МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

О. В. Дяченко, Д. А. Гапон, Н. В. Рудевіч, С. В. Швець,
Т. С. Донецька, Р. С. Ложкін

ПЕРЕДАЧА ІНФОРМАЦІЇ В ЕЛЕКТРОЕНЕРГЕТИЦІ: ЗАСОБИ, ПРОТОКОЛИ, СТАНДАРТИ, КІБЕРБЕЗПЕКА

Навчальний посібник
для бакалаврів та магістрів
спеціальності G3 «Електрична інженерія»
усіх форм навчання

Затверджено
редакційно-видавничою
радою НТУ «ХПІ»,
протокол № 2 від 26.06.2025 р.

Харків
НТУ «ХПІ»
2025

УДК 621.311:004.6(075.8)
П 27

Рецензенти:

В. С. Блиндюк, д-р техн. наук, проф., проректор з науково-педагогічної роботи, Харківський національний університет імені В. Н. Каразіна;

О. О. Мірошник, д-р техн. наук, проф., зав. кафедри електропостачання та енергетичного менеджменту, Державний біотехнологічний університет

Передача інформації в електроенергетиці: засоби, протоколи, стандарти, П 27 кібербезпека: навчальний посібник / О. В. Дяченко, Д. А. Гапон, Н. В. Рудевіч, С. В. Швець, Т. С. Донецька, Р. С. Ложкін. – Харків : НТУ «ХПІ», 2025. – 256 с.

ISBN 978-617-05-0564-4

Детально розглянуто основи побудови, функціонування та інтеграції систем передачі інформації, основні протоколи, стандарти, архітектури, а також комунікаційне обладнання та канали зв'язку. Окрему увагу приділено цифровій трансформації енергетичних систем, концепціям Smart Grid, IoT, хмарних технологій та кібербезпеці енергосистем.

Призначено для студентів усіх форм навчання спеціальності G3 «Електрична інженерія».

Іл. 71. Табл. 8. Бібліогр. 27 назв.

УДК 621.311:004.6(075.8)

ISBN 978-617-05-0564-4

ЗМІСТ

ПЕРЕДМОВА

Сучасний розвиток енергетичної галузі невід'ємно пов'язаний з активною цифровізацією та впровадженням інтелектуальних технологій. У цьому контексті навчальні дисципліни «Передача інформації в електроенергетиці» та «Інформаційна безпека в електроенергетиці» посідають ключове місце у підготовці магістрів за спеціальністю G3 «Електрична інженерія», освітньої програми «Електроенергетика». Вони забезпечують формування фахових компетентностей, необхідних для проєктування, впровадження, підтримки та модернізації інформаційно-комунікаційних систем, що обслуговують енергетичну інфраструктуру.

На відміну від інших робіт [1–13] цей посібник зосереджений саме на системах передачі інформації та її захисті як критичному елементі цифрового управління енергосистемами. Посібник не дублює підходи, зосереджені на обліку чи керуванні, а інтегрує знання про канали зв'язку, протоколи, мережеві архітектури, стандарти, безпеку та стійкість систем зв'язку у межах єдиної техніко-системної парадигми [26, 27].

Основними завданнями, які стоять перед студентами під час вивчення дисциплін, є:

– засвоєння принципів функціонування систем передачі інформації в енергетиці;

– розуміння архітектури сучасних інформаційно-комунікаційних мереж;

– набуття практичних навичок аналізу та проєктування таких систем;

– вивчення сучасних технологій Smart Grid, IoT, SCADA, AMI, хмарних рішень та кіберзахисту;

– здатність до адаптації в умовах динамічної трансформації цифрової енергетики;

– оволодіння основами інформаційної безпеки в енергетичних системах, зокрема знанням засобів захисту інформації, виявлення загроз та забезпечення стійкості до кіберінцидентів.

Матеріал посібника охоплює повний цикл розвитку систем зв’язку — від базових фізичних принципів до застосування комплексних інформаційних платформ. Зокрема, особливу увагу приділено ролі інформаційних технологій у формуванні цифрового диспетчерського управління, на базі SCADA-систем, інтеграції засобів телекомунікацій з обліковими та керуючими платформами.

