



ЦЕНТР НТИ МЭИ

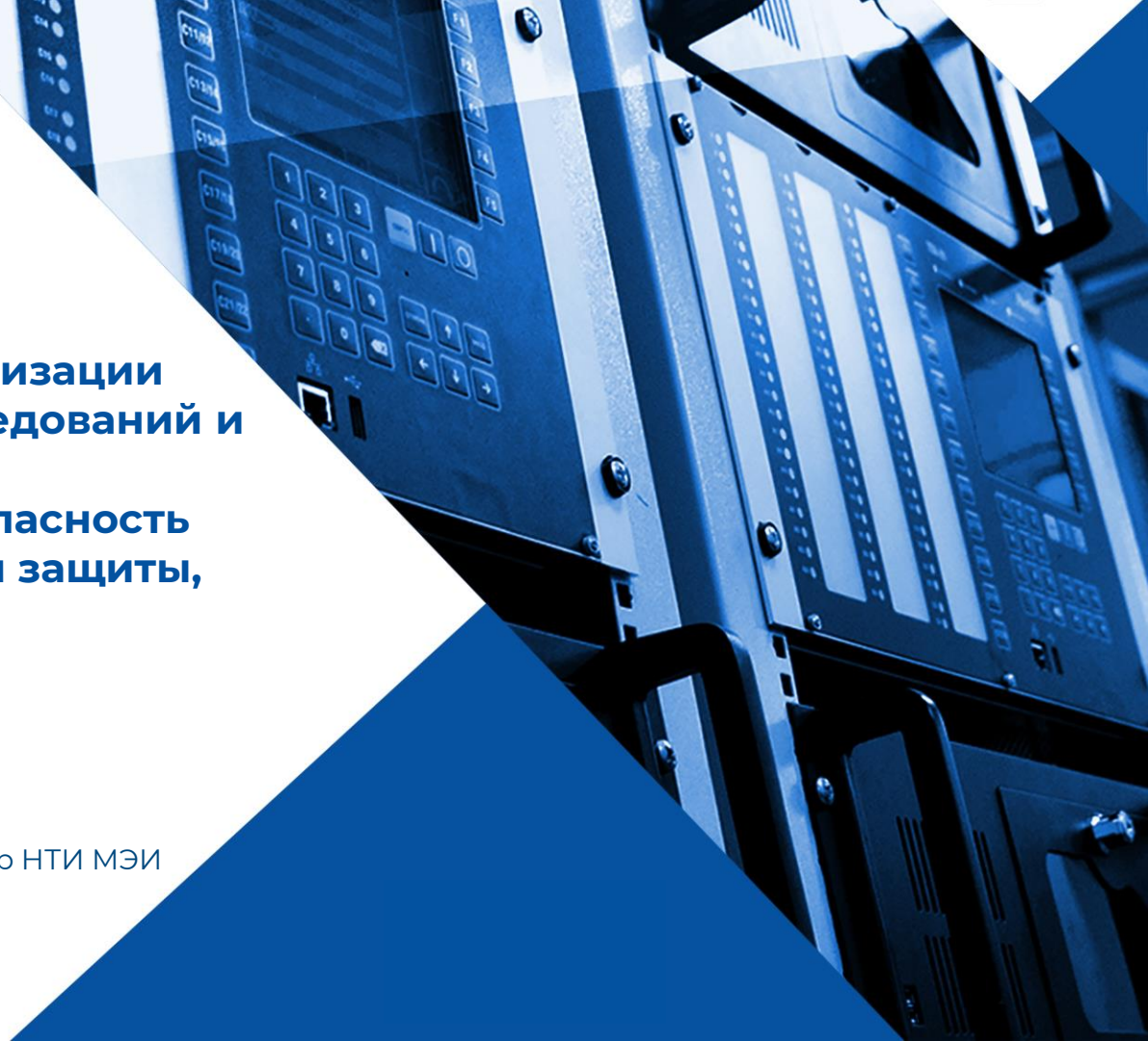
ТЕХНОЛОГИИ ТРАНСПОРТИРОВКИ
ЭЛЕКТРОЭНЕРГИИ РАСПРЕДЕЛЕННЫХ
ИНТЕЛЛЕКТУАЛЬНЫХ ЭНЕРГОСИСТЕМ

