



ЦЕНТР НТИ МЭИ

ТЕХНОЛОГИИ ТРАНСПОРТИРОВКИ
ЭЛЕКТРОЭНЕРГИИ РАСПРЕДЕЛЕННЫХ
ИНТЕЛЛЕКТУАЛЬНЫХ ЭНЕРГОСИСТЕМ

«Частные вопросы применения системы поддержки принятия решения для управления устойчивостью»

Карантаев В.Г.

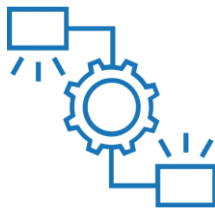
к.т.н. доцент кафедры РЗиАЭ

WWW.NTI.MPEI.RU



Эволюция систем РЗА и требований к ним

Электромеханическая
элементная база



- чувствительность;
- селективность;
- быстродействие;
- надежность

Микропроцессорная
элементная база



Сохраняем старые, но добавляем новые требования:

- Устойчивость функционирования защищаемого объекта
- Кибербезопасность защищаемого объекта
- **Благонадежность (trustworthiness)**

ПРОТОКОЛ

совместного заседания Научно-технического совета НП «НТС ЕЭС»

и Секции по проблемам надёжности и безопасности больших систем энергетики Научного совета РАН по системным исследованиям в энергетике на тему:

«Кибербезопасность РЗА и систем управления современных объектов электроэнергетики»

г. Москва

№

2/20

16 декабря 2020 г.

Парьев С., Правиков Д., Карантаев В. (2020). Особенности применения риск-ориентированного подхода для обеспечения кибербезопасности промышленных объектов //

Безопасность информационных технологий. №4, Том 27. URL: <https://bit.mephi.ru/index.php/bit/article/view/1304>

http://tc194.ru/publicnoe_obsuzhdenie_proektov

<https://blog.iiconsortium.org/2018/10/trustworthiness-and-the-permeation-of-trust-in-iiot-systems.html>

Тенденции в электроэнергетической отрасли

ВИД ИСПОЛНЕНИЯ		на 01.01.2009		на 01.01.2018		на 01.01.2021	
		110-220	330-750	110-220	330-750	110-220	330-750
Эл.мех	РЗ и СА	86%	74%	68%	42%	65%	39%
	ПА	46%	53%	29%	23%	19%	17%
МЭ	РЗ и СА	8%	11%	4%	9%	4%	8%
	ПА	36%	23%	10%	12%	11%	8%
МП	РЗ и СА	6%	15%	28%	49%	31%	53%
	ПА	18%	24%	61%	65%	71%	74%

А.В. Жуков Международная конференция и выставка «Релейная защита и автоматика энергосистем 2021
Доклад: «Развитие РЗА в эпоху цифровизации: цели, задачи, решения.

Современное ИЭУ как объект защиты



Современное ИЭУ и подсистема РЗА – это:

- Компьютерная система.
- Объект критической информационной инфраструктуры.
- Значимый объект критической информационной инфраструктуры.

Современное ИЭУ как объект защиты



КС - это человеко-машинная система, представляющую совокупность электронно-программируемых технических средств обработки, хранения и представления данных, программного обеспечения (ПО), реализующего информационно-коммуникационные технологии (ИКТ) осуществления каких-либо функций, и информации (данных).

Куликов А.Л., Зинин В.М. Требования к информационной безопасности в электроэнергетике и их реализация в интеллектуальных устройствах цифровых подстанций // Интеллектуальная Электротехника. 2022. № 3. С. 49-78. DOI: 10.46960/2658-6754_2022_3_49

Н.А. Гайдамакин. Учебно методический комплекс Теоретические основы компьютерной безопасности Екатеринбург 2008. 212 с.

