

Заседание НИК В5 РНК СИГРЭ

В5.12 Требования к обеспечению кибербезопасности (устойчивости функционирования) цифровых систем РЗА

В.Г. Карантаев (ФГБОУ ВО «НИУ МЭИ»)



cigre

For power system expertise

26.06.2024

СТРУКТУРА ДОКЛАДА

1. Актуальность и ключевые задачи работы проблемной рабочей группы В5.12.
2. Текущие результаты.
3. Выводы

АКТУАЛЬНОСТЬ

Задачи и вызовы:

- Состояние кибервойны
- Тренд «атаки на цепочку поставки»:
 - программное обеспечение с открытым кодом.
- Обеспечение устойчивого функционирования КИИ РФ при проведении в отношении ее компьютерных атак (ФЗ-187 статья 1).
- Обеспечение технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации (Указы 250, 166).
- Переход к применению доверенных программно-аппаратных комплексов (ПП 1912).

КАК ЭТО СВЯЗАНО С РЗА СЕЙЧАС ?



Современное ИЭУ и подсистема РЗА ПС – 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).

ЧТО НАДО СДЕЛАТЬ



ПАК ИЭУ РЗА должен стать доверенным программно-аппаратным комплексом.

Доверенный ПАК ИЭУ РЗА 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).

КЛЮЧЕВЫЕ РЕЗУЛЬТАТЫ

Задание для Проблемной рабочей группы В5.12. содержит:

- 10 задач.
- 7 планируемых результатов.

По задаче 2 ПРГ: «Анализ зарубежного и отечественного опыта по обеспечению кибербезопасности...»

- ✓ Проанализированы ключевые части серий международных стандартов:
 - ✓ МЭК 62351-8, 14
 - ✓ МЭК 62443-4-1, МЭК 62443-4-2.
- ✓ Проанализирована практика реализации требований международными вендорами.
- ✓ Проанализированы требования Росстандарта ТК 362 «Защита информации» национальных стандартов и проектов в области разработки безопасного программного обеспечения (РБПО).
 - ✓ Обновлен ГОСТ 56939-202х – 25 процессов РБПО.
 - ✓ ГОСТ Р 71207-2024 – статический анализ ПО.
 - ✓ Акцент внимания на заимствованном коде и композиционном анализе.
- ✓ Проанализированы актуальные требования ФСТЭК России по построению процессов проектирования и производства программного обеспечения (процессы безопасной разработки программного обеспечения) и их сертификации.

КЛЮЧЕВЫЕ РЕЗУЛЬТАТЫ

По 4 задаче ПРГ 8: «Разработка требований к обеспечению кибербезопасности цифровых систем РЗА...» на основе анализа МЭК 62351, МЭК 62443, Приказа Минэнерго № 101, Распоряжения ПАО «Россети» № 62Р сформирована структура требования к доверенному ПАК ИЭУ РЗА:

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

Разработка безопасного программного обеспечения (РБПО) для РЗА



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



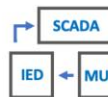
Функциональные
испытания РЗА



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

КЛЮЧЕВЫЕ РЕЗУЛЬТАТЫ



По 8 задаче ПРГ: «Разработка программ обучения...»
подготовлены:

➤ **Учебные курсы:**

- Учебный курс «Основы кибербезопасности микропроцессорных устройств релейной защиты и автоматики». – 1 учебный курс.
 - Учебный курс «Введение в разработку защищенных ИСУЭ и АСУ ТП с использованием ViPNetSIES» - 1 учебный курс;
- Учебно-методический комплекс Лаборатории ВСКЗИ АСУ ОЭ.
- Учебный курс «Построение процессов разработки безопасного программного обеспечения» - 3 учебных курса;
- Разработаны отраслевые кейсы для киберполигона Ampire+ЦДЭС.

КЛЮЧЕВЫЕ РЕЗУЛЬТАТЫ

По 9 задаче ПРГ: «Разработка прототипа системы РЗА со встроенными и наложенными СЗИ...» :

- Разработан прототип криптографически защищенных MMS и GOOSE с использованием отечественных криптографических средств защиты информации.
- Проведены стендовые испытания.
- Опубликовано и доложены результаты в журнале Релейщик и других периодических изданиях.

ВМЕСТО ЗАКЛЮЧЕНИЯ

- По теме ПРГ В 5.12 05.07 в НИУ МЭИ будет защищаться кандидатская диссертация.
- Результаты ПРГ В 5.12 докладывались на заседании НТС ЕЭС в 2023 году.
- Разработаны отраслевые кейсы для киберполигона Ampire+ЦДЭС.
- Разработана концепция по обеспечению кибербезопасности в течение жизненного цикла:
 - Прототип системы поддержки принятия решения (СППР УНКБ (управление надежностью и кибербезопасностью)).

СПАСИБО ЗА ВНИМАНИЕ



cigre

For power system expertise



АКТУАЛЬНОСТЬ

Новые задачи и вызовы:

- ✓ Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».
- ✓ Указ Президента Российской Федерации от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации».
- ✓ Постановление Правительства РФ от 14.11.2023 № 1912 «О порядке перехода субъектов критической информационной инфраструктуры Российской Федерации на преимущественное применение доверенных программно-аппаратных комплексов на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации».