Москва, 29 сентября - 1 октября

МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ И ВЫСТАВКА

РЕЛЕЙНАЯ ЗАЩИТА И АВТОМАТИКА ЭНЕРГОСИСТЕМ 2021

ТЕХНОЛОГИИ РЗА ЦПС, ОБЕСПЕЧИВАЮЩИЕ ПОВЫШЕННУЮ УСТОЙЧИВОСТЬ К КИБЕРАТАКАМ

ВОЛОШИН А.А., ВОЛОШИН Е.А., НУХУЛОВ С.М.,
ДОБРЫНИН В.И., БЛАГОРАЗУМОВ Д.О.

ФГБОУ ВО «НИУ «МЭИ», «Центр НТИ МЭИ»

Россия

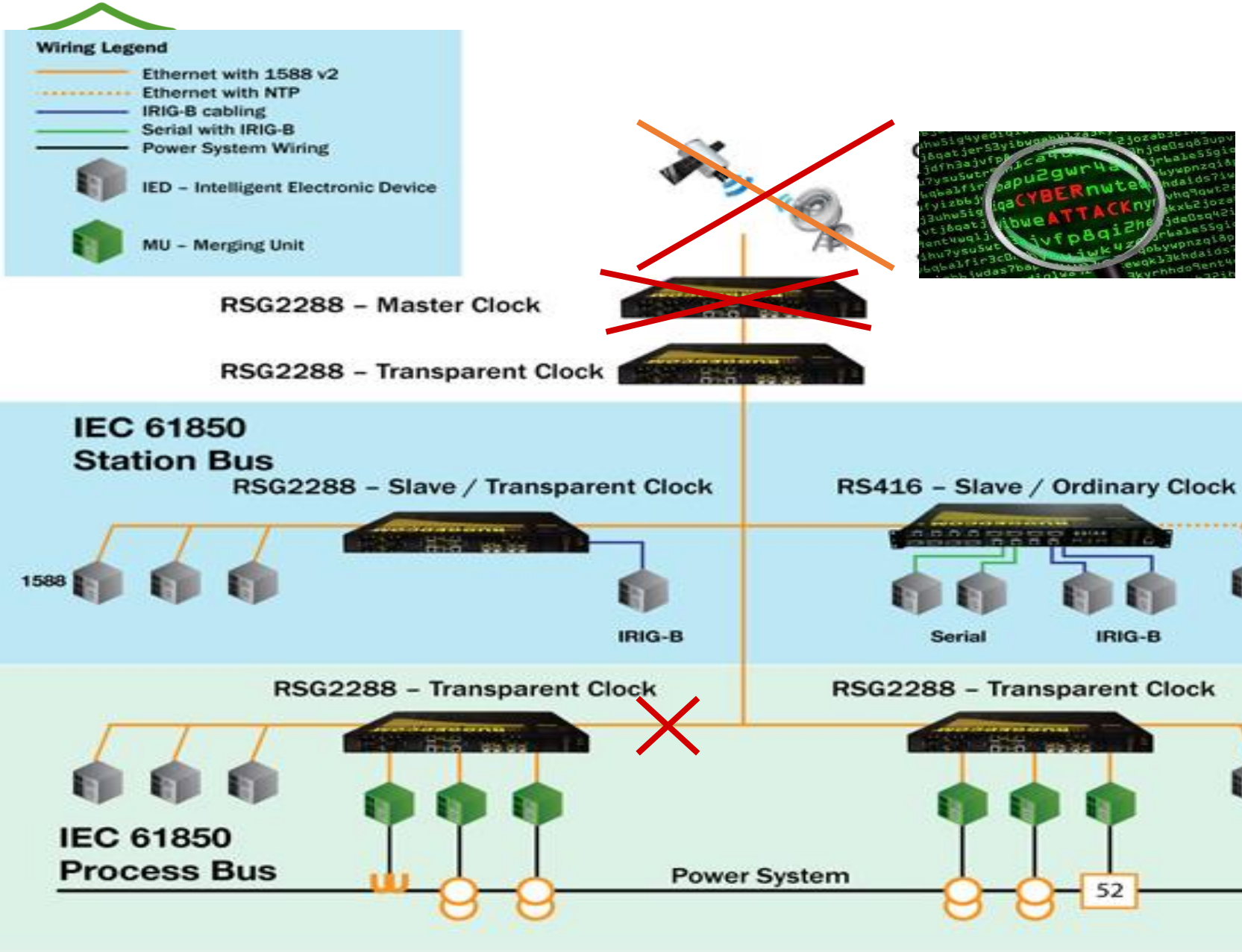
БЛАГОРАЗУМОВ ДМИТРИЙ ОЛЕГОВИЧ

ВАРИАНТЫ КИБЕРАТАК НА КОМПЛЕКС РЗА

В связи с внедрением новых информационных технологий при разработке систем РЗА необходимо рассматривать появление новых видов киберугроз.

- К таким видам угроз относятся кибератаки, направленные на нарушение целостности информации, передаваемой по локальной вычислительной сети.
- Нарушение информационной безопасности энергообъектов может привести к несанкционированному управлению коммутационными аппаратами (КА), разрушению информационной инфраструктуры энергообъекта и несанкционированным отключениям магистральных ЛЭП, электростанций и потребителей.

