Применение систем поддержки принятия решений в процессах управления объектами электроэнергетики для обеспечения ИБ

VI Международная
научно-техническая конференция
«РЕЛЕЙНАЯ ЗАЩИТА И АВТОМАТИКА»

Карантаев
Владимир

Структура доклада

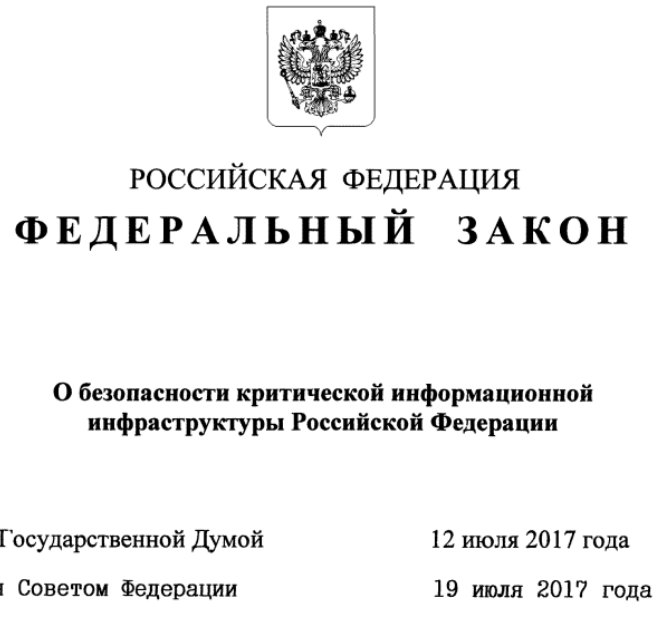
1. Введение;
2. Способ моделирования угроз;
3. Использование технологий искусственного интеллекта для принятия решений в отрасли электроэнергетики;
4. Компьютерный эксперимент;
5. Практическая значимость.

Многолетние отраслевые тренды

- Количество высокоавтоматизированных объектов ЭЭ будет расти.
- Будет увеличиваться доля МП устройств РЗА.
- Возможность проведения КА сохранится.
- Потенциал нарушителей может вырасти.
- Специалистов в области информационной безопасности и кибербезопасности будет по прежнему не хватать.

  (Экспертов всегда не бывает много)

Влияние требований НПА на методические вопросы создания защищенных ИЭУ, АСУ, ИУС



РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

О безопасности критической информационной инфраструктуры Российской Федерации

Принят Государственной Думой 12 июля 2017 года

Одобрен 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.

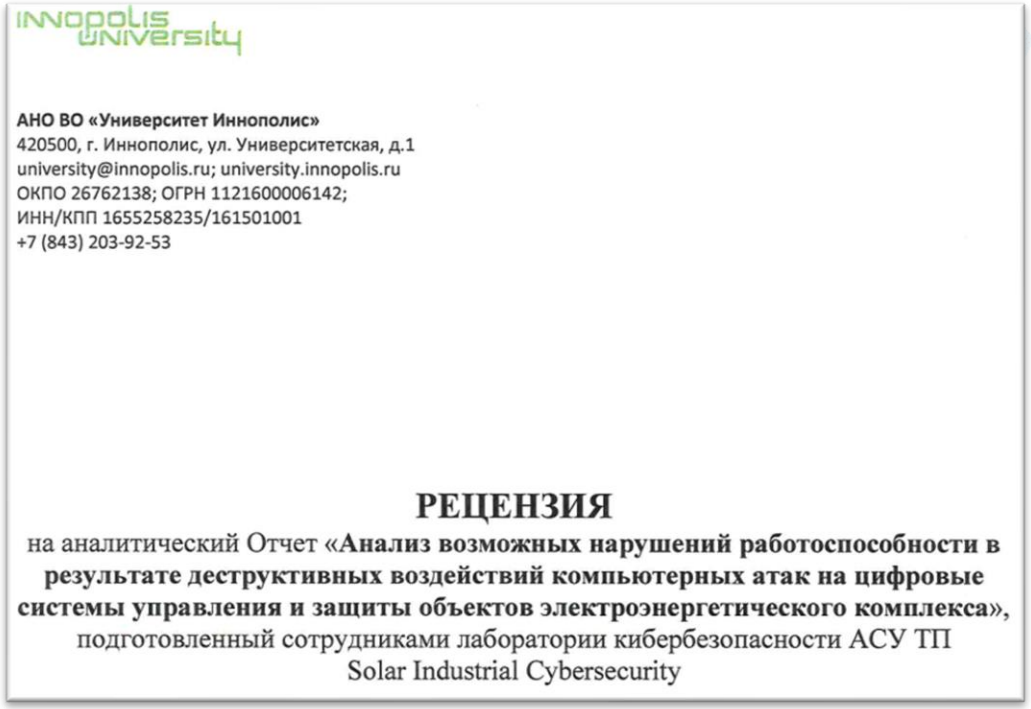
Компьютерная атака - целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания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

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»

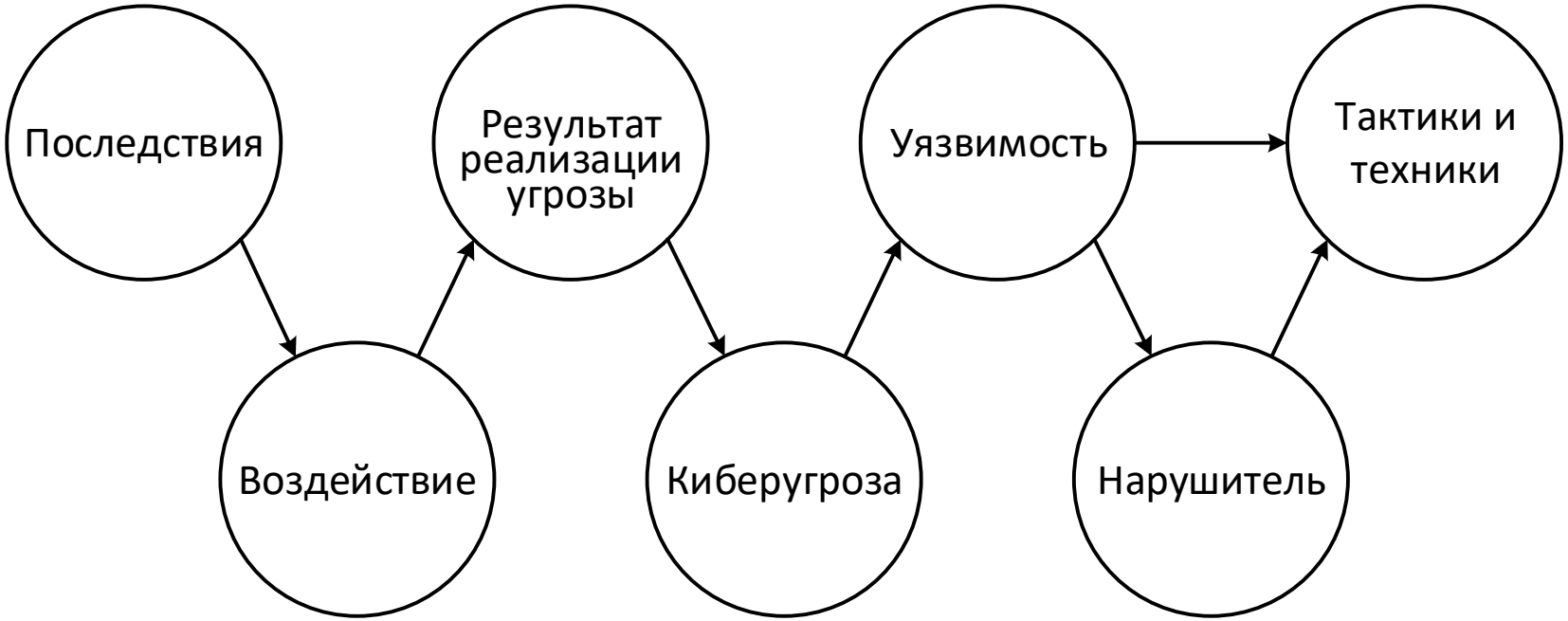
Connect Карантаев В.Г., Карпенко В.И. Анализ нарушений работоспособности объектов электроэнергетики вследствие кибератак/Connect 2020 г./ № 1–2 11–12 с.

