МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПОЛІСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
Факультет інженерії та енергетики
Кафедра електрифікації, автоматизації виробництва та інженерної екології

Кваліфікаційна робота
на правах рукопису

Дячук Артем Сергійович

УДК 621.359.4

КВАЛІФІКАЦІЙНА РОБОТА

Обґрунтування шляхів підвищення стійкості енергетичної системи м. Житомир в умовах зовнішньої військової загрози
(тема роботи)

141 «Електроенергетика, електротехніка та електромеханіка»
(шифр і назва спеціальності)

Подається на здобуття освітнього ступеня бакалавр

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
Дячук А.С.
(підпис, ініціали та прізвище здобувача вищої освіти)

Керівник роботи

Цивенкова Н.М.
(прізвище, ім'я, по батькові)
к.т.н., доцент
(науковий ступінь, вчене звання)

Житомир – 2025

АНОТАЦІЯ

Дячук А.С. Обґрунтування шляхів підвищення стійкості електромереж в умовах зовнішньої військової загрози. – Кваліфікаційна робота на здобуття освітнього ступеня бакалавра за спеціальністю 141 Електроенергетика, електротехніка та електромеханіка, освітньою програмою «Енергетика». – Поліський національний університет, Житомир, 2025 рік.

Мета роботи: обґрунтування комплексу шляхів та заходів, спрямованих на підвищення стійкості електромереж України в умовах військової загрози.

Предмет дослідження: теоретичні, методичні та практичні аспекти обґрунтування шляхів підвищення спроможності електромереж протистояти руйнуванням, адаптуватися до змінених умов, мінімізувати негативні наслідки.

Ключові слова: військова загроза, децентралізація, енергетична безпека, кібербезпека, критична інфраструктура, мікро мережі, резервування, стійкість електромереж, фізичний захист.

SUMMARY

Diachuk A.S. Justification of Ways to Enhance the Resilience of Power Grids under Conditions of External Military Threat. – Bachelor's Thesis for the degree in specialty 141 Electrical Power Engineering, Electrical Engineering, and Electromechanics, educational program "Power Engineering". – Polissia National University, Zhytomyr, 2025.

Objective: To justify a set of ways and measures aimed at enhancing the resilience of Ukraine's power grids under conditions of military threat.

Subject of Research: Theoretical, methodological, and practical aspects of justifying ways to enhance the capability of power grids to withstand destruction, adapt to changed conditions, and minimize negative consequences.

Keywords: military threat, decentralization, energy security, cybersecurity, critical infrastructure, microgrids, redundancy, power grid resilience, physical protection.

ЗМІСТ

ВСТУП

Актуальність теми. Електроенергетична система є однією з найважливіших складових критичної інфраструктури сучасної держави, фундаментом її економічного розвитку, соціальної стабільності. Надійне та безперебійне функціонування електромереж забезпечує життєдіяльність суспільства, промисловості, транспорту, зв'язку, медичних та освітніх закладів.

Цілеспрямовані удари мають руйнівний характер, призводячи до масштабних пошкоджень обладнання, тривалих відключень електроенергії для мільйонів споживачів, виникнення гуманітарних проблем та завдання колосальних економічних збитків державі. Процес відновлення пошкоджених об'єктів є надзвичайно складним, потребує значних фінансових, матеріально-технічних та людських ресурсів, а також тривалого часу, що додатково ускладнюється постійною загрозою повторних ударів. У таких умовах виникає нагальна потреба у переході від переважно ситуативного реагування та аварійного ремонту до фундаментального, системного підходу, спрямованого на підвищення стійкості (resilience) електромереж до зовнішніх руйнівних впливів. Таким чином, наукове дослідження та технічне обґрунтування ефективних шляхів зміцнення енергетичної інфраструктури, підвищення її здатності протистояти атакам, мінімізувати їх наслідки та швидко відновлювати функціональність набуває виняткової актуальності та є критично важливим завданням для забезпечення національної безпеки, сталого функціонування економіки та життєдіяльності України в умовах війни та у повоєнний період.

Метою роботи є комплексне обґрунтування науково-технічних та організаційних шляхів і заходів, спрямованих на підвищення стійкості електромереж України в умовах зовнішньої військової загрози.

Для досягнення поставленої мети в кваліфікаційній роботі вирішуються такі ***завдання***:

- проаналізувати сучасний стан електроенергетичної системи України та

детально охарактеризувати типи зовнішніх військових загроз для її об'єктів;

- визначити та систематизувати основні вразливості ключових елементів електромереж до впливу факторів військової агресії;
- узагальнити релевантний вітчизняний та світовий досвід забезпечення стійкості критичної інфраструктури в умовах надзвичайних ситуацій воєнного характеру;
- розглянути загальні організаційно-технічні підходи до підвищення рівня захищеності та надійності функціонування електромереж;
- запропонувати та обґрунтувати конкретні технічні, технологічні та організаційні заходи для підвищення стійкості українських електромереж, адаптовані до сучасних викликів;
- провести попередню оцінку потенційної ефективності запропонованих шляхів та заходів.

Об'єкт дослідження: процес забезпечення функціонування та підвищення рівня стійкості національної електроенергетичної системи України в умовах дестабілізуючого впливу зовнішніх військових загроз.

Предмет дослідження: теоретичні основи, методичні підходи та практичні рішення щодо обґрунтування шляхів підвищення спроможності електромереж протистояти руйнуванням, адаптуватися до змінених умов, мінімізувати негативні наслідки та забезпечувати швидке відновлення функціональності.

Методи досліджень. Для вирішення поставлених завдань у роботі використано комплекс загальнонаукових та спеціальних методів дослідження, зокрема: системний аналіз – для вивчення електромережі як складної взаємопов'язаної системи та її вразливостей; порівняльний аналіз – для вивчення та адаптації міжнародного досвіду; методи логічного аналізу і синтезу – для обробки інформації, виявлення причинно-наслідкових зв'язків, ідентифікації проблем та розробки пропозицій; а також методи експертних оцінок та

прогнозування – для обґрунтування доцільності та потенційної ефективності.

Практичне значення одержаних результатів. Практична цінність отриманих у роботі результатів полягає у можливості їх застосування проектними організаціями при розробці проектів модернізації та захисту енергооб'єктів, енергетичними компаніями (операторами системи передачі та розподілу) при формуванні планів розвитку та інвестиційних програм, а також органами державної влади та місцевого самоврядування при розробці галузевих програм підвищення стійкості, формуванні планів реагування на надзвичайні ситуації воєнного характеру та при оновленні відповідної нормативно-технічної документації. Впровадження обґрунтованих у роботі рішень сприятиме підвищенню надійності електропостачання, зменшенню збитків від ворожих атак та зміцненню загальної безпеки держави.

Перелік публікацій автора за темою дослідження:

1. Дячук А. С.
КОМПЛЕКСНИЙ ЗАХИСТ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ:
ФІЗИЧНА БЕЗПЕКА, КІБЕРСТІЙКІСТЬ ТА МОДЕРНІЗАЦІЯ
«СТУДЕНТСЬКІ ЧИТАННЯ – 2024» ПОЛІСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ 31 жовтня 2024 року м. Житомир
2. Дячук А. С.
ПІДВИЩЕННЯ СТІЙКОСТІ ЕНЕРГОСИСТЕМИ ЧЕРЕЗ ДЕЦЕНТРАЛІЗАЦІЮ, ДИВЕРСИФІКАЦІЮ ТА ВПРОВАДЖЕННЯ МІКРОМЕРЕЖ
НАУКОВІ ЧИТАННЯ за підсумками І-го туру Всеукраїнського конкурсу студентських наукових робіт з галузей знань і спеціальностей НАДІЙНОСТІ ЕНЕРГОСИСТЕМИ 23 квітня 2025 р. м. Житомир

РОЗДІЛ 1
АНАЛІЗ СТАНУ ТА ОСОБЛИВОСТІ БУДОВИ ЕЛЕКТРОМЕРЕЖ УКРАЇНИ

1.1. Будова сучасної електроенергетичної системи

Електроенергетична система України (Об'єднана енергетична система, далі - ОЕС) є складним технологічним комплексом, призначеним для виробництва, передачі та розподілу електричної енергії споживачам на всій території країни. Її стабільне функціонування є запорукою національної безпеки, економічного розвитку та соціальної стабільності. До повномасштабного вторгнення ОЕС України була однією з найбільших та найпотужніших у Східній Європі, синхронізованою з енергосистемами пострадянських країн. У березні 2022 року відбулася історична подія – синхронізація ОЕС України з континентальною європейською енергосистемою ENTSO-E, що значно підвищило її потенційну стійкість та можливості для взаємодопомоги.