**Практический опыт организации
научно-прикладных исследований и
подготовки кадров в
направлении "Кибербезопасность
интеллектуальных систем защиты,
автоматики и управления
энергосистемами»**

Владимир Карантаев

к.т.н., руководитель направления Центр 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

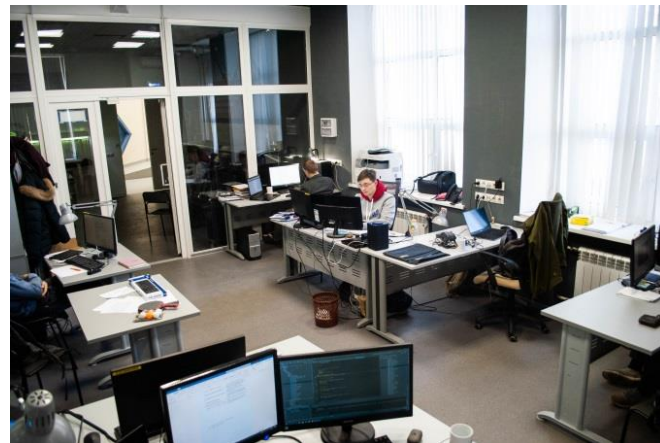


«Интеллектуальные системы защиты, автоматики и управления энергосистемами»

Магистерская программа разработана специалистами Центра компетенций НТИ на базе МЭИ при поддержке ПАО «Россети ФСК ЕЭС» для реализации плана Минэнерго Российской Федерации по цифровой трансформации электроэнергетики.

Разработана и запущена в 2018 г.

- Данная программа направлена на изучение программно-аппаратного обеспечения, необходимого для реализации новейших технологий и устройств СРЗА. В процессе обучения ты изучишь технологии
 - алгоритмов оптимизации
 - методов обеспечения кибербезопасности
 - методов искусственного интеллекта
 - онтологических систем
 - мультиагентных систем



<http://nti.mpei.ru/magistracy-mpei/>

Киберполигон Центра НТИ МЭИ

Назначение киберполигона:

- проведение киберучений;
- исследование защищенности устройств и систем, исследование совместимости средств защиты и оборудования АСУ ТП и РЗА;
- оценка последствий реализации кибератак;
- повышение квалификации в области информационной безопасности;
- разработка и исследование новых способов обеспечения информационной безопасности АСУ ТП и РЗА;
- получение практических навыков по настройке встроенных и наложенных средств защиты информации;
- повышение квалификации в области проектирования систем обеспечения информационной безопасности объектов электроэнергетики.




infotecs®

kaspersky


ARMA INFOWATCH
ARMA

Направления прикладных исследований

- Оценка влияния деструктивных воздействий компьютерных атак на цифровые объекты электроэнергетического комплекса
- 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.
- Вопросы внедрения центров по мониторингу и реагированию на инциденты ИБ в субъектах электроэнергетики как части общей системы ситуационной осведомленности.
- Эффективность использования встраиваемых средств криптографической защиты при межсетевом взаимодействии между автоматизированными и автоматическими системами цифровых подстанций.
- Применение методов искусственного интеллекта для обеспечения устойчивого и безопасного функционирования автоматизированными и автоматическими системами цифровых подстанций.

Системы поддержки принятия решений, экспертные системы с использованием онтологического подхода

Методы машинного обучения

Публикаций по теме кибербезопасность интеллектуальных систем защиты, автоматики и управления энергосистемами

2019 – 7 публикаций;

2020 – 8 публикации;

2021 – 10 публикаций;

2022 – 5 публикаций.

Из них:

4 публикации в изданиях индексируемых SCOPUS.

1 публикация в издании рецензируемом ВАК.

1 публикация в изданиях международного совета CIGRE

1 учебное пособие НИУ МЭИ

2022 – план 3 публикации в изданиях рецензируемых ВАК.

Подготовлен к публикации Лабораторный практикум.

Количество докладов по теме кибербезопасность интеллектуальных систем защиты, автоматике и управления энергосистемами

Доклады на научно-практических конференциях:

2019 – 6 докладов;

2020 – 12 докладов;

2021 – 13 докладов;

2022 – 3 доклада.

