24.07.2025

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

Половинко Вячеслав, АМТ-ГРУП

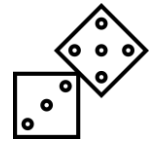
КТО НАШ НАРУШИТЕЛЬ?

Кто наш нарушитель?

Тип нарушителя	Случайно	С умыслом	Особенности нарушителя	Особенности атаки	Сложность защиты
Внутренний	Неплохо помогают стандартные СЗИ	Требуются высоко профессиональные команды и серьезные компенсирующие меры	Имеет идентификаторы (лицо, видео, носители, СКУД, паспорт) - оставляет хороший цифровой и физический след	Понятен объем - разные виды деструктивных воздействий (не только кибер-, но и реальный ущерб)	Помощь служб, сотрудников, граждан
Внешний	Неплохо помогают стандартные СЗИ	Требуются высоко профессиональные команды и серьезные компенсирующие меры	Максимально анонимен, значительные ресурсы	Только кибер ущерб	Помощь очень ограничена
Внешний с внутренним	Неплохо помогают стандартные СЗИ	Требуются высоко профессиональные команды и серьезные компенсирующие меры	"+"	"+"	"+"

Какие компетенции нашего нарушителя?

- **Обладают базовыми возможностями по реализации угроз**
  Реализовывают только известные угрозы, направленные на известные уязвимости с использованием общедоступных инструментов.
  - Авторизованные пользователи, бывшие работники, хакеры, поставщики ПО, АПК, обеспечивающих систем, обеспечивающий персонал (администрация, охрана, уборщики и т.д.).
- **Обладают базовыми повышенными возможностями по реализации угроз**
  Реализовывают угрозы, в том числе направленные на неизвестные уязвимости с использованием специально созданных для этого инструментов или свободно распространяемых в сети «Интернет», и не имеют возможностей реализации угроз на физически изолированные сегменты систем и сетей.
  - Системные администраторы и администраторы ИБ, лица, привлекаемые для установки, настройки, испытаний, ПНР, поставщики вычислительных услуг и услуг связи, конкурирующие организации, преступные группы.
- **Обладают средними возможностями по реализации угроз**
  Реализовывают угрозы, в том числе на выявленные ими неизвестные уязвимости с использованием самостоятельно разработанных для этого инструментов, но не имеют возможностей реализации угроз на физически изолированные сегменты систем и сетей.
  - Разработчики ПО и АПК, террористические или экстремистские группировки.
- **Обладают высокими возможностями по реализации угроз**
  Имеют практически неограниченные возможности по реализации угроз, в том числе с использованием недекларированных возможностей и программных и программно-аппаратных закладок, встроенных в компоненты систем и сетей.
  - Специальные службы иностранных государств.



Случайно

Умысел

AMT GROUP

Кто наш целевой нарушитель?

Тип нарушителя	Случайно	С умыслом	Особенности нарушителя	Особенности атаки	Сложность защиты
Внутренний	Неплохо помогают стандартные СЗИ	Требуются высоко профессиональные команды и серьезные компенсирующие меры	Имеет идентификаторы (лицо, видео, носители, СКУД, паспорт) - оставляет хороший цифровой и физический след	Понятен объем - разные виды деструктивных воздействий (не только кибер-, но и реальный ущерб)	Помощь служб, сотрудников, граждан
Внешний	Неплохо помогают стандартные СЗИ	Требуются высоко профессиональные команды и серьезные компенсирующие меры	Максимально анонимен, значительные ресурсы	Только кибер ущерб	Помощь очень ограничена
Внешний с внутренним	Неплохо помогают стандартные СЗИ	Требуются высоко профессиональные команды и серьезные компенсирующие меры	"+"	"+"	"+"

Как мы защищаемся?

Тип нарушителя	Случайно	С умыслом	Особенности нарушителя	Особенности атаки	Сложность защиты
Внутренний	Неплохо помогают стандартные СЗИ	Требуются высоко профессиональные команды и серьезные компенсирующие меры	Имеет идентификаторы (лицо, видео, носители, СКУД, паспорт) - оставляет хороший цифровой и физический след	Понятен объем - разные виды деструктивных воздействий (не только кибер-, но и реальный ущерб)	Помощь служб, сотрудников, граждан
Внешний	Неплохо помогают стандартные СЗИ	Требуются высоко профессиональные команды и серьезные компенсирующие меры	Максимально анонимен, значительные ресурсы	Только кибер ущерб	Помощь очень ограничена
Внешний с внутренним	Неплохо помогают стандартные СЗИ	Требуются высоко профессиональные команды и серьезные компенсирующие меры	"+"	"+"	"+"

Модель защиты с помощью InfoDiode

Тип нарушителя	Случайно	С умыслом	Особенности нарушителя	Особенности атаки	Сложность защиты
Внутренний	Неплохо помогают стандартные СЗИ	Требуются высоко профессиональные команды и серьезные компенсирующие меры	Имеет идентификаторы (лицо, видео, носители, СКУД, паспорт) - оставляет хороший цифровой и физический след	Понятен объем - разные виды деструктивных воздействий (не только кибер-, но и реальный ущерб)	Помощь служб, сотрудников, граждан
Внешний	Неплохо помогают стандартные СЗИ	Требуются высоко профессиональные команды и серьезные компенсирующие меры	Максимально анонимен, значительные ресурсы	Только кибер ущерб	Помощь очень ограничена
Внешний с внутренним	Неплохо помогают стандартные СЗИ	Требуются высоко профессиональные команды и серьезные компенсирующие меры	"+"	"+"	"+"

