08.09.2021

АМТ-ГРУП

InfoDiode: безопасность сегментов КИИ в территориально-распределенной сети предприятия

Волков Пётр – ведущий аналитик АМТ-ГРУП

Современное предприятие 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 архивирования данных
  - Отопление, вентиляция, кондиционирование (HVAC)
  - Системы безопасности (как информационной, так и общей)
  - Диспетчерские
  - Системы поставщиков и подрядчиков
- ПО в рамках сети OT/ICS (АСУ ТП), как правило, «унаследовано»
  - ПО создавалось без учета ИБ, ряд промышленных протоколов не предполагают аутентификацию

Сети крупных и территориально-распределенных предприятий

- Разнообразие связей с внешними и внутренними агентами
- Разнообразие ролей
- Разнообразие угроз
- Разная тяжесть последствий
- Зачастую бессистемный подход к организации ИБ

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

Фактор времени

Ряд средств защиты доказали свою эффективность за счет применения принципов асинхронности и «пространственного разделения»

- **Двухфакторная аутентификация на базе RSA** – достаточно успешно противостоит фишинговым атакам. Имея только удаленный доступ, осуществить фишинговую атаку становится невозможно

- **Аппаратное обеспечение TPM** – ключи шифрования никогда не покидают выделенные криптографические аппаратные модули и не появляются в памяти компьютера, на котором работает TPM. Без физического демонтажа оборудования похитить ключи шифрования оказывается невозможно

- **Однонаправленные шлюзы** – физически способны передавать информацию только в одном направлении – от критически важной ОТ 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

Фактор пространства

Домены безопасности и повышение уровня защищенности их периметра

Сегментирование сети

Домен безопасности - домен, который реализует свою политику безопасности и управляется одним органом управления*.

* https://csrc.nist.gov/glossary/term/security_domain (National Institute of Standards and Technology (NIST)) **Ключевые аспекты** – своя политика безопасности и изолированный орган управления

- ❑ Домены организовываются по территориальному признаку/по назначению
- ❑ Обычно на границе домена ставится Firewall
- ❑ Могут быть иерархическими

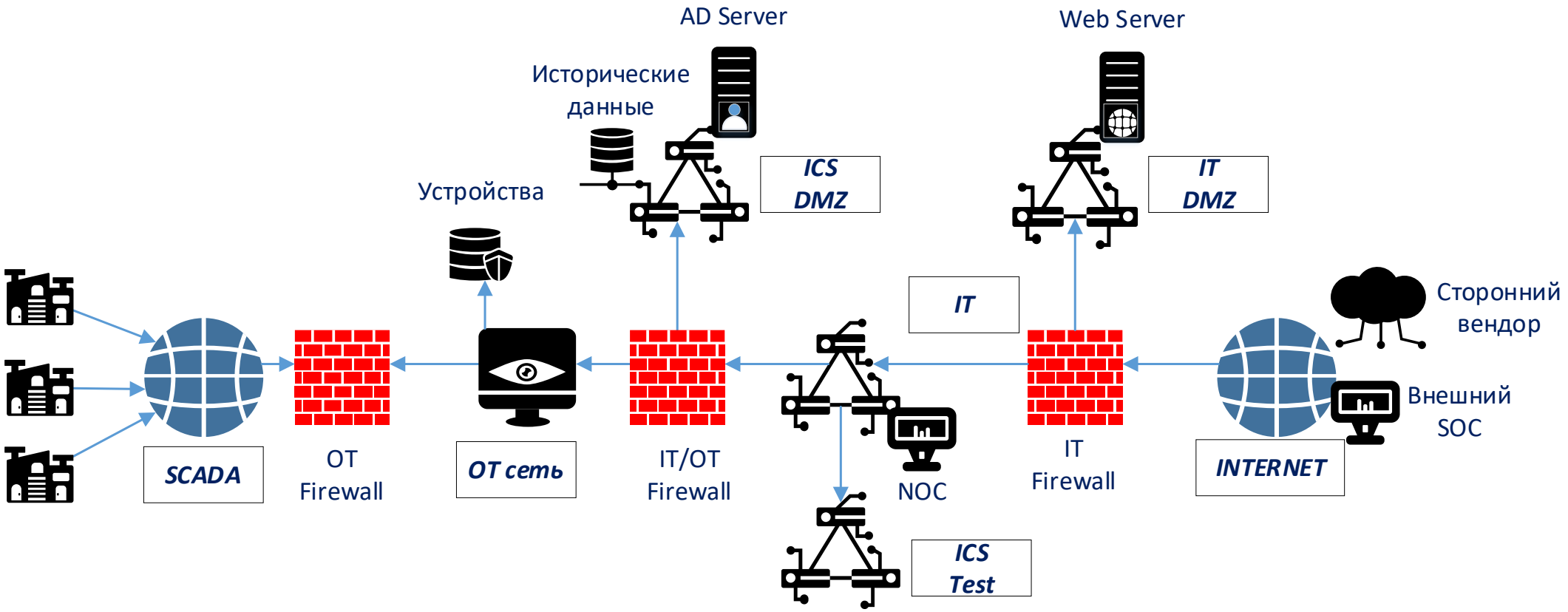
По назначению:

- ❑ Продуктивный сегмент
- ❑ Колл-центр
- ❑ «Песочница»
- ❑ Ситуационный центр
- ❑ Лаборатория ИБ
- ❑ Объект КИИ
- ❑ …

По расположению:

- ❑ Центральный офис
- ❑ Филиал
- ❑ Удалённый/автономный объект
- ❑ Внешний ЦОД
- ❑ …

Сегментирование сети на домены



Что такое CDS

- **Cross Domain Solutions (CDS)** - это система/набор решений для обеспечения безопасности информации, состоящая из специализированного ПО, а иногда и аппаратного обеспечения, которое предоставляет инструменты для ручного или автоматического ограничения доступа или передачи информации между двумя или более доменами/сегментами безопасности*.

