

ЦЕНТР КОМПЕТЕНЦИЙ НТИ на базе НИУ "МЭИ"

ТЕХНОЛОГИИ ТРАНСПОРТИРОВКИ
ЭЛЕКТРОЭНЕРГИИ И РАСПРЕДЕЛЕННЫХ
ИНТЕЛЛЕКТУАЛЬНЫХ ЭНЕРГОСИСТЕМ

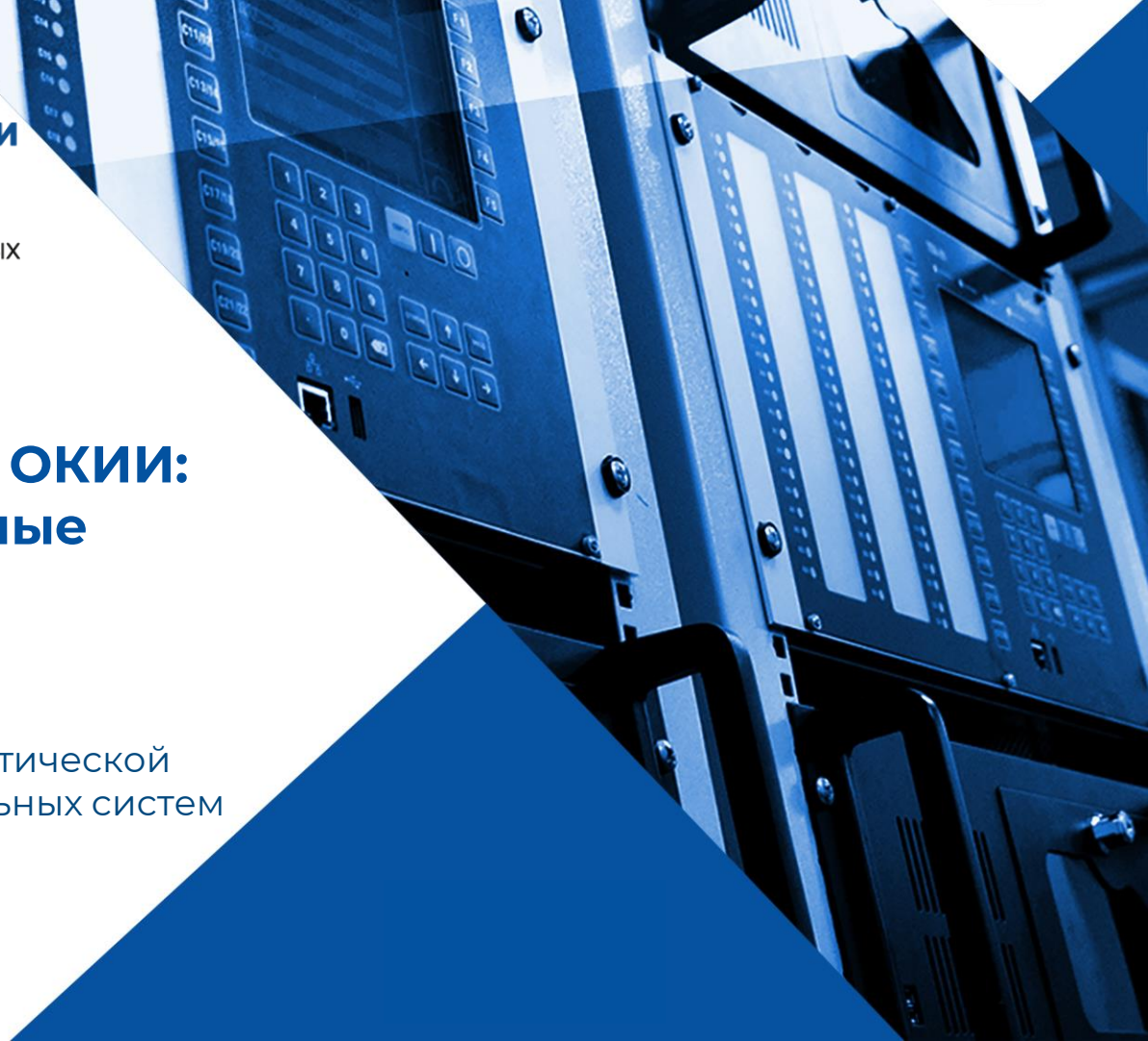
Вопросы разработки доверенных ПАК АСУ ОКИИ: технологии и требуемые компетенции

Владимир Карантаев

К.Т.Н.

