ЦЕНТР КОМПЕТЕНЦИЙ НТИ
на базе НИУ “МЭИ”

ТЕХНОЛОГИИ ТРАНСПОРТИРОВКИ
ЭЛЕКТРОЭНЕРГИИ И РАСПРЕДЕЛЕННЫХ
ИНТЕЛЛЕКТУАЛЬНЫХ ЭНЕРГОСИСТЕМ

Вопросы встраивания СКЗИ при разработке доверенных ПАК: технологии и требуемые компетенции

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

WWW.NTI.MPEI.RU

Ключевые продукты Центра НТИ МЭИ

ЦЕНТР КОМПЕТЕНЦИЙ НТИ
на базе НИУ "МЭИ"

Интеллектуальная система РЗА

Открытая АСУТП

ПАК «Цифровой двойник энергосистемы»

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

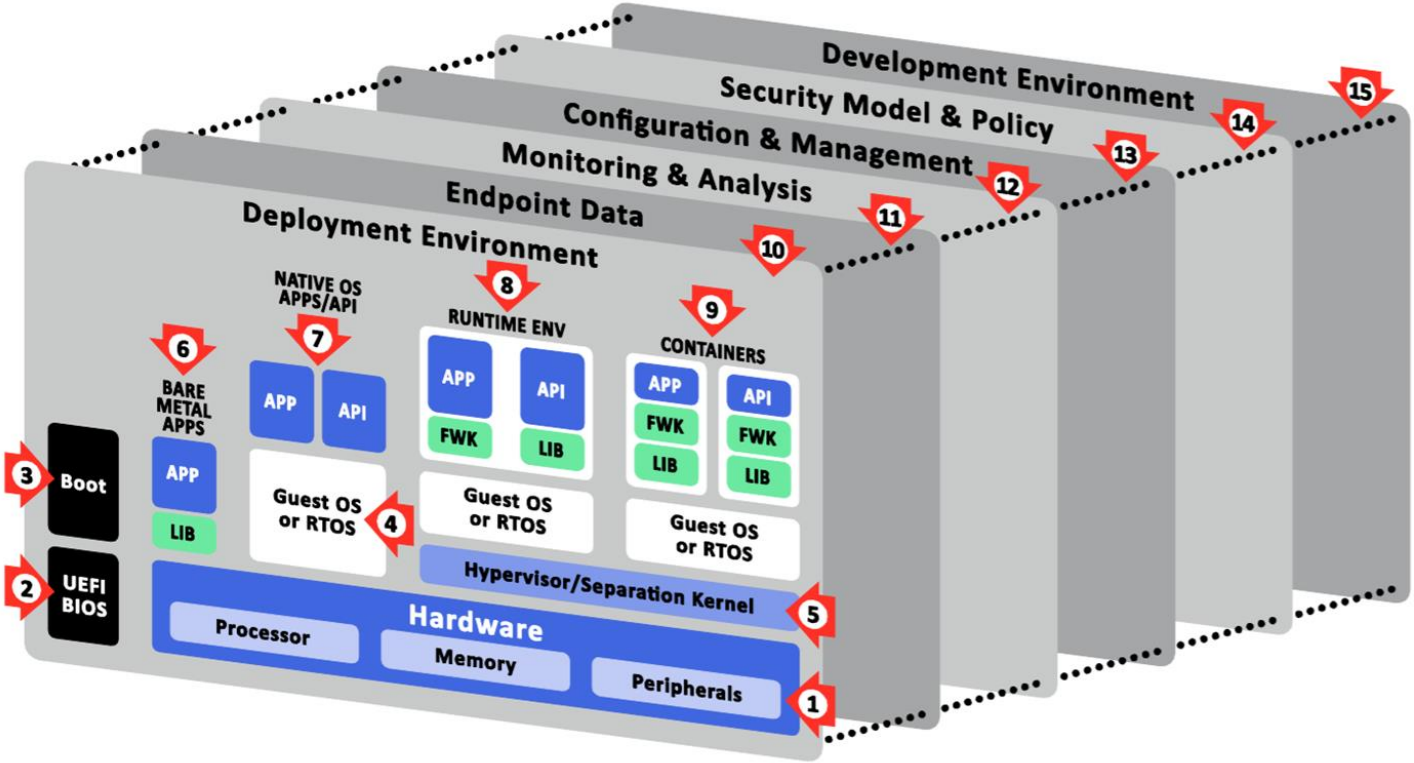
Разрабатываемые ПАКи должны стать доверенными программно-аппаратными комплексами.

