



Однонаправленная
передача данных

Защита
объектов КИИ

Экспорт
видеопотоков в
ситуационный
центр

Сегментирование
сетей АСУ ТП

Info
-Diode



IT

11.09.2024

AMT-ГРУП

Система однонаправленной
передачи данных InfoDiode



ПРОБЛЕМЫ И АКТУАЛЬНЫЕ УГРОЗЫ, НОРМАТИВНАЯ БАЗА И СТАНДАРТЫ

ВАРИАНТЫ ЗАЩИТЫ СЕТЕЙ, РЕШЕНИЯ НА РЫНКЕ И INFODIODE

ЗАЩИТА С ПОМОЩЬЮ ОДНОНАПРАВЛЕННОГО ШЛЮЗА

АППАРАТНЫЕ РЕШЕНИЯ INFODIODE

АППАРАТНО-ПРОГРАММНЫЕ РЕШЕНИЯ INFODIODE

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





- 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
 - ❑ Двухнаправленность 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



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	Соккрытие 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



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

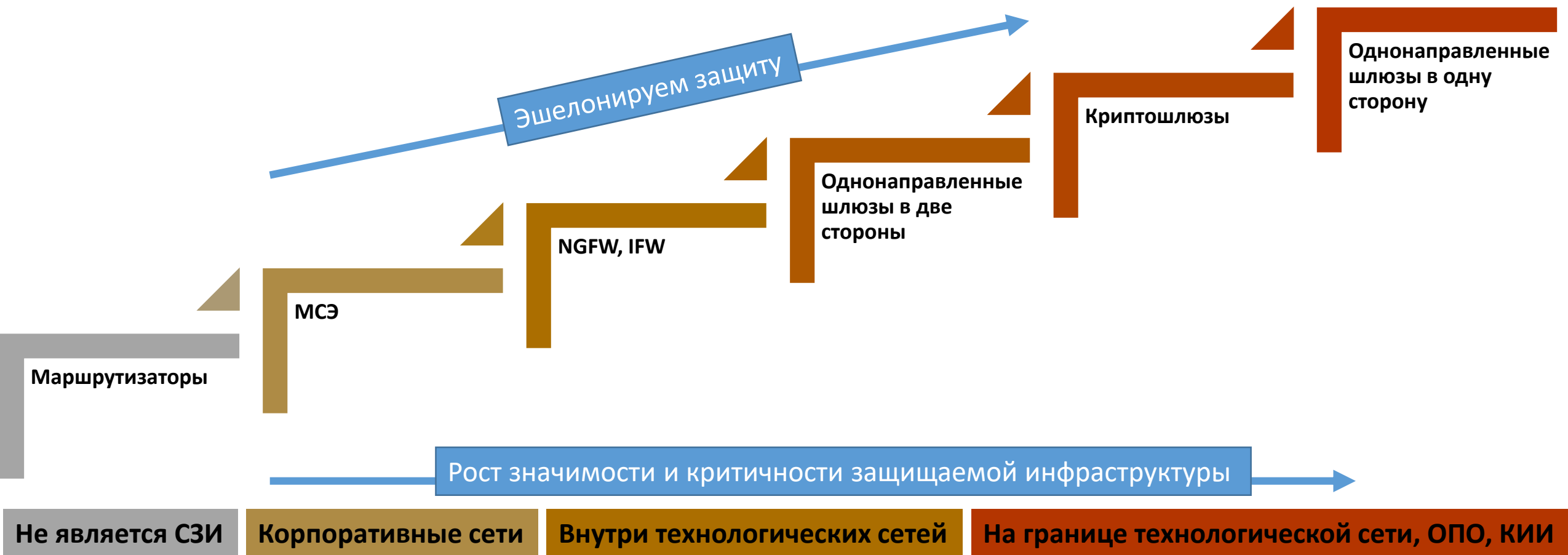
Тип кибератаки	InfoDiode	Решения на базе ПО
1) Фишинг / скачивание ПО с помощью системы drive-by-download	Возможно	Возможно
2) Социальная инженерия – кража пароля / регистраторы нажатий клавиш	Возможно	Относительно легко
3) Компрометация контроллера домена – создание учетной записи хоста или МСЭ	Возможно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

