12.07.2023

АМТ-ГРУП

Системы однонаправленной передачи данных, как элемент комплексной защиты АСУ ТП

Волков Пётр – ведущий аналитик АМТ-ГРУП

Устройство однонаправленной передачи данных функционирует на физическом уровне

- **Однонаправленный шлюз** – устройство, обеспечивающее передачу файловой и потоковой информации в одном направлении и не позволяющее передачу в обратном
  - Однонаправленность передачи гарантируется аппаратными решениями
  - Применяется для соединения разных сегментов сети и используется в области защиты информации

Диоды данных – эффективное решение для защиты значимой информационной инфраструктуры

Диоды данных обеспечивают:

- ❑ Защиту периметра сегмента сети
- ❑ Предотвращение развития атаки ещё на этапе рекогносцировки
- ❑ Принципиальную невозможность взломать/неправильно настроить аппаратную компоненту
- ❑ Блокировку удалённого воздействия на защищаемый сегмент сети
- ❑ Связность ИТ-инфраструктуры и непрерывность бизнес-процессов

Линейка решений InfoDiode

Все решения «диод» можно условно разделить на два класса

Аппаратные «диоды»

Плюсы
- Недорого
- Решают базовые задачи изоляции
- Plug&Play
- Не требуют сопровождения службы эксплуатации

Минусы
- Не имеют IP, MAC адреса
- Требуют коммутации «порт-порт»
- Передать даже асинхронный TCP/IP трафик не получится

Аппаратно-программные «диоды»

Плюсы
- Передают асинхронный и даже синхронный TCP/IP трафик
- Несколько видов прикладного трафика одновременно
- Полноценное СЗИ (NAT, списки доступа, порты, контроль изменений конфигурации, контроль доступа)
- Интеграции: SIEM, SNMP, AD, Syslog, NTP…

Минусы
- Могут занимать 3 или более RU
- Требуют специалиста в эксплуатации с базовыми навыками
- Требуют периодического (хотя и редкого) обновления ПО

Соблюдается принцип однонаправленности **физический сигнал только в одну сторону**

InfoDiode.ru

АК InfoDiode эффективно сочетают все лучшие практики по защите периметра КИИ в случае необходимости передачи UDP, Syslog, SPAN и др. трафика

АК INFODIODE

Характеристики

Базовое аппаратное решение для монтажа на DIN-рейку или Desktop вариант.

MINI

Характеристики

Базовое аппаратное решение для монтажа в стойку.

RACK single

Характеристики

Аппаратное решение для монтажа в стойку (два «диода» в одном).

RACK - double

InfoDiode.ru

АПК InfoDiode PRO - позволяют передавать файловый и иной трафик по однонаправленному каналу

АПК INFODIODE PRO

- **Многофункциональный** (передает несколько видов протоколов и видов трафика одновременно: например, видео, файлы), имеет много апробированных сценариев реализации: репликация СУБД, ВМ, обновление ПО и т.п.
- **Высокопроизводительный** в части файловой передачи, в том числе реализует приоритезацию трафика, деление канала и т.п.
- **Поддерживает широкий спектр файловых протоколов** (FTP/FTPS, SMB, SMTP, UDP, SFTP)
- **Высокая надёжность** – кластерный вариант
- **Интегрируется в ИТ/ИБ ландшафт** (SIEM, SNMP, AD, Syslog, NTP…)
- **Реализован на российской платформе**, российском программном обеспечении производства АМТ-ГРУП

InfoDiode.ru

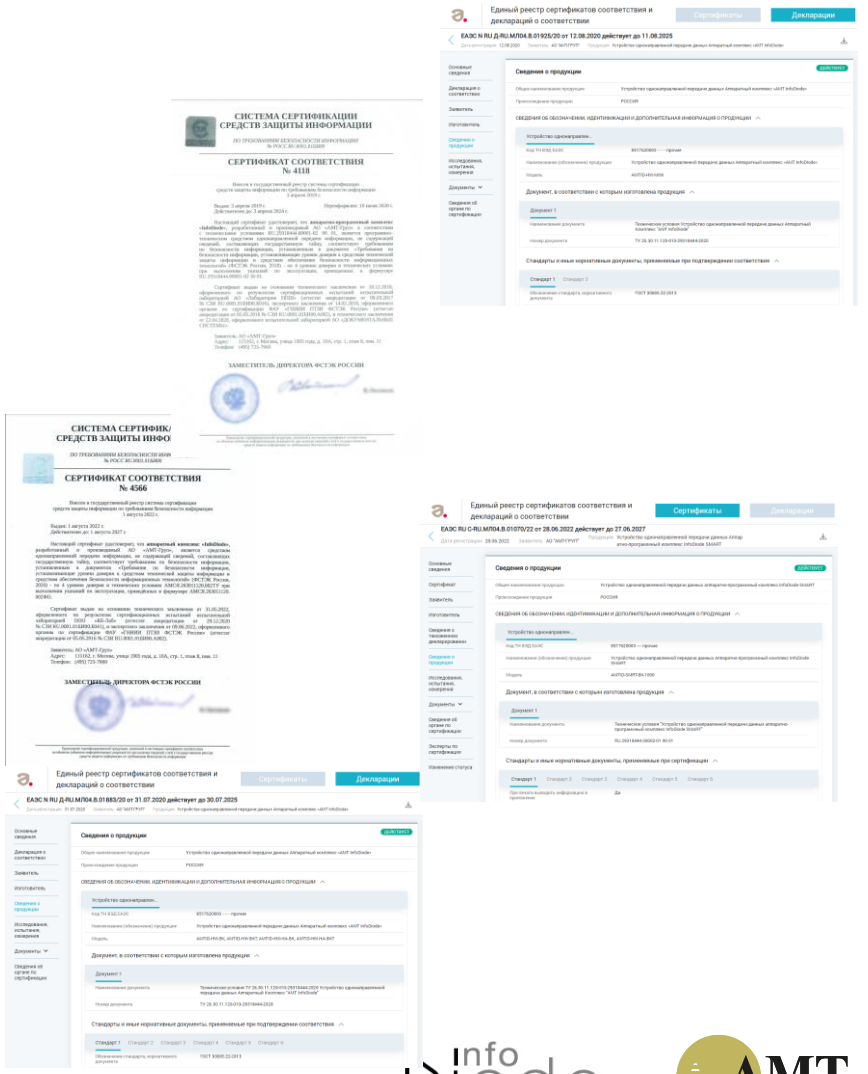
АПК InfoDiode SMART – решение для использования с АСУ ТП

АПК INFODIODE SMART

- **Компактный – 1U rack решение.** Упрощает встраивание в разнородную инфраструктуру
  - Виртуальные среды, серверы заказчика, докеры, операционные системы
- **Поддерживает пром. протоколы** (Modbus, OPC UA/DA, IEC, MQTT, S7…)
- **Многофункциональный** (передает несколько видов трафика одновременно: например, видео, файлы, пром. протоколы)
- **Предоставляет возможность разрабатывать собственные коннекторы** под конкретные задачи и для передачи требуемых промышленных протоколов
- **Реализован на российской платформе**, российском программном обеспечении производства АМТ-ГРУП