Актуальные задачи при обеспечении безопасности ОКИИ в ЭЭ

Необходимость организации:

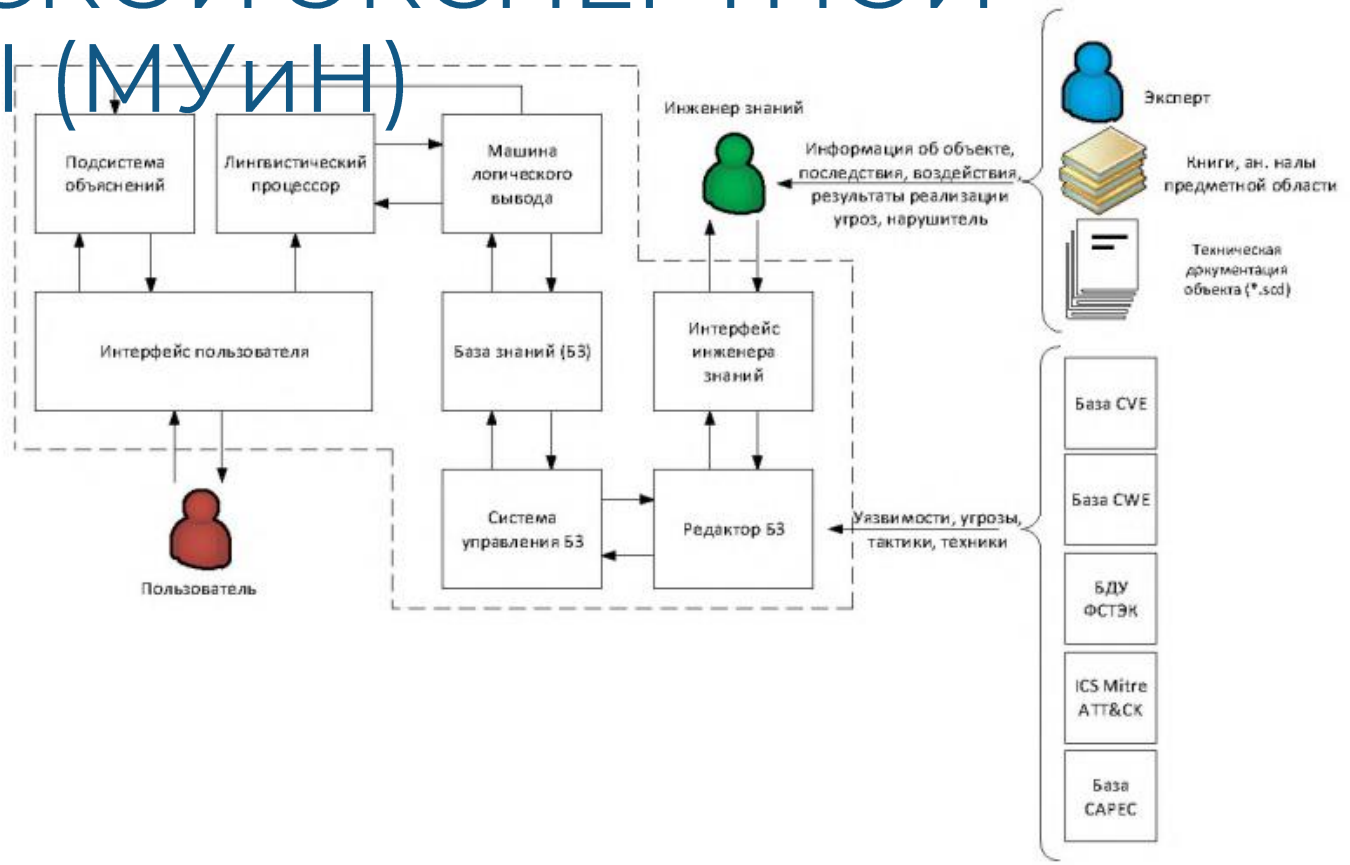
- ✓ Разработки методической основы для моделирования угроз с учетом отраслевой специфики.
- ✓ Управления уязвимостями в АСУ и САУ в условиях ограниченных ресурсов.
- Организация реагирования на КА в АСУ и САУ в условиях ограниченных ресурсов и особенностей управления технологическим процессом.
- Организация расследования аварий и последствий КИ.

