц
- Мониторинг удаленных сетей (SNMP)/ Nagios





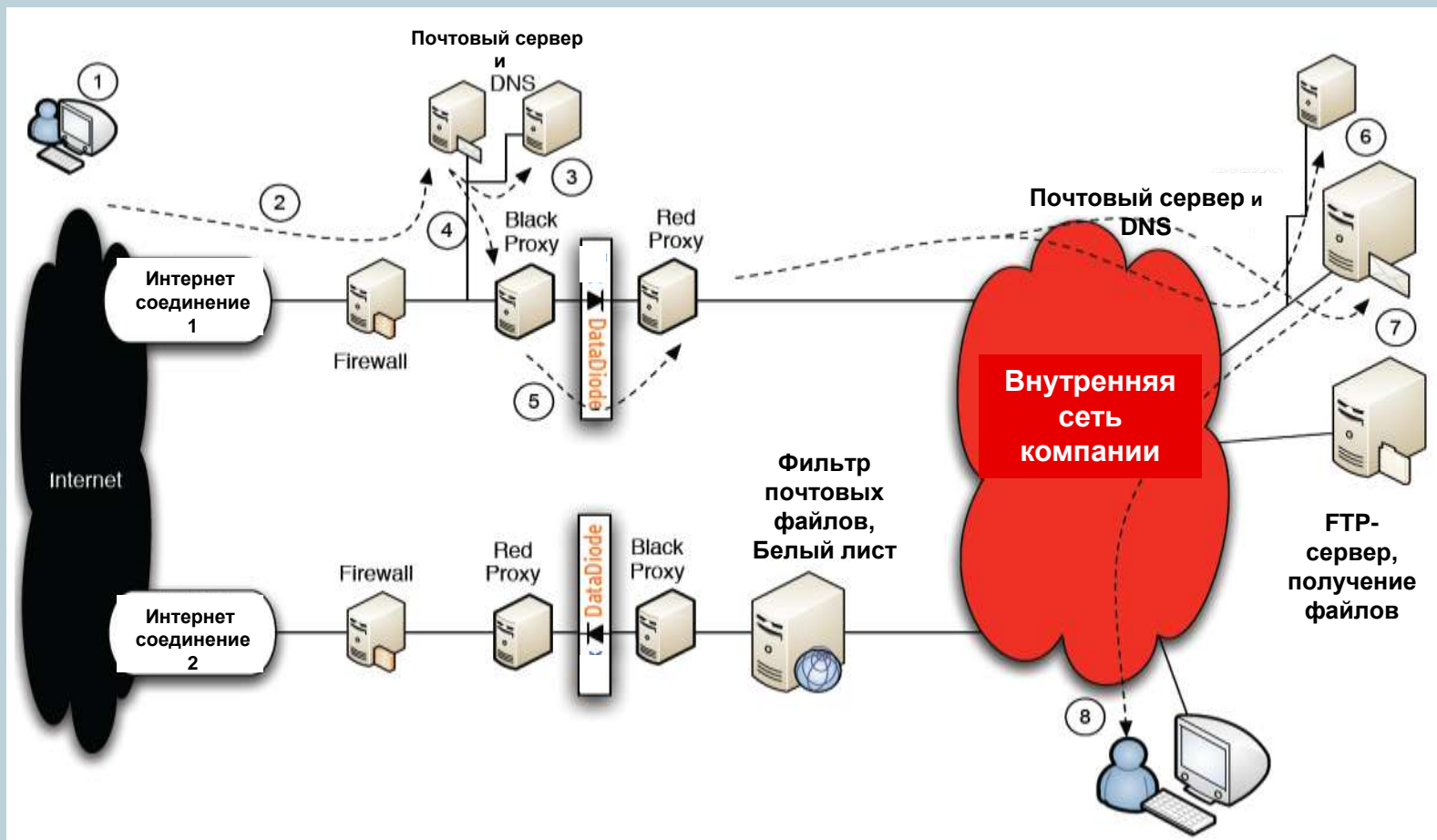


- Контролируемое двунаправленное соединение
- Исходящие файлы изолируются прежде чем они поступят в защищенный сегмент сети
- DMZ и Фильтр обеспечивают контроль файлов поступающих в защищенный сегмент сети