Невозможно

Возможно

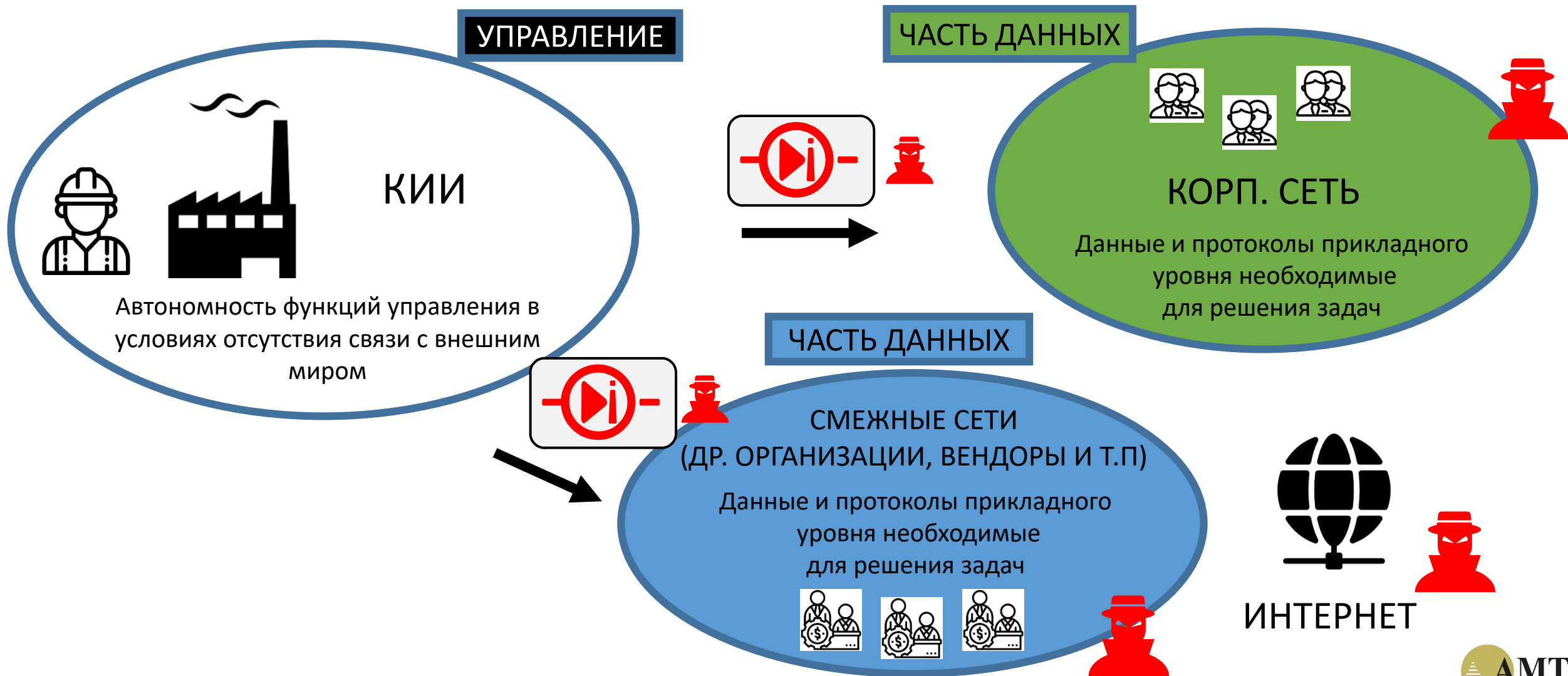
Относительно легко

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





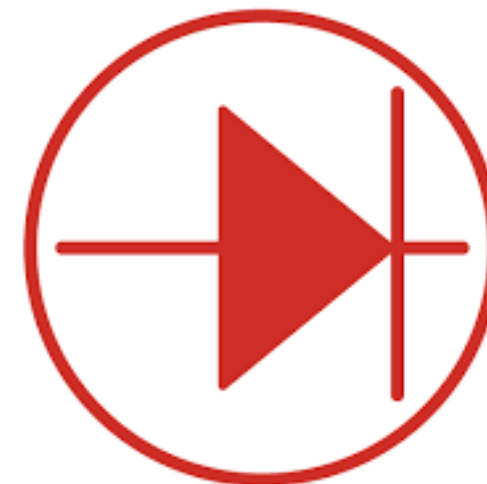




РЕШЕНИЯ НА РЫНКЕ INFODIODE ОТ АМТ-ГРУП



- **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

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

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



Wonderware
Historian



NAUMEN



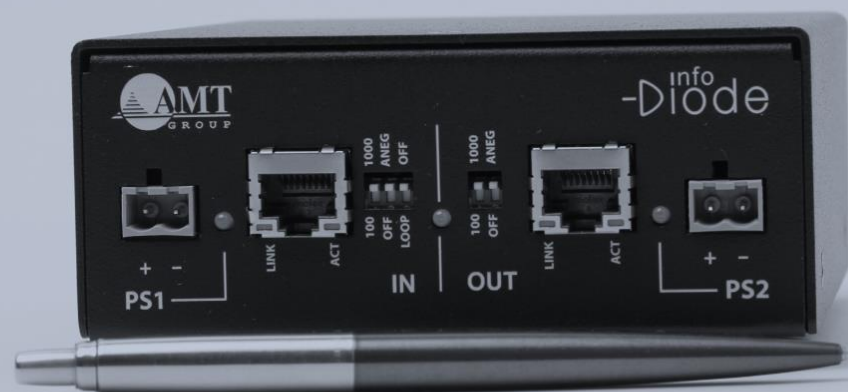
Kaspersky
Private Security
Network



Kaspersky®
Industrial
CyberSecurity



АППАРАТНЫЕ РЕШЕНИЯ INFODIODE



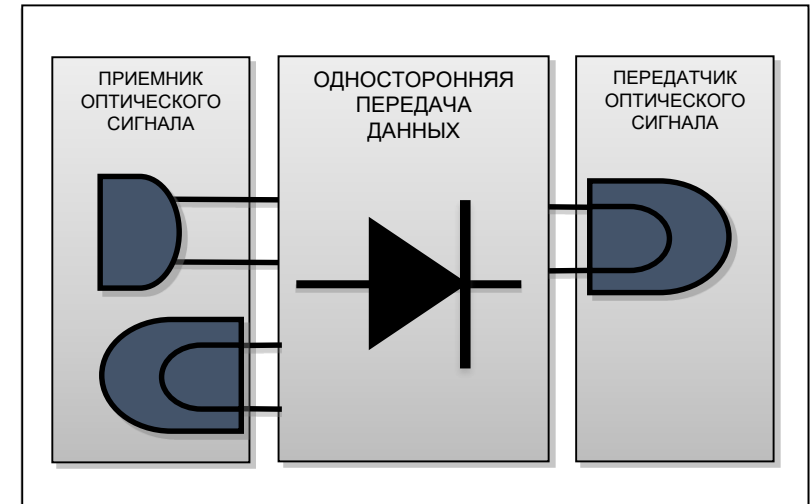
Аппаратная односторонняя передача данных

