ЦЕНТР НТИ МЭИ

ТЕХНОЛОГИИ ТРАНСПОРТИРОВКИ
ЭЛЕКТРОЭНЕРГИИ РАСПРЕДЕЛЕННЫХ
ИНТЕЛЛЕКТУАЛЬНЫХ ЭНЕРГОСИСТЕМ

Разработка автоматизированных систем объектов электроэнергетики с применением встраиваемых СКЗИ и вопросы подготовки кадров

Владимир Карантаев
к.т.н., доцент
MBA

WWW.NTI.MPEI.RU

Визитка: Владимир Карантаев

Практик

Стаж деятельности в области ИТ и ИБ - 20 лет (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

Структура доклада

- Программа прикладных исследований Центра НТИ МЭИ
- Теория и практика применения встраиваемых СКЗИ в АСУ
- Вопросы подготовки специалистов

ЦЕНТР НТИ МЭИ

ТЕХНОЛОГИИ ТРАНСПОРТИРОВКИ
ЭЛЕКТРОЭНЕРГИИ РАСПРЕДЕЛЕННЫХ
ИНТЕЛЛЕКТУАЛЬНЫХ ЭНЕРГОСИСТЕМ

Программа прикладных исследований Центра НТИ МЭИ

WWW.NTI.MPEI.RU

Деятельность ЦК НТИ МЭИ

Научно-исследовательское направление:

- Выполнение научно-исследовательских работ по программе ЦК НТИ
- Выполнение НИОКР по заказу организаций реального сектора экономики
- Трансфер разработанных технологий

Образовательное направление:

- Новые основные образовательные программы
- Программы дополнительного профессионального образования
- Учебно-методическая деятельность

Инфраструктурное направление:

- Центр коллективного пользования
- Лаборатория информационной безопасности
- Полигон интеллектуальных систем управления микрогрид
- Переносные комплексы для определения реальных характеристик электроэнергетического оборудования

Направления прикладных исследований

Оценка влияния компьютерных инцидентов на устойчивость функционирования цифровых объектов электроэнергетического комплекса

Изучение существующих методов оценки угроз кибербезопасности.

Развитие отраслеориентированных методов оценки угроз кибербезопасности.

Построение имитационных математических моделей

Построение полунатурных моделей

Применение методов искусственного интеллекта для обеспечения устойчивого и безопасного функционирования автоматизированными и автоматическими системами цифровых подстанций.

Разработка Системы поддержки принятия решений, экспертные системы с использованием онтологического подхода

Методы машинного обучения

Направления прикладных исследований

Оценка эффективности использования встраиваемых средств криптографической защиты информации в автоматизированных и автоматических системах объектов критической информационной инфраструктуры объектов электроэнергетики:

- АСУ ТП
- РЗА
- АИСКУЭ (ИСУЭ)

Анализ оптимальности построения применяемых и перспективных архитектур ЦПС с точки зрения влияния на них факторов угроз кибератак.

Анализ оптимальности применяемых и перспективных архитектур построения IED (терминал РЗА) с точки зрения влияния на них факторов угроз кибератак.

- Встраиваемые ОС
- Механизмы безопасности

Вопросы внедрения центров по мониторингу и реагированию на инциденты ИБ в субъектах электроэнергетики, как части общей системы ситуационной осведомленности.

План 2023:

Создание специализированной лаборатории практической кибербезопасности:

- Теория и практика использования встраиваемых СКЗИ:

  Системы коммерческого учета (ИСУЭ)

  Системы РЗА

- Развитие и внедрение практик разработки безопасного программного обеспечения.

Перспективные направления работ и исследований:

- Разработка и использование распределенных инфраструктур ложных целей в системах управлениях Цифровой энергетики.
- Изучение вариантов развития технологий программно-аппаратных комплексов «песочницы» для применения в инфраструктуре индустриальных систем управления.
- Встраиваемые реалтайм операционные системы с реализованными механизмами безопасности.
- Анализ угроз БИ и формирование мер защиты для инфраструктуры электрозарядных станции, ЭЗС.

