МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМ. В. ДАЛЯ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЕЛЕКТРОНІКИ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК ТА ІНЖЕНЕРІЇ

До захисту допускається
Завідувач кафедри
_____ Скарга-Бандурова І.С.
«____»_____ 20__ р.

МАГІСТЕРСЬКА РОБОТА

НА ТЕМУ:

КОМПЛЕКСНА ТЕМА: SMART GRID. МОДЕЛІ ТА МЕТОДИ РЕЛЕЙНОГО ЗАХИСТУ ТА АВТОМАТИКИ ЕЛЕКТРИЧНОЇ ЧАСТИНИ ОБ'ЄКТІВ ЕНЕРГЕТИЧНОЇ СИСТЕМИ

Освітньо-кваліфікаційний рівень "Магістр"
Спеціальність 122 – "Комп'ютерні науки"

Науковий керівник роботи:	_____ (підпис)	В. В. Єлісєєв (ініціали, прізвище)
Консультант з охорони праці:	_____ (підпис)	Я. О. Критська (ініціали, прізвище)
Студент:	_____ (підпис)	О.М. Гусаченко (ініціали, прізвище)
Група:		КН-173м

Сєвєродонецьк 2019

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВОЛОДИМИРА ДАЛЯ

Факультет Інформаційних технологій та електроніки
Кафедра Комп'ютерних наук та інженерії
Освітньо-кваліфікаційний рівень магістр
Напрям підготовки
(шифр і назва)
Спеціальність 122 – «Комп'ютерні науки»
(шифр і назва)

ЗАТВЕРДЖУЮ:

Завідувач кафедри
І.С. Скарга-Бандурова
«_____» _____20____р.

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Гусаченко Олександра Миколайовича
(прізвище, ім'я, по батькові)

1. Тема роботи **КОМПЛЕКСНА ТЕМА: SMART GRID. МОДЕЛІ ТА МЕТОДИ РЕЛЕЙНОГО ЗАХИСТУ ТА АВТОМАТИКИ ЕЛЕКТРИЧНОЇ ЧАСТИНИ ОБ'ЄКТІВ ЕНЕРГЕТИЧНОЇ СИСТЕМИ**
керівник проекту (роботи) Єлісєєв В. В., д.т.н., професор
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від " " 2019 р. № ____
2. Термін подання студентом роботи
3. Вихідні дані до роботи

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) 1) Аналіз методів і моделей систем рза у smartgrids. постановка задачі досліджень; 2) Методи та моделі розробки РЗА; 3) Розробка пристрою релейного захисту і автоматики; 4) Питання охорони праці, екології.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
Електронні плакати

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада Консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Критська Яна Олександрівна		

7. Дата видачі завдання _____

Керівник _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Аналітичний огляд літератури за темою роботи	1.09.18 – 1.10.18	
2	Аналіз стандартів IEC-61499 і IEC-61850	1.09.18 - 1.10.18	
3	Аналіз методів і моделей розробки МПРЗА	2.10.18 – 9.10.18	
4	Розробка вимог до пристрою РЗА	10.10.18 – 24.10.18	
5	Розробка пристрою РЗА	25.10.18 – 25.11.18	
6	Розгляд питань охорони праці та основних напрямків їх дотримання	14.11.18 – 15.12.18	
7	Оформлення пояснювальної записки	22.12.18 – 29.12.18	
8	Оформлення презентації роботи	30.12.18 – 6.01.19	

Студент _____ _____
(підпис) (прізвище та ініціали)

Керівник _____ _____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Гусаченко Олександр Миколайович. Комплексна тема: Smart grid. Моделі та методи релейного захисту та автоматики електричної частини об’єктів енергетичної системи.

В роботі проведено аналіз існуючих методів та моделей релейного захисту і автоматики та вибрано найбільш ефективні з них відносно поставленої задачі у розробці інтелектуального пристрою релейного захисту. Визначено вимоги щодо апаратного і програмного забезпечення пристрою. Розроблено структурні та функціональні схеми пристрою релейного захисту і автоматики за міжнародними стандартами для подальшої розробки пристрою на їх основі.

Дотримання міжнародних стандартів надає можливості використовування пристрою як для вітчизняних, так і для європейських електромережах.

АННОТАЦИЯ

Гусаченко Александр Николайович. Комплексная тема: Smart Grids. Модели и методы релейной защиты и автоматики электрической части объектов энергетической системы.

В работе проведен анализ существующих методов и моделей релейной защиты и автоматики и выбрано наиболее эффективные из них относительно поставленной задачи на разработку интеллектуального устройства релейной защиты. Определены требования к аппаратному и программному обеспечению устройства. Разработаны структурные и функциональные схемы устройства релейной защиты и автоматики по международным стандартам для дальнейшей разработки устройства на их основе.

Поддержка международных стандартов предоставляет возможности использовать устройства как для отечественных, так и для международных электросетей.

ABSTRACT

Gusachenko Olexander Mikolaevich. Crosscutting theme: Smart Grid. Methods and models of protective relaying and automation electric parts in energy system objects.

The paper analyzes the existing methods and models of relay protection and automation and selects the most effective of them in relation to the task assigned for the development of an intelligent relay protection device. Also was defined a hardware and software requirements for device. For next designed of IED was develop a structural and functional schemes of RPA devices according to international standards for the further development of devices based.

The support for international standards provides opportunities to use the device for both domestic and international power grids.

ЗМІСТ

СКОРОЧЕННЯ

CHP – combined heat and power unit

DER – distributed energy resource

DES – distributed energy storage

DG – distributed generators

DMS – distribution management system

EMS – energy management system

ESS – energy storage systems

FB – функціональний блок

NIST – The National Institute of Standards and Technology

PV – photovoltaic

IED – intelligent electronic device

АСУ ТП –автоматична система управління технологічним процесом

ПЗО – пристрої зв’язку з об’єктами

РЗА – релейная защита и автоматика

СПЗ – системне програмне забезпечення

МПРЗА – мікропроцесорний пристрій РЗА

ВСТУП

З розвитком енергетичних мереж, питання про стабільне і якісне енергопостачанні стало займати особливе місце. Цифрові технології дозволили створювати розподілені системи енергопостачання і з'єднувати їх в єдину енергосистему, так звані SmartGrids.

SmartGrids (SG) – це електрична мережа, що містить в собі різноманітні оперативні та енергоощадні заходи, включаючи розумні лічильники, розумних споживачів, поновлювані джерела енергії та ресурси забезпечення енергоефективності. Електронне керування параметрами електроенергії, керування її виробництвом і розподілом є важливими аспектами розумної енергосистеми [1].

Важливе місце у SG приділено швидкому та якісному виявленню та усуненню пошкоджених електроенергетичної системи а саме релейного захисту та автоматики. Безліч провідних світових компаній такі як: ABB Group, Siemens, Schneider Electric, General Electric, займаються створенням ефективних систем релейного захисту та автоматики (РЗА) на базі мікропроцесорних систем.

Релейний захист призначений для виявлення та автоматичного відключення пошкодженого електроустаткування та сигналізації про пошкодження.

Розвиток у сфері інформаційних технологій надає можливість створення більш функціональних РЗА – на основі мікропроцесорних технологій.

Мікропроцесорні реле (МР) використовуються в системах релейного захисту і автоматики більше десяти років. За цей час досягнуті високі показники надійності роботи, розроблені програмні пакети, що дозволяють інтегрувати МР в автоматичні системи управління технологічним процесом (АСУ ТП).

Більшість мікропроцесорних систем РЗА або інтелектуальних електронних пристроїв (IED) в Україні – закордонного виробництва. Такі фірми як SIEMENS, AREWA (ALSTOM), ABB, SCHNEIDER ELECTRIC, GE розробили значну кількість IED, що мають високу технологічну якість.

Але їх застосування в електроенергетичних мережах України зустрічає ряд проблем:

- недостатня ефективність функціонування при експлуатації в умовах вітчизняних ЕЕМ;
- неможливість безпосередньої інтеграції IED закордонного виробництва в більшість існуючих на даний момент АСУ ТП України;
- висока ціна IED закордонних виробників, при цьому адаптація таких пристроїв до вітчизняних електромереж ще більше збільшує їх вартість.

Значний внесок у розвиток МП систем РЗА в Україні внесли Стогній Б.С. [2], Кириленко О.В. [3] (Інститут Електродинаміки НАН України). Досить вагомі результати були отримані в Київському, Львівському, Мінському, Новочеркаському і Ризькому політехнічних інститутах. В останні роки розробкою і впровадженням мікропроцесорними РЗА займаються вітчизняні фірми такі як:

- ВО «Київприлад», конструкторське бюро «Реле й автоматики»;
- підприємство «Хартрон-Інкор»;
- ПРАТ «СНПО «Імпульс».

Слід зазначити, що пристрої даних виробників успішно конкурують з закордонними аналогами.

Проте впровадження вітчизняних IED в електромережі інших країн у даний час може бути забезпечено тільки закордонними фірмами-виробниками. Тому комплексний характер проблеми й особливості розробки РЗА в Україні, потребують розв'язання зазначених проблем шляхом розробки за новітніми методами і моделями, що відповідають міжнародним стандартам, регламентуючим розробку інтелектуальних електричних пристроїв.

Для вирішення цієї проблеми ПрАТ СНВО «Імпульс» поставлена задача на розробку інтелектуального пристрою релейного захисту і автоматики із використанням міжнародних стандартів розробки мікропроцесорних систем РЗА.

Мікропроцесорні пристрої релейного захисту повинні відповідати таким вимогам як: селективність, швидкодія, чутливість, надійність. IED-пристрій із вдало підібраною моделлю та методами розробки, може в повній мірі відповідати усім вимогам до систем релейного захисту та автоматики.

Саме цим і обґрунтована тема магістерської роботи, що вирішує науково-прикладне завдання розроблення методів та моделей інформаційної технології системи РЗА.

Об'єкт дослідження – процеси забезпечення релейного захисту та автоматики.

Предмет дослідження – методи та моделі розробки системи релейного захисту.

Метою роботи є аналіз існуючих методів і моделей побудови систем релейного захисту і автоматики, виявлення їх переваг та недоліків, та обрати найбільш ефективну модель для подальшого проектування пристрою релейного захисту на їх основі.

Для досягнення мети дослідження необхідно вирішити такі завдання:

– провести аналіз моделей, що регламентуються міжнародними стандартами;
– розробити вимоги до апаратної та програмної частин основуючись із обраних моделей;
– розробити функціональні та структурні схеми системи РЗА.

В роботі аналізуються існуючі методі і моделі розробки IED та міжнародні стандарти, що регламентують їх розробку.

В результаті аналізу планується визначити найбільш ефективні методи і моделі розробки РЗА пристрів для їх реалізації на апаратній платформі ImPR1 під управлінням операційної системи реального часу Linux-RT.

В роботі запропоновано використання новітніх методів і моделей розробки інтелектуальних електронних пристроїв у вигляді системного програмного забезпечення. Результати роботи використовуються при розробці серії IED-пристроїв ImPR1 в ПрАТ «СНВО «Імпульс».

Актуальність даної роботи полягає у необхідності розробки пристрою, що відповідає міжнародним стандартам розробки інтелектуальних систем, при цьому зберігається можливість їх використання на вітчизняних електромережах.

Апробація матеріалів роботи. Основні положення, ідеї, висновки магістерської роботи доповідалися та обговорювалися на форумі «ІТ-Ідея», наукових семінарах кафедри КНІ протягом 2017-2018 рр.

Практичне значення отриманих результатів полягає в тому, що основні наукові положення магістерської роботи використовуються при розробці ряду пристроїв релейного захисту ImPR1 в ПрАТ "СНВО “Імпульс”.

Публікації. За темою магістерської роботи з викладенням її основних результатів опубліковано 3 наукових праці, серед яких 1 стаття у наукових фахових виданнях України; 2 тези доповідей.

РОЗДІЛ 1: АНАЛІЗ МЕТОДІВ І МОДЕЛЕЙ СИСТЕМ РЗА У SMARTGRIDS. ПОСТАНОВКА ЗАДАЧІ ДОСЛІДЖЕНЬ

1.1 Аналіз вимог до функціональних характеристик SmartGrids та MicroGrids.

1.1.1 Визначення SmartGrids і MicroGrids. Основні структурні компоненти SmartGrids і MicroGrids.

Енергетичні проблеми, з якими стикається світ, кардинально змінять інфраструктуру постачання електроенергії. Основна архітектура первинних мереж була розроблена для задоволення потреб великих виробництв та живлення електроенергією у режимі реального часу. Перехід до більш стійкого електропостачання вимагає гнучкої та розумної енергетичної інфраструктури, підготовленої до боротьби з масовим зростанням поновлюваних джерел енергії та співвіднесеним двотарифним навантаженням та інформаційними потоками.

Створення стійкого, масштабованого, модульного, стандартизованого підходу до енергосистеми майбутнього, вимагає, одночасно великих та маленьких кроків [4].

Значення великих означає пошук шляхів подолання прогалин між регіональними з'єднаннями, тому нові джерела чистої енергетики можуть бути достатніми, щоб бути вигідними.

Невеликі кроки означають створення мікродеревних мереж невеликих комерційних та житлових гравців для створення чистих нульових будівель.

Посилаючись на це можна виділити два типи мереж:

- SmartGrids;
- MicroGrids.

У роботі [5] визначаються наступні поняття:

MicroGrids – це електрична система, що включає в себе безліч навантажень і розподілених енергоресурсів, які можуть працювати паралельно з більш широкою сіткою або малої незалежної енергосистемою. Підвищена надійність з розподіленою генерацією, збільшення ефективності зі зменшеною довжиною передачі і простіша інтеграція альтернативних джерел енергії.

SmartGrids являє собою модернізовану електричну сітку, яка використовує інформаційні та комунікаційні технології для збору і обробки інформації, такої як інформація про поведінку постачальників і споживачів, автоматичним чином для підвищення ефективності, надійності, економії і стійкості виробництва і розподілу електроенергії.

Виробництво електроенергії в традиційній енергосистемі має високу централізацію, при цьому енергія тече в одному напрямку від великих синхронних генераторів через мережу передачі/розподілу до кінцевих користувачів. Проте технологічні проблеми, пов'язані з

традиційними електроустаткуваннями, а також екологічними проблемами, що викликані спалюванням викопного палива, стимулювали дослідження та розробку нових технологій енергосистеми. З появою одиниць розподіленого енергоресурсу (DER) технології *MicroGrids* привертають все більшу увагу як ефективного засобу інтеграції таких ДСЗ-одиниць в енергосистеми. На базі Європейської технологічної платформи SmartGrids [4], MicroGrids являє собою платформу, яка полегшує інтеграцію розподілених генераторів (DG), систем накопичення енергії (ESS) та навантажень для забезпечення того, що енергосистема може забезпечити стабільні, конкурентоспроможні ціни і надійна електрика. На рисунку 1.1 показана типова структура, що включає DG, такі як комбінований тепловий та енергетичний блок (CHP), мікротурбіни, PV-системи, системи енергії вітру, паливні елементи; сховище розподіленого енергоспоживання (DES), таке як батареї, маховики, електричні транспортні засоби, гнучкі навантаження та пристрої управління [6].

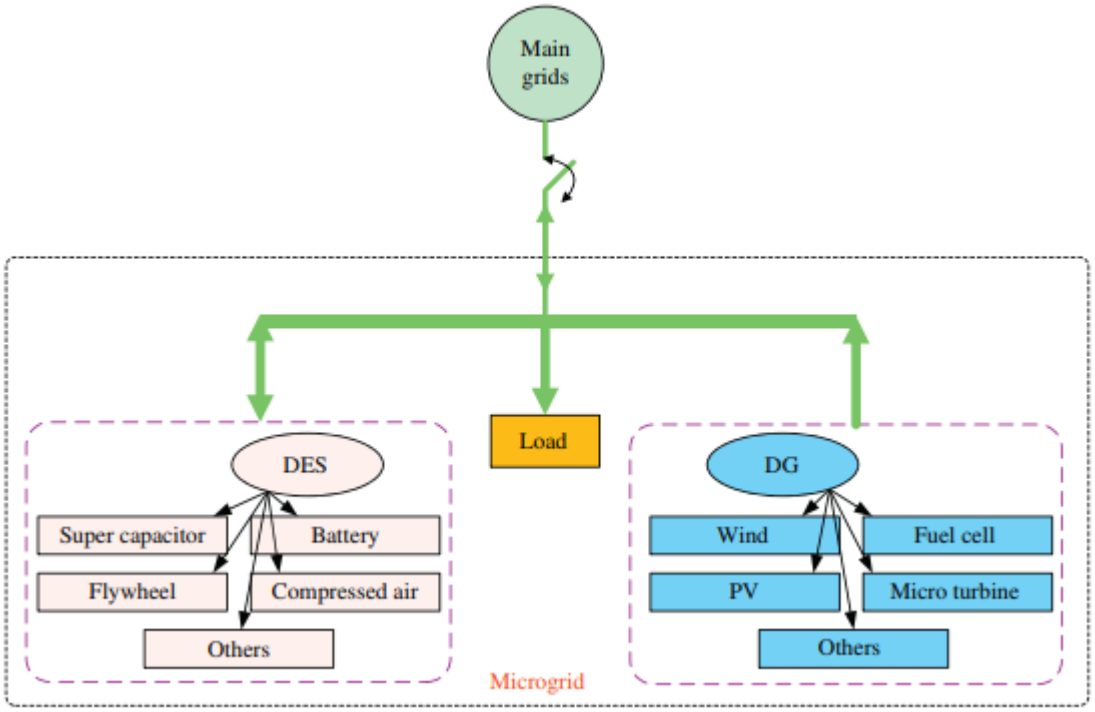

Рисунок 1.1 - Типова схема MicroGrids

До основних елементів SmartGrids відносяться наступні модулі:

– SCADA (supervisory control and data acquisition system) - автоматизована система
– управління;
– EMS (energy management system) - система управління енергоспоживанням;
– DMS (distribution management system) - система організації розподілу;
– OMS (outage management system) - система управління аварійними відключеннями
– GIS (geographic information system) - геоінформаційні системи;

- WAMS (Wide-Area Measurement Systems) - Система моніторингу перехідних режимів;
- MDMS (Meter Data Management System) - система управління даними вимірів;
- SER (Sequence Event Record System) - система послідовного запису помилок;
- DFR (Digital Fault Recorder System) - система цифрової аварійний реєстрації;
- PMU (Phasor Measurement Units) - пристрої векторних вимірювань зараз не входить в SG, але фахівці кажуть, що даний пристрій стане невід'ємною частиною SG.

