



Однонаправленная
передача данных

Защита
объектов КИИ

Экспорт
видеопотоков в
ситуационный
центр

Сегментирование
сетей АСУ ТП

-Diode^{info}

IT

02.02.2021

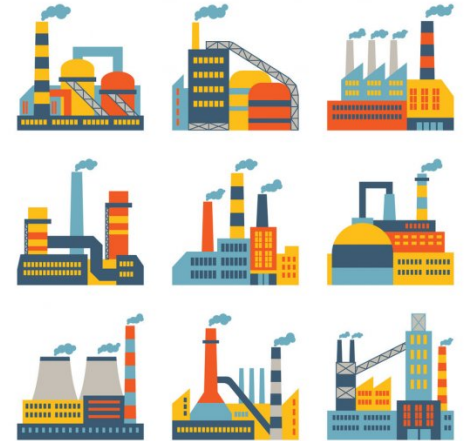
АМТ-ГРУП

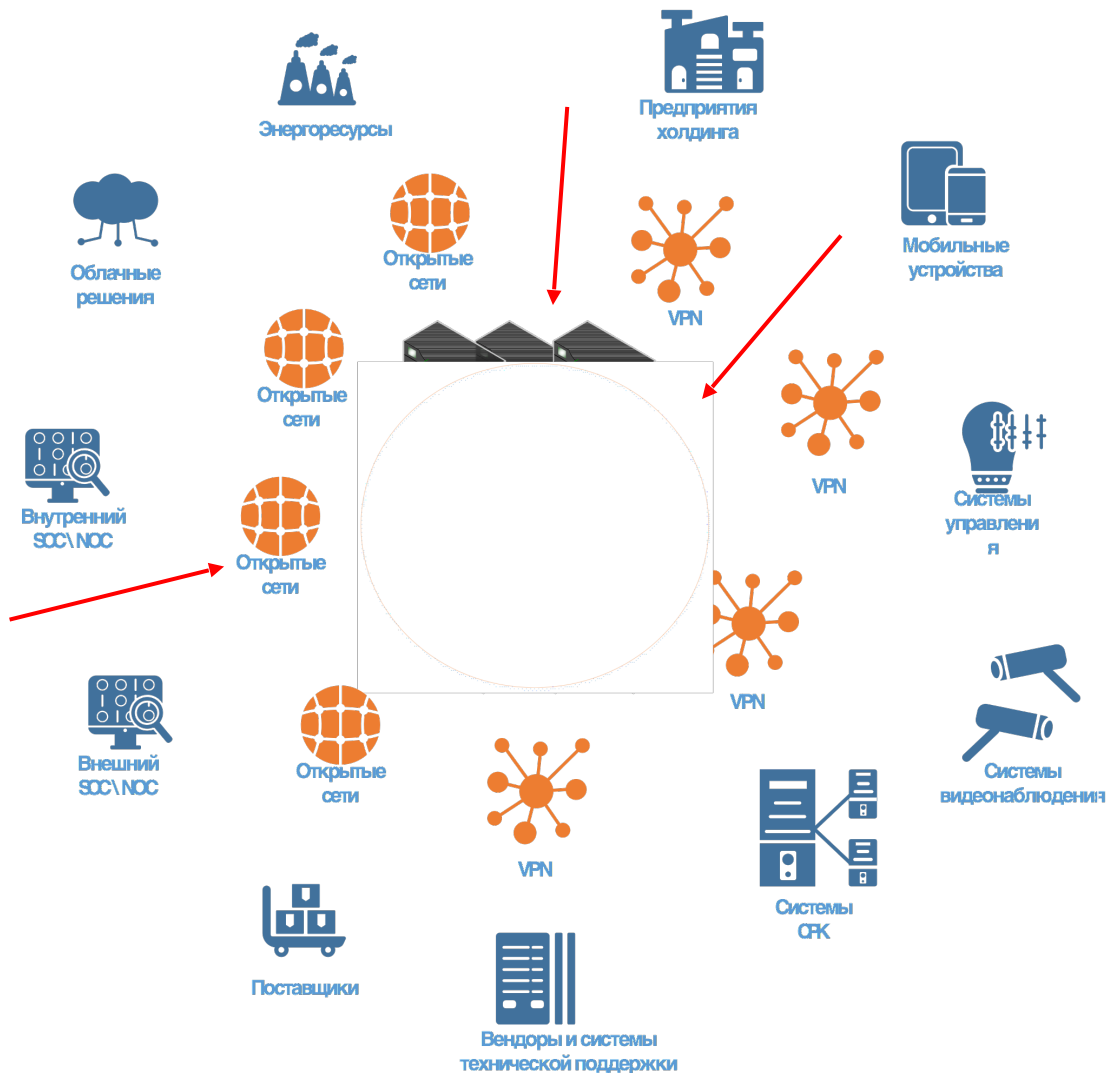
Диоды как эффективные инструменты защиты периметра АСУ ТП.
Актуальные проблемы защиты и доступные решения.

Общий подход к построению защиты с использованием диодов



- ❑ Типовое предприятие может иметь до 500 связей с внешними контрагентами, партнерами, вендорами и организациями
 - ❑ Облачные решения
 - ❑ Поддержка ПО, ИТ поддержка
 - ❑ Системы архивирования данных
 - ❑ Отопление, вентиляция кондиционирование (HVAC)
 - ❑ Системы безопасности (как информационной, так и общей)
 - ❑ Диспетчерские
 - ❑ Системы поставщиков и подрядчиков
- ❑ ПО в рамках сети OT\ICS (АСУТП) как правило «унаследовано»
 - ❑ ПО создавалось без учета ИБ, ряд промышленных протоколов не предполагают аутентификацию





СТРАТЕГИЯ СНИЖЕНИЯ РИСКОВ

Пять ключевых элементов стратегии:

- ☐ Инвентаризация доступа
- ☐ Выделение «слоев»\уровней привилегий
- ☐ Сетевая сегментация и «защита в глубину»
- ☐ Защита, основанная на управлении рисками
- ☐ Нулевое доверие

Приказ ФСТЭК №239: «Об утверждении требований по обеспечению безопасности значимых объектов КИИ РФ». От 25.12.2017

Приказ ФСТЭК №17: «Требования по защите информации, содержащейся в государственных информационных системах». От 11.02.2014

Приказ ФСТЭК №21: «Требования по защите персональных данных». От 18.02.2014

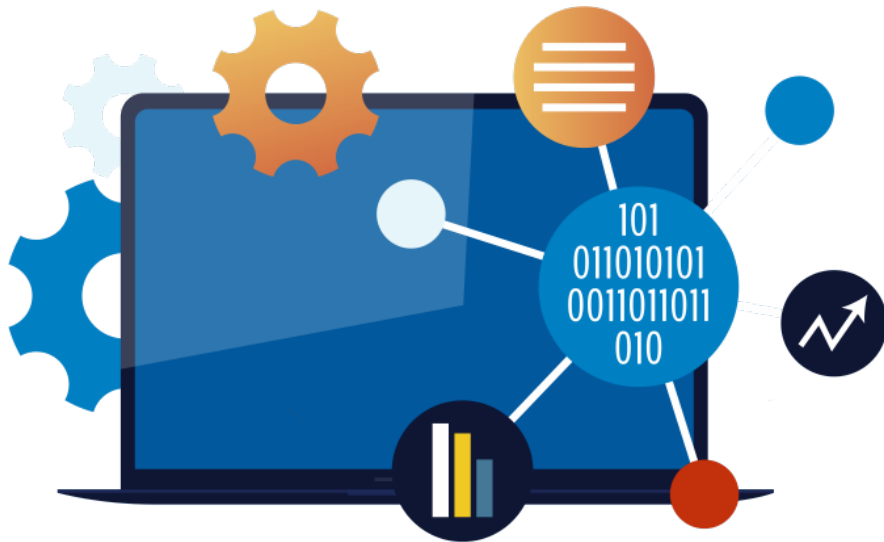
Федеральный закон №187: «О безопасности критической информационной инфраструктуры Российской Федерации». От 26.06.2017

