30.03.2026

АМТ-ГРУП

Решения InfoDiode, InfoRelay, SecureKiosk

ПРОБЛЕМЫ И АКТУАЛЬНЫЕ УГРОЗЫ

Современная организация уже давно не изолированный сегмент

- Типовая организация может иметь до 500 связей с внешними контрагентами, партнерами, вендорами и организациями
  - Облачные решения
  - Поддержка ПО, ИТ-поддержка
  - Системы бэкапирования
  - Отопление, вентиляция, кондиционирование (HVAC)
  - Системы безопасности (как информационной, так и общей)
  - Диспетчерские
  - Системы поставщиков и подрядчиков
- ПО в рамках сети OT/ICS (АС УТП) как правило «унаследовано»
  - ПО создавалось без учета ИБ, ряд пром. протоколов не предполагают аутентификацию в принципе

AMT GROUP

Технологические и закрытые сети: вызовы и риски

- Диспетчеризация и ситуационные центры
- Техническое обслуживание: планирование работы бригад, интеграция с системами управления персоналом
- Инвентаризация, учет, оформление заказов
- Планирование производства, интеграция с системами ERP, MES
- Централизованная поддержка и подрядные организации
- Аутсорсинг ИБ, SOC, систем обнаружения вторжений
- Мониторинг, разработка ПО для объектов
- Взаиморасчеты, взаимоотношения с клиентами
- Обновление ПО

Сопряжение технологических (закрытых) и корп. сетей, которые, в свою очередь, сопрягаются с Интернет и имеют меньший уровень доверия

Интерес киберпреступников к промышленным объектам растет! Уязвимостей больше, поверхность атаки на КИИ шире

- **Уязвимость «нулевого дня» - реальность сегодняшнего дня**
- **Скорость распространения атаки > скорости распространения защиты**
- **Канал взаимодействия с «системой-жертвой» - ключ к успешной атаке**
  - Двунаправленность важна на самом раннем этапе - при рекогносцировке, многие техники реализуются на основе двустороннего взаимодействия (RAT, phishing, др.)
- **Длительные сценарии развития атаки являются нормой**
  - Использование вспомогательных модулей для защиты вредоносного ПО от обнаружения
- **Вектор атаки смещается на человеческий фактор**
- **Общедоступность средств атаки**

Общие тренды

- **ПО в сети OT/ICS (АСУ ТП) часто «унаследовано»**
  - ПО создавалось без учета ИБ, ряд промышленных протоколов не предполагают аутентификацию, EOL, Аппаратные средства и сети не предполагают установки СЗИ
- **«Неразбериха» между блоками ИБ, ИТ, АСУ ТП**
- **Зарубежный опыт с задержкой транслируется в российские реалии**
  - Регуляторы многих секторов уже включили в свои документы требования и рекомендации по применению продуктов класса «диод»

Страновые особенности

AMT GROUP

ЛИНЕЙКА РЕШЕНИЙ INFODIODE

Аппаратное решение L1 уровня в стойку

*** Два в одном (экономит место в стойке)**

Что это

АК InfoDiode RACK single/ double

Как применять

- Передача SPAN трафика для IDS
- Передача данных SIEM агентов
- Передача syslog и UDP трафика
- Передача данных, которые изначально конвертированы в UDP

Преимущества

- Недорогое устройство
- Не требует настройки
- Высокий MTBF
- Можно менять порты (медь, оптика)

Аппаратное решение L1 уровня на DIN рейку

Что это

АК InfoDiode MINI

Как применять

- Передача SPAN трафика для IDS
- Передача данных SIEM агентов
- Передача syslog и UDP трафика
- Передача данных, которые изначально конвертированы в UDP

Преимущества

- Недорогое устройство
- Не требует настройки
- Высокий MTBF
- **Поддерживает 100Mbs/1Gbs**
- **Монтаж на DIN рейку, установка на стол**

AMT GROUP

Решение для файловой передачи и не только – базовый и кластерный варианты

*** Повышенная отказоустойчивость**

Что это

АПК InfoDiode PRO base

Как применять

- Передача файлов, почты
- Создание «хранилищ черного дня»
- Передача данных SIEM агентов
- Передача syslog и UDP трафика
- Основа для междоменных решений

Преимущества

- Политики файловой передачи
- Настройка приоритетов передачи
- Расширенная модель SIEM событий
- Мониторинг, КС файлов, обработка
- Интеграция с LDAP

Решение для передачи промышленных протоколов

Что это

АПК InfoDiode SMART

Как применять

- Изоляция АСУ ТП, передача пром. протоколов, в том числе в энергетике
- Передача данных в MES, СЦ
- Передача IoT/IIoT трафика
- Передача данных SIEM агентов
- Передача syslog и UDP трафика

Преимущества

- Высокая производительность для промышленного трафика
- Продвинутая модель мониторинга
- Минимальные задержки – 20 мс
- Форматно-логический контроль сообщений JSON

Решение для передачи промышленных протоколов – версия light

Что это

АПК InfoDiode SMART light

АПК InfoDiode SMART light e

Как применять

- Передача Modbus, IEC-104 небольшого файлового трафика
- Применение на небольших или удаленных объектах
- Передача данных в АСУ ТП, MES, СЦ
- Передача syslog и UDP трафика

Преимущества

- Недорогое решение для небольших объектов
- Базовые коннекторы включены
- Планируется версия с LTE

AMT GROUP

Решение для физической коммутации сети – реле (включатель/переключатель)

*** 2 пары по 3 порта –**
различные сценарии применения

Что это

АПК InfoRelay ВК – 2/6 ports

Как применять

- Создание временного регламентированного канала
- Временный доступ к «хранилищу черного дня»
- Организация параллельного InfoDiode канала доступа

Преимущества

- Таймер коммутации
- Разные режимы включения
- Коммутация кнопкой, через сухие контакты, в том числе удаленно

Решение для безопасной передачи файлов между доменами – передача из общественных мест

АПК SecureKiosk tower

Что это

Как применять

- «Единое окно» в общедоступном месте для безопасной файловой передачи между доменами через InfoDiode

Преимущества

- Комплексное решение с InfoDiode
- Интеграция с СКУД, видеонаблюд.
- Реализация концепции ZeroTrust
- Можно ставить два и более киосков
- Могут быть киоски на прием и на передачу

Решение для безопасной передачи файлов между доменами – рабочее место сотрудника

Что это

АПК SecureKiosk desktop

Как применять

- Рабочее место сотрудника для передачи файлов -в или –из закрытого сегмента через InfoDiode

Преимущества

- Комплексное решение с InfoDiode
- Реализация концепции ZeroTrust
- Можно ставить два и более
- Могут быть рабочие места на прием и передачу
- Не требует больших аппаратных мощностей

Больше информации о продуктах InfoDiode

https://infodiode.ru/

Telegram-канал InfoDiode

E-mail: InfoDiode@amt.ru

Техническая поддержка: **https://support.amt.ru**

НОРМАТИВНАЯ БАЗА И СТАНДАРТЫ

Перечень мер приказов ФСТЭК России, реализуемых применением InfoDiode

Приказ ФСТЭК N 17 от 11 февраля 2013 г. и N 21 от 18.02.2013 г.

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта
ЗИС.16	Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер защиты информации или внутри разрешенных сетевых протоколов
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы
ЗИС.22	Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы
ЗИС.23	Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами

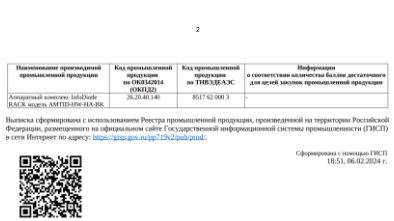
Приказ ФСТЭК N 239 от 25 декабря 2017 г. и N 31 от 14 марта 2014 г.

