

Межсетевой экран для промышленных сетей - баланс между защитой, доступностью и надежностью



RTT – разработчик и производитель защищенных, безопасных и доверенных сетевых решений.

Мы создаем оборудование, которое позволяет создать основу надежной и функциональной мультисервисной сети передачи данных.

Портфолио: сетевое оборудование.

- Год основания 2009
- Головной офис г. Москва
- Лицензиат ФСТЭК, ФСБ, МО РФ
- Резидент Сколково
- Аккредитованная ИТ-организация
- Входим в перечень ГИСП

15 лет работаем и создаем сетевые решения

#джиттер

#конфиденциальность

#скорость

#доступность

#шифрование

Какие факторы влияют на баланс?

#отказоустойчивость

#фильтрация

#надежность

#защита

#резервирование

#безопасность

Какие факторы влияют на баланс?



1. Производительность и пропускная способность
2. Уровень безопасности и защита от угроз
3. Работа с промышленными протоколами
4. Надежность и отказоустойчивость
5. Автоматизация и простота управления
6. Доступность
7. Интеграция с IT- и OT-сетями
8. Экономическая выгодность (цена/качество)
9. Соответствие отраслевым стандартам
10. Масштабируемость
11. Энергопотребление
12. Поддержка со стороны производителя
13. ...
14. ...

#1 Защита

Число процессов, направленных на обеспечение защиты, должно быть рационально обоснованным, а их внедрение тщательно проанализированным и структурированным.

А что нужно для защиты
промышленной сети?

А что нужно для защиты
промышленной сети?

ОТВЕТ:

**применение промышленных средств
сетевой безопасности**

Аспекты нормативной базы и сертификации

Законодательство

- Федеральный закон № 187
- Приказ ФСТЭК № 239
- Приказ ФСТЭК № 235
- Приказ ФСТЭК № 31

Меры

ИАФ.2
ЗИС. 2
ЗИС. 3
ЗИС. 4



Тип средств защиты информации*

Межсетевые экраны
(МЭ, FW, Industrial FW)

....

* по данным ресурса
bduasutp.fstec.ru

Требования по сертификации

- Государственный реестр сертифицированных СЗИ
- Реестр РЭП (Единый реестр российской радиоэлектронной продукции)
- Реестр российского ПО

Отраслевые требования

Требования к функционалу оборудования

- аппаратная часть
- программная часть

Применение сертифицированных СЗИ

Типизация межсетевых экранов

- А - уровня сети
- Б - уровня логических границ сети
- В - уровня узла
- Г - уровня веб-сервера
- Д - уровня промышленной сети



отличия тип Д от тип А

Идентификатор компонента требований	Название компонента требований
FAU_ARP.1	Сигналы нарушения безопасности
FAU_GEN.1	Генерация данных аудита
FAU_SAR.1	Просмотр аудита
FAU_SAR.3	Выборочный просмотр аудита
FAU_SEL.1	Избирательный аудит
FIA_UAU.1	Выбор момента аутентификации
FIA_UAU.2	Аутентификация до любых действий пользователя
FIA_UID.1	Выбор момента идентификации
FIA_UID.2	Идентификация до любых действий пользователя
FDP_IFC.2	Полное управление информационными потоками
FDP_IFF.1	Простые атрибуты безопасности
FMT_MOF.1	Управление режимом выполнения функций безопасности
FMT_MTD.1	Управление данными функций безопасности
FMT_SMF.1	Спецификация функций управления
FMT_SMR.1	Роли безопасности
FMT_MSA.1	Управление атрибутами безопасности
FPT_FLS.1	Сбой с сохранением безопасного состояния
FPT_RCV.1	Ручное восстановление
FPT_RCV.2	Автоматическое восстановление
FPT_RCV.4	Восстановление функции
FPT_TST.1	Тестирование функциональных возможностей безопасности
FRU_FLT.2	Ограниченная отказоустойчивость

ТИП Д “из коробки”

МЭ типа Д – уровня промышленной сети
(ИТ.МЭ.Д4.ПЗ)

“должен обеспечивать контроль и фильтрацию промышленных протоколов передачи данных (Modbus, Profibus, CAN, HART, Industrial Ethernet и (или) иные протоколы).”

- 1 Аудит и мониторинг
(контроль событий, журналирование)
- 2 Аутентификация и идентификация
(управление доступом пользователей)
- 3 Управление информационными потоками
(основная функция межсетевого экрана)
- 4 Управление функциями безопасности
(настройка и контроль политик безопасности)
- 5 Защита от сбоев
(устойчивость системы при отказах)
- 6 Отказоустойчивость
(проверка исправности, отказоустойчивость системы)

Есть ли еще факторы?

