



Однонаправленная
передача данных

-InfoDiode

Защита
объектов КИИ и ОПО

Экспорт
видеопотоков в
ситуационный
центр

Сегментирование
сетей АСУ ТП

КТ

10.02.2025

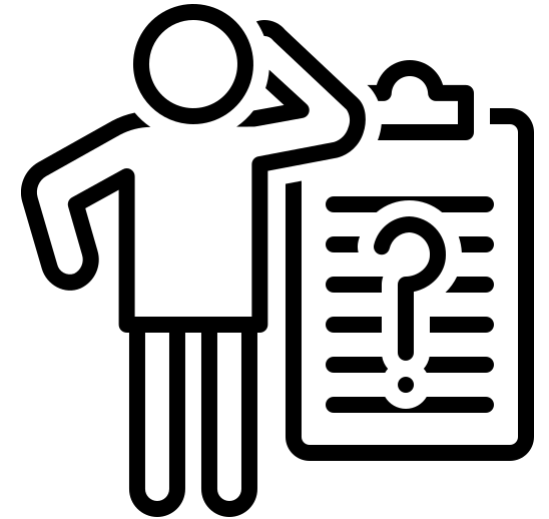
Решения с воздушным зазором InfoDiode в составе комплексных проектов по защите КИИ. Новые функции и решения.

Половинко Вячеслав, АМТ-ГРУП

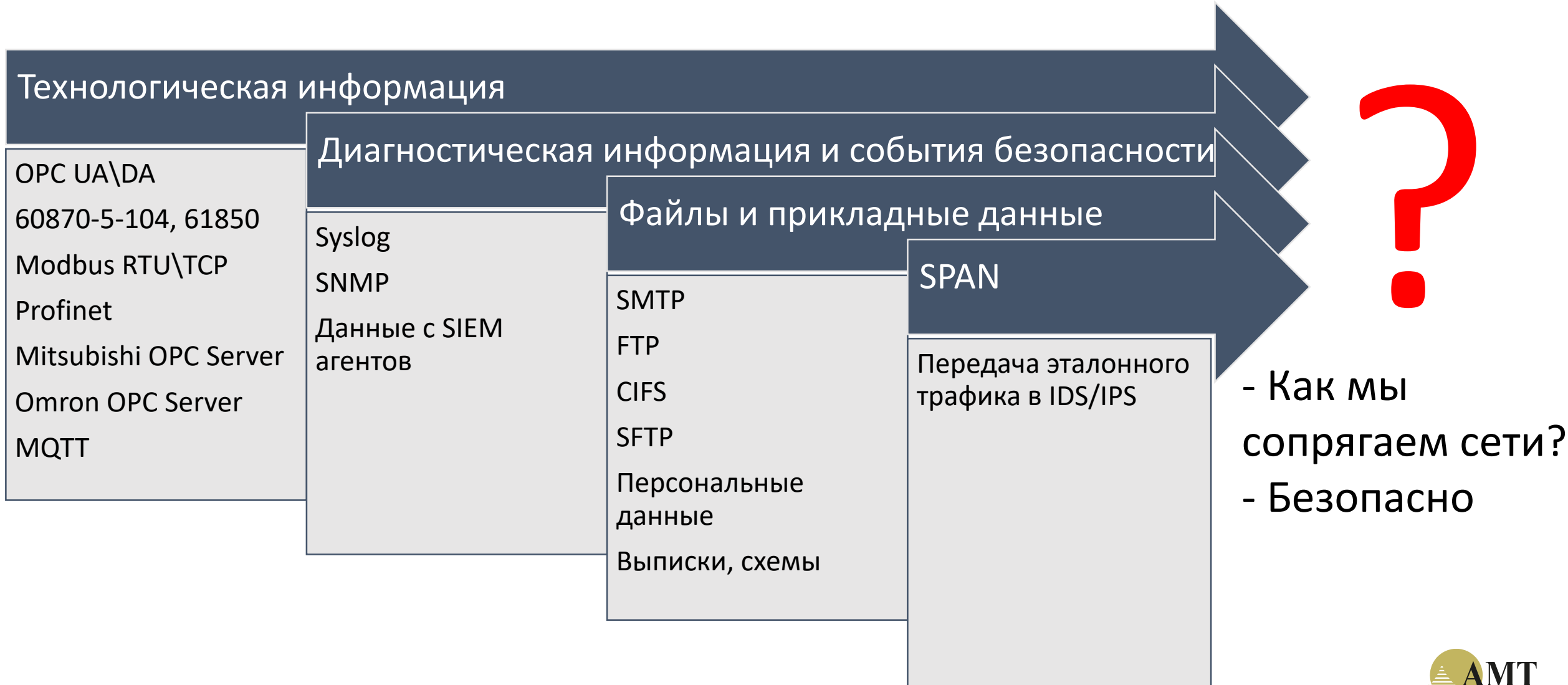


СОВРЕМЕННЫЕ ВЫЗОВЫ

1. Требования регулятора никуда не делись
2. Атаки перешли из разряда гипотетических в практическую плоскость
3. Нужны простые решения для защиты периметра
4. Объем передаваемых данных большой, а критериев разрешенного трафика немного
5. Внутренний нарушитель присутствует



Критическая и закрытая инфраструктура является **важным источником** данных для других систем



Комплексно решить две задачи:

- НЕ нарушать функционирование (доступность) самого объекта
- Обеспечить должный уровень конфиденциальности данных в источнике



Изоляция с помощью InfoDiode – один из ключевых аспектов **безопасной** передачи данных

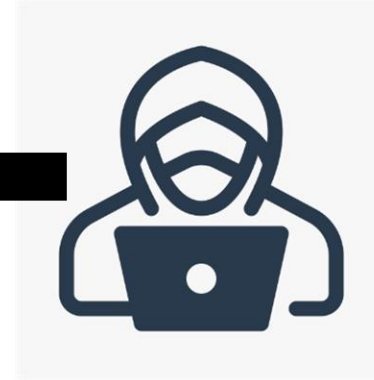
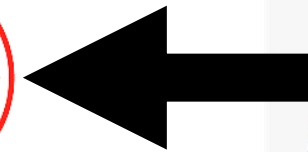
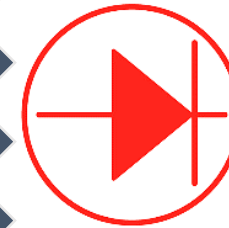
Технологическая информация

Диагностическая информация и события безопасности

Файлы и прикладные данные

SPAN

- Объекты удалены
- Объекты критичны
- Объекты автономны
- Объекты хранят значимые данные
- Объекты ограничено защищены от удаленного вектора атак
- Объекты являются частью централизованной системы контроля



Как мы
сопрягаем сети

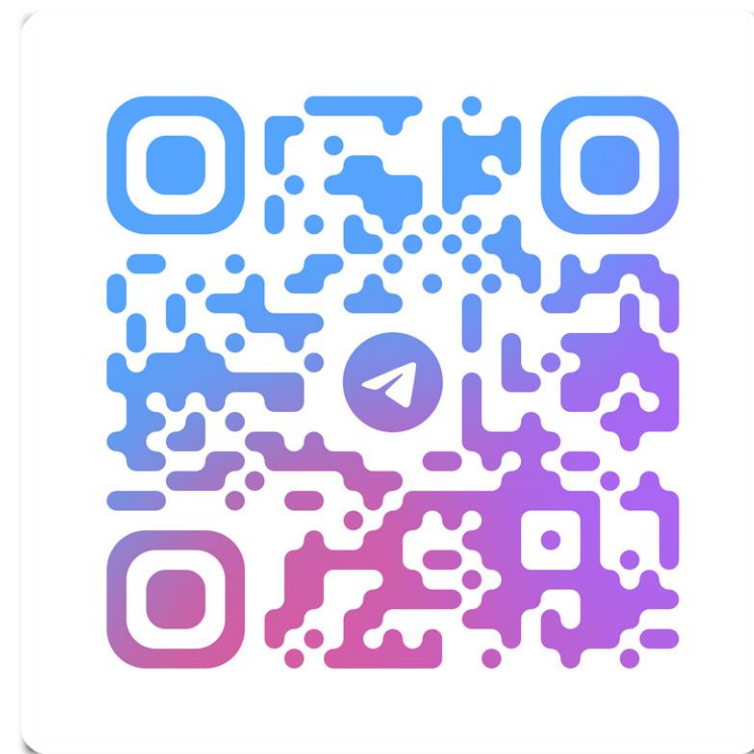
Почему именно InfoDiode? InfoDiode функционирует на физическом уровне

