Хмельницький національний університет
Факультет інформаційних технологій
Кафедра комп'ютерної інженерії та інформаційних систем

# КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Кіберфізична система для захисту об'єктів критичної інфраструктури (на прикладі Smart Grid – розумні електромережі)
Назва теми

КвРКІ 200108.20.04.81 ПЗ
Шифр

Галузь знань *12 «Інформаційні технології»*
Шифр, назва

Спеціальність *123 «Комп'ютерна інженерія»*
Шифр, назва

Освітня програма *«Комп'ютерна інженерія та програмування»*
Назва

Виконав: студент IV курсу, група КІ2-21-4 _____ Віктор ЗЕМСЬКИЙ
Підпис Ініціали, прізвище

Керівник _____ Єлизавета ГНАТЧУК
Підпис, дата Ініціали, прізвище

Нормоконтролер _____ Тетяна КИСІЛЬ
Підпис, дата Ініціали, прізвище

До захисту допускаю:
зав. кафедри комп'ютерної інженерії та інформаційних систем _____ Ольга ПАВЛОВА
Підпис Ініціали, прізвище

«16» червня 2025 р.

Хмельницький 2025

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Комп'ютерної інженерії та інформаційних систем

Освітній рівень бакалавр

Галузь знань 12 Інформаційні технології

Спеціальність 123 Комп'ютерна інженерія

Освітня програма «Комп'ютерна інженерія та програмування»

ЗАТВЕРДЖУЮ

Зав. кафедри Ольга ПАВЛОВА

" 10 " 01 2025 р.

**ЗАВДАННЯ**
**НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА**

Віктору ЗЕМСЬКОМУ

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Кіберфізична система для захисту об'єктів критичної інфраструктури (на прикладі Smart Grid – розумні електромережі)

Керівник проекту (роботи) Єлизавета ГНАТЧУК, д.т.н., професор

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 07.02.2025 р. № 23

2. Строк подання студентом проекту (роботи) на кафедру 01.06.2025 р.

3. Вихідні дані до проекту (роботи) Завдання на кваліфікаційну роботу

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)

Огляд ризиків та загроз для розумних електромереж, як об'єктів критичної інфраструктури

Проєктування кіберфізичної системи Smart Grid

Програмно-апаратна реалізація кіберфізичної системи для захисту обєктів критичної інфраструктури

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

Багаторівнева архітектура захисту Smart Grid

Архітектура кіберфізичної системи Smart Grid

Результати роботи кіберфізичної системи

6. Консультанти розділів дипломного проекту (роботи)

| Розділ | Прізвище, ініціали та посада консультанта | Підпис, дата | |
|---|---|---|---|
| | | завдання видав | завдання прийняв |
| Нормоконтроль | Тетяна КИСІЛЬ, доцент кафедри КІІС | | |
| Антиплагіат | Андрій НІЧЕПОРУК, доцент кафедри КІІС | | |

7. Дата видачі завдання «_10_»_____01_____2025 р.

## КАЛЕНДАРНИЙ ПЛАН

| №з/п | Назва етапів (розділів) дипломного проекту (роботи) | Термін виконання етапів проекту (роботи) | Примітка |
|---|---|---|---|
| 1 | Вибір напряму дослідження та узгодження тематики кваліфікаційної роботи з керівником | 10.01.2025 | виконано |
| 2 | Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження | 01.02.2025 | виконано |
| 3 | Робота над розділом 1 – дослідження предметної області та постановка задачі | 01.03.2025 | виконано |
| 4 | Робота над розділом 2 – вибір компонентів для проєктування кіберфізичної системи захисту об'єктів критичної інфраструктури | 01.04.2025 | виконано |
| 5 | Робота над розділом 3 – проєктування кіберфізичної системи захисту об'єктів критичної інфраструктури | 29.04.2025 | виконано |
| 6 | Оформлення пояснювальної записки згідно вимог | 25.05.2025 | виконано |
| 7 | Попередній захист ВКР | 26.05.2025 | виконано |
| 8 | Захист ВКР на засіданні ЕК | Червень 2025 року | |

Студент _____ Віктор ЗЕМСЬКИЙ
Підпис Ініціали, прізвище

Керівник роботи _____ Єлизавета ГНАТЧУК
Підпис Ініціали, прізвище

| № рядка | формат | Позначення | Найменування | Кіл. листів | № екз | Примітка |
|---|---|---|---|---|---|---|
| | | | Текстові документи | | | |
| 1 | | КвРКІ 200108.20.04.81 ПЗ | Пояснювальна записка | 60 | | |
| | | | | | | |
| | | | Графічні матеріали | | | |
| 2 | | КвРКІ 200108.20.04.81 Е8 | Багаторівнева архітектура захисту Smart Grid | 1 | | |
| | | | | | | |
| 3 | | КвРКІ 200108.20.04.81 Е8 | Архітектура кіберфізичної системи Smart Grid | 1 | | |
| | | | | | | |
| 4 | | КвРКІ 200108.20.04.81 Е8 | Результати роботи кіберфізичної системи | 1 | | |

КвРКІ 200108.20.04.81 ВП

| Зм | Арк | № докум | Підпис | Дата |
|---|---|---|---|---|
| Розробив | | Земський | | 16.06.25 |
| Перевір. | | Гнатчук | | |
| Н. контр. | | Кисіль | | 16.06.25 |
| Затв. | | Павлова | | 16.06.25 |

Відомість проекту

| Літера | Аркуш | Аркушів |
|---|---|---|
| У | 1 | 1 |

ХНУ, КІ2-21-4

# АНОТАЦІЯ

Тема кваліфікаційної роботи: «Кіберфізична система для захисту об'єктів критичної інфраструктури (на прикладі Smart Grid – розумні електромережі)».

Автор роботи: Віктор ЗЕМСЬКИЙ.

Керівник роботи: Єлизавета ГНАТЧУК.

Пояснювальна записка: 60 с., 8 рис., 10 табл., 3 дод., 50 джерел.

Графічна частина: 3 креслення.

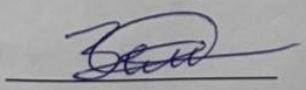
КІБЕРФІЗИЧНА СИСТЕМА, КРИТИЧНА ІНФРАСТРУКТУРА, РОЗУМНІ ЕЛЕКТРОМЕРЕЖІ, IoT, ЗАГРОЗИ, РИЗИКИ.

Метою дипломної роботи є підвищення рівня захисту об'єктів критичної інфраструктури на прикладі Smart Grid (розумних електромереж) шляхом створення кіберфізичної системи для захисту об'єктів критичної інфраструктури.

Об'єктом дослідження є кіберфізична система, призначена для моніторингу, управління та захисту об'єктів критичної інфраструктури, зокрема енергетичних систем.

Предмет дослідження – методи та засоби проектування, моделювання і реалізації кіберфізичних систем, орієнтованих на забезпечення стійкої роботи Smart Grid.

Під час проведення даного дослідження був використаний метод систематичного огляду літератури для вивчення і аналізу предметної області даного дослідження з текстових джерел інформації.



Підпис студента

30.05.2025

Дата

## ЗМІСТ

# ВСТУП

Актуальність дослідження обумовлена сучасними викликами, з якими стикається енергетичний сектор у глобальному масштабі. Зростання частоти екстремальних погодних явищ, децентралізація генерації, поява великої кількості відновлюваних джерел енергії, нестабільність споживчого навантаження, а також підвищені вимоги до безперервного електропостачання роблять традиційні підходи до управління електромережами недостатньо ефективними. Одночасно, об’єкти енергетичної інфраструктури входять до переліку критично важливих, порушення роботи яких може призвести до значних економічних втрат, соціального напруження та навіть загроз національній безпеці.

У цьому контексті розумні електромережі (Smart Grid) виступають як стратегічне рішення, здатне забезпечити адаптивне, безпечне й надійне управління енергосистемами нового покоління. Однак ефективність та живучість таких мереж прямо залежить від рівня інтеграції кіберфізичних систем, технологій, що поєднують фізичну інфраструктуру з інтелектуальними цифровими платформами.

Саме тому дослідження, спрямоване на створення й моделювання кіберфізичної системи захисту для Smart Grid, є надзвичайно актуальним. Воно відповідає вимогам сучасної енергетичної трансформації, сприяє розвитку національної енергетичної безпеки та закладає основу для сталого функціонування критичної інфраструктури в умовах цифрової епохи.

Кіберфізичні системи є одним з ключових напрямів розвитку сучасних технологій управління складними технічними об’єктами. Вони являють собою інтеграцію фізичних пристроїв, сенсорів, виконавчих механізмів та програмно-інформаційних платформ, що взаємодіють у реальному часі через захищені комунікаційні канали. У сфері енергетики такі системи мають особливе значення, адже забезпечують безпеку, гнучкість і автономність управління розподіленими енергетичними ресурсами. З огляду на глобальні виклики, такі як зростання енергоспоживання, децентралізацію генерації, вплив кліматичних змін,

необхідність у впровадженні інтелектуальних рішень у критичну інфраструктуру зростає щороку.

Розумні електромережі (Smart Grid) є яскравим прикладом застосування кіберфізичних систем у сучасній енергетиці. Вони поєднують традиційні електромережі з цифровими технологіями, що дозволяє не лише передавати енергію, а й ефективно управляти нею. Smart Grid здатна реагувати на зміни в реальному часі, інтегрувати відновлювані джерела енергії, балансувати навантаження, знижувати втрати та забезпечувати високий рівень надійності. Однак реалізація таких систем неможлива без комплексного підходу до їх архітектури, включаючи апаратні рішення, програмне забезпечення, комунікаційні протоколи та захисні механізми.

Об’єктом дослідження є кіберфізична система, призначена для моніторингу, управління та захисту об’єктів критичної інфраструктури, зокрема енергетичних систем.

Предмет дослідження – методи та засоби проектування, моделювання і реалізації кіберфізичних систем, орієнтованих на забезпечення стійкої роботи Smart Grid.

# 1 ОГЛЯД РИЗИКІВ ТА ЗАГРОЗ ДЛЯ РОЗУМНИХ ЕЛЕКТРОМЕРЕЖ, ЯК ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

## 1.1 Аналіз існуючих загроз для Smart Grid

З розвитком інтелектуальних енергетичних інфраструктур і ускладненням мережевих систем, «розумні» енергомережі (smart grids) активно досліджуються через їхній потенціал у зміцненні та захисті енергетичної інфраструктури. Різні дослідження розглядали питання механізмів виявлення загроз і реагування на них у контексті побудови кібербезпекової архітектури.

Смарт-мережі знаходяться у центрі численних досліджень, особливо у частині виявлення кіберзагроз і вразливостей [1]. Вони особливо вразливі до кібератак. Близько 40% найбільш серйозних атак за останні роки були спрямовані на енергетичні компанії. Наприклад, в Іспанії національне оцінювання вразливості виявило серйозні загрози типу відмови в обслуговуванні (DoS) та витоку даних, що становлять високий ризик для смарт-мережевих операцій.

Зростання взаємопов'язаності енергетичних систем розширює площину атак, зокрема за рахунок впровадження IoT-пристроїв і мережевих комунікацій, що робить енергомережі більш вразливими до зовнішніх загроз. Крім того, значна частка децентралізованих відновлюваних джерел енергії створює нові виклики безпеки, особливо в частині забезпечення захищеності комунікаційних протоколів для керування такими джерелами [2].

У напрямку підвищення кібербезпеки старт-мереж вже досягнуто певного прогресу у розробці стандартів та фреймворків для забезпечення безпеки комунікаційних систем смарт-мереж. Основні домени безпеки конфіденційність, цілісність, доступність та захист приватності даних розглянуто у рамках комплексного фреймворку, розробленого NIST на основі вибраних стандартів для оцінки рівня зрілості системи. Це уніфікована модель для оцінювання рівня безпеки, яка широко застосовується у світі [3].

Інші дослідницькі роботи також вивчали архітектури безпеки, побудовані за

рівневим принципом. Наприклад:

- рівень керування та передачі даних для забезпечення захищеної комунікації;
- криптографічний сервісний рівень для реалізація шифрування;
- сервіс керування безпекою, системи виявлення та запобігання вторгнень (IDS/IPS);
- рівень абстракції доступу до мережі забезпечує контроль доступу.

Системи виявлення загроз (IDS/ADS) збирають дані з мережевого трафіку та забезпечують моніторинг у реальному часі, а також попередження про потенційні загрози. Системи ADS (Anomaly Detection System) орієнтовані на виявлення аномалій. В одному з досліджень була представлена нова система IDS, яка використовує штучний інтелект для виявлення як відомих, так і нових загроз, застосовуючи методи машинного навчання для ідентифікації аномального мережевого трафіку. Такі системи вже довели свою ефективність у підвищенні рівня безпеки енергомереж та ідентифікації підозрілої активності.

Методи машинного навчання також використовуються для виявлення аномалій у багатьох потоках даних від сенсорів або лічильників на рівні збору даних (sensing tier), де надходять тисячі точок даних щохвилини. Це забезпечує нижчий рівень хибнопозитивних спрацьовувань і підвищену точність виявлення [12].

Сукупний ефект від тисяч і тисяч невеликих акумуляторних систем (наприклад, побутових накопичувачів енергії) також підвищує стійкість енергомережі до кібератак завдяки її децентралізації та гнучкості.

STRIDE – це загальноприйнята модель класифікації загроз, розроблена компанією Microsoft. Вона дозволяє ідентифікувати основні вектори атак у складних інформаційних і кіберфізичних системах (таблиця 1.1).

В контексті Smart Grid, інтелектуальної енергомережі, яка поєднує цифрові технології, датчики, розподілені обчислення та фізичні компоненти, STRIDE допомагає системно проаналізувати можливі загрози.

Таблиця 1.1 – Аналіз загроз за моделлю STRIDE

| Категорія загрози | Опис | Приклади для Smart Grid |
|---|---|---|
| Spoofing | Підміна ідентичності | Підміна користувача або контролера |
| Tampering | Несанкціонована модифікація даних | Зміна даних лічильника |
| Repudiation | Відмова від дій | Заперечення споживання електроенергії |
| Information Disclosure | Розголошення інформації | Витік даних споживачів |
| Denial of Service | Відмова в обслуговуванні | DoS-атака на SCADA |
| Elevation of Privilege | Підвищення привілеїв | Отримання прав адміністратора |

Spoofing identity (підміна ідентичності) – це коли зловмисник видає себе за інший вузол або пристрій системи. Уразливими компонентами системи є смарт-лічильники, RTU, SCADA, шлюзи зв’язку. Прикладами є імітація легітимного пристрою Smart Meter для надсилання підроблених даних.

При підміні пристрою керування під час аутентифікації можливими наслідками можуть бути доступ до конфіденційної інформації; некоректне управління електронавантаженням; порушення стабільності енергосистеми.

Засобами захисту можуть бути сертифікати цифрової автентифікації; використання TLS або IPsec та механізми двофакторної аутентифікації пристроїв.

Tampering with data (модифікація даних) – це несанкціоноване змінення даних у процесі їх передачі або зберігання. Уразливими компонентами є канали телеметрії, бази даних, лічильники. Прикладами є підміна команд керування (наприклад, «вимкнути підстанцію»); зміна даних споживання електроенергії з метою шахрайства.

Можливими наслідками є порушення балансу генерації/споживання; відмова енергосистеми; фінансові втрати.

Засобами захисту можуть бути цифрові підписи; контроль цілісності (хешування) та шифрування даних у сховищах і при передачі.

Repudiation (заперечення дій) – це неможливість довести, що дія дійсно була здійснена певним користувачем або пристроєм**.** Уразливими компонентами в такому випадку можуть бути журнали подій, облік операцій з обладнанням.

Прикладами можуть бути відмова оператора або лічильника від виконаної команди або відсутність логів подій критичних команд.

До можливих наслідків можна віднести **у**складнення розслідування інцидентів, втрата довіри до системи та неможливість юридичного доказу порушення.

Засоби захисту це протоколи з авторизацією та легуванням, незаперечність підписів та тривалий захист журналів.

Information disclosure (розголошення інформації) – це витік конфіденційної інформації або стану енергомережі. Уразливі компоненти в даному випадку, це канали телеметрії, дані SCADA, споживчі дані.

Прикладами є перехоплення трафіку між Smart Meter і сервером або аналіз даних про споживання для визначення поведінки користувачів (профайлінг).

До можливих наслідків слід віднести **з**агрозу приватності користувачів, потенційну допомогу в плануванні фізичних атак та втрата конкурентної інформації.

Засоби захисту, які можуть використовуватись, це використання VPN/SSL, контроль доступу до даних (RBAC) та шифрування даних у всіх точках.

Denial of Service (відмова в обслуговуванні) – навмисне перевантаження або блокування системи для унеможливлення її нормального функціонування.

Уразливі компоненти при цьому це сервери диспетчеризації, канали зв’язку, контролери підстанцій. Прикладами є DoS/DDoS-атаки на шлюзи або сервери SCADA або флудинг запитами з ботнету IoT-пристроїв.

Можливими наслідками можуть бути неможливість вчасно реагувати на критичні зміни в мережі; відключення цілих районів електромережі; загроза життю та безпеці людей.

Засобами захисту є резервні канали зв’язку, IDS/IPS-системи та рофілювання трафіку й rate limiting.

Elevation of privilege (підвищення привілеїв) при цьому зловмисник отримує доступ до функцій або даних, які йому не призначені.

Уразливі компоненти при цьому, це сервери, вразливе ПЗ, операційні системи контролерів.

Прикладами є **е**ксплуатація вразливості в ПЗ для доступу до адміністративного інтерфейсу та підміна прошивки пристрою.

Можливими наслідками можуть бути повний контроль над об’єктом Smart Grid; можливість саботажу або диверсії; масштабні енергетичні відключення.

Засоби захисту при цьому це **ж**орсткий контроль прав доступу; регулярне оновлення програмного забезпечення та аудит прав користувачів.

Аналіз за моделлю STRIDE дозволяє системно охопити всі основні вектори атак на кіберфізичну систему Smart Grid. Для забезпечення її надійності та безпеки необхідно застосовувати комплексний підхід, який включає криптографічний захист, моніторинг, сегментацію мережі, а також постійне оновлення політик безпеки. Детальний аналіз загроз за моделлю STRIDE дає змогу виявити потенційні вразливості на всіх етапах функціонування Smart Grid від збору даних до їх обробки й передачі. Особливу увагу слід приділяти захисту кінцевих пристроїв та шлюзів, які часто є найвразливішими елементами системи. Важливим також є впровадження механізмів аутентифікації та контролю доступу для запобігання несанкціонованому втручанню. Безперервне навчання персоналу та моделювання сценаріїв кіберінцидентів дозволяє підтримувати високий рівень готовності до можливих атак.