Модель защиты с помощью InfoDiode смещается на целевые группы нарушителей

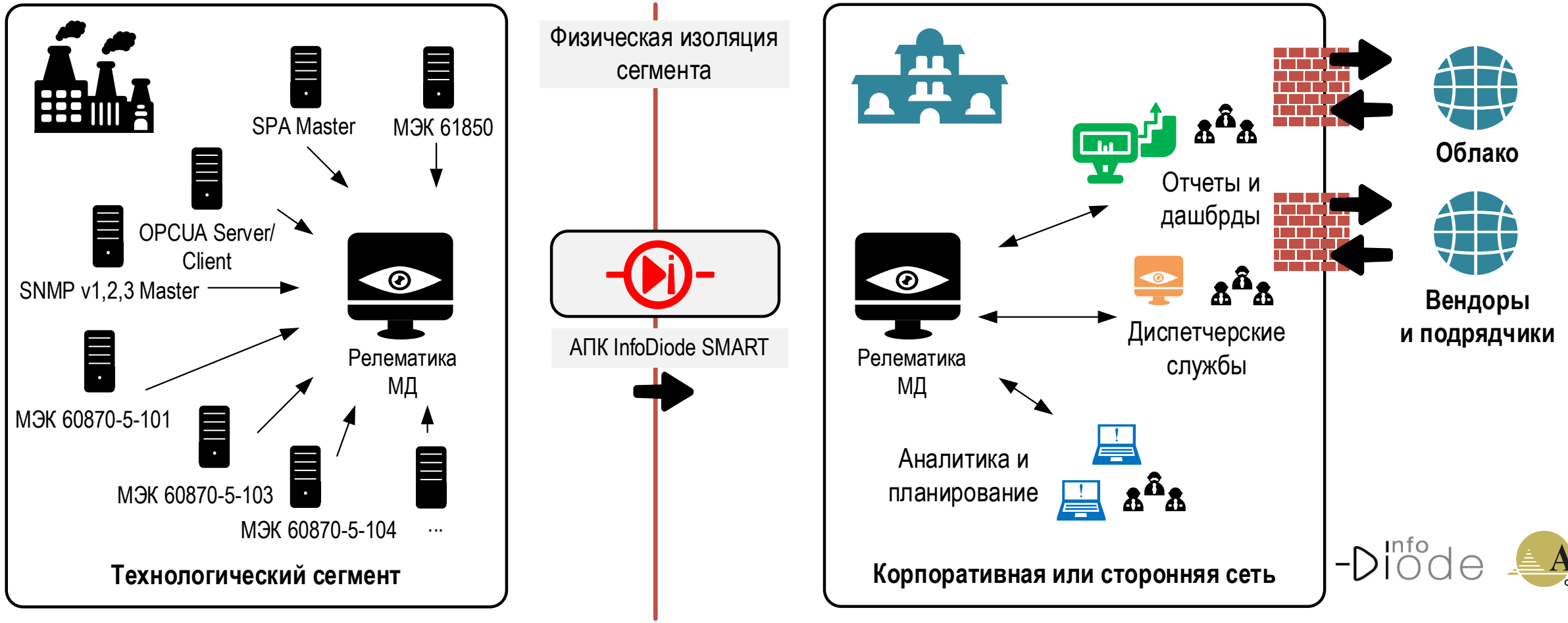
Тип нарушителя	Случайно	С умыслом	Особенности нарушителя	Особенности атаки	Сложность защиты
Внутренний	Неплохо помогают стандартные СЗИ	Требуются высоко профессиональные команды и серьезные компенсирующие меры	Имеет идентификаторы (лицо, видео, носители, СКУД, паспорт) - оставляет хороший цифровой и физический след	Понятен объем - разные виды деструктивных воздействий (не только кибер-, но и реальный ущерб)	Помощь служб, сотрудников, граждан
Внешний	Неплохо помогают стандартные СЗИ	Требуются высоко профессиональные команды и серьезные компенсирующие меры	Максимально анонимен, значительные ресурсы	Только кибер ущерб	Помощь очень ограничена
Внешний с внутренним	Неплохо помогают стандартные СЗИ	Требуются высоко профессиональные команды и серьезные компенсирующие меры	"+"	"+"	"+"

Преимущества локализации нарушителя с помощью InfoDiode

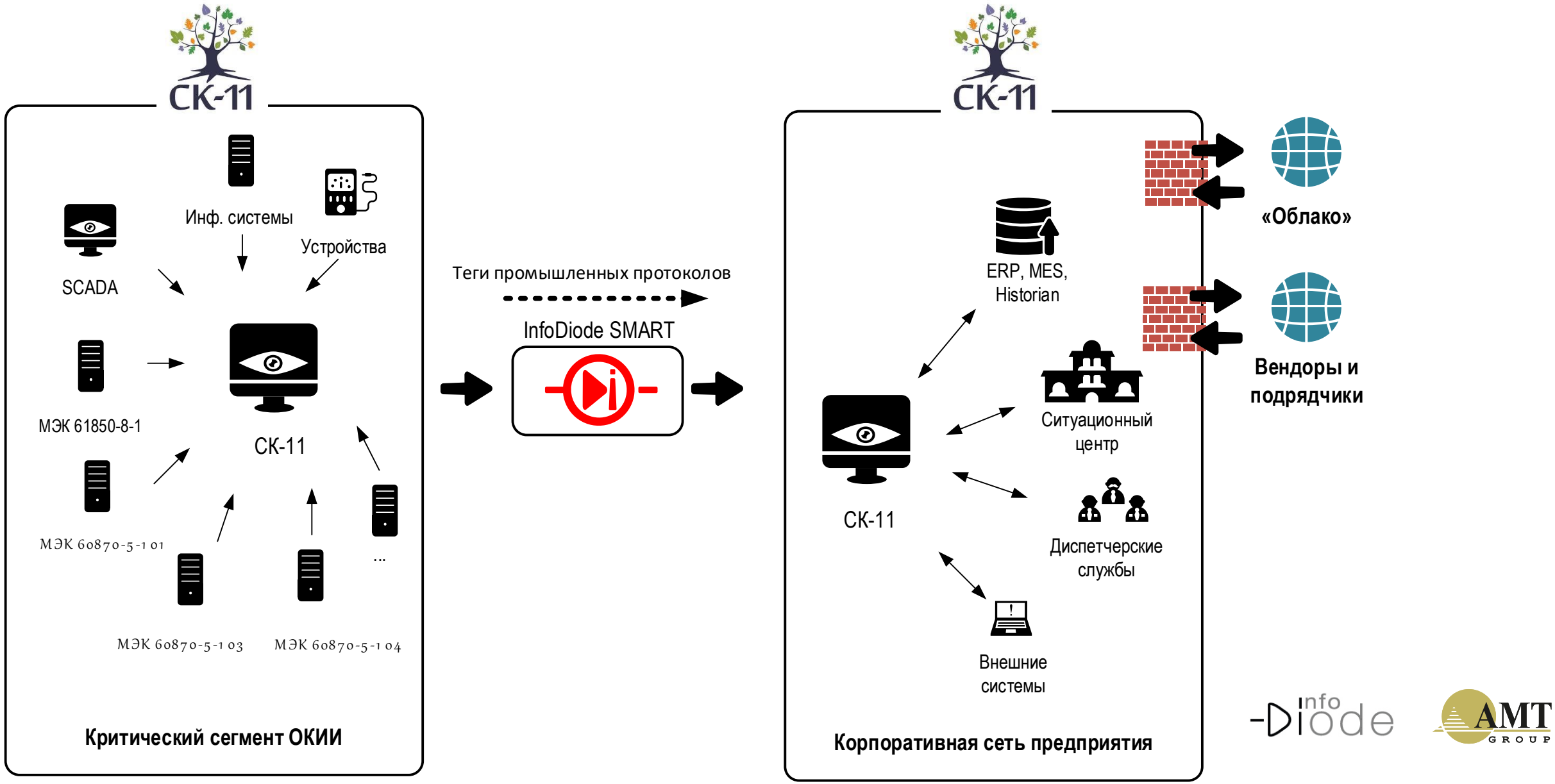
- **Полностью исключить внешнего злоумышленника с удаленным вектором атаки**
- **Сфокусироваться на мерах в отношении внутреннего нарушителя и эффективнее расследовать инциденты**
- **Сэкономить средства (и Capex и Opex)**
- **Максимально усложнить жизнь внутреннему нарушителю в части успешности кибератак, связанных с удаленным управлением, выводом данных**
- **Буквально и точно выполнить требования по сегментации сети ТСПД, КСПД**

