
10.02.2022

# АМТ-ГРУП

## Практические сценарии применения комплексов InfoDiode для защиты доверенных сегментов АСУ ТП

1. Какие бывают «диоды»

2. Какие бывают сценарии применения «диодов»

# 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

# Виды диодов

# 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**

InfoDiode.ru

# 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

info Diode
AMT GROUP

InfoDiode.ru

# Сценарии применения диодов

# Сценарии применения «диодов» 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 «диодов» 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 «диодов» 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

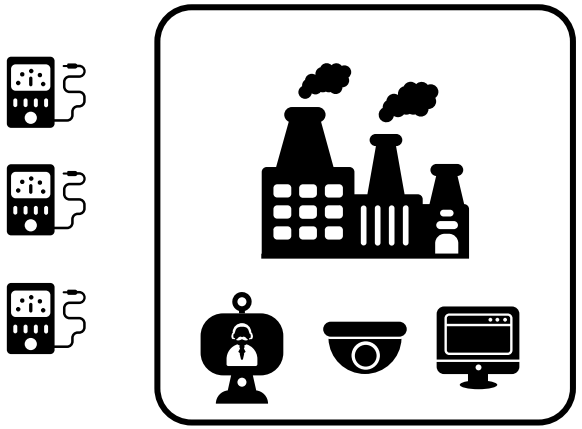
Данные для инфоматов, визуальные панели,

Организация

Полевой уровень

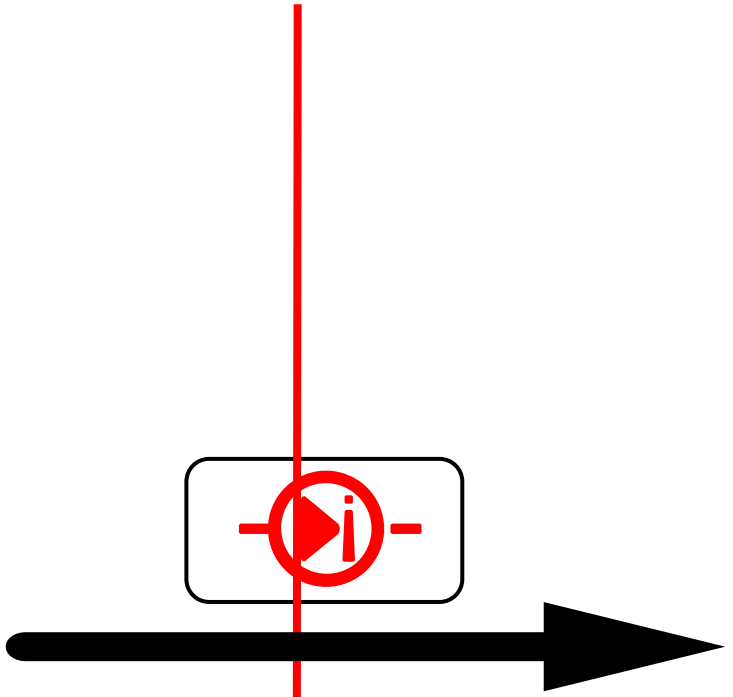
# Деление на домены с локализацией данных и управления - это естественный процесс

- Целостность/Полезность
- Доступность
- Конфиденциальность
- Контроль/Надежность



Данные

Управление

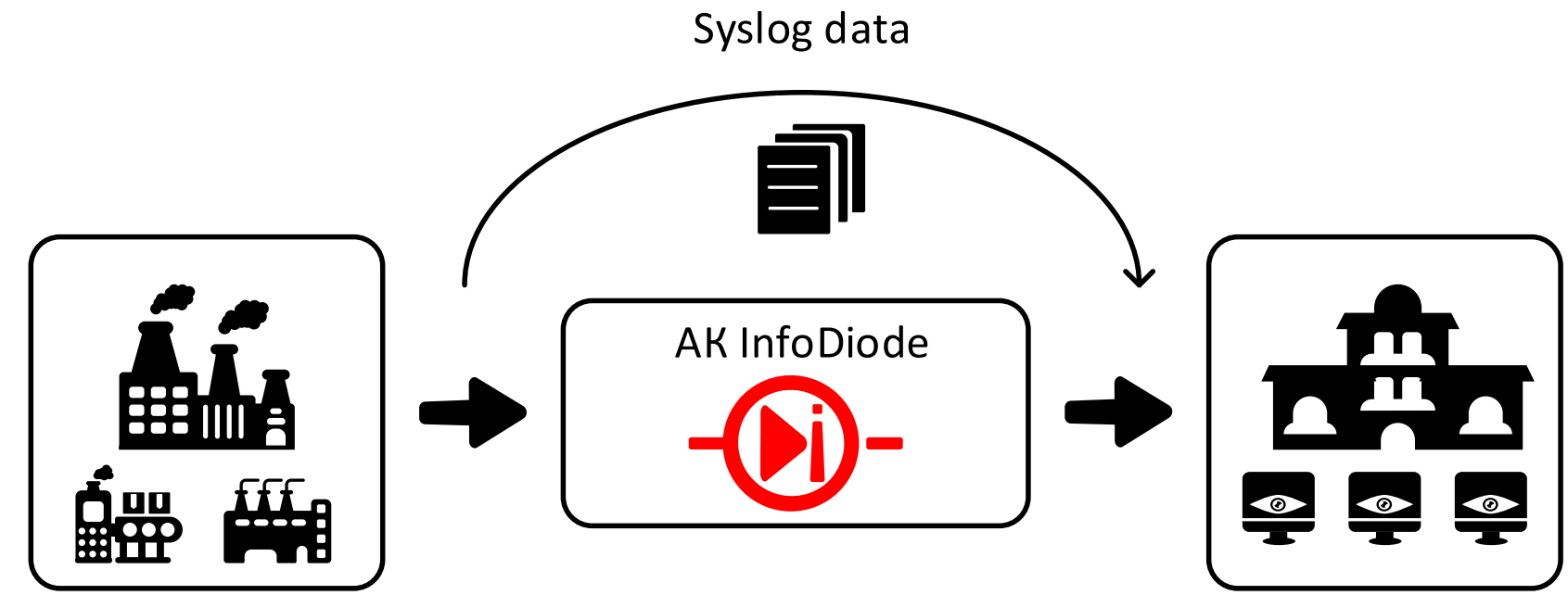


- Анализ
- Мониторинг
- Контроль
- Планирование

Доверенный сегмент (домен)

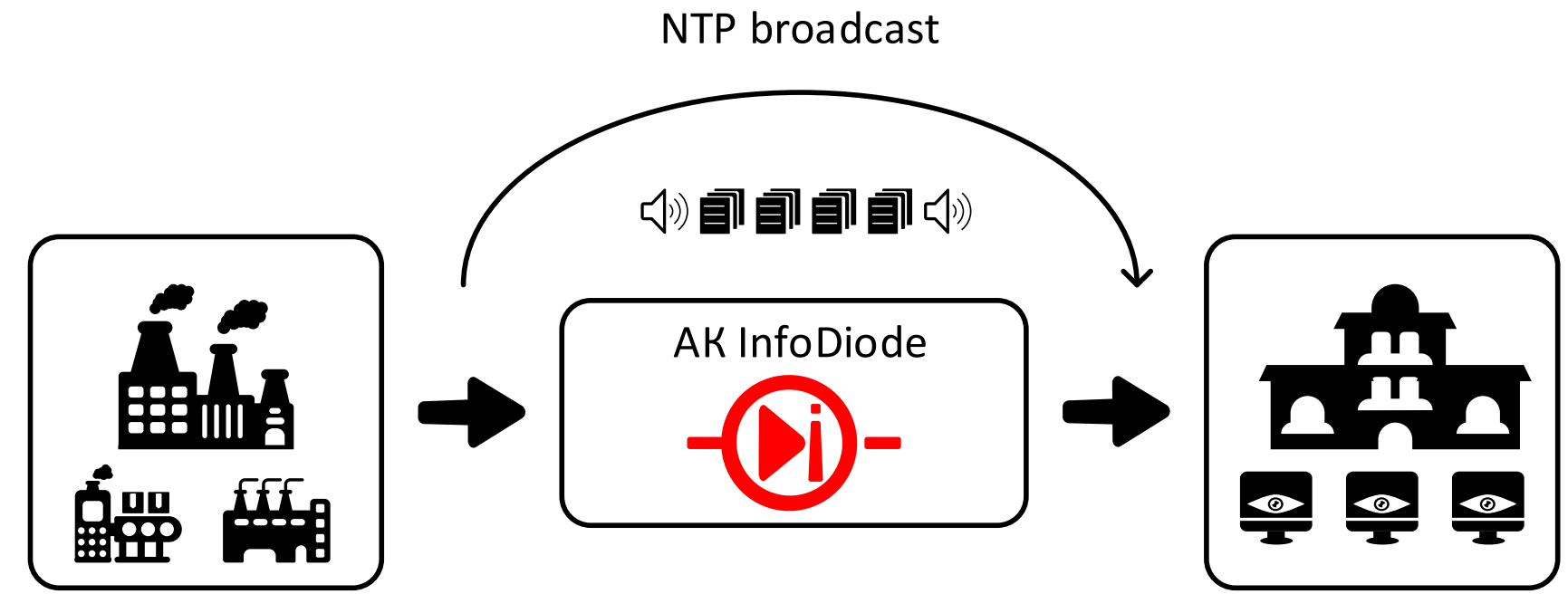
Недоверенный сегмент (домен)