Окрім кіберзагроз, розумні електромережі (Smart Grids) як об'єкти критичної інфраструктури, піддаються також іншим видам загроз, які можуть

вплинути на їхню стабільність, ефективність та надійність.

До основних категорій некібернетичних загроз відносяться фізичні загрози, природні загрози, технічні загрози, економічні та соціальні загрози, інфраструктурні та логістичні загрози

До фізичних загроз відносяться:

1. Вандалізм і саботаж:

– умисне пошкодження трансформаторів, підстанцій, ліній електропередач;

– напади на інфраструктурні об’єкти, зокрема в умовах політичної нестабільності або терористичних актів.

2. Несанкціонований фізичний доступ:

– злом приміщень, де розташоване обладнання (SCADA, сервери, контролери);

– ризик викрадення або підміни компонентів системи.

Природні загрози можуть бути як кліматичні так і геофізичні. Наприклад, екстремальні погодні умови, до яких можна віднести бурі, повені, урагани можуть пошкодити лінії електропередач, трансформатори та інше обладнання.

Геофізичні події – це землетруси, зсуви, лісові пожежі, руйнування або знищення фізичних об'єктів мережі.

Геомагнітні бурі, тобто сонячні спалахи можуть викликати індукційні струми в довгих ЛЕП і призвести до виходу з ладу трансформаторів.

До технічних загроз (помилки, збої, відмови) можна віднести наступні:

1. Відмова обладнання через знос обладнання, старіння мереж, перегрів трансформаторів, короткі замикання.

2. Людський фактор, тобто помилки персоналу при конфігурації, обслуговуванні або ремонті обладнання.

3. Неправильне програмування логіки керування.

4. Взаємозалежності систем, тобто вихід з ладу однієї частини системи (наприклад, зв’язку) може порушити роботу інших компонентів.

Економічні та соціальні загрози, до яких відносяться нестабільність цін на енергоресурси, тобто різкі коливання цін на енергію (електроенергія, газ) впливають на економічну модель роботи Smart Grid, надмірне навантаження через піковий попит, перевантаження мережі, ризик аварійного відключення або віялових відключень, законодавчі та нормативні обмеження, тобто недосконаліть нормативної бази, зокрема щодо інтеграції відновлюваних джерел, стандартів обміну даними, зберігання енергії тощо.

До інфраструктурних та логістичних загроз відносяться залежність від інших інфраструктур, порушення у роботі зв'язку, водопостачання чи транспортної системи може вплинути на управління мережею, проблеми з обслуговуванням та ремонтом, дефіцит запчастин, нестача персоналу, довготривалий час реагування на аварії.

Отже, для ефективного функціонування Smart Grid необхідно враховувати не лише кіберзахист, але й фізичні, природні, технічні, економічні та соціальні ризики. Лише комплексний підхід до безпеки — технічний, організаційний, нормативний та експлуатаційний — дозволяє забезпечити стабільність критичної інфраструктури.

## 1.2 Аналіз ризиків системи Smart Grid

Система Smart Grid, як приклад сучасної кіберфізичної інфраструктури, поєднує в собі цифрові обчислення, телекомунікації та фізичне управління енергетичними потоками. Її складність і критичне значення зумовлюють потребу в ретельному аналізі ризиків. Оцінка ризиків дозволяє виявити найвразливіші місця системи та прийняти превентивні заходи.

Для оцінки ризиків в Smart Grid застосовують традиційну методику (таблиця 1.2).

$$\text{Ризик} = \text{Імовірність} \times \text{Вплив}$$

Імовірність виникнення події визначається на основі історичних даних, сценаріїв моделювання, поточної безпеки системи.

Вплив**,** тобто критичність наслідків, оцінюється за впливом на фізичні об’єкти, безперервність енергопостачання, безпеку громадян тощо.

Таблиця 1.2 –Матриця ризиків

| Загроза | Ймовірність | Вплив | Рівень ризику |
|---|---|---|---|
| DoS-атака на канали зв'язку SCADA | Висока | Високий | Критичний |
| Фізичне пошкодження трансформатора | Середня | Високий | Високий |
| Підміна розумного лічильника | Середня | Середній | Середній |
| Витік персональних даних | Низька | Високий | Середній |
| Відмова обладнання | Висока | Середній | Високий |
| Відмова від централізованого управління | Середня | Високий | Високий |
| Геомагнітна буря | Низька | Високий | Середній |
| Атака на IoT-пристрої | Висока | Середній | Високий |

Централізовані елементи управління, такі як SCADA-системи та диспетчерські центри, залишаються найбільш привабливими цілями для зловмисників через їхній критичний вплив на функціонування всієї інфраструктури Smart Grid. Компрометація цих систем може призвести до масштабних відключень, втрати контролю над енергетичними потоками, або навіть до аварій техногенного характеру. Ще більш вразливими є масові віддалені пристрої, зокрема «розумні лічильники» (Smart Meters), які встановлюються у споживачів. Через велику кількість таких пристроїв і їхнє розміщення в незахищених фізичних умовах, вони можуть стати зручною точкою входу для атак.

Критичні інциденти нерідко виникають внаслідок комбінованих загроз, наприклад, коли фізичне втручання у пристрій супроводжується атакою на програмне забезпечення. Такі гібридні атаки є особливо небезпечними, оскільки здатні обійти стандартні механізми захисту. До того ж, навіть загрози з низькою ймовірністю, але потенційно катастрофічним впливом, не можна ігнорувати. Саме тому при побудові системи кіберзахисту важливо враховувати не лише найвірогідніші, а й найнебезпечніші сценарії.

Важливу роль відіграє впровадження політик управління доступом, обмеження привілеїв, та багатофакторна аутентифікація. Потрібно регулярно оновлювати програмне забезпечення, усувати відомі вразливості, а також проводити тестування на проникнення. Сегментація мережі допомагає локалізувати потенційні інциденти та запобігати їх поширенню на всю систему. Крім того, навчання персоналу та відпрацювання сценаріїв реагування на інциденти має стати регулярною практикою.

В умовах стрімкої цифровізації енергетичного сектору Smart Grid системи повинні бути не лише ефективними, але й стійкими до складних і багатоетапних загроз.

Впровадження стандартизованих підходів, таких як NIST або IEC 62443, може слугувати базою для побудови безпечної архітектури. Потрібно також враховувати ризики ланцюгів постачання, особливо коли мова йде про імпортоване обладнання або програмне забезпечення.

Нарешті, взаємодія між операторами, урядовими структурами та кібербезпековими аналітиками є ключовою для своєчасного виявлення і нейтралізації нових типів загроз.

## 1.3 Особливості розумних електромереж Smart Grid

Розумні електромережі (Smart Grid) – це інтелектуальна система розподілу енергії, яка поєднує інформаційні технології з електричними мережами, щоб

зробити процес управління електричною енергією більш ефективним, надійним та адаптивним до змінних умов. Розумні електромережі використовують сучасні технології, щоб оптимізувати споживання енергії, знизити витрати та підвищити надійність енергопостачання (рисунок 1.1).


Рисунок 1.1 – Особливості розумних електромереж

Розглянемо більш детальніше особливості розумних електромереж:

1. Двосторонній обмін інформацією. У традиційних мережах електроенергія передається лише в один бік від генератора до споживача. У розумних мережах дані про споживання енергії та стан мережі передаються в реальному часі не тільки від постачальника до споживача, але й у зворотному напрямку. Це дозволяє, наприклад, користувачам з генераторами на відновлюваних джерелах (сонячними панелями, вітровими турбінами) передавати зайву енергію назад у мережу.

2. Автоматизація та моніторинг. Розумні електромережі мають автоматичні

системи моніторингу та управління, які дозволяють виявляти проблеми (наприклад, пошкодження в мережі) і швидко реагувати на них. Вони можуть автоматично налаштовуватися для оптимізації розподілу енергії, забезпечуючи більш ефективне використання ресурсів.

3. Інтеграція відновлюваних джерел енергії. Однією з ключових особливостей є здатність інтегрувати відновлювальні джерела енергії (сонячні панелі, вітрові турбіни, гідроелектростанції) в загальну енергомережу. Це дозволяє зменшити залежність від викопних джерел енергії та знизити рівень викидів вуглецю.

4. Інтелектуальні лічильники та моніторинг споживання. У розумних мережах використовуються розумні лічильники, які дозволяють споживачам стежити за споживанням енергії в реальному часі. Це не тільки дає змогу споживачам краще контролювати свої витрати, але й дозволяє енергетичним компаніям більш ефективно управляти навантаженням на мережу.

5. Динамічне управління попитом. Розумні мережі можуть впроваджувати динамічні ціни на енергію, що змінюються в залежності від попиту та пропозиції. Це дозволяє оптимізувати споживання енергії, мотивуючи користувачів споживати енергію в часи низького попиту, що допомагає знизити навантаження на мережу та заощаджувати ресурси.

6. Захист від кіберзагроз. Оскільки розумні мережі включають в себе численні пристрої та комунікаційні канали, питання кібербезпеки є надзвичайно важливим. Розумні електромережі потребують високого рівня захисту від хакерських атак та інших кіберзагроз, щоб забезпечити стабільність і безпеку енергетичної інфраструктури.

7. Енергоефективність та зниження витрат. Завдяки автоматизованому управлінню та оптимізації розподілу енергії, розумні мережі сприяють енергоефективності та зниженню витрат на електричну енергію для споживачів та енергетичних компаній.

8. Мобільні додатки та взаємодія з користувачами. Споживачі можуть мати

доступ до своїх даних про споживання енергії через мобільні додатки або веб-платформи, що дозволяє їм здійснювати контроль за витратами, налаштовувати режим роботи пристроїв (наприклад, кондиціонерів, обігрівачів) і брати участь у програмах «попиту за ціною» (наприклад, відкласти споживання електрики на час низького попиту).

9. Зменшення викидів парникових газів. Оскільки розумні мережі сприяють інтеграції відновлюваних джерел енергії і підвищують ефективність енергоспоживання, вони можуть значно знизити викиди парникових газів**.** Це важливий аспект для боротьби зі змінами клімату.

10. Гнучкість та адаптивність. Розумні мережі можуть швидко адаптуватися до змін у попиті та пропозиції енергії, що дозволяє уникати перевантажень мережі та запобігати аваріям. Вони можуть інтегрувати нові технології, такі як накопичувачі енергії, і працювати з ними для збереження енергії на випадок пікових навантажень.

11. Взаємодія між споживачами та енергетичними компаніями. Розумні мережі дозволяють споживачам брати активну участь у процесі управління енергоспоживанням, що може допомогти енергетичним компаніям краще прогнозувати попит і пропозицію. Споживачі можуть, наприклад, отримувати бонуси за участь у програмах з управління попитом.

Розумні електромережі – це не просто технологічний крок вперед, а й важливий етап у розвитку сучасних енергетичних систем, що дозволяє підвищити їх ефективність, знижувати витрати, оптимізувати використання відновлювальних джерел енергії та зменшувати вплив на навколишнє середовище.

Традиційні електромережі будувалися за принципом централізованого постачання електроенергії від виробника до споживача. Вони не передбачають активної участі користувача, а їх функціонування базується на статичних моделях споживання. Дані про витрати електроенергії збираються вручну або з великою затримкою, що ускладнює своєчасне реагування на проблеми. У разі виникнення аварій такі системи не здатні швидко локалізувати несправність, тому потрібне

втручання персоналу.

На противагу цьому, розумні електромережі забезпечують двосторонню комунікацію між усіма елементами мережі. Завдяки цифровим технологіям дані збираються й аналізуються в реальному часі, що дає змогу оперативно приймати рішення. Smart Grid автоматично виявляє несправності, відокремлює пошкоджені ділянки та мінімізує збої. Крім того, вони інтегрують поновлювані джерела енергії, такі як сонячні та вітрові установки, створюючи гнучку децентралізовану інфраструктуру.

В таблиці 1.3 наведені основні відмінності традиційних та розумних електромереж.

Таблиця 1.3 – Основні відмінності між традиційними електромережами та розумними електромережами

| Критерій | Традиційна електромережа | Розумна електромережа (Smart Grid) |
|---|---|---|
| Моніторинг споживання | Ручний або періодичний (раз на місяць) | Автоматичний, у реальному часі |
| Збір даних | Мінімальний, затримка в часі | Безперервний, з точним аналізом даних |
| Кібербезпека | Мінімальний захист | Впроваджені сучасні засоби криптографії та контролю доступу |
| Передача енергії | Односпрямована від виробника до споживача | Двостороння, можливий зворотній потік від споживача (наприклад, від сонячних панелей) |
| Реакція на аварії | Повільна, часто потребує ручного втручання | Автоматичне виявлення та ізоляція проблемних ділянок |
| Участь споживача | Пасивна роль | Активна участь (моніторинг, контроль споживання, участь у ринку) |

Кінець таблиці 1.3

| Критерій | Традиційна електромережа | Розумна електромережа (Smart Grid) |
|---|---|---|
| Ефективність | Низька через втрати, перевантаження | Вища завдяки оптимізації навантаження та автоматизації |
| Автоматизація | Низький рівень | Високий рівень автоматичного управління |
| Прогнозування | Відсутнє або базове | Вдосконалені алгоритми прогнозування на основі великих даних |

Особливу роль у Smart Grid відіграють розумні лічильники, які дозволяють споживачам контролювати власне енергоспоживання, зменшувати витрати й підвищувати енергоефективність.

У традиційних системах такий контроль відсутній. Smart Grid також використовує механізми кібербезпеки: шифрування, автентифікацію та контроль доступу, що знижує ризики кіберзагроз.

Автоматизація управління енергетичними потоками дозволяє значно знизити втрати енергії, оптимізувати навантаження та забезпечити баланс між генерацією й споживанням. Це особливо важливо для інтеграції динамічних джерел енергії, таких як ВДЕ. Крім того, Smart Grid здатна прогнозувати пікові навантаження, попереджувати перевантаження та адаптувати роботу системи до поточних умов. Завдяки цьому забезпечується висока надійність, гнучкість і масштабованість електропостачання.

Інтернет речей (IoT) є ключовим компонентом інфраструктури розумних електромереж. Його головна функція – забезпечення взаємодії між фізичними пристроями через мережеве середовище, що дозволяє збирати, передавати та аналізувати дані в режимі реального часу. У контексті Smart Grid це означає, що кожен елемент системи? від трансформатора до розетки у споживача, може бути

«розумним» та підключеним до мережі.

Мільйони сенсорів і пристроїв IoT, температурні датчики, лічильники, контролери потужності, зарядні станції для електромобілів, домашні енергосистеми тощо, створюють цифровий «нервовий центр» електромережі. Це дозволяє Smart Grid автоматично регулювати навантаження, виявляти несправності, прогнозувати пікові навантаження та ефективно керувати розподілом енергії (рисунок 1.2).


Рисунок 1.2 – Інтернет речей у розумних електромережах

Особливу роль відіграє взаємодія Smart Grid з електромобілями (EV), які через IoT можуть не лише заряджатися, але й повертати енергію назад у мережу (технологія Vehicle-to-Grid, V2G). Це створює гнучку систему накопичення енергії на транспорті. Інтеграція IoT дозволяє створити децентралізовану,

адаптивну та самонавчальну енергосистему. Саме завдяки IoT, Smart Grid перетворюється зі звичайної інфраструктури в інтелектуальну енергетичну екосистему.

## 1.4 Висновки до першого розділу

У межах розділу 1 проведено аналіз загроз та ризиків, які виникають в об’єктах критичної інфраструктури, зокрема в Smart Grid. Сучасні розумні електромережі є відповіддю на глобальні виклики, пов’язані з підвищеним енергоспоживанням, нестабільністю джерел живлення та необхідністю екологічної трансформації. На відміну від традиційних систем, Smart Grid базується на цифрових технологіях, автоматизації, двосторонній комунікації та активній участі споживача. В основі цієї концепції лежить інтеграція відновлюваних джерел енергії, інтелектуальне управління та гнучкість у реагуванні на зміни попиту.

Проведений огляд підтвердив, що Smart Grid не є лише модернізацією старої мережі, а являє собою нову енергетичну екосистему. Основні її компоненти – це Smart Meters, SCADA-системи, IoT-пристрої, автоматизовані підстанції та розподілені джерела енергії, що працюють синхронно для досягнення високої ефективності та надійності.

Разом з тим, зростання рівня цифровізації супроводжується появою нових ризиків і загроз. До найбільш критичних належать кібератаки на інфраструктурні вузли (SCADA, диспетчерські центри), втручання в роботу Smart Meters, або порушення в ланцюгах постачання. Комбінація фізичних і кіберзагроз може мати катастрофічні наслідки, тому важливо використовувати моделі оцінки загроз, як-от STRIDE, а також впроваджувати криптографію, моніторинг, сегментацію мереж і навчання персоналу.

# 2 ПРОЄКТУВАННЯ КІБЕРФІЗИЧНОЇ СИСТЕМИ SMART GRID

## 2.1 Аналіз вимог до кіберфізичної системи Smart Grid

Проєктування кіберфізичної системи Smart Grid – це складний процес, який об'єднує електроенергетичну інфраструктуру з цифровими технологіями для забезпечення надійного, ефективного та гнучкого управління енергетичними потоками.

Функціональні вимоги до кіберфізичної системи Smart Grid передбачають наявність механізмів для автоматизованого збору даних з елементів мережі, зокрема інформації про напругу, струм, частоту та інші параметри енергопостачання, зокрема:

1. Автоматизований збір даних про стан мережі (струм, напруга, частота).
2. Обробка та передача даних у реальному часі.
3. Виявлення аварій та реакція на них.
4. Дистанційне управління енергетичними приладами.
5. Підтримка взаємодії з розподіленими джерелами енергії.

Система повинна забезпечувати безперебійну передачу цих даних у режимі реального часу до центрів обробки, де інформація аналізується та використовується для прийняття рішень щодо управління мережею.

Однією з ключових функцій є здатність виявляти аварійні ситуації, здійснювати локалізацію порушень і виконувати коригувальні дії. Важливою складовою є підтримка двостороннього зв’язку зі споживачами та джерелами енергії, що дає змогу реалізувати дистанційне керування навантаженням та інтеграцію відновлюваних джерел енергії. Крім того, система повинна мати можливість зберігання історичних даних, що необхідно для аналізу трендів і прогнозування.

Нефункціональні вимоги визначають якісні характеристики системи (таблиця 2.1). Передусім, це висока надійність, яка означає здатність системи функціонувати без відмов упродовж тривалого часу, навіть за умови пікового

навантаження.

