28.06.2024

АМТ-ГРУП

Практика применения решений InfoDiode в качестве элемента комплексной защиты АСУ ТП

Волков Пётр – ведущий аналитик АМТ-ГРУП

Цифровая трансформация предприятия требует неразрывности информационных потоков

- АСУ ТП участвует во множестве взаимодействий с различными информационными системами:
  - Управление производством (MES)
  - Анализ данных (в т.ч. предиктивный анализ на основе ML)
  - Системы архивирования данных
  - Поддержка ПО, ИТ-поддержка
  - Системы безопасности (как информационной, так и общей)
  - Диспетчерские
  - Техническая поддержка
- Политика ИБ требует изоляции АСУ ТП и ОКИИ от любых внешних воздействий

Однонаправленные шлюзы в качестве элемента комплексной защиты АСУ ТП

Комплексный подход для предотвращения разных классов атак

Разнообразие защищаемых объектов:

- ❑ Защита удалённого подключения
- ❑ Защита на границе сегментов
- ❑ Защита обособленных и смежных сегментов
- ❑ Защита в сети IT
- ❑ Защита внутри сети OT (промышленные протоколы)
- ❑ …

Разнообразие средств защиты:

- ❑ Аутентификация и авторизация
- ❑ Обновления ПО
- ❑ Антивирусная защита
- ❑ Firewall
- ❑ Диод
- ❑ DLP
- ❑ SOC/SIEM
- ❑ …

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

Разные средства являются частью стратегии и имеют разную степень эффективности

- **Антивирус** – не всегда может противостоять распространению вредоносного ПО, поскольку сигнатуры такого ПО могут поступать позже, чем запустится ПО

- **Патчи ПО в части безопасности** – не всегда могут обеспечить закрытие эксплойтов известных уязвимостей. Требуется время на проверку совместимости обновления с инфраструктурой, на его получение, установку и т.п. Иногда обновления могут быть ошибочными

- **Системы обнаружения вторжений** – являются детективными, но не превентивными мерами защиты. Они способствуют оперативному выявлению проблемы, ее локализации, но требуют времени на реагирование, которое может быть использовано вредоносным ПО для реализации атаки

Гарантированная однонаправленность

- **Однонаправленные шлюзы** – физически способны передавать информацию только в одном направлении – от критически важной сети к ИТ/корпоративной/интернет-сети, не имея возможности доставлять информацию обратно.
  - В однонаправленно защищенных сетях ни один управляющий сигнал физически не может быть передан внутрь сегмента

Политика нулевого доверия может быть эффективно построена именно на диодах

Software

- Уязвимость «нулевого дня» и др. уязвимости
- Скорость распространения атаки vs скорость распространения защиты
- Общедоступность средств атаки
- Особенности конфигурирования сами могут приводить к проблемам
- Открыто декларируются бэкдоры и workaround для многих Firewall

Hardware

- Работают на аппаратных принципах – физически изолируют сеть
- Невозможно взломать, взлом ПО на АПК не приводит к нарушению функции безопасности
- Аппаратные решения вообще не имеют софта и неуязвимы для стороннего софта
- Удаленное конфигурирование в целях «взлома» невозможно

Практика применения решений InfoDiode

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

DIASOFT всё по-настоящему
МОНИТОР ЭЛЕКТРИК
ТЕРРАЛИНК ТЕХНОЛОДЖИС
КРУГ
Wonderware Historian
kepware
Decima
СВД Встраиваемые Системы
MasterOPC www.masteropc.ru
ISS
ИНДАСОФТ ЦИФРОВИЗАЦИЯ ПРОИЗВОДСТВА
Атомик Софт
MasterSCADA
NAUMEN
WinCC Professional
TIA V17

PostgreSQL
Windows Server Update Services
Microsoft SQL Server
ELK
ZABBIX
kafka
RabbitMQ

Kaspersky Private Security Network
КВАЗАР
ARMA INFOWATCH ARMA
CyberLympha DATAPK
MaxPatrol SIEM
PT ISIM
Kaspersky Industrial CyberSecurity
axxtel
HONEY CORN
InfoDiode
AMT GROUP