СПОСОБ МОДЕЛИРОВАНИЯ УГРОЗ КИБЕРБЕЗОПАСНОСТИ



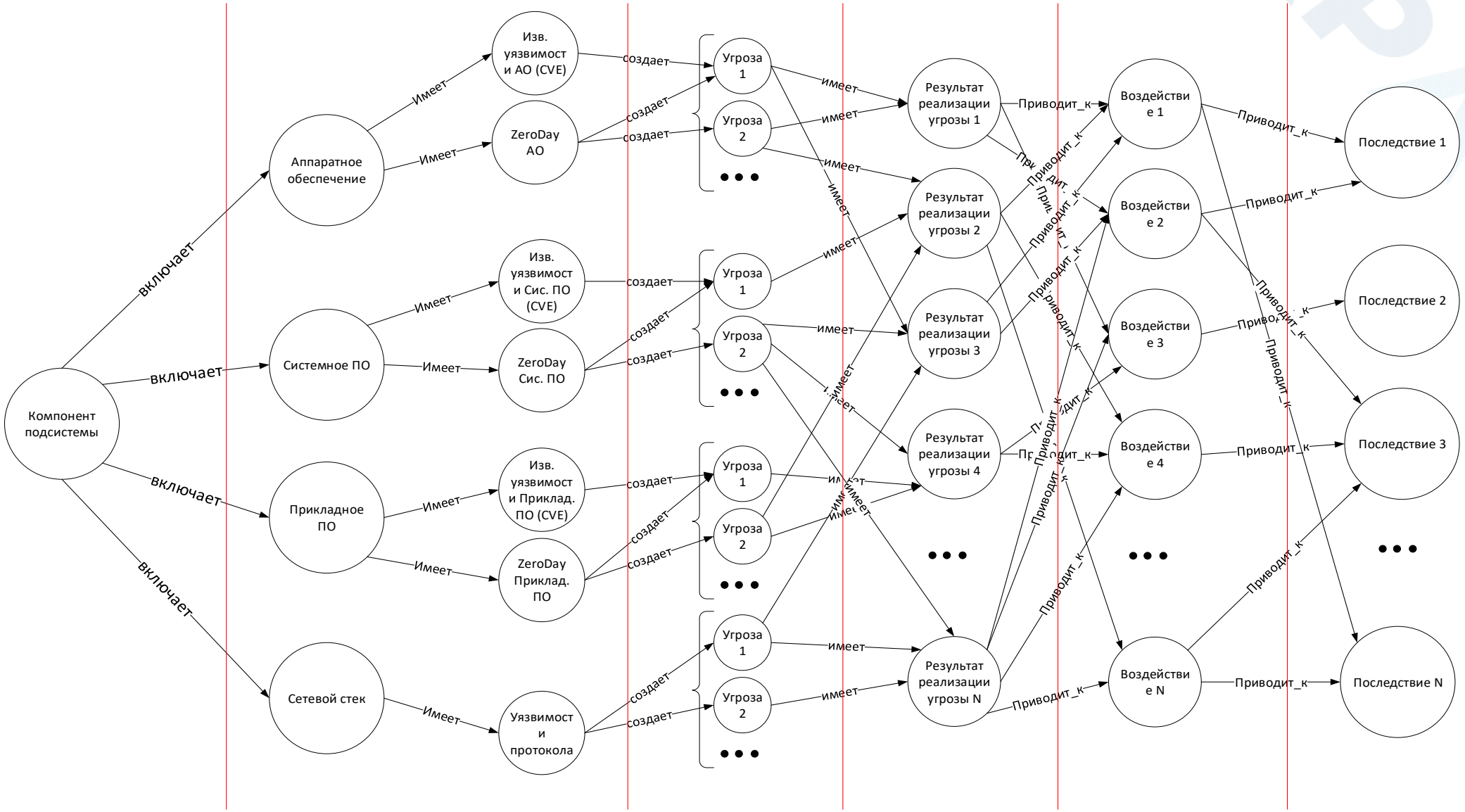
Карпенко, В. И. разработка экспертной системы для оценки влияния деструктивных воздействий компьютерных атак на подстанции с высшим классом напряжения 500 кВ с децентрализованной архитектурой вторичных подсистем / В. И. Карпенко, В. Г. Карантаев // Современные тенденции развития цифровых систем релейной защиты и автоматики : Материалы научно-технической конференции молодых специалистов в рамках форума «РЕЛАВЭКСПО-2021», Чебоксары, 20–22 апреля 2021 года. – Чебоксары: Чувашский государственный университет имени И.Н. Ульянова, 2021. – С. 186-199. – EDN SHDEND.

ОБЩАЯ АРХИТЕКТУРА СТАТИЧЕСКОЙ ЭКСПЕРТНОЙ СИСТЕМЫ (МУиН)

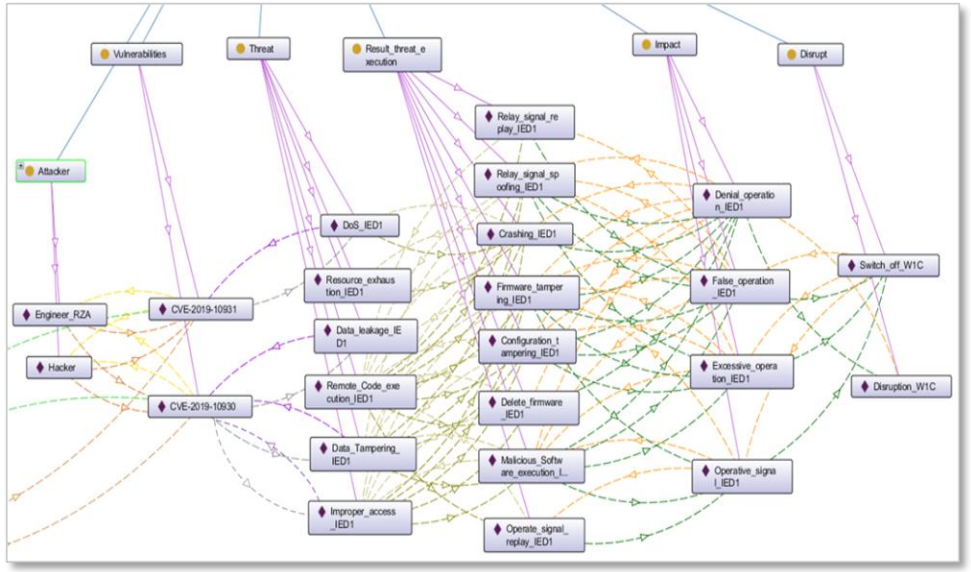


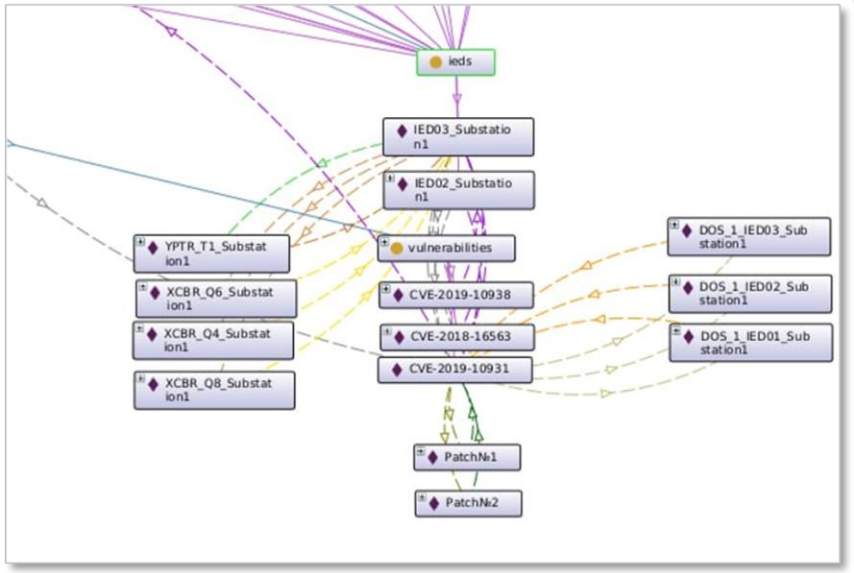
Карпенко, В. И. разработка экспертной системы для оценки влияния деструктивных воздействий компьютерных атак на подстанции с высшим классом напряжения 500 кВ с децентрализованной архитектурой вторичных подсистем / В. И. Карпенко, В. Г. Карантаев // Современные тенденции развития цифровых систем релейной защиты и автоматики : Материалы научно-технической конференции молодых специалистов в рамках форума «РЕЛАВЭКСПО-2021», Чебоксары, 20–22 апреля 2021 года. – Чебоксары: Чувашский государственный университет имени И.Н. Ульянова, 2021. – С. 186-199. – EDN SHDEND.

