SC D2 Russia

Presented by *Vladimir Karantaev*

Moscow – 23 July 2020

cigre

For power system expertise

WG D2.*51* *Working Group* Implementation of Security Operations Centers (SOC) in Electric Power Industry as Part of Situational Awareness System

Convener: Vladimir Karantaev

Email: vladimir.karantaev@gmail.com

Secretary: Alexey Gurevich

Email: AlexeyG09@gmail.com

cigre
For power system expertise

Scope of work

•

1. The first part of group work will involve a survey of use of SOC in utilities worldwide, reviewing, exploration and analysis of national regulations in cybersecurity sphere in relation to mandatory implementation of SOC for EPU.
2. A second part of group work will involve reviewing, exploration and analysis of dedicated IEC/ISO/IEEE standards in field of cybersecurity of Power Grids (Smart Grids). Preparing recommendation for development if it is needed.
3. Learning and analysis of cybersecurity best practices for building and organizing internal or outscoring IT and OT SOCs.
4. Development of recommendations for building and organising integrated SOC in EPU.
5. Development of requirements and architectures of the new SOCs in EPU.

cigre
For power system expertise

Отраслевые исследования

РНК СИГРЭ

Результаты деятельности объединенной проблемной рабочей группы №2 комитетов B5/D2 опубликованы:

- Сборник докладов международная выставка РЗА 2017
- Обзор деятельности ПРГ РНК СИГРЭ "Кибербезопасность РЗА и систем управления современных объектов электроэнергетики" Генгринович Е.Л., Гуревич А.Ю., Карантаев В.Г., Никандров М.В. Релейщик №2, 2019 стр. 27-29

CIGRE

- ТВ 790 Cybersecurity requirements for PACS and the resilience of PAC architectures WG B5.66
- WG D 2.51 «Implementation of Security Operations Centers (SOC) in Electric Power Industry as Part of Situational Awareness System»

Лаборатория Касперского: Дащенко Ю. «Моделирование угроз в условиях методической неопределенности»

Исследование **Лаборатории кибербезопасности АСУ ТП** «Анализ возможных нарушений работоспособности в результате деструктивных воздействий компьютерных атак на цифровые системы управления и защиты объектов электроэнергетического комплекса».

Connect Карантаев В.Г., Карпенко В.И. Анализ нарушений работоспособности объектов электроэнергетики вследствие кибератак/Connect 2020 г./ № 1–2 11–12 стр

Результаты работы ПРГ №2 РНК СИГРЭ

Таблица 2. Степень критичности для оборудования энергосистемы

№	Наименование объекта защиты	Степень критичности
1	системы релейной защиты и автоматики	Высокий
2	системы противоаварийной автоматики	Высокий
3	системы регистрации аварийных событий и процессов	Средний
4	системы определения места повреждения	Средний
5	системы мониторинга переходных режимов	Средний
6	автоматизированные системы управления технологическими процессами	Низкий
7	системы телемеханики	Низкий
8	автоматизированные системы мониторинга и диагностики оборудования	Низкий

Тип исполнения вторичного оборудования электрических подстанций и распредустройств генерации:
- электромеханические;
- микропроцессорные 1 типа;
- микропроцессорные 2 типа (МЭК 61850).

Журнал Релейщик №2-2019 27 с.

Общий принцип объединения подходов ИБ и ФБ

Исследование РНК СИГРЭ. Объединенная группа ПРГ-2 исследовательских комитетов B5/D2