ГОТОВЫЕ РЕШЕНИЯ

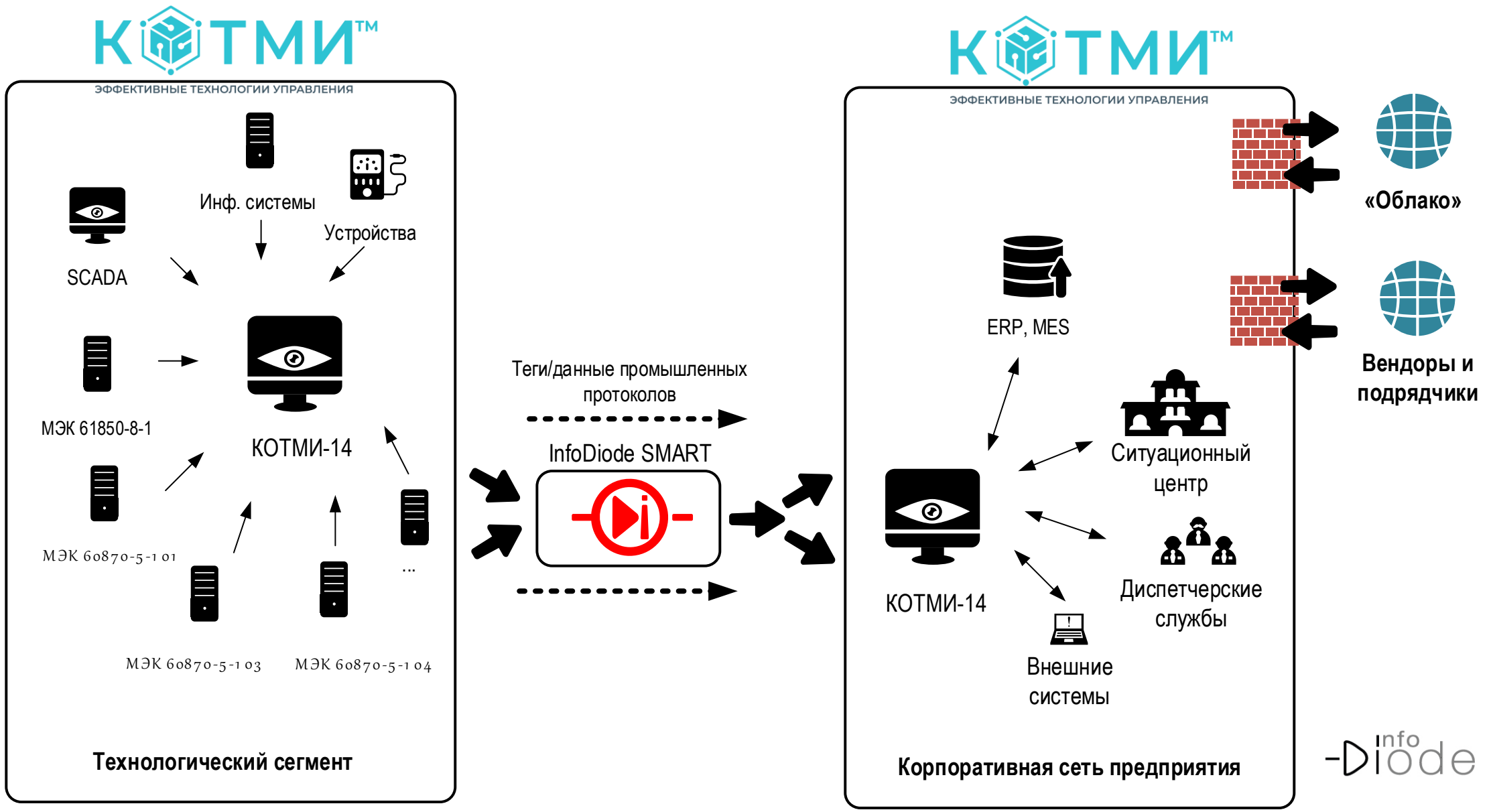
Решения для объектов энергетики – Релематика (передача данных в ЦУС)