\* приложение другого производителя

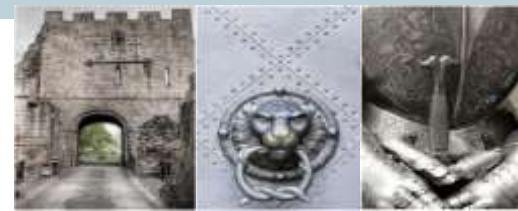


# Пример комплексного решения: Электронная почта

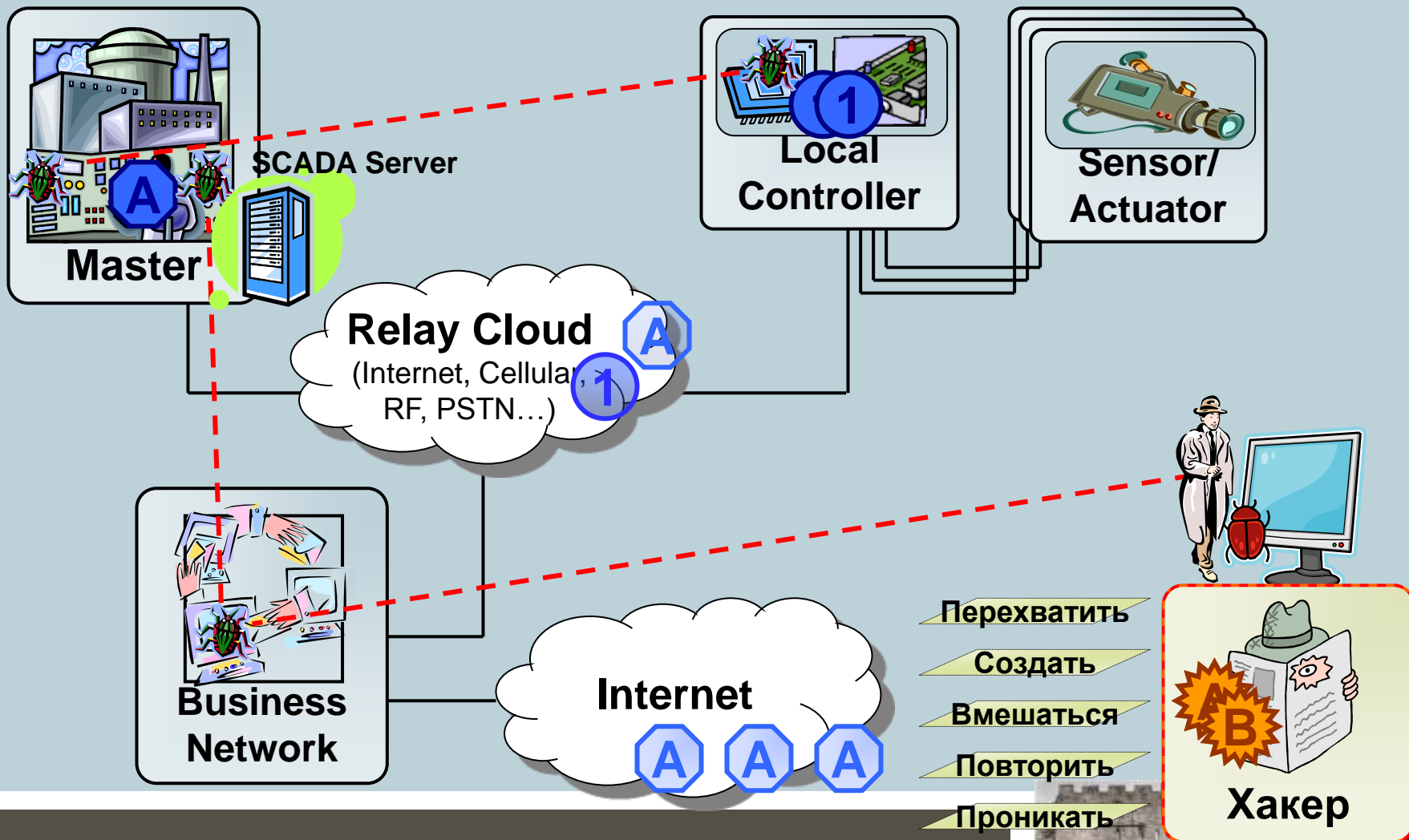


# Промышленность

- Электроэнергетика (сети, сбыты, генерация, включая атомные станции)
- Нефть и Газ (добыча, переработка)
- Водоканалы
- Оборонная промышленность
- Автомобильные и железнодорожные системы управления
- Инфраструктура портов
- Контроль воздушного движения
- Налоговые органы
- Телеком компании