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

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"

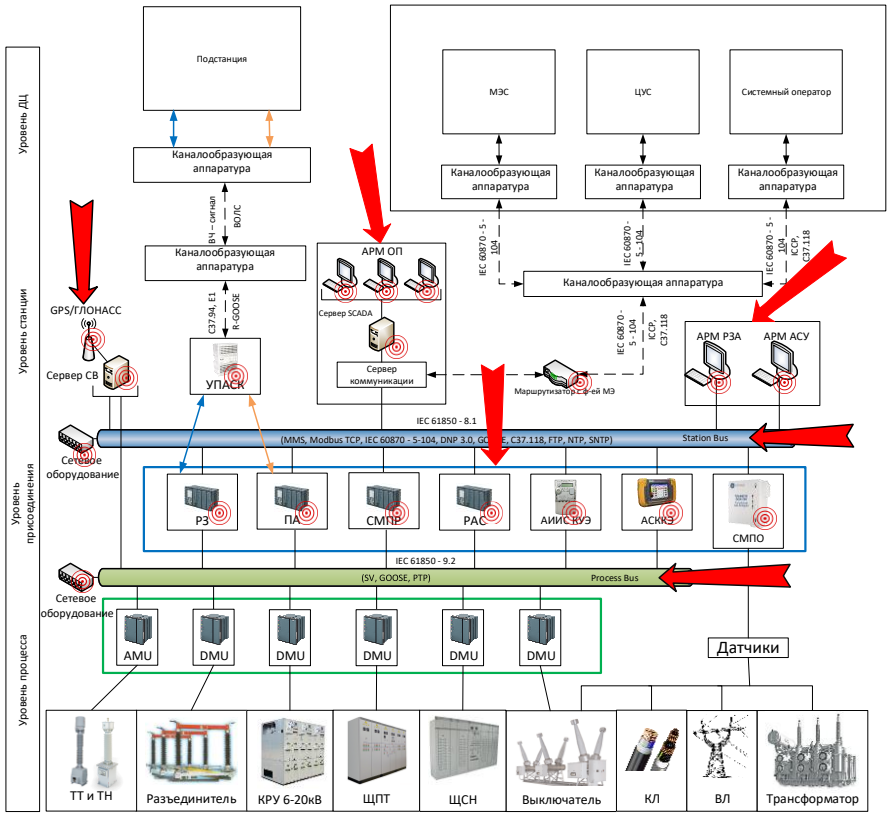
- (1) Угрозы, связанные с аппаратурой
- (2)(3) Угрозы, связанные с процессом начальной загрузки
- (4)(5) Угрозы, связанные с системным ПО
- (6)(7)(8)(9) Угрозы, связанные с прикладным ПО
- (10) Угрозы, связанные с процессом установки (развертывания) ПО
- (11) Угрозы, связанные с доступом к данных ПЛК
- (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

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

Угрозы, которые могут быть нейтрализованы только с помощью СКЗИ

В соответствии с «**Базовой моделью угроз безопасности информации в интеллектуальных системах учёта электрической энергии (мощности)».**

разработанной Министерством энергетики Российской федерации совместно с Федеральной службой безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю и Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации, определены угрозы, которые могут быть нейтрализованы только с помощью СКЗИ:

– УБИ.0692 - Угроза неправомерных действий в каналах связи: при передаче данных (информации) по каналам связи (включая каналы связи между сегментами ИВК в случае распределенной архитектуры ИВК), не защищенным от перехвата нарушителем, передаваемой по ним информации или от несанкционированных воздействий на эту информацию; Перечень передаваемой информации приведен в разделе 3.4;

