



Однонаправленная
передача данных

Защита
объектов КИИ

Экспорт
видеопотоков в
ситуационный
центр

Сегментирование
сетей АСУ ТП

Info
-Diode

IT

26.05.2022

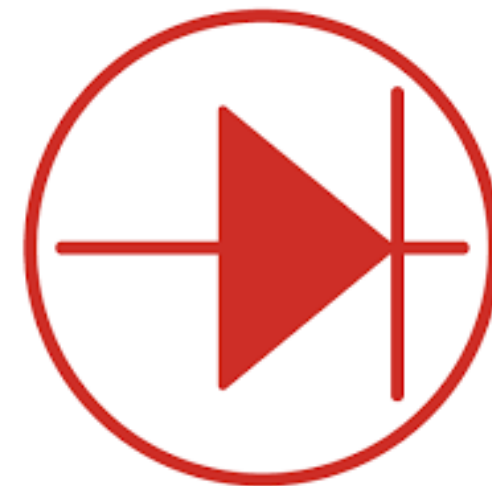
AMT-ГРУП

Новые решения по однонаправленной
передаче данных. Промышленные
протоколы через InfoDiode

1. Какие бывают
«диоды»

2. Как применение
диодов локализует
вектор атаки и как
организуется передача
пром. протоколов

- **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
односторонности
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
AK InfoDiode, rack module	2 AK 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