* https://csrc.nist.gov/glossary/term/cross_domain_solution (National Institute of Standards and Technology (NIST))

Цель применения CDS состоит в том, чтобы позволить доверенному сетевому домену обмениваться информацией с другими доменами в одностороннем или двунаправленном порядке, не создавая угроз безопасности, которые обычно возникают при подключении к сети. Такие решения как правило требуют сертификации регулятора.

Политика нулевого доверия может быть эффективно построена именно на диодах

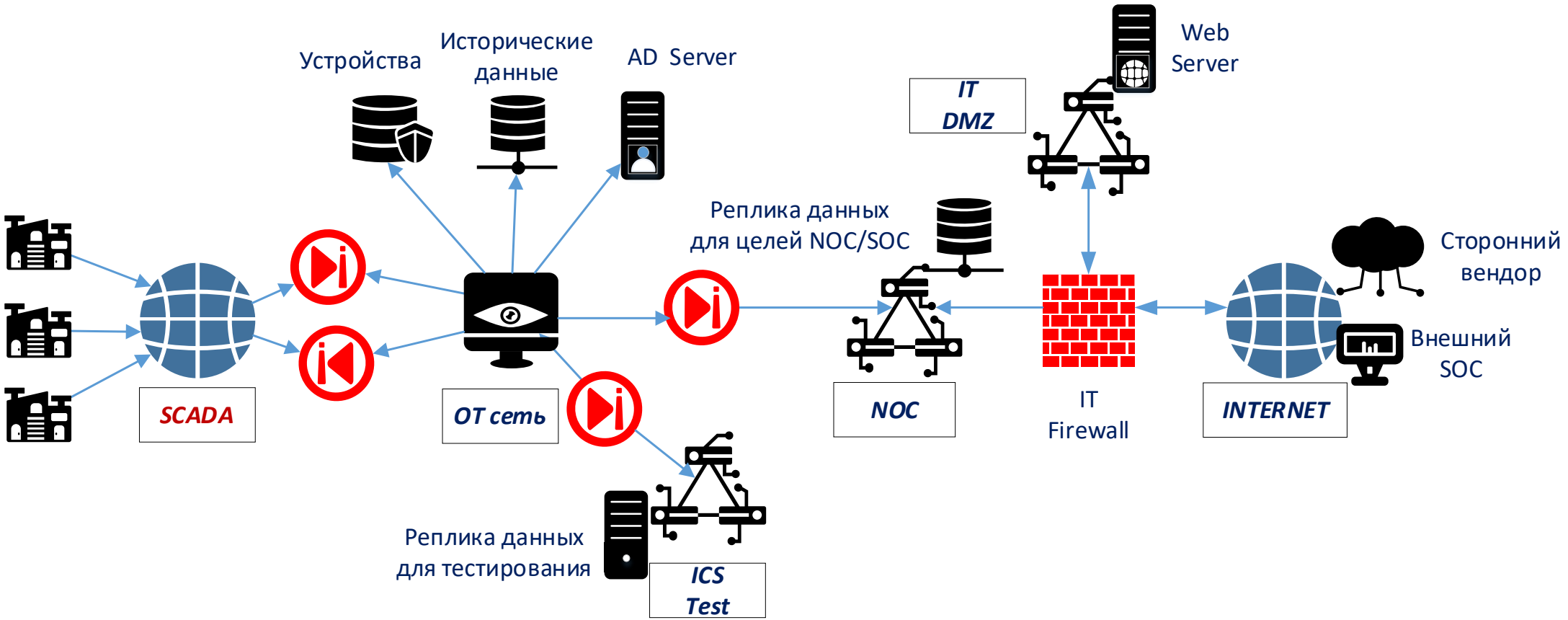
Software

- 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

Пример перехода от защиты только на Firewall к защите с использованием InfoDiode



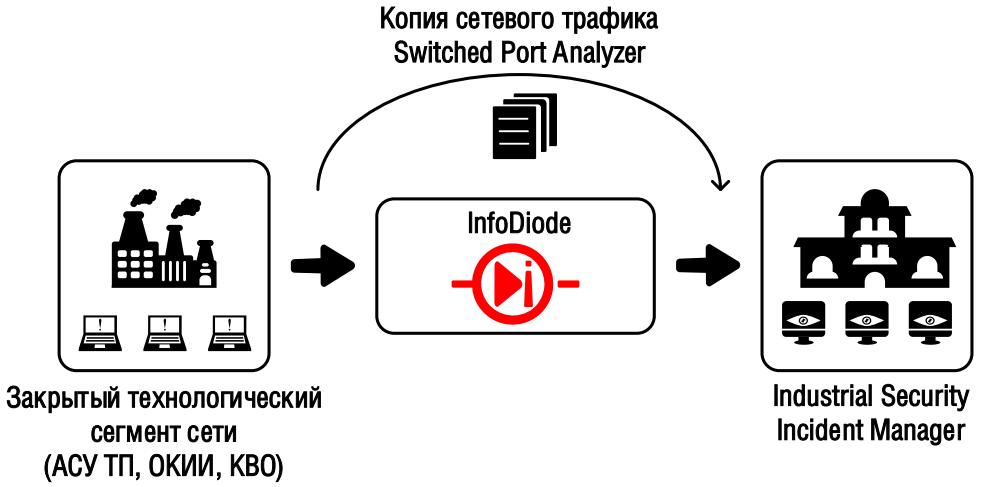
Сценарии защиты периметра, основанные на однонаправленной передаче данных

