28.08.2024

АМТ-ГРУП

Система однонаправленной передачи данных InfoDiode

Содержание

AMT GROUP

ПРОБЛЕМЫ И АКТУАЛЬНЫЕ УГРОЗЫ

Современная организация уже давно не изолированный сегмент

- Типовое предприятие 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

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

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

ВАРИАНТЫ ЗАЩИТЫ СЕТЕЙ

Варианты защиты сегментов сети не ограничиваются только Firewall или воздушным зазором

Типовые варианты защиты:

- Использование программных средств, прежде всего - межсетевых экранов Firewall

- Физическая изоляция сегментов сети – «воздушный» зазор

Каждый из вариантов имеет свои преимущества и недостатки

Программные решения – не всегда надежный инструмент защиты критической инфраструктуры и ОПО

Тип кибератаки	InfoDiode	Решения на базе ПО
1) Фишинг / скачивание ПО с помощью системы drive-by-download		
2) Социальная инженерия – кража пароля / регистраторы нажатий клавиш		
3) Компрометация контроллера домена – создание учетной записи хоста или МСЭ		
4) Атака на незащищенные серверы – SQL-инъекция / DOS / buffer-overflow		
5) Атака на незащищенных клиентов - скомпрометированные веб- и файловые серверы		
6) Перехват сеанса – MIM / кража HTTP-файлов cookie / внедрение команд		
7) Совместный доступ к VPN / распространение вредоносного ПО		
8) Уязвимости МСЭ – ошибки / нулевые дни / пароль по умолчанию / недостатки решений		
9) Ошибки и упущения – неверные правила/конфигурации МСЭ		
10) Подделка IP–адреса		

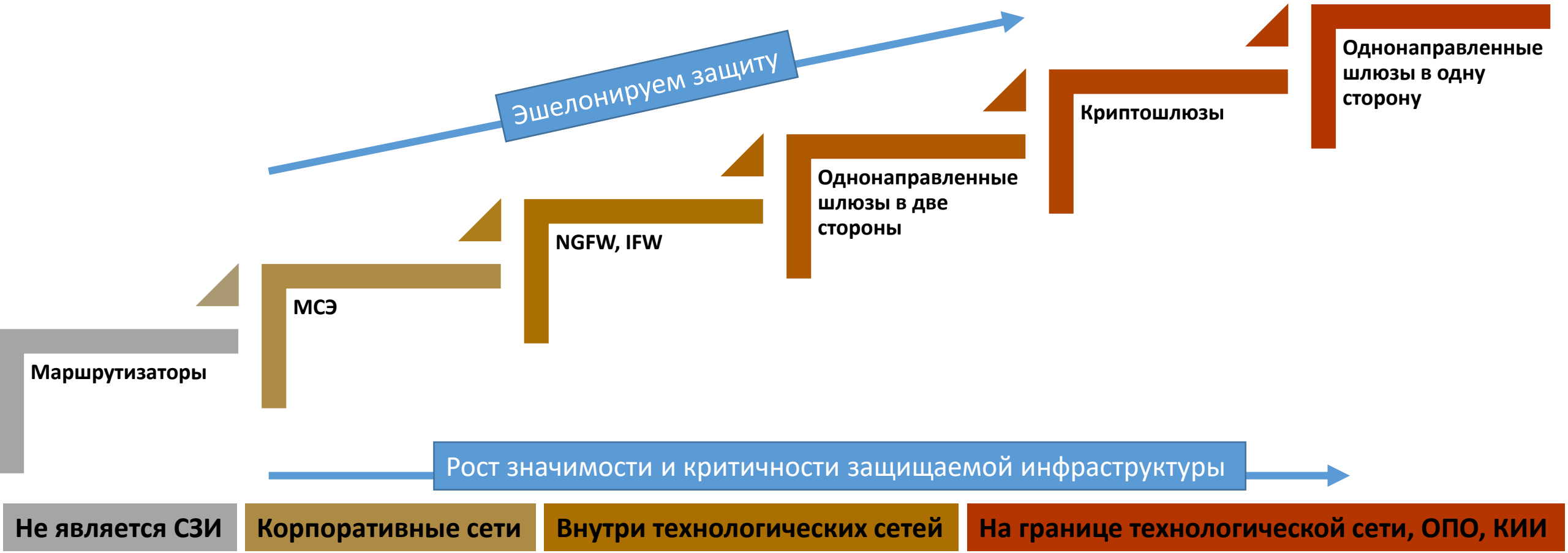
Невозможно

Возможно

Относительно легко

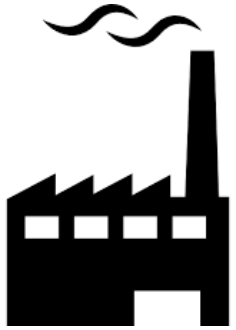
AMT GROUP

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



Сегментация сети – локализуем управление, передаем данные

УПРАВЛЕНИЕ



КИИ

Автономность функций управления в условиях отсутствия связи с внешним миром

ЧАСТЬ ДАННЫХ

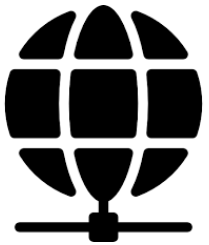
КОРП. СЕТЬ

Данные и протоколы прикладного уровня необходимые для решения задач

ЧАСТЬ ДАННЫХ

СМЕЖНЫЕ СЕТИ
(ДР. ОРГАНИЗАЦИИ, ВЕНДОРЫ И Т.П)

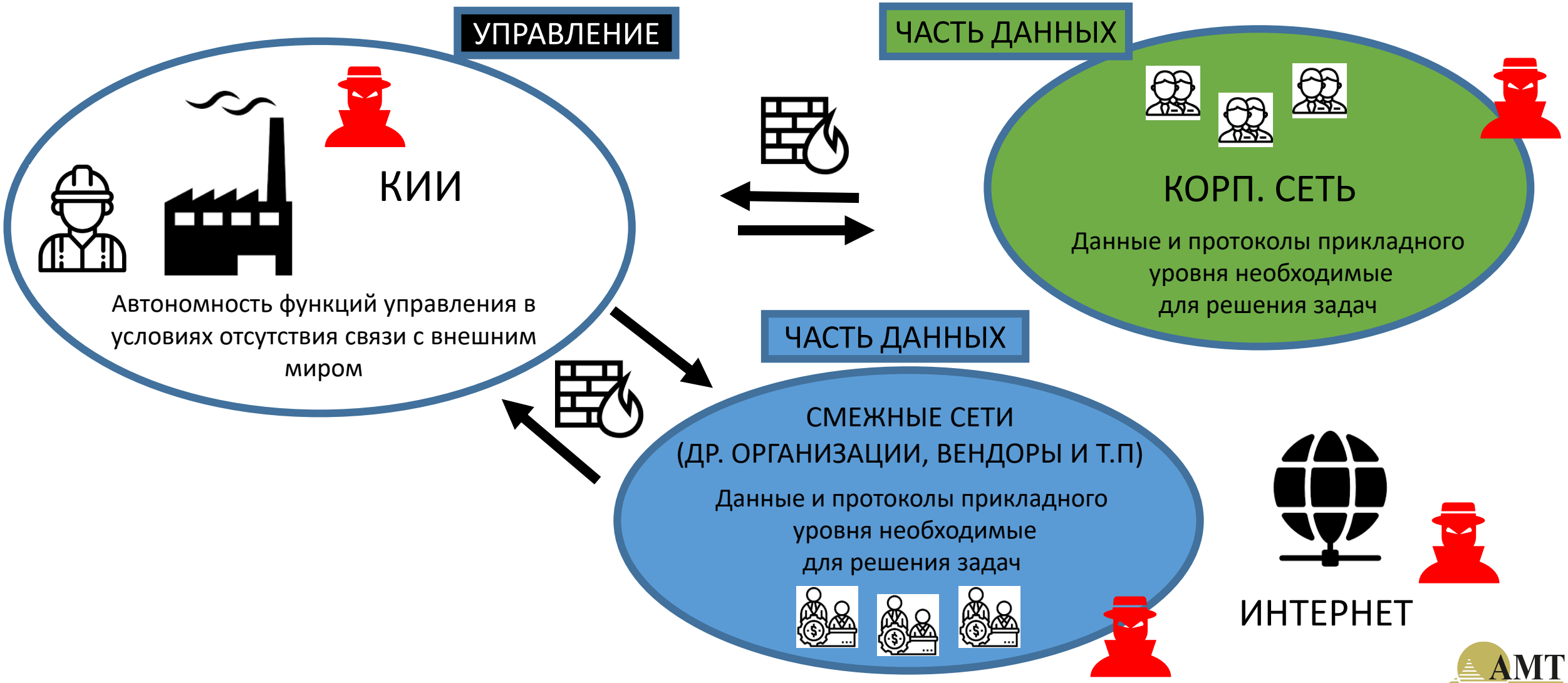
Данные и протоколы прикладного уровня необходимые для решения задач