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта
ЗИС.2	Защита периметра информационной (автоматизированной) системы
ЗИС.3	Эшелонированная защита информационной (автоматизированной) системы
ЗИС.4	Сегментирование информационной (автоматизированной) системы
ЗИС.6	Управление сетевыми потоками
ЗИС.8	Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы
ЗИС.18	Блокировка доступа к сайтам или типам сайтов, запрещенных к использованию
ЗИС.31	Защита от скрытых каналов передачи информации
ЗИС.34	Защита от угроз отказа в обслуживании (DOS, DDOS-атак)
ЗИС.35	Управление сетевыми соединениями

* Больше информации в части реализуемых требований нормативных актов размещено на сайте infodiode.ru

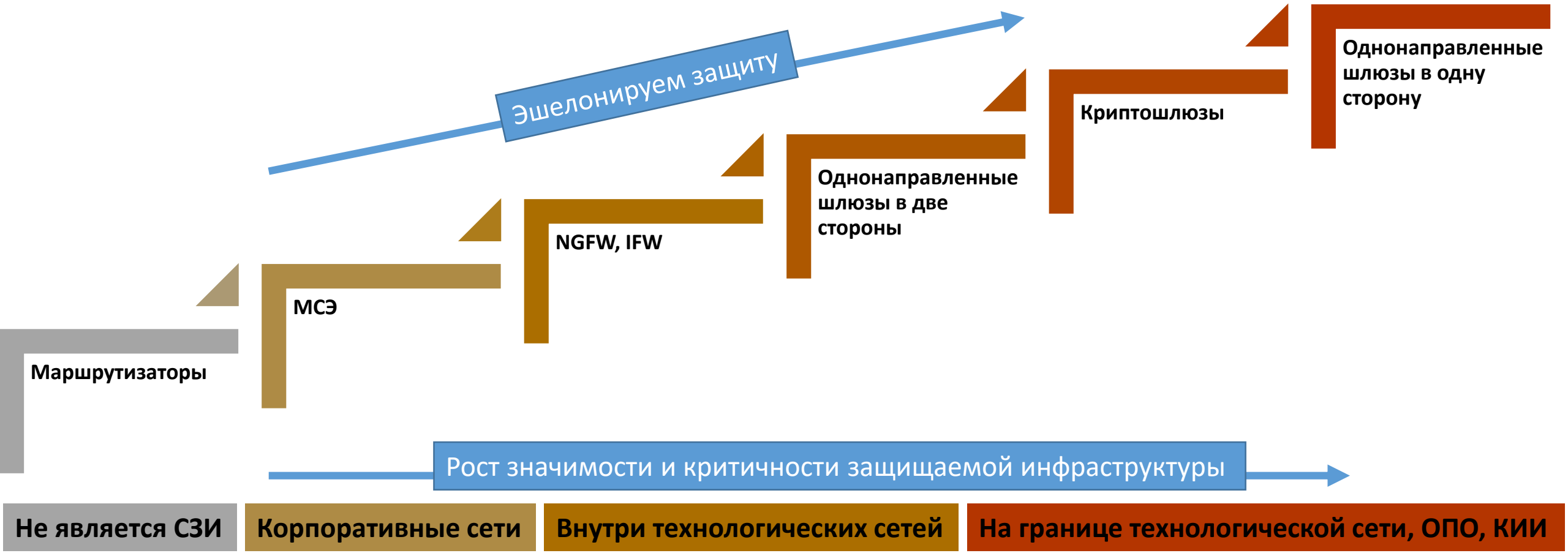
InfoDiode включен в реестры, завершена его сертификация

1. **Сертификаты ФСТЭК (УД4)** – на всю линейку решений
2. **Реестр Минпромторга** – включены и аппаратный, и программно-аппаратный комплексы
3. **Реестр Минцифры** – программное обеспечение
4. **Сертификаты и декларации ЕАС** – на всю линейку решений



ВАРИАНТЫ ЗАЩИТЫ СЕТЕЙ И КОМПЛЕКСНЫЕ РЕШЕНИЯ

Для каждого объекта или сегмента свой уровень защиты. Эшелонированная защита - ключ к повышению безопасности

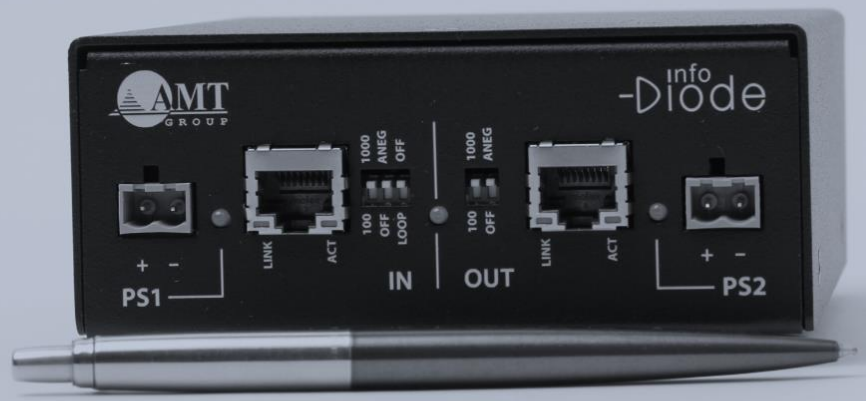


Устройство однонаправленной передачи данных функционирует на физическом уровне

- **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

Продукты InfoDiode совместимы со многими СЗИ, АСУ ТП, ИТ решениями

АППАРАТНЫЕ РЕШЕНИЯ INFODIODE



Аппаратный комплекс InfoDiode – простое и эффективное решение для сегментации сети

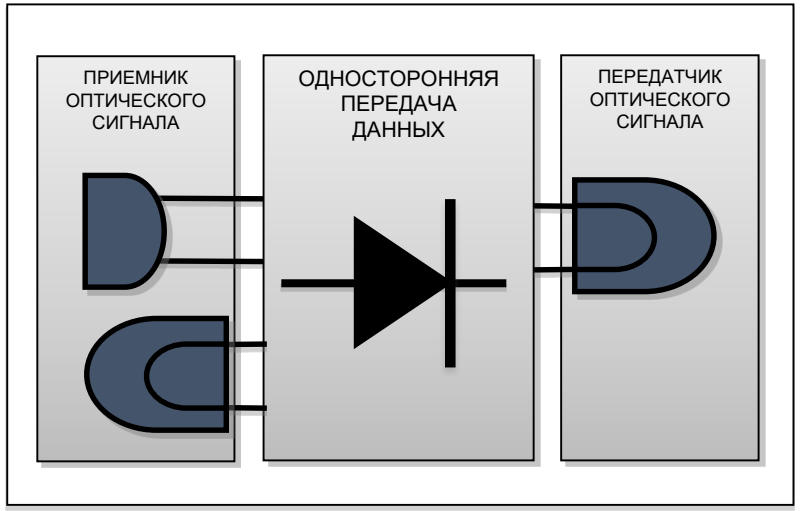
Аппаратная односторонняя передача данных

- Односторонний поток данных из защищаемой зоны сети
- Отсутствие внешнего доступа в защищаемую зону сети
- Отсутствие двунаправленного соединения TCP / IP
- Программная атака не может изменить политику аппаратной безопасности

Конфиденциальность сети

- Разрыв сетевого протокола = асинхронный режим передачи
- Только «полезная нагрузка»
- Диод «невидим» в сети
- Диод данных не имеет ни IP-адреса, ни MAC-адреса
- Защищает все IP-и MAC-адреса исходных сетевых устройств, исключает внешнее сканирование сети и построение карт защищенных сетей