# Передача Syslog трафика для целей сбора и мониторинга




Контроль состояния информационных систем и ресурсов, сбор диагностических данных, алертинг

# Передача NTP – такты времени

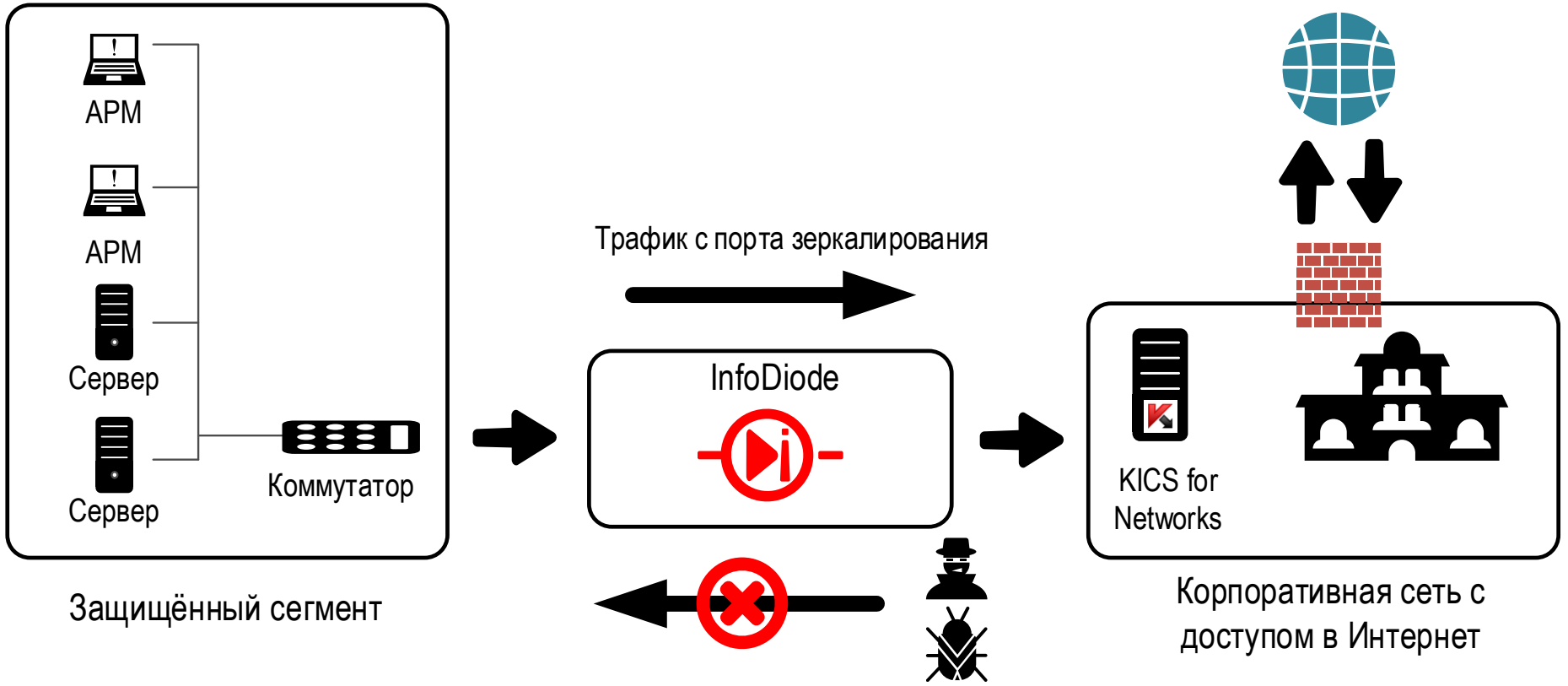



Закрытый технологический сегмент сети (АСУ ТП, ОКИИ, КВО)

Ситуационный центр
Мониторинг событий

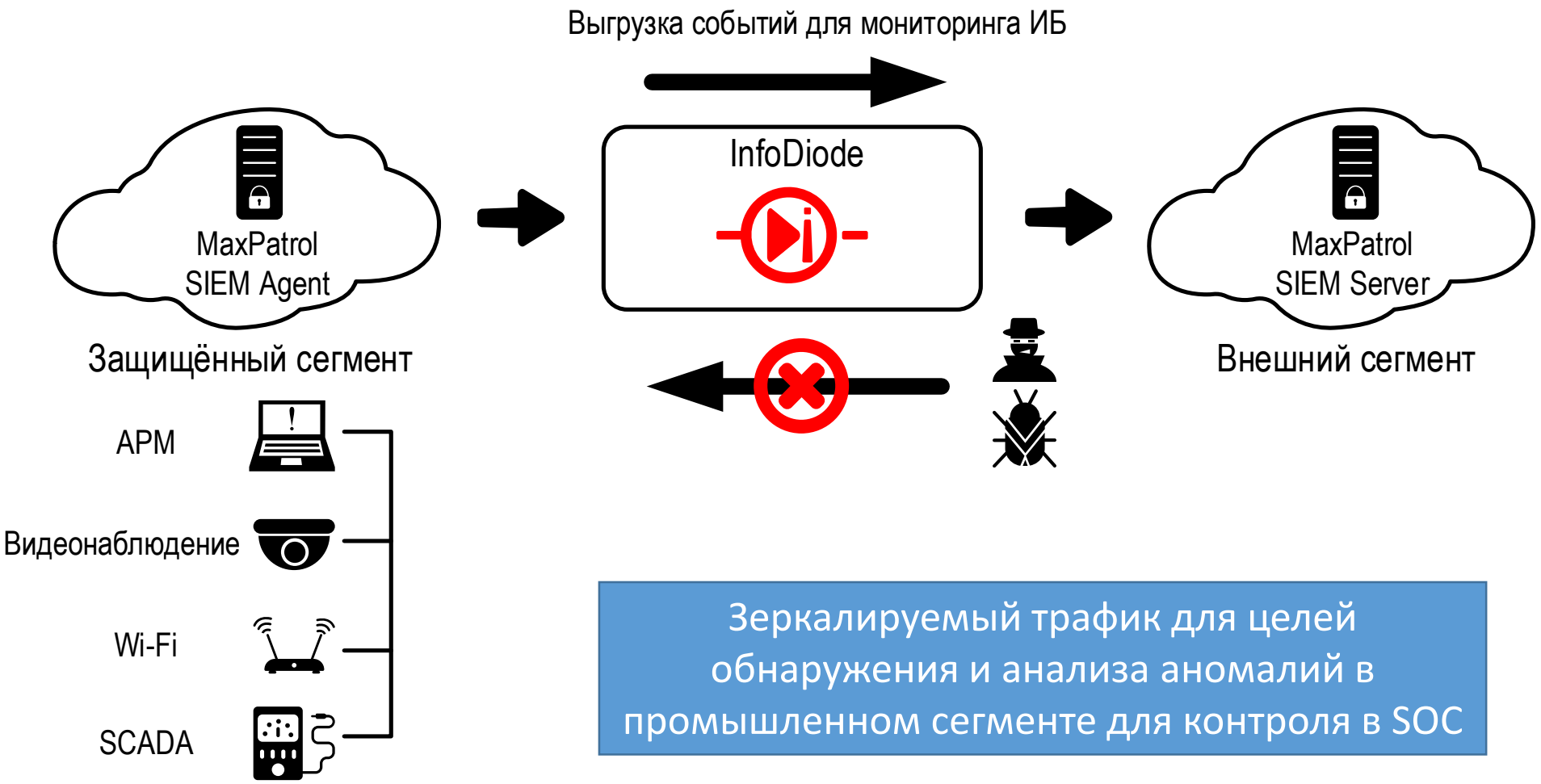
Широковещательные рассылки NTP, такты времени для внешних потребителей