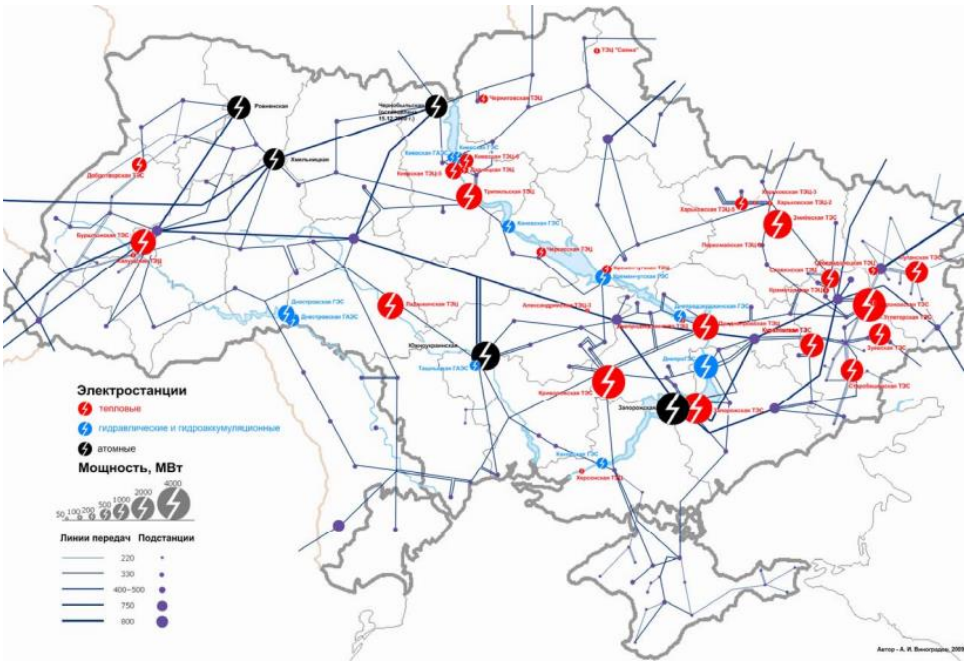

Рис. 1.1 Структурна схема енергосистеми України [6]

Таблиця, представлена в Додатку А

Об'єднана енергетична система України включає електростанції для виробництва енергії, електричні мережі для її передачі та розподілу, а також системи управління, що забезпечують її стабільну роботу.[9]

Особливостями ОЕС України, що впливають на її стійкість, є значна територіальна протяжність, певна централізація генерації та управління, а також наявність критично важливих вузлів (великі ПС, АЕС, магістральні ЛЕП), пошкодження яких може мати системні наслідки.

1.2. Типи зовнішніх військових загроз та їх потенційний вплив на об'єкти електромереж

Повномасштабна військова агресія проти України продемонструвала широкий спектр загроз, що застосовуються для ураження об'єктів критичної інфраструктури, зокрема електромереж. Ці загрози можна класифікувати наступним чином:

Рис. 1.2 Фото. Уражений трансформатор підстанції крилатою ракетою [15]

Таблиця, представлена в Додатку Б

Потенційний вплив цих загроз є руйнівним:

- Пряме фізичне знищення або пошкодження обладнання (трансформаторів, генераторів, ЛЕП), що потребує тривалого та дороговартісного ремонту або заміни.
- Втрата генеруючих потужностей, що призводить до дефіциту електроенергії в системі.
- Порушення цілісності мережі, "розриви" зв'язків між регіонами, що ускладнює передачу енергії та балансування системи.
- Каскадні аварії, коли пошкодження одного елемента призводить до перевантаження та відключення інших, викликаючи системний збій.
- Втрата керованості системою внаслідок кібератак або руйнування центрів управління.
- Тривалі перерви в електропостачанні споживачів, що має критичні соціальні, економічні та гуманітарні наслідки.

1.3. Аналіз основних вразливостей національних електромереж в контексті воєнних дій

Досвід протистояння військовій агресії виявив низку системних вразливостей українських електромереж. Великі електростанції та вузлові підстанції є габаритними, стаціонарними об'єктами, які важко замаскувати та захистити від потужних кінетичних ударів, при цьому особливо вразливим є унікальне високовольтне обладнання, як-от автотрансформатори 330-750 кВ, виробництво та доставка якого займає тривалий час.[16] Також, оскільки історично мережа розвивалася з певним рівнем централізації, пошкодження кількох ключових магістральних ЛЕП або вузлових підстанцій може призвести до ізоляції окремих регіонів чи великих генеруючих центрів від основної системи, чому сприяє недостатня кількість альтернативних маршрутів передачі енергії в деяких зонах. Додатковою проблемою є те, що значна частина високовольтного обладнання,

зокрема автотрансформатори та елегазові вимикачі, не виробляється в Україні або виробляється в недостатніх обсягах, а залежність від іноземних постачальників та довгі логістичні ланцюги ускладнюють швидке відновлення. Важливим аспектом є кібер вразливості: використання різнорідного обладнання та програмного забезпечення, недостатня сегментація мереж, потенційні вразливості у протоколах зв'язку та операційних системах створюють ризики для успішних кібератак на системи SCADA та РЗА. Не слід забувати і про те, що частина обладнання підстанцій та ЛЕП експлуатується тривалий час і може мати знижену стійкість до зовнішніх впливів, таких як вібрації від вибухів чи уламкові пошкодження, та потребувати частішого ремонту. Окрім технічних аспектів, існує проблема людського фактору та логістики, пов'язана з необхідністю роботи ремонтних бригад в небезпечних умовах, ризиками для життя персоналу та проблемами з доступом до пошкоджених об'єктів у зоні бойових дій або на замінованих територіях. Усі ці вразливості в сукупності визначають чутливість енергосистеми до цілеспрямованих атак і зумовлюють необхідність пошуку комплексних рішень для підвищення її стійкості.

1.4. Поняття стійкості електроенергетичних систем та критерії її оцінки в умовах надзвичайних ситуацій воєнного характеру

Традиційно для оцінки роботи енергосистем використовувалося поняття надійності, що характеризує здатність системи виконувати свої функції (безперебійне постачання електроенергії заданої якості) в нормальних умовах експлуатації. Однак в умовах цілеспрямованих руйнівних впливів, таких як військова агресія, більш доречним та комплексним є поняття стійкості.[16]

Стійкість електроенергетичної системи визначається як її здатність протистояти руйнівним зовнішнім впливам, зокрема військовим, мінімізувати їх наслідки, адаптуватися до змінених умов та швидко відновлювати свою функціональність. Вона включає такі ключові компоненти, як опірність

(Robustness), тобто здатність системи витримувати певний рівень впливу без суттєвої втрати функціональності, наприклад, за рахунок фізичного захисту об'єктів чи використання обладнання підвищеної міцності; резервування (Redundancy), що означає наявність надлишкових елементів або альтернативних шляхів передачі енергії для компенсації виходу з ладу основних; адаптивність (Adaptability/Resourcefulness) – здатність гнучко змінювати структуру та режими роботи у відповідь на пошкодження чи зміну умов, як-от перехід на острівні режими роботи, оперативне перерозподілення потоків потужності чи мобілізація ресурсів; а також швидкість відновлення (Rapidity/Recovery), яка характеризує здатність швидко локалізувати пошкодження, провести ремонтні роботи та відновити електропостачання споживачів. Критерії оцінки стійкості в умовах воєнних дій є багатогранними і можуть охоплювати збереження керованості системою, тобто можливість диспетчерського персоналу контролювати параметри та керувати режимами роботи навіть при часткових пошкодженнях; мінімізацію масштабів та тривалості відключень, особливо для критичної інфраструктури; час відновлення критично важливих об'єктів, таких як ключові електростанції, підстанції та магістральні лінії; здатність окремих частин енергосистеми функціонувати автономно в ізольованих (острівних) режимах; а також оцінку економічних збитків від руйнувань та перерв в електропостачанні.[23] Загалом, оцінка стійкості є складним завданням, що вимагає аналізу багатьох факторів та, потенційно, використання методів моделювання для прогнозування поведінки системи за різних сценаріїв атак.

