Защита сетевого периметра как один из ключевых элементов комплексной системы безопасности КИИ

13.02.2024

Конференция “Комплексный подход к промышленной кибербезопасности. Защита АСУ ТП. Безопасность КИИ”

Айбек Абдыманап, исполнительный директор RTT

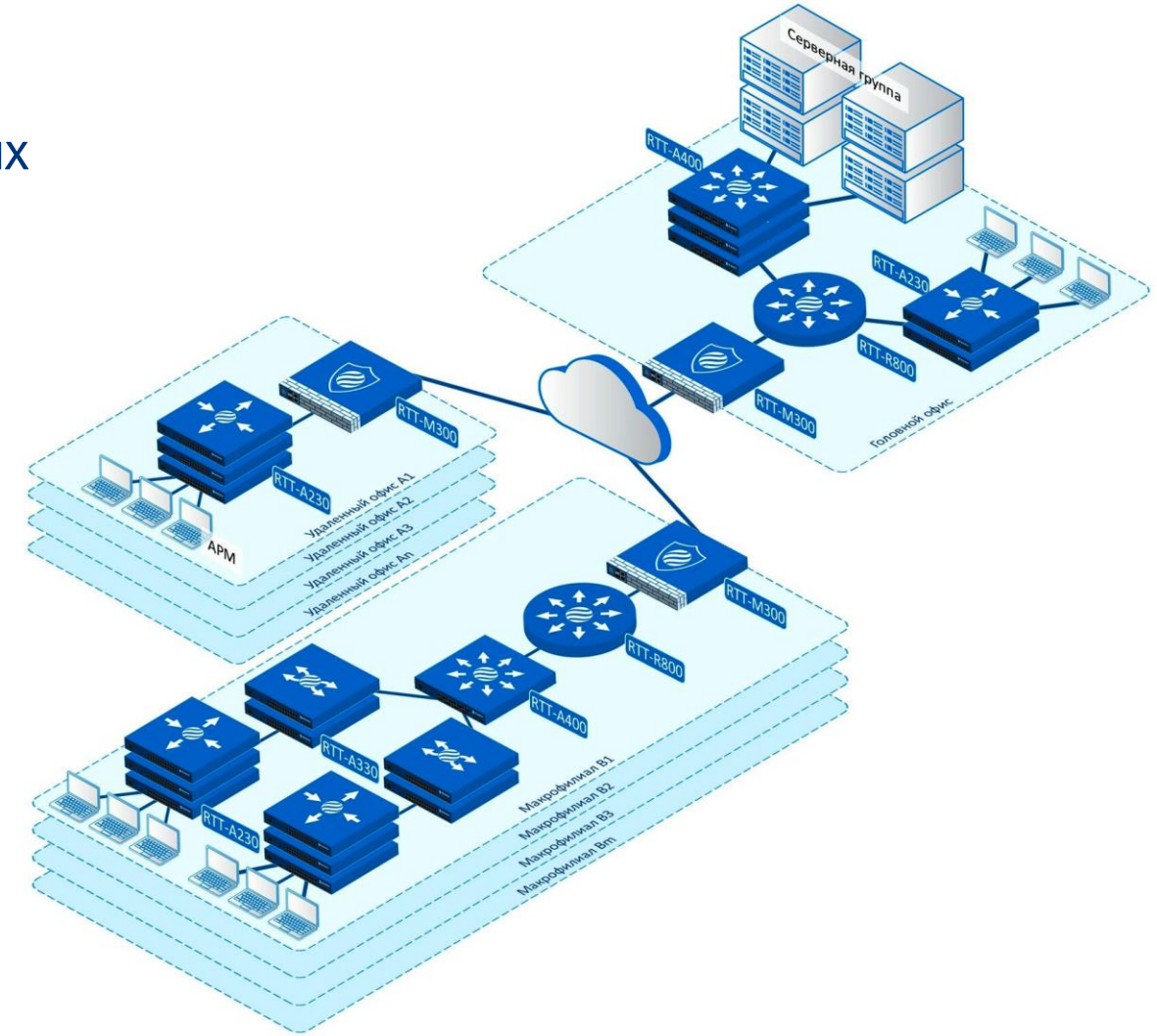
План

1. О компании
2. Зачем защищать сетевой периметр КИИ?
3. Что там защищать?
4. Как это защищать?
5. Чем это защищать?
6. Наш опыт создания «пром» МсЭ
7. Дальнейшие планы
8. Вопросы