# Работа с IDS/IPS системами KICS for Networks (Kaspersky)



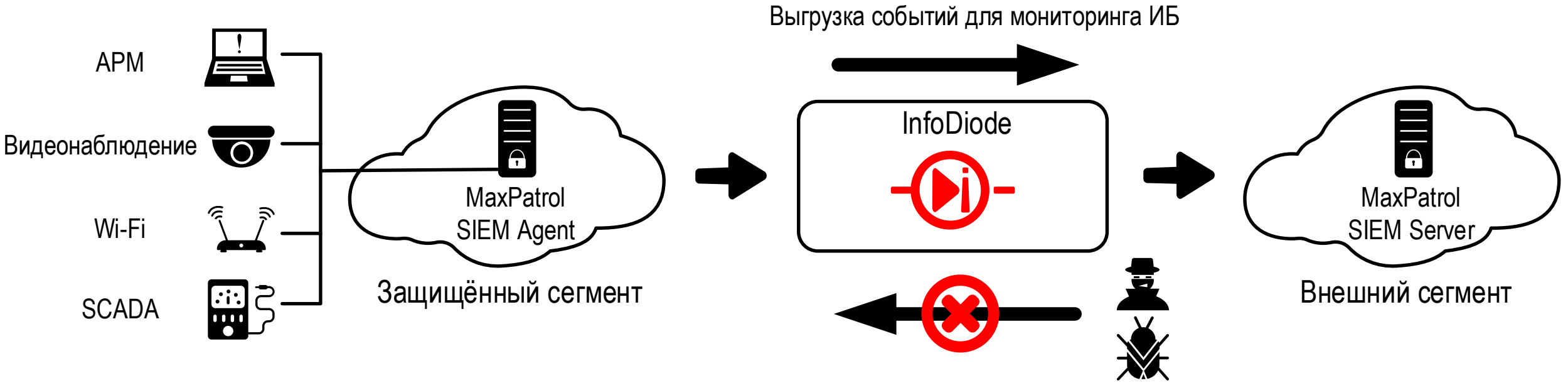

Зеркалируемый трафик для целей обнаружения и анализа аномалий в промышленном сегменте для контроля в SOC

# Работа с IDS/IPS системами PT ISIM (Positive Technologies)



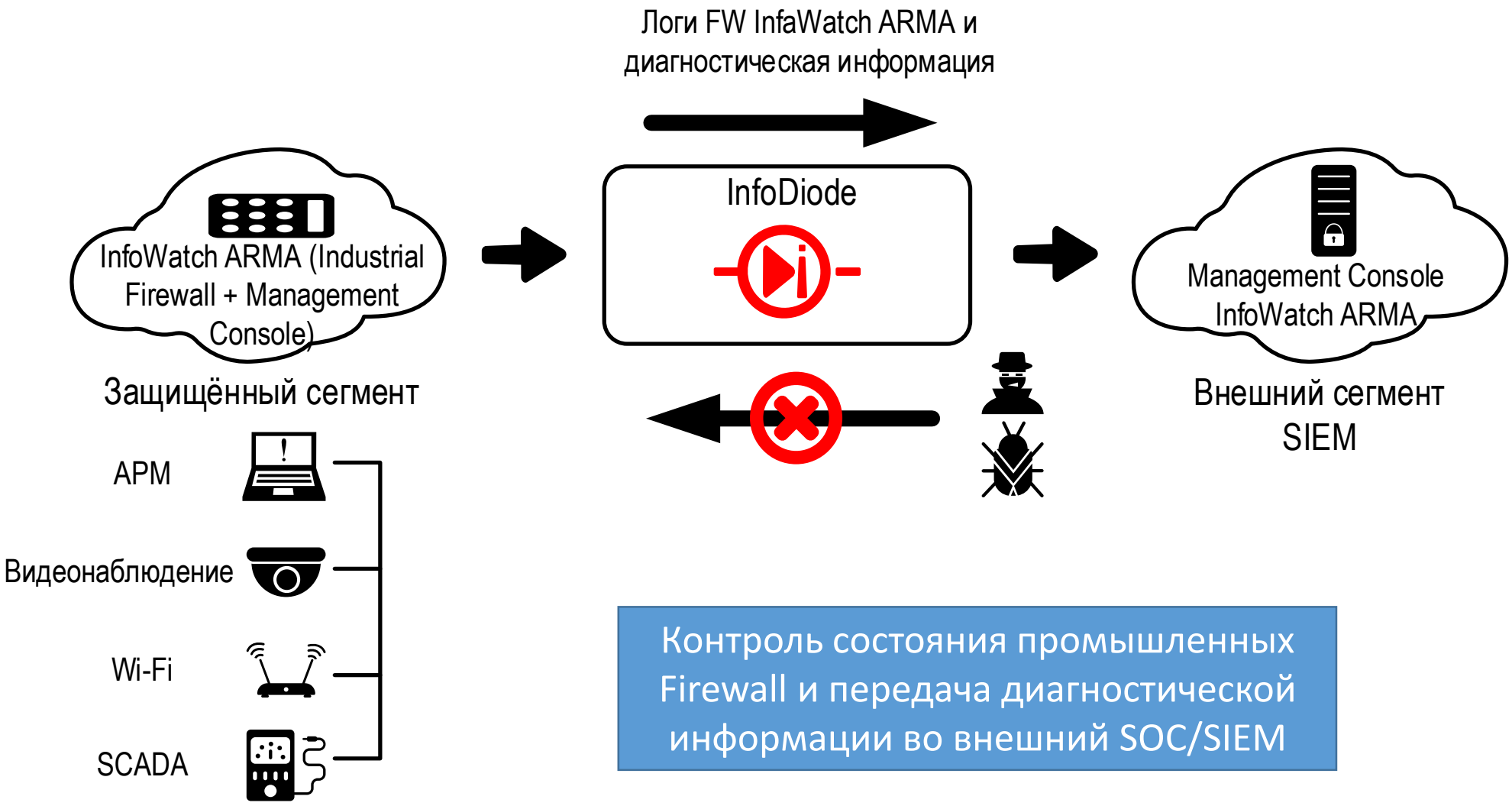

Зеркалируемый трафик для целей обнаружения и анализа аномалий в промышленном сегменте для контроля в SOC

