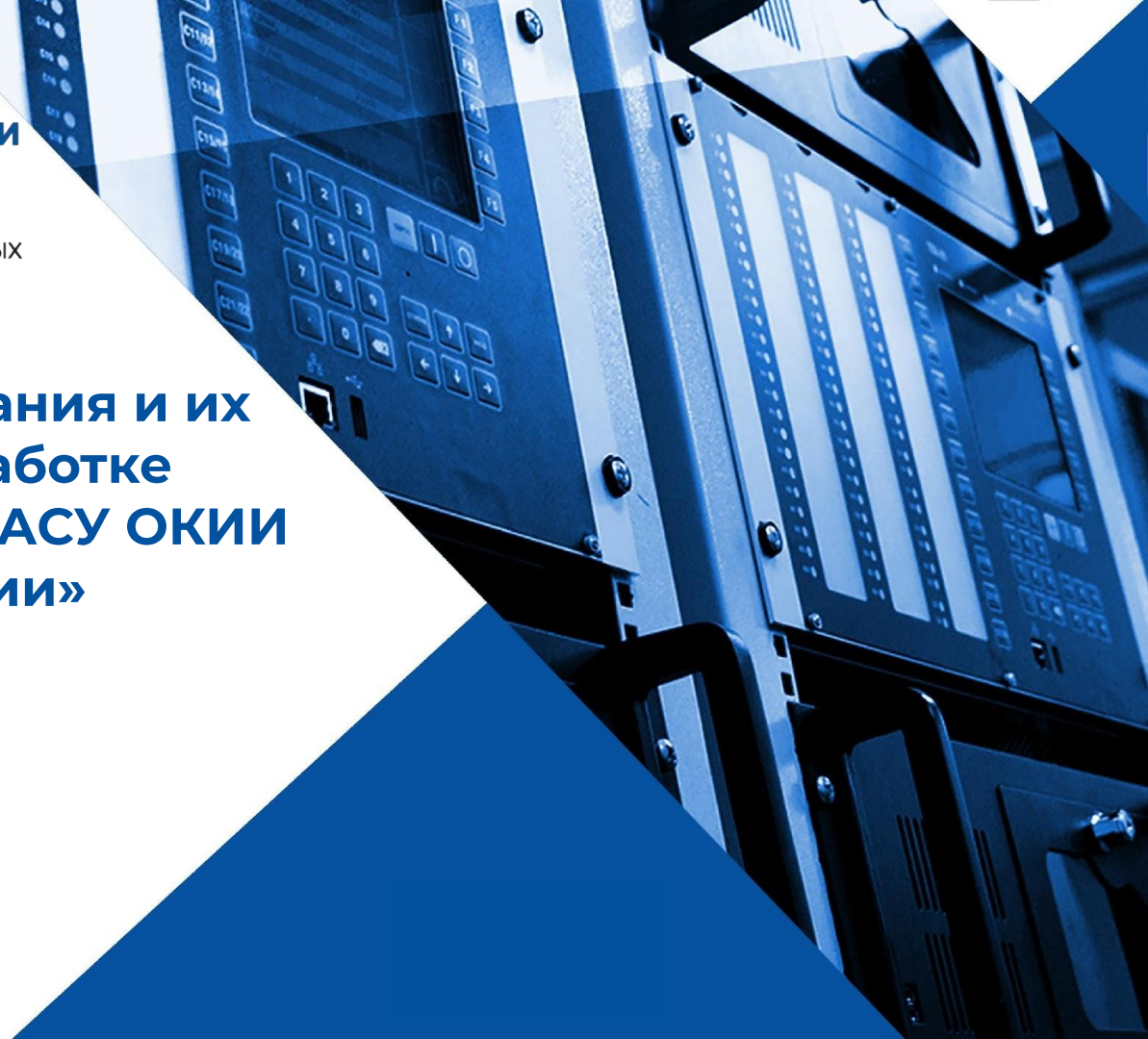
ЦЕНТР КОМПЕТЕНЦИЙ НТИ
на базе НИУ “МЭИ”