ЦЕНТР НТИ МЭИ

ТЕХНОЛОГИИ ТРАНСПОРТИРОВКИ
ЭЛЕКТРОЭНЕРГИИ РАСПРЕДЕЛЕННЫХ
ИНТЕЛЛЕКТУАЛЬНЫХ ЭНЕРГОСИСТЕМ

Теория и практика применения встраиваемых СКЗИ в АСУ

WWW.NTI.MPEI.RU

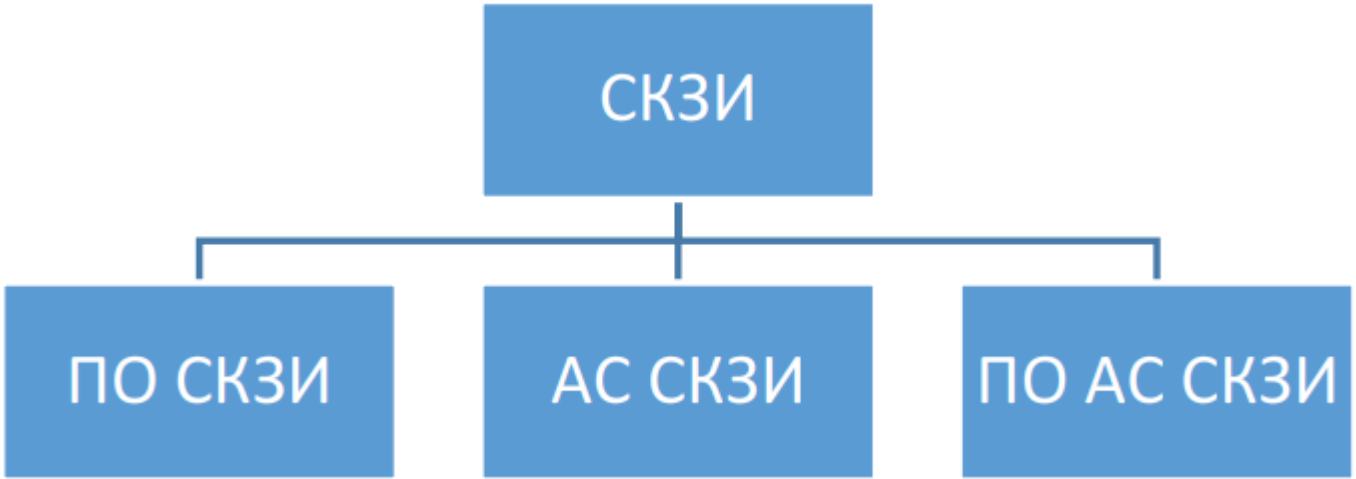
Сценарии применения встраиваемых СКЗИ

- Криптографическая защита информации при информационном обмене:

Протоколы: MMS, МЭК 60870-5-104, R-GOOSE, DLMS, GOOSE

- Реализация встроенных механизмов безопасности: статический контроль целостности.
- Строгая аутентификация на устройствах ЦПС (ИЭУ)
- Реализация ролевой модели управления (RBAC) доступом к ЗОКИИ ЦПС (Подсистеме РЗА).
- Предотвращение атак на цепочку поставки.
- Удаленная аттестация устройств.