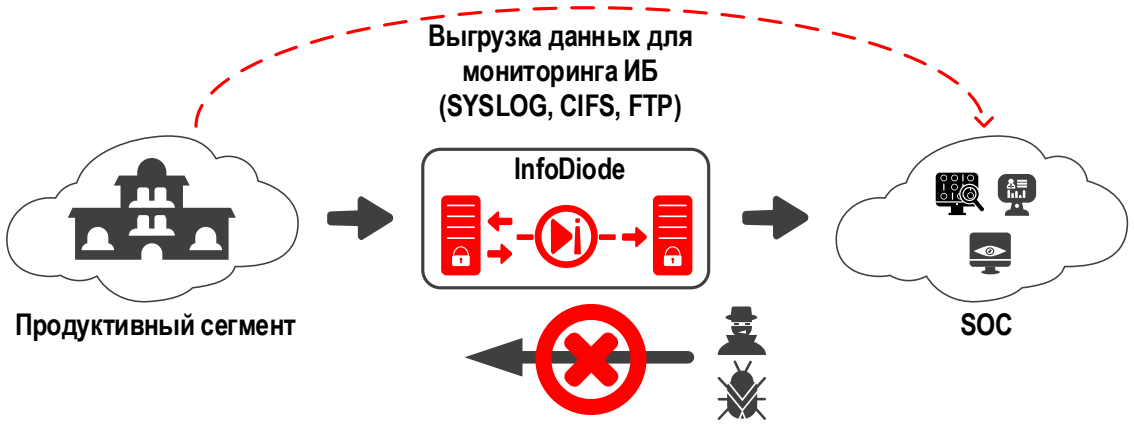
Односторонняя отправка данных из домена

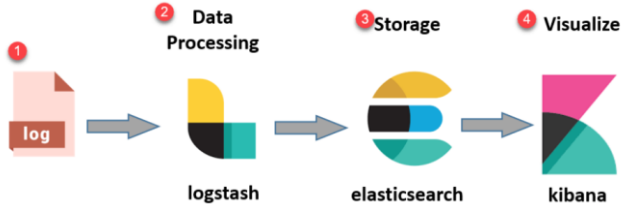
Мониторинг сети

Вариант 1. Передача копии технологического трафика закрытого сегмента во внешнюю систему мониторинга с использованием SPAN.

Вариант 2. Передача событий технологической сети с использованием Syslog на внешнюю систему мониторинга.