Таблиця 2.1 – Нефункційні вимоги

| Категорія | Вимога |
|---|---|
| Надійність | Безперебійна робота в умовах пікового навантаження |
| Масштабованість | Можливість додавання нових пристроїв без змін архітектури |
| Безпека | Шифрування даних, автентифікація, контроль доступу |
| Сумісність | Підтримка міжнародних стандартів (IEC 61850, Modbus, MQTT тощо) |
| Час відгуку | Обробка подій критичної важливості за < 100 мс |

Масштабованість системи передбачає можливість розширення її функціоналу або підключення додаткових пристроїв без необхідності значної реконструкції архітектури. Безпека є критичним аспектом і передбачає використання шифрування для захисту переданих даних, впровадження автентифікації користувачів та пристроїв, а також контроль доступу до компонентів системи. Сумісність із міжнародними стандартами, такими як IEC 61850, Modbus або MQTT, дозволяє забезпечити інтеграцію з іншими системами. Окремо варто підкреслити важливість швидкого часу відгуку: система повинна мати здатність оперативно реагувати на події, зокрема обробляти критичні ситуації з мінімальними затримками.

Smart Grid об’єднує традиційні та відновлювані джерела енергії, створюючи гнучку енергетичну екосистему. Джерела енергії включають теплові електростанції, гідроелектростанції, сонячні панелі, вітрові турбіни та біогазові установки. Серед споживачів виділяють побутових абонентів (житлові будинки),

комерційні об’єкти (магазини, офіси), промислові підприємства, а також зарядні станції електротранспорту (таблиця 2.2).

Таблиця 2.2 – Порівняння типів джерел енергії

| Джерело | Переваги | Недоліки |
|---|---|---|
| Сонце | Відновлюване, екологічне | Залежність від погоди |
| Вітер | Низькі експлуатаційні витрати | Нестабільність виробництва |
| ТЕС | Висока потужність | Викиди CO2 |
| ГЕС | Регульованість | Екологічний вплив |

Вибір протоколів комунікації є одним із ключових етапів проєктування кіберфізичної системи Smart Grid, оскільки саме через ефективну передачу інформації забезпечується координація між усіма її компонентами. У системі передбачається взаємодія численних пристроїв: датчиків, контролерів, шлюзів, серверів, операторських панелей та хмарних сервісів (рисунок 2.1). Відповідно, використовуються як локальні протоколи для комунікації на невеликі відстані, так і глобальні протоколи для передачі даних у масштабах всієї мережі.

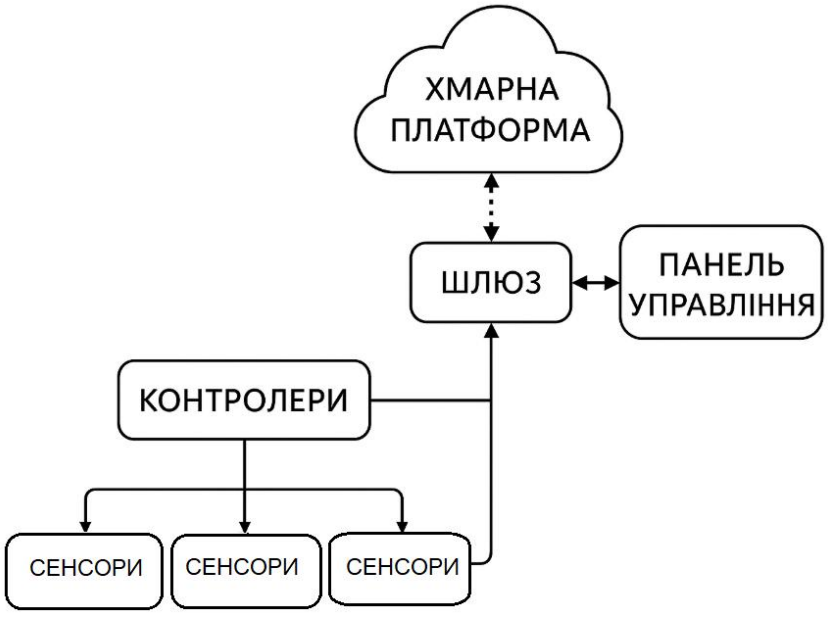



Рисунок 2.1 – Узагальнена схема комунікаційної архітектури Smart Grid

Серед локальних протоколів, особливу роль відіграє ZigBee, який є малопотужним радіопротоколом, оптимізованим для застосувань у сфері автоматизації будівель і розумних лічильників. Його перевагами є низьке енергоспоживання та проста реалізація в сітчастих мережах.

Інший поширений протокол Modbus використовується для зв'язку між ПЛК (програмованими логічними контролерами) та іншими пристроями, особливо в промислових умовах, де важлива стабільність і простота впровадження. Протокол BLE (Bluetooth Low Energy) використовується для бездротового обміну даними на короткі дистанції та є доцільним у побутовому секторі або в рамках IoT-пристроїв.

На рівні глобальної мережі використовуються протоколи, які здатні забезпечити надійний обмін великими обсягами даних. Протокол MQTT (Message Queuing Telemetry Transport) вирізняється простотою, легкістю та ефективністю роботи в середовищах із обмеженими ресурсами. Він є популярним у системах Інтернету речей та передбачає передачу повідомлень за моделлю «публікатор-підписник». LoRaWAN є відмінним вибором для передавання невеликих обсягів даних на великі відстані з мінімальним енергоспоживанням, що робить його корисним для датчиків, розташованих у віддалених районах. Технології стільникового зв'язку, такі як LTE та 5G, пропонують високу пропускну здатність і низьку затримку, що є критично важливим для задач реального часу, наприклад, в управлінні енергопостачанням під час аварій.

Протокол IEC 61850 є міжнародним стандартом, спеціально розробленим для автоматизації електричних підстанцій. Його переваги полягають у структурованості даних, підтримці високошвидкісної комунікації та забезпеченні взаємодії між пристроями різних виробників.

Вибір конкретного протоколу або їх комбінації визначається архітектурою системи, фізичними умовами розміщення обладнання, вимогами до швидкості, безпеки та надійності передачі даних. Таким чином, комунікаційна підсистема Smart Grid має бути гнучкою, масштабованою та сумісною з різноманітними

технологіями передачі інформації.

Кібербезпека є ключовим аспектом проєктування Smart Grid, оскільки порушення цілісності або доступності системи може призвести до значних економічних і соціальних наслідків.

Тобто, для кіберфізичних систем таких як розумні електромережі ключовими вимогами є технічні вимоги, функціональні вимоги та не функціональні вимоги.

До технічних вимог відносяться такі, як рівень споживання, генерація (включаючи ВДЕ), точки підключення.

До функціональних вимог відносяться автоматичне балансування навантажень, моніторинг у реальному часі, можливість роботи в мікромережах.

Нефункціональні вимоги – це кібербезпека, масштабованість та надійність.

## 2.2 Ключові функції кіберфізичної системи Smart Grid

Смарт грід – це кіберфізична система, що включає фізичні компоненти (електромережі, датчики, виконавчі пристрої) і кіберкомпоненти (системи управління, обчислювальні модулі, зв'язок).

До ключових функцій системи Smart Grid відносяться наступні:

- моніторинг в режимі реального часу;
- автоматичне повторне вмикання та ізоляція пошкоджених ділянок;
- інтеграція ВДЕ з урахуванням нестабільності виробітку;
- активне управління попитом (Demand Response);
- кібербезпека – захист протоколів, аутентифікація пристроїв, шифрування даних.

Моніторинг у режимі реального часу дозволяє системі Smart Grid безперервно відстежувати параметри електромережі, такі як напруга, струм, частота та якість енергії. Завдяки датчикам і смарт-лічильникам інформація оперативно передається до центрів управління. Це забезпечує своєчасне

виявлення порушень і аварійних ситуацій. Оператори мають змогу швидко реагувати на зміни навантаження або неполадки. Такий моніторинг дозволяє запобігти серйозним збоям, мінімізуючи час простою. Також це підвищує ефективність використання ресурсів і знижує експлуатаційні витрати. Реальний час дозволяє прогнозувати споживання енергії з високою точністю. Інформація з різних сегментів мережі об'єднується в єдину систему. Це сприяє прозорості та гнучкому керуванню інфраструктурою. Моніторинг є основою для реалізації інших інтелектуальних функцій системи.

Система Smart Grid оснащена функцією автоматичного виявлення несправностей та реакції на них. У разі короткого замикання або іншої аварії система виконує локалізацію пошкодженої ділянки. Після цього відбувається її автоматична ізоляція, що дозволяє уникнути поширення проблеми. Здорові частини мережі залишаються активними, забезпечуючи безперебійне живлення. Автоматичне повторне вмикання дозволяє перевірити, чи проблема була тимчасовою. Якщо короткочасне порушення зникло, подача енергії відновлюється без втручання оператора. Це суттєво скорочує час відновлення після інциденту. Також зменшується кількість звернень до служби підтримки. Інтелектуальні вимикачі та реле відіграють ключову роль у цьому процесі. Така функція підвищує надійність і стабільність енергосистеми.

Системи Smart Grid враховують варіативність у виробленні енергії з ВДЕ, таких як сонце та вітер. Вони інтегрують ці джерела за допомогою передбачуваного планування і адаптивного управління. Алгоритми прогнозування враховують погодні умови для оптимізації розподілу енергії. У моменти надлишку виробництва енергія може накопичуватися в акумуляторах або використовуватись для потреб споживачів. При нестачі ВДЕ вмикаються резервні джерела або зменшується споживання через механізми управління попитом. Це дозволяє збалансувати енергетичну систему навіть за умов нестабільності. Інтеграція супроводжується постійним моніторингом і адаптацією режимів роботи мережі. Завдяки цьому ВДЕ стають надійною частиною енергосистеми.

Така гнучкість зменшує залежність від викопного палива. Крім того, зменшуються викиди парникових газів і підвищується екологічна сталість.

Активне управління попитом – це система, яка дозволяє гнучко регулювати споживання електроенергії. Споживачі можуть змінювати свій режим використання енергії у відповідь на сигнали від оператора або ціни на ринку. Наприклад, у години пікового навантаження можна зменшити споживання, щоб уникнути перевантаження мережі. Учасники програми отримують фінансову компенсацію або знижки за участь у Demand Response. Це сприяє зниженню потреби у запуску резервних потужностей. Такі заходи особливо важливі при інтеграції нестабільних ВДЕ. Споживачі, обладнані смарт-лічильниками, можуть автоматично реагувати на зміни в системі. Управління здійснюється як у промисловості, так і в побутовому секторі. Це підвищує ефективність і стійкість енергосистеми. Активне управління попитом – це крок до створення «розумного» споживача енергії.

У зв’язку з цифровізацією енергетичної системи питання кібербезпеки стає надзвичайно важливим. Smart Grid потребує захисту від зовнішніх і внутрішніх кіберзагроз. Захищені комунікаційні протоколи (наприклад, IEC 61850) мінімізують ризик втручання в мережу. Аутентифікація пристроїв гарантує, що до системи підключаються лише довірені елементи. Передача даних між компонентами шифрується за допомогою сучасних криптографічних алгоритмів. Постійний моніторинг безпеки дозволяє виявляти аномальні дії або вторгнення. Всі компоненти Smart Grid проходять сертифікацію на відповідність стандартам безпеки. Регулярні оновлення програмного забезпечення захищають від відомих вразливостей. У разі загрози система може автоматично ізолювати скомпрометовану ділянку. Кібербезпека забезпечує не лише конфіденційність, а й цілісність і доступність енергосистеми.

Багаторівнева архітектура захисту є ключовим підходом до забезпечення кібербезпеки в системах Smart Grid. Вона передбачає впровадження засобів захисту на кожному функціональному рівні, від фізичного обладнання до

прикладного програмного забезпечення. Такий підхід дозволяє створити цілісну, стійку до загроз систему, яка здатна виявляти, стримувати та реагувати на кіберінциденти на всіх етапах роботи мережі.

Багаторівнева архітектура захисту передбачає реалізацію заходів безпеки на кожному функціональному рівні системи Smart Grid (рисунок 2.2):


Рисунок 2.2 – Багаторівнева архітектура захисту Smart Grid

Архітектура складається з рівня споживача, рівня передачі даних, рівня управління, хмарні та дата-центри та рівня адміністрування.

Рівень споживача включає побутових, комерційних і промислових користувачів, які взаємодіють із мережею через смарт-лічильники та інші інтелектуальні пристрої. Цей рівень є найближчим до кінцевого користувача і

тому вразливим до атак, зокрема через неконтрольований доступ до обладнання. Захист полягає у використанні сертифікованих пристроїв із вбудованими механізмами шифрування і аутентифікації. Також застосовуються брандмауери на рівні «розумного будинку» або підприємства. Потрібно забезпечити регулярне оновлення програмного забезпечення споживацьких пристроїв для усунення вразливостей. Важливим є захист персональних даних користувача та даних про споживання енергії. Користувачі мають проходити автентифікацію для доступу до систем управління споживанням. Також необхідна інформаційна безпека Wi-Fi та ZigBee-мереж, які використовуються для передачі даних. Інформування споживачів про ризики та принципи безпеки є частиною комплексного підходу.

Рівень передачі даних відповідає за комунікацію між пристроями Smart Grid, включаючи сенсори, контролери, лічильники та сервери. Тут застосовуються різні канали передачі, такі як оптоволоконні, радіоканали, PLC (Power Line Communication), мобільні мережі. Основною загрозою на цьому рівні є перехоплення або модифікація даних під час їх передачі. Для запобігання цьому впроваджуються протоколи шифрування (наприклад, TLS, IPsec). Важливою функцією є виявлення атак типу «людина посередині» (MITM). Використання VPN-тунелів та цифрових сертифікатів забезпечує довіреність каналів зв’язку. Автентифікація кінцевих пристроїв є обов’язковою умовою доступу до мережі. Також слід застосовувати сегментацію мережі для локалізації потенційних атак. Моніторинг трафіку в реальному часі дозволяє виявити аномалії. Рівень передачі даних – це критичний вузол, що з’єднує фізичну інфраструктуру з цифровою платформою управління.

На рівні управління функціонують системи диспетчерського керування, автоматизації, SCADA та інші інструменти контролю. Тут ухвалюються рішення про балансування навантаження, виявлення аварій, перемикання джерел живлення тощо. Захист цього рівня є пріоритетом, оскільки він безпосередньо впливає на роботу всієї енергосистеми. Основною загрозою є спроба зовнішнього втручання в алгоритми управління або підміна команд. Системи повинні бути

ізольованими або функціонувати в окремих віртуальних середовищах. Адміністрування доступу реалізується через багатофакторну автентифікацію та контроль прав користувачів. Журналювання дій операторів дозволяє проводити аудит безпеки. Регулярні тести на проникнення та моделювання інцидентів допомагають оцінити стійкість. Особлива увага приділяється сумісності з протоколами безпеки (наприклад, IEC 62351). Цей рівень – мозковий центр Smart Grid, який потребує найвищого рівня захисту.

Рівень адміністрування включає організаційне управління, політики безпеки, контроль доступу та реагування на інциденти. Саме тут формуються правила та процедури взаємодії всіх компонентів системи Smart Grid. Ключовим елементом є керування ідентифікацією та правами користувачів. Адміністративні заходи передбачають створення планів реагування на надзвичайні ситуації, резервного відновлення та управління ризиками. Використовуються системи SIEM (Security Information and Event Management) для централізованого моніторингу подій. Регулярні аудити безпеки та оцінки відповідності стандартам дозволяють підтримувати високий рівень захисту. Навчання персоналу з питань кібербезпеки є обов'язковим заходом. Усі зміни в системі повинні фіксуватись у відповідних логах. Адміністрування забезпечує інтеграцію технічного та людського факторів у єдину політику захисту. Цей рівень формує основу для стійкого функціонування всієї енергетичної інфраструктури.зберігаються, обробляються та аналізуються великі обсяги даних із усіх частин системи. Хмарні рішення забезпечують масштабованість, резервування та аналітику на основі ШІ. Головною небезпекою тут є несанкціонований доступ до критичних даних або їх витік. Захист передбачає використання ізольованих середовищ, багаторівневої аутентифікації та шифрування як даних у русі, так і в спокої. Хмарні провайдери мають відповідати стандартам безпеки (ISO/IEC 27001, SOC 2). Резервне копіювання даних гарантує відновлення після збоїв або атак типу ransomware. Контроль доступу базується на ролях (RBAC), щоб обмежити можливості користувачів. Важливо постійно оновлювати системи безпеки та виявлення

загроз. Дата-центри повинні бути фізично захищені та мати енергетичну незалежність. Цей рівень є цифровим ядром, де обробка даних перетворюється на рішення в реальному часі.

Передача даних між компонентами Smart Grid має бути захищена за допомогою шифрування (наприклад, AES, TLS). Впровадження віртуальних приватних мереж (VPN) дозволяє захистити канали зв’язку. Використання цифрових сертифікатів забезпечує безпечну аутентифікацію вузлів. Системи контролю трафіку допомагають виявляти аномальну або зловмисну активність. Створення тунелів для передачі критичних даних мінімізує ризик їх перехоплення. Захищені протоколи (наприклад, HTTPS, MQTT з TLS) є стандартом. Для вразливих сегментів мережі застосовується додаткова ізоляція. Контроль затримок та доступності зв’язку важливий для захисту в реальному часі.

Системи SCADA управляють ключовими об'єктами енергетичної інфраструктури, тому потребують найвищого рівня захисту. Доступ до інтерфейсів SCADA обмежується через контроль доступу та ролі користувачів. Впроваджуються міжмережеві екрани (фаєрволи), що фільтрують трафік між мережами. Для додаткової безпеки впроваджується сегментація мережі на DMZ та внутрішню зону. Системи журналювання подій контролюють дії операторів та автоматів. Захист операційної системи серверів SCADA виконується шляхом ізоляції служб. Проводиться постійний моніторинг стану SCADA-серверів та PLC-контролерів. Сценарії реагування на інциденти повинні бути автоматизовані.

В хмарних інфраструктурах впроваджуються системи виявлення вторгнень (IDS) і попередження атак (IPS). Дата-центри розділяють внутрішню і зовнішню мережу, забезпечуючи сегментацію. Усі віртуальні машини повинні бути ізольовані одне від одного на рівні гіпервізора. Проводиться регулярне резервне копіювання даних для забезпечення стійкості до атак. Дані шифруються як при зберіганні, так і при передачі. Доступ до інфраструктури обмежений через VPN та багатофакторну автентифікацію. Застосовуються політики безперервного моніторингу та реагування на інциденти (SOC). Перевірка відповідності

стандартам (наприклад, ISO 27001) є обов’язковою.

