ЦЕНТР КОМПЕТЕНЦИЙ НТИ
на базе НИУ "МЭИ"
ТЕХНОЛОГИИ ТРАНСПОРТИРОВКИ ЭЛЕКТРОЭНЕРГИИ И РАСПРЕДЕЛЕННЫХ ИНТЕЛЛЕКТУАЛЬНЫХ ЭНЕРГОСИСТЕМ

Частные вопросы разработки защищенной встраиваемой операционной системы для АСУ ТП объектов КИИ

Владимир Карантаев
к.т.н.
Руководитель центра экспертизы практической кибербезопасности индустриальных систем Центра НТИ МЭИ

WWW.NTI.MPEI.RU

Визитка: Владимир Карантаев

Практик

Стаж деятельности в области ИТ и ИБ - 22 года (с 2002 года).

10 + лет экспертной и прикладной деятельности в направлении Кибербезопасность АСУ ТП

Ex ИнфоТеКС **Ex** Kaspersky

Проекты в ПАО Россети

Соавтор и организатор первых киберучений национального уровня

Преподаватель и исследователь

к.т.н. специальность 05.09.03 "Электротехнические комплексы и системы"

Автор курса лекций «Основы кибербезопасности РЗА энергосистем»

Центр НТИ МЭИ Кафедра РЗиАЭ.

Консультант

Ключевые продукты Центра НТИ МЭИ

ЦЕНТР КОМПЕТЕНЦИЙ НТИ
на базе НИУ "МЭИ"

Интеллектуальная система РЗА

Открытая АСУТП

ПАК «Цифровой двойник энергосистемы»

Структура доклада

ЦЕНТР КОМПЕТЕНЦИЙ НТИ
на базе НИУ "МЭИ"

- Тренды в развитии систем индустриальной автоматизации и автоматики.
- Угрозы безопасности информации систем индустриальной автоматизации и автоматики.
- Потребности разработчиков отечественных доверенных ПАК (ПЛК, РСУ, ПАЗ, ИЭУ).
- Вопросы разработки защищенной встраиваемой операционной системы реального времени.

Открытая АСУ ТП(O-PAS)

ЦЕНТР КОМПЕТЕНЦИЙ НТИ
на базе НИУ "МЭИ"

Сведения

- Разработчик – Open Process Automation Forum (Open Group)
- Инициатор – ExxonMobil
- В России развивается силами ПАО «Газпромнефть» и РГ «ОАСУТП»

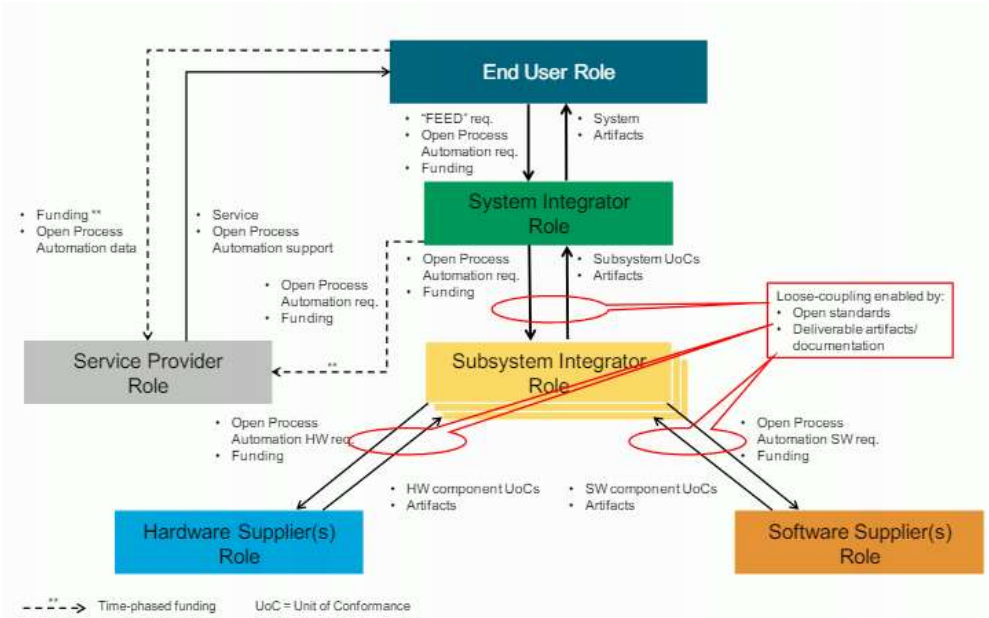
Ключевые положения

- Изменение бизнес-модели рынка АСУ ТП
- Взаимозаменяемость компоненты разных поставщиков
- Отделение прикладных задач от системного ПО и аппаратных платформ
- Встроенные требования защищенности не хуже IEC62443 SL2

