



Однонаправленная
передача данных

Защита
объектов КИИ и ОПО

Экспорт
видеопотоков в
ситуационный
центр

Сегментирование
сетей АСУ ТП

-InfoDiode

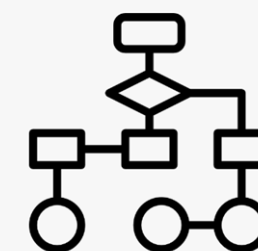
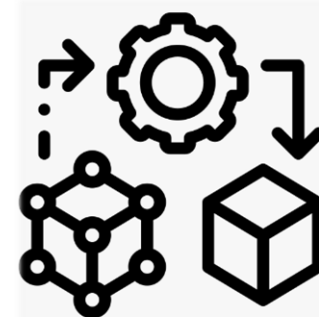
КТ

17.10.2024

Функции и направления развития решений InfoDiode в сетях с воздушным зазором. Развитие "дата диодов" как междоменных решений

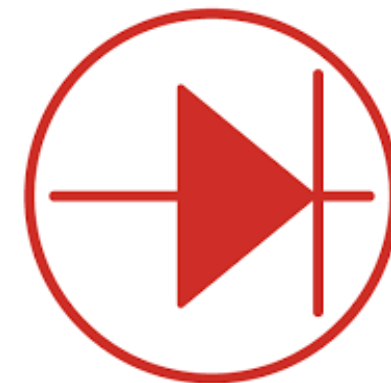
Половинко Вячеслав (АМТ-ГРУП)

1. InfoDiode – это еще один МСЭ?
2. «Приходил вендор, который сказал, что есть решение - «диод данных». Если очень нужно - его можно включить в двунаправленный режим». Это тоже «диод»?
3. Какой класс атак существует на решения класса «диод данных», если в нем реализована функция безопасности «на уровне физики»?
4. Как InfoDiode может передавать двунаправленные протоколы, если связь симплексная?