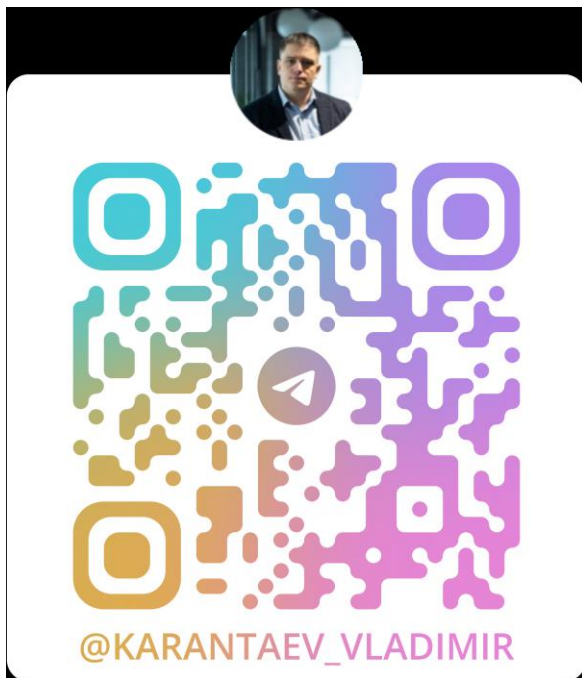
Лидер центра экспертизы практической
кибербезопасности промышленных систем
Центра НТИ МЭИ

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

Ключевые продукты Центра НТИ МЭИ

Интеллектуальная система РЗА



Открытая АСУТП



ПАК «Цифровой двойник энергосистемы»



Современные ПЛК:

- CPU
- Оперативная память
- Энергонезависимая память (Flash)
- Сетевые интерфейсы Ethernet
- BIOS/UEFI
- Операционная система (например, Linux)
- Системное ПО
- Прикладное ПО
- ЖК экран



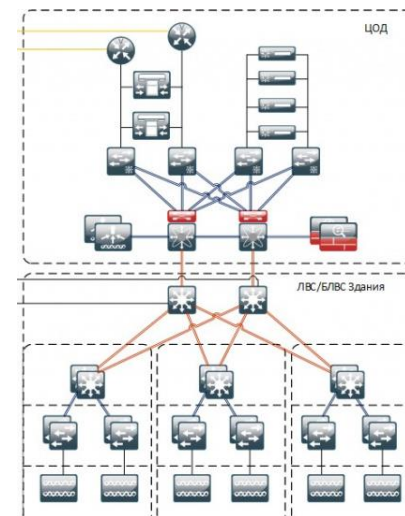
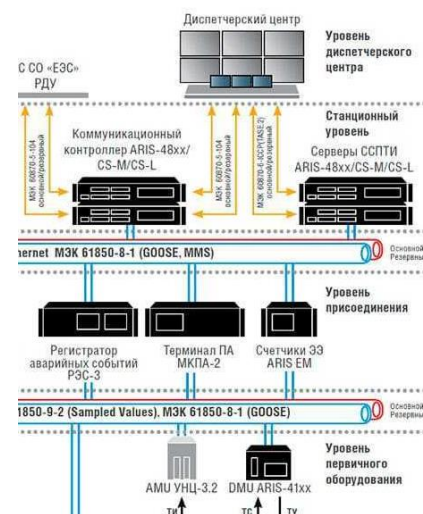
Это ПЛК или не ПЛК?

Практические задачи, которые мы решали:

- **Основная задача** – разработать прототип ПЛК АСУ ТП ОА.
- Оценить риски возникновения технологической зависимости.

Связанные задачи:

- Выбор СНК, выбор архитектуры
- Операционная система
- Загрузчик
- Набор инструментов разработчика
- Эмуляторы и аппаратные средства для тестирования.



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**).