“Скорость”

“Резервирование”

“Отказоустойчивость”

“Дополнительный функционал”

Есть ли еще факторы?

“Простота настройки”

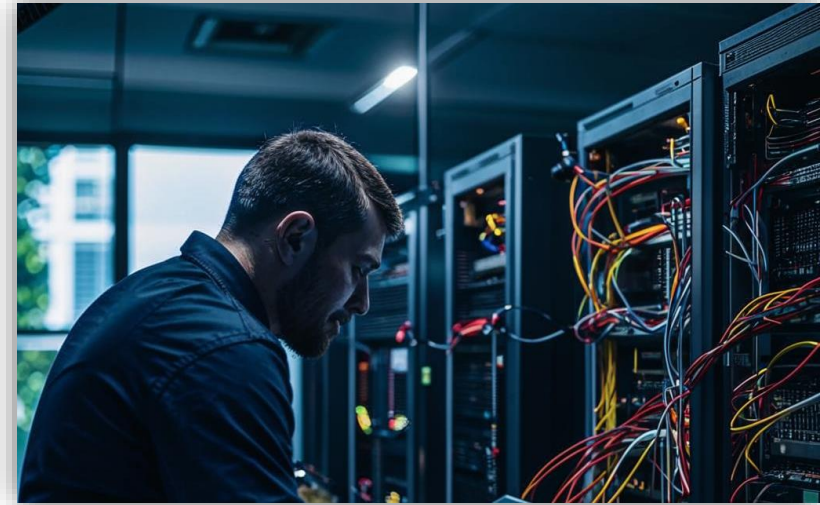
“Надежность”

“Безопасность”

“Задержки при передаче трафика”

IT и OT

- **IT (information technology)** — это технологии, которые помогают создавать, хранить, обрабатывать и передавать данные, обеспечивая поддержку бизнес-процессов, коммуникации и анализа в различных организациях и отраслях
- **OT (operation technology)** — это технологии, которые управляют, контролируют и автоматизируют физические процессы на заводах, фабриках и других объектах промышленности



OT охватывает такие технологии, как:

- Системы управления производственными процессами (например, SCADA, DCS)
- Программируемые логические контроллеры (PLC)
- Датчики и устройства сбора данных
- Системы мониторинга и контроля



Так в чем различие?

Безопасность IT

Конфиденциальность

Целостность

Доступность

Главная задача - обеспечить
конфиденциальность данных

Безопасность OT

Доступность

Целостность

Конфиденциальность

Главная задача - обеспечить
непрерывность (доступность)
технологического процесса

2 Доступность

Доступность (availability) в ОТ-сетях означает постоянную и бесперебойную работу систем и оборудования.

Доступность (пример)

ИТ.МЭ.Д4.ПЗ

Выбор момента
идентификации **FIA_UID.1.2**

Замечание по применению: должна быть предусмотрена возможность выполнения определенных действий без прохождения процедуры идентификации с целью максимальной оперативности. Примером таких действий является переводение МЭ в состояние, **не оказывающее влияние на функционирование автоматизированной системы управления.**

Не влиять на штатный режим функционирования
(режим "пропускать всё", если оказываем негативное влияние)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК РОССИИ)

Утвержден ФСТЭК России
12 сентября 2016 г.