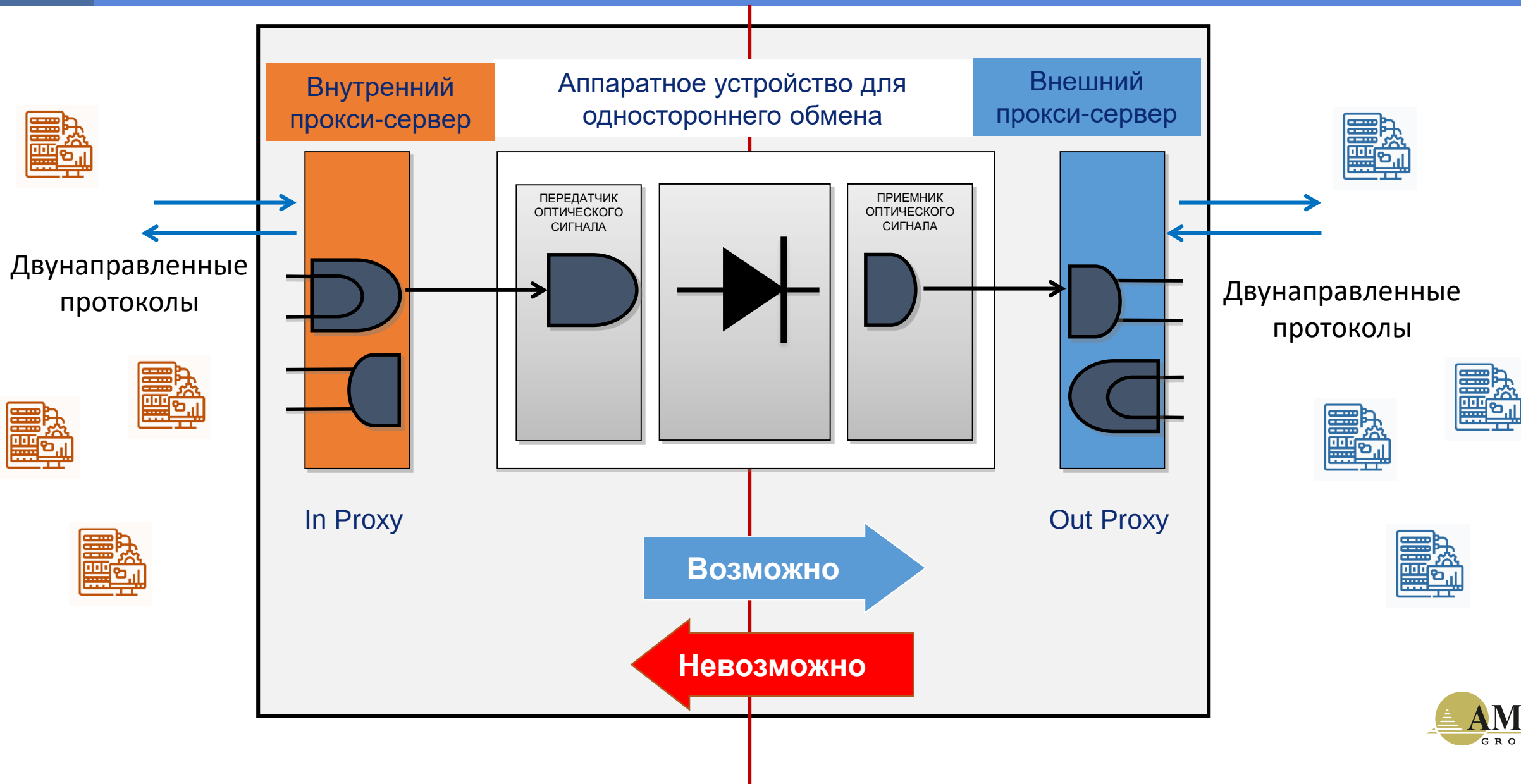


- **Ключевые признаки**

- Однонаправленность и воздушный зазор гарантируются физическим принципом – НЕ программным
- «Диоды» в двунаправленный режим НЕ переключаются
- Просто открыть порты, настроить ACL в «диодах и «обмен пойдет» - НЕЛЬЗЯ
- «Диоды» с ПО тоже нужно обновлять
- Современные решения этого класса позволяют передавать данные практически всех видов протоколов



InfoDiode передает данные двунаправленных протоколов, завершая сами протоколы, и выполняя разрыв протокола между левой и правой частями InfoDiode



«Диоды данных» эволюционируют как и вся экосистема СЗИ

Аппаратные «диоды»

- Недорого
- Решают базовые задачи изоляции, применяются в основном в COB/IDS
- Plug&Play, не требуют сопровождения службы эксплуатации
- Не передают данные двунаправленных протоколов



Аппаратно-программные «диоды»

- Решают задачу передачи протоколов прикладного уровня, в том числе промышленных протоколов, передают несколько видов трафика одновременно
- Доп функции СЗИ (NAT, white list/порты, контроль изменений конфигурации, контроль доступа, ввод в домен)
- Возможности по контролю за функционированием: SNMP, Syslog, NTP...



Междоменные решения

- Регламентируют обмен и дополняют «традиционные диоды» функциями и решениями по контролю прикладного трафика
- Более комплексный подход к защите периметра организации
- Интегрируются с другими СЗИ в целях повышения эффективности контроля периметра



В основе обмена
всегда лежит принцип

**физический сигнал
только в одну сторону**

Междоменные решения – это ответ на ряд новых вызовов при обмене информацией между сетями разного уровня доверия

- 1. Увеличение интенсивности обмена** в рамках производственных циклов, обмена данными с контрагентами и органами власти
- 2. Возможность утечки данных по тем же каналам**, которые используются для сопряжения доменов, систем
- 3. Компрометация вендоров** (в том числе СЗИ) для организации атаки, использование обновлений ПО, патчей в качестве инструмента атаки
- 4. Рост количества атак на ИТ-ресурсы топ-менеджеров, руководства**, в том числе в целях использования в качестве «плацдарма» для развития атаки



Домен – логически объединенная совокупность организационно-технических активов и ресурсов, подчиняющихся единой политике безопасности