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

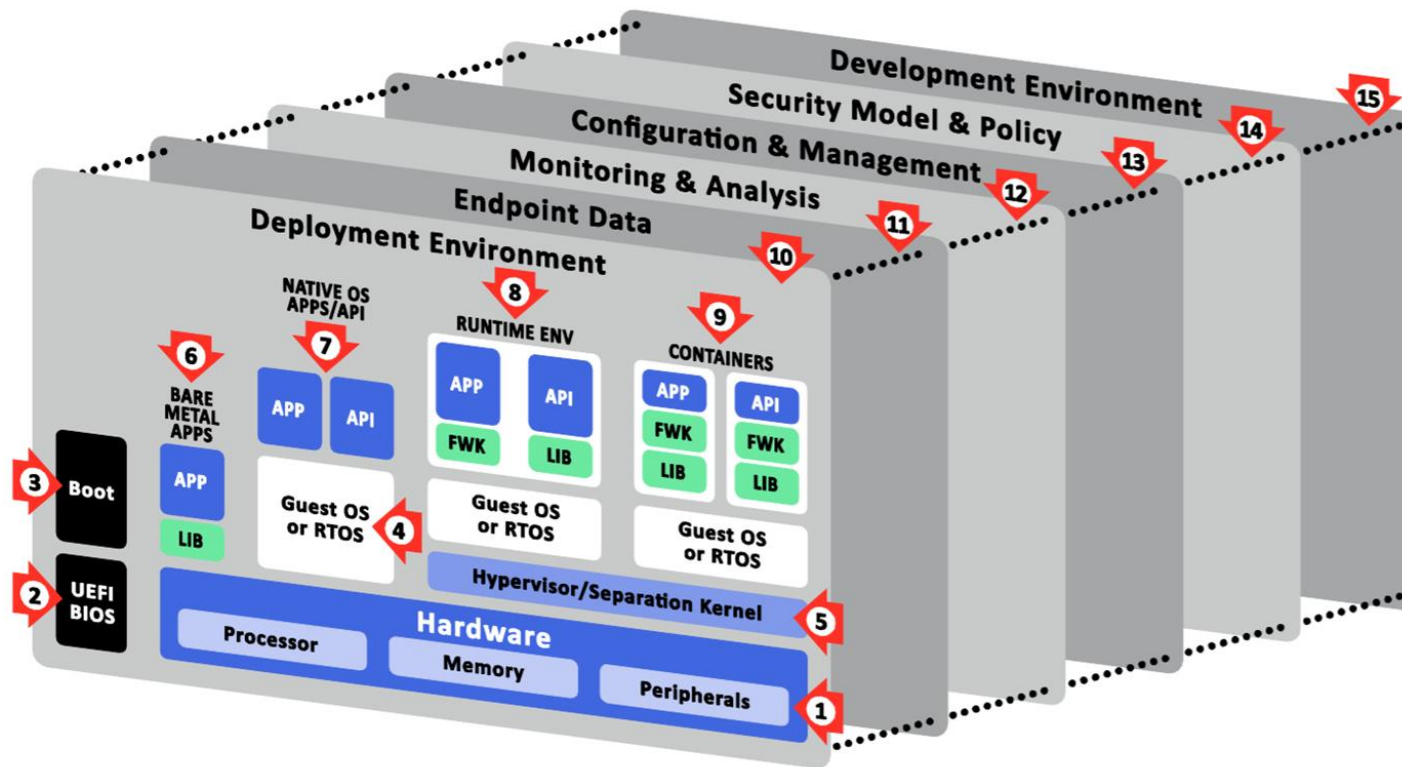
- При создании доверенных ПАК необходимо начинать с разработки модели угроз и нарушителя, после чего планомерно подбирать механизмы безопасности, которые могут помочь в противодействии выявленным угрозам и сценариям реализации атак.
- Системы должны разрабатываться с учетом анализа угроз функциональной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



ЦЕНТР КОМПЕТЕНЦИЙ НТИ
на базе НИУ "МЭИ"



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 данным 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;