# Работа с системами контроля защищенности MaxPatrol (Positive Technologies)



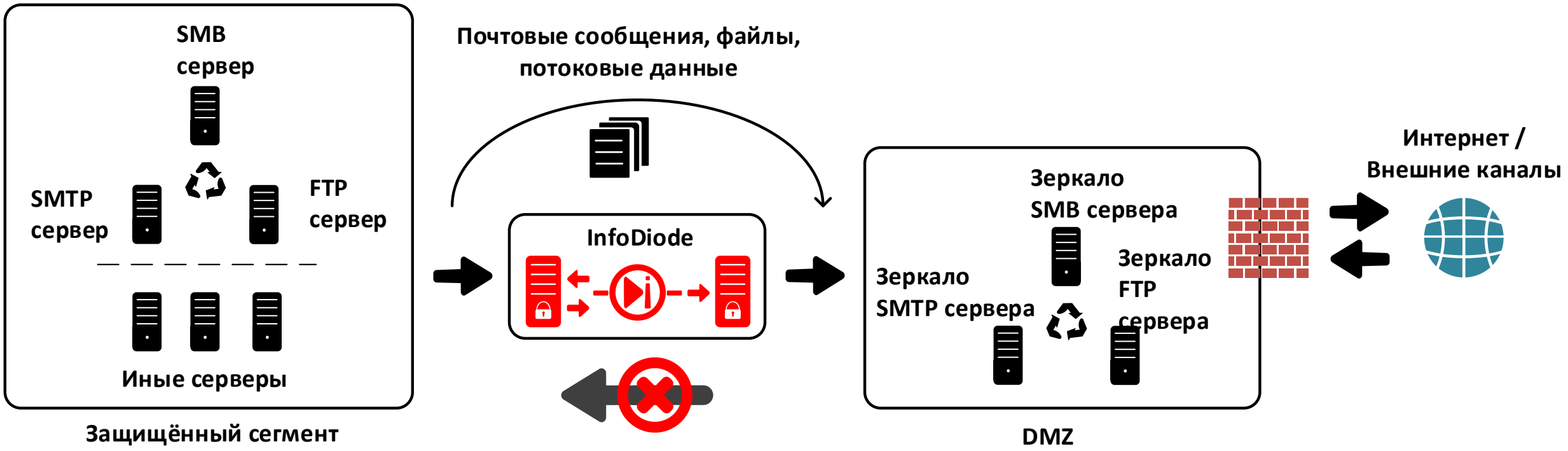

Логи с АРМ (Windows, Linux) в доверенном сегменте для целей контроля средствами SIEM (SOC)

# Получение диагностических данных от пром. Firewall и передача их в SIEM



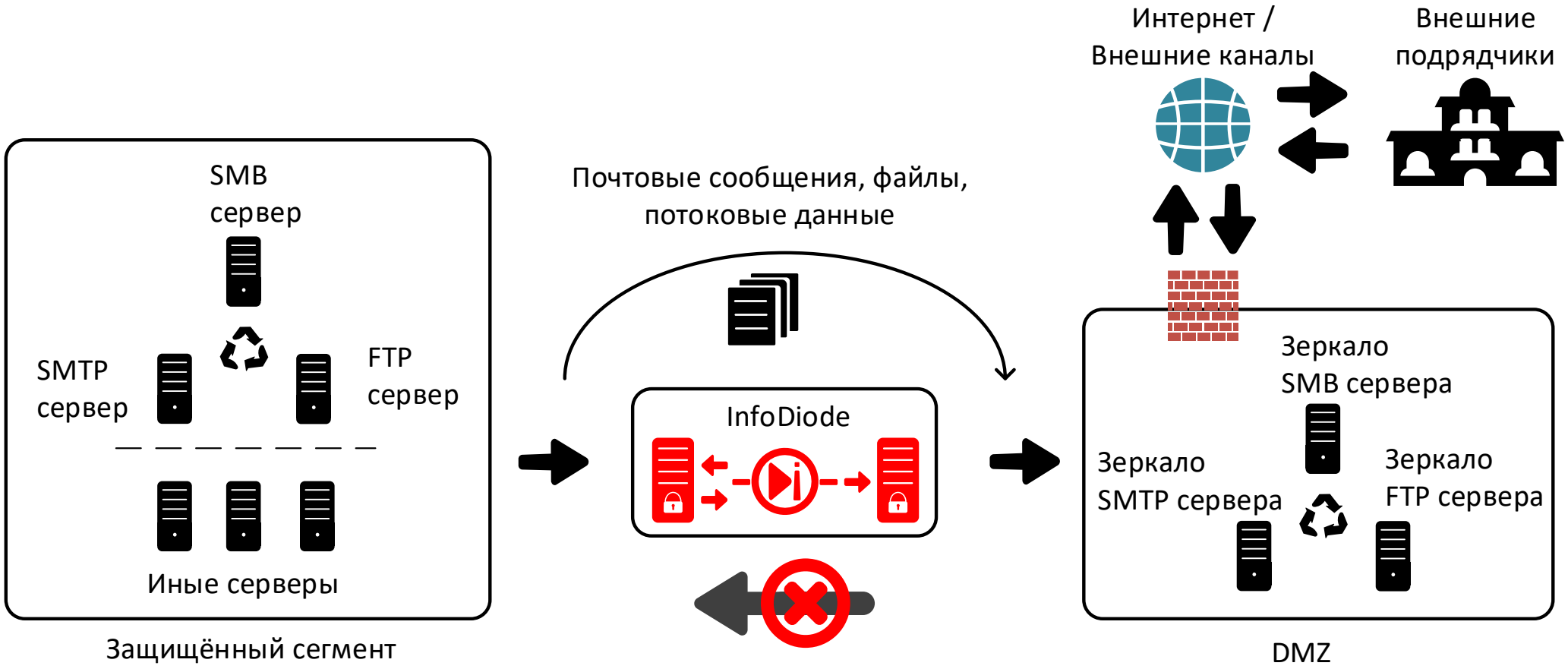

Контроль состояния промышленных Firewall и передача диагностической информации во внешний SOC/SIEM

# Передача электронной почты внешним потребителям




Пересылка почтовых сообщений потребителям вне закрытого сегмента

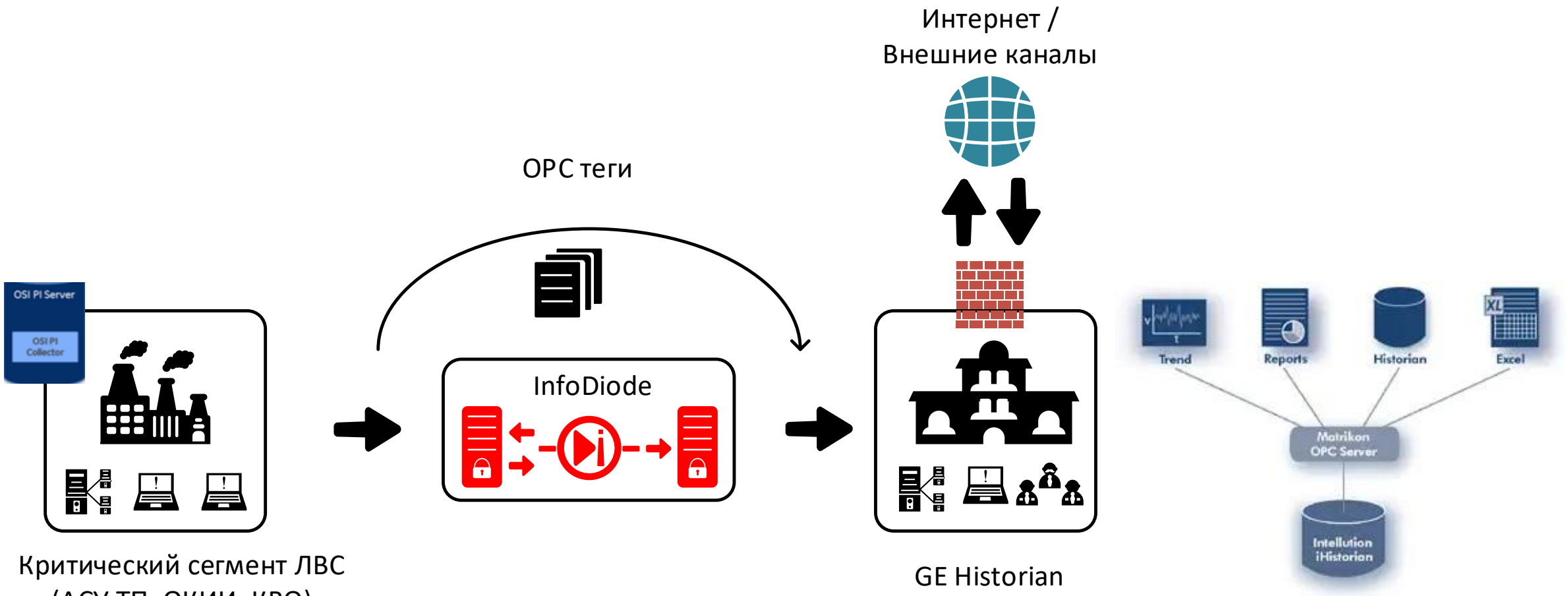
# Передача файловой информации внешним потребителям