ПРОБЛЕМЫ СУЩЕСТВУЮЩИХ ПРОТОКОЛОВ СИНХРОНИЗАЦИИ ВРЕМЕНИ

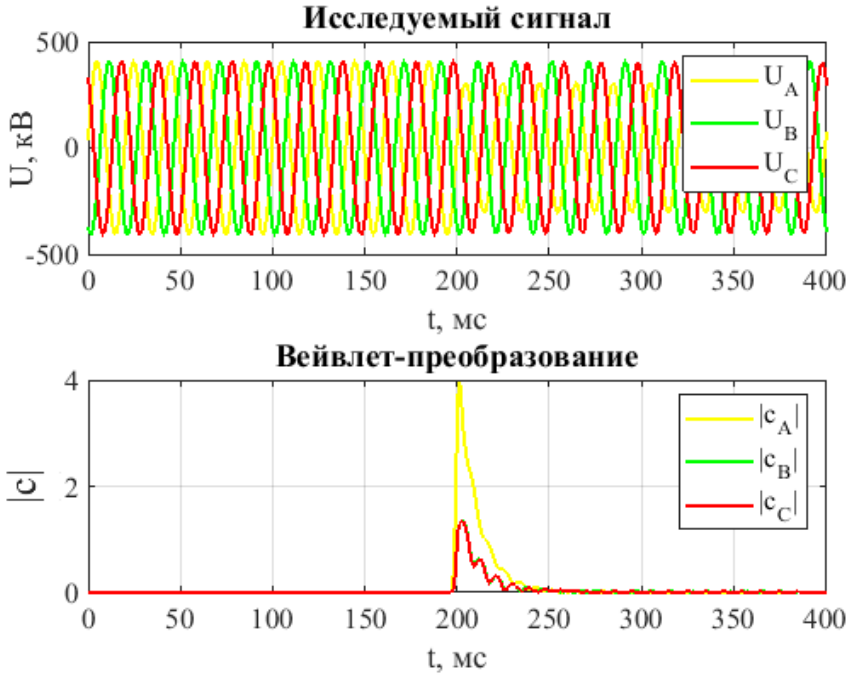


ВОЗМОЖНЫЕ ВАРИАНТЫ ЗАЩИТЫ ОТ КИБЕРАТАК

В рамках настоящей работы предлагается применять 2 типа дополнительных технологических алгоритмов РЗА:

- Первый тип алгоритмов предназначен для выявления кибервоздействий, направленных на подмену измеряемых сигналов. Для этого необходимо обрабатывать измерения, получаемые от УСО подключенных к одним точкам энергообъекта и вычислять на их основе измерения в других точках, а затем проводить сравнение вычисленных и измеренных значений. В случае выявления несоответствий определяются недостоверные измерения и их источник
- Второй тип алгоритмов предназначен для предотвращения реализации несанкционированной команды аварийного отключения электрооборудования. Для этого в УСО применяются алгоритмы пускового органа (ПО), основанные на применении вейвлет преобразования. Указанные алгоритмы предотвращают возможность несанкционированного аварийного отключения в нормальном режиме работы. Таким образом существенно повышается устойчивость электроэнергетических систем к кибервоздействиям, т.к. для реализации неправомерных действий потребуется существенно больше времени и ресурсов.

СХЕМА ПРЕДЛАГАЕМОГО СПОСОБА ЗАЩИТЫ ОТ КИБЕРАТАК

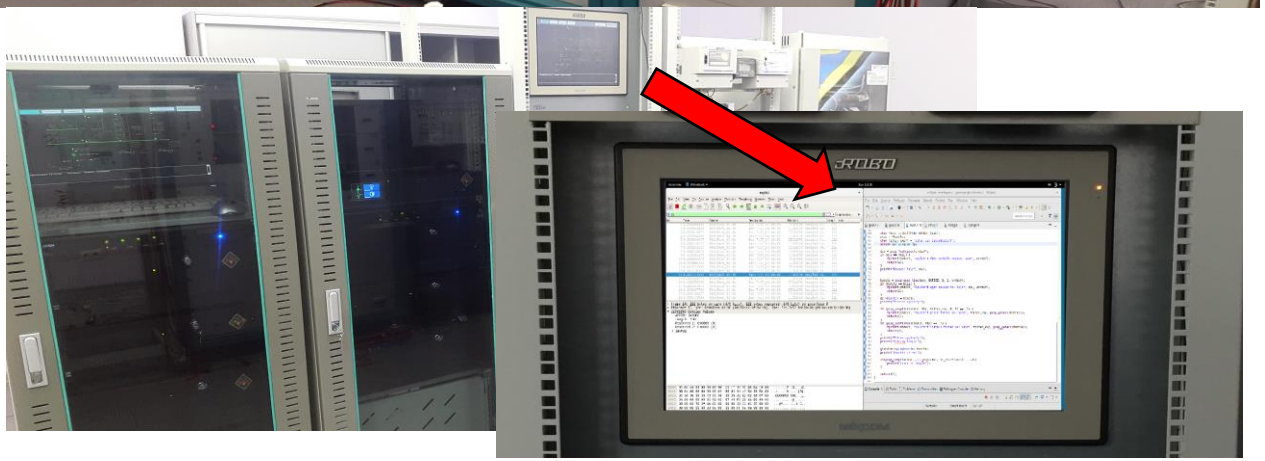


При возникновении аварийной ситуации, когда требуется срабатывание устройства защиты, пусковой сигнал от устройства релейной защиты будет разрешен пусковым органом защиты от кибератак, работа которого основана на вейвлет-преобразовании и фиксации момента аварийной возмущения.