O-PAS.
Изменения в модели бизнеса

ЦЕНТР КОМПЕТЕНЦИЙ НТИ
на базе НИУ "МЭИ"

- Усиление роли системных интеграторов
- Расширение количества поставщиков компонентов
- Выделение сервисных компаний независящих от поставщиков и/или интеграторов
- Сертификация всех компонентов на соответствие стандарту
- Роли МОЖНО совмещать



O-PAS.
Концепция архитектуры

ЦЕНТР КОМПЕТЕНЦИЙ НТИ
на базе НИУ "МЭИ"

- Общая шина на базе OPC UA
- Общая информационная модель начиная с уровней ПЛК и шлюзов в формате OPC UA
- Централизованное управление конфигурацией АСУТП, включая программирование ПЛК, независящее от конкретных вендоров АСУТП
- Мультифункциональные сервера с набором контейнеров для выполнения задач АСУТП, СУУТП, мониторинга, ML и т.п.
- Использование IEC 61131-10 совместимых программных ПЛК от различных вендоров
- Встроенные требования к безопасности

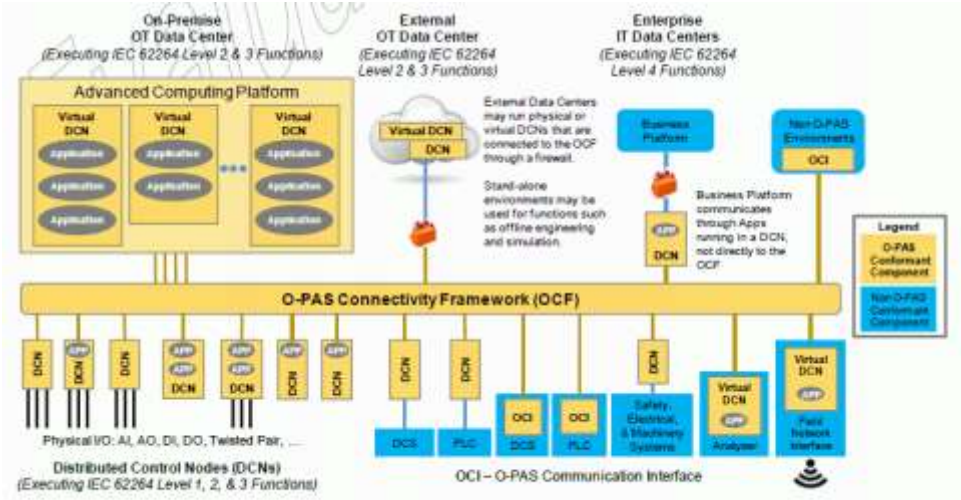


Figure 1: Concept Diagram of a Process Automation System of O-PAS Conformant Components

Рабочая группа по открытой промышленной АСУ ТП

ЦЕНТР КОМПЕТЕНЦИЙ НТИ
на базе НИУ "МЭИ"

Создан приказ Минпромторга №2939 от 14 августа 2023 г.

В состав группы входят более 20 крупных промышленных компаний.

#1
Независимость
Вендорная и платформенная независимость

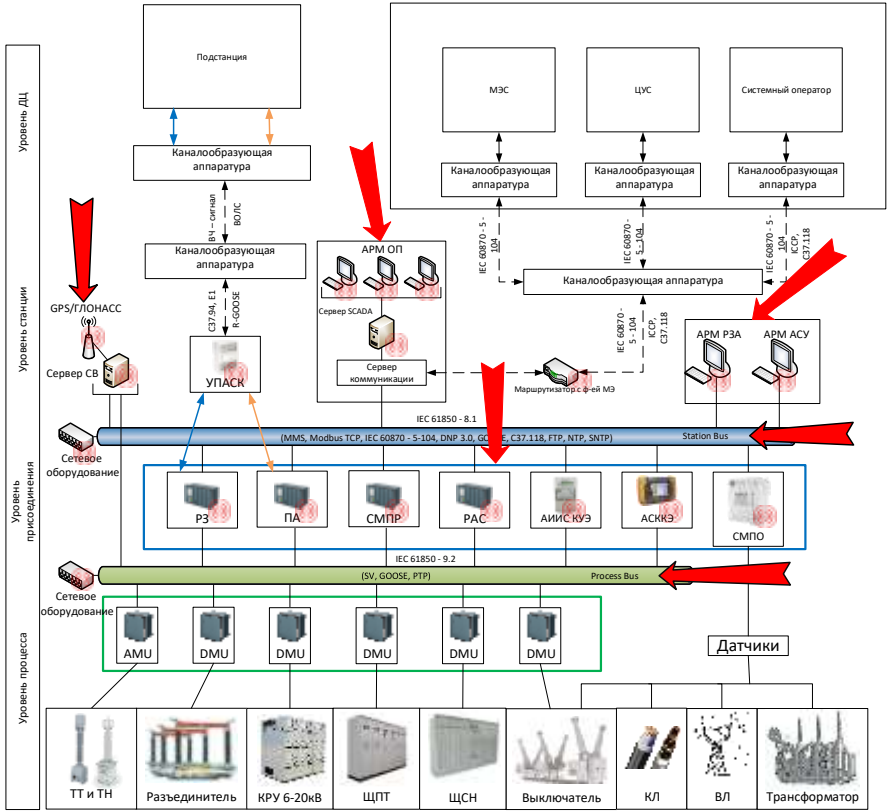
#2
Открытость
Открытость решений, систем и их компонентов