ТЕХНОЛОГИИ ТРАНСПОРТИРОВКИ
ЭЛЕКТРОЭНЕРГИИ И РАСПРЕДЕЛЕННЫХ
ИНТЕЛЛЕКТУАЛЬНЫХ ЭНЕРГОСИСТЕМ



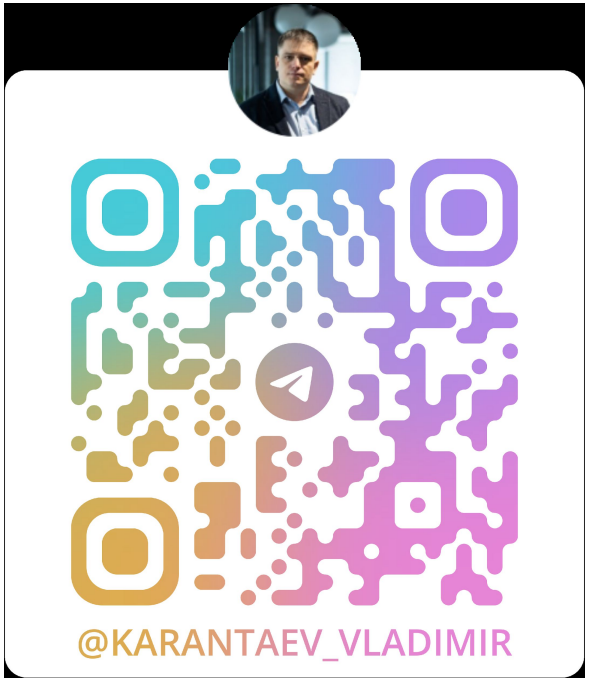
«Технические требования и их реализация при разработке доверенных ПАК для АСУ ОКИИ Российской Федерации»

Владимир Карантаев
К.Т.Н.

WWW.NTI.MPEI.RU

О себе

Директор по продуктам ИБ



Практик

Директор по продуктам ИБ ООО «НЭК.ТЕХ» (R&D Центр «Национальной энергетической корпорации»), MBA.

- Ex ИнфоТеКС Ex Kaspersky (KasperskyOS Department)
- В ИТ и ИБ - 22 года (с 2002 года)
- 10 + лет экспертной и прикладной деятельности в направлении Кибербезопасность АСУ ТП
- Соавтор и организатор первых киберучений национального уровня

Популяризатор технологий

- Технологии RISC-V – координатор Технологического комитета Альянса RISC-V
- Прикладная криптография
- Разработка безопасного ПО

Преподаватель и исследователь

- к.т.н. , автор экспертного курса лекций «Основы кибербезопасности РЗА энергосистем»
- Лидер Центра практической кибербезопасности НТИ МЭИ, Кафедра РЗиАЭ.

Консультант в кибербезопасности АСУ ТП

Современное МП устройство как объект защиты

Современное МП устройство: ИЭУ, ПЛК УСПД – это:

- Компьютерная система.
- Объект критической информационной инфраструктуры.
- Значимый объект критической информационной инфраструктуры.
- Доверенный ПАК.

- 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

ПНСТ 905-2023 КИИ. ДПАК. Термины и определения

Программно-аппаратный комплекс; ПАК: Комплекс радиоэлектронной продукции и программного обеспечения, работающих совместно для выполнения одной или нескольких определенных задач, функционально-технические характеристики которого задаются исключительно совокупностью программного обеспечения и радиоэлектронной продукции и не могут быть реализованы при их разделении.

Доверенный программно-аппаратный комплекс; ДПАК: Программно-аппаратный комплекс, соответствующий требованиям обеспечения технологической независимости критической информационной инфраструктуры, функциональности, надежности и **защищенности.**