InfoDiode.ru

InfoDiode применяется в различных отраслях, накоплен значительный опыт

ОТРАСЛИ

- Энергетика
  - Электрогенерация
  - Электрораспределительные сети
- Добыча полезных ископаемых
  - Добыча углеводородов
  - Горнодобывающая промышленность
  - Горно-обогатительные комбинаты
- Промышленность
  - Промышленное производство
  - Химическая промышленность
  - Нефтепереработка
- Транспортировка углеводородов
- Управление транспортом
  - РЖД
- Финансовые организации и банки
- Здравоохранение
- Информационные агентства

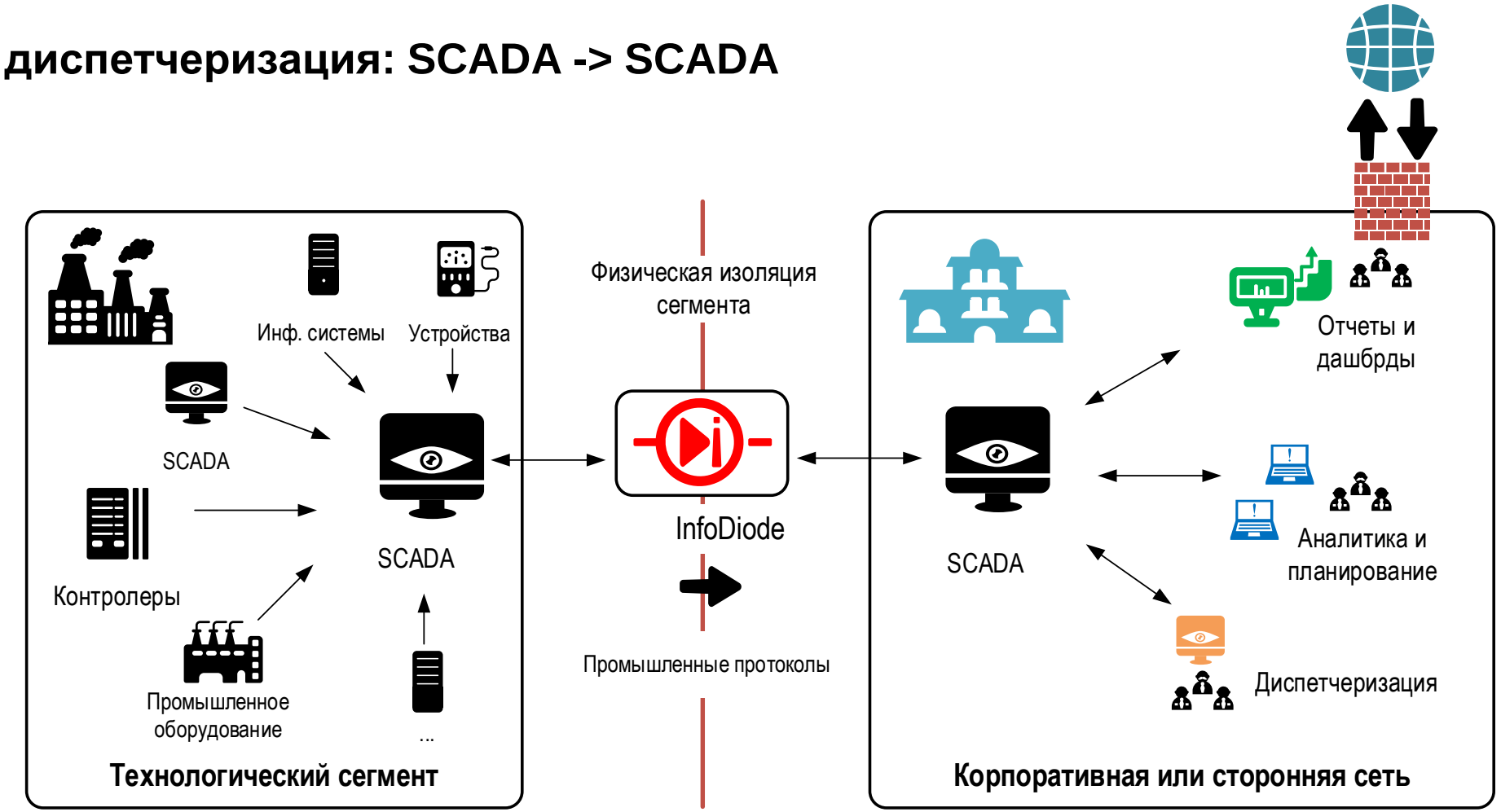
ЦЕЛИ

- АСУТП
  - Цифровые двойники
  - Аналитика
  - Управление
  - Получение данных от датчиков
- ИБ
  - Обновление: KPSN
  - Ловушки (Deception)
  - Изоляция «песочницы»
  - Обнаружение вторжений
- Диспетчеризация
  - SOC/NOC
  - Оповещения
  - Видеонаблюдение
- Техподдержка
  - Трансляция экранов АРМ
- Прикладные
  - Обновление WSUS
  - Бэкапы

