



Однонаправленная
передача данных

info
-Diode

Защита
объектов КИИ

Экспорт
видеопотоков в
ситуационный
центр

Сегментирование
сетей АСУ ТП

IT

10.02.2023

АМТ-ГРУП

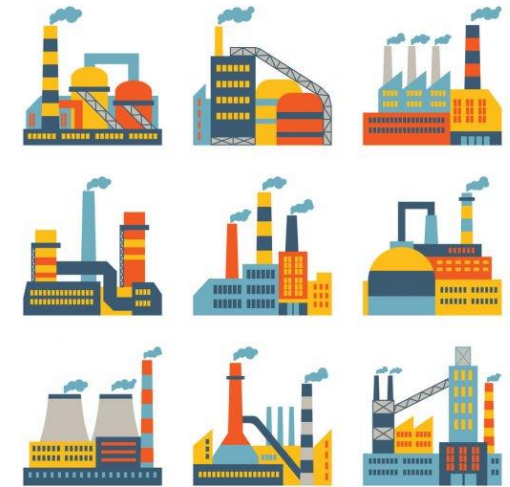
Практические решения по защите АСУ ТП с использованием решений класса «диод». Вопросы совместимости СЗИ и решений АСУ ТП.

Предпосылки
применения
диодов

Как
сегментировать
сетевой
периметр
пром. объекта

С чем уже
совместим
InfoDiode

1. Риски для КИИ растут и увеличиваются (год от года риски для КИИ растут)
 1. <https://www.comnews.ru/content/215455/2021-07-14/2021-w28/rossiyskie-obekty-kii-podverglis-usilennym-atakam>)
 2. <https://cisoclub.ru/v-rossii-rastyot-kolichestvo-kiberatak-na-sistemy-gosudarstvennogo-upravleniya-i-obekty-kii/>
 3. <https://www.vedomosti.ru/technology/articles/2023/01/16/959104-hakeri-atakovali-gosorgani-chasche%20>
2. Нормативная база делает акцент на защиту КИИ. **Регулятор менее лояльно относится к сдвигу сроков реализации мер защиты. 166 Указ Президента. Постановление правительства 1478**
3. Зарубежные вендоры СЗИ уходят/ушли/(запрещены для внедрения) с рынка (Fortigate, Infoblox, Cisco, IBM и др.), **Сетевой периметр стал менее защищен. Сертификаты ФСТЭК отозваны**
4. Российские вендоры не всегда могут предложить законченные решения. Например, промышленные **межсетевые экраны** или комплексные решения по безопасности. **Выбор отечественных СЗИ пока ограничен.**
5. Поставка и поддержка программно-аппаратных и аппаратных решений в сегменте АСУ ТП ограничены, в ряде случаев невозможна. (Siemens, GE, Honeywell, Bently Nevada и др.). **Данные, по-прежнему, нужны за пределами технол. сегмента**



Инфраструктура СЗИ по некоторым направлениям строится фактически с нуля

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



1. Длительный сценарий подготовки

6 месяцев и более

2. Использование двунаправленного канала

Узнать топологию сети, сканировать инфраструктуру

3. Использование известных уязвимостей

ПО в технологическом сегменте

4. Использование известных уязвимостей СЗИ

прежде всего программных

5. Прямая или косвенная «помощь вендоров»

«Коллекции бэкдоров»