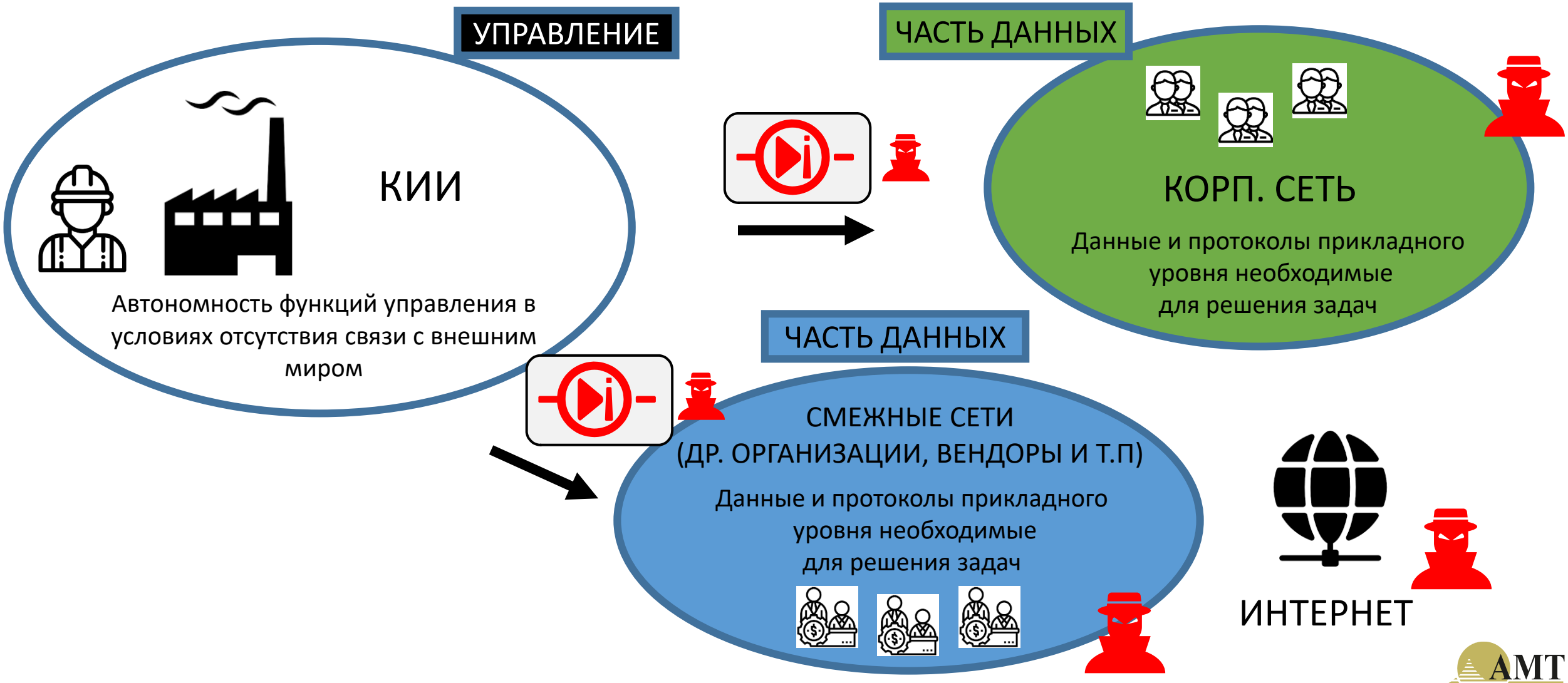
ИНТЕРНЕТ

AMT GROUP

Сети, изолированные программными решениями, достаточно уязвимы



Сети, изолированные аппаратными решениями – эффективно изолированные сети



РЕШЕНИЯ НА РЫНКЕ INFODIODE ОТ 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

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**

AMT GROUP

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

АПК InfoDiode позволяет соответствовать лучшим практикам по защите периметра КИИ, передавать файловый, промышленный и иной трафик

АПК INFODIODE PRO

Базовый вариант	Кластерный вариант
InProxy, OutProxy сервер	2 InProxy, 2 OutProxy сервера
АК InfoDiode, rack module	2 АК InfoDiode, rack module, Cluster
Форм фактор - 3U	Форм-фактор - 6U

Диод снаружи

АПК INFODIODE SMART

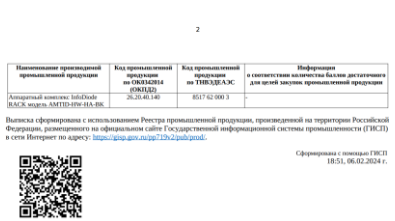
Базовый вариант
InProxy, OutProxy сервер
«диод внутри»
Форм фактор - 1U

Диод внутри

AMT GROUP

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



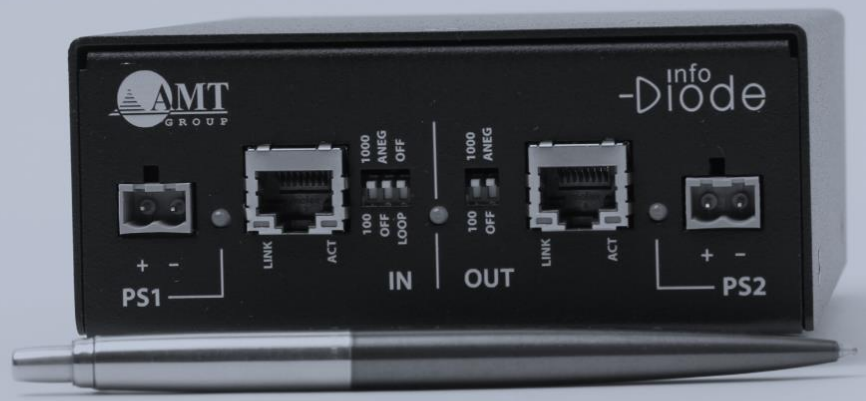
Продукты InfoDiode совместимы со многими СЗИ, АСУ ТП, ИТ решениями

Kaspersky
Private Security
Network

CyberLympha
DATAPK

Kaspersky
Industrial
CyberSecurity

АППАРАТНЫЕ РЕШЕНИЯ INFODIODE



Аппаратный комплекс InfoDiode – простое и эффективное решение для сегментации сети

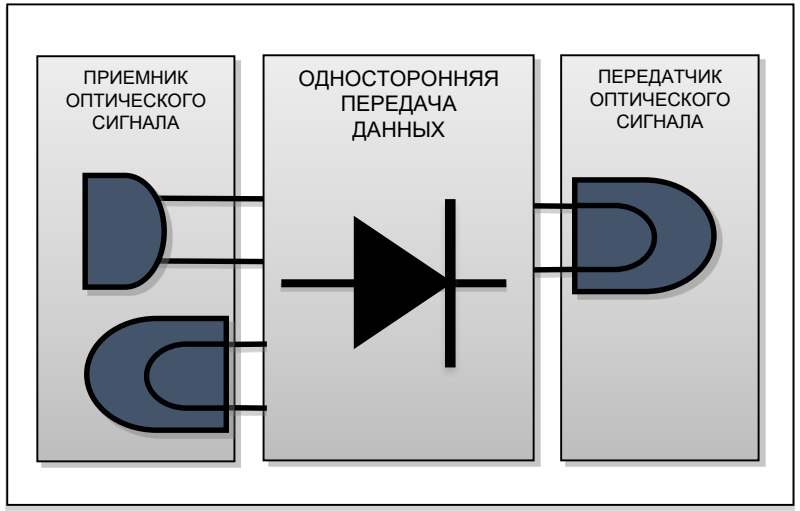
Аппаратная односторонняя передача данных