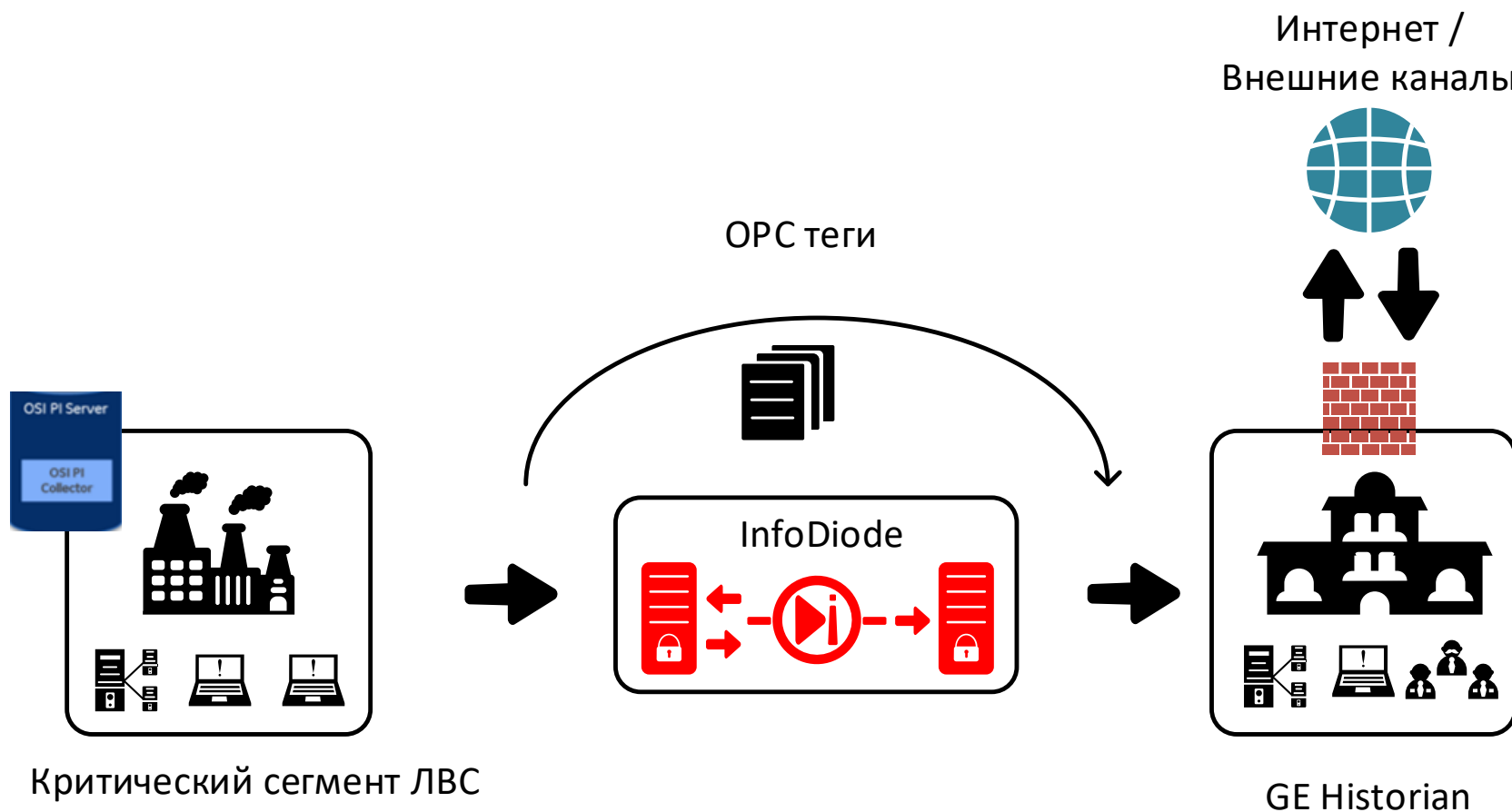
Диод внутри

Сценарии применения диодов



Передача OPC тегов через инструменты General Electric ETL во внешнее хранилище

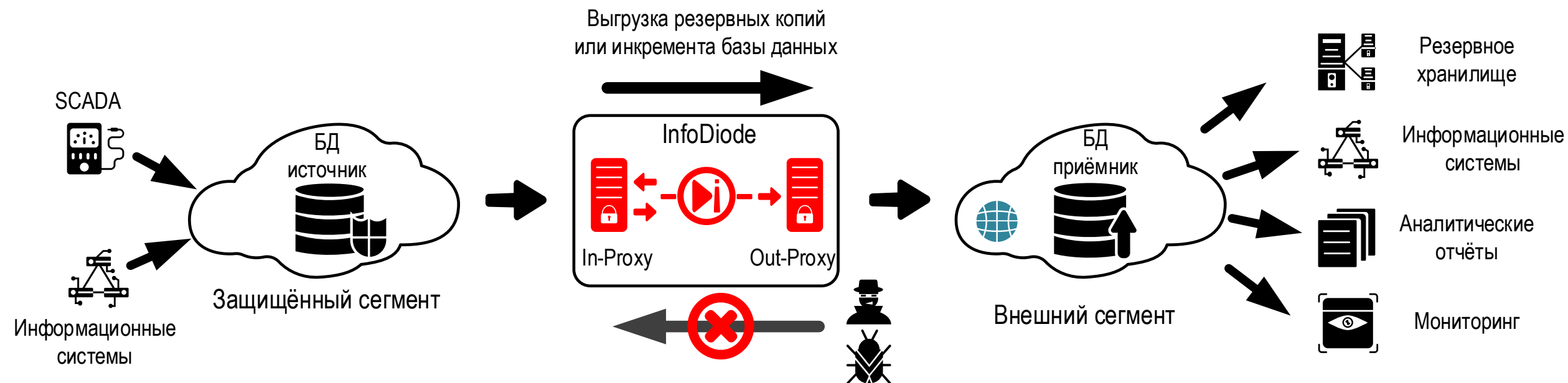
АПК INFODIODE PRO