1.1.2 Варіанти архітектур SmartGrids і MicroGrids

Архітектура зв'язку розглядає аспекти комунікації SmartGrids, розглядаючи загальні випадки використання SmartGrids для виявлення вимог та розглядати їх адекватність існуючим стандартам зв'язку для виявлення прогалин стандартів зв'язку. Вона надає набір рекомендацій щодо роботи з стандартизації, а також уявлення про те, як можна зробити профілювання та специфікації сумісності.

Основні еталоні архітектури SmartGrids і MicroGrids наведені нижче.

*Національний інститут стандартів і технологій (**NIST**)* представив концептуальну модель SmartGrids, яка забезпечує рамки високого рівня для SmartGrids, який визначає сім доменів високого рівня та показує всі комунікації та енергетичні/електричні потоки, що зв'язують кожний домен та як вони взаємопов'язані.

Незважаючи на те, що модель NIST є здоровою та визнаною основою, її необхідно адаптувати, щоб врахувати деякі специфічні вимоги контексту ЄС, які модель NIST не розглянула. Введено два основні елементи для створення концептуальної моделі ЄС. Перший - домен розподіленого енергетичного ресурсу (DER), який дозволяє вирішувати дуже важливу роль, яку DER відіграє у європейських цілях. Другий - це концепція гнучкості (розроблена в SGCG / SP), що споживає, виробляє та зберігає групу разом у об'ємі гнучкості.

Концептуальна модель ЄС є моделлю верхніх шарів (або головною моделлю), а також буде мостом між базовими моделями в різних точках зору базової архітектури.

Архітектурна модель розумних мереж (SGAM) спрямована на підтримку розробки випадків використання інтелектуальних мереж з архітектурним підходом, що дозволяє представляти точку зору взаємодії нейтрально технологічно як для поточної реалізації електромережі і майбутні реалії інтелектуальної мережі.

Це тривимірна модель, яка об'єднує розміри п'яти пластів сумісності (бізнес, функція, інформація, комунікація та компонент) з двома параметрами SmartGrids Plane:

- зони (представляють ієрархічні рівні управління енергосистемою: процес, поле, станція, операція, підприємство та ринок)

– домени (охоплюють повний ланцюжок перетворення електричної енергії: масові генерування, передача, розподіл, споживачі та споживачі).

Методологія SGAM

Ця структура SGAM може бути використана методологією SGAM для оцінки випадків використання інтелектуальних мереж та способів їх підтримки стандартами, що дозволяє аналізувати розрив стандартів. Ця модель значною мірою розвинута у версію v2.0, з чіткішими основними визначеннями, більш детальним представленням елементів (зон, доменів тощо), роз'ясненням методології та повним докладним прикладом.

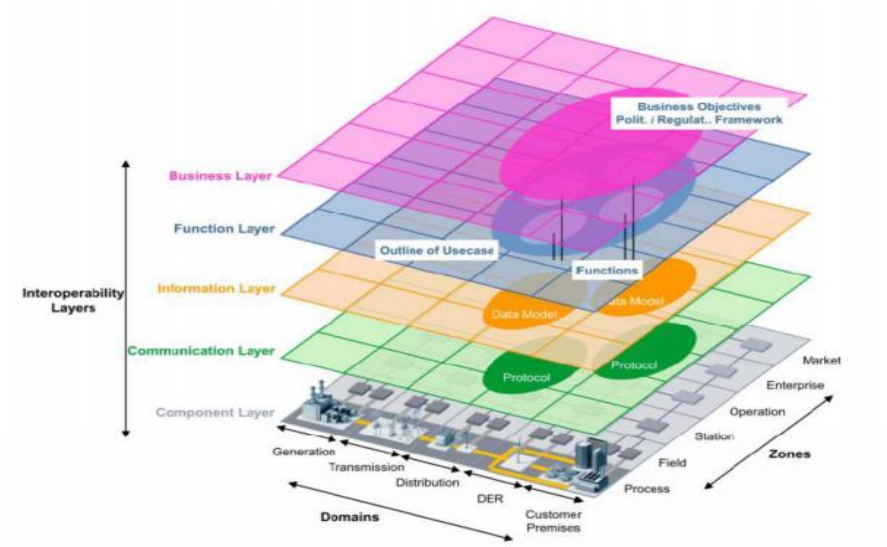

Рисунок 1.2 - Архітектурні точки зору SGAM

Архітектурні точки зору:

– Вони представляють обмежений набір способів подання абстракцій різних поглядів зацікавлених сторін на систему SmartGrids. Чотири точки зору були обрані SG-CG/RA: бізнес, функціонал, інформація та зв'язок, а також пов'язані з ними архітектури:
– Бізнес-архітектура адресована з точки зору методології, з тим щоб гарантувати, що будь-які ринкові чи бізнес-моделі вибираються, правильні бізнес-послуги та основні архітектури розробляються послідовно та узгоджено;
– Функціональна архітектура забезпечує мета-модель, яка описує функціональні архітектури та надає архітектурний огляд типових функціональних груп інтелектуальних мереж;
– Інформаційна архітектура розглядає поняття моделювання даних та інтерфейсів і як вони застосовні в моделі SGAM. Крім того, він запроваджує концепцію "-логічних

інтерфейсів", яка спрямована на спрощення розробки специфікацій інтерфейсу, особливо у випадку декількох суб'єктів, що мають відносини між доменами.

1.1.3 Цифрова підстанція. Місце у SmartGrids. Структура

Однією з найважливіших складових частин концепції SmartGrids є цифрова підстанція (ЦПС). Під ЦПС розуміється підстанція з високим рівнем автоматизації управління, в якій практично всі процеси інформаційного обміну як між елементами ЦПС, так і обміну з зовнішніми системами, а також управління роботою ЦПС здійснюються в цифровому вигляді на основі протоколів IEC, зокрема з відкритого об'єктно-орієнтованому стандарту IEC-61850.

Відповідно до цього стандарту, пристрої повинні підтримувати можливість прийому та передачі інформації за рядом протоколів (рис. 1.3).

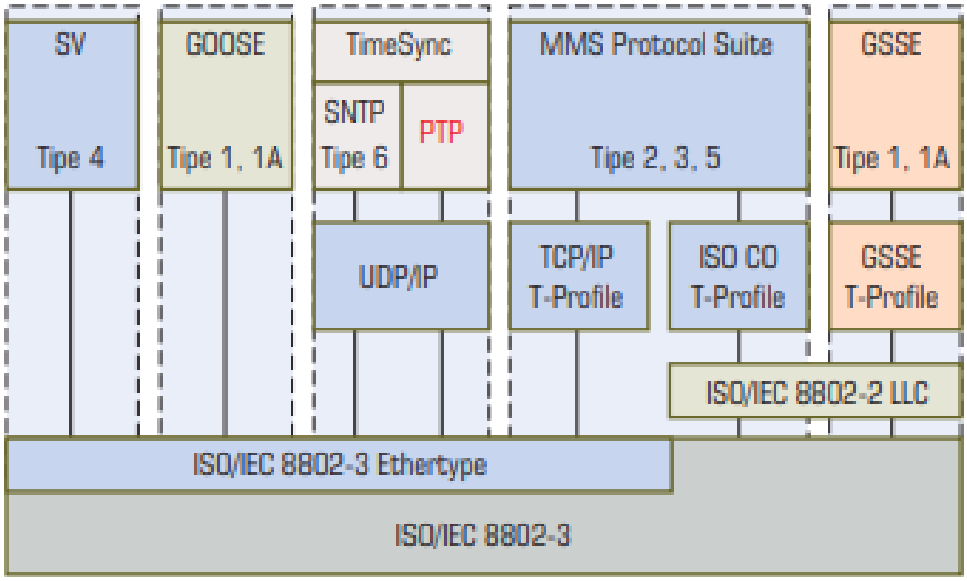

Рисунок 1.3 - Огляд функціональності і профілі відповідно до IEC-61850-8-1

Структура ЦПС, відповідно до стандарту IEC-61850 представлена на рисунку 1.4. Система автоматизації енергооб’єкта, побудованого за технологією цифрової підстанції, ділиться на три рівні:

1) польовий рівень (рівень процесу);
2) рівень приєднання;
3) станційний рівень.

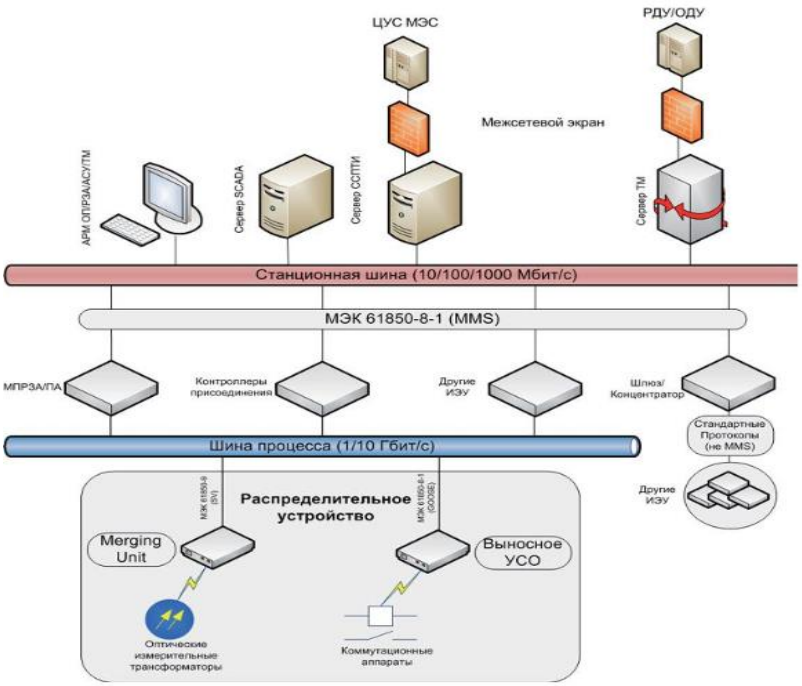

Рисунок 1.4 - Структура цифрової підстанції

Польовий рівень складається з:

– первинних датчиків для збору дискретної інформації і передачі команд управління на комутаційні апарати (microRTU);
– первинних датчиків для збору аналогової інформації (цифрові трансформатори струму і напруги).

Рівень приєднання складається з інтелектуальних електронних пристроїв:

– пристроїв управління і моніторингу (контролери приєднання, багатофункціональні вимірювальні прилади, лічильники АСКОЕ, системи моніторингу трансформаторного обладнання тощо);
– терміналів релейного захисту та локальної протиаварійної автоматики (РЗА).

Станційний рівень складається з:

– серверів верхнього рівня (сервер бази даних, сервер SCADA, сервер телемеханіки, сервер збору і передачі технологічної інформації, концентратор даних);
– АРМ персоналу підстанції.

З основних особливостей побудови системи в першу чергу необхідно виділити новий «польовий» рівень, який включає в себе інноваційні пристрої первинного збору інформації: виносні УСО, цифрові вимірювальні трансформатори, вбудовані мікропроцесорні системи діагностики силового обладнання тощо.

Цифрові вимірювальні трансформатори передають миттєві значення напруги і струмів по протоколу IEC-61850-9-2 пристроїв рівня приєднання. Дані від цифрових вимірювальних трансформаторів, як оптичних, так і електронних, перетворюються в широкомовні Ethernet-пакети з використанням мультиплексорів (Merging Units), передбачених стандартом IEC-61850-9. Пакети, сформовані мультиплексорами передаються по мережі Ethernet (шині процесу) в пристрої рівня приєднання (контролери АСУ ТП, РЗА, ПА та ін.) Частота дискретизації передавання даних не гірше 80 точок на період для пристроїв РЗА і ПА та 256 точок на період для АСУ ТП , АИИС КУЕ і ін.

Дані про стан комутаційних апаратів і інша дискретна інформація (положення ключів режиму управління, стан ланцюгів обігріву приводів і ін.) Збираються з використанням виносних пристроїв зв'язку з об'єктами (ПЗО), встановлених в безпосередній близькості від комутаційних апаратів. Виносні модулі УСО мають релейні виходи для управління комутаційними апаратами і синхронізуються з точністю не нижче 1 мс. Передача даних від виносних ПЗО здійснюється по оптоволоконного зв'язку, що є частиною шини процесу по протоколу IEC-61850-8-1 (GOOSE). Передача команд управління на комутаційні апарати також здійснюється через виносні ПЗО з використанням протоколу IEC-61850-8-1 (GOOSE).

1.2 Релейний захист автоматики у цифрових підстанціях

1.2.1 Місце РЗА в енергетичних системах

Енергетичні системи (ЕС) – це складні системи, всі елементі котрої пов'язані з технологічним циклом. Вихід з ладу будь якого елементу енергетичної системи може призвести до часткової або повної її зупинки. Як і кожна інша технічна система, енергетична система вразлива до аварійних ушкоджень. Отже, з метою запобігання виникнення ушкоджень при експлуатації енергетичної системи застосовується комплекс автоматичних пристроїв, що складається з пристроїв автоматичного керування і автоматичного регулювання.

До цех пристроїв відносяться пристрої релейного захисту, основною метою яких є захист електричних мереж, електроустаткування від пошкоджень або при порушенні нормального режиму їх роботи.

1.2.2 Структура РЗА

Релейний захист це система автоматичного керування, що отримує інформацію про токи, напругу і стан комутаційних елементів в окремих частинах електричної мережі, в результаті

обробки котрої вона видає керуючі сигнали для вимикачів, а також інші повідомлення, що дозволяють фіксувати і аналізувати процеси електричної мережі.

Кожна схема релейного захисту може бути представлена у загальному вигляді, що наведена на рисунку.

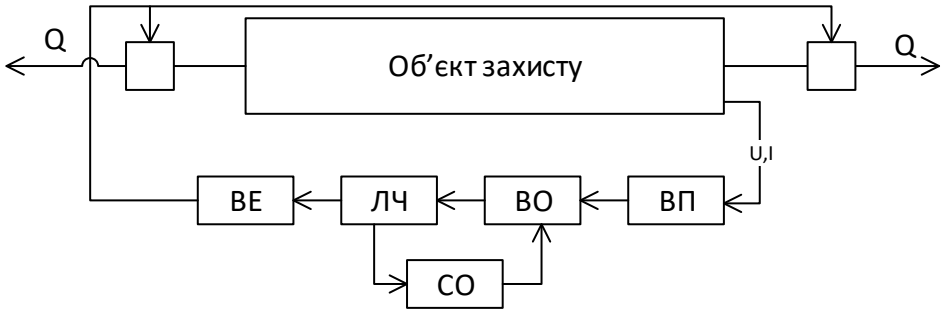

Рисунок 1.5 - Структурна схема релейного захисту

Інформація о стані об'єкта перетворюється за допомогою вимірювальних перетворювача (ВП) у зручний для обробки вигляд. У якості перетворювача виступають трансформатори току і напруги. Вимірювальних орган (ВО) безперервно контролює стан і режими роботи об'єкту захисту. Логічна частина (ЛЧ) оброблює інформаціє, зо надана вимірювальними елементами і формує керуючі сигнали через виконавчі елементи (ВЕ) на комутаційну апаратуру, світлову або звукову сигналізацію. Сигнальний орган фіксує спрацювання захисту в цілому або окремих блоків.

Релейні захисти розподіляють за їх призначенням.

1.2.3 Види основних пошкоджень об'єктів енергетичної інфраструктури, яких можна уникнути застосовуючи РЗА

Функцією систем РЗА є захист від електричної несправності і правильне їх застосування потребує чіткого визначення несправності. Можливі такі несправності:

- переміжна дуга;
- міжфазне коротке замикання;
- коротке замикання фаза - нуль;
- удар блискавки;
- механічне пошкодження;
- сплеск напруги;
- відмова вимикача;
- замикання на землю;
- теплове перевантаження;

– втрата синхронізації;
– значне зниження частоти.

За характером тривалості їх можна розділити на чотири типи:

1. побіжна – потребує короткочасного вимкнення мережі;
2. постійна – вимагає втручання людини, для відновлення мережі;
3. самозгасна – поступово швидко зникає;
4. напівпостійна – вимагає довготривалого вимкнення, порядку декількох десятків секунд, щоби поступово зникнути.

1.2.4 Вимоги до релейного захисту

До релейного захисту пред'являється ряд вимог:

– селективність – це властивість захисту відключати тільки пошкоджений елемент. Вибірковість досягається відповідним вибором принципу дії захисту і вибором її установок з таким розрахунком, щоб захист не могла спрацьовувати в режимах, в яких вона не повинна спрацьовувати;
– швидкодія захисту в розподільних мережах скорочує розмір пошкоджень (руйнувань), що викликаються КЗ зменшує періоди зниження напруги;
– чутливість – здатність захисту чітко спрацьовувати при пошкодженнях, в зоні її дії;
– надійність – це здатність пристрою захисту правильно працювати в нормальному, ненормальному і аварійному режимах. Розрізняють надійність спрацьовування і надійність неспрацьовування захисту. В загальному випадку вимоги до них можуть бути неоднаковими внаслідок можливих різних наслідків від помилкового спрацьовування або відмови в спрацьовуванні захисту.

1.3 Постановка завдання і обґрунтування методики досліджень

Розробка ефективних систем релейного захисту є однією з основних елементів ефективної роботи цифрової підстанції, бо саме вони є одним із головних елементів з забезпечення стабільного енергообміну у електроенергетичній мережі і захистом від пошкоджень на лінії.

Метою роботи є аналіз існуючих методів і моделей побудови систем релейного захисту і автоматики, виявлення їх переваг та недоліків, та обрати найбільш ефективну модель для подальшого проектування пристрою релейного захисту на їх основі.

Для досягнення цієї мети необхідно:

– провести аналіз моделей, що регламентуються міжнародними стандартами IEC-61850 та IEC-61499;
– розробити вимоги до апаратної та програмної частин основуючись із обраних моделей;
– розробити функціональні та структурні схем системи РЗА.