Адміністратори мають обмежений доступ згідно з політикою мінімальних привілеїв. Усі дії адміністраторів логуються з подальшим аудитом. Введено багатофакторну автентифікацію для захисту адміністративних облікових записів. Регулярне оновлення паролів та їх зберігання в захищеному вигляді є обов’язковим. Визначаються чіткі політики безпеки та інструкції щодо реагування на інциденти. Проводиться навчання персоналу щодо сучасних кіберзагроз. Адміністративний доступ сегментується по рівнях чутливості систем. Встановлюється моніторинг поведінки користувачів для виявлення підозрілої активності.

Отже, інтелектуальні лічильники потребують захисту від несанкціонованого доступу та підробки даних.

Впроваджується шифрування даних, які лічильники передають до системи обліку.

Аутентифікація користувача забезпечує доступ лише зареєстрованим абонентам. Важливим є захист прошивки лічильника від зміни або ін’єкцій шкідливого коду. Встановлюється контроль доступу до портів та інтерфейсів пристрою. Застосовуються сертифікати безпеки для верифікації пристроїв. Передбачено журналювання доступу до інтелектуальних пристроїв.

Регулярне оновлення програмного забезпечення допомагає усувати вразливості.

Розглянемо приклади застосування розумних електромереж.

1. Сонячні панелі на дахах будинків.

У міських умовах встановлення сонячних панелей на дахах будинків дозволяє децентралізовано генерувати електроенергію. Це зменшує навантаження на центральну мережу і знижує витрати споживачів на електроенергію. Панелі підключаються до Smart Grid через інвертори з можливістю зворотного живлення в мережу (Net Metering). Надлишки електроенергії, які не використовуються на місці, можуть бути передані іншим споживачам або в накопичувачі. Система

моніторингу забезпечує контроль за продуктивністю панелей у реальному часі. Завдяки Smart Grid власники отримують аналітику щодо генерації та споживання енергії. Інтелектуальна мережа координує розподіл енергії залежно від попиту. Панелі можуть працювати в зв'язці з акумуляторами для забезпечення автономності у разі аварій. Таке рішення підвищує енергонезалежність міста. Крім того, воно сприяє зниженню викидів $CO_2$ та розвитку екологічної урбаністики.

2. Електромобілі з технологією V2G (Vehicle-to-Grid).

Технологія V2G дозволяє електромобілям не тільки заряджатися, але й віддавати енергію назад у мережу. У місті це дає змогу використовувати автопарк як мобільні акумулятори. В години пікового навантаження Smart Grid може запитувати енергію від автомобілів. Така інтеграція стабілізує мережу, особливо при нестабільному виробітку від ВДЕ. Кожен електромобіль підключається через спеціальну V2G-станцію, що підтримує двосторонній потік енергії. Передача регулюється автоматично через алгоритми, які враховують стан заряду, графік використання авто та потреби мережі. Власники авто можуть отримувати фінансову винагороду за участь у балансуванні мережі. Система забезпечує захист з'єднання та шифрування обміну даними. V2G робить електромобілі важливою частиною енергетичної інфраструктури, а не лише транспортом. Такий підхід сприяє переходу до сталого і взаємопов'язаного енергоспоживання в місті.

3. Централізоване управління через SCADA.

Система SCADA (Supervisory Control and Data Acquisition) є центральним елементом управління Smart Grid. Вона забезпечує моніторинг і контроль за всіма об'єктами міської енергомережі, від підстанцій до споживачів. Через SCADA оператори мають доступ до даних у реальному часі, включаючи напругу, струм, навантаження та аварії. Система дозволяє автоматизовано вмикати чи вимикати лінії, реагувати на несправності й оптимізувати розподіл енергії. SCADA може взаємодіяти з іншими платформами, зокрема з аналітичними сервісами на базі AI. Захист SCADA-систем є критичним, вона повинна бути ізольована від зовнішніх

загроз, використовувати шифрування та багаторівневу автентифікацію. Завдяки візуалізації даних оператори можуть швидко приймати рішення в кризових ситуаціях. Інтерфейс SCADA дозволяє керувати ресурсами як вручну, так і в автоматичному режимі. У містах SCADA часто поєднується з системами розумного транспорту, освітлення та водопостачання. Це забезпечує інтеграцію енергосистеми в єдину цифрову інфраструктуру «розумного міста».

4. Алгоритми прогнозування попиту (на основі AI).

Штучний інтелект (AI) використовується для прогнозування енергетичного попиту на основі історичних даних, погодних умов, часу доби та інших факторів. Це дозволяє енергосистемі заздалегідь готуватися до змін у навантаженні. Алгоритми враховують події в місті, сезонність і поведінку споживачів. Завдяки цьому оператори можуть краще планувати роботу генерувальних потужностей і зберігання енергії. AI дозволяє мінімізувати втрати енергії та уникнути перевантажень мережі. Також можливе динамічне ціноутворення для стимулювання зміни споживчої поведінки. Прогнози можуть оновлюватися в режимі реального часу при надходженні нових даних. Моделі машинного навчання (ML) постійно навчаються на нових ситуаціях, підвищуючи точність з часом. Це створює основу для гнучкого попиту (demand response) та ефективного управління ресурсами. Прогнозування є критично важливим для інтеграції ВДЕ, які залежать від погодних умов.

5. Виявлення аномалій у мережі (ML + IDS).

Системи виявлення вторгнень (IDS, Intrusion Detection Systems), підсилені машинним навчанням, дозволяють вчасно ідентифікувати незвичну активність у мережі. Вони аналізують трафік, поведінку пристроїв та інші параметри, щоб виявити потенційні загрози або помилки. Наприклад, система може виявити збої в роботі трансформатора або спробу кібератаки. Машинне навчання дозволяє розпізнавати не лише відомі атаки, а й нові, нетипові шаблони. IDS працює в режимі реального часу та може ініціювати автоматичну ізоляцію підозрілих компонентів. Це зменшує ризик поширення загрози в межах міської мережі.

Системи інтегруються з іншими компонентами безпеки (SIEM, SCADA, SOC) для створення єдиного поля контролю. Виявлені інциденти документуються для подальшого аналізу та покращення моделей. Такі рішення особливо важливі в умовах динамічного середовища з тисячами взаємопов'язаних пристроїв. Завдяки цьому міська Smart Grid стає не тільки розумною, а й стійкою до зовнішніх і внутрішніх загроз.

Розглянемо компоненти системи (таблиця 2.3).

Таблиця 2.3 – Приклади компонентів системи Smart Grid

| Компонент | Тип | Функціональне призначення | Приклади/Протоколи/ Захист |
|---|---|---|---|
| Сенсори напруги, струму, температури | IoT-пристрої | Збір фізичних параметрів у реальному часі для моніторингу стану мережі | Modbus, MQTT, HTTPS, TLS |
| Інтелектуальні лічильники (Smart meters) | Smart Devices | Двосторонній облік споживання та генерації електроенергії; передача даних в реальному часі | DLMS/COSEM, 128-bit AES |
| DERMS | Програмно-апаратна система | Координація та оптимізація роботи розподілених джерел енергії | IEC 61850, REST API, VPN-захист |
| BESS | Фізичний ресурс | Збереження надлишкової енергії та її подача у мережу при пікових навантаженнях | CAN, MODBUS, контролери з обмеженим доступом |

Кінець таблиці 2.3

| Компонент | Тип | Функціональне призначення | Приклади/Протоколи/ Захист |
|---|---|---|---|
| HMI | Інтерфейс SCADA | Візуалізація даних, ручне або автоматизоване керування обладнанням оператором | Proprietary protocols, VLAN, MFA |

Розглянемо етапи впровадження такої системи:

1. Проєктування архітектури.

На цьому етапі визначається загальна структура системи з урахуванням масштабів, вимог та обмежень. Визначаються ключові функціональні блоки: генерація, передача, розподіл, облік та управління. Ураховуються аспекти масштабованості, сумісності з наявною інфраструктурою та резервування. Розробляється модель взаємодії між фізичними пристроями та інформаційною системою. Закладається структура мережевої безпеки, зокрема сегментація, контроль доступу та протоколи. Проєктування виконується із урахуванням норм енергетичної безпеки та екологічних стандартів. Враховується потреба інтеграції з зовнішніми платформами (DERMS, ERP, SCADA тощо). На завершення формується технічне завдання для подальших етапів розробки.

2. Вибір компонентів та технологій.

Обираються апаратні рішення: сенсори, контролери, лічильники, комунікаційні пристрої. Проводиться аналіз сумісності обраних компонентів з майбутнім програмним середовищем. Обираються протоколи обміну даними (наприклад, MQTT, IEC 61850, Modbus). Впроваджуються сучасні засоби захисту: TPM-модулі, криптографія, VPN. Враховується вартість, надійність, сертифікація та можливість техпідтримки компонентів. Для Smart Grid критично важливо обрати енергоефективні та відмовостійкі пристрої. Вибір технологій включає

також ПЗ для аналітики, візуалізації та обробки даних. Остаточне рішення затверджується після узгодження з технічними та фінансовими експертами.

3. Моделювання і тестування.

Перед впровадженням реальної системи створюється цифрова модель Smart Grid. Віртуальне середовище дозволяє змоделювати сценарії навантажень, відмов та атак. Тестування охоплює як функціональні, так і не функціональні характеристики системи. Перевіряється робота окремих вузлів, а також взаємодія між ними. Здійснюється кібертестування: симуляція втручань, відмова зв'язку, втрати пакетів. Аналізуються затримки, споживання енергії, швидкість реакції системи. За результатами виявлені недоліки усуваються, конфігурації коригуються. Після проходження тестів формуються рекомендації до впровадження в реальне середовище.

4. Поетапне розгортання.

Встановлення компонентів відбувається у кілька етапів, починаючи з пілотних зон. Кожен етап включає монтаж, налаштування та інтеграцію нових пристроїв у мережу. Проводиться перевірка працездатності після кожного підключення. Тестуються функції моніторингу, передачі даних, керування та захисту. На основі аналізу результатів вирішується про перехід до наступного етапу. Поетапний підхід дозволяє зменшити ризики та швидко реагувати на неполадки. Впровадження супроводжується постійним технічним та інформаційним моніторингом. Завершальним етапом є повна інтеграція всіх підсистем в єдину архітектуру.

5. Навчання персоналу.

Персонал проходить навчання для ефективного керування новою системою. Тренінги охоплюють апаратну, програмну, мережеву та інформаційну частини. Особливу увагу приділяють процедурі реагування на інциденти. Працівники навчаються працювати з інтерфейсами SCADA, HMI, DERMS. Пояснюються основи інформаційної безпеки та вимоги до автентифікації. Створюються інструкції та методичні матеріали з експлуатації обладнання. Часто

впроваджується система тестування знань та сертифікації персоналу. Навчання є безперервним процесом, проводяться оновлення при зміні системи.

6. Обслуговування, оновлення, кібермоніторинг.

Після впровадження важливо забезпечити безперервне технічне обслуговування. Регулярно оновлюється ПЗ, прошивки пристроїв, бази даних та політики безпеки. Проводиться резервне копіювання критичних даних та конфігурацій. Система моніторингу постійно аналізує трафік та виявляє підозрілу активність. Реагування на інциденти має бути швидким і структурованим (playbooks). Впроваджуються платформи SIEM, SOC або інші системи кіберспостереження. Періодично виконуються аудит безпеки та тестування на проникнення. Обслуговування забезпечує довгострокову стабільність, захищеність і розвиток системи.

7. Нормативно-правові та стандартизаційні аспекти.

Врахування вимог міжнародних стандартів і нормативів (IEC, IEEE, ISO). Аналіз національних законодавчих актів, що регулюють енергетику та кібербезпеку. Ліцензування обладнання та сертифікація систем відповідно до вимог ринку. Включення положень щодо захисту персональних даних та конфіденційності. Розгляд вимог до екологічного впливу і стійкості системи. Визначення ролі державного регулятора та співпраці з ним. Встановлення стандартів звітності та аудиту безпеки інфраструктури. Документування процедур відповідності для забезпечення сертифікації.

8. Інтеграція з наявною інфраструктурою

Аналіз поточного стану існуючих систем та їхньої готовності до інтеграції. Визначення точок взаємодії нової та існуючої інфраструктури. Ретрофіт застарілого обладнання для забезпечення сумісності з новими технологіями. Забезпечення плавного переходу з мінімальними перебоями в роботі мережі. Розробка гібридних рішень для поетапного впровадження технологій Smart Grid. Визначення методів забезпечення обміну даними між різними системами. Забезпечення зворотного сумісного тестування під час інтеграції. Розробка плану

підтримки та обслуговування на перехідному періоді.

9. Управління ризиками та кризовий менеджмент.

Ідентифікація потенційних кіберзагроз та технічних ризиків. Розробка планів реагування на інциденти та аварійних ситуацій. Визначення сценаріїв відмов та процедур їх оперативного усунення. Забезпечення резервного копіювання критичних даних і систем. Впровадження засобів оперативного моніторингу і реагування на загрози. Проведення періодичних аудітів безпеки та тестування на проникнення. Оцінка ефективності заходів захисту та постійне їх вдосконалення. Співпраця з експертними центрами для отримання консультацій і підтримки.

10. Графік реалізації та контрольні точки.

Створення детальної дорожньої карти впровадження проекту. Визначення основних фаз, етапів та термінів реалізації. Призначення відповідальних команд і розподіл обов’язків. Розробка системи моніторингу прогресу на кожному етапі. Встановлення контрольних точок для оцінки досягнутих результатів. Забезпечення системи звітності для відстеження витрат і ефективності. Коригування плану реалізації на підставі поточних результатів тестування. Організація зустрічей для обговорення складних моментів і планування наступних кроків.

11. Перспективи розвитку та інновації

Аналіз тенденцій розвитку технологій у сфері енергетики. Оцінка можливості інтеграції нових технологічних рішень в систему. Розгляд перспектив використання штучного інтелекту для прогнозування навантажень. Вивчення потенціалу блокчейн-технологій для забезпечення прозорості. Оцінка можливостей для підвищення енергоефективності та зниження викидів. Відстеження нових стандартів і протоколів комунікації. Впровадження концепцій «розумних міст» і інтеграції з іншими критичними інфраструктурами. Планування етапів модернізації системи відповідно до еволюції ринку.

## 2.3 Висновки до другого розділу

У межах розділу 2 проведено аналіз вимог, які висуваються до кіберфізичних систем захисту об’єктів критичної інфраструктури. Запропоновано багаторівневу архітектуру захисту. Багаторівнева архітектура захисту є критично важливою складовою забезпечення надійності та стійкості Smart Grid до кіберзагроз. Кожен рівень, від споживача до адміністрування, виконує власні функції безпеки, створюючи комплексну систему захисту енергетичної інфраструктури.

Такий підхід дозволяє запобігати несанкціонованому доступу, забезпечувати цілісність та конфіденційність даних, а також швидко реагувати на потенційні інциденти.

Важливу роль відіграє впровадження сучасних засобів автентифікації, шифрування, моніторингу трафіку та міжмережевих екранів. Безперервне логування подій, багатофакторна автентифікація й контроль дій персоналу підвищують рівень захисту системи в цілому. Окрему увагу необхідно приділяти сегментації мережі та резервному копіюванню, що дозволяє забезпечити відновлення роботи у разі атак.

# 3 ПРОГРАМНО-АПАРАТНА РЕАЛІЗАЦІЯ КІБЕРФІЗИЧНОЇ СИСТЕМИ ДЛЯ ЗАХИСТУ ОБЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

## 3.1 Опис апаратного забезпечення кіберфізичної системи для захисту об’єктів критичної інфраструктури

Кіберфізична система для захисту об’єктів критичної інфраструктури на прикладі Smart Grid, або розумних електромереж, являє собою поєднання апаратних і програмних рішень, що працюють у режимі реального часу для забезпечення безпеки, стабільності та надійності енергосистеми. У такій системі тісно взаємодіють фізичні компоненти мережі з цифровими інтелектуальними модулями.

З апаратної точки зору до складу системи входять датчики напруги, струму, температури, трансформатори, контролери потужності, високошвидкісні комутатори, а також модулі для збору та передавання даних у реальному часі. У розподільчих підстанціях встановлюються програмовані логічні контролери (PLC), які керують параметрами живлення і реагують на зміну навантаження. Крім того, в системі використовуються фідери з автоматизованим перемиканням, а також інтелектуальні лічильники (smart meters), що передають дані до диспетчерських центрів.

Кіберфізична система складається з ряду функціональних вузлів, кожен з яких виконує окрему роль у моніторингу та управлінні процесами в енергомережі. У кожному вузлі встановлені фізичні давачі, що фіксують параметри середовища, такі як, напругу, струм, температуру, вібрацію або наявність газів. Отримані дані миттєво передаються до вбудованих контролерів, які аналізують значення відповідно до заданих алгоритмів. Виконавчі пристрої, такі як реле чи автоматичні вимикачі, реагують на сигнали від контролерів у разі виявлення аномалій. Комунікаційні модулі забезпечують надійний обмін інформацією між вузлами системи через дротові або бездротові мережі, зокрема Ethernet, 4G або LoRa. Для стабільної роботи всіх компонентів застосовуються резервовані

джерела живлення, які підтримують функціональність навіть при збої основної енергосистеми. Вузли об’єднуються у єдину інтелектуальну мережу, яка дозволяє приймати рішення децентралізовано та з високою швидкістю. Така архітектура робить систему гнучкою, масштабованою й здатною до автономного реагування на критичні ситуації.

В таблиці 3.1 наведено ключові апаратні компоненти та приклади обладнання.

Таблиця 3.1 – Основні типи сенсорів (давачів) у Smart Grid

| Назва сенсора | Призначення | Приклад моделі |
|---|---|---|
| Датчик струму | Вимірювання потужності/перевантаження | LEM CT, ABB Rogowski Coil |
| Датчик напруги | Моніторинг стабільності напруги в мережі | Siemens 7KE85, Schneider VAMP |
| Температурний давач | Контроль перегріву трансформаторів/кабелів | PT100, DHT22 (для повітря) |
| Вібраційний сенсор | Виявлення механічних аномалій у підстанціях | SW-420, Brüel & Kjær віброметр |
| Оптичні давачі | Виявлення дугових розрядів та іскріння | AFL Optical Arc Sensor |
| Газоаналізатор | Аналіз часток SF6 або CO у трансформаторній олії | Vaisala MHT410 |

У таблиці наведені типові давачі, які застосовуються для моніторингу фізичних параметрів у розумних електромережах. Датчики струму та напруги дають змогу постійно контролювати стан енергосистеми й реагувати на відхилення, наприклад, перенавантаження або обриви ліній.