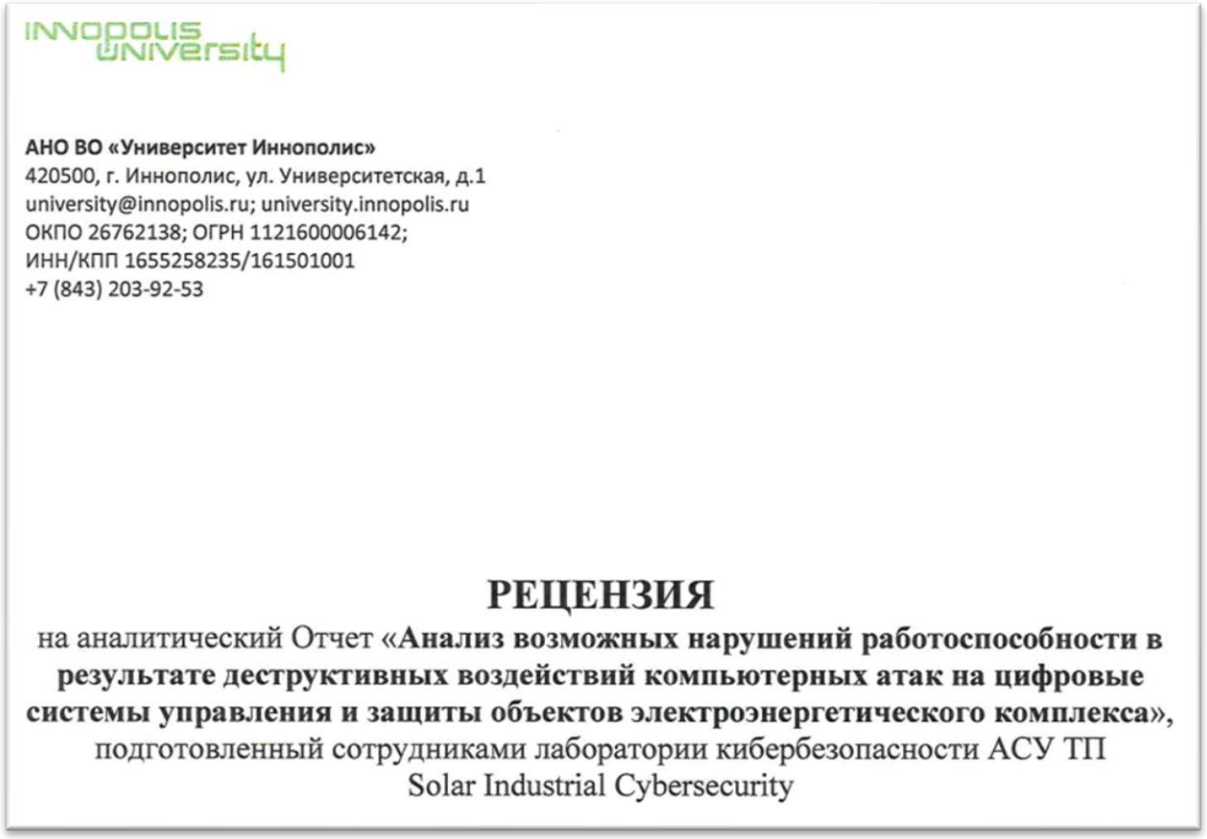
Моделирование угроз кибербезопасности в разрезе функциональной безопасности объектов электроэнергетики.
Д. Даренский http://rza-expo.ru/doc/rza_materialy3.pdf

Актуальные угрозы или история одного НИР

Результаты исследования отражают экспертную позицию авторского коллектива.

Наиболее значимый практический результат работы – это следующий вывод: **нарушение устойчивости функционирования объектов электроэнергетики с высоким уровнем цифровизации вторичных систем из-за воздействия на них кибератак возможно.**

Достигнутый результат заставляет по иному воспринимать риски цифровой трансформации электроэнергетической отрасли.