Как сегментировать сетевой периметр



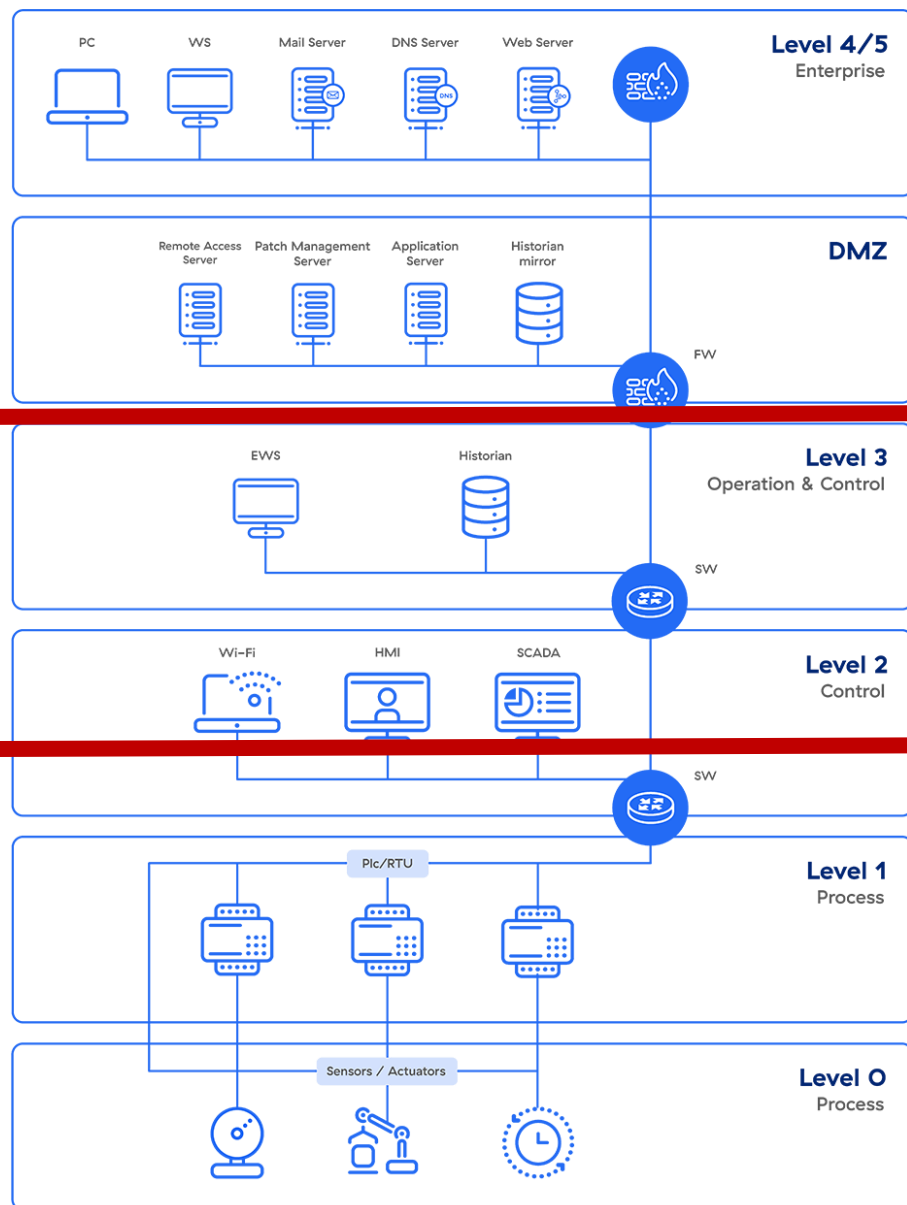
АСУ ТП трактуется как **группа решений технических и программных средств, предназначенных для автоматизации управления технологическим процессом**

В реальности АСУ ТП имеет интеграционные связи:

- Системами мониторинга
- Контроллерами домена
- Системами резервного копирования
- Более общей автоматизированной системой управления предприятием
- Внешними потребителями – контрагентами, подрядчиками, центрами мониторинга, центрами безопасности, ситуационными центрами, центрами принятия решений и т.п.