Аппаратное устройство для одностороннего обмена



SPAN трафик, тунелинг UDP

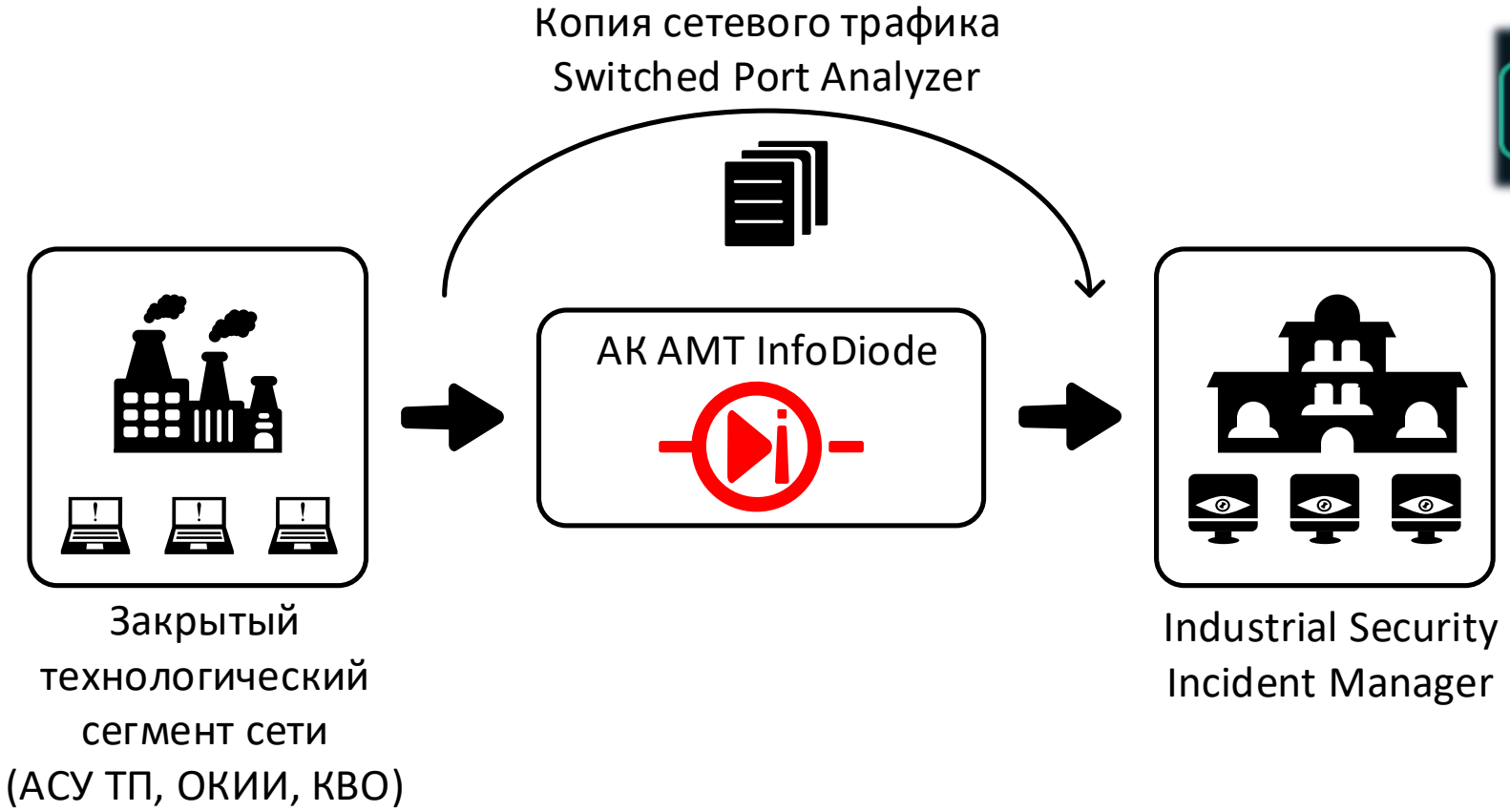
Возможно

Невозможно

AMT GROUP

SPAN-mirroring

Вариант 1. Передача копии технологического трафика закрытого сегмента во внешнюю систему мониторинга с использованием SPAN. Копия технологического трафика передается во внешний ПАК глубокого анализа трафика, который обеспечивает поиск следов нарушений информационной безопасности в сетях АСУ ТП, помогает на ранней стадии выявлять кибератаки, активность вредоносного ПО, неавторизованные действия персонала (в том числе злоумышленные)



Kaspersky Industrial CyberSecurity

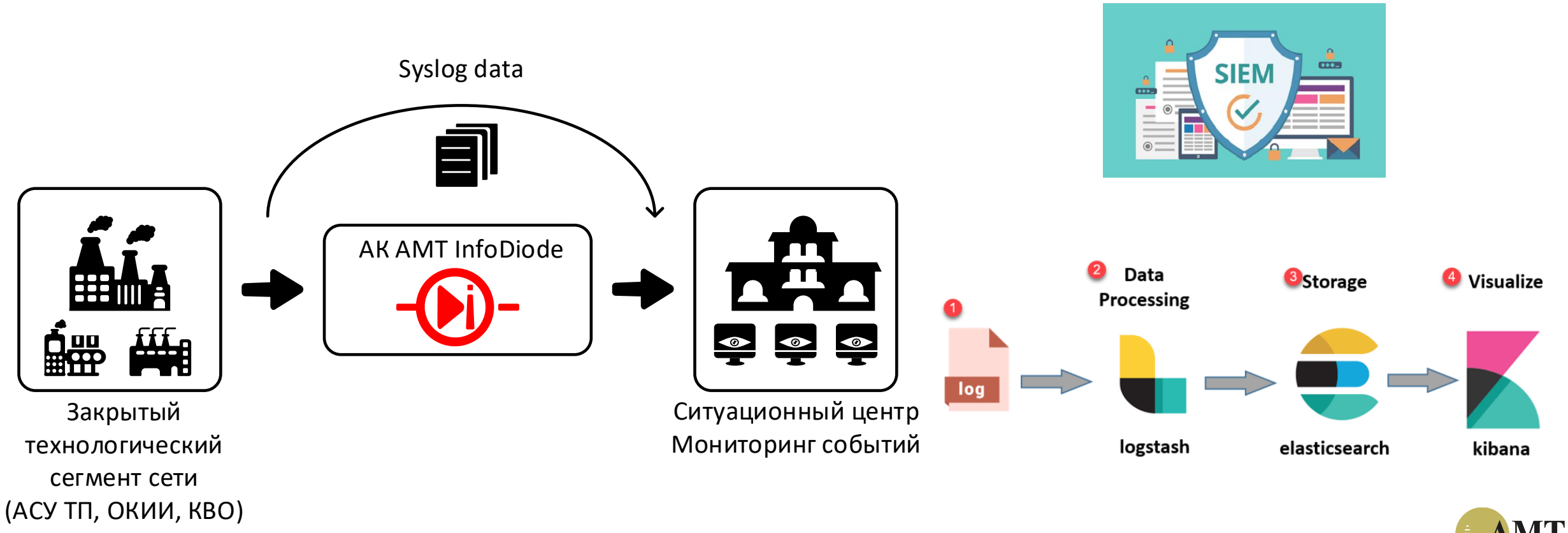
PT ISIM

Rhebo
Industrial Network Continuity

AMT GROUP

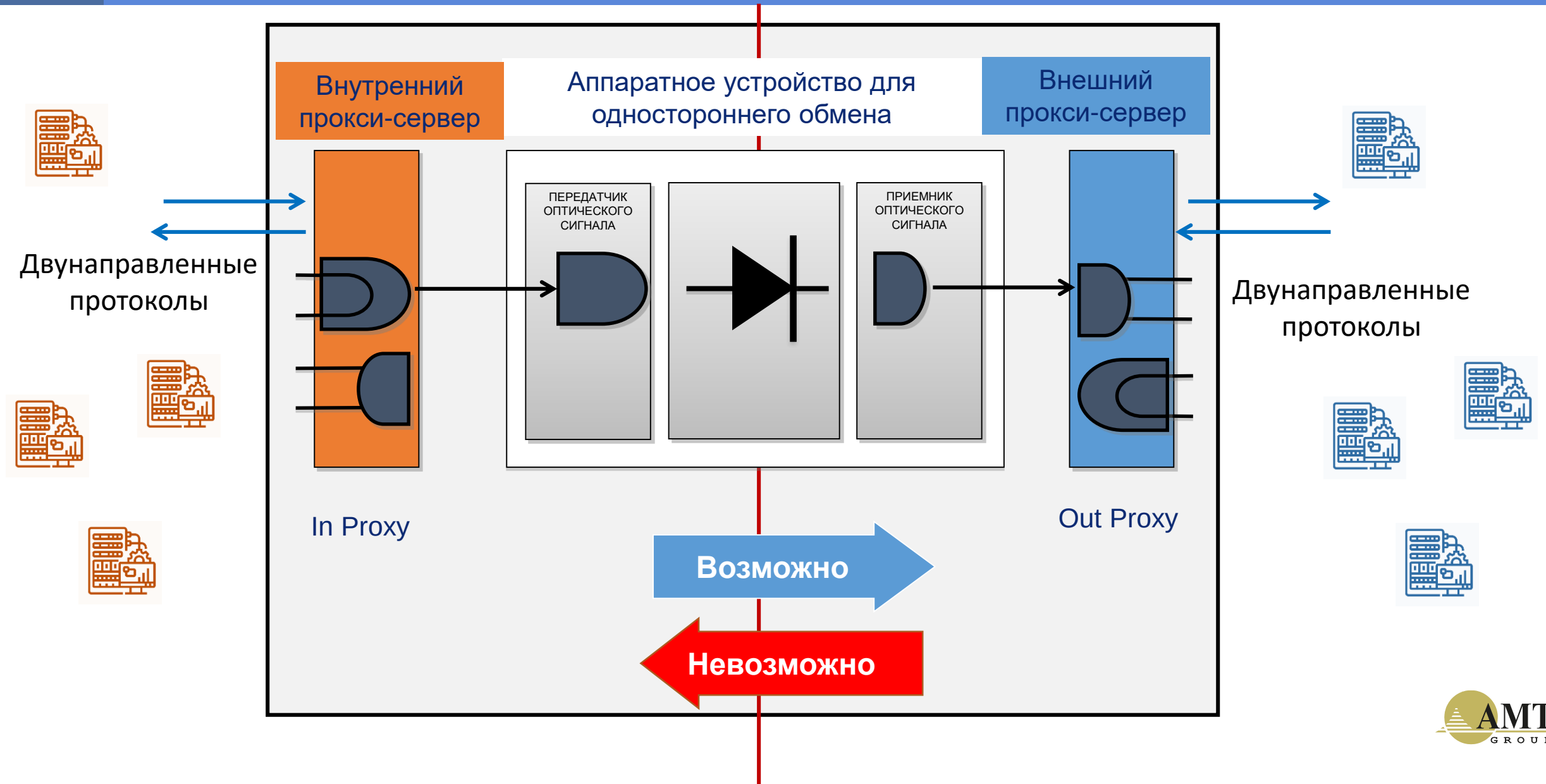
Передача данных для NOC и SOC через АК InfoDiode