INNOPOLIS UNIVERSITY

АНО ВО «Университет Иннополис»
420500, г. Иннополис, ул. Университетская, д.1
university@innopolis.ru; university.innopolis.ru
ОКПО 26762138; ОГРН 1121600006142;
ИНН/КПП 1655258235/161501001
+7 (843) 203-92-53

РЕЦЕНЗИЯ

на аналитический Отчет «**Анализ возможных нарушений работоспособности в результате деструктивных воздействий компьютерных атак на цифровые системы управления и защиты объектов электроэнергетического комплекса**», подготовленный сотрудниками лаборатории кибербезопасности АСУ ТП Solar Industrial Cybersecurity

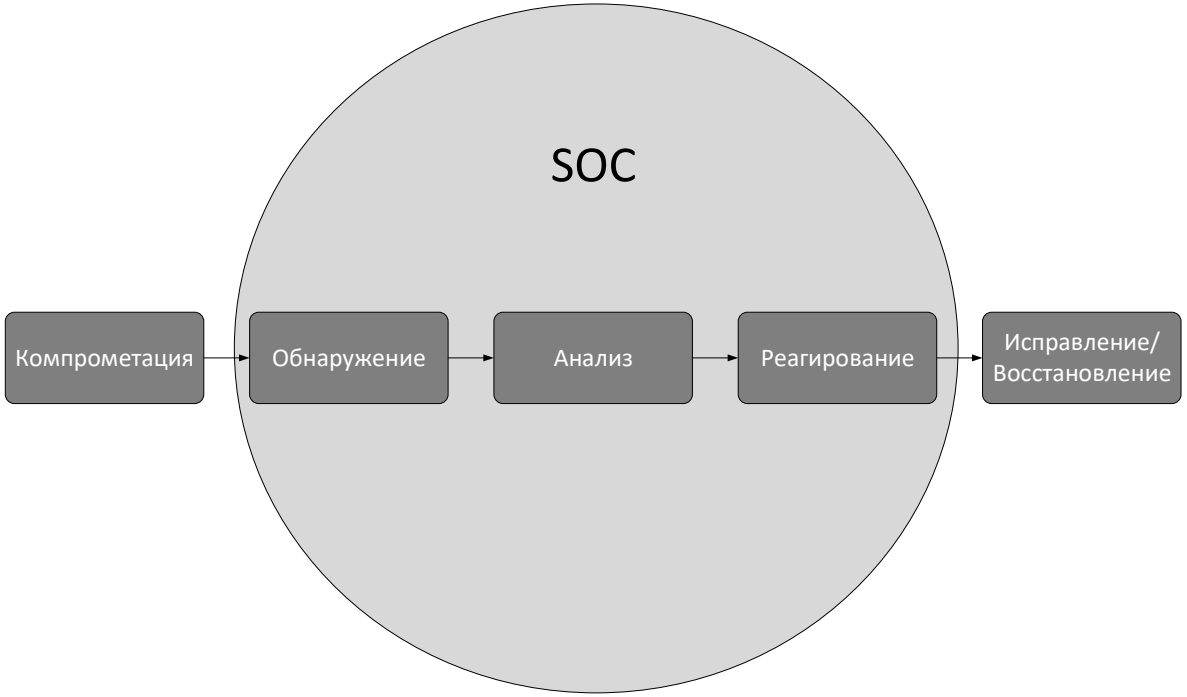
Презентация МФЭС 2019 Карантаев В.Г.
«Вопросы реализации киберзащищенной цифровой подстанции на основе российских технологий»
Connect Карантаев В.Г., Карпенко В.И. Анализ нарушений работоспособности объектов электроэнергетики вследствие кибератак/Connect 2020 г./ № 1–2 11–12 стр

Зрелый SOC для OT – это:

- Мониторинг в режиме 24x7x365.
- Высокий уровень экспертизы.
- Выстроенные процессы.
- Выделенный аналитик, контролирующий инфраструктуру.
- Продвинутая аналитика, включающая

Threat Intelligence и Threat Hunting.

- Расследование/изучение каждого события безопасности.
- Индивидуальный план реагирования на инциденты.



Доклад: Карантаев В.Г. «Модели представления managed detection and response (MDR) в АСУ ТП» https://goo-gl.su/RAIND3x

Входные условия старта и последующего развития

Этап №1:

- В инфраструктуре объекта защиты отсутствуют средства защиты информации.