Влияние требований НПА на методические вопросы создания защищенных ИЭУ



РОССИЙСКАЯ ФЕДЕРАЦИЯ ФЕДЕРАЛЬНЫЙ ЗАКОН

О безопасности критической информационной инфраструктуры Российской Федерации

Принят Государственной Думой

12 июля 2017 года

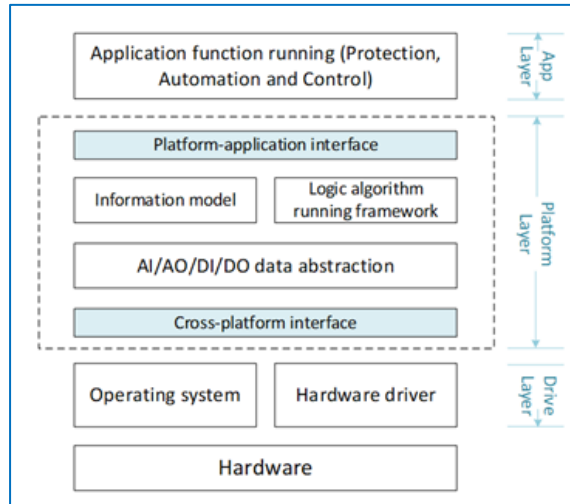
Одобрено Советом Федерации

19 июля 2017 года

Федеральный закон регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (далее также - критическая информационная инфраструктура) в целях ее **устойчивого функционирования при проведении в отношении ее компьютерных атак.**

Компьютерная атака - целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, **в целях нарушения и (или) прекращения их функционирования** и (или) создания угрозы безопасности обрабатываемой такими объектами информации;

Устойчивость функционирования защищаемого объекта



CIGRE B5.60 The schematic diagram of PAC platform software architecture

— это способность объекта сохранять свои основные функции с заданным качеством (в заданных пределах) под воздействием деструктивных факторов (в частности, под воздействием компьютерных атак)

Парьев С., Правииков Д., Карантаев В. (2020). Особенности применения риск-ориентированного подхода для обеспечения кибербезопасности промышленных объектов //

Безопасность информационных технологий. №4, Том 27. URL: <https://bit.mephi.ru/index.php/bit/article/view/1304>

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.



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

Задачи текущего этапа при создании современных ИЭУ

Определить:

- Состав основных функций ИЭУ (минимально необходимых и достаточных)
- Критерии оценки состояния ИЭУ РЗА.
- Способы оценки критериев качества, которые должны быть гарантированы при воздействии компьютерных атак.
- Требования к механизмам безопасности, корректная реализация которых позволит гарантировать заданные критерии качества в заданных пределах.
- Отраслевую организационную структуру и методы оценки соответствия требованиям.

Взаимосвязь классических свойств РЗА и средств их реализации в ИЭУ РЗА

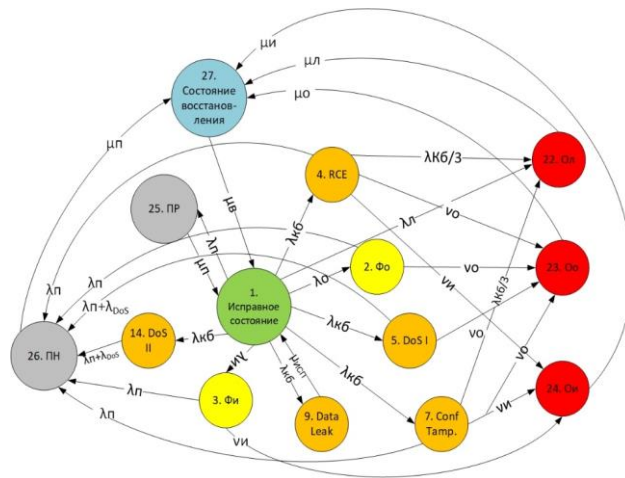
Функция	Средства реализации	Какие свойства РЗА затрагивает
Прием информации от точек контроля [УСО, ЭТТ/ЭТН]	Обмен информацией по ЛВС по протоколу SV + библиотеки/программные модули	Селективность, Надежность
Обработка полученной информации от точек контроля	Библиотеки алгоритмов, Приложение или программный модуль	Селективность, Чувствительность
Обмен информацией с соседними ИЭУ РЗА	Обмен информацией по ЛВС по протоколу GOOSE + библиотеки/программные модули	Надежность
Обмен информацией с дискретными устройствами сопряжения с объектом	Обмен информацией по ЛВС по протоколу GOOSE + библиотеки/программные модули	Надежность
Реализация алгоритма РЗА	Библиотеки алгоритмов, Приложение или программный модуль	Селективность, Чувствительность, Быстродействие, Надежность
Хранение файла(ов) конфигурации (логика РЗА + параметры каждой защиты)	Файл(ы) конфигурации на файловой системе, хранимые на ПЗУ	Селективность, Чувствительность, Быстродействие, Надежность
Использование файла конфигурации	Файл(ы) конфигурации на файловой системе + библиотеки/программные модули чтения данных из файла	Селективность, Чувствительность, Быстродействие, Надежность
Прием и обработка сигналов СОЕВ	Обмен информацией по протоколам RTP, (S)NTP + библиотеки	Селективность, Чувствительность, Надежность

Приведено описание средств реализации функций ИЭУ РЗА, которые обязательно должны сохраняться для поддержания основных свойств РЗА.