Предпосылки сегментации АСУ ТП лежат уже в модели Purdue

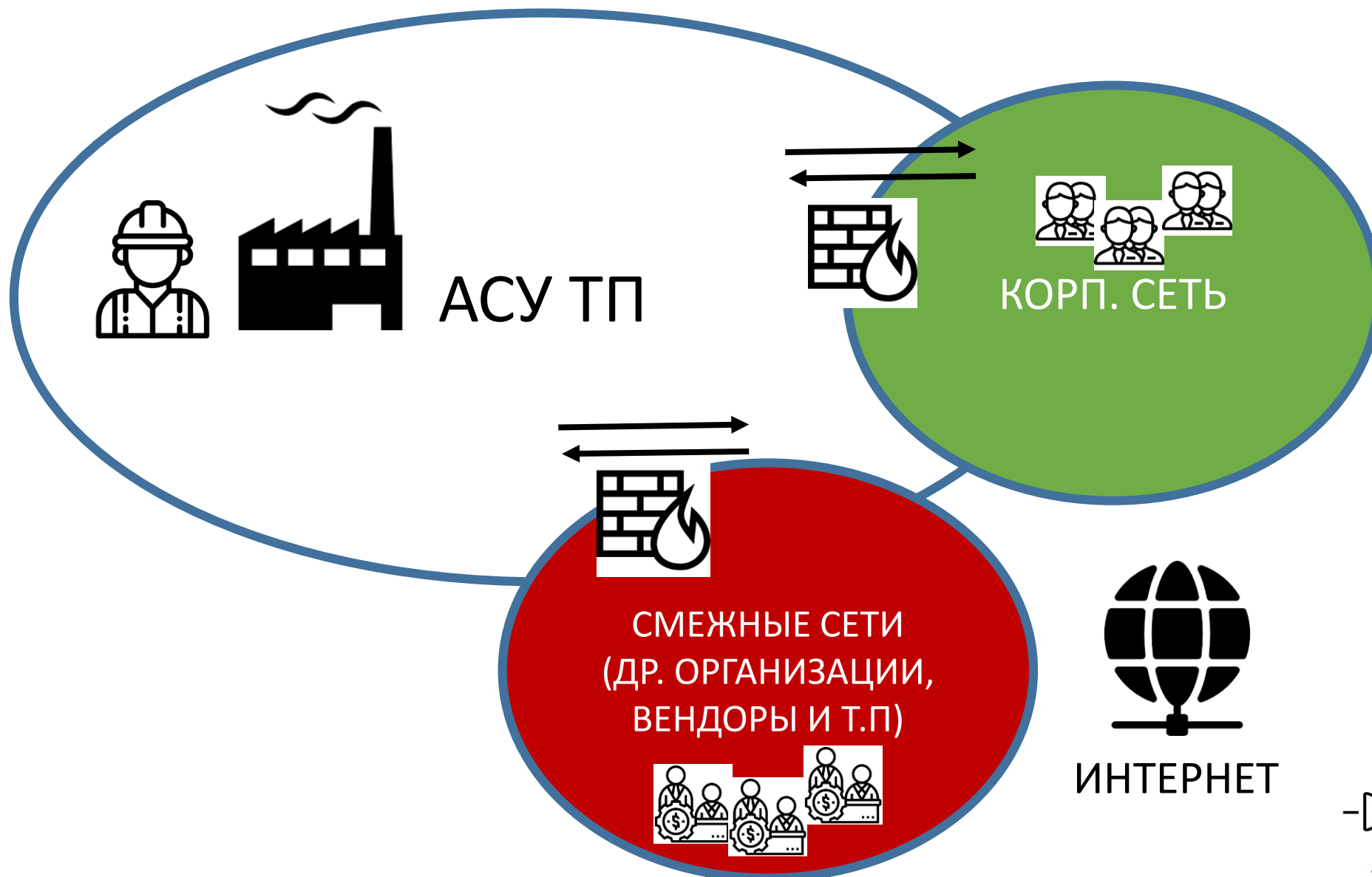


BI, ERP, MES

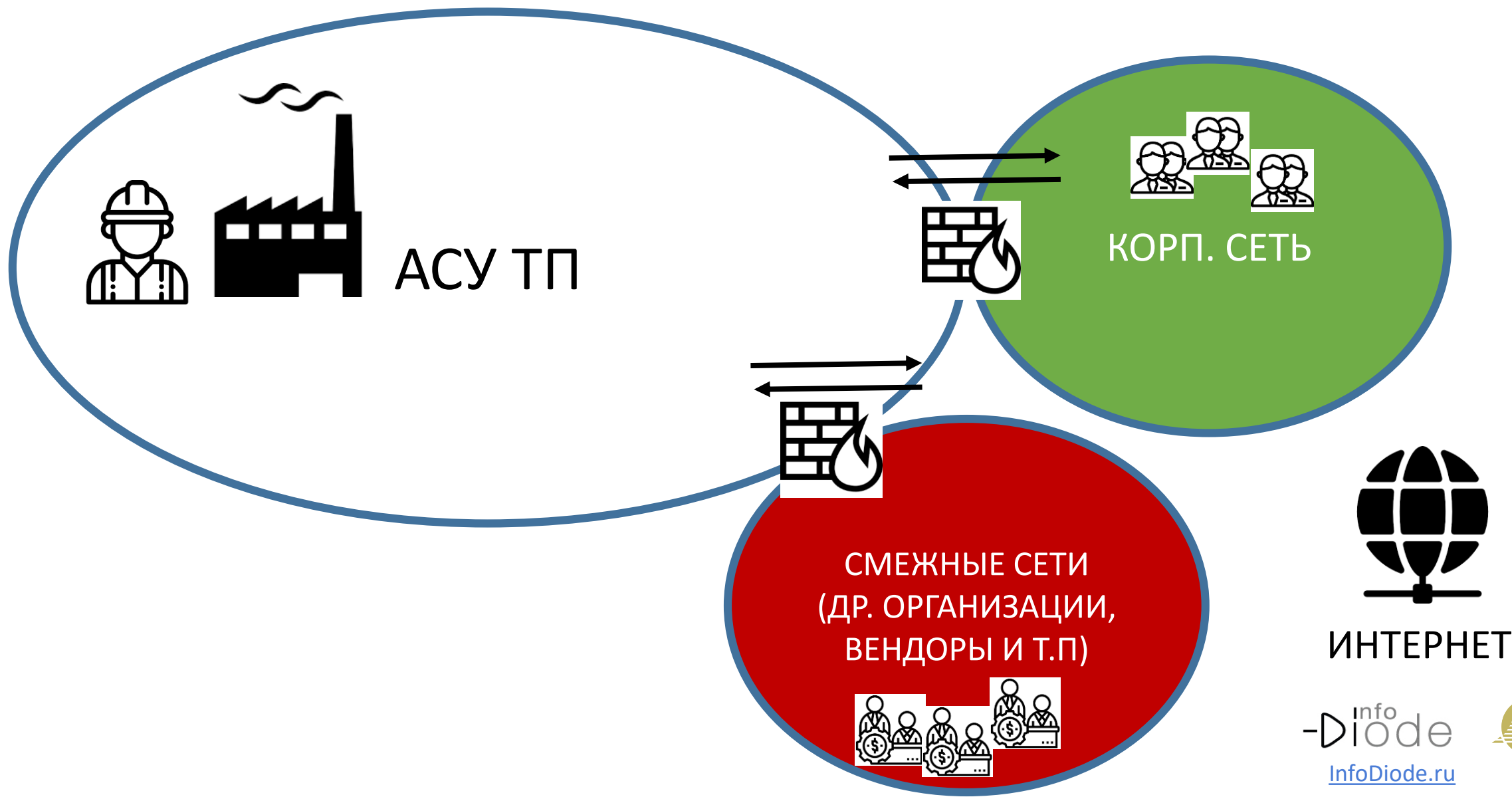
АСУ ТП

КИП