Сертифицированное решение

- Вся линейка АК InfoDiode и АПК InfoDiode PRO сертифицирована ФСТЭК УД4
  - АПК InfoDiode SMART в процессе сертификации
- Все продукты линейки InfoDiode соответствуют требованиям тех. регламента Таможенного Союза
- Включение в Реестр российской промышленной продукции (МинПромТорг) - в процессе



Комплексный подход для предотвращения разных классов атак

Разнообразие защищаемых объектов:

- ❑ Защита удалённого подключения
- ❑ Защита на границе сегментов
- ❑ Защита обособленных и смежных сегментов
- ❑ Защита в сети IT
- ❑ Защита внутри сети OT (промышленные протоколы)
- ❑ …

Разнообразие средств защиты:

- ❑ Аутентификация и авторизация
- ❑ Обновления ПО
- ❑ Антивирусная защита
- ❑ Firewall
- ❑ Диод
- ❑ DLP
- ❑ SOC/SIEM
- ❑ …

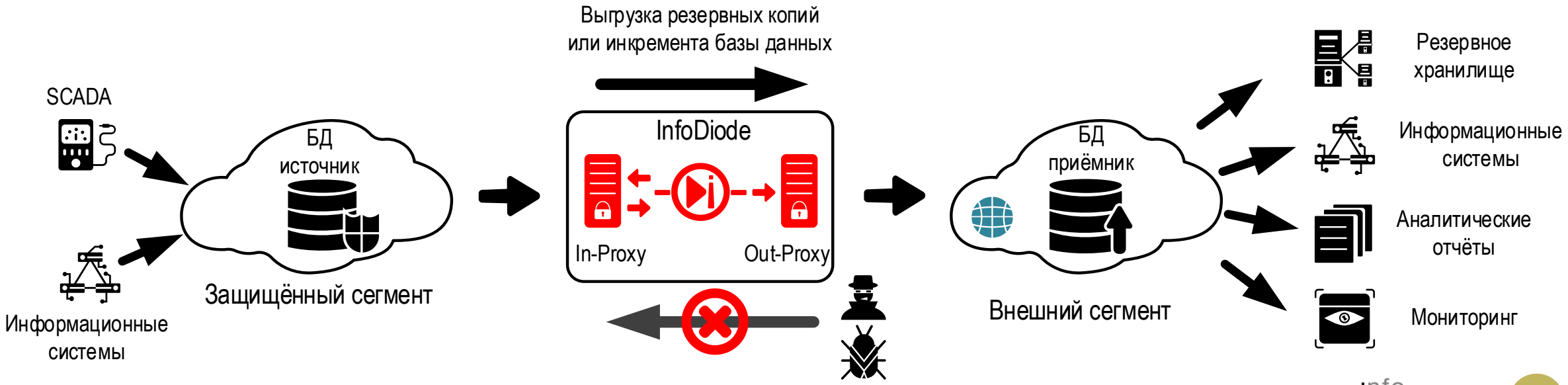
Эффективно противодействовать атаке - означает **предотвратить** конкретные этапы/последствия атаки **каждый раз**, когда такая атака осуществляется

Сценарии комплексной защиты объектов КИИ с использованием InfoDiode

Репликация баз данных через InfoDiode

Взаимодействие с СУБД для репликации данных на удалённую площадку

- ❑ Изоляция доверенного сегмента от внешних воздействий при помощи InfoDiode
- ❑ Оперативное предоставление информации для мониторинговых, аналитических и др. систем
- ❑ Автоматизация операций в соответствии с настраиваемым расписанием