Вариант 2. Передача событий технологической сети с использованием Syslog на внешнюю систему мониторинга. Логирование событий внутри технологического сегмента в централизованной системе мониторинга событий позволяет существенно снизить вероятность возникновения аварийных ситуаций и консолидировать все данные в едином ситуационном центре

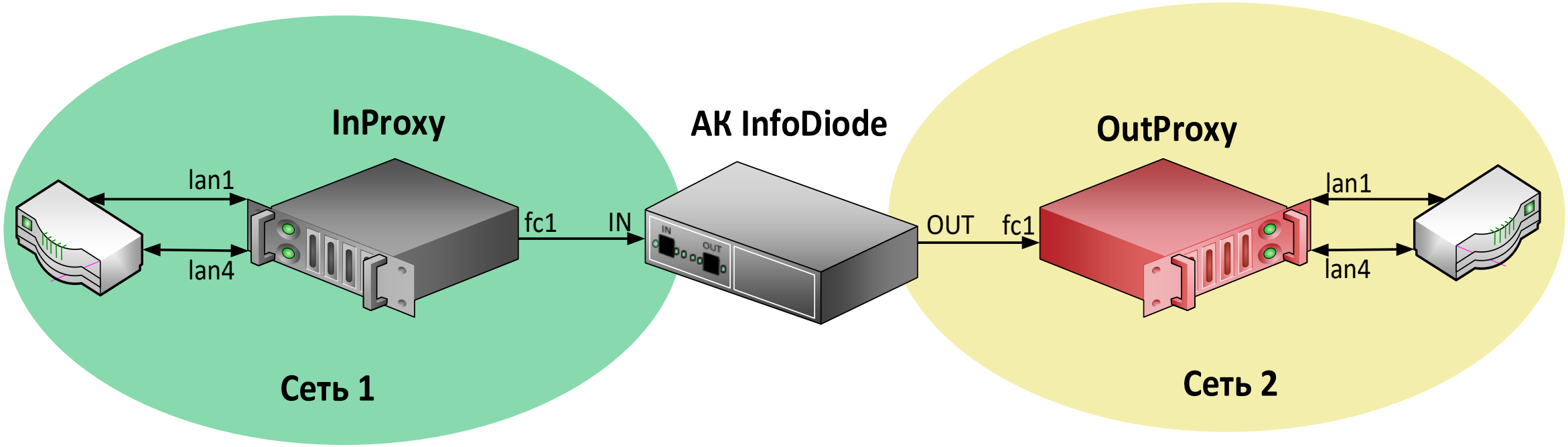


АППАРАТНО-ПРОГРАММНЫЕ РЕШЕНИЯ INFODIODE PRO

Решения InfoDiode позволяют передавать двунаправленные протоколы, терминируя их на себе