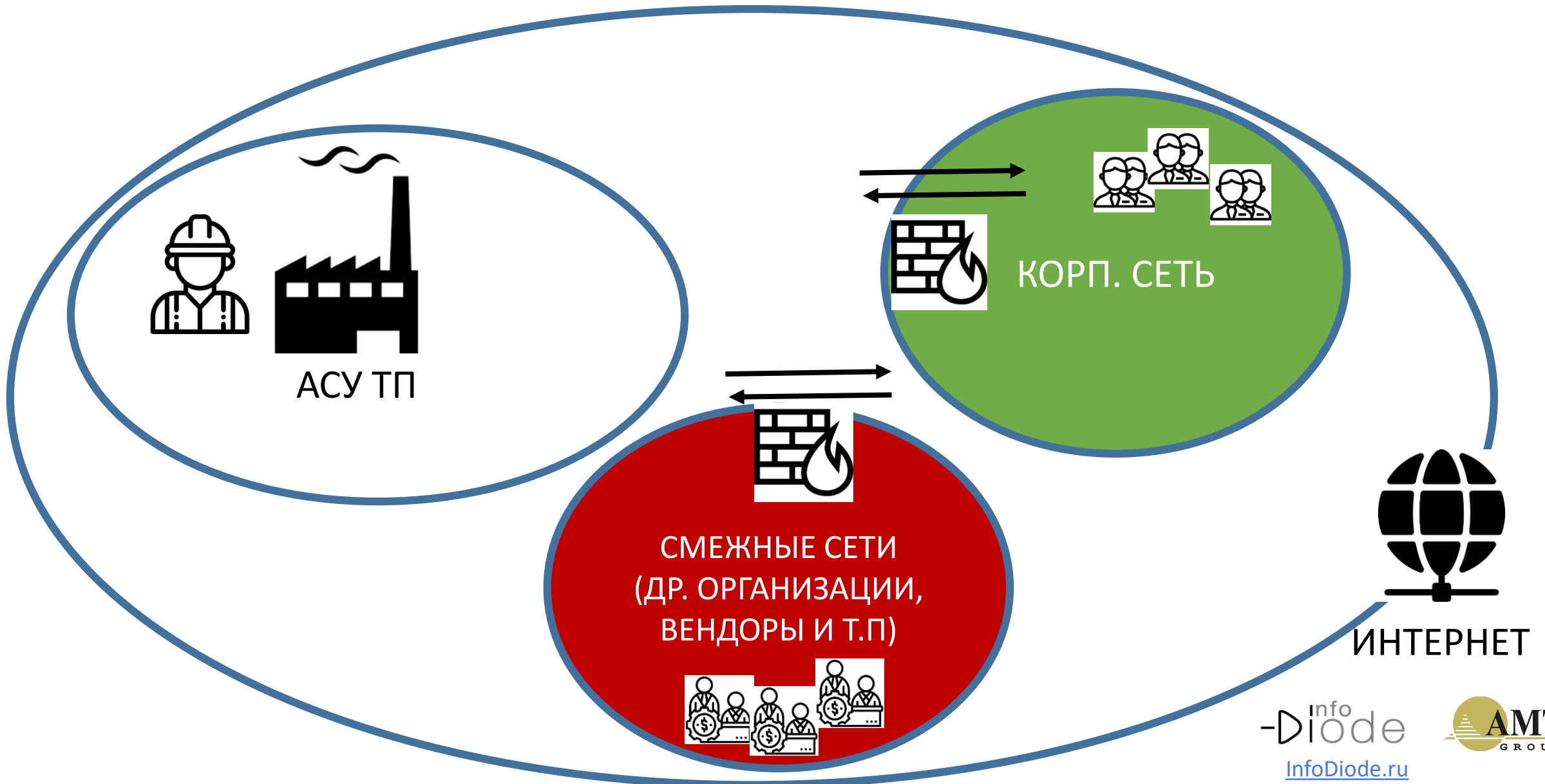
Взгляд со стороны специалиста АСУ ТП тяготеет к расширению границ АСУ ТП



Взгляд со стороны специалиста ИБ тяготеет к изоляции АСУ ТП в существующих границах



Взгляд со стороны ИТ специалиста нацелен на поддержание целостности, удобства администрирования и надежность сети, а не на ее сегментацию