Требование УПДЗ (Управление доступом субъектов доступа к объектам доступа)

Требование ЗСВ4 (Защита среды виртуализации): Управление (фильтрация, маршрутизация, контроль соединений, **однаправленная передача** и иные способы управления) информационными потоками

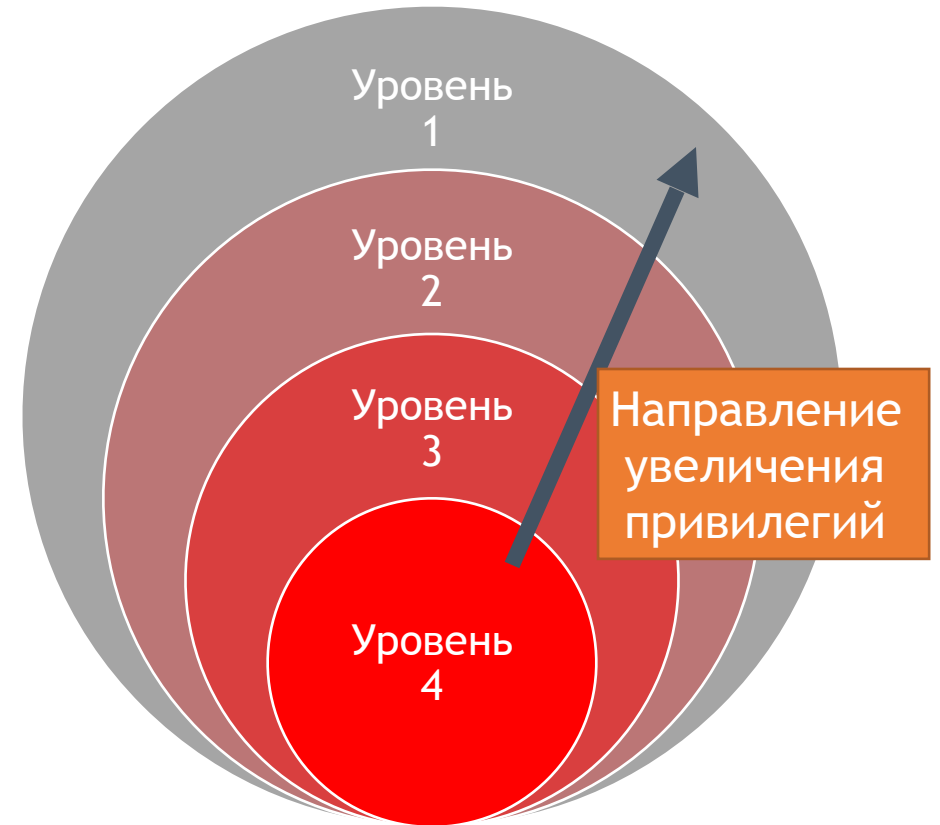
- NIST SP800-82. Guide to Industrial Control Systems (ICS) Security (<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf>)
- Cybersecurity for Industrial Control Systems - Документ Национального агентства по безопасности информационных систем Франции (https://www.ssi.gouv.fr/uploads/2014/01/industrial_security_WG_Classification_Method.pdf)
- Группа стандартов по управлению ИБ в системах промышленной автоматизации ANSI/ISA-62443
- Документы института SANS, в частности Tactical Data Diodes in Industrial Automation and Control Systems (<https://www.sans.org/reading-room/whitepapers/firewalls/tactical-data-diodes-industrial-automation-control-systems-36057>)
- Документы NERC. NERC 1300 CIP-002 R3 Routable Protocols and Data Diode Devices (<http://www.nerc.com/page.php?cid=3|22|354>)
- Стандарт API Standard 1164. Pipeline SCADA Security
- <https://us-cert.cisa.gov/ncas/alerts/aa20-205a> - NSA and CISA **Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems**
 - Агентство национальной безопасности
 - Агентство кибербезопасности и защиты инфраструктуры

- ❑ Инвентаризация доступа
 - ❑ Кто имеет доступ (организации, люди, системы)
 - ❑ Почему имеют доступ (работа, поддержка, управление, контроль, резерв, ИТ)

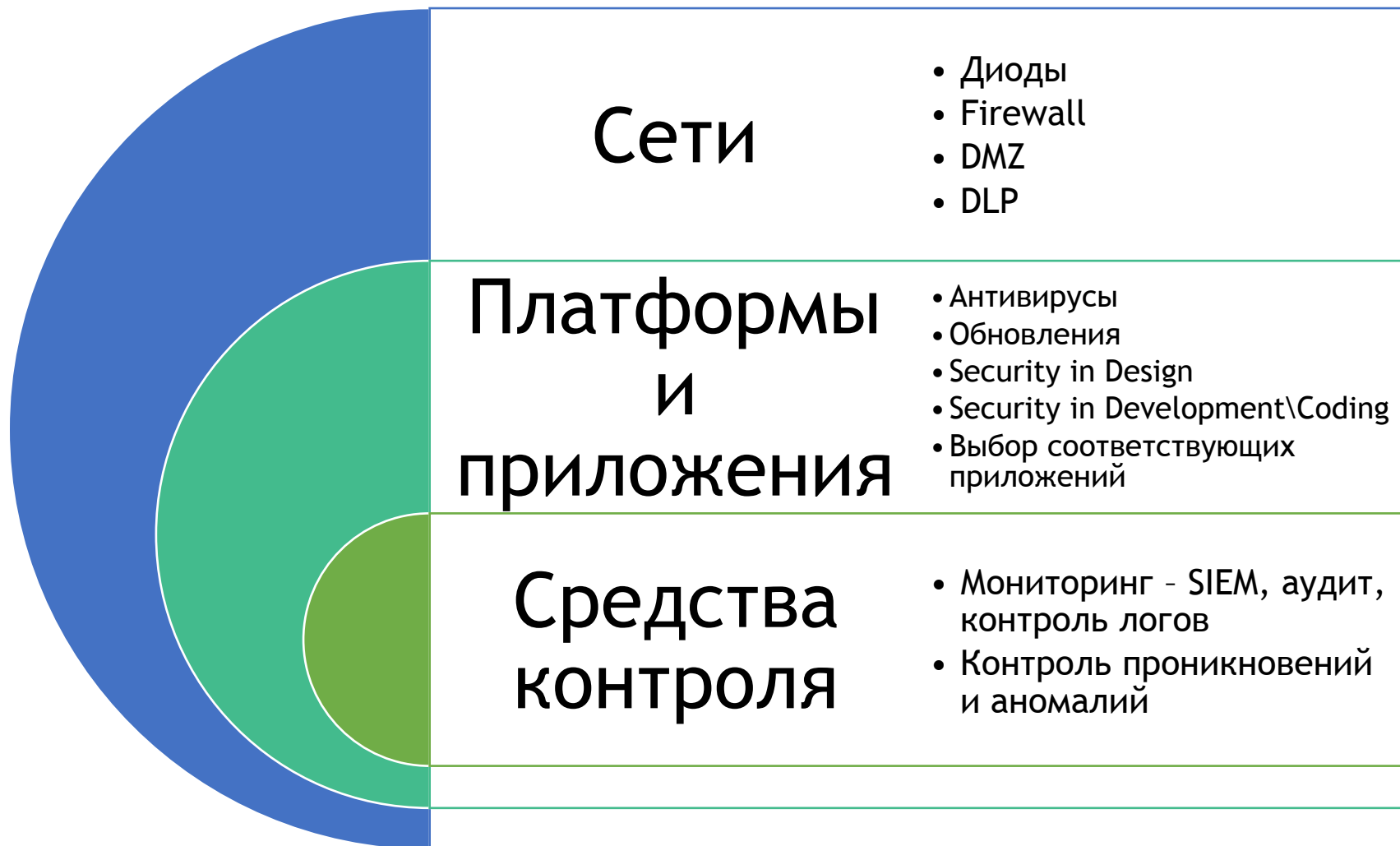


Вы не можете обеспечить
безопасность того, что вы не
видите и не учитываете

- ❑ Привилегированные слои получения доступа
 - ❑ Доступ только тем, кто уполномочен выполнять те или иные функции
 - ❑ Выделить уровни доступа уменьшаемые привилегии за счет использования различных средств защиты
 - ❑ Принцип может применяться **не только к системам**, но и к сетевым сегментам, доменам