О компании

Профиль: оборудование для создания доверенных и защищенных сетевых решений

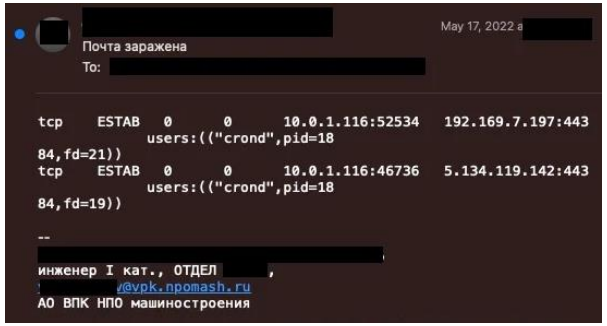
Факты:
- Работаем с 2009 г.
- Лицензиат ФСТЭК, ФСБ, МО РФ
- Резидент Сколково
- Аккредитованная ИТ-организация
- Входим в перечень ГИСП
- 6500+ единиц продукции выпущено
- 260+ довольных заказчиков



Зачем защищать сетевой периметр КИИ?

I. Затем, что атакуют

- Проникновение в сеть “НПО Машиностроения”
  07.08.2023, SentinelLABS



- Атака на систему мониторинга орошения и очистки сточных вод в Долине Иордана
  09.04.2023, Jerusalem Post

- И еще 100+ инцидентов ежегодно по всему миру

II. Затем, что технологии

Основные источники угроз АСУ в России в 2023 г.

Заражения через интернет – самый частый вектор атак на системы пром. автоматизации
Kaspersky ICS CERT

III. Затем, что требуют

- 31-й приказ ФСТЭК. АСУТП. Состав мер: ЗИС.2 – Защита периметра ИС (АС) и др.
  fstec.ru

- 239-й приказ ФСТЭК. КИИ. Состав мер: ЗИС.2 – Защита периметра ИС (АС) и др.
  fstec.ru

- 235-й приказ ФСТЭК. КИИ. Средства: межсетевые экраны и др.
  fstec.ru

Что там защищать?

Объекты защиты (31-приказ):