Висновки по розділу 1

Аналіз стану електроенергетичної системи України та характеру зовнішніх військових загроз дозволяє зробити наступні висновки:

1. ОЕС України є складним, критично важливим комплексом, функціонування якого зазнало безпрецедентного впливу внаслідок

повномасштабної військової агресії. Незважаючи на значні руйнування та втрату частини потужностей, система продемонструвала певну живучість, зокрема завдяки синхронізації з ENTSO-E та зусиллям енергетиків.

2. Військові загрози для електромереж є різноманітними та включають масовані ракетні та дронові атаки, артилерійські обстріли, кібератаки та фізичні диверсії, спрямовані на ключові елементи генерації, передачі та розподілу.
3. Основними вразливостями українських електромереж є фізична відкритість та концентрація ключових вузлів, топологічні обмеження, залежність від імпорту унікального обладнання, потенційні кібер вразливості та зношеність частини фондів.
4. В умовах війни поняття надійності стає недостатнім; ключовою характеристикою є стійкість системи – її здатність протистояти атакам, адаптуватися та швидко відновлюватися. Оцінка стійкості має враховувати здатність системи зберігати керованість, мінімізувати відключення та швидко відновлювати критичні функції.
5. Глибоке розуміння структури енергосистеми, характеру загроз та наявних вразливостей є необхідною передумовою для розробки та обґрунтування ефективних заходів з підвищення її стійкості, що є основним завданням наступних розділів роботи.

РОЗДІЛ 2
ЗАГАЛЬНІ НАПРЯМКИ ТА ПІДХОДИ ДО ПІДВИЩЕННЯ СТІЙКОСТІ ЕЛЕКТРОМЕРЕЖ

2.1. Світовий досвід забезпечення стійкості критичної інфраструктури, зокрема електромереж, в умовах загроз

Після аналізу стану енергосистеми, характеру загроз та ключових вразливостей (Розділ 1), наступним кроком є визначення загальних стратегічних напрямків та підходів, які можуть слугувати основою для розробки конкретних заходів з підвищення стійкості електромереж. Цей розділ розглядає міжнародний досвід, загальні організаційно-технічні заходи, роль ключових стратегічних принципів (резервування, децентралізація, диверсифікація) та нормативно-правове підґрунтя для забезпечення стійкості в умовах зовнішньої військової загрози.[15]

Проблема забезпечення стійкості критичної інфраструктури, включно з електроенергетикою, є актуальною для багатьох країн світу, хоча причини цієї проблеми можуть відрізнятися – від природних катастроф та тероризму до кіберзагроз та військових конфліктів. Аналіз міжнародного досвіду дозволяє виокремити певні загальні тенденції та підходи, які можуть бути адаптовані до українських реалій.

- Ізраїль: Маючи тривалий досвід протистояння ракетним та мінометним обстрілам, Ізраїль приділяє значну увагу фізичному захисту критичних об'єктів (hardening), дублюванню систем управління та сегментації мережі для запобігання каскадним відключенням. Активно використовуються системи раннього попередження та швидкого реагування.
- США: Основний фокус спрямований на підвищення стійкості до екстремальних погодних явищ (урагани, лісові пожежі) та кібератак. Розвиваються концепції "розумних мереж" (Smart Grid), мікромереж

(Microgrids), впроваджуються стандарти кібербезпеки (напр., від NERC - North American Electric Reliability Corporation), розробляються плани відновлення після масштабних збоїв (black start).

- Європейський Союз: Після повномасштабного вторгнення в Україну, ЄС посилив увагу до енергетичної безпеки та захисту критичної інфраструктури. Акцент робиться на диверсифікації джерел енергії, посиленні міждержавних з'єднань, підвищенні кібербезпеки та розробці спільних планів реагування на кризові ситуації.
- Інші регіони: Досвід країн, що пережили збройні конфлікти, часто вказує на важливість децентралізованих рішень, використання мобільних генеруючих установок та підстанцій, а також швидких, хоч і тимчасових, методів ремонту пошкоджених ліній.

Загальні уроки з міжнародного досвіду:

- Необхідність комплексного підходу, що поєднує фізичний захист, кібербезпеку, мережеву топологію та організаційні заходи.
- Важливість проактивного планування: оцінка ризиків, розробка сценаріїв, створення планів дій та їх регулярне тестування (навчання, тренування).
- Тенденція до децентралізації: розвиток розподіленої генерації та мікро мереж для зменшення залежності від великих централізованих вузлів.
- Критична роль інформаційної безпеки та захисту систем управління.
- Необхідність тісної співпраці між операторами інфраструктури, державними органами, військовими та службами надзвичайних ситуацій.

Хоча жоден іноземний досвід не може бути повністю скопійований через унікальність масштабу та характеру загроз в Україні, вивчення міжнародних практик надає цінні ідеї та перевірені концепції для адаптації.[15]

2.2. Загальні організаційно-технічні заходи для підвищення рівня захищеності електроенергетики

Таблиця 2.1 – Загальні організаційно-технічні заходи

Категорія заходу	Захід	Опис
Організаційний	Удосконалення планування та управління ризиками	Регулярна аналізу загроз із урахуванням нових видів озброєнь. Розробка детальних сценаріїв атак та їх наслідків.
	Розробка та впровадження планів стійкості	Створення комплексних планів: превентивні дії під час атаки, відновлення.
	Підготовка та захист персоналу	Регулярні навчання персоналу щодо дій в екстремальних умовах, психологічна підтримка, створення безпечних місць роботи персоналу.
	Міжвідомча координація	Налагодження ефективної взаємодії та обміну інформацією в реальному часі.
	Створення стратегічних запасів	Формування та розосереджене зберігання аварійного запасу критичного обладнання, матеріалів, палива.
	Посилення інформаційної безпеки та доступу	Впровадження суворих політик доступу до об'єктів систем,контроль персоналу, протидія витоку важливої інформації.
Технічний	Елементарний фізичний захист	Системи відеоспостереження, контроль доступу, освітлення периметру.
	Інженерний захист	Зведення захисних споруд навколо критичного обладнання, маскування, заглиблення кабельних ліній.
	Підвищення надійності обладнання	Використання сучасного обладнання з вищими класами стійкості до зовнішніх чинників. Модернізація застарілого обладнання.
	Впровадження системи моніторингу	Системи раннього виявлення пошкоджень, перевантажень, кібератак
	Базові заходи кібербезпеки	Мережева сегментація, , антивірусний захист, оновлення ПЗ, впровадження аутентифікації .

Організаційні заходи охоплюють удосконалення планування управління ризиками, розробку планів стійкості, підготовку персоналу, міжвідомчу координацію, створення стратегічних запасів та посилення інформаційної безпеки.