Відмінністю цього навчального посібника від інших є комплексний, міждисциплінарний підхід, що дозволяє студенту не лише володіти технічним інструментарієм, але й глибоко орієнтуватися у нормативному полі, питаннях сумісності, кібербезпеки та експлуатаційної надійності. На відміну від більш фрагментарних за змістом посібників, наприклад, [14, 22] дана робота спрямована на формування цілісного світогляду щодо функціонування інформаційно-комунікаційних технологій у енергосистемах.

Послідовна структура подання матеріалу — від фундаментальних понять до аналізу прикладів реальних впроваджень у вітчизняній та міжнародній практиці — сприяє розвитку у студентів не лише аналітичного, а й конструктивного інженерного мислення. У результаті опанування дисципліни майбутній фахівець буде готовим до прийняття обґрунтованих рішень у сфері цифрового енергетичного інжинірингу.

Автори сподіваються, що навчальний посібник стане надійною основою для фахової підготовки нової генерації інженерів енергетичної галузі — обізнаних, гнучких, здатних працювати на стику електротехніки, інформаційних технологій та управління.

Навчальний посібник був підготовлений колективом кафедри «Автоматизація та кібербезпека енергосистем» Національного технічного університету «Харківський політехнічний інститут». Автори висловлюють щиру подяку всім, хто так чи інакше допоміг у підготовці остаточної версії книги до публікації.

Всі зауваження та пропозиції щодо посібника автори просять надсилати на адресу: 61002, Харків, вул. Кирпичова, 2, НТУ «ХПІ» каф. АКЕС.

Автори

ВСТУП

Сучасна електроенергетика є однією з найважливіших галузей національної економіки, що забезпечує життєдіяльність усіх сфер суспільства — від побутових споживачів до великих промислових підприємств, транспорту, IT-інфраструктури та соціальних об’єктів. У зв’язку зі зростанням масштабів та складності енергетичних систем, а також із постійним підвищенням вимог до надійності, безпеки та ефективності їхньої роботи, зростає роль інформаційних технологій, які забезпечують безперебійну взаємодію між усіма елементами енергетичної інфраструктури.

Одним із ключових напрямів, що забезпечує стабільне функціонування енергосистеми, є *передача інформації*. Вона охоплює процеси збору, обробки, передачі, зберігання та аналізу даних, необхідних для прийняття оперативних рішень, автоматичного керування та координації роботи енергетичних об’єктів. В умовах цифровізації, активного впровадження концепції Smart Grid (інтелектуальних мереж), а також розвитку децентралізованої генерації (в тому числі з відновлюваних джерел енергії), роль якісної, швидкої та захищеної передачі інформації зростає в геометричній прогресії.

Починаючи від провідних телемеханічних ліній у середині XX століття й до сучасних XXI ст. волоконно-оптичних мереж і безпровідних систем зв’язку, еволюція засобів та методів передачі інформації відображає технологічний розвиток усієї енергетичної галузі. У сучасних умовах вже недостатньо передавати лише базові сигнали про стан обладнання. Необхідно забезпечувати інтеграцію складних даних у реальному часі: показників потужності, струму, напруги, частоти, температури, сигналів тривог, повідомлень про аварійні події, команд керування, параметрів прогнозування тощо.

Системи передачі інформації в електроенергетиці є невід’ємною частиною автоматизованих систем управління технологічними процесами (АСУ ТП), систем диспетчерського керування SCADA, автоматизованих систем комерційного обліку електроенергії (АСКОЕ), а також релейного захисту та автоматики (РЗА).

Від якості передачі інформації напряму залежать такі показники, як час реагування систем захисту, точність обліку електроенергії, достовірність сигналів диспетчера, ефективність регулювання режимів роботи енергосистеми.

Проблема ускладнюється ще й тим, що електроенергетична інфраструктура має територіально розподілений характер, а передача інформації повинна бути гарантовано надійною навіть у складних умовах: при високих рівнях електромагнітних завад, в умовах аварійних ситуацій, в умовах фізичної або кіберзагрози. Усе це висуває високі вимоги до вибору середовища передачі (мідний кабель, оптика, радіоканал, супутниковий зв'язок тощо), до протоколів комунікації, швидкості обміну даними, захисту інформації, стійкості до втрат пакетів та помилок, можливості дублювання каналів.