- 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



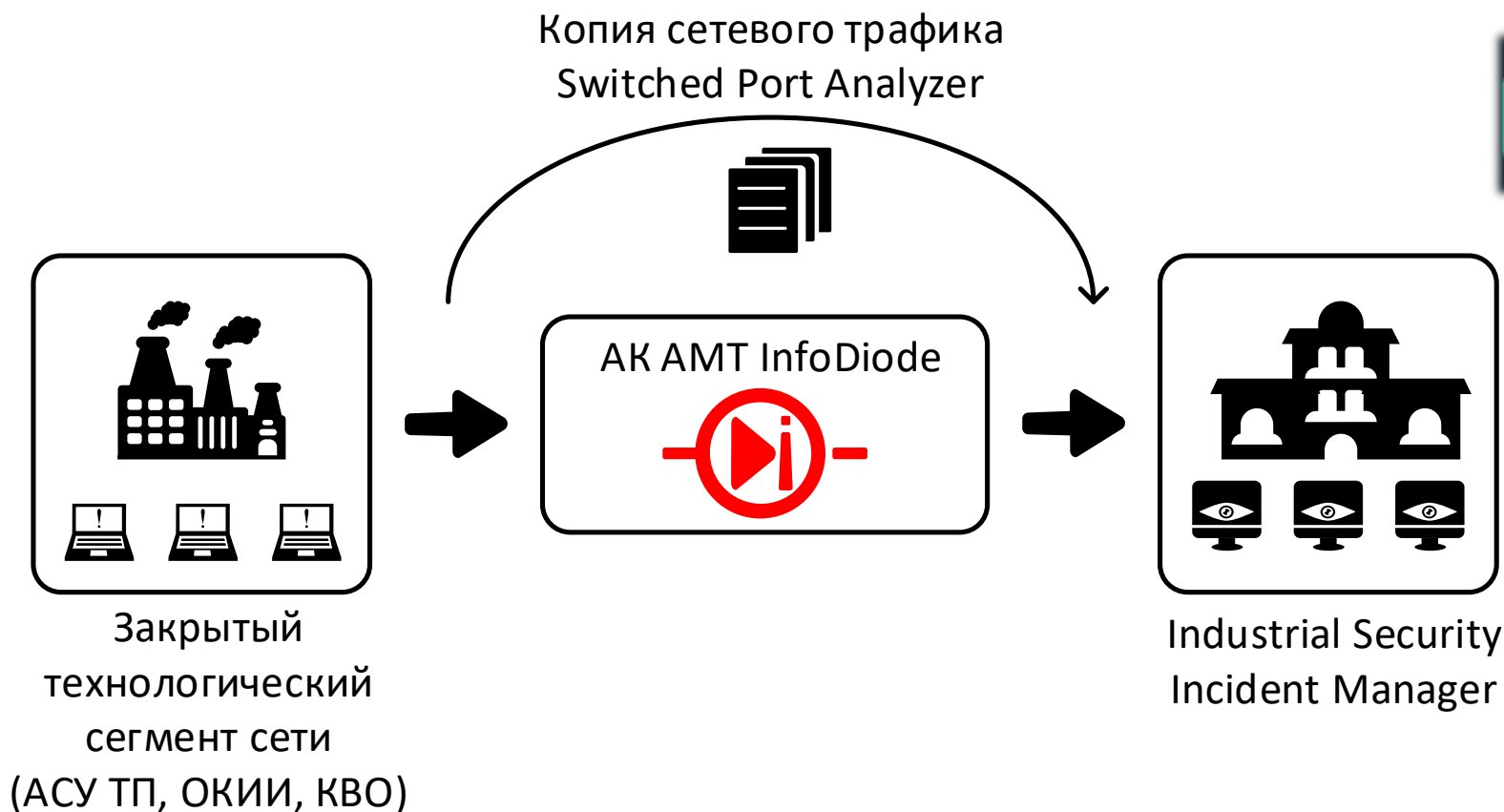
SPAN трафик, тунелинг UDP

Возможно

Невозможно

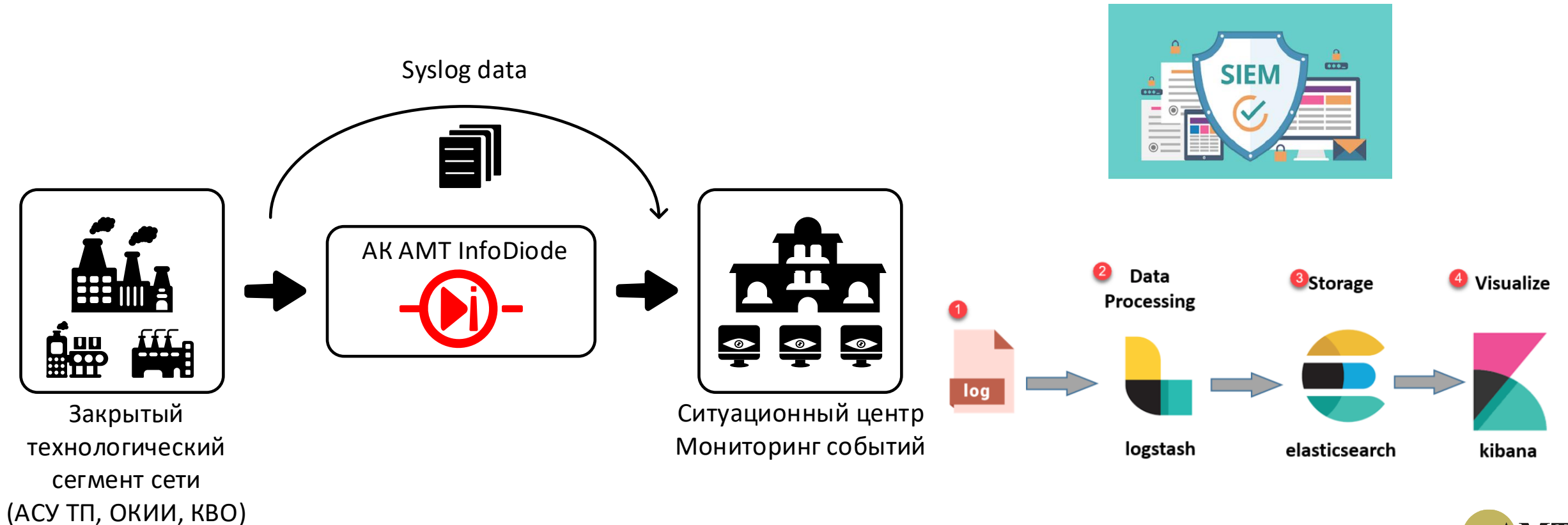
SPAN-mirroring

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 NOC и SOC через АК InfoDiode

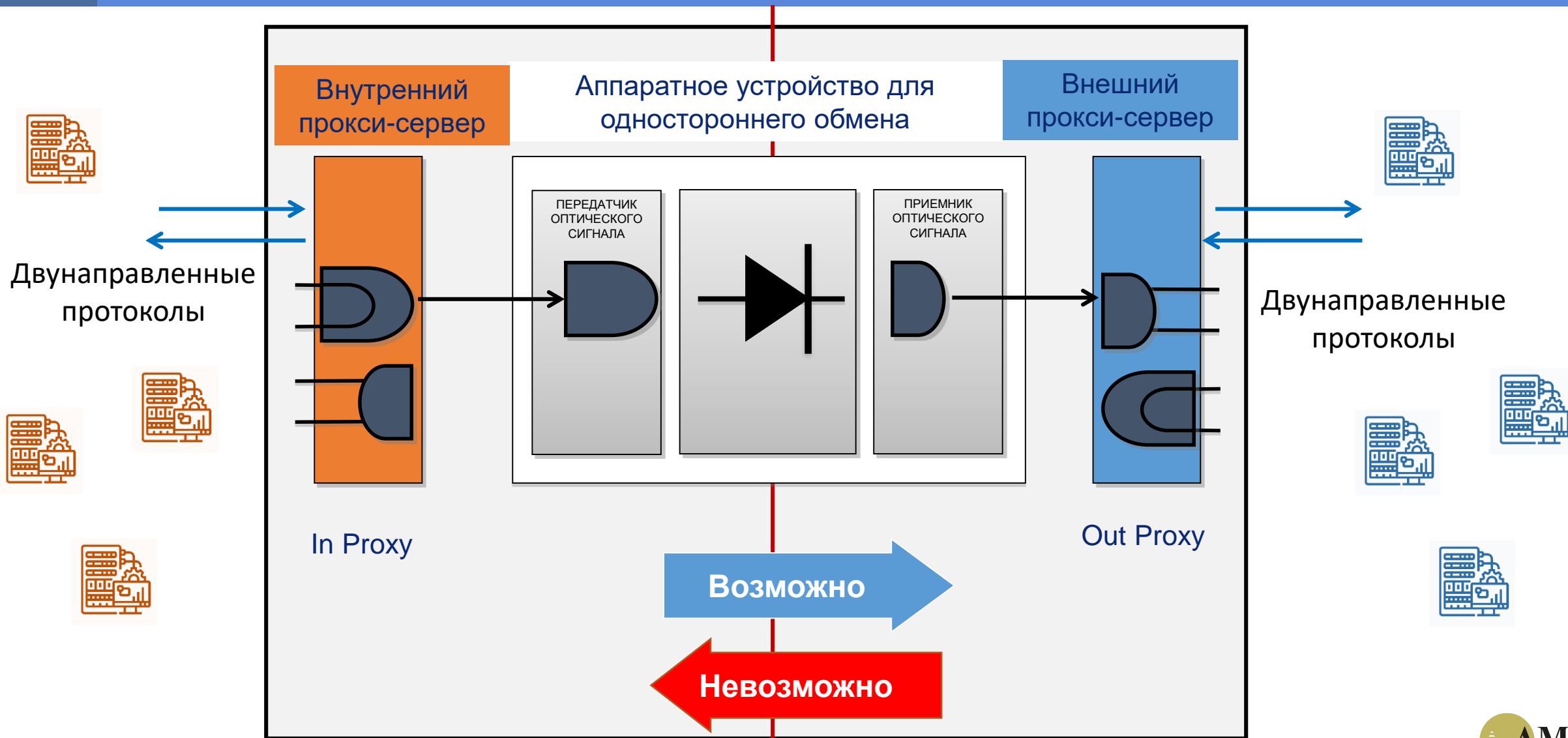
Вариант 2. Передача событий технологической сети с использованием Syslog на внешнюю систему мониторинга. Логирование событий внутри технологического сегмента в централизованной системе мониторинга событий позволяет существенно снизить вероятность возникновения аварийных ситуаций и консолидировать все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