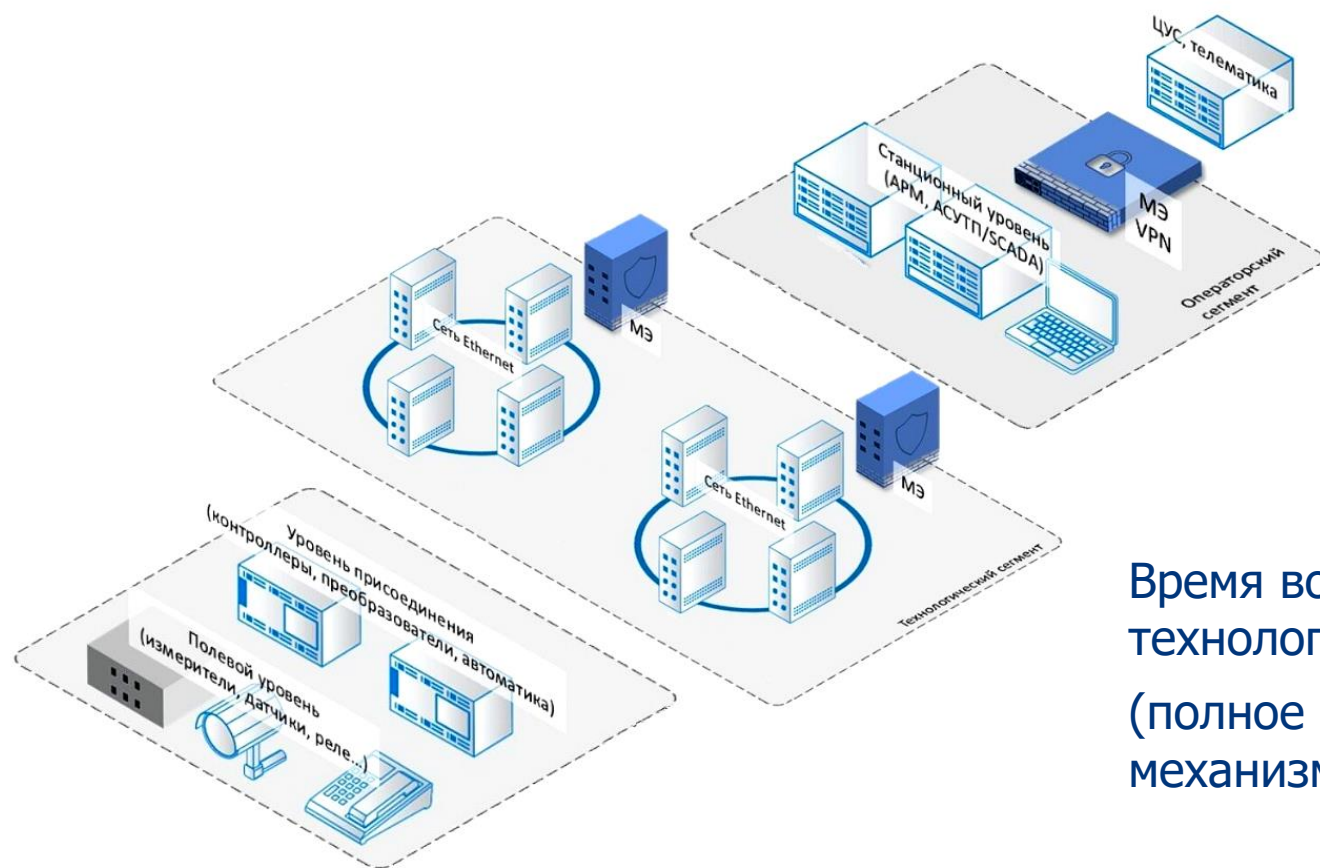
МЕТОДИЧЕСКИЙ ДОКУМЕНТ

**ПРОФИЛЬ ЗАЩИТЫ
МЕЖСЕТЕВЫХ ЭКРАНОВ ТИПА «Д»
ЧЕТВЕРТОГО КЛАССА ЗАЩИТЫ**

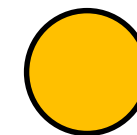
ИТ.МЭ.Д4.ПЗ

2016

Пример резервированной промышленной Ethernet-сети

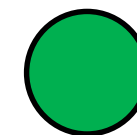


Время восстановления связи
SCADA – ПЛК ~1..5 сек.
механизмы: L3- резервирование?