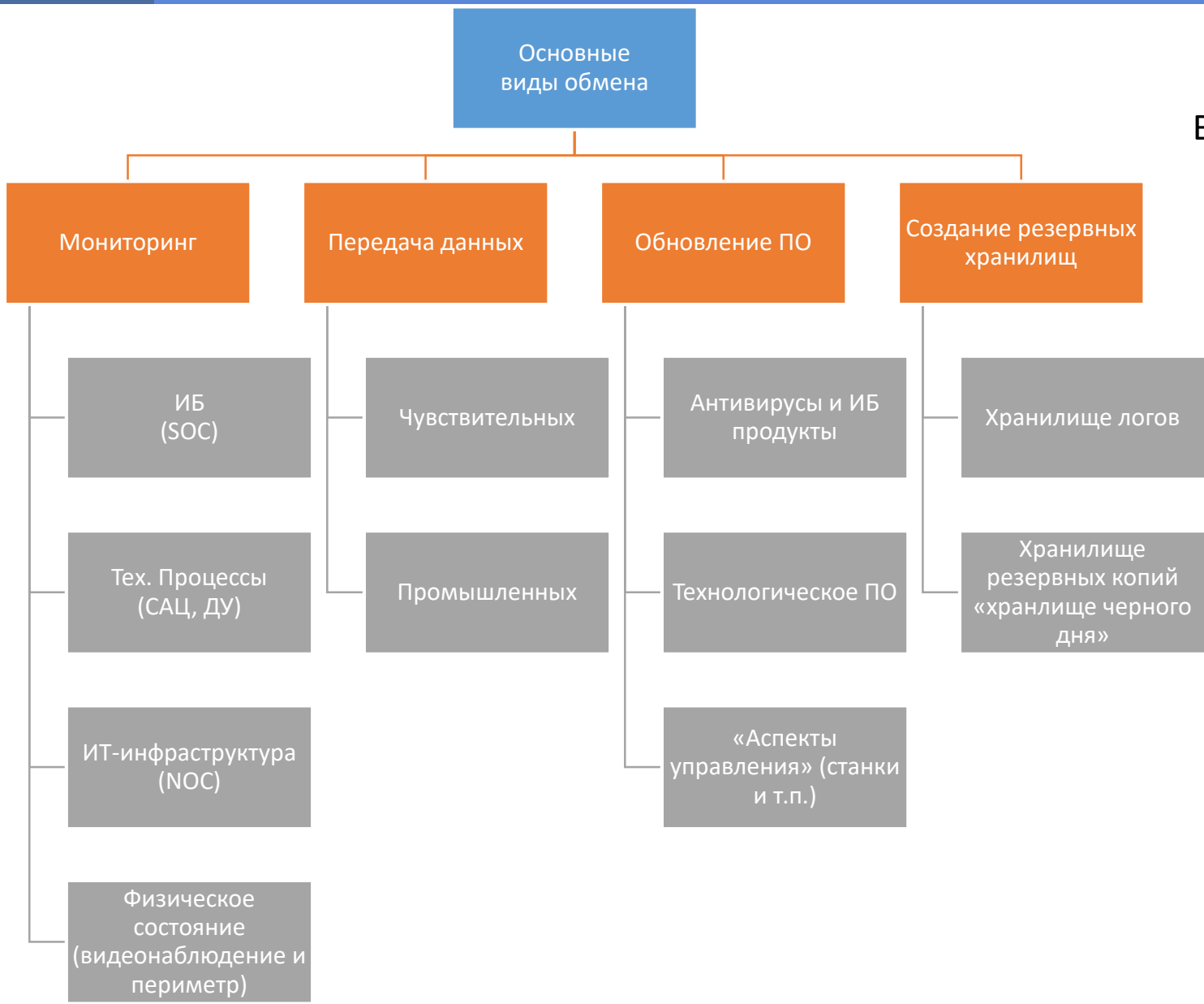
Домен содержит данные, информационные системы и сети определенных классов, категорий безопасности, которые сегментированы, в том числе, в зависимости от возможностей передачи информации. Для некоторых доменов требуется установление большей степени доверия, тогда как для других - меньшей