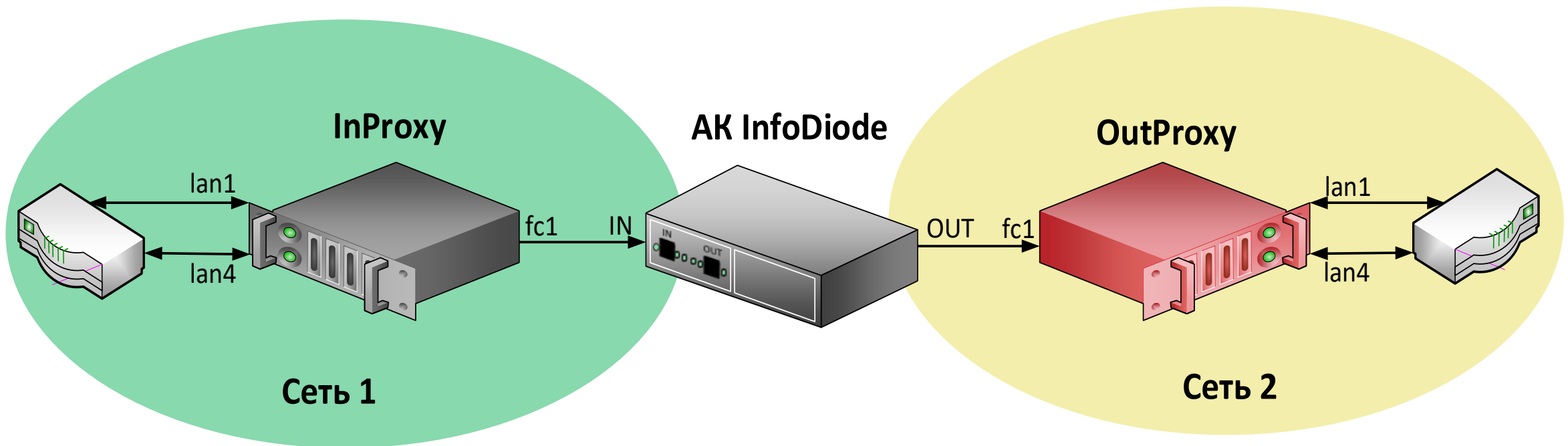


АППАРАТНО-ПРОГРАММНЫЕ РЕШЕНИЯ INFODIODE PRO

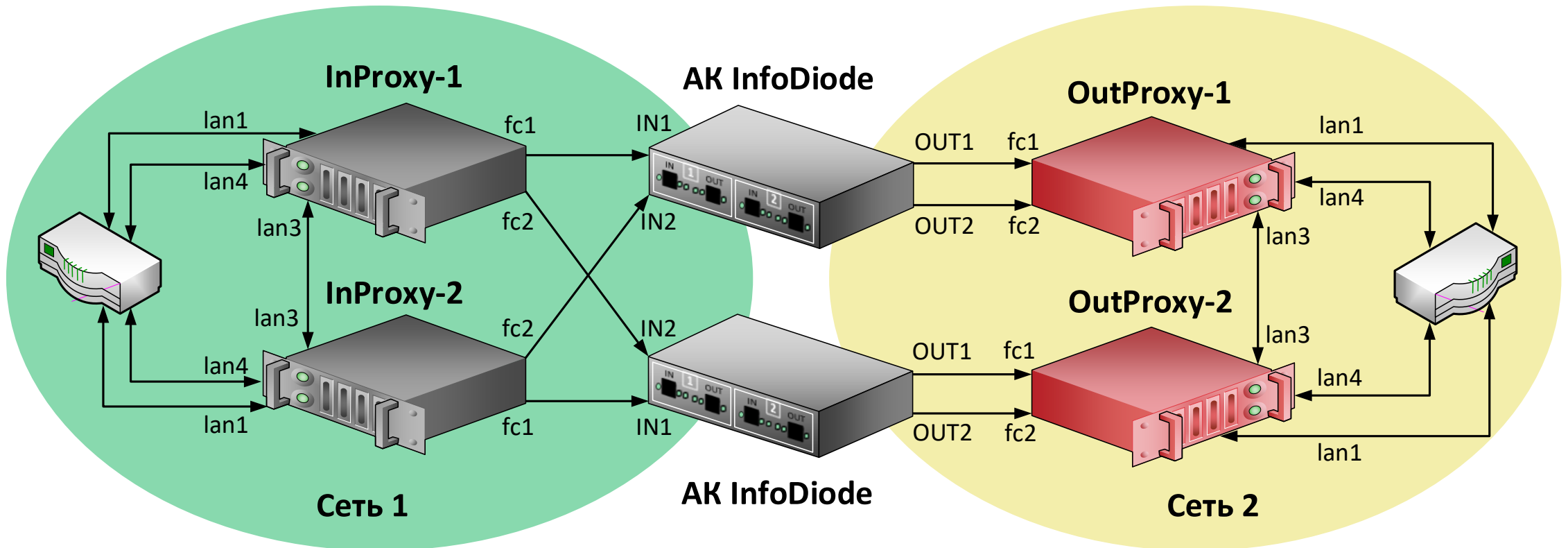


Решения InfoDiode позволяют передавать двунаправленные протоколы, терминируя их на себе





Дублирование всех элементов комплекса



The screenshot shows the 'Network interfaces' configuration page in the InfoDiode PRO web interface. The page has a dark header with the 'diode' logo, 'In-Proxy' status, and 'Apply changes' buttons (Apply and Discard). A sidebar on the left contains navigation menus for Streaming Services, Proxy Services, Server Settings, DNS Settings, Date and Time, Localization, Network interfaces, Network routes, System Administration, User management, and Monitoring. The main content area displays a table of network interfaces:

ID	Ping	Pub.	Man.	IP Address	MAC address		
eth1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.1.50/24	00:e0:ed:35:68:1b	<input type="checkbox"/>	<input type="checkbox"/>
eth2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.1.1/24	54:a0:50:85:d8:41	<input type="checkbox"/>	<input type="checkbox"/>
eth3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10.0.187.187/24	54:a0:50:85:d8:42	<input type="checkbox"/>	<input type="checkbox"/>
eth4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.4.50/24	54:a0:50:85:d8:43	<input type="checkbox"/>	<input type="checkbox"/>
eth5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>