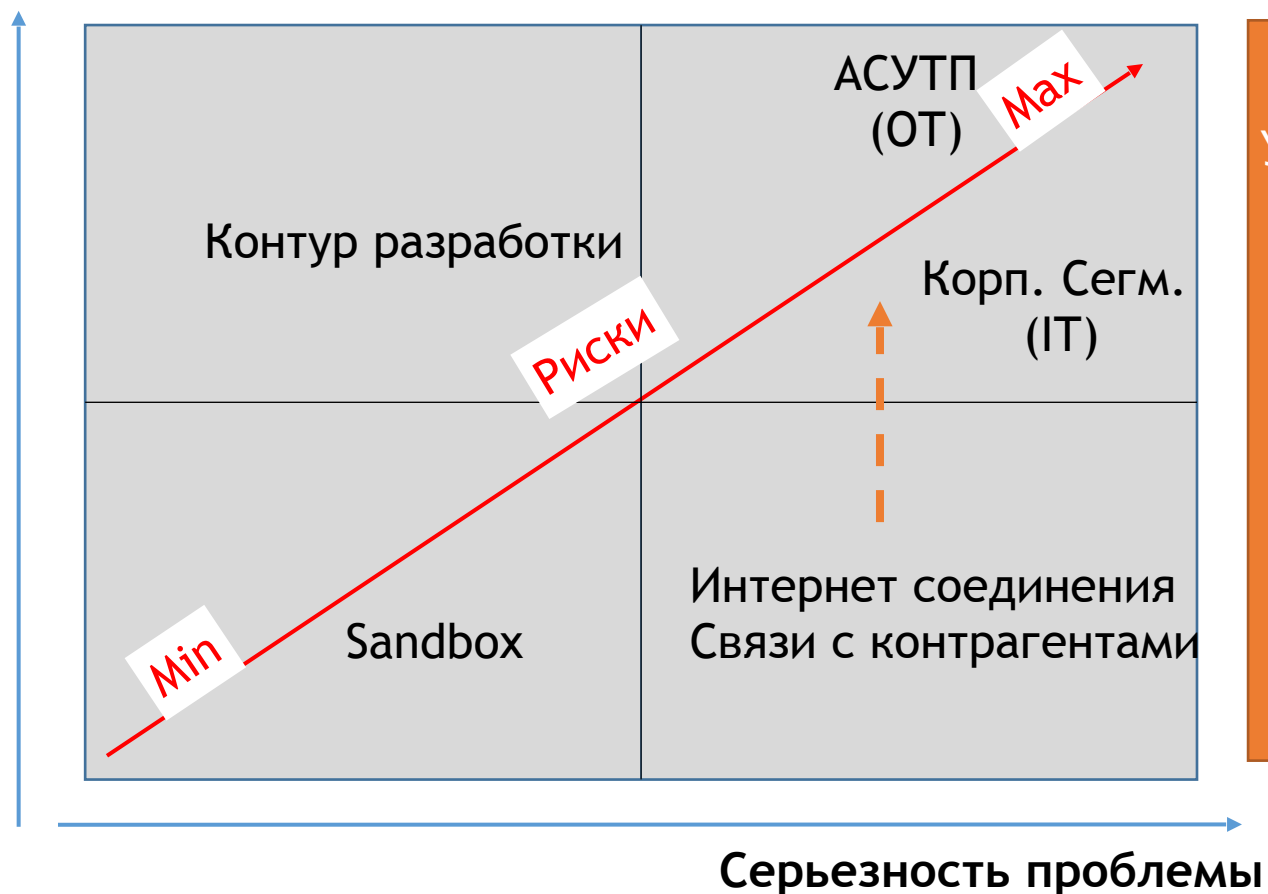
Каждый уровень защиты дает свои преимущества

Различные уровни контроля доступа между сегментами

Желательно не полагаться на один инструмент

Устройства ограничивающие доступ на физическом уровне серьезно ограничивают угрозы и изменяют вектор атаки

Ценность активов



Приоретизируйте «сетевые связи» с учетом риска
 Уровень риска = серьезность проблемы + ценность активов

Чем выше риск, тем более серьезные средства защиты должны применяться

- *Устройства ограничивающие доступ на физическом уровне серьезно ограничивают угрозы и изменяют вектор атаки*

Интернет соединения и соединения с контрагентами обладают наибольшим потенциалом риска

1

- Доверяй, но проверяй
- Пропускаем и затем начинаем проверять, контролировать

FW + политика

2

- Не доверять, но проверять все
- Проверяем все изначально, контролируем любые отклонения

FW + набор средств защиты + политика

3

- Нулевое доверие
- Исключаем воздействие на отдельные сегменты в принципе

FW + набор средств защиты + политика +
устройства ограничивающие доступ на
физическом уровне

Software



- ☐ Уязвимость «нулевого дня» и др. уязвимости
- ☐ Скорость распространения атаки vs скорость распространения защиты
- ☐ Общедоступность средств атаки
- ☐ Вектор атаки смещается на человеческий фактор
- ☐ Особенности конфигурирования сами могут приводить к проблемам

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

Рынок решений. Решения от АМТ-ГРУП



Российские вендоры

Часто не рассматривают линейку таких устройств как основную. Как следствие - внимание, уделяемое этим устройствам остаточное.

Прежде всего в части:

1. Развития
2. Технической поддержки
3. Наращивания и масштабирования
4. Сроков производства и поставки и т.п.

АМТ-ГРУП

Предлагает комплексные решения:

1. Имеет полную линейку устройств, которые поставляет на рынок уже более 6-и лет.
2. Развивает продукт (см. новые линейки, скорость выхода версий ПО, участие в конференциях и т.п.)
3. Имеет продуктовую линейку: АК и АПК

Зарубежные вендоры

Практически отсутствуют на российском рынке

1. Санкции
2. По причинам отсутствия сертификатов соответствия от регуляторов





InfoDiode
rack module

- Встроенные резервированные блоки питания AC
- Высота 1 RU
- Малая глубина, возможность монтажа 2 устройств с двух сторон шкафа



InfoDiode
rack module Cluster

- Резервированное подключение 1+1
- Встроенные резервированные блоки питания AC для каждого из модулей
- Высота 1 RU
- Малая глубина, возможность монтажа устройств с двух сторон шкафа