Крім технічних аспектів, значну роль відіграє також інформаційна безпека. Поширення кіберзагроз, зловмисного втручання, хакерських атак змушує операторів систем передачі та розподілу електроенергії впроваджувати спеціалізовані механізми шифрування, автентифікації, виявлення аномалій у трафіку.

У контексті навчання майбутніх фахівців-енергетиків важливо формувати системне розуміння процесів передачі інформації — як із технічної точки зору (фізика сигналу, протоколи зв'язку, архітектура мережі), так і з точки зору програмного забезпечення, конфігурації систем SCADA, взаємодії елементів за допомогою стандартів типу IEC 60870–5–104, IEC 61850, Modbus, DNP3, а також з урахуванням специфіки функціонування АСКОЕ, РЗА та цифрових підстанцій.

Навчальний посібник має на меті дати ґрунтовні знання щодо організації, принципів роботи та типових рішень у сфері передачі інформації в енергетичних об'єктах. Посібник призначено для магістрів що навчаються по спеціальності G3 «Електрична інженерія», інженерів-практиків, а також фахівців, які займаються проєктуванням, впровадженням або експлуатацією енергетичних систем.

Отже, вивчення теми передачі інформації в електроенергетиці є не лише актуальним, але й критично необхідним для розуміння сучасних тенденцій розвитку галузі. Надійна, швидка, захищена та масштабована передача даних — це основа ефективного функціонування всієї енергосистеми майбутнього.

1. ЗАГАЛЬНА ХАРАКТЕРИСТИКА ТА ОСНОВНІ ВІДОМОСТІ ПРО СИСТЕМИ ПЕРЕДАЧІ ІНФОРМАЦІЇ

У сфері електроенергетики, як і в будь-якій іншій складній технічній галузі, критично важливим є своєчасне отримання, передача, обробка та використання інформації. Сучасні енергетичні системи функціонують не тільки за рахунок потоків електроенергії, але й завдяки обміну великими обсягами даних, які передаються між етапами генерації, транспортування, розподілу та споживання. У цьому контексті інформація є не лише допоміжним елементом, а основним чинником, що забезпечує управління, надійність і ефективність роботи всієї енергетичної системи.

Будь-який процес управління тісно пов'язаний зі збиранням, обробкою, збереженням, передачею та подальшим використанням інформації, яка є результатом попередніх етапів її обробки.

Основні терміни:

Повідомлення (відомості, дані) — це результат дії фізичного об'єкта або прояв його стану, який може бути переданий іншому об'єкту. Важливо, що повідомлення має матеріальну основу, а отже — може передаватися. Воно може бути як результатом цілеспрямованої дії, так і випадковим наслідком змін об'єкта. Якщо дані не можуть бути передані, вони не вважаються повідомленням.

Інформація — це частина повідомлення, яка була раніше невідомою отримувачу. Отже, якщо отримувач уже володіє певними відомостями, вони не несуть для нього нової інформації. Це також означає, що одне повідомлення може містити різну кількість інформації залежно від ступеня новизни для одержувача.

Джерело інформації — це об'єкт, що генерує інформацію, тоді як *приймач* (одержувач) — це той, хто її сприймає і використовує за призначенням. Зазвичай джерело та одержувач розташовані на певній (іноді значній) відстані один від одного.

У процесі передачі виникає потреба зберігати достовірність (точність) переданої інформації, адже вона може спотворюватися під впливом зовнішніх

факторів. Такі фактори, що викликають викривлення інформації, називають *перешкодами* (*завадами*). Перешкоди мають, як правило, випадковий характер і їхнє джерело зазвичай невідоме.

Щоб зменшити вплив перешкод, у системах зв'язку передбачаються спеціальні методи обробки сигналів, які надають їм форму та структуру, що забезпечують надійну передачу інформації без спотворень навіть за наявності завад.

Сигнал — це фізичний носій інформації, у якому існує однозначний зв'язок між його параметрами та переданим повідомленням. Незалежно від того, як змінюється форма чи структура сигналу, обсяг інформації, що він несе, залишається незмінним [15, 18–22].