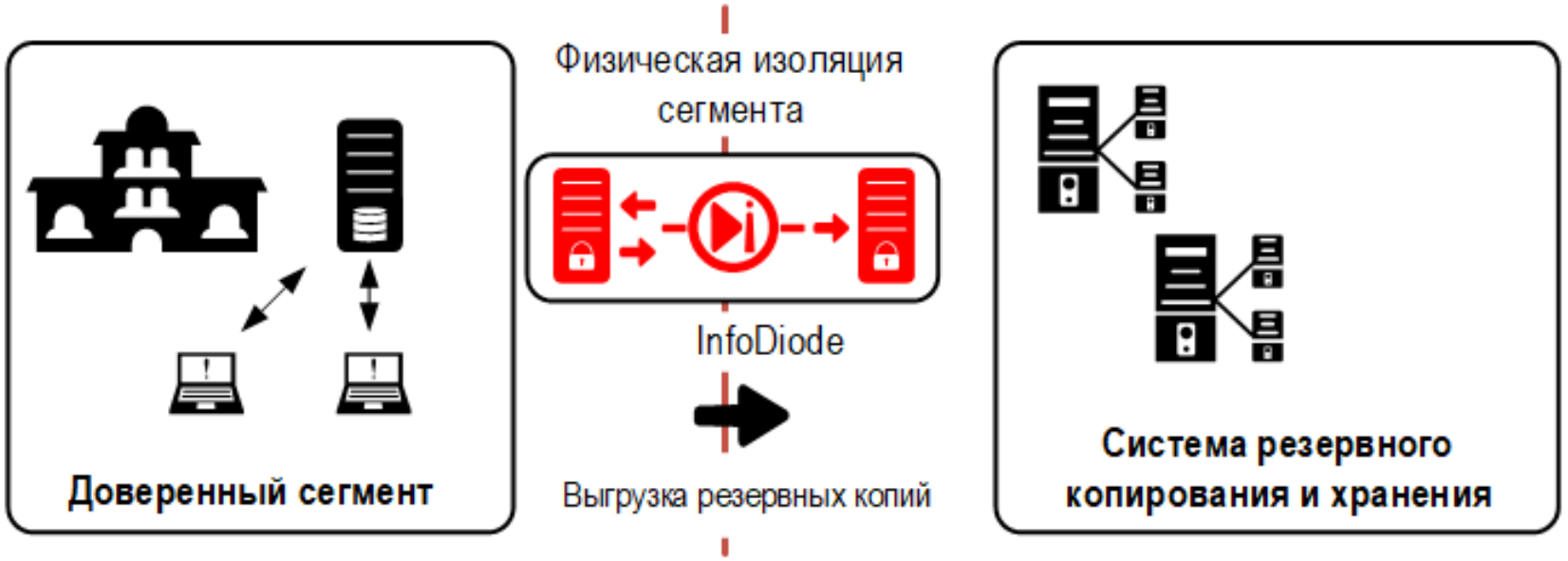


InfoDiode.ru

Резервное копирование на удалённую площадку через InfoDiode

Резервное копирование в удалённый ЦОД через однонаправленный канал

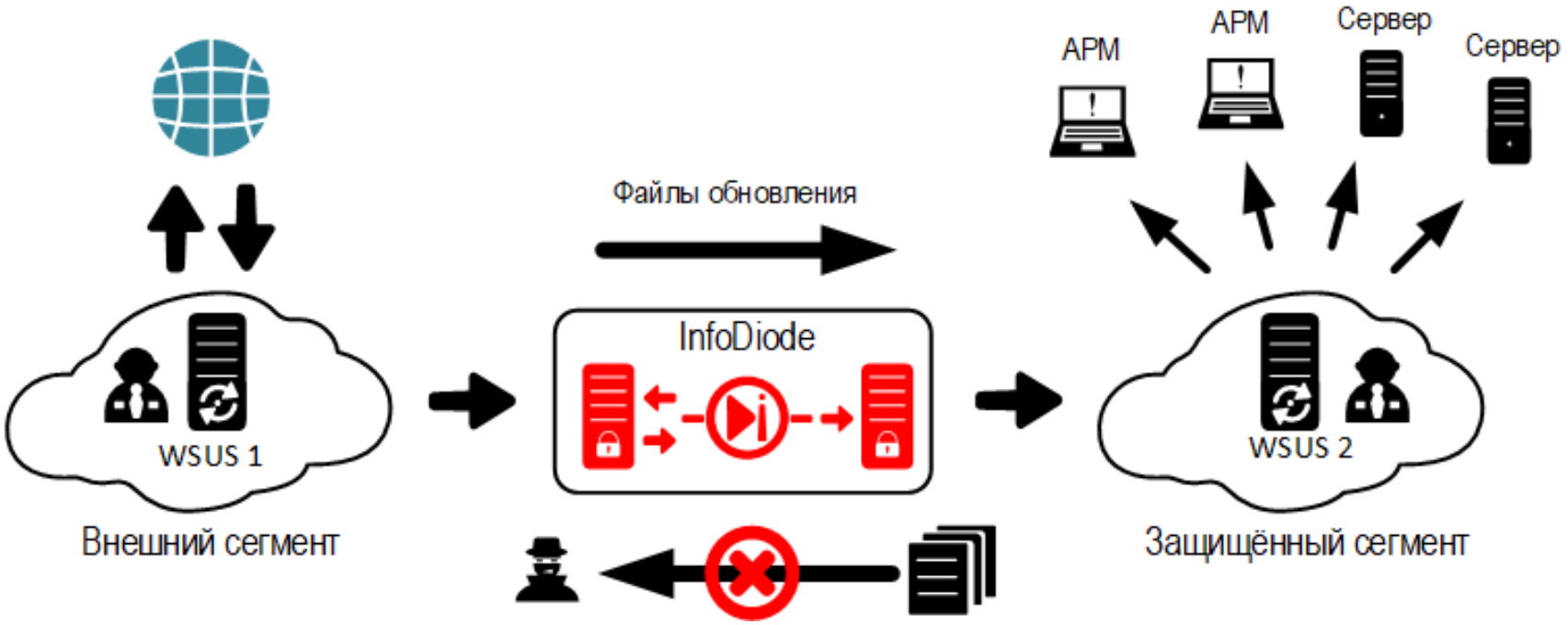
- ❑ Изоляция доверенного сегмента от внешних воздействий при помощи InfoDiode
- ❑ Централизация управления резервными копиями и катастрофоустойчивость
- ❑ Автоматизация операций в соответствии с настраиваемым расписанием



Установка обновлений программного обеспечения через InfoDiode

Обеспечение управления обновлениями ПО

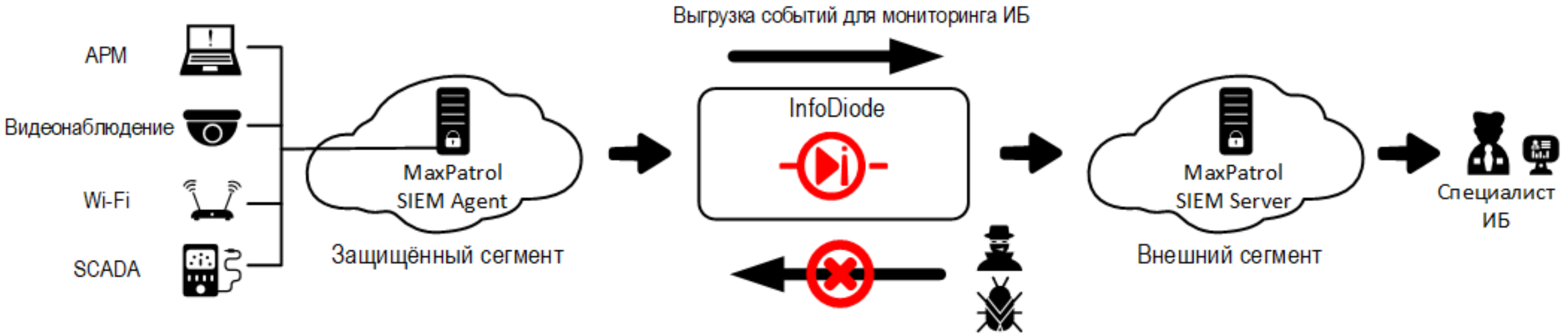
- ❑ Ограничение доступа к защищённому сегменту при помощи InfoDiode
- ❑ Обеспечение обновления ПО стандартными средствами (WSUS)
- ❑ Блокировка двунаправленных взаимодействий с защищаемым сегментом



Передача данных в Центр обеспечения безопасности (SOC) - SIEM

Передача данных о событиях ИБ из защищённого сегмента в SOC на примере MaxPatrol SIEM