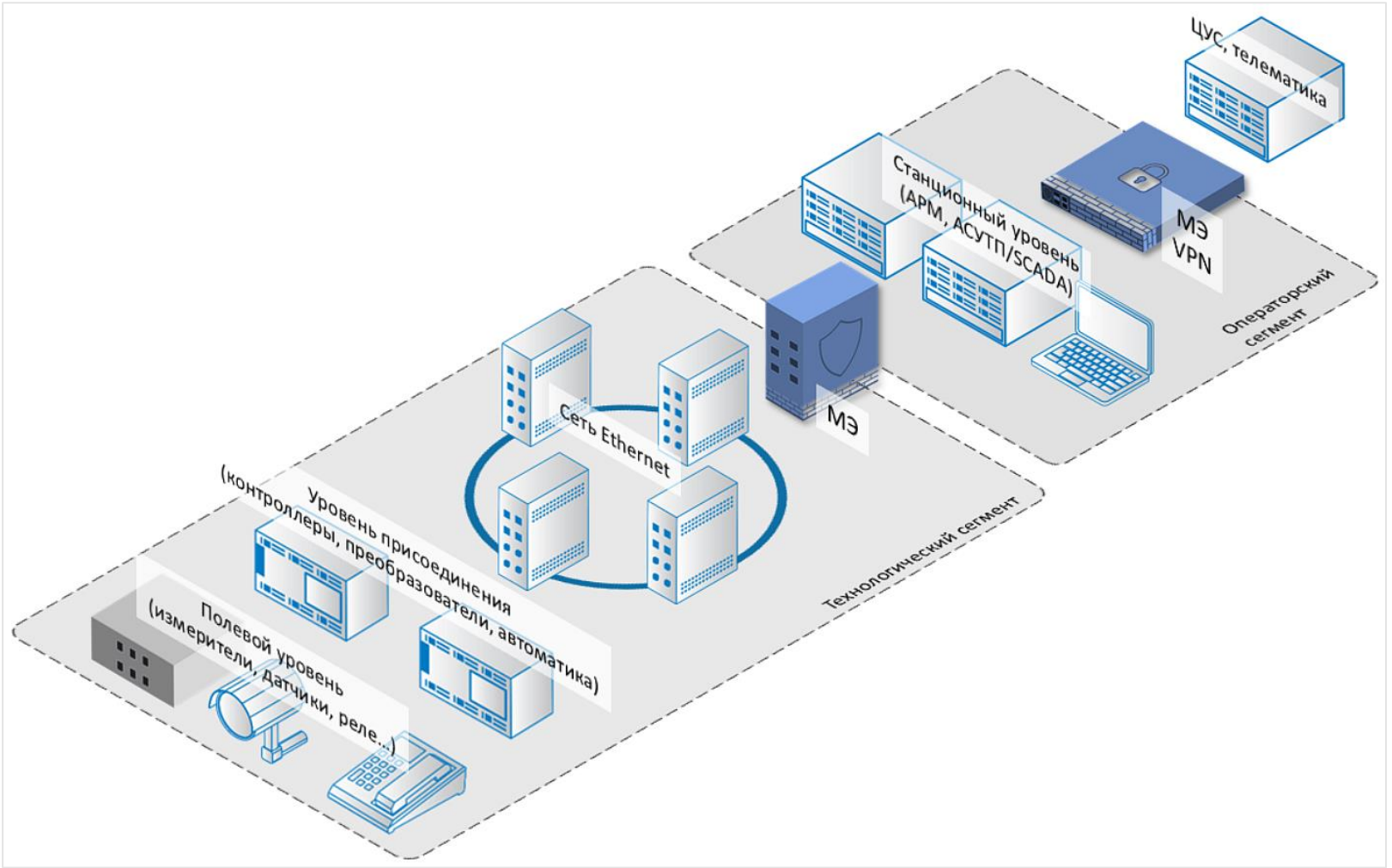
- критически важная информация о параметрах объекта или процесса
- ПТК (АРМ, серверы, ТКО, ПЛК, исполн. устройства, ПО, СЗИ

Несколько периметров:

- Технологический сегмент
- Операторский сегмент
- ДМЗ

Контроль и фильтрация:

- пром. протоколов МЭК (MMS и др.), SV, Modbus, Profibus;
- стандартных протоколов TCP/IP, RDP, FTP



Как это защищать?

Требования регулятора

Защита от угроз:

- угроза возможна – блокирование и нейтрализация
- угроза есть – локализация и минимизация последствий
- угроза реализована – восстановление штатного режима функционирования

Главное – не навреди:

- обеспечить доступность, целостность, конфиденциальность данных
- соотноситься с мерами пром., эко. и др. безопасности
- не влиять на штатный режим функционирования

(режим “пропускать всё”, если оказываем негативное влияние)

Отраслевые требования

Меры защиты от угроз:

- Выделение шин данных (процессов, управления и др.)
- Логическая сегментация с защитой периметров сегментов
- Организация ДМЗ (АРМ, АСУ, серверы, сеть, телемеханика)
- Экранирование смежных подсистем (мониторинга, тех. безопасность)

Чем это защищать? (1)

Отраслевые требования:

- Сертификация по МЭК 61850
- Климатическое исполнение УХЛ4/О4 (от +1°С до +55°С, влажность 98% при 35°С)
- Программный или программно-технический МЭ типа “Д” на границе технологического сегмента
- Программно-технический МЭ типа “А” или “Д” на границе операторского сегмента
- Поддержка протокола VRRP – для сетевой надежности
- Поддержка протоколов ICMP, SNMPv.3, SYSLOG – для мониторинга и диагностики
- Встроенная система диагностики – состояние портов, исправность блоков питания, температура ЦПУ, загрузка ЦПУ
- Резервирование блоков питания с горячей заменой (опционально)

Чем это защищать? (2)

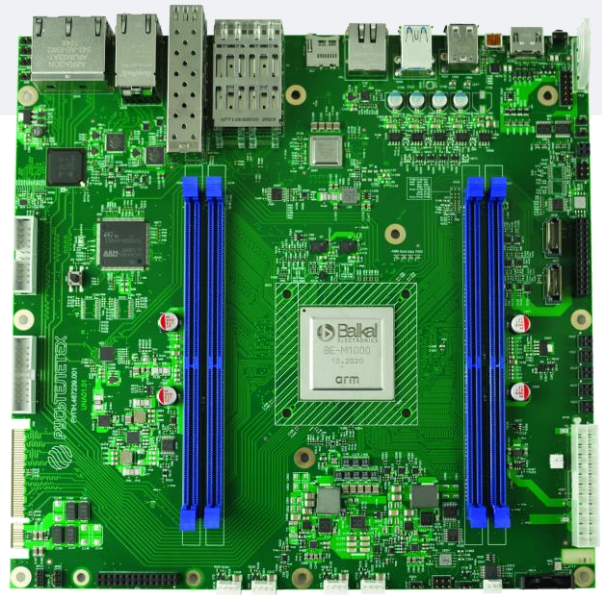
Наименование	Сертификация	Модели	Фото
Изделие «Межсетевой экран «UserGate»	- МЭ: А4, Б4, Г4, Д4 - СОВ: С4 - УД: УД4	X1, C100, C150	
ПАК ШБ “Check Point Security Gateway версии R77.30”	- МЭ: А4, Д4 - СОВ: С4 - УД: УД4	SG5600	
ПАК “Dionis DPS”	- МЭ: А4, Д4 - СОВ: С4 - УД: УД4	DPS-1003S/1003SD	
ПАК “ViPNet Coordinator IG 4”	- МЭ: А4, Б4, Д4 - УД: УД4	IG10 I1/I2, IG100 I1	
ПО “Система сетевой безопасности Mirada”	- МЭ: Б4, Д4 - СОВ: С4 - УД: УД4	ПО	
Прогр. компл. “InfoWatch ARMA Industrial Firewall”	- МЭ: Д4 - СОВ: С4 - УД: УД4, 3Б	ПО	

Наш опыт создания «пром» МЭ

RTT-M300x

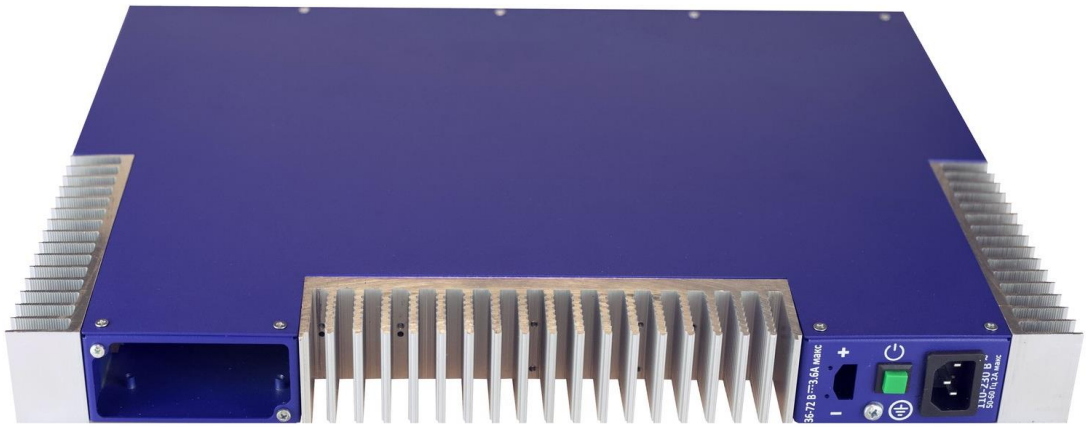
Универсальные шлюзы безопасности

- Первая подсерия на процессорах Baikal-M. В roadmap'е выпуск на других ЦПУ
- Аппаратная часть собственной разработки. Универсальная сетевая платформа
- Программная часть собственной разработки. Кроссплатформенное решение



