



Защита
объектов КИИ

Однонаправленная
передача данных

Сегментирование
сетей АСУ ТП

Экспорт
видеопотоков в
ситуационный
центр



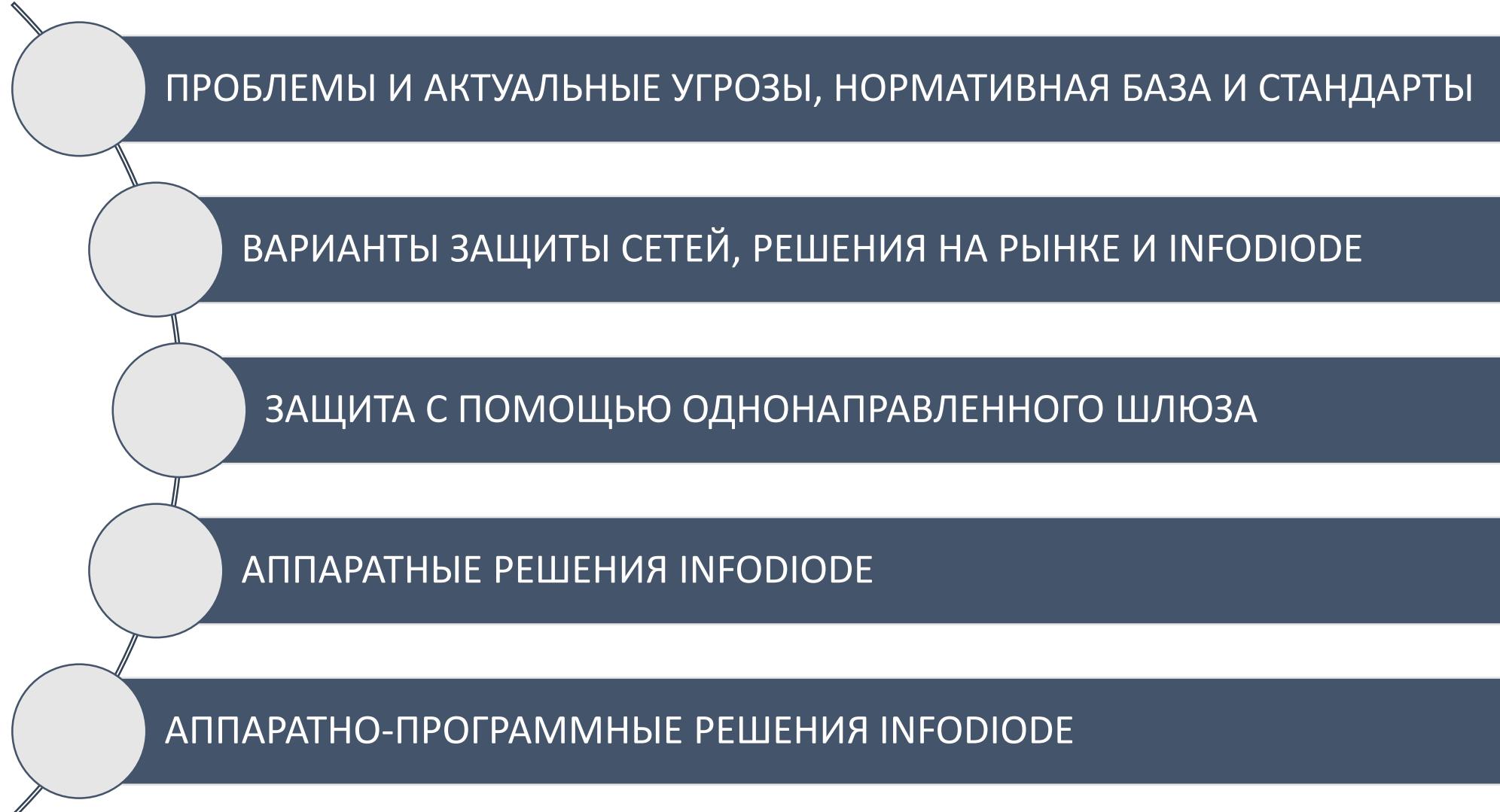
IT

15.03.2024

АМТ-ГРУП

Система однонаправленной
передачи данных InfoDiode

Содержание



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



Последствия атак – существенны!

- Системы, управляющие физическими объектами и процессами
 - Энерго- и электроснабжение
 - Водоснабжение и системы охлаждения
 - Вентиляция
 - Промышленное оборудование
 - Системы физической защиты
 - Системы программной защиты
 - Персональные данные
 - Сети передачи критических данных
 - Связь



Конфиденциальность
Целостность
Доступность

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**

- 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»



Общие тренды

Страновые особенности

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, односторонняя 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 | Скрытие 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

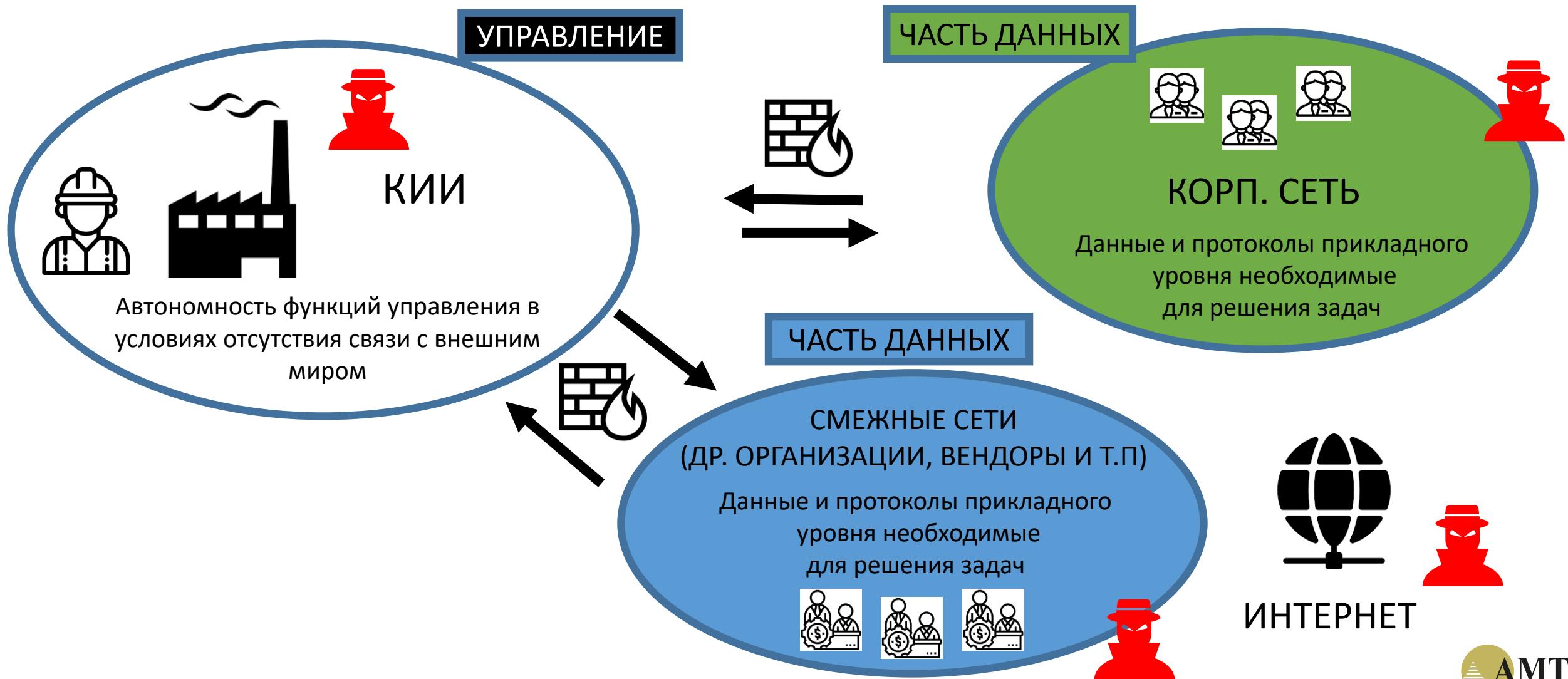
Эффективно противодействовать атаке – означает **предотвратить** конкретные этапы/последствия атаки **каждый раз**, когда такая атака осуществляется



