



IT

Центры
обработки
данных

Комплексная
безопасность

Прикладные
информационные
системы

Коммуникационные
решения

ИБ

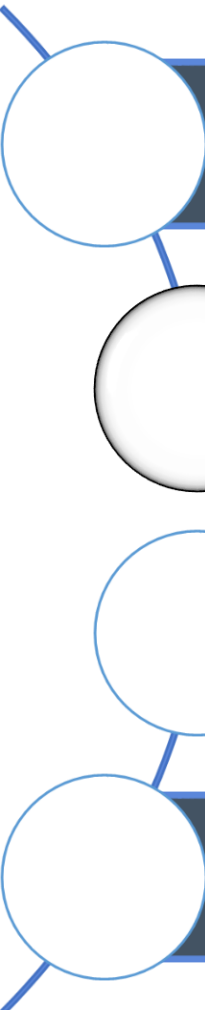
17.02.2020

АМТ-ГРУП

Применение однонаправленных шлюзов
для локализации угроз на границах КИИ
объектов промышленности, нефтегаза и
энергетики

Половинко В.В.



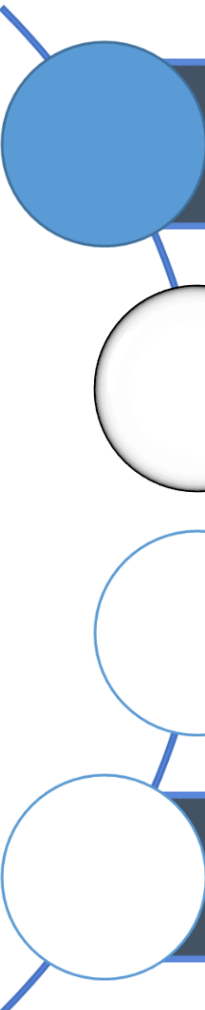


Предпосылки применения устройств класса диод для сегментации сетей

Типовые решаемые задачи (на примере АПК InfoDiode)

Особенности и ограничения применения устройств класса диод

Этапы проектов с применением устройств класса диод (на примере АПК InfoDiode)