Виды возможных атак

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

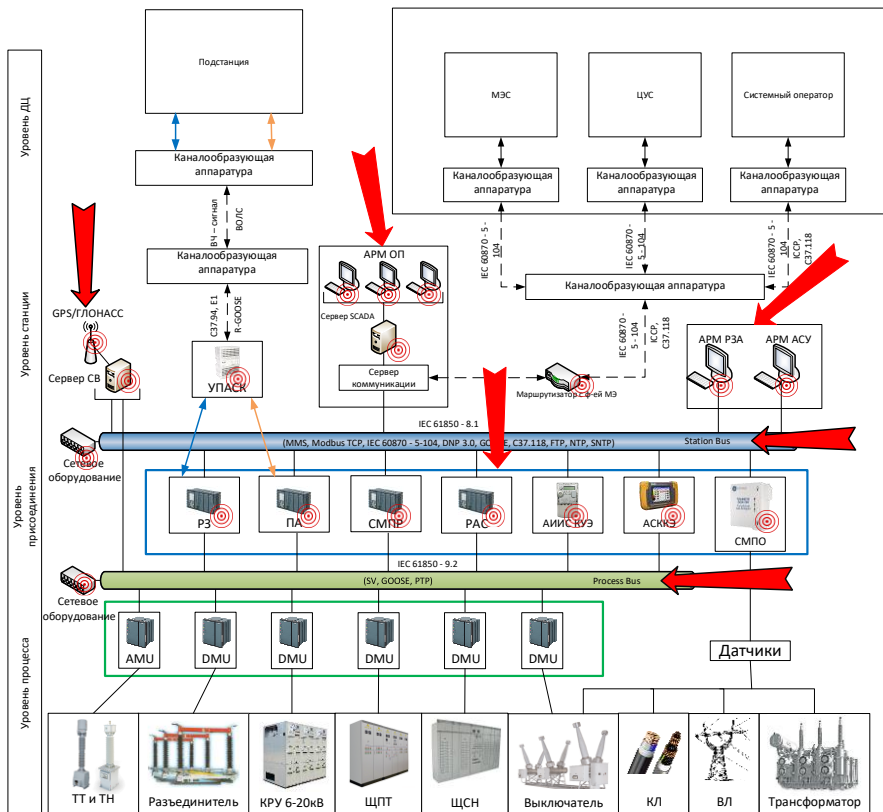
Возможные векторы воздействия



Атаки на Endpoints



Атаки на протоколы





- 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



ЦЕНТР КОМПЕТЕНЦИЙ НТИ
на базе НИУ "МЭИ"

Уровень безопасности (УБ, SL)	Определение	Средства	Ресурсы	Навыки	Мотивация
УБ -1 (SL -1)	Предотвращать неавторизованное раскрытие информации посредством ее несанкционированного извлечения или случайного обнародования;	простые	низкие	общие	низкая
УБ -2 (SL -2)	Предотвращать неавторизованное раскрытие информации субъекту, активно ее ищущему с использованием простых средств, при незначительных ресурсах, посредственных навыках и низкой мотивации;				
УБ -3 (SL -3)	Предотвращать неавторизованное раскрытие информации субъекту, активно ее ищущему с использованием изощренных средств при умеренных ресурсах, наличии специальных познаний в IACS и умеренной мотивации;	изощрённые	умеренные	специальные	умеренная
УБ -4 (SL -4)	Предотвращать неавторизованное раскрытие информации субъекту, активно ее ищущему с использованием изощренных средств при обширных ресурсах, наличии специальных познаний в IACS и высокой мотивации.		обширные	специальные	высокая мотивация

Модель нарушителя МЭК 62443 и Методика ФСТЭК России



ЦЕНТР КОМПЕТЕНЦИЙ НТИ
на базе НИУ "МЭИ"

Уровень безопасности (УБ, SL)	Вид нарушителей
УБ -1 (SL -1)	Н1 Нарушитель, обладающий базовыми возможностями
УБ -2 (SL -2)	
УБ -3 (SL -3)	Н2 Базовые повышенные возможности по реализации угроз безопасности информации
УБ -4 (SL -4)	Н3 Средние возможности по реализации угроз безопасности информации
	Н4 Высокие возможности по реализации угроз безопасности информации

Структура требований к доверенному ПАК



ЦЕНТР КОМПЕТЕНЦИЙ НТИ
на базе НИУ "МЭИ"



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:

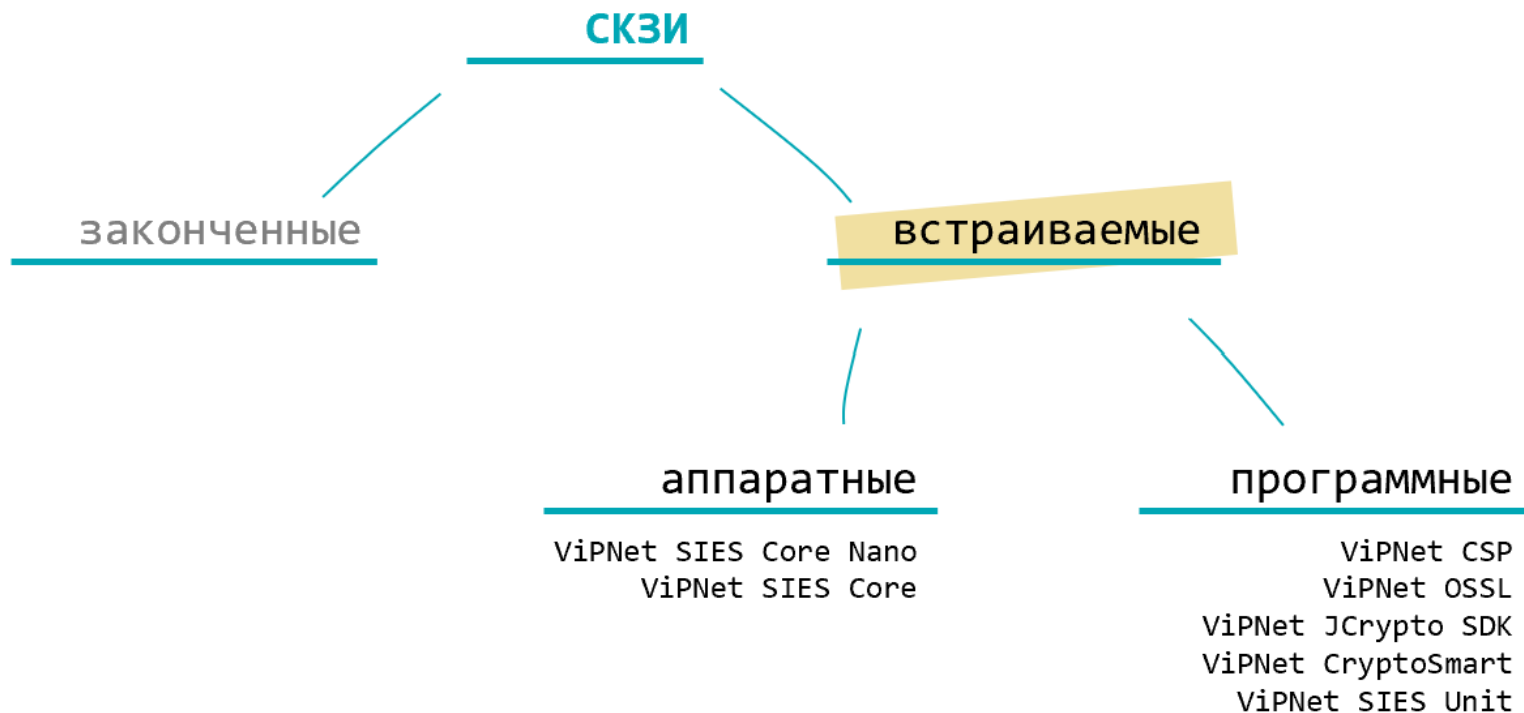
- Внутренний пентест.
- Внешний пентест.
- Сертификация во ФСТЭК России.
- Требования к проектированию и производству программного обеспечения (РБПО):
- Соответствие ГОСТ 56939-2024 .
- Сертификация процессов РБПО в компании.