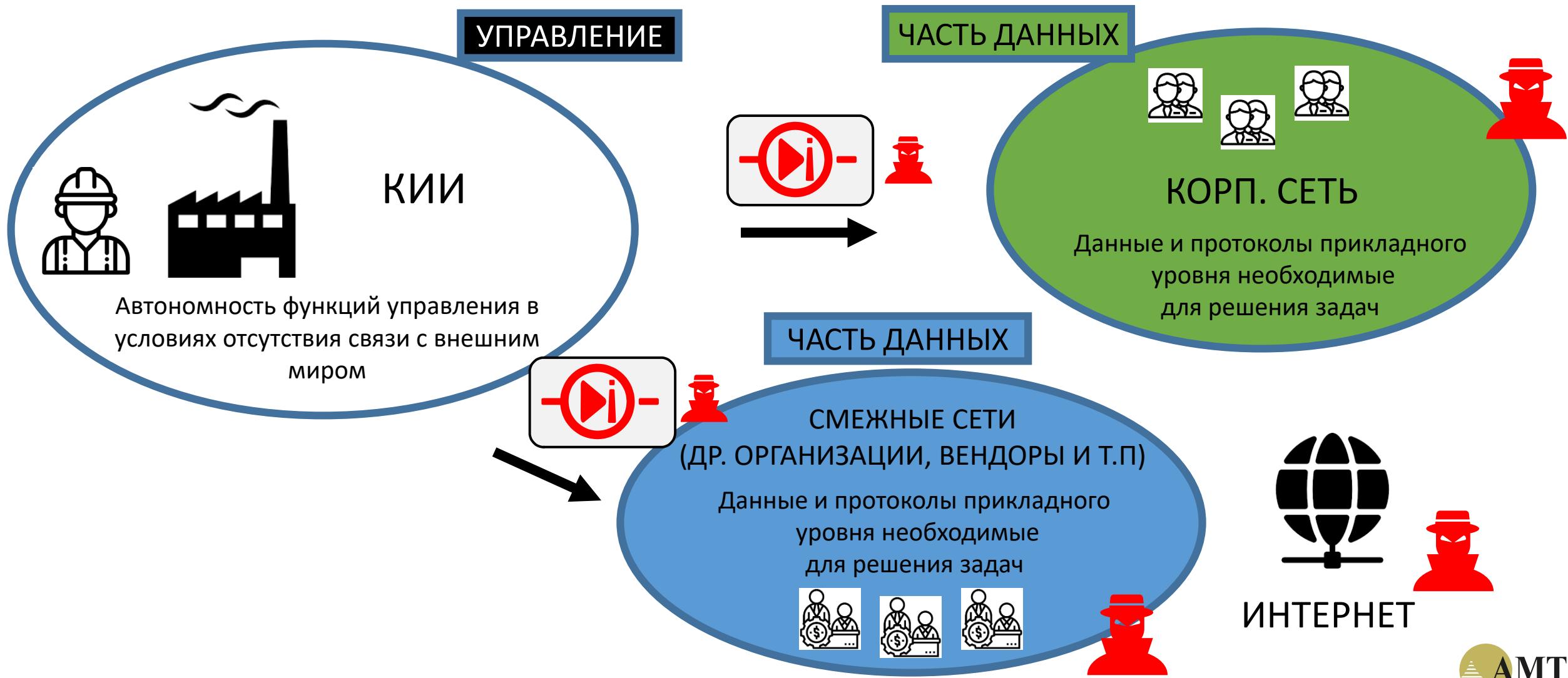
Сегментация сети – локализуем управление, передаем данные



Сети, изолированные программными решениями, достаточно уязвимы



Сети, изолированные аппаратными решениями – эффективно изолированные сети

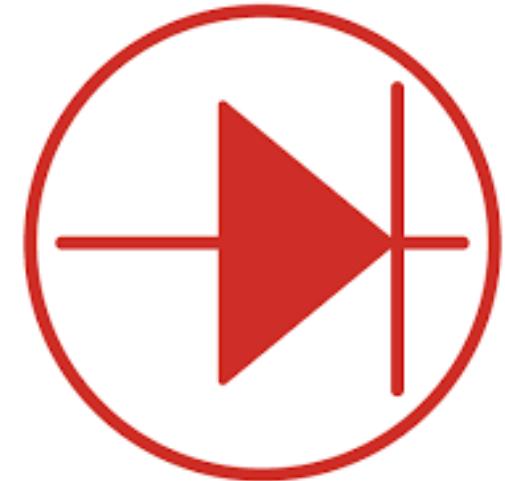


РЕШЕНИЯ НА РЫНКЕ INFODIODE ОТ АМТ-ГРУП



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

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

AK 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
АПК InfoDiode, rack module	2 АПК 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

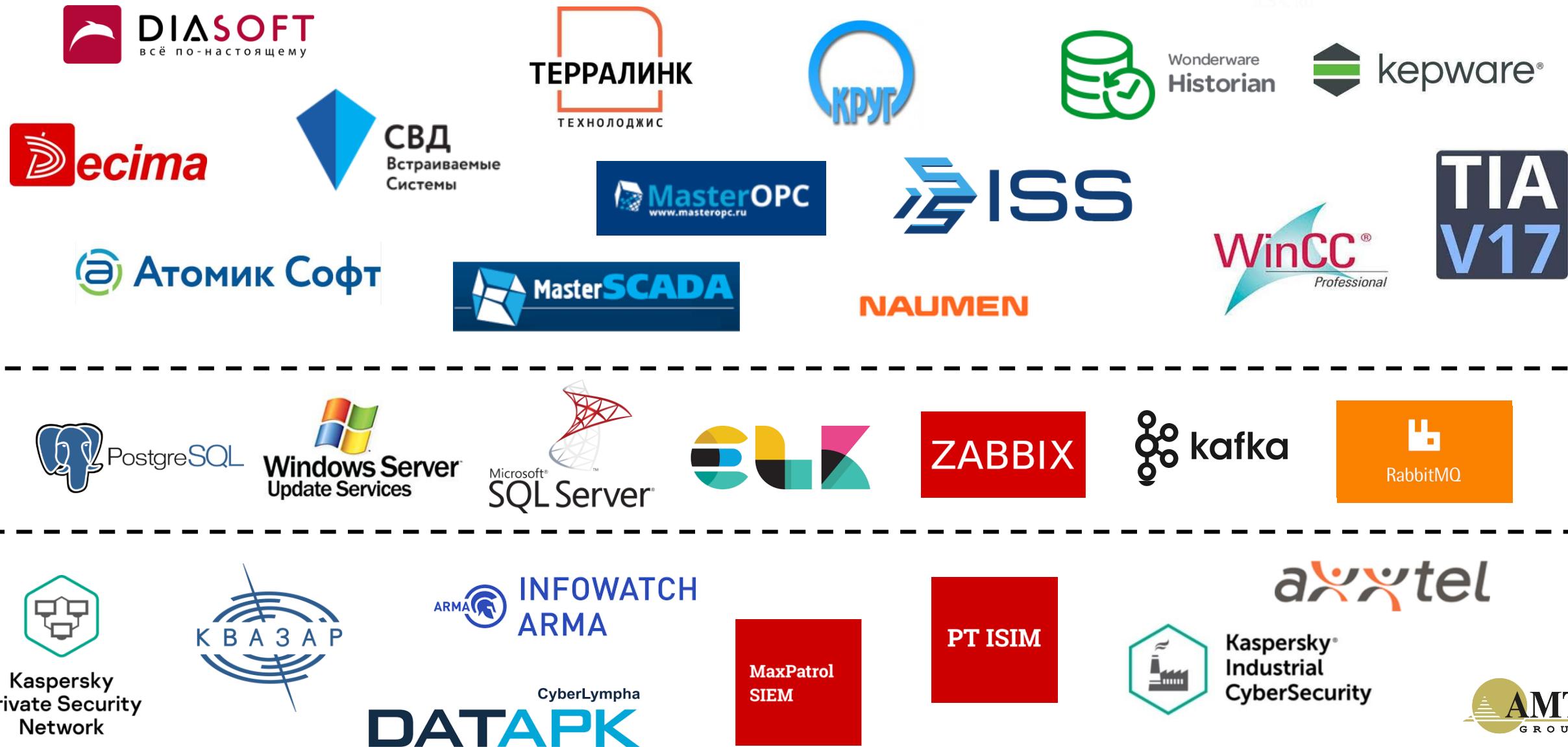
Диод внутри

InfoDiode включен в реестры, завершена его сертификация

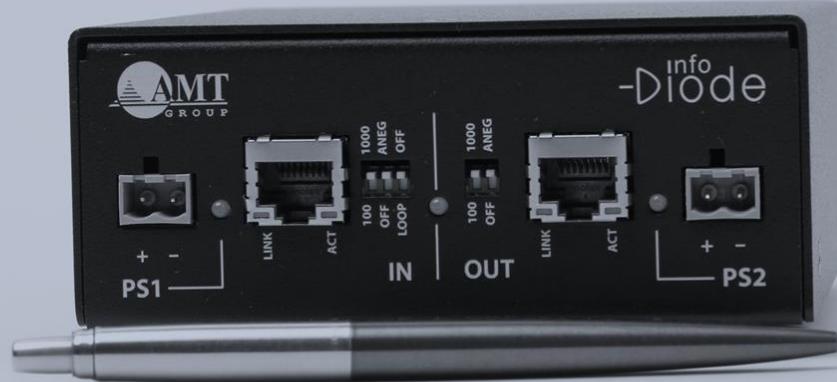
- 1. Сертификаты ФСТЭК (УД4) – на всю линейку решений**
- 2. Реестр Минпромторга – включены и аппаратный, и программно-аппаратный комплексы**
- 3. Реестр Минцифры – программное обеспечение**
- 4. Сертификаты и декларации ЕАС – на всю линейку решений**