- 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

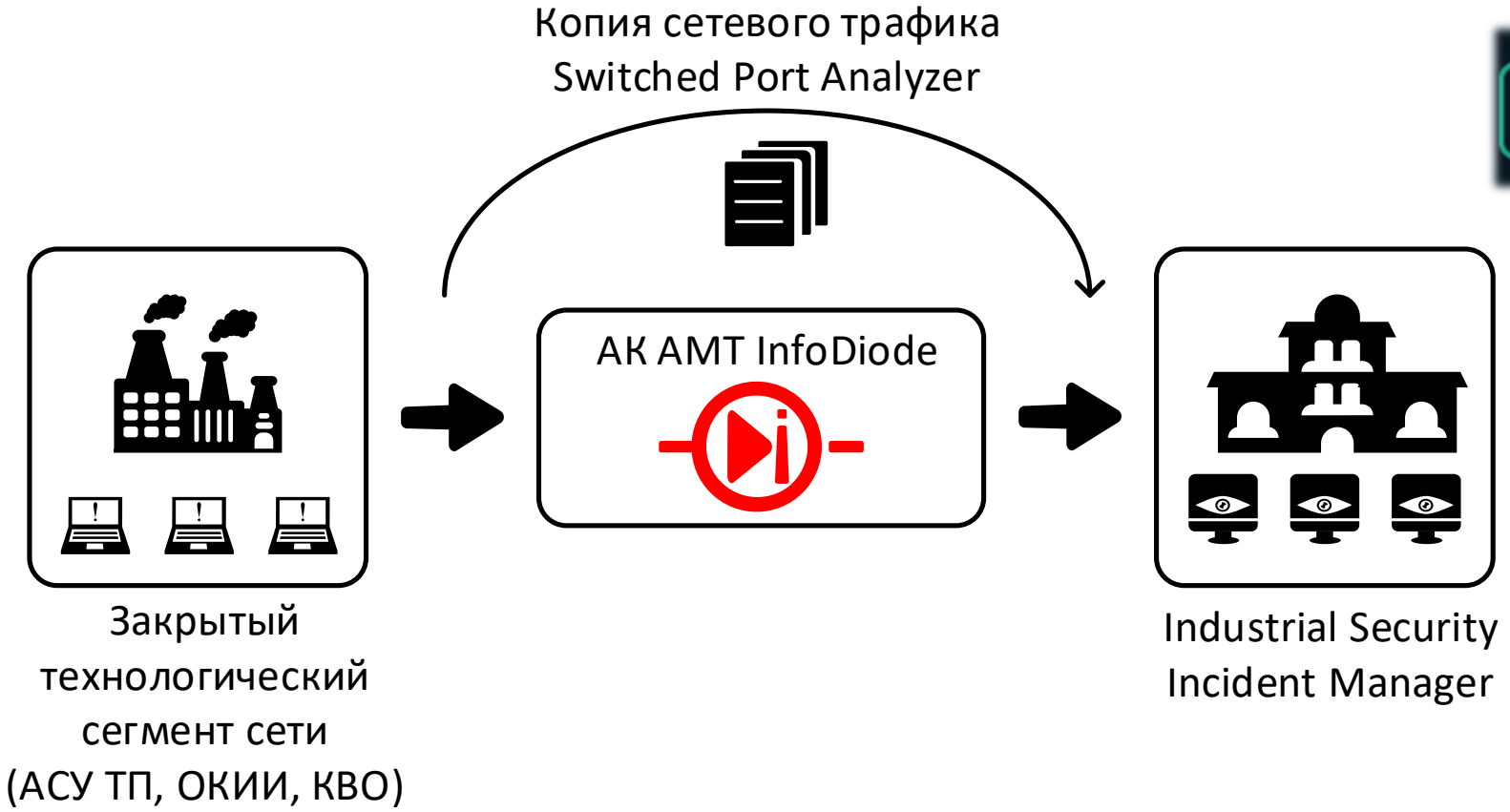
Возможно

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

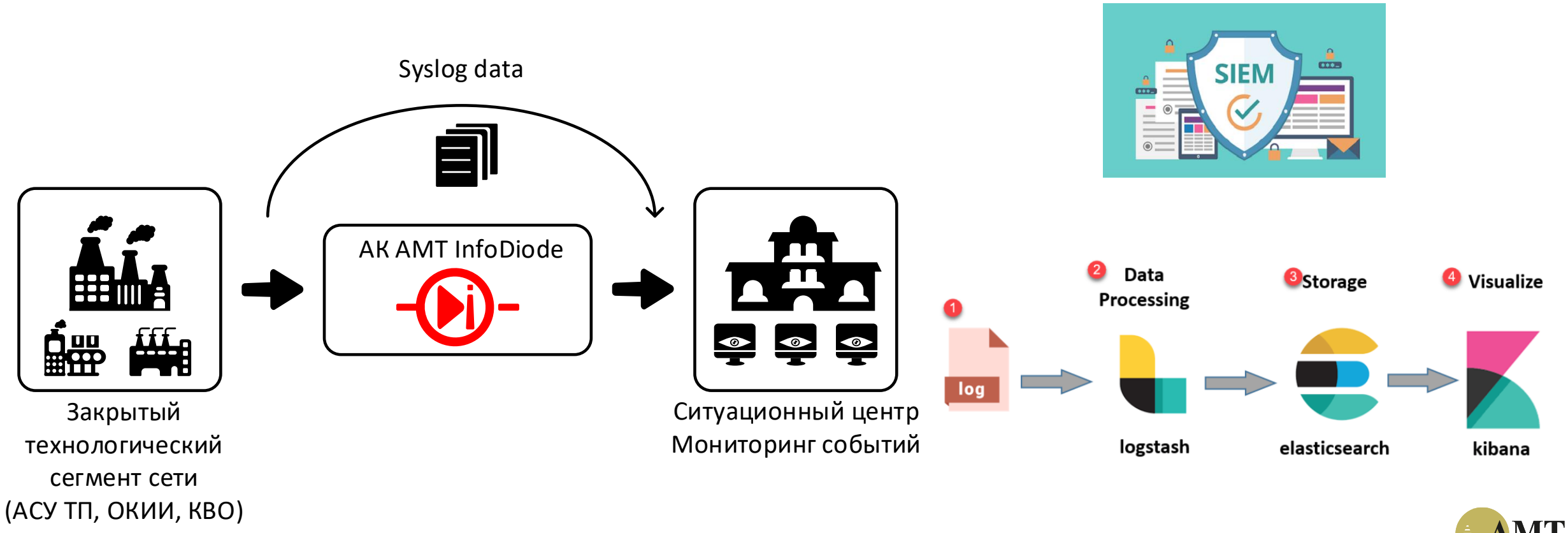
PT ISIM

Rhebo
Industrial Network Continuity

AMT GROUP

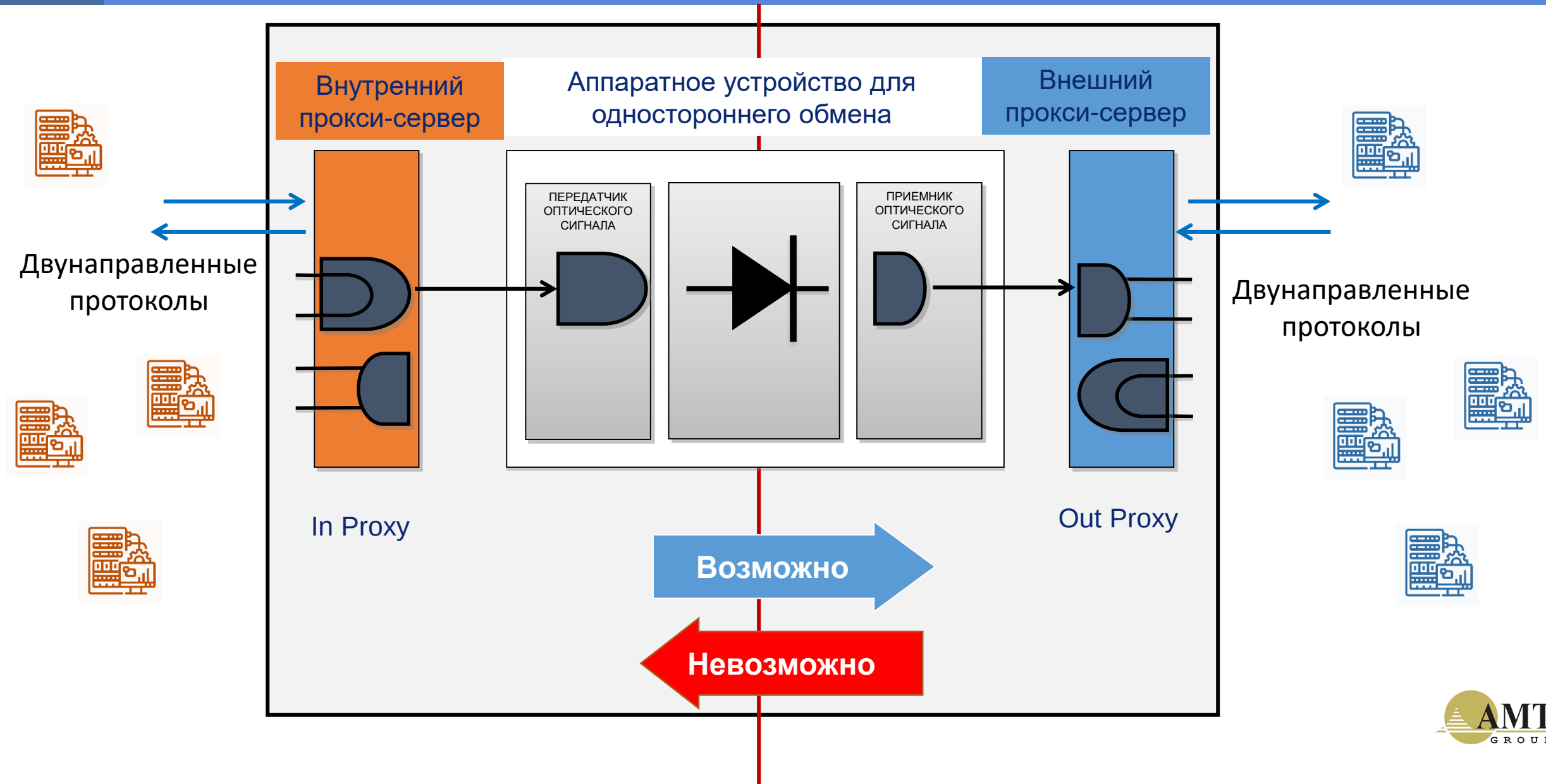