#3
Универсальность архитектуры
Универсальность архитектуры, модульная совместимость и взаимозаменяемость

#4
Универсальность
Универсальность по отношению к индустриальным отраслевым стандартам и межотраслевая применимость

Модель угроз ЦПС

ЦЕНТР КОМПЕТЕНЦИЙ НТИ
на базе НИУ "МЭИ"



Виды возможных атак

- GPS/ГЛОНАСС Spoofing
- GOOSE Spoofing
- MITM MMS
- MITM МЭК 60870 - 5 – 104
- Brute Force
- Риски успешных APT с ущербом кибер- и физическим характеристикам ЦПС и SmartGrids (ААС ЕЭС, цифровым сетям)

Возможные векторы воздействия

Атаки на Endpoints

Атаки на протоколы

Современное ИЭУ как объект защиты

Современное ИЭУ и подсистема РЗА – это:

- Компьютерная система.
- Объект критической информационной инфраструктуры.
- Значимый объект критической информационной инфраструктуры.
- КС - это человеко-машинная система, представляющую совокупность электронно-программируемых технических средств обработки, хранения и представления данных, программного обеспечения, реализующего информационно-коммуникационные технологии осуществления каких-либо функций, и информации (данных).

Доверенные ПАКи АСУ

Разрабатываемые ПАКи должны стать доверенными программно-аппаратными комплексами.

Доверенный ПАК должен одновременно соответствовать всем критериям:

1. Сведения о программно-аппаратном комплексе содержатся в едином реестре российской радиоэлектронной продукции
2. Предъявленному комплексу требований к ПО
3. Программно-аппаратный комплекс в случае реализации в нем **функции защиты информации** соответствует требованиям, установленным Федеральной службой по техническому и экспортному контролю и (или) Федеральной службой безопасности Российской Федерации в пределах их полномочий, что должно быть подтверждено соответствующим документом **(сертификатом).**

ПП 1912

Методология разработки доверенных ПАК (ПЛК, РСУ, ПАЗ, ИЭУ) на основе принципа Secure by Design

- При создании доверенных ПАК необходимо начинать с разработки модели угроз и нарушителя, после чего планомерно подбирать механизмы безопасности, которые могут помочь в противодействии выявленным угрозам и сценариям реализации атак.
- Системы должны разрабатываться с учетом анализа угроз функциональной надежности и информационной безопасности.
- Внедрение процессов РБПО является практической реализацией принципа Security-by-design (безопасности на архитектурном уровне) при разработке программного обеспечения и программно-аппаратных комплексов, в том числе доверенных ПАК: **ПЛК, РСУ, ПАЗ, ИЭУ.**

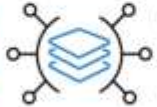
Разработка безопасного программного обеспечения (РБПО) для ПАК АСУ