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

пнет 905— 2023

Критическая информационная инфраструктура

ДОВЕРЕННЫЕ ПРОГРАММНО-АППАРАТНЫЕ КОМПЛЕКСЫ

Термины и определения

Издание официальное

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

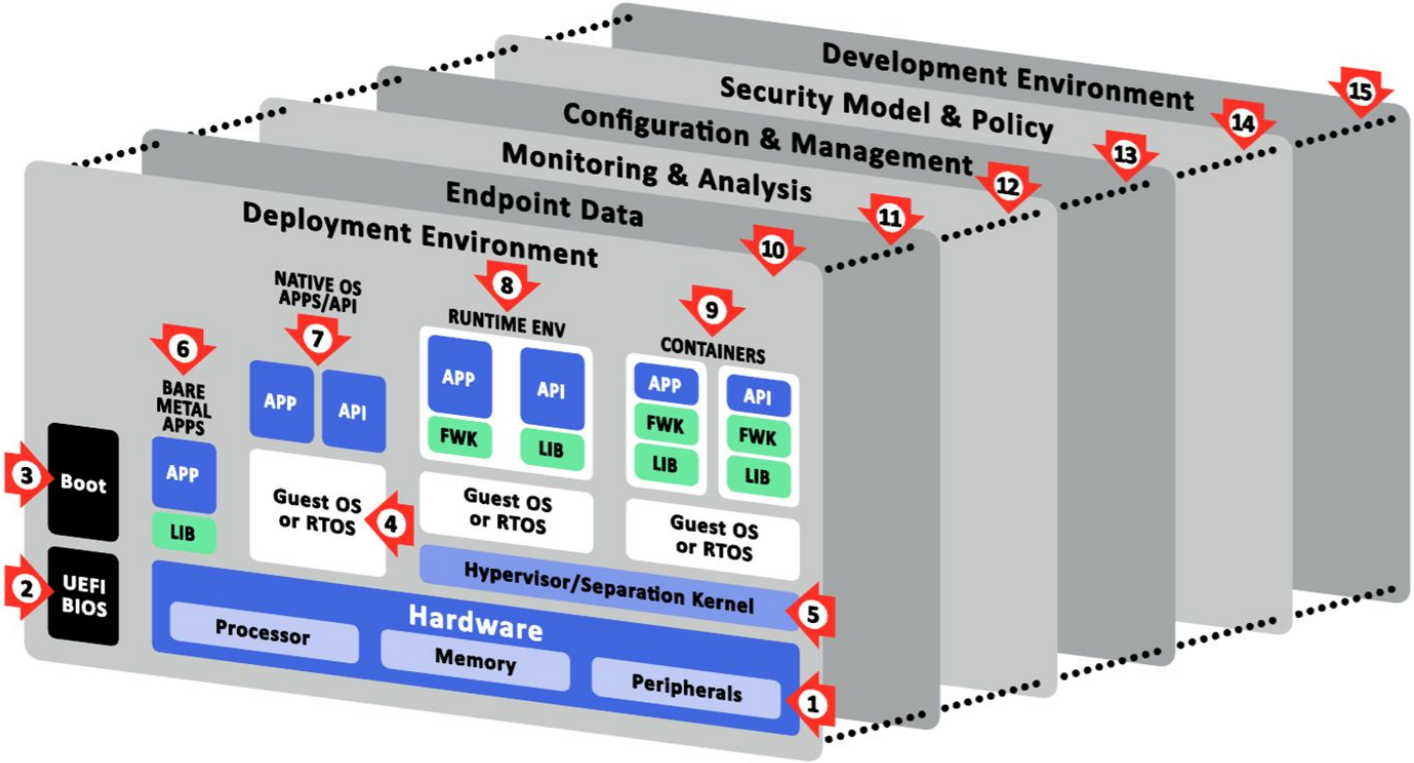
- При создании доверенных ПАК необходимо начинать с разработки модели угроз и нарушителя, после чего планомерно подбирать механизмы безопасности, которые могут помочь в противодействии выявленным угрозам и сценариям реализации атак.
- Системы должны разрабатываться с учетом анализа угроз функциональной 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.**

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

- Доверенная система: Система, для которой доказано (обосновано) соответствие целям безопасности при условии выполнения предположений безопасности. Примечание – Доверенным может быть также элемент системы.
- Конструктивный подход (к обеспечению информационной безопасности): Подход, при использовании которого системе в процессе её создания с момента замысла придаются характеристики (свойства), которые должны обеспечивать соответствие целям безопасности, включая проверку такого соответствия.
    - Проект ГОСТ Р Системы с конструктивной информационной безопасностью. Методология разработки

- Устойчивость функционирования (защищаемого объекта) определяется, как способность объекта сохранять свои основные функции с заданным качеством (в заданных пределах) под воздействием деструктивных факторов (в частности, под воздействием компьютерных атак). При этом не должно оказываться негативного влияния, выходящего за заранее заданные пределы, на жизнь и здоровье персонала, населения, на окружающую среду и т.д.» Парьев С.Е., Правиков Д.И., Карантаев В.Г., Особенности применения риск-ориентированного подхода для обеспечения кибербезопасности промышленных объектов: научный журнал Безопасность информационных технологий. Москва, 2020 – т. 27 № 4, с.37-52.