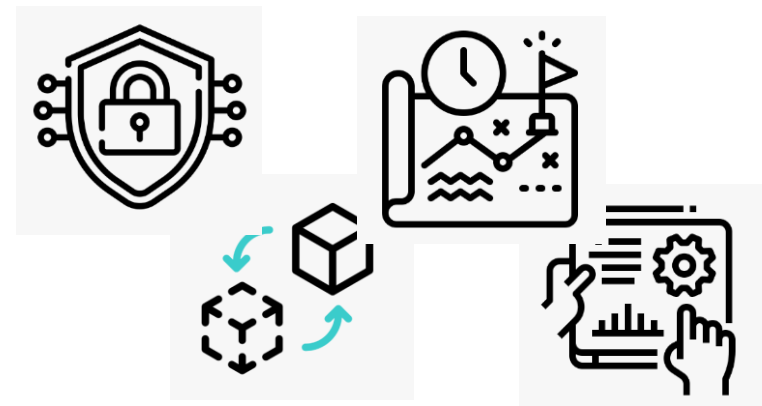
- ☐ **Более доверенная сеть (в ряде случаев сеть/система-источник)** - область, формирующая наибольшие риски в отношении утраты, компрометации, нарушения характеристик обрабатываемой информации, систем, сегментов, данных, процессов
- ☐ **Менее доверенная сеть (недоверенная сеть, в ряде случаев сеть/система-приемник)** - область, формирующая наибольшие риски в части вероятности организации атак из нее на иные сегменты и сети
- ☐ **Периметр** - граница доверенной сети, на которой выполняется аутентификация запросов, регулируются информационные потоки, применяются организационно-технические меры для снижения рисков в отношении информации, сетей, данных, процессов

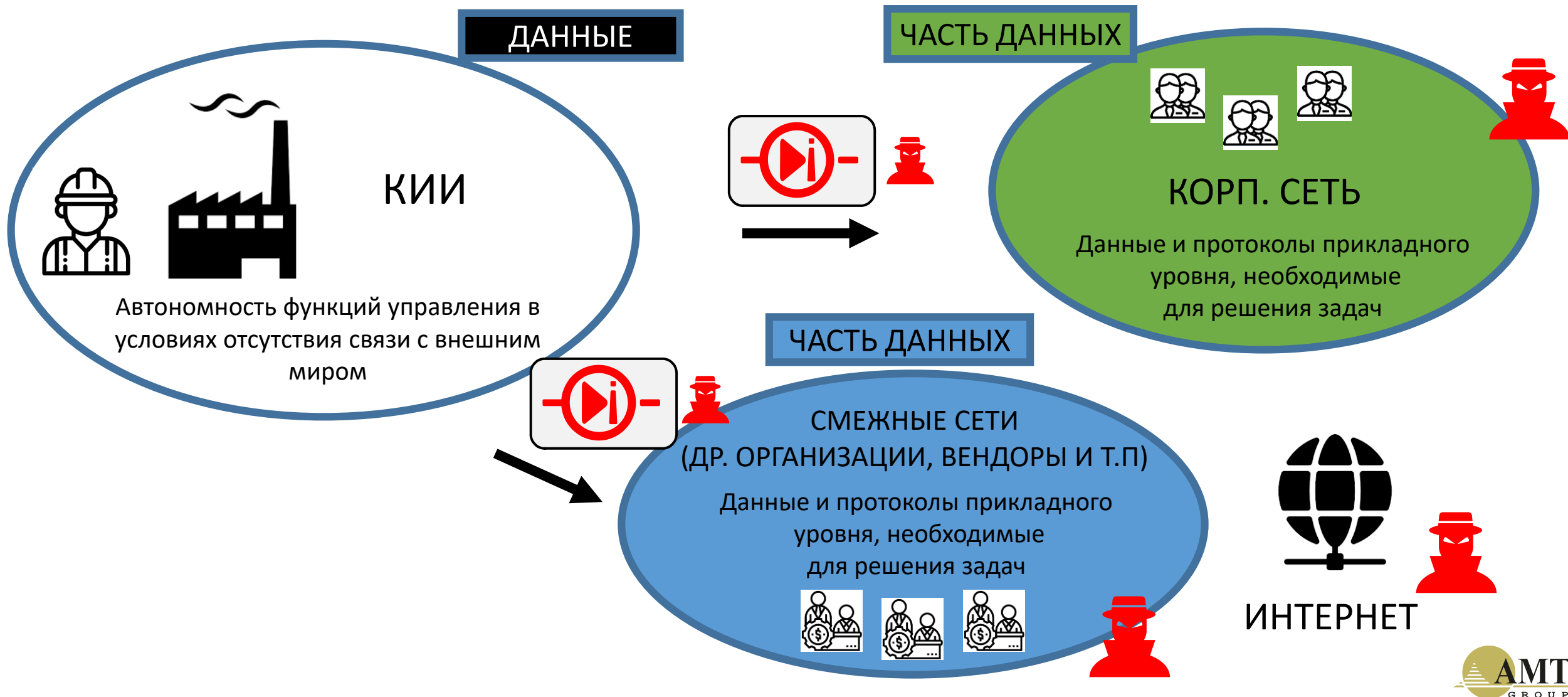
Отношения между доменами описываются в организационно-распорядительных документах (политиках безопасности)

Для чего мы сопрягаем Домены с разным уровнем доверия?