– УБИ.083 - Угроза несанкционированного доступа к системе по беспроводным каналам: при передаче данных (информации) по беспроводным каналам связи, не защищенным от перехвата нарушителем, передаваемой по ним информации или от несанкционированных воздействий на эту информацию.

https://docs.cntd.ru/document/607167779

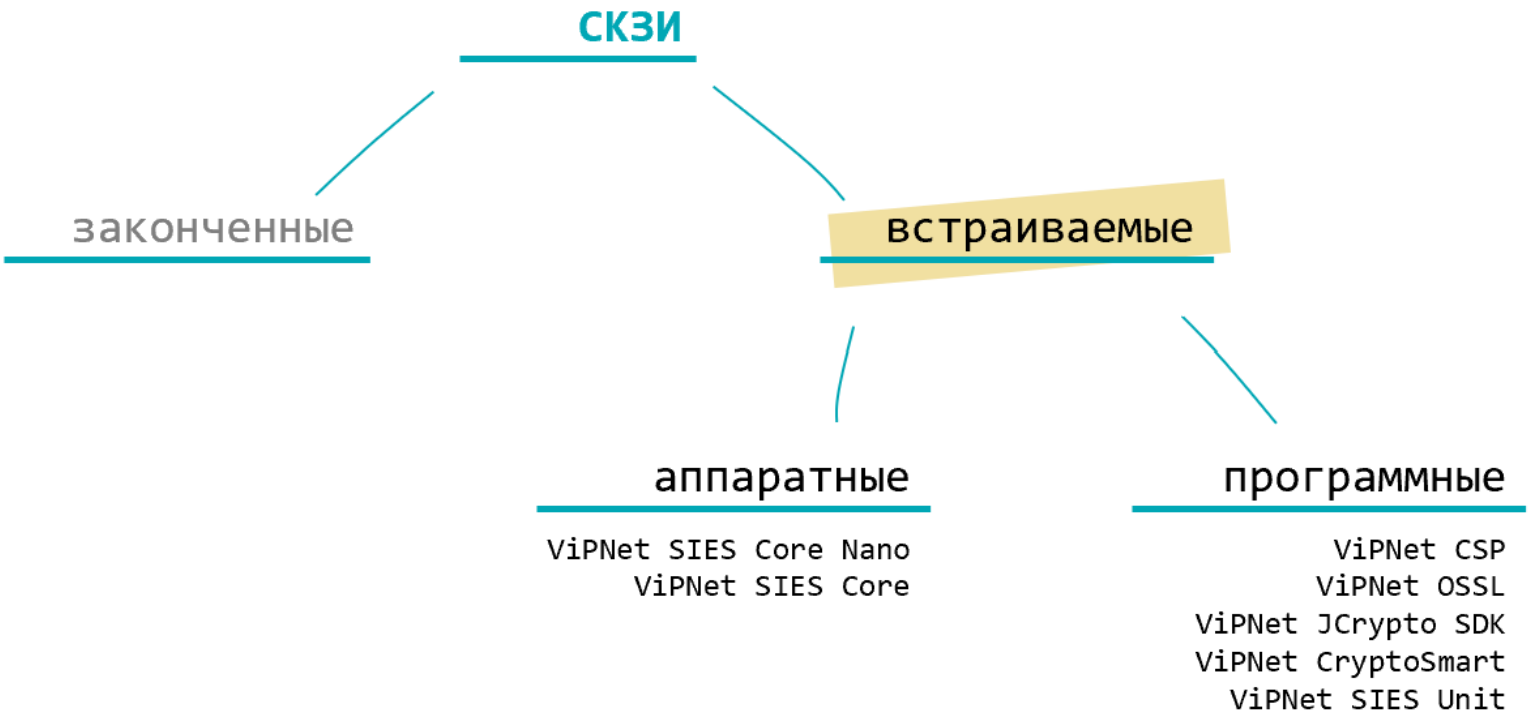
Методология разработки доверенных ПАК (ПЛК, РСУ, ПАЗ, ИЭУ) на основе принципа Secure by Design