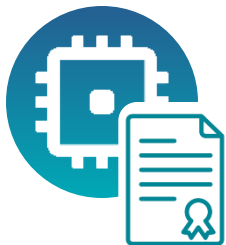
Структура вимог до довіреного ПАК

FR 1 – Identification and authentication control (IAC)		
Component requirement ,Requirement enhancement	УБ-3 (CR-12 RE - 5 EDR - 0)	УБ-4 (CR- 12 RE -7 EDR - 0)
FR 2 – Use control (UC)		
Component requirement ,Requirement enhancement	УБ-3 (CR-11 SAR -1 RE - 8 EDR - 2)	УБ-4 (CR- 11 SAR -1 RE - 11 EDR - 2)
FR 3 – System integrity (SI)		
Component requirement ,Requirement enhancement	УБ-3 (CR-8 RE - 8 EDR - 6)	УБ-4 (CR- 8 RE -11 EDR - 6)
FR 4 – Data confidentiality (DC)		
Component requirement ,Requirement enhancement	УБ-3 (CR-3 RE - 2 EDR - 0)	УБ-4 (CR-3 RE - 2 EDR - 0)
FR 5 – Restricted data flow (RDF)		
Component requirement ,Requirement enhancement	УБ-3 (CR-1 RE - 1 EDR - 0)	УБ-4 (CR-1 RE - 1 EDR - 0)
FR 6 – Timely response to events (TRE)		
Component requirement ,Requirement enhancement	УБ-3 (CR-2 RE - 1 EDR - 0)	УБ-4 (CR-2 RE - 1 EDR - 0)
FR 7 – Resource availability (RA)		
Component requirement ,Requirement enhancement	УБ-3 (CR-7 RE - 4 EDR - 0)	УБ-4 (CR-7 RE - 4 EDR - 0)