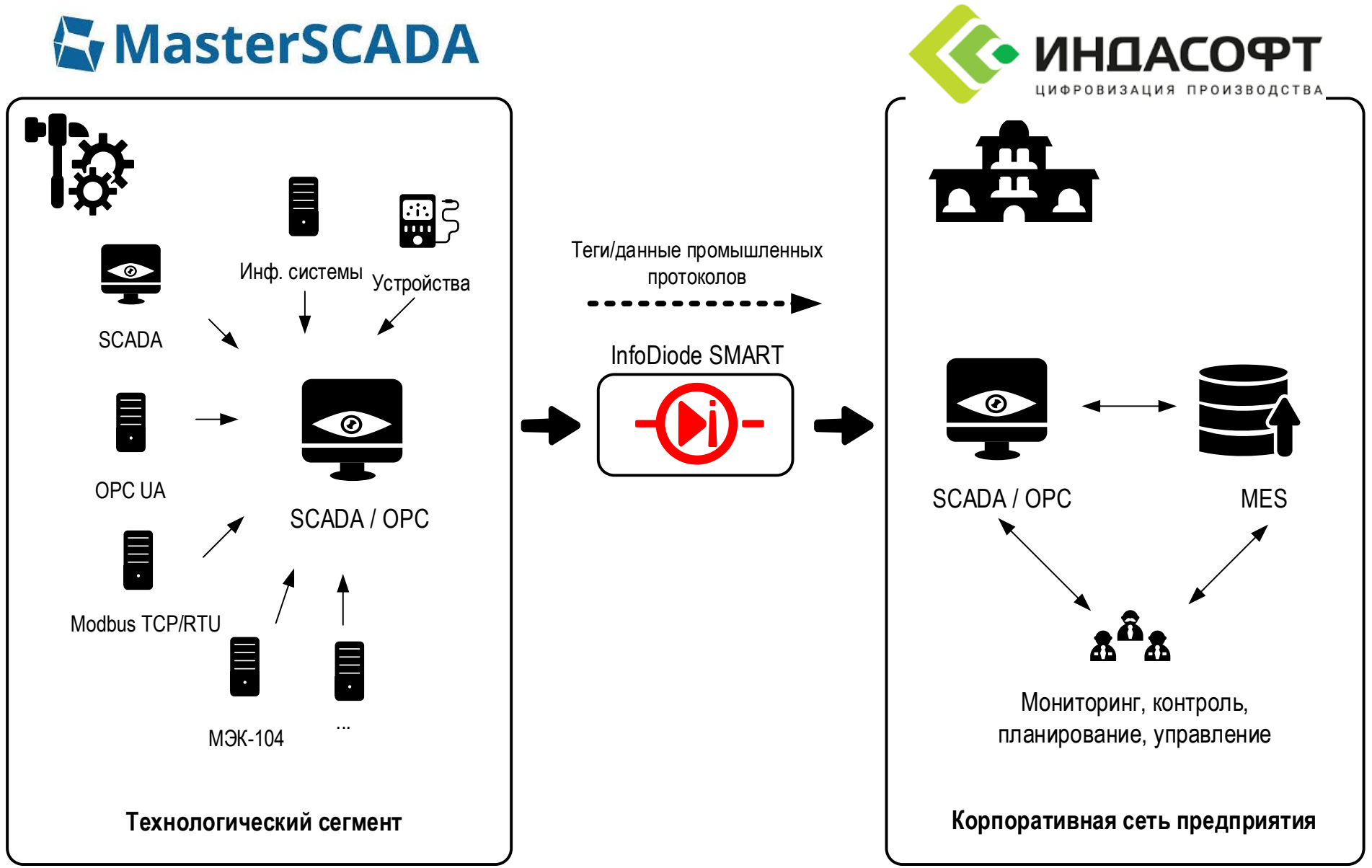
Решения для объектов энергетики – InfoDiode и СК-11 Монитор-электрик (передача данных в ЦУС)



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

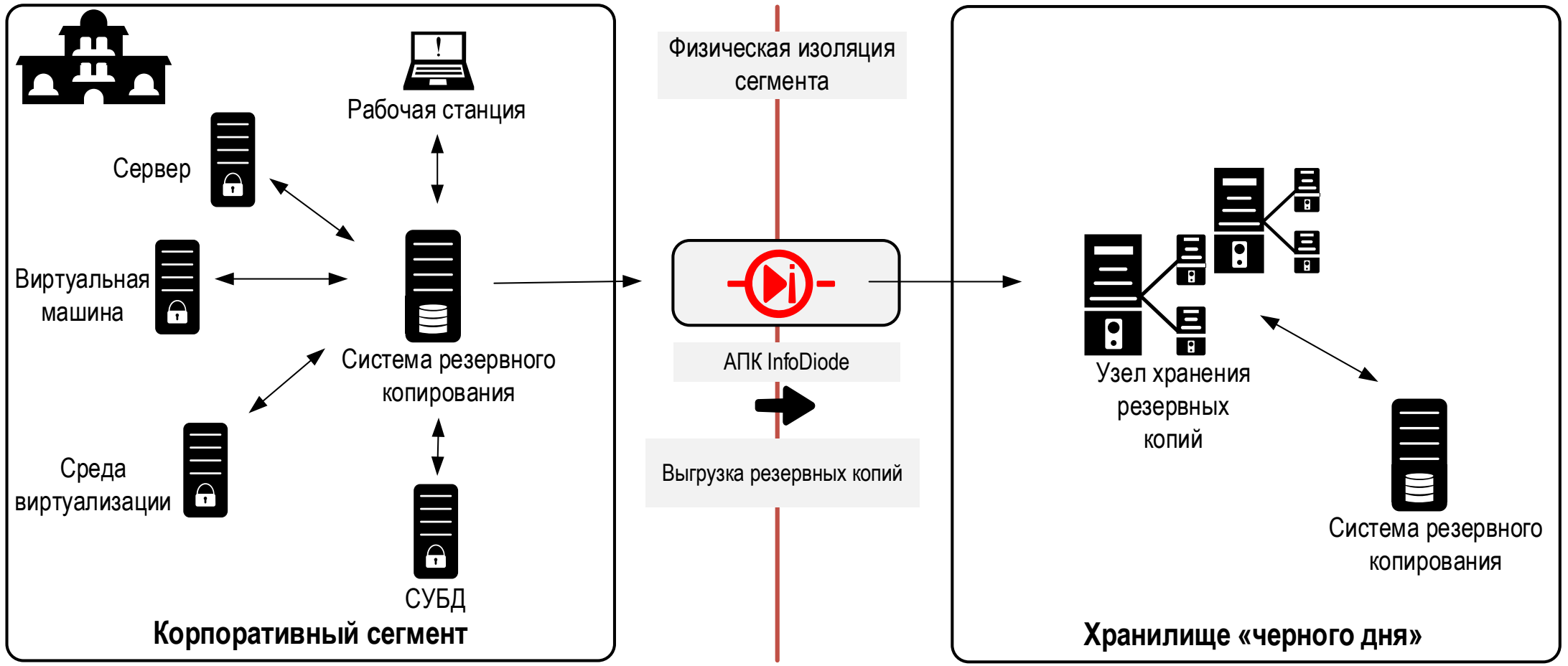


Решения для MES и Historian – InfoDiode и Indusoft (внедрение MES в условиях изоляции АСУ ТП сегмента)



Решения в области построения защищенных решений - InfoDiode и Киберпротект (хранилище «черного дня»)