Обучение

Выбор и обоснование применения СКЗИ

Испытания на быстродействие РЗА

Разработка требований с учетом специфики РЗА

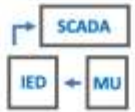


Анализ состава и свойств применяемых библиотек от сторонних поставщиков

Функциональные испытания РЗА

Определение измеримых целевых показателей

Внедрение и применение доверенных средств разработки ПО



Испытания на соответствие МЭК 61850

Моделирование угроз и Нарушителей для РЗА

Статический анализ кода

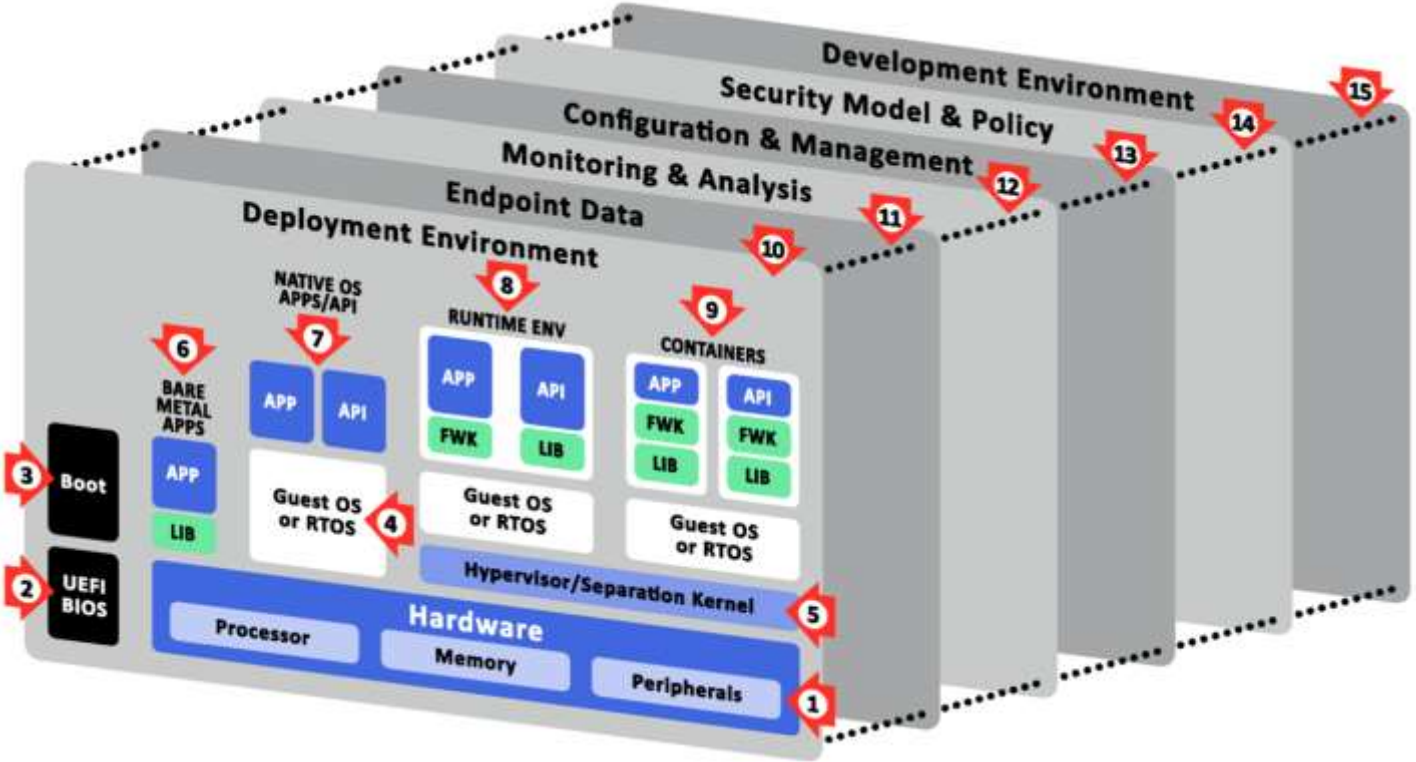
Испытания на проникновение (pen test)

Разработка архитектуры ПО и ПАК

Динамический анализ кода

Подготовка плана устранения уязвимостей

Где могут возникать угрозы безопасности ПЛК? (1)



IIC Security Framework, https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf

Где могут возникать угрозы безопасности ПЛК? (2)

- (1) Угрозы, связанные с аппаратурой
- (2)(3) Угрозы, связанные с процессом начальной загрузки
- (4)(5) Угрозы, связанные с системным ПО
- (6)(7)(8)(9) Угрозы, связанные с прикладным ПО
- (10) Угрозы, связанные с процессом установки (развертывания) ПО
- (11) Угрозы, связанные с доступом к данных ПЛК
- (12) Угрозы, связанные с процессом мониторинга
- (13) Угрозы, связанные с процессами управления и конфигурирования
- (14) Угрозы, связанные с политиками и моделями безопасности
- (15) Угрозы, связанные с процессом разработки

Цели атак (негативные последствия)

- Несанкционированное изменение уставок/конфигурации/проекта ПЛК
- Подмена контрольно-измерительной информации, собираемой ПЛК
- Исполнение ложных команд на ПЛК
- Создание временной недоступности ПЛК
- Вывод из строя ПЛК
- Создание (устойчивого) бэкдора из ПЛК

Структура требования к доверенному ПАК

- Функциональные требования безопасности.
- Нефункциональные требования.
- Требования к тестированию и оценке соответствия.
- Требования к проектированию и производству программного обеспечения (РБПО).