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)

ЦЕНТР КОМПЕТЕНЦИЙ НТИ
на базе НИУ "МЭИ"

- (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

Компьютерная атака - целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации;

ФЗ-187 Статья 2

Полезные международные НТД

- Международный стандарт МЭК 62443-3-3, который представлен в РФ в виде ГОСТ Р МЭК 62443-3-3-2016
- Международный стандарт IEC 62443-4-2(2019) Безопасность систем промышленной автоматизации и управления. Часть 4-2. Технические требования к безопасности компонентов IACS

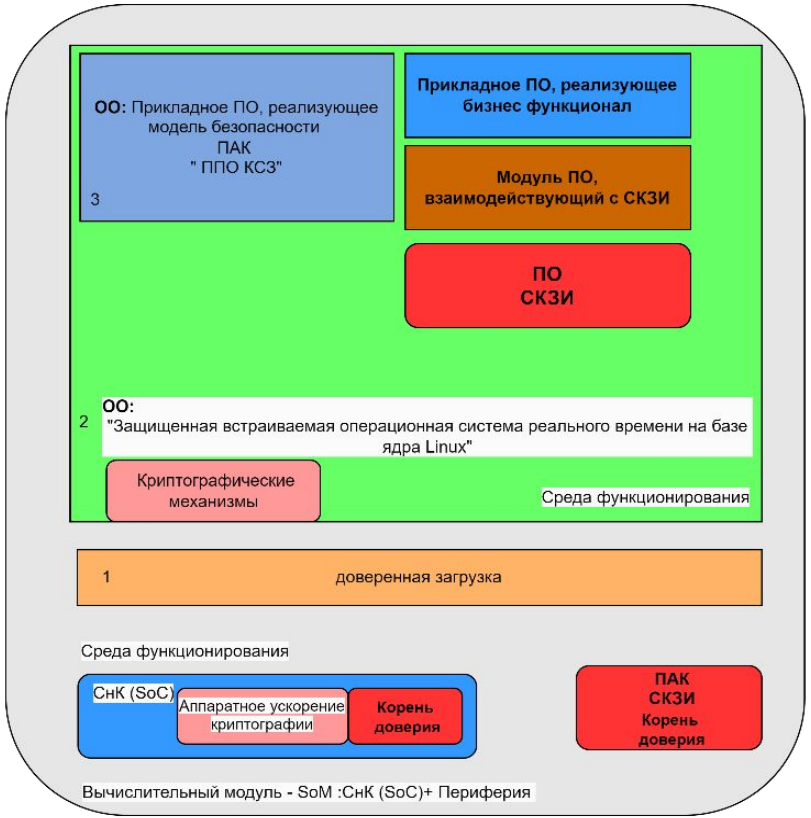
Модель нарушителя МЭК 62443 и Методика ФСТЭК России

Уровень безопасности (УБ, SL)	Вид нарушителей
УБ -1 (SL -1)	H1 Нарушитель, обладающий базовыми возможностями
УБ -2 (SL -2)	
УБ -3 (SL -3)	H2 Базовые повышенные возможности по реализации угроз безопасности информации
УБ -4 (SL -4)	H3 Средние возможности по реализации угроз безопасности информации
	H4 Высокие возможности по реализации угроз безопасности информации

Структура требований к доверенному ПАК

Функциональные требования безопасности:
Идентификация и аутентификация
Управление доступом
Контроль целостности
Регистрация событий безопасности
Доверенная загрузка
•**Нефункциональные требования:**
Время загрузки
Джиттер ЗВОС
•**Требования к тестированию и оценке соответствия:**
Внутренний пентест.
Внешний пентест.
Сертификация во ФСТЭК России.
•Требования к проектированию и производству программного обеспечения (РБПО):
Соответствие ГОСТ 56939-2024 .
Сертификация процессов РБПО в компании.