- **Однонаправленный шлюз (InfoDiode)** – устройство, которое передает информацию (**сигнал**) в одном направлении, то есть, не передает **физический сигнал** обратно
 - Однонаправленность передачи гарантируется **физическими (аппаратными)** решениями





<https://infodiode.ru/>

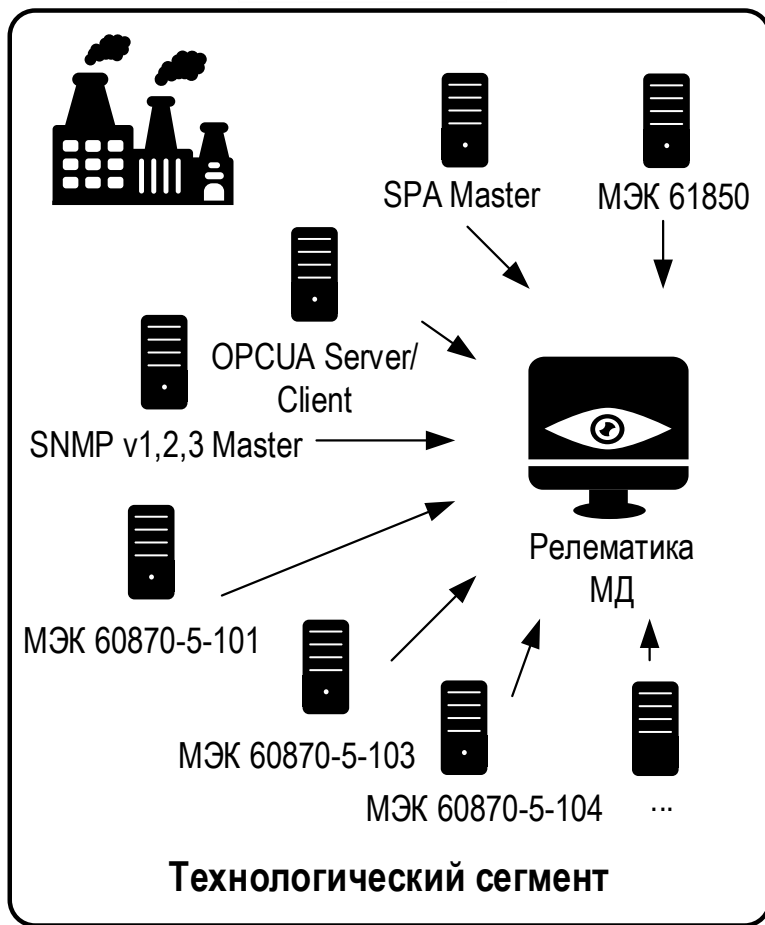


Telegram-канал InfoDiode



ЧТО НОВОГО

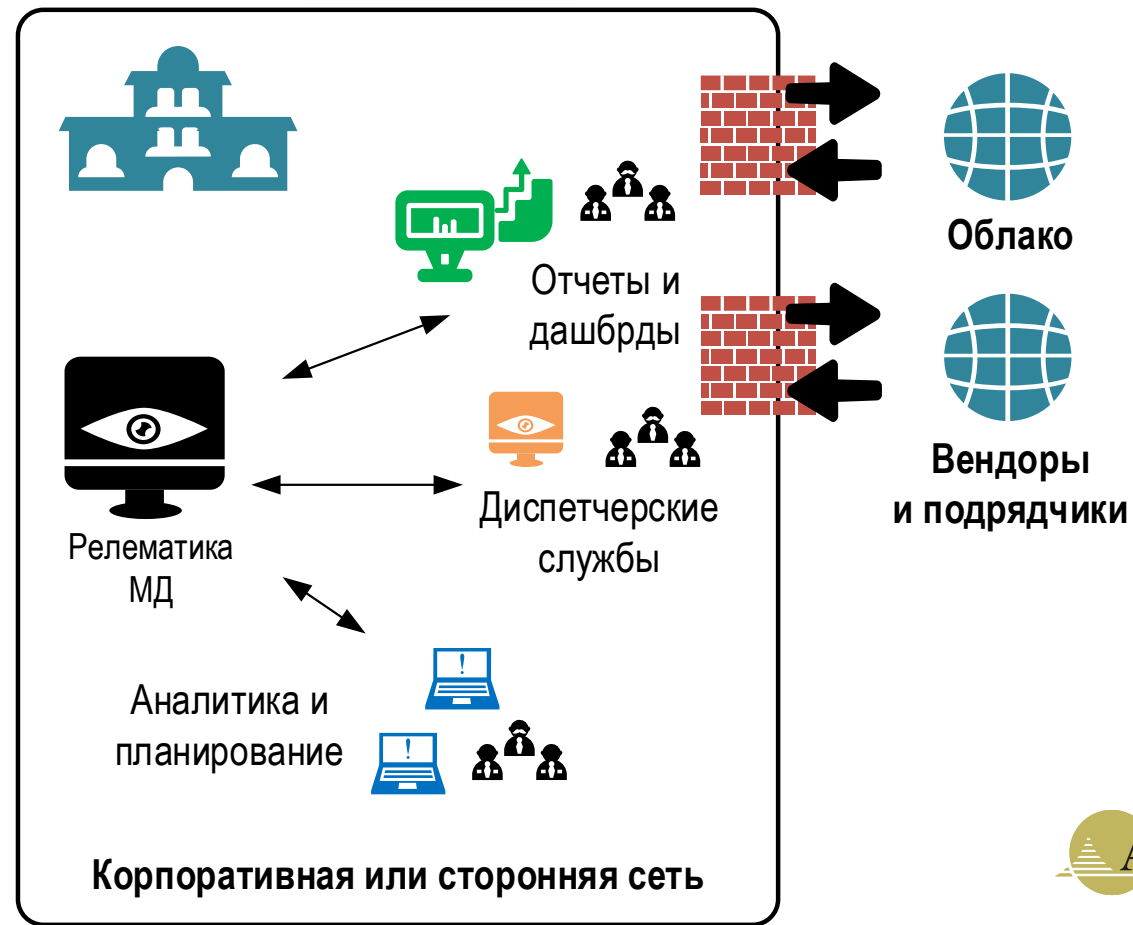
Решения для объектов энергетики – Релематика (передача данных в ЦУС)