Односторонняя отправка данных из АСУТП для мониторинга и контроля

Цифровые двойники и диспетчеризация: SCADA -> SCADA

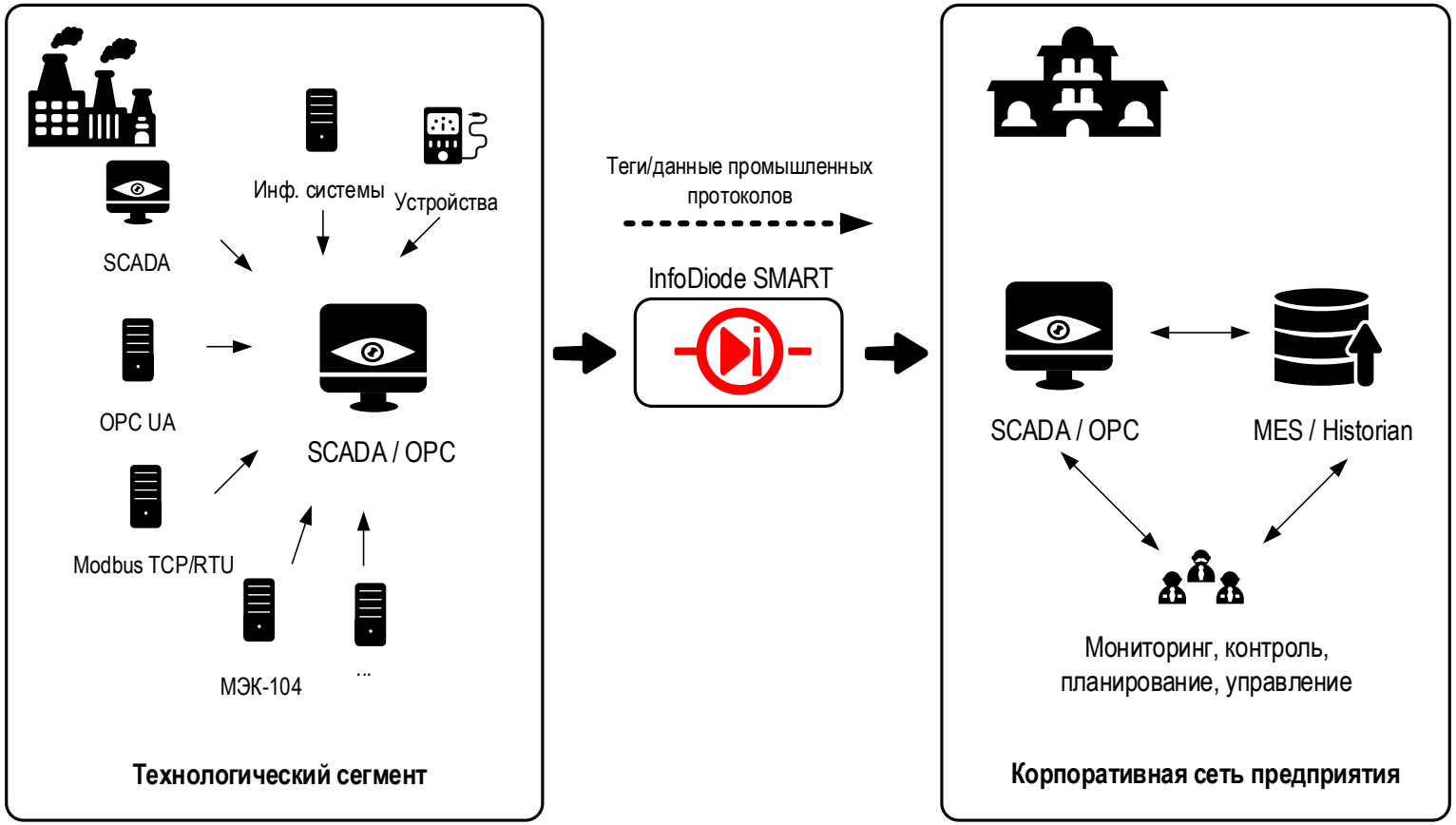
- Alpha.SCADA
- IIoT.Istok
- MasterSCADA
- КОТМИ-14
- СК-11
- СДКУ «Фокус»