В указанных видах обменов **принципиально (!) исключено удаленное администрирование и управление защищаемыми объектами из менее доверенного сегмента**





Междоменные решения фокусируются только на части обменов с воздушным зазором

Основные виды обмена

Мониторинг

ИБ (SOC)

Тех. Процессы (САЦ, ДУ)

ИТ-инфраструктура (NOC)

Физическое состояние (видеонаблюдение и периметр)

Передача данных

Чувствительных

Промышленных

Обновление ПО

Антивирусы и ИБ продукты

Технологическое ПО

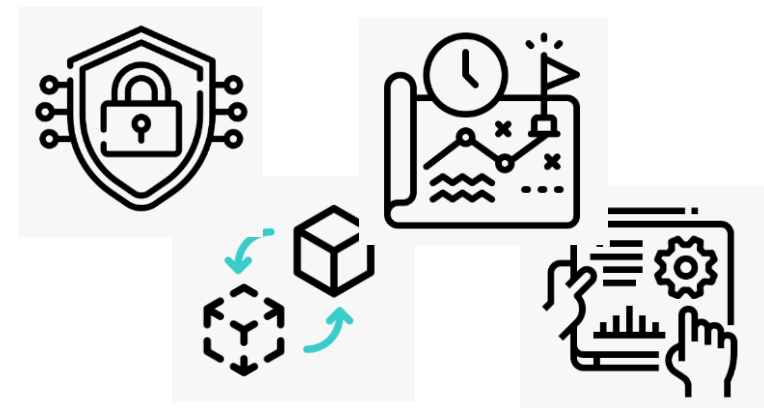
«Аспекты управления» (станки и т.п.)

Создание резервных хранилищ

Хранилище логов

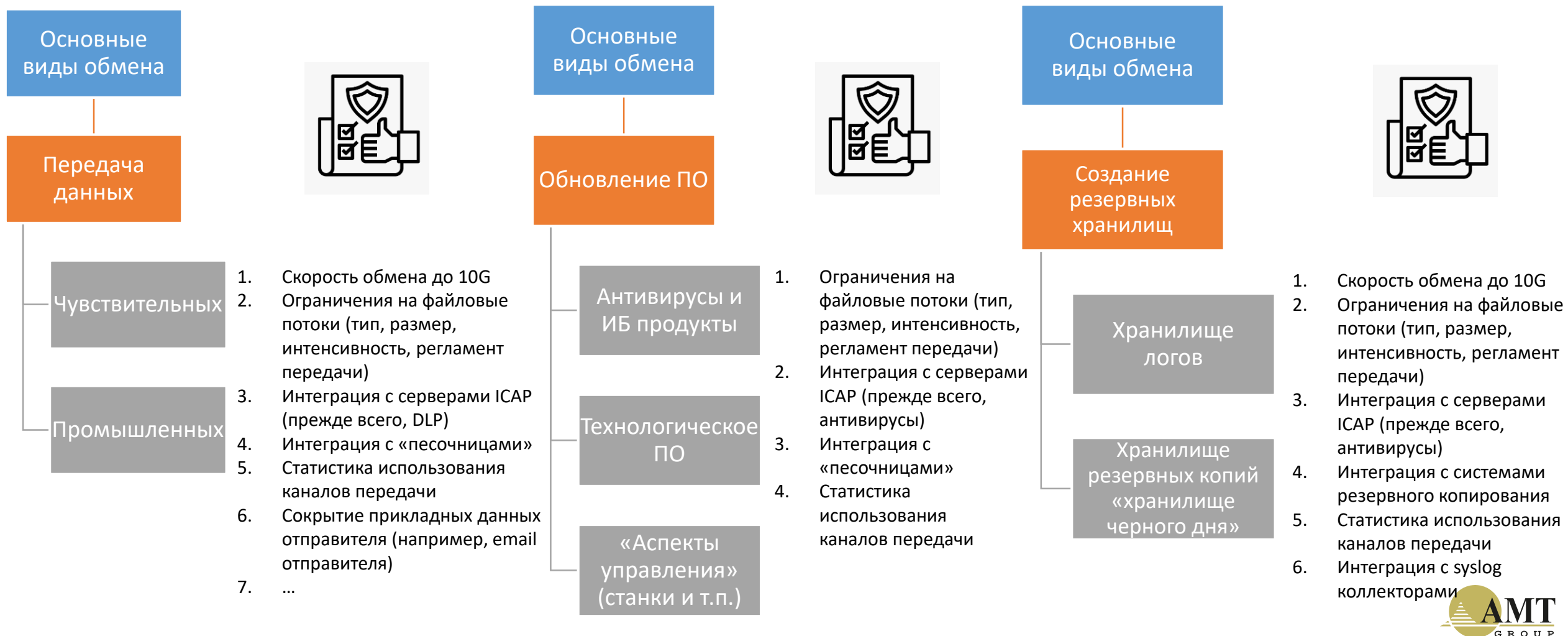
Хранилище резервных копий «хранилище черного дня»