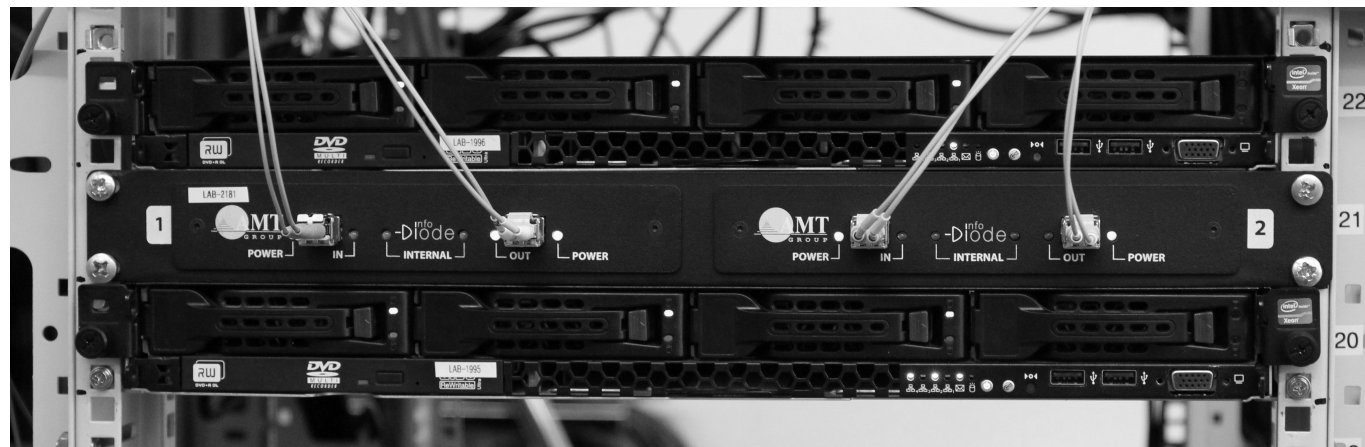


InfoDiode
Mini

- На DIN — рейку
- На монтажную пластину
- Напряжение питания 9-36 VDC
- Два ввода питания для резервирования по схеме 1+1
- Адаптер питания 12 V и 1,25 A для настольного размещения



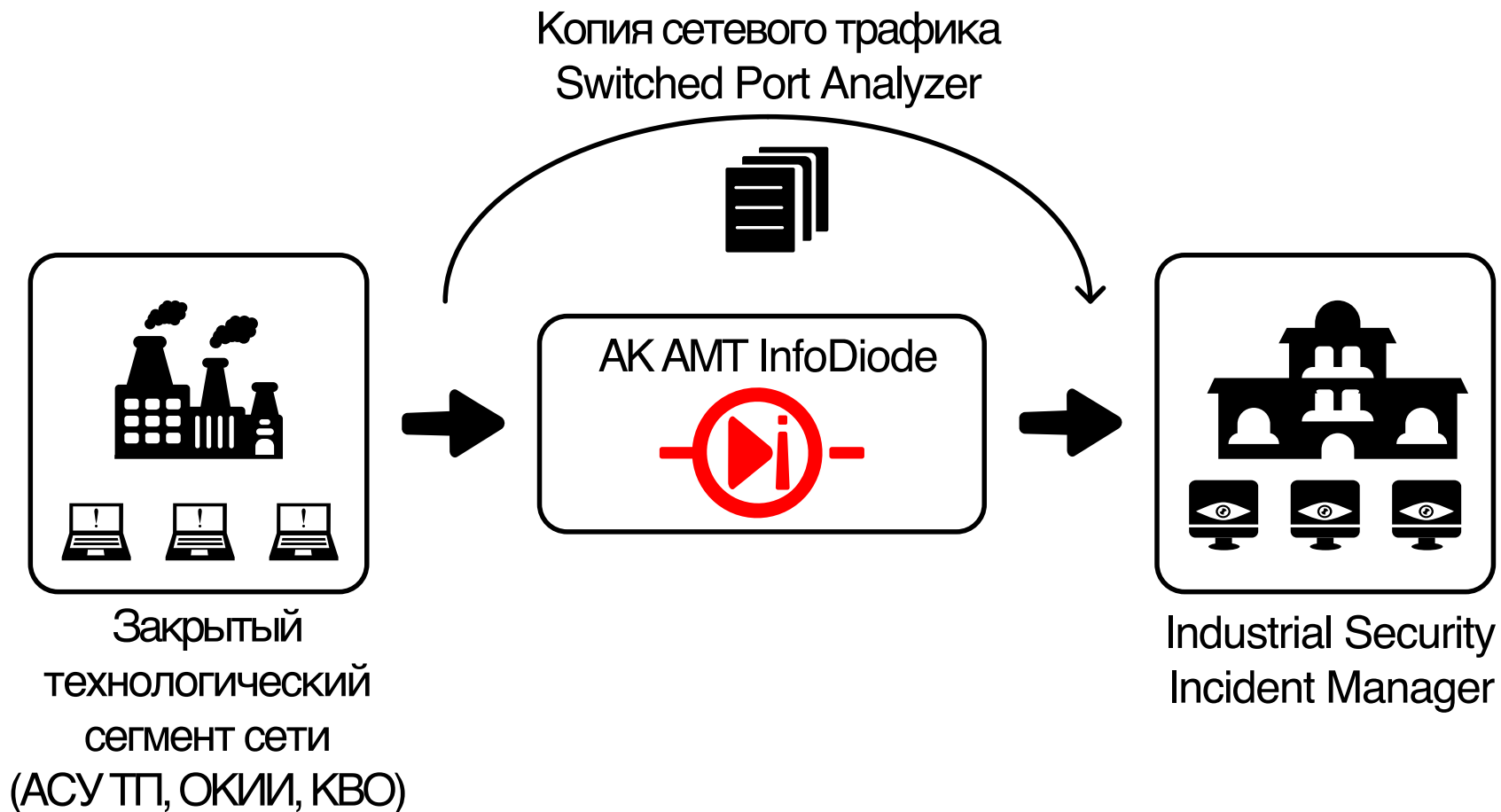
- Сертификация ФСТЭК НДВ4, УД4
- Сертификат соответствия требованиям тех.регламента Таможенного Союза
- Производство устройств сертифицировано



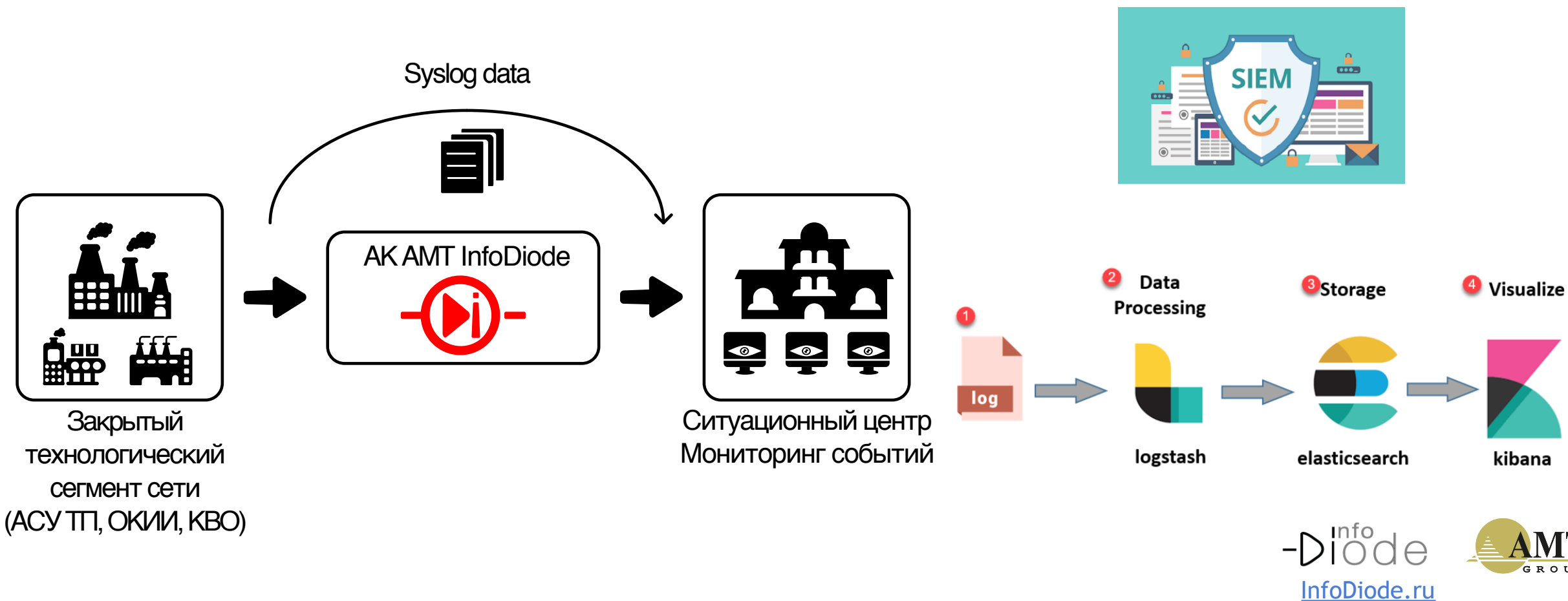
Базовый вариант	Кластерный вариант
InProxy, OutProxy сервер	2 InProxy, 2 OutProxy сервера
АК InfoDiode, rack module	2 АК InfoDiode, rack module, Cluster
Форм фактор - 3U	Форм-фактор - 6U