Температурні сенсори використовуються у трансформаторних підстанціях і розподільчих щитах для запобігання перегріву, який може призвести до пожежі

або виходу з ладу обладнання.

Вібраційні давачі дозволяють виявляти механічні відхилення, наприклад, розбалансування обмоток або несправності у вентиляторних блоках.

Оптичні сенсори фіксують виникнення дугових розрядів, а газоаналізатори визначають наявність шкідливих газів у трансформаторному маслі, що свідчить про внутрішні дефекти.

Виконавчі пристрої, або активні компоненти, є ключовими елементами кіберфізичної системи, що безпосередньо здійснюють фізичний вплив на енергетичну інфраструктуру у відповідь на аналітичні рішення системи керування. На відміну від сенсорів, які лише збирають дані, ці пристрої відповідають за виконання конкретних дій — розмикання або перемикання живлення, запуск систем охолодження, адаптацію режимів роботи обладнання. Вони забезпечують швидке реагування на критичні ситуації, зокрема короткі замикання, перевантаження, перегрів або нестабільність у мережі. Завдяки інтеграції з програмованими логічними контролерами (PLC), виконавчі пристрої можуть функціонувати як автономно, так і в рамках централізованої стратегії управління мережею.

У таблиці 3.2 наведено основні типи таких пристроїв із прикладами обладнання, що використовується у сучасних Smart Grid системах.

Таблиця 3.2 – Виконавчі пристрої (активні компоненти)

| Тип пристрою | Функція в системі | Приклад обладнання |
|---|---|---|
| PLC-контролери | Місцеве управління та реакція на події | Siemens S7-1500, Schneider M340 |
| Інтелектуальні реле | Розмикання/перемикання живлення | ABB REF615, SEL-751A |
| Автоматичні вимикачі | Захист ліній від короткого замикання | ABB SACE Emax2, Eaton NZM |

Кінець таблиці 3.2

| Тип пристрою | Функція в системі | Приклад обладнання |
|---|---|---|
| Smart Meter (лічильник) | Облік і передача енергоспоживання | Kamstrup OMNIPOWER, Landis+Gyr |
| Вентилятори/ охолоджувачі | Терморегуляція трансформаторів | Rittal вентиляторні блоки |

У таблиці наведені пристрої, які безпосередньо впливають на роботу системи, це виконавчі механізми. Програмовані логічні контролери (PLC) є ядром керування на місцях. Вони приймають сигнали з сенсорів і видають команди на відповідні дії (наприклад, розмикання кола, активація охолодження).

Інтелектуальні реле працюють як захисні елементи, які автоматично вимикають лінії при фіксації небезпечних умов, зокрема коротких замикань.

Автоматичні вимикачі відключають живлення на рівні секцій або підстанцій. Smart-лічильники дозволяють не лише обліковувати споживання, але й передавати ці дані в реальному часі, що створює основу для аналітики та адаптивного тарифування.

Вентилятори або інші охолоджувачі активуються при перевищенні температурного порогу, запобігаючи термічному навантаженню обладнання.

Комунікаційна апаратура є критично важливою складовою кіберфізичних систем, оскільки забезпечує безперервний і захищений обмін даними між усіма елементами мережі. У контексті Smart Grid така апаратура дозволяє сенсорам, виконавчим пристроям, контролерам і аналітичним модулям взаємодіяти в режимі реального часу. Вона забезпечує зв’язок як на рівні локальної мережі (LAN), так і для віддаленого доступу до центрів керування через глобальні мережі. Залежно від умов експлуатації та архітектури системи, застосовуються як дротові технології (Ethernet, оптика), так і бездротові рішення (4G/5G, LoRa, Wi-Fi).

Особливу увагу приділяють надійності зв’язку, швидкості обміну, стійкості

до завад і відповідності промисловим стандартам. У таблиці 3.3 подано основні типи комунікаційних пристроїв із прикладами їх використання у системах розумної енергетики.

Таблиця 3.3 – Комунікаційна апаратура

| Модуль | Призначення | Стандарт/приклад |
|---|---|---|
| Модем для передачі даних | Зв’язок між вузлами | 4G/5G модеми, LoRa-модулі |
| Ethernet-комутатори | Локальна передача даних | Cisco IE-4000, Hirschmann RSP |
| Промисловий шлюз (Gateway) | Концентрація даних з різних давачів | Moxa UC-8100, Siemens RUGGEDCOM RX1400 |

Ця таблиця демонструє пристрої, які забезпечують надійну передачу даних між елементами кіберфізичної системи.

Модеми (зокрема, 4G/5G або LoRa) використовуються для бездротового обміну даними в умовах, де проводове підключення обмежене або недоцільне.

Ethernet-комутатори утворюють локальні мережі з високою пропускною здатністю між різними вузлами системи.

Промислові шлюзи виконують роль концентраторів даних, вони збирають інформацію з великої кількості давачів, конвертують протоколи та передають дані у SCADA-систему або хмару для подальшої обробки. Усі ці компоненти мають бути стійкими до електромагнітних завад, коливань температур і вологості, тому зазвичай мають посилений корпус і сертифікацію промислового стандарту.

Обробка та логіка – це найважливіша частина кіберфізичної системи, який забезпечує аналіз даних, прийняття рішень і координацію дій усіх апаратних компонентів. У Smart Grid ці функції реалізуються за допомогою вбудованих обчислювальних модулів, таких як мікроконтролери, промислові комп’ютери, логічні контролери (PLC), а також програмовані логічні інтегральні схеми

(FPGA).

Вони обробляють дані, отримані з сенсорів, виконують логічні та математичні операції, керують виконавчими пристроями і підтримують зв’язок із вищими рівнями керування SCADA або хмарними платформами. Вибір обчислювального модуля залежить від складності задач, необхідної швидкості реагування, умов експлуатації та обсягу оброблюваних даних.

Нижче представлено ключові типи обчислювальних пристроїв, які застосовуються у кіберфізичних системах критичної інфраструктури. До вбудованих обчислювальних модулів відносяться:

– мікроконтролери, які використовуються для простих задач обробки (ESP32, STM32);

– промислові ПК, що використовуються для виконання аналітики в реальному часі (Advantech UNO, Beckhoff IPC);

– FPGA/SoC використовуються у задачах високошвидкісного реагування на події (Intel Cyclone, Xilinx Zynq).

Ці обчислювальні елементи забезпечують інтелектуальну обробку даних у реальному часі. Мікроконтролери підходять для простих систем моніторингу або автоматичного реагування на локальні події (наприклад, вимкнення при перегріві). Промислові комп’ютери, як правило, використовуються на рівні підстанцій або диспетчерських центрів. Вони аналізують дані, будують моделі навантаження, прогнозують споживання тощо.

FPGA і SoC застосовуються в системах, де критична мінімальна затримка, наприклад, для реалізації алгоритмів захисту від короткого замикання або динамічного балансу фаз у мережі.

Апаратна частина кіберфізичної системи Smart Grid – це сукупність прецизійних сенсорів, швидкодіючих контролерів і мережевих інтерфейсів, що забезпечують повну прозорість і оперативне реагування на зміни в енергосистемі. Така інфраструктура дозволяє не тільки підтримувати стабільну роботу мережі, а й передбачати аварійні стани на основі даних у реальному часі.

3.2 Опис програмного забезпечення кіберфізичної системи для захисту об’єктів критичної інфраструктури

Програмна реалізація охоплює низку модулів для аналізу даних, прогнозування споживання, оптимізації розподілу навантаження, а також синхронізації роботи елементів у межах єдиної енергомережі.

Використовуються SCADA-системи для диспетчерського управління, ПЗ для керування мікромережами (microgrid controllers), а також алгоритми на основі машинного навчання для виявлення аномалій у споживанні чи змін у топології мережі (талиця 3.4). Комунікація між компонентами забезпечується за допомогою захищених протоколів (наприклад, IEC 61850), що дозволяє забезпечити узгоджену та швидку реакцію на зміну ситуації в системі.

Таблиця 3.4 – Класи програмного забезпечення для системи Smart Grid

| Категорія ПЗ | Основне призначення | Приклади систем |
|---|---|---|
| SCADA-системи | Диспетчерське керування, візуалізація процесів | Siemens WinCC, GE iFIX, Inductive Ignition |
| ПЗ для PLC/RTU | Програмування логіки керування пристроями на місці | Siemens TIA Portal, Codesys |
| Платформи обліку/аналітики | Облік енергії, генерація звітів, побудова трендів | OpenMUC, EnergyCAP, OSIsoft PI |
| Прогнозуючі алгоритми | Моделі попередження несправностей і навантаження | Python/ML-моделі з TensorFlow, PyTorch |
| Платформи оптимізації | Балансування генерації, навантаження, тарифів | GridLAB-D, HOMER Grid |
| Протокольні інтерфейси | Забезпечення обміну даними між компонентами системи | IEC 61850, Modbus, DNP3 |

Кінець таблиці 3.4

| Категорія ПЗ | Основне призначення | Приклади систем |
|---|---|---|
| Платформи IoT/Edge | Обробка даних на краю мережі, локальна логіка | Node-RED, Azure IoT Edge, Balena |

SCADA-системи є центральним інтерфейсом оператора, що дозволяє у реальному часі бачити стан мережі, отримувати аварійні сигнали, керувати вузлами і створювати історичні звіти. Підтримують графічне середовище, інтеграцію з БД і високий рівень кастомізації.

Програмування за допомогою PLC/RTU це коли контролери керуються за допомогою спеціалізованого ПЗ (наприклад, TIA Portal), де створюється логіка реагування на сигнали, як стандартна логіка, так і адаптивні сценарії. Можливе розширення функціоналу через скрипти чи функціональні блоки.

Платформи для енергетичної аналітики об’єднують телеметрію з розподілених лічильників і вузлів, будують графіки споживання, виявляють аномалії у споживанні, створюють звітність для регуляторів та дозволяють проводити аудит енергоефективності.

Алгоритми прогнозування застосовується для прогнозу навантажень, сезонного споживання, ймовірності відмов, виявлення атипових подій. Наприклад, класифікація стану трансформатора на основі температури, струму й історичних відмов.

ПЗ для оптимізації енергомережі дозволяють створювати математичні моделі мережі, симулювати режими роботи, визначати оптимальні конфігурації підстанцій, черговість ввімкнення резервів, маршрути передачі енергії тощо.

Протоколи та інтерфейси обміну використовуються, щоб модулі, що реалізують стандарти IEC 61850, DNP3, Modbus TCP/RTU тощо, гарантували сумісність обладнання різних виробників і стабільний зв’язок між системами управління та польовими пристроями.

Edge/IoT-платформи, у системах із багатьма вузлами частина логіки

переноситься на край мережі. Це дозволяє зменшити затримки, зберегти функціональність при втраті зв'язку з центром і реалізувати автономне прийняття рішень.

### 3.3 Архітектура Smart Grid

Архітектура Smart Grid є багаторівневою та включає в себе цілу низку технологій: IoT-сенсори, інтелектуальні лічильники, системи телеметрії, AI-аналітику, хмарні сервіси та BI-інтерфейси для моніторингу та прийняття рішень (рисунок 3.1).

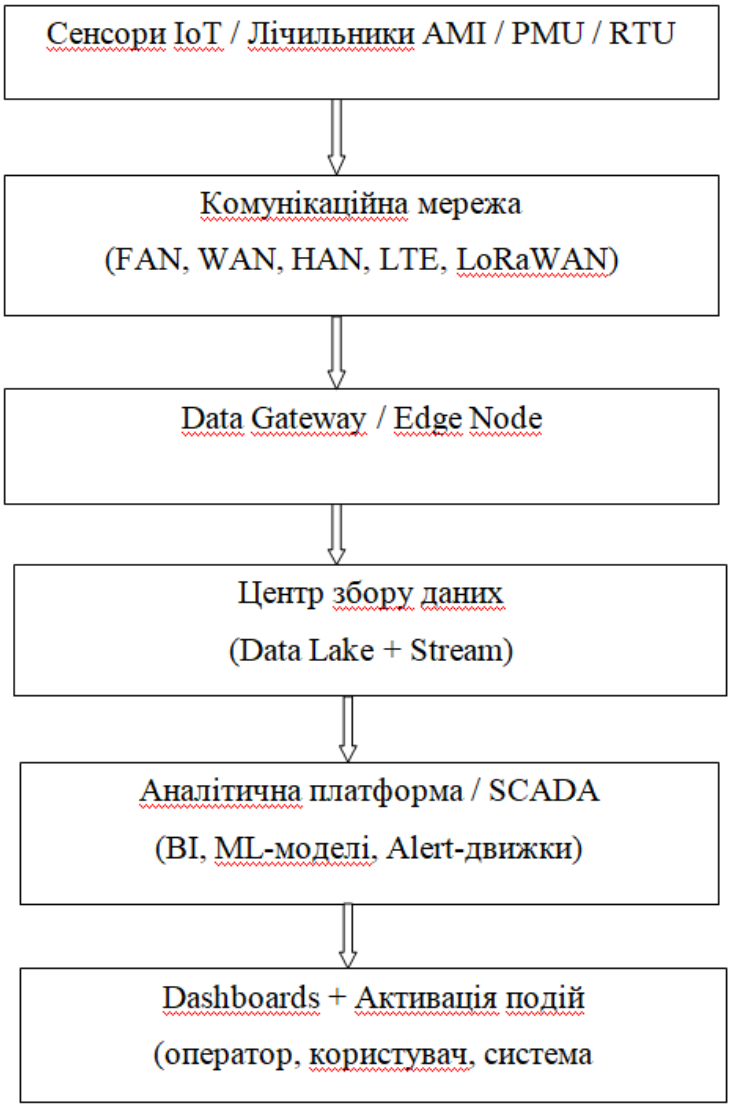



Рисунок 3.1 – Архітектура Smart Grid

Першим рівнем такої архітектури є рівень збору даних (Edge / Field Level), де відбувається збір даних з фізичних пристроїв у полі.

Компонентами цього рівня є різні здавачі та сенсори, наприклад, наступні:

– Smart Meters (AMI) здійснюють вимірювання споживання у реальному часі;

– PMU (Phasor Measurement Units) забезпечують вимірювання фазових параметрів;

– IoT сенсори збирають дані про температуру трансформаторів, напругу та струм;

– DER є пристроями розподіленої генерації (сонячні, вітрові);

– EV Chargers / батареї обчислюють заряд, розряд та використання.

На комунікаційному рівні відбувається передача даних у центр управління. Технології, які при цьому використовуються можуть бути наступні:

– FAN (Field Area Network), як от ZigBee, LoRaWAN, Wi-SUN;

– WAN (Wide Area Network)**,** наприклад, LTE, 5G, Ethernet;

– HAN (Home Area Network) забезпечують зв’язок між приладами в будинку;

– протоколи такі, як MQTT, OPC UA, Modbus, DNP3.

Рівень попередньої обробки забезпечує функцію буферизації та обробки на рівні edge-пристроїв.

Компоненти, які при цьому використовуються це:

– Edge Gateway для фільтрації, агрегації та шифрування;

– Node-RED/Azure IoT Edge/AWS Greengrass – це low-code автоматизація.

Центральний рівень даних призначений для логіки, аналітики та зберігання даних.

Компоненти, які для цього використовуються є наступними:

– Data Lake/Data Warehouse для зберігання великих обсягів (Parquet, SQL);

– Stream Processing це Apache Kafka, Spark Streaming;

– Time-series DB – це InfluxDB, TimescaleDB для швидкого аналізу;

– AI/ML це Scikit-learn, TensorFlow, Azure ML.

Рівень аналітики та візуалізації використовується для того, щоб такі користувачі, як оператори, аналітика бачили результат.

Інструменти які для цього використовуються, це BI-платформи, такі як Power BI, Grafana, Tableau, Apache Superset; SCADA-панелі для контролю у реальному часі, сигнали тривоги та HEMS/Mobile App як інтерфейси для користувача.

Важливим є також врахування питань безпеки**,** масштабованості та відмовостійкості**.**

У системах Smart Grid, що поєднують фізичну інфраструктуру з цифровими технологіями, питання безпеки є критично важливим. Вразливість до кібератак, зловживань даними або перехоплення сигналів може призвести не лише до фінансових втрат, а й до загроз для життя населення (наприклад, аварійні відключення або перегрів трансформаторів).

Ключові аспекти безпеки включають наступні:

1. Криптографічний захист використання сучасних методів шифрування (TLS, AES) для передачі даних від IoT-пристроїв до центральних вузлів.

2. Аутентифікація та контроль доступу означає впровадження систем багатофакторної аутентифікації, сертифікатів (PKI) для пристроїв і користувачів.

3. Сегментація мережі**,** тобто поділ мережі на безпечні зони (наприклад, SCADA-сегмент відокремлений від загальнодоступного IoT-рівня).

4. Виявлення аномалій та атак**,** використання IDS/IPS-систем (Intrusion Detection/Prevention Systems), а також алгоритмів штучного інтелекту для прогнозування потенційно шкідливої активності.

5. Оновлення прошивок та програмного забезпечення регулярне та безпечне оновлення firmware для запобігання відомим уразливостям.

Енергетична система повинна мати можливість масштабуватись, тобто розширюватись у відповідь на зростаючі потреби споживачів, інтеграцію нових пристроїв, джерел енергії та технологій без втрати ефективності чи стабільності.

Основними рішеннями тут є:

1. Хмарна архітектура (Cloud-native)**,** тобто застосування платформ Azure, AWS або GCP дозволяє масштабувати обчислення, зберігання та сервіси за потреби.

2. Мікросервісна структура дозволяє розподілення логіки на окремі сервіси, які можна масштабувати незалежно.

3. Паралельна обробка великих даних, тобто Apache Kafka, Spark, Flink забезпечують обробку потоків даних у режимі реального часу.

4. Контейнеризація та оркестрація при використанні Docker і Kubernetes дозволяє швидко розгортати нові компоненти у мережі.

Smart Grid повинен залишатися функціональною у випадках часткових відмов, перебоїв у живленні, кібератак або природних катастроф. Стійкість системи визначає її здатність зберігати критичні функції та відновлюватися після інцидентів.

Існують наступні стратегії забезпечення відмовостійкості:

1. Резервування (redundancy)**,** коли критичні елементи (сервери, маршрутизатори, підстанції) мають дублікати, готові взяти на себе навантаження у разі збою.

2. Автоматичне самовідновлення (self-healing) коли мережі можуть автоматично перенаправляти потоки енергії, замінювати пошкоджені лінії чи перемикатися на альтернативні джерела живлення.