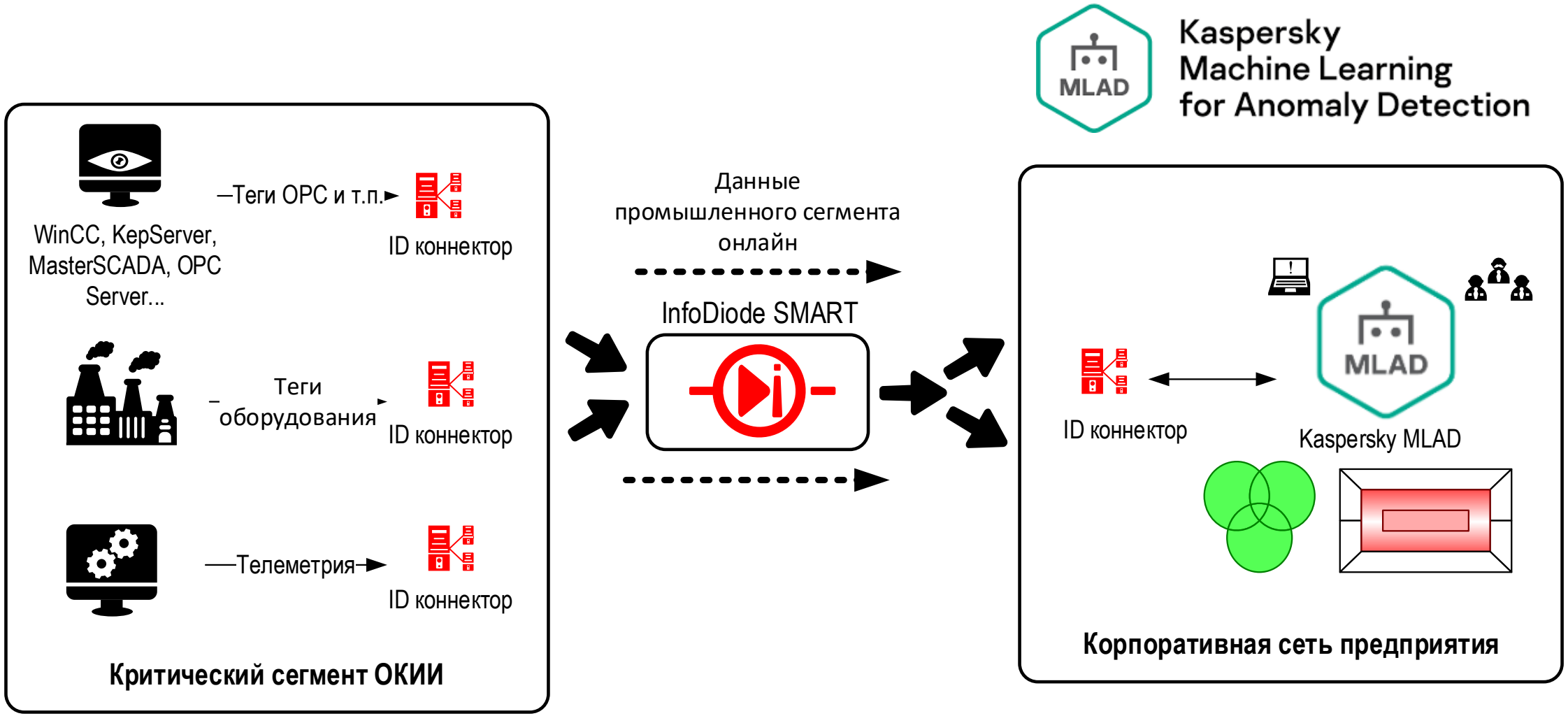
КИБЕР Бэкап



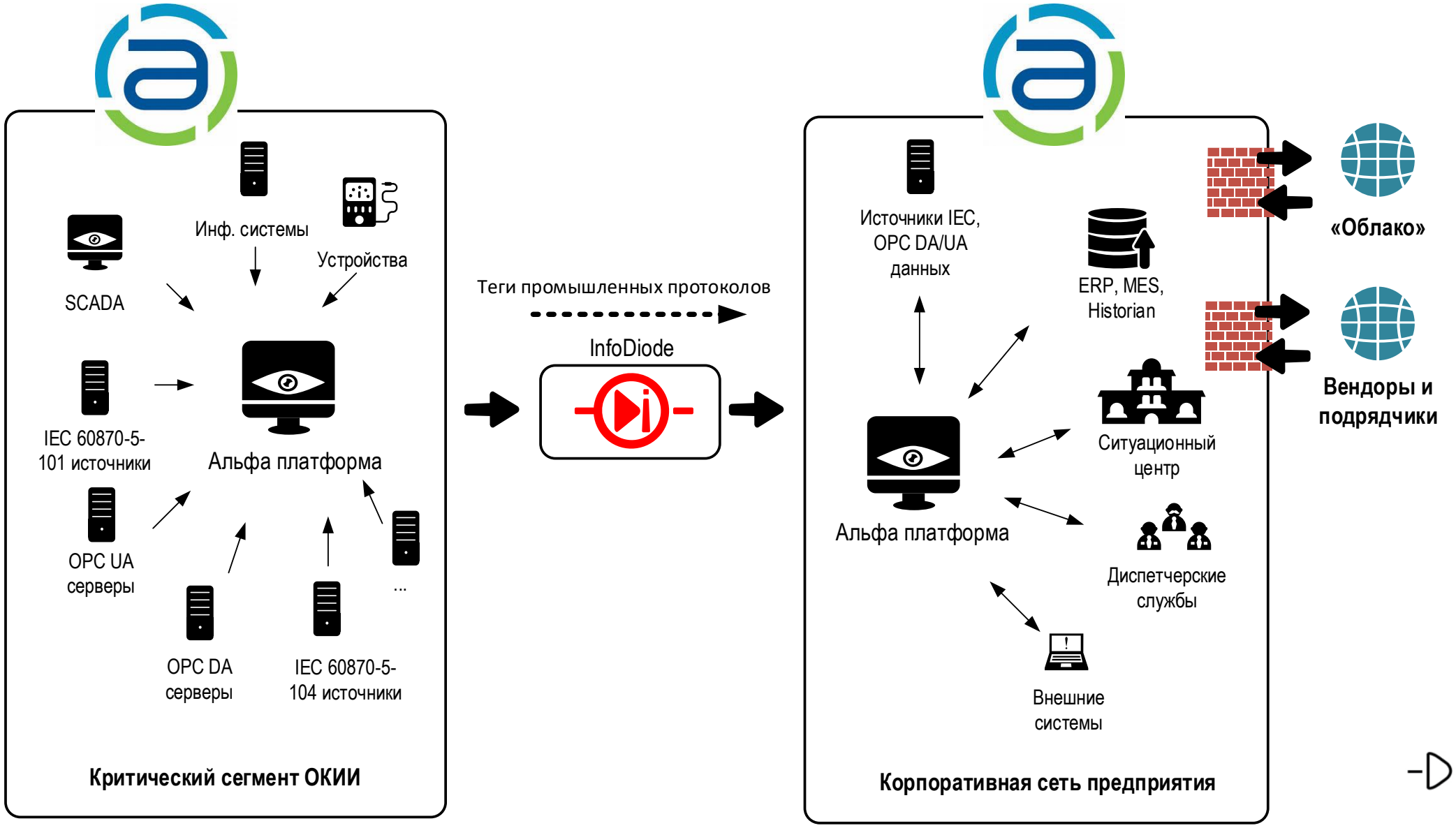
InfoDiode

AMT GROUP

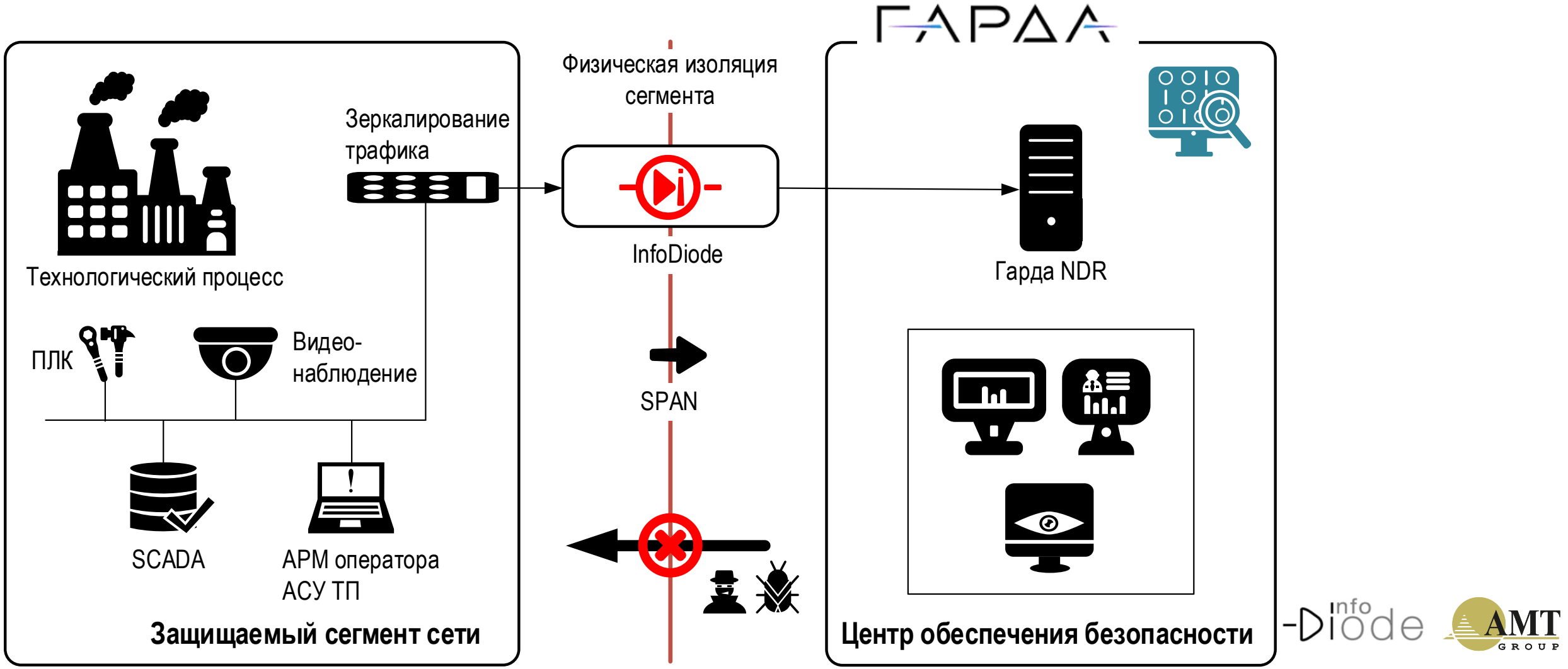
Решения класса Machine Learning – InfoDiode и Kaspersky MLAD (сбор данных из АСУ ТП для поиска аномалий и предиктивной аналитики)



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 СОВ)



InfoDiode обеспечивает однонаправленную передачу данных, НО:

1. **Что мы передаем и принимаем?**

2. **Что делать, если двунаправленный критически необходим?**

МЕЖДОМЕННЫЙ ОБМЕН

InfoDiode становится частью междоменных решений (МДР)

Междоменные решения InfoDiode - интегрированный комплекс решений по обеспечению безопасности

Комплекс состоит из специализированного программного и аппаратного обеспечения с интерфейсами для ручного или автоматического предоставления 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 СОВ/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