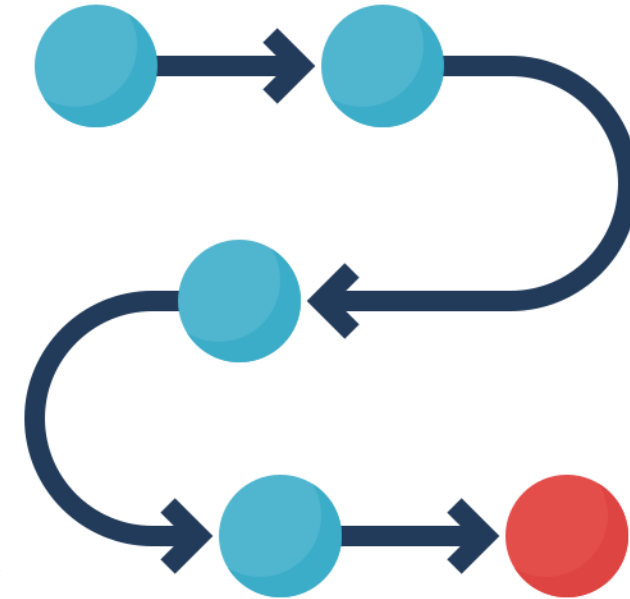


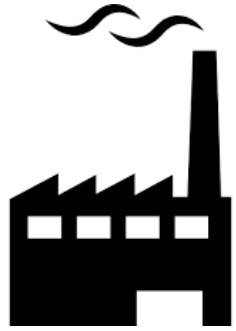
Корректный подход к сегментации сети - локализация функций управления в рамках одного физически изолированного сетевого сегмента



Последовательные шаги помогут более четко сегментировать сеть АСУ ТП

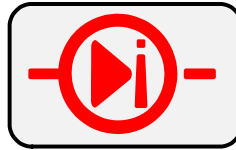
1. **Определить, где именно (программно) сосредоточены функции управления технологическим процессом** (старт/остановка, реализация кризисных мер в отношении технологического процесса).
2. **Определить, где проходит граница физической изоляции сети АСУ ТП.** Граница должна быть выбрана таким образом, чтобы объект оставался автономным и безопасно функционирующим в условиях отсутствия связи с внешним миром.
3. **Определить перечень информации прикладного уровня (промышленные, файловые, технологические протоколы), используемой внешними по отношению к АСУ ТП потребителями.**
4. **Убедиться, что в условиях пп. 1, 2 и 3 функционирование АСУ ТП происходит надежно и безопасно.** Пп. 1–4 могут быть выполнены без приобретения и применения дополнительных средств и мер защиты и завершаться организацией воздушного зазора между защищаемым объектом/АСУ ТП и иными доменами.
5. **Применить средства защиты соответствующего класса, обеспечивающие передачу данных потребителям без потери автономности объекта защиты.**





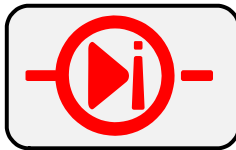
АСУ ТП

1. Автономность функций управления
2. Автономность в условиях отсутствия связи с внешним миром



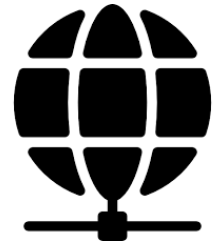
КОРП. СЕТЬ

1. Требуемые данные и протоколы прикладного уровня
2. Достаточность информации для решения задач



СМЕЖНЫЕ СЕТИ (ДР. ОРГАНИЗАЦИИ, ВЕНДОРЫ И Т.П)

1. Требуемые данные и протоколы прикладного уровня
2. Достаточность информации для решения задач



ИНТЕРНЕТ

- оставить нужное в АСУ ТП
- изолировать ОКИИ
- сохранить управляемость сетевой инфраструктуры

С чем уже совместим InfoDiode, какие бывают диоды





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 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, - 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

- 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!