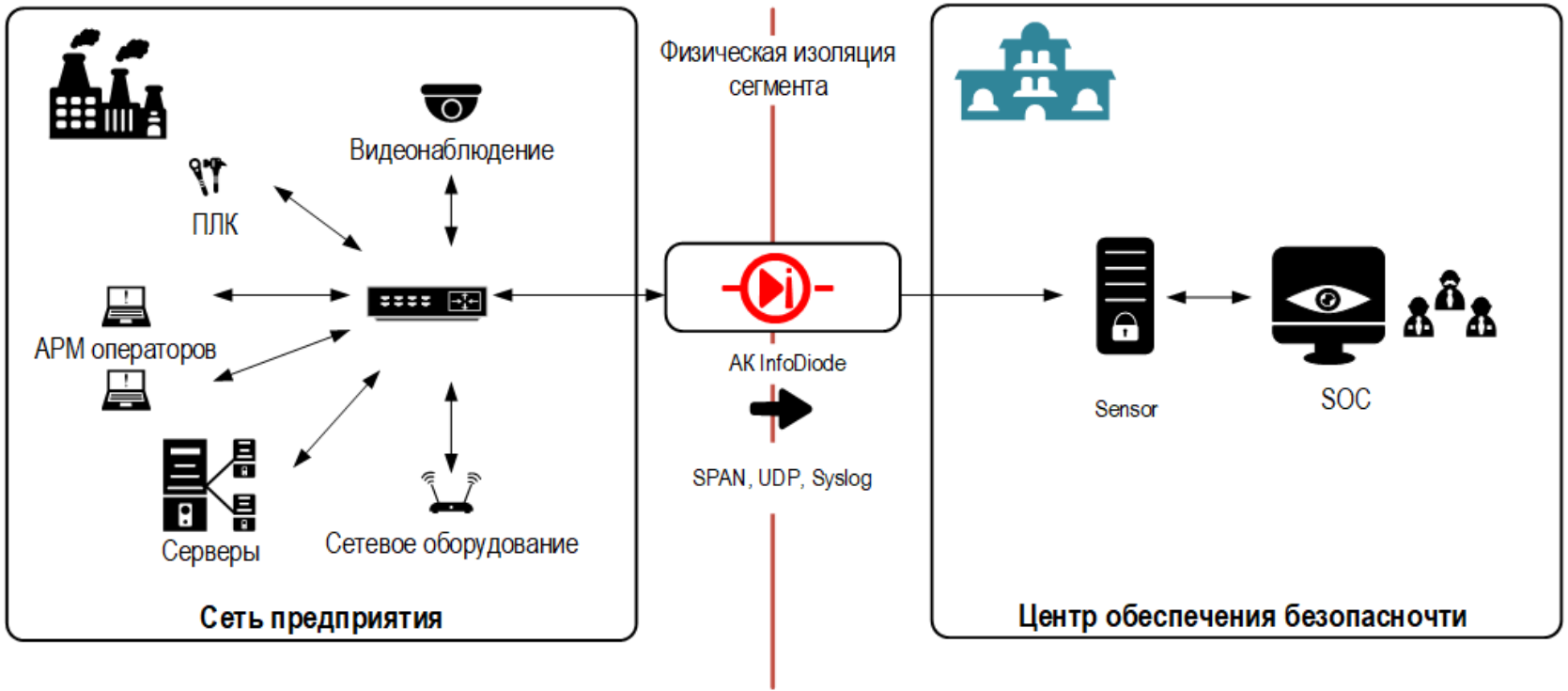
- ❑ Централизация мониторинга и управления ИБ
- ❑ Сбор данных о событиях ИБ на агенте с последующей передачей в SOC
- ❑ Изоляция доверенного сегмента от воздействий из сегмента ИБ с помощью InfoDiode



Передача данных в Центр обеспечения безопасности (SOC)

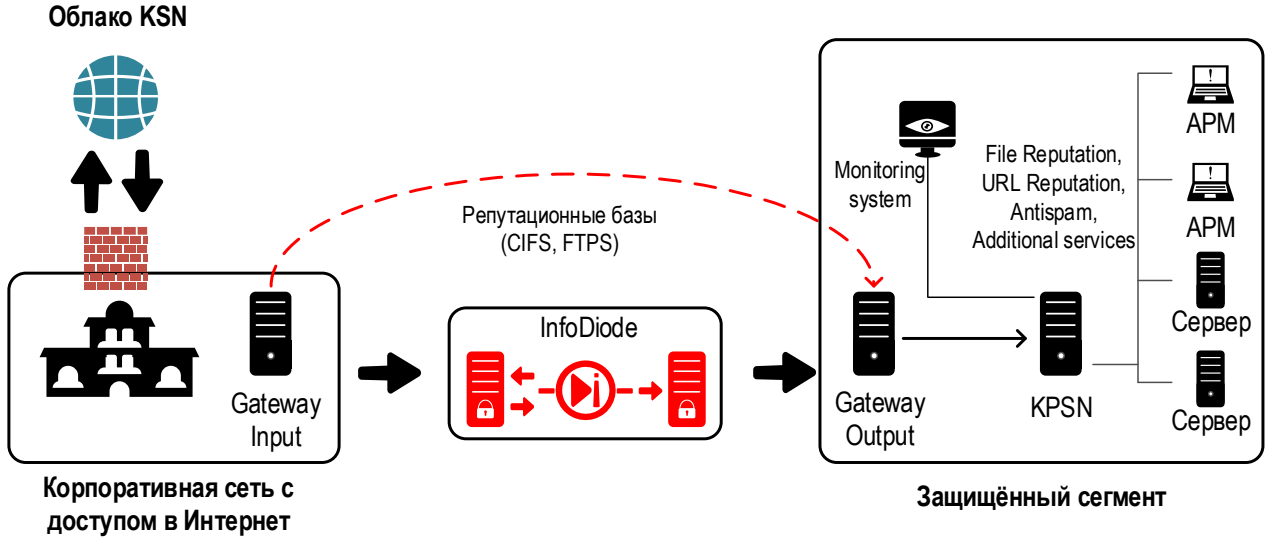
Взаимодействие с SIEM (на примере PT ISIM, CL DATAPK и KICS for Networks)

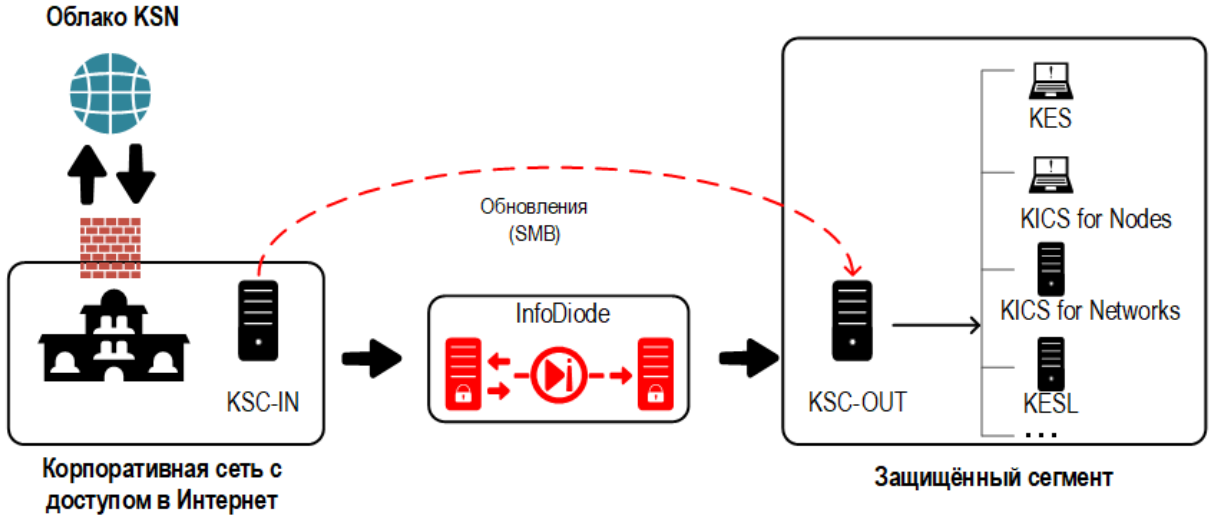
- ❑ Построение системы обнаружения вторжений с InfoDiode
- ❑ Передача зеркалированных данных на сенсор SIEM для анализа и поиска признаков атаки
- ❑ Изоляция доверенного сегмента от воздействий из сегмента ИБ с помощью InfoDiode



