ЦЕНТР НТИ МЭИ

ТЕХНОЛОГИИ ТРАНСПОРТИРОВКИ
ЭЛЕКТРОЭНЕРГИИ РАСПРЕДЕЛЕННЫХ
ИНТЕЛЛЕКТУАЛЬНЫХ ЭНЕРГОСИСТЕМ

Частые вопросы использования ИС СППР на основе технологий ИИ для управления цифровыми объектами электроэнергетики в условиях проведения компьютерных атак

Владимир Карантаев

к.т.н., руководитель направления Центр НТИ МЭИ

WWW.NTI.MPEI.RU

Образ будущего цифровой электроэнергетики в 2025 г.

«В энергетике проведена необходимая модернизация, преодолен разрыв между скоростью старения оборудования и внедрением нового оборудования на основе цифровых технологий. Потребителям предоставляется электроэнергия по оптимальному тарифу с прогнозируемым необходимым качеством и надежностью. Создана система готовая противостоять многообразию рисков: технологической зависимости, рисков нарушения надежного, безопасного, эффективного функционирования»

http://digitenergy.ru/wp-content/themes/energy/img/pdf/0.pdf

Тенденции в электроэнергетической отрасли

ВИД ИСПОЛНЕНИЯ		на 01.01.2009 г.		на 01.01.2015 г.	
		110-220	330-750	110-220	330-750
Эл.мех.	РЗ и СА	86%	74%	63,87%	51,0%
	ПА	46%	53%	41,04%	38,40%
МЭ	РЗ и СА	8%	11%	7,51%	10,19%
	ПА	36%	23%	16,96%	13,94%
МП	РЗ и СА	6%	15%	28,62%	38,81%
	ПА	18%	24%	41,99%	47,67%

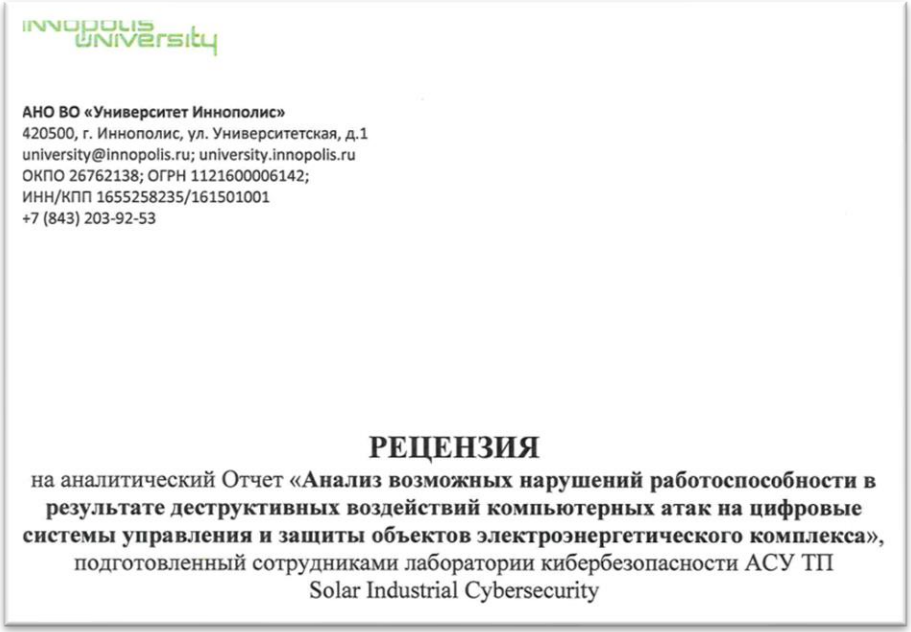
А.В. Жуков 5-я Международная научно-техническая конференция «Современные направления развития систем релейной защиты и автоматики энергосистем»