Below the table is a 'Save' button. The bottom part of the screenshot shows the 'Interconnect' section with fields for ID, IP address RX, and RX MAC, and another 'Save' button.

```
<?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"/>
        <dest address="192.168.188.0/24"/>
        <port start="514" end="514"/>
      </rule>
    </subsystem>
  </subsystems>
</server>
```

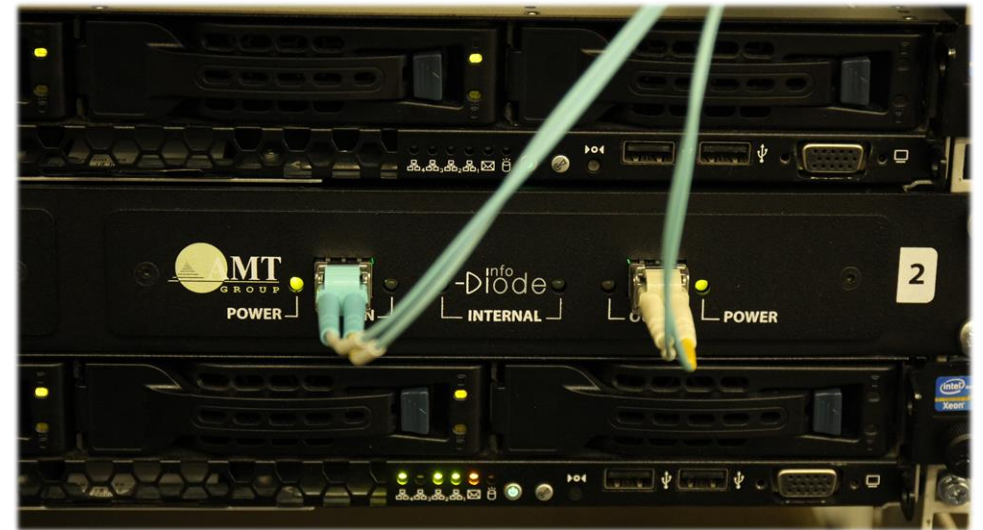
The screenshot shows the 'UDP Tunneling' configuration page in the InfoDiode PRO web interface. The page has a dark header with the 'diode' logo, 'In-Proxy' status, and 'Apply changes' buttons (Apply and Discard). The main content area displays the 'UDP Tunneling' section with a table of tunneling rules:

Enabled	Source	Destination	NAT source	NAT destination	
<input checked="" type="checkbox"/>	0.0.0.0/0	192.168.1.1/32:4000		192.168.2.2:5000	<input type="checkbox"/>

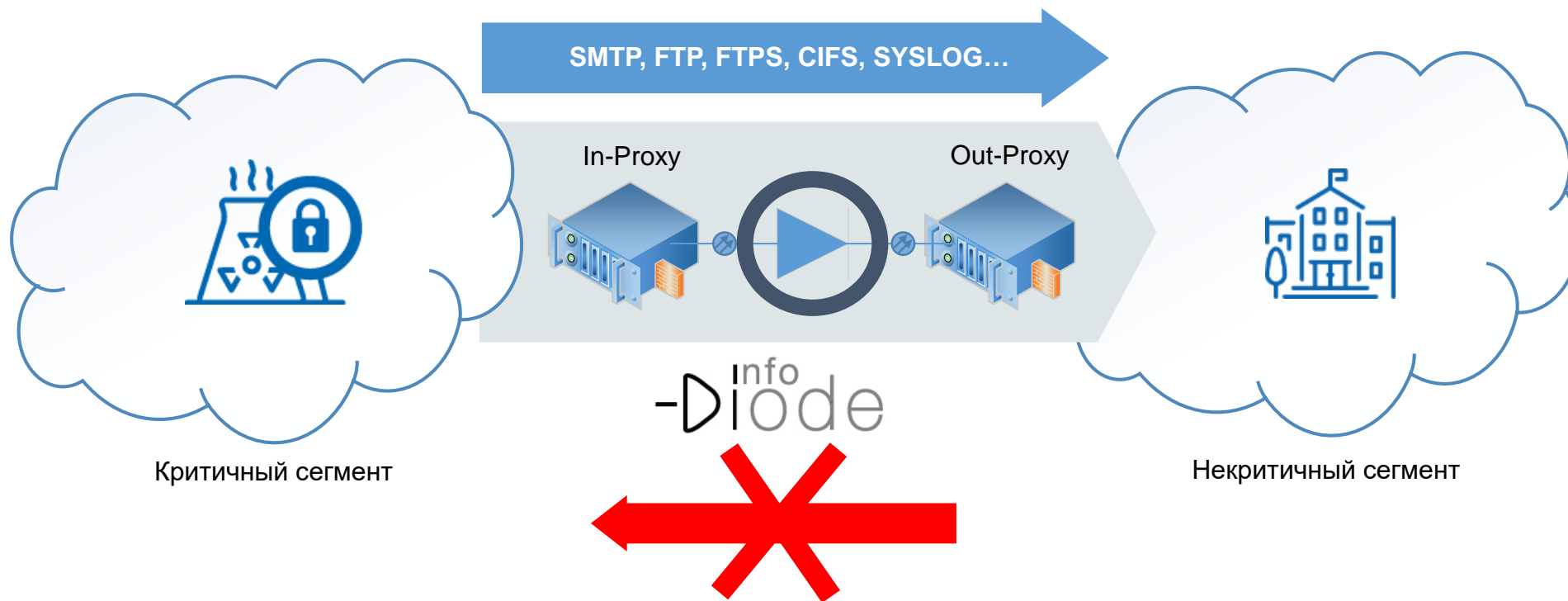
Below the table is an 'Add route' button. The left sidebar shows navigation menus for Streaming Services, UDP Tunneling, IPsec Tunneling, Proxy Services, and Server Settings.