Рассматривается минимальный набор основных функций без которых ИЭУ РЗА не может выполнять задачи предотвращения аварий и ограничения последствий технологических нарушений.

Для оценки Кг разработан метод расчета на основе комбинации полумарковского процесса и гибридного способа моделирования угроз ИБ.

№	Описание состояния
1	Исправное состояние ИЭУ РЗА
2	ИЭУ функционирует с дефектом, приводящим к отказу срабатывания
3	ИЭУ функционирует с дефектом, приводящим к излишнему срабатыванию
4	Состояние, в котором на ИЭУ РЗА реализуется угроза исполнения произвольного кода (CVE-2019-10938)
5	... на ИЭУ РЗА реализуется угроза отказа в обслуживании (DoS) (CVE-2019-10931)
6	... на ИЭУ РЗА реализуется угроза подмены конфигурации устройства (CVE-2019-10930)
7	...

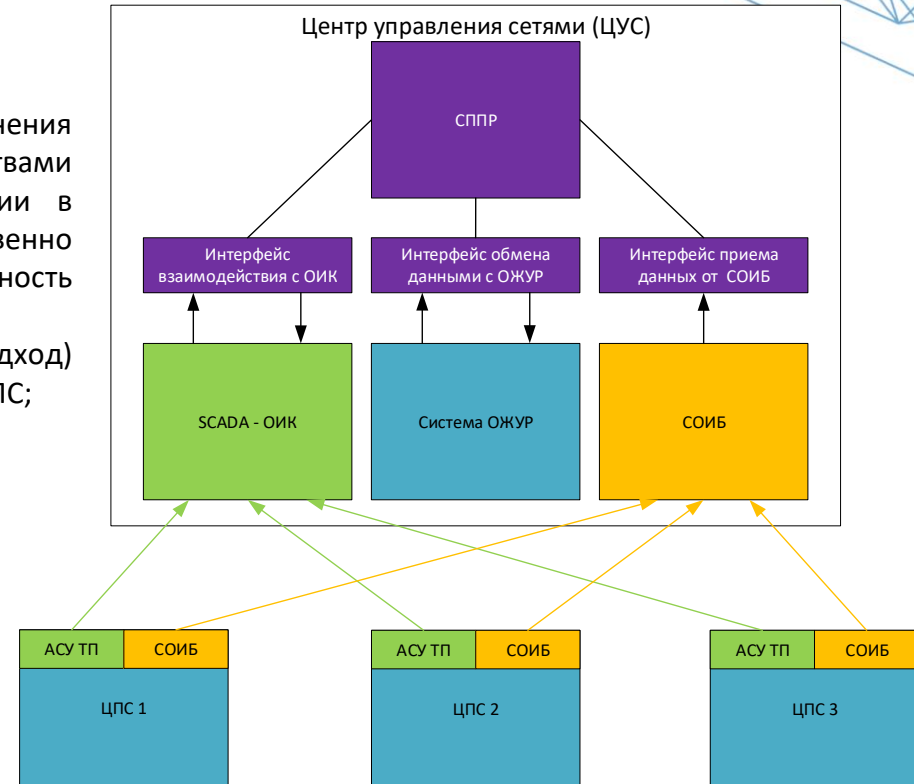


Технологии ИИ в управление компьютерными инцидентами на объектах электроэнергетики

Реальна ли возможность внедрения технологий искусственного интеллекта в управлении компьютерными инцидентами?