- ❑ Компактный, упрощает встраивание в разнородную инфраструктуру
 - ❑ Виртуальные среды, серверы заказчика, докеры, операционные системы
- ❑ Обеспечивает поддержку промышленных протоколов (MQTT, Modbus, IEC104...)
- ❑ Улучшает нефункциональные показатели текущего продукта
- ❑ Потенциально предусматривает исполнение в различных форм-факторах
- ❑ Учитывает перспективный сегмент IoT устройств

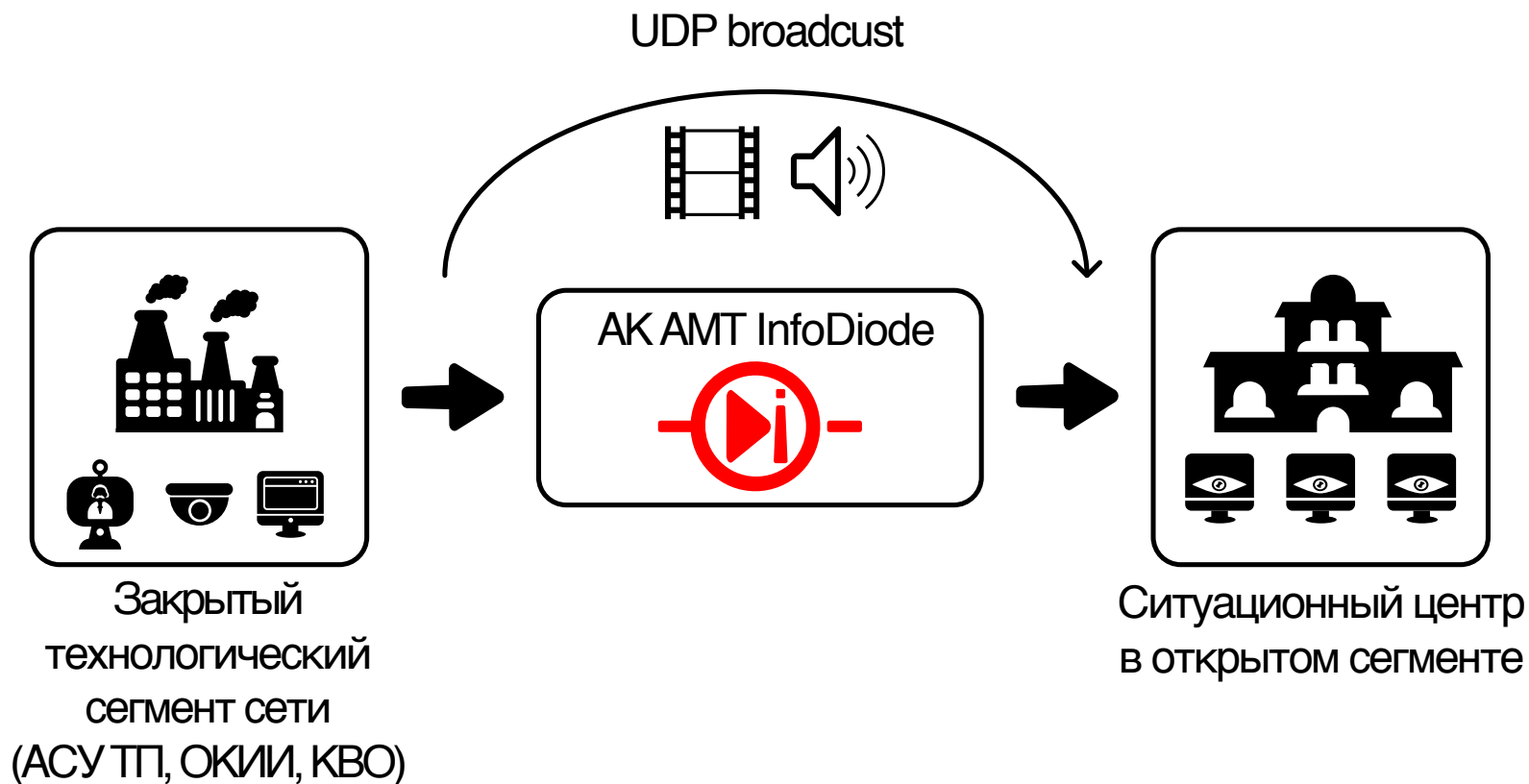




Вариант 2. Передача событий технологической сети с использованием Syslog на внешнюю систему мониторинга. Логирование событий внутри технологического сегмента в централизованной системе мониторинга событий позволяет существенно снизить вероятность возникновения аварийных ситуаций и консолидировать все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



Вариант 3. Передача видео- и аудио-трафика из закрытого сегмента с использованием UDP, в том числе широковеостательных видеопотоков. Часто бывает важно осуществлять удаленный видео-мониторинг, получение сигналов от системы оповещения внутри закрытого технологического сегмента. Использование АК InfoDiode обеспечивает получение видео- и аудио- потоков, при этом гарантирует изоляцию закрытого сегмента



ПК, для которых установка доп. ПО невозможна:

- Специфичная (нетиповая, устаревшая) ОС
- ПК категорирован

1



2



3

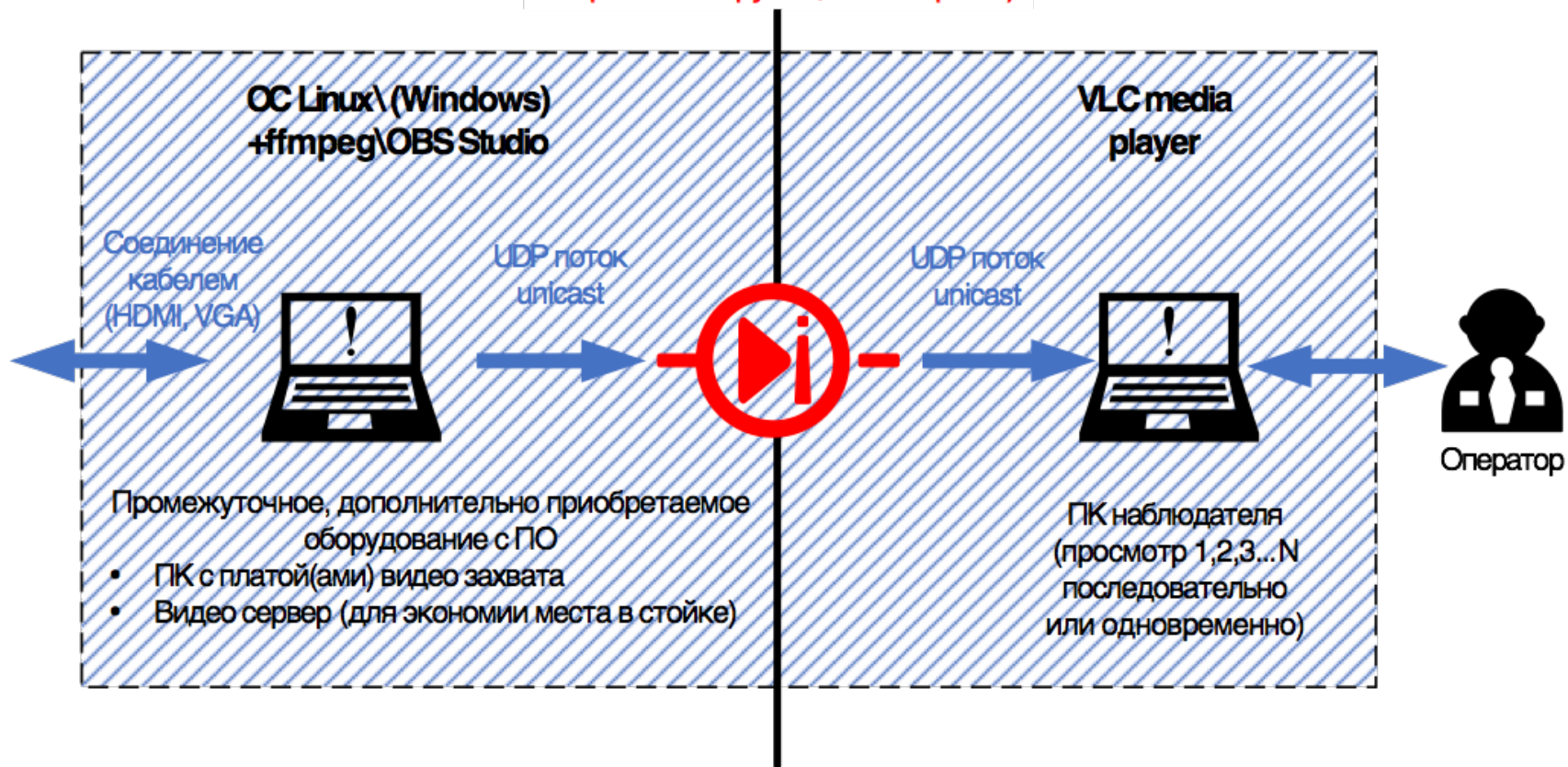


...

N



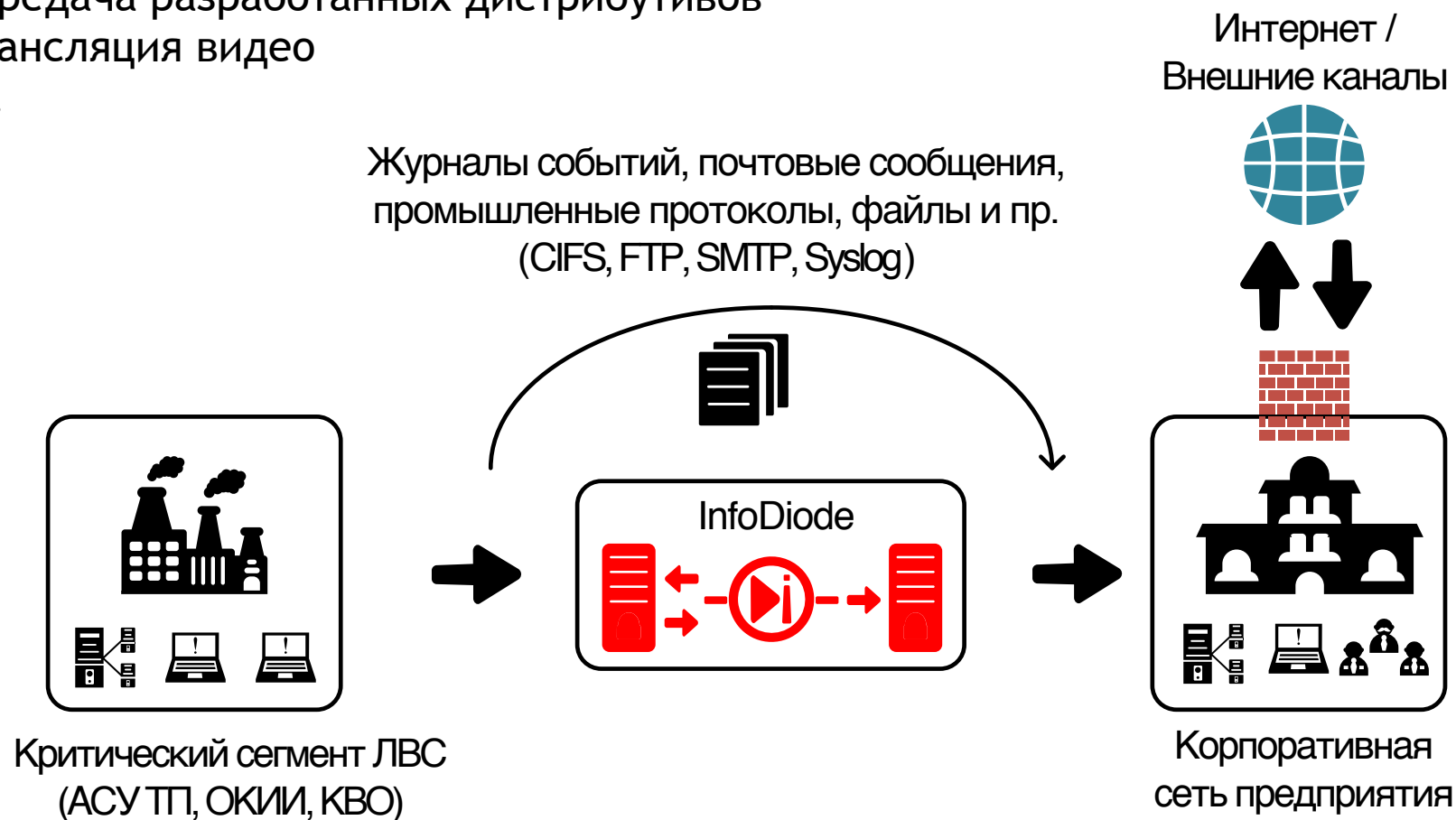
Передача данных в обратную сторону **НЕВОЗМОЖНА**
(аппаратная защита при сохранении функции контроля)



Вариант 1. Экспорт данных

В данном сценарии обеспечивается гарантия целостности передаваемых данных.

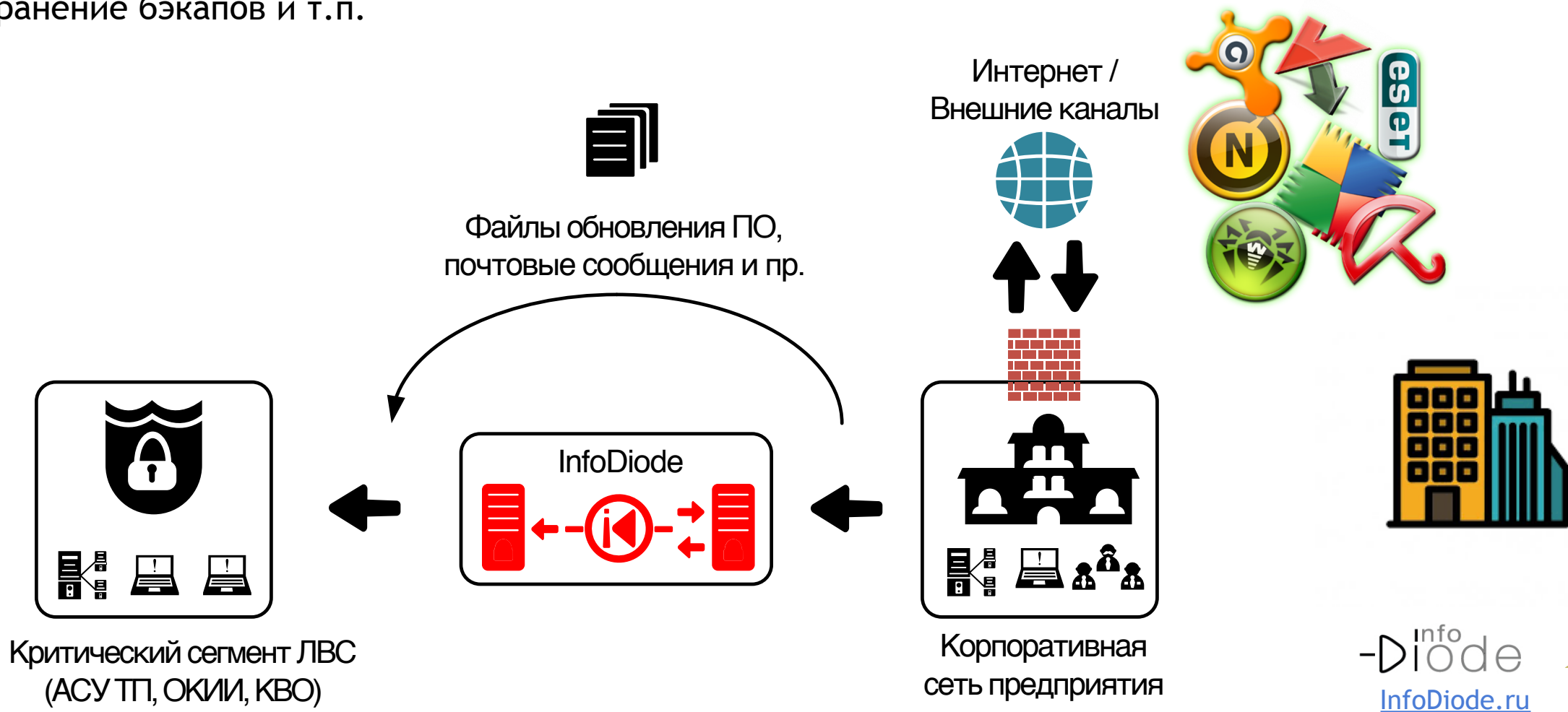
- Экспорт данных для ситуационных центров
- Реплика ВМ, баз данных
- Передача разработанных дистрибутивов
- Трансляция видео
- и т.п.