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

- 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

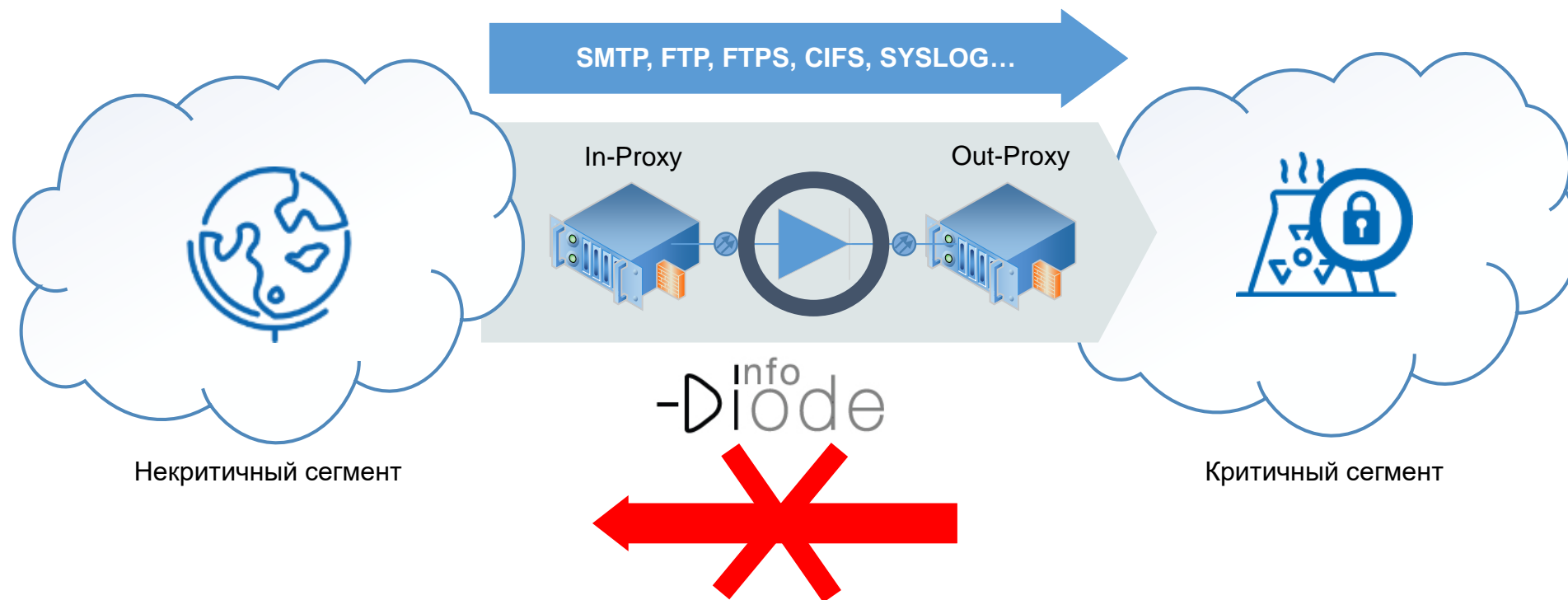


Сценарий 1 - Однонаправленная выгрузка данных из критичного технологического сегмента



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

Сценарий 2 - Однонаправленная загрузка данных в защищаемую информационную систему



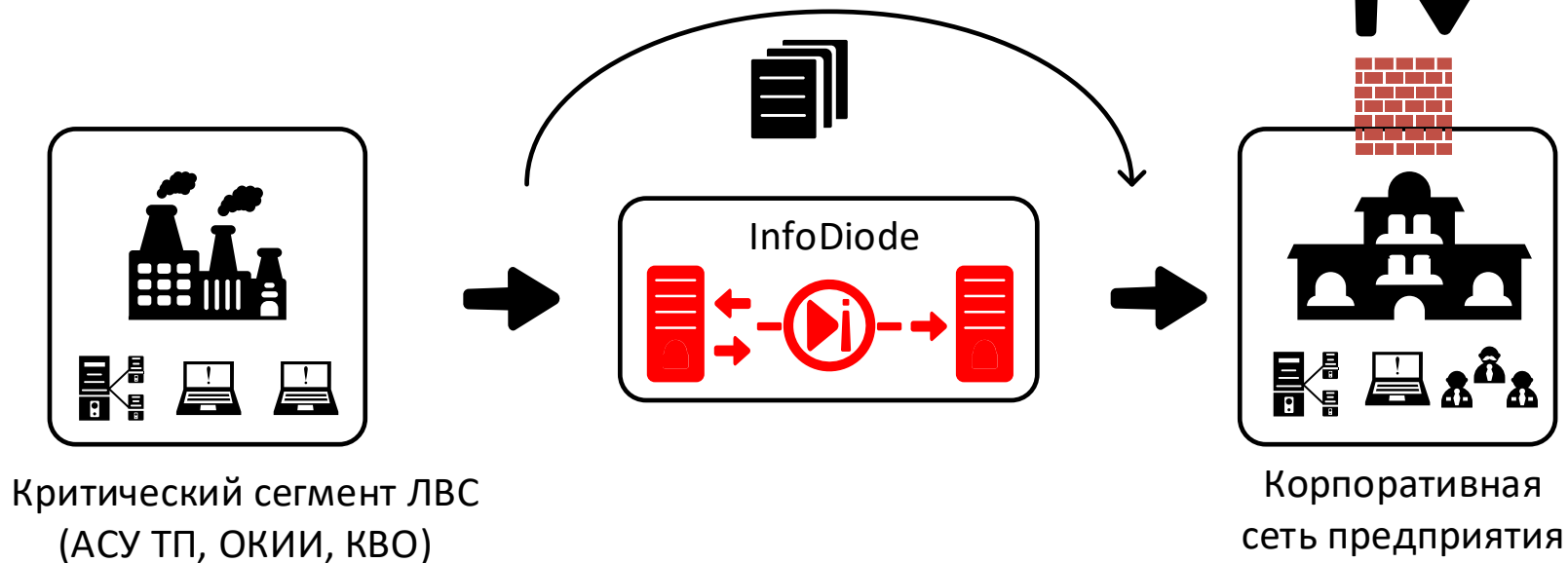
- **Загрузка** данных в конфиденциальные информационные системы
- **Нельзя, чтобы данные «утекли»** из крит. информационных систем
- Нужно исключить возможность управления объектом

Вариант 1. Экспорт данных

В данном сценарий обеспечивается гарантия целостности передаваемых данных.

- Экспорт данных для ситуационных центров
 - Реплика VM, баз данных
 - Передача разработанных дистрибутивов
 - Трансляция видео
- и т.п.