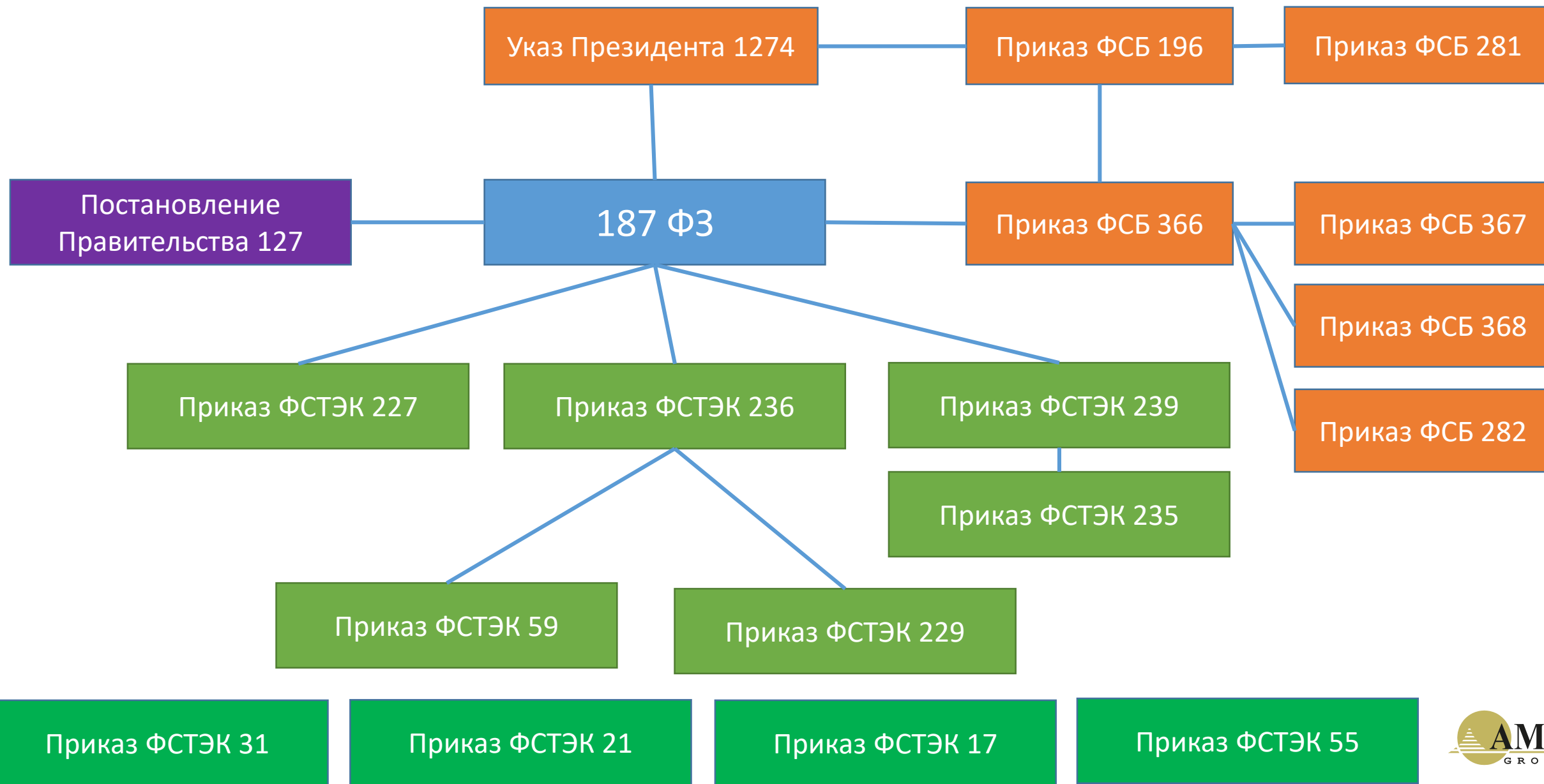
Предпосылки применения устройств класса диод для сегментации сетей

Типовые решаемые задачи (на примере АПК InfoDiode)

Особенности, ограничения, нюансы применения устройств класса диод

Этапы проектов с применением устройств класса диод (на примере АПК InfoDiode)

ТИП УГРОЗЫ	СЛУЧАЙНЫЕ УГРОЗЫ 	ХАКТИВИСТЫ 	ОРГАНИЗОВАННАЯ ПРЕСТУПНОСТЬ 	ПРОМЫШЛЕННЫЙ ШПИОНАЖ 
Мотивация злоумышленника	Получение площадки для атак	Дискредитация/публичная политика/слава	Финансовая выгода	Конкурентная борьба/саботаж/военные действия
Цели	Любой узел/хост в сети Интернет	Любая организация	Финансовый сектор, торговля	Любая индустрия/фокус на ТЭК
Тренды	Постепенно переходит в индустрию и взаимодействие с организационной преступностью	Случайно, непредсказуемо	Получение долговременного доступа в сети жертв	Расширение спектра целевых отраслей/влияние на цепочки поставок



Базовые требования для организаций

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

АСУ ТП, КВО

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

Госаппарат

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

Банки и пр.