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

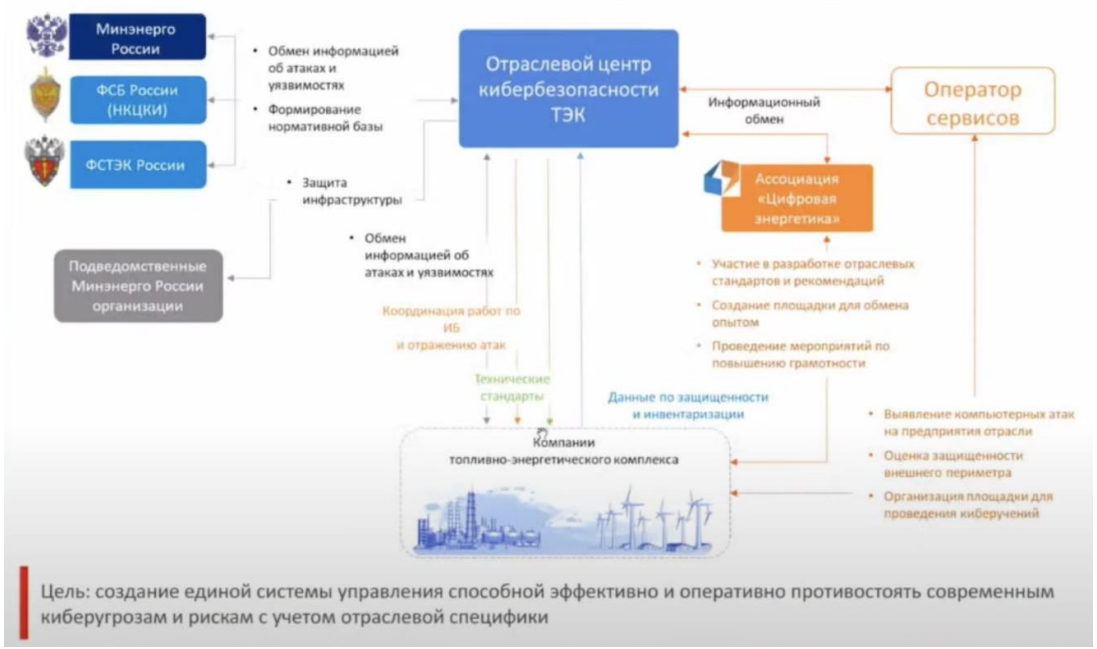
Презентация МФЭС 2019 Карантаев В.Г.

«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

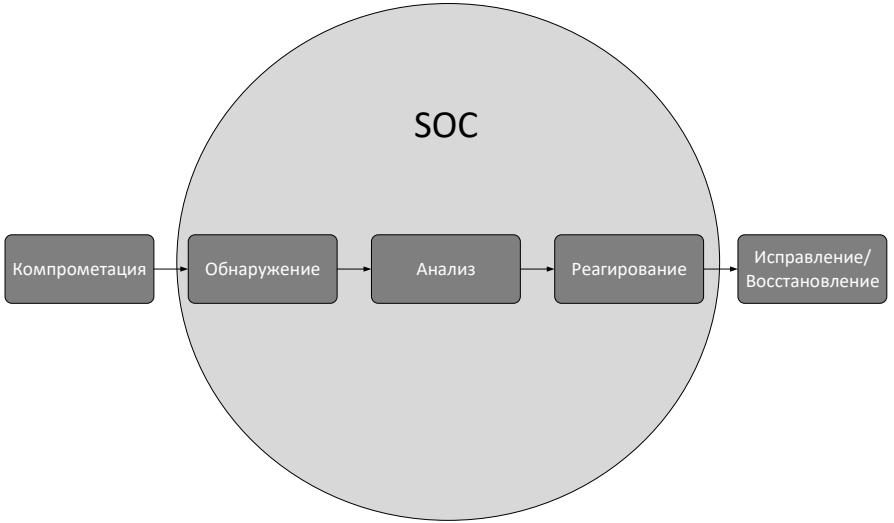
Тенденции в электроэнергетической отрасли. Продолжение

- Проведение тренировок и киберучений
- Мероприятия по оценке защищенности
- Совершенствование нормативно-правового регулирования



Применение SOC на объектах электроэнергетики
Можно, но сложно

- 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.