Потребности разработчиков доверенных ПАК (ПЛК, РСУ, ПАЗ, ИЭУ)

- Поддержка необходимой аппаратной части (СнК, периферия);
- Детерминированное поведение (реальное время);
- Возможность реализации алгоритмов защит и IEC 61850 (reliability, performance, ready components);
- Ускорение прохождения аттестации ПАО “Россети” и других форм добровольной сертификации;
- Удобный и функциональный инструментарий разработчика;
- Качественная техподдержка;
- Длительные (10+ лет) сроки поддержки;
- Удовлетворение адаптированных требований МЭК 62443 и МЭК 62351;
- Разработка доверенного пакета поддержки плат (Board Support Package, BSP) на базе ISA ARM, RISC V;
- Сертификация во ФСТЭК России.

Доверенный пакет поддержки плат

ЦЕНТР КОМПЕТЕНЦИЙ НТИ
на базе НИУ "МЭИ"

Пакет поддержки плат (BSP) должен содержат все компоненты необходимые для запуска Linux на конкретной аппаратной платформе:

- Загрузчик (Доверенный загрузчик);
- Ядро Linux;
- Драйверы специфичиные для выбранной платы;
- Дерево устройств;
- Загрузочные скрипты и файлы конфигурации;
- Бинарный файл прошивки

Понятие защищенной операционной системы

ЦЕНТР КОМПЕТЕНЦИЙ НТИ
на базе НИУ "МЭИ"

Классика:

- **Definition 2.5**. A secure operating system is an operating system where its access enforcement satisfies the **reference monitor** concept [Anderson].

Базовые термины:

- **Операционная система; ОС:**
  Комплекс взаимосвязанных программ, предназначенных для управления ресурсами средств вычислительной техники и организации взаимодействия с пользователем

- **Защищённой (доверенной)** целесообразно считать ОС, которая не только реализует заданные априорно требования безопасности, но и адекватна угрозам безопасности, специфичным для отечественных АС, в том числе для которой отсутствует возможность несанкционированного влияния на её работу извне, при этом владелец (пользователь) защищённой ОС должен иметь однозначное представление об алгоритме функционирования её защитных механизмов во всех режимах работы.

- **Дистрибутив Linux** - это комплект взаимосогласованного программного обеспечения, включающий ОС на базе ядра Linux, системное программное обеспечение и приложения, а также систему управления программным обеспечением

Зарубежные операционные системы

ЦЕНТР КОМПЕТЕНЦИЙ НТИ
на базе НИУ "МЭИ"

LF ENERGY

timesys

WNDRVR

Mentor Graphics®

MontaVista

Linaro

Коммерческие продукты в России практически отсутствуют!

Требования к ИЭУ РЗА

ЦЕНТР КОМПЕТЕНЦИЙ НТИ
на базе НИУ "МЭИ"

Требования к протоколам передачи данных:

Протокол	Мин. размер пакета, байт	Макс. Размер пакета, байт	Мин. время между пакетами, мс	Макс. время между пакетами, мс
SV	163	1536	0,25	0,42
GOOSE	200	1536	4	10000
MMS	220	1536	20	1000
SNTP	80	80	200	200
PTP	80	80	200	200
FTP (FTPS)	1536	1536	200	200
ICMP	32	32	4	4

Требования к быстродействию:

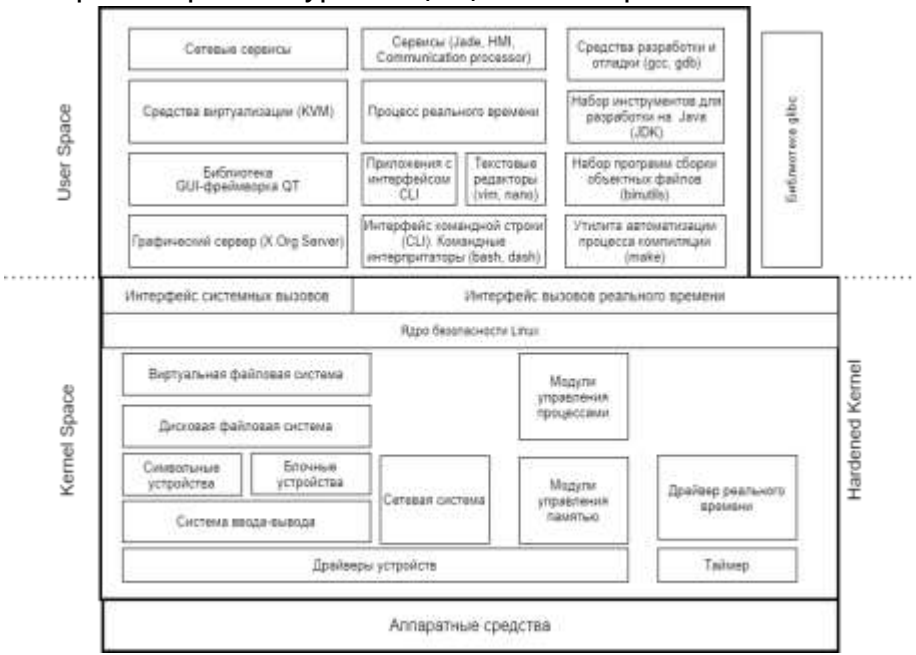
Наиболее требовательным типом защиты является дифференциальная защита линий, время срабатывания которой должно быть не более чем 25 мс.