Этап №2:

- В инфраструктуре объекта защиты внедрены «базовые» СЗИ:

- Шлюз безопасности на периметре
- Антивирусное ПО

Этап №3:

- На объектовом уровне внедрены специализированные СЗИ для защиты АСУ ТП:

- ICS Threat Detection Systems/ICS Asset Management System/ICS Network Intrusion Detection System (IDS).
- Индустриальные МЭ – Тип «Д» ФСТЭК России.
- EndPoint Protection.

Этап № 4:

- АСУ содержат развитый функционал встроенных СЗИ и СКЗИ.

Базовая архитектура объекта защиты

Выявляем сетевые узлы, критичные для защиты на объектовом уровне в IT-сегменте

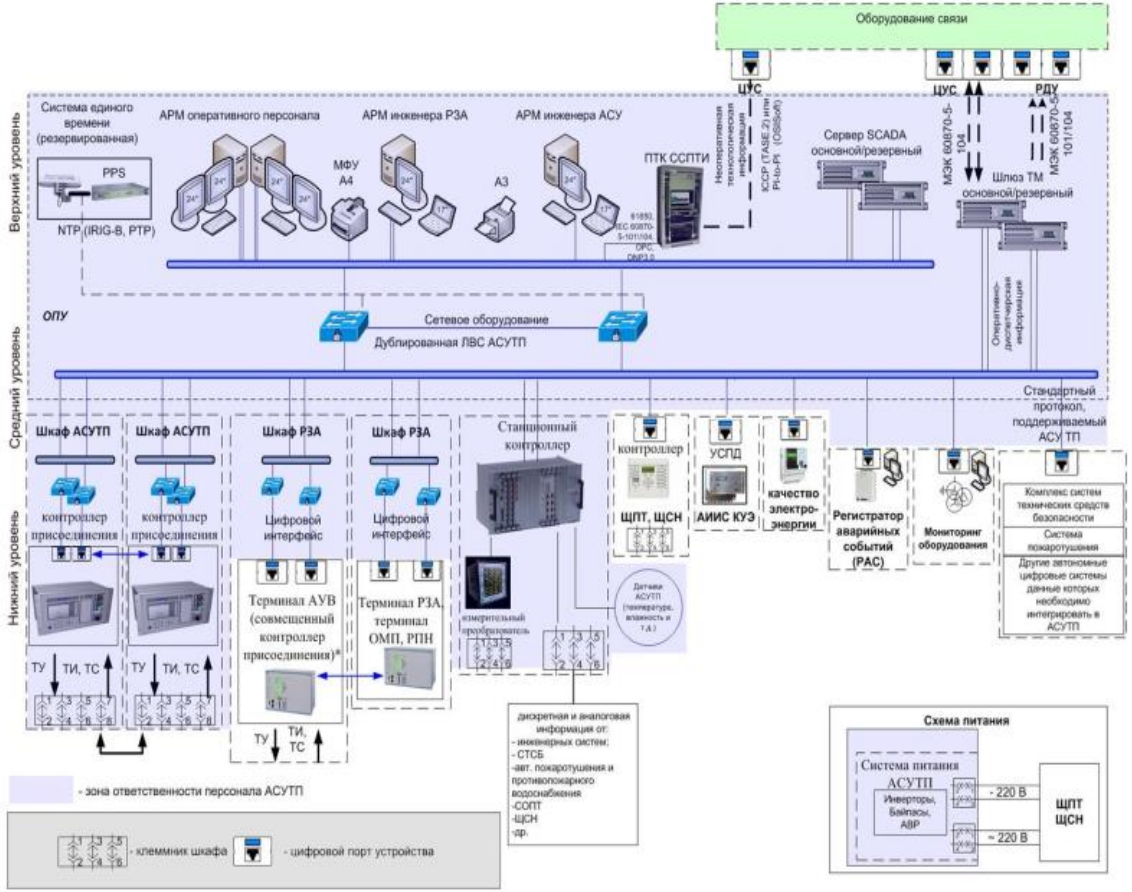
- ✓ **АРМ – персонала ПС;**

Выявляем сетевые узлы, критичные для защиты на объектовом уровне в ОТ-сегменте.