Передача данных для NOC и SOC через АК InfoDiode

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

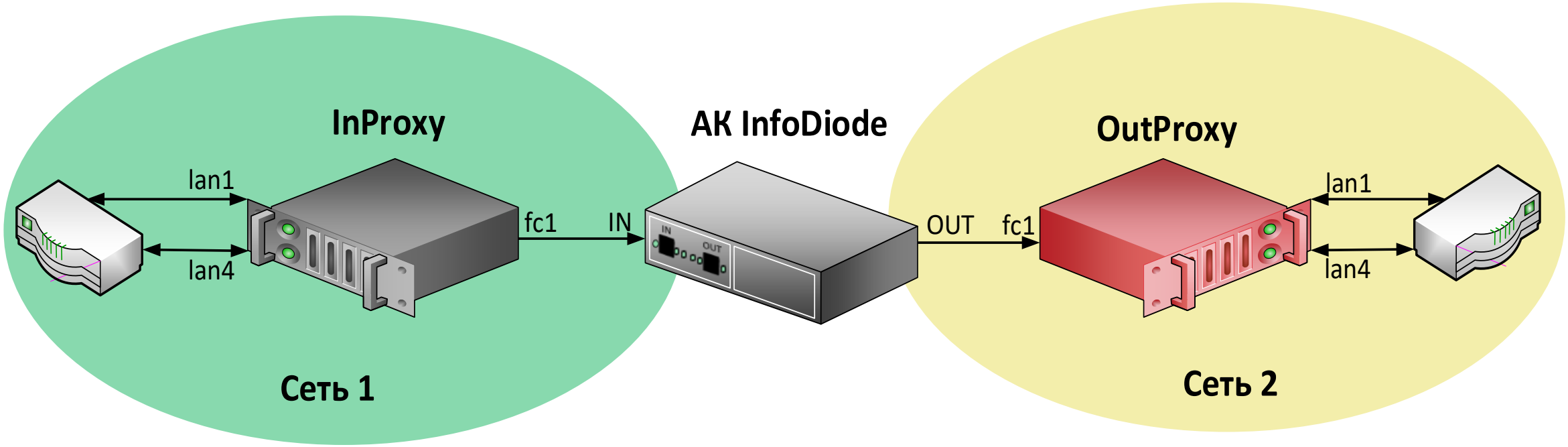


АППАРАТНО-ПРОГРАММНЫЕ РЕШЕНИЯ INFODIODE PRO

Решения InfoDiode позволяют передавать двунаправленные протоколы, терминируя их на себе