Сформировано на основе требований СТО ПАО Россети № 56947007-29.120.70.241-2017; № 56947007-29.240.10.302-2020; № 56947007-29.240.10.299-2020

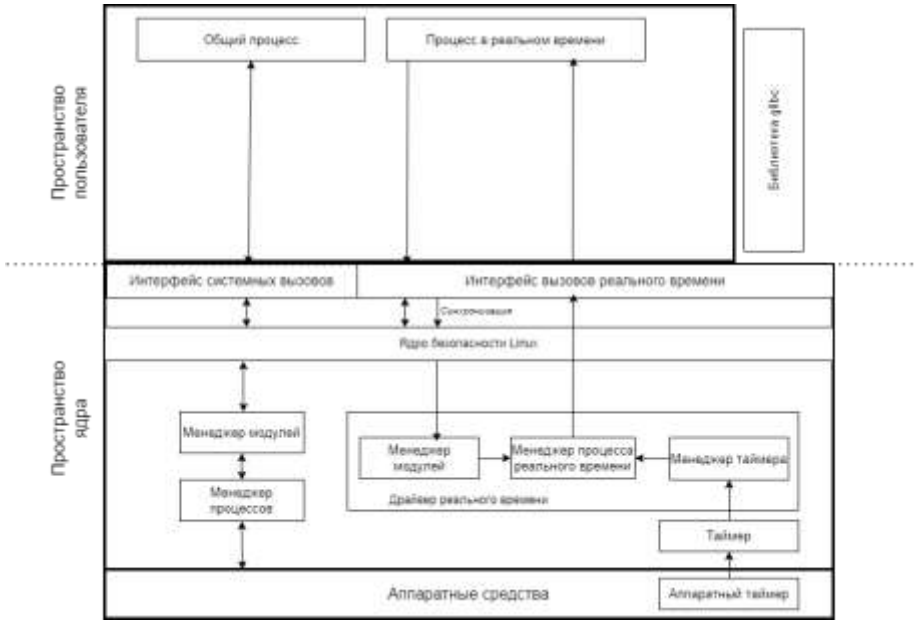
Проект архитектуры ЗОСРВ, разработанной в Центре НТИ МЭИ

ЦЕНТР КОМПЕТЕНЦИЙ НТИ
на базе НИУ "МЭИ"

Проект архитектуры защищенной встраиваемой ОСРВ



Взаимодействие процессов реального времени в защищенной встраиваемой ОСРВ



Требование

Максимальное время отклика на прерывание (джиттер) – (70 ± 30) мкс.

Повышение защищенности

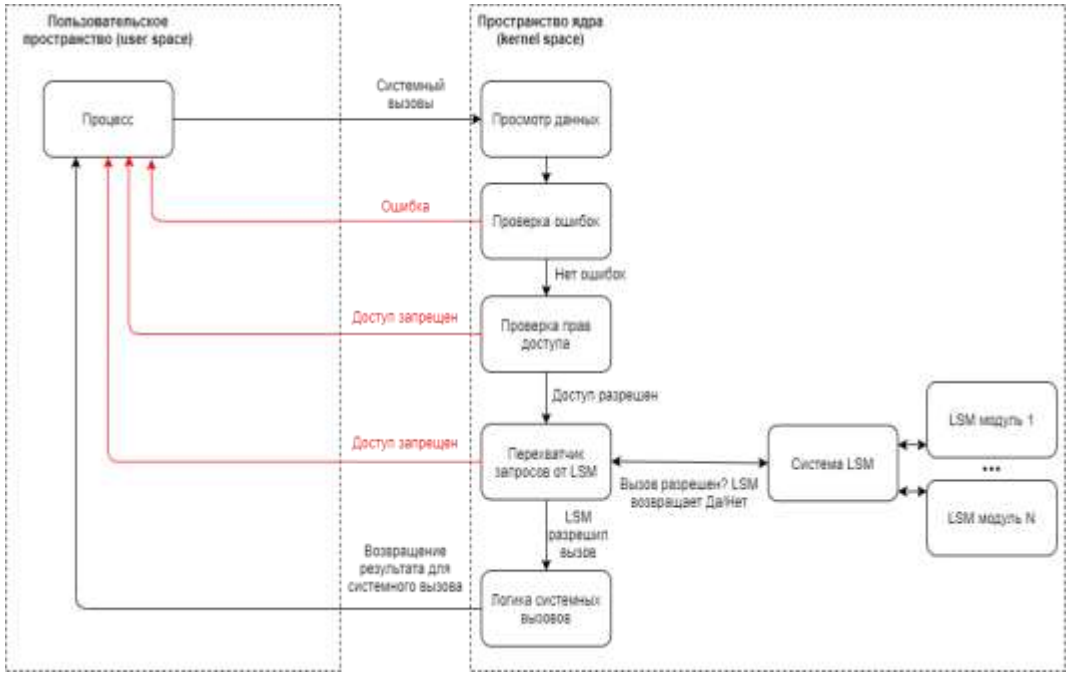
ЦЕНТР КОМПЕТЕНЦИЙ НТИ
на базе НИУ "МЭИ"