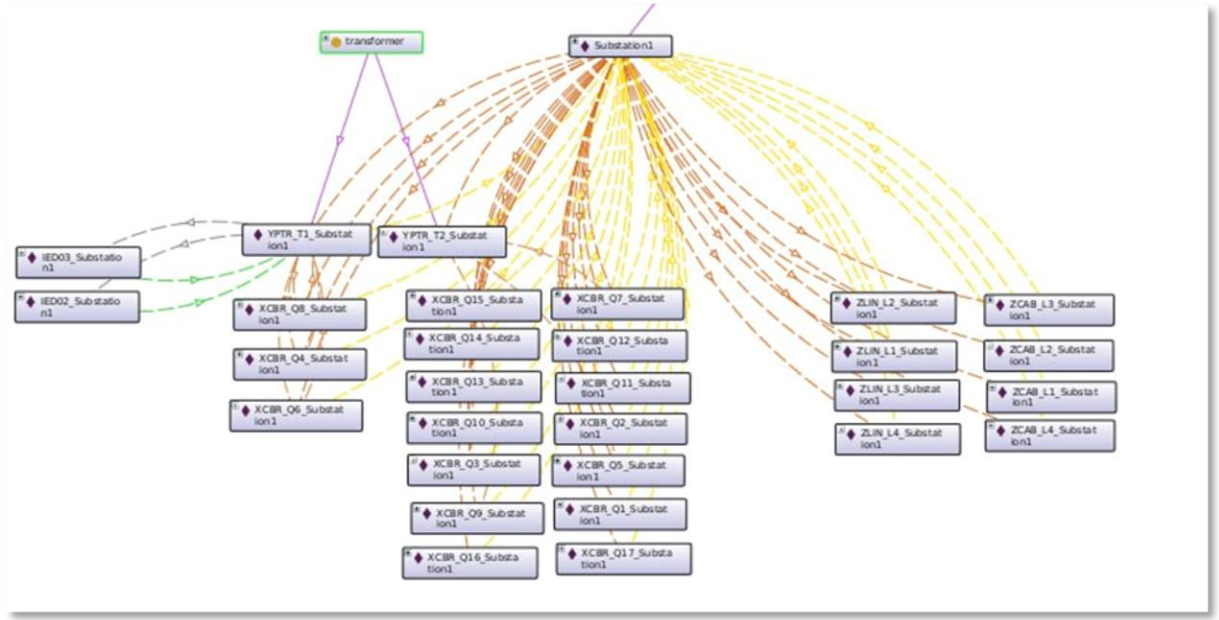
Проект онтологии



Пример онтологии СППР







Задачи текущего этапа при создании современных ИЭУ, АСУ, ИУС

Определить:

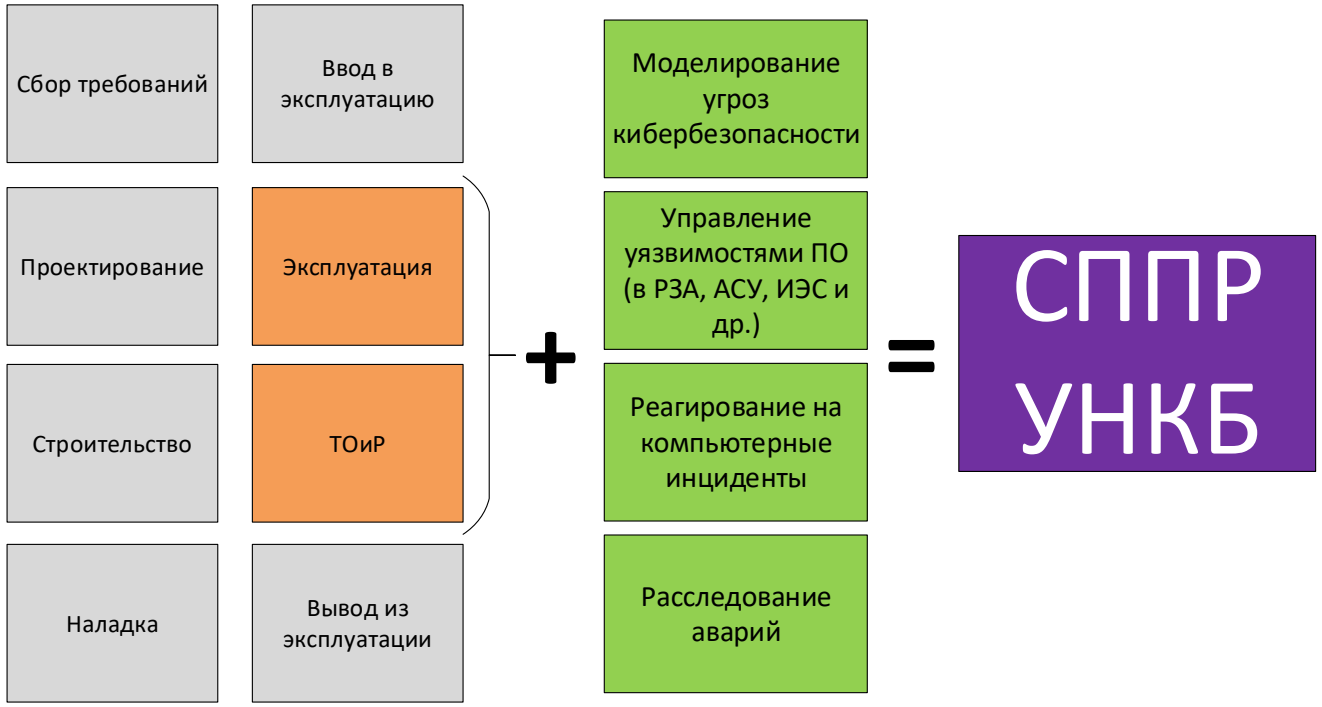
- Состав основных функций (минимально необходимых и достаточных).
- **Критерии оценки состояния.**
- **Способы оценки критериев качества, которые должны быть гарантированы при воздействием компьютерных атак.**
- Требования к механизмам безопасности, корректная реализация которых позволит гарантировать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

Все приведенные пункты справедливы как для **ИЭУ РЗА**, так и для отраслевых **АСУ** и **ИУС**, в связи схожестью технологического стека:

- Аппаратное обеспечение.
- Системное ПО.
- Прикладное ПО.