Статус

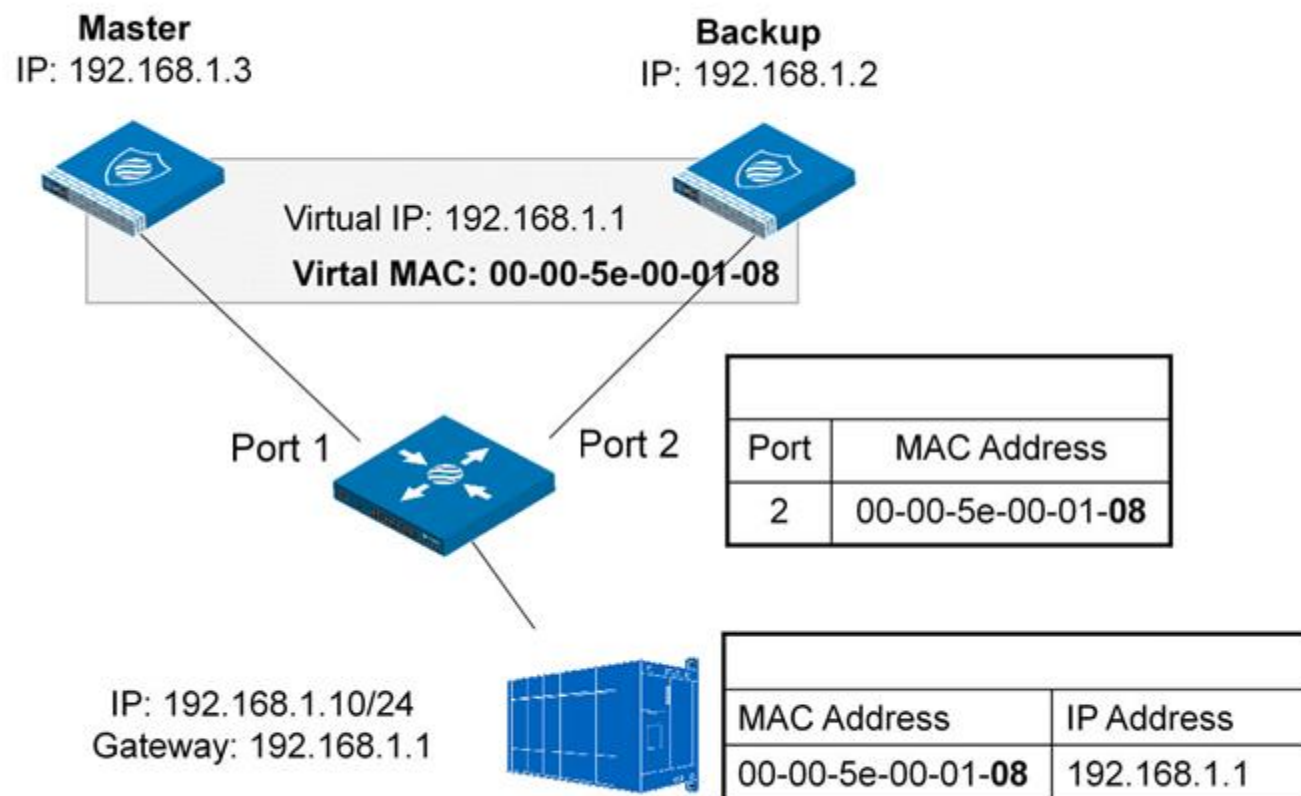
Время восстановления сети
технологического сегмента 0 мс !
(полное резервирование)
механизмы: (PRP, HSR, MRP и т.д)



Задача проста, но на практике оказывается сложной !

Кластеризация, резервирование, VRRP

- Полное резервирование устройства
- Синхронизация конфигурации
- Поддержка режима active/active,
- **Поддержка режима active/passive**
- **Синхронизация сессии**
- **Виртуальный IP и MAC**



Нет периода обновления ARP-таблиц на конечных устройствах, что позволяет организовать бесшовное резервирование

3 Надежность

Надежность (reliability) в ОТ-сетях определяется способностью системы или устройства стабильно выполнять поставленные задачи, соответствуя заданным требованиям

Дополнительные требования для обеспечения надежности

Дополнительные требования к аппаратной части:

- Пассивное охлаждение
- Расширенный диапазон температур
- Защита от перепадов напряжения
- Резервированный блок питания
- Дополнительная визуальная индикация
- Устойчивость к вибрациям и механическим воздействиям
- Электромагнитная совместимость (ЕМС)
- IP30 и выше