Накопение данных из АСУТП для анализа и систематизации

Системы управления производством и аналитика: SCADA -> MES / Historian

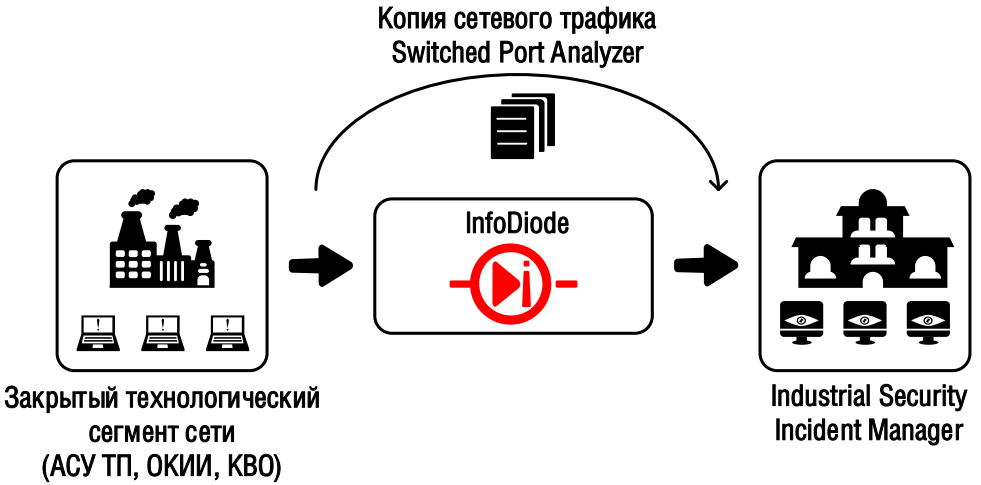
- TL.Solutions
- I-DS (Indusoft Digital Services)
- Aveva/Wonderware Historian



Односторонняя отправка данных ИБ в SOC и средства ИБ

Мониторинг сети

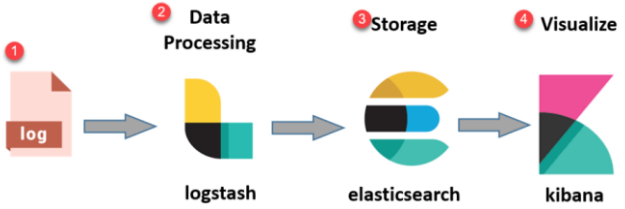
- Передача копии технологического трафика закрытого сегмента во внешнюю систему мониторинга с использованием SPAN
- Передача событий технологической сети с использованием Syslog на внешнюю систему мониторинга
- Передача оповещений безопасности с «сенсоров»