- 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.**

Структура требования к доверенному ПАК

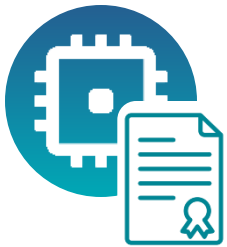
- Функциональные требования безопасности.
- Нефункциональные требования.
- Требования к тестированию и оценке соответствия.
- Требования к проектированию и производству программного обеспечения (РБПО).

Виды СКЗИ

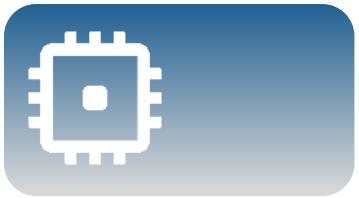


https://infotecs.ru/upload/iblock/f41/wcj2uxserfom4nqgxinkg5lzsxzdmlmi.pdf

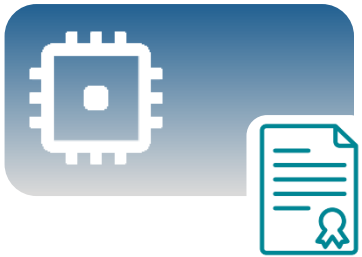
Встраивание СКЗИ



1 Найти сертифицированное СКЗИ



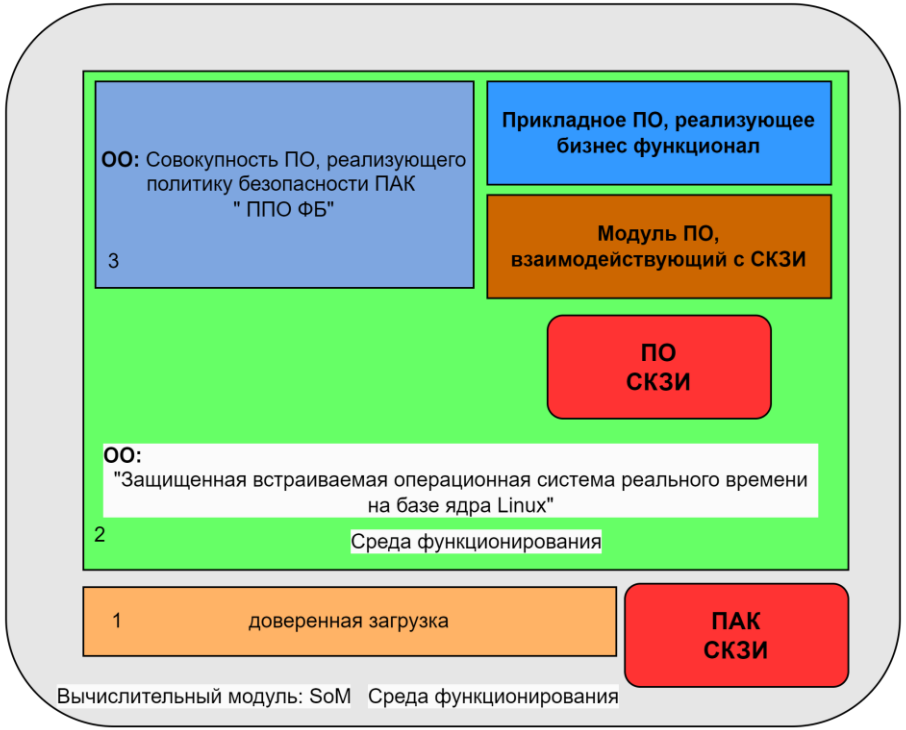
2 Встроить СКЗИ в ПО или ПАК



3 Провести оценку влияния

https://infotecs.ru/upload/iblock/f41/wcj2uxserfom4nqgxinkg5lzsxzdmlmi.pdf

Доверенные ПАКи на инженерном языке



- Средство доверенной загрузки
- Защищенная встраиваемая ОС
- Прикладное ПО, реализующее ФБ
- СКЗИ
- ПО, взаимодействующее с СКЗИ

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.
- Встраивание СКЗИ и оценка СФ.