Стадии жизненного цикла объектов ЭЭ

На Рисунке выделены стадии жизненного цикла объекта электроэнергетики и задачи обеспечения информационной безопасности в их течении. Для решения обозначенных задач предлагается использовать систему поддержки принятия решений «Управление надежностью и кибербезопасностью» (СППР УНКБ)



ВИДЫ ЗАДАЧ ПРИНЯТИЯ РЕШЕНИЙ (ЗПР)

Задачи принятия решений делятся на:

- Хорошо формализованные
- Плохо формализованные

Условия принятия решений классифицируются:

- Условия определенности
- Условия риска
- Условия неопределенности

Плохо формализуемым ЗПР обычно соответствует принятие решений в условиях неопределенности или риска и качественное задание цели

Башлыков А.А., Основы конструирования интеллектуальных систем поддержки принятия решений в атомной энергетике

Отраслевые задачи принятия решений (ЗПР)

Группа задач:

- Провести моделирование угроз ИБ (позволяет говорить об ЭС и онтологии),
- Оценить показатели «функциональной надежности»,
- Оценить возможность наступления киберфизических последствий (позволяет говорить об ЭС и онтологии),
- Оценить потенциальные ущербы,
- Провести категорирование объектов КИИ систем распределенных высокоавтоматизированных объектов электроэнергетики в следствии проведения КА.

Решения, которые предстоит принять:

- Определить и утвердить:
- Перечень актуальных сценариев КА, техник и тактик нарушителей
- Перечень возможных киберфизических последствий,
- Перечень недопустимых событий в работе подсистем высокоавтоматизированных объектов электроэнергетики в следствии проведения КА»
- Уровень ущербов

Вид ЗПР: плохо формализованная ЗПР

Отраслевые задачи принятия решений (ЗПР)

Группа задач:

- «Организация управления уязвимостями в ПО МП ИЭУ РЗА распределенных высокоавтоматизированных объектов электроэнергетики»,
- Штатная ситуация
- Внештатный ситуация

Решения, которые предстоит принять:

- Выбрать объекты ЭЭ и конкретные виды МП ИЭУ РЗА (виды защит) для проведения работ в условиях существующих объективных ресурсных ограничений в определенных заранее ситуациях

Вид ЗПР: плохо формализованная ЗПР

Отраслевые задачи принятия решений (ЗПР)

Группа задач:

- Реагирование на КИ в подсистеме РЗА высокоавтоматизированных объектов электроэнергетики.

Решения, которые предстоит принять:

- Выбрать объекты ЭЭ и конкретные виды МП ИЭУ РЗА (виды защит) для проведения работ в условиях существующих объективных ресурсных ограничений.
- Провести действия в рамках оперативно-технологического управления в условиях проведения КА в отношении высокоавтоматизированных объектов электроэнергетики.
- Провести действия в рамках этапа «расследования аварий».

Вид ЗПР: плохо формализованная ЗПР

Стратегические задачи

Разработка практических подходов к:

- Переводу принятия решений по управлению ОЭ в условиях совершения КА из класса слабо формализованных задач в хорошо формализованные.
- Управление показателями "функциональной надежности" и отказоустойчивости подсистемы РЗА высокоавтоматизированных объектов электроэнергетики, в том числе, в условиях совершения КА.
- Оптимизация показателей "функциональной надежности" и отказоустойчивости подсистемы РЗА высокоавтоматизированных объектов электроэнергетики , в том числе, в условиях совершения КА.

Реальность внедрения технологий искусственного интеллекта

К компьютерным информационным системам, ориентированным на решение Задач Принятия Решений в наиболее общем виде относят:

- Системы принятия решений (СПР)
- Системы поддержки принятия решений (СППР)
- Экспертные системы, которые могут быть частью СППР

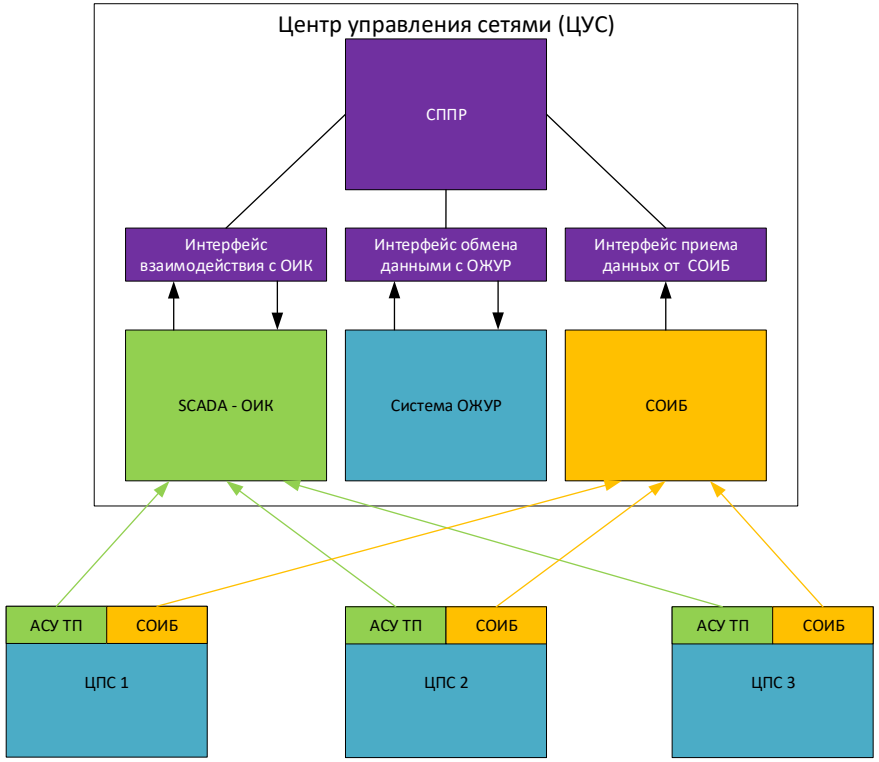
По мнению авторов решение поставленных задач возможно путем разработки

Интеллектуальной СППР – экспертной СППР, ориентированной на поиск решений в указанных предметных областях: информационная безопасность, кибербезопасность, функциональная надежность, оперативно-технологическое управление, использующая знания высококвалифицированных специалистов-экспертов этих предметных областей.