2.3. Роль резервування, децентралізації та диверсифікації в забезпеченні стійкості електропостачання

Три ключові стратегії є основоположними для побудови стійких систем, зокрема енергетичних: резервування, децентралізація та диверсифікація. Перший принцип, резервування, передбачає створення надлишковості на різних рівнях для забезпечення функціонування системи у разі відмови або пошкодження окремих елементів. Це включає мережеве резервування шляхом будівництва паралельних ліній електропередачі, закільцювання мереж для створення обхідних шляхів, а також дублювання диспетчерських центрів, резервування обладнання через встановлення запасних трансформаторів і вимикачів на підстанціях та використання мобільних підстанцій і резервування живлення шляхом забезпечення об'єктів енергетики та критичних споживачів автономними джерелами, такими як дизель-генератори чи акумуляторні батареї.

Як приклад використання ліній електропередач високої напруги розглянемо спрощену схему енергосистеми, що наведена на (рис. 2.1) [6]

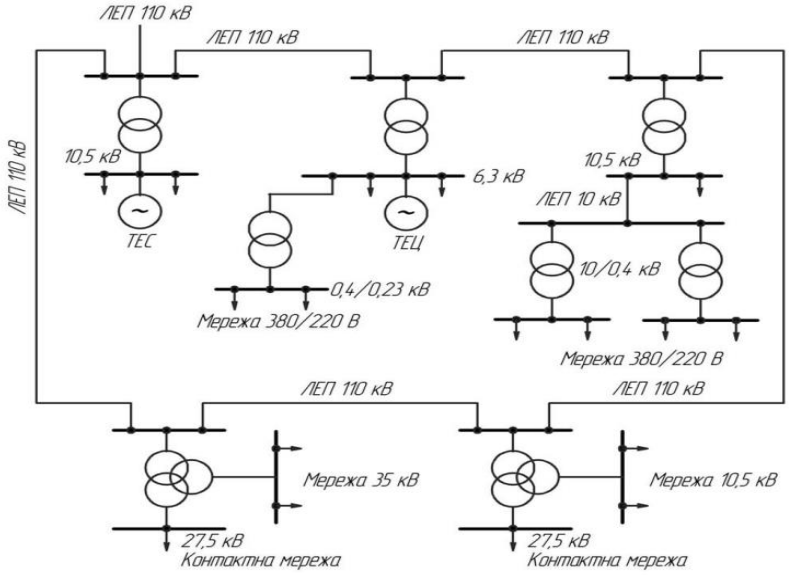

Рис. 2.1 Спрощена однолінійна схема закільцьованої електромережі [6]

Другий принцип, децентралізація, спрямований на зменшення залежності системи від великих централізованих вузлів через розвиток більш розподілених структур. Це досягається стимулюванням розподіленої генерації (СЕС, ВЕС, біогазові установки, когенераційні установки тощо) ближче до споживачів, що зменшує навантаження на магістральні мережі; формуванням мікромереж (Microgrids) – локальних систем, здатних працювати автономно; та розвитком можливостей розподіленого управління частинами енергосистеми з регіональних центрів.[7] Третій принцип, диверсифікація, означає збільшення різноманітності елементів та підходів для зменшення ризику одночасного виходу з ладу багатьох компонентів через спільну причину. Це стосується диверсифікації джерел енергії (збалансований мікс АЕС, ТЕС, ГЕС, ВДЕ), маршрутів транспортування енергії (наявність кількох незалежних коридорів ЛЕП), постачальників критичного обладнання та використовуваних технологій і протоколів зв'язку. Впровадження цих принципів дозволяє створити більш гнучку та живучу енергосистему, здатну краще протистояти цілеспрямованим атакам.

2.4. Нормативно-правові аспекти забезпечення функціонування електромереж в умовах воєнного стану та зовнішніх загроз

Ефективне підвищення стійкості електромереж неможливе без відповідного нормативно-правового забезпечення, яке має враховувати специфіку функціонування критичної інфраструктури в умовах війни. Зокрема, законодавство про воєнний стан визначає особливий режим роботи таких об'єктів, повноваження військового командування та органів влади щодо управління ресурсами, а також забезпечення безпеки та порядку на них. Важливу роль відіграє Закон України "Про критичну інфраструктуру" [7], який встановлює загальні засади її ідентифікації, класифікації та захисту, визначає відповідальність власників і операторів та повноваження державних органів. Однак цей закон потребує подальшої деталізації через розробку та затвердження секторальних вимог, особливо для електроенергетики, з урахуванням специфічних військових ризиків.

На технічному рівні, існуючі стандарти та правила, такі як Правила улаштування електроустановок (ПУЕ), Кодекс системи передачі, Кодекс систем розподілу, ДСТУ та СОУ, потребують перегляду й доповнення.[12] Це необхідно для врахування вимог щодо підвищення фізичної та кібернетичної стійкості, а також для впровадження чітких критеріїв захищеності при проектуванні нових та реконструкції існуючих об'єктів електромереж. Зі свого боку, регуляторні акти Національної комісії, що здійснює державне регулювання у сферах енергетики та комунальних послуг, можуть передбачати тимчасові зміни до правил ринку електроенергії, тарифної політики чи процедур приєднання до мереж, щоб стимулювати впровадження заходів стійкості та розвиток розподіленої генерації.

Окремо варто згадати міжнародне гуманітарне право, зокрема Женевські конвенції та Додаткові протоколи. Хоча МГП передбачає захист цивільних об'єктів, включаючи електростанції та мережі, від прямих атак, практика ведення війни агресором демонструє ігнорування цих норм. Тим не менш, фіксація таких

порушень залишається важливою для документування воєнних злочинів та забезпечення майбутньої відповідальності.

Проблеми та виклики: Необхідність швидкої адаптації нормативної бази до мінливих умов війни, забезпечення виконання вимог в умовах обмежених ресурсів, пошук балансу між вимогами безпеки та економічною доцільністю, гармонізація українського законодавства з європейськими нормами у сфері захисту критичної інфраструктури.

Висновки по розділу 2

Отже, за результатами аналізу загальних напрямків та підходів до підвищення стійкості електромереж можна зробити декілька ключових висновків.

1. Комплексне завдання, що вимагає системного підходу, який інтегрує найкращі світові практики, адаптовані до специфічних українських реалій в умовах військової загрози.
2. Необхідне підґрунтя для стійкості формують загальні організаційно-технічні заходи, включаючи удосконалення планування та управління ризиками, належну підготовку персоналу, ефективну міжвідомчу координацію, створення стратегічних запасів, забезпечення фізичного захисту об'єктів та впровадження базових заходів кібербезпеки.
3. Ключовими для побудови гнучкої та живучої енергосистеми є стратегічні принципи резервування на різних рівнях (мережевому, обладнання, живлення), децентралізації (через розвиток розподіленої генерації та мікро мереж) та диверсифікації: джерел енергії, маршрутів передачі, технологій. Крім того, критично важливим є належне нормативно-правове забезпечення, що враховує специфіку воєнного стану та сучасні загрози, для ефективного впровадження заходів стійкості та адекватного регулювання роботи галузі в кризових умовах.

РОЗДІЛ 3
ОБҐРУНТУВАННЯ КОНКРЕТНИХ ШЛЯХІВ ПІДВИЩЕННЯ СТІЙКОСТІ ЕЛЕКТРОМЕРЕЖ УКРАЇНИ

3.1. Пропозиції щодо фізичного захисту та маскування критично важливих вузлів електромережі

На основі аналізу стану ОЕС України, ідентифікованих загроз та вразливостей (Розділ 1), а також розглянутих загальних принципів та підходів до підвищення стійкості (Розділ 2), цей розділ присвячений обґрунтуванню та деталізації конкретних заходів і пропозицій, спрямованих на зміцнення українських електромереж в умовах зовнішньої військової загрози. Ці пропозиції охоплюють фізичний захист, кібербезпеку, адаптацію мережевих структур, модернізацію обладнання та підготовку персоналу.[9]

Ключові об'єкти енергетичної інфраструктури, такі як великі підстанції та генеруючі потужності, є вразливими до кінетичних атак із застосуванням ракетного озброєння, безпілотних літальних апаратів та артилерії. Ця вразливість обґрунтовує необхідність впровадження комплексної, багаторівневої системи фізичного захисту та маскування. Основна мета таких заходів – зменшити ймовірність прямого ураження критичних елементів, мінімізувати пошкодження від уламків та вибухової хвилі, а також суттєво ускладнити процес виявлення та наведення для засобів ураження противника.