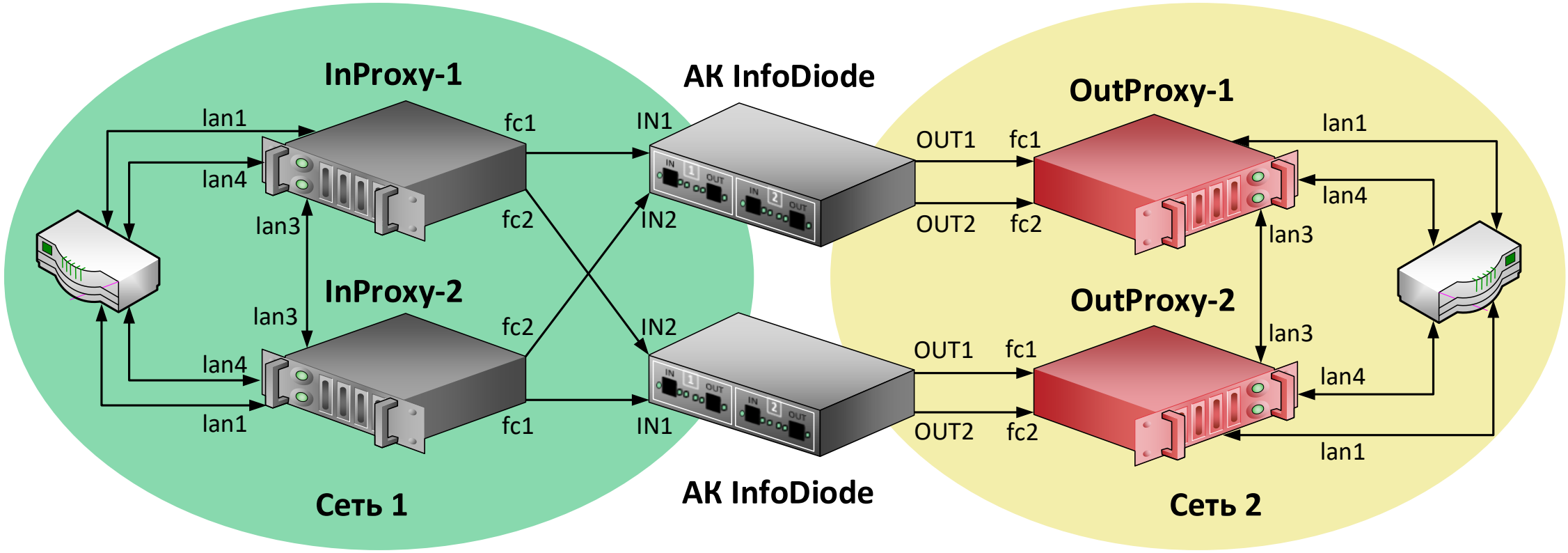


Базовый вариант АПК InfoDiode PRO

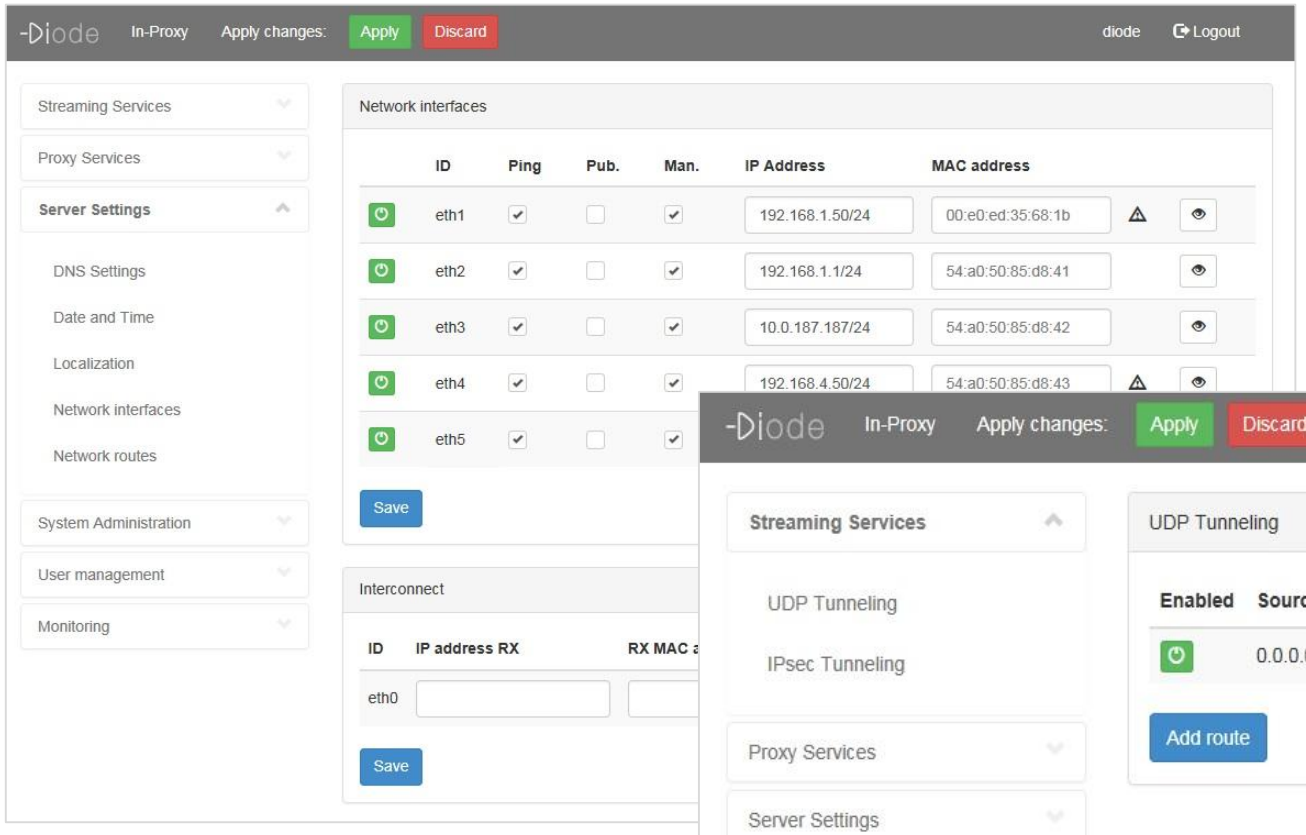


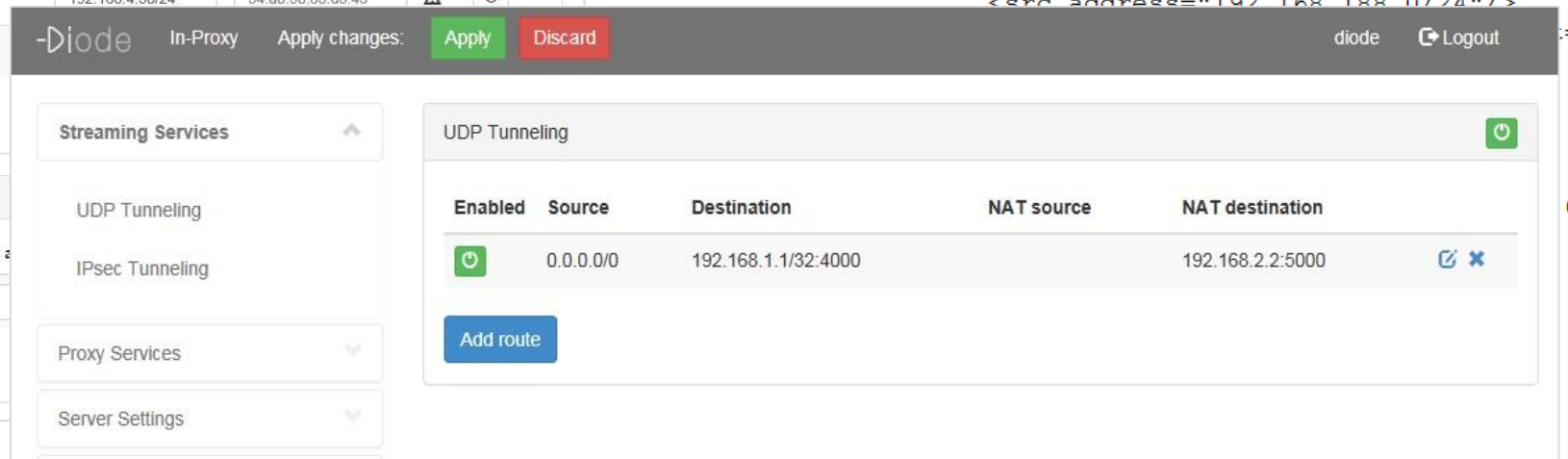
Кластерный вариант АПК InfoDiode PRO – отказоустойчивый вариант