Технологии ИИ в ЗПР по управлению объектами электроэнергетики

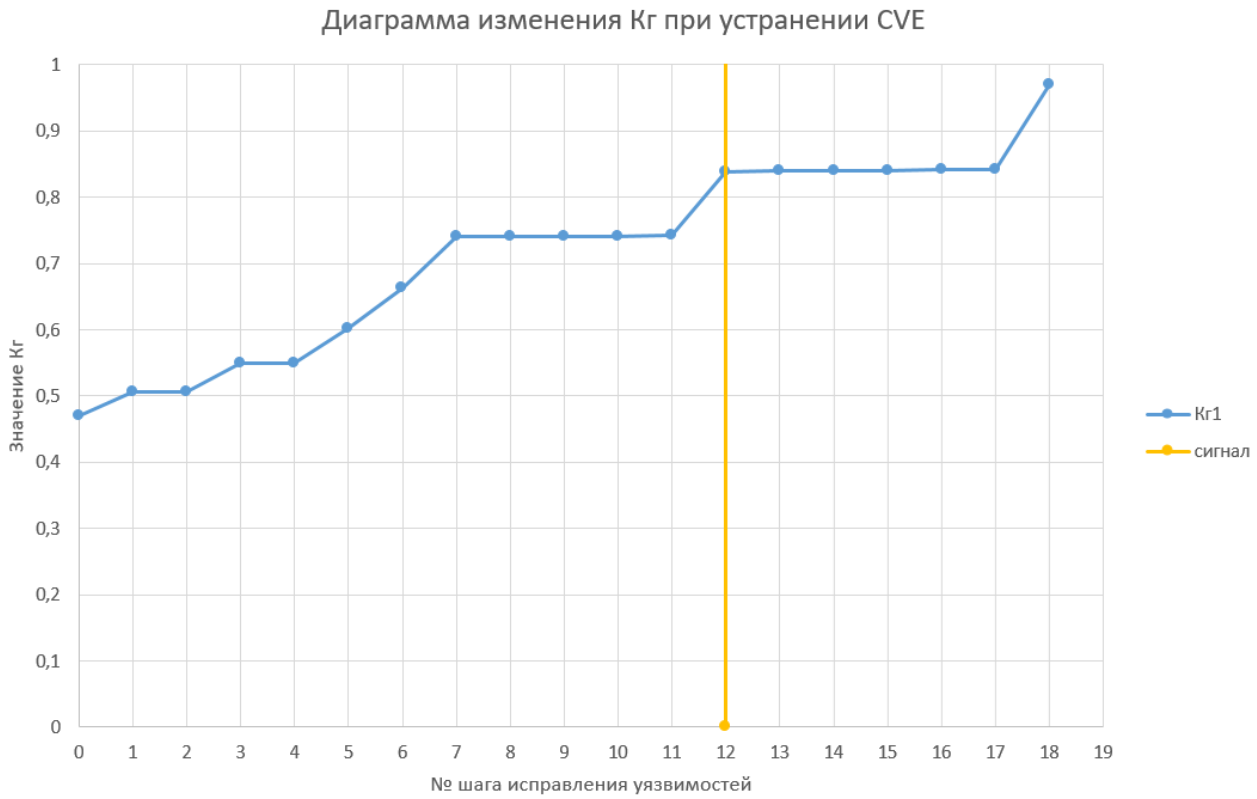
Основу ИС СППР составляют:

- Гибридный способ Моделирования угроз (слайд№6).
- Способ количественной оценки влияния мер по управлению уязвимостями программного обеспечения на повышение коэффициента готовности программно-аппаратного микропроцессорного интеллектуального устройства (ПАК МП ИЭУ), основанного на математической имитационной модели (слайд№20).
- Способ количественной оценки влияния компьютерных атак на надежность функционирования программно-аппаратного микропроцессорного интеллектуального устройства (ПАК МП ИЭУ) релейной защиты и автоматики (слайд№19).
- Задействованы подходы инженерии знаний (Онтологический подход) для моделирования угроз кибербезопасности подсистемы РЗА ЦПС (слайды№7-9).



Компьютерный эксперимент. Управление надежностью ИЭУ РЗА

№ шага	Кг	Устраненная уязвимость CVE
0	0,46933	Исходное положение
1	0,50625	CVE-2019-10930
2	0,50657	CVE-2019-10931
3	0,54985	CVE-2021-33719
4	0,55023	CVE-2019-12255
5	0,60167	CVE-2019-12260
6	0,66372	CVE-2019-12261
7	0,74004	CVE-2019-12263
8	0,74004	CVE-2019-12265
9	0,74073	CVE-2019-12258
10	0,74142	CVE-2019-12259
11	0,74211	CVE-2019-12264
12	0,83883	CVE-2019-12257
13	0,83972	CVE-2021-33720
14	0,8406	CVE-2021-37206
15	0,8406	CVE-2021-41769
16	0,84149	CVE-2018-11451
17	0,84238	CVE-2018-16563
18	0,96925	CVE-2019-10938



Карантаев, В. Г. Количественный анализ влияния компьютерных атак на надежность функционирования ИЭУ РЗА цифровой подстанции / В. Г. Карантаев, В. И. Карпенко // Релейная защита и автоматизация. – 2022. – № 4(49). – С. 43-48. – EDN EQYTWW.

Задача оптимизации использования ресурсов для повышения готовности подсистемы РЗА в условиях влияния компьютерных атак

Отраслевая задача: Планирование работ по обеспечению безопасности ЗОКИИ (ИЭУ РЗА) (управление уязвимостями (УУ), обновление программного обеспечения (ОПО)) на этапе их эксплуатации в условиях ограниченности трудового ресурса инженерного персонала;

Задача исследования: Оптимизировать использование трудовых ресурсов инженерного персонала для УУ и ОПО системного и прикладного ПО ИЭУ РЗА в целях максимизации готовности подсистемы РЗА действующих объектов электроэнергетики.

Критерии оптимизации:

1. Максимальный стационарный коэффициент готовности основной и резервной РЗА электрического присоединения.
2. Максимальная загрузка инженерного персонала с учетом их ресурса.
3. Минимальный простой силового оборудования.

Задача оптимизации. Входные данные

Входные данные:

- SSD файл подстанции;
- CIM модель электрической сети;
- CID от ИЭУ РЗА;
- Описание уязвимостей ИЭУ РЗА из открытых источников (MITRE CVE, BDU FSTEC);
- Информация о ресурсах инженерного персонала для проведения работ по УУ и ОПО;
- Карта дорог между подстанциями;
- График ремонтов силового оборудования;
- График ТОиР РЗА;
- Информация о доступных патчах безопасности;

Приоритеты критериев выбора объекта для работ:

1. Мощность объекта → поиск max
2. Класс напряжения объекта → поиск max
3. Объем работ по ИЭУ РЗА → поиск max
4. Тип объекта → поиск max
5. Мощность оборудования → поиск max
6. Класс напряжения оборудования → поиск max
7. Коэффициент готовности резервированной РЗА → поиск min
8. Категории потребителей (чем выше категория и выше доля → поиск max
9. Время в пути до объекта → поиск min