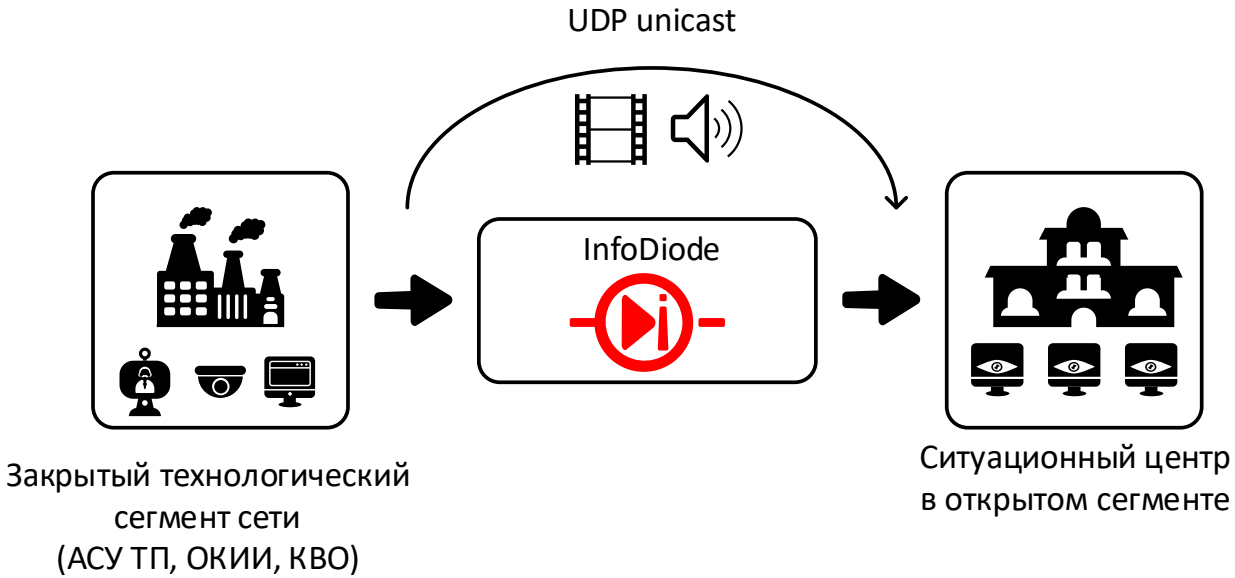


InfoDiode.ru

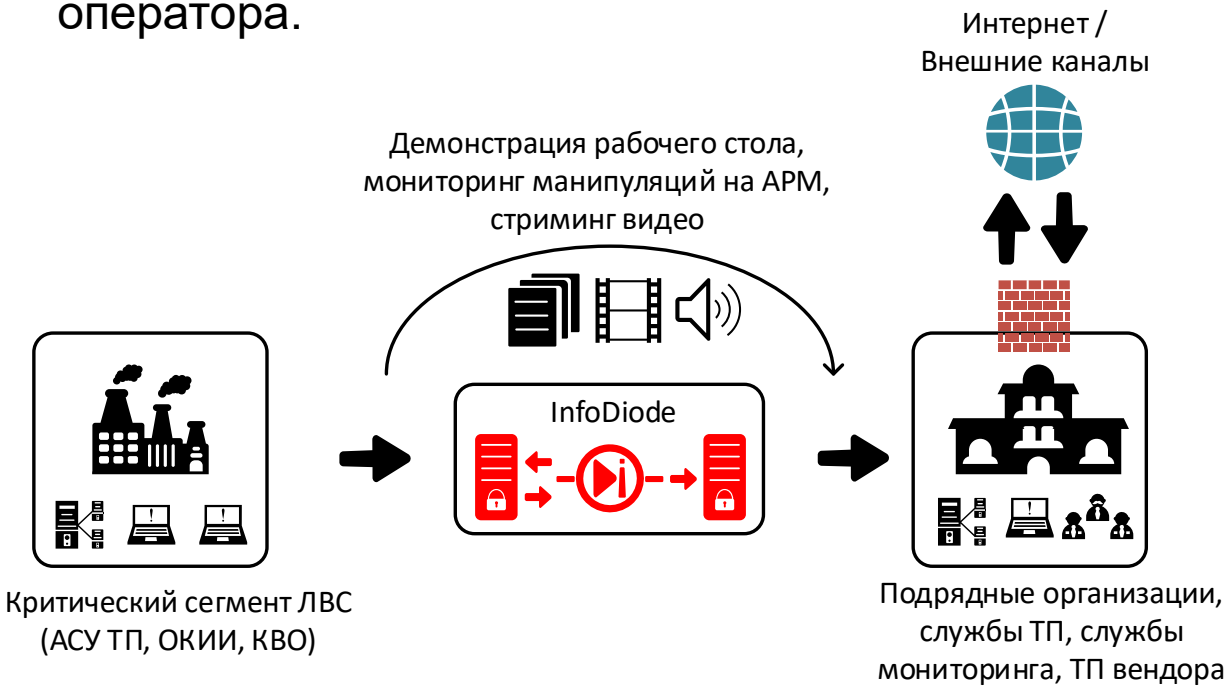
Односторонняя отправка данных из домена

Мониторинг окружения

Вариант 1. Трансляция видео с камер видеонаблюдения.



Вариант 2. Демонстрация рабочего стола оператора.