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



АППАРАТНЫЕ РЕШЕНИЯ INFODIODE



Аппаратный комплекс InfoDiode – простое и эффективное решение для сегментации сети

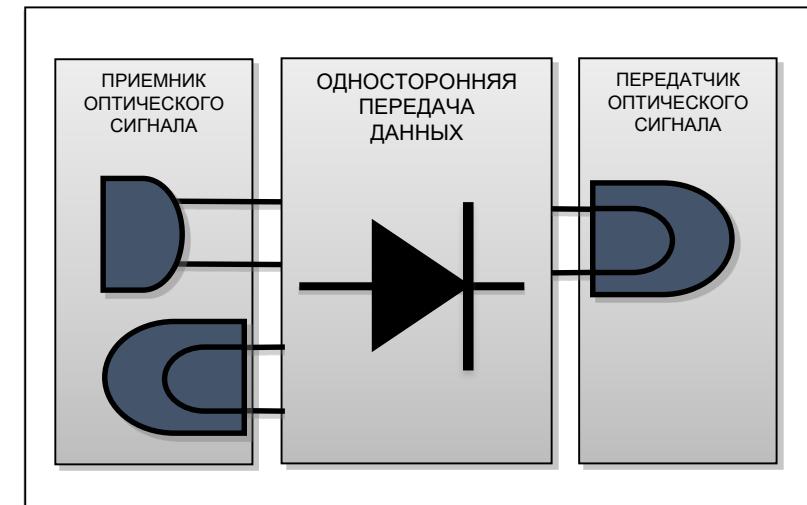
Аппаратная односторонняя передача данных

- 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



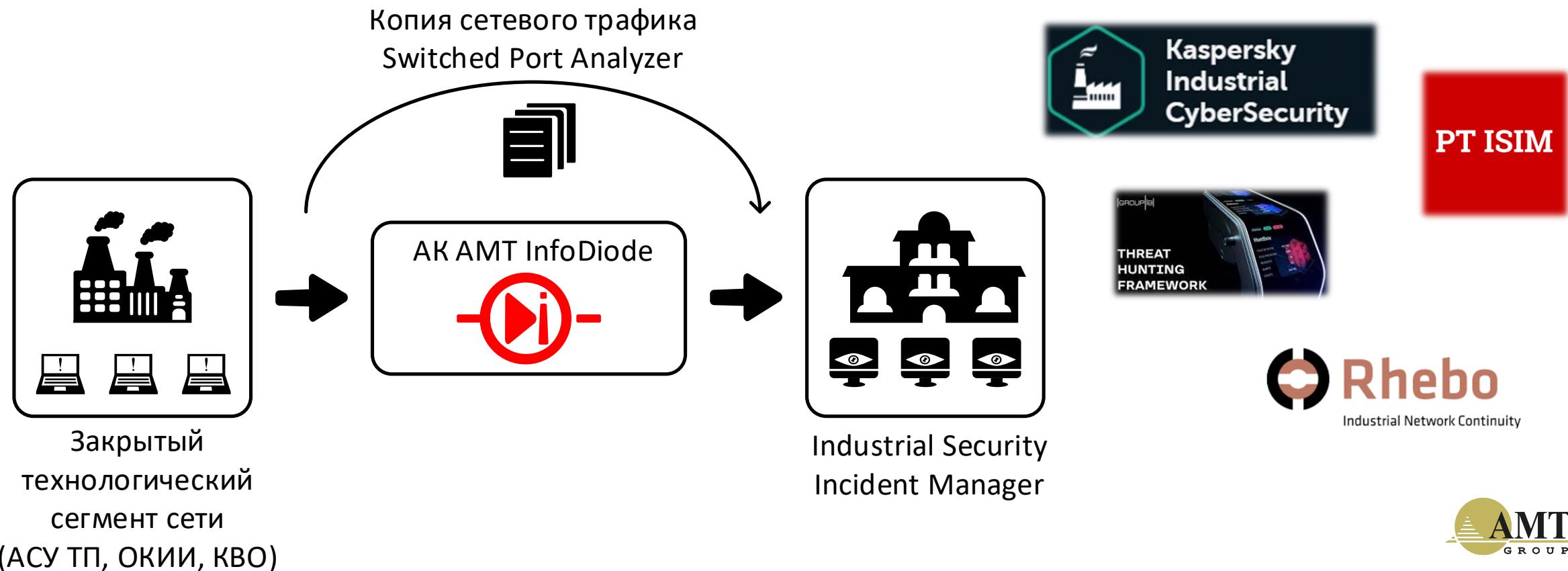
SPAN трафик, туннелинг UDP

Возможно

Невозможно

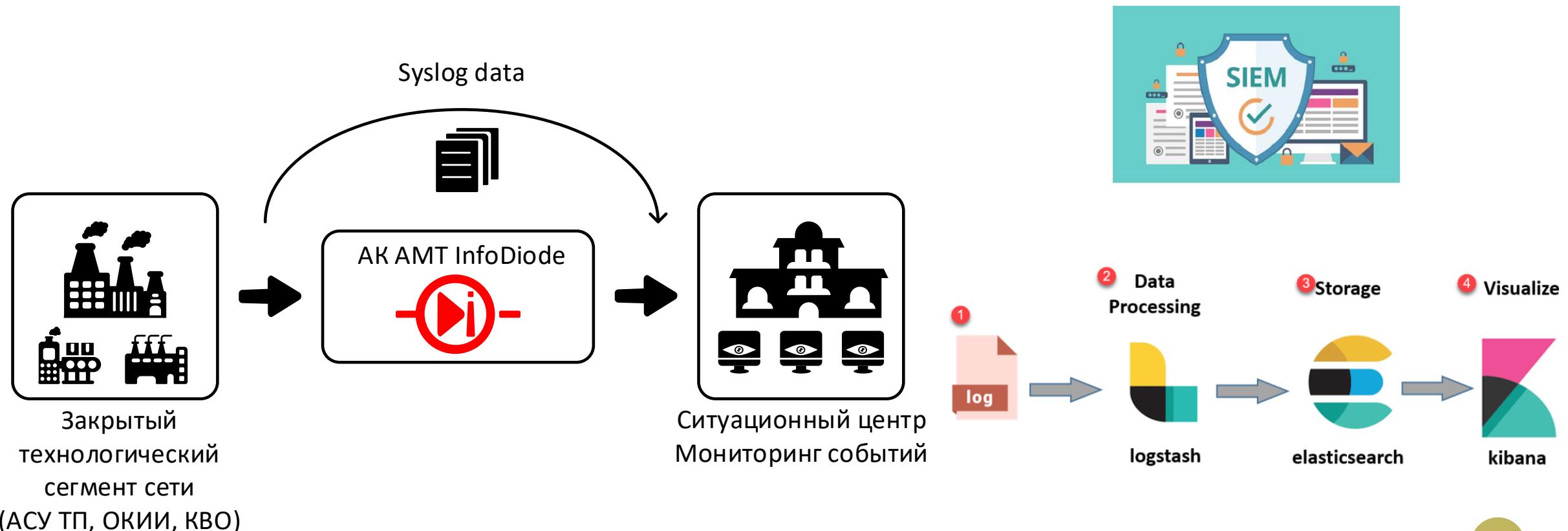
SPAN-mirroring

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)