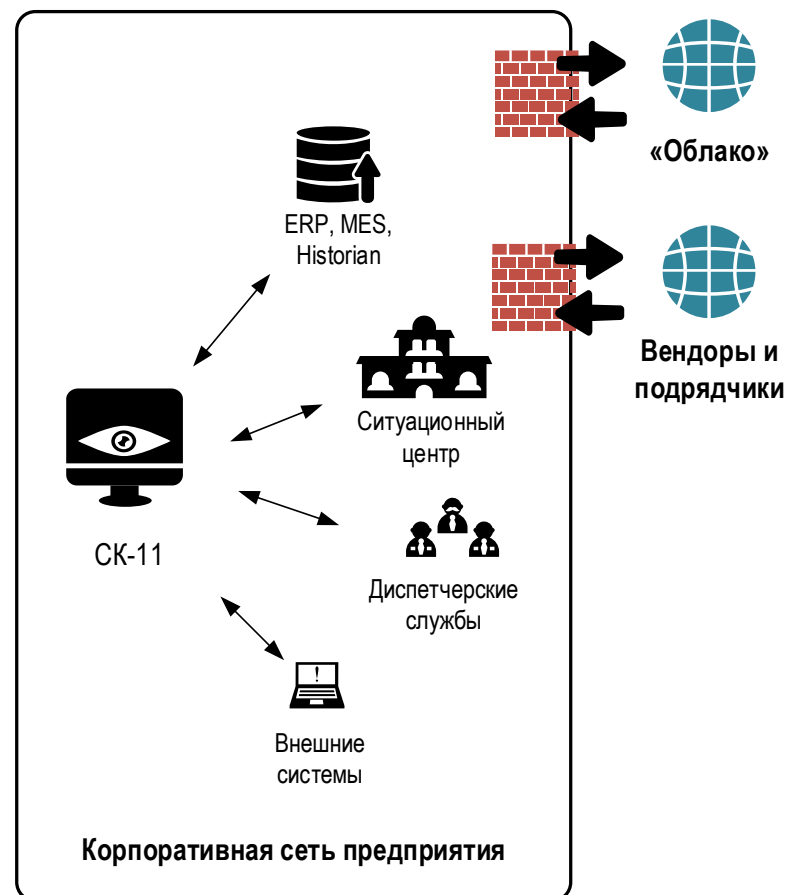
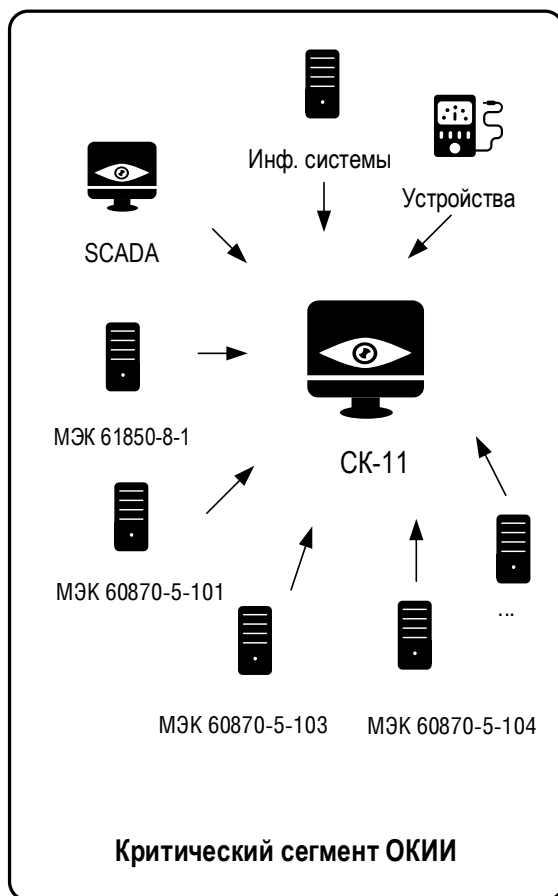
Физическая изоляция
сегмента



АПК InfoDiode SMART



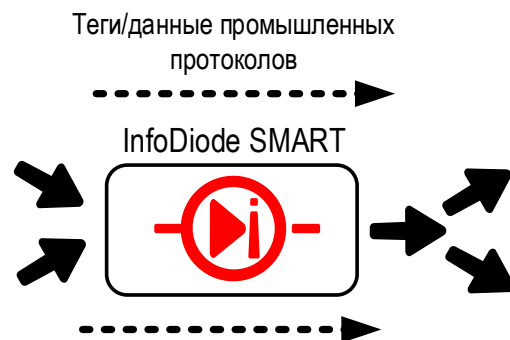
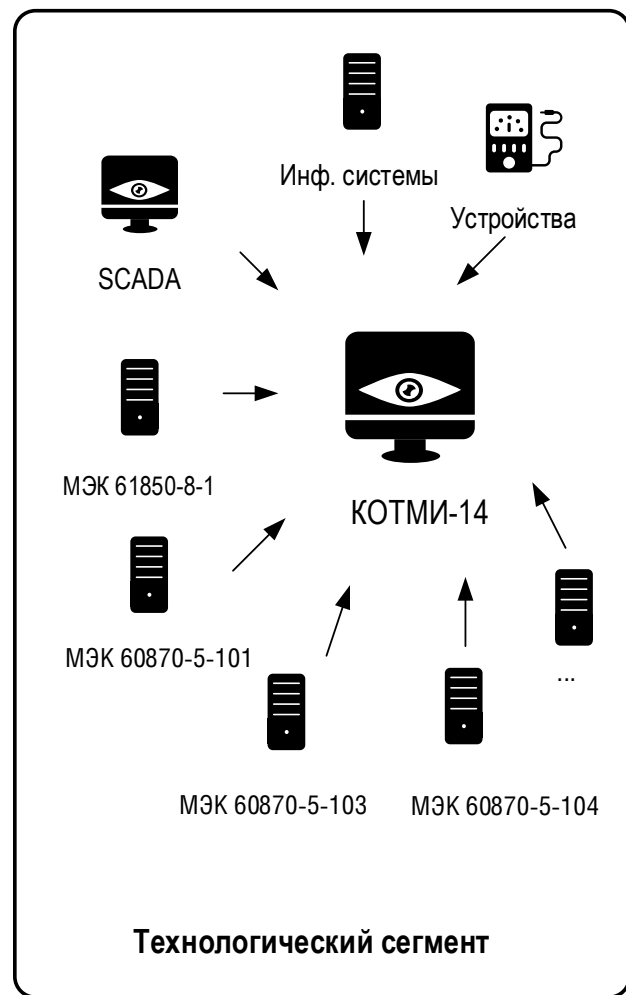
Решения для объектов энергетики – InfoDiode и СК-11 Монитор-электрик (передача данных в ЦУС)



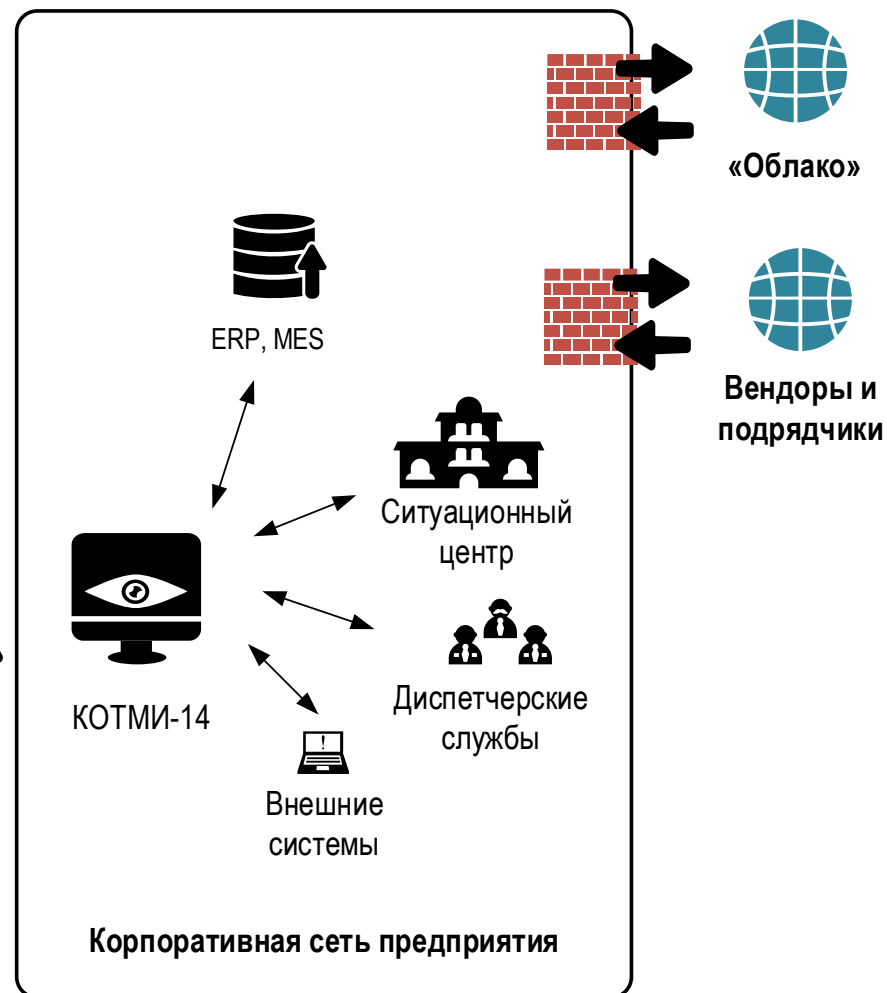
Решения для объектов энергетики – InfoDiode и КОТМИ-14 (передача данных в ЦУС и САЦ)