Вариант 2. Импорт данных

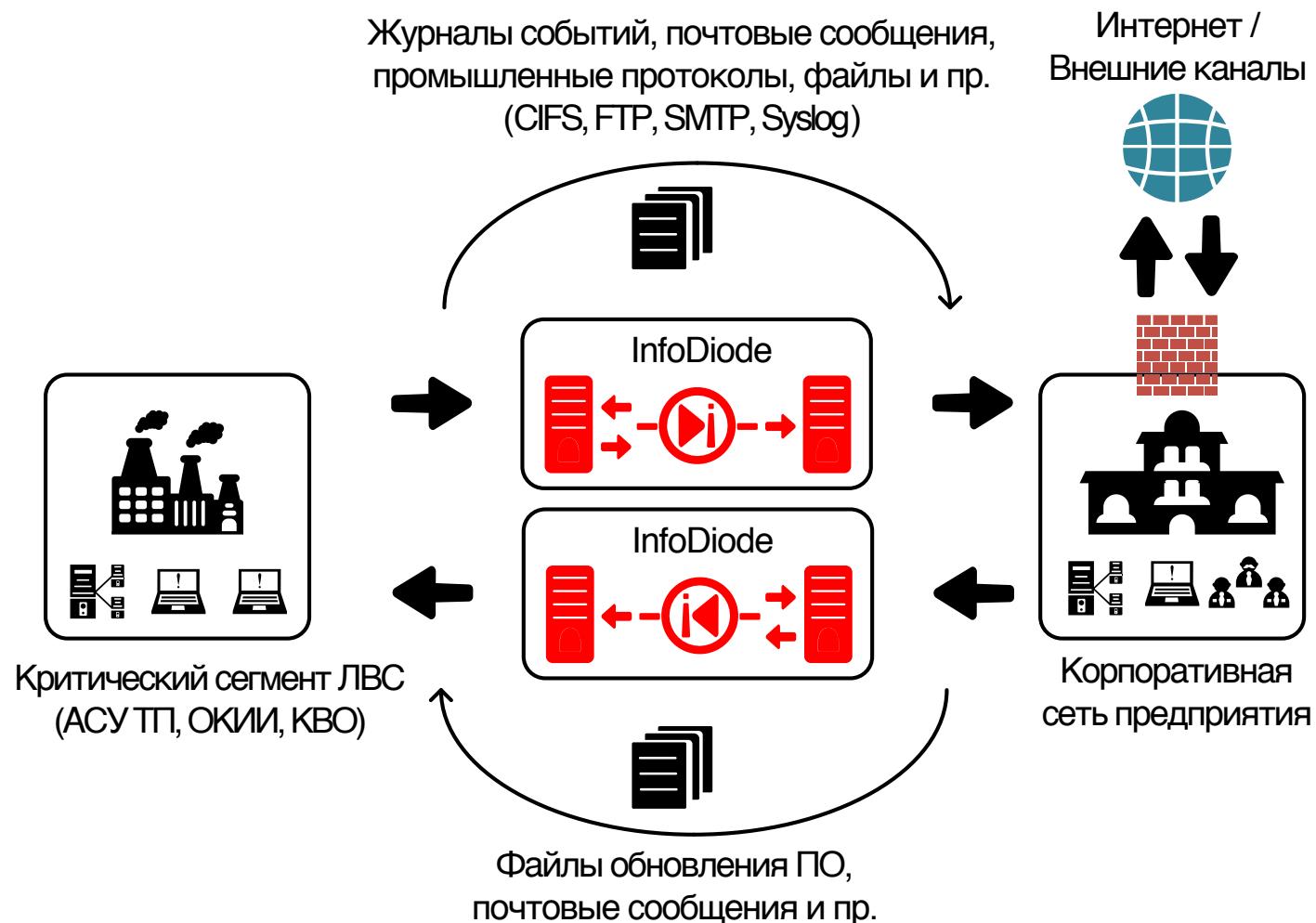
В данном сценарии обеспечивается гарантия конфиденциальности защищаемых данных.

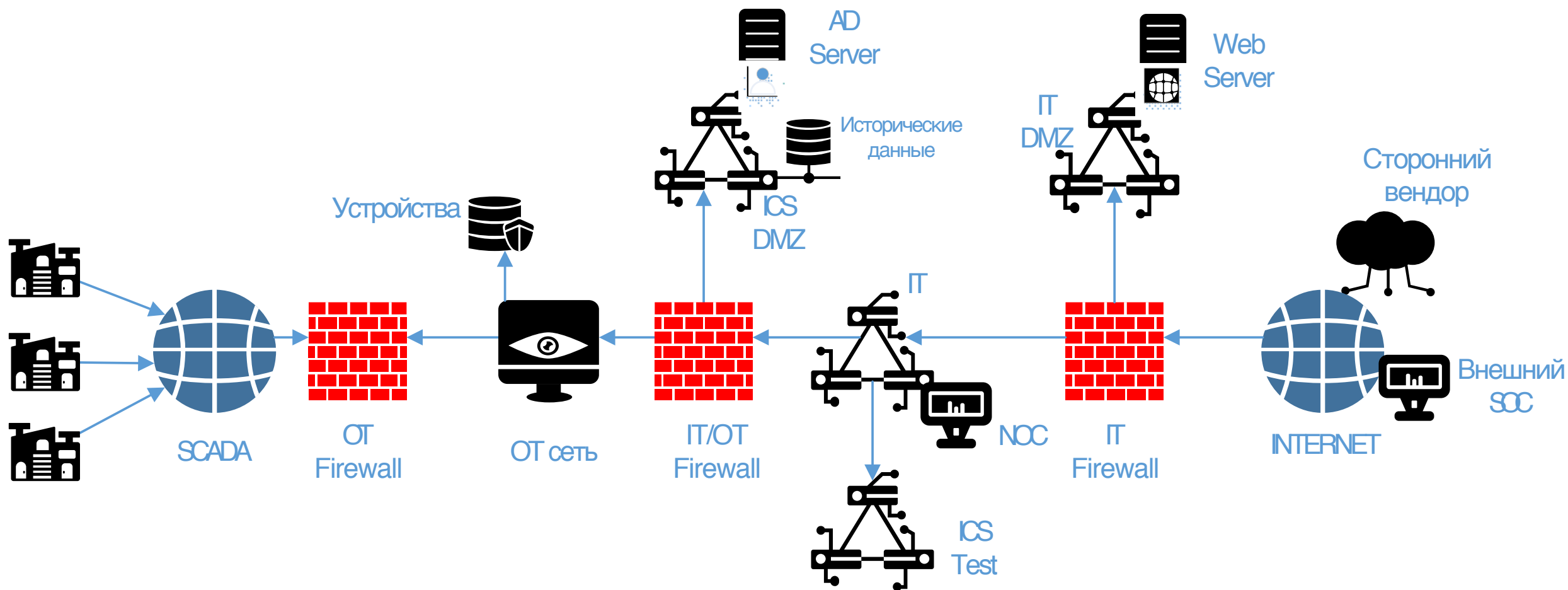
- Загрузка обновлений
- Хранение бэкапов и т.п.