1.1. Узагальнена схема побудови комунікаційної мережі

Сучасні системи телемеханіки функціонують на основі комунікаційних мереж. Такі мережі складаються з різних елементів (вузлів), що відповідають за створення, трансформацію, збереження та передачу інформації. Вузли між собою з'єднані за допомогою ліній зв'язку. Загальну структуру комунікаційної мережі можна побачити на (рис. 1.1).

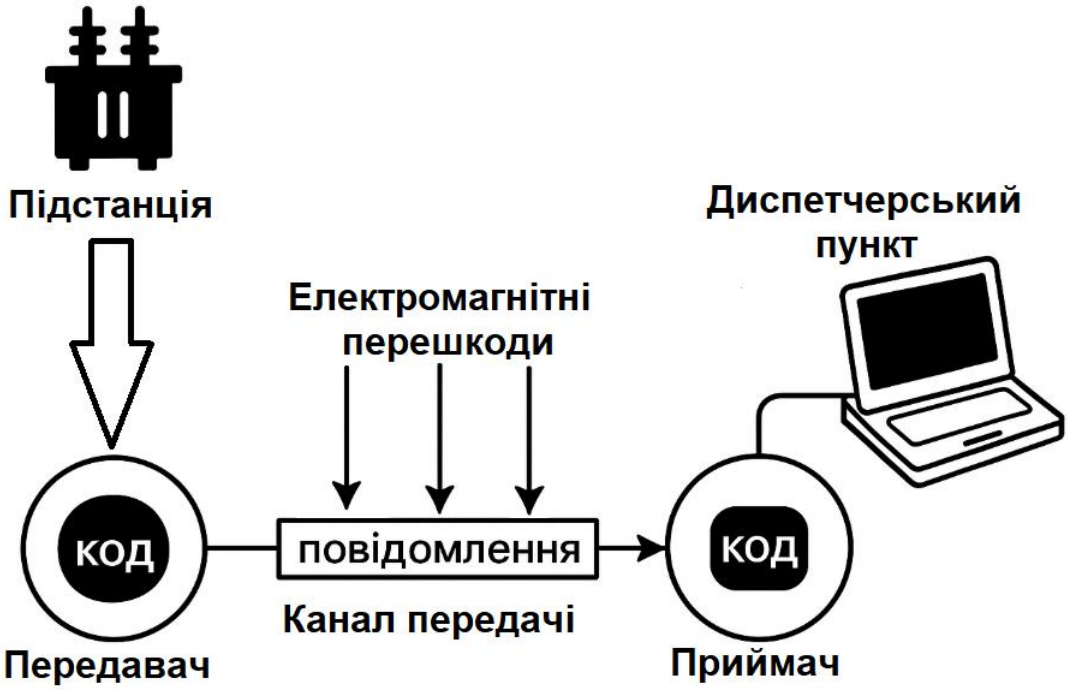

Рисунок 1.1 – Загальна модель комунікаційної мережі

Відмінною рисою таких мереж є значна відстань між окремими вузлами у порівнянні з розмірами простору, який займає кожен окремий об’єкт. Наприклад, у випадку міжсистемної лінії електропередач, довжина самої лінії значно перевищує фізичні розміри підстанцій, розташованих на її початку та в кінці.

Усі комунікаційні процеси передбачають наявність двох основних компонентів:

– джерела інформації або передавача (наприклад, промислові контролери, вимірювальні пристрої, датчики тощо);

– приймача інформації (наприклад, комп’ютери, виконавчі механізми, принтери тощо).

Передавач надсилає повідомлення, що складається з певної послідовності символів, до приймача за допомогою каналу зв’язку або загального середовища передачі, спільного для обох сторін.

Передавач включає елементи введення даних, кодувальний блок і сам передавач. *Приймач*, своєю чергою, складається з модуля приймання сигналу, пристрою декодування та засобу виводу інформації [15, 18–22].

Оскільки сама інформація не має фізичних параметрів (як–от колір, смак тощо), для її передачі використовується спеціальне кодування. Завдяки цьому передавач змінює фізичні властивості середовища, через яке здійснюється передача. Приймач зчитує ці зміни та відновлює початкове повідомлення. Щоб процес був коректним, обидва пристрої повинні використовувати узгоджені коди.