Kaspersky Industrial CyberSecurity

CyberLympha DATAPK

PT ISIM

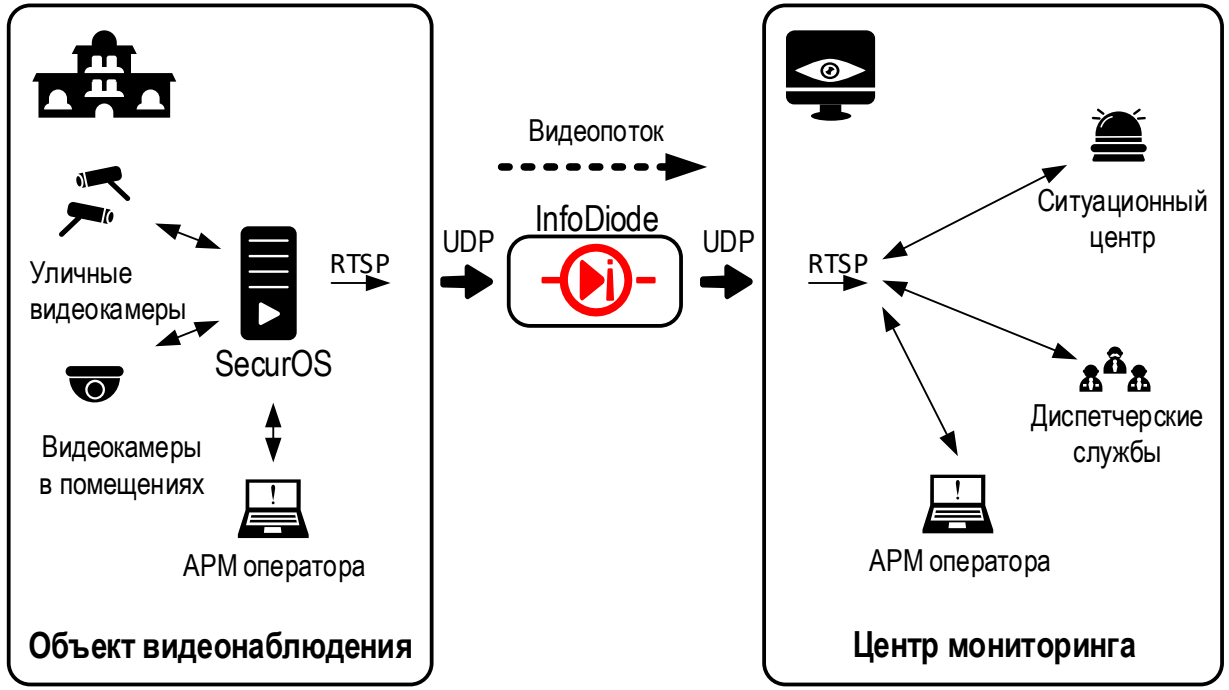


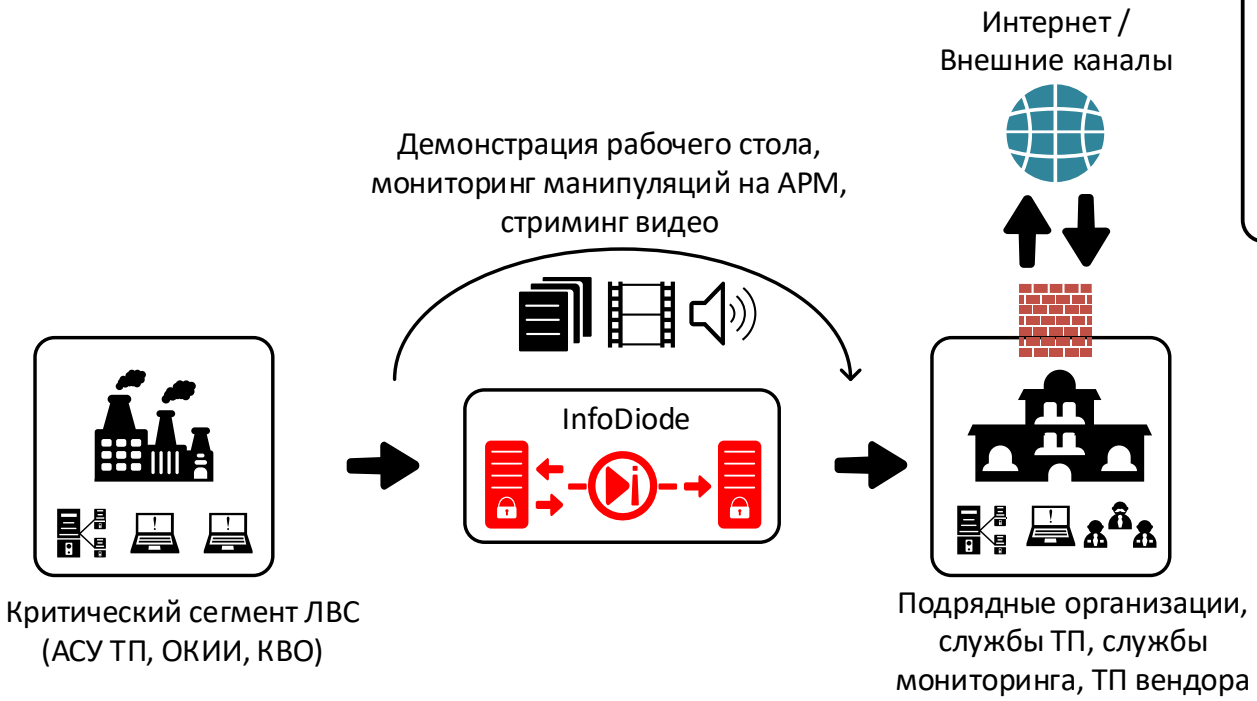
InfoDiode.ru

Односторонняя отправка данных для наблюдения и тех. поддержки

Мониторинг окружения

- Трансляция видео с камер видеонаблюдения.
  - Напрямую с видеокамер
  - С видеосервера (SecurOS)
- Демонстрация рабочего стола оператора.