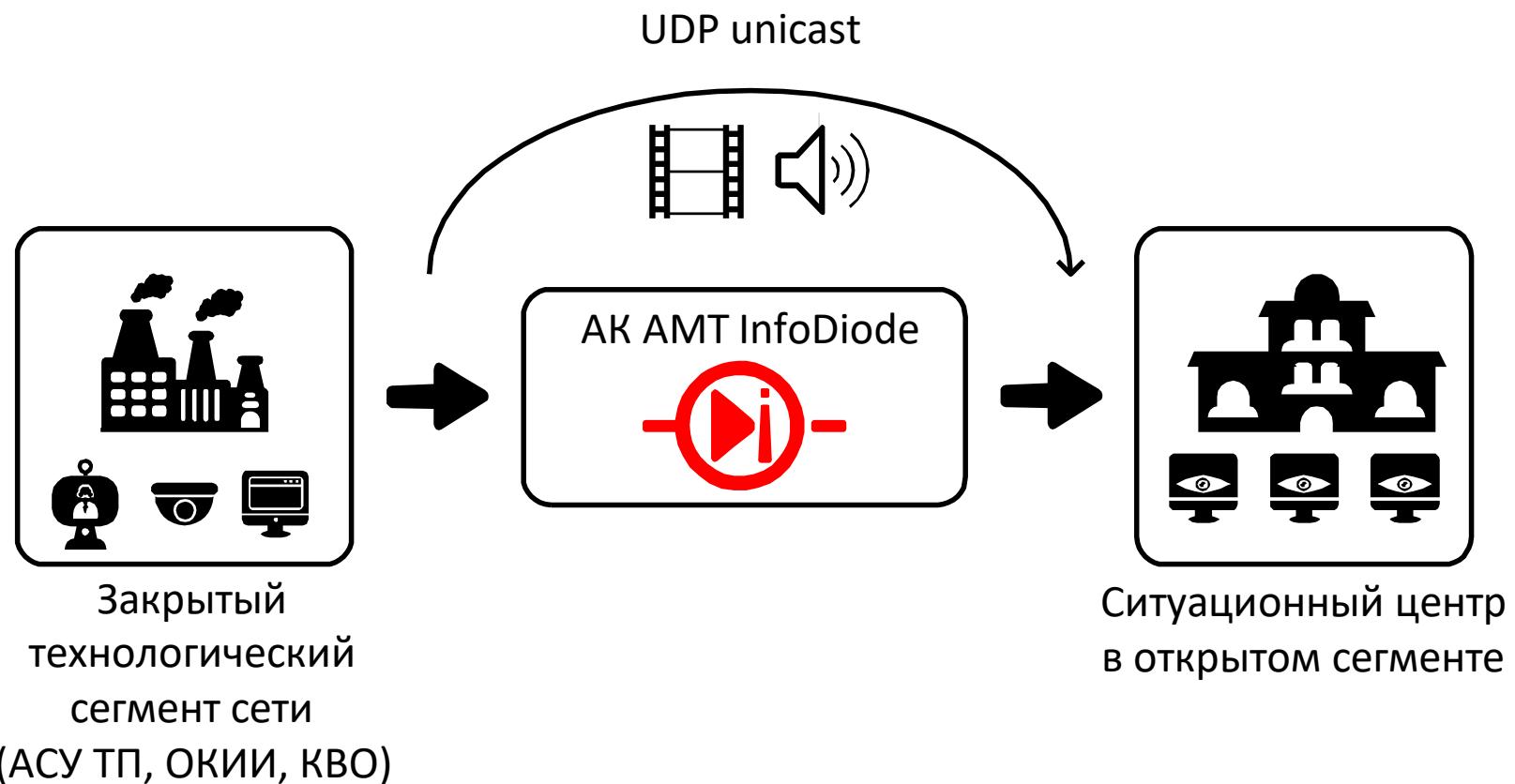
Передача данных для НОС и СОЦ через АК InfoDiode

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



Передача видео потока через AK InfoDiode

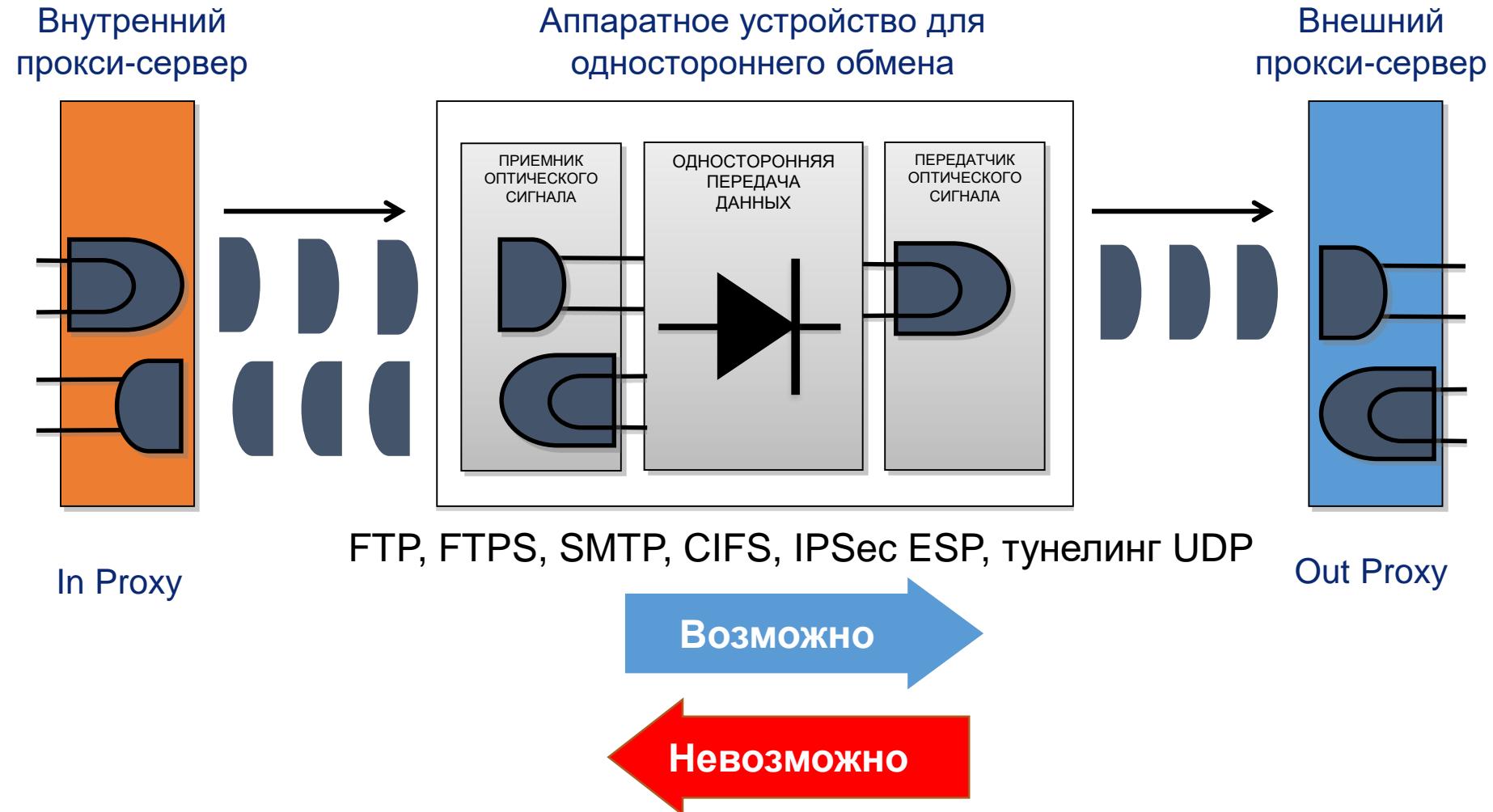
Вариант 3. Передача видео- и аудио-трафика из закрытого сегмента с использованием UDP, в том числе широковещательных видеопотоков. Часто возникает потребность осуществлять удаленный видеомониторинг, получение сигналов от системы оповещения внутри закрытого технологического сегмента. Использование AK InfoDiode обеспечивает получение видео- и аудио- потоков, при этом гарантирует изоляцию закрытого сегмента



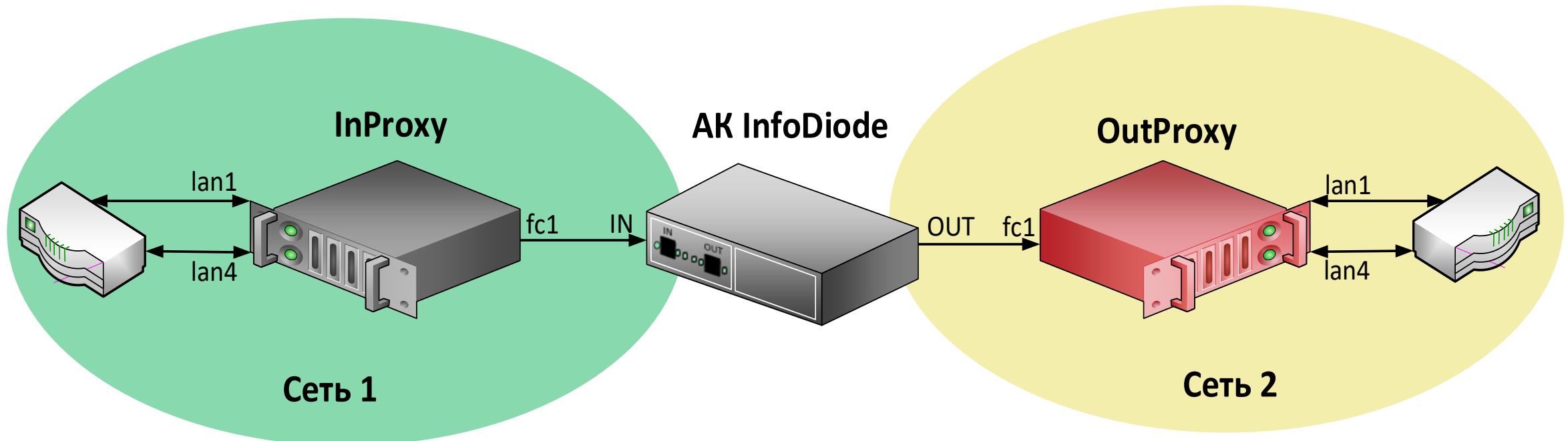
АППАРАТНО-ПРОГРАММНЫЕ РЕШЕНИЯ INFODIODE PRO