ЭФФЕКТИВНЫЕ ТЕХНОЛОГИИ УПРАВЛЕНИЯ

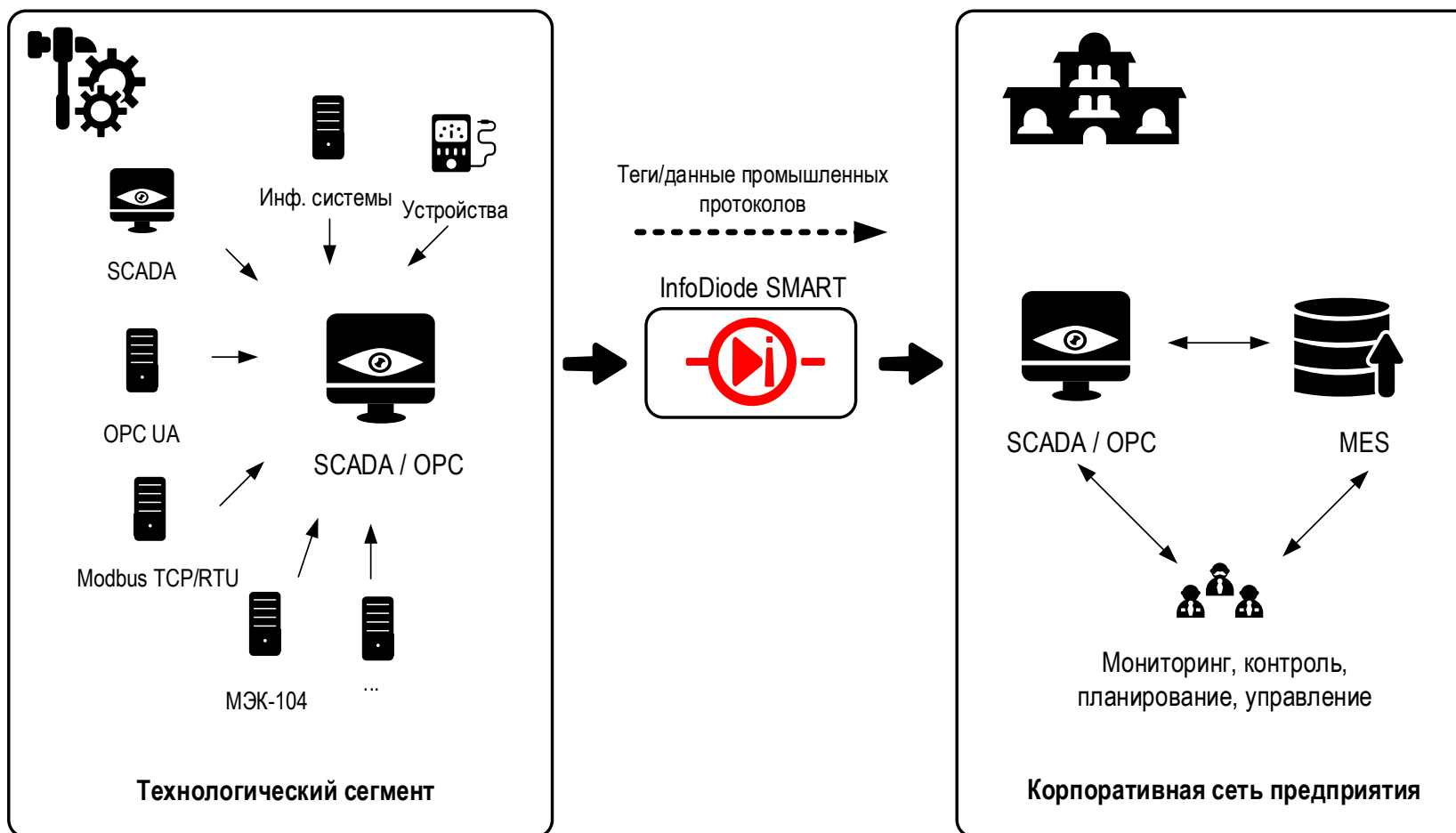


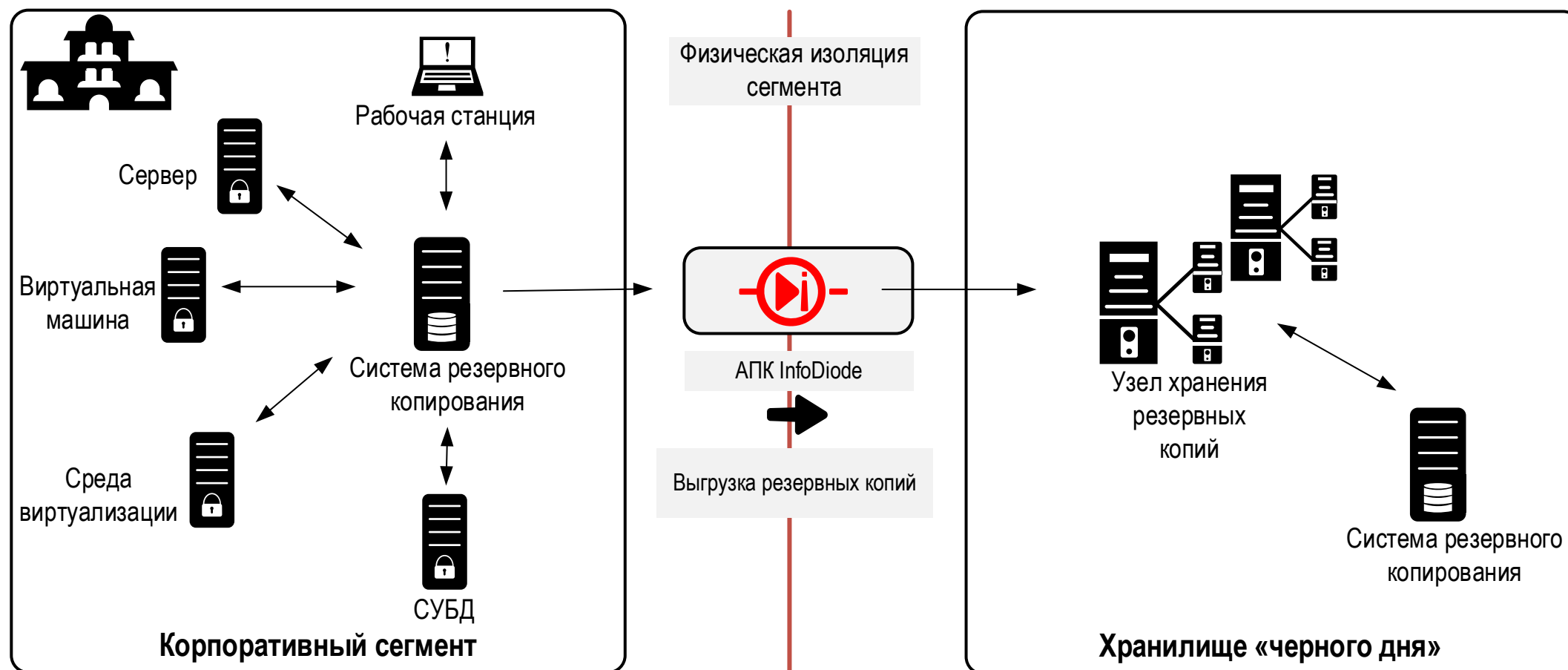
ЭФФЕКТИВНЫЕ ТЕХНОЛОГИИ УПРАВЛЕНИЯ



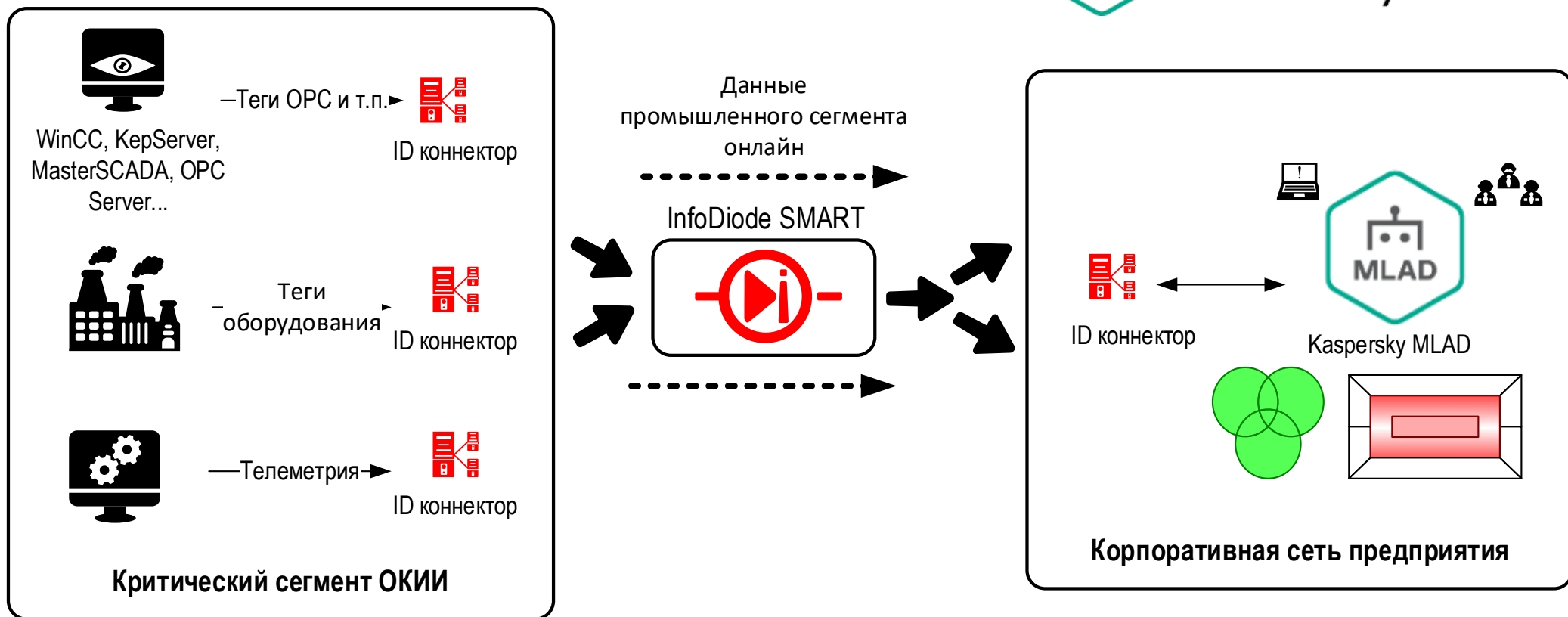