- Managed detection and response (MDR) delivery models for industrial control systems (ICS) https://youtu.be/qOY1xfezp9Q
- CoLaboratory Industrial Cybersecurity Meetup #4 https://youtu.be/FrpX3THqSTw

Базовая архитектура объекта защиты

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

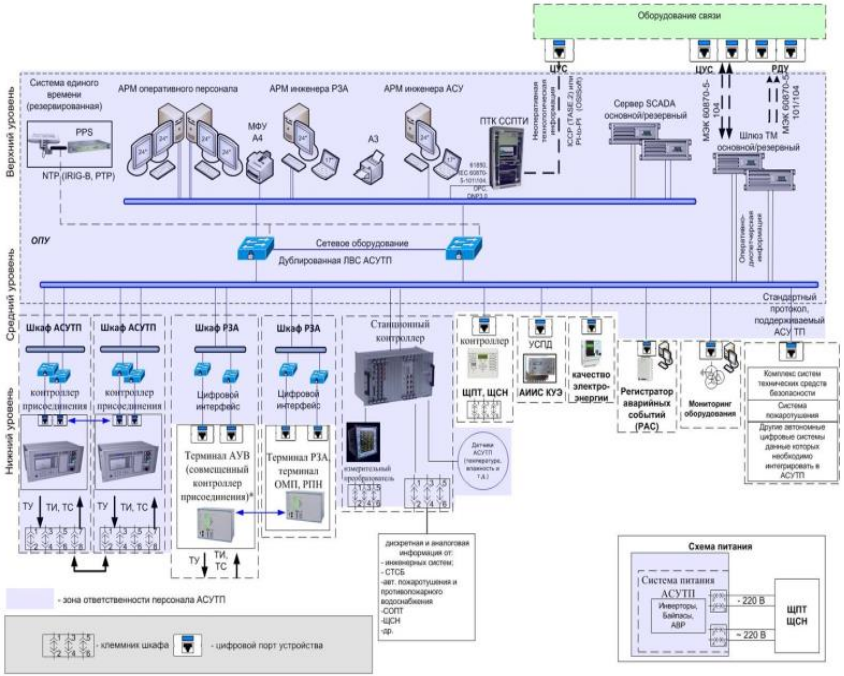
- АРМ – персонала ПС;

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

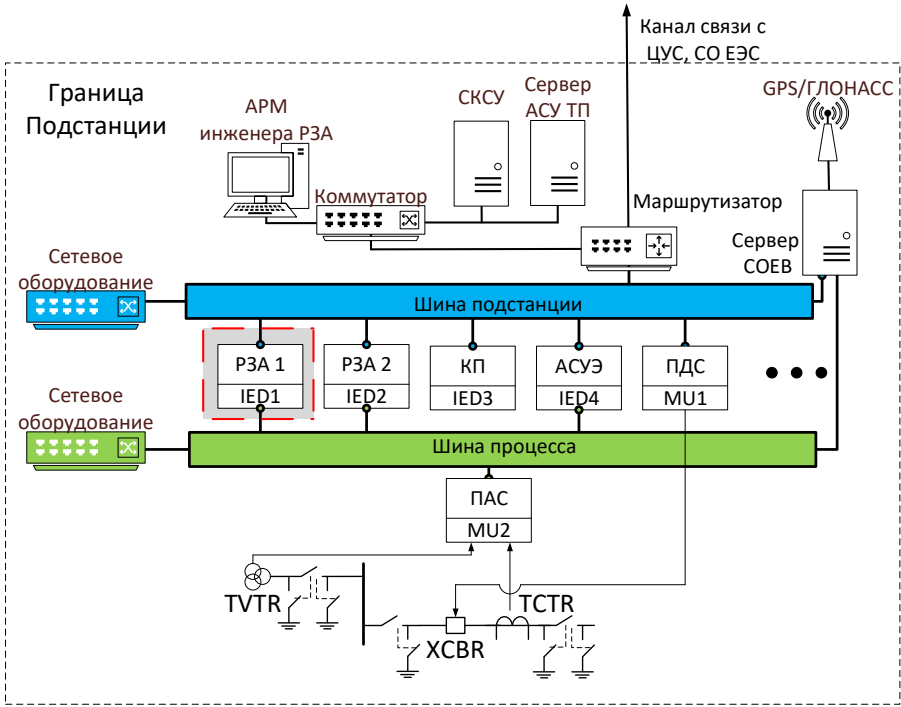


- Managed detection and response (MDR) delivery models for industrial control systems (ICS) https://youtu.be/qOY1xfezp9Q
- CoLaboratory Industrial Cybersecurity Meetup #4 https://youtu.be/FrpX3THqSTw

Место полигонов в практике создания и эксплуатации SOC

Виртуализация инфраструктуры,
использование концепции Infrastructure as Code (IaC)
позволят организовать:

- Инфраструктуру близкую к реальной.
- Тренировки SOC: Red Team – Blue Team без риска нарушить реальный технологический процесс.
- Изучить специфические объекты защиты и источники событий безопасности.
- Освоить практики подключения источников событий безопасности.
- Изучение поведения злоумышленников и накопление статистики атак с использованием части полигона в качестве deception system.