InfoDiode.ru

Обновление средств защиты (KSC, KSPN, др.) через InfoDiode





Обновление СЗИ с InfoDiode на примере KSC и KSPN:

- ❑ Ограничение доступа к защищённому сегменту при помощи InfoDiode
- ❑ Реализацию возможности оперативно обновлять средства ИБ в защищённом сегменте
- ❑ Пресечение двустороннего взаимодействия с защищённым сегментом извне

InfoDiode.ru

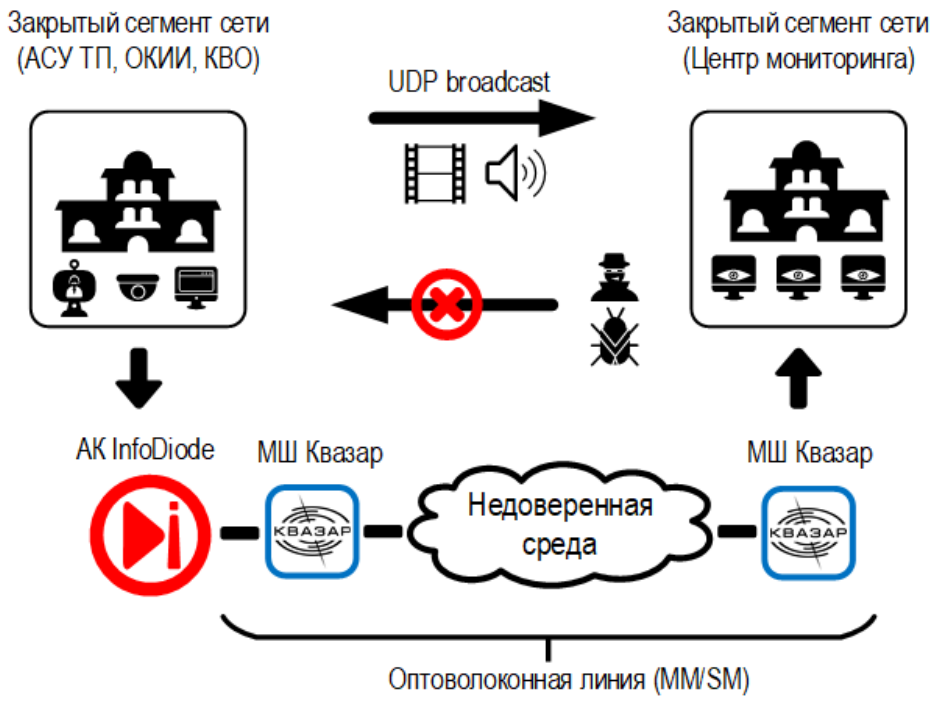
Криптозащита передаваемых через InfoDiode данных – МШ «Квазар»

Взаимодействие с системами криптозащиты на примере МШ «Квазар»

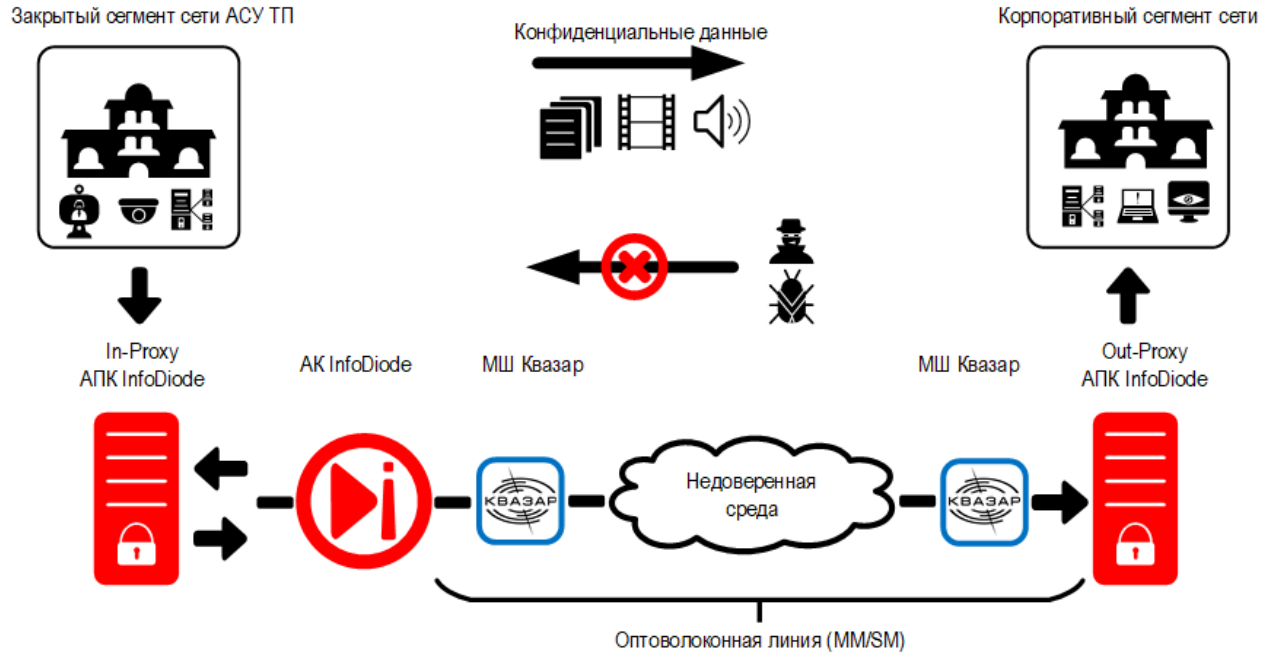
- Защита передаваемых данных от утечки и компрометации путём шифрования данных на недоверенном участке