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



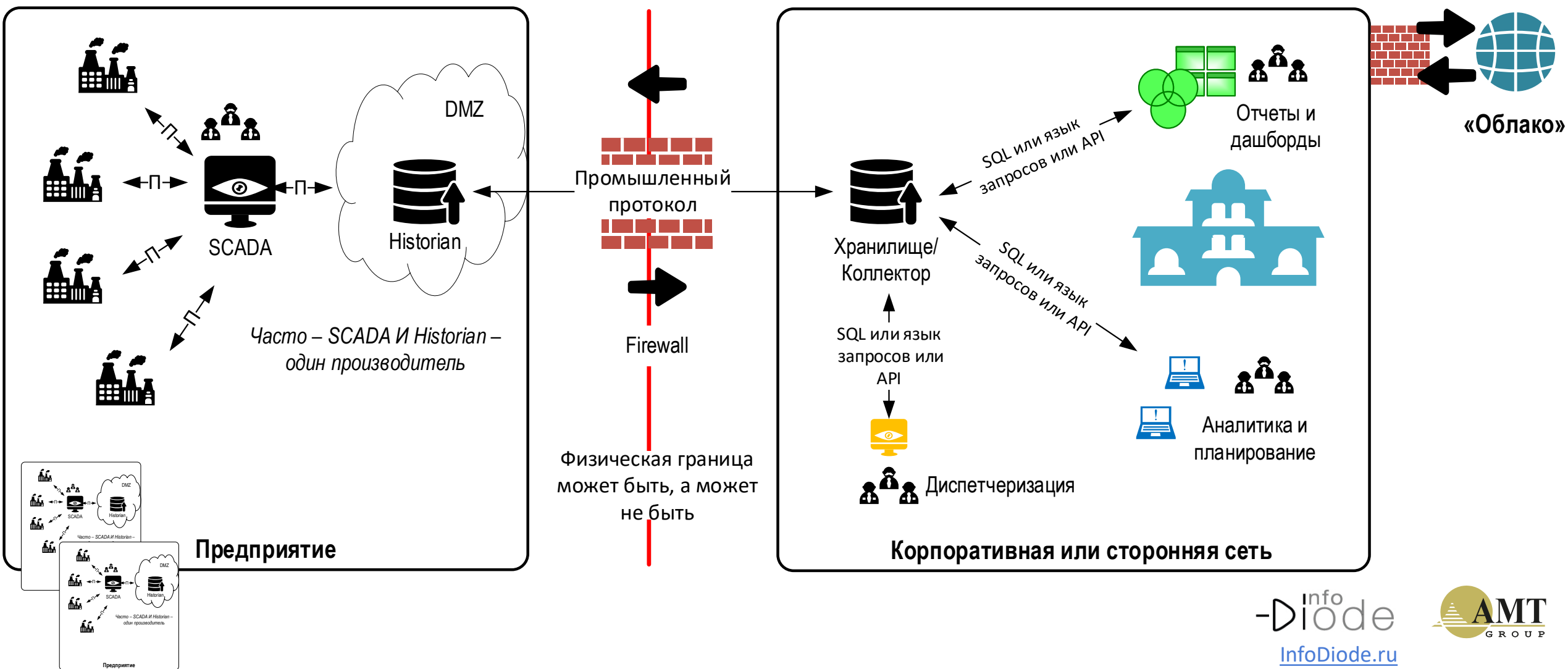
АПК INFODIODE PRO



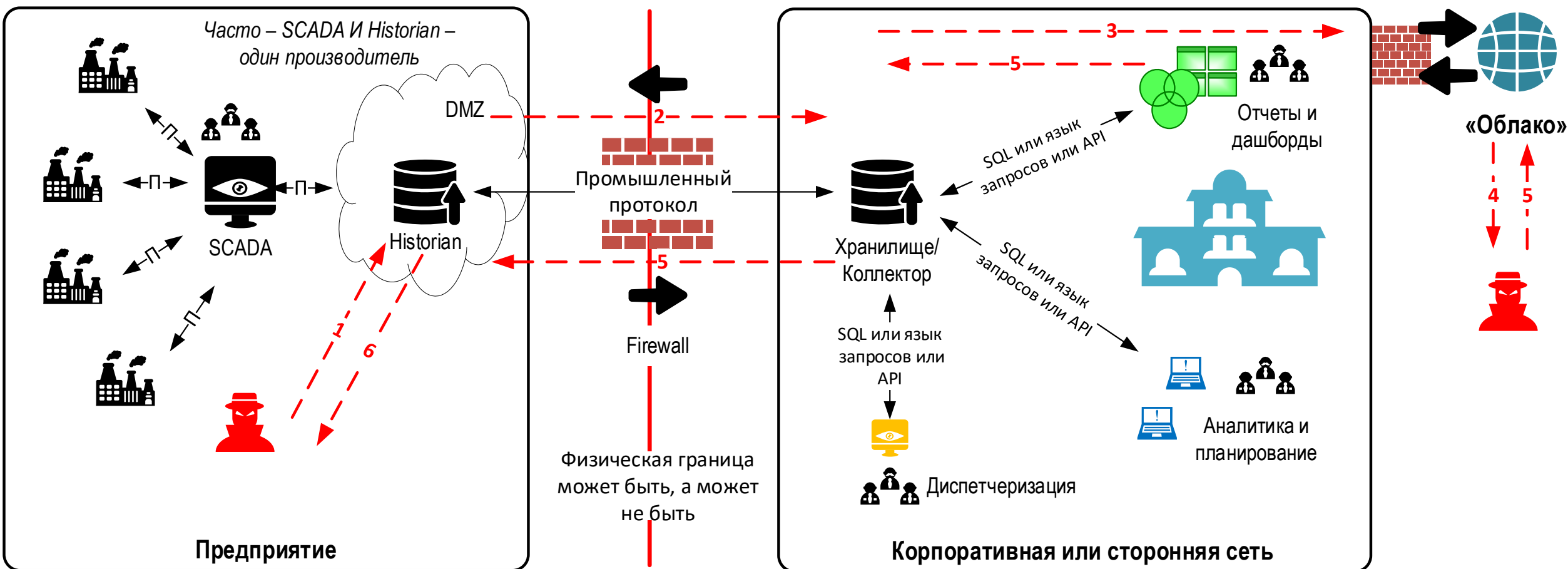
Инкрементальный (частотой до 5 секунд)
обмен инкрементом БД и полный бэкап БД
по расписанию