Вимоги повинні описувати створення пристрою для реалізації наступного функціоналу:

– створення вільної логіки захистів;
– створення вільної логіки автоматики;
– забезпечення функцій контролю, реєстрації і сигналізації;
– забезпечення сервісних функції.

Аналіз наукових робіт у області розробки моделей та методів а також стандартів щодо роботи інтелектуальних пристроїв допоможуть підкреслити основні переваги та недоліки існуючих підходів у розробці інтелектуального пристрою релейного захисту. Це допоможе обрати найбільш оптимальний варіант їх подальшої реалізації.

1.4 Висновки до розділу

В цьому розділі розглянута концепція SmartGrid та її елементів (MicroGrid). Проаналізовано вимоги до їх функціональних характеристик та розглянуті можливі варіанти архітектури SmartGrid і MicroGrid. Визначено місце і роль цифрових підстанцій у SmartGrid. Також розглянута роль і місце релейного захисту і автоматики в ЦП. Визначена структура РЗА та основні види пошкоджень, для запобігання котрих необхідне використання релейного захисту. Розглянуті основні вимоги до основні систем релейного захисту. Згідно з розглянутим вище матеріалом сформульовано задачі на магістерську роботу.

Згідно до вищевикладеним виникла необхідність у розробленні системи релейного захисту за новітніми технологіями і існуючими стандартами.

РОЗДІЛ 2: МЕТОДИ ТА МОДЕЛІ РЕЛЕЙНОГО ЗАХИСТУ І АВТОМАТИКИ

Згідно до поставлених задач в першому розділі провести аналіз існуючих методів та моделей релейного захисту.

Запорукою до побудови ефективної енергосистеми є досягнення стандартизації всіх етапів її циклу життя. Введення загальних правил побудови усіх елементів енергосистеми дозволяє забезпечити їх безпечну та ефективну роботу.

Саме з цією метою створена міжнародна некомерційна організація із стандартизації в сфері електричних, електронних та суміжних технологій – International Electrotechnical Commission (IEC). [7]. Існування стандартів вимагає підтримки деякого вектора в розробці методів і моделей всіх елементів електроенергетики починаючи від їх побудови, випробувань і закінчуючи технічним обслуговуванням і експлуатацією.

За опис моделі підстанції та зв’язок елементів електросистеми відповідає серія стандартів IEC-61850. А моделі побудови розподілених систем керування промисловим процесом описані у стандарті IEC-61499 [8]. Ці два стандарти є базовими, щодо розробки ефективної енергосистеми та інтеграцією її до Smart Grid. IEC-61850 надає пристрою універсальність в комунікації із зовнішніми пристроями. Також дозволяє синхронізувати пристрій з іншими IED зарубіжних виробників, що також надають підтримку даного стандарту.

IEC-61499 визначає методи та моделі розробки програмованих логічних контролерів на основі використання функціональних блоків. Цей принцип розробки дозволяє організовувати програмне забезпечення із застосуванням функції багатократного використання а також надає можливості графічного складання електричних схем з використанням систем автоматичного програмування (САПР).

2.1 Модель підстанції за IEC-61850

Одним з найважливіших стандартів організації моделі підстанції є IEC-61850 «Мережі і системи зв'язку на підстанціях», що описує формати потоків даних, види інформації, правила опису елементів енергосистеми і звід правил для організації подієвого протоколу передачі даних.

IEC-61850 є об’єктно-орієнтованим протоколом, що фокусуєтеся на автоматизації підстанції. Протокол включає реалізацію цілого ряду стандартів з передачі даних [9].

Він описує передачу даних, а також закріплює вимоги до опису електричних систем на всіх рівнях, починаючи від рівня системи в цілому, закінчуючи конфігурацією окремого терміналу релейного захисту та автоматики (РЗА).

2.1.1 Інформаційна модель

Зокрема, стандарт IEC-61850-7 описує об'єктну модель підстанції.

Стандарт описує модель автоматизації підстанції з максимальною деталізацією всіх функцій і пристроїв підстанції. Особлива увага приділяється принципам організації зв’язку поміж пристроями.

Обмін інформацією будується на чітко визначеній інформаційній моделі пристроїв.

Метамодель містить класи для опису пристрою відносно моделей даних і обміну інформацією [10].

Стандарт визначає наступні загальні класи:

a) Сервер - представляє зовнішню видиму поведінку пристрою. Всі інші моделі ACSI є частиною сервера.
b) Логічний пристрій (LD) - представляє інформацію, вироблену і споживану групою доменних функцій прикладної програми.
c) Логічний вузол (LN) - містить інформацію, вироблену і споживану однією доменною функціональною прикладною функцією, наприклад, захист від перенапруги або вимикач.
d) Об'єкти даних - забезпечують засоби для визначення типізованої інформації, наприклад, положення комутатора з інформацією про якість і мітку часу, що міститься в логічних вузлах.

Кожна з цих моделей визначається як клас. Класи містять атрибути та послуги. Концептуальна діаграма класів ACSI зображена на рисунку 2.1.

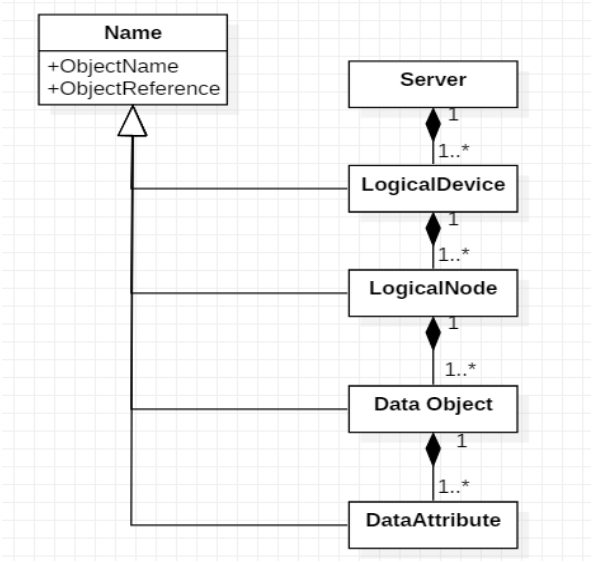

Рисунок 2.1 –Діаграма класів ACSI

Ця інформаційна модель реалізується всередині фізичного пристрою і включає в себе апаратні засоби, операційну систему тощо.

Кілька логічних пристроїв можуть міститися в одному пристрої, групуючи логічні вузли. Так на малюнку LN XCBR містить екземпляр класу Pos, що має близько 20 атрибутів, що представляють керовану інформацію.

Атрибут Pos.cstVal може приймати два стани - ON/OFF.

Всі елементи інформаційної моделі визначаються як класи (абстрактний тип даних, який задає загальну поведінку для групи об'єктів з однаковими атрибутами, сервісами, взаємодіями і семантикою).

Класи даних представлені в якості ієрархічної структури, а звернення здійснюється по імені (LD / LN.DO.DA). Так звернення до атрибута PhA класу даних A логічного вузла MMXU і логічного пристрою Hmelnitsk_HS3 матиме вигляд:

Hmelnitsk_HS3/MMXU.A.PhA

Імена атрибутів є стандартизованими і мають семантику стосовно IEC-61850.

Так серія стандартів визначає класи логічних вузлів і класів даних (IEC-61850-7-4), класів загальних даних (IEC-61850-7-3) і моделей сервісів (IEC-61850-7-2).

2.1.2 Абстрактний інтерфейс служби зв’язку (ACSI)

Передача інформації між пристроями здійснюється за допомогою ієрархічної моделі класу і сервісів, що надаються цими класами. ACSI включає в себе ряд моделі, які надають послуги, що працюють з об'єктами даних, атрибутами даних і наборами даних. Моделі ACSI наведені на рисунку 2.2.

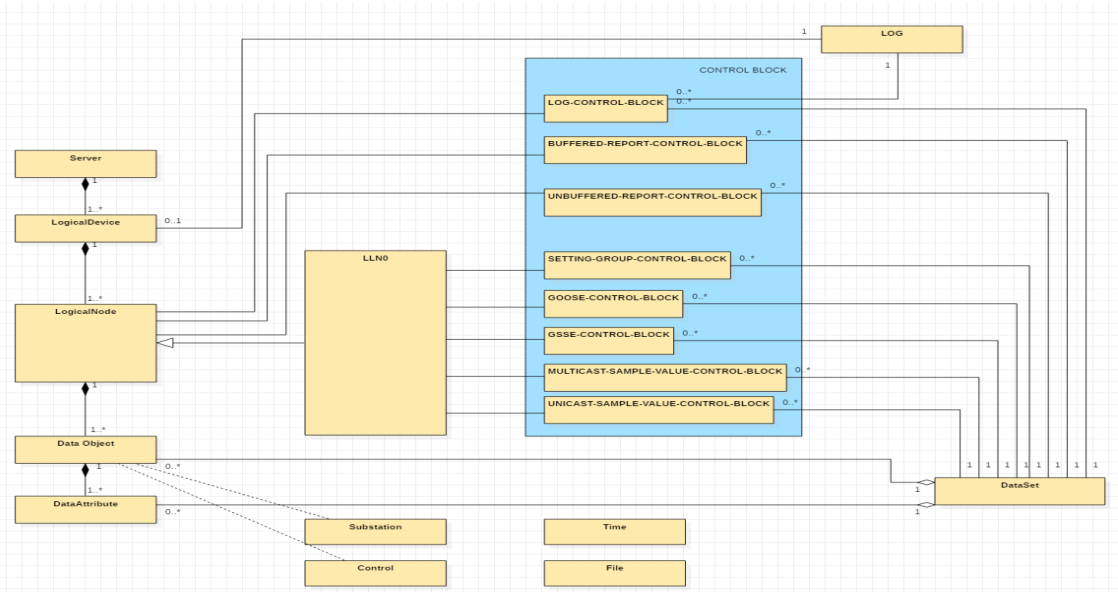

Рисунок 2.2 – Концептуальна модель послуг

Модель SERVER – представляє зовнішнє видиме пристрій. Визначає сервіс пошуку списку імен всіх логічних пристроїв або файлів доступних для клієнта.

Модель ASSOCIATION – визначає сервіси для встановлення зв'язку між клієнтом і сервером і сервіси для управління асоціаціями при розсилці повідомлень. Визначає сервіси установки, переривання і відключення з'єднання.

Модель Logical Device – представляє інформацію, вироблену і споживану групою прикладних функцій, специфічних для предметної області.

Модель Logical Node – містить інформацію, що створюється і споживається однією прикладною функцією для конкретного домену.

Модель DATA використовується для прямого доступу до даних і їх атрибутів, а також надання звітів і реєстрації.

Модель DATA-SET дозволяє здійснювати групування даних і атрибутів даних. Використання аналогічне моделі DATA.

Модель SETTING-GROUP-CONTROL-BLOCK - визначає виконання перемикання з одного набору значень на інший, а також як редагувати групи налаштувань.

Моделі REPORT-CONTROL-BLOCK і LOG-CONTROL-BLOCK описують умови створення звітів і журналів відповідно до параметрів, заданими клієнтом.

Модель GSE забезпечує можливість швидкого і надійного розподілу даних по всій системі. Використовує широкомовні і багатоадресні сервіси для відправки інформації про подію більш ніж одному LD. IEC-61850-7-2 визначає два керуючих класу і структури двох повідомлень:

- універсальна об'єктно-орієнтована подія підстанції (GOOSE) підтримує обмін широким діапазоном можливих спільних даних, організованих набором даних;
- загальна подія стану підстанції (GSSE) надає можливість передавати інформацію про зміну стану.

Обмін інформацією базується на механізмі «видавець/передплатник» за допомогою локального буфера.

Модель MULTICAST-SAMPLE-VALUE-CONTROL-BLOCK – здійснює передачу даних миттєвих повідомлень. Обмін здійснюється за допомогою DATA-SET. Дані з набору відносяться до класу загальних даних SAV. Механізм обміну інформацією - «публікація-підписка».

Модель CONTROL описує сервіси для керування пристроями. Визначає сервіси, що дозволяють управляти даними з боку клієнта.

Модель Time and time synchronization забезпечує єдиний синхронізований час для додатків, локалізованих в сервері підстанції та IED-пристроях.

2.1.3 Конфігурація підстанції за стандартом IEC-61850

Конфігурація підстанції здійснюється за допомогою мови опису конфігурації підстанції SCL, описаного в IEC-61850-6. Даних стандарт визначає формат файлів опису конфігурації IED і їх параметрів, а також топології підстанції та системи зв'язку.

Завдяки стандартизованої об'єктної моделі IED, комунікаційних з'єднань між ними і первинним обладнанням досягається сумісний міжрівневий обмін конфігураційною інформацією між пристроями і автоматичними системами управління різних виробників.

Стандарт виділяє 4 типи конфігураційних файлів (Рисунок 2.3):

– ICD (IED capability description) - файл опису характеристик і технічних можливостей IED-пристрої;
– SSD (System specification description) - файл опису специфікації системи, описує однолінійну систему підстанції та необхідні логічні вузли.
– SCD (Substation Configuration Description) - файл опису повної конфігурації підстанції. Містить інформації з окремих ICD і SDD.
– CID (Configured IED Description) - файл опису пристрою. Описує конкретні функції і параметри взаємодії IED пристрою в рамках проекту.

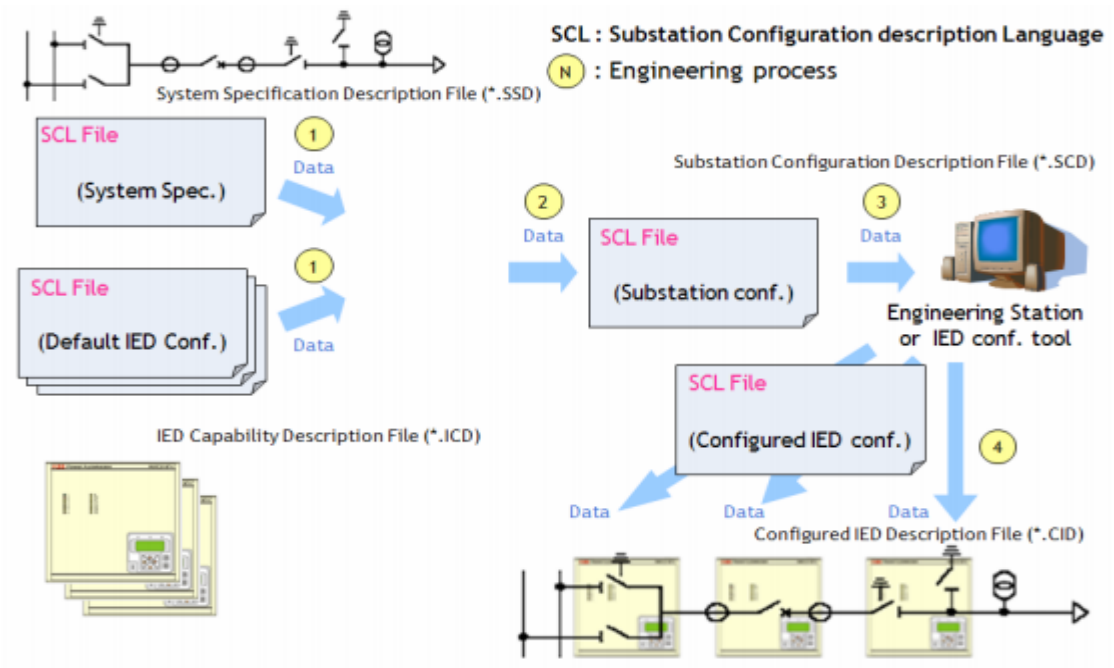

Рисунок 2.3 – Конфігураційні файли згідно з IEC-61850-6

2.2 Методи і моделі проектування сучасних розподілених систем керування промисловими процесами.

Внутрішня логіка IED-пристрою виконується за допомогою методів та моделей описаних у стандартах IEC-61131, IEC-61499.

Основним стандартом для розробки систем керування процесами довгий час був IEC-61131 [11]. Однією з найважливіших цілей стандарту є уніфікація концепцій програмування керуючих систем. Стандарт затверджує п’ять мов, що використовується для програмування логіки керування промисловими процесами (Таблиця 2.1).

Таблиця 2.1 – Мови програмування щодо стандарту IEC-61131

Abbr	English	Українська назва
LD	Ladder diagram	Релейно-контактні схеми
FBD	Function Block Diagram	Діаграма функціональних блоків
SFC	Sequence Function Chart	Діаграми послідовно-функціональні
ST	Structured Text	Структурований текст
IL	Instruction List	Список інструкцій

Даний стандарт вводить концепцію функціонального блока (FB), що включає окрему функціональність. Функціональний блок може включати один алгоритм і дані.
Функціональні блоки застосовуються для моделювання та проектування систем автоматизації. Функціональні блоки можуть бути використані також для підтримки всього життєвого циклу системи, включаючи проектування, розробку, валідацію і обслуговування.

Стандарт IEC 61131-3 має ряд недоліків:

1) Використання глобальних даних;
2) Неможливість прямого керування порядком виконання функціональних блоків.

Відсутність підтримки передових методів розробки збільшує затрати часу та коштів на розробку системи керування та зменшує її надійність. Системи розроблені відносно цього стандарту є централізованими а термін розподілена обробка відноситься лише до зняття інформації з датчиків через промислову мережу та обробкою її у PLC.

На зміну стандарту IEC-61131 введено IEC-61499. Його архітектура базується на основі свого попередника. Основним елементом також виступає FB. Однак концепція блока розширена. Одним з основних розширень є інтерфейс на основі події, що дозволяє явно визначити послідовність виконання FB. Другим нововведенням полягає в об’єктній та компонентній орієнтації – FB може містити декілька алгоритмів. Однак ці алгоритми є інкапсульованими і не мають прямого доступу.

Також ФБ на відміну від свого попередника із стандарту IEC 61131-3 не має глобальних змінних – функціональний блок представляє собою незалежну одиницю, що може бути реалізована, протестована і використана окремо від інших блоків.

2.2.1 Модель системи щодо стандарту IEC-61499

Система представляє сукупність пристроїв, що взаємодіють поміж собою за допомогою комунікаційної мережі (Рисунок 2.4). Ця мережа складається з сегментів і ліній зв'язку.