Средство криптографической защиты информации

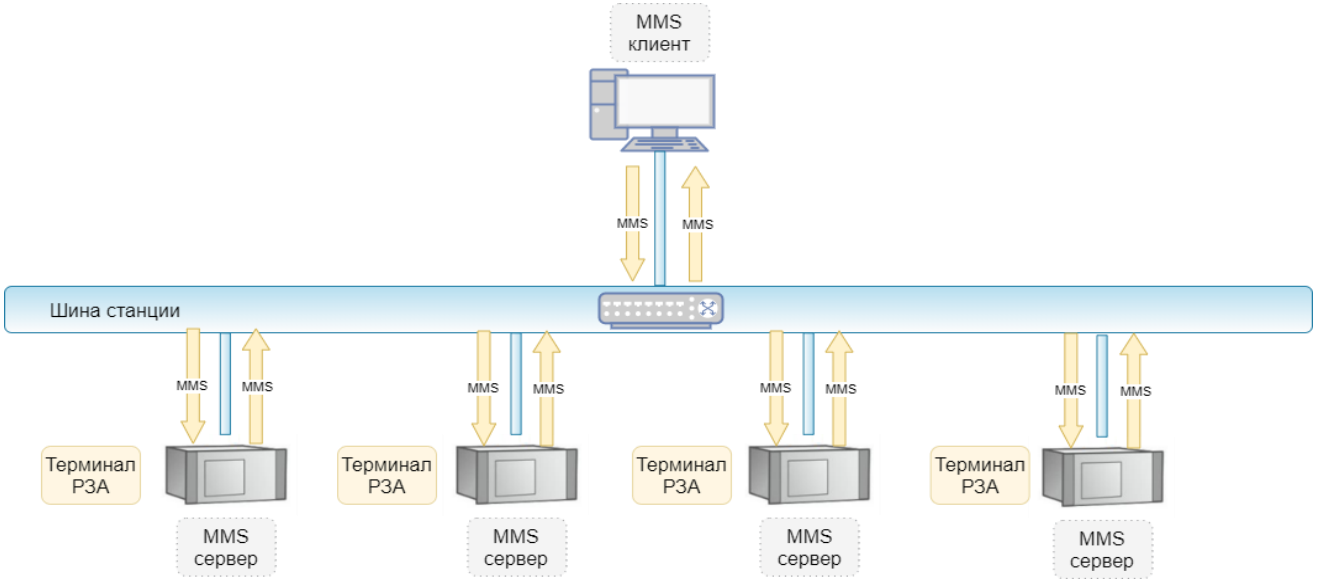


Средство криптографической защиты информации; СКЗИ:
Шифровальное (криптографическое) средство, предназначенное для защиты информации, не содержащей сведений, составляющих государственную тайну, и представляющее собой совокупность одной или нескольких составляющих:
- программного обеспечения (ПО СКЗИ);
- аппаратных средств (АС СКЗИ);
- программного обеспечения аппаратных средств (ПО АС СКЗИ).

Задачи исследования

- Провести обзор и анализ способов защиты промышленных протоколов передачи данных, применяемых в России и в мире.
- Выбрать подходящий способ/бы защиты при организации межсетевого взаимодействия с использованием стека протоколов МЭК 61850-8-1 (MMS и GOOSE).
- Разработать прототип криптографически защищенного стека протоколов МЭК 61850-8-1 (MMS и GOOSE).
- Сформировать перечень количественно оцениваемых параметров работы (бенчмарки) криптографически защищенного стека протоколов МЭК 61850-8-1 (MMS и GOOSE).
- Провести исследования прототипа и получить количественно оцененные параметры работы (бенчмарки) криптографически защищенного стека протоколов МЭК 61850-8-1 (MMS и GOOSE).
- Подготовить технико-экономическое обоснование применения предлагаемых способов защиты при организации межсетевого взаимодействия с использованием стека протоколов МЭК 61850-8-1 (MMS и GOOSE).

Реализация стенда защищенного сетевого взаимодействия



Шифронабор	Установка соединения, мс	Проверка сертификата, мс	Шифрование, мс	Дешифрование, мс
TLS_RSA_WITH_AES_128_CBC_SHA	101,821	0,001201	0,015668	0,035625
TLS_RSA_WITH_AES_256_CBC_SHA	107,962	0,001412	0,015681	0,041221
TLS_RSA_WITH_AES_128_CBC_SHA256	130,884	0,002176	0,015984	0,050579
TLS_RSA_WITH_AES_256_CBC_SHA256	139,963	0,004838	0,019468	0,052833

Требования к теоретическим знаниям

- Для реализации криптографической защиты протокола MMS необходимо освоить:
- компьютерные сети (стек TCP/IP; особенности реализации MMS (МЭК 61850-9-1); владение программами-анализаторами трафика);
- инструменты виртуализации (умение развернуть и настроить программные продукты виртуализации);
- информационная безопасность (моделирование угроз безопасности информации; алгоритмы шифрования; хеш-функция; принципы взаимодействия по TLS; формирование шифронаборов);
- операционные системы (администрирование Linux);
- системы контроля версий (Git);
- программирование (C, CMake, IDE).