Типовое предприятие разделено на два логических сегмента: технологический и корпоративный

АПК INFODIODE SMART

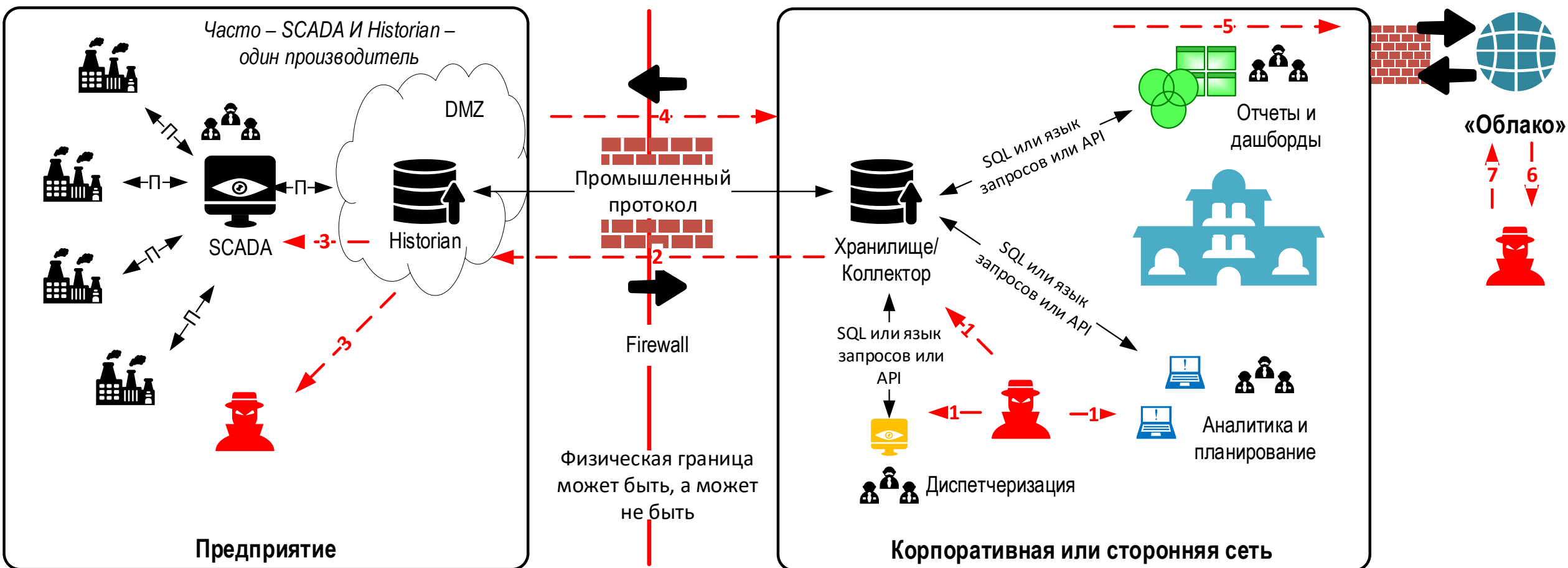


АПК INFODIODE SMART



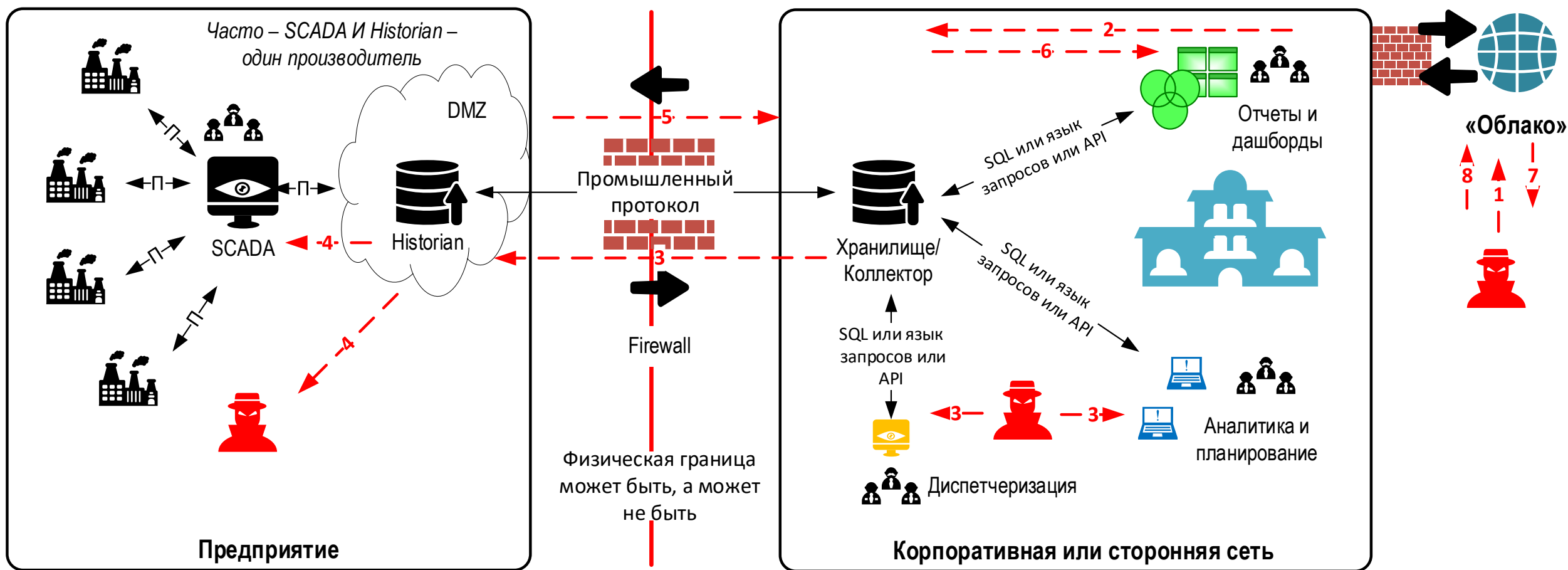