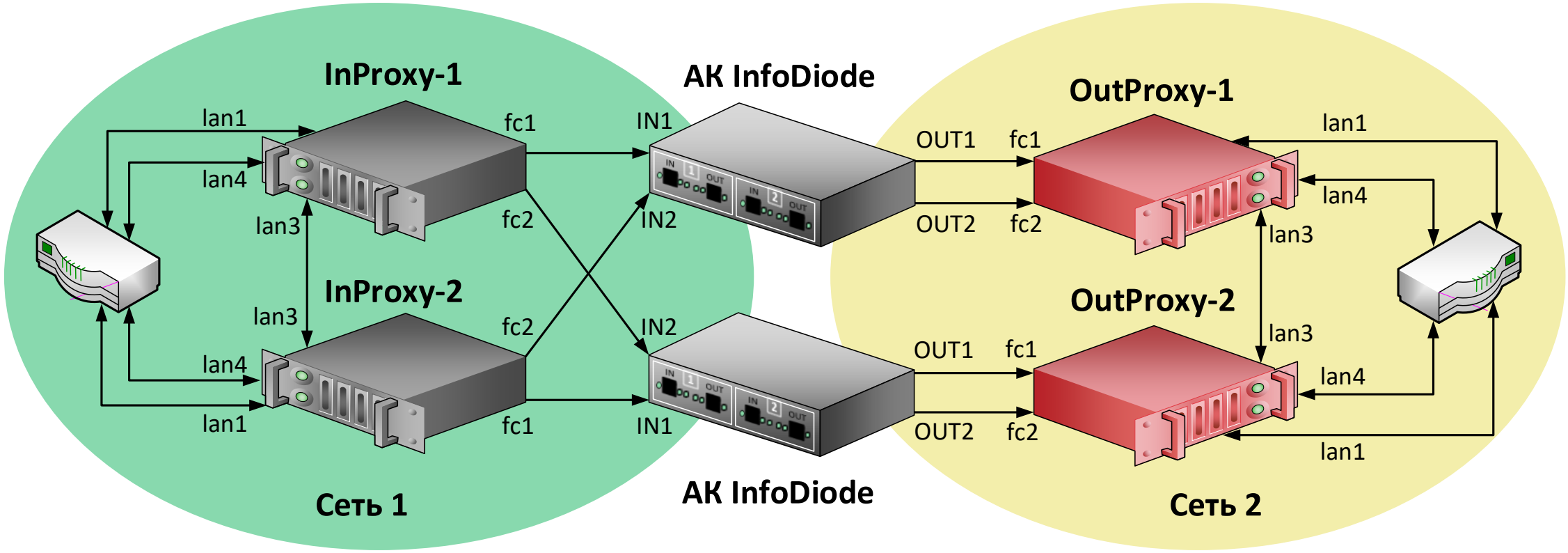


Базовый вариант АПК InfoDiode PRO

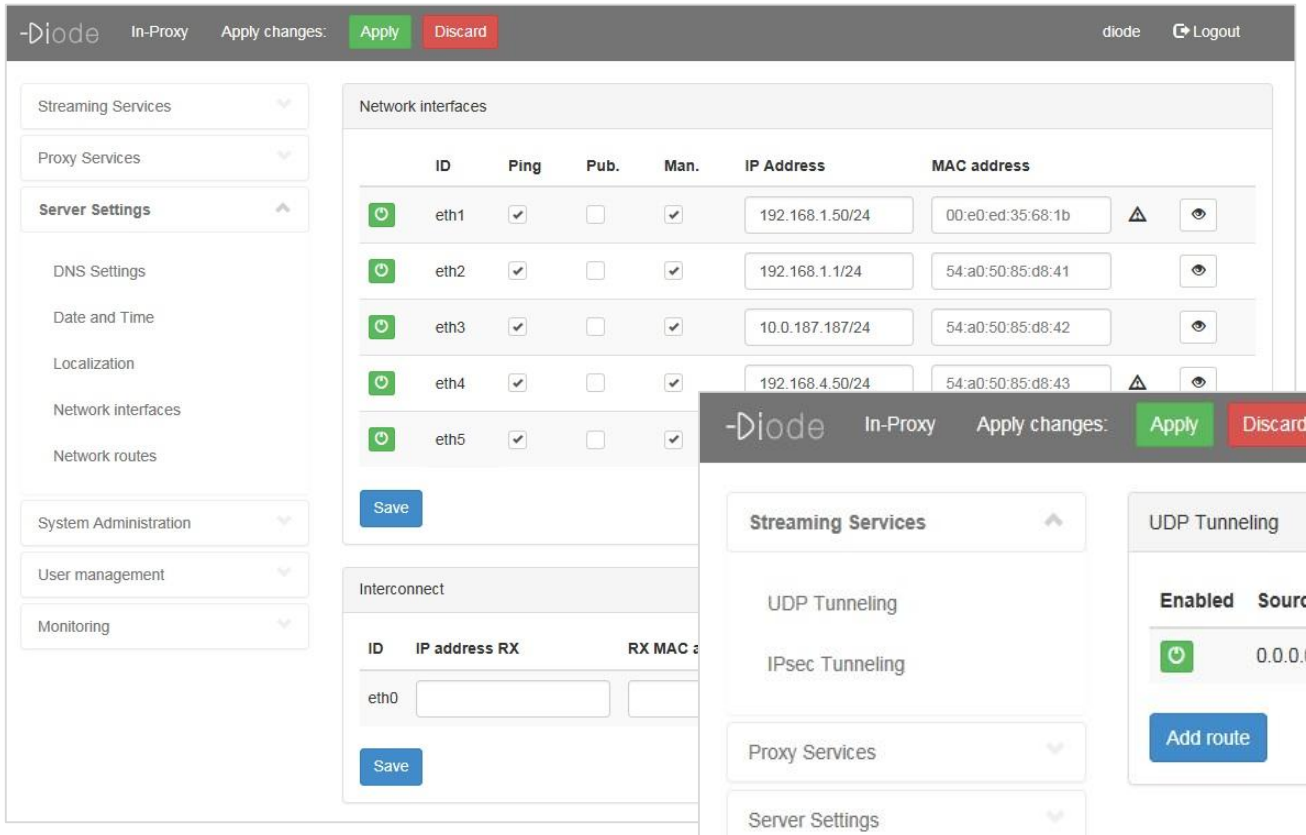


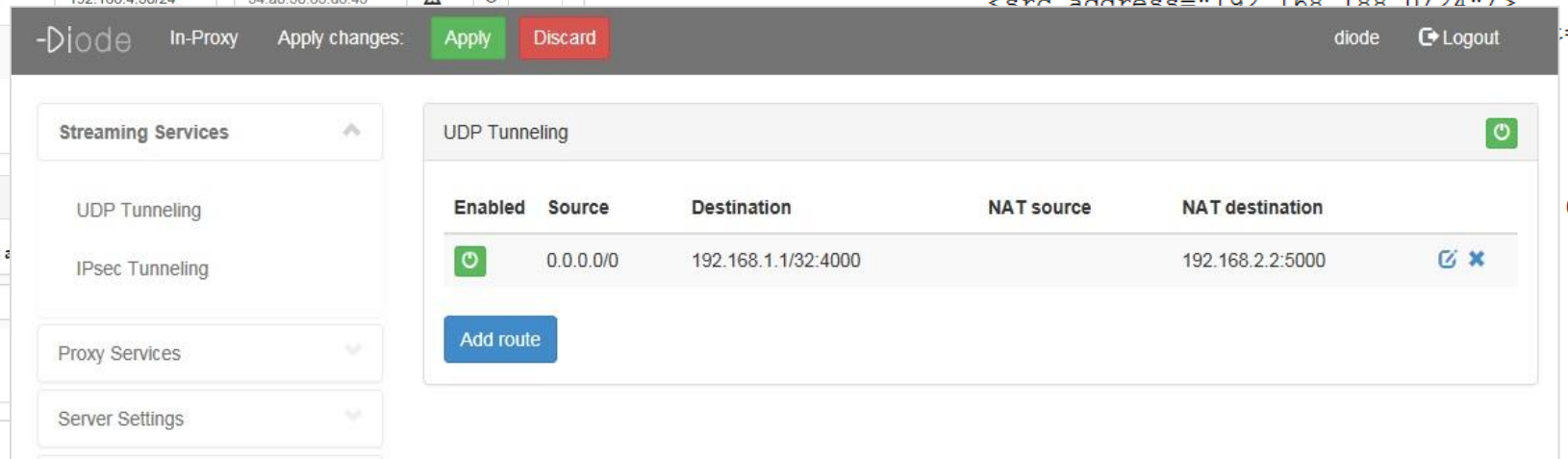
Кластерный вариант АПК InfoDiode PRO – отказоустойчивый вариант

Дублирование всех элементов комплекса



Удобный и понятный интерфейс администрирования АПК InfoDiode PRO






```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<server target="tx" version="1.0"
xmlns="urn:ru:amt:diode:config:server:1.0">
    <language>en</language>
    <country>RU</country>
    <timeZone>Asia/Yerevan</timeZone>
    <license/>
    <subsystems>
        <subsystem
xmlns="urn:ru:amt:diode:config:subsystems:udp:1.0">
            <enabled>true</enabled>
            <rule enabled="true">
                <src address="192.168.188.0/24"/>
```

- User-friendly Web-интерфейс (русская и английская версии)
- Возможность управления посредством CLI и XML
- Специальный режим защиты против случайных изменений

AMT GROUP

Возможности и параметры АПК InfoDiode PRO

- Производительность UDP - 900 Mbps
- Производительность прокси сервисов – 300 Mbps
- Поддержка протоколов FTP/FTPS, CIFS, SMTP, SFTP и др.
- Приоритезация передачи данных и потоков
- Помехоустойчивое кодирование
- Configuration/system backup
- Syslog/SIEM интеграция
- NTP синхронизация
- Интеграция с AD
- Формирование файла мета-информации для его анализа средствами DLP (чтение), Syslog аудит
- SNMP v2c и v3, syslog

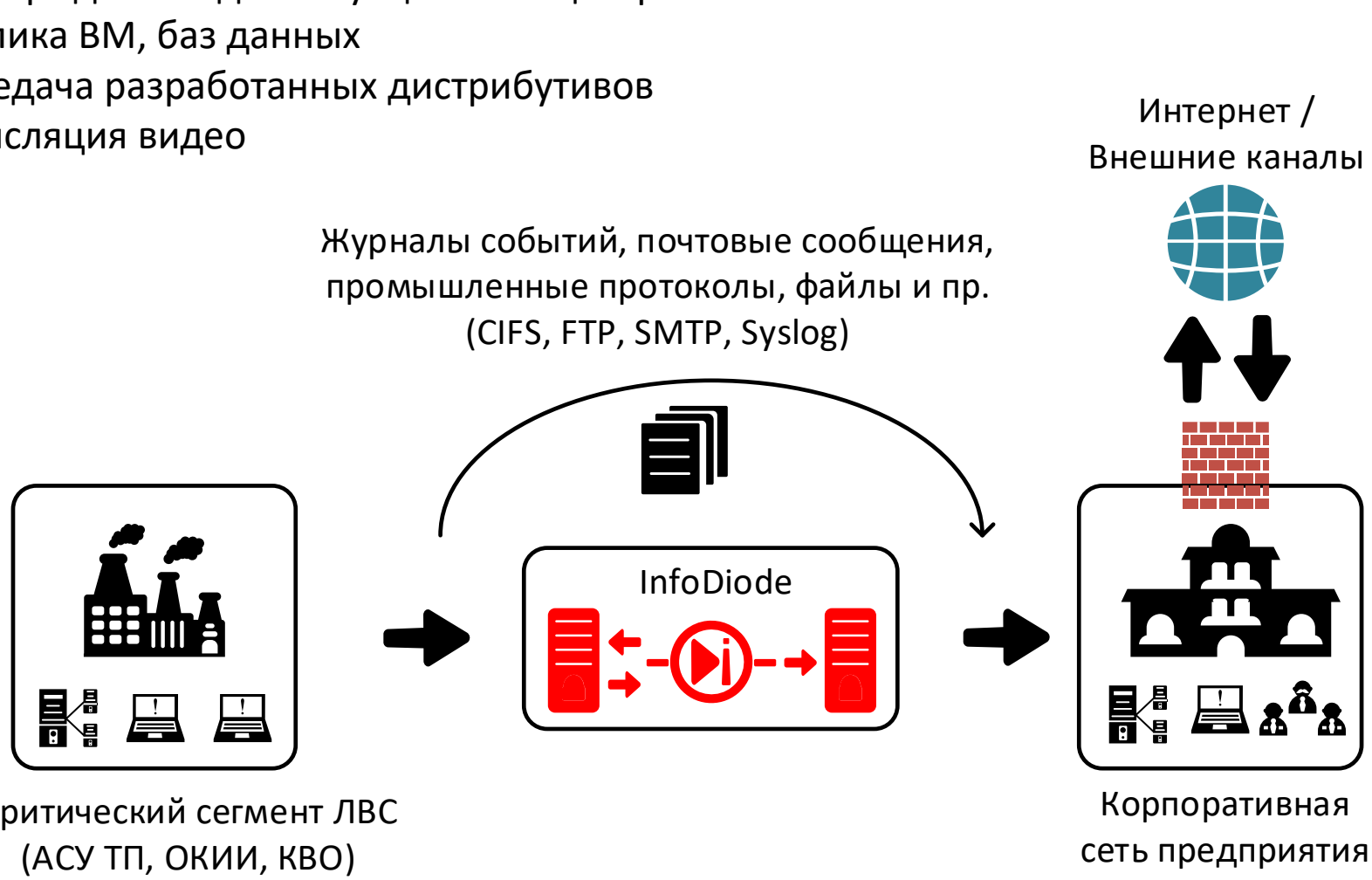
Передача данных и реплик из защищенного сегмента через АПК InfoDiode PRO

Вариант 1. Экспорт данных

В данном сценарий обеспечивается гарантия целостности передаваемых данных.