Функція, що виконується системою керування, описується з використанням додатку, який може знаходиться в одному або розділюватись за кількома пристроями.

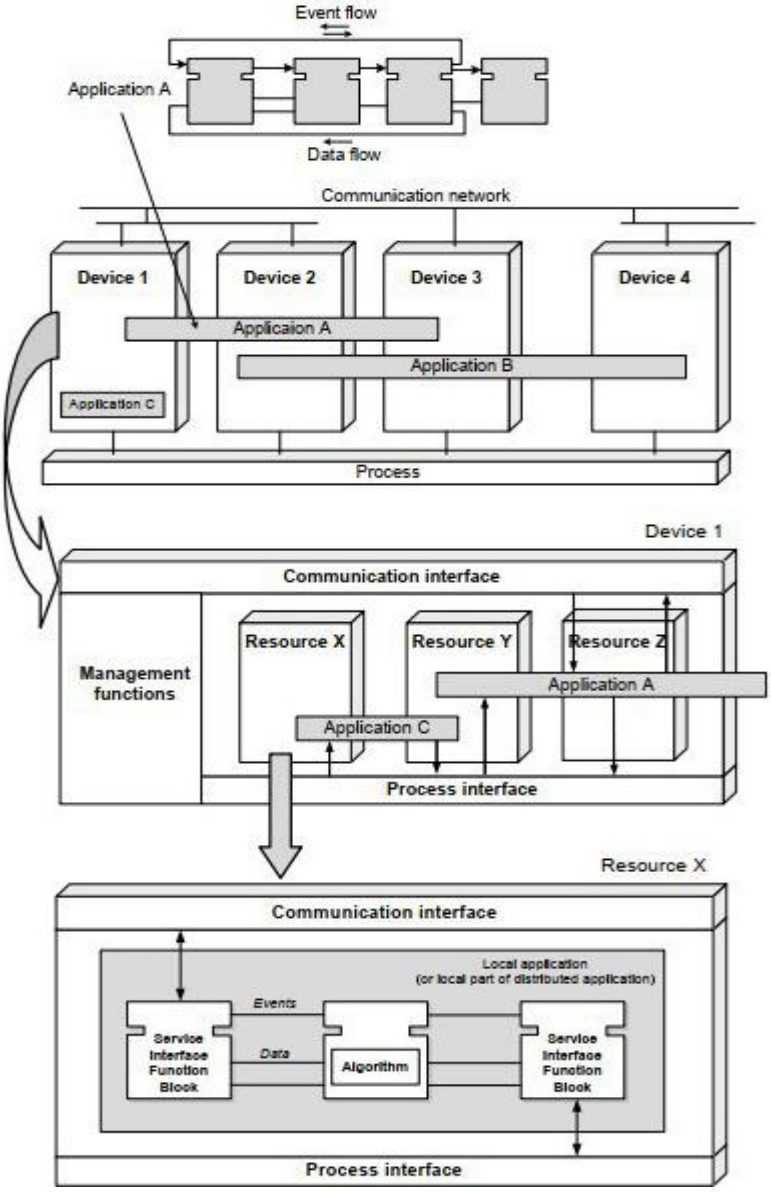

Рисунок 2.4 – Програми управління згідно IEC-61499

Пристрій являє собою фізичну сутність, здатну виконувати одну або кілька специфіковані функцій в певному контексті і має щонайменше один інтерфейс. Інтерфейс може бути:

– інтерфейсом керованого процесу;
– комунікаційним інтерфейсом.

Ресурс – є функціональною одиницею, що має незалежне управління своїми операціями, включаючи планування та виконання алгоритмів. Незалежно від інших ресурсів може бути створений, конфігурований, запущений або видалений. Ресурс відповідає за прийом даних і подій з керуючого процесу або комунікаційної мережі. Найважливішою функцією є диспетчеризація .

Додаток є програмної функціональної одиницею. Він призначений для вирішення певної задачі в системі управління і представляється у вигляді мережі пов'язаних між собою функціональних блоків. Модель додатки представлена на рисунку 2.5.

Основним елементом проектування в IEC-61499 є функціональний блок [12], який представляє собою специфічний програмний компонент з інтерфейсом.

Інтерфейс представляє подієві та інформаційні входи і виходів для взаємодії з оточуючими його елементами. Інформаційні входи/виходи (I/O) визначаються у вигляді змінних FB.

Функціональні блоки розподіляють на три типи:

– Базисний (Рисунок 2.5 а);
– Складовий (Рисунок 2.5 б);
– Сервісні інтерфейсні функціональні блоки (СІФБ);

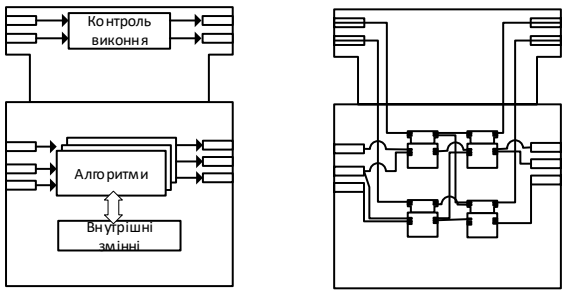

Рисунок 2.5 - Базісний (а) і складовий (б) функціональні блоки

Функції базисного FB визначаються машиною станів (Execution Control Chart – ECC) по типу автомат Мура [13]. Із станом можуть бути пов’язані алгоритми і вихідні події, визначені однією з мов PLC, що визначені у стандарті IEC-61131-3. Подія активізує базисний FB, після чого він проходить ряд станів виконуючи свої алгоритми і видає вихідні сигнали.

Діаграма машини станів виконується під управлінням спеціальної машини станів OSM (Operation State Machine) (рис. 2.6).

Стан s0 можна інтерпретувати як вільний стан FB, стан s1 - як стан оцінки переходів діаграми ECC (EC-переходів) і стан s2 - як стан виконання EC-акцій, пов'язаних з поточним EC-станом.

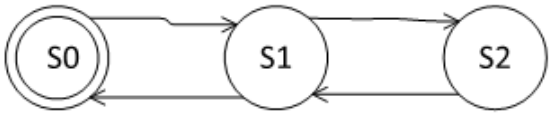

Рисунок 2.6 – Спеціальна машина станів

СІФБ надають один або кілька сервісів з додатком на основі відображення сервісних примітивів на входи і виходи ФБ. Вони працюють як «обгортка», абстрагуючи апаратні засоби. Цим вони схожі на драйвери пристроїв. Сервіс надається у вигляді набору сервісних послідовностей, які в свою чергу представляються послідовністю сервісних транзакцій. Сервісна транзакція складається з вхідного сервісного примітиву і декількох вихідних сервісних примітивів.

2.2.2 Моделі виконання функціональних блоків

Стандарт визначає абстрактну модель виконання функціональних блоків, що допускає різні інтерпретації. Така невизначеність може привести до того, що різні середовища можуть мати різні результати виконання при одній інтерпретації блоку.

З метою повної визначеності моделі необхідно створити модель виконання – модель правил, визначаючий порядок виконання мережі функціональних блоків на пристрої або ресурсі.

В ідеалі модель виконання повинна відповідати ряду вимог:

– інтуїтивно зрозумілою;
– простою в реалізації;
– мати передбачувану поведінку;
– з хорошою реактивністю;
– не мати зациклень;
– детермінованою;
– піддаватись верифікації;
– незалежної від засобів її реалізації.

На рисунку 2.7 приводиться можливе розділення моделей за режимом виконання.

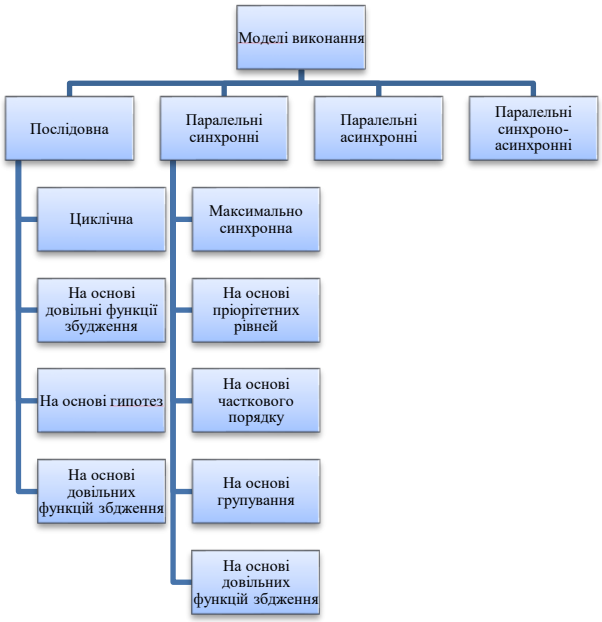

Рисунок 2.7 – Розподілення моделей виконання

У *циклічній моделі виконання* функціональні блоки виконуються циклічно, послідовно один за одним в заздалегідь визначеному порядку, наприклад, fbA, fbC, fbB, fbD. Отже в дана модель передбачає існування списку опитування FB [13].

Синхронна модель виконання передбачає наявність генератора імпульсів для синхронізації. Виконання гранул (EC-переходів або FB) проводиться в моменти дискретного часу t, t+1, …, t – 1, t+n (Рисунок 2.8).

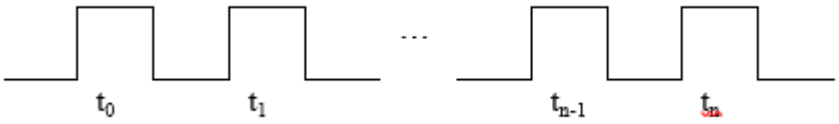

Рисунок 2.8 – Дискретний час визначаємий генератором імпульсів

В один момент часу виконуються всі гранули, що можуть бути виконані.

Синхронна модель виконання має такі переваги:

- ясність і зрозумілість для інженера;
- ФБ, які отримали вхідний сигнал раніше виконуються раніше, що надає їй справедливості;
- відсутність зациклення і відтискування.

Але як і кожна модель вона має недоліки. А саме залежність результату від послідовності виконання ФБ у фронті. Ця проблема може бути вирішена виконанням моделі у якості двохступінчастої схеми виконання з проміжною буферізацією виходів [15]. При цьому за переднім фронтом виконуються дії за першою стунінню а по задньому – другої ступені. Однак такий прийом потребуэ введення проміжного буфера для буферизації вихідних сигналів.

Модель виконання, що заснована на послідовній гіпотезі визначена аксіоматично і базється на шести постулатах [14], що наведені у таблиці 2.2.

Таблиця 2.2 – Постулати до моделі виконання заснованої н послідовній гіпотезі

№	Постулат
1	Твердження: Функціональний блок може бути активований тільки при входженні події на подію Коментар: Це стосується основних і композитних блоків. Функціональні блоки інтерфейсу обслуговування (SIFB) можуть бути активовані зсередини, внутрішніми подіями ресурсу, наприклад. переривання таймера, зовнішні сигнали тощо. Вони, однак, можуть бути вказані явно, коли створюється SIFB
2	Твердження: Виконання (одне виконання) є критичним розділом Коментар: Ми інтерпретуємо його як: "Запуск функціонального блоку" не може бути витіснений іншим запуском функціонального блоку. Проте ресурс може бути витіснений для реєстрації зовнішніх подій і розміщення їх у черзі.
3	Твердження: єдиний запуск основного функціонального блоку – короткий
4	Твердження: Введення подій функціонального блоку очищається після переходу одного ECC, незалежно від того, чи ця подія використовувалася в оцінці, чи ні
5	Твердження: Вихідні події видаються відразу після завершення відповідної дії
6	Твердження: Якщо функціональний блок випускає кілька вихідних подій в одному стані ECC, вони випромінюються послідовно. Частково випливає з постулату 5 та інших явних визначень

Прийомі і обробка вхідного сигналу виконується як єдине ціле до тих пір, поки в ньому є дозволені ЄС-переходи. Вихідні сигнали виводяться послідовно, по мірі їх виникнення.

Функціональний блок, що першим отримав сигнал – виконується в першу чергу. Це забезпечує справедливість моделі. Реалізація послідовної моделі потребує наявності черги (FIFO).

В моделі виконання, що заснована на прямому виклику (Direct Function Call), генерація нової події реалізується шляхом виклику методу run, пов'язаного з ФБ [15].

Особливістю моделі є використання обчислень вглиб на рівні ЕС-переходів. Гранулою виконання є ЕС-акція. Недоліком методу є залежність часу поширення сигналу від топології мережі FB, причому цей час може бути значним.Дана модель не є оптимальною для використання сфері електроенергетики.

Модель виконання на основі збудження (спускових функцій) визначає порядок виконання функціональних блоків. Окрім порядку виконання модель включа включає правила обробки вхідних і видачі вихідних сигналів, правила передачі сигналів іншим блокам а також правила інтерпретації ECC [15]. Модель потребує введення ряду визначень (Таблиця 2.3).

Таблиця 2.3 – Визначення для моделі виконання на основі спускових функцій

Визначення	Опис
$FB = \{fb_1, fb_2, \dots, fb_n\}$	безліч FB, що входять в систему і підлягають виконанню
$EI^j = \{ei_1^j, ei_2^j, \dots, ei_k^j\}$	безліч подієвих входів блоку fb_j (надалі для простоти верхній індекс буде опускатися)
$ZEI: EI \to \{0,1\}$	функція значень вхідних подієвих змінних

Якщо *EI* $(ei_j) = 1$, то вхідна подієва змінна ei_j встановлена (сигнал присутній на вході), інакше - скинута.

Предикат $activeFB: FB \to \{true, false\}$ визначає, які функцыональні блоки є активними в поточний момент модельного часу. Предикат задає спускову функцію. Інтерпретатором буде зроблена спроба запуску активного FB.

Позначимо $\{fb \in FB | activeFB(fb)\}$ як безліч активних ФБ в поточний момент модельного часу. Позначимо $FB_{ap} = \{fb \in FB | activeFBPrev(fb)\}$ – як безліч ФБ, які були активними безпосередньо в минулому.

Предикат $enabled(fb_j) = \exists ei \in EI[ZEI(ei) = 1]$ визначає, ча є дозволеним в поточний момент модельного часу блок fbj. Функціональний блок є дозволеним якщо хочаб н одному із подієвих входів є сигнал.

Визначимо $FB_e = \{fb \in FB | enabled(fb)\}$ як множина дозволених FB.

Функція EOS(fb_j) визначає лінійно-упорядковану мультімножину (послідовність), що видані блоком $fb_j \in FB$ при своєму поповненні. В даному випадку сигнали ідентифікуються

виходами подій АИ, на яких вони знаходяться. Впорядкованість визначається порядком видачі сигналів.

Функція EIS (fb_j) визначає послідовність сигналів, які з'явилися на входах функціональних блоків в результаті виконання блоку fbj. Впорядкованість визначається порядком появи сигналів на входах.

Функція OF (fb_j) визначає послідовність блоків-приймачів сигналів, виданих з блоку fbj при його виконанні. Впорядкованість визначається порядком отримання відповідними блоками вхідних сигналів.

Функція $pr: FB \cup EI \to N_0 = \{0,1,2, \dots\}$ визначає пріоритет блоку або подієвого входу. Відношення переваги $Pref \subseteq FB \times FB$ служить для визначення найбільш бажаних блоків для виконання. Це відношення часткового порядку. Якщо $(fb_i, fb_j) \subseteq Pref$, то виконання блоку fb_i краще виконання блоку fb_j.

Відношення $PoolOrder \subseteq FB \times FB$ задає жорсткий порядок виконання ФБ в циклічної моделі. За допомогою цього відносини все ФБ пов'язані в кільце опитування.

Ставлення $EvConn \subseteq FB \times FB$ визначає подієві зв'язку між ФБ як цілими одиницями. Позначимо prefb – безліч попередників блоку fb по відношенню EvConn.

Предикат activeEI(ei_j) визначає, чи є подієвий вхід ei_j активним. Сигнал на активному вході підлягає обов'язковій обробці.

Функція $\tau^j: EI^j \to N \cup \{\omega\}$ визначає часи прибуття (порядкові номери) сигналів на подієвих входах блоку fbj. Надалі для простоти верхній індекс буде опускатися. Якщо $\tau^j(ei_k) = \omega$, то вважається, що на подієвої лінії eik сигнал відсутній. У кожен новий момент модельного часу локальні годинник для реєстрації вхідних сигналів в системі скидаються в нуль.

Використовуючи спусковий механізм, можна визначити майже будь-яку іншу модель включаючи нетрадиційні моделі виконання. Така гнучкість, що досягається при генерації моделей виконання, дозволяє встановити підвищений пріоритет для конкретного шляху критичного проходу сигналу за певних умов або умовно виключити і включити FB в процес планування, що є дуже корисним при проектуванні реконфігованих систем.

2.2.3 Методи побудування сучасних IED

Однією з головних вимог до сучасних розподілених систем промислового керування є їх швидкодія. По перш за все це час реагування на подію і її обробки а також гнучкість інтелектуального електронного пристрою.

Ця вимога досягається не лише ефективно обраними моделями комунікації і алгоритмів захисту та автоматики, але й вимогами побудови самої системи. Використання операційних систем широкого споживання не в змозі забезпечити її виконання.

Програмовані логічні контролери (ПЛК) дозволяють отримати бажаний час роботи, але втрачається їх універсальність, бо кожна зміна у логікі роботи потребує зміни в програмному коді і повного його перезапису до мікропроцесорної системи.

Забезпечення необхідного рівня сервісу в певний проміжок часу без втрати гнучкості РЗА надають мікропроцесорні системи релейного захисту з використанням операційних систем реального часу (RTOS – real time operation system).

Операційні системи реального часу розподіляють на системи *жорсткого* та *м'якого* реального часу. До систем жорсткого реального часу відносяться RTOS, що можуть забезпечити необхідний час виконання завдання реального часу навіть в найгірших випадках. Системи жорсткого реального часу не дозволяють затримок реакції системи, так як це може призвести до втрати актуальності результатів, великих фінансових втрат і навіть аварій.

Системи які можуть забезпечити необхідний час виконання завдання реального часу в середньому, називається операційною системою м'якого реального часу. В системі м'якого реального часу затримка реакції вважається відновлювальною помилкою не є фатальною. Якщо система не встигла обробити процес, це призведе до зупинки його іншим та повторним продовженням його роботи після.