3. Безперервний моніторинг за допомогою сенсорів та системи SCADA, що постійно відстежують параметри мережі, що дозволяє миттєво реагувати на аномалії.

4. Плани аварійного реагування та резервного копіювання передбачають сценарії повного або часткового відновлення (Disaster Recovery Plans), із регулярним створенням бекапів.

Врахування цих трьох аспектів є ключем до побудови надійної, безпечної та довготривалої інфраструктури Smart Grid, що здатна адаптуватись до викликів

сучасного енергетичного середовища.

Зображення типового симулятора розумної електромережі у загальних рисах покзано на рисунку 3.2.

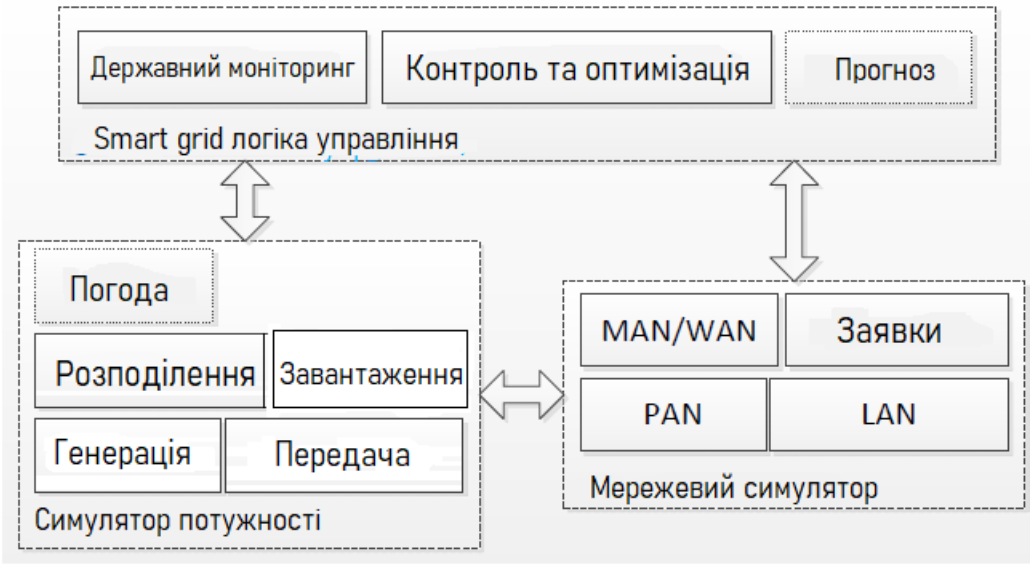



Рисунок 3.2 – Структурна схема симулятора розумної електромережі

Симулятор енергосистеми відповідає за моделювання та імітацію енергомережі, включаючи генератори енергії (як традиційні, так і відновлювані), мережу передачі та розподілу електроенергії, а також навантаження кінцевих користувачів. Кожен з цих системних елементів ставить перед собою різноманітні вимоги щодо моделювання, часової шкали та керування. Це, у свою чергу, робить точне моделювання всієї енергомережі складним процесом; з цієї причини, а також в інтересах якомога точнішого моделювання явищ в енергомережі, більшість існуючих симуляторів енергосистеми зосереджені на частинах енергосистеми. Крім того, оскільки погодні умови можуть впливати на стан генераторів та навантажень, складні симулятори енергосистем також часто інтегрують метеорологічні дані.

Мережевий симулятор використовується для оцінки впливу комунікаційної інфраструктури на продуктивність програм, що працюють поверх неї. Такий інструмент може підтримувати симуляції кількох протоколів на різних рівнях

стеку мережевих протоколів, включаючи протоколи канального, мережевого, транспортного та прикладного рівнів. Розширені мережеві симулятори включають підтримку кількох дротових та бездротових технологій, що використовуються в персональних мережах (PAN), локальних мережах (LAN), міських мережах (MAN) та глобальних мережах (WAN).

На рисунку 3.2. логіку керування було відокремлено від симуляторів живлення та мережі, щоб підкреслити її важливу роль в інтелектуальній мережі як основного елемента для прийняття рішень. На практиці функціональність цього блоку враховується в компонентах інструментів моделювання комунікаційних або енергетичних систем, орієнтованих на інтелектуальні мережі. Ці компоненти включають інтелектуальні лічильники, виконавчі механізми та програми керування та оптимізації. На цьому рисунку показано фреймворк для ко-симуляції (так званий GECO) [40].

Фреймворк інтегрує динамічний симулятор енергосистеми (PSLF) та мережевий симулятор (ns-2) разом за допомогою механізму синхронізації, метою якого є усунення накопичення помилок через явні точки синхронізації між різними симуляторами (явна синхронізація використовувалася в симуляторі EPOCHS).

Динаміка енергосистеми розраховувалася в раундах симуляції (з використанням покрокового підходу), результат яких (тобто новий стан системи) розглядається як подія для глобального планувальника подій. Цей планувальник реалізовано в ns-2 та об'єднує події мережі та енергосистеми в глобальну чергу подій. Інструмент використовувався для оцінки продуктивності схеми резервного захисту віддаленого реле в енергомережі на основі програмних агентів, пов'язаних з окремими реле та контролером інтелектуальної мережі. Два необхідні типи агентів (ведучий та головний) були реалізовані на прикладному рівні в ns-2.

Адевси – це інтегрований симулятор енергетики та мереж, який відповідає принципам гібридного моделювання та симуляції на основі формалізму специфікації дискретних подійних систем (DEVS) [41]. Симулятор інтегрує

моделі дискретних подій для підсистеми зв'язку; безперервні моделі динаміки підсистеми енергетики та дискретні моделі для керування.

Моделі, пов'язані з комунікацією, були реалізовані в інструменті ns-2, тоді як решта моделей (як безперервні, так і дискретні) були реалізовані за допомогою інструменту моделювання adevs, який забезпечує реалізацію методу DEVS.

Моделі на основі диференціально-алгебраїчних рівнянь для виробництва та передачі електроенергії, реалізовані за допомогою adevs, були інтегровані в ns-2 за допомогою інтерфейсу, який дозволяв маніпулювати цими моделями як єдиним процессом дискретних подій. Роль контролера моделювання взяв на себе ns-2. Комбінований інструмент ns-2/adevs був використаний у тематичному дослідженні для автоматичного керування навантаженням та оцінили вплив затримки та пропускної здатності мережі на продуктивність схеми керування скиданням навантаження.

Тісно пов'язаний з цим інструментом THYME, який є програмною бібліотекою для створення симуляторів, що інтегрують модулі на основі adevs для динаміки енергосистеми з існуючими мережевими симуляторами, такими як ns-2 та OMNET++, а також дискретними системами керування.

Платформа спільного моделювання, що поєднує симулятор відкритої розподільчої системи (Opendss) та симулятор мережі ns-2, представлена в роботі [42]. Виконання окремих симуляторів відбувається послідовно, а обмін даними між ними здійснюється за допомогою файлів сценаріїв. Інструмент OpenDSS моделює дискретні події та підтримує аналіз стаціонарного стану систем розподілу електроенергії та розподілених систем відновлюваної генерації.

Комбінований симулятор було використано для оцінки схеми керування, яка активує розподілені акумулятори живлення в сегменті розподільчої мережі для компенсації тимчасової втрати потужності від великого фотоелектричного сонячного джерела (така втрата може, наприклад, бути пов'язана з явищем «хмарного перехідного періоду» або «сонячного рампінгу»). Результати оцінили вплив затримки зв'язку між лічильником, який контролює вихід сонячної

фотоелектричної панелі, та контролером накопичувача, який керує накопичувачами.

На відміну від попередніх симуляторів, що були специфічними для певної предметної області, моделювання інтелектуальних енергетичних мереж може підтримуватися багатодоменним моделюванням та рішеннями для моделювання.

В галузі багатодоменного моделювання мова Modelica отримала велику увагу за останні кілька років завдяки своїй здатності пропонувати широкий набір стандартних бібліотек для фізичного моделювання та точно моделювати явища з безперервною динамікою, подібні до тих, що спостерігаються в енергетичних системах. Modelica спочатку включала підтримку стаціонарного та детального моделювання перехідних процесів енергетичних систем через бібліотеку Spot, а зараз через бібліотеку PowerSystems [43]. Бібліотека містить моделі для різних елементів енергосистеми, включаючи виробництво електроенергії, лінії електропередач, навантаження, трансформатори, конденсаторні батареї тощо.

Симулятор живлення, змодельований за допомогою Modelica, можна поєднати із симулятором комунікаційної мережі для оцінки продуктивності мережевих алгоритмів керування з жорсткими вимогами до синхронізації в інтелектуальних мережах.

У цьому контексті автори роботи [44] пропонують симулятор інтелектуальної мережі, що складається з ns-2 (для моделювання мережі) та Modelica (для моделювання систем енергетики та керування). Щоб уникнути ускладнень синхронізації, було прийнято рішення дозволити ns-2 бути головним контролером часу моделювання, а Modelica виконуватися на запити, надіслані ns-2. Наслідком цього вибору є те, що хоча мережеві події можуть оброблятися вчасно, події всередині Modelica не можуть бути поширені на ns-2.

В галузі моделювання розподілених або федеративних інтелектуальних мереж, GridSpice – це хмарна платформа для моделювання, що інтегрує інструмент Gridlab-D для моделювання виробництва та розподілу електроенергії та MATPOWER (програмне забезпечення на базі Matlab) для оптимального

моделювання потоків потужності [45, 46]. Інструмент не поєднує в собі жодного спеціалізованого мережевого симулятора, а натомість спирається на абстрактне мережеве моделювання, що надається GridLAB-D. Відмінною рисою GridSpice є те, що симуляції виконуються на кластері з динамічним розміром, що складається з робочих вузлів, які виконують частини симуляції (підзадачі симуляції), та головного вузла, відповідального за створення симуляції та синхронізацію між її підзадачами. Для кожної нової симуляції ініціюється процес супервізора, реалізований у RePast Simphony; метою супервізора є планування нових підзадач (які згодом розподіляються між доступними робочими вузлами); підтримка глобального тактового сигналу симуляції та синхронізація граничних станів між підзадачами.

GridSpice – це приклад багатоагентної системи; супервізор – це симулятор дискретних подій на основі агентів, у якому кожне завдання підсимуляції (для розподілу, виробництва чи ринку) є агентом. Інструмент можна використовувати для таких досліджень, як оптимізація розміщення розподіленої генерації та розробка оптимальних графіків диспетчеризації для гнучких навантажень.

Симулятор EPOCHS [47] об'єднує мережевий симулятор ns-2 з двома симуляторами потужності (PSLF для моделювання електромеханічних перехідних процесів та PSCAD/EMTDC для моделювання електромагнітних перехідних процесів) та підсистемою агента, що дозволяє користувачам досліджувати продуктивність алгоритмів керування інтелектуальною мережею в складних сценаріях. Симулятор дотримується моделі з часовими кроками, використовуючи фіксовані точки синхронізації, а різні підсистеми (енергетична, мережева та агентне керування) є інтегровано через проміжне програмне забезпечення RTI. Мотивацією для розробки EPOCHS було те, що оскільки системи зв'язку та живлення ставали все тіснішими, виникла потреба у тестуванні нових схем захисту та керування, які могли б повною мірою використовувати нові засоби зв'язку. Ці нові схеми разюче відрізнялися від традиційних систем захисту, які базували свої рішення на локальних вимірюваннях, та звичайних систем

керування, що працювали через повільні системи зв'язку з передбачуваною продуктивністю. RTI дотримувалася духу HLA як основи для об'єднання симуляторів, але використовувала спеціальний інтерфейс для легшої реалізації. Репрезентативне тематичне дослідження включало оцінку продуктивності резервної релейної системи за наявності несправностей, що спричиняють перебої в лінії.

Віртуальна лабораторія інтеграції сітки (VirGIL) – це модульна платформа для спільного моделювання, яка спирається на інтерфейс функціонального макета (FMI) для інтеграції симулятора комерційної енергосистеми (Powerfactory від DIgSILENT), симулятора мережі (OMNeT++), моделей усієї будівлі (спрощені моделі, отримані з EnergyPlus та виражено за допомогою Modelica) та компонент для оптимізації та керування [48].

FMI – це відкритий стандарт, який підтримує обмін моделями між інструментами, що можуть використовувати різну базову семантику (наприклад, дискретні автомати та диференціальні алгебраїчні рівняння), та спільне моделювання динамічних моделей. У VirGIL різні компоненти експортуються як функціональні одиниці макету (FMU) (як FMU для спільного моделювання або FMU для обміну моделями), а координація їх виконання, а також обмін даними вирішуються інструментом моделювання Ptolemy II, який підтримує аналіз та проектування гетерогенних систем. VirGIL використовувався для оцінки простого алгоритму реагування на попит для зменшення споживання енергії будівлею шляхом коригування параметрів роботи системи опалення, вентиляції та кондиціонування повітря (HVAC) та реалізації вольт-варіантного керування шляхом коригування реактивної потужності, що подається від акумулятора, підключеного до будівлі, що тестується.

Платформа FNCS використовує федеративний підхід для інтеграції симулятора розподілу електроенергії (GridLAB-D), симулятора передачі, розробленого Тихоокеанською північно-західною національною лабораторією, та мережевого симулятора (NS-3) [49]. FNCS підтримує федерацію, вводячи низку

компонентів, що працюють в окремих симуляторах, та компонент (брокер FNCS), що працює в окремому процесі. Компоненти, інтегровані в симулятори, включають міжсимуляційний комунікатор, який обробляє зв'язок між брокером та симулятором, компонент управління зв'язком, що дозволяє вузлам усередині симуляторів надсилати та отримувати повідомлення від інших симуляторів, та компонент управління часом (що включає низку стратегій синхронізації з різними характеристиками використання ресурсів та продуктивності), який забезпечує інтерфейси для синхронізації часу між симуляторами. У мережевий симулятор інтегровано прикладний компонент для реалізації агентів прикладного рівня. Брокер обробляє доставку повідомлень між симуляторами. У зв'язку з цим FNCS дотримується схеми публікації/підписки HLA та реалізує її за допомогою ZeroMQ.

Розглянемо процес візуалізації результатів (рисунок 3.3).

При візуалізації відбуваються наступні дії:

– карта трансформаторів отримує статус через SCADA + сенсори;
– графік споживання формується з AMI + IoT даних;
– ВДЕ вклад агрегація DER (сонце, вітер) з edge-пристроїв;
– прогноз навантаження за результатами AI/ML-аналітики у хмарі.

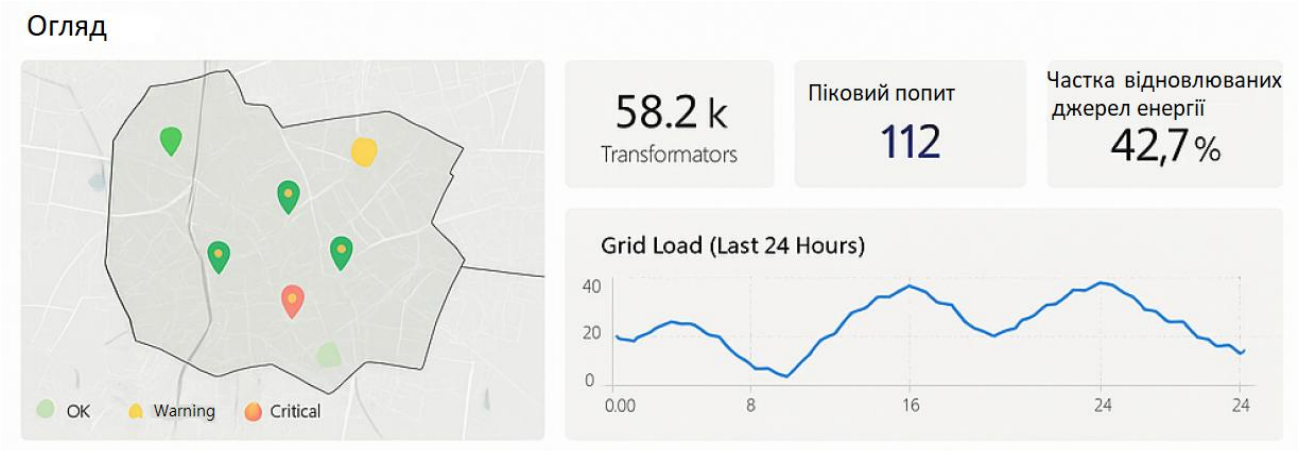



Рисунок 3.3 – Візуалізація результатів роботи системи

Розглянемо детальніше, які дані можна отримувати за допомогою розроблюваної кіберфізичної системи для захисту об’єктів критичної інфраструктури (рисунок 3.4).

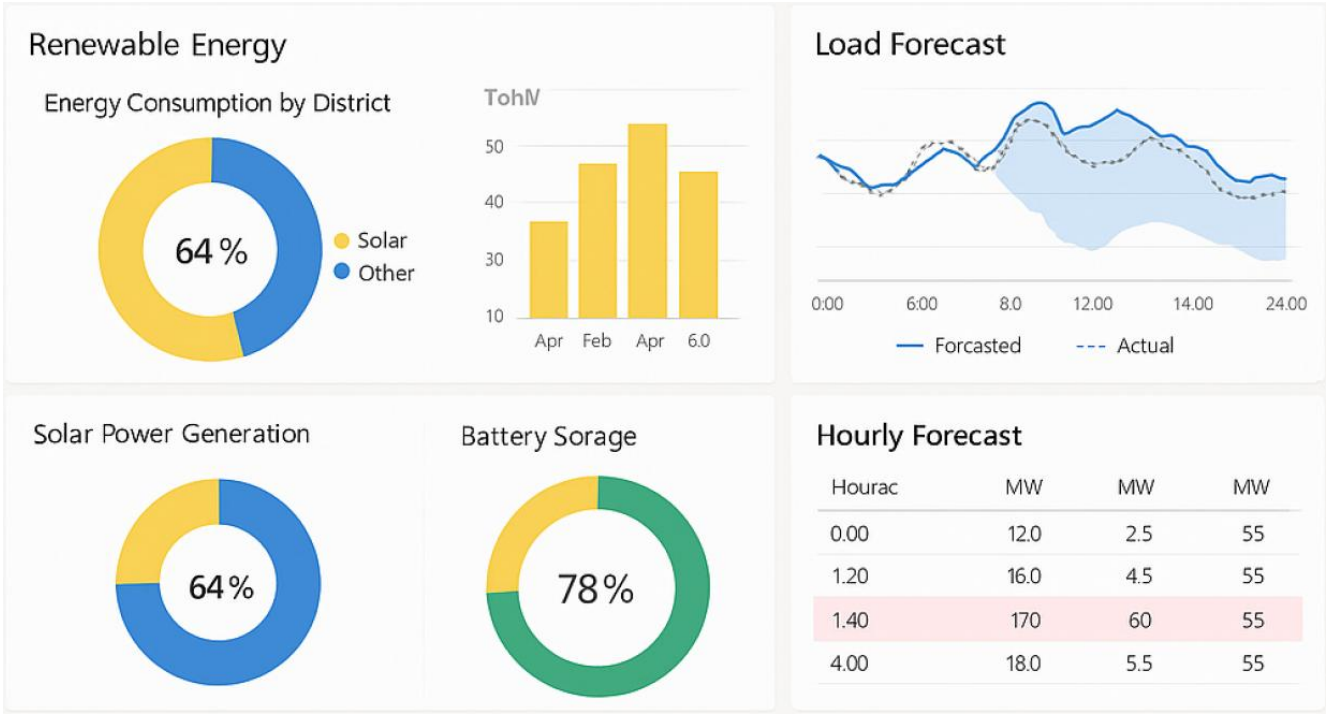



Рисунок 3.4 – Візуалізація показників

Наприклад, оперативна панель енергомережі дає інформацію про наступне:

– карта станцій, тобто активні тривоги, аварії, попередження, тощо;

– графік навантаження трансформаторів;

– smart alarms, тобто дані про напругу, частоту, коефіцієнт потужності.