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"/>
```

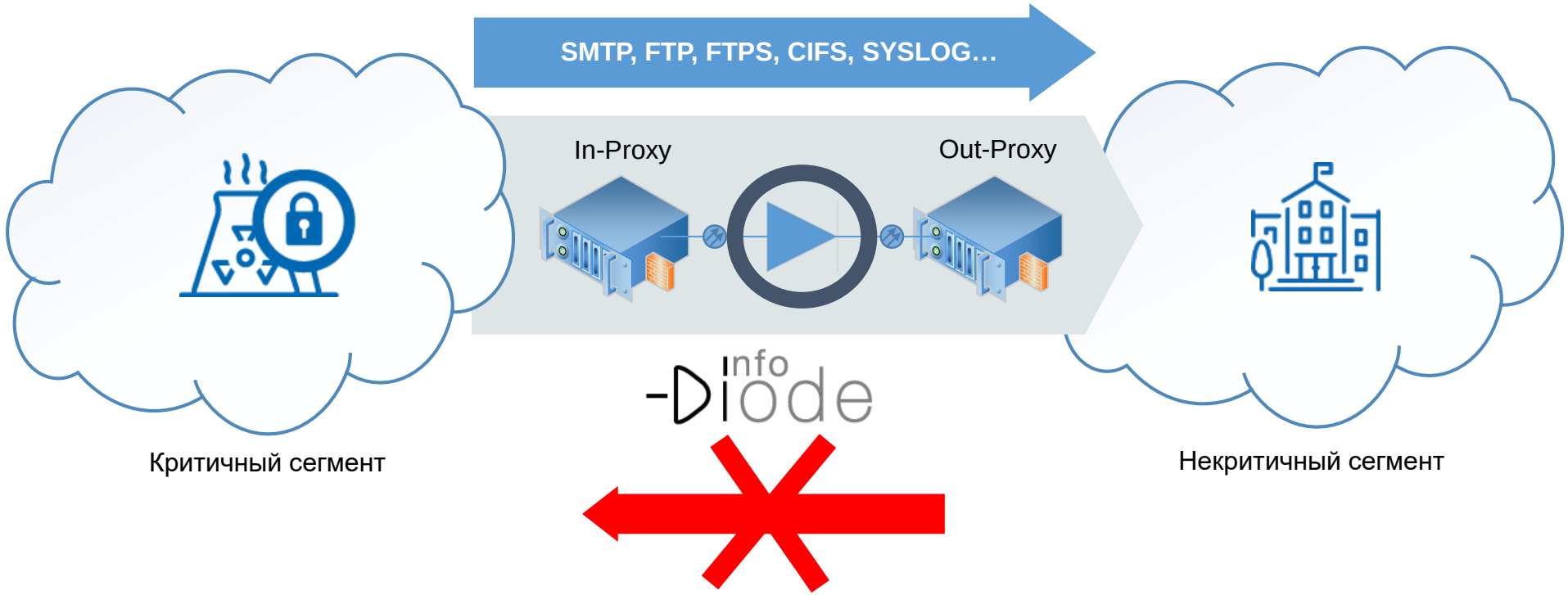
- User-friendly Web-интерфейс (русская и английская версии)
- Возможность управления посредством CLI и XML
- Специальный режим защиты против случайных изменений

AMT GROUP

Возможности и параметры АПК InfoDiode PRO

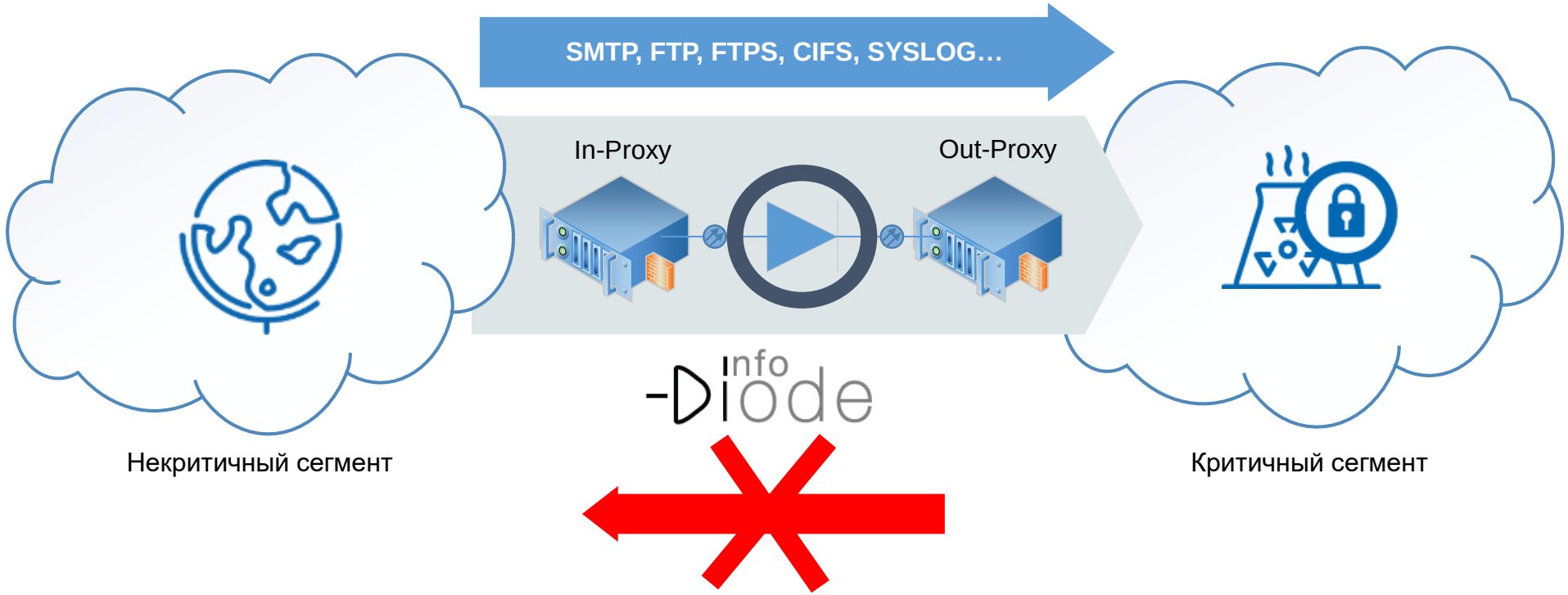
- Производительность UDP - 900 Mbps
- Производительность прокси сервисов – 300 Mbps
- Поддержка протоколов FTP/FTPS, CIFS, SMTP, SFTP и др.
- Приоритезация передачи данных и потоков
- Помехоустойчивое кодирование
- Configuration/system backup
- Syslog/SIEM интеграция
- NTP синхронизация
- Интеграция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

Сценарий 1 - Однонаправленная выгрузка данных из критичного технологического сегмента



- **Выгрузка** данных из критичных сегментов
- Нужно исключить **информационные воздействия извне**
- Нужно исключить возможность управления объектом

Сценарий 2 - Однонаправленная загрузка данных в защищаемую информационную систему



- **Загрузка** данных в конфиденциальные информационные системы
- **Нельзя, чтобы данные «утекли»** из крит. информационных систем
- Нужно исключить возможность управления объектом

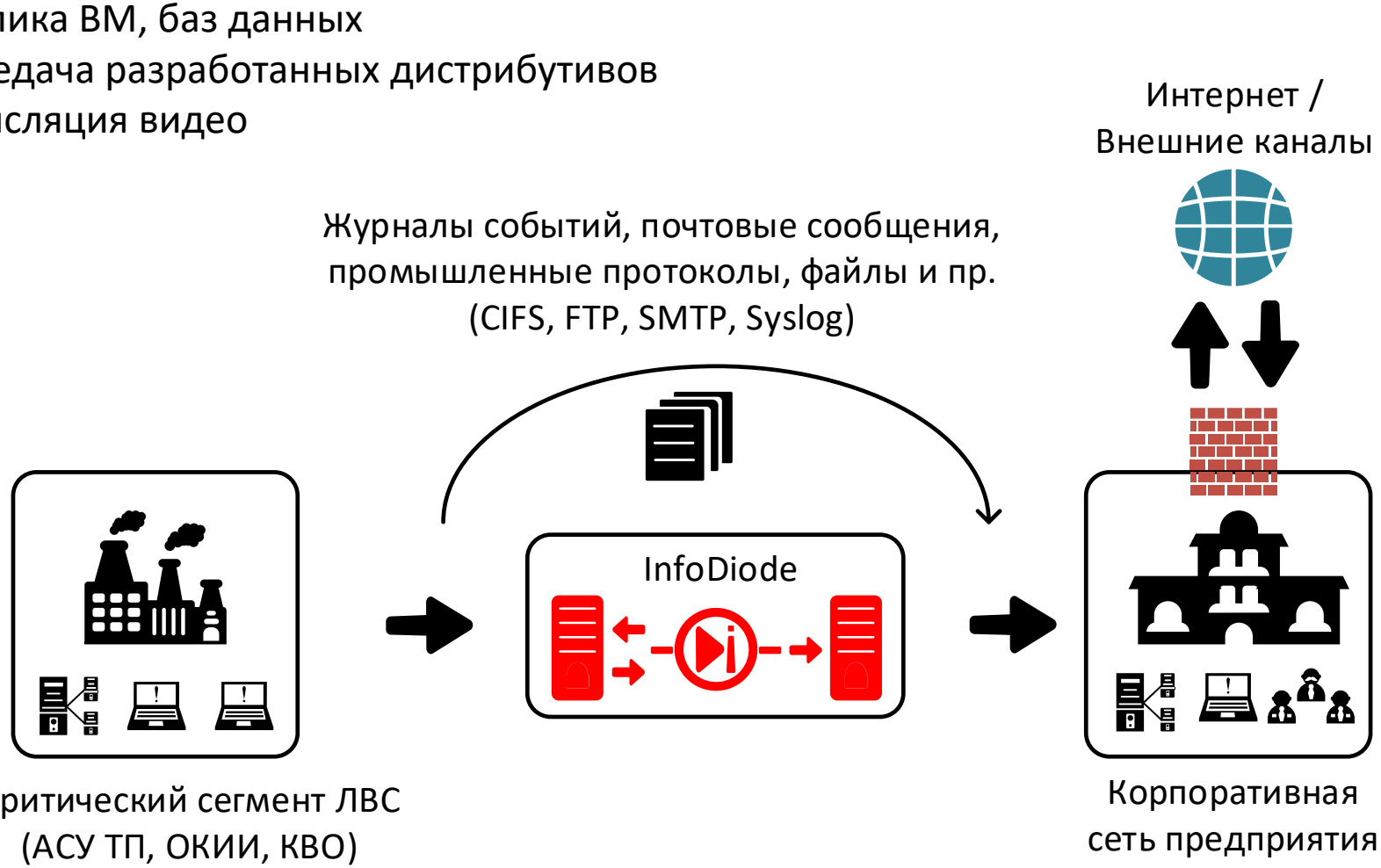
Передача данных и реплик из защищенного сегмента через АПК InfoDiode PRO

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.

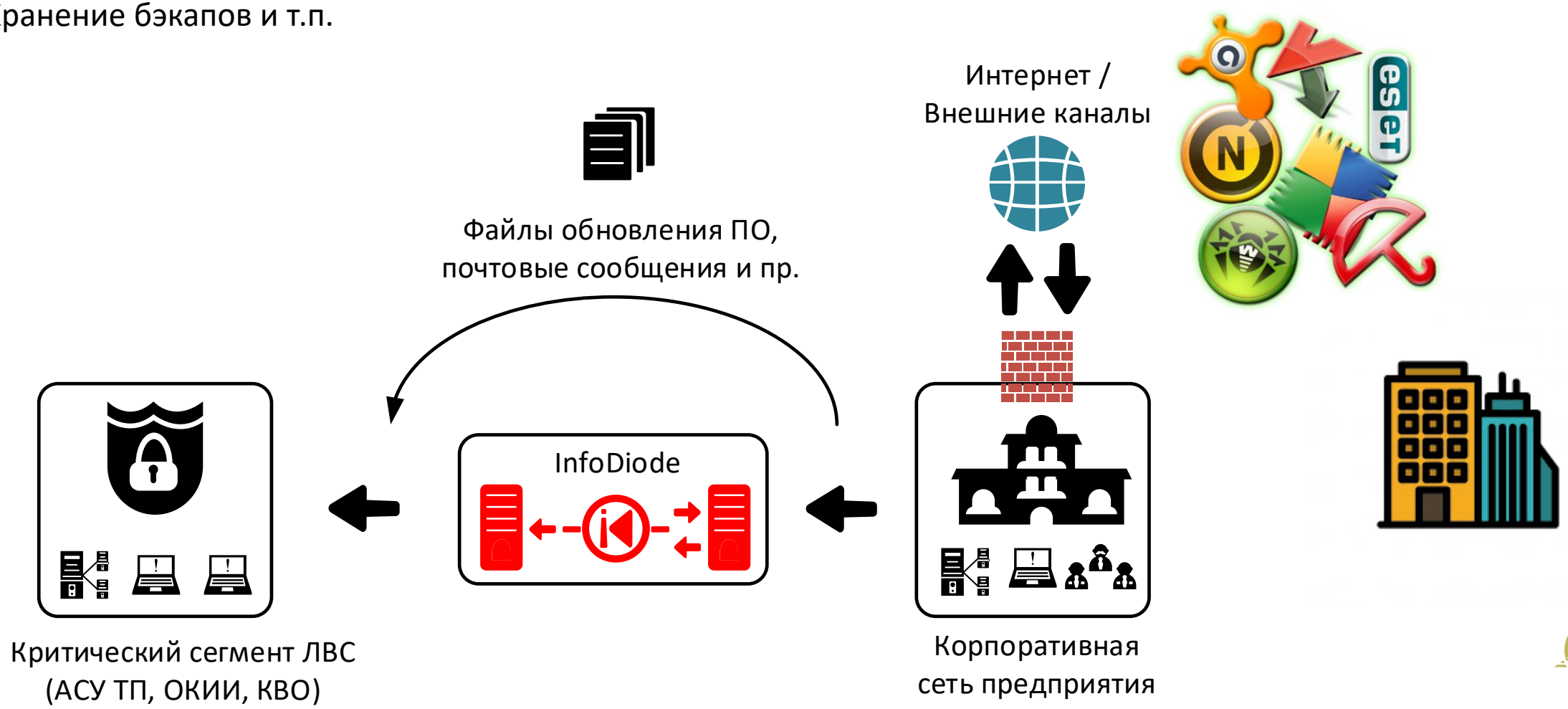


Получение обновлений и данных в защищаемый сегмент через АПК InfoDiode PRO

Вариант 2. Импорт данных

В данном сценарии обеспечивается гарантия конфиденциальности защищаемых данных.

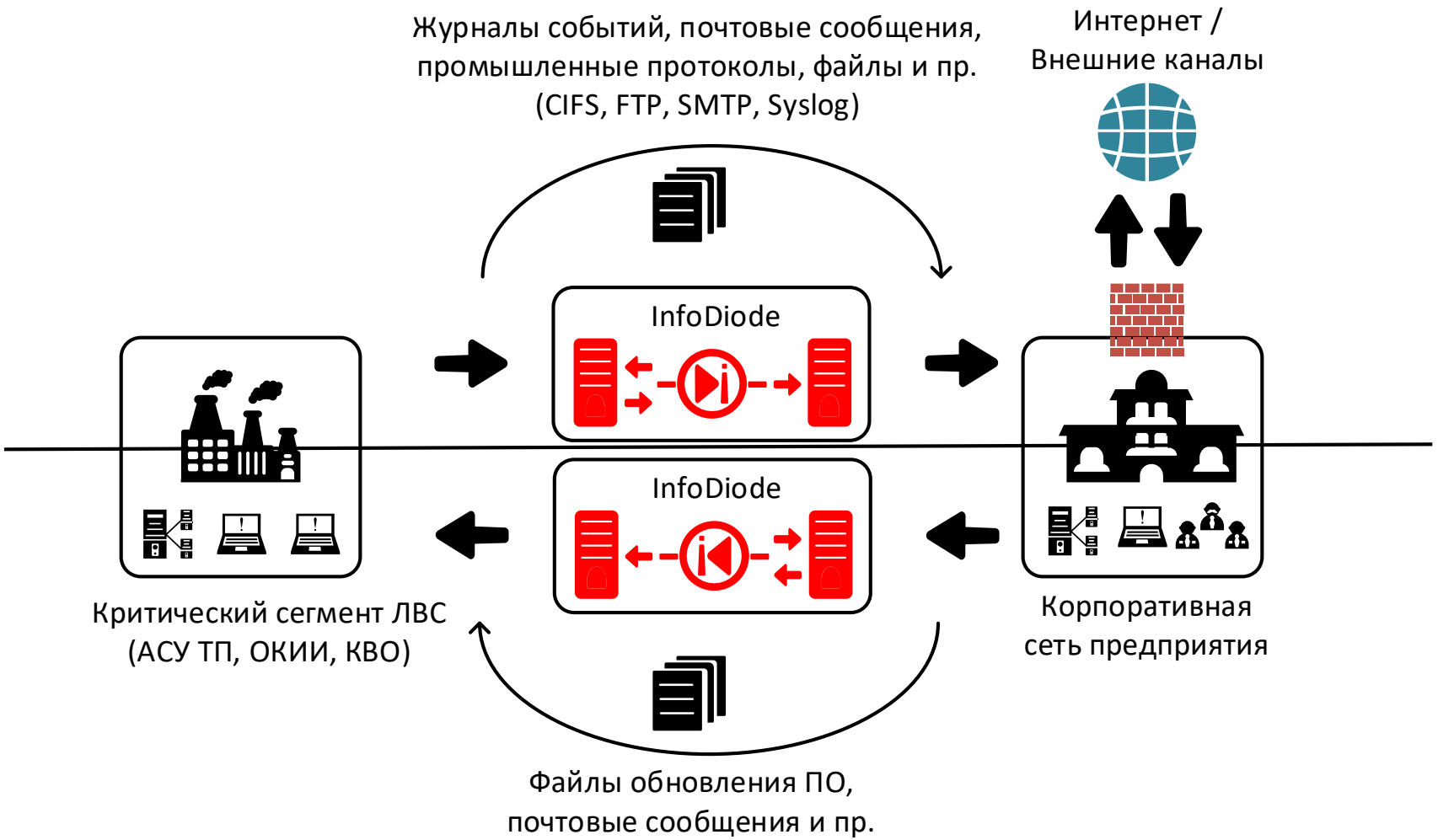