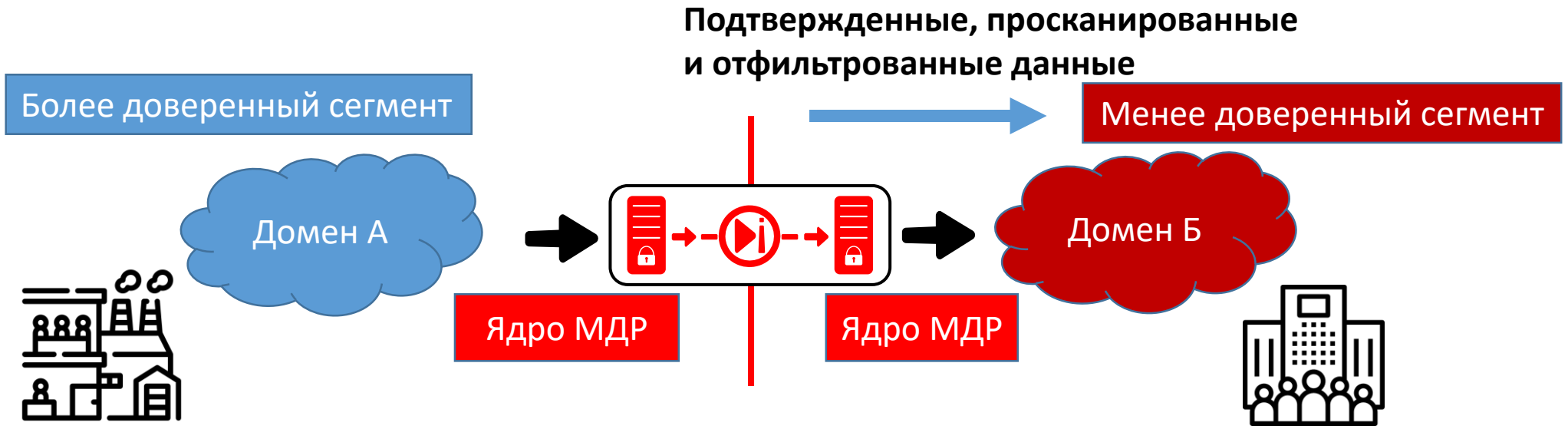


В основе обмена всегда лежит принцип

физический сигнал только в одну сторону

Междоменные решения могут повышать уровень безопасности в разных сценариях применения

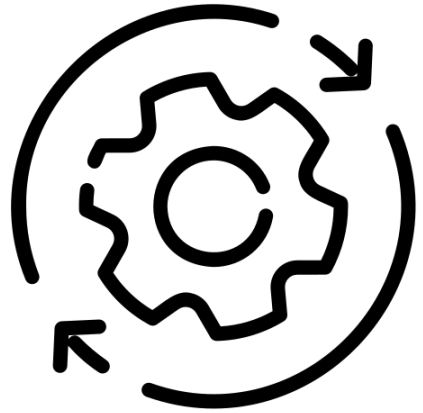
Сценарий 1



Сценарий 2

МДР решения фокусируются, в первую очередь, на контроле, а не на транспорте

- **Соблюдение политик безопасности передачи данных между доменами безопасности**
  - Блокирование всего трафика между доменами по умолчанию **(только «белые списки» передачи данных через МДР)**
  - Ограничения на файловые потоки **(тип, размер, интенсивность, регламент передачи)**
  - Фильтрация, санитарная обработка трафика - устранение вредоносного содержимого и/или предотвращения потери конфиденциальных данных **(интеграция с серверами ICAP - DLP, антивирусы, «песочницы»)**



- **Защита МДР**
  - Использование в составе МДР однонаправленных шлюзов, исключающих одновременную компрометацию удаленным вектором атаки обеих сторон СЗИ, размещаемых в сопрягаемых доменах

- **Ведение аудита**
  - аудит каналов передачи данных, состояния системы, изменений в конфигурации

AMT GROUP

КОМПЛЕКСНОЕ СОПРЯЖЕНИЕ ДОМЕНОВ

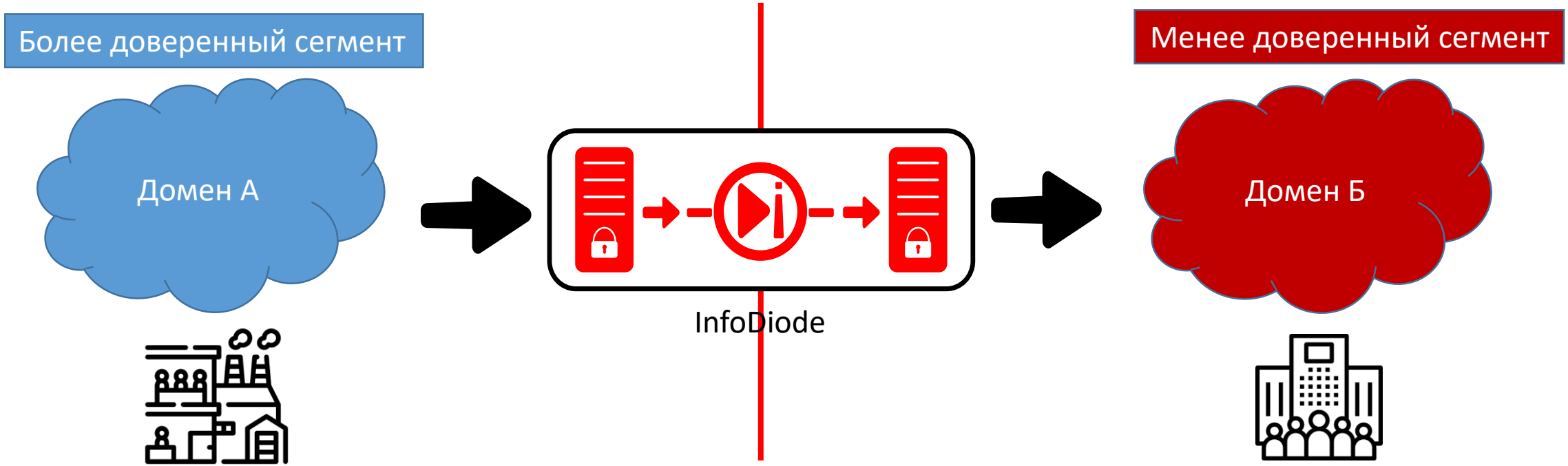
АПК InfoRelay - устройство для организации временного канала доступа

АПК INFORELAY

- **Не ограничивает применение существующих СЗИ.** Может использоваться как дополнение существующих схем защиты, так и как самостоятельное устройство. Совместим со всеми типами СЗИ (МСЭ, InfoDiode, криптошлюзы)
- **Физическая коммутация сетей** – физическая коммутация или раскоммутация сетей по требованию и под контролем специалиста ИБ
- **Двойной контроль включения** (локально и по вынесенной кнопке). Аудит операций включения.
- **Таймер коммутации** – строго ограниченный период сопряжения сетей для решения задач. Контроль пограничных состояний (пропало электропитание, забыли выключить и т.п.)
- **Реализован на российской платформе** производства АМТ-ГРУП