Вариант-2: Вектор атаки реализуется их корпоративного сегмента

АПК INFODIODE SMART



Вариант-3: Вектор атаки реализуется из-за пределов организации

АПК INFODIODE SMART



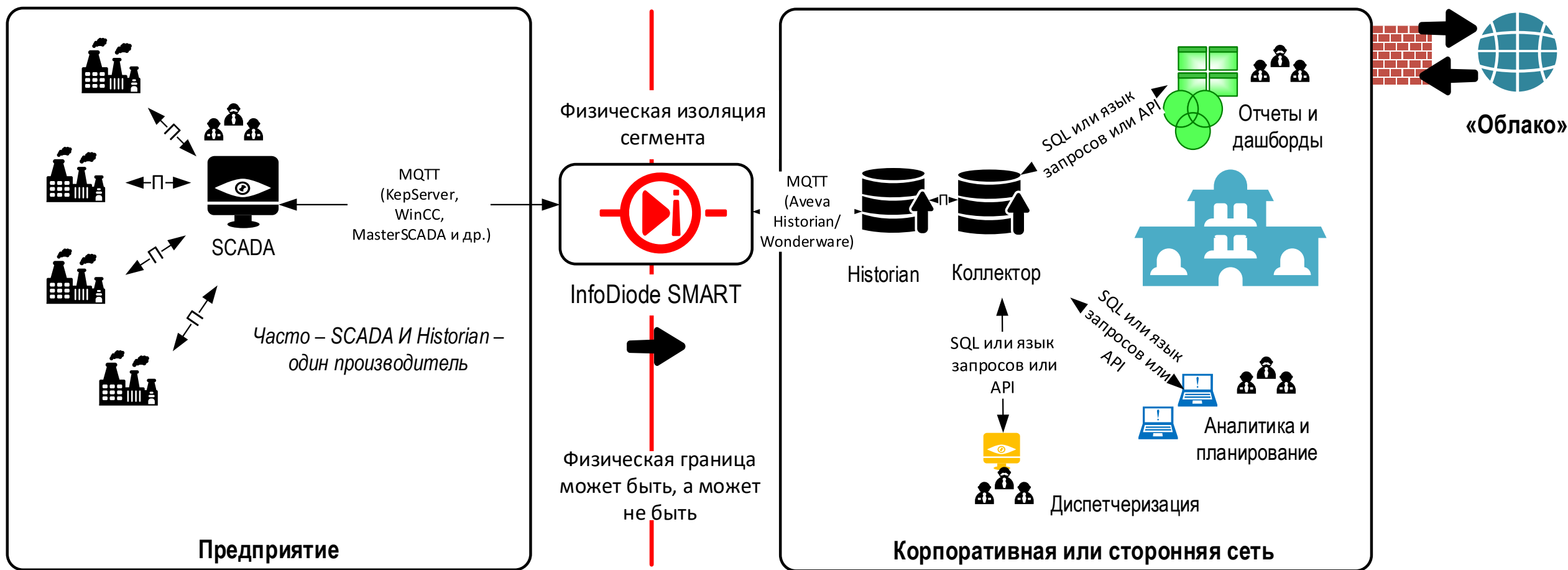
Ожидаемые результаты атак не сводятся только к «катастрофе»