АПК InfoDiode PRO – решения для передачи асинхронного TCP\IP трафика

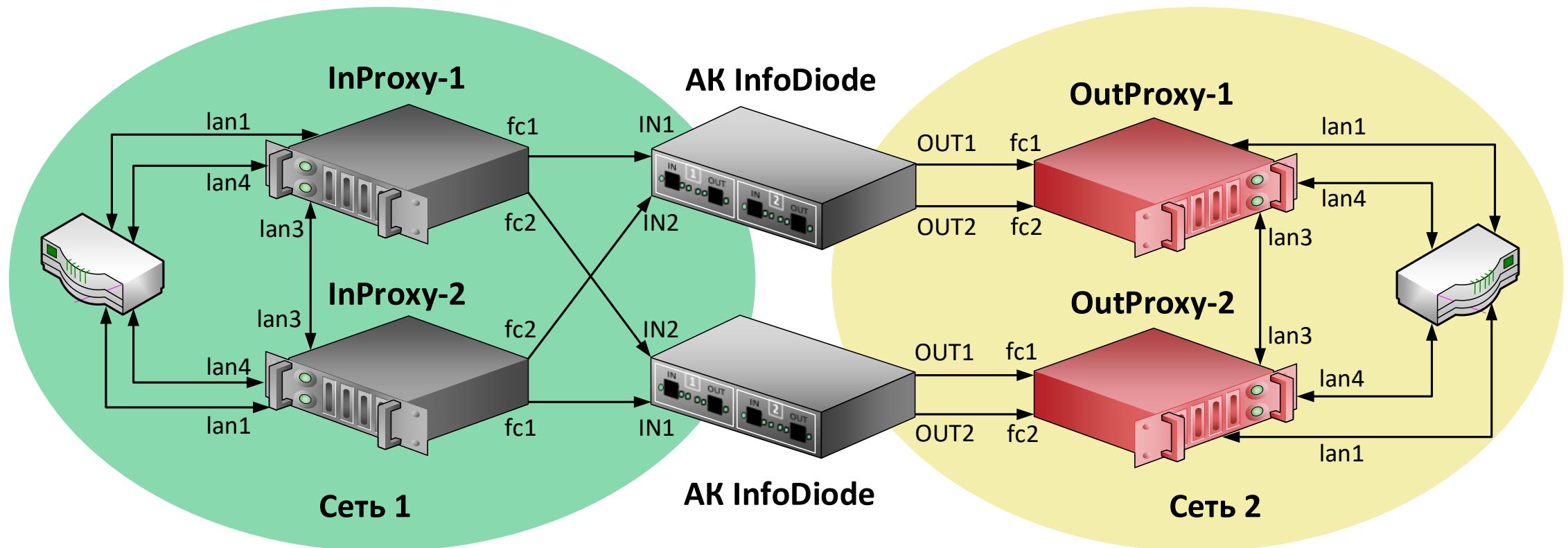


Базовый вариант АПК InfoDiode PRO



Кластерный вариант АПК InfoDiode PRO – отказоустойчивый вариант

Дублирование всех элементов комплекса



Удобный и понятный интерфейс администрирования АПК InfoDiode PRO

The screenshot displays the InfoDiode PRO administrative interface. On the left, a sidebar lists various management sections: Streaming Services, Proxy Services, Server Settings (expanded), DNS Settings, Date and Time, Localization, Network interfaces, Network routes, System Administration (expanded), User management, and Monitoring. The main content area has tabs for 'Network interfaces' and 'Streaming Services'. Under 'Network interfaces', there is a table listing five interfaces (eth1-eth5) with columns for ID, Ping, Pub., Man., IP Address, and MAC address. Below this is a 'Save' button. Under 'Streaming Services', there are sections for 'Interconnect' (with a table for 'eth0') and 'Proxy Services' (with a table for 'eth0'). A large XML configuration snippet is overlaid on the right side of the interface.

```

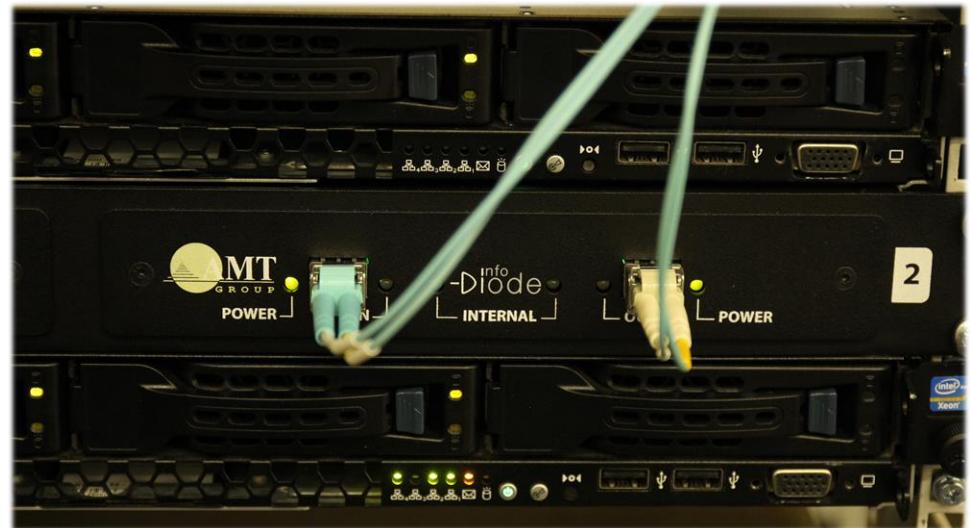
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<server target="tx" version="1.0"
xmlns="urn:ru:amt:diode:config:server:1.0">
<language>en</language>
<country>RU</country>
<timeZone>Asia/Yerevan</timeZone>
<license/>
<subsystems>
    <subsystem
        xmlns="urn:ru:amt:diode:config:subsystems:udp:1.0">
        <enabled>true</enabled>
        <rule enabled="true">
            <src address="192.168.1.50" />
            <dst port="514" />
        </rule>
    </subsystem>
</subsystems>

```

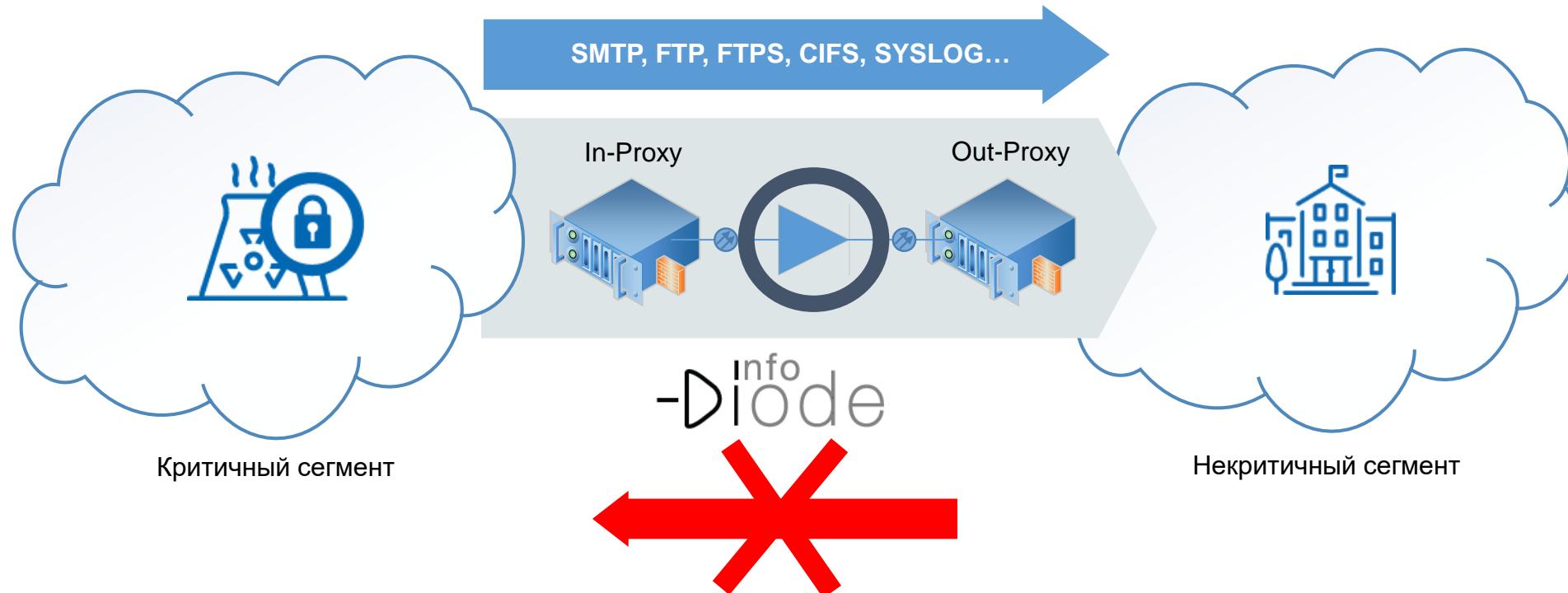
- User-friendly Web-интерфейс (русская и английская версии)
- Возможность управления посредством CLI и XML
- Специальный режим защиты против случайных изменений