В соответствии с СТО 56947007- 25.040.40.226-2016

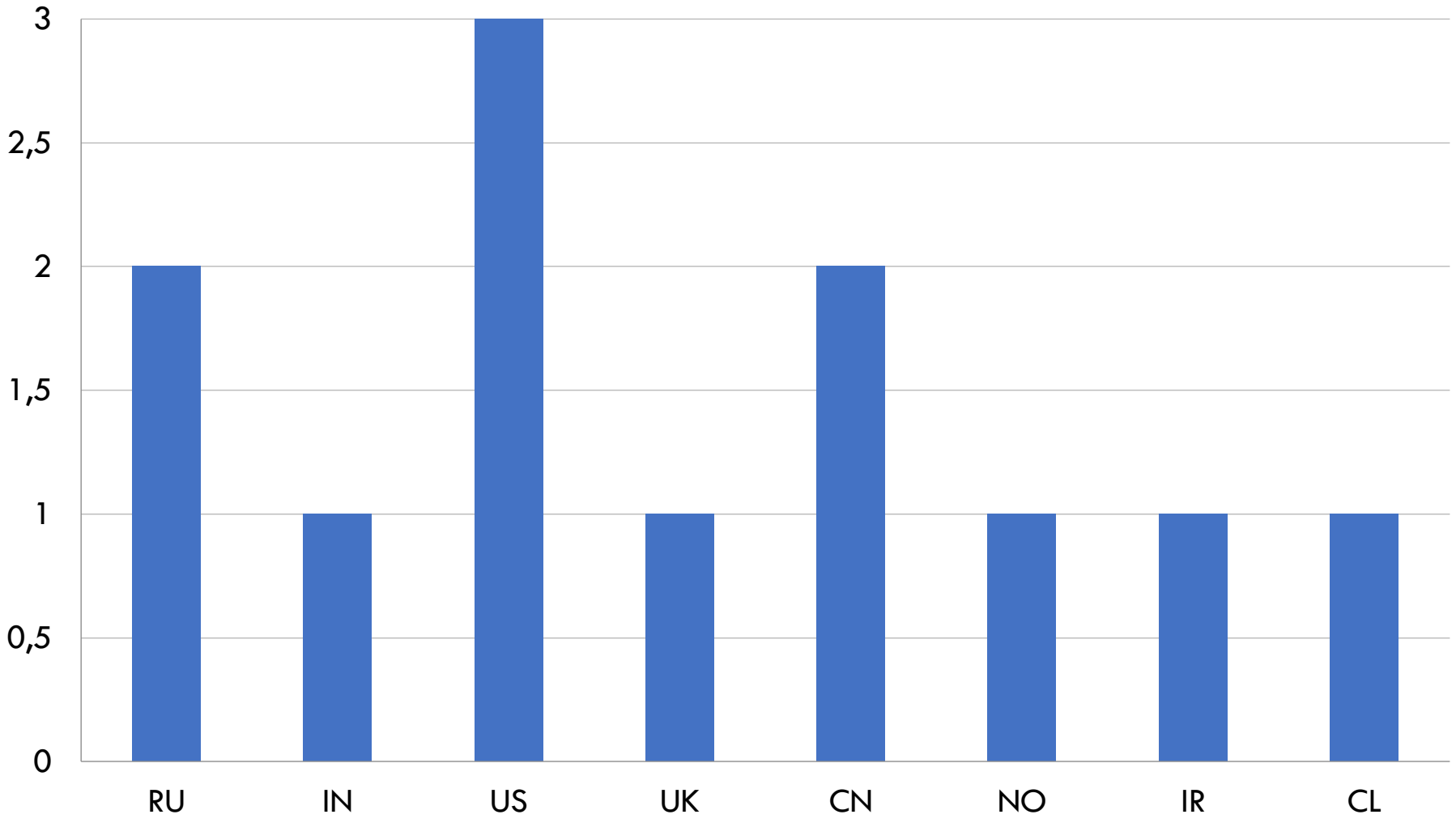
ПАО «ФСК ЕЭС»,
в ПТК АСУ ТП должны быть реализованы:

- ✓ **АРМ оперативного персонала.**
- ✓ **АРМ инженера РЗА.**
- ✓ **АРМ инженера АСУ.**
- ✓ **Серверы SCADA.**
- ✓ **Серверы телемеханики.**

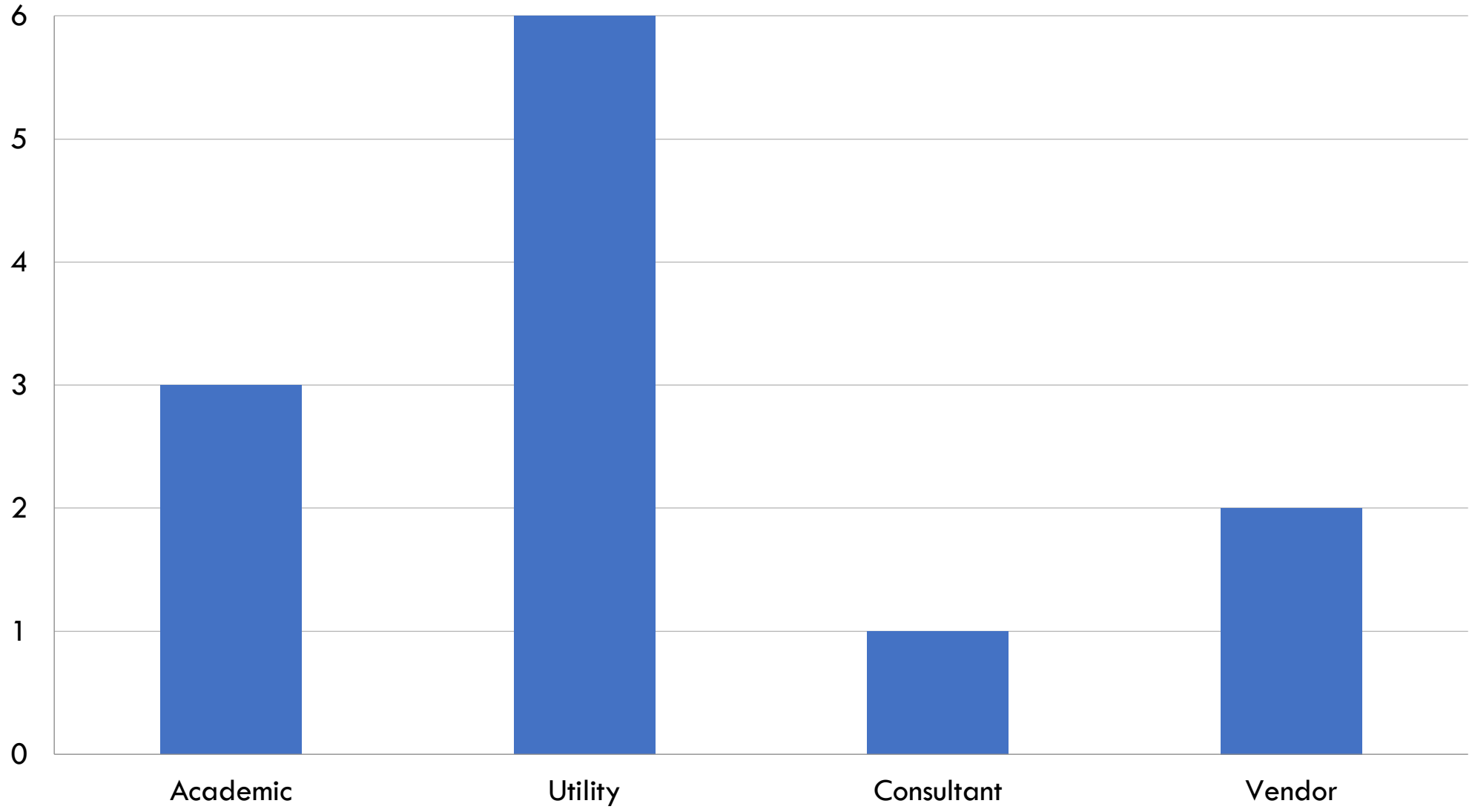


Доклад: Карантаев В.Г. «Модели представления managed detection and response (MDR) в АСУ ТП» https://goo-gl.su/RAIND3x

WG D2.51 Country Membership



WG D2.51 Type Membership



Working Group Program

№	Name of event	Planned	Actual Date
1	Initial approval from Technical Committee	October 2019	
2	Preparation and approval of the working group plan of works	July 2020	
3	To prepare of CIGRE SC D2 publication with status of the WG D 2.51 works result	November 2020	
4	To prepare a final survey	Feb 2021	
5	To prepare a draft of an article for the Electra magazine - WG D2.51 servey results	November 2021	
6	To prepare a draft of the Technical Brochure for the review in SC D2	November 2021	
7	To prepare of CIGRE SC D2 publication with status of the WG D 2.51 works result	November 2021	
8	To prepare the final draft of Technical Brochure	March 2022	
9	Publication of the article in the Electra magazine - WG D2.51 results achieved	Aprile 2022	
10	To arrange a webinar	May 2022	
11	To arrange a tutorial	August 2022	
12	Publication of the Technical Broshure	August 2022	

Working Group Program Cont.

№	Meeting plan	Date	Actual Date
1	To arrange and conduct the first online meeting of the WG in 2020	June 2020	10 June 2020
2	To arrange and conduct the second online meeting of the WG in 2020	August 2020	
3	To arrange and conduct the third online meeting of the WG in 2020	November 2020	