Результаты интеллектуальной деятельности:

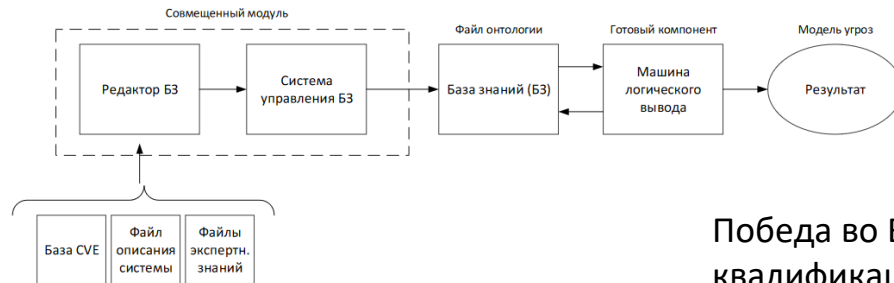
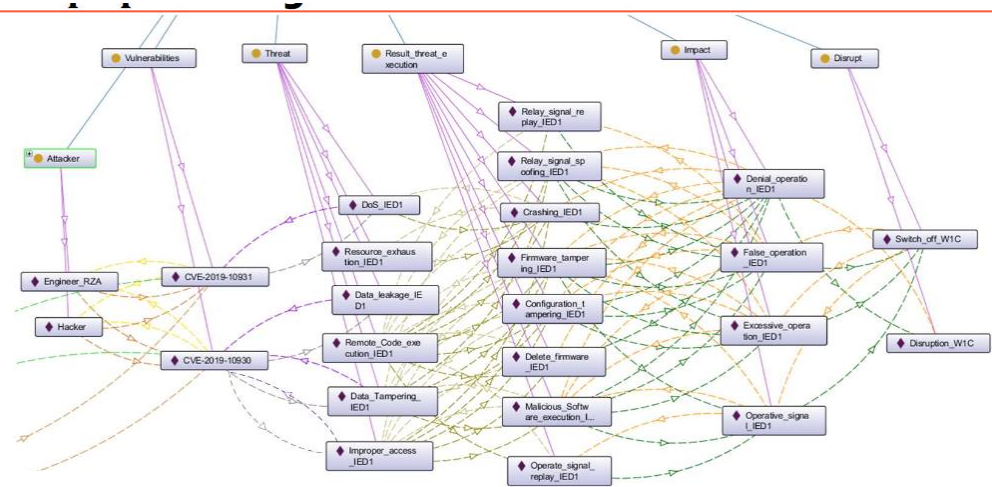
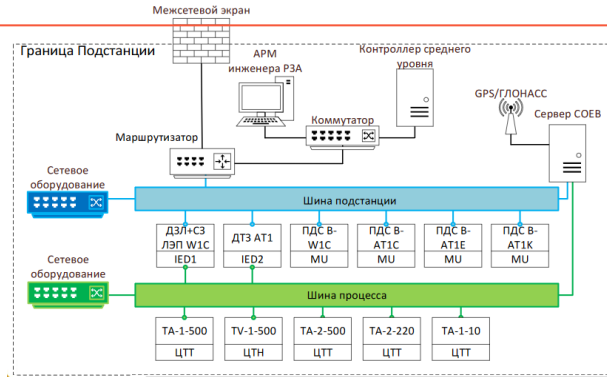
2022 подана одна заявка о выдаче патента на изобретение:

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

2023 год:

Государственная регистрация в ФИПС прав авторов и правообладателей программ для электронных вычислительных машин.

Карпенко В.И. Экспертная система для оценки влияния деструктивных воздействий компьютерных атак на подстанции



Победа во Всероссийском конкурсе выпускных квалификационных работ среди 350 работ из 32 технических вузов России.

Планы:

Новые направления исследований:

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

Выполнение НИОКР по заказу ПАО «Россети».

Организация и проведение киберучений.

Внедрение в учебный процесс практик использования киберполигона, реализованного программно в «виртуальной» инфраструктуре .

Спасибо за внимание

ул. Красноказарменная, д. 17
Москва, Россия

Владимир Карантаев
KarantayevVG@mpei.ru

WWW.NTI.MPEI.RU