1. **Катастрофические последствия: авария, ущерб экологии и т.п.** – слабо мотивированный результат
2. **Шифрование данных и элементов инфраструктуры** – получение денег или выкупа
3. **Манипулирование рынком** – остановка производства в четко определенные сроки для целей «игры» на фондовом рынке
4. **Промышленный шпионаж** - получение конкурентных экономических преимуществ за счет получения конфид. данных
5. **Промышленная атака** - получение конкурентных экономических или военных преимуществ за счет остановки производства, без экологического ущерба, но для нанесения долговременного урона



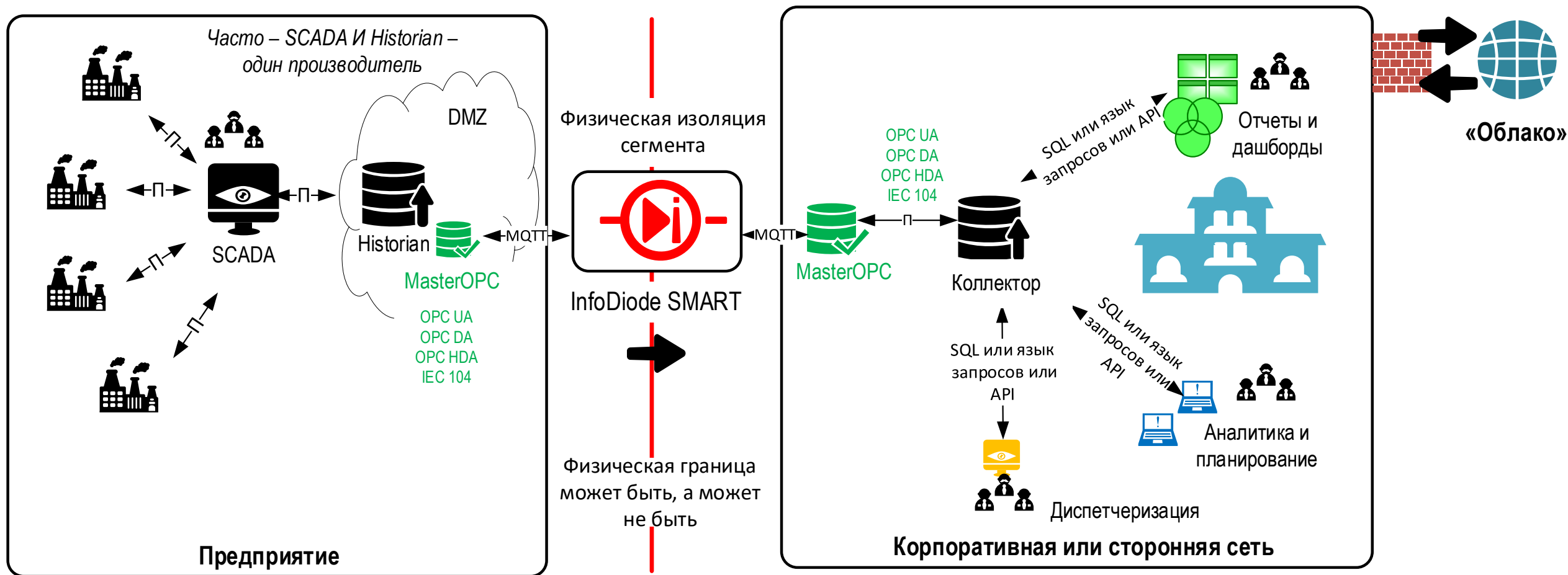
Для современных SCADA систем возможно непосредственное взаимодействие с InfoDiode SMART по MQTT протоколу