При цьому варто враховувати наявність *перешкод* (шумів), які можуть спотворювати сигнали та ускладнювати процес їх правильного відновлення. Щоб мінімізувати ці впливи, кодування надає сигналам такої форми й структури, що дозволяє ефективно передавати їх навіть у складних умовах. Тобто, *кодування — це процес трансформації інформаційного повідомлення в сигнал, придатний до надійної передачі*.

У результаті цього процесу створюються *кодовані сигнали*, які здатні протистояти впливу перешкод і забезпечити високу точність переданої інформації.

Передавач і приймач разом із лінією зв’язку формують повноцінний пристрій комунікації. Основна його задача — забезпечити потрібну кількість каналів для передачі інформації.

Лінія зв’язку — це фізичне середовище, яке з’єднує передавач і приймач. Вона може бути як матеріальною (наприклад, дротовою — електричною або оптоволоконною), так і бездротовою (наприклад, радіохвильовою, лазерною чи акустичною) [15, 18–22].

Канал зв’язку — це незалежний шлях, яким передається інформація від джерела до приймача. Під «незалежністю» мається на увазі відсутність впливу одного каналу на інший. Таким чином, кожен канал має чітко визначений початок — у джерелі інформації, і завершення — у відповідному приймачі [22].

Кожна система зв’язку, незалежно від типу переданої інформації, повинна відповідати таким ключовим вимогам:

– забезпечувати високу точність передачі та стійкість до впливу перешкод;

– гарантувати ефективну передачу даних з мінімальними втратами;

– бути економічно вигідною в процесі обміну інформацією.

У складних умовах експлуатації, таких як вплив електромагнітних завад, відмінності потенціалів заземлення, зношення компонентів системи або поява випадкових перешкод у каналі зв’язку, виникає потреба у забезпеченні високої точності та стійкості до завад при передаванні інформації. За таких обставин необхідно реалізовувати надійні механізми захисту повідомлень від таких потенційних загроз:

– непомічені помилки окремих бітів у потоці даних;

– неправильно прийняті інформаційні кадри, що виникають через збої синхронізації;

– втрата частини інформації, яка не фіксується приймаючою стороною;

– вставка сторонніх або спотворених даних, що виникають під впливом перешкод;

– порушення логічної послідовності повідомлень, зокрема розриви чи зміщення взаємопов’язаних елементів.

Ефективність передачі інформації зазвичай пояснюється як досягнення максимально можливої швидкості обміну даними за умови дотримання заданих рівнів точності та стійкості до перешкод. Інакше кажучи, йдеться про передавання найбільшого обсягу даних за найкоротший проміжок часу [15, 18–22].

Досягнення мінімального часу передачі забезпечується використанням оптимізованих протоколів, здатних ефективно працювати в умовах обмеженої пропускної здатності каналу зв’язку та за наявності непередбачуваних або нестабільних завад — особливо у випадках, коли обробляються непостійні (динамічні) потоки інформації.

Щодо економічної доцільності, то вона передбачає зменшення витрат на обладнання та загальні фінансові ресурси, необхідні для передавання даних. Це враховується ще на етапі проєктування системи, де перевага надається стандартизованим рішенням, типовим проєктам і уніфікованим технічним компонентам.

1.2. Модель відкритої взаємодії інформаційних систем

Україна входить до складу Міжнародної електротехнічної комісії (IEC) — провідної організації, що займається розробкою стандартів у галузі електротехніки, електроніки та суміжних технологічних напрямків. Частина стандартів IEC створюється у співпраці з Міжнародною організацією зі стандартизації (ISO).

Щоб уникнути проблем, пов’язаних з існуванням великої кількості несумісних стандартів та кодів, ISO було розроблено еталонну модель взаємодії відкритих систем (OSI). Вона слугує основою для створення нових стандартів у сфері передачі даних, описуючи процес комунікації на концептуальному рівні.