Требование УПДЗ (Управление доступом субъектов доступа к объектам доступа)
Требование ЗСВ4 (Защита среды виртуализации): Управление (фильтрация, маршрутизация, контроль соединений, **однонаправленная передача** и иные способы управления) информационными потоками

Дополнительное регулирование для КИИ

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

Инциденты

Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (**ГосСОПКА**)

Среди **типовых** вариантов защиты можно выделить два:

- ☐ Использование программных средств, прежде всего - межсетевых экранов
- ☐ Физическая («воздушная») изоляция сегментов сети

Каждый из вариантов имеет свои преимущества и недостатки



Межсетевой экран (Firewall)

ПЛЮСЫ

МИНУСЫ



1.	Приемлемая защита периметра	Любой программный комплекс уязвим
2.	Удобство использования и невысокая стоимость	Нет гарантии от взлома и ошибок конфигурации
3.		Неудовлетворительная модель угроз

Примеры:

[АНБ эксплуатировало уязвимость межсетевых экранов PIX от Cisco более десяти лет](#)[XSS-уязвимость нулевого дня позволяет похищать учетные данные пользователей Cisco ASA](#)[Уязвимости в межсетевых экранах Kerio Control позволяют скомпрометировать корпоративную сеть](#)

«Воздушный зазор» - физическая изоляция защищаемого сегмента

ПЛЮСЫ

МИНУСЫ

1.

Гарантия от внешнего проникновения

Дублирование инфраструктуры, невозможность автоматизации

2.

Высокая общая стоимость решения из-за дублирования

3.

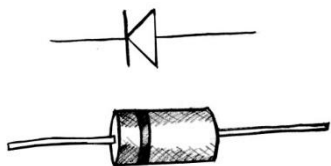
Провоцирует персонал на нарушение режима ИБ



- ❑ 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



Однонаправленные шлюзы



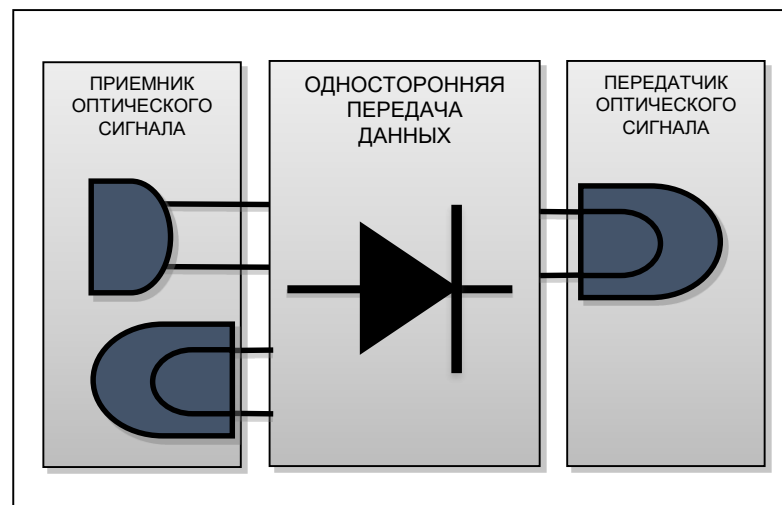
ПЛЮСЫ

МИНУСЫ



1.	Аппаратное разделение сегментов на физическом уровне сети	Незначительные сетевые задержки при передаче данных (по сравнению с сетевым оборудованием)
2.	Невозможность проникновения в защищаемый сегмент	
3.	Поддерживается множество сетевых протоколов	

Аппаратное устройство для
одностороннего обмена



SPAN трафик, тунелинг UDP

Возможно

Невозможно

Аппаратное устройство для одностороннего обмена

Области применения АК «AMT Mini InfoDiode»:

- Однонаправленный обмен информацией для сетей различного уровня критичности через публичные сети
- Безопасная передача данных из критически важных систем для последующего анализа на специализированных системах ИБ и системах мониторинга
- Безопасная запись с датчиков на серверы, расположенные в защищенном сегменте сети