- Загрузка обновлений
- Хранение бэкапов и т.п.



Асинхронный обмен с подтверждением через АПК InfoDiode PRO

Вариант 3. Одновременная выгрузка и загрузка данных

- Объединение варианта 1 и 2 для АПК InfoDiode
- Либо изолированные, либо синхронизированные контуры



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

Сценарии применения АПК InfoDiode SMART могут быть типизированы

1

Офис

Для руководства и внешних сотрудников

2

Агрегирующая SCADA, MES, ERP, Hist.

Контроль и мониторинг состояния «инфраструктуры»

3

СЦ, Министерство, ГИС

Отчетность и контроль ситуации

АСУ ТП

АСУ ТП локальная

Предприятие

Полевой уровень

Сценарии применения АПК InfoDiode SMART могут быть типизированы

4

Головной холдинг

Цепочки поставок и номенклатуры

Предприятие

5

Интернет

Патчи обновлений, получение информации

Организация

6

Вендоры, подрядчики

ТП, получение патчей, предоставление реплик

Предприятие

Полевой уровень

Сценарии применения АПК InfoDiode SMART могут быть типизированы

7

Подразделение: SOC, NOC, архивы

Контроль ИБ, сети, конфиденц. и резервные сегменты

Предприятие

8

Контрагенты (учебные заведения и т.п.)

Методически значимая информация, данные для исследований

Предприятие

9

Конечные потребители

Данные для инфоматов, визуальные панели,

Организация

Полевой уровень

Промышленные протоколы через InfoDiode SMART - уже реальность

Any
Allen-Bradley Suite
Aromat Suite
AutomationDirect Suite
Building Automation Suite
Contrex Suite
Cutler-Hammer Suite
DNP3 Suite
EFM Suite
Fanuc Focas Suite
Fisher ROC Suite
GE Suite
Honeywell Suite
IEC 60870-5 Suite
IT and Infrastructure Suite
Manufacturing Suite