Роли и компетенции в команде

Роль	Компетенции	Необходимость
Ведущий разработчик	C (middle+); CMake (высокие); Linux (базовые); Git (базовые); SSL/TLS (выше среднего); компьютерные сети (базовые); Wireshark.	Критичная
Разработчик	C (junior+); CMake (базовые); Linux (базовые), Git (базовые); SSL/TLS (базовые); компьютерные сети (базовые); Wireshark.	Высокая
Аналитик	Linux (базовые), компьютерные сети (высокие); SSL/TLS (высокие).	Высокая
DevOps	Bash (средние), Linux (высокие), Git (базовые), GitLab/GitHub (базовые), Gitlab CI/Jenkins.	Средняя
QA	SSL/TLS (базовые); Linux (базовые); C (минимальные); любой скриптовый язык (высокие); компьютерные сети (базовые); Wireshark.	Низкая (только при увеличении количества разработчиков)

ЦЕНТР НТИ МЭИ

ТЕХНОЛОГИИ ТРАНСПОРТИРОВКИ
ЭЛЕКТРОЭНЕРГИИ РАСПРЕДЕЛЕННЫХ
ИНТЕЛЛЕКТУАЛЬНЫХ ЭНЕРГОСИСТЕМ

Применение ВСКЗИ в ИСУЭ

WWW.NTI.MPEI.RU

Нормативно-правовая база

Постановление Правительства РФ от 19 июня 2020 г. N 890

"О порядке предоставления доступа к минимальному набору функций интеллектуальных систем учета электрической энергии (мощности)"

Правила предоставления доступа к минимальному набору функций интеллектуальных систем учета электрической энергии (мощности)
Приказ Министерства энергетики РФ от 6 октября 2021 г. N 1021 "Об утверждении порядка и методики кодификации мест установки приборов учета электрической энергии и точек поставки электрической энергии"

Приказ Министерства энергетики РФ от 30 декабря 2020 г. N 1234 "Об утверждении перечня и спецификации защищенных протоколов передачи данных, которые могут быть использованы для организации информационного обмена между владельцами и пользователями интеллектуальных систем учета электрической энергии (мощности)«
Приказ Министерства цифрового развития, связи и массовых коммуникаций РФ от 30 декабря 2020 г. N 788 "Об утверждении перечня и спецификации защищенных протоколов передачи данных, которые могут быть использованы для организации информационного обмена между компонентами интеллектуальной системы учета электрической энергии (мощности) и приборами учета электрической энергии, которые могут быть присоединены к такой системе"

Нормативно-правовая база

Указ Президента Российской Федерации от 2 июля 2021 г. № 400
«Стратегия национальной безопасности Российской Федерации»

Информационная безопасность названа одним из

9 стратегических национальных приоритетов

48. Быстрое развитие информационно-коммуникационных технологий сопровождается повышением вероятности возникновения угроз безопасности граждан, общества и государства.

51. …… Вооруженные силы таких государств отрабатывают действия по выведению из строя объектов критической информационной инфраструктуры Российской Федерации.

55. Использование в Российской Федерации иностранных информационных технологий и телекоммуникационного оборудования повышает уязвимость российских информационных ресурсов, включая объекты критической информационной инфраструктуры Российской Федерации, к воздействию из-за рубежа.

Нормативно-правовая база

Указ Президента Российской Федерации от 2 июля 2021 г. № 400
«Стратегия национальной безопасности Российской Федерации»

57. Достижение цели обеспечения информационной безопасности осуществляется путем реализации государственной политики, направленной на решение следующих задач:

3) предотвращение деструктивного информационно-технического воздействия на российские информационные ресурсы, включая объекты критической информационной инфраструктуры Российской Федерации;

13) обеспечение приоритетного использования в информационной инфраструктуре Российской Федерации российских информационных технологий и оборудования, отвечающих требованиям информационной безопасности, в том числе при реализации национальных проектов (программ) и решении задач в области цифровизации экономики и государственного управления;

Нормативно-техническая база

Национальный стандарт Российской Федерации ГОСТ Р 58940-2020 "Требования к протоколам обмена информации между компонентами интеллектуальной системы учета и приборами учета", утвержден приказом Росстандарта от 28.07.2020 N 415

Предварительный национальный стандарт ПНСТ 354-2019 "Интернет вещей. Протокол беспроводной передачи данных на основе узкополосной модуляции радиосигнала (NB-Fi), утвержден приказом Росстандарта от 19.02.2019 N 7-пнст

Предварительный национальный стандарт Российской Федерации ПНСТ 433-2020 "Информационные технологии. Интернет вещей. Требования к платформе обмена данными для различных служб интернета вещей", утвержден приказом Росстандарта от 11.08.2020 N 42-пнст