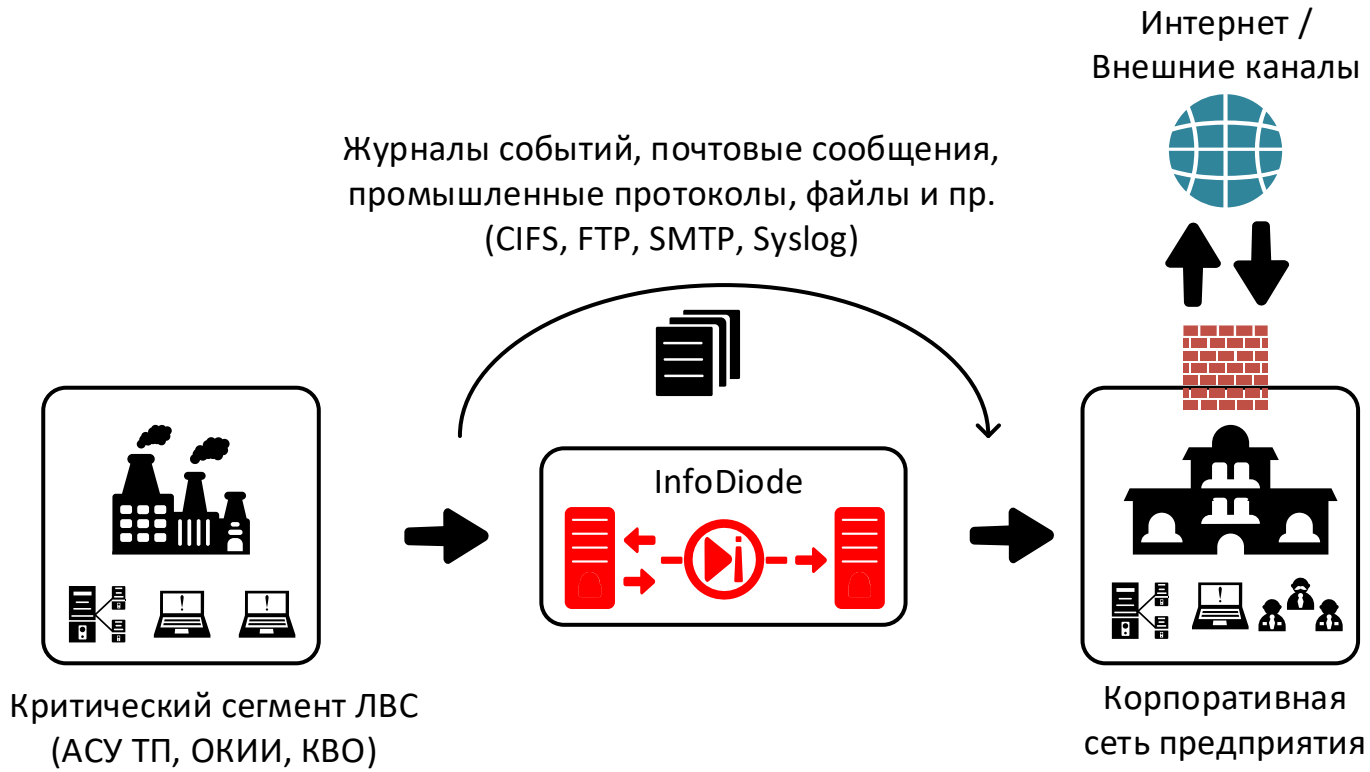
InfoDiode.ru

Односторонняя отправка данных из домена

Экспорт данных

В данном сценарии обеспечивается гарантия целостности передаваемых данных.

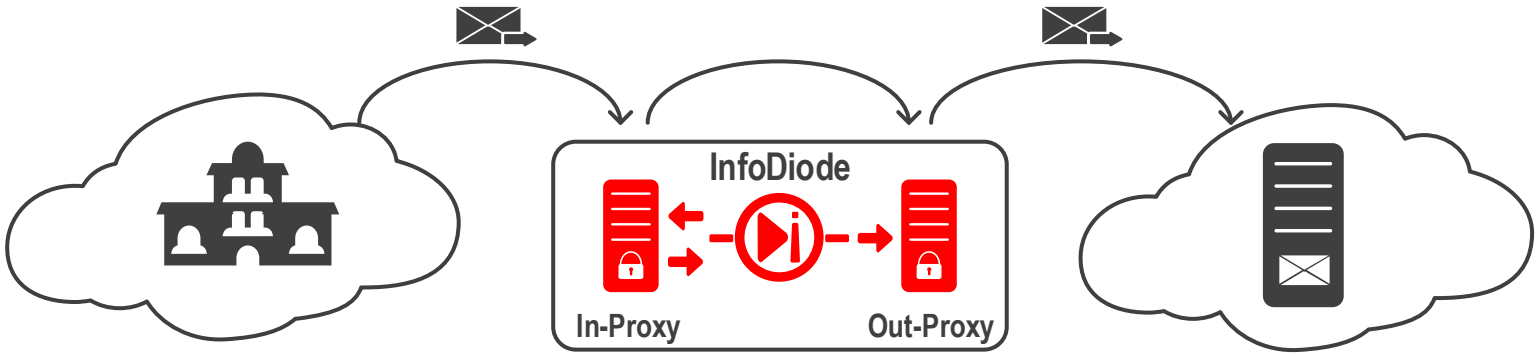
- ❑ Экспорт данных для ситуационных центров
- ❑ Реплика ВМ, баз данных