Решения для MES и Historian – InfoDiode и Indusoft (внедрение MES в условиях изоляции АСУ ТП сегмента)

MasterSCADA

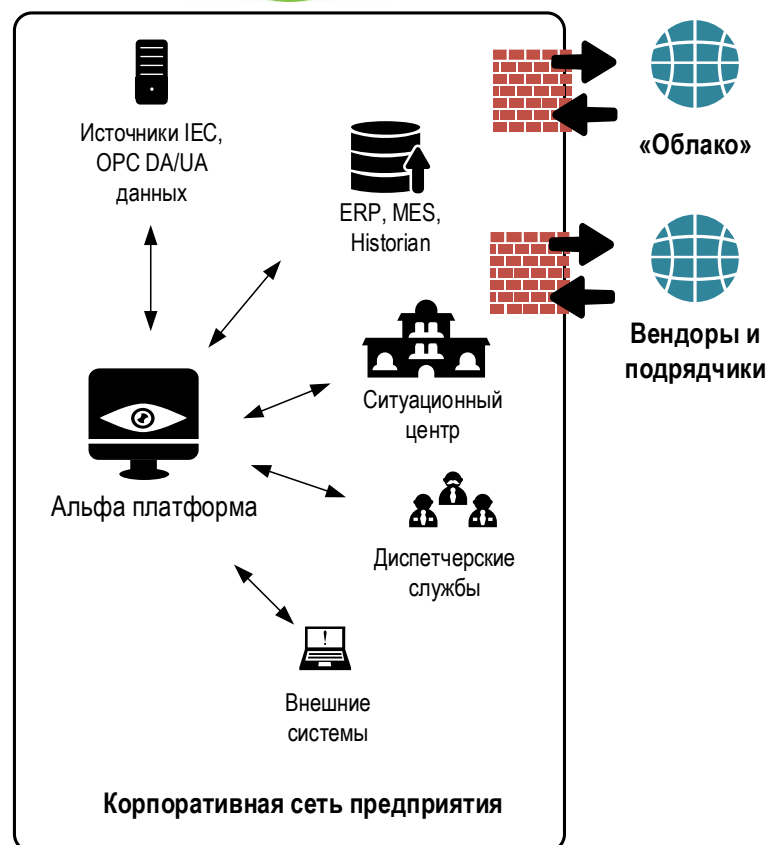
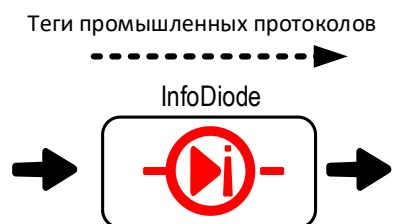
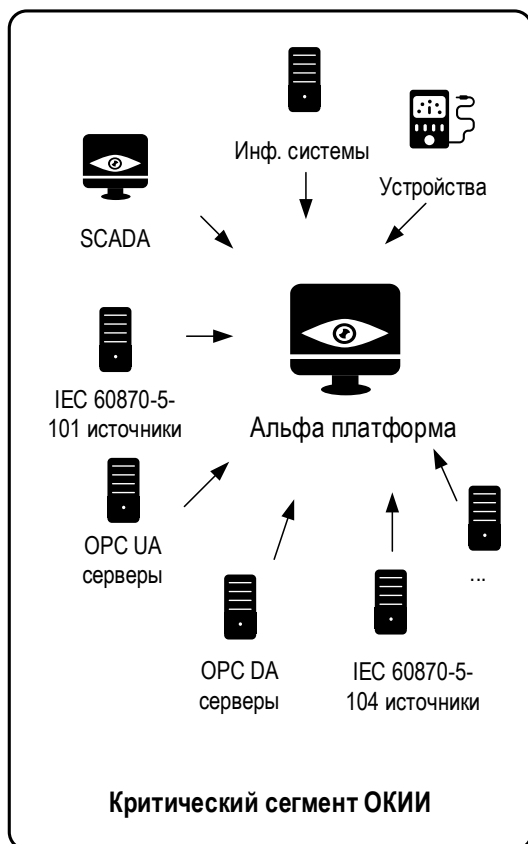