Більшість програмного забезпечення орієнтоване на «м'який» реальний час. Для подібних систем характерно:

– гарантований час реакції на зовнішні події;
– жорстка підсистема планування процесів;
– підвищені вимоги до часу реакції на зовнішні події або реактивності.

2.3 Вимоги до пристрою релейного захисту

Виходячи із розглянутих методів та моделей а також стандартів, регламентуючих розробку РЗА пристроїв висунуто вимоги, що наводяться в даному розділі.

Розробити інтелектуальний електронний пристрій ImPR1, що є багатофункціональним пристроєм, який поєднує різні функції захисту, автоматизації, контролю, місцевого та дистанційного пульта керування.

ImPR1 призначений для використання в електростанціях (теплових, ядерних і т. д.), підстанціях та розподільних мережах всіх класів напруги (від 6 до 750 кВ).

Метою створення пристрою є:

- розв'язання проблем захисту, автоматики, контролю, локального та дистанційного керування енергосистем з застосуванням інтелектуальних пристроїв релейного;
- підтримання сучасного рівня автоматизації при будівництві систем автоматизації підстанцій з використанням приладів ImPR1;
- забезпечення високої надійності та безпеки роботи підстанцій систем автоматизації відповідно до вимог діючої нормативної документації в енергетичній сфері;

Пристрій повинен складатися із:

- Апаратного забезпечення;
- Системного програмного забезпечення (СПЗ).

2.3.1 Вимоги до апаратного забезпечення:

Апаратне забезпечення ImPR1 повинно забезпечувати повноцінну роботу щодо свого функціонального призначення. Це накладає деякі вимоги до його апаратного складу. Отже для повноцінної роботи релейного захисту необхідна наявність наступних модулів (Рисунок 2.9):

- модуль центрального процесору для виконання основних функції захисту та автоматики (ImPR1_CPUM);
- модуль живлення (ImPR1_PSM);
- пристрої зв’язку з об’єктом (ПЗО) для прийому первинних сигналів від PD та передачі керуючих сигналів (залежно від конфігурації може містити один чи більше модулі I/O дискретних сигналів (ImPR1_DIM, ImPR1_DOM, ImPR1_DIDOM), модулі I/O аналогових сигналів (ImPR1_AIM, ImPR1_AIDOM));
- інтерфейс людина-машина (ImPR1_HMIU);
- генмонтажна плата (ГП).

Комплектація кожного пристрою не є жорстко визначена а може змінюватись відповідно захисту відносно котрого цей пристрій використовується. Але наявність таких модулів як CPUM, PSM та HMIU є обов’язковим.

Модуль центрального процесору – це ядро ImPR1. Від відповідає за всі обчислення логіки релейного захисту і формування відповідних сигналів а також за комунікацію з іншими пристроями в системі цифрової підстанції. CPUM повинен забезпечувати ефективне виконання системного програмного забезпечення.

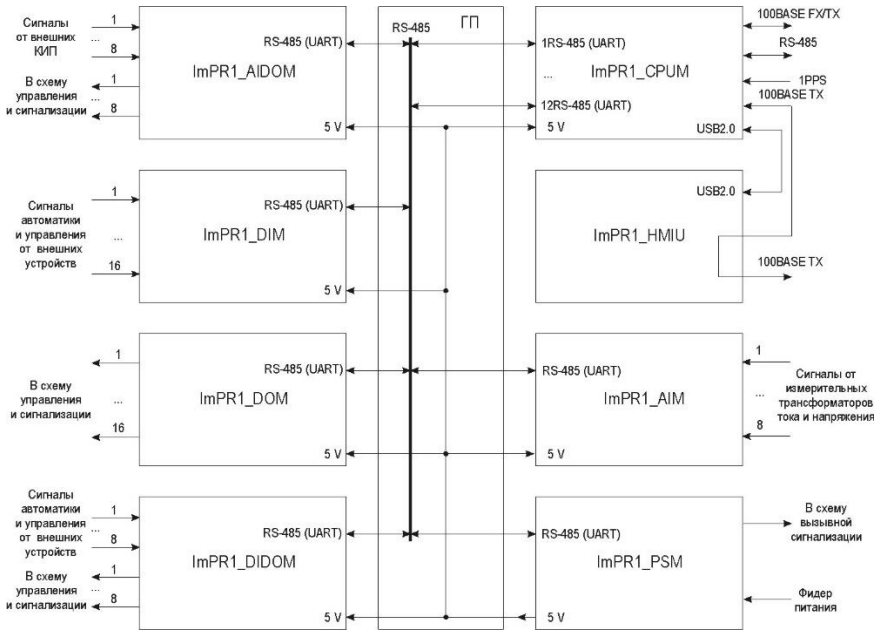

Рисунок 2.9 – Структурна схема ImPR1

Модуль центрального процесору ImPR1 обрано SMARC-T4378 фірми Embedian, що базується на процесорі Sitara AM4378 на основі Cortex-A9 виробництва Texas Instruments.

Модуль SMARC-T4378 має наступні характеристики:

- Процесор - TI Sitara AM4378 (1x Cortex-A9 1000 МГц);
- Графічний процесор PowerVR SGX530;
- Підсистема PRU-ICSS
- 512 МБ (@ 800 МГц) або 1 ГБ (1 ГГц) оперативної пам'яті DDR3L
- 4 Гбайт eMMC 5.0 flash
- SPI NOR 4 МБ
- 2 контролера Ethernet 10/100/1000
- Інші входи/виходи, такі як USB, UART, SPI, I2C, GPIO та ін.

2.3.2 Вимоги до системного програмного забезпечення

Системне програмне забезпечення повинно забезпечувати ефективну і безперебійну роботу захисту, що призначено окремому пристрою. Це потребує наявності в його складі наступних елементів:

- стартова система;
- операційна система реального часу;
- базові програми;
- бібліотеки функціональних блоків (FB);
- налаштування СПЗ.

Стартова система є невід'ємною частиною покупного модуля SMARC. Розробка стартовою системи не виконується. Стартова система стороннього виробника повинна забезпечувати наступні функції при включенні живлення ImPR1:

– ініціалізація вузлів мікропроцесора SMARC необхідних для завантаження програм СПЗ в оперативну пам'ять;
– завантаження виконуваного коду СПЗ в оперативну пам'ять модуля SMARC;
– передача управління СПЗ.

У якості RTOS повинна бути використана операційна система Linux-RT. Оскільки в якості апаратної платформи SMARC для ImPR1_CPUM обраний модуль SMARC-T4378 фірми Embedian, з мікропроцесором Sitara AM4378, то в якості RTOS може бути використана ОС Linux-RT надається Texas Instruments. Дистрибутив Linux-RT фірми Texas Instruments поставляється разом з драйверами для периферії мікропроцесора.

Системне програмне забезпечення ImPR1 повинно забезпечувати ряд функцій:

1) Функції релейного захисту ImPR1:
   – створення вільної логіки захистів;
   – струмового захисту;
   – захисту по напрузі;
   – логічного захистів;
   – дистанційного захисту;
   – диференціального захисту;
   – захисту по частоті;
   – дугового захисту.
2) Функції автоматики ImPR1:
   – створення вільної логіки автоматики;
   – управління апаратами;
   – частотної автоматики;
   – автоматики введення резерву;
   – автоматики повторного включення;
   – пристрій резервування відмови вимикача.
3) Функції контролю, реєстрації і сигналізації ImPR1:
   – контроль оперативних ланцюгів;
   – контроль ланцюгів вимірювання;

- контроль синхронізму;
- центральна схема збору інформаційних сигналів;
- визначення місця пошкодження;
- контроль справності і розрахунок ресурсу високовольтного вимикача;
- світлова і звукова сигналізації;
- реєстрація подій в нормальному і аварійному режимах;
- осцилографування аварійних процесів.

4) Сервісні функції ImPR1:
   - перегляду журналу подій;
   - перегляду осцилограм аварійних ситуацій;
   - індикації поточних величин;
   - завдання уставок;
   - вільно програмовані режими триколірної світлової індикації;
   - вільно програмовані функціональні клавіші;
   - синхронізація календаря і годин астрономічного часу;
   - налаштування логіки захистів і конфігурація;
   - обмін даними з АСК (автоматичні системи керування);
   - виключення несанкціонованого зміни конфігурації пристрою за допомогою системи паролів;
   - самодіагностика протягом всього часу роботи.

Функції релейного захисту і автоматики а також функції контролю, реєстрації і сигналізації повинні бути представлятись в якості функціональних блоків, використання котрих можливе при підключенні бібліотеки функціональних блоків. Бібліотека FB розробляється як окремий комплекс програм з метою незалежного супроводу алгоритмів FB від базових програм СПЗ.

Сервісні функції повинні реалізовуватись як сервісні програми операційної системи ImPR1 із використанням існуючих бібліотек, що входять до складу операційної системи та додаткових бібліотек (бібліотека для забезпечення обміну за стандартом IEC-61850, що використовується для комунікації пристрою з іншими інтелектуальними пристроями РЗ і АСК).

2.3.3 Вимоги систем комунікації пристрою з зовнішніми елементами мережі

Система комунікації повинна забезпечувати дотримання міжнародних стандартів комунікації, зокрема серії стандартів IEC-61850. Дотримання правил, що регламентуються

міжнародними стандартами комунікації надає інтелектуальним електронним пристроям більшої універсальності, зрозумілості в моделі підстанції, а також надає можливості комунікації IED з пристроями інших виробників, що також дотримуються цих стандартів.

2.3.4 Вимоги щодо бібліотеки ФБ

Бібліотека функціональних блоків повинна розроблюватись з дотриманням міжнародних стандартів IEC-61499. Посилаючись на переваги і недоліки моделей виконання функціональних блоків, що розглянуто в даному розділі в якості моделі виконання для подальшої її реалізації в бібліотеці ФБ обрано спеціальну синхронну модель. Синхронна модель виконання справедливість виконання а також не має зациклень і відтискання. Дана модель є простою в реалізації і подальшій її підтримці.

2.4 Висновки за розглянутими моделями

На основі проведеного аналізу методів та моделей, що регламентуються стандартами IEC-61850 та IEC-61499 визначено найбільш ефективні моделі для подальшої їх реалізації в інтелектуальному пристрої РЗА ImPR1.

За розглянутими моделями щодо стандарту IEC-61499 для подальшої реалізації її в пристрої релейного захисту ImPR1 в якості моделі виконання функціональних блоків обрано синхронну модель виконання. Дана модель є простою в реалізації та забезпечує достатній рівень безпеки і справедливості виконання алгоритмів FB.

2.5 Постановка завдання і обґрунтування розробки

З метою реалізації інтелектуального пристрою релейного захисту слід виконати наступні пункти:

1. Розробити архітектуру взаємодії системного програмного забезпечення;
2. Реалізувати інтерфейс комунікації за стандартом IEC-61850;
3. Реалізувати програми виклику функціональних блоків на обраній моделі виконання;

2.6 Висновки до розділу

В даному розділі було розглянуто основні моделі побудови цифрових підстанцій і існуючих методів і моделей розробки пристроїв релейного захисту. Також визначено вимоги щодо проектування інтелектуального пристрою релейного захисту і розроблено структурну схеми пристрою.

На основі проведеного аналізу існуючих моделей виконання FB обрано синхронну модель виконання для подальшої її реалізації в пристрої від ПрАТ СНВО «Імпульс» ImPR1, як базової моделі виконання функціональних блоків. Ця модель є простою в реалізації і ефективною у використанні. До переваг можна віднести її справедливість виконанні FB, відсутність зациклень і відтискання.

Для організації моделі комунікації із зовнішніми пристроями та АСУ обрано модель стандарту IEC-61850, що дозволяє будувати універсальну систему комунікації інтелектуальних пристроїв, що в свою чергу дозволяє налаштовувати комунікації із пристроями інших виробників, підтримуючих цей стандарт.

Розробка інтелектуальних енергосистем є пріоритетною задачею і повинна бути максимально регламентованою на всіх її рівнях. Отже дотримання існуючих стандартів є невід’ємним.

Посилаючись на проведений аналіз методів і моделей релейного захисту була поставлена задача на проектування апаратного та програмного забезпечення пристрою релейного захисту і автоматики.

Актуальність розробки пристрою з підтримкою міжнародних стандартів комунікації IEC-61850, що забезпечує можливість сумісної роботи пристрою із пристроями інших фірм-виробників, що також підтримують ці стандарти. А виконання програмного забезпечення на базі моделі виклику FB згідно до стандарту IEC-61499 надає пристрою легкості і зрозумілості в проектуванні захистів.

РОЗДІЛ 3: РОЗРОБКА ПРИСТРОЮ РЕЛЕЙНОГО ЗАХИСТУ

Відповідно до 2.3 пристрій релейного захисту складається із апаратного і програмного забезпечення. Отже відповідно до вимог визначених у другому розділі слід провести розробку архітектури апаратного і програмного забезпечення пристрою.

3.1 Апаратне забезпечення системи РЗА

Розробка пристрою релейного захисту і автоматики виконується відповідно до технічного вимог на розробку пристрою ImPR1 на ПрАТ СНВО «Імпульс».

Розробка модуля центрального процесору (Рисунок 3.1) реалізується на базі мікропроцесора AM4378 фірми Texas Instruments (згідно до п. 2.3.1 – системні характеристики CPUM).

Цей вибір обґрунтований в першу чергу якістю і надійністю даного виробника та гарної підтримкою споживача. Також даний мікропроцесор розробляється для використання на базі операційної системи реального часу TI-RTOS або Linux-RT. Використання програмного забезпечення, що надаються виробником для інтелектуального пристрою системного захисту значно облегшує розробку системного програмного забезпечення для повноцінного функціонування захисту і автоматики.

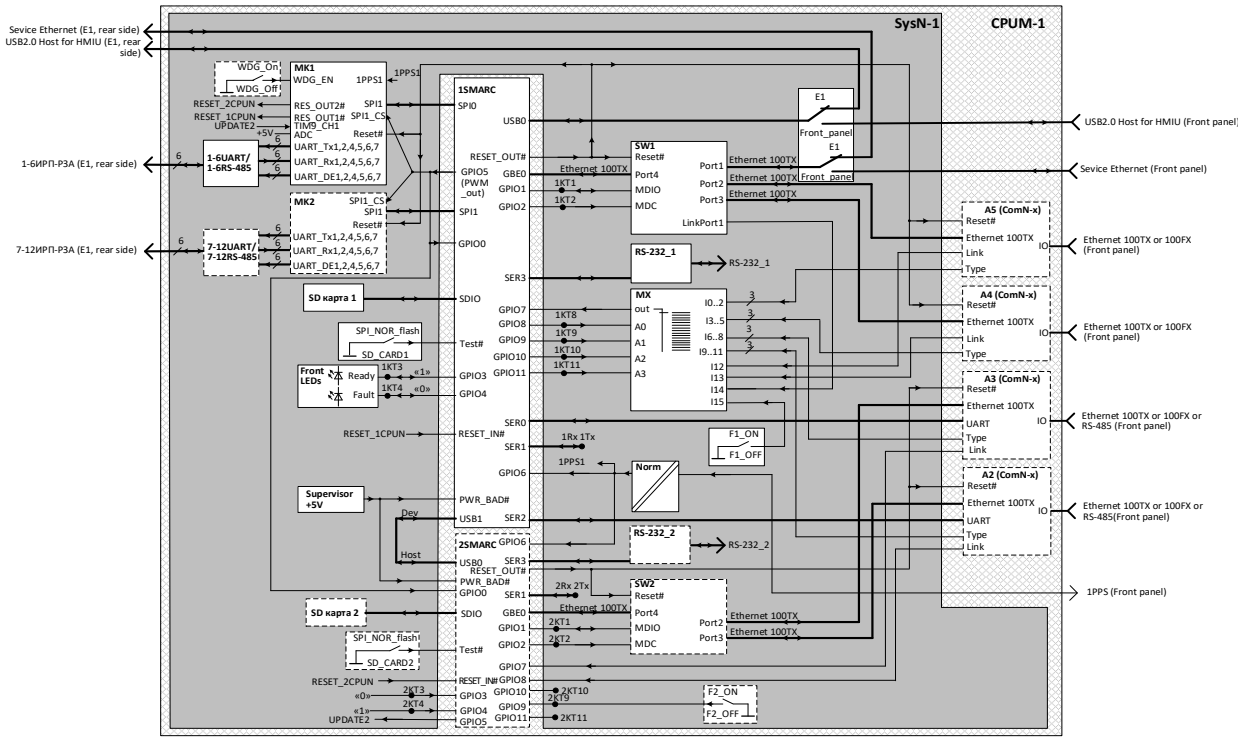

Рисунок 3.1 - Структурна схема ImPR1_CPUM

Мікропроцесор AM4378 реалізований на базі високопродуктивного одноядерного ARM процесора Cortex-A9. Структурна схема мікропроцесора AM4378 представлена на рисунку 3.2.

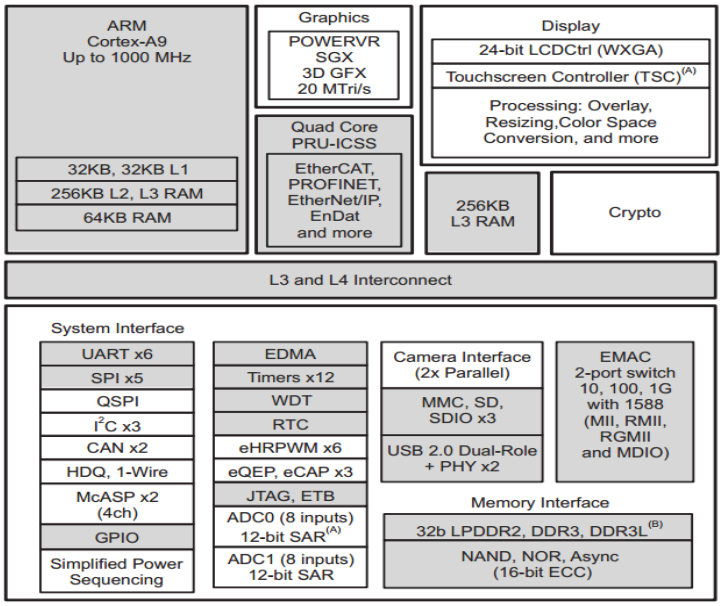

Рисунок 3.2 – Структурна схема мікропроцесора AM4378

У якості операційної системи для даного модуля Texas instruments пропонує два варіанти використання:

– на базі операційної системи TI-RTOS;
– на базі операційної системи Linux-RT.