Односторонняя отправка данных из домена

Экспорт данных

- ❑ Передача разработанных дистрибутивов
- ❑ Отправка уведомлений



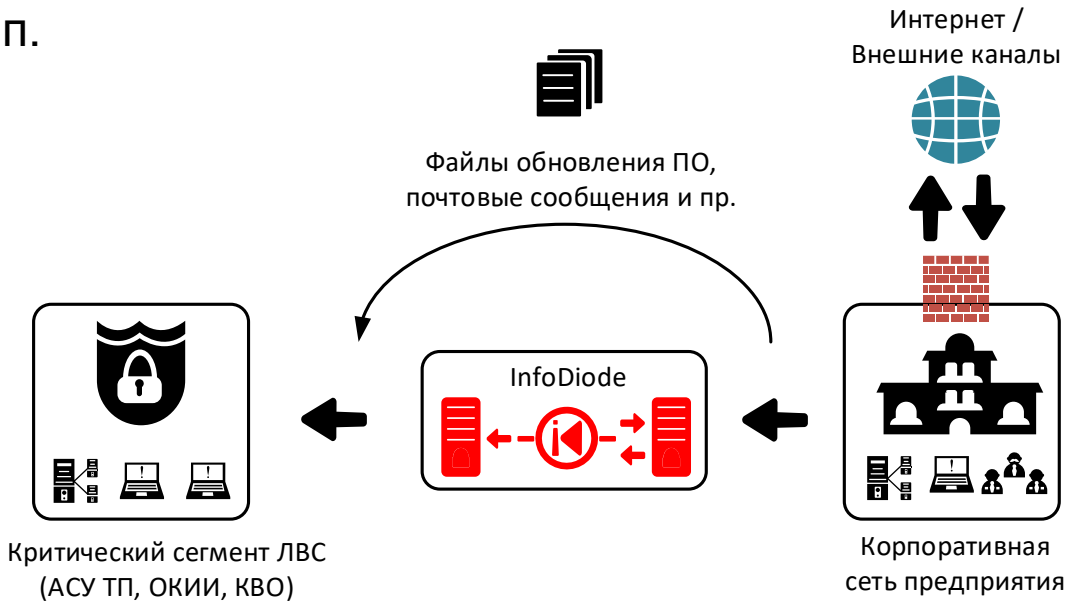
Одностороннее получение данных в домен

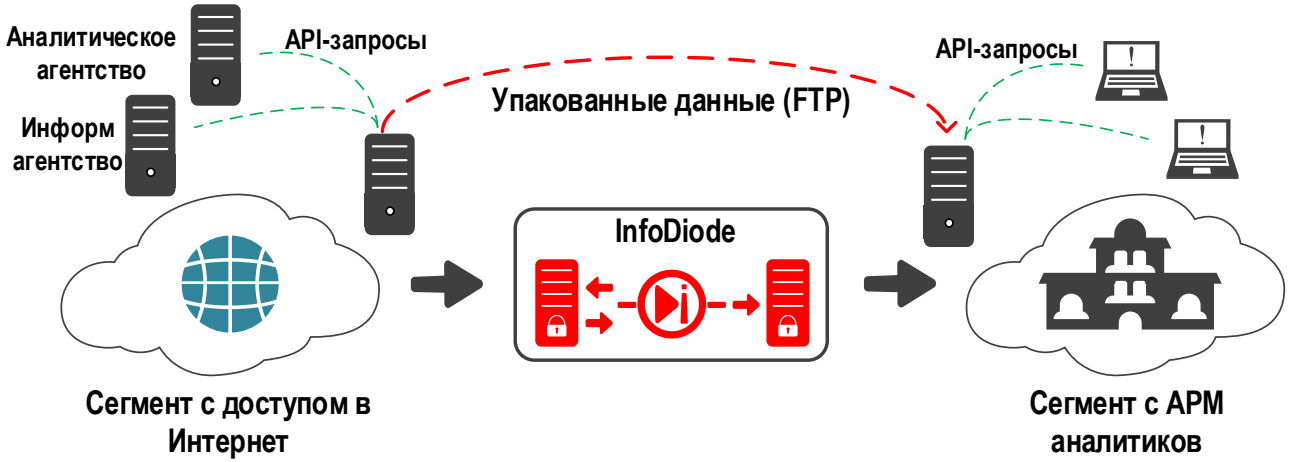
Импорт данных

В данном сценарии обеспечивается гарантия конфиденциальности защищаемых данных.

- ❑ Загрузка обновлений
- ❑ Получение информации от внешнего источника
- ❑ Хранение бэкапов

и т.п.



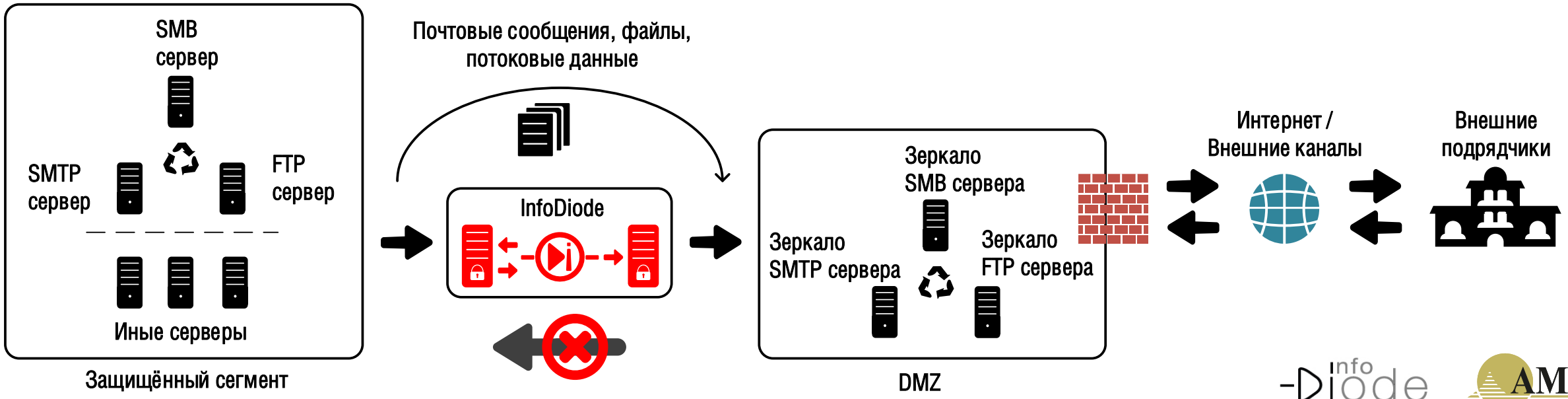


InfoDiode.ru

Изоляция домена

Вариант 1. Лаборатория информационной безопасности

Вариант 2. Демилитаризованная зона (DMZ)