Возможности и параметры АПК InfoDiode PRO

- Производительность UDP - 900 Mbps
- Производительность прокси сервисов – 300 Mbps
- Поддержка протоколов FTP/FTPS, CIFS, SMTP, SFTP и др.
- Приоритизация 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

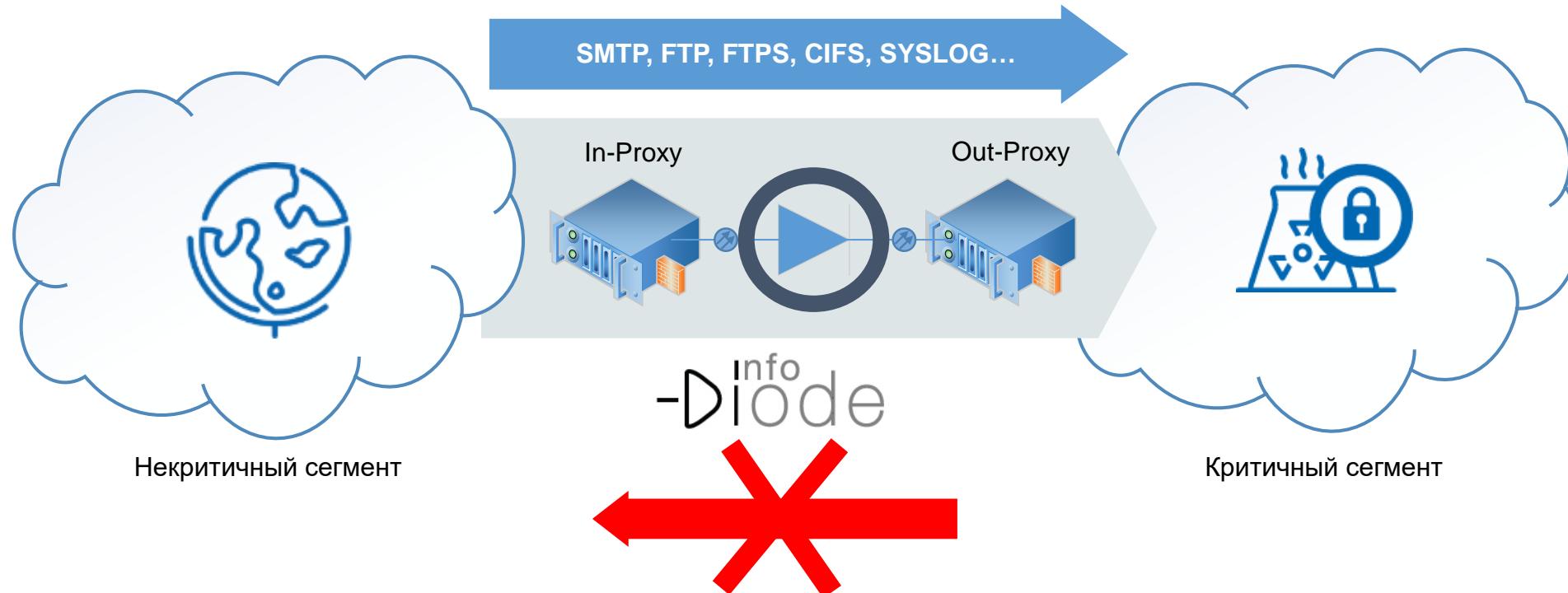


Сценарий 1 - Однонаправленная выгрузка данных из критичного технологического сегмента



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

Сценарий 2 - Однонаправленная загрузка данных в защищаемую информационную систему



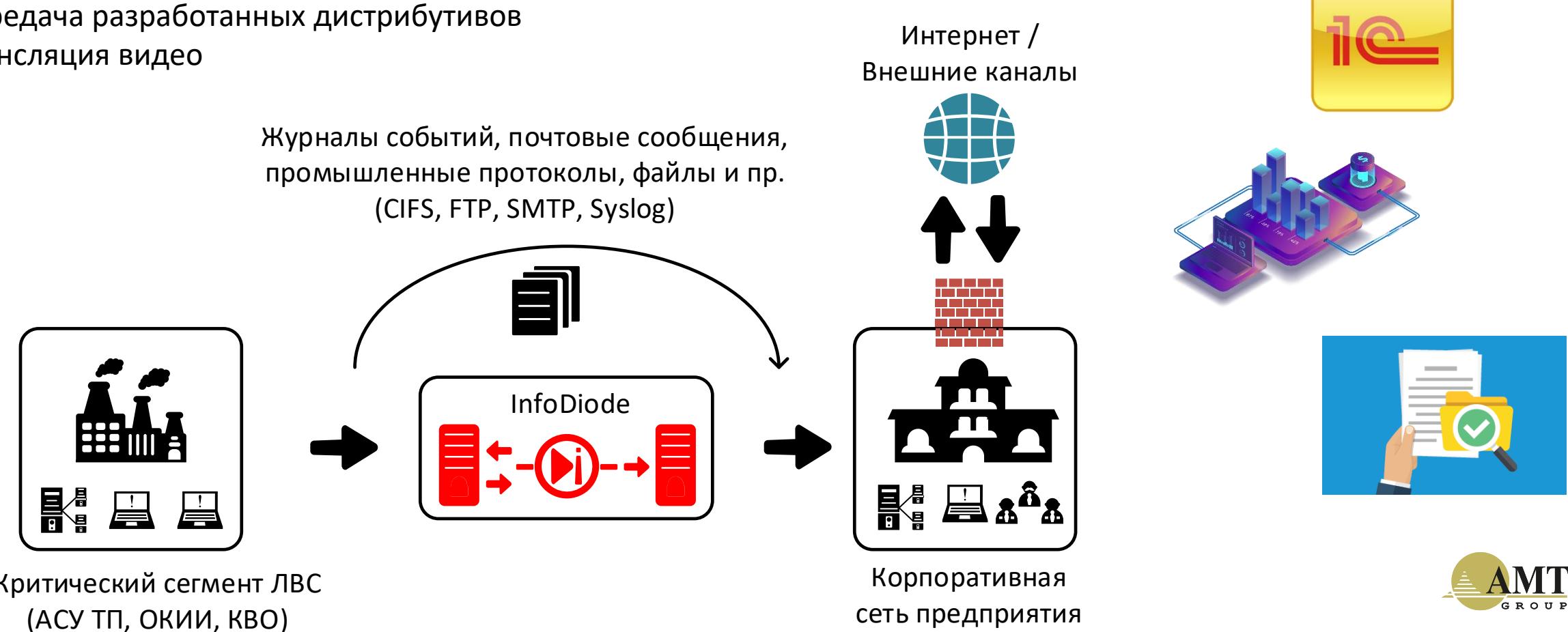
- Загрузка данных в конфиденциальные информационные системы
- Нельзя, чтобы данные «утекли» из крит. информационных систем
- Нужно исключить возможность управления объектом

Вариант 1. Экспорт данных

В данном сценарии обеспечивается гарантия целостности передаваемых данных.