Обмен файловыми данными с внешними потребителями, в том числе уведомление внешних систем о поступлении данных – POST запросы, SIEM события

InfoDiode.ru

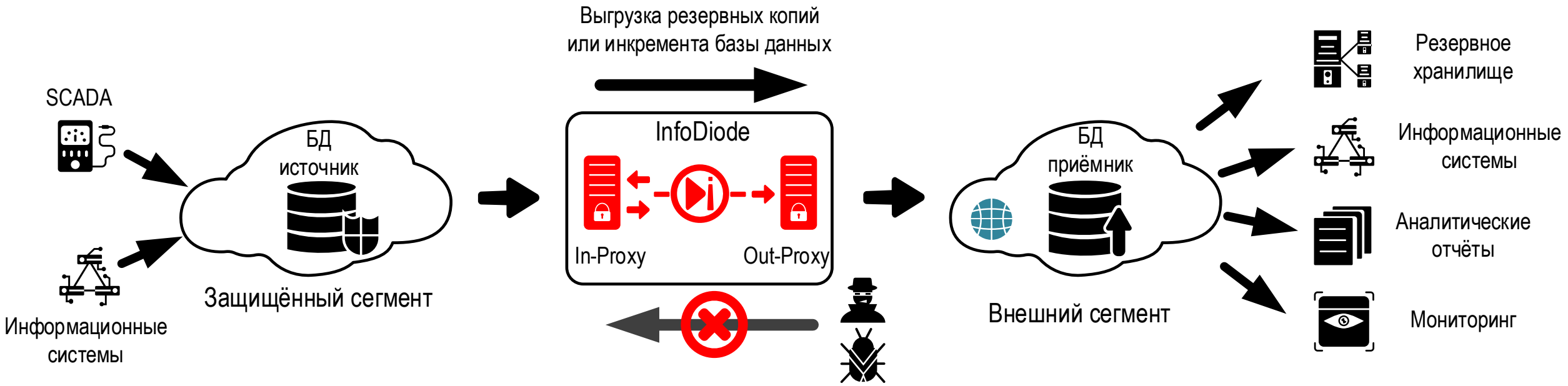
# Передача OPC тегов через инструменты General Electric ETL во внешнее хранилище




Передача OPC тегов для целей накопления и анализа средствами iHistorian и GE Proficy Historian

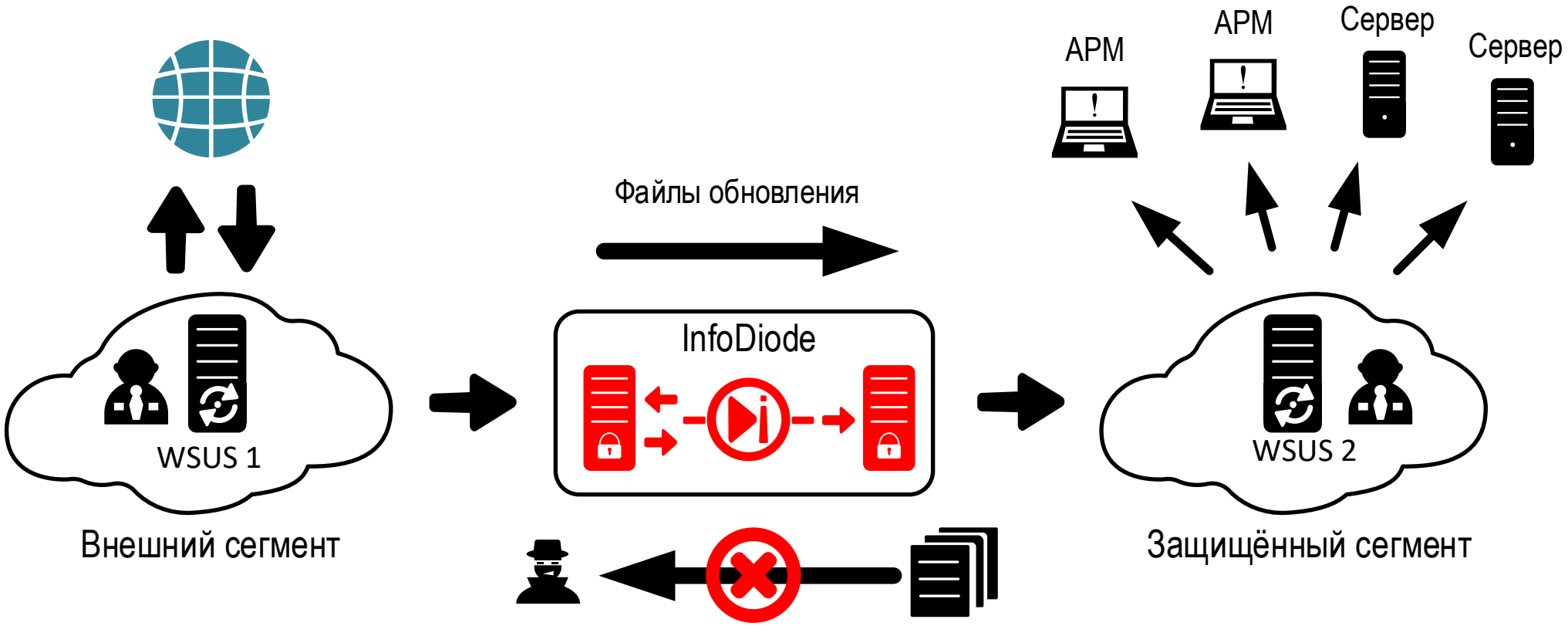
InfoDiode.ru

# Передача инкрементальных и полных реплик СУБД MS SQL/Postgre SQL




Инкрементальный (частотой до 5 секунд) обмен инкрементом БД и полный бэкап БД по расписанию

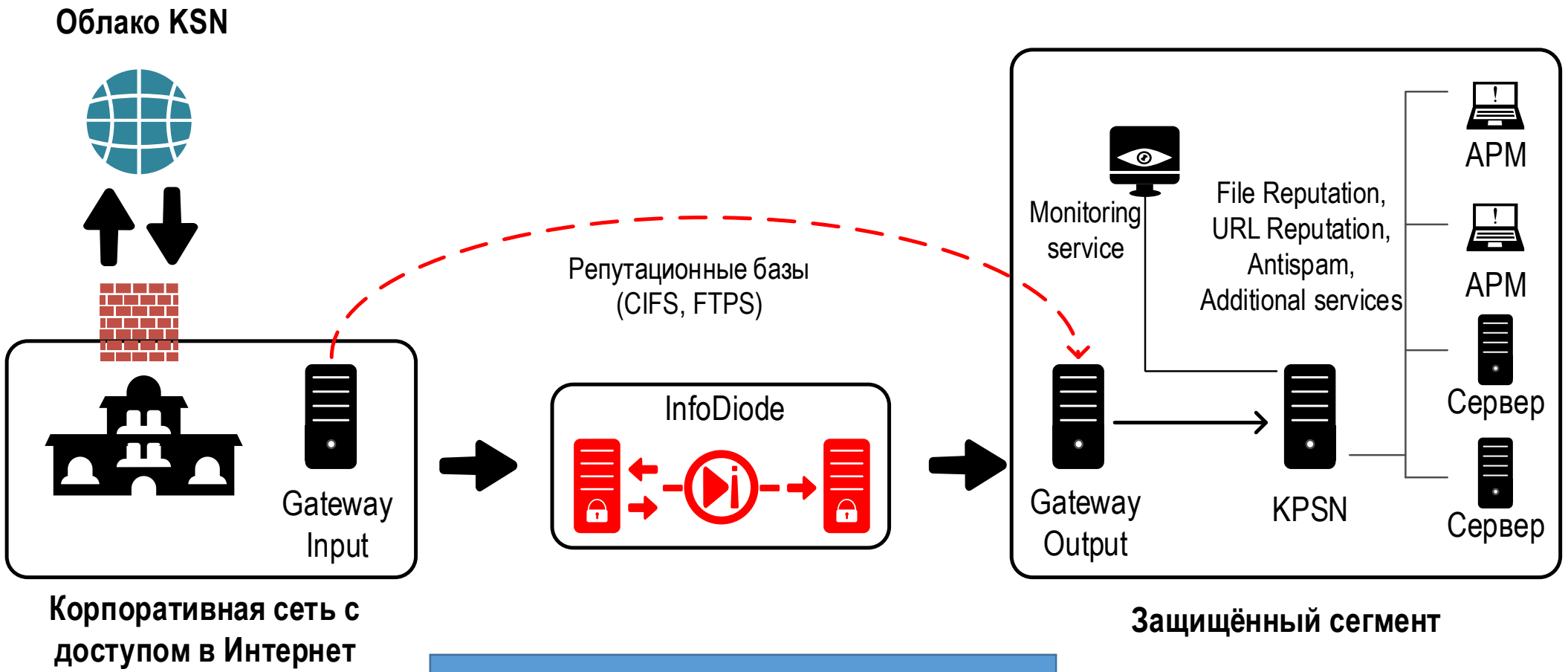
# Получение обновлений MS Windows через «диод» внутрь защищенного сегмента