- Изоляция доверенного сегмента от воздействий извне с помощью InfoDiode

1



2

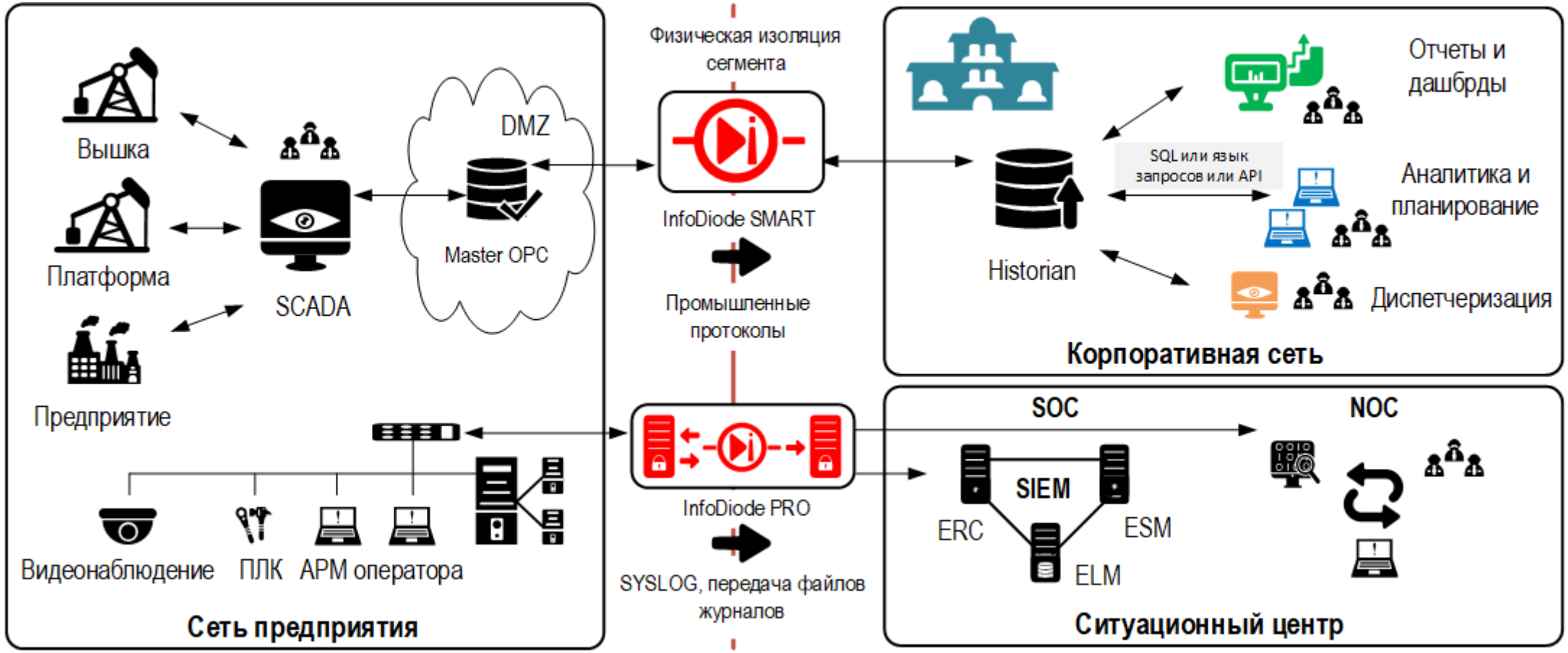


InfoDiode.ru

Сценарии взаимодействия с АСУ ТП с использованием InfoDiode

Агрегация данных АСУ ТП (SCADA-SCADA) на примере добычи нефти

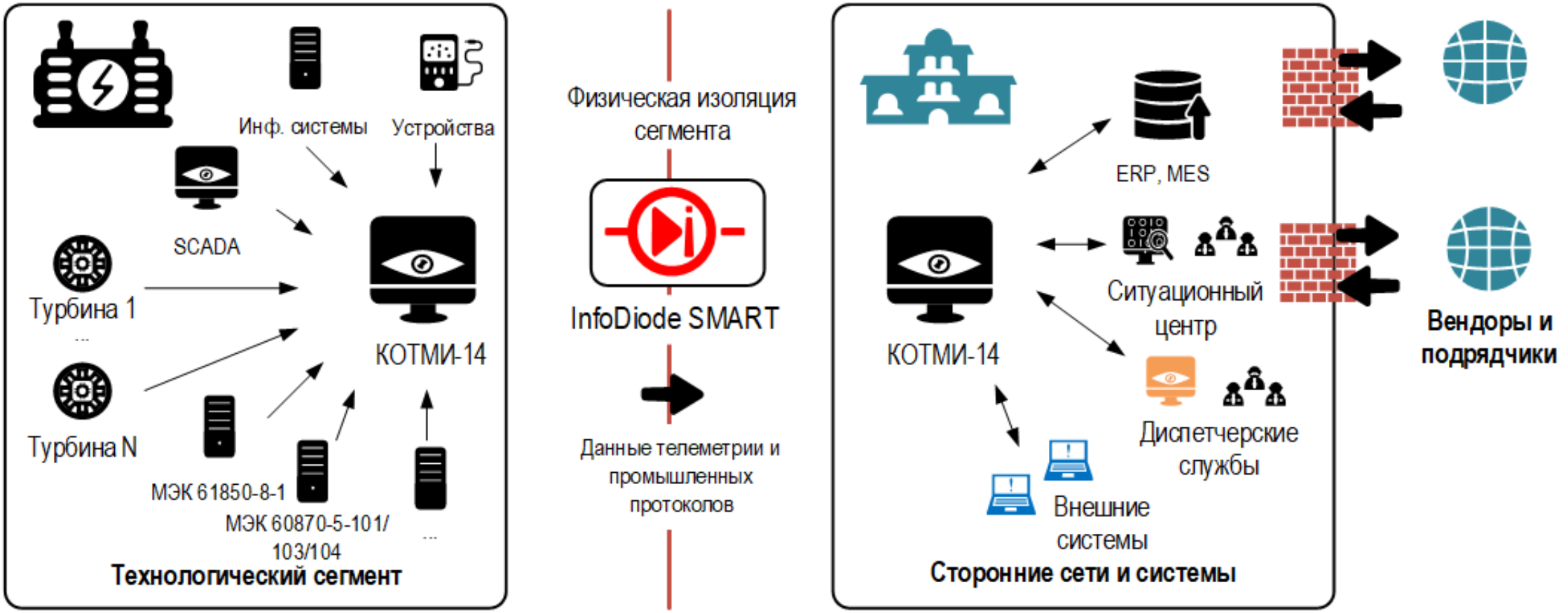
MasterSCADA – программная платформа для создания АСУ ТП, MES, решения задач учета, автоматизации и диспетчеризации объектов промышленности, ЖКХ, энергетики и автоматизации зданий.