Задача оптимизации. Результаты и эффекты

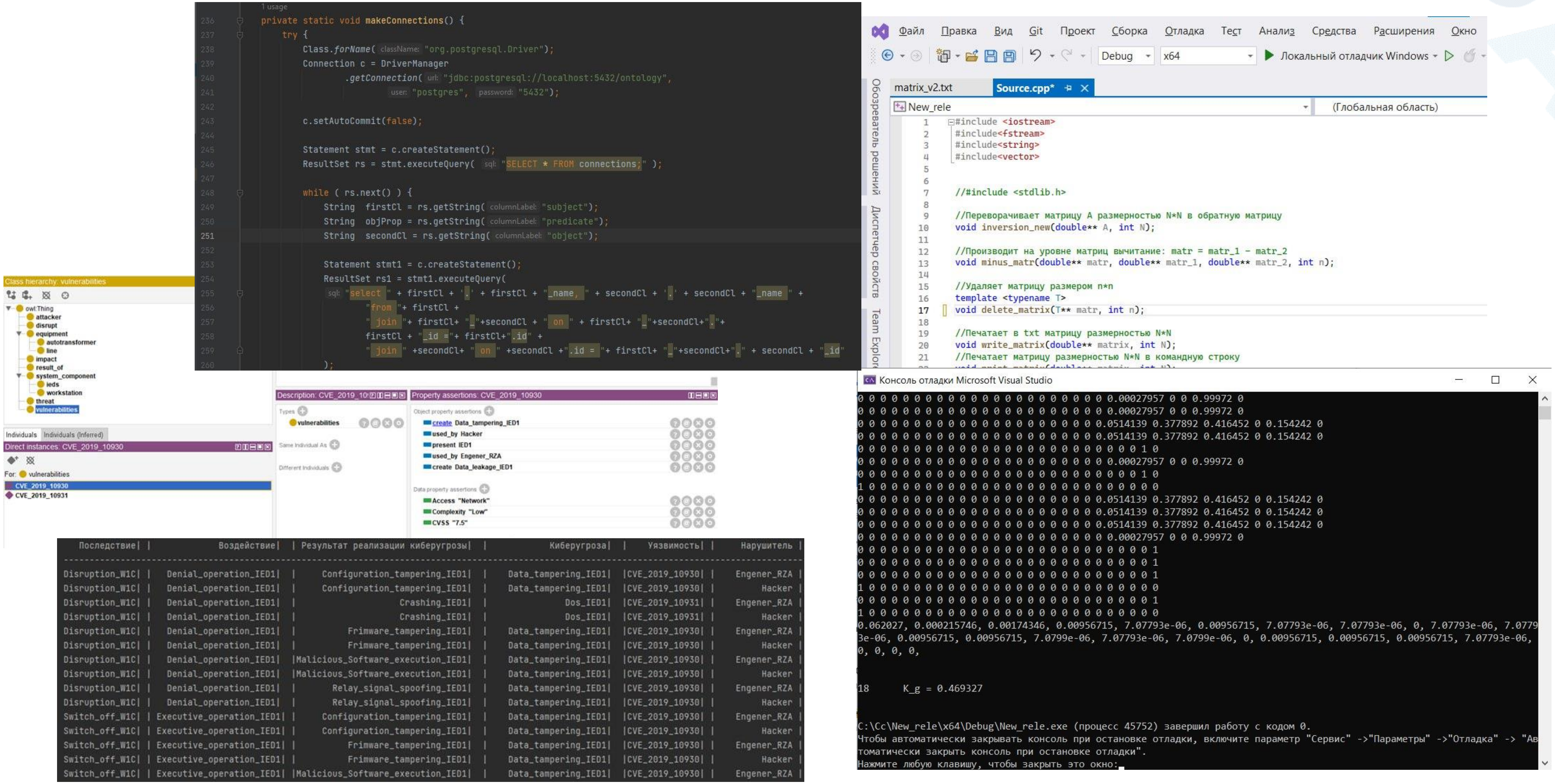
Результат работы алгоритма: журнал перемещений и работ для инженерных бригад на 30 дней.

Журнал содержит записи вида: *объект (ПС) – присоединение – ИЭУ РЗА – вид работ – статус (выполнено/в работе и др.)*

Эффекты от применения СППР:

1. Сокращение времени на принятие решения о действиях инженерного персонала для работ по УУ и ОПО;
2. Повышение устойчивости ИЭУ РЗА при проведении в отношении них компьютерных атак;
3. Сокращение расхода горюче-смазочных материалов для обеспечения транспортировки инженерного персонала;
4. Повышение надежности электроснабжения в подведомственном районе;

Компьютерный эксперимент. Управление надежностью ИЭУ РЗА



Последствие	Воздействие	Результат реализации киберугрозы	Киберугроза	Уязвимость	Нарушитель
Disruption_W1C	Denial_operation_IED1	Configuration_tampering_IED1	Data_tampering_IED1	CVE_2019_10930	Engener_RZA
Disruption_W1C	Denial_operation_IED1	Configuration_tampering_IED1	Data_tampering_IED1	CVE_2019_10930	Hacker
Disruption_W1C	Denial_operation_IED1	Crashing_IED1	Dos_IED1	CVE_2019_10931	Engener_RZA
Disruption_W1C	Denial_operation_IED1	Crashing_IED1	Dos_IED1	CVE_2019_10931	Hacker
Disruption_W1C	Denial_operation_IED1	Frimware_tampering_IED1	Data_tampering_IED1	CVE_2019_10930	Engener_RZA
Disruption_W1C	Denial_operation_IED1	Frimware_tampering_IED1	Data_tampering_IED1	CVE_2019_10930	Hacker
Disruption_W1C	Denial_operation_IED1	Malicious_Software_execution_IED1	Data_tampering_IED1	CVE_2019_10930	Engener_RZA
Disruption_W1C	Denial_operation_IED1	Malicious_Software_execution_IED1	Data_tampering_IED1	CVE_2019_10930	Hacker
Disruption_W1C	Denial_operation_IED1	Relay_signal_spoofing_IED1	Data_tampering_IED1	CVE_2019_10930	Engener_RZA
Disruption_W1C	Denial_operation_IED1	Relay_signal_spoofing_IED1	Data_tampering_IED1	CVE_2019_10930	Hacker
Switch_off_W1C	Executive_operation_IED1	Configuration_tampering_IED1	Data_tampering_IED1	CVE_2019_10930	Engener_RZA
Switch_off_W1C	Executive_operation_IED1	Configuration_tampering_IED1	Data_tampering_IED1	CVE_2019_10930	Hacker
Switch_off_W1C	Executive_operation_IED1	Frimware_tampering_IED1	Data_tampering_IED1	CVE_2019_10930	Engener_RZA
Switch_off_W1C	Executive_operation_IED1	Frimware_tampering_IED1	Data_tampering_IED1	CVE_2019_10930	Hacker
Switch_off_W1C	Executive_operation_IED1	Malicious_Software_execution_IED1	Data_tampering_IED1	CVE_2019_10930	Engener_RZA