АПК INFODIODE SMART



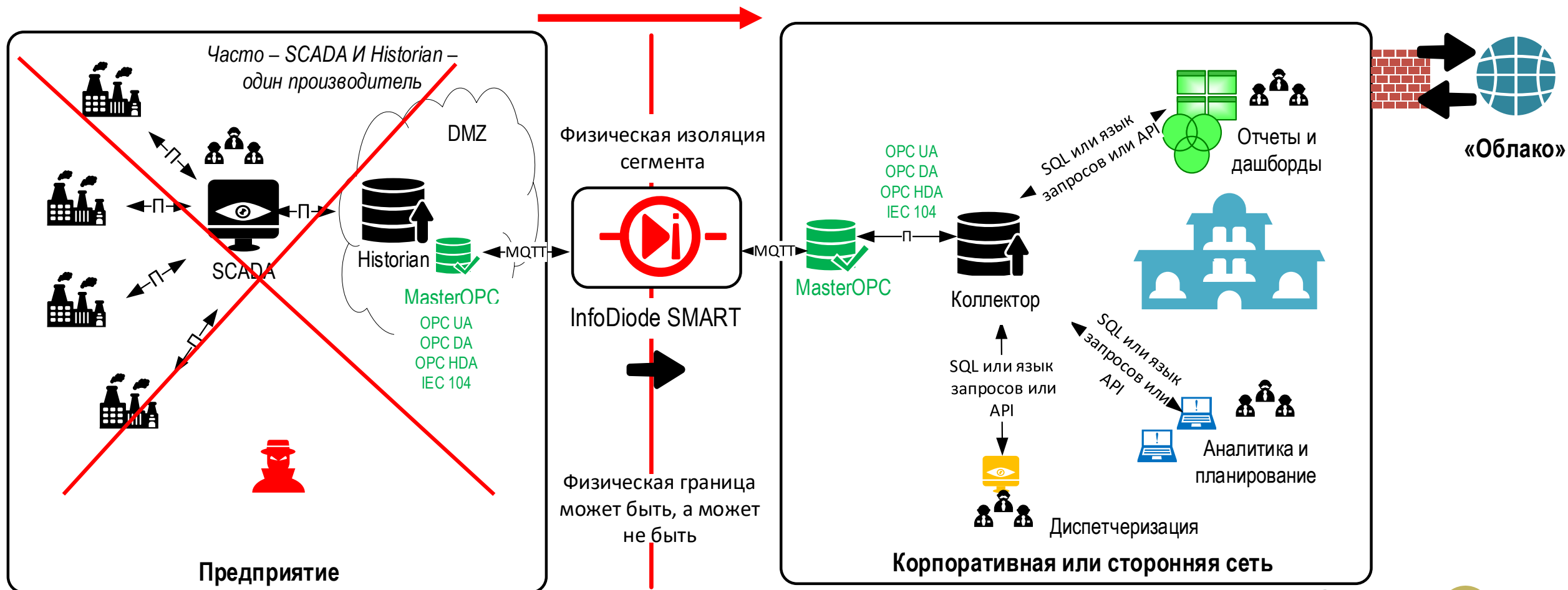
Если взаимодействие с InfoDiode SMART напрямую невозможно – используются коннекторы – от партнеров MasterSCADA (MasterOPC)

АПК INFODIODE SMART



- Управляющее воздействие извне исключено
- Получение информации крайне ограничено