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

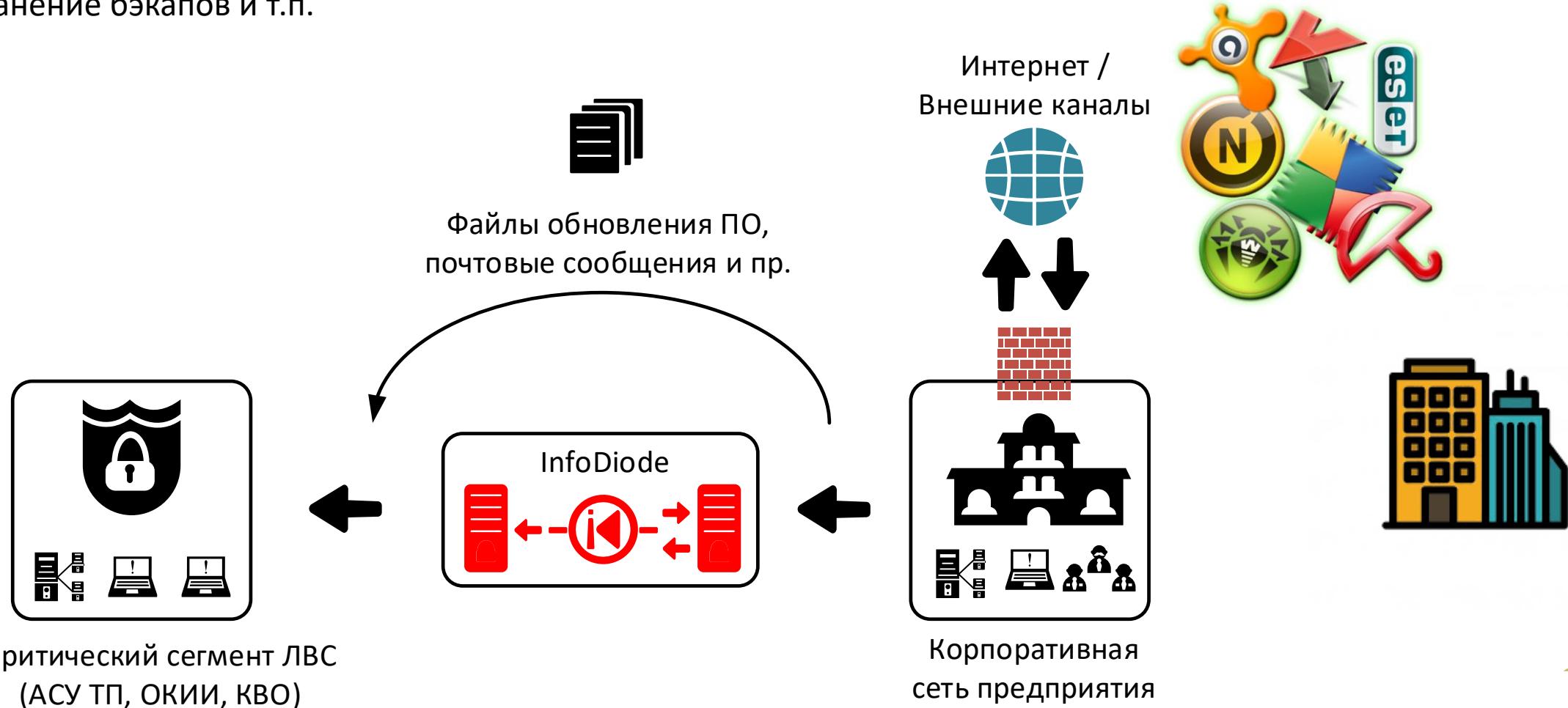
и т.п.



Вариант 2. Импорт данных

В данном сценарии обеспечивается гарантия конфиденциальности защищаемых данных.

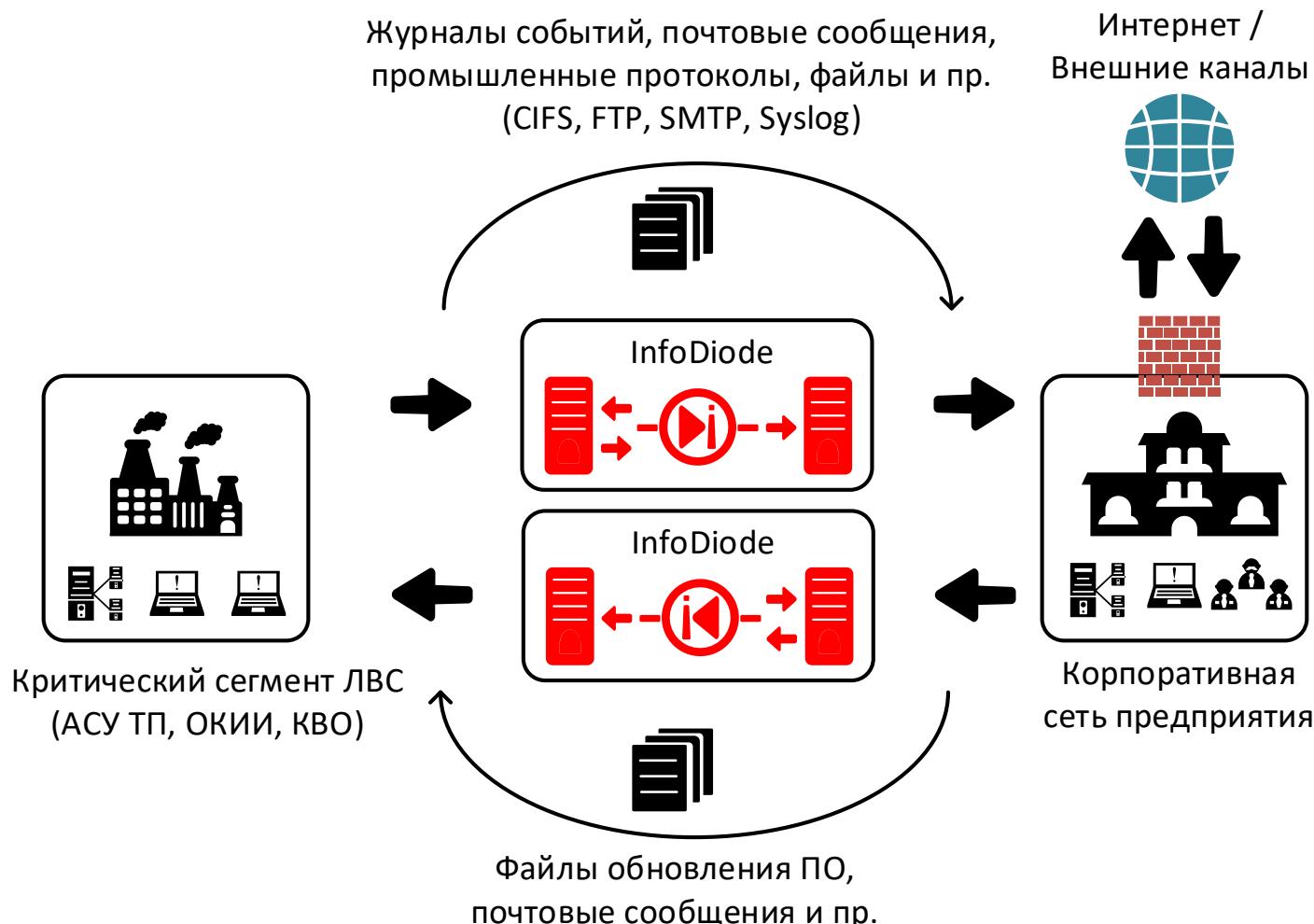
- Загрузка обновлений
- Хранение бэкапов и т.п.



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 - новое решение по защите КИИ от АМТ-ГРУП



АПК INFODIODE SMART



OPC UA

Защита и мониторинг КИИ

Обеспечивает защиту и мониторинг объекта КИИ, исключая какое-либо воздействие на него.

Поддержка пром. протоколов OPC UA, Modbus, MQTT

Обеспечивает защищенное удаленное взаимодействие критичных сегментов отдельных предприятий и организаций через недоверенные сети. Передает данные за границу доверенного периметра сети по протоколам OPC UA, Modbus, MQTT, FTP(S), CIFS, SFTP, UDP, др.

Основа для организации цифровых двойников

Передает реплики критических информационных ресурсов (OPC серверов, SCADA систем основных вендоров) за границы периметра АСУ ТП и КИИ для последующей обработки и анализа.

Централизованные диспетчерские и ситуационные центры

Обеспечивает центры реальными онлайн данными, в том числе с видеофиксацией, в условиях гарантированной изоляции объектов наблюдения.

Агрегация данных из SCADA систем в ERP, MES и «облака»

Передает данные из нескольких SCADA систем в ERP, MES системы, облачные решения, исключив какое-либо обратное влияние со стороны этих систем.

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.