Застосування моделі OSI в енергетиці має важливе значення і дозволяє:

а) досягти сумісності телемеханічних систем і пристроїв, вироблених різними підприємствами, як в Україні, так і за кордоном;

б) забезпечити передачу оперативної інформації з прикріпленими часовими мітками та якісними атрибутами;

в) передавати як традиційні, так і нові типи даних з високою точністю та у більшому обсязі;

г) уніфікувати протоколи обміну даними для різних рівнів енергетичної ієрархії, зокрема:

– між диспетчерськими центрами (або пунктами керування);

– між пунктами керування та енергооб'єктами (електростанціями, підстанціями тощо);

– у межах одного об'єкта або диспетчерського пункту, для внутрішнього обміну даними.

Ключовою ідеєю моделі OSI є поділ процесу обміну даними на окремі логічні рівні, кожен з яких виконує чітко визначені функції та взаємодіє виключно з суміжними рівнями — вхідним і вихідним. Така модульна структура дозволяє досягти високої сумісності та взаємозамінності компонентів, незалежно від їх виробника чи реалізації [15, 18–22].

У моделі OSI виділяють сім основних функціональних рівнів (рис. 1.2).

1. Фізичний рівень відповідає за фізичне середовище передачі даних — це може бути електричний або оптичний канал з відповідними інтерфейсами (блоками підключення до лінії), які з'єднують вузли або станції. На цьому рівні розглядаються характеристики середовища передачі, параметри сигналу та його частотні властивості. Фізичний рівень є безпосереднім матеріальним зв'язком між двома вузлами, що може бути, наприклад, провідним кабелем, радіоканалом, волоконно-оптичною лінією або іншим каналом високої частоти.

До основних характеристик фізичного рівня, що впливають на надійність передачі, належать швидкість передачі сигналу, стійкість до перешкод, співвідношення сигнал/шум, а також ймовірність виникнення помилок у вигляді спотворення або втрати бітів.

2. Канальний рівень відповідає за формування та передачу кадрів між двома вузлами, а також за виявлення й корекцію помилок, які можуть виникати на фізичному рівні — зокрема, помилок синхронізації чи неправильного розміру кадру. Якщо виявляється помилка, наприклад через перешкоди в каналі, цей

рівень ініціює повторну передачу пошкодженого кадру. Таким чином, канальний рівень забезпечує безперебійну і надійну передачу даних для верхніх рівнів моделі [15, 18–22].

Рисунок 1.2 – Модель взаємодії відкритих систем OSI

3. Мережевий рівень відповідає за визначення маршруту й контроль над доставкою повідомлень від відправника до кінцевого вузла. Цей маршрут може складатися з кількох фізичних сегментів, які не завжди з'єднані безпосередньо між собою.

4. Транспортний рівень управляє процесом передачі даних від відправника до отримувача. Він виконує роль посередника між прикладним програмним забезпеченням і фізичною мережею, забезпечуючи незалежність верхніх рівнів від особливостей нижчих.

5. Сеансовий рівень (іноді називають часовим) відповідає за встановлення, підтримку і контроль з'єднання між об'єктами рівня представлення даних. Тут визначається тип зв'язку, реєстрація в мережі, а також початок і завершення передачі інформації.

6. Рівень представлення даних відповідає за синтаксичне оформлення інформації — кодування і трансформацію бітових потоків у формат, зрозумілий приймачу, відновлюючи оригінальний вигляд даних.

7. Прикладний рівень або рівень користувача — це найвищий рівень, на якому вирішуються прикладні завдання, наприклад, передача файлів, робота з базами даних або віддалене управління [22].

Три нижні рівні (фізичний, канальний, мережевий) відомі як комунікаційні, вони відповідають за доставку повідомлень. Верхні три рівні орієнтовані на прикладне забезпечення і працюють з самим вмістом інформації. Транспортний рівень служить посередником між комунікаційними і прикладними рівнями.

Основний принцип моделі OSI полягає в тому, що кожен рівень взаємодіє лише з безпосередньо сусідніми — верхнім і нижнім рівнями. Кожен рівень надає послуги вищому і звертається за послугами до нижчого. При цьому рівень, який ініціює запит, передає параметри і дані нижчому рівню, а потім переходить у режим очікування, не заглиблюючись у деталі виконання запиту.