InfoDiode.ru

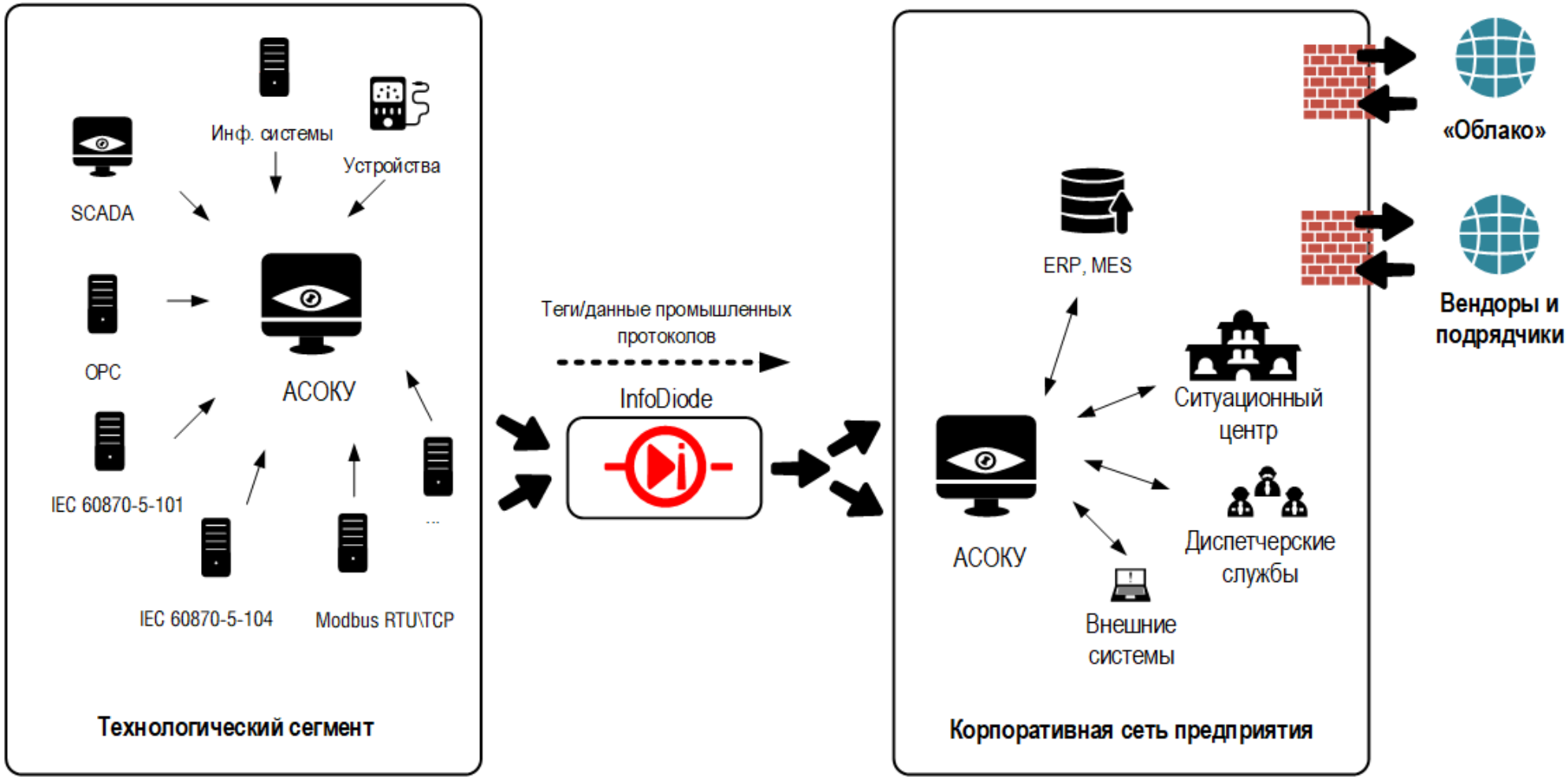
Передача данных АСУ ТП в корпоративную сеть (SCADA-SCADA) на примере ГЭС

КОТМИ-14 - программное обеспечение, предназначенное для создания диспетчерских информационно-управляющих систем



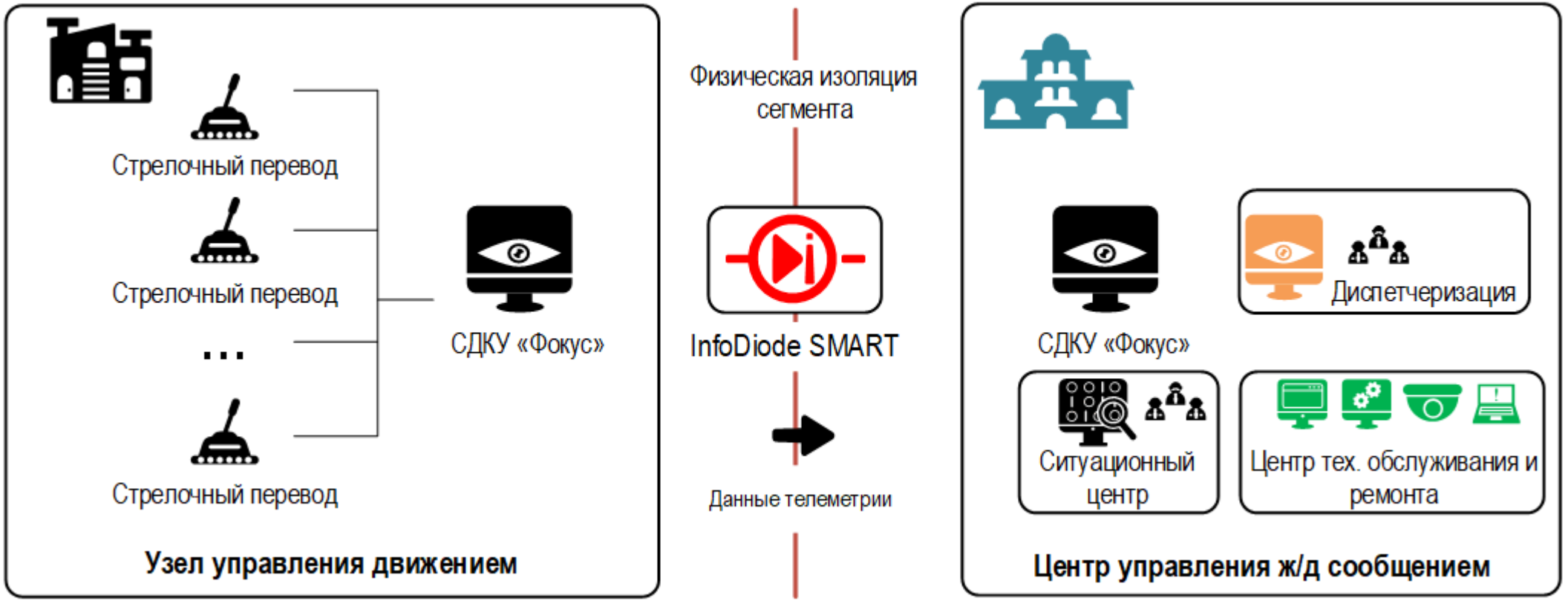
Агрегация данных АСУ ТП (SCADA-SCADA)