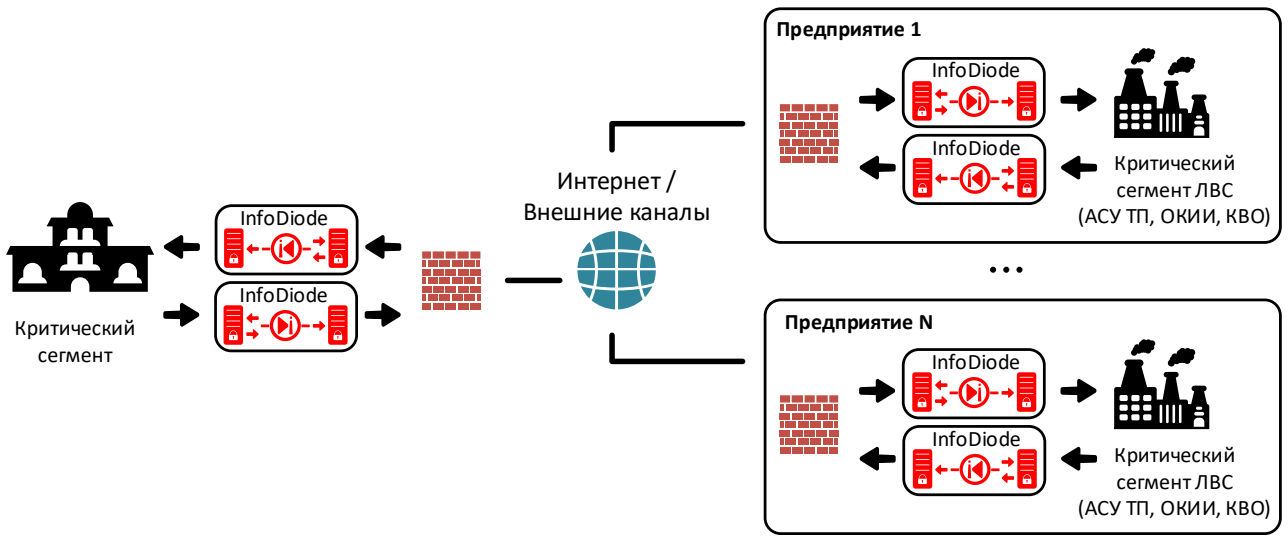


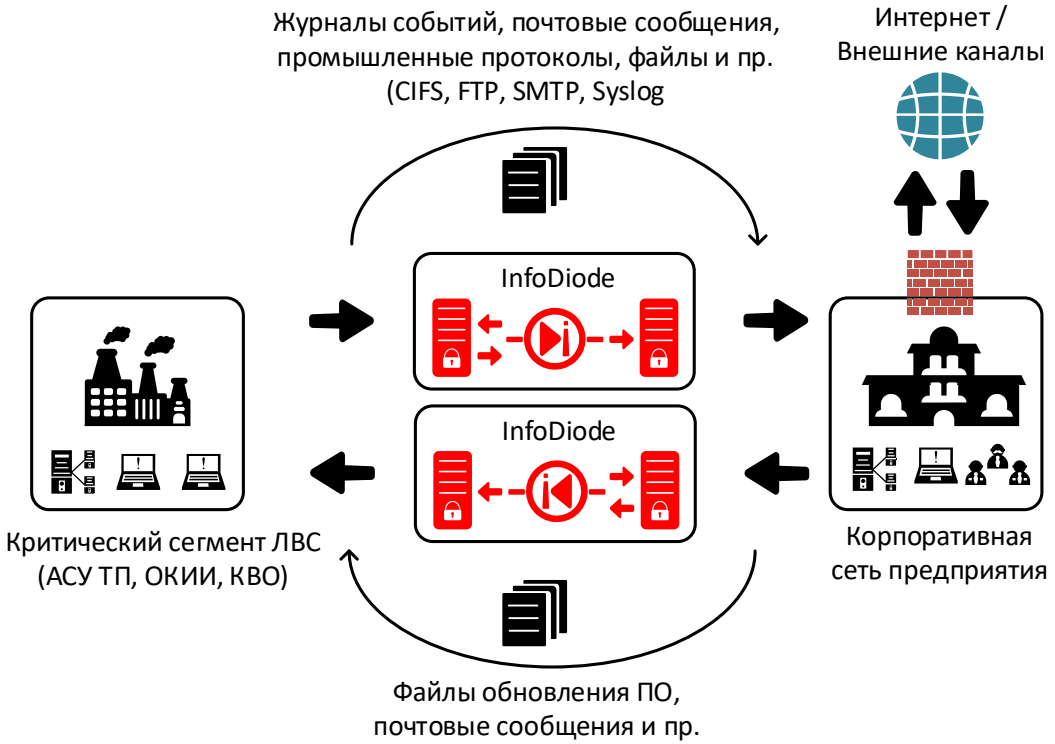
InfoDiode.ru

Комплексный сценарий

Применение средств однонаправленной передачи не запрещает организовывать одновременно несколько каналов – по одним реализуются сценарии получения данных, а по другим – отправки.

Двунаправленное воздействие по-прежнему невозможно.





InfoDiode.ru

InfoDiode

АК «InfoDiode» эффективно сочетают все лучшие практики по защите периметра

- Стоимость аппаратных диодов начинается от 150 т.р.