Пример определения максимума модуля коэффициентов вейвлет-преобразования

КИБЕРПОЛИГОН «ЦИФРОВАЯ ЭНЕРГЕТИКА»

ИСПЫТАНИЯ ПУСКОВОГО ОРГАНА ЗАЩИТЫ ОТ КИБЕРАТАК НА МОДЕЛИ ЦПС, РЕАЛИЗОВАННОЙ В ПАК RTDS



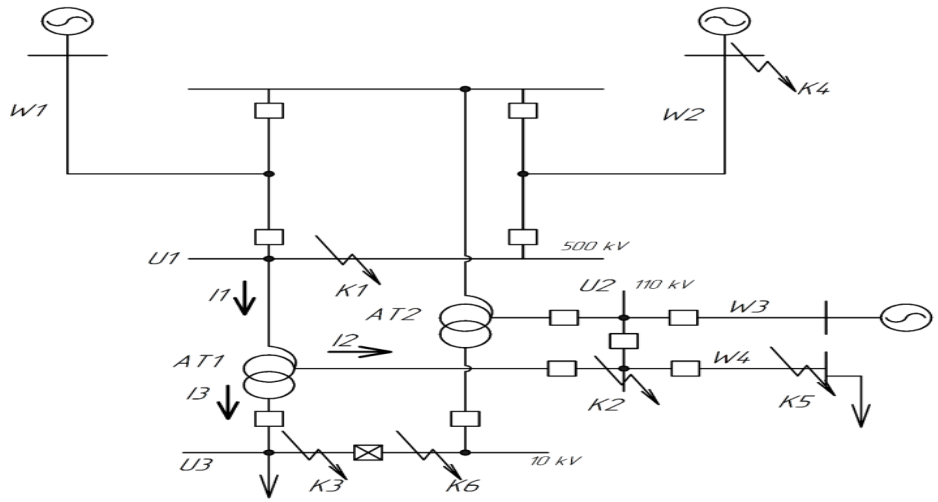
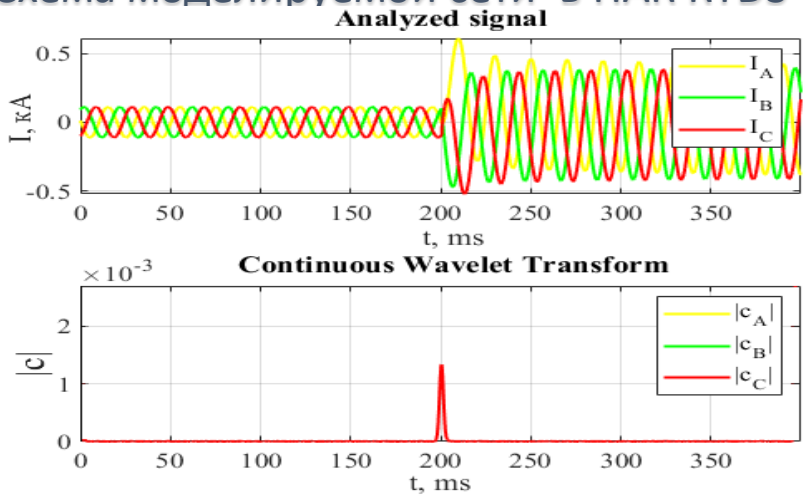
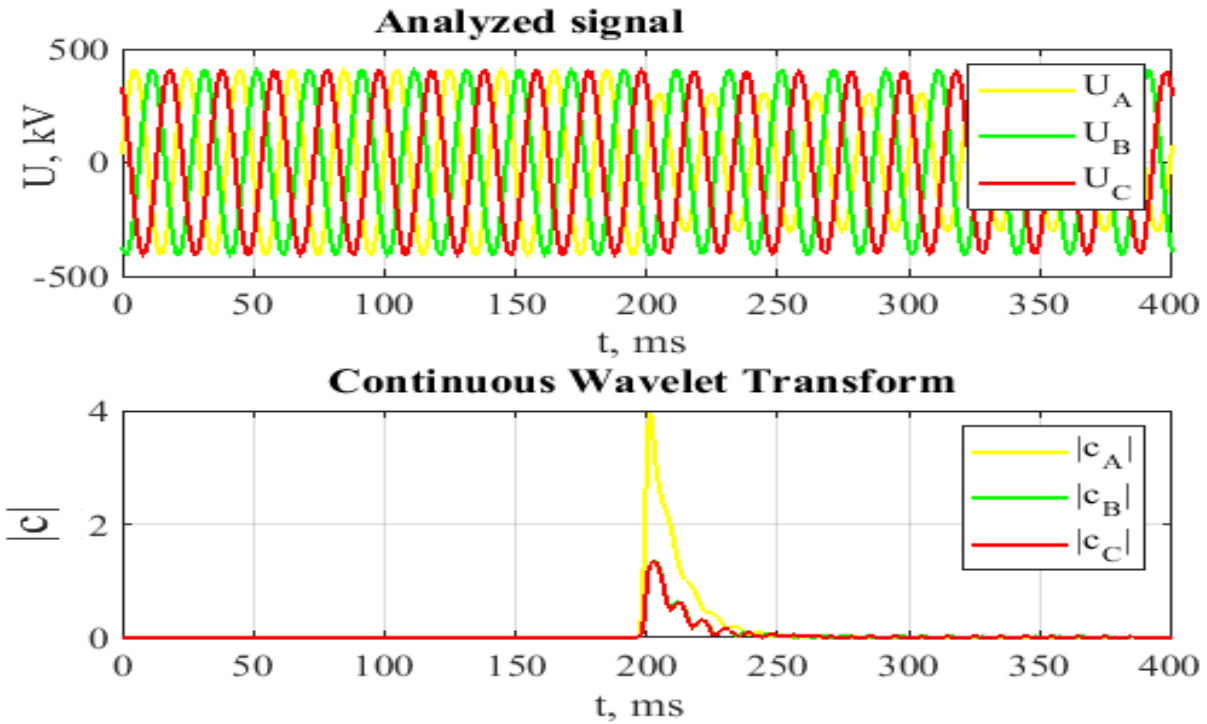
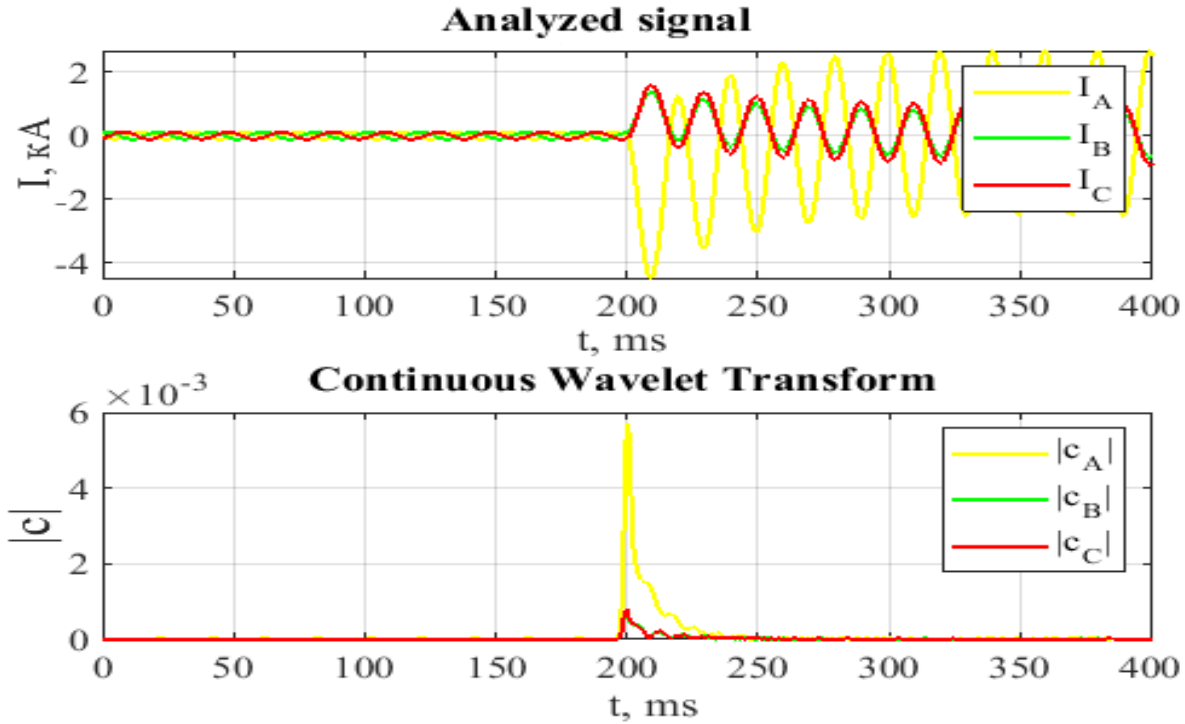