Одним з ключових напрямків є зведення інженерних захисних споруд, як стаціонарних, так і швидкозбірних, навколо найбільш важливого обладнання – силових автотрансформаторів, систем релейного захисту та автоматики, пунктів управління. Рекомендується використання залізобетонних конструкцій (стін, саркофагів), розрахованих на захист від вторинних факторів ураження. Як доповнення або основний захист для менш критичного обладнання можуть застосовуватися габіонні конструкції, блоки HESCO чи земляні вали. У випадках,

де це технічно можливо та економічно доцільно, слід розглядати варіанти часткового заглиблення обладнання або будівництва підземних споруд, особливо для резервних пунктів управління.

Окремої уваги потребує захист від безпілотних літальних апаратів. Це включає встановлення фізичних перешкод, наприклад, спеціальних антидронових сіток, над відкритими розподільними пристроями (ВРП) та іншим обладнанням. Також, у тісній координації з військовими підрозділами, може розглядатися можливість застосування локальних систем радіоелектронної боротьби (РЕБ) для протидії ударним БПЛА. Невід'ємною частиною захисту є маскування, спрямоване на зменшення візуальної та теплової помітності об'єктів. Доцільно використовувати маскувальні сітки відповідного типу, фарбувати обладнання у кольори, що зливаються з навколишньою місцевістю, та застосовувати заходи для зниження теплового випромінювання. Ефективним може бути і створення хибних об'єктів – макетів обладнання або імітаторів теплових сигнатур – для введення противника в оману.

Важливим принципом підвищення стійкості є розосередження. При проектуванні нових об'єктів або реконструкції існуючих підстанцій рекомендується уникати надмірної концентрації критично важливого обладнання на обмеженій площі.[19] Також слід практикувати створення розосереджених, захищених складів для зберігання аварійного запасу обладнання, що ускладнює його одночасне знищення.

3.2. Заходи з підвищення кібербезпеки систем управління та моніторингу електромереж

Кібератаки на системи управління, релейного захисту та канали зв'язку становлять серйозну загрозу для енергетичної інфраструктури, адже можуть призвести до масштабних збоїв і навіть фізичних пошкоджень. Це обґрунтовує необхідність створення комплексної, багаторівневої системи захисту

технологічних (ОТ) та інформаційно-комунікаційних систем від несанкціонованого доступу, шкідливих впливів та витоку інформації.

Захист периметру та кінцевих точок передбачає застосування промислових міжмережевих екранів та систем виявлення/запобігання вторгненням, а також антивірусного захисту та контролю додатків на обладнанні. Не менш важливим є надійний контроль доступу з використанням багатофакторної автентифікації, принципу мінімальних привілеїв, суворого контролю віддаленого доступу та регулярного аудиту прав. Також необхідно забезпечити постійний моніторинг подій безпеки мати відпрацьовані плани реагування на інциденти, впровадити безпечні процедури оновлення програмного забезпечення та управління конфігураціями, і використовувати криптографічний захист для критичних каналів зв'язку та даних.

3.3. Розробка та впровадження адаптивних схем електропостачання та мікромереж

Підвищення гнучкості та адаптивності електромережі є ключовим фактором для зменшення наслідків ворожих атак та прискорення відновлення електропостачання. Це обґрунтовується необхідністю знизити залежність від пошкоджених магістральних ліній чи вузлових підстанцій та забезпечити можливість автономної роботи для найбільш критичних споживачів та зон.[19]

Для наглядного прикладу можна продемонструвати певні фрагменти схем для пояснення принципу дії АВР.

У цьому випадку спрацьовує максимальний струмовий захист трансформатора Т1: реле КА2 (рис. 3.1, 3.2) своїми контактами подає оперативний струм через увімкнений тумблер SA8 на обмотку проміжного реле KLT4. Реле KLT4 спрацьовує із витримкою часу замикає контакти KLT4.1 і KLT4.2, подаючи живлення на котушки вимикання вимикачів Q1 і Q2 – YATQ1 і YATQ2 [10]

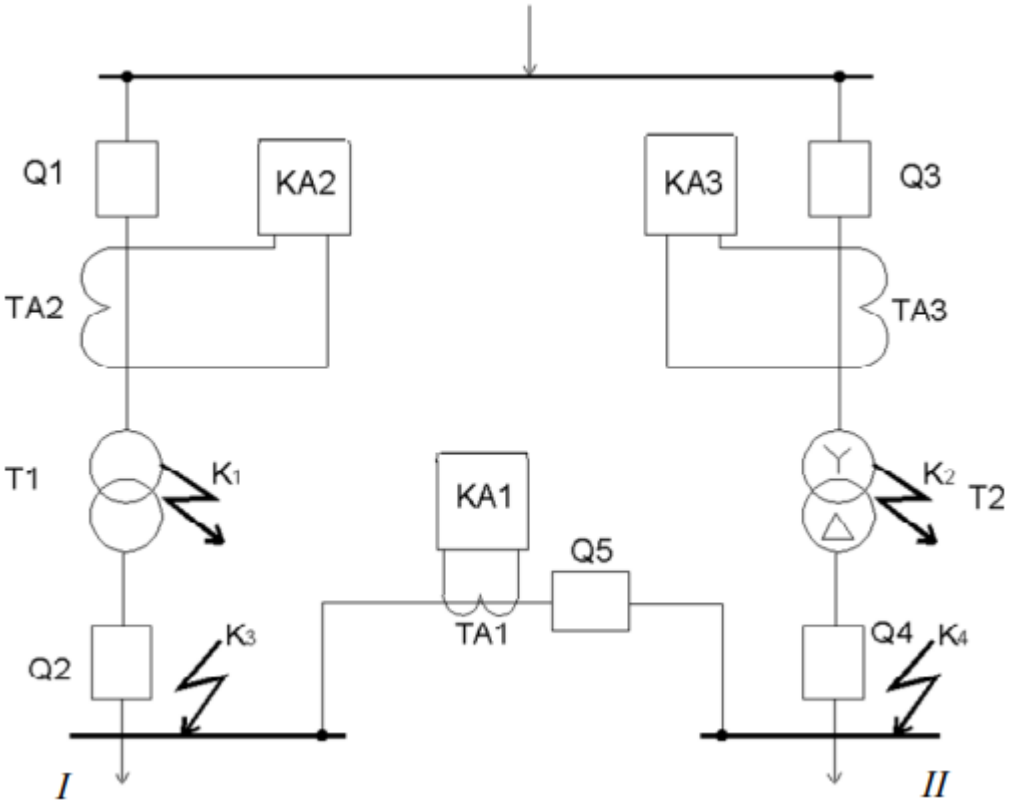

Рис. 3.1 Фрагмент схеми електричних з’єднань підстанції для пояснення принципу дії АВР [13]

Досягнення цієї мети передбачає, по-перше, оптимізацію топології існуючих мереж через аналіз вразливостей, будівництво додаткових ліній для резервування та підвищення закільцьованості. По-друге, важливим є впровадження засобів автоматизації в розподільних мережах, таких як реклоузери, керовані роз'єднувачі та системи телемеханіки, що дозволяють швидко локалізувати пошкодження та автоматично перемикати живлення за допомогою схем АВР та систем типу FLISR (Fault Location, Isolation, and Service Restoration).