- Экспорт данных для ситуационных центров
- Реплика ВМ, баз данных
- Передача разработанных дистрибутивов
- Трансляция видео

и т.п.

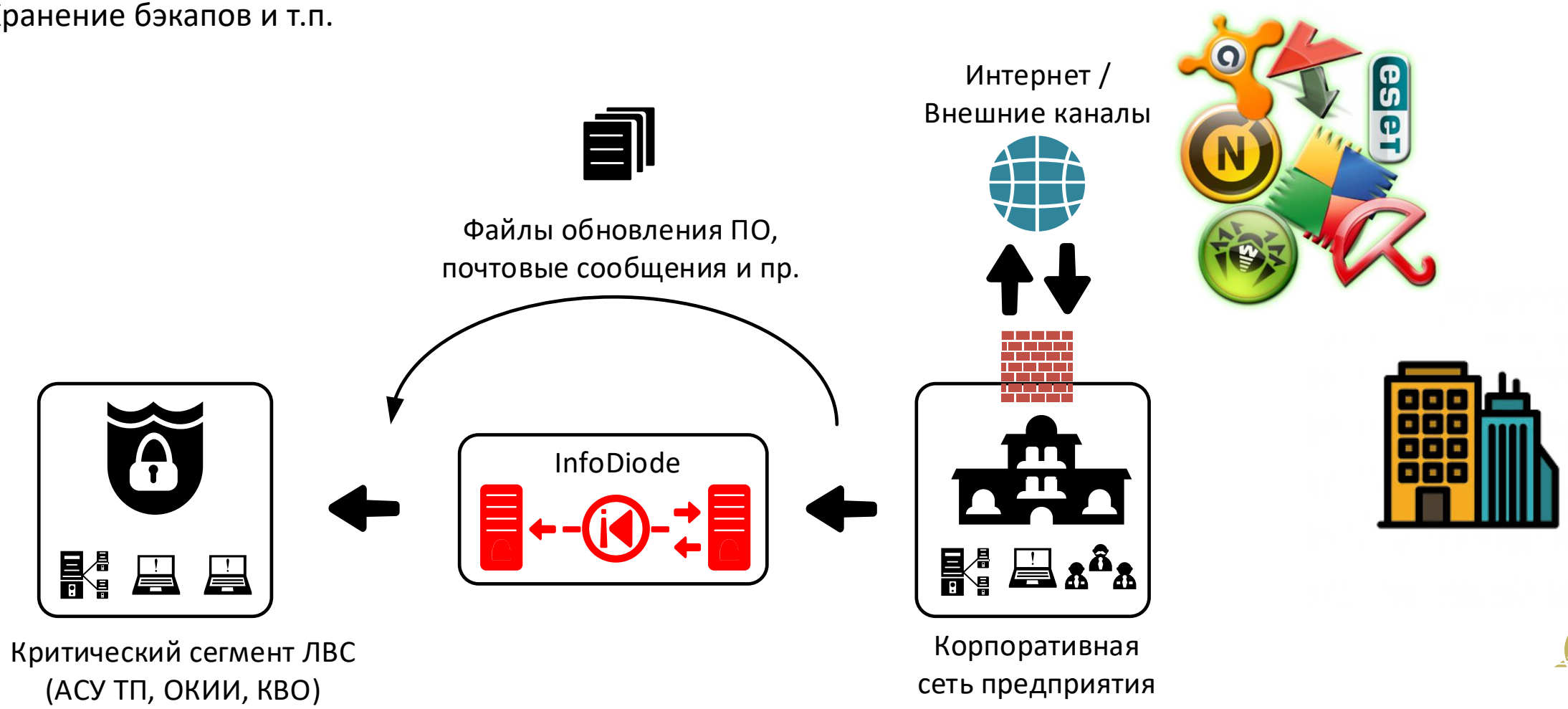


Получение обновлений и данных в защищаемый сегмент через АПК InfoDiode PRO

Вариант 2. Импорт данных

В данном сценарии обеспечивается гарантия конфиденциальности защищаемых данных.

- Загрузка обновлений
- Хранение бэкапов и т.п.



АППАРАТНО-ПРОГРАММНЫЕ РЕШЕНИЯ INFODIODE SMART

АПК InfoDiode SMART можно использовать в разнородной инфраструктуре КИИ

АПК INFODIODE SMART

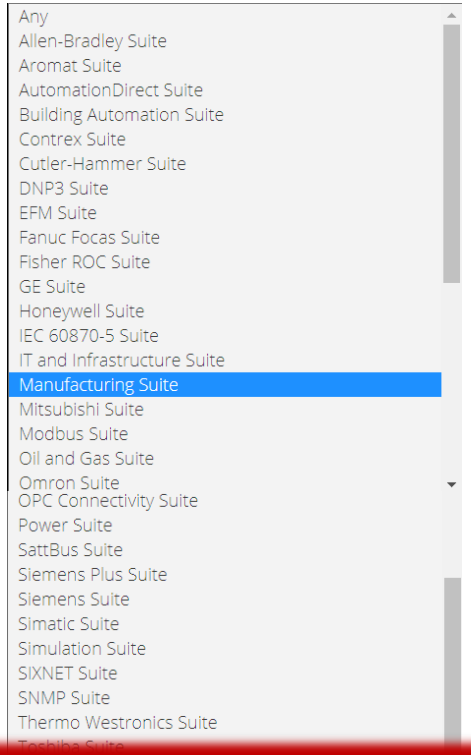
OPC UA

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

AMT GROUP

Промышленные протоколы через InfoDiode SMART - уже реальность

Удаленные АРМ



Modbus

Промышленные протоколы

info-Diode

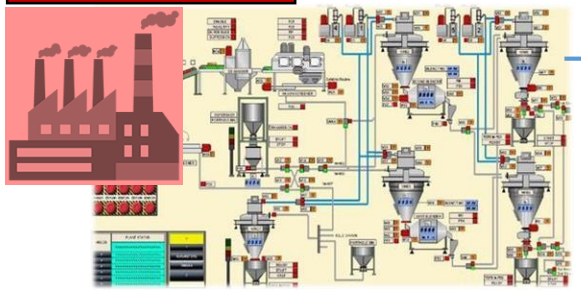
Ситуационные центры

ДОВЕРЕННЫЙ СЕГМЕНТ
Управление оборудованием

НЕДОВЕРЕННЫЙ СЕГМЕНТ
Ситуац. центры, диспетчерские, подрядчики, SOC, NOC

АПК InfoDiode SMART позволяет собирать данные SCADA за границами периметра

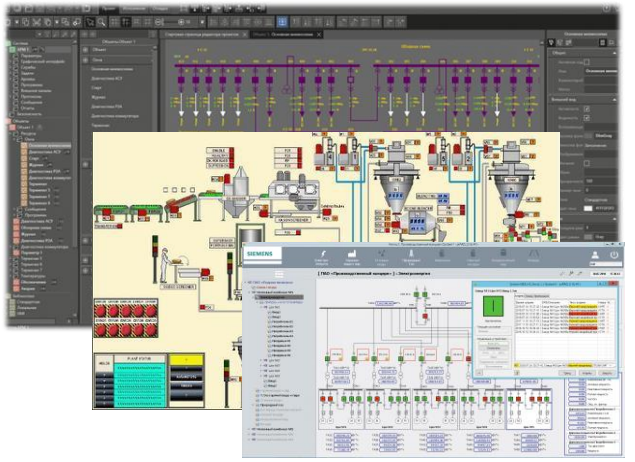
KepServerEX



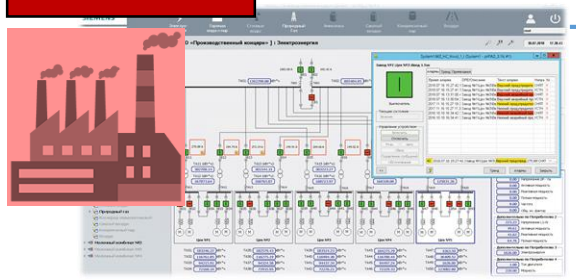
Коннектор

info-Diode

Коннектор
OPC UA сервер



WINCC OA

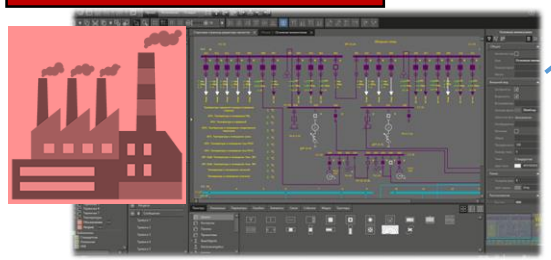


Коннектор
OPC UA

info-Diode

Централизованные
диспетчерские
Ситуационные центры

MasterSCADA 4D



Коннектор
OPC UA

AMT GROUP

Линейка решений для комплексной защиты КИИ

1. **АК InfoDiode** - базовое, сертифицированное ФСТЭК УД (4), аппаратное решение, гарантирующее защиту на аппаратном уровне и эффективно решающее задачу по передаче UDP, Syslog, SPAN трафика за пределы КИИ.