Схема моделируемой сети в ПАК RTDS

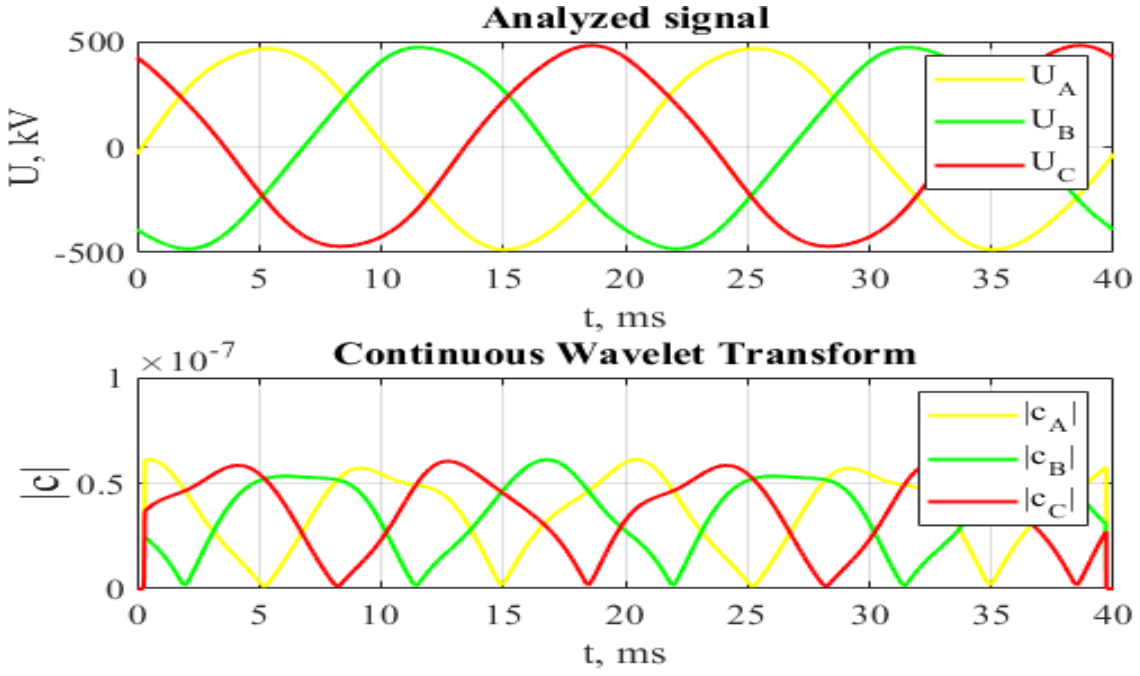


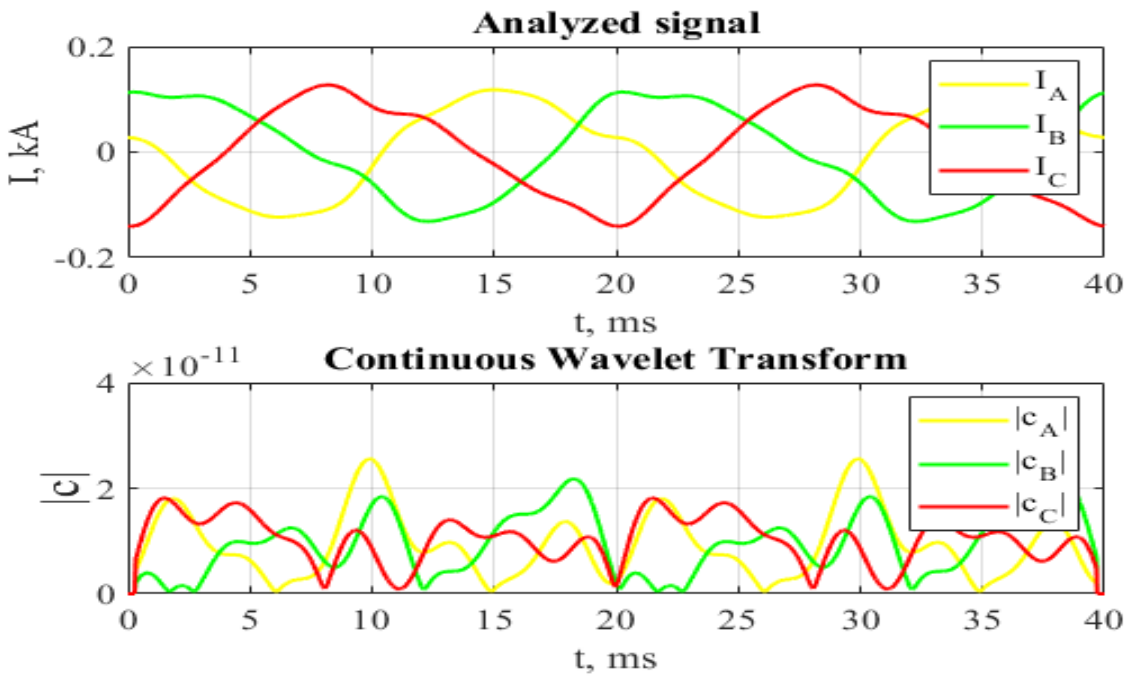
ДЕЙСТВИЕ АЛГОРИТМА ПРИ КОРОТКИХ ЗАМЫКАНИЯХ



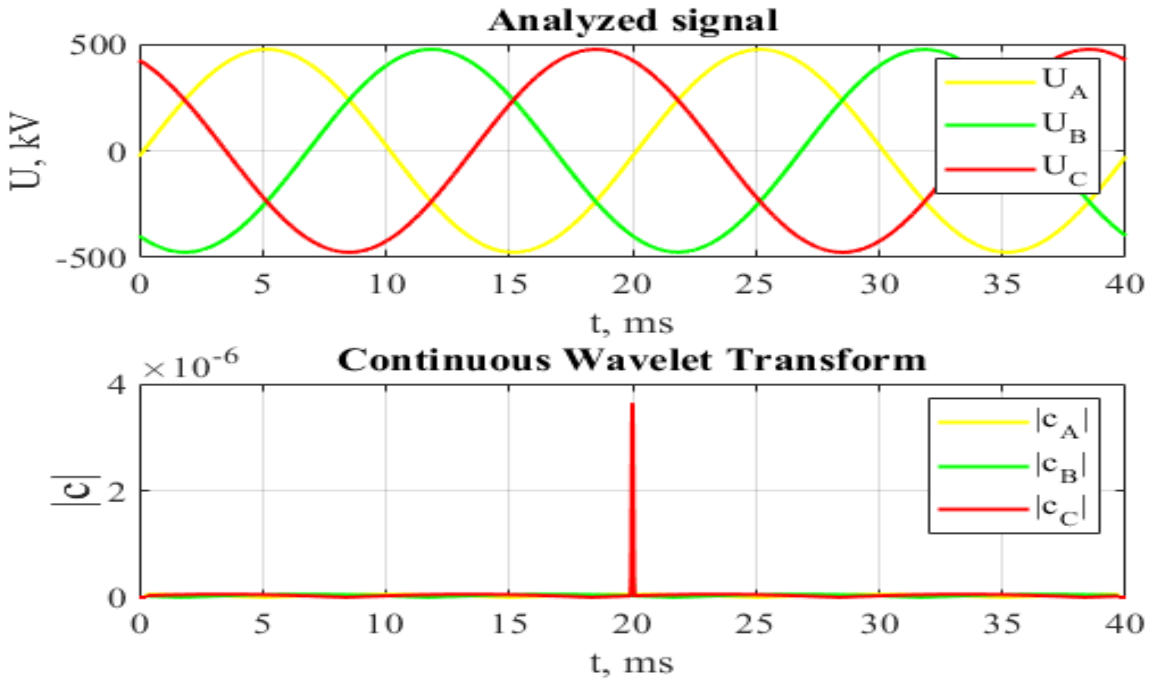


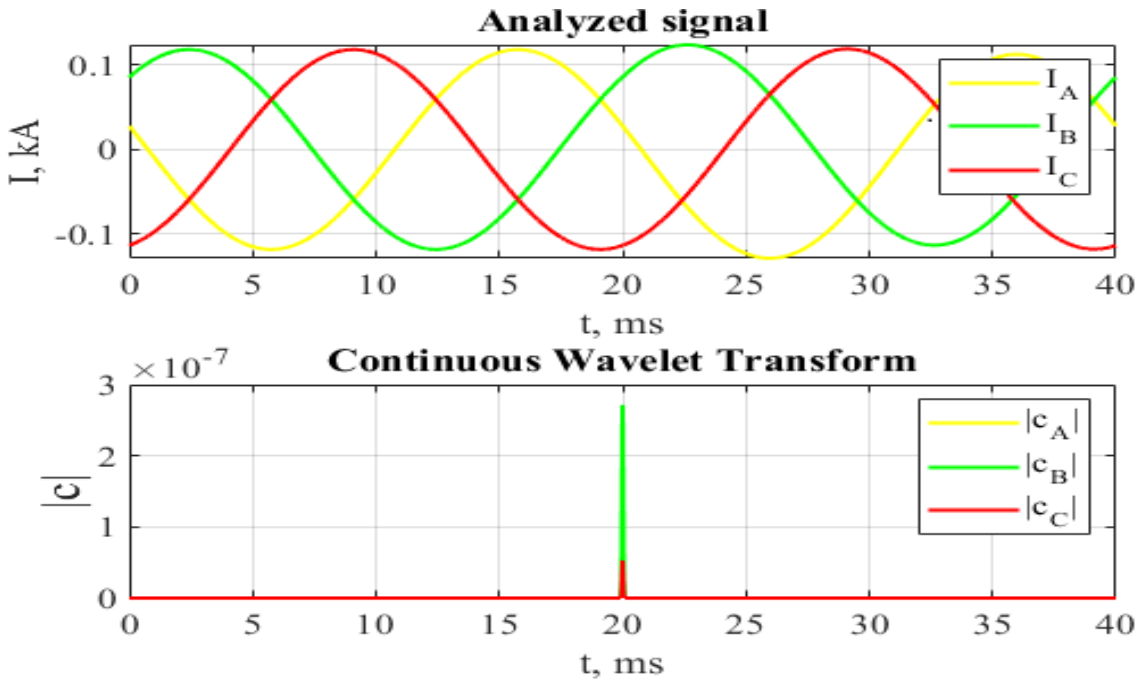
ДЕЙСТВИЕ АЛГОРИТМА ПРИ НЕСИНУСОИДАЛЬНЫХ РЕЖИМАХ



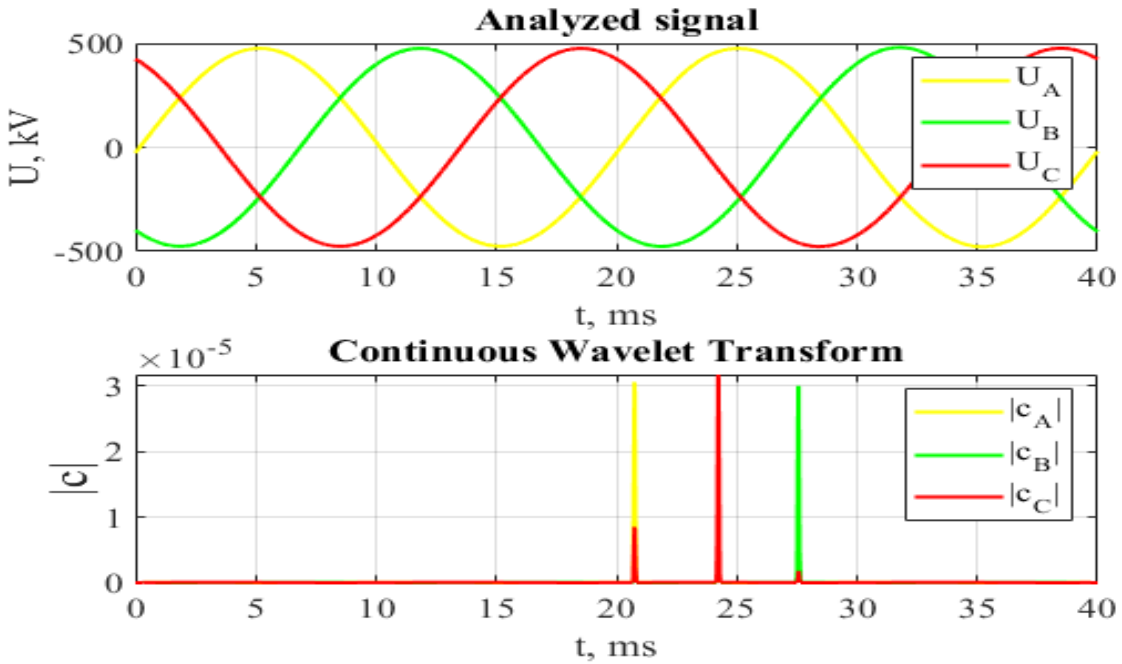


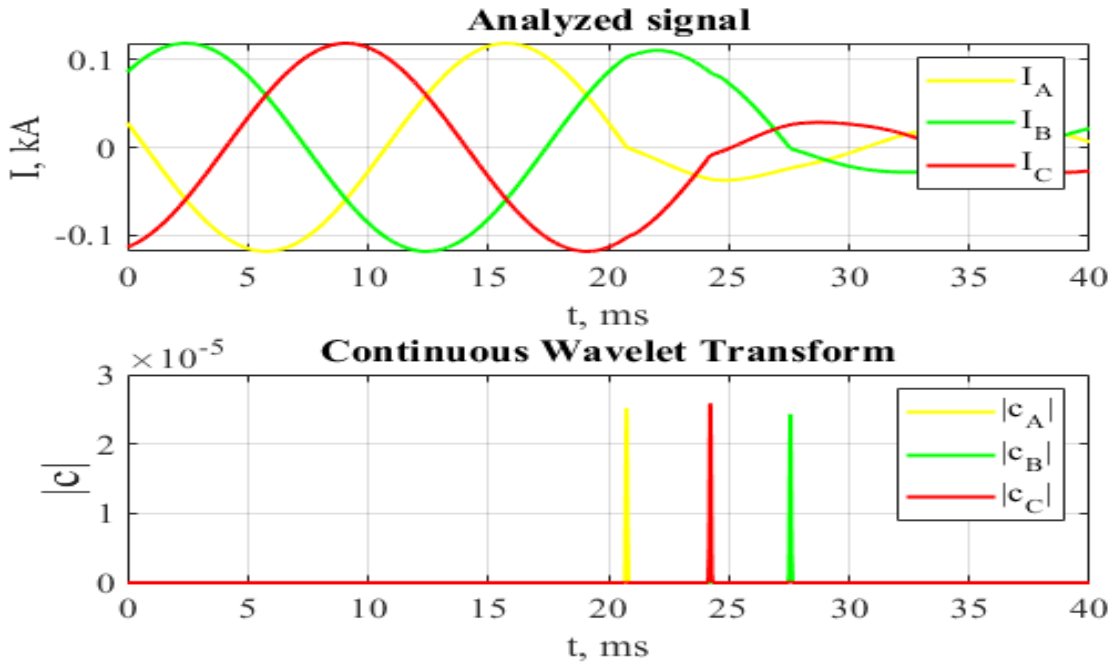