Защита промышленных сетей. RTT-M300F

- Расширенный температурный диапазон (-5°C...+55°C)
- Безвентиляторный дизайн
- Влагопылезащищенность IP30
- Электропитание 115 – 240 В, 50 Гц, не более 1 А
- Резервное питание 18-72 В DC, не более 5 А
- Анализ промышленных протоколов MODBUS/TCP, MQTT



Функциональные возможности

Комплексная защита сетевой инфраструктуры:

- Межсетевое экранирование (Firewall)
- Защита от вторжений (IDS/IPS)
- Журналирование трафика (Logging)
- Анализ и инспекция пакетов (LiteDPI)
- Проксирование трафика (Proxy)
- Трансляция сетевых адресов (xNAT)
- Создание «частных» сетей (VPN)
- Потоковая антивирусная защита (AV)
- Аутентификация (AAA)
- Кластеризация (HA)
- Маршрутизация (RIP, OSPF, ECMP, xBGP)
- Сервер DHCP, DNS, NTP

Система и управление:

- Полное управление через Web-интерфейс
- Подключение по SSH
- Мониторинг служб и платформы
- Резервные копии системы и сервисов
- Обновление из доверенного репозитория
- Журналирование системы
- Резервирование (CARP)
- Экспорт/импорт настроек
- Оповещение об обнаруженных ошибках
- Доверенная загрузка системы
- Автоматическое восстановление после сбоев

RTT-M300x Аппаратные конфигурации

Характеристика	Значение	
Наименование (модель)	RTT-M300	RTT-M300F
Форм-фактор	1U (19” Rack unit)	
Центральный процессор	Baikal-M1000, 8-core 1,5 GHz ARM Cortex-A57	
ОЗУ	До 32 Гбайт (до 4 модулей DIMM) 2400 МГц DDR4	
ПЗУ	2 порта SATA 3.0	
Сетевые интерфейсы	4 x GE, 2 x 10GE (SFP+), 2 x GE Combo	
Карты расширения	8xGE (RJ45), 2x10GE (SFP+), 4xGE Switch*	
Порт OOB	1 x FE (RJ45)	
Влагопылезащищенность	IP20	IP30
Пассивное охлаждение	Нет	Да
Диапазон рабочих температур	-5°C … +45°C	-5°C … +55°C
Габариты	444 × 44 × 383 мм	444 × 44 × 403 мм
Вес	Не более 5 кг	Не более 7 кг
Электропитание	115 – 240 В, 50Гц, не более 1 А	
Резервное питание*	1+1 Hot plug	18-72 В DC, не более 5 А

Производительность

Характеристика	Значение	
Размер пакета, байт	64	1500
Количество правил фильтрации	100	
Пропускная способность в режиме фильтрации L4, Мбит/с	120	2500
Пропускная способность в режиме фильтрации L4, кпак/с	205	300
Пропускная способность в режиме фильтрации + Lite DPI (на примере 100 правил IP drop + 5 правил offset drop), Мбит/с	120	2500

RTT-M300x. Roadmap

- Кластеризация active/active + балансировка трафика
- Контентная фильтрация, L7
- Интеграция с SOC
- VPN с ГОСТ
- Функции L2 (LACP, VLAN и т.д.)
- Полноценный API для HTTPs
- Браузер логов

А ты доверяешь своей сети?

www.ртт.рф +7 (495) 234-9777 info@rusteletech.ru

RTT