Mitsubishi Suite
Modbus Suite
Oil and Gas Suite
Omron Suite
OPC Connectivity Suite
Power Suite
SattBus Suite
Siemens Plus Suite
Siemens Suite
Simatic Suite
Simulation Suite
SIXNET Suite
SNMP Suite
Thermo Westronics Suite

Промышленные протоколы

info-Diode

Конвертеры

Удаленные АРМ

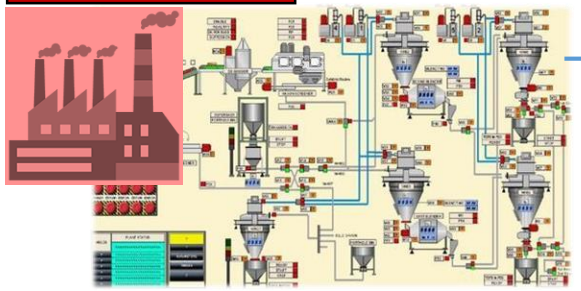
Ситуационные центры

ДОВЕРЕННЫЙ СЕГМЕНТ
Управление оборудованием

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

АПК InfoDiode SMART позволяет собирать данные SCADA за границами периметра

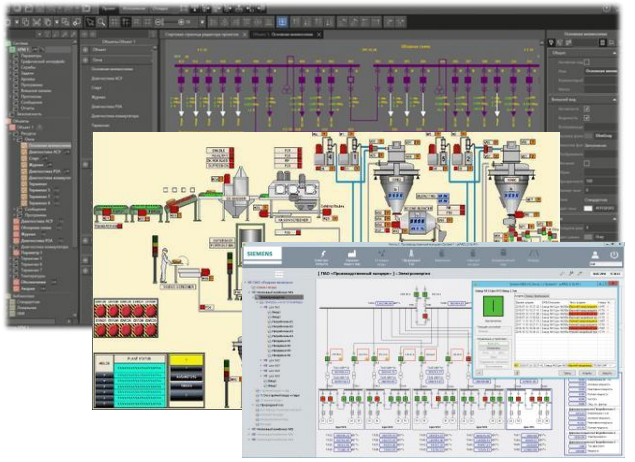
KepServerEX



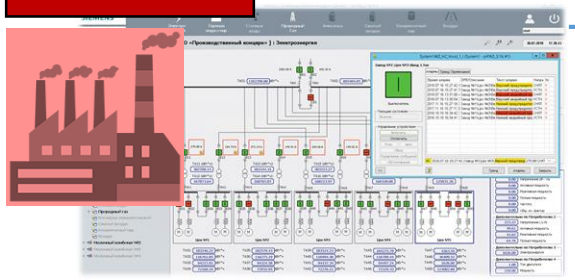
Коннектор

info-Diode

Коннектор OPC UA сервер



WINCC OA

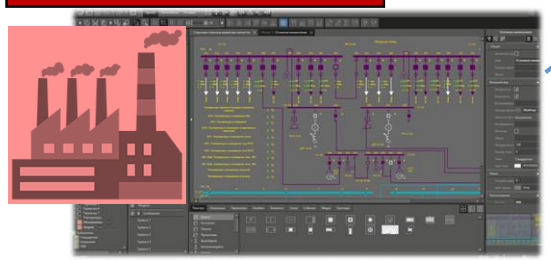


Коннектор OPC UA

info-Diode

Централизованные диспетчерские Ситуационные центры

MasterSCADA 4D



Коннектор OPC UA

AMT GROUP

АПК InfoDiode SMART дополняет линейку 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

Количество отраслей применения InfoDiode постоянно увеличивается

InfoDiode используется в:

- ТЭК
- Платежные системы
- Финансовые организации
- Силовые ведомства
- Производство
- Транспортные компании
- Энергетика
- др.

Банк России

РусГидро

Росфинмониторинг

Транснефть

РЖД

РОСЭНЕРГОАТОМ
ЭЛЕКТРОЭНЕРГЕТИЧЕСКИЙ ДИВИЗИОН РОСАТОМА

КРЭТ

sollers

ЮНИПРО

ЦИК

ЕВРОСИБЭНЕРГО

Генеральная прокуратура РФ

ФСТЭК

Министерство здравоохранения РФ

НСПК
НАЦИОНАЛЬНАЯ СИСТЕМА ПЛАТЕЖНЫХ КАРТ

Ростелеком

ERG

AMT GROUP

ЛИЦЕНЗИИ И ПОДДЕРЖКА ВНЕДРЕНИЯ INFODIODE

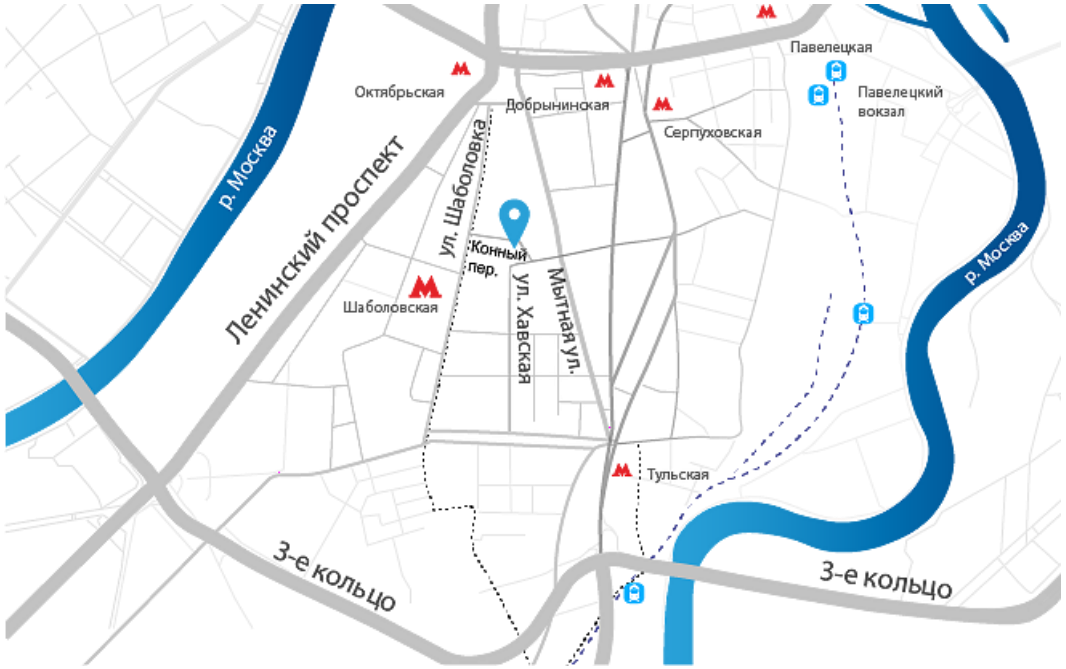
Лицензионная политика и комплексные решения от АМТ-ГРУП

- 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!