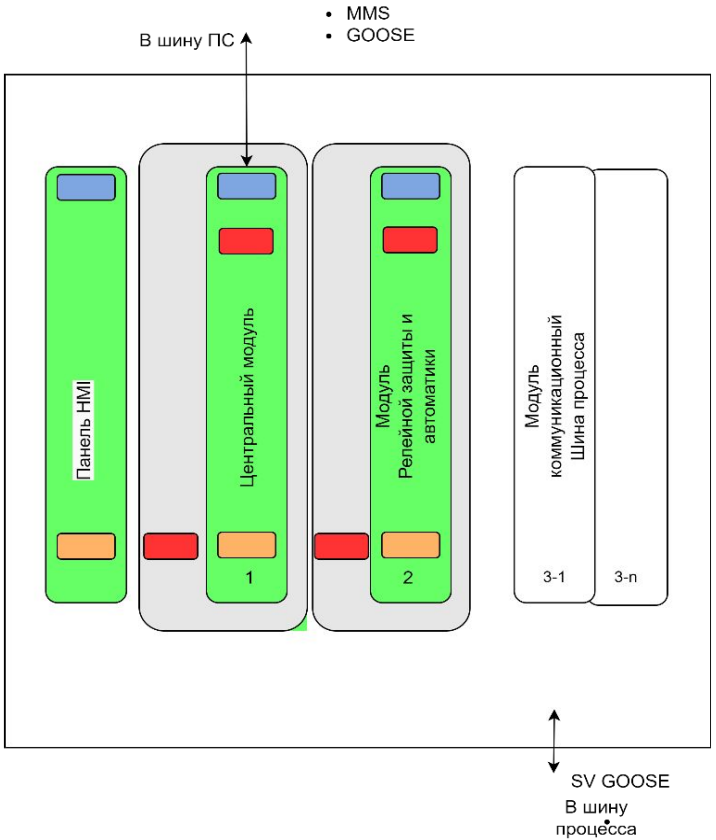
Доверенные ПАКи на инженерном языке



Комплекс средств защиты информации ДПАК:

- SoM: СнК+ Аппаратный корень доверия (СКЗИ)
- Средство доверенной загрузки (secure boot, encrypted boot)
- Защищенная встраиваемая ОС
- Прикладное ПО, реализующее ФБ
- ПО СКЗИ
- ПО, взаимодействующее с СКЗИ

Сценарии применения ВСКЗИ



- Корень доверия.
- Доверенная загрузка/Реализация цепочки доверия..
- **Удаленная «аттестация» ДПАК**
- Доверенное обновление.
- Доверенное локальное и дистанционное конфигурирование.
- Локальная и дистанционная аутентификация пользователей.

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

Поддержка необходимой аппаратной части (СнК, периферия);

- Доступность СнК на базе ISA лишенной санкционных рисков, SOM и отладочные комплекты на их основе.
- Аппаратный корень доверия и ПО для реализации доверенной загрузки.
- Защищенная OTP.
- Доверенные среды исполнения (TEE).
- Аппаратное ускорение алгоритмов криптографии Кузнечик, Магма и Стрибог.
- Ядра с частотой от 1,5 ГГц

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

- 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.
- Встраивание СКЗИ и оценка влияния СФ.

Возможные вызовы для производителей ПАК

- Готовность доказать «отечественность» своих программных продуктов, построенных на базе Open Source.
- Внедрение практик DevOps.
- Внедрение практик DevSecOps.
- Внедрение SCA (Software Composition Analysis)- анализ зависимостей в проекте.
- Готовность предоставить и управлять Software Bill of Materials.
- Готовность перенести инфраструктуру CI/CD в пределы РФ.
- Готовность поддержать ОС Linux.

Доверенный пакет поддержки плат

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

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

Требуемые компетенции

Формальные:

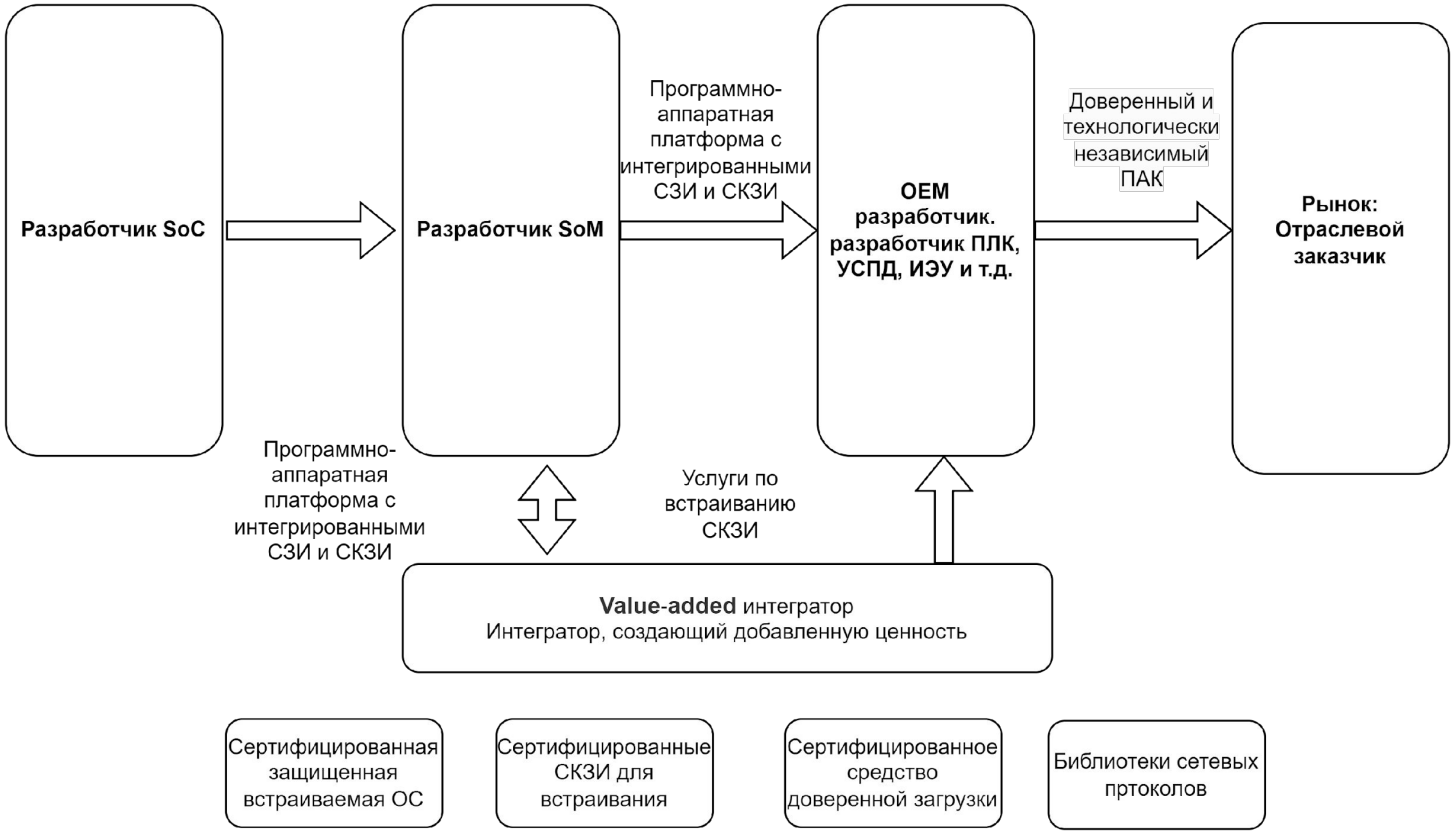
Определены требованиями, предъявляемыми при получении:

- Лицензий ФСТЭК России
  - Лицензия ФСТЭК (ТЗКИ) Лицензия ФСТЭК на деятельность по технической защите конфиденциальной информации.
  - Лицензия ФСТЭК на деятельность по разработке и производству средств защиты конфиденциальной информации.
- Лицензии ФСБ России
  - В соответствии с Постановлением Правительства РФ от 16.04.2012 N 313

Требуемые для создания доверенного ПАК:

- Разработка или применения сертифицированных СДЗ.
- Разработки или применения сертифицированных защищенных встраиваемых ОС.
- Встраивание СКЗИ и оценка влияния СФ.
- Практики РБПО.
- Реализации прикладного ПО с функциями безопасности.
- Внутренний пентест (Оценка защищенности)
- Сертификация во ФСТЭК России.

Как разработать доверенный ПАК и не сойти с ума



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).

Выводы

Для создания доверенных и технологически независимых ПАК необходимо:

- Организовать комплексную подготовку команд разработчиков существующих вендоров.
- Способствовать масштабированию применения практико-ориентированного обучения на базе универсальных УМК в корпоративных университетах и отраслевых ВУЗах.
- Рассмотреть целесообразность поддержки развития бизнес-модели отраслевых интеграторов, создающих добавленную ценность.

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

ЦЕНТР КОМПЕТЕНЦИЙ НТИ
на базе НИУ “МЭИ”

Телеграм канал Центра НТИ МЭИ

Вопросы?

Карантаев Владимир

к.т.н. KarantayevVG@mpei.ru

http://ЦДЭС.РФ