ДЕЙСТВИЕ АЛГОРИТМА ПРИ НАБРОСАХ МОЩНОСТИ



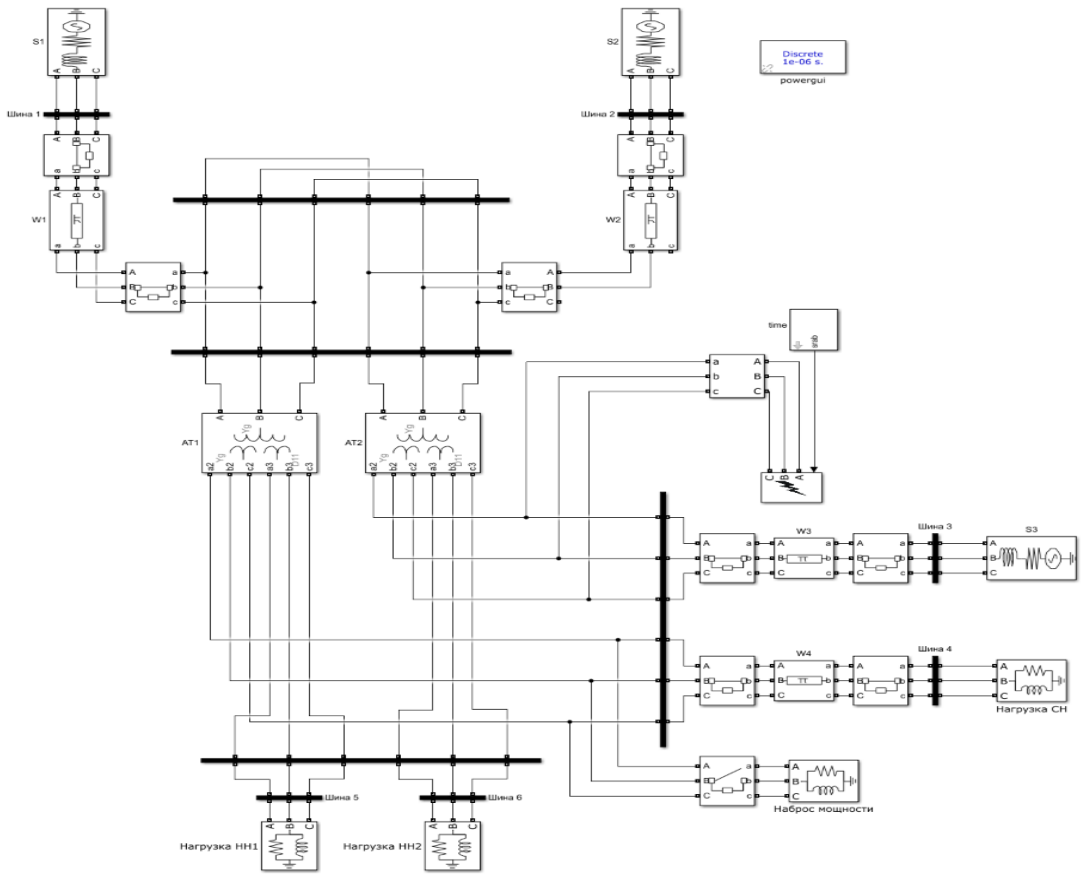


ДЕЙСТВИЕ АЛГОРИТМА ПРИ ОТКЛЮЧЕНИЯХ ЛИНИИ

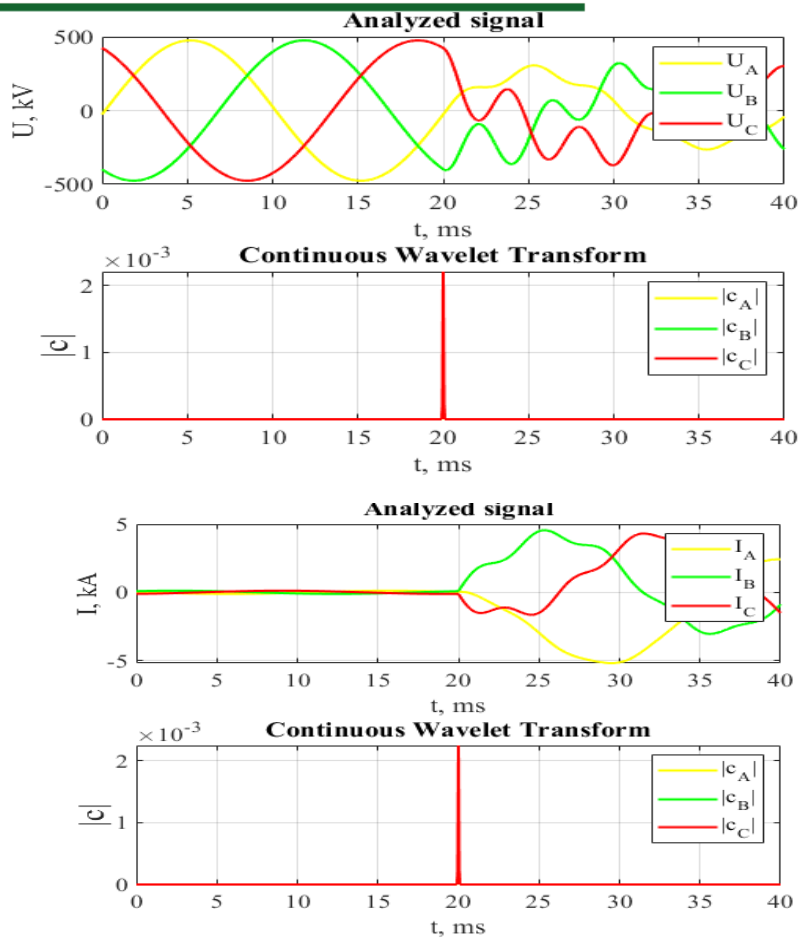




ПРОВЕРКА АЛГОРИТМА НА МОДЕЛИ В СРЕДЕ MATLAB



Модель в среде моделирования Simulink



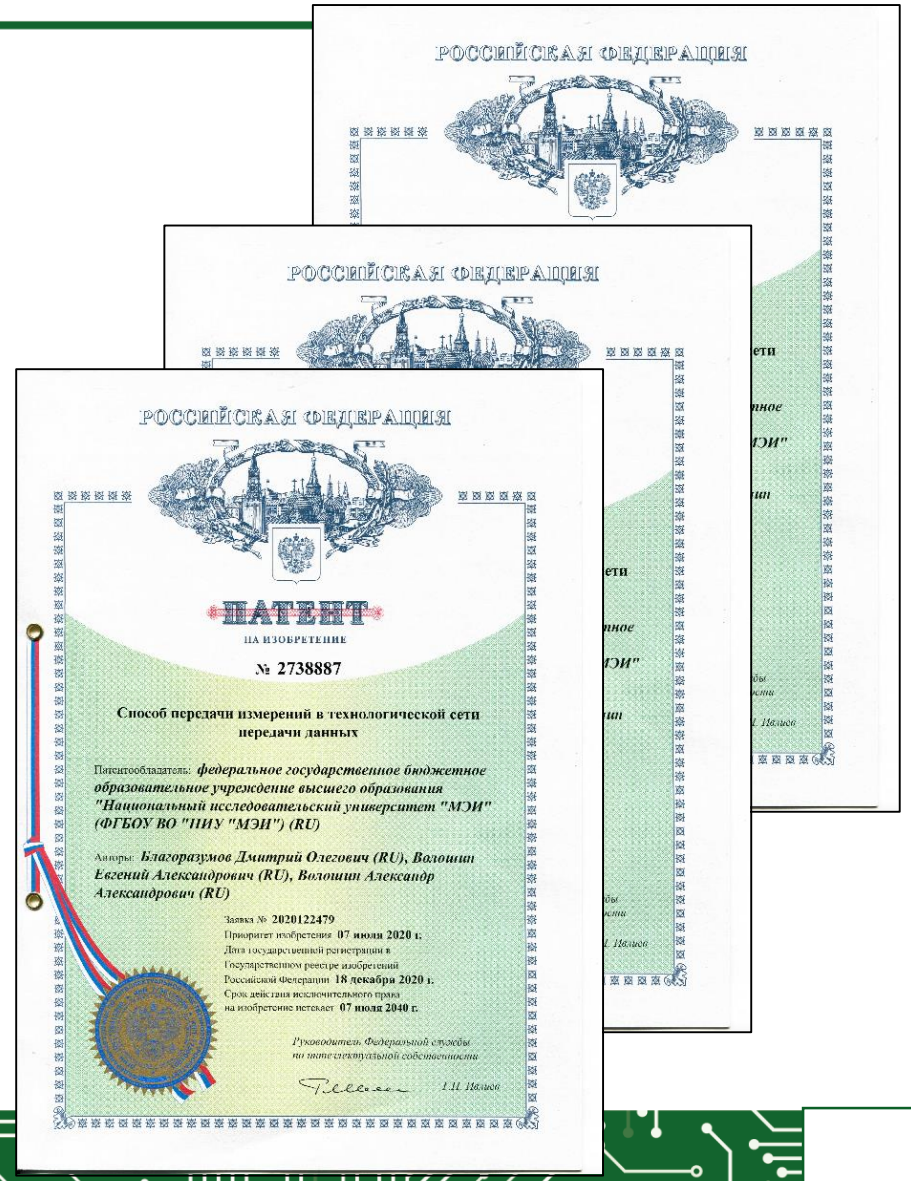
Определение максимума вейвлет-функции для тока и напряжения

СПОСОБЫ ПОВЫШЕНИЯ УСТОЙЧИВОСТИ К КИБЕРАТАКАМ