Для даних альтернатив Texas Instruments надає повні пакети програмного забезпечення, а також SDK та середовище програмування на основі IDE eclipse;

Використання SMARC на платформі Linux-RT надає ряд переваг, головною з яких – це наявність безлічі сервісних програм і бібліотек операційної системи, що полегшує процес розробки своїх додатків.

3.1.1 Обмін з пристроями зв’язку з об’єктами

Робота пристрою базується на прийомі інформаційних та формування керуючих сигналів релейного захисту і автоматики. Отже для забезпечення обміну пристрій містить наступні пристрої зв’язку з об’єктами:

– ImPR1_AIM - модуль вводу аналогових сигналів;
– ImPR1_AIDOM - модуль вводу аналогових і виведення дискретних сигналів;
– ImPR1_DIM - модуль введення дискретних сигналів;

- ImPR1_DOM - модуль формування дискретних сигналів;
- ImPR1_DIDOM - модуль введення та формування дискретних сигналів;
- ImPR1_PSM - модуль живлення.

ПЗО підключаються до мікроконтролерів МК1 і МК2 по RS-485. До кожного модуля можливо підключити до шести пристроїв. Наявність двох мікроконтролерів обґрунтована зниженням навантаження на інтерфейс і створювання черг повідомлень. Обмін поміж SMARC і мікроконтролерами відбувається по SPI.

Функція обміну з ПЗО повинна забезпечувати виконання таких операцій:

- ініціалізація робочих змінних функції;
- формування кадру запиту за даними настройки функції і даними з оперативною бази даних (далі - ОБД);
- отримання кадрів відповідей з даними по кожному МСО;
- контроль даних кадру відповіді;
- запис даних кадру відповіді в ОБД.

3.1.2 Організація обміну

Функція обміну відповідає за обмін SMARC з пристроями зв’язку з об’єктами

- запити від SMARC в МК1, МК2 по SPI;
- відповіді від МК1, МК2 в 1SMARC по SPI.

Алгоритм обміну складається з такої послідовності дій:

a) ініціатором циклу обміну виступає 1SMARC, формуючи низький рівень сигналу CS (сигнал виходу PWM-таймера (GPIO5)) на інтерфейс SPI1 (МК1, МК2) і передає відповідний кадр запиту в МК1 і МК2, в цей же час МК1 і МК2 передають в 1SMARC кадри відповідей з даними від абонентів, отриманими в попередньому циклі обміну по ІРП-РЗА, і з даними своєї діагностики;
b) після закінчення обміну, CPUM формує сигнал CS (сигнал виходу PWM-таймера 1SMARC) на SPI високого рівня.

Більш детальний огляд обміну між ПЗО та CPUM описано у відповідних технічних вимогах на розробку пристроїв зв’язку з об’єктами.

3.2 Архітектура взаємодії СПЗ

Сучасний пристрій релейного захисту це складний комплекс програмного забезпечення, що забезпечує не тільки виконання задач із релейного захисту і автоматики, але й ряд інших задач. Перелік основних програм, що потребуєтеся від пристрою релейного захисту для забезпечення основного функціоналу наведено в таблиці 3.1.

Таблиця 3.1 – Основні програми СПО

Найменування програми	Функції, що виконуються програмою
Програма ініціалізації	Ініціалізація СПО відповідно до даних прикладної конфігурації
Програма ведення часу	Визначення значення поточного моменту часу, синхронізація часу
Програма обміну з ПЗО	Періодичний обмін з каналами введення аналогових сигналів, введення дискретних сигналів і виведення дискретних сигналів при запитах їх поточного стану та результатів самодіагностики, при формуванні дискретних сигналів
Менеджер виклику ФБ	Циклічний запуск прикладних програм з періодом, заданим при конфігуруванні
Бібліотека ФБ	Функції, що викликаються на виконання менеджером виклику ФБ: - функції захисту, автоматики, контрою ланцюгів, логіки і вимірювання; - базові функції; - функції місцевого ІЧМ;
Аварійний осцилограф	Осцилографування аварійних процесів
Регістратор подій	Реєстрація подій
Програма обміну с HMIU	Обмін даними виведеними на дисплей і світлодіодні панелі HMIU, прийом даних стану клавіатури і результатів самодіагностики HMIU
Програма обробки HMIU	Формування зображення виводиться на дисплей HMIU, обробка команд від HMIU, висновок індикації
Програма авторизації	Контроль і захист від несанкціонованого доступу до ImPR1
Програма обміну по Ethernet	Обмін інформацією з зовнішніми абонентами по каналах зв'язку Ethernet
FTP сервер	Організація файлового введення-виведення при обміні файлами по мережі Ethernet
Програма фонової діагностики	Контроль працездатності технічних і програмних засобів ImPR1 в процесі функціонування

Для реалізації роботи інтелектуального пристрою релейного захисту слід реалізувати модель взаємодії логічних функцій системного програмного забезпечення (Рисунок 3.3).

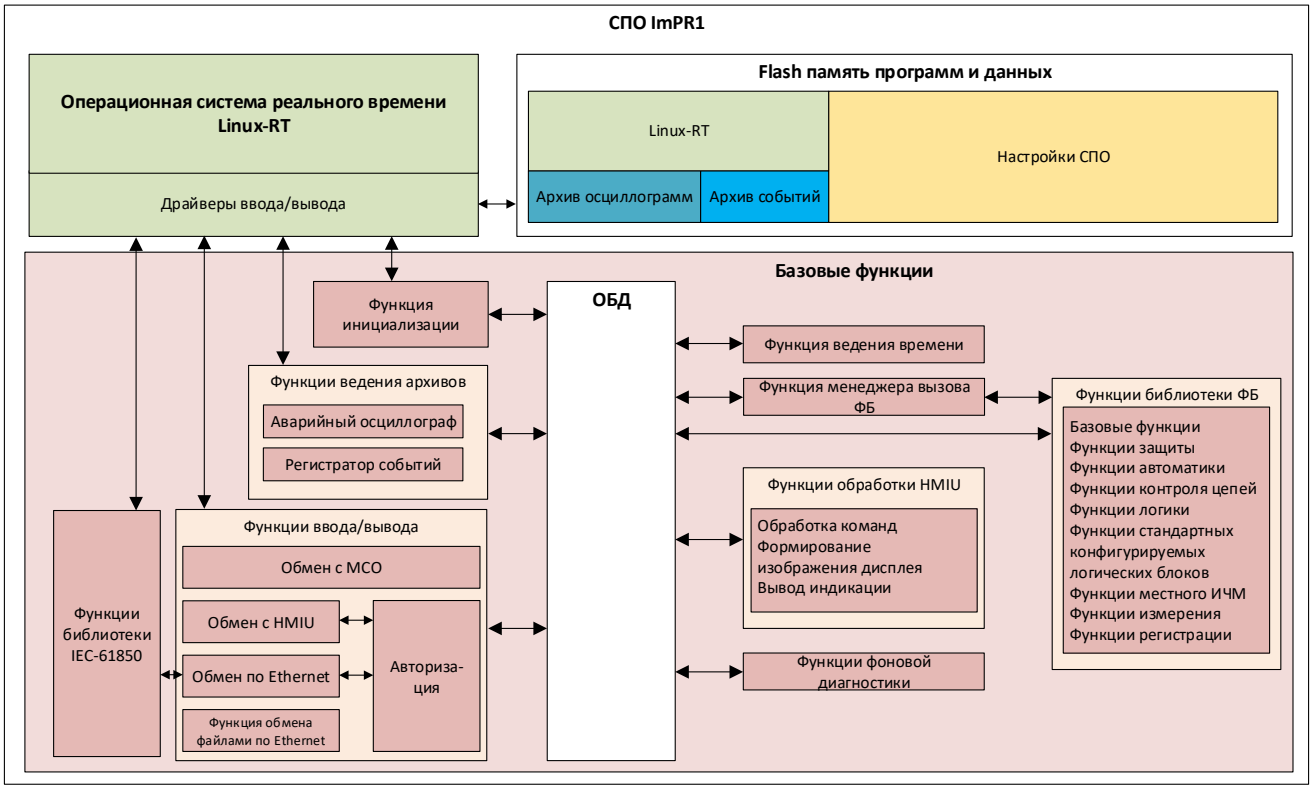

Рисунок 3.3 – Функцыональна схема взаэмодії функцій СПЗ

3.2.1 Функція запису ОБД до ПЗУ

При виконанні логіки розрахунку певних FB виникає завдання збереження значень змінних ОБД в незалежній пам'яті для забезпечення подальшої ініціалізації FB з урахуванням стану FB на момент відключення живлення ImPR1.

Збереження значень змінних ОБД в незалежній пам'яті потрібно:

– запам'ятовування стану світлодіодів на момент відключення живлення ImPR1;
– ФБ тригер з пам'яттю, відновлює стан виходу тригера після подачі живлення на ImPR1;
– запам'ятовування останньої поданої команди на комутаційний апарат в системах залізничної автоматики на момент відключення живлення ImPR1. Після подачі живлення на ImPR1 перевіряється стан комутаційного апарату і поданої раніше команди, при невідповідності положення комутаційного апарату формується аварійна сигналізація.

3.3 Реалізація інтерфейсу комунікації на основі моделі IEC-61850

З метою налагоджування комунікації із зовнішніми пристроями та автоматичними системами керування за протоколами, що регламентуються стандартом IEC-61850 використовується бібліотека з відкритим сирцевим кодом IEC-61850 [16].

Бібліотека забезпечує взаємодію (Рисунок 3.4) програмного забезпечення інтелектуального пристрою релейного захисту з апаратним забезпеченням для обміну даними з іншими пристроями через інтерфейси RS-475 та Ethernet за протоколами, що регламентуються стандартом IEC-61850.

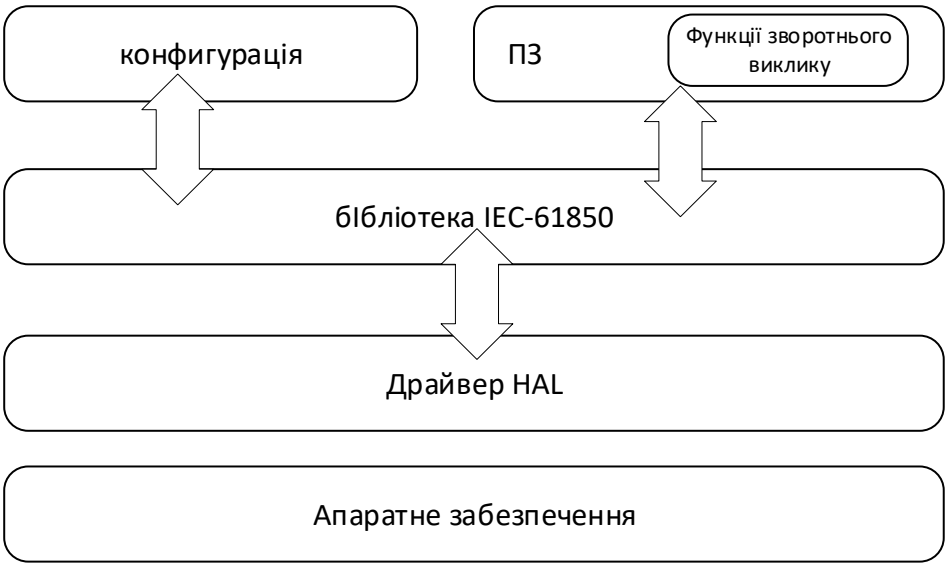

Рисунок 3.4 - Відображення взаємодії ПЗ і апаратного забезпечення через бібліотеку IEC-61850

Бібліотека підтримує такі операції управління: вибір, вибір із значенням, управління, активація по часу, робота і скасування.

Для використання серверної частини моделі управління необхідно встановити обробники зворотного виклику для керованого об'єкта даних. Бібліотека має три різних типи функцій зворотного виклику, пов'язаних з управлінням. Вони будуть викликатися стеком серверів в різних станах моделі управління IEC-61850.

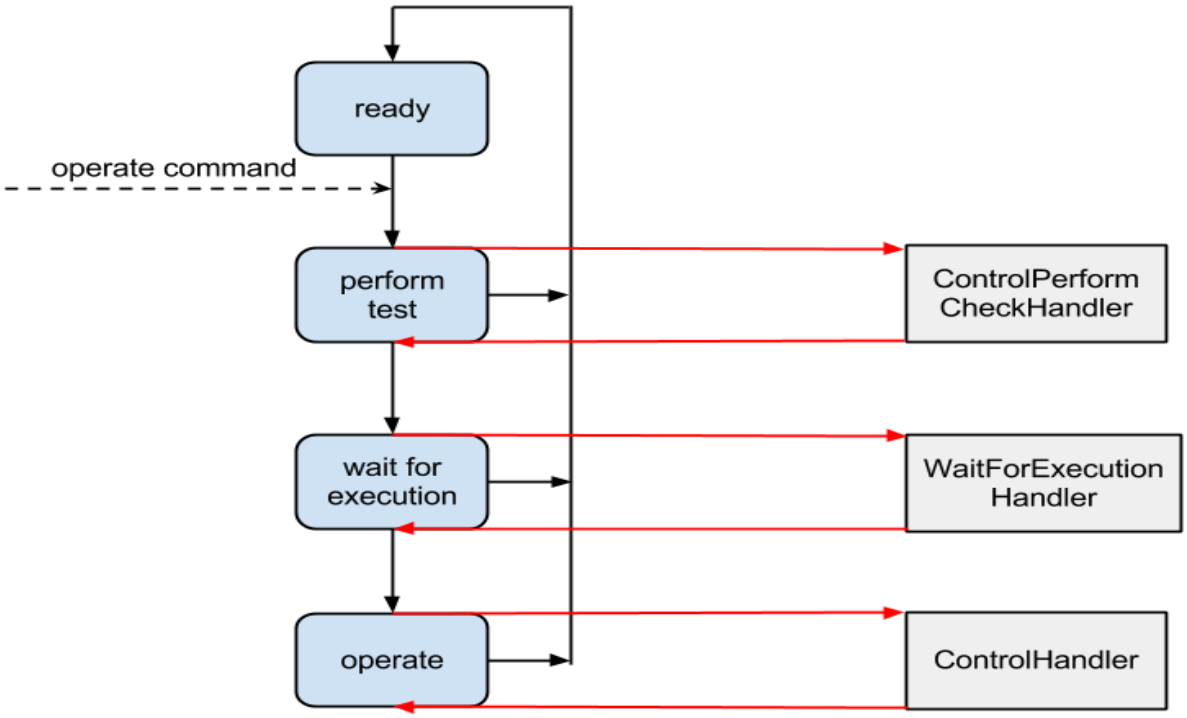

Рисунок 3.5 - Базовий кінцевий автомат моделей управління МЕК 61850 і відповідних функцій зворотного виклику.

Якщо не використовується, кінцевий автомат управління знаходиться в стані готовності. Після отримання запиту на роботу від клієнта кінцевий автомат перемикається в стан PerformCheck. У цьому стані серверний додаток може виконувати статичні тести (для перевірки, чи допускає стан процесу виконання операції управління). У разі помилки сервер відправляє негативну відповідь і перемикається назад в стан готовності. У разі успіху кінцевий автомат управління перемикається в стан WaitForExecution – у цьому стані можуть виконуватися динамічні тести.

Така реалізація обміну допомагає зменшити навантаження на інтерфейси Ethernet, бо під час відсутності повідомлень знаходиться у стані очікування і не займає інтерфейс його опитуваннями.

3.4 Реалізація менеджера функціональних блоків на основі синхронної моделі виклику

З метою розподілення навантаження виконання функціональних блоків здійснюється не в одному а і кількох менеджерах FB (Рисунок 3.6). Так при старті інтелектуального пристрою буде створено стільки менеджерів FB, скільки типів функціональних блоків за часом виконання описано у конфігураційному файлі. Отже якщо конфігурація створена користувачем містить тільки 1мс функціональні блоки то буде створено тільки один процес для виконання , якщо конфігурація містить деяку кількість 1мс і 3мс блоків, то буде створено два менеджери FB.

Обмін даними між менеджерами виконується через розподілену пам’ять.. Кожен менеджер має свій час виклику: наприклад менеджер 3 мс блоків викликається кожні 3 мс і у встановленому порядку виконує всі функціональні блоки, що містить.

