



Доверенные решения для критической информационной инфраструктуры

NGFW

СРЕДСТВА СЕТЕВОЙ БЕЗОПАСНОСТИ

Николай Заугольный
Руководитель направления сетевой безопасности

Figure 1. Magic Quadrant for Network Firewalls



Palo Alto



PA-7080



PA-220

ИнфоТЭК



xF5000



xF100

НИИ Масштаб



3500SPR



500KRF

❑ Коммутационные матрицы:

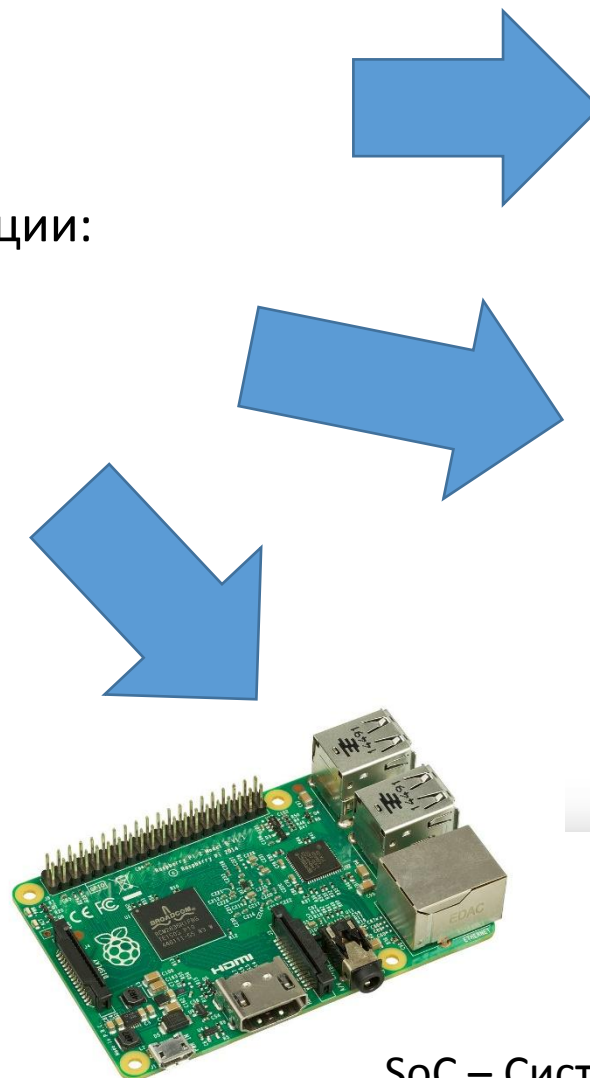
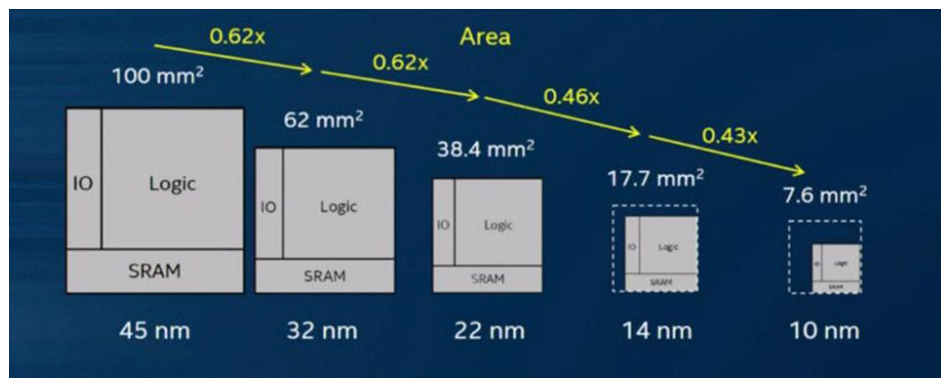
FPGA, ASIC

❑ Увеличение производительности процессоров за счет их специализации:

NPU, GPU, TPU

❑ Механизмы доверенной загрузки устройства:

ARM TrustZone



SmartNIC



Многопроцессорные модульные системы

SoC – Системы на кристалле



ФУНКЦИОНАЛЬНОСТЬ

- ☐ Устойчивость к новым угрозам
- ☐ Удобство, простота
- ☐ Стандартизация по требованиям

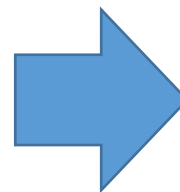
ДОВЕРИЕ

- ☐ Доверенная загрузка аппаратных устройств
- ☐ Доверенная среда исполнения ПО

СООТВЕТСТВИЕ

- ☐ Соответствие выполняемой задаче
- ☐ Модульность, масштабируемость

1. Полезный трафик пропустить.
2. Вредный трафик отфильтровать.
3. Не допустить воздействия на целевую систему (сетевой сегмент) согласно заложенной модели безопасности.
4. Обработать трафик в режиме реального времени (со скоростью интерфейса).
5. Эффективно обеспечивать сетевую защиту любых устройств от IoT до Дата-центров.
6. Подключать функционал по требованию.
7. Умно потреблять энергию.



Использование современных алгоритмов и методик работы с трафиком L2-L7 OSI.

Модульная структура ПО и аппаратной части = легкая модернизация.

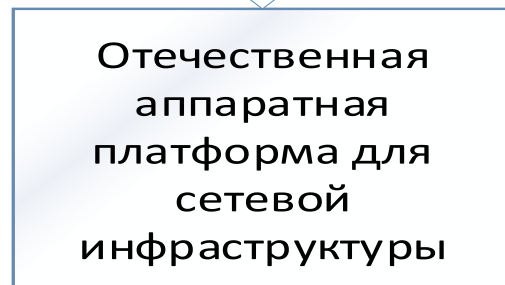
Постоянное совершенствование продукта NGFW и его возможностей.

Универсальная серверная платформа TSP Доверенный NGFW

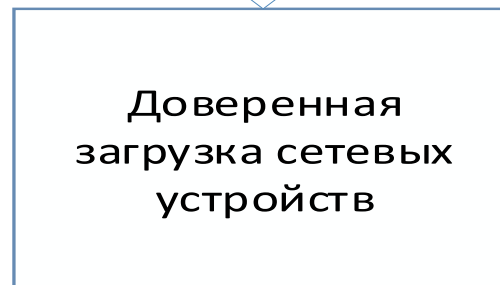
Средство сетевой безопасности нового поколения?



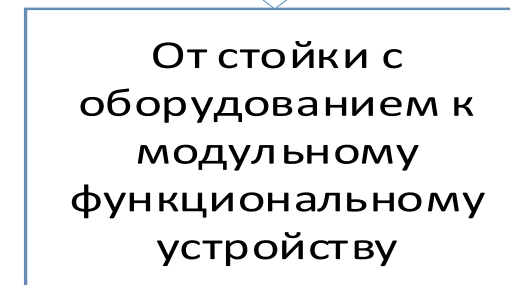
ФАЗА 1

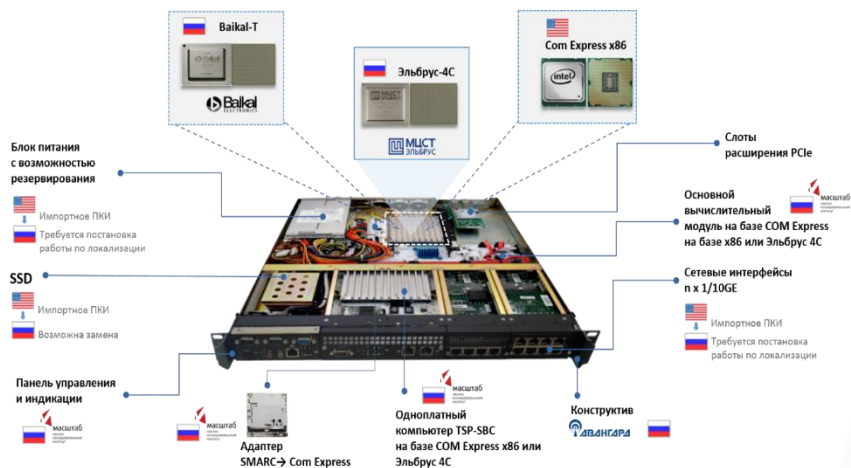


ФАЗА 2



ФАЗА 3





Линейка :