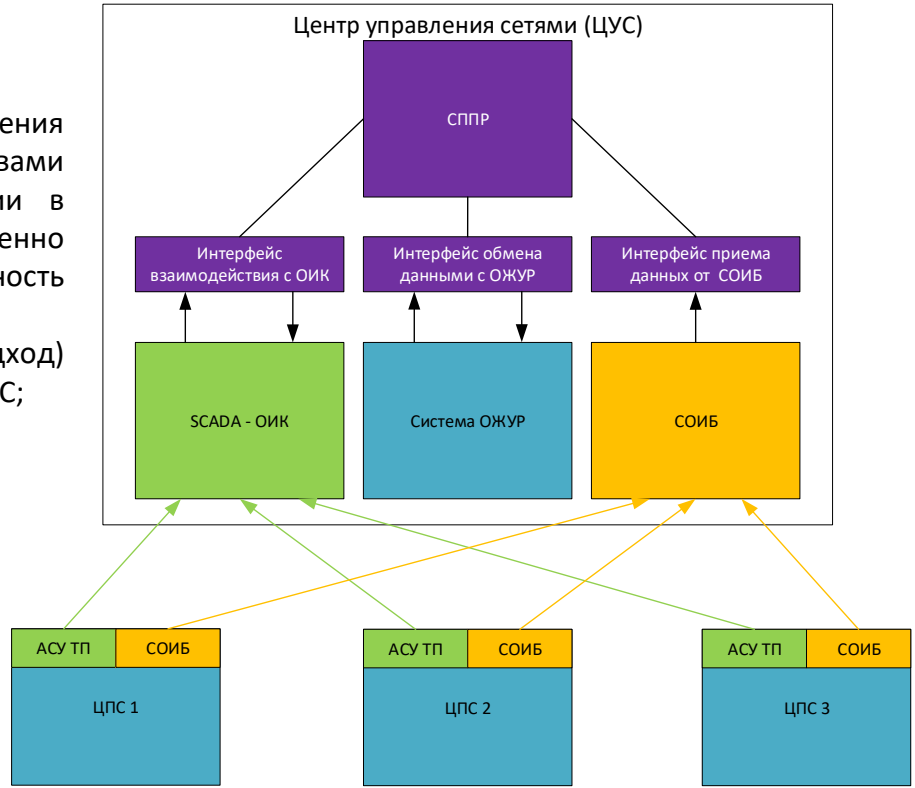


Технологии ИИ в управление инцидентами ИБ на объектах электроэнергетики

Реальна ли возможность внедрения технологий искусственного интеллекта в управление инцидентами ИБ?

Основу ИС СППР составляют:

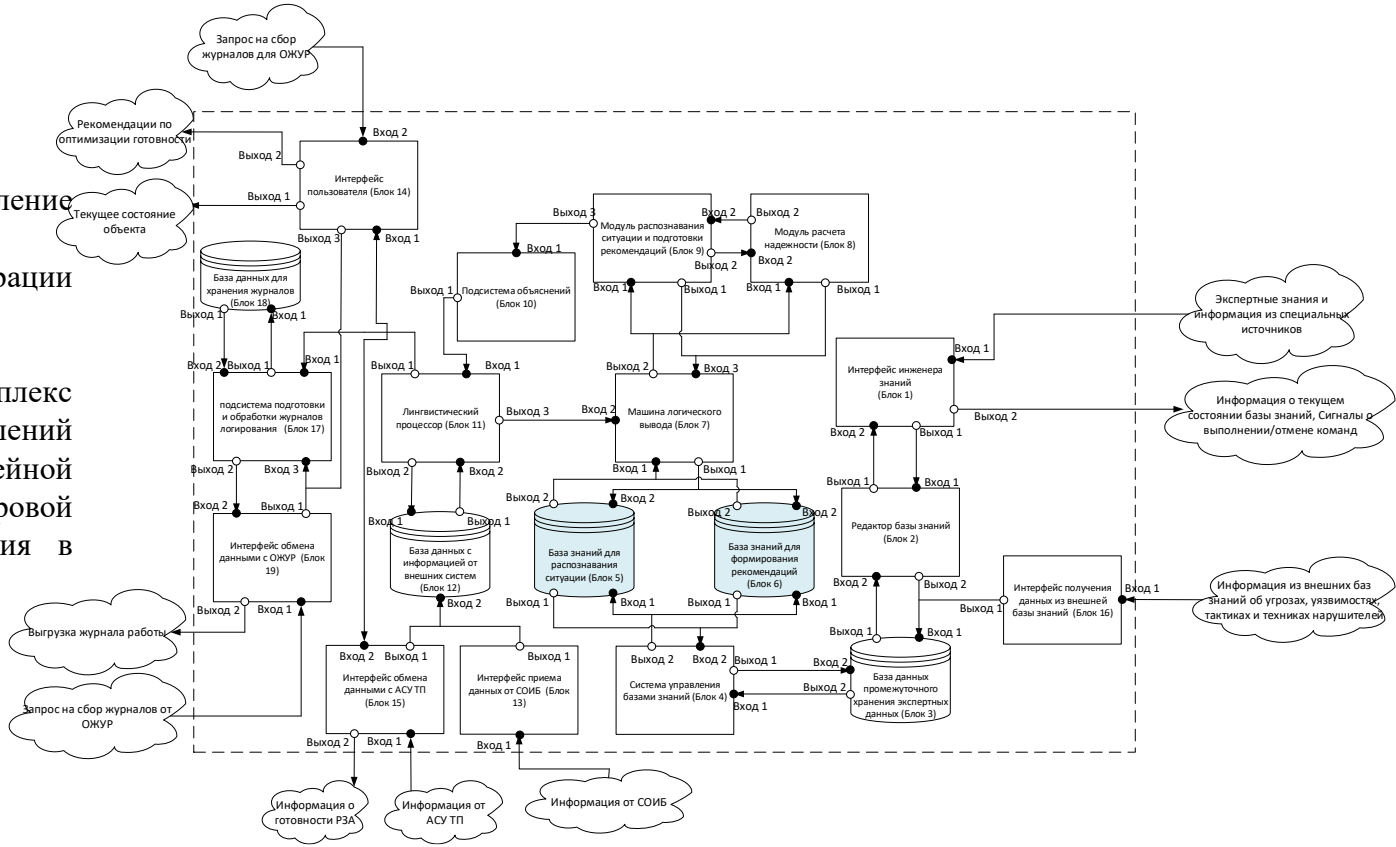
- Способ расчета показателей надежности с возможностью изменения коэффициентов расчетной модели ИЭУ РЗА, обладающего свойствами ремонтопригодности и восстанавливаемости, при проведении в отношении него компьютерных атак. Способ позволяет количественно оценить деструктивное влияние компьютерных атак на надежность функционирования ИЭУ РЗА
- Задействованы подходы инженерии знаний (Онтологический подход) для моделирования угроз кибербезопасности подсистемы РЗА ЦПС;



Уникальность результата

01.06.2022 подано заявление №2022114852
о выдаче патента Российской Федерации на изобретение

«Программно-аппаратный комплекс системы поддержки принятия решений по управлению подсистемой релейной защиты и автоматики цифровой подстанции в условиях проведения в отношении нее компьютерных атак»



Планы:

- Разработать и использовать распределенные инфраструктуры ложных целей в системах управлениях Цифровой энергетики.
- Изучить варианты развития технологий программно-аппаратных комплексов «песочницы» для применения в инфраструктуре индустриальных систем управления.
- Организовать стендовые и полигонные испытания ИС СППР.
- Провести анализ угроз БИ и формирование мер защиты для инфраструктуры электрозарядных станции, ЭЗС.
- Принять участие в организации и проведении киберучений.

Спасибо за внимание

ул. Красноказарменная, д. 17
Москва, Россия

Владимир Карантаев
KarantayevVG@mpei.ru

WWW.NTI.MPEI.RU