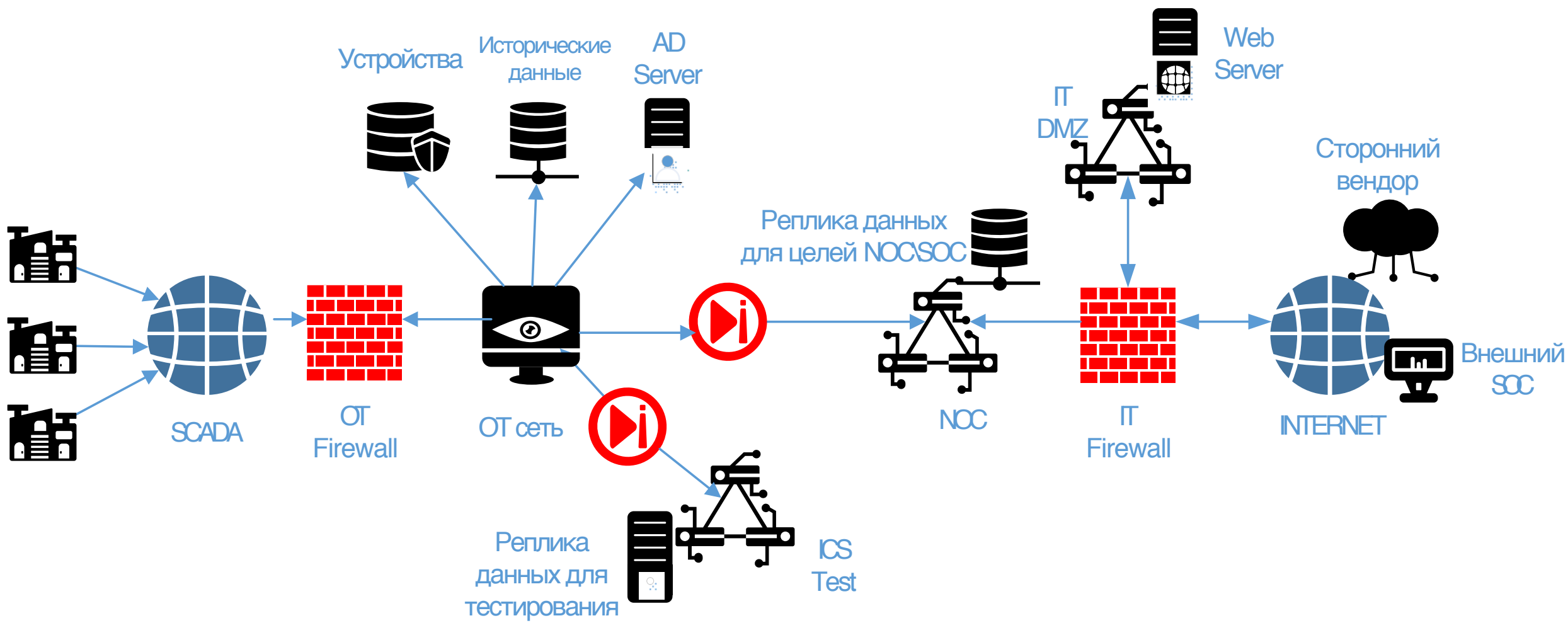


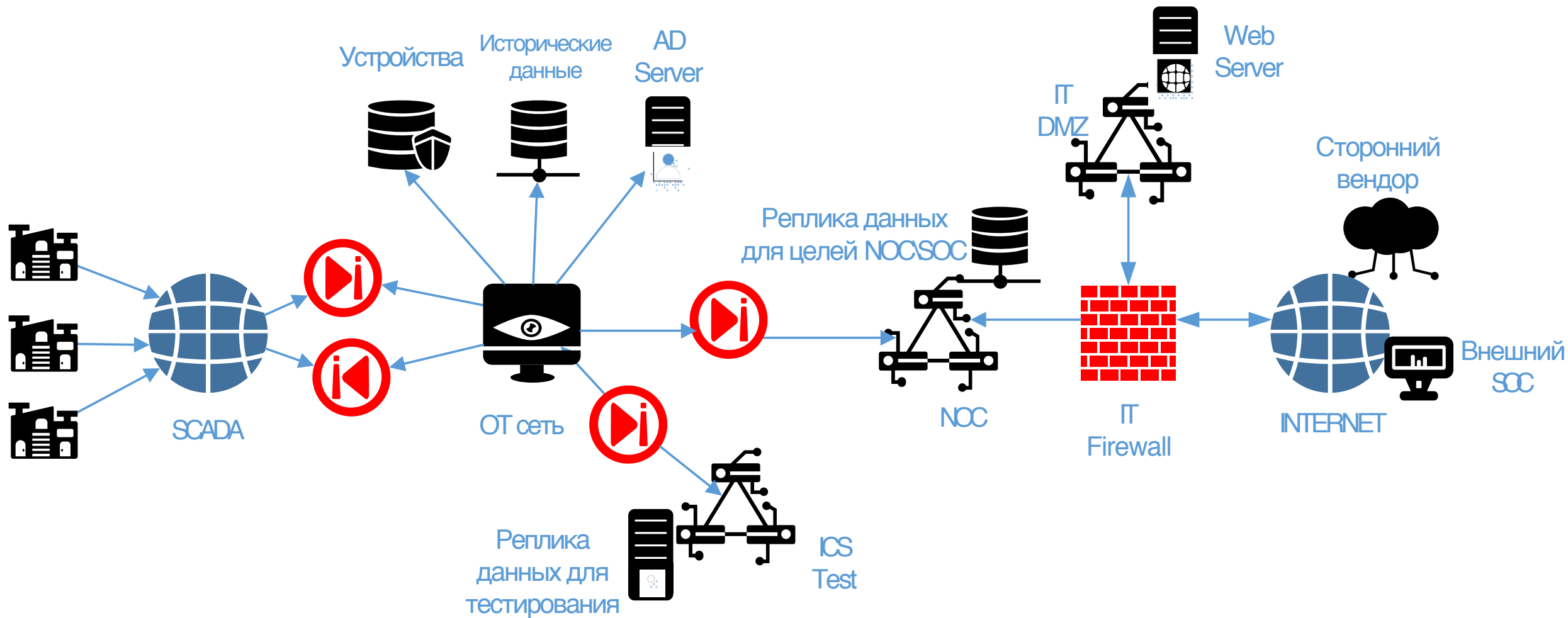
Вариант 3. Одновременная выгрузка и загрузка данных

- Объединение варианта 1 и 2 для АПК InfoDiode
- Либо изолированные, либо синхронизированные контуры









- **Состав спецификации**

- Оборудование – комплект, производство АМТ-ГРУП
- Лицензии – полнофункциональные и бессрочные
- Техническая поддержка оборудования
- Компоненты для формирования ЗИП
- 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: 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!