TSP -500, TSP-4E, TSP -1200, TSP-1500, TSP-3000, TSP-3500



УНИВЕРСАЛЬНАЯ ТЕЛЕКОММУНИКАЦИОННАЯ СЕРВЕРНАЯ ПЛАТФОРМА TSP – МОДЕРНИЗИРОВАННЫЙ ЭЛЕМЕНТ УНИФИКАЦИИ

Семейство универсальных серверных платформ TSP состоит из унифицированных платформ различного уровня производительности с возможностью гибкого наращивания сетевых интерфейсов и подключения различных средств защиты информации.



ВОЗМОЖНОСТЬ УСТАНОВКИ
МИКРОПРОЦЕССОРОВ
ОТЕЧЕСТВЕННЫХ
И ЗАРУБЕЖНЫХ
ПРОИЗВОДИТЕЛЕЙ



ВЫСОКАЯ ПЛОТНОСТЬ ETHERNET
ПОРТОВ



ОТЕЧЕСТВЕННАЯ ЭЛЕМЕНТНАЯ БАЗА



КОМПАКТНОСТЬ

КРОНОС



ПК КРОНОС:

МО РФ: НДВ-2, МЭ-2Б, СОВ-2 (ИТ.СОВ.С2.ПЗ),
РДВ

АПК КРОНОС:

МО РФ: НДВ-2, МЭ-2А, СОВ-2 (ИТ.СОВ.С2.ПЗ),
РДВ*

Сертификат соответствия Техническому
регламенту Таможенного Союза

004/2011.020/2011

Минкомсвязи РФ: ОС-1-СПД-2220 от 20.03.2018
года

КРОНОС ЭРА:

ФСТЭК: НДВ-2, НДВ-4, МЭ-2Б, МЭ-4Б, СОВ-2
(ИТ.СОВ.С2.ПЗ), РДВ (1 кв. 2020 г.)

МО РФ: НДВ-2, НДВ-4, МЭ-2Б, МЭ-4Б, СОВ-2
(ИТ.СОВ.С2.ПЗ), РДВ (1 кв. 2020 г.)

Программный и аппаратно-программный комплекс межсетевого экрана с функциями системы обнаружения вторжений

Модельный ряд КРОНОС позволяет подобрать аппаратную платформу в соответствии с потребностями различных заказчиков: от небольших компаний до операторов связи и центров обработки данных. Межсетевые экраны КРОНОС, реализованные на аппаратных платформах, производство которых локализовано на территории РФ, включены в реестр телекоммуникационного оборудования российского происхождения. Обеспечивается качественная гарантийная и сервисная поддержка продукта. Комплексы КРОНОС сертифицированы Министерством обороны РФ и ФСТЭК, могут быть использованы в составе специальных сетей связи для защиты информации, содержащей сведения, составляющие государственную тайну.



**ШИРОКИЕ
ФУНКЦИОНАЛЬНЫЕ
ВОЗМОЖНОСТИ**

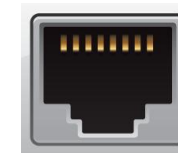
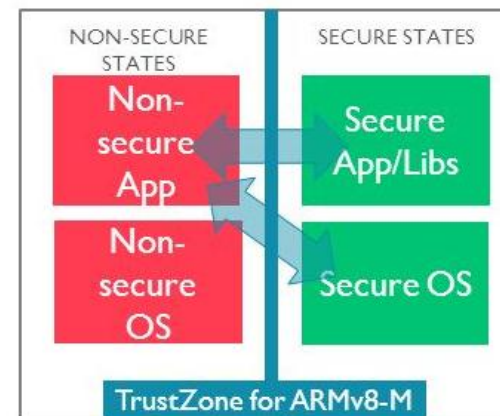