Виды СКЗИ

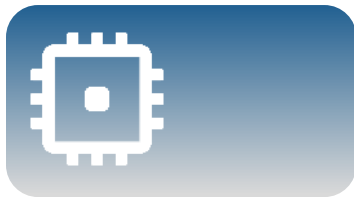


Встраивание СКЗИ



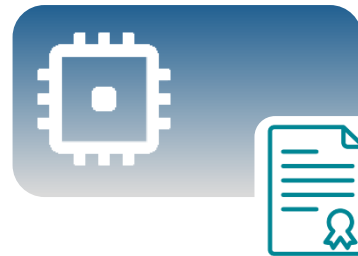
1

Найти
сертифицированное
СКЗИ



2

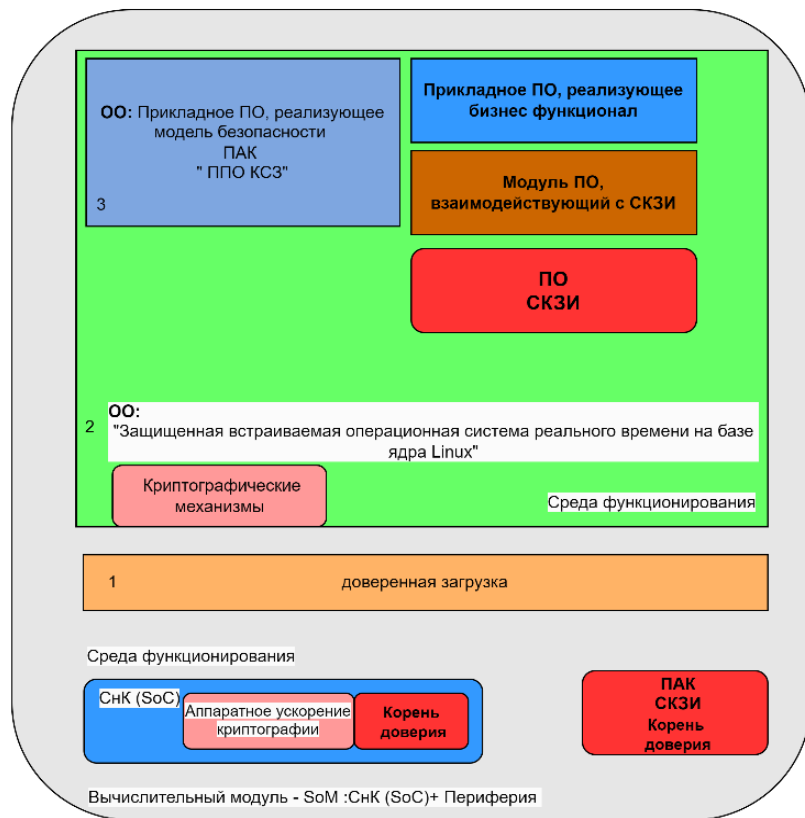
Встроить СКЗИ
в ПО или ПАК



3

Провести
оценку влияния

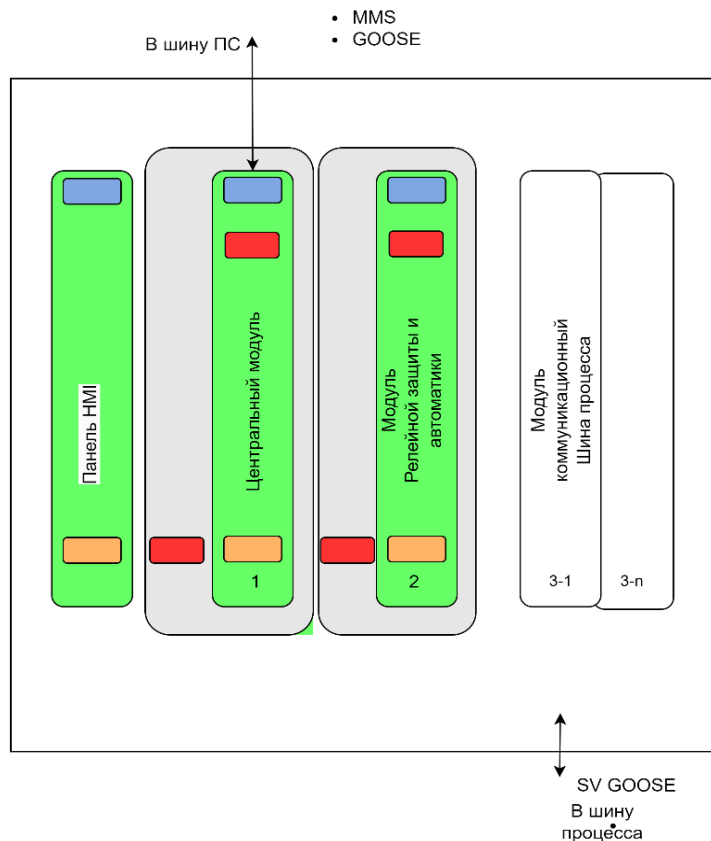
Доверенные ПАКи на инженерном языке



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);
 - Аппаратный корень доверия и ПО для реализации доверенной загрузки
- 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 поддерживать ОС Linux.





РБПО: суммарно 25 процессов,
из них 8 – новые относительно ГОСТ Р 56939-2016

- Инициализация и планирование процессов разработки безопасного программного обеспечения
- Формирование и поддержание в актуальном состоянии правил кодирования
- Обеспечение целостности кода при разработке программного обеспечения
- Обеспечение информационной безопасности используемых секретов и ключей подписи, а также процесса электронной подписи кода
- Использование инструментов композиционного анализа
- Проверка собранного бинарного кода на предмет наличия признаков внедрения вредоносного кода через цепочки поставок
- Безопасная доставка программного обеспечения пользователям
- Обеспечение безопасности при выводе программного обеспечения из эксплуатации
- Добавлены требования по обязательному наличию IT-инфраструктуры
- Управление версиями, Bug tracking / управление заданиями, CI/CD
- 25 января 2024 года завершено общественное обсуждение
- <https://fstec.ru/tk-362/standarty/proekty/proekt-natsionalnogo-standarta-gost-r-56939>



Порядок сертификации процессов безопасной разработки программного обеспечения средств защиты информации

утвержден приказом ФСТЭК России
от 1 декабря 2023 г. № 240

вступает в силу с 1 июня 2024 г.

Пункт 71.1 Положения о системе сертификации СЗИ (утверждено приказом ФСТЭК России от 3 апреля 2018 г. № 55) Предоставляет право разработчику самостоятельно проводить испытания СЗИ в случае внесения в сертифицированное СЗИ изменений, в том числе изменений, связанных с добавлением новых функций безопасности информации, или изменений в имеющиеся функции безопасности информации, с обновлением версий ПО, включая совершенствование функций его безопасности или добавления новых функций безопасности, а также с добавлением новых или изменением существующих аппаратных платформ.