Способ передачи измерений в технологической сети передачи данных

Способ синхронизации по времени устройств РЗА с использованием параметров аварийного режима

Способ блокирования ложных сигналов аварийного отключения



ВЫВОДЫ

- Был предложен способ обеспечения бесперебойного электроснабжения потребителей с повышением защиты потребителей от кибератак и сохранением высокого качества их защиты от повреждений в сети электроснабжения.
- В основе способа лежит алгоритм фиксации аварийных возмущений в синусоидах тока и напряжения.
- Продемонстрированные опыты показывают, что в момент появления аварийных ситуаций, коротких замыканий, на временной диаграмме модулей комплексных коэффициентов появляется всплеск. В отсутствии коротких замыканий, модули комплексных коэффициентов сохраняют маленькие величины.
- В соответствии с этим, если в цифровых сетях злоумышленниками будет сгенерирован сигнал на отключение от релейной защиты, он будет заблокирован пусковым органом защиты от кибератак.

ЦЕНТР КОМПЕТЕНЦИЙ НТИ
на базе НИУ "МЭИ"
ТЕХНОЛОГИИ ТРАНСПОРТИРОВКИ ЭЛЕКТРОЭНЕРГИИ И РАСПРЕДЕЛЕННЫХ ИНТЕЛЛЕКТУАЛЬНЫХ ЭНЕРГОСИСТЕМ

СПАСИБО ЗА ВНИМАНИЕ!

Докладчик:
Благоразумов Дмитрий Олегович

Контакты:
blagorazumov.do@mail.ru