Использование штатного сервера WSUS для передачи согласованных обновлений внутрь доверенного сегмента

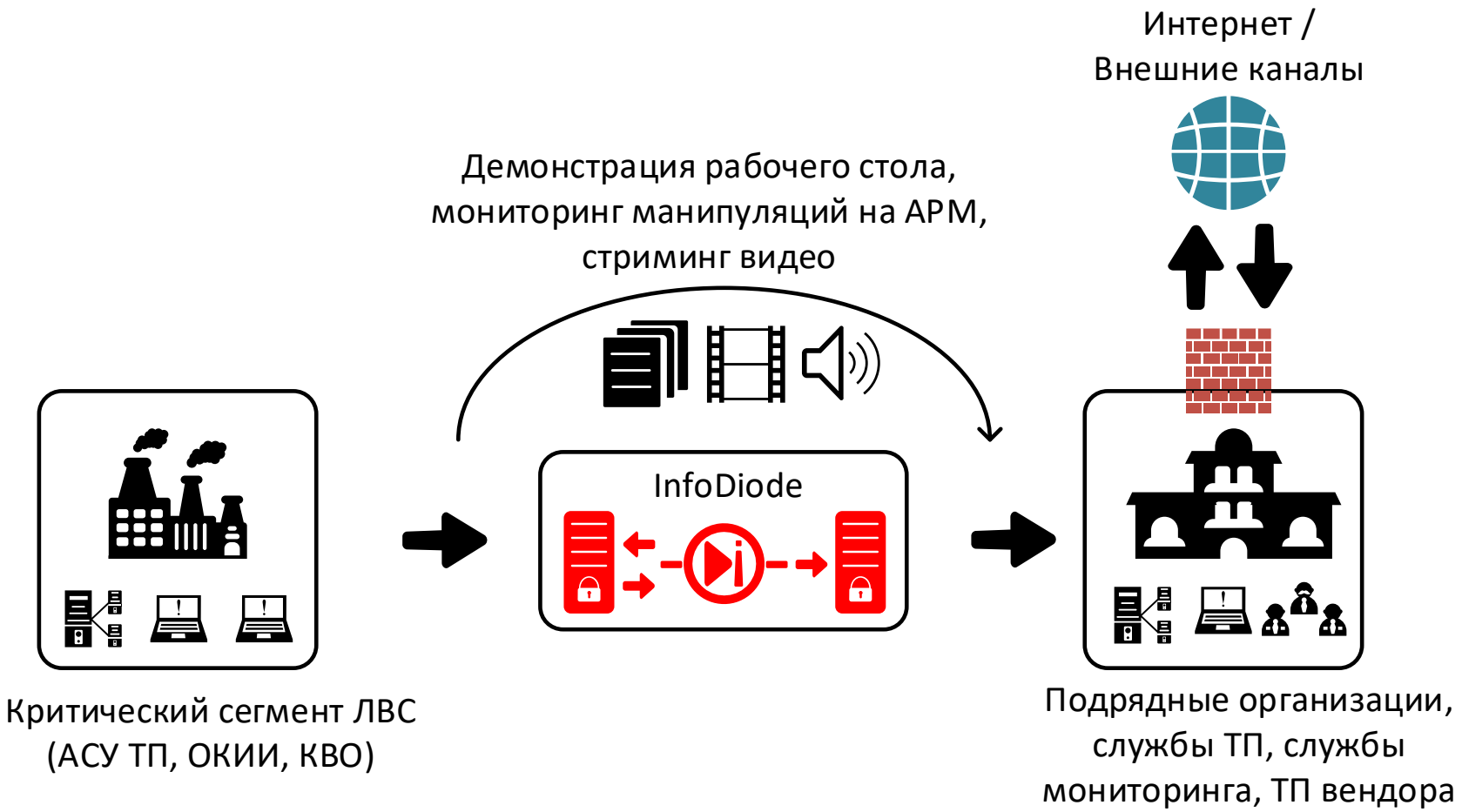
InfoDiode.ru

# Получение обновлений KPSN (Kaspersky) через InfoDiode внутрь защищенного сегмента



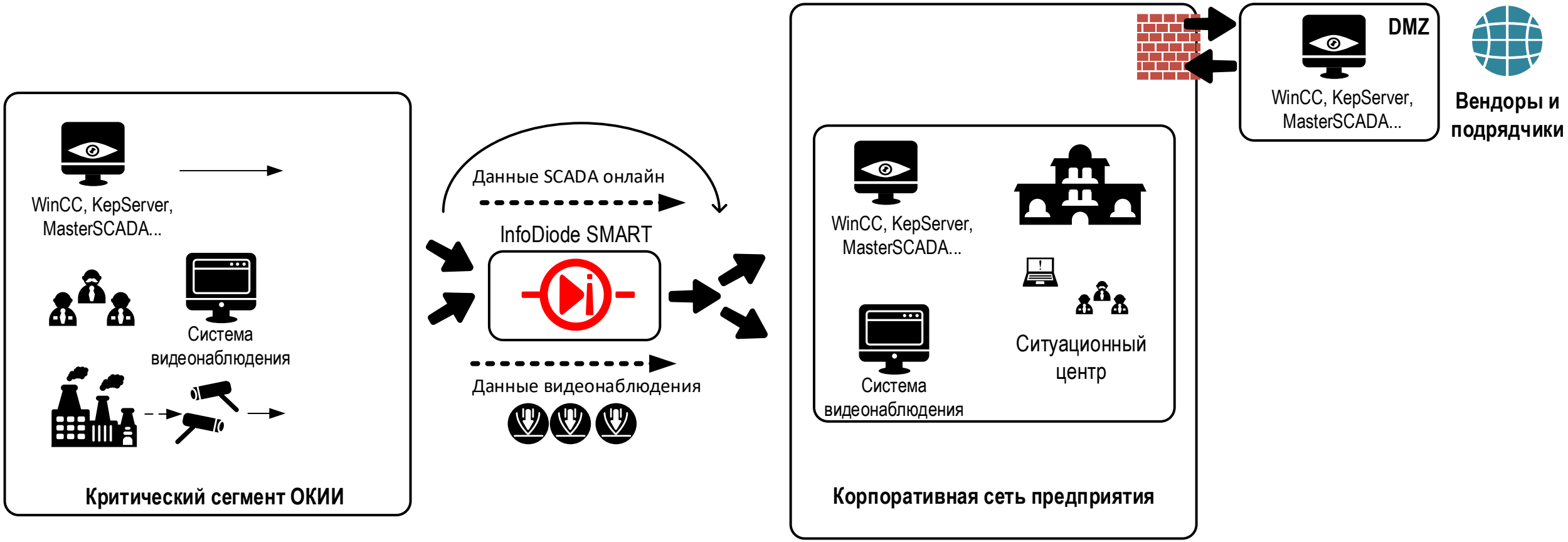

Использование штатного сервера KPSN для передачи обновлений антивируса и баз репутаций внутрь доверенного сегмента