**ПОСТОЯННЫЙ МОНИТОРИНГ И
ОБНАРУЖЕНИЕ ВТОРЖЕНИЙ
В РЕЖИМЕ, БЛИЗКОМ К РЕАЛЬНОМУ ВРЕМЕНИ**

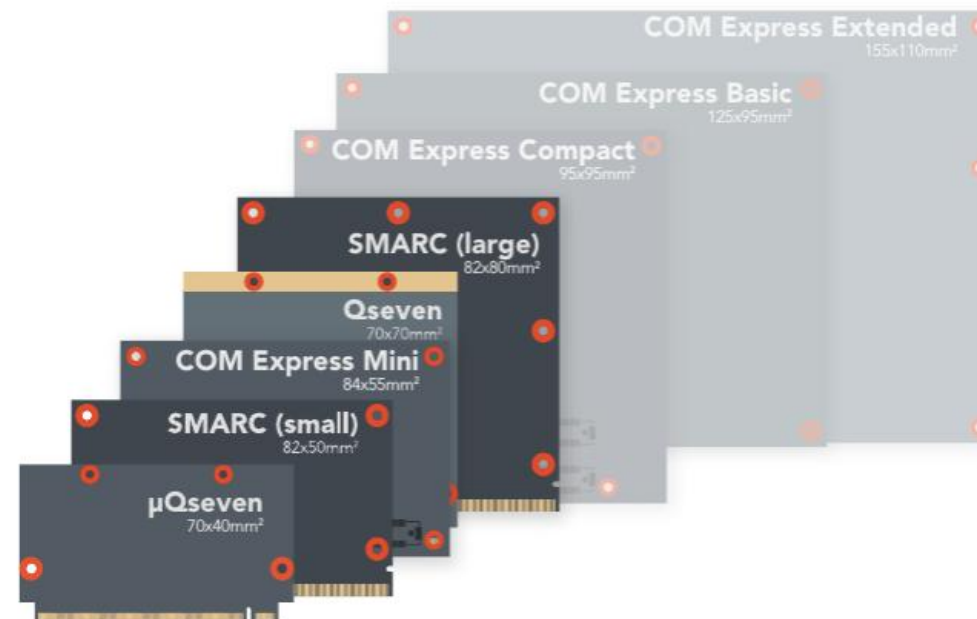


**ВОЗМОЖНОСТЬ
ВЫБОРА
АППАРАТНОЙ
ПЛАТФОРМЫ**

- ✓ Межсетевой экран (с функциями крипто)
- ✓ Доверенная загрузка
- ✓ Доверенное исполнение ПО
- ✓ Компактный размер
- ✓ ТОРП
- ✓ Назначение: IoT и Smart системы, СЗО,



>2 x 1Gb Ethernet



- ✓ Продукт должен быть ориентирован на открытые сегменты российского рынка и на выбранные приоритетные сегменты: объекты КИИ, СЗО.
- ✓ Необходимо использование внешнего софинансирования и модели кооперации для разработки продукта.
- ✓ Использование бизнес-моделей цифровой экономики – предоставление функций продукта по требованию, оплата по фактическому объему потребления и/или результатам потребления (интеграция с рынком страхования кибер-рисков).
- ✓ Возможность глубокой доработки продукта на этапе его эксплуатации (DevOps).
- ✓ Развитые экосистемы разработчиков, реализация модели разделения выручки.
- ✓ Партнерства с провайдерами облачных сервисов и операторами связи, внедряющими на своих сетях технологии SDN&NFV.

Enterprise
Cloud
Platform **Veil**

ГЕЛИОС

КРОНОС

Telecommunication
Server Platform

TSP

 **LARGO**

 **AVES**

АО «НИИ «Масштаб»

- Платформы виртуализации
- Сетевая безопасность
- Защищенная видеоконференцсвязь
- Сопровождение и поддержка полного жизненного цикла продуктов
- Проектирование систем и сетей связи, ИТ инфраструктуры
- Реализация комплексных проектов "под ключ"



масштаб
научно-
исследовательский
институт



АВТОМАТИКА

Спасибо за внимание!
mashtab.org