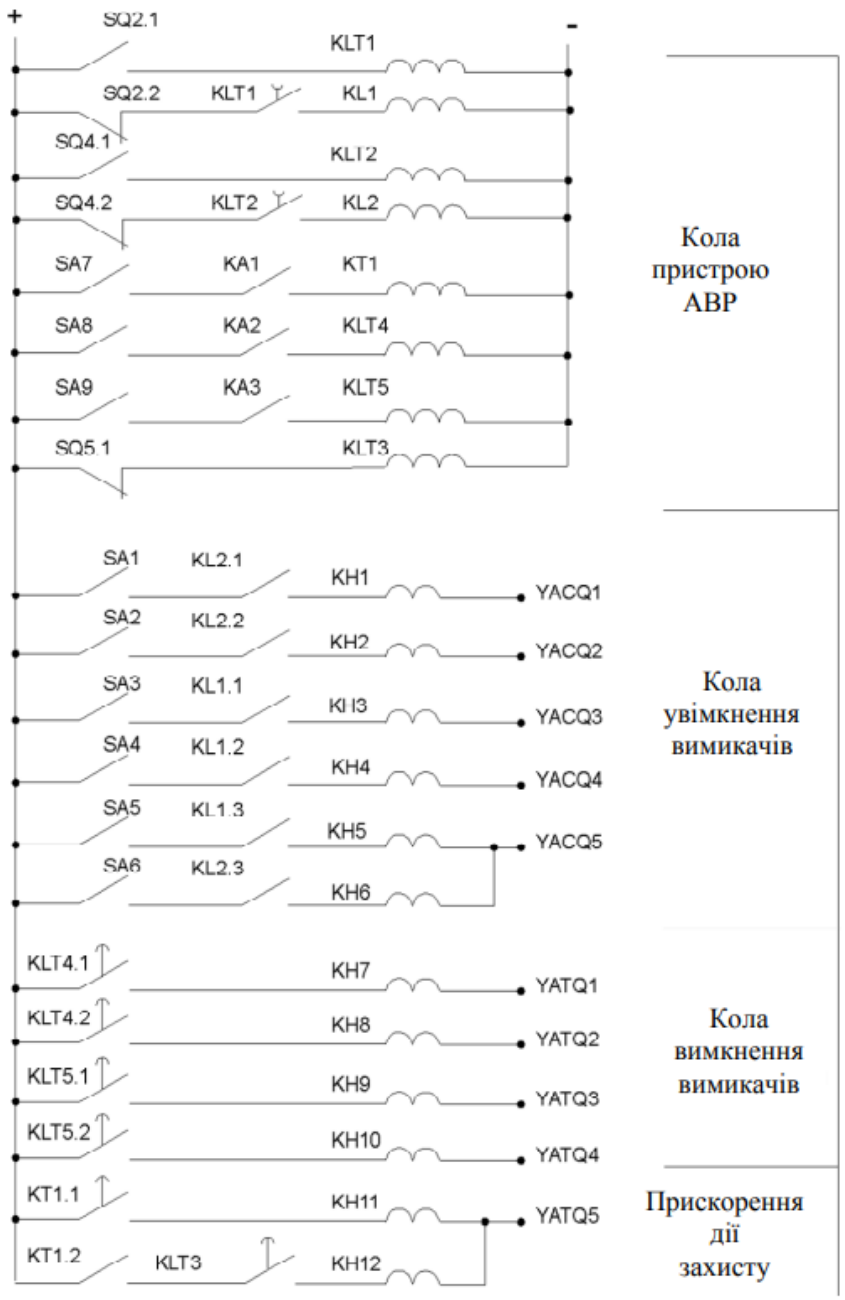

Рис. 3.2 Схема пристрою АВР і релейного захисту [13]

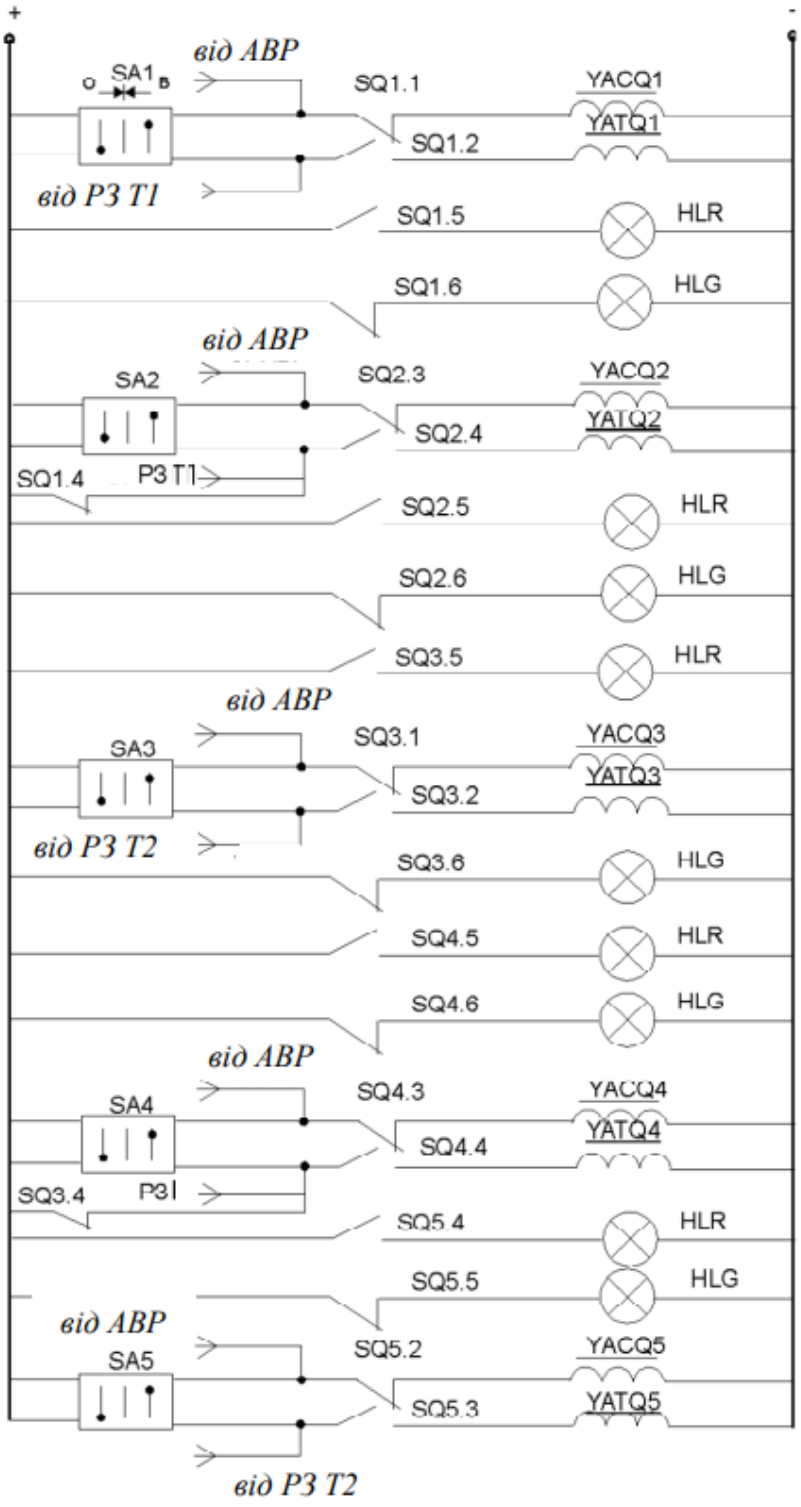

Рис. 3.3 Схема управління та сигналізації положення вимикачів [13]

По-третє, перспективним напрямком є створення мікро мереж для критичних об'єктів чи районів (наприклад, лікарень, військових частин, окремих

громад). Такі мікромережі об'єднують локальну генерацію, системи накопичення енергії та інтелектуальні контролери, забезпечуючи можливість роботи в автономному ("острівному") режимі при відключенні від основної мережі.[10] Розвиток мікро мереж тісно пов'язаний зі стимулюванням розподіленої генерації через спрощення процедур підключення та створення економічних стимулів. Крім того, впровадження програм керування попитом додає гнучкості системі, дозволяючи оперативно регулювати споживання під час дефіциту потужності або для запобігання перевантаженню мережі.