АСОКУ - автоматизированная система оперативного контроля и управления



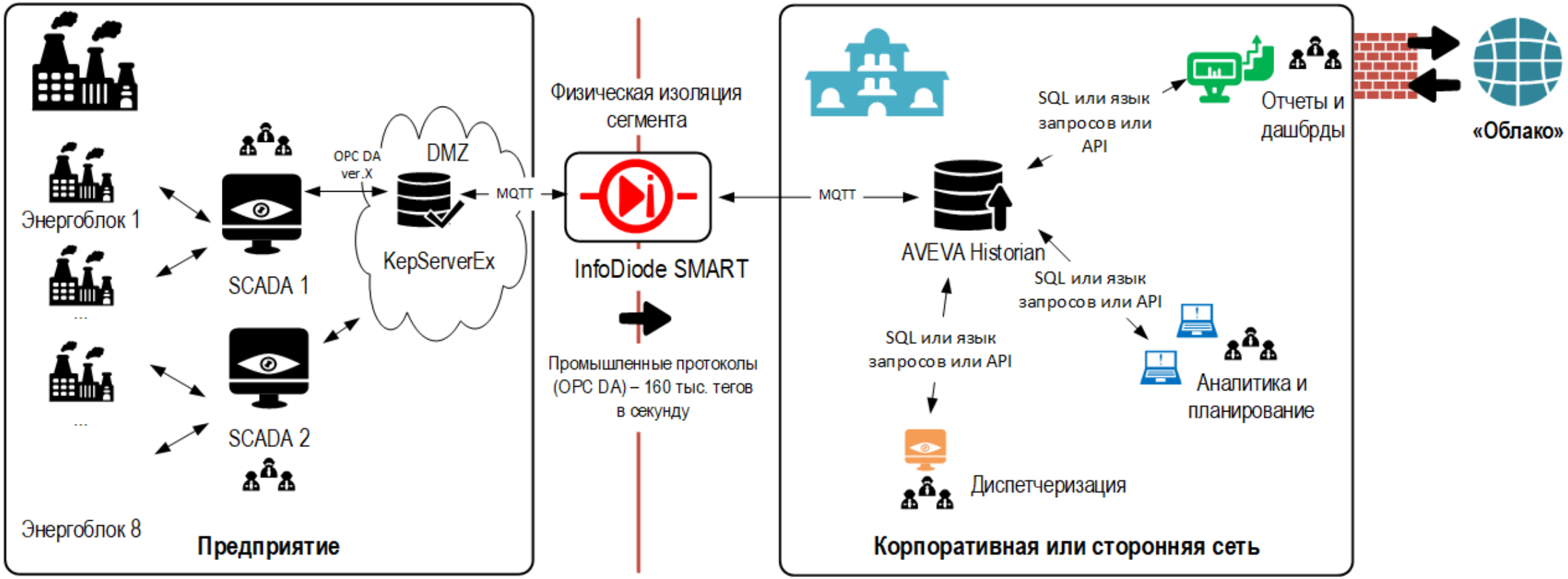
Агрегация данных АСУ ТП (SCADA-SCADA) на примере ж/д

СДКУ «Фокус» - отечественная система диспетчерского контроля и управления



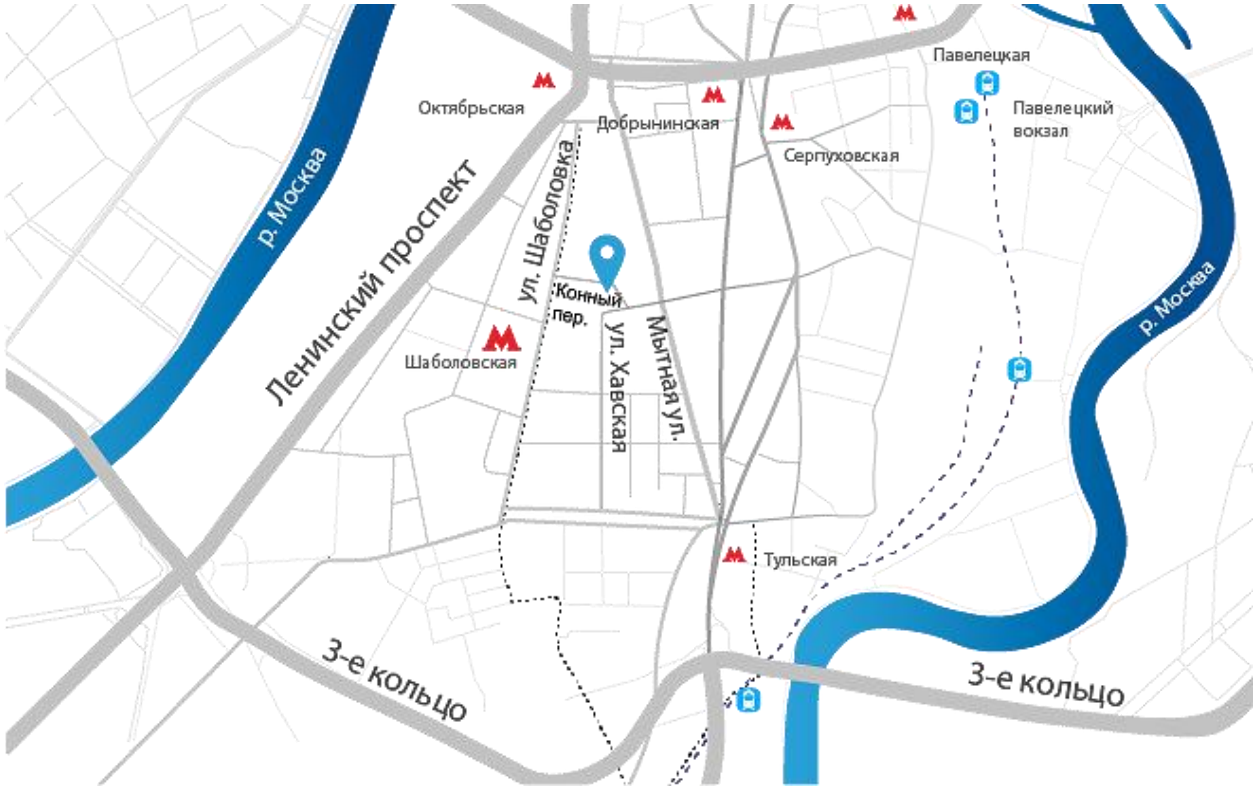
Передача данных АСУ ТП в корпоративную сеть (SCADA-Historian)

KEPServerEX + AVEVA Historian (ранее Wonderware Historian)



Как с нами связаться

- Адрес: 115162, Россия, Москва, ул. Шаболовка, д. 31, корп. Б, подъезд 3, этаж 2, вход с Конного переулка
- Телефон/Факс: +7 (495) 725-7660, +7 (495) 646-7560
- Факс: +7 (495) 725-7663
- E-mail: **InfoDiode@amt.ru**
- Сайт: **InfoDiode.ru**
- Техническая поддержка: **https://support.amt.ru**



СПАСИБО ЗА ВНИМАНИЕ!