За стандартами IEC рекомендовано використовувати архітектуру EPA з підвищеною продуктивністю замість класичної семирівневої моделі OSI, що

дозволяє зменшити час реакції в умовах обмеженої пропускної здатності. У архітектурі EPA передбачено лише три рівні: прикладний, канальний та фізичний.

1.3. Інформація як об’єкт передачі в енергетиці

Інформація в енергетиці — це сукупність даних про стан об’єктів енергосистеми, процеси виробництва, передачі та споживання електроенергії, а також про зовнішні та внутрішні фактори, які впливають на ці процеси. Це можуть бути:

– електричні параметри (напруга, струм, частота);

– стан обладнання (ввімкнено/вимкнено, аварія, сигналізація);

– значення лічильників (потужність, споживання, генерація);

– команди диспетчера (управління перемикачами, навантаженням);

– дані про погоду, стан мереж, резерви потужності;

– сигнали про загрози, втручання, збої.

З технічної точки зору, *інформація — це сигнал, що несе певне повідомлення*, зрозуміле для системи, яке можна зберігати, передавати, обробляти або використовувати для ухвалення рішень [2, 6–20].

Залежно від характеру, джерела і способу використання, інформацію в енергетиці можна поділити на кілька категорій:

1) *За характером даних*:

а) аналітична — для оцінки та прогнозування (наприклад, тренди навантаження);

б) оперативна — для керування (виконання команд, перемикання);

в) діагностична — для обслуговування та профілактики (напруга обмоток трансформатора, температура);

г) аварійна — критична інформація про відхилення або збої;

2) *За джерелом*:

а) внутрішня (від обладнання: трансформаторів, вимикачів, лічильників);

б) зовнішня (від супутникових систем, погодних датчиків, системи централізованого керування);

3) *За способом передачі*:

а) точкова (між двома пристроями);

б) мережева (через загальні мережі або інтернет);

в) трансляційна (широкомовна — одна точка передає багатьом);

4) *За частотою оновлення:*

а) неперервна (аналогові сигнали);

б) періодична (цифрові вимірювання з фіксованим інтервалом);

в) подієва (передається лише при зміні стану або значення).

Місце інформації в управлінні енергосистемою. Вимоги до інформації в енергетичних системах. Енергосистема — це комплексний, ієрархічний об’єкт, що вимагає координації на різних рівнях :

– локальний рівень — обладнання підстанцій, ПЛ, трансформаторів;

– регіональний — РЕМ, ОЕС, диспетчерські центри;

– національний — НЕК «Укренерго», оператор системи передачі;

– міжнародний — обмін даними з суміжними системами ENTSO-E.

На рисунку 1.3 показані інформаційні потоки в ієрархії енергосистеми.

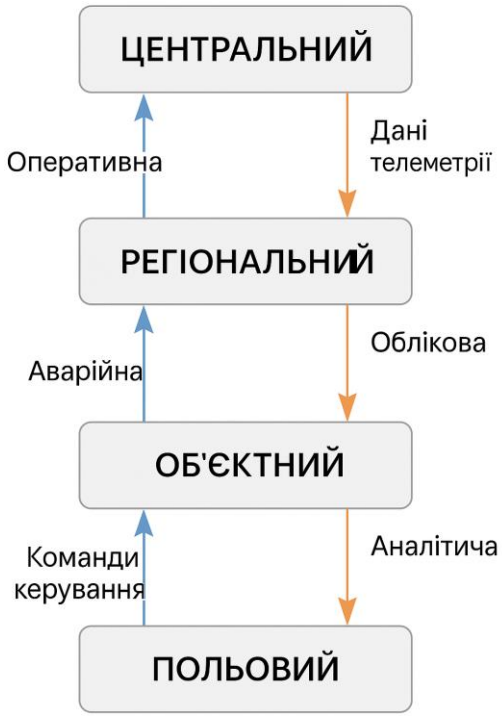

Рисунок 1.3 – Інформаційні потоки в ієрархії енергосистеми

Уся ця багаторівнева система неможлива без постійного інформаційного обміну. Від оперативного надходження інформації залежить:

– коректність регулювання частоти і потужності;

– забезпечення балансу виробництва і споживання електроенергії;

– виявлення аварій і прийняття запобіжних заходів;

– формування звітності та ведення обліку.