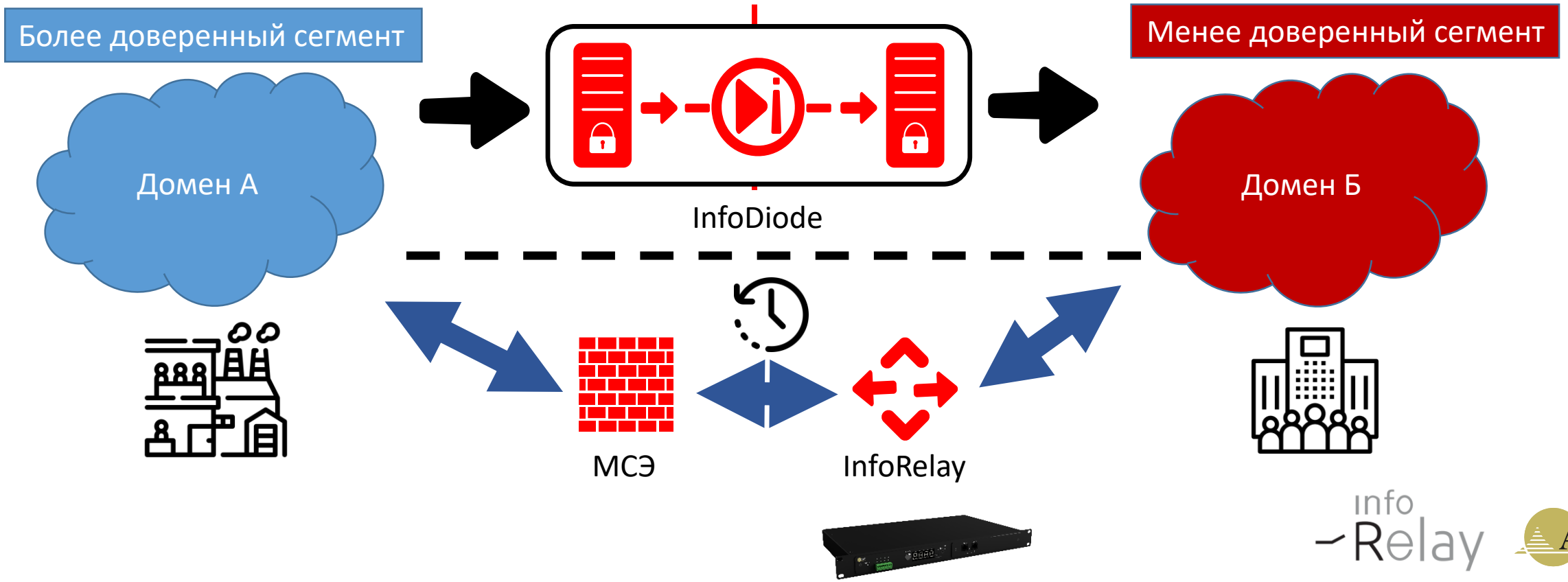
Исходный сценарий изоляции КИИ с InfoDiode

Исходный сценарий
Реализован обмен данными через InfoDiode. Обеспечена изоляция критической инфраструктуры, выполнены требования регулятора



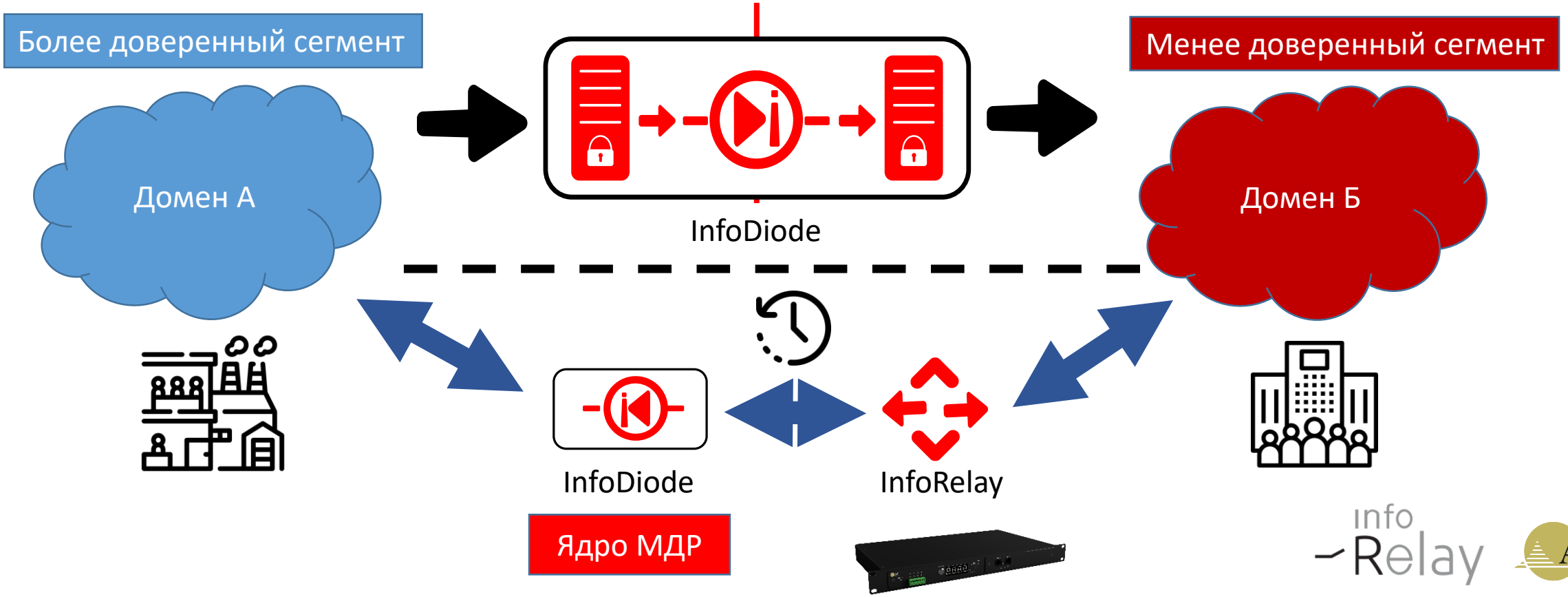
Применение InfoRelay совместно с InfoDiode и МСЭ

Сценарий 1
Операции пуско-наладки, выполняемые удаленно, регламентное планово-профилактическое обслуживание сложных энергетических и промышленных систем, обновление программного обеспечения (в том числе СЗИ), расследование инцидентов нарушения работоспособности и инцидентов ИБ



Применение InfoRelay в условиях применения 2-х InfoDiode

Сценарий 2
Периодические операции передачи данных (файлы, уставки, обновления) в защищаемый сегмент по строго регламентированному каналу с сохранением передачи данных через основной InfoDiode



InfoDiode – это линейка решений

https://infodiode.ru/

Telegram-канал InfoDiode

СПАСИБО ЗА ВНИМАНИЕ!