Используя инструмент для проверки параметров безопасности (kconfig-hardened-check[1]), выявили, что согласно лучшим мировым практикам, ядро Linux с базовыми настройками не соответствует 57% требований безопасности.

Посредством переконфигурирования удалось снизить долю несоответствий до 11 % (не устраненные несоответствия связаны с используемыми версиями системных модулей).

Отмечено, что переконфигурирование незначительно снижает быстродействие ОС, однако данное снижение не является значительным.

Модули безопасности Linux



1 – https://github.com/a13xp0p0v/kconfig-hardened-check

Состав дистрибутива

ЦЕНТР КОМПЕТЕНЦИЙ НТИ
на базе НИУ "МЭИ"

Компонент	Версия	Обоснование выбора
Ядро	5.10	LTS версия ядра, поддерживаемая Технологическим центром исследования безопасности ядра Linux
Yocto	4.0	Ведущие разработчики встраиваемых ОС, при выборе ядра версии 5.10 ориентируются на данную версию Yocto
Библиотека GUI-фреймворка QT	5.15.2	Ведущие разработчики встраиваемых ОС, при выборе ядра версии 5.10 ориентируются на данную версию QT
Системная библиотека glibc	2.33	Максимальная LTS версия, поддерживая QT 5.15.2
Компилятор gcc	10.2	Максимальная стабильная версия, поддерживаемая ядром 5.10 и QT 5.15.2
Отладчик gdb	10.2	Максимальная стабильная версия, поддерживаемая ядром 5.10 и QT 5.15.2
Утилита автоматизации процесса компиляции make	4.3	Стабильная версия, совместимая с gcc 10.2, gdb 10.2
Набор программ сборки объектных файлов binutils	2.36	Стабильная версия, совместимая с gcc 10.2, gdb 10.2 и make 4.3
Java	AXIOM JDK	Отечественная JDK, отвечающая требованиям безопасности
RTPatch	PREEMPT RT 5.10	Напрямую зависит от версии ядра Linux.

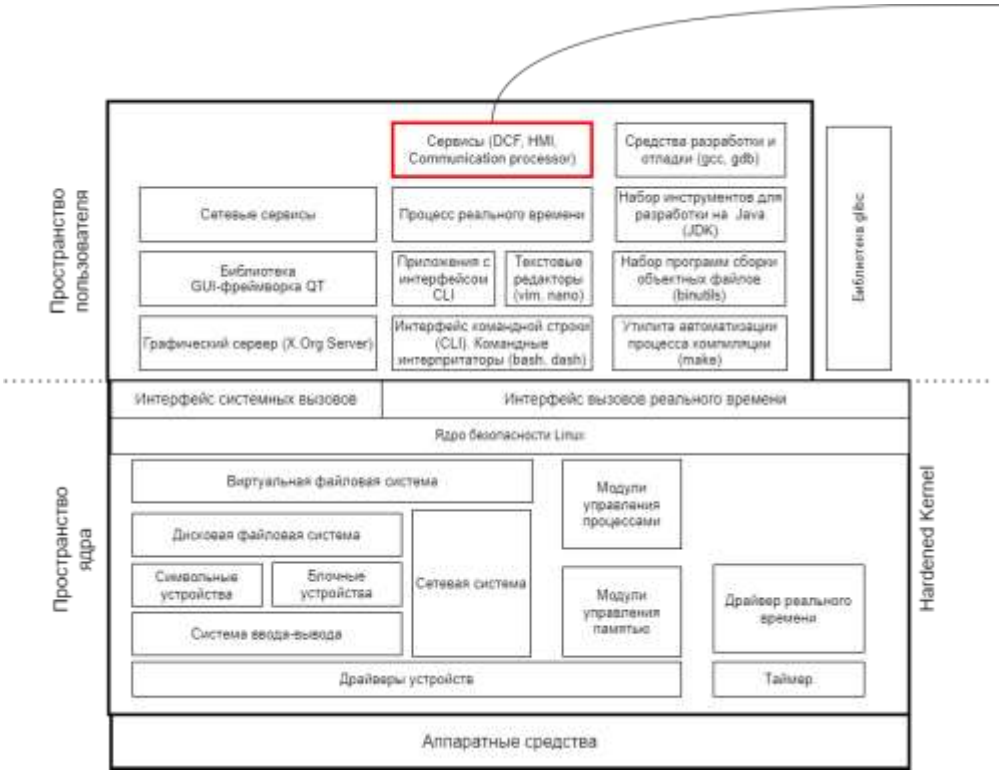
Оптимальная комбинация модулей безопасности Linux