Споживання енергії по сегментах, наприклад:

– теплові карти по кварталах/районах;

– тренди споживання по часу (день/тиждень/місяць);

– порівняння по таких показниках, як комерційний, побутовий, промисловий сегмент.

ВДЕ-вклад (Solar, Wind Input Dashboard) показує потужність генерації в реальному часі; вклад в загальний баланс та накопичення енергії (батареї):

заряд/розряд.

AI-прогноз навантаження (Forecast Dashboard) демонструє прогноз на добу/тиждень; відхилення від реального навантаження та рекомендовані дії (DR – demand response).

До показників ефективності (Grid KPIs) відносяться наступні:

- SAIDI/SAIFI (середня тривалість/кількість перерв);
- втрати енергії по лініях;
- відсоток аварій з автоматичним відновленням.

## 3.4. Висновки до третього розділу

Розробка архітектури, апаратного й програмного забезпечення кіберфізичних систем для захисту об’єктів критичної інфраструктури, таких як розумні електромережі, є складним інженерним процесом, який вимагає тісної інтеграції між фізичним і цифровим рівнями. В основі архітектури лежить модульна побудова: система розділяється на незалежні, але взаємопов’язані функціональні блоки, кожен з яких виконує конкретне завдання від збору даних до прийняття рішень та виконання дій. На фізичному рівні визначаються ключові вузли (підстанції), точки генерації, об'єкти споживання та обираються відповідні сенсори й виконавчі пристрої. Ретельно підбирається апаратне забезпечення з урахуванням вимог до надійності, енергоспоживання, швидкодії та стійкості до зовнішніх факторів. На базовому рівні це мікроконтролери, PLC, промислові шлюзи, що обробляють сигнали в реальному часі.

Програмне забезпечення, своєю чергою, розробляється з урахуванням багаторівневої логіки, від локальної (edge) обробки на вузлах до централізованої координації через SCADA-системи та аналітичні платформи. У розробці застосовуються сучасні парадигми, такі як, гібридні моделі, що поєднують правила та ML алгоритми, контейнеризація (Docker), протокольна сумісність (IEC 61850, MQTT, Modbus), кіберзахист. Особлива увага приділяється забезпеченню

безперервності та автономності, оскільки система повинна залишатися працездатною навіть за втрати зв’язку чи часткових відмов. Тестування архітектури проходить на основі симуляцій, прототипування, а згодом через «м’який запуск» із реальними вузлами.

Таким чином, комплексна інтеграція апаратних компонентів і програмної логіки формує розумну інфраструктуру, здатну працювати стабільно, передбачувано і безпечно в умовах високої відповідальності.

# ВИСНОВКИ

У роботі за результатами виконаних теоретичних та практичних досліджень було розроблено кібкрфізичну систему для захисту об’єктів критичної інфраструктури на прикладі системи Smart Grid.

У першому розділі проведено аналіз загроз та ризиків, які виникають в об’єктах критичної інфраструктури, зокрема в Smart Grid. Сучасні розумні електромережі є відповіддю на глобальні виклики, пов’язані з підвищеним енергоспоживанням, нестабільністю джерел живлення та необхідністю екологічної трансформації. На відміну від традиційних систем, Smart Grid базується на цифрових технологіях, автоматизації, двосторонній комунікації та активній участі споживача. В основі цієї концепції лежить інтеграція відновлюваних джерел енергії, інтелектуальне управління та гнучкість у реагуванні на зміни попиту.

Проведений огляд підтвердив, що Smart Grid не є лише модернізацією старої мережі, а являє собою нову енергетичну екосистему. Основні її компоненти – це Smart Meters, SCADA-системи, IoT-пристрої, автоматизовані підстанції та розподілені джерела енергії, що працюють синхронно для досягнення високої ефективності та надійності.

Разом з тим, зростання рівня цифровізації супроводжується появою нових ризиків і загроз. До найбільш критичних належать кібератаки на інфраструктурні вузли (SCADA, диспетчерські центри), втручання в роботу Smart Meters, або порушення в ланцюгах постачання. Комбінація фізичних і кіберзагроз може мати катастрофічні наслідки, тому важливо використовувати моделі оцінки загроз, як-от STRIDE, а також впроваджувати криптографію, моніторинг, сегментацію мереж і навчання персоналу.

У другому розділі виконано аналіз вимог, які висуваються до кіберфізичних систем захисту об’єктів критичної інфраструктури. Запропоновано багаторівневу архітектуру захисту. Багаторівнева архітектура захисту є критично важливою

складовою забезпечення надійності та стійкості Smart Grid до кіберзагроз. Кожен рівень, від споживача до адміністрування, виконує власні функції безпеки, створюючи комплексну систему захисту енергетичної інфраструктури.

Такий підхід дозволяє запобігати несанкціонованому доступу, забезпечувати цілісність та конфіденційність даних, а також швидко реагувати на потенційні інциденти.

Важливу роль відіграє впровадження сучасних засобів автентифікації, шифрування, моніторингу трафіку та міжмережевих екранів. Безперервне логування подій, багатофакторна автентифікація й контроль дій персоналу підвищують рівень захисту системи в цілому. Окрему увагу необхідно приділяти сегментації мережі та резервному копіюванню, що дозволяє забезпечити відновлення роботи у разі атак.

У третьому розділі представлена розробка архітектури, апаратного й програмного забезпечення кіберфізичних систем для захисту об’єктів критичної інфраструктури, таких як розумні електромережі, є складним інженерним процесом, який вимагає тісної інтеграції між фізичним і цифровим рівнями. В основі архітектури лежить модульна побудова: система розділяється на незалежні, але взаємопов’язані функціональні блоки, кожен з яких виконує конкретне завдання від збору даних до прийняття рішень та виконання дій. На фізичному рівні визначаються ключові вузли (підстанції), точки генерації, об'єкти споживання та обираються відповідні сенсори й виконавчі пристрої. Ретельно підбирається апаратне забезпечення з урахуванням вимог до надійності, енергоспоживання, швидкодії та стійкості до зовнішніх факторів. На базовому рівні це мікроконтролери, PLC, промислові шлюзи, що обробляють сигнали в реальному часі.

Програмне забезпечення, своєю чергою, розробляється з урахуванням багаторівневої логіки, від локальної (edge) обробки на вузлах до централізованої координації через SCADA-системи та аналітичні платформи. У розробці застосовуються сучасні парадигми, такі як, гібридні моделі, що поєднують

правила та ML алгоритми, контейнеризація (Docker), протокольна сумісність (IEC 61850, MQTT, Modbus), кіберзахист. Особлива увага приділяється забезпеченню безперервності та автономності, оскільки система повинна залишатися працездатною навіть за втрати зв’язку чи часткових відмов. Тестування архітектури проходить на основі симуляцій, прототипування, а згодом через «м’який запуск» із реальними вузлами.

Таким чином, комплексна інтеграція апаратних компонентів і програмної логіки формує розумну інфраструктуру, здатну працювати стабільно, передбачувано і безпечно в умовах високої відповідальності.

## ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ


1. Cintuglu M. H., Mohammed O. A., Akkaya, K., Uluagac, A. S. A survey on smart grid cyber-physical system testbeds. *IEEE Communications Surveys & Tutorials*. 2016. Vol.19(1). Pp. 446-464.

2. Yu X., Xue Y. Smart grids: A cyber–physical systems perspective. *Proceedings of the IEEE*. 2016. Vol. 104(5). Pp. 1058-1070.

3. Jha A. V., Appasani B., Ghazali A. N., Pattanayak P., Gurjar D. S., Kabalci E., Mohanta D. K. Smart grid cyber-physical systems: Communication technologies, standards and challenges. *Wireless Networks*, 2021. Vol. 27(4). Pp. 2595-2613.

4. Wang Q., Zhang G., Wen F. A survey on policies, modelling and security of cyber-physical systems in smart grids. *Energy Conversion and Economics*. 2021. Vol. 2(4). Pp. 197-211.

5. Hasan M. K., Habib A. A., Shukur Z., Ibrahim F., Islam S., Razzaque M. A. Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations. *Journal of network and computer applications*. 2023. Vol. 209. Pp.103540.

6. Li B., Lu R., Wang W., Choo K. K. R. Distributed host-based collaborative detection for false data injection attacks in smart grid cyber-physical system. *Journal of Parallel and Distributed Computing*. 2017. Vol. 103. Pp. 32-41.

7. Weerakkody S., Sinopoli B. Challenges and opportunities: Cyber-physical security in the smart grid. *Smart grid control: overview and research opportunities*. 2019. Pp. 257-273.

8. Guo Q., Hiskens I. A., Jin D. K., Su W., Zhang L. Cyber-physical systems in smart grids: Security and operation. *IET Cyber-Physical Systems: Theory & Applications*. 2017. Vol. 2(4). Pp.153-154.

9. Zhang H., Liu B., Wu H. Smart grid cyber-physical attack and defense: A review. *IEEE Access*. 2021. Vol. 9. Pp. 29641-29659.

10. Bhadani U. Smart grids: A cyber–physical systems perspective. *International*

*Research Journal of Engineering and Technology (IRJET)*. 2024. Vol. 11(06). P. 801.

11. Narayanan S. N., Khanna K., Panigrahi B. K., Joshi A. Security in smart cyber-physical systems: a case study on smart grids and smart cars. In *Smart cities cybersecurity and privacy*. 2019. Pp. 147-163. Elsevier.

12. Kumar N., Zeadally S., Misra S. C. Mobile cloud networking for efficient energy management in smart grid cyber-physical systems. *IEEE Wireless Communications*. 2016. Vol. *23*(5). Pp. 100-108.

13. Wadhawan Y., AlMajali A., Neuman C. A comprehensive analysis of smart grid systems against cyber-physical attacks. *Electronics*. 2018. Vol. 7(10). P. 249.

14. Leitao P., Karnouskos S., Ribeiro L., Lee J., Strasser T., Colombo A. W. Smart agents in industrial cyber–physical systems. *Proceedings of the IEEE*. 2016. Vol. 104(5). Pp. 1086-1101.

15. Osman N. F. M., Elamin A. A. A., Ahmed E. S. A., Saeed R. A. Cyber-physical system for smart grid. In *Artificial intelligence paradigms for smart cyber-physical systems*. 2021. Pp. 301-323.

16. Zhu Y., Wen H., Zhao R., Jiang Y., Liu Q., Zhang P. Research on data poisoning attack against smart grid cyber–physical system based on edge computing. *Sensors*. 2023. Vol. 23(9). P. 4509.

17. Alrowaili Y., Saxena N., Srivastava A., Conti M., Burnap P. A review: Monitoring situational awareness of smart grid cyber-physical systems and critical asset identification. *IET Cyber-Physical Systems: Theory & Applications*. 2023. Vol. 8(3). Pp. 160-185.

18. Haggi H., Song M., Sun W. A review of smart grid restoration to enhance cyber-physical system resilience. *2019 IEEE Innovative Smart Grid Technologies-Asia (ISGT Asia)*. 2019. Pp. 4008-4013.

19. You M., Liu Q., Sun H. New communication strategy for spectrum sharing enabled smart grid cyber-physical system. *IET Cyber-Physical Systems: Theory & Applications*. 2017. Vol. 2(3). Pp. 136-142.

20. Haggi H., Song M., Sun W. A review of smart grid restoration to enhance

cyber-physical system resilience. *2019 IEEE Innovative Smart Grid Technologies-Asia (ISGT Asia)*. 2019. Pp. 4008-4013.

21. Jha A. V., Ghazali A. N., Appasani B., Mohanta D. K. Risk identification and risk assessment of communication networks in smart grid cyber-physical systems. *Security in Cyber-Physical Systems: Foundations and Applications*. 2021. Pp. 217-253.

22. Jha A. V., Appasani B., Ghazali A. N., Bizon N. A comprehensive risk assessment framework for synchrophasor communication networks in a smart grid cyber physical system with a case study. *Energies*. 2021. Vol. 14(12). P. 3428.

23. Manias D. M., Sabe, A. M., Radaideh M. I., Gaber A. T., Maniatakos M., Zeineldin H., El-Saadany E. F. Trends in Smart Grid Cyber-Physical Security: Components, Threats and Solutions. *IEEE Access*. 2024.

24. Chen B., Wang J., Shahidehpour M. Cyber–physical perspective on smart grid design and operation. *IET Cyber-Physical Systems: Theory & Applications*. 2018. Vol. 3(3). Pp. 129-141.

25. Li B., Lu R., Xiao G. *Detection of False Data Injection Attacks in Smart Grid Cyber-Physical Systems*. 2020. Springer.

26. Li H. Communications for control in cyber physical systems: theory, design and applications in smart grids. 2016. Morgan Kaufmann.

27. Sharma G. A survey on secure communication technologies for smart grid cyber physical system. *e-Prime-Advances in Electrical Engineering, Electronics and Energy*. 2024. Vol. 10. P. 100831.

28. Gavriluta C., Boudinet C., Kupzog F., Gomez-Exposito A., Caire R. Cyber-physical framework for emulating distributed control systems in smart grids. *International journal of electrical power & energy systems*. 2020. Vol. 114. P.105375.

29. Hasan M. K., Abdulkadir R. A., Islam S., Gadekallu T. R., Safie N. A review on machine learning techniques for secured cyber-physical systems in smart grid networks. *Energy Reports*. 2024. Vol. 11. Pp. 1268-1290.

30. Xu L., Guo Q., Yang T., Sun H. Robust routing optimization for smart grids considering cyber-physical interdependence. *IEEE Transactions on Smart Grid*. 2018. Vol. 10(5). Pp. 5620-5629.

31. Nuruzzaman M., Rana S. IOT-enabled condition monitoring in power distribution systems: a review of SCADA-based automation, real-time data analytics, and cyber-physical security challenges. *Journal of Sustainable Development and Policy*. 2025. Vol. 1(01). Pp. 25-43.

32. Borlase S., Fan J., Feng X., Giri J., Wilson D., Gray G. R., Tournier J. C. Real-Time Grid Management. In *Smart Grids*. 2017. Pp. 179-252. CRC Press.

33. De Lange R., Van Den Berg C., Van Rooyen R., Rudolph J., Singh N. Smart Monitoring and Control Systems for Rural Microgrids. In *2024 IEEE PES/IAS PowerAfrica*. 2024. Pp. 1-5.

34. Zhang Y., Chen Z., Ma K., Chen F. A decentralized IoT architecture of distributed energy resources in virtual power plant. *IEEE Internet of Things Journal*. 2022. Vol. 10(10). Pp. 9193-9205.

35. Chen S., Ebe F., Morris J., Lorenz H., Kondzialka C., Heilscher G. Implementation and test of an IEC 61850-based automation framework for the automated data model integration of DES (ADMID) into DSO SCADA. *Energies*. 2022. Vol. 15(4). P. 1552.

36. Bani-Ahmed A., Nasiri A., Stamenkovic I. Foundational support systems of the smart grid: State of the art and future trends. *International Journal of Smart Grid*. 2018. Vol. 2(1). Pp. 1-12.

37. Švenda G., Kanjuh S. Engineering Aspects of Implementation of Distribution State Estimator. In *Experiences on Use of State Estimator in Power System Operations*. 2024. pp. 125-166. Cham: Springer International Publishing.

38. Shahinzadeh H., Azani S., Baghernezhad A., Mehrabani-Najafabadi S., Gharehpetian G. B., Jurado F. Cyber Threats and Resilience in Smart Grids and Microgrids: A Cybersecurity Perspective on Challenges and Innovations. In *2024 19th Iranian Conference on Intelligent Systems (ICIS)*. 2024. Pp. 299-308).

39. Barghouti A. A distributed trust model simulator for energy grid of things distributed energy resource management system. 2022.

40. Tightiz L., Yang H. A comprehensive review on IoT protocols' features in smart grid communication. *Energies*. 2020. Vol. 13(11). P. 2762.

41. Emmanuel M., Rayudu R. Communication technologies for smart grid applications: A survey. *Journal of Network and Computer Applications*. 2016. Vol. 74. Pp. 133-148.

42. Baimel D., Tapuchi S., Baimel N. Smart grid communication technologies-overview, research challenges and opportunities. In *2016 International Symposium on Power Electronics, Electrical Drives, Automation and Motion (SPEEDAM)*. 2016. Pp. 116-120.

43. Goudos S. K., Sarigiannidis P., Dallas P. I., Kyriazakos S. Communication protocols for the IoT-based smart grid. In *IoT for Smart Grids: Design Challenges and Paradigms*. 2018. Pp. 55-83. Cham: Springer International Publishing.

44. Kabalci Y. A survey on smart metering and smart grid communication. *Renewable and Sustainable Energy Reviews*. 2016. Vol. 57. Pp. 302-318.

45. Baimel D., Tapuchi S., Baimel N. Smart grid communication technologies. *Journal of Power and Energy Engineering*. 2016. Vol. 4(08). P. 1.

46. Rekik S., Baccour N., Jmaiel M., Drira K. Wireless sensor network based smart grid communications: Challenges, protocol optimizations, and validation platforms. *Wireless Personal Communications*. 2017. Vol. 95. Pp. 4025-4047.

47. Kong P. Y. A review of quantum key distribution protocols in the perspective of smart grid communication security. *IEEE Systems Journal*. 2020. Vol. 16(1). Pp. 41-54.