# Онлайн-стриминг рабочего стола АРМ оператора




Организация наблюдения за АРМ оператора в СЦ, на внешнем рабочем месте за пределами доверенного сегмента

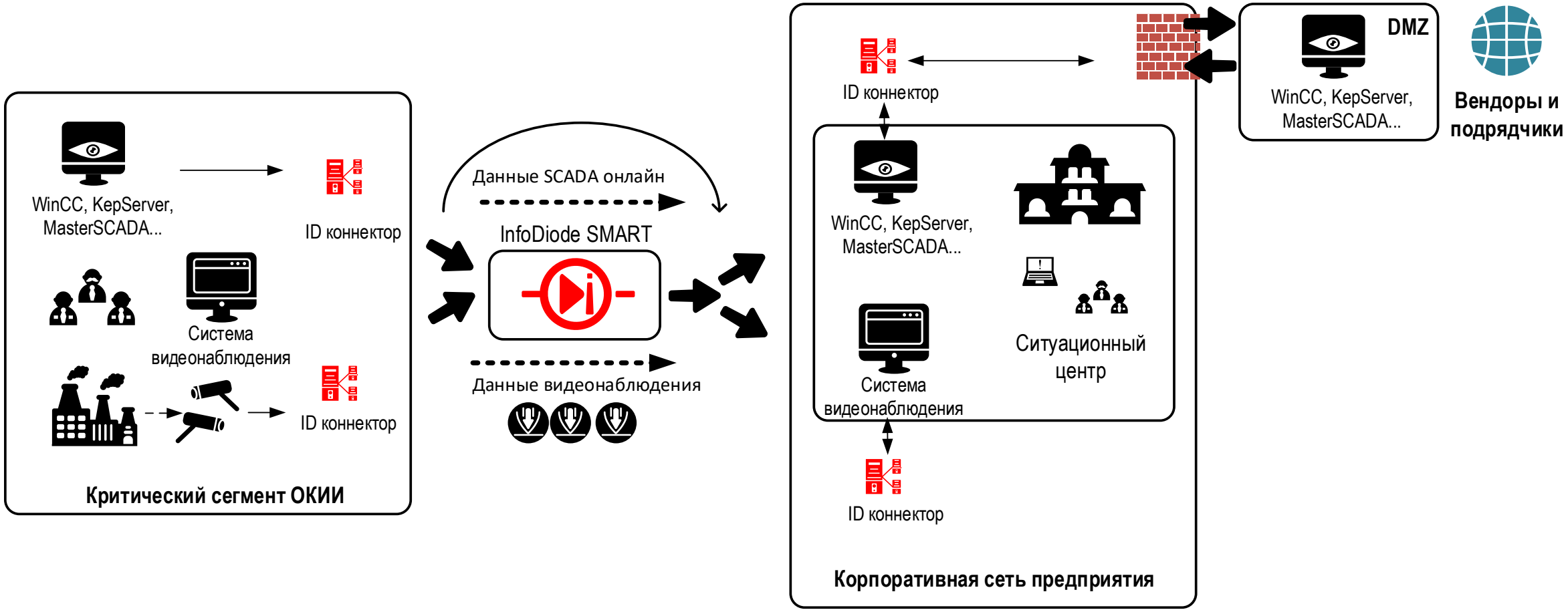
# Передача OPC тегов (UA/DA, IEC 104 тегов) в Historian или внешний OPC сервер по MQTT




Передача данных источников в Aveva Historian, Metris DiOMera, KepServer, WinCC OA/TIA Portal

InfoDiode.ru

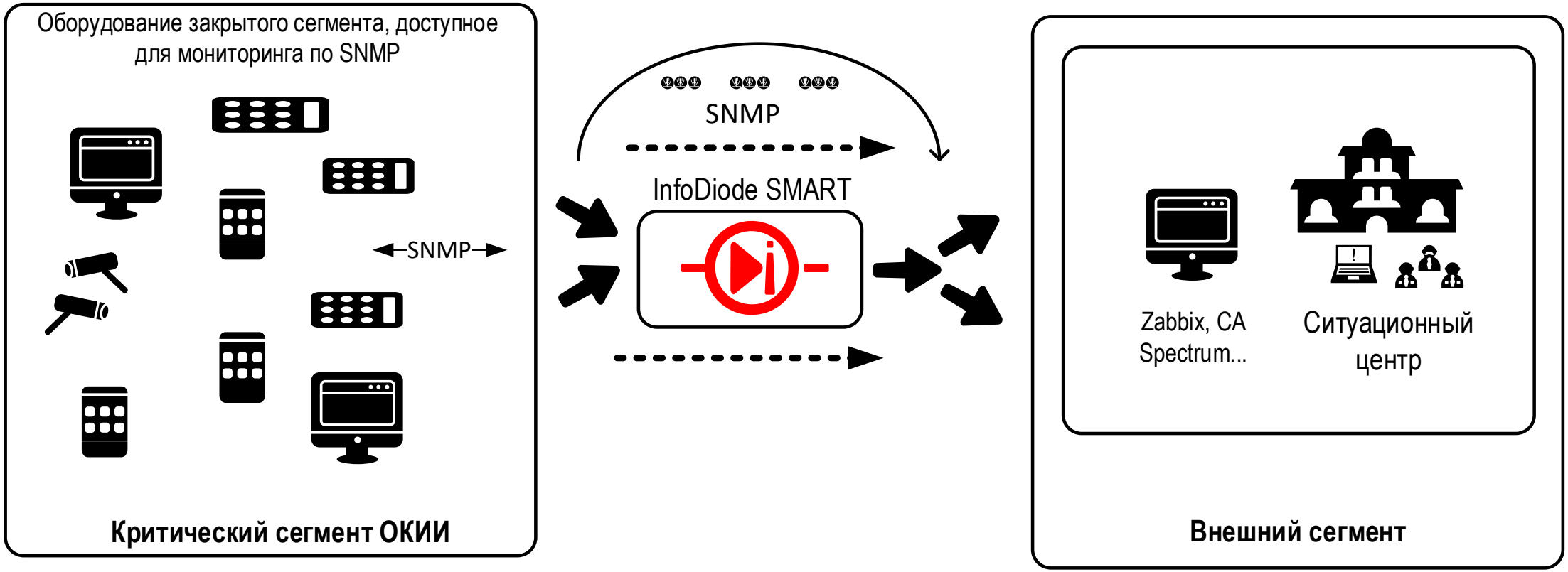
# Передача OPC тегов в Historian или внешний OPC сервер с использованием коннекторов




Передача данных источников в Aveva Historian, Metris DiOMera, KepServer, WinCC OA/TIA Portal