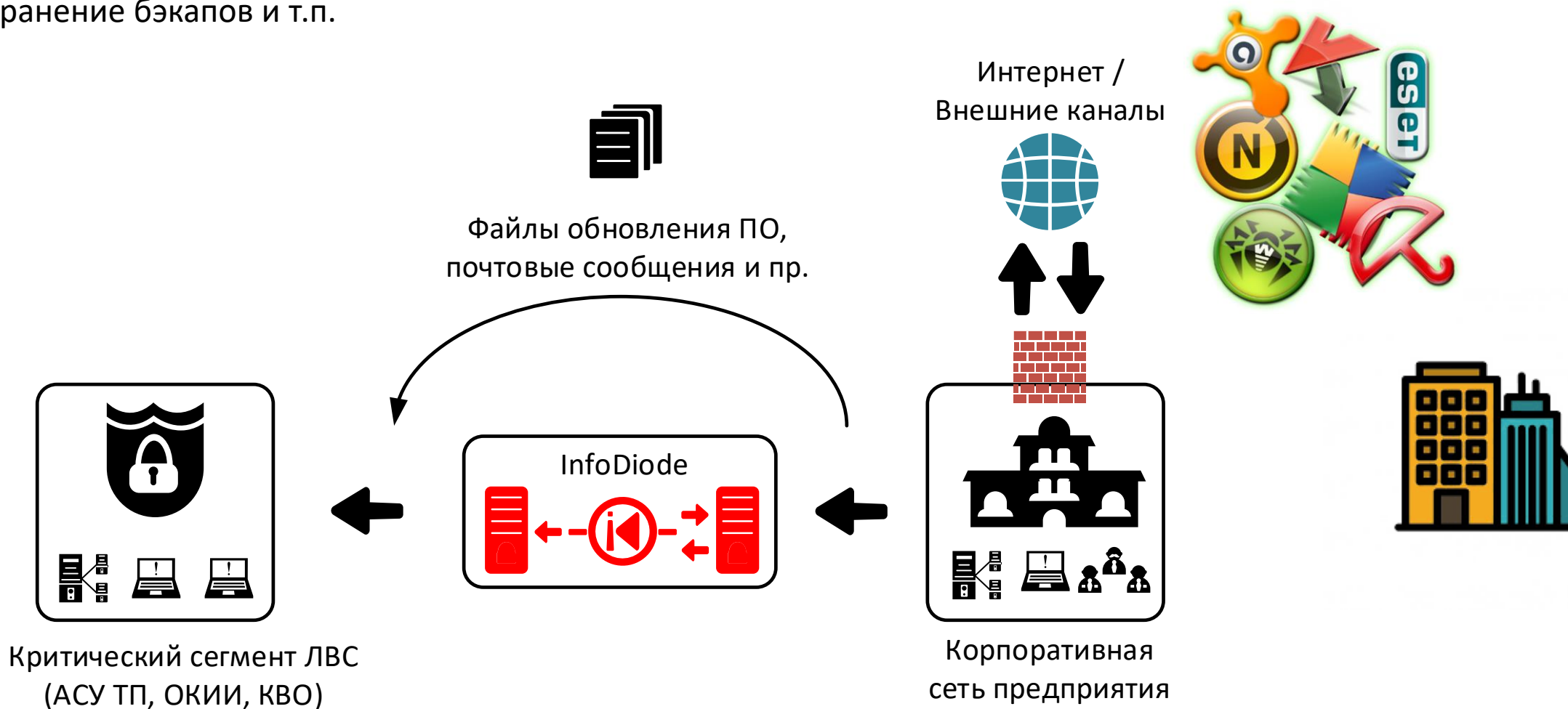
Журналы событий, почтовые сообщения,
промышленные протоколы, файлы и пр.
(CIFS, FTP, SMTP, Syslog)



Вариант 2. Импорт данных

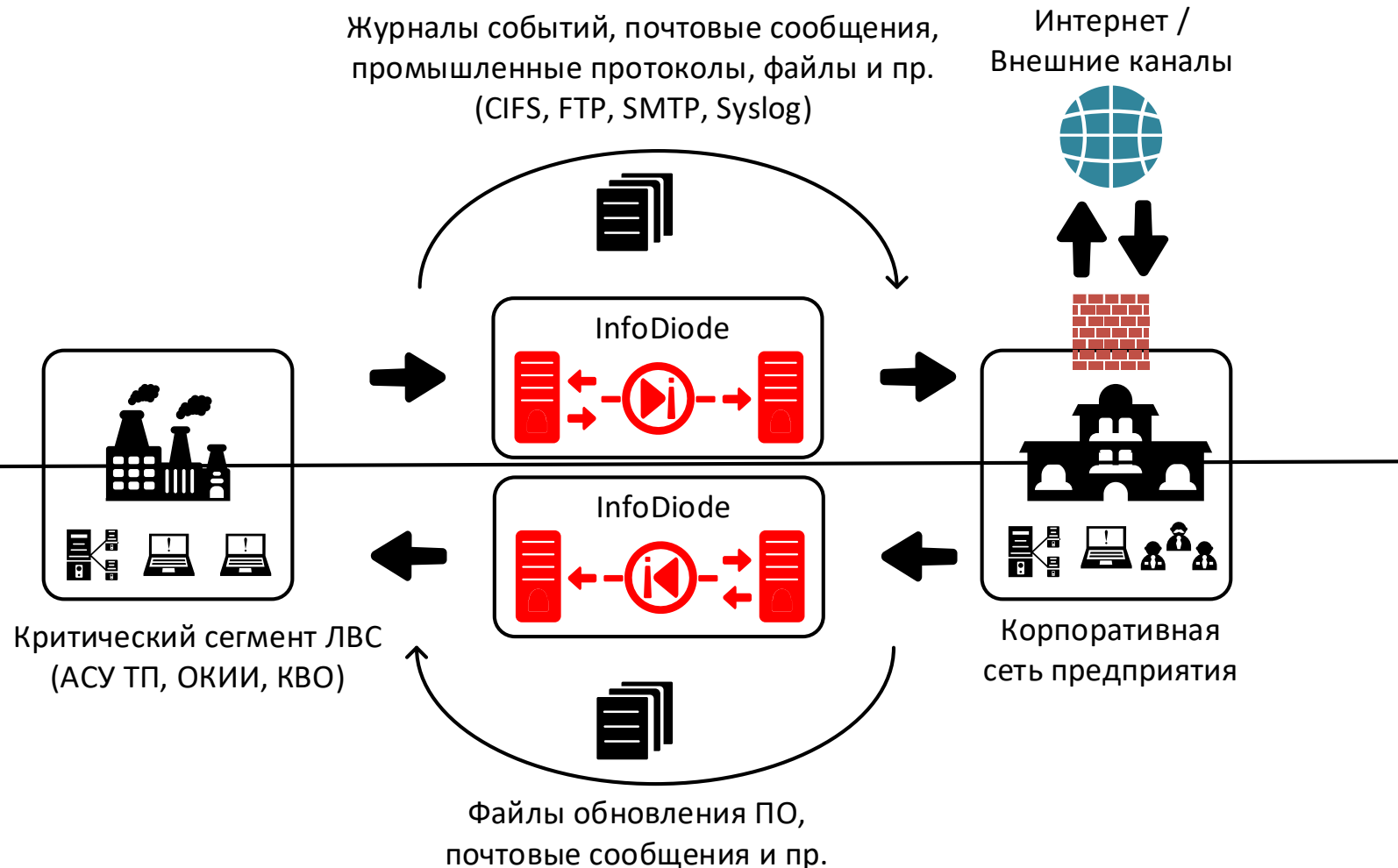
В данном сценарии обеспечивается гарантия конфиденциальности защищаемых данных.

- Загрузка обновлений
- Хранение бэкапов и т.п.



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



- 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



АСУ ТП

2

Агрегирующая
SCADA, MES, ERP, Hist.