4	To arrange and conduct the first online meeting of the WG in 2021	March 2021	
5	To arrange and conduct an off-line meeting of the WG in 2021	July 2021	
6	To arrange and conduct the second online meeting of the WG in 2021	November 2021	
7	To arrange and conduct the first online meeting of the WG in 2022	March 2022	
8	To arrange and conduct an off-line meeting of the WG in 2022 on CIGRE Session	August 2022	

cigre
For power system expertise

Деятельность в НИК D2 РНК СИГРЭ

Рабочая группа РГ4 «Обеспечение информационной безопасности для систем связи и управления в электроэнергетике»

– рук. Карантаев Владимир Геннадьевич

Сформирована подгруппа в составе:

Карантаев В. – Центр НТИ МЭИ

Гуревич А. – АО «СО ЕЭС»

Дрюков В. – ООО «Солар Секьюрити»

Кузнецов А. – ООО «Солар Секьюрити»

Даренский Д. – Positive Technology

Текущий статус работ

- Подготовлена анкета-опросник.

Цель: обобщение и представление в обезличенном виде лучших практик построения SOC в компаниях субъектах электроэнергетики.

- Подготовлена первая версия черновик ТВ.

Планируемый результат в РФ:

- Представление результатов работы группы в НТС ПАО «Россети», НТС ЕЭС.
- **Срок: второй квартал 2022.**

Выпуск брошюры D2 РНК СИГРЭ. «Частные вопросы внедрения центров по мониторингу и реагированию на инциденты ИБ в субъектах электроэнергетики РФ как части общей системы ситуационной осведомленности"».

- **Срок: Четвертый квартал 2022.**

Планируемый результат WG D 2.51

- Публикация в журнале Electra
- Проведение обучающего курса на сессии CIGRE
- Подготовка и публикация ТВ