3.4. Шляхи модернізації та застосування обладнання підвищеної надійності та стійкості до зовнішніх впливів

Використання сучасного, надійного та стійкого обладнання є важливим фактором для зменшення ймовірності відмов та прискорення відновлення мережі після атак, оскільки це підвищує витривалість компонентів та полегшує ремонтні процеси. Досягти цього можна через реалізацію програм пріоритетної заміни застарілого та зношеного критичного обладнання, що вже вичерпало свій ресурс або не відповідає сучасним вимогам стійкості.

При закупівлі нового обладнання необхідно включати до технічних вимог параметри підвищеної стійкості до зовнішніх чинників (вібрації, ударні навантаження, за потреби – електромагнітні імпульси) та віддавати перевагу обладнанню в захищеному виконанні, наприклад, комплектним розподільчим установкам з елегазовою ізоляцією замість відкритих аналогів. Важливими аспектами також є максимальна стандартизація типів обладнання та застосування модульних рішень (як-от блочно-модульні підстанції) для спрощення й прискорення монтажу та ремонту. Крім того, слід впроваджувати сучасні цифрові системи релейного захисту та автоматики на базі мікропроцесорних пристроїв з розширеними функціями діагностики, осцилографування та підтримкою сучасних протоколів, а також використовувати системи векторних

вимірювань для моніторингу динамічної стійкості, що загалом підвищує надійність захисту та спрощує аналіз роботи системи.

Також варто враховувати, що використання такого водночас примітивного за конструкцією, але дещо складного в плані реалізації захисту енергетичних об’єктів як «HESCO» (рис. 3.4) та (рис. 3.5) чи звичайних насипів із піску та ґрунту є недостатнім, адже переважна кількість пошкоджень енергетичних об’єктів припадає саме на кінетичні пошкодження, як правило БПЛА, крилаті та балістичні ракети, іноді детонація бойової частини яких відбувається без доторкання до цілі, це у свою чергу збільшує радіус ураження прилеглих ЛЕП та інших елементів нашої енергетичної інфраструктури. Прикладом цього можна вважати інцидент із одним з двох трансформаторів на ПС в якого влучила крилата ракета, залишки укріплень з піску після ураження можна розгледіти на (рис.1.2)

Рис 3.4 Розгортання Бар’єру HESCO [12]

Рис 3.4 Наповнення Бар’єру HESCO [12]

Також варта уваги і така система захисту як підземні підстанції, але як зазначають енергетики, такий вид захисту має як і суттєві переваги так і вагомі недоліки.

До переваг можна віднести: захищення об’єкта від уламків які детонували поряд, краща стійкість до ударної хвилі.

До недоліків віднесемо: не можливість виконати дане завдання із усіма випадками в нашій енергосистеми, проблема полягає саме в тому, що план побудови наших ПС не розраховував на таку модернізацію, під трансформаторами розташовані масивні системи кріплення трансформатора, кабельні силові та сигнальні комунікації, та системи захисту від погодних умов та аварій на ПС. Таке переобладнання коштуватиме дуже дорого, а роботи над модернізацією триватимуть від одного календарного місяця. Це у свою чергу означитиме, що навантаження від цього об’єкту під час переобладнання буде розподіллено по іншим ПС, що ще більше навантажуватиме їх, а деякі з них і так

працюють на межі від своїх можливостей. Це пояснюється тим, що багато підстанцій було знищено та пошкоджено, і це навантаження також перейшло до їх. Варто також зазначити, що ситуація змінюється із кожним днем, енергетики працюють над вирішенням цих проблем та відновлюють енергетичні об’єкти, але нажаль не все можна відновити через критичні пошкодження, у таких випадках необхідно відбудовувати все з початку чи навіть будувати у іншому місці в інший спосіб.

Рис. 3.5 Комплектування одного із подібних сховищ «GRITEC» енергетичним обладнанням [7]

В такому випадку коли все перебудовується із самого початку, вже має сенс спланувати ПС із підземними трансформаторами. Варто розуміти, що такий вид захисту хоч і є одним із найдієвіших засобів захисту обладнання на ПС, але навіть він не здатен врятувати об’єкт від прямого влучання бойової частини.

3.5. Підготовка персоналу та розробка планів дій на випадок реалізації військових загроз

Людський фактор є вирішальним в умовах кризи, адже навіть найсучасніші технічні засоби неефективні без належно підготовленого, оснащеного та захищеного персоналу.[5] Тому ключовим завданням є забезпечення спроможності енергетиків ефективно діяти в екстремальних умовах війни. Це вимагає розробки та регулярного проведення спеціалізованих навчань та протиаварійних тренувань, які максимально реалістично імітують умови воєнних дій (масовані атаки, робота під обстрілами, кібератаки, блекаути) та відпрацьовують взаємодію з військовими і ДСНС.

Необхідно створити чіткі, покрокові інструкції та алгоритми дій для персоналу на випадок різних сценаріїв, визначити пріоритети відновлення та розробити плани евакуації. Важливими є психологічна підготовка персоналу, проведення тренінгів зі стресостійкості та забезпечення доступу до психологічної підтримки. Крім того, першочерговим є забезпечення безпеки: надання персоналу засобів індивідуального броне захисту, оснащення бригад захищеним транспортом, розробка безпечних маршрутів та забезпечення надійними засобами автономного зв'язку. Для оперативного реагування також доцільно формувати висококваліфіковані мобільні аварійно-відновлювальні бригади, повністю оснащені необхідною технікою, інструментами та матеріалами.

Висновки по розділу 3

Таким чином, за результатами розгляду конкретних шляхів підвищення стійкості електромереж України можна зробити висновок, що це завдання вимагає реалізації комплексного підходу.

1. Він має включати взаємопов'язані заходи у ключових сферах: фізичного захисту, кібербезпеки, адаптації мережевої інфраструктури, модернізації

обладнання та підготовки персоналу. Було показано, що запропоновані конкретні заходи, серед яких будівництво інженерних укриттів, сегментація технологічних мереж, впровадження мікро мереж, використання стійкого обладнання та спеціалізована підготовка персоналу, безпосередньо спрямовані на нейтралізацію або мінімізацію впливу ідентифікованих військових загроз, а також на компенсацію системних вразливостей ОЕС України.

2. При цьому обґрунтування кожного заходу базується на аналізі ризиків, досвіді протидії повномасштабній агресії та загальних принципах побудови стійких систем, розглянутих у попередньому розділі. Важливо відзначити, що реалізація цих пропозицій потребує значних ресурсів, координації зусиль та часу, однак вона є критично необхідною для забезпечення сталого функціонування енергосистеми та життєдіяльності країни в умовах тривалої зовнішньої військової загрози. Розглянуті пропозиції створюють основу для наступного етапу роботи – оцінки їх потенційної ефективності, яка буде проведена у наступному розділі.

ВИСНОВОК

У даній роботі проведено дослідження та обґрунтування шляхів підвищення стійкості електромереж України в умовах зовнішньої військової загрози. Актуальність теми визначається безпрецедентними викликами, пов'язаними з цілеспрямованими та систематичними атаками на об'єкти критичної енергетичної інфраструктури країни, що призводить до значних руйнувань, масштабних відключень електроенергії та створює загрозу для національної безпеки, економіки та життєдіяльності населення. Метою роботи було обґрунтування комплексу взаємопов'язаних заходів для зміцнення спроможності українських електромереж протистояти цим загрозам, мінімізувати їх наслідки та прискорити відновлення.