В указанных видах обменов **принципиально (!) исключено удаленное администрирование и управление защищаемыми объектами из менее доверенного сегмента**



На данном этапе междоменные решения развиваются преимущественно в этих направлениях

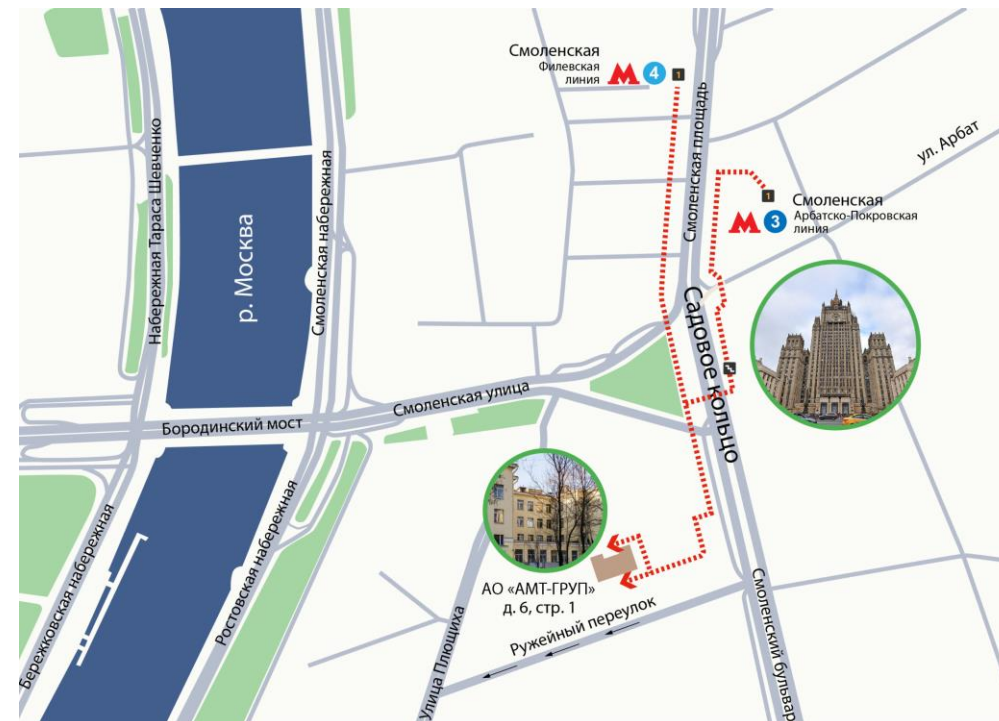
Планируемые функции междоменных решений InfoDiode



- ☐ **Повышение скорости канала передачи – до 10G**
- ☐ **Ограничения на файловые потоки
(тип, размер, интенсивность, регламент передачи)**
- ☐ **Статистика использования каналов передачи**
- ☐ **Интеграция с серверами ICAP
(DLP, антивирусы, «песочницы»)**
- ☐ **Интеграция с системами резервного копирования**



- Адрес: 119121, Россия, Москва, Ружейный переулок, 6с1
- 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!