Решения класса Machine Learning – InfoDiode и Kaspersky MLAD (сбор данных из АСУ ТП для поиска аномалий и предиктивной аналитики)

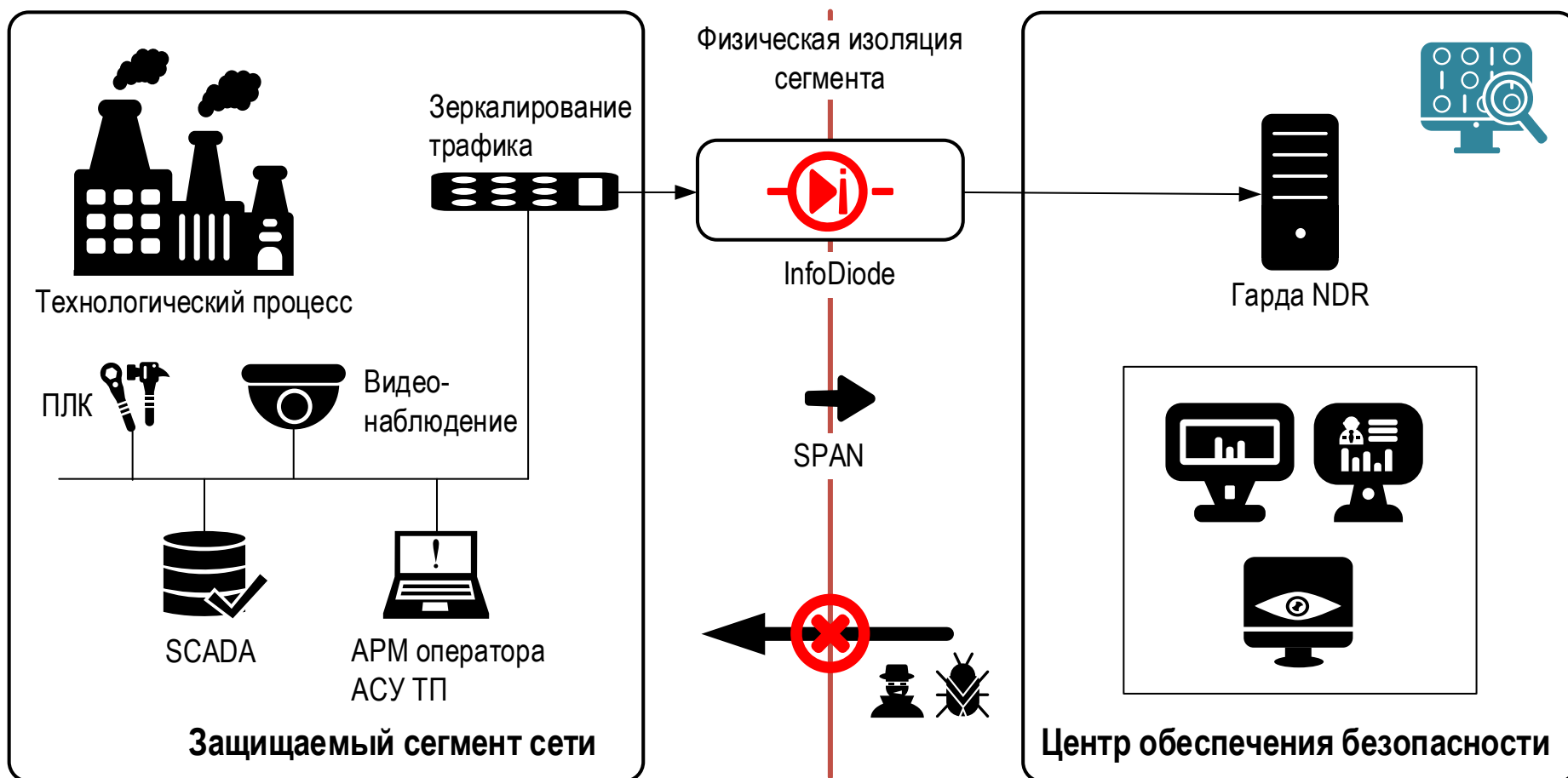


Решения для сбора данных из АСУ ТП – Альфа Платформа (сбор данных с самых разных источников АСУ ТП)



Решения класса NDR и Deception– InfoDiode и Гарда (имитация инфраструктуры, обнаружение аномалий в рамках COB)

ГАРДА





ЧТО ДАЛЬШЕ

Междоменные решения InfoDiode - интегрированный комплекс решений по обеспечению безопасности

Комплекс, как правило, состоит из специализированного программного, и, в ряде случаев, аппаратного обеспечения с интерфейсами для ручного или автоматического предоставления и/или ограничения доступа к информации разных категорий значимости, а также интерфейсов для организации передачи такой информации



«Диоды данных» эволюционируют, как и вся экосистема СЗИ

Аппаратные «диоды»

- Недорого
- Решают базовые задачи изоляции, применяются, в основном, в COB/IDS
- Plug&Play, не требуют сопровождения службы эксплуатации
- Не передают данные двунаправленных протоколов



Аппаратно-программные «диоды»

- Решают задачу передачи протоколов прикладного уровня, в том числе промышленных протоколов, передают несколько видов трафика одновременно
- Доп функции СЗИ (NAT, white list/порты, контроль изменений конфигурации, контроль доступа, ввод в домен)
- Возможности по контролю за функционированием: SNMP, Syslog, NTP...



Междоменные решения

- Регламентируют обмен и дополняют «традиционные диоды» функциями и решениями по контролю прикладного трафика
- Более комплексный подход к защите периметра организации
- Интегрируются с другими СЗИ в целях повышения эффективности контроля периметра