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

5



Интернет

Патчи обновлений, получение информации

6



Вендоры, подрядчики

ТП, получение патчей, предоставление реплик



Предприятие



Организация



Предприятие



Полевой уровень

Сценарии применения АПК InfoDiode SMART могут быть типизированы

7



Подразделение:
SOC, NOC, архивы

Контроль ИБ, сети, конфиденц.
и резервные сегменты



8



Контрагенты (учебные
заведения и т.п.)

Методически значимая
информация, данные для
исследований



9



Конечные
потребители

Данные для инфоматов,
визуальные панели,



Предприятие



Предприятие

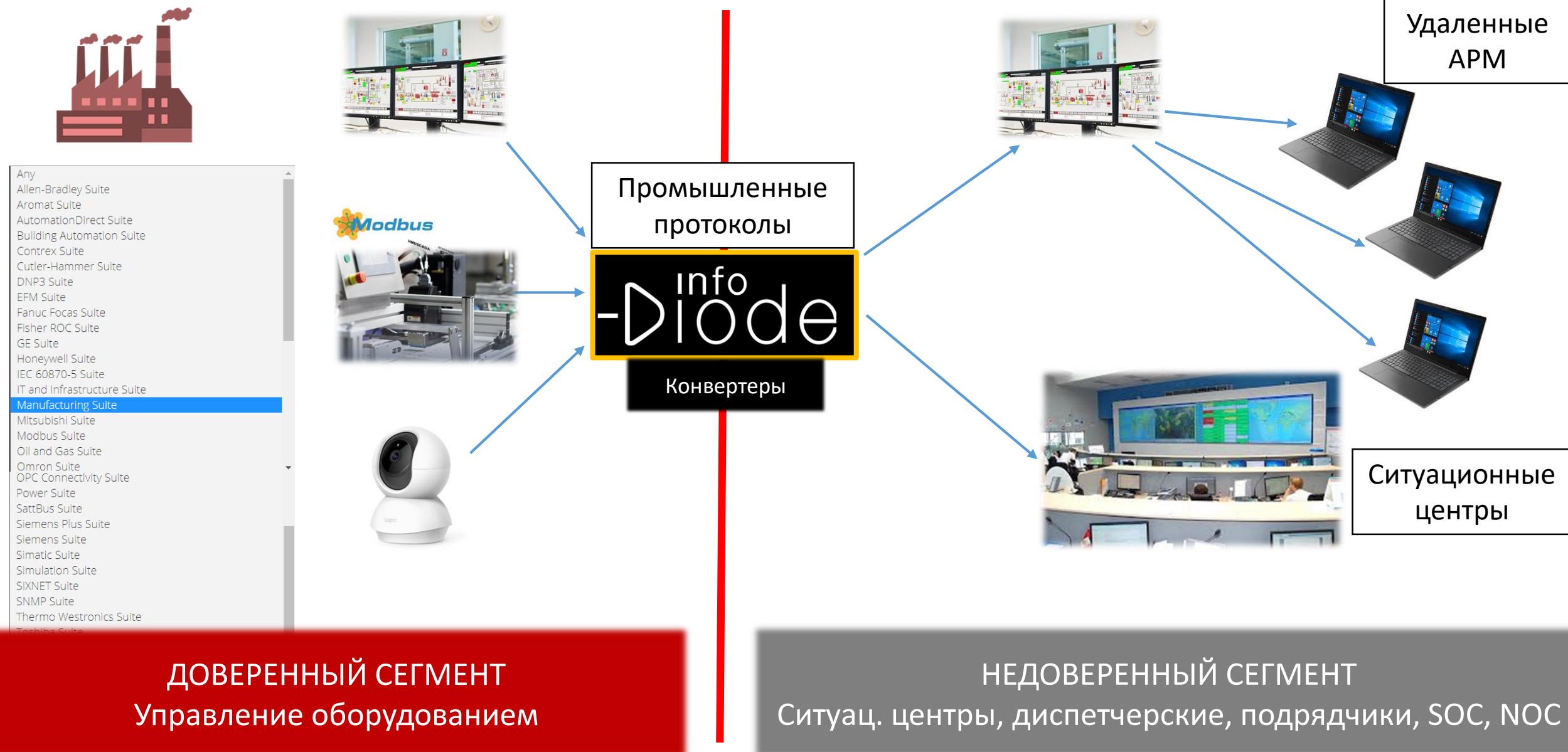


Организация

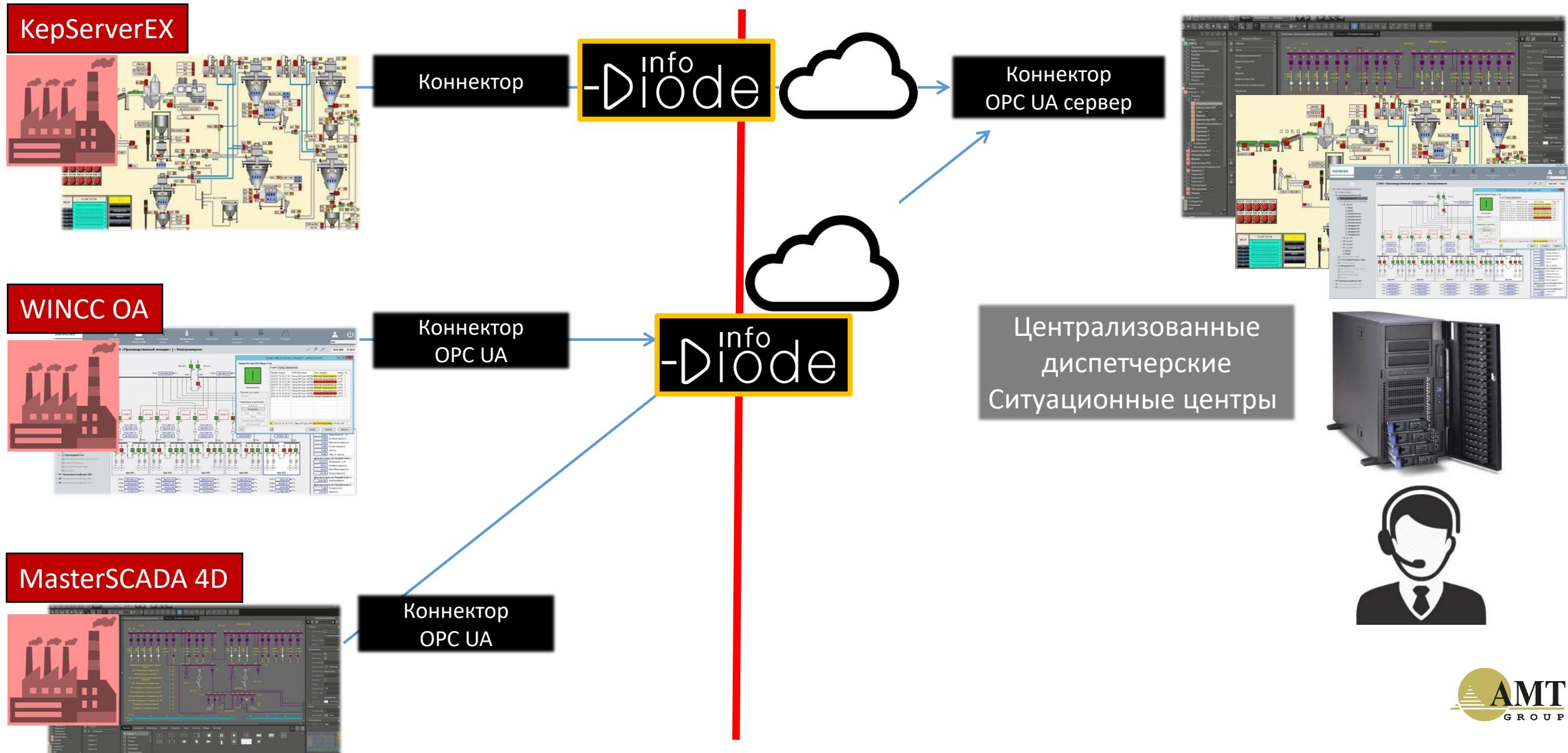


Полевой уровень

Промышленные протоколы через InfoDiode SMART - уже реальность



АПК InfoDiode SMART позволяет собирать данные SCADA за границами периметра



АПК InfoDiode SMART дополняет линейку решений для комплексной защиты КИИ

1. АПК **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.



ФСТЭК



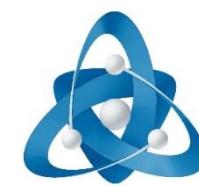
Министерство
здравоохранения РФ



РусГидро



ЦИК



РОСЭНЕРГОАТОМ
ЭЛЕКТРОЭНЕРГЕТИЧЕСКИЙ ДИВИЗИОН РОСАТОМА



ЕВРОСИБЭНЕРГО



Ростелеком



Росфинмониторинг



Генеральная
прокуратура РФ



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: 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!