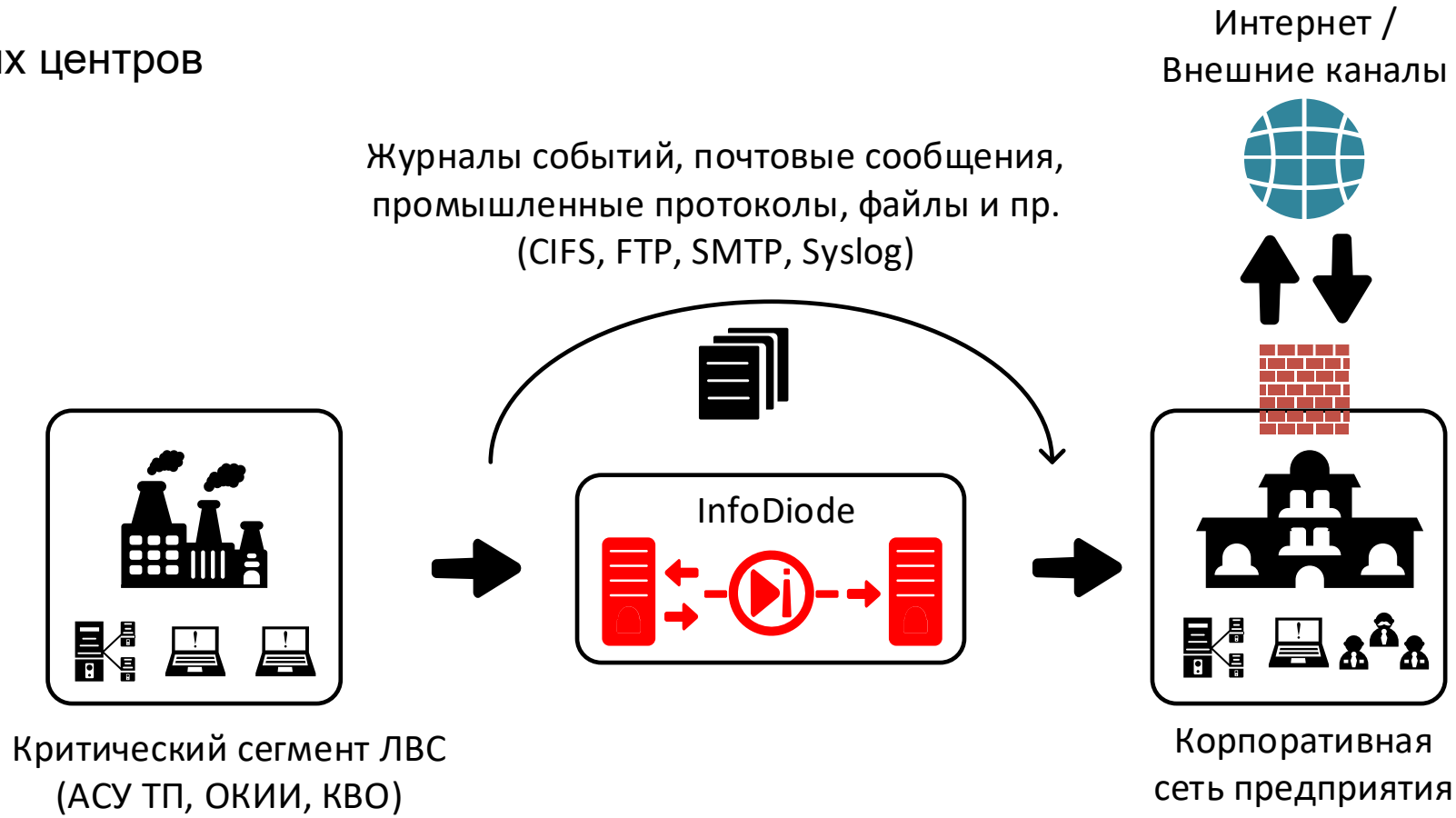


InfoDiode.ru

Односторонняя отправка данных файловыми потоками

Экспорт данных

- Экспорт данных для ситуационных центров