Основу ИС СППР составляют:

- Способ расчета показателей надежности с возможностью изменения коэффициентов расчетной модели ИЭУ РЗА, обладающего свойствами ремонтпригодности 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;



Подана заявка на патент на изобретение № 2022114852/28 (031243)

Форма N 91 ИЗ-2017
910,371



Тел.: 8-495-777-01-01
E-mail: info@nauka.ru
Москва
109456

На № - от -
Наш № 2022114852/28(031243)
При переписке просим ссылаться на номер заявки
Исходящая корреспонденция от **13.09.2022**

УВЕДОМЛЕНИЕ
о положительном результате формальной экспертизы
заявки на изобретение

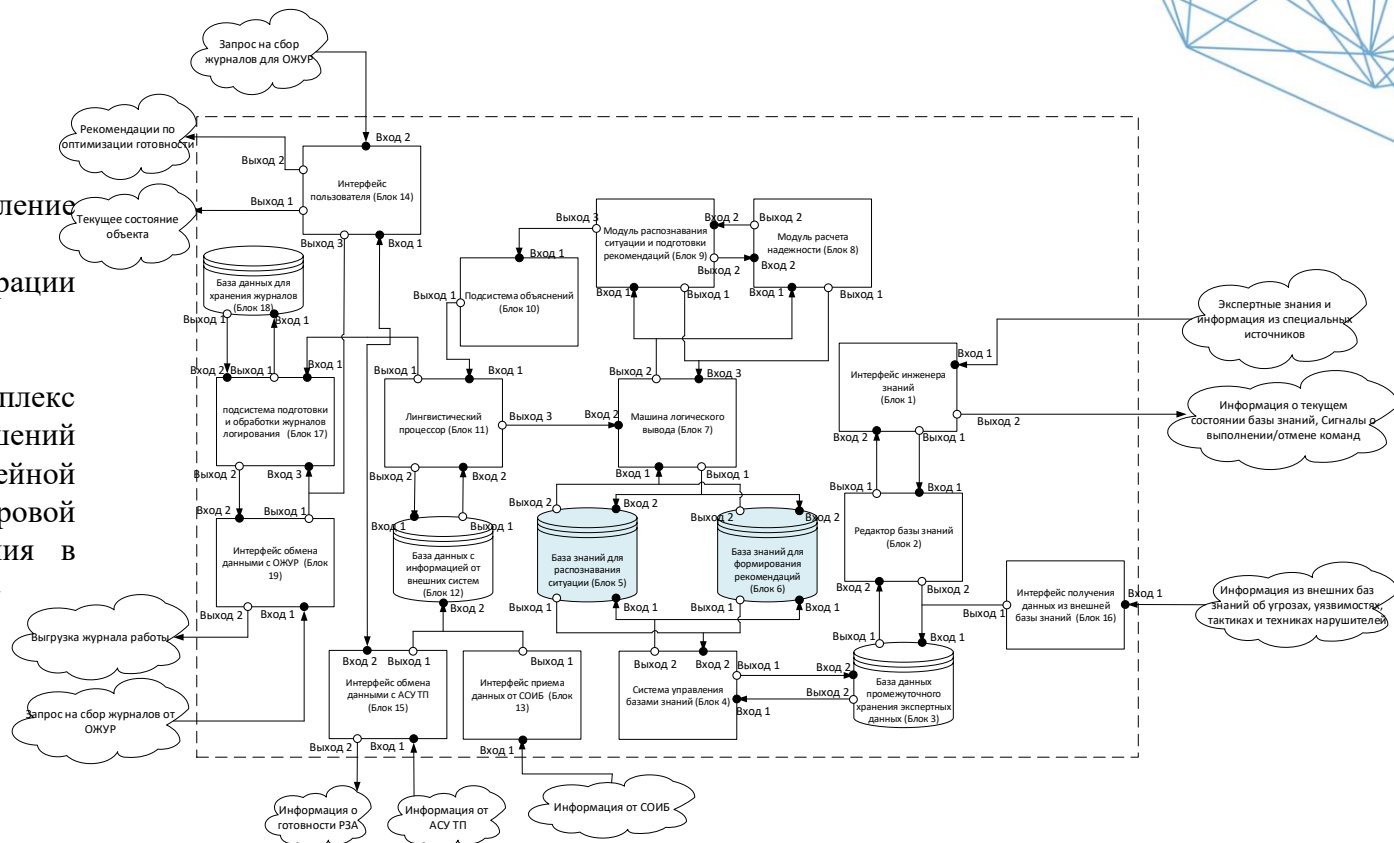
(21) Заявка № 2022114852/28(031243)

Дата поступления документов заявки 01.06.2022

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»



Требования ИБ и механизмы безопасности



В документах МЭК определено, что использование принципа «Secure by Design» наиболее эффективно при создании современных систем и комплексов в Цифровой энергетике.