УНИКАЛЬНОСТЬ РЕЗУЛЬТАТА

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ПАТЕНТ

НА ИЗОБРЕТЕНИЕ
№ 2798437

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПО УПРАВЛЕНИЮ ПОДСИСТЕМОЙ РЕЛЕЙНОЙ ЗАЩИТЫ И АВТОМАТИКИ ЦИФРОВОЙ ПОДСТАНЦИИ В УСЛОВИЯХ ПРОВЕДЕНИЯ В ОТНОШЕНИИ НЕЕ КОМПЬЮТЕРНЫХ АТАК

Патентообладатели: *Карантаев Владимир Геннадьевич (RU), Карпенко Владислав Игоревич (RU)*

Авторы: *Карантаев Владимир Геннадьевич (RU), Карпенко Владислав Игоревич (RU)*

Заявка № **2022114852**
Приоритет изобретения **01 июня 2022 г.**
Дата государственной регистрации в Государственном реестре изобретений Российской Федерации **22 июня 2023 г.**
Срок действия исключительного права на изобретение истекает **01 июня 2042 г.**

Руководитель Федеральной службы по интеллектуальной собственности

Ю.С. Зубов

1/1

Получен патент Российской Федерации на изобретение № 2798437

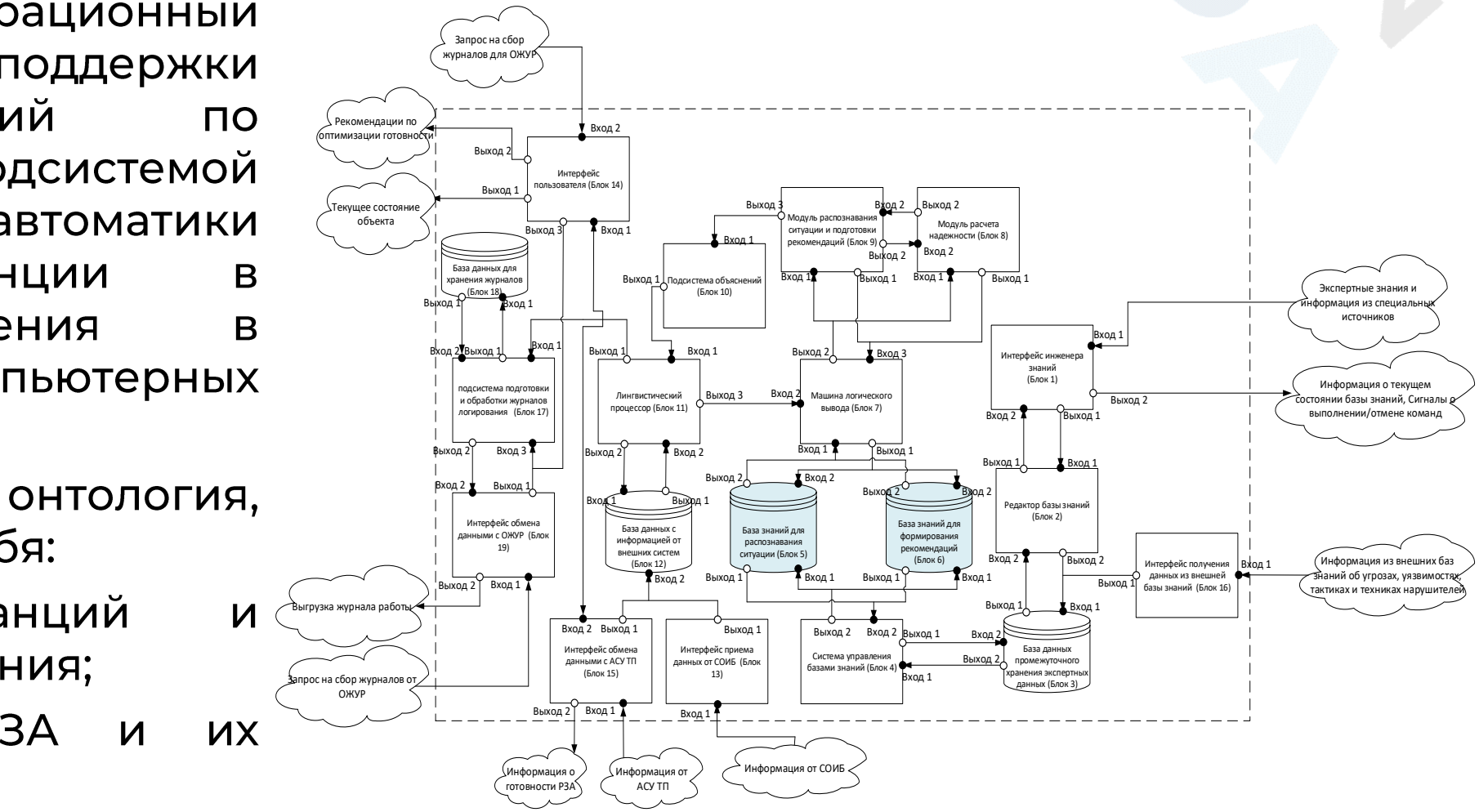
«Программно-аппаратный комплекс системы поддержки принятия решений по управлению подсистемой релейной защиты и автоматики цифровой подстанции в условиях проведения в отношении нее компьютерных атак»

Оценка уровня зрелости

Разработан демонстрационный прототип системы поддержки принятия решений по управлению подсистемой релейной защиты и автоматики цифровой подстанции в условиях проведения в отношении нее компьютерных атак.

Основой является онтология, которая включает в себя:

- Описание подстанций и силового оборудования;
- Описание ИЭУ РЗА и их уязвимостей;
- Описание моделей угроз для каждого ИЭУ РЗА и др.



Практическая значимость результатов исследования

- Применение разработанного программно-аппаратного комплекса интеллектуальной системы поддержки принятия решений «Управление надежностью и кибербезопасностью» (Далее -ИС СППР УНКБ) позволит на практике автоматизировать процесс использования полученных оригинальных способов:
- способ моделирования угроз,
- методику оценки частных показателей функциональной надежности,
- способ управления уязвимостями, для целей максимизации коэффициента готовности интеллектуальных электронных устройств релейной защиты цифровых подстанций при минимизации простоев силового оборудования и ресурсов ремонтных бригад.

«ИС СППР УНКБ» по управлению надежностью и кибербезопасностью интеллектуальных электронных устройств релейной защиты цифровой подстанции с применением семантических технологий искусственного интеллекта, позволит максимизировать коэффициент готовности при минимизации простоев силового оборудования и ресурсов ремонтных бригад.

Прогнозируемые эффекты

Эффекты, которые могут быть получены от применения «ИС СППР УНКБ»:

1. Сокращение времени на принятие решения о действиях инженерного персонала для работ по УУ и ОПО;
2. Повышение устойчивости ИЭУ РЗА при проведении в отношении них компьютерных атак;
3. Сокращение расхода горюче-смазочных материалов для обеспечения транспортировки инженерного персонала;
4. Повышение надежности электроснабжения в подведомственном районе;

СПАСИБО
за внимание!

Карантаев Владимир Карпенко Владислав