2. **АПК InfoDiode PRO** – сертифицированное ФСТЭК УД (4) решение для передачи значимых файловых потоков, дистрибутивов, реплик ВМ и баз данных, электронной почты, бэкапов и т.п. из доверенного сегмента вовне.

3. **АПК InfoDiode SMART** – новое решение для передачи за пределы периметра КИИ промышленных и специфических протоколов, в том числе видео, для интеграции SCADA систем, организации удаленных ситуационных центров за границей периметра, в условиях гарантированной изоляции КИИ

АППАРАТНО-ПРОГРАММНЫЕ РЕШЕНИЯ INFORELAY

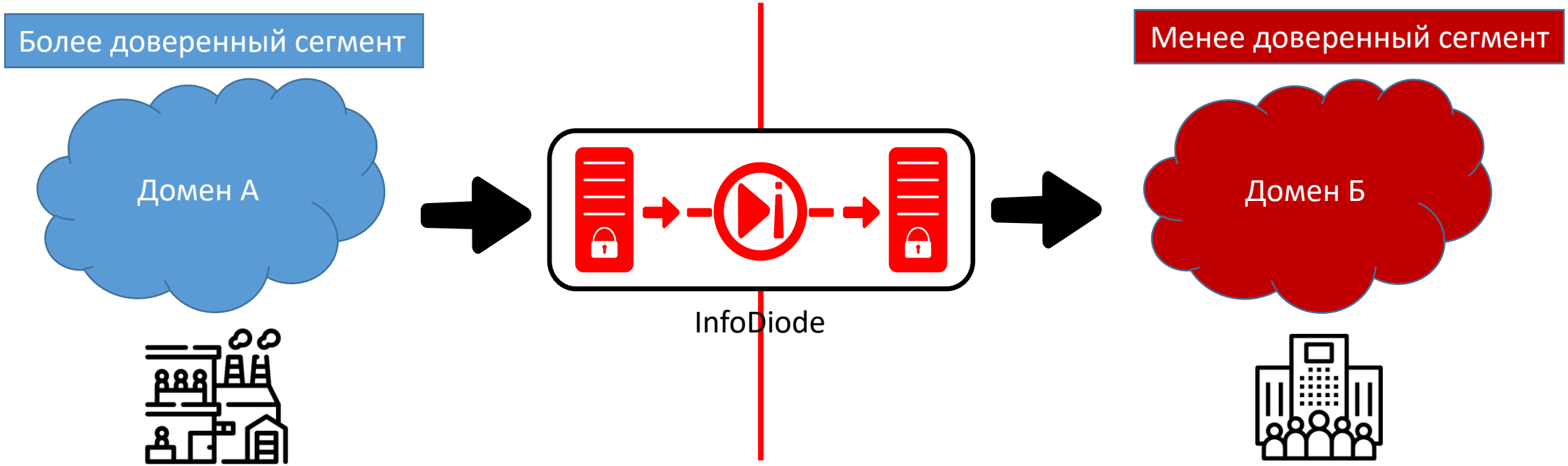
АПК InfoRelay - устройство для организации временного канала доступа

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
- **Аудит операций включения и аудит неисправности** – фиксация фактов включения, отдельные роли: Администратор и Аудитор
- **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

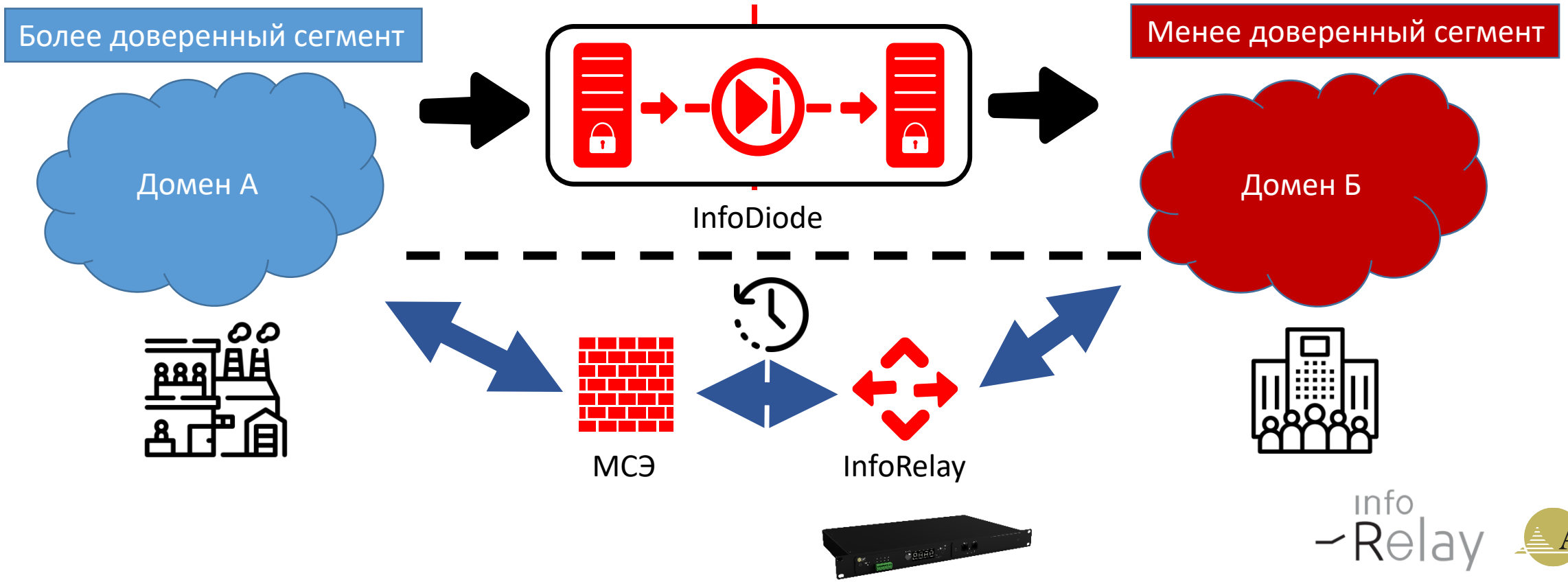
Исходный сценарий изоляции КИИ с InfoDiode

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



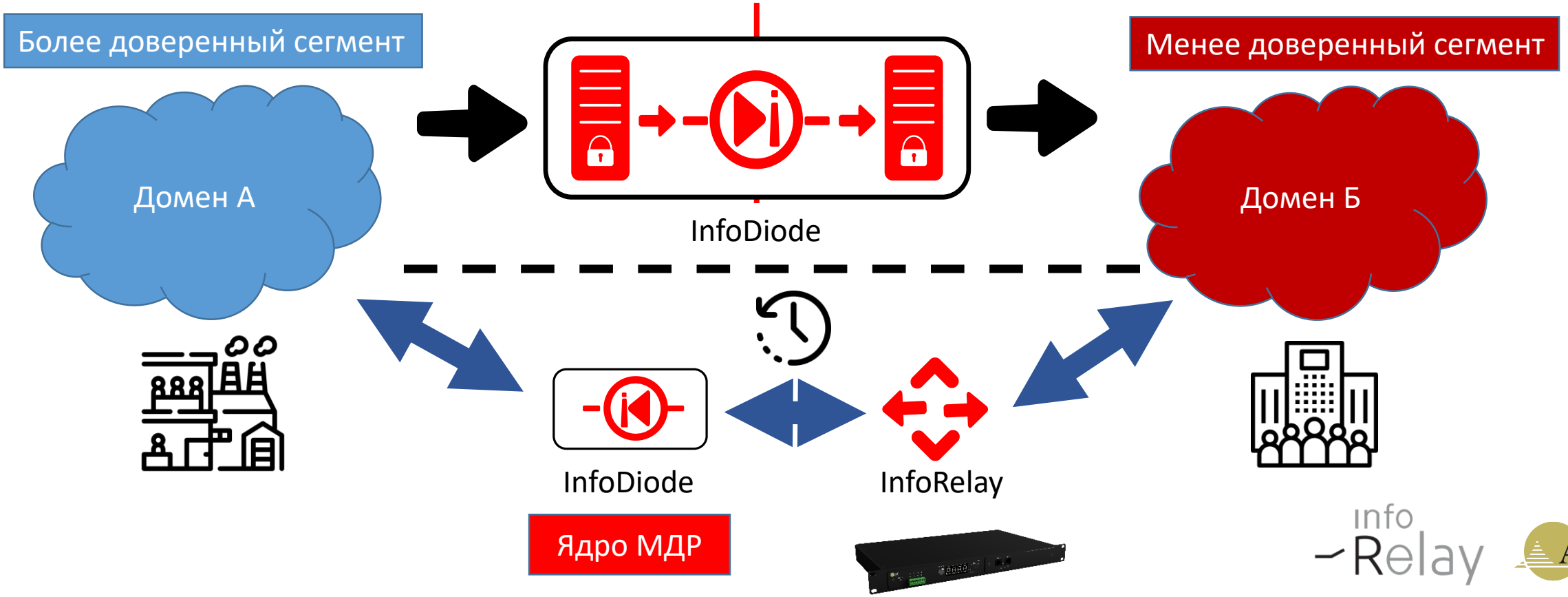
Применение InfoRelay совместно с InfoDiode и МСЭ