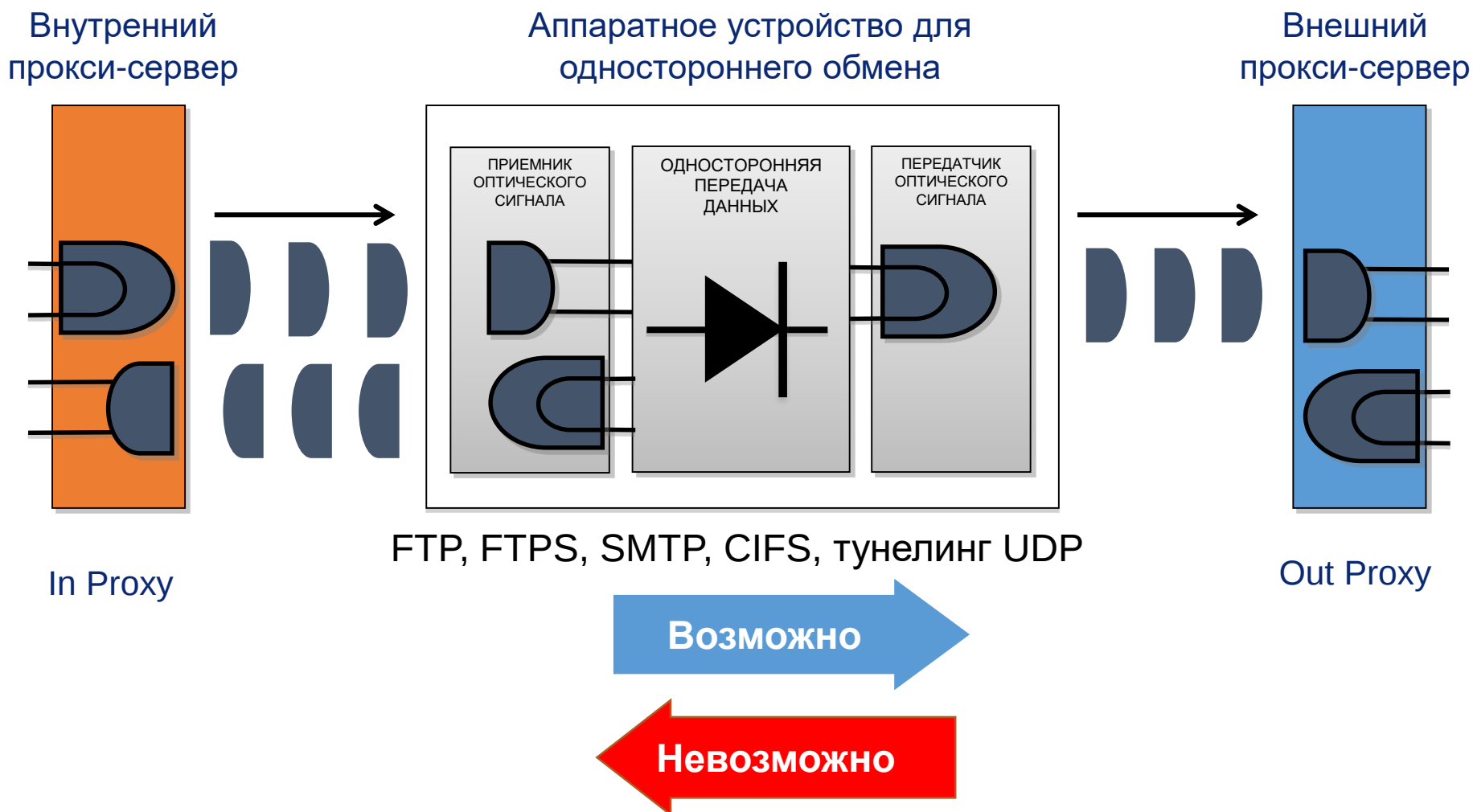
Варианты монтажа:

- Настольное исполнение
- На DIN-рейку
- На монтажную пластину

Габаритные размеры:

- 120 x 50 x 146 мм

АПК – 2 тип - три компонента (2-а сервера и 1 аппаратный диод)





Базовый вариант



Форм фактор - 3U
(2 сервера, АК InfoDiode)

Кластерный вариант



Форм-фактор 6U
(4 сервера, 2 АК InfoDiode)