48. Rehmani M. H., Davy A., Jennings B., Assi C. Software defined networks-based smart grid communication: A comprehensive survey. *IEEE Communications Surveys & Tutorials*. 2019. Vol. 21(3). Pp. 2637-2670.

49. Tsampasis E., Bargiotas D., Elias C., Sarakis L. Communication challenges in

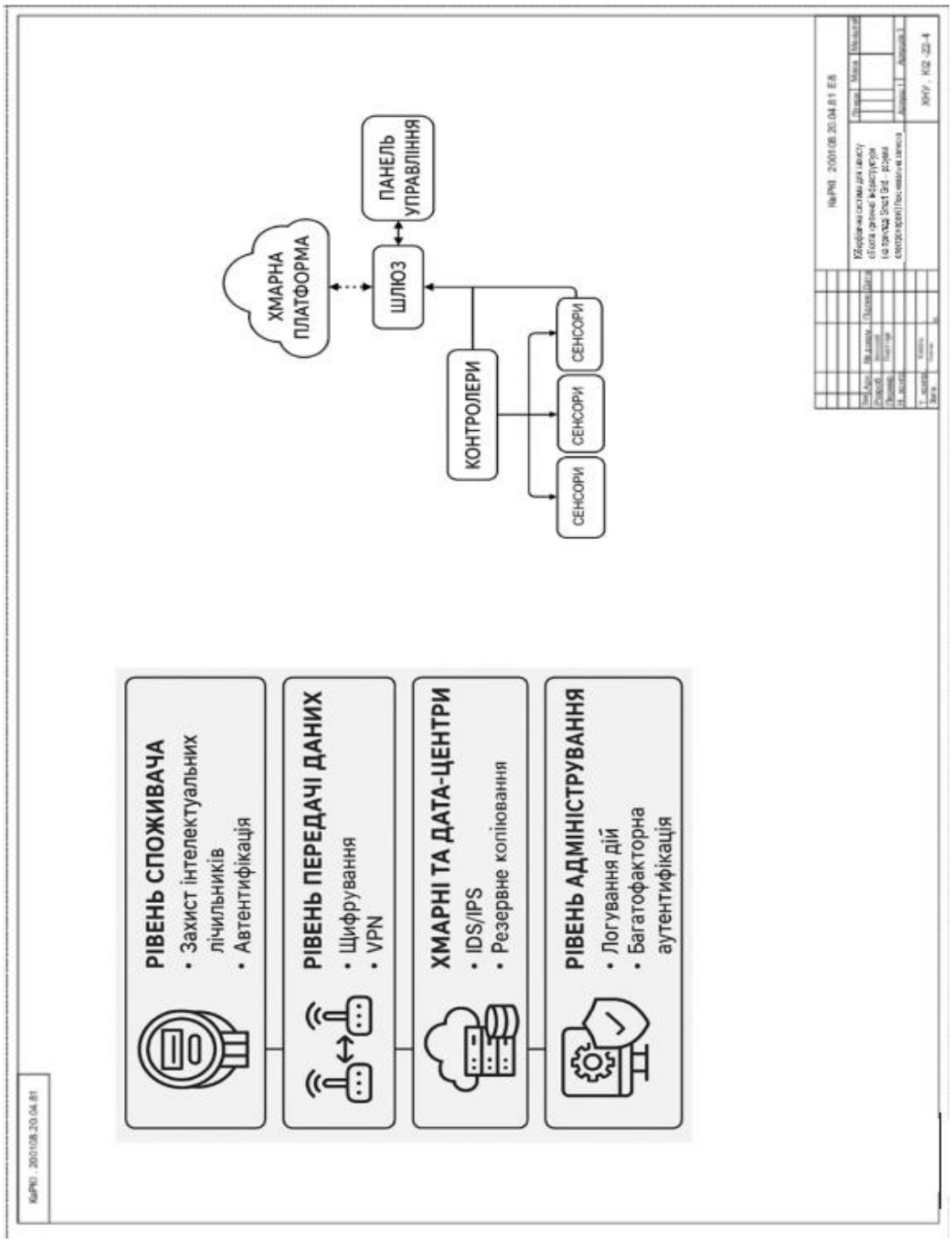
smart grid. In *MATEC web of conferences*. 2016. Vol. 41. P. 01004.

50. Nafi N. S., Ahmed K., Gregory M. A., Datta M. A survey of smart grid architectures, applications, benefits and standardization. *Journal of Network and Computer Applications*. 2016. Vol. 76. Pp. 23-36.

**Додаток А**

(обов’язковий)

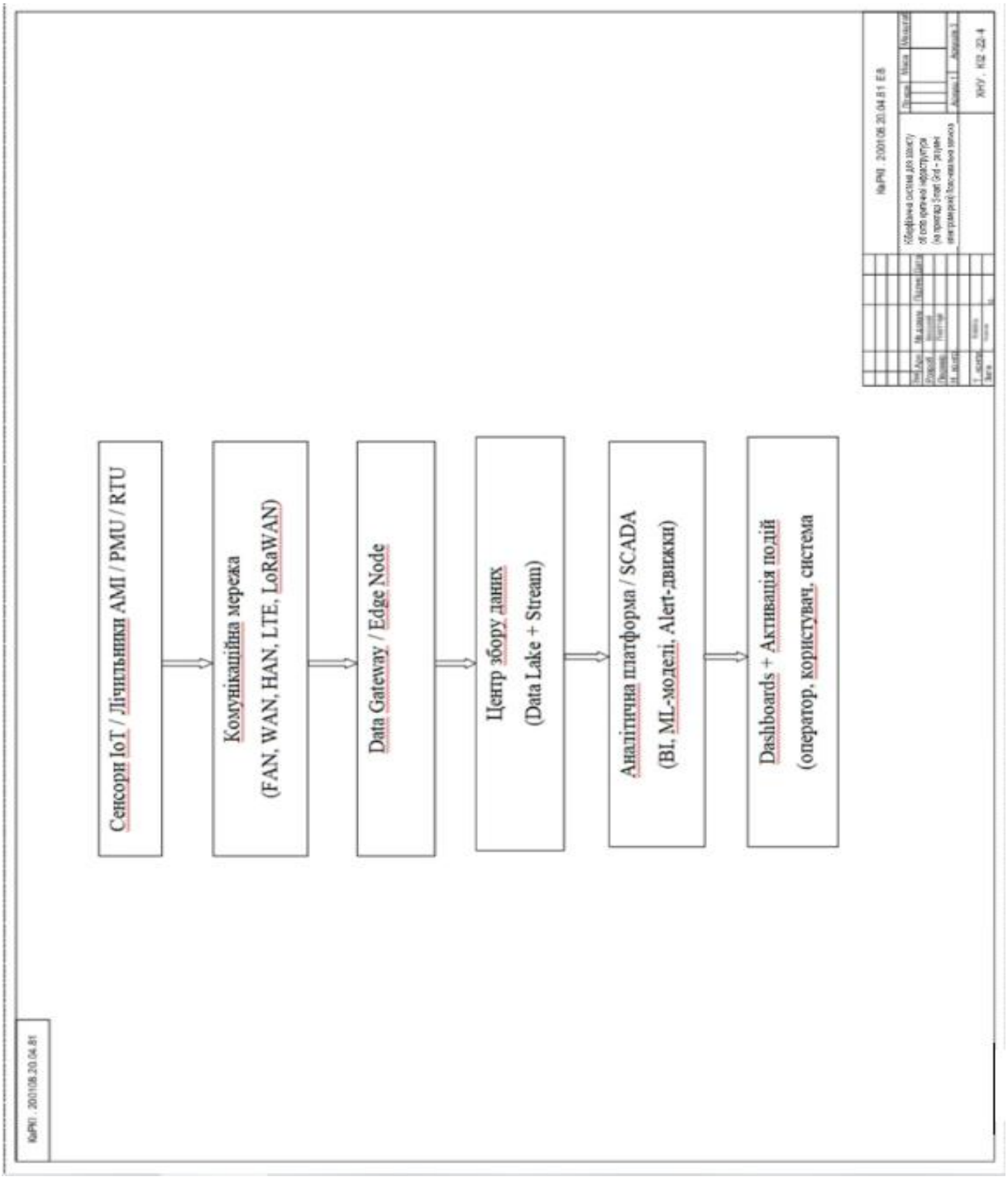
## КОПІЯ КРЕСЛЕННЯ «АРХІТЕКТУРА КІБЕРФІЗИЧНОЇ СИСТЕМИ»



**Додаток Б**

(обов’язковий)

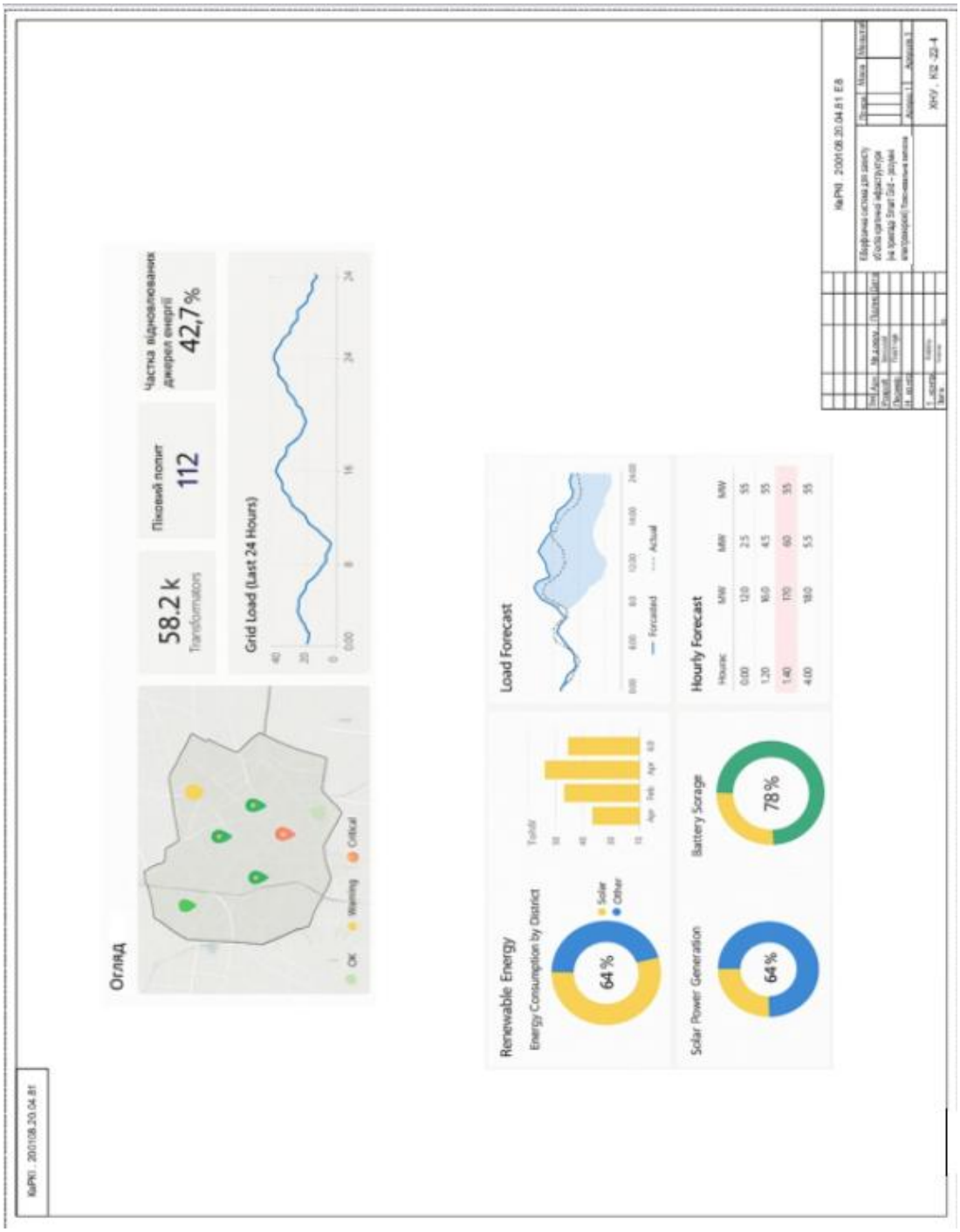
**КОПІЯ КРЕСЛЕННЯ «АРХІТЕКТУРА КІБЕРФІЗИЧНОЇ СИСТЕМИ SMART GRID»**



**Додаток В**

(обов’язковий)

# КОПІЯ КРЕСЛЕННЯ «РЕЗУЛЬТАТИ РОБОТИ КІБЕРФІЗИЧНОЇ СИСТЕМИ»



**Протокол аналізу звіту подібності експертом**

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

**Автор:** Віктор ЗЕМСЬКИЙ

**Співавтор:**

**Назва:** Земський_Кіберфізична система для захисту об'єктів критичної інфраструктури (на прикладі Smart Grid – розумні електромережі)

**Експерт:**

**Підрозділ:** Кафедра комп'ютерної інженерії та інформаційних систем

**Коефіцієнт подібності 1:**4.9%

**Коефіцієнт подібності 2:**2.2%

**Мікропробіли:** 64

**Заміна букв:** 0

**Інтервали:** 0

**Білі знаки:** 0

**Дата створення звіту:** 2025-06-15 07:30:58.0

**Після аналізу Звіту подібності констатую наступне:**

☒ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

2025-06-15 Доцент Андрій Нічепорук

*Дата* експерт

Sun Jun 15 08:23:18 EEST 2025, Медзатий Дмитро Миколайович, Хмельницький національний університет, ХНУ

# Anti-Plagiarism (UA) v-15.281 Educational

**The maximum coincidence with one document 0.0%**

Dictionaries check: en_US, ru_RU, ua_UA. **Errors in the documents: 11%**

| | Document | | Sum coincidence on the DB | |
|---|---|---|---|---|
| | Symbols | Lexemes | Symbols | Lexemes |
| ID: 245907<br>Title: БКР Кіберфізична система для захисту об'єктів критичної інфраструктури (на прикладі Smart Grid – розумні електромережі)<br>Added in a DB: 2025-06-15<br>Authors: Віктор ЗЕМСЬКИЙ<br>Heads: Єлизавета ГНАТЧУК<br>Consultants:<br>Opponents: | 104232 | 898 | 1013 (1%) | 15 (2%) |

Plagiarism sources

| ID | Description | Plagiarism presence in the document | |
|---|---|---|---|
| | | Symbols | Lexemes |

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

# РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дипломник: Земський Віктор Романович

Тема: Кіберфізична система для захисту об'єктів критичної інфраструктури (на прикладі Smart Grid – розумні електромережі)

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг кваліфікаційної роботи:

Кількість листів креслень ___3____ Кількість сторінок записки ___60___

1. Короткий зміст роботи та прийнятих рішень: Метою кваліфікаційної роботи є підвищення рівня захисту об'єктів критичної інфраструктури на прикладі Smart Grid (розумних електромереж) шляхом створення кіберфізичної системи для захисту об'єктів критичної інфраструктури.

2. Висновок про відповідність роботи дипломному завданню: Робота повністю відповідає поставленому завданню.

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У межах розділу 1 проведено аналіз загроз та ризиків, які виникають в об'єктах критичної інфраструктури, зокрема в Smart Grid. Сучасні розумні електромережі є відповіддю на глобальні виклики, пов'язані з підвищеним енергоспоживанням, нестабільністю джерел живлення та необхідністю екологічної трансформації. На відміну від традиційних систем, Smart Grid базується на цифрових технологіях, автоматизації, двосторонній комунікації та активній участі споживача. В основі цієї концепції лежить інтеграція відновлюваних джерел енергії, інтелектуальне управління та гнучкість у реагуванні на зміни попиту. У межах розділу 2 проведено аналіз вимог, які висуваються до кіберфізичних систем захисту об'єктів критичної інфраструктури. Запропоновано багаторівневу архітектуру захисту. Багаторівнева архітектура захисту є критично важливою складовою забезпечення надійності та стійкості Smart Grid до кіберзагроз. Кожен рівень, від споживача до адміністрування, виконує власні функції безпеки, створюючи комплексну систему захисту енергетичної інфраструктури. В 3му розділі

була здійснена розробка архітектури, апаратного й програмного забезпечення кіберфізичних систем для захисту об'єктів критичної інфраструктури, таких як розумні електромережі, в тісній інтеграції між фізичним і цифровим рівнями.

4. Позитивні сторони роботи: Загалом, проведені дослідження свідчать про перспективність запропонованої системи, комплексна інтеграція апаратних компонентів і програмної логіки формує розумну інфраструктуру, здатну працювати стабільно, передбачувано і безпечно в умовах високої відповідальності.

5. Негативні сторони роботи: недостатня увага приділена огляду існуючих рішень в сфері захисту розумних електромереж.

6. Оцінка графічного оформлення та пояснювальної записки роботи: Пояснювальна записка оформлена коректно, згідно діючих стандартів оформлення документації.

7. Відгук про роботу в цілому: Робота виконана на достатньому технічному рівні.

8. Інші зауваження: _____

9. Оцінка дипломної роботи: задовільно D (3,50)

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) Онищко Оксана Григорівна, к. пед. наук, доцент ІПЗ, УНУ

"___"_____2025 р. _____(підпис)

Завідувачу кафедри КІІС
д-р. філософії, доц. Ользі ПАВЛОВІЙ

Віктора ЗЕМСЬКОГО
ПІБ здобувача вищої освіти

ФІТ, 4 курсу, групи КІ2-21-4

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 01.07.2022, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений(а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Strike-Plagiarism та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

13 червня 2025 року

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ

КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Кіберфізична система для захисту об'єктів критичної інфраструктури (на прикладі Smart Grid – розумні електромережі)

Автор: Віктор ЗЕМСЬКИЙ

Спеціальність: 123– Комп'ютерна інженерія

Освітня програма: освітньо-професійна

Науковий керівник: Єлизавета ГНАТЧУК, д.т.н., професор

Після аналізу звіту подібності зроблено такий висновок:

| № | Висновок | Позначка про відповідність |
|---|---|---|
| 1 | Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту. | відповідає |
| 2 | Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи | |
| 3 | Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат. | |
| 4 | Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту. | |

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
2) окремі виявлені збіги є загальновживаними фразами або виразами;
3) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів, що не є модифікацією тексту.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості StrikePlagiarism, складає 4.92% і адресується до 1 першоджерела; та системою Anti-Plagiarism складає 0%, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ Єлизавета ГНАТЧУК

Гарант ОП _____ Сергій ЛИСЕНКО

Завідувач кафедри КІІС _____ Ольга ПАВЛОВА