- Реплика ВМ, баз данных

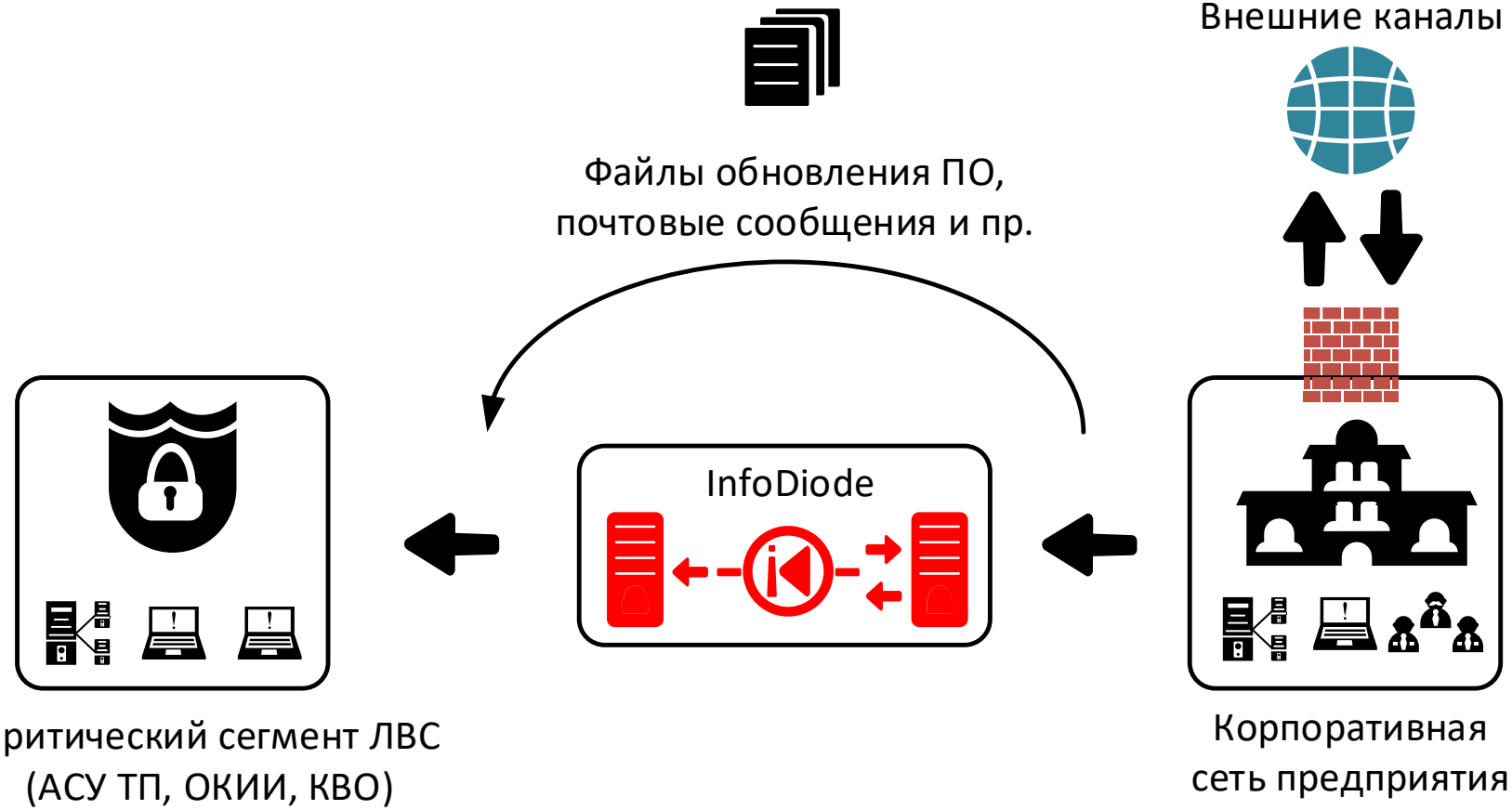


Одностороннее получение обновлений в АСУТП

Загрузка обновлений

- WSUS
- прошивки
- антивирусные базы

и т.п.