Контроль и мониторинг
состояния «инфраструктуры»

АСУ ТП
локальная

3

СЦ,
Министерство, ГИС

Отчетность и контроль
ситуации



Предприятие



Полевой уровень

Сценарии применения АПК InfoDiode SMART могут быть типизированы

4



Головной
холдинг

Цепочки поставок и
номенклатуры



Предприятие

5



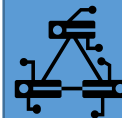
Интернет

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



- 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
- Toshiba Suite



Modbus



Промышленные
протоколы

Info
-Diode

Конвертеры



Удаленные
АРМ

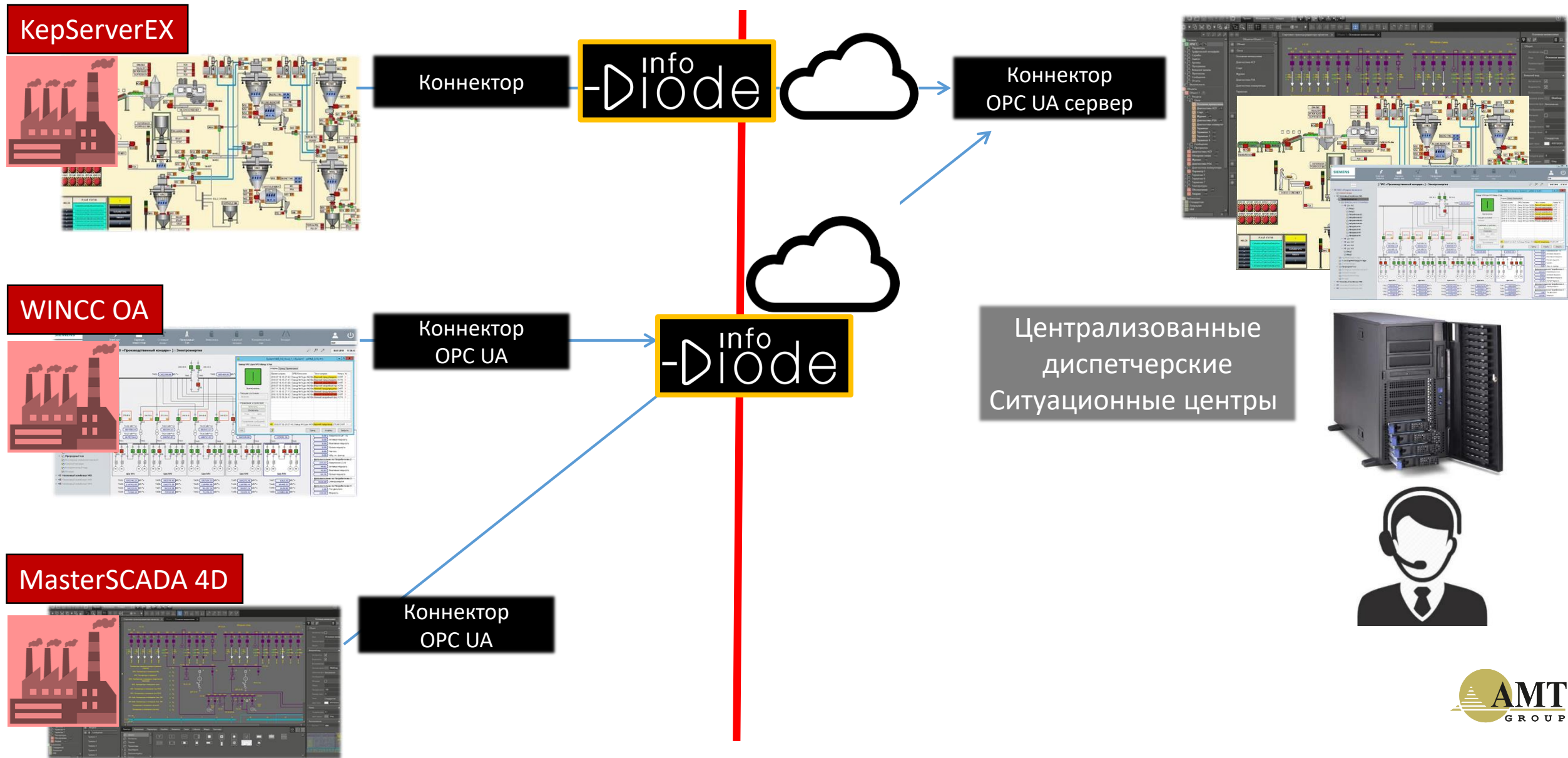


Ситуационные
центры

ДОВЕРЕННЫЙ СЕГМЕНТ
Управление оборудованием

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

АПК InfoDiode SMART позволяет собирать данные SCADA за границами периметра



- 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

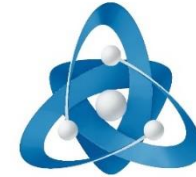


InfoDiode используется в:

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



Росфинмониторинг



РОСЭНЕРГОАТОМ
ЭЛЕКТРОЭНЕРГЕТИЧЕСКИЙ ДИВИЗИОН РОСАТОМА



Генеральная
прокуратура РФ



ЦИК



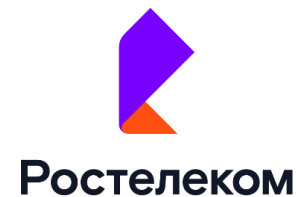
ФСТЭК



Министерство
здравоохранения РФ



НСПК
НАЦИОНАЛЬНАЯ
СИСТЕМА
ПЛАТЕЖНЫХ
КАРТ



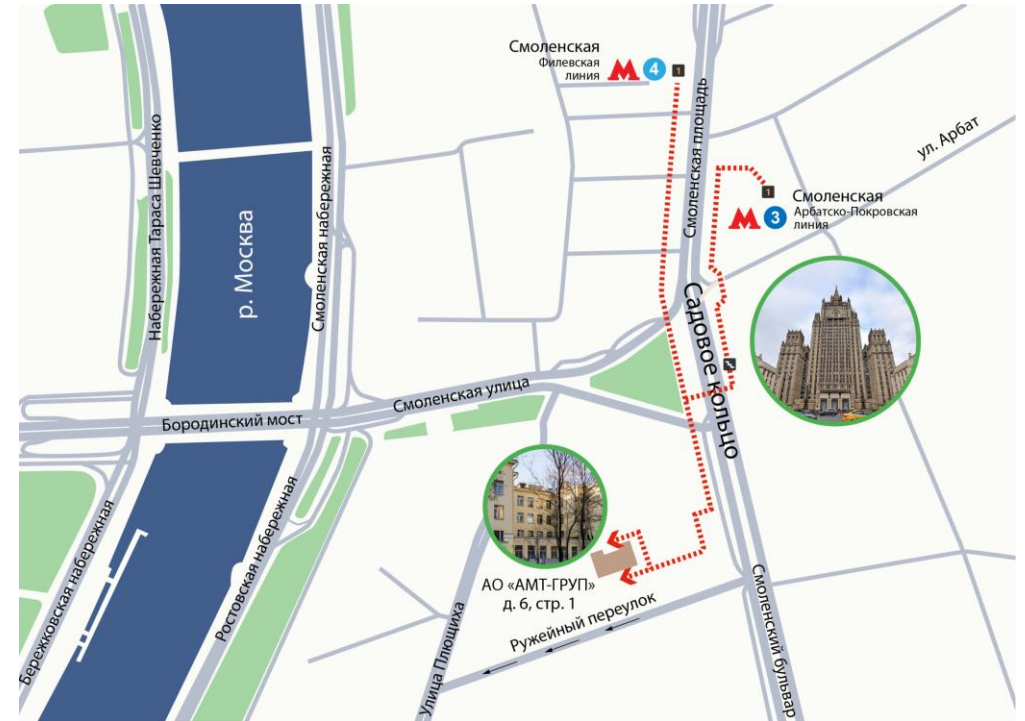
ЛИЦЕНЗИИ И ПОДДЕРЖКА ВНЕДРЕНИЯ INFODIODE



- 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



- 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!