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



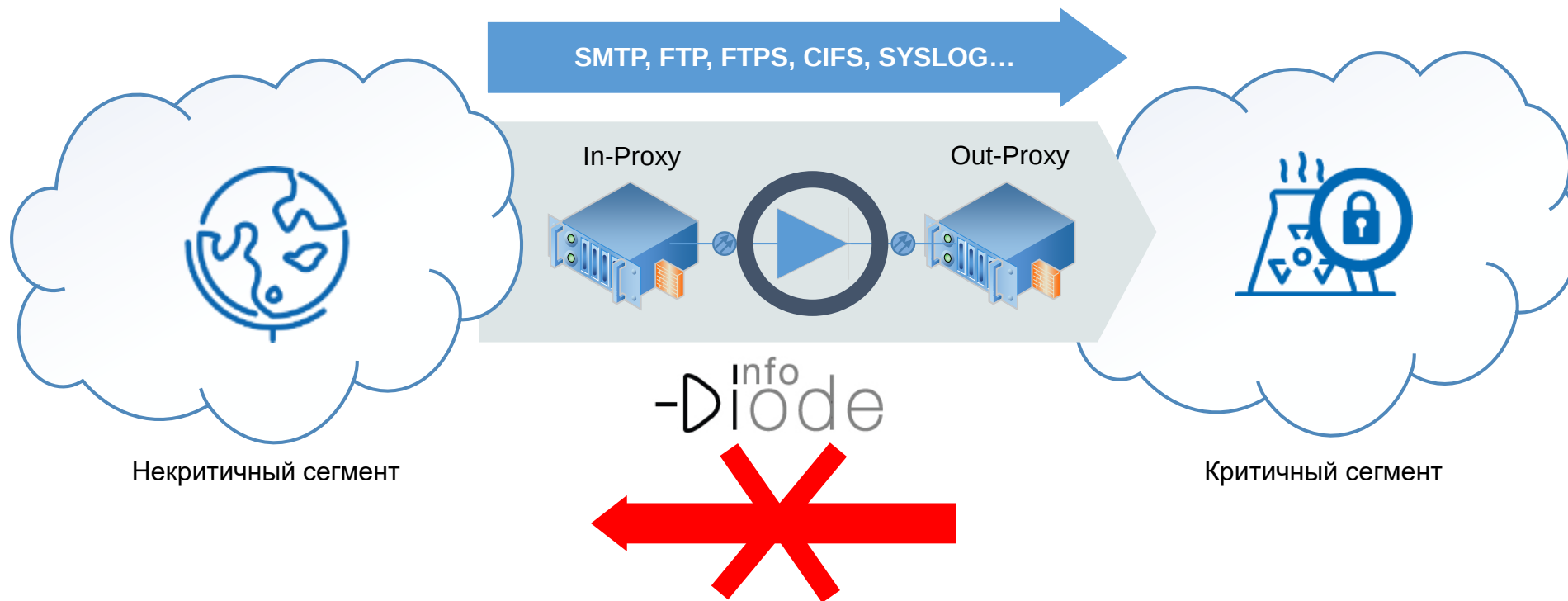
Предпосылки применения устройств класса диод для сегментации сетей

Типовые решаемые задачи (на примере АПК InfoDiode)