Разработка безопасного программного обеспечения (РБПО) для ПАК АСУ

Обучение

Выбор и обоснование применения СКЗИ

Испытания на быстродействие РЗА

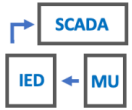
Разработка требований с учетом специфики РЗА

Анализ состава и свойств применяемых библиотек от сторонних поставщиков

Функциональные испытания РЗА

Определение измеримых целевых показателей

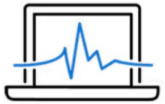
Внедрение и применение доверенных средств разработки ПО



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

Требуемые компетенции

Формальные:

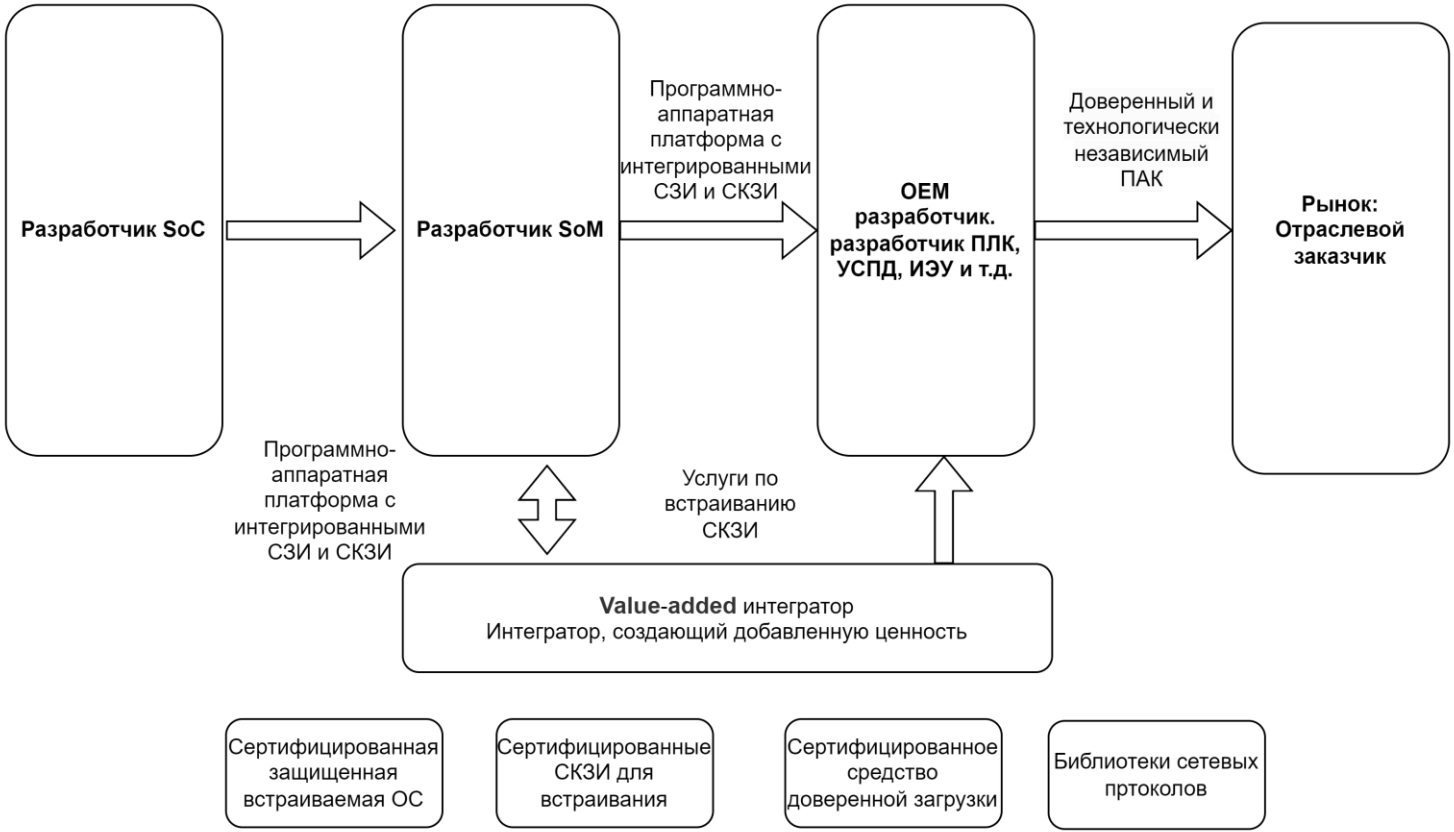
Определены требованиями, предъявляемыми при получении:

- 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:

- Разработки 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.
- Сертификация во ФСТЭК России.

Как разработать доверенный ПАК и не сойти с ума



О Лаборатории ВСКЗИ АСУ ОЭ

ЦЕНТР КОМПЕТЕНЦИЙ НТИ
на базе НИУ "МЭИ"

Создание Лаборатории ВСКЗИ АСУ ОЭ является результатом многолетнего партнерства НИУ МЭИ и отечественного разработчика средств криптографической защиты информации (СКЗИ) АО «ИнфоТеКС».

В новом пространстве студенты НИУ МЭИ и сотрудники компаний-производителей комплексов АСУ, АСУ ТП, ИСУЭ, РЗА и др. смогут получить практические навыки разработки доверенных программно-аппаратных комплексов с применением решения ViPNet SIES.

Лаборатория входит в состав Центра экспертизы в практической кибербезопасности Центра НТИ МЭИ и объединяет в себе накопленный опыт АО «ИнфоТеКС» и НИУ МЭИ в области криптографической защиты информации и создания доверенных программно-аппаратных комплексов для обеспечения кибербезопасности объектов электроэнергетики.

ЦЕНТР КОМПЕТЕНЦИЙ НТИ
на базе НИУ "МЭИ"

Об учебном курсе

Учебный курс **«Введение в разработку защищенных ИСУЭ и АСУ ТП с использованием ViPNetSIES»** практико-ориентированная образовательная инициатива, разработанная на основе результатов партнерства НИУ МЭИ и одного из ведущих вендоров в области криптографической защиты информации – АО «ИнфоТеКС».

Курс рассматривает теоретические и практические аспекты использования программно-аппаратных комплексов на базе ViPNet SIES, а также вопросы практической разработки функций безопасности доверенных программно-аппаратных комплексов (ПЛК, УСПД и др.) в соответствии с методикой использования продуктов ViPNet SIES, разработанной на кафедре РЗиАЭ НИУ МЭИ с учетом специфики отрасли электроэнергетики.

Дата очередного курса: ноябрь 2024.
Учебных часов по программе: 72 ч.
Режим обучения: 5 рабочих дня по 8 академических часов в день.
Обучение проходит с 10.00 ч. до 17.00 ч.
Формат обучения: очный, с отрывом от работы

Уникальность:
Доступ к экспертам АО «ИнфоТеКС» во время ежедневных Q&A сессий.

ЦЕНТР КОМПЕТЕНЦИЙ НТИ
на базе НИУ "МЭИ"

Как масштабировать?

Разработан типовой Учебно-методический комплекс для Лабораторий ВСКЗИ АСУ ОЭ. УМК оснащен необходимым современным оборудованием, комплексом программного обеспечения и методическими материалами:

- АРМ Обучаемого
- АРМ Руководителя учебного курса
- АРМ Администратора Лаборатории
- Учебный стенд на основе ПЛК АРКС400.Р410 (ООО «НВТ-Системы») со встроенным программно-аппаратным комплексом СКЗИ ViPNet SIES Core;
- Компоненты решения ViPNet SIES.

Предлагаем распространить использование **УМК** на:

- Корпоративные университеты энергокомпаний
- Отраслевые ВУЗы

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

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