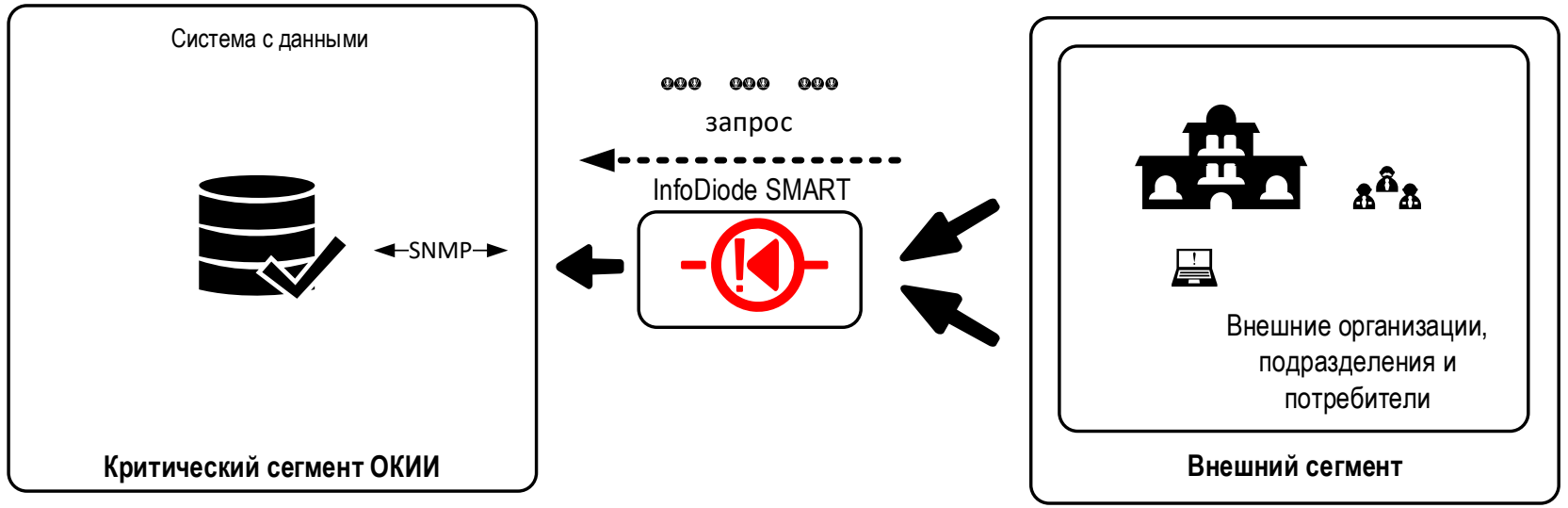
InfoDiode.ru

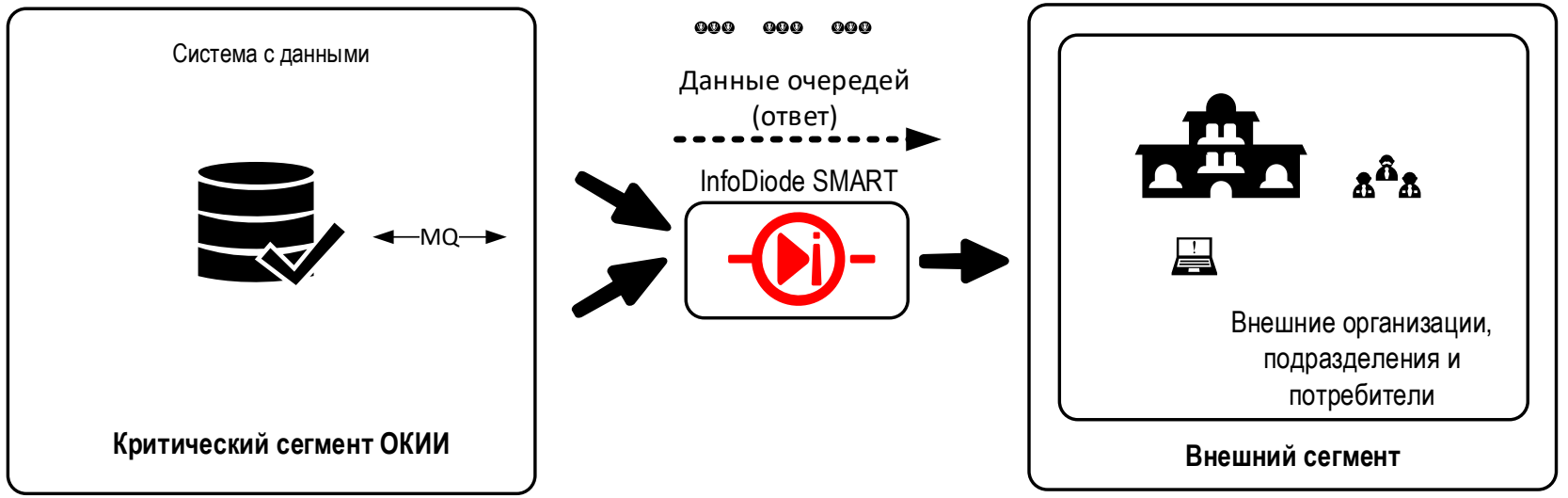
# Мониторинг оборудования закрытого контура по SNMP




Получение данных мониторинга оборудования по SNMP из закрытого сегмента – «подписка» по тем же OID, которые существуют в закрытом сегменте

# Передача данных через очереди (например RabbitMQ)




Построение систем типа «запрос-ответ», близких к синхронным, но работающих по изолированным каналам связи

InfoDiode.ru

# АМТ-ГРУП предоставляет полную линейку решений класса «диод» для защиты КИИ и АСУ ТП

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.

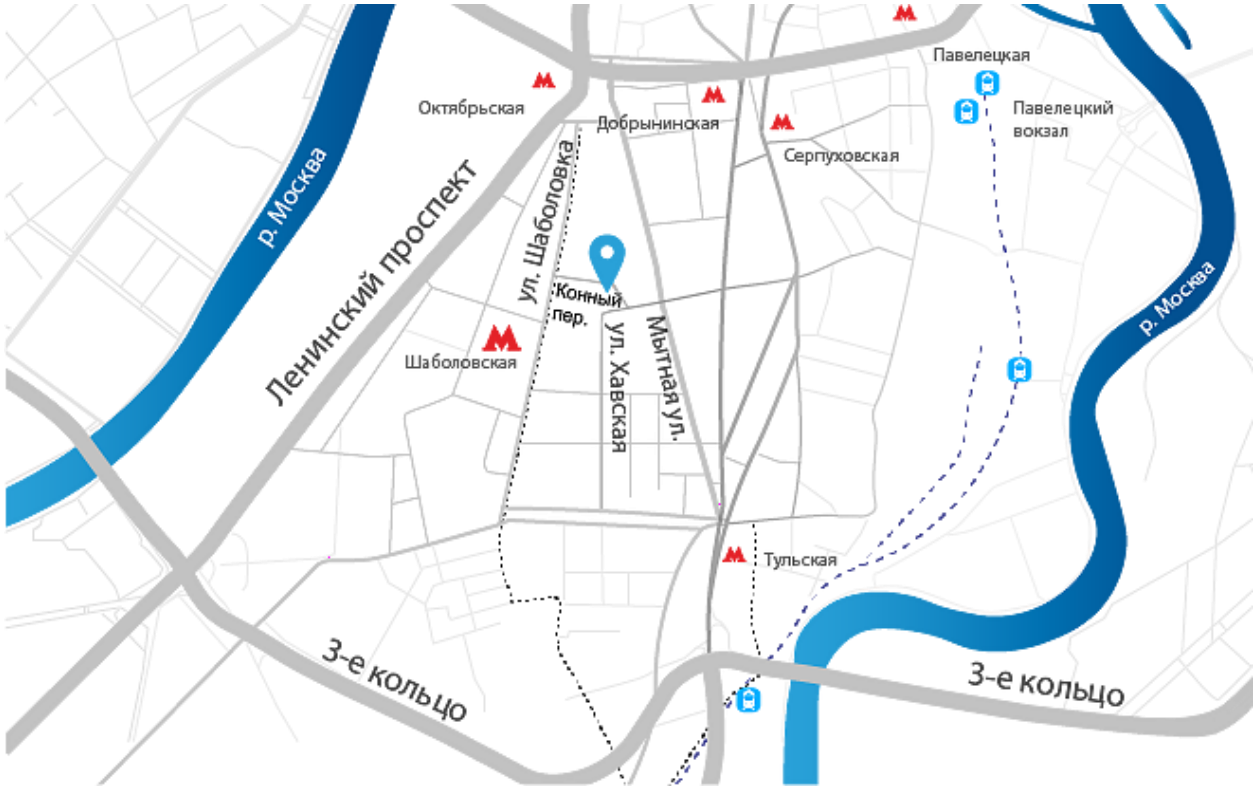
2. **АПК InfoDiode PRO** – сертифицированное ФСТЭК УД (4) решение для передачи значимых файловых потоков, дистрибутивов, реплик ВМ и баз данных, электронной почты, бэкапов и т.п. из доверенного сегмента вовне.

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.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!