Предварительный национальный стандарт Российской Федерации ПНСТ 438-2020 (ИСО/МЭК 30141:2018) "Информационные технологии. Интернет вещей. Типовая архитектура", утвержден приказом Росстандарта от 18.08.2020 N 47-пнст

Предварительный национальный стандарт Российской Федерации ПНСТ 446-2020 (ИСО/МЭК 21823-2:2020) "Информационные технологии. Интернет вещей. Совместимость систем интернета вещей. Часть 2. Совместимость на транспортном уровне", утвержден приказом Росстандарта от 18.08.2020 N 55-пнст

Предварительный национальный стандарт Российской Федерации ПСНТ* 420-2020 "Информационные технологии. Промышленный интернет вещей. Типовая архитектура", утвержден приказом Росстандарта от 23.07.2020 N 29-пнст

Предварительный национальный стандарт Российской Федерации ПНСТ 418-2020 "Информационные технологии. Интернет вещей. Структура системы интернета вещей реального времени (RT-IoT)", утвержден приказом Росстандарта от 23.07.2020 N 27-пнст

Нормативно-техническая база

Криптографическая защита информации:

- **Р 1323565.1.028-2019** "Информационная технология. Криптографическая защита информации. Криптографические механизмы защищенного взаимодействия контрольных и измерительных устройств"
- **Р 1323565.1.032-2020** "Информационная технология. Криптографическая защита информации. Использование российских криптографических механизмов для реализации обмена данными по протоколу DLMS"
- **Р 1323565.1.029-2019** "Информационная технология. Криптографическая защита информации. Протокол защищенного обмена для индустриальных систем"

Текущий статус

- Проанализированы НПА и НТД в области построения защищенных ИСУЭ

Предложения:

Пересмотреть Базовую модель угроз БИ ИСУЭ;

Учесть при разработке НТД положения Базовой модели угроз БИ ИСУЭ;

Учесть при разработке НТД положения требований безопасности информации к операционным системам: Встраиваемым операционным системам (тип "Б") (ФСТЭК России);

Учесть при разработке НТД требования к встроенным механизмам защиты в СнК.

- Сформированы критерии выбора встраиваемого СКЗИ для реализации прототипа защищенной ИСУЭ
- Выбран приоритетный партнер для сотрудничества.

Роли и компетенции в команде

Роль	Требования к компетенциям
Методолог	• общеметодологическое управление; • нормативно-правовая база; • нормативно-техническая база; • знание решения СКЗИ в полном объеме.
Архитектор	• паттерны проектирования систем класса IIoT; • компьютерные сети; • промышленные протоколы передачи данных, M2M протоколы; • базовые знания C++; • знание решения СКЗИ в полном объеме
Интеграция на уровне SCADA	• компьютерные сети; • промышленные протоколы передачи данных, M2M протоколы; • ОС Linux; • C++; • базовые знания в криптографии; • знание криптографического модуля
Интеграция на уровне PLC	• промышленные протоколы передачи данных, M2M протоколы; • знание электротехники; • Знание схемотехники • Linux; • C++; • базовые знания в криптографии; • знание криптографического модуля.

Подготовка кадров

Бакалавриат: «Электроэнергетика»

Магистерская программа:

«Интеллектуальные системы защиты, автоматики и управления энергосистем»

- разработка ПО для РЗА и АСУТП,
- основы ИБ в Электроэнергетике,
- нейронные сети и машинное обучение,
- онтологии и методы логического вывода,
- Адаптивные системы управления

Специализированные курсы ДПО:

- Внедрение практик БРПО;
- Разработка АСУ, защищенных с использованием встраиваемых криптографических средств

Что необходимо для ускорения работ

От вендоров СКЗИ:

- SDK и удобные средства разработки к программным и программно-аппаратным СКЗИ;
- Выделенный ресурс со стороны вендора СКЗИ на поддержку работ по интеграции и встраиванию СКЗИ;
- Прогнозируемый план развития продуктов (СКЗИ);
- Программу по работе с Вузами и их исследовательскими центрами.

От учебных центров:

- Специализированные учебные курсы, ориентированные на:
  - Компании вендоры АСУ
  - Проектные организации
  - Эксплуатирующие организации

От Заказчиков:

- Многолетняя взаимоувязанная программа НИОКР

Спасибо за внимание

ул. Красноказарменная, д. 17
Москва, Россия

WWW.NTI.MPEI.RU