Национальный стандарт ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования»

Доверенный пакет поддержки плат



ЦЕНТР КОМПЕТЕНЦИЙ НТИ
на базе НИУ "МЭИ"

Пакет поддержки плат (BSP) должен содержать 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;

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



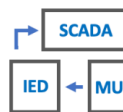
Функциональные испытания РЗА



Определение измеримых целевых показателей



Внедрение и применение доверенных средств разработки ПО



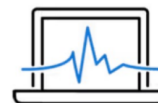
Испытания на соответствие МЭК 61850



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:

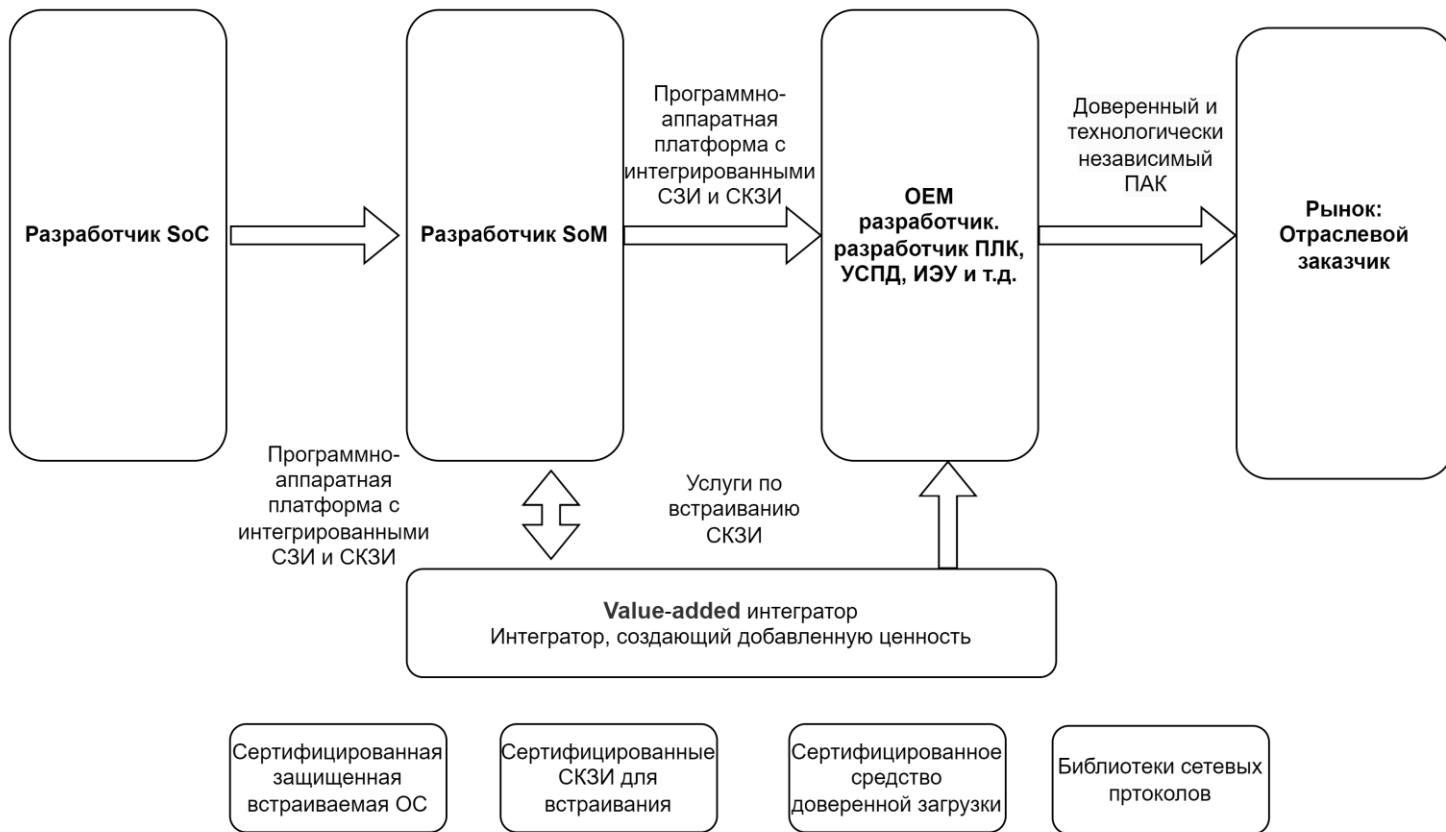
Определены требованиями, предъявляемыми при получении:

- 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:

- 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



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.





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.





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.P410 (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





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).



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



Telegram 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>