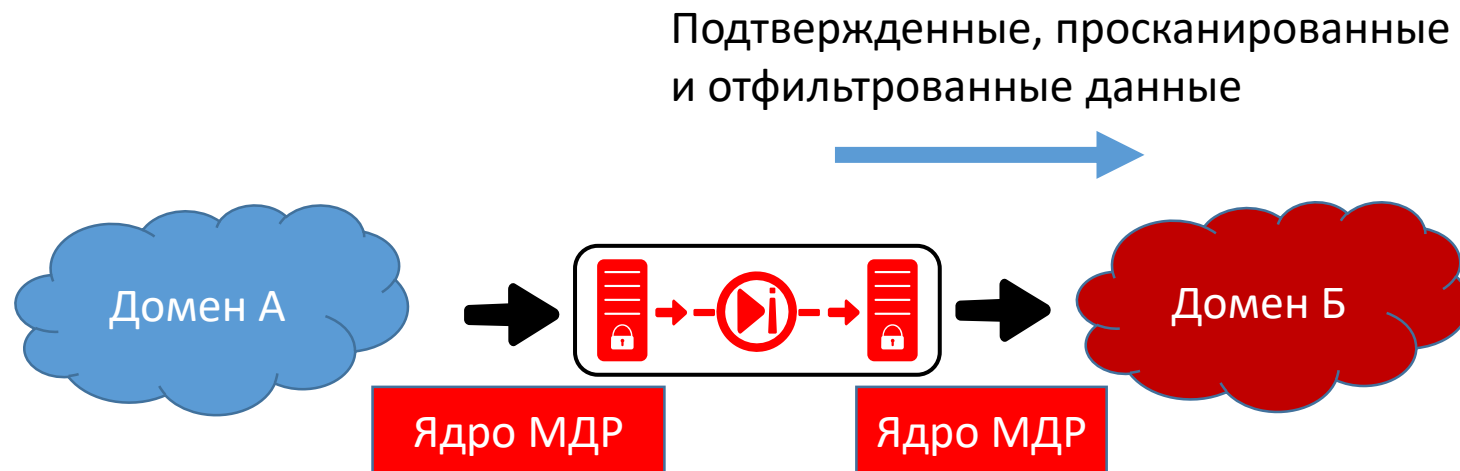


В основе обмена
всегда лежит принцип

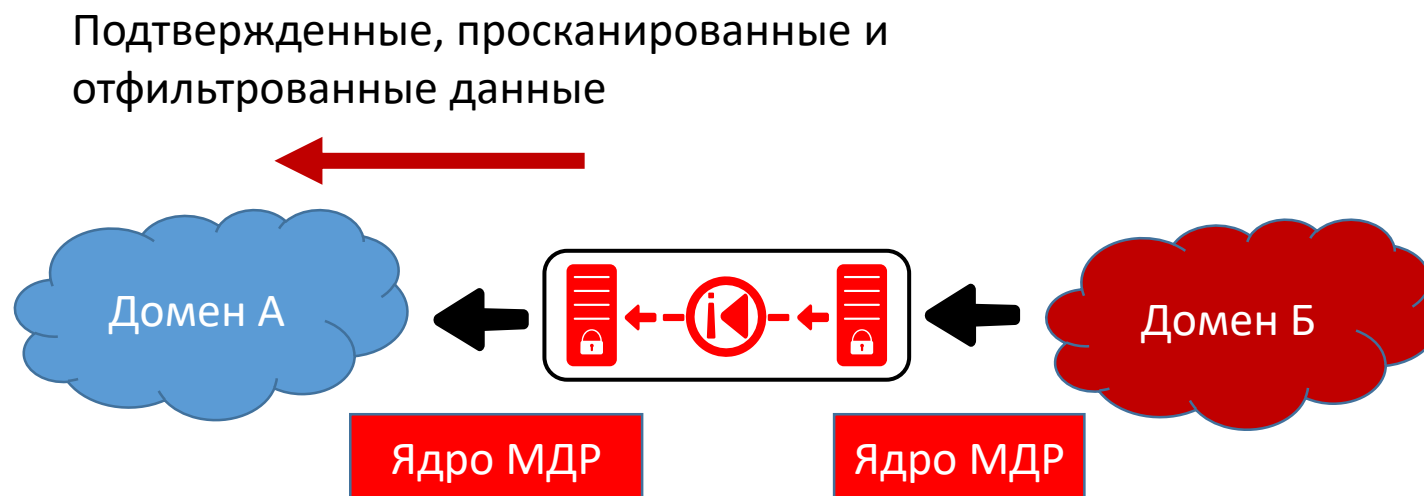
**физический сигнал
только в одну сторону**

Междоменные решения могут повышать уровень безопасности в разных сценариях применения