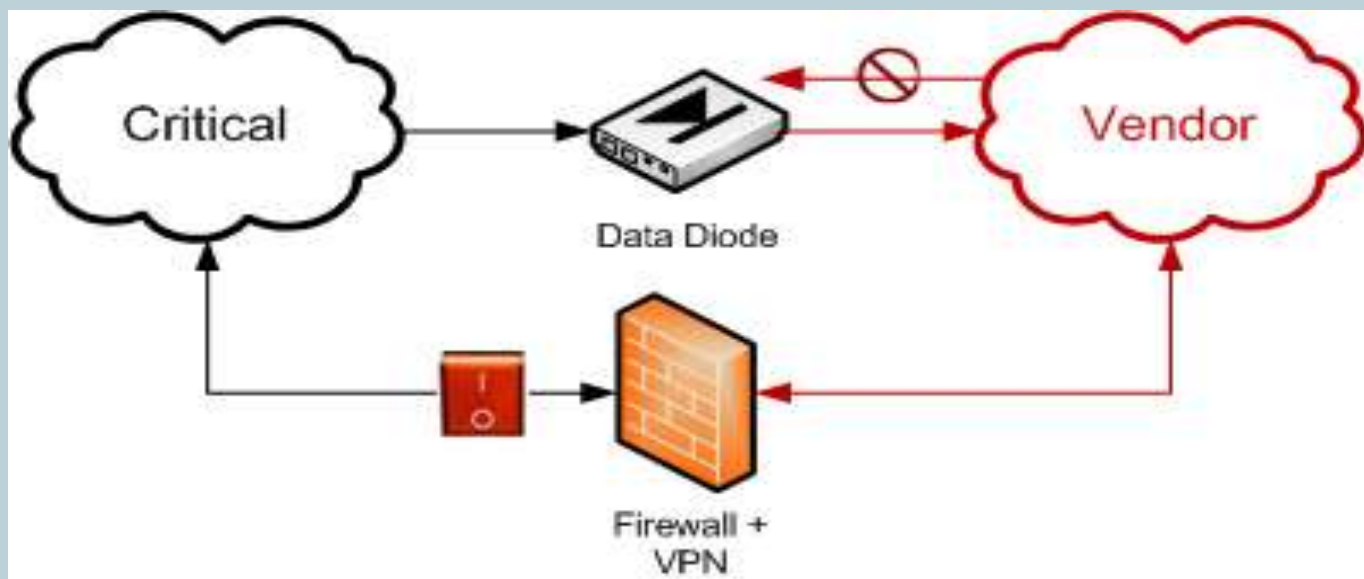


# Критическая инфраструктура: Угрозы!



# Пример: Решение для сервисных компаний

- Возможность безопасно мониторить работоспособность системы управления через удаленный доступ
- Обратный канал по умолчанию отключен, но может быть активирован по запросу



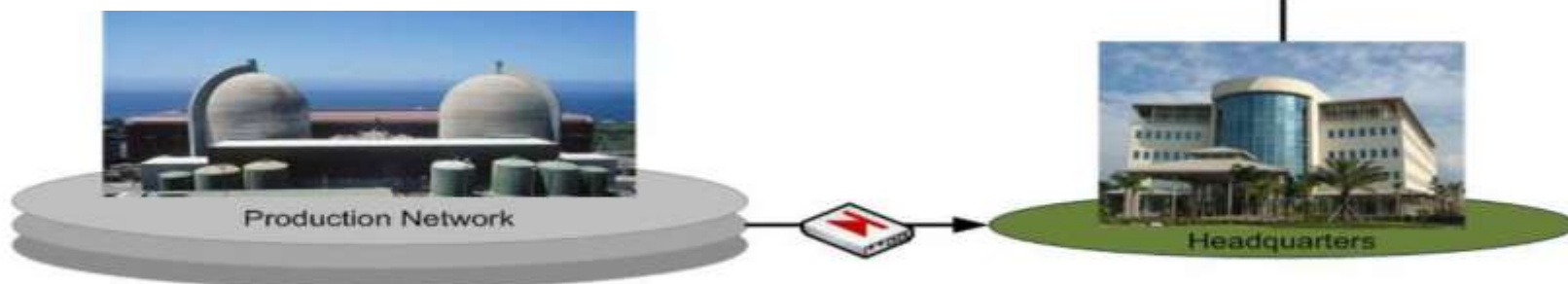
# Пример: Атомные станции (до)



# Пример: Атомные станции (после)

Все требуемые данные через корпоративную сеть направляются регулятору.

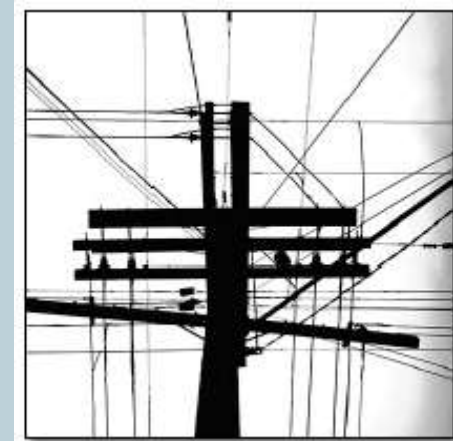
Защищенность корпоративной сети обеспечена ДатаДиодами