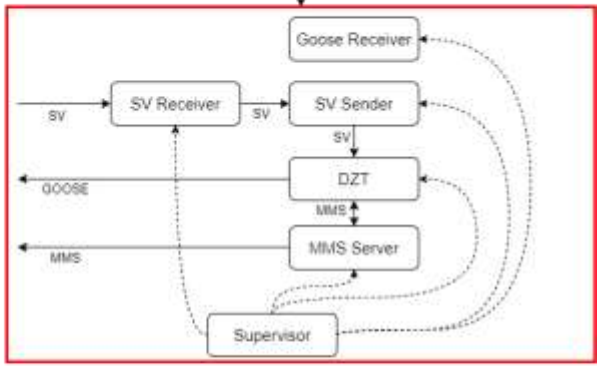
ЦЕНТР КОМПЕТЕНЦИЙ НТИ
на базе НИУ "МЭИ"

- **Default модуль**
  - **Capabilities** – механизм управления привилегиями позволяющий предоставить доступ процессам к определённым возможностям, которые обычно есть только у суперпользователя. Используется.
- **Major модуль (может быть использован только один Major LSM)**
  - **SELinux** – реализация монитора безопасности. Основа для реализации ролевой политики управления доступом (Role-Based Access Control (RBAC). Используется.
- **Minor модули (могут использоваться совместно)**
  - BPF – осуществление фильтрации и модификации сетевых пакетов, управление доступом к сетевым ресурсам. Используется.
  - **Integrity/IMA (Integrity Measurement Architecture)** – контроль целостности системы. Используется.
  - Keys – управление ключами. Планируется использование.
  - Landlock – создание изолированной программной среды. Планируется использование.
  - Loadpin – реализация загрузки всех ресурсов ядра из единой файловой системы, недоступной для записи. Планируется использование.
  - **Lockdown** – обеспечение целостности и конфиденциальности объектов ядра при обращении к ним из пользовательского пространства. Планируется использование.
  - Safesetid – более точный контроль при переключении пользователей. Планируется использование.
  - **Yama** – детализация процесса управления доступом. Планируется использование.

Реализация функций РЗА на базе защищенной встраиваемой ОС

ЦЕНТР КОМПЕТЕНЦИЙ НТИ
на базе НИУ "МЭИ"





Выводы

Реализация концепции **Secure by design** (безопасности на архитектурном уровне) и требований безопасной разработки выглядит наиболее перспективно с учетом:

- необходимости удовлетворять требования по функциональной надежности и безопасности;
- наличия требований по быстродействию телекоммуникационных протоколов и оптимальности затрат.

Для создания доверенных и технологически независимых ПАК на базе ОС с ядром Linux необходимо получить от поставщика:

- доверенный набор инструментов (toolchain).
- доверенный пакет поддержки аппаратной платформы (BSP).
- доверенный способ и процесс создания и использования образа программного обеспечения для ПЛК, ИЭУ РЗА (trusted image).

ЦЕНТР КОМПЕТЕНЦИЙ НТИ
на базе НИУ "МЭИ"
ТЕХНОЛОГИИ ТРАНСПОРТИРОВКИ ЭЛЕКТРОЭНЕРГИИ И РАСПРЕДЕЛЕННЫХ ИНТЕЛЛЕКТУАЛЬНЫХ ЭНЕРГОСИСТЕМ

Телеграм канал Центра НТИ МЭИ

Вопросы?

Карантаев Владимир

к.т.н.
Лидер Центра экспертизы в практической кибербезопасности Центра НТИ МЭИ

KarantayevVG@mpei.ru

http://ЦДЭС.РФ