Особенности, ограничения, нюансы применения устройств класса диод

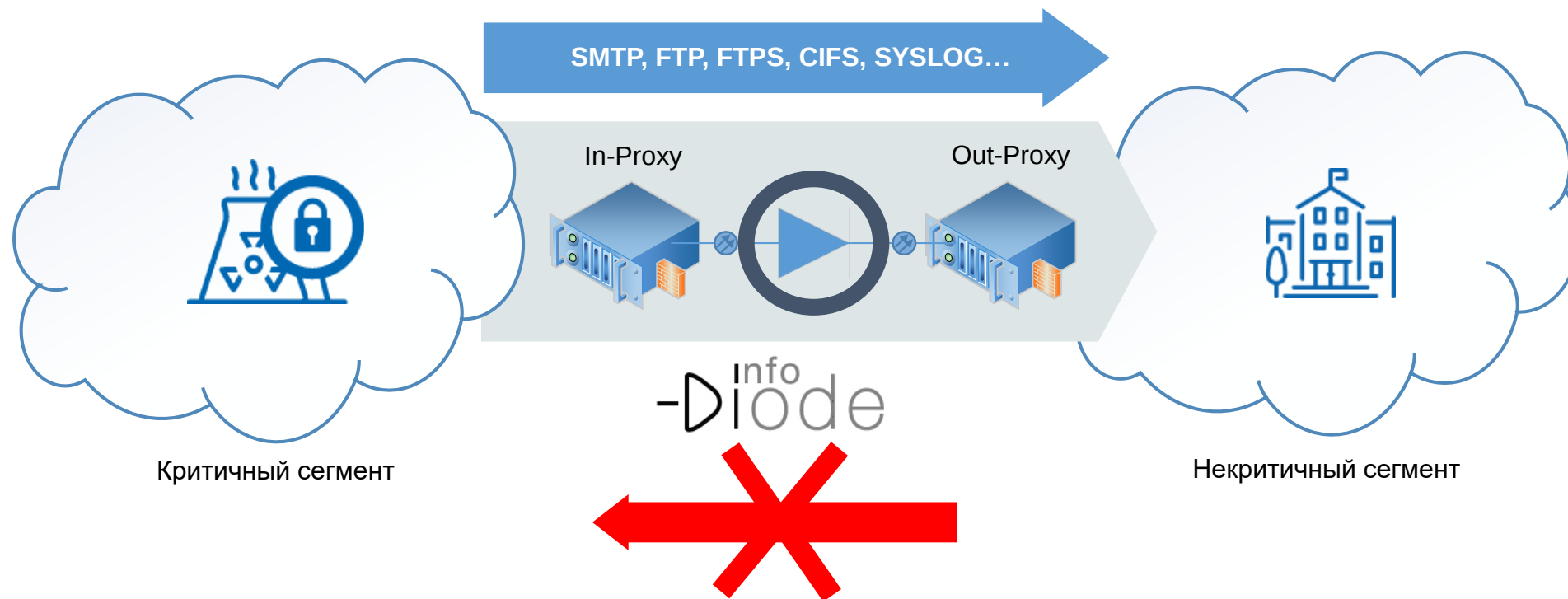
Этапы проектов с применением устройств класса диод (на примере АПК InfoDiode)

Сценарий 1 - Однонаправленная загрузка данных в защищаемую информационную систему



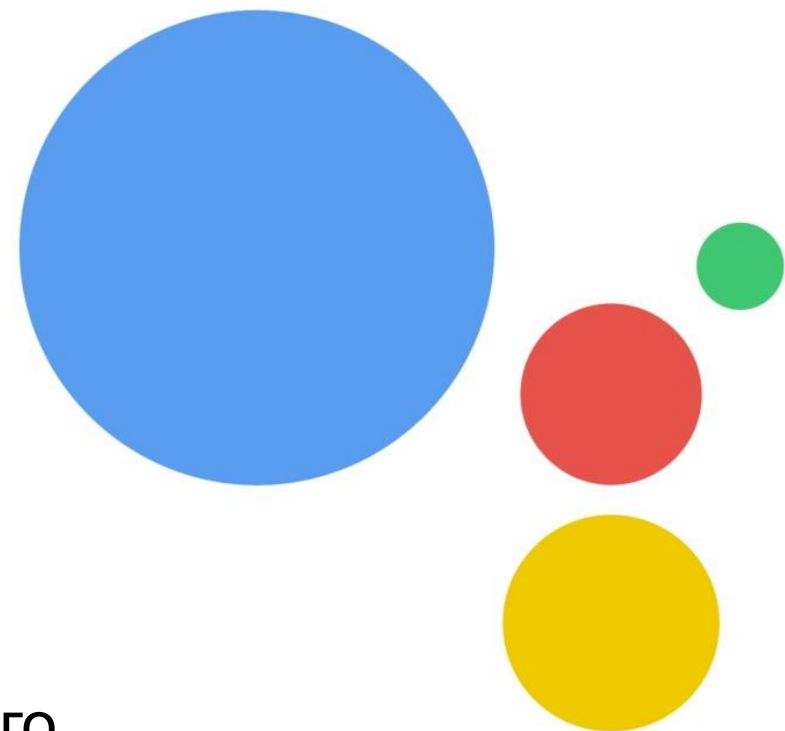
- **Загрузка** данных в конфиденциальные информационные системы
- **Нельзя, чтобы данные «утекли»** из крит. информационных систем
- Нужно исключить возможность управления объектом