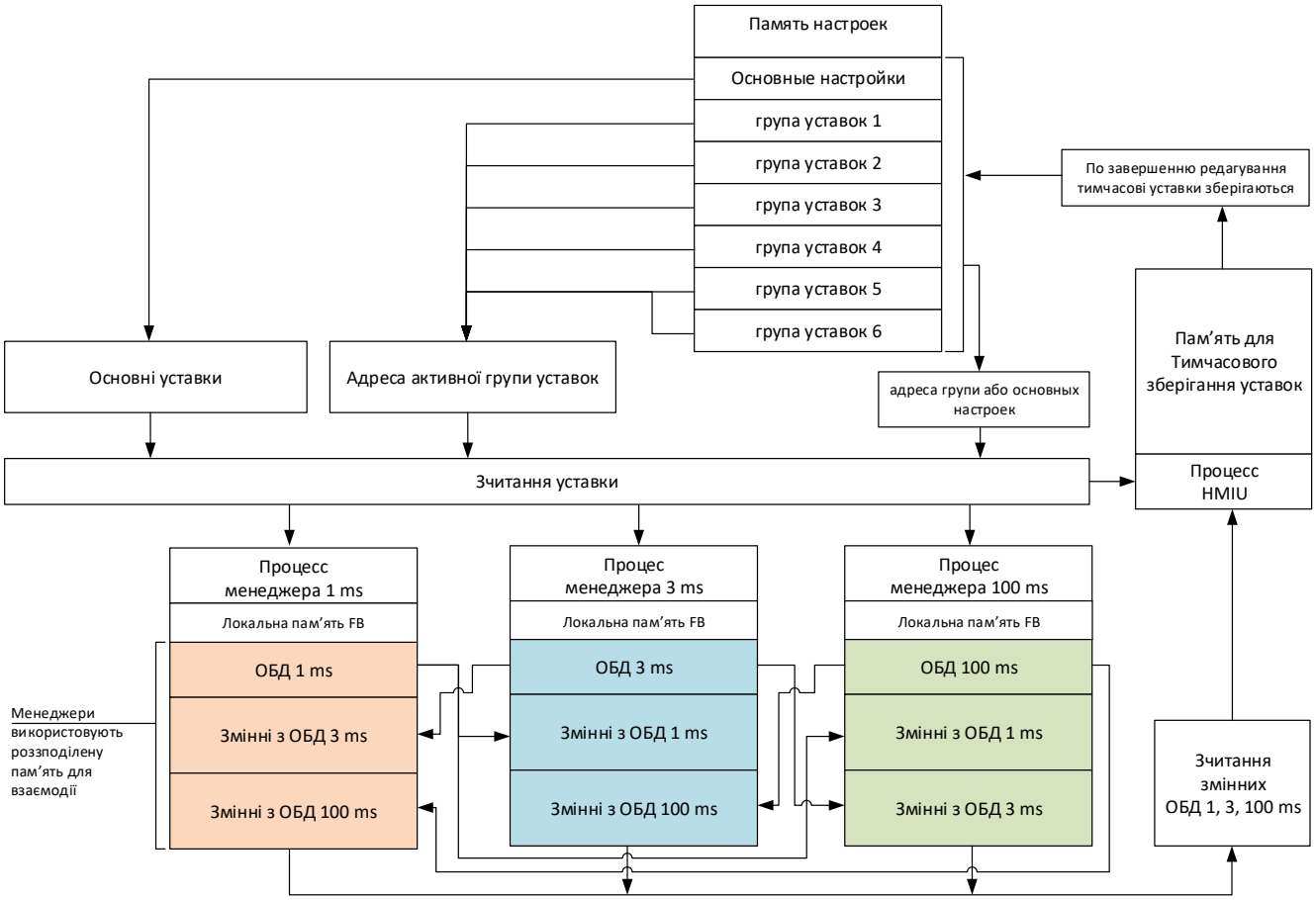

Рисунок 3.6 - Структурна схема обміну даними поміж менеджерами FB

Основні та групові уставки функціональних блоків знаходяться оперативній базі даних. При старті менеджерів або виході з конфігураційного режиму проходить зчитання уставок із пам’яті в пам’ять процесу. Ця операція проводиться для більш швидкого подальшого звернення до них. Варто зазначити, що будь які зміни в уставках окрім зазначених вище режимах не можливі. При конфігураційному режимі уставки записуються у тимчасову пам’ять, що є зеркальним відображенням поточної групи уставок та основних уставок, таким чином ми отримуємо заповнений шаблон уставок для подальшого редагування. По завершенню редагування уставок – тимчасова група перевіряється на відповідність нововведених уставок і

після успішної перевірки вони записуються на місце поточних уставок. Якщо зберігаємі уставки – групові, то вони записуються у поточну групу або під вказаним для запису номером групи.

ImPR1 може містити від 1 до 6 груп налаштувань. Кількість груп налаштувань і їх дані задаються в настройках прикладної конфігурації. Зміна активної групи налаштувань може бути ініційовано в такий спосіб:

- оператором по команді з місцевого ІЧМ;
- оператором при редагуванні уставок ImPR1 в САПР ІПО;
- прикладною програмою через функціональний блок GRSET.

Всі менеджери виконуються за синхронною моделлю виконання ФБ. Отже їх робота повинна бути синхронізована. При появі переднього фронту виконуються всі функціональні блоки викликаного менеджера у встановленому порядку. Так як кожен з менеджерів містить тільки FB своєї часової групи – необхідність постійного виклику всіх менеджерів відсутня – викликаються лише ті менеджери дискретний час котрих вийшов. Після відпрацювання менеджеру лічильник часу цього менеджера скидається і відлік для нього починається знов. Таким чином навантаження на процесор знижується так як нема необхідності й заходити в функції ФБ, якщо він ще не повинен працювати.

3.5 Висновки до розділу

Розроблено структурні і функціональні до пристрою релейного захисту згідно до визначених в другому розділі вимог, що забезпечує функціонування інтелектуального пристрою релейного захисту ImPR1.

За поставленими задачами було виконано:

- розроблено архітектуру взаємодії системного програмного забезпечення;
- спроектовано інтерфейс комунікації за стандартом IEC-61850;
- розроблена функціональна схема виклику функціональних блоків на обраній моделі виконання згідно до IEC-61499;
- розроблено структурну схем системи РЗА.

Спроектоване програмне забезпечення надає підтримку міжнародних стандартів IEC-61850 та IEC-61499. Така реалізація дозволяє отримати універсальний пристрій, що має можливість налагоджувати обмін з пристроями інших виробників, які також мають підтримку цих стандартів.

РОЗДІЛ 4: РОЗДІЛ 4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ. ЕКОЛОГІЯ

В даному розділі проведено аналіз потенційних небезпечних та шкідливих виробничих факторів, причин пожеж. Розглянуті заходи, які дозволяють забезпечити гігієну праці і виробничу санітарію. На підставі аналізу розроблені заходи з техніки безпеки та рекомендації з пожежної профілактики.

Завданням даної магістерської роботи було аналіз методів та моделей релейного захисту і автоматики і розробка пристрою РЗА за обраними моделями. Так як в процесі написання проектування СПО використовувалося ПК, то аналіз потенційно небезпечних і шкідливих виробничих чинників виконується для персонального комп'ютера на якому буде розроблятися програмне забезпечення для пристрою.

4.1 Загальні питання з охорони праці

В законі України «Про охорону праці» визначається, що охорона праці - це система правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних і лікувально-профілактичних заходів та засобів, спрямованих на збереження життя, здоров'я і працездатності людини у процесі трудової діяльності.

При роботі з обчислювальною технікою змінюються фізичні і хімічні фактори навколишнього середовища: виникає статична електрика, електромагнітне випромінювання, змінюється температура і вологість, рівень вміст кисню і озону в повітрі. Повітря забруднюється шкідливими хімічними речовинами антропогенного походження за рахунок деструкції полімерних матеріалів, які використовуються для обробки приміщень та обладнання. Неправильна організація робочого місця сприяє загальному і локальній напрузі м'язів шиї, тулуба, верхніх кінцівок, викривлення хребта і розвитку остеохондрозу. На всіх підприємствах, в установах, організаціях повинні створюватися безпечні і нешкідливі умови праці.

4.1.1 Правові та організаційні основи охорони праці

Основним організаційним напрямом у здійсненні управління в сфері охорони праці є усвідомлення пріоритету безпеки праці і підвищення соціальної відповідальності держави, і особистої відповідальності працівників.

Користувачі персональних комп’ютерів, для яких ця робота є головною, підлягають медичним оглядам: попереднім — під час влаштування на роботу і періодичним — протягом професійної

діяльності раз на два роки. Жінок з часу встановлення вагітності та в період годування дитини грудьми до роботи з ПК не допускають.

Обов’язки працівників щодо додержання вимог нормативно-правових актів з охорони праці (ст. 14), відповідальність робітників всіх категорій за порушення вимог щодо охорони праці (ст. 44) та структура організації/виробництв системи управління охорони праці визначені у [17].

4.1.2 Організаційно-технічні заходи з безпеки праці

В організації/підприємстві проводиться навчання і перевірка знань з питань охорони праці відповідно до вимог Типового положення про порядок проведення навчання і перевірки знань з питань охорони праці, затвердженого наказом Держнаглядохоронпраці України від 26.01.2005 N 15, зареєстрованого в Міністерстві юстиції України 15.02.2005 за N 231/10511 [18]. Також впроваджені організаційні заходи з пожежної безпеки - навчання і перевірку знань відповідно до вимог Типового положення про інструктажі, спеціальне навчання та перевірку знань з питань пожежної безпеки на підприємствах, в установах та організаціях України, затвердженого наказом Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи від 29.09.2003 N 368, зареєстрованого в Міністерстві юстиції України 11.12.2003 за N 1148/8469 [19].

4.2 Аналіз стану умов праці

Робота над створенням математичної моделі прогнозування критичного стану небезпечного процесу проходитиме в приміщенні відповідної установи. Для даної роботи достатньо однієї людини, для якої надано робоче місце зі стаціонарним комп’ютером.

4.2.1 Вимоги до приміщень

Вимоги до приміщення визначаються за його розмірами. Геометричні розміри приміщення зазначені в табл. 4.1.

Таблиця 4.1 –Розміри приміщення

Найменування	**Значення**
Довжина, м	5
Ширина, м	5
Висота, м	3
Площа, $м^2$	25
Об’єм, $м^3$	75

Згідно з [20] розмір площі для одного робочого місця оператора персонального комп’ютера має бути не менше 6 кв. м, а об’єм — не менше 20 куб. м. Отже, дане приміщення цілком відповідає зазначеним нормам.

Для зручності спільної роботи з іншими працівниками (обговорення ідей, з’ясування проблем і т.д.) в кімнаті є дивани і журнальний стіл, обставлені живими квітами. Також робочий процес пов’язаний з багатьма документами, теками, журналами для чого приміщення облаштоване принтером і шафою для зручності. Задля дотримання визначеного рівня мікроклімату в будівлі встановлено систему опалення та кондиціонування.

Для забезпечення потрібного рівного освітленості кімната має вікно та систему загального рівномірного освітлення, що встановлена на стелі. Для дотримання вимог пожежної безпеки встановлено порошковий вогнегасник та систему автоматичної пожежної сигналізації.

4.2.2 Вимоги до організації місця праці

При порівнянні відповідності характеристик робочого місця нормативним основні вимоги до організації робочого місця за [21] (табл. 4.2) і відповідними фактичними значеннями для робочого місця, констатуємо повну відповідність.

Таблиця 4.2 – Характеристики робочого місця

Найменування параметра	Фактичне значення	Нормативне значення
Висота робочої поверхні, мм	750	680 ÷800
Висота простору для ніг, мм	730	не менше 600
Ширина простору для ніг, мм	660	не менше 500
Глибина простору для ніг, мм	700	не менше 650
Висота поверхні сидіння, мм	470	400 ÷500
Ширина сидіння, мм	400	не менше 400

Глибина сидіння, мм	400	не менше 400
Висота поверхні спинки, мм	600	не менше 300
Ширина опорної поверхні спинки, мм	500	не менше 380
Радіус кривини спинки в горизонтальній площині, мм	400	400
Відстань від очей до екрану дисплея, мм	800	700 ÷800

4.2.3 Навантаження та напруженість процесу праці

Під час виконання робіт використовують ПК та периферійні пристрої (лазерні та струменеві), що призводить до навантаження на окремі системи організму. Такі перекоси у напруженні різних систем організму, що трапляються під час роботи з ПК, зокрема, значна напруженість зорового аналізатора і довготривале малорухоме положення перед екраном, не тільки не зменшують загального напруження, а навпаки, призводять до його посилення і появи стресових реакцій.

Рекомендовано застосування екранних фільтрів, локальних світлофільтрів (засобів індивідуального захисту очей) та інших засобів захисту, а також інші профілактичні заходи на ведені в [21].

Роботу за дипломним проектом визнано, таку, що займає 50% часу робочого дня та за восьмигодинної робочої зміни рекомендовано встановити додаткові регламентовані перерви: – для розробників програм тривалістю 15 хв через кожну годину роботи.

4.3 Виробнича санітарія

На підставі аналізу небезпечних та шкідливих факторів при виробництві (експлуатації), пожежної безпеки можуть бути надалі вирішені питання необхідності забезпечення працюючих достатньою кількістю освітлення, вентиляції повітря, організації заземлення, тощо.

4.3.1 Аналіз небезпечних та шкідливих факторів при виробництві (експлуатації) виробу

Аналіз небезпечних та шкідливих виробничих факторів виконується у табличній формі (табл. 4.3). Роботу, пов'язану з ЕОМ з ВДТ, у тому числі на тих, які мають робочі місця,

обладнані ЕОМ з ВДТ і ПП, виконують із забезпеченням виконання [22], які встановлюють вимоги безпеки до обладнання робочих місць, до роботи із застосуванням ЕОМ з ВДТ і ПП. Переважно роботи за проектами виконують у кабінетах чи інших приміщеннях, де використовують різноманітне електрообладнання, зокрема персональні комп’ютери (ПК) та периферійні пристрої. Основними робочими характеристиками персонального комп'ютера є:

- робоча напруга U=+220В +-5%;
- робочий струм I=2А;
- споживана потужність Р=350 Вт.

Таблиця 4.3 – Аналіз небезпечних і шкідливих виробничих факторів

Небезпечні і шкідливі виробничі фактори	Джерела факторів (види робіт)	Кількісна оцінка	Нормативні документи
1	2	3	4
фізичні			
Підвищена температура поверхонь обладнання	експлуатація ЕОМ, принтерів, сканерів чи/або серверного обладнання для роботи	2	ДСН 3.3.6.042-99
підвищений рівень шуму на робочому місці	-//-	2	ДСН 3.3.6.037-99
підвищена або знижена вологість повітря	-//-	2	ДСН 3.3.6.042-99
підвищена або знижена рухливість повітря	-//-	1	ДСН 3.3.6.042-99
підвищений рівень напруги електричної мережі, замикання якої може відбутися через тіло людини	-//-	4	ГОСТ 12.1.030-81 ГОСТ 13109-97
недостатність природного світла	порушення умов праці (вимог до приміщень)	2	ДБН В.2.5-28:2015

недостатнє освітлення робочої зони	порушення гігієнічних параметрів виробничого середовища	3	ДБН В.2.5-28:2015
підвищена яскравість світла	порушення умов праці (організації місця праці - налагодження моніторів)	1	ДСанПіН 3.3.2.007-98
понижена контрастність	-//-	1	ДСанПіН 3.3.2.007-98
психофізіологічні:			
- нервово-психічна перевантаження (розумове, перенапруження аналізаторів-зорових)	- пошук інформації для постановки теми; - пошук та аналіз аналогів і літератури; - пошук наявних технологій, моделювання та аналіз алгоритмів; - виконання роботи за темою диплома, тестування; - оформлення роботи	4	НПАОП 0.00-1.28-10 ДСанПіН 3.3.2.007-98
- фізичні (статичне – сидіння)	порушення умов праці (організації місця праці - сидіння користувача,) та організації робочого часу - безперервна робота)	2	НПАОП 0.00-1.28-10 ДСанПіН 3.3.2.007-98

Робочі місця мають відповідати вимогам Державних санітарних правил і норм роботи з візуальними дисплейними терміналами електронно-обчислювальних машин, затверджених постановою Головного державного санітарного лікаря України від 10.12.98 N 7 [21].

4.3.2 Пожежна безпека

В приміщенні наявна затверджена «План-схема евакуації з кабінету (приміщення)». Пожежна безпека при застосуванні ЕОМ забезпечується:

1) системою запобігання пожежі,
2) системою протипожежного захисту,

3) організаційно-технічними заходами.

Згідно [99] таке приміщення, площею 25 м^2, відноситься до категорії "В" (пожежонебезпечної) та для протипожежного захисту в ньому проектом передбачено устаткування автоматичною пожежною сигналізацією із застосуванням датчиків-сповіщувачів РІД-1 (сповіщувач димовий ізоляційний) в кількості 1 шт., і застосуванням первинних засобів пожежогасіння. Відповідно до норм первинних засобів пожежогасінні пропонується використовувати:

- ручний вуглекислий вогнегасник ОУ-5 в кількості 1 шт.;
- повсть 1 1 м^2, кошму 2×1,5 м^2 або азбестове полотно 2×2 м^2 в кількості 1 шт.

4.3.3 Електробезпека

На робочому місці виконуються наступні вимоги електробезпеки: ПК, периферійні пристрої та устаткування для обслуговування, електропроводи і кабелі за виконанням та ступенем захисту відповідають класу зони за ПУЕ (правила улаштування електроустановок), мають апаратуру захисту від струму короткого замикання та інших аварійних режимів. Лінія електромережі для живлення ПК, периферійних пристроїв і устаткування для обслуговування, виконана як окрема групова три- провідна мережа, шляхом прокладання фазового, нульового робочого та нульового захисного провідників. Нульовий захисний провідник використовується для заземлення (занулення) електроприймачів. Штепсельні з'єднання та електророзетки крім контактів фазового та нульового робочого провідників мають спеціальні контакти для підключення нульового захисного провідника. Електромережа штепсельних розеток для живлення персональних ПК, укладено по підлозі поруч зі стінами відповідно до затвердженого плану розміщення обладнання та технічних характеристик обладнання. Металеві труби та гнучкі металеві рукави заземлені. Захисне заземлення включає в себе заземлюючих пристроїв і провідник, який з'єднує заземлюючий пристрій з обладнанням, яке заземлюється - заземлюючий провідник.

4.4 Гігієнічні вимоги до параметрів виробничого середовища

4.4.1 Мікроклімат

Мікроклімат робочих приміщень – це клімат внутрішнього середовища цих приміщень, що визначається діючої на організм людини з'єднанням температури, вологості, швидкості переміщення повітря. Оптимальні значення для температури, відносної вологості й рухливості повітря для зазначеного робочого місця відповідають [23] і наведені в табл. 4.4:

Таблиця 4.4

Норми мікроклімату робочої зони об’єкту

Період року	**Категорія робіт**	**Температура С^0**	**Відносна вологість %**	**Швидкість руху повітря, м/с**
Холодна	легка-1 а	22 - 24	40 – 60	0,1
Тепла	легка-1 а	23 - 25	40 – 60	0,1

4.4.2 Освітлення

У проекті, що розробляється, передбачається використовувати суміщене освітлення. У світлий час доби використовуватиметься природне освітлення приміщення через віконні отвори, в решту часу використовуватиметься штучне освітлення. Штучне освітлення створюється газорозрядними лампами.

Розрахунок освітлення.

Для виробничих та адміністративних приміщень світловий коефіцієнт приймається не менше -1/8, в побутових – 1/10:

$$S_b = \left(\frac{1}{5} \div \frac{1}{10}\right) \cdot S_n, \tag{4.1}$$

де S_b – площа віконних прорізів, м^2;

S_n – площа підлоги, м^2.