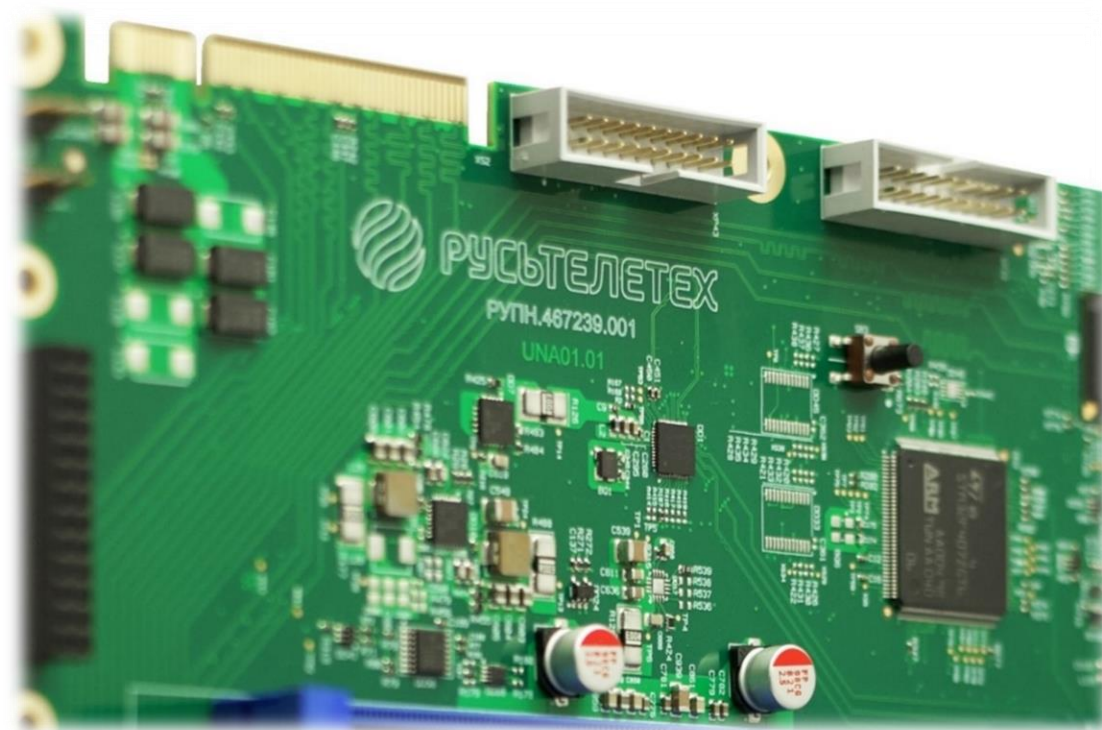
Дополнительные требования к функциональной части:

- Реализация протоколов резервирования
- Обеспечение удаленной диагностики аппаратных параметров
- Гибкость в интеграции с централизованными системами мониторинга

Универсальный промышленный шлюз безопасности RTT-M300F

Проект разработки межсетевого экрана

- Название проекта: **UTM RTT- M300**
- Старт проекта: 2020
- 3 серии изделий
- Аппаратная часть собственной разработки
- Программная часть собственной разработки
- 2022 – разработаны и выпущены межсетевые экраны
- 2023 – выпущена серия межсетевых экранов в промышленном исполнении RTT-M300F
- Сертификация ФСТЭК МЭ А4, Д4, СОВ С4, УД4*



* в работе

RTT-M300F (промышленное исполнение)



- Новый корпус IP30
- Доработана схемотехника изделия
- Реализовано полностью пассивное охлаждение (-5...+55 C) ~30 Вт
- Разработана новая система электропитания
- Доработана визуальная индикация состояния устройства
- Доработана система контроля параметров аппаратной части
- Разработана карта расширения для промышленных интерфейсов
- Повышена электромагнитная совместимость (EMC)

REFOS

СОВ

- Обнаружение аномалий в трафике
- Anti-DDOS
- Обновляемая база уязвимостей
- Визуализация найденных угроз

Сетевые функции

- Поддержка IPv4/IPv6
- xNAT (DNAT, SNAT, PAT)
- NTP/SNTP
- DHCP-сервер/клиент
- DNS-сервер
- Маршрутизация RIP, OSPF, BGP, BFD
- Профилирование трафика

Межсетевой экран

- Stateful/Stateless Firewall
- Фильтрация по гео-признаку
- Изменение политики фильтрации

AAA

- Управление группами пользователей
- Комбинированная система аутентификации по локальной БД, Radius, LDAP
- Многопользовательская аутентификация

DPI

- Инспекция протоколов (Modbus, IEC104, MQTT)
- Raw offset для своих правил
- Правила фильтрации отдельных типов сообщений

Веб-прокси

- HTTP-proxy
- Фильтрация URL
- Собственный список фильтрации URL/IP
- Проверка почтовых сообщений
- Проверка сертификатов SSL

Система и управление

- Полное управление через Web
- Подключение по SSH
- Мониторинг служб
- Работа в режиме кластера (Active/Active, Active/Passive)
- Автоматическое восстановление

Антивирус

- Работа с внешними антивирусами



Обеспечение баланса

Защита	Функционал REFOS
Доступность	Отказоустойчивость, функционал по резервированию устройства
Надежность	Промышленное исполнение RTT-M300F

Ждем Вас на стенде!

павильон 2, зал 10, стенд С 20



Вопросы?

Благодарим за внимание!

Воробьев Сергей
Менеджер по продукту
RTT
тел: +7-495-234-9-777 доб. 250
e-mail: s.vorobyev@rusteletech.ru