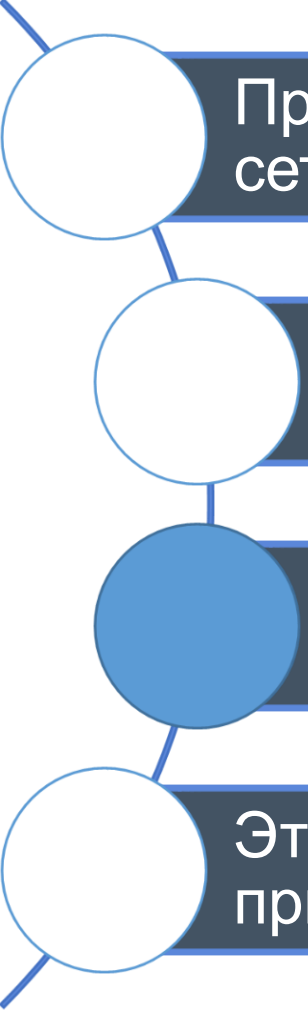
Сценарий 2 - Однонаправленная выгрузка данных из критичного технологического сегмента



- **Выгрузка** данных из критичных сегментов
- Нужно исключить **информационные воздействия извне**
- Нужно исключить возможность управления объектом

- Поддержка протоколов FTP\FTPS, CIFS, SMTP и др.
- Приоритезация передачи данных и потоков
- Помехоустойчивое кодирование
- Configuration/system backup
- Syslog/SIEM интеграция
- NTP синхронизация
- Интеграция с AD
- Формирование файла мета-информации для его анализа средствами DLP (чтение), Syslog аудит
- SNMP v2c и v3, syslog





Предпосылки применения устройств класса диод для сегментации сетей

Типовые решаемые задачи (на примере АПК InfoDiode)

Особенности, ограничения, нюансы применения устройств класса диод

Этапы проектов с применением устройств класса диод (на примере АПК InfoDiode)