$S_n = a \cdot b = 5 \cdot 5 = 25$ м^2,

$S = 1/8 \cdot 25 = 3{,}125$ м^2.

Приймаємо 2 вікна площею S=1,6 м^2 кожне.

Світильники загального освітлення розташовуються над робочими поверхнями в рівномірно-прямокутному порядку. Для організації освітлення в темний час доби передбачається обладнати приміщення, довжина якого складає 5 м, ширина 5 м, світильниками ЛПО2П, оснащеними лампами типа ЛБ (дві по 80 Вт) з світловим потоком 5400 лм кожна.

Розрахунок штучного освітлення виробляється по коефіцієнтах використання світлового потоку, яким визначається потік, необхідний для створення заданої освітленості при загальному рівномірному освітленні. Розрахунок кількості світильників n виробляється по формулі (4.2):

$$n = \frac{E \cdot S \cdot Z \cdot K}{F \cdot U \cdot M}, \tag{4.2}$$

де E – нормована освітленість робочої поверхні, визначається нормами – 300 лк;

S – освітлювана площа, м^2; S = 25 м^2;

Z – поправочний коефіцієнт світильника (Z = 1,15 для ламп розжарювання та ДРЛ;

Z = 1,1 для люмінесцентних ламп) приймаємо рівним 1,1;

K – коефіцієнт запасу, що враховує зниження освітленості в процесі експлуатації – 1,5;

U – коефіцієнт використання, залежний від типу світильника, показника індексу приміщення і т.п. – 0,575

M – число люмінесцентних ламп в світильнику – 2;

F – світловий потік лампи – 5400лм (для ЛБ-80).

Підставивши числові значення у формулу (4.2), отримуємо:

$$n = \frac{300 \cdot 25 \cdot 1{,}1 \cdot 1{,}5}{5400 \cdot 0{,}575 \cdot 2} \approx 2{,}0$$

Приймаємо освітлювальну установку, яка складається з 2-х світильників, які складаються з двох люмінесцентних ламп загальною потужністю 160 Вт, напругою – 220 В.

4.5 Вентилювання

У приміщенні, де знаходяться ЕОМ, повітрообмін реалізується за допомогою природної організованої вентиляції (вентиляційні шахти), тобто при V приміщення > 40 м^3 на одного працюючого допускається природна вентиляція. Цей метод забезпечує приток потрібної кількості свіжого повітря, що визначається в СНіП.

Також має здійснюватися провітрювання приміщення, в залежності від погодних умов, тривалість повинна бути не менше 10 хв. Найкращий обмін повітря здійснюється при наскрізному провітрюванні.

4.6 Заходи з організації виробничого середовища та попередження виникнення надзвичайних ситуацій

Загальний опір захисного заземлення визначається за формулою:

$$R_{ççï} = \frac{R_ç \cdot R_n}{R_n \cdot n \cdot \eta_ç + R_ç \cdot \eta_n} \tag{4.3}$$

де $R_з$ - опір заземлення, якими можуть бути труби, опори, кути і т.п., Ом;

R_n - опір опори, яка з'єднує заземлювачі, Ом;

n - кількість заземлювачів;

$\eta_з$ - коефіцієнт екранування заземлювача; приймається в межах 0,2 ÷ 0,9; $\eta_з = 0,7$

η_n - коефіцієнт екранування сполучної стійки; приймається в межах 0,1 ÷ 0,7; $\eta_n = 0,5$;

Опір заземлення визначається за формулою:

$$R_ç = \frac{\rho}{2\pi \cdot l}\left(\ln\frac{2 \cdot l}{d} + \frac{1}{2}\ln\frac{4 \cdot t + l}{4 \cdot t - l}\right) \tag{4.4}$$

де ρ - питомий опір ґрунту, залежить від типу грунту, Ом·м;

для піску - 400 ÷ 700 Ом·м; приймаємо ρ = 400 Ом·м;

l - довжина заземлювача, м; для труб - 2-3 м; l = 3 м;

d - діаметр заземлювача, м; для труб - 0,03-0,05 м; d = 0,05 м;

t - відстань від середини забитого в ґрунт заземлювача до рівня землі, м; t = 2 м.

$$R_ç = \frac{400}{2\pi \cdot 3}\left(\ln\frac{2 \cdot 3}{0,05} + \frac{1}{2}\ln\frac{4 \cdot 2 + 3}{4 \cdot 2 - 3}\right) = 110, \hat{I}ì$$

Опір смуги, що з'єднує заземлювачі, визначається за формулою:

$$R_n = \frac{\rho}{2\pi \cdot L} \cdot \ln\frac{2 \cdot L^2}{b \cdot t_l} \tag{4.5}$$

де L - довжина смуги, що з'єднує заземлювачі (м) і приблизно дорівнює периметру будівлі: $П_{буд.} = 42 \cdot 2 + 38 \cdot 2 = 160$ м; L = 160 м;

b - ширина смуги, м; b = 0,03 м;

t_1 - глибина заземлення від рівня землі, м; t_1 = 0,5 м.

$$R_n = \frac{400}{2\pi \cdot 160} \cdot \ln \frac{2 \cdot 160^2}{0{,}03 \cdot 0{,}5} = 5{,}99,\ Îì$$

Кількість заземлювачів захисного заземлення визначається за формулою:

$$n = \frac{2 \cdot R_ç}{4 \cdot \eta_ç} = \frac{2 \cdot 110}{4 \cdot 0{,}7} = 79\ øò \qquad (4.6)$$

де 4 - допустимий загальний опір, Ом;

2 - коефіцієнт сезонності.

Визначаємо загальний опір захисного заземлення:

$$R_{ççï} = \frac{110 \cdot 5{,}99}{5{,}99 \cdot 79 \cdot 0{,}7 + 110 \cdot 0{,}5} = 1{,}7\ Îì$$

Висновок: дане захисне заземлення буде забезпечувати електробезпеку будівлі, так як виконується умова: $R_{ззп} < 4$ Ом.

4.7 Охорона навколишнього природного середовища

4.7.1 Загальні дані з охорони навколишнього природного середовища

Діяльність за темою магістерської роботи, а саме: Інформаційні технології прогнозування критичних станів небезпечних процесів на основі нейромережевого моделювання в процесі її виконання впливає на навколишнє природнє середовище і регламентується нормами діючого законодавства: Законом України «Про охорону навколишнього природного середовища», Законом України «Про забезпечення санітарного та епідемічного благополуччя населення», Законом України «Про відходи», Законом України «Про охорону атмосферного повітря», Законом України «Про захист населення і територій від надзвичайних ситуацій техногенного та природного характеру», Водний кодекс України.

Основним екологічним аспектом в процесі діяльності за даними спеціальностями є процеси впливу на атмосферне повітря та процеси поводження з відходами, які утворюються, збираються, розміщуються, передаються на видалення (знешкодження), утилізацію, тощо в ІТ галузі.

Вплив на атмосферне повітря при нормальних умовах праці не оказує, бо не має в приміщенні сканерів, принтерів та інших джерел викиду забруднюючих речовин в повітря робочої зони.

В процесі діяльності розробника математичної моделі за допомогою ПК виникають процеси поводження з відходами ІТ галузі. Нижче надано перелік відходів, що утворюються в процесі роботи:

Відпрацьовані люмінесцентні лампи - I клас небезпеки

Акумулятор для джерел безперебійного живлення – III клас безпеки

Змінні носії інформації - IV клас небезпеки

Макулатура - IV клас небезпеки

Побутові відходи - IV клас небезпеки

4.7.2 Вимоги до збору, пакування та розміщення відходів ІТ галузі

Наводяться вимоги зберігання виявлених за своєю роботою відходів відповідно до вимог [24].

Відходи в міру їх накопичення збирають у тару, відповідну класу небезпеки, з дотриманням правил безпеки, після чого доставляють до місця тимчасового зберігання відходів відповідно до затвердженої схеми їх розміщення. Зазначені для зберігання відходів місця чи об'єкти повинні використовуватися лише для заявлених відходів.

Не допускається зберігання відходів у невстановлених схемою місцях, а також перевищення норм тимчасового зберігання відходів.

Способи тимчасового зберігання відходів визначаються видом, агрегатним станом і класом небезпеки відходів:

- Відходи I класу небезпеки зберігаються в герметичній тарі (сталеві бочки, контейнери). У міру наповнення тару з відходами закривають герметично сталевий кришкою;

- Відходи II класу небезпеки в залежності від агрегатного стану зберігаються в поліетиленових мішках, бочках, сховищах та інших видах тари, яка запобігає поширенню шкідливих речовин;

- Відходи III класу небезпеки зберігаються в тарі, яка забезпечує локалізацію зберігання, дозволяє виконувати вантажно-розвантажувальні і транспортні роботи і виключає поширення в ОС шкідливих речовин;

- Відходи IV класу небезпеки можуть зберігатися відкрито на промисловому майданчику у вигляді конусоподібної купи, звідки їх автонавантажувачем перевантажують у самоскид і доставляють на місце утилізації або захоронення;

4.7.3 Визначення впливу та заходів щодо поводження з відходами ІТ галузі

З метою визначення та прогнозування впливу відходів на навколишнє середовище, своєчасного виявлення негативних наслідків, їх запобігання відповідно до Закону України «Про відходи» повинен здійснюватися моніторинг місць утворення, зберігання, і видалення відходів. Відомості про місце утворення та місце розташування відходів зазначаються та наводяться у таблиці 4.5.

Таблиця 4.5 – Відомості про місце утворення та місце розташування відходів

№ з/п	Код та найменування відходів за ДК - 005-96	Технологічний процес або виробництво, де утворюються відходи / клас небезпеки	Місце розташування відходу, тара та її кількість, місткість, розміри у разі наявності майданчиків розташування відходів необхідно зазначити тип покриття та наявність даху)
1	7710.3.1.26 Лампи люмінесцентні, та відходи, які містять ртуть, інші зіпсовані або відпрацьовані	1	буд.3, кв. 86
2	7710.3.1.01 Макулатура паперова та картонна (Макулатура)		буд.3, кв. 86
3	Акумулятор для джерел безперебійного живлення	3	буд.3, кв. 86

4.8 Висновки до четвертого розділу

В результаті проведеної роботи було зроблено аналіз умов праці, шкідливих та небезпечних чинників, з якими стикається робітник. Було визначено параметри і певні характеристики приміщення для роботи над запропонованим проектом написаному в дипломній роботі, описано, які заходи потрібно зробити для того, щоб дане приміщення відповідало необхідним нормам і було комфортним і безпечним для робітника. Приведені рекомендації щодо організації робочого місця, а також важливу інформацію щодо пожежної та електробезпеки. Були наведені розміри приміщення та значення температури, вологості й рухливості повітря, необхідна кількість і потужність ламп та інші параметри, значення яких впливає на умови праці робітника, а також – наведені інструкції з охорони праці, техніки безпеки при роботі на комп’ютері.

А також визначені основні екологічні аспекти впливу на навколишнє природнє середовище та зазначені заходи щодо поводження з ними.

ВИСНОВОК

Було проведено аналіз існуючих методів та моделей інтелектуальних пристроїв РЗА, обрано найбільш ефективні для подальшої реалізації. Розроблено вимоги, щодо розробки пристрою і визначено апаратне та програмне забезпечення для реалізації пристрою.

Розроблено архітектуру взаємодії системного програмного забезпечення (функціональну та структурну схем системи РЗА) і спроектовано інтерфейс комунікації за стандартом IEC-61850 та програми виклику функціональних блоків на обраній моделі виконання.

Результатом роботи є розроблені структурні і функціональні схеми пристрою релейного захисту ImPR1. Право на розробку програмного забезпечення із використанням визначених в роботі структур а також методів та моделей належать ПрАТ СНВО «Імпульс». Даний пристрій працює під управлінням Linux-RT, що надає йому гнучкості у налаштуванні, і динаміки у виборі типу захисту. Наявність повнофункціональної операційної системи надають можливості швидкої зміни конфігурації пристрою навіть без перезапуску операційної системи (досить виклику команди в терміналі на перезапуск служби) а файлова ієрархія системи (FHS) GNU/Linux забезпечує високий рівень кібер-безпеки.

ЛІТЕРАТУРА

[1] SmartGrids Europeadn Technolgy Platphorm, «ETIP SNET,» [Онлайновий]. Available: https://www.etip-snet.eu/. [Дата звернення: 2018].

[2] Б. С. Стогній, «Google Академія,» 2017. [Онлайновий]. Available: https://scholar.google.com.ua/citations?user=7-UewIEAAAAJ&hl=ru.

[3] О. В. Кириленко, «Google Academy,» 2017. [Онлайновий]. Available: https://scholar.google.com.ua/citations?user=zLu5BicAAAAJ&hl=uk.

[4] A. Hirsch, Y. Parag та J. Guerrero, *Microgrids: A review of technologies, key drivers, and outstanding issues,* 2018.

[5] V. Sharma, «What is the difference between a microgrid and a smartgrid?,» [Онлайновий]. Available: https://www.researchgate.net/post/What_is_the_difference_between_a_microgrid_and_a_smart grid. [Дата звернення: 1 12 2018].

[6] «Розумна енергосистема,» 27 09 2018. [Онлайновий]. Available: https://uk.wikipedia.org/wiki/%D0%A0%D0%BE%D0%B7%D1%83%D0%BC%D0%BD%D0%B0_%D0%B5%D0%BD%D0%B5%D1%80%D0%B3%D0%BE%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0.

[7] «International Electrotechnical Commission,» 23 November 2018. [Онлайновий]. Available: https://en.wikipedia.org/wiki/International_Electrotechnical_Commission.

[8] «The IEC61499. The new standart in automation,» [Онлайновий]. Available: http://www.iec61499.de/. [Дата звернення: 2018].

[9] «IEC-61850,» 17 March 2018. [Онлайновий]. Available: https://en.wikipedia.org/wiki/IEC_61850.

[10] «Communication networks and systems for power utility automation - ALL PARTS,» [Онлайновий]. Available: https://webstore.iec.ch/publication/6028. [Дата звернення: 2018 12 2].

[11] «IEC 61131-3,» 10 Квітня 2018. [Онлайновий]. Available: https://uk.wikipedia.org/wiki/IEC_61131-3.

[12] L. Ferrarini та C. Veber, «Implementation approaches for the execution model of IEC 61499 applications,» June 2004. [Онлайновий]. Available: https://ieeexplore.ieee.org/document/1417418.

[13] V. V. Vyatkin та V. D. Dubinin, «Execution Model of IEC61499 Function Block based on Sequential Hypothesis,» 2006. [Онлайновий]. Available: https://pdfs.semanticscholar.org/1fcf/ce8ea96ef07f063e443d2d3b9a5dfefe8e32.pdf.

[14] В. Дубынин та В. Вяткий, «Модели последовательного выполнения функциональных блоков iec 61499 на основе динамически изменяемых приоритетов,» *Известия высших учебных заведений. Поволжский регион. Технические науки,* pp. 13-22, 2007.

[15] В. Н. Дубинин, «Формализация моделей выполнения блоков IEC-61499,» *Известия высших учебных заведений. Поволжский регион. Технические науки,* pp. 12-23, 2011.

[16] M. Zillgith, «Open source libraries for IEC 61850 and IEC 60870-5-104,» [Онлайновий]. Available: https://libiec61850.com/libiec61850/. [Дата звернення: 2018 12 5].

[17] *НПАОП 0.00-6.03-93 «Порядок опрацювання та затвердження власником нормативних актів про охорону праці, що діють на підприємстві».*

[18] *НПАОП 0.00-4.12-05 «Типове положення про порядок проведення навчання і перевірки знань з питань охорони праці».*

[19] *НАПБ Б.02.005-2003 «Типове положення про інструктажі, спеціальне навчання та перевірку знань з питань пожежної безпеки на підприємствах, в установах та організаціях України».*

[20] *ДСН 3.3.6.042-99 «Санітарні норми мікроклімату виробничих приміщень».*

[21] *ДСанПіН 3.3.2.007-98 «Правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин».*

[22] *НПАОП 0.00.-1.28-10 «Правил охорони праці під час експлуатації електронно-обчислювальних машин».*

[23] *ДСН 3.3.6.042-99 «Санітарні норми мікроклімату виробничих приміщень».*

[24] *ДСанПіН 2.2.7.029 «Гігієнічні вимоги щодо поводження з промисловими відходами та визначення їх класу небезпеки для здоров'я населення»..*

[25] P. Samal та G. Shaji, «What is the difference between a MicroGrids and a SmartGrids?,» www.quora.com, [Онлайновий]. Available: https://www.quora.com/What-is-the-difference-between-smart-grid-and-microgrid. [Дата звернення: 1 12 2018].

[26] К. О. Горелік Т.Г., «Цифровая подстанция. Подходы к реализации,» *Научно-техническая фирма "Энергопрогресс" (Москва) ,* pp. 15-17, 2013.

[27] Д. Василевский, «Цифровая подстанция: где здесь РЗА?,» Цифровая подстанция, [Онлайновий]. Available: http://digitalsubstation.com/blog/2017/07/24/tsifrovaya-podstantsiya-gde-zdes-rza/. [Дата звернення: 2 12 2018].

[28] А. Губанов, «Как примирить релейную защиту и Smart Grid,» 2011 июля 17. [Онлайновий]. Available: http://rza.org.ua/news/read/Kak-primirit-releynuyu-zashchitu-i-Smart-Grid_1685.html.

[29] I. E. Commission, «IEC-61850-7-2,» 24 August 2010. [Онлайновий]. Available: https://webstore.iec.ch/publication/6015.

[30] *НАПБ Б.03.002-2007 «Норми визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпекою».*

[31] *102. Методичні вказівки до виконання та захисту магістерської роботи за спеціальностями 122 "Комп'ютерні науки та інформаційні технології" (8.05010101 "Інформаційні управляючі системи та технології (за галузями)", 8.05010102 "ІТП"), 123 "Комп. Інженерія".*

[32] В. М. Зинин, А. М. Подлесный та В. Г. Карантаев, «ЦИФРОВАЯ ПОДСТАНЦИЯ - ОБЪЕКТ КРИТИЧЕСКОЙ ИНФРАСТУКТУРЫ,» ИнСат, [Онлайновий]. Available: https://insat.ru/articles/?id=51664. [Дата звернення: 1 12 2018].