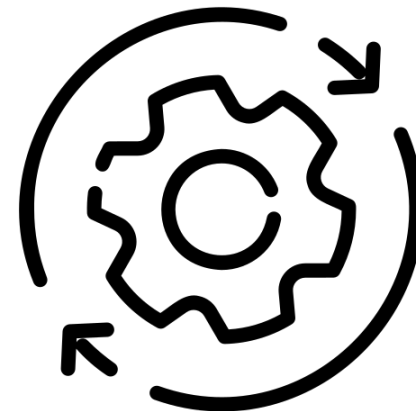
Сценарий 1



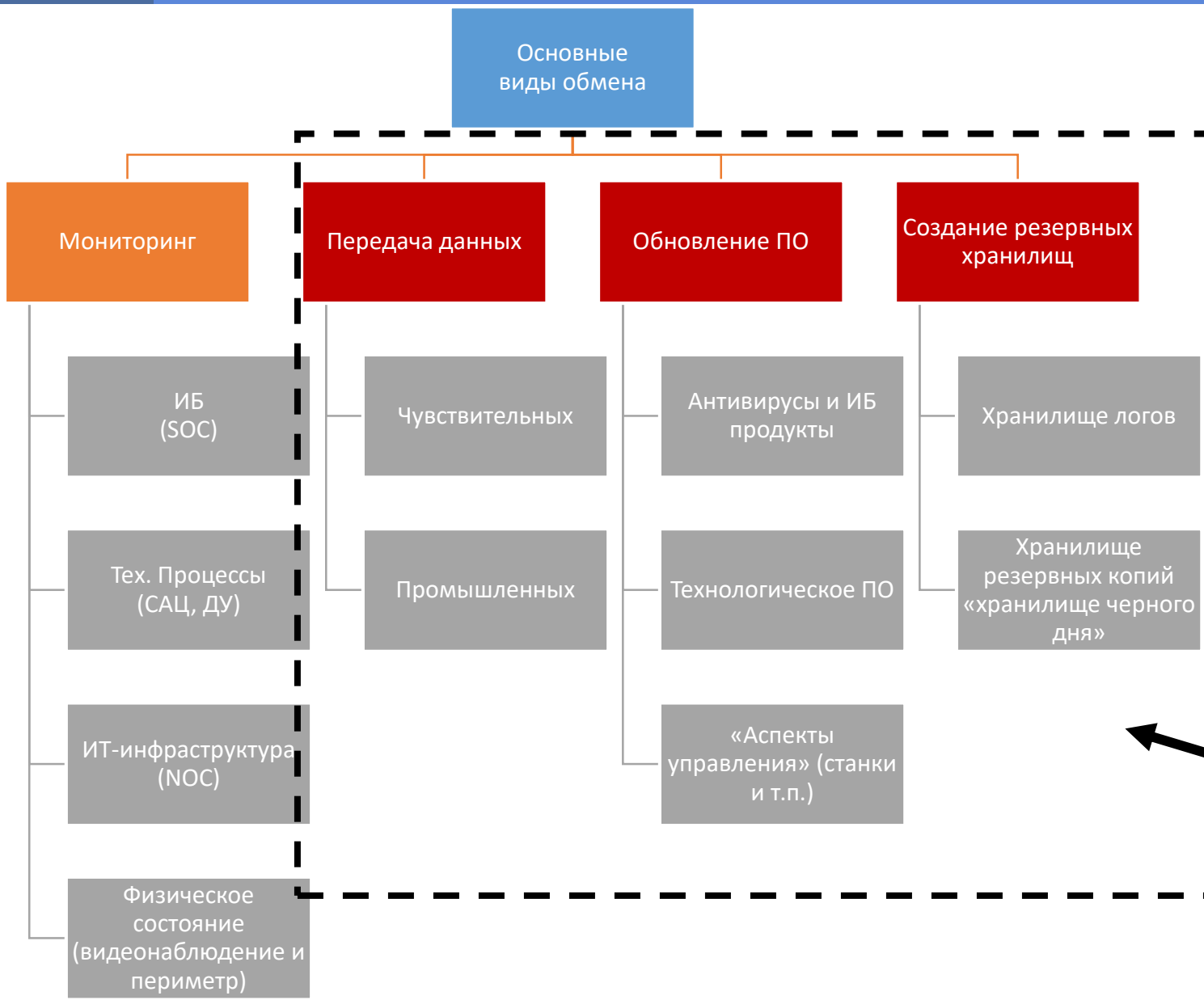
Сценарий 2



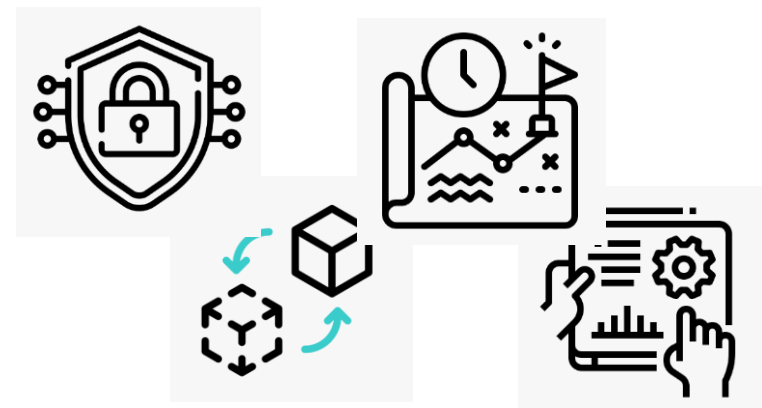
- **Отдельный интерфейс между ядром МДР и каждым из подключенных доменов безопасности**
 - для приема данных от прошедших проверку подлинности и авторизованных пользователей и/или исходных систем
- **Соблюдение политик безопасности для передачи данных между доменами безопасности**
 - блокирование всего трафика между доменами по умолчанию и обеспечение соблюдения путей, по которым данные могут передаваться через МДР.
 - Использование InfoDiode и средств фильтрации, нормализации, преобразования, санитарной обработки трафика для устранения вредоносного содержимого и/или предотвращения потери конфиденциальных данных
- **Представление отфильтрованных данных в удобной форме**
 - для утверждения целевым системами и/или пользователями с сохранением разделения доменов безопасности
- **Защита МДР**
 - обеспечение функций для управления, поддержание защищенного, проверяемого и исправного состояния, позволяющего осуществлять мониторинг системы и оповещать о выявлении ошибок и инцидентов
- **Ведение аудита**
 - аудит безопасности механизмов контроля доступа к элементам системы, аудит безопасности каналов передачи данных, состояния системы и любых изменений в конфигурации



Междоменные решения фокусируются только на части обменов с воздушным зазором



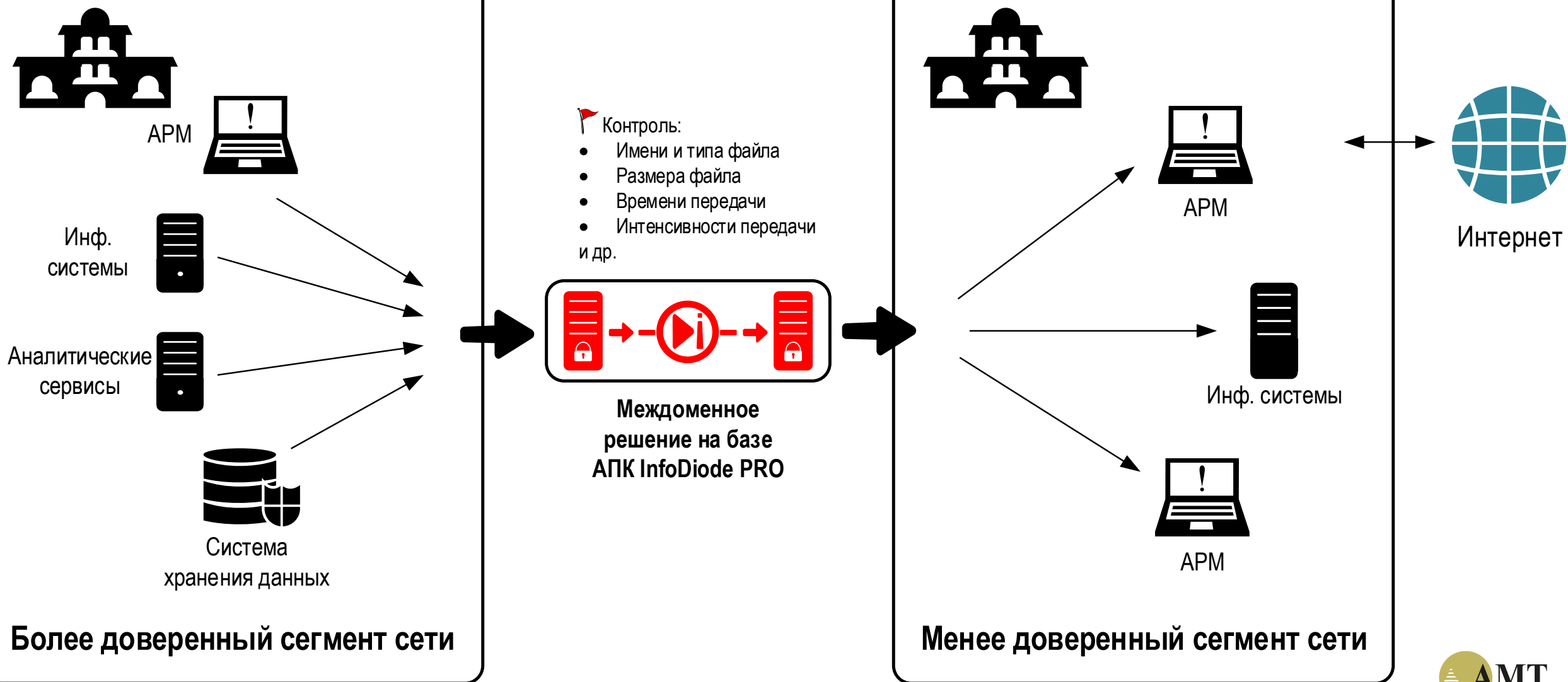
В указанных видах обменов **принципиально (!)** **исключено удаленное администрирование и управление защищаемыми объектами из менее доверенного сегмента**



На данном этапе междоменные решения развиваются преимущественно в этих направлениях

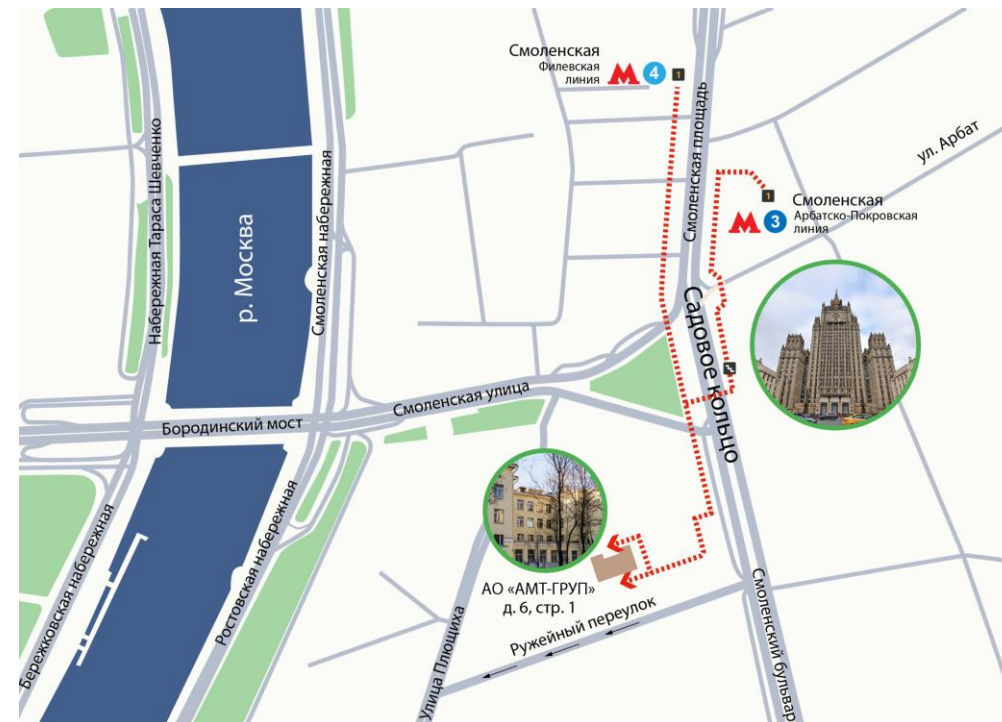
- ☐ **Повышение скорости канала передачи – до 10G**
- ☐ **Ограничения на файловые потоки
(тип, размер, интенсивность, регламент передачи)**
- ☐ **Статистика использования каналов передачи**
- ☐ **Интеграция с серверами ICAP
(DLP, антивирусы, «песочницы»)**
- ☐ **Интеграция с системами резервного копирования**







- Адрес: 119121, Россия, Москва, Ружейный переулок, 6с1
- 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!