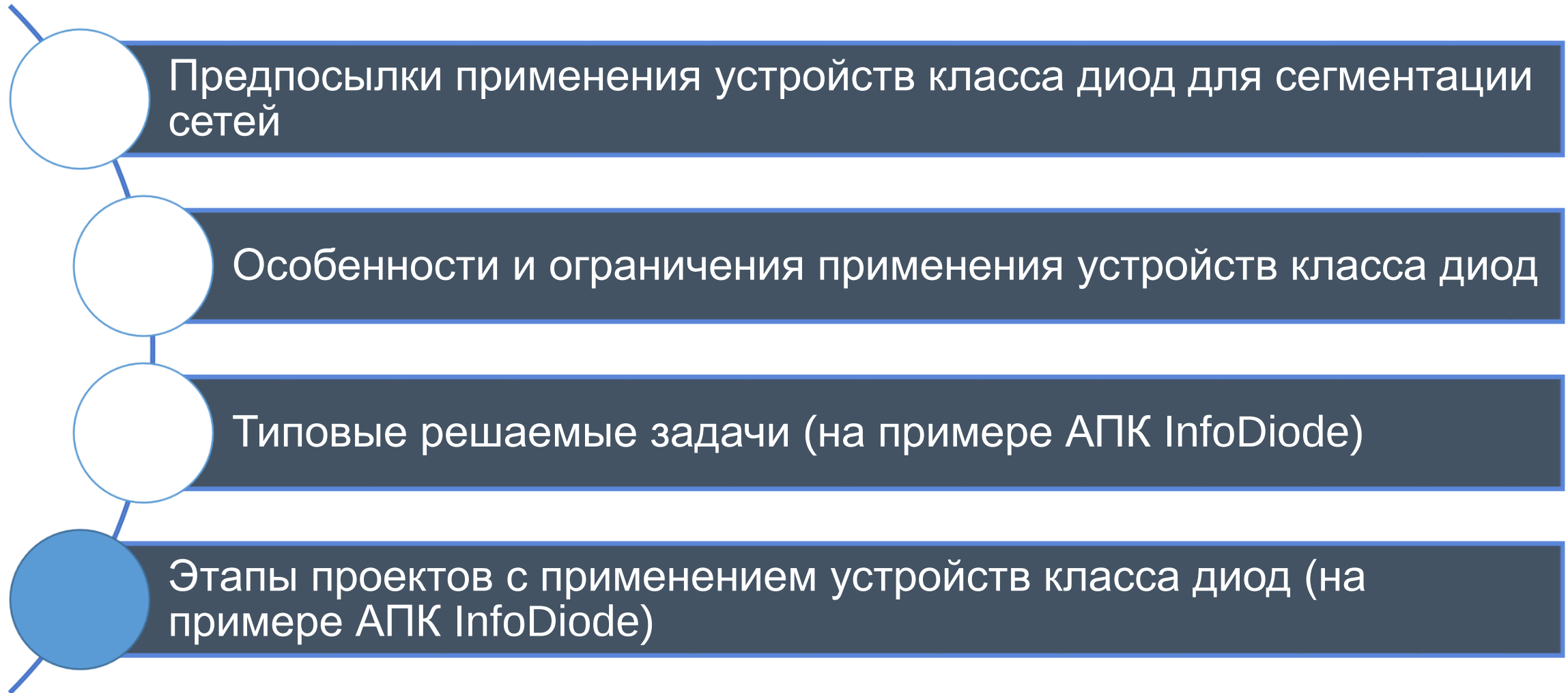
«Спорные практики»

- ☐ Диод «для галочки»
- ☐ Ожидание - диод будет работать также как маршрутизатор (пропускать весь TCP/IP трафик)
- ☐ Ожидание - можно поставить в любом месте без предварительного проектирования и таким образом решить проблему безопасности



- ☐ Начинать с модели угроз
- ☐ Анализ прежде всего информационных потоков, а не физических элементов сети
- ☐ Может потребоваться физическое перепроектирование сети
- ☐ Добиться единственного места сопряжения сетей – через диод, в остальных местах воздушный зазор
- ☐ Мы рекомендуем не ставить диод без необходимости внутрь ТСПД
- ☐ В такого класса устройствах важен аспект импортозамещения, наличия сертификации
- ☐ Диод – это не так страшно





- Презентация\демонстрация\вебинар, предоставление необходимых документов по продукту
- Консультации по всем техническим вопросам
- Документ-опросник с целью собрать первичные требования
- Пилот, тестирование интеграции с существующими системами, помощь в подготовке протоколов, защита решения внутри компании
- Помощь в формировании и защите бюджета, подготовка ТЭО
- Подготовка технических требований, ТЗ, подготовка конкурса
- Проведение инструктажа для сотрудников
- Помощь в разработке эксплуатационных документов
- Консультации по вопросам защиты данных и организации мероприятий ИБ

-Diode^{info}

- 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!