В результаті проведеного дослідження було досягнуто поставленої мети та вирішено наступні завдання, що дозволило сформулювати такі основні висновки:

Аналіз стану Об'єднаної енергетичної системи України та характеру сучасних військових загроз підтвердив високий ступінь вразливості ключових елементів мережі до різноманітних засобів ураження, включаючи ракетні удари, атаки БПЛА, артилерійські обстріли, кібератаки та фізичні диверсії. Виявлено основні системні вразливості, пов'язані з фізичною концентрацією та відкритістю об'єктів, типологічними особливостями мережі, залежністю від імпорту критичного обладнання, потенційними кіберзагрозами та станом основних фондів. Встановлено, що в умовах війни традиційного поняття надійності недостатньо, а ключовою метою стає забезпечення стійкості системи.

Узагальнення вітчизняного та світового досвіду, а також розгляд загальних підходів до підвищення стійкості критичної інфраструктури показали, що ефективне вирішення проблеми можливе лише на основі комплексного, багаторівневого підходу. Він має поєднувати організаційні заходи та технічні рішення . Доведено ключову роль стратегічних принципів резервування, децентралізації та диверсифікації у побудові гнучкої та живучої енергосистеми.

Підтверджено важливість адекватного нормативно-правового забезпечення, що враховує специфіку воєнного стану.

На основі проведеного аналізу було розроблено та обґрунтовано комплекс конкретних шляхів підвищення стійкості українських електромереж. Ці пропозиції охоплюють: посилення фізичного захисту критичних вузлів за допомогою інженерних споруд та маскування; впровадження багаторівневої системи кібербезпеки технологічних мереж та систем управління; розвиток адаптивних схем електропостачання через оптимізацію топології, автоматизацію та створення мікро мереж; модернізацію та застосування обладнання з підвищеними характеристиками надійності та стійкості; а також посилену підготовку персоналу, розробку детальних планів дій та забезпечення безпеки енергетиків. Кожен запропонований захід спрямований на нейтралізацію конкретних загроз або компенсацію виявлених вразливостей.

Проведена оцінка потенційної ефективності запропонованих рішень показала, що, незважаючи на значні фінансові витрати та технічні й організаційні складнощі впровадження, їх реалізація є технічно можливою та економічно обґрунтованою. Основний економічний ефект полягає у попередженні колосальних збитків від руйнувань інфраструктури та тривалих перерв в електропостачанні, а також у забезпеченні стратегічно важливої енергетичної безпеки країни. Водночас наголошено на необхідності ретельної пріоритезації заходів з урахуванням наявних ресурсів, рівня критичності об'єктів та аналізу ризиків.

Проведене дослідження дозволило систематизувати проблеми забезпечення стійкості електромереж в умовах війни та обґрунтувати комплексний підхід до їх вирішення. Практичне значення отриманих результатів полягає у тому, що вони можуть слугувати основою для розробки конкретних програм та проектів модернізації і захисту енергетичної інфраструктури України енергетичними компаніями, проектними інститутами

та органами державної влади, сприяючи підвищенню енергетичної безпеки та загальної стійкості держави під час та після завершення воєнних дій. Подальші дослідження доцільно спрямувати на детальне техніко-економічне моделювання окремих запропонованих рішень, розробку методики заходів та дослідження нових технологій захисту енергооб'єктів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Arghandeh, R., Von Meier, A., Mehrmanesh, L. та ін.: Щодо визначення кіберфізичної стійкості в енергосистемах. Відновити. Сустейн. Energy Rev. 58, 1060–1069 (2016)
2. Wang, C., Ju, P., Wu, F., Pan, X., Wang, Z.: Систематичний огляд стійкості енергосистеми з точки зору генерації, мережі та навантаження. Відновити. Сустейн. Energy Rev. 167, 112567 (2022).
3. Zhang, H., Bie, Z., Li, G., Lin, Y.: Метод оцінки та показники стійкості енергосистеми після катастроф. J. Eng. 2019(16), 880–883 (2019).
4. Аббасі, С., Бараті, М., Лім, Дж. Дж.: Паралельна секційна схема відновлення для стійких інтелектуальних мережевих систем. IEEE Trans. Smart Grid 10 (2), 1660–1670 (2019).
5. Бі, З., Лін, Ю., Лі, Г. та ін.: Боротьба з крайнощами: дослідження стійкості енергосистеми. IEEE Proc. 105(7), 1253–1266 (2017).
6. Василець С. В., Василець К. С. Техніка високих напруг: Навчальний посібник. Рівне: 2018.
7. Жежеленко В. В., Саєнко Ю. Л. Якість електроенергії на промислових підприємствах: навч. посіб. Київ: НТУУ «КПІ», 2011. 78 с.
8. Закон України «Про критичну інфраструктуру» від 16.11.2021 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text.
9. Кандаперумал, Г., Срівастава, А. К.: Стійкість систем розподілу електроенергії: концепції, класифікація, оцінка, виклики та потреби в дослідженнях. IET Smart Grid 3, 133–143 (2020).
10. Кириленко О. В., Павловський В. В., Лутченко С. А. Електричні системи та мережі. Керування режимами роботи. Київ: Техніка, 2009. 105 с.
11. Постанова про затвердження кодексу систем розподілу / Затв. Постановою НКРЕКП від 14.03.2018 № 310. URL: https://zakon.rada.gov.ua/laws/show/v0310874-18#Text.
12. Постанова про затвердження кодексу системи передачі / Затв. Постановою НКРЕКП від 14.03.2018 № 309. URL:

https://zakon.rada.gov.ua/laws/show/v0309874-18#Text.

13. Кутін В.М., Рубаненко О.Є. Релейний захист та системна автоматика. Вінниця: ВНТУ, 2018.
14. Лі Р., Ассанте М., Конвей Т.: Аналіз кібератаки на українську енергомережу. Технічний звіт (2016).
15. Лін, Ю., Бі, З., Цю, А.: Огляд ключових стратегій у реалізації стійкості енергосистеми. Глоб. Енергетичне з'єднання. 1(випуск 1), 70–78 (2018).
16. Павленко О., Антоненко А., Ніцович Р., Євтушок С., Суходоля О.: Оцінка стійкості енергетичної інфраструктури України. Dixi Hrup (2022).
17. Правила улаштування електроустановок / Міненерговугілля України. 6-е вид., перероб. і доп. Харків: Форт, 2017. 296 с.
18. Правила улаштування електроустановок / Міненерговугілля України. 6-е вид., перероб. і доп. Харків: Форт, 2017. 385–390 с.
19. Правила улаштування електроустановок / Міненерговугілля України. 6-е вид., перероб. і доп. Харків: Форт, 2017. 428–448 с.
20. Рід, Д. А., Капур, К. К., Крісті, Р. Д.: Методологія оцінки стійкості мережевої інфраструктури. IEEE Syst. J. 3(2), 174–180 (2009).
21. Родж, П.Е., Кольєр, З.А., Мансіллас, Дж., МакДонаг, Дж.А., Лінков, І.: Метрики для енергетичної стійкості. Енергетична політика, 249–256 (2014).
22. Роккетта, Р.: «Надійні обчислювальні структури для аналізу надійності, вразливості та стійкості електромережі». Доктор філософії в галузі техніки, Ліверпульський університет (2018).
23. Сіллєрс, Дж.: Розкриваючи реальність знищеної енергетичної інфраструктури України (2023).
24. Суходоля О. М., Рябцев Г. Л., Харазішвілі Ю. М., Бобро Д. Г., Завгородня С. П. Визначення рівня та оцінка загроз енергетичній безпеці: Збірник доповідей аналітиків. – 160 с. Київ (2022).
25. Харазішвілі Ю., Квілінський А., Суходоля О. та ін.: Системний підхід до оцінки та стратегії енергетичної безпеки: приклад України. Енергії 14, 2126 (2021).