В НПА РФ зафиксирован приоритет использования ВСЗИ.

Предложения

Разработать и на уровне национального отраслевого стандарта утвердить:

- Политику управления доступом в ИЭУ и подсистему РЗА на основе субъект-сущностного подхода.
- Разработать или адаптировать формальную модель безопасности, наиболее подходящую для реализации в ИЭУ, на основе которой будут разработаны средства защиты информации, входящие в состав ИЭУ.

В формальной модели управления доступом ИЭУ в качестве реализуемых средством защиты информации политик управления доступом предлагаются:

- Ролевая политика доступа
- Политика мандатного контроля целостности

Имплементация на практике моделей безопасности ИЭУ позволит реализовать принцип наименьших привилегий при эксплуатации, что снизит возможность влияния «человеческого фактора» на устойчивость функционирования ЗОКИИ

Предложения

Обязательными механизмами безопасности, реализуемыми в встраиваемой ОС ИЭУ должны стать:

Доверие

- Российские CPU и MCU
- Доверенные операционные системы
- Доверенная загрузка устройства
- Доверенные обновления
- Удаленная аттестация устройства

Аутентификация

- Устройства
- Пользователя
- Обеспечение целостности и аутентичности для данных, передаваемых устройством
- Поддержка LDAP Lightweight Directory Access Protocol)

Сетевая безопасность

- Встроенный МЭ
- Криптографически защищенные протоколы обмена (MMS, GOOSE, МЭК 60870-5-104)

Механизмы безопасности

- Ролевое управление доступом
- Мандатное управление доступом
- Аудит событий безопасности
- Статический и динамический контроль целостности
- Мониторинг и обнаружение атак

Карантаев В. Вопросы реализации киберзащищенной цифровой подстанции на основе российских технологий // Круглый стол НИК D2 РНК СИГРЭ на IX Международной научно-практической конференции «Автоматизация и информационные технологии в энергетике» (Москва, 2019)

Карантаев В. Вопросы реализации доверенных Интеллектуальных Электронных Устройств //«Релейная защита и автоматика энергосистем 2020» 26 – 28 мая 2020 г., Москва

Требования к SOC/CPU:

Chain of Trust:

- RoT: OTP, TPM, SE
- Реализация доверенной среды исполнения (TEE)
- Средство доверенной загрузки
- Механизмы контроля целостности основной ОС и механизмов безопасности

Встроенный датчик случайных чисел

MMU

Многоядерность

Аппаратная реализация PTP

Аппаратная реализация PRP/HSR

Требования к ОС:

Поддержка реального времени

SMP/AMP

Средства отладки

Расширенная длительная техническая поддержка

Длительные сроки поддержки поставляемого SDK

Встроенная подсистема безопасности (монитор безопасности)

Встроенные механизмы безопасности

Криптографическая подсистема

Защищенное хранилище

Доверенное обновление (OTA)



Про кооперацию

Формирование кооперационных цепочек вендоров ИЭУ, СнК , СЗИ и отраслевых экспертных центров взаимовыгодно и позволит разработать защищенные ИЭУ, сократить затраты на их разработку, а также время вывода на рынок. Создаст хороший потенциал экспортопригодных технологий.

Контактная информация

ул. Красноказарменная, д. 17
Москва, Россия

Карантаев Владимир Геннадьевич
к.т.н.

vladimir.karantaev@yandex.ru
тел. +7 (915) 221-15-96

WWW.NTI.MPEI.RU



ЦЕНТР НТИ МЭИ

[Главная](#) [Структура](#) [Видео](#) [Контакты](#) [Отдел научных исследований](#) [Отдел подготовки кадров](#) [Еще](#)

ЦЕНТР НТИ МЭИ

ТЕХНОЛОГИИ
ТРАНСПОРТИРОВКИ
ЭЛЕКТРОЭНЕРГИИ И
РАСПРЕДЕЛЕННЫХ
ИНТЕЛЛЕКТУАЛЬНЫХ
ЭНЕРГОСИСТЕМ