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



АПК InfoRelay – спорные практики

- **Длительный срок (таймер) каждого включения InfoRelay** - выше риск компрометации защищаемого сегмента
- **InfoRelay находится большой % времени во включенном состоянии - риск компрометации защищаемого сегмента**
  - Лучше 99% процентов находится в защищенном состоянии и 1% в незащищенном
- **Сильно регламентированный характер включения InfoRelay (расписание)** - выше риск компрометации защищенного сегмента
- **Больше сторонних средств, которые определяют включение InfoRelay** - выше риск компрометации сегмента за счет случайного выхода из строя внешнего элемента управления
- **Недостаточный контроль за физическим доступом к InfoRelay** – выше риск «неогранизованного» сопряжения сегментов

КИОСКИ ДАННЫХ НА БАЗЕ INFODIODE - БЕЗОПАСНАЯ ПЕРЕДАЧА ДАННЫХ МЕЖДУ ДОМЕНАМИ

Решение для безопасной передачи файлов между доменами – передача из общественных мест

Что это

АПК SecureKiosk tower

Как применять

- «Единое окно» в общедоступном месте для безопасной файловой передачи между доменами через InfoDiode

Преимущества

- Комплексное решение с InfoDiode
- Интеграция с СКУД, видеонаблюд.
- Реализация концепции ZeroTrust
- Можно ставить два и более киосков
- Могут быть киоски на прием и на передачу

Решение для безопасной передачи файлов между доменами – рабочее место сотрудника

Что это

АПК SecureKiosk desktop

Как применять

- Рабочее место сотрудника для передачи файлов -в или –из закрытого сегмента через InfoDiode

Преимущества

- Комплексное решение с InfoDiode
- Реализация концепции ZeroTrust
- Можно ставить два и более
- Могут быть рабочие места на прием и передачу
- Не требует больших аппаратных мощностей

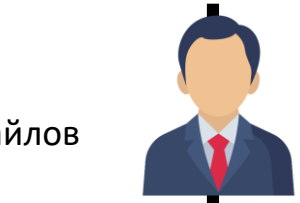
«Киоски данных» и автономные системы передачи данных являются частью междоменных решений

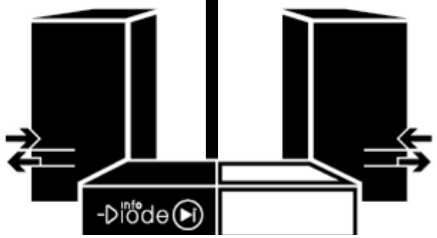
Сокрытие сети
Разрыв протоколов
Отсутствие обратной связи

Более доверенная сеть
Технологическая сеть
Закрытая сеть

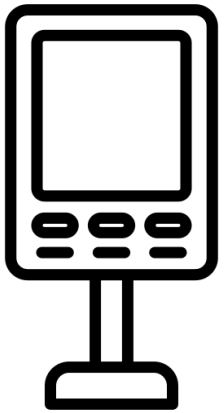
Передача файлов

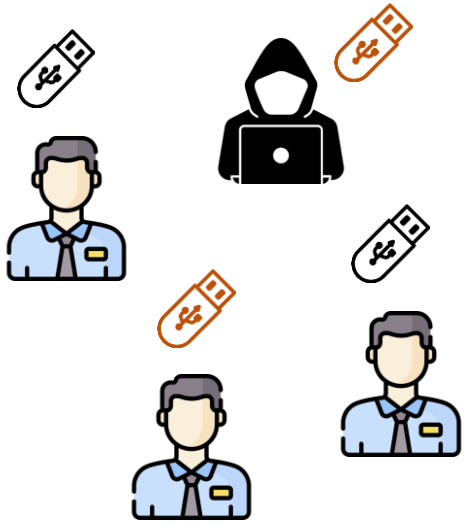
Передача файлов





АПК InfoDiode PRO





Пользователи с носителями информации

Песочница
Антивирус
Криптопровайдер

обновления, данные из внешних систем, данные для архивирования и накопления, запросы к данным…

ЛИЦЕНЗИИ И ПОДДЕРЖКА ВНЕДРЕНИЯ INFODIODE

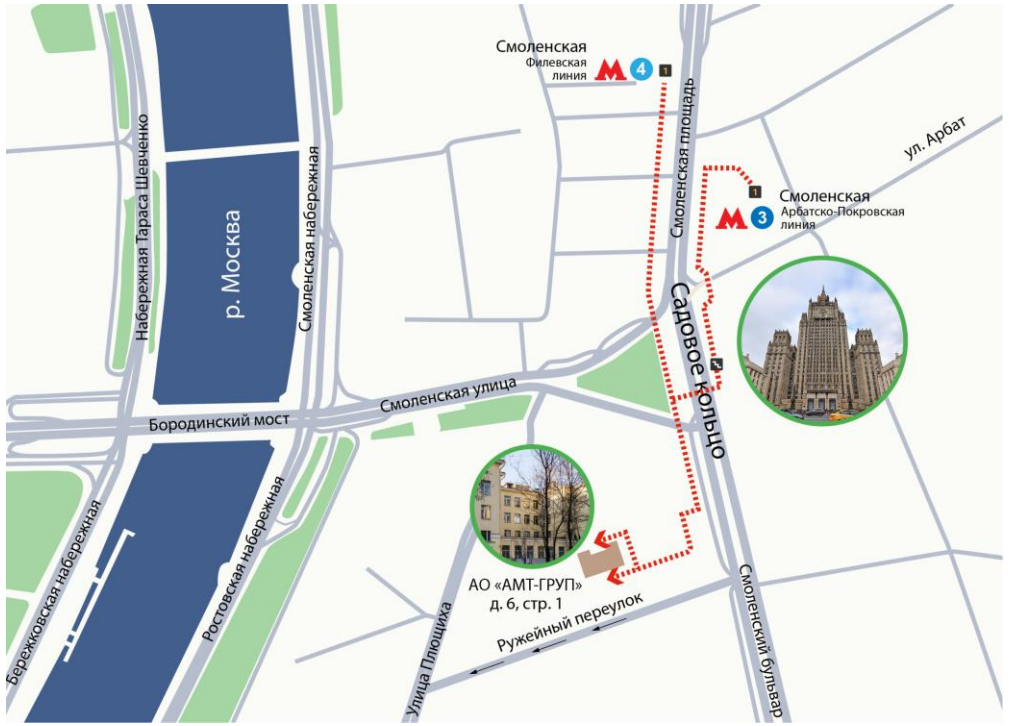
Лицензионная политика и комплексные решения от АМТ-ГРУП

- Состав спецификации
  - Оборудование – комплект, производство АМТ-ГРУП + лицензии на ПО (бессрочные и полнофункциональные)
  - Техническая поддержка оборудования и ПО
  - Отдельно компоненты для формирования ЗИП склада (без покупки дополнительного ПО)
  - Работы по внедрению и интеграции

- Техническая поддержка - варианты
  - 8x5 или 24x7
  - Комбинация – ПО 24x7, замена оборудования 8x5
  - ЗИП для клиента или только ремонт оборудования
  - Выезд технического специалиста для ремонта

Как с нами связаться

- 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!