InfoDiode

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

InfoDiode.ru

АПК InfoDiode PRO - позволяют передавать файловый и иной трафик по однонаправленному каналу

АПК INFODIODE PRO

- **Многофункциональный** (передает несколько видов протоколов и видов трафика одновременно: например, видео, файлы), имеет много апробированных сценариев реализации: репликация СУБД, ВМ, обновление ПО и т.п.
- **Высокопроизводительный** в части файловой передачи, в том числе реализует приоритезацию трафика, деление канала и т.п.
- **Поддерживает широкий спектр файловых протоколов** (FTP/FTPS, SMB, SMTP, UDP, SFTP)
- **Высокая надёжность** – кластерный вариант
- **Интегрируется в ИТ/ИБ ландшафт** (SIEM, SNMP, AD, Syslog, NTP…)
- **Реализован на российской платформе**, российском программном обеспечении производства АМТ-ГРУП

InfoDiode.ru

АПК InfoDiode SMART – решение для использования с АСУ ТП

АПК INFODIODE SMART

- **Компактный – 1U rack решение**
- **Поддерживает промышленные протоколы**
- **Многофункциональный**
  передает несколько видов трафика одновременно: например, видео, файлы, пром. протоколы
- **Предоставляет возможность разрабатывать собственные коннекторы** под конкретные задачи и для передачи требуемых промышленных протоколов
- **Реализован на российской платформе**, российском программном обеспечении производства АМТ-ГРУП

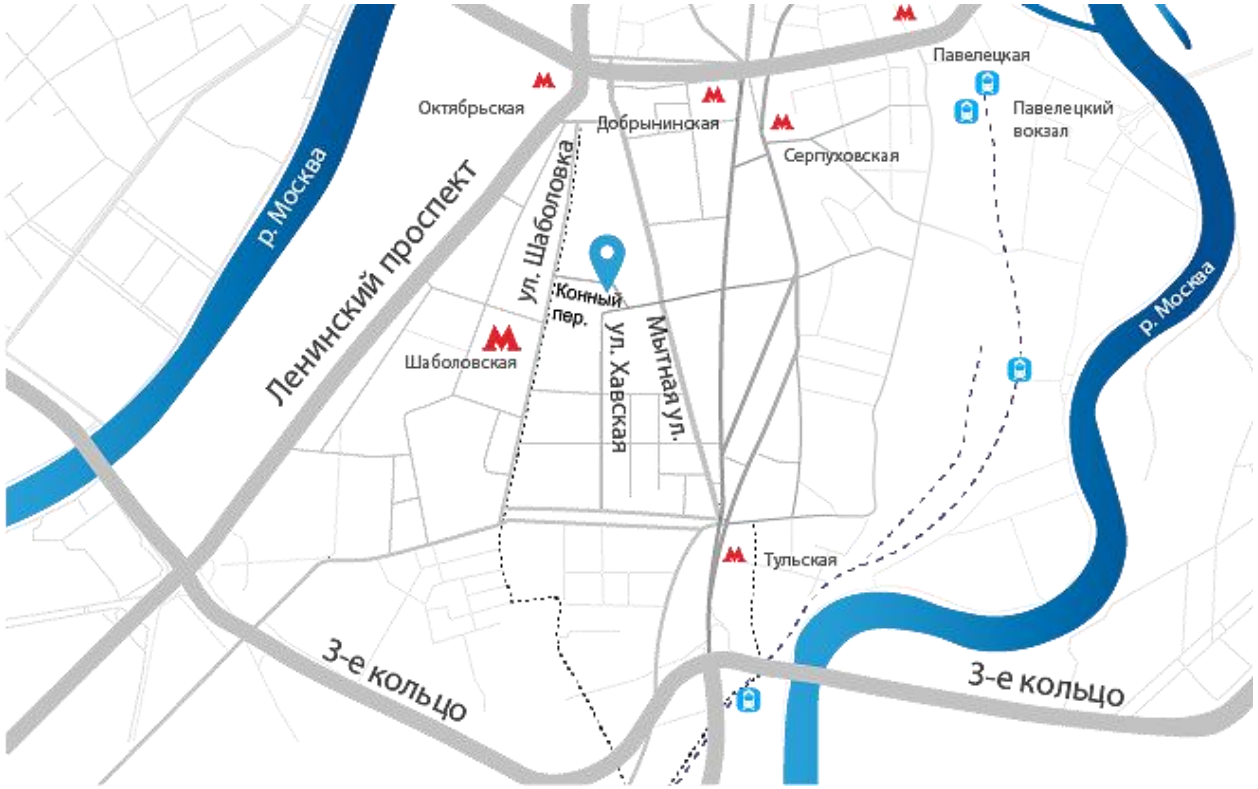
InfoDiode включен в реестры, завершена его сертификация

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

InfoDiode.ru

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!