# Пример: Электроэнергетика

- **Голландия/Евросоюз**

- Регулятор контролирует производство и потребление электроэнергии
- Получает данные от всех энергетических компаний страны
- ДатаДиод позволяет Регулятору сохранять уровень защищенности своей сети



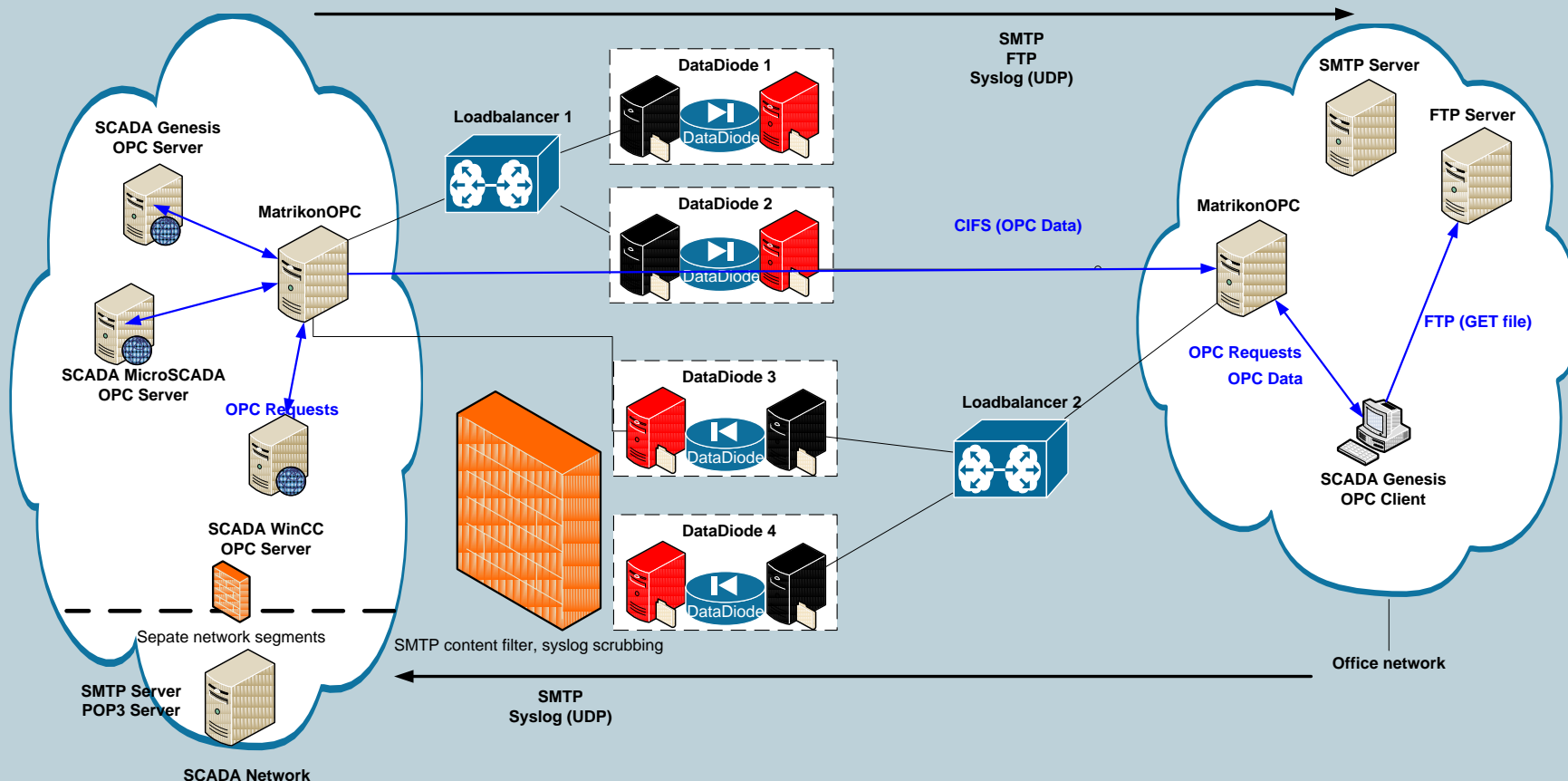
- **ОАО «Русгидро»/Россия**

- Взаимодействие СКАДА и Бизнес сегментов сетей на станционном уровне
- ДатаДиод обеспечивает безопасный доступ к данным контура оперативного управления





# Пример: Типовое решение для ОАО «Русгидро»



# Спасибо за внимание!



## ДатаДиод

### Система управления доступом в сеть



### Система контроля за действиями персонала



Evgeny Gengrinovich  
Executive Director SNITEGROUP GmbH  
tel. +7(985) 9288602, E-mail: gel@snitegroup.com