ЛИНЕЙКА АК INFODIODE

InfoDiode
rack module

• Встроенные резервированные блоки питания AC

• Высота 1 RU

• Малая глубина, возможность монтажа 2 устройств с двух сторон шкафа

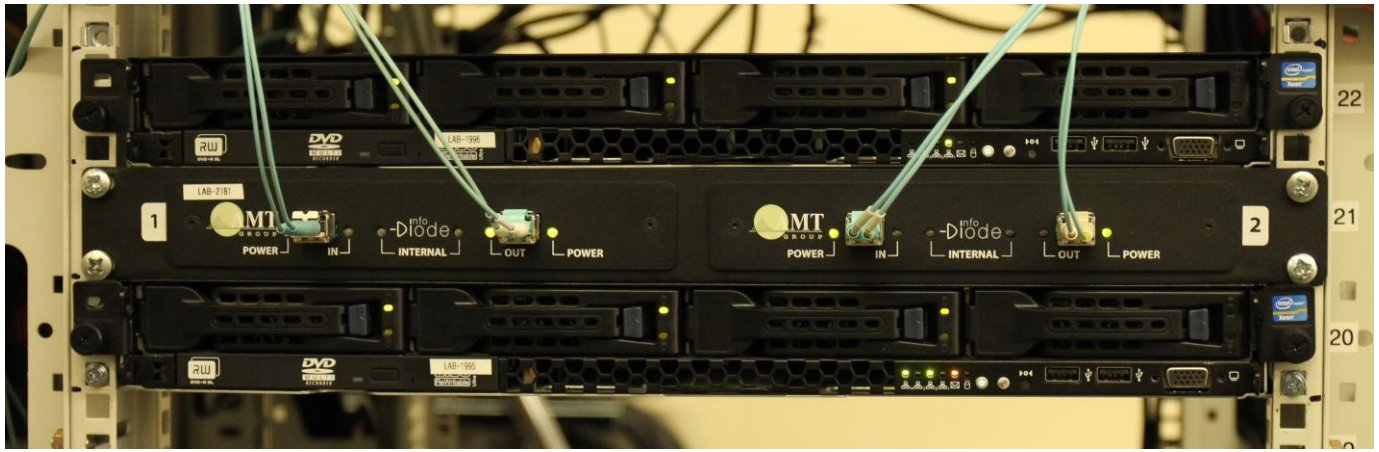
InfoDiode
rack module Cluster

• 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

АПК InfoDiode позволяет соответствовать лучшим практикам по защите периметра и организовать передачу файлового и иного трафика



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

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

InfoDiode.ru

Структура предложений устройств диод на российском рынке

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.

Зарубежные вендоры

Практически отсутствуют на российском рынке

1. Санкции
2. Отсутствие сертификатов соответствия от регуляторов

АМТ-ГРУП

Предлагает комплексные решения:

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

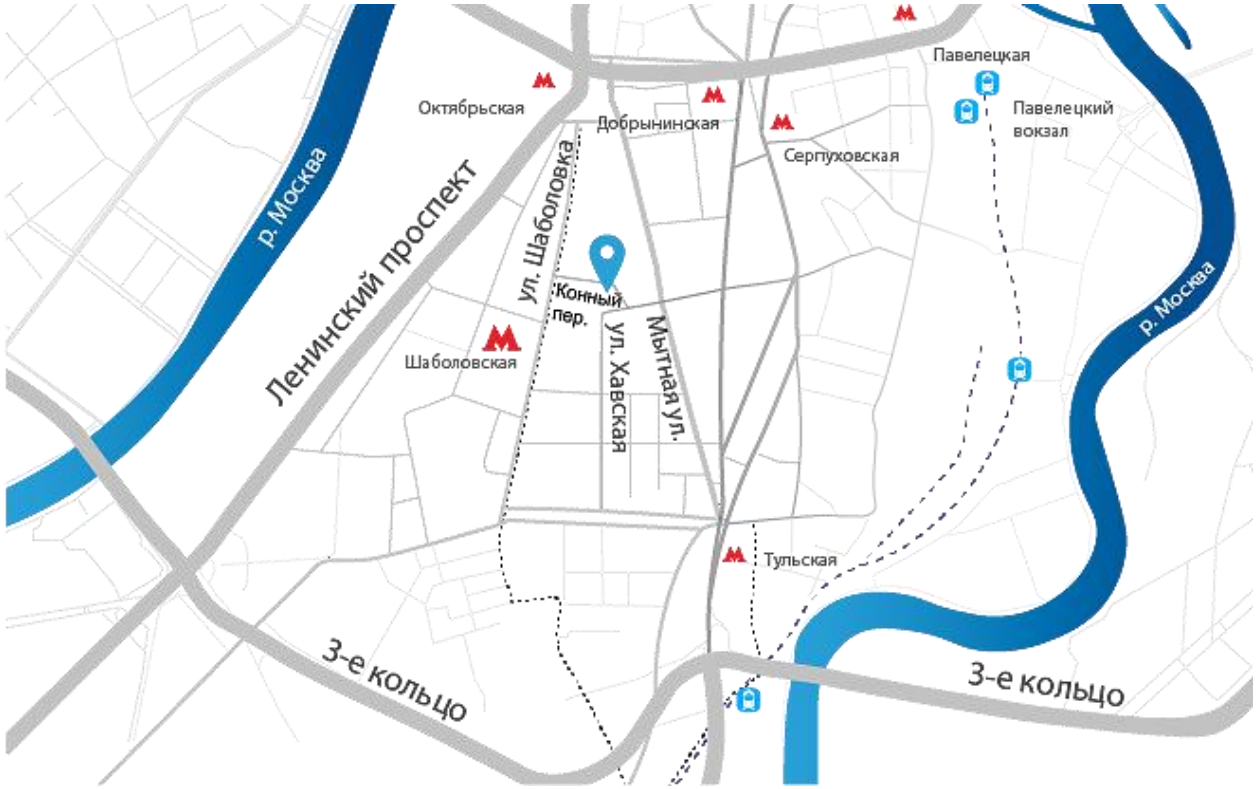
Лицензионная политика и комплексные решения АМТ-ГРУП

- **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

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!