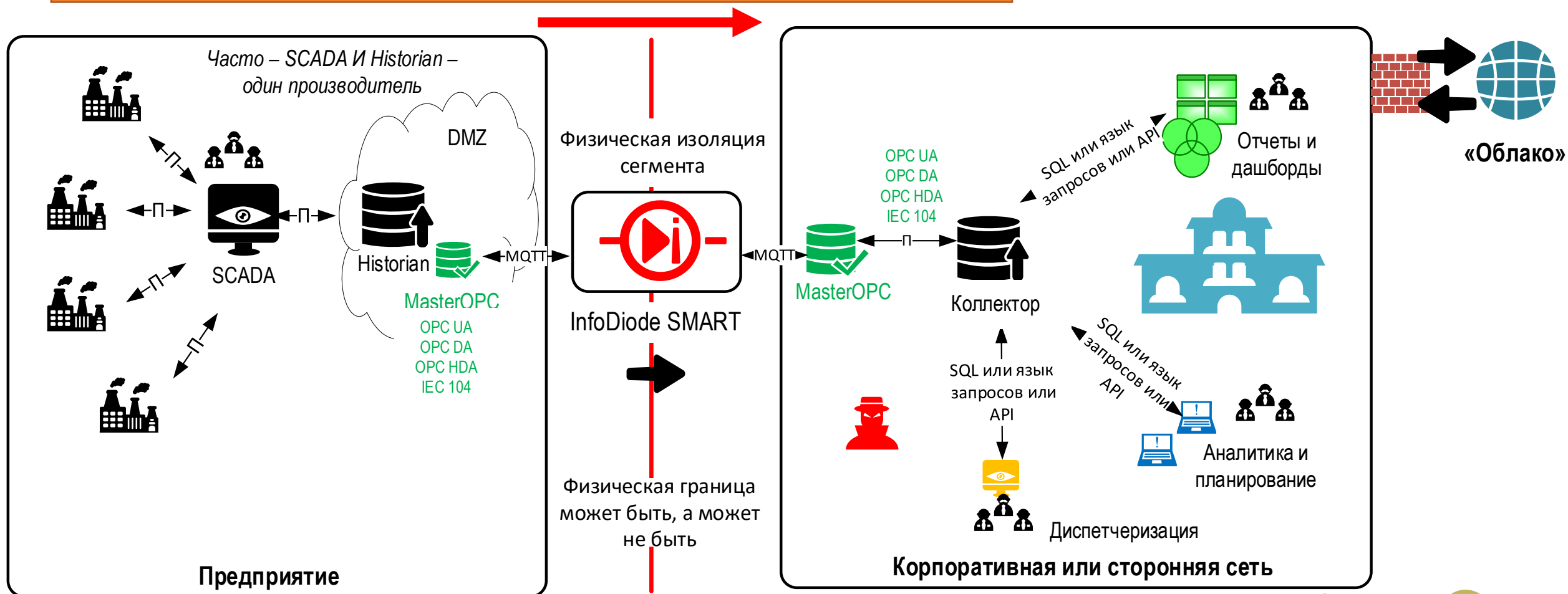
АПК INFODIODE SMART



Локализация вектора атаки из корпоративного сегмента

- Управляющее воздействие исключено
- Получение информации лимитировано предоставляемыми данными

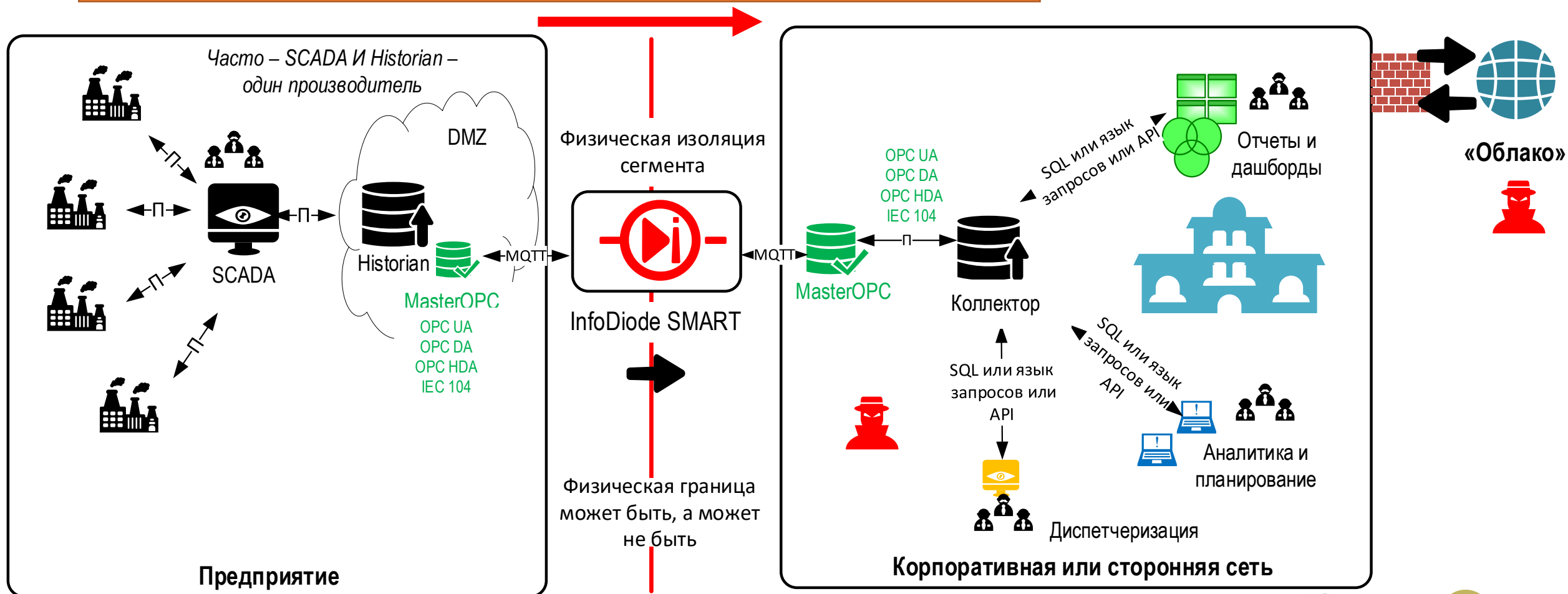
АПК INFODIODE SMART



Локализация вектора атаки из-за пределов организации

- Управляющее воздействие исключено
- Получение информации лимитировано предоставляемыми данными

АПК INFODIODE SMART



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



- 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!