Інформація як об’єкт передачі має відповідати низці вимог що наведені в (табл. 1.1). Також у сучасних умовах особливої ваги набуває кіберзахищеність інформації, особливо в умовах загроз для критичної інфраструктури держави.

Таблиця 1.1 – Вимоги до передачі інформації в електроенергетиці

№	Вимога	Пояснення
1	Актуальність	Дані мають бути свіжими, не застарілими
2	Точність	Мінімальні похибки вимірювання
3	Цілісність	Дані не повинні бути спотворені
4	Своєчасність	Інформація має надходити в потрібний час
5	Надійність	Дані повинні бути доступні при збої в мережі
6	Безпека	Захист від несанкціонованого доступу

У традиційних системах телемеханіки інформація передавалася в аналоговому вигляді — наприклад, як струм 4–20 мА [4, 5]. У сучасних системах усе більше пристроїв перетворює фізичні сигнали в цифрову форму (рис. 1.4), що має низку переваг:

– висока точність;

– збереження цілісності;

– можливість шифрування;

– простота обробки та архівації;

– універсальність каналів передачі (мережі Ethernet, GSM, оптика).

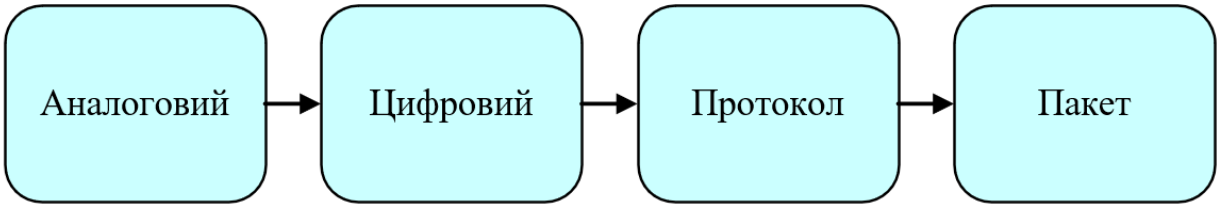

Рисунок 1.4 – Перетворення сигналів

До найпоширеніших пристроїв джерел інформації в електроенергетиці, належать:

– вимірювальні прилади (струм, напруга, температура);
– лічильники обліку (електролічильники, теплолічильники);
– RTU — для збирання даних на підстанціях;
– PLC — контролери автоматики;
– сенсори IoT — сучасні бездротові пристрої;
– системи SCADA — диспетчерські сервери;
– панелі HMI — операторські інтерфейси.

Усі ці пристрої не тільки вимірюють, а й передають інформацію далі — до керівного рівня або в хмарні сервіси.

Інформація в електроенергетиці є критично важливою складовою безперервного, безпечного та ефективного функціонування енергосистем. Від її якості, повноти та своєчасності залежить коректне керування мережами, попередження аварій, балансування системи, забезпечення потреб споживачів та інтеграція нових технологій, таких як Smart Grid, ВДЕ чи електромобільність.

Знання структури інформаційних потоків, типів даних, вимог до передачі, джерел і приймачів інформації є базовою передумовою для підготовки висококваліфікованих інженерів у сфері електроенергетики.

1.3.1. Математичне розуміння інформації

Інформація — це поняття, яке ми зазвичай сприймаємо інтуїтивно, і його неможливо повністю описати через інші базові величини. Будь-яка система містить у собі інформацію про власний стан, і цю інформацію можна передавати з відносно невеликими витратами ресурсів. Наприклад, креслення електростанції

чи підстанції містить багато структурних даних про об’єкт, проте на відміну від самої електростанції, його легко і швидко можна передати в будь-яке місце з мінімальними зусиллями.

Однією з важливих властивостей інформації є можливість її копіювання без втрати якості.

З *математичної точки зору* інформацію можна розглядати як міру впорядкування множини, що містить різні об’єкти. Для уявного позначення стану об’єкта використовують символи — наприклад, цифри від 0 до 9 представляють 10 різних станів. Визначення стану об’єкта можна вважати отриманням інформації про нього.

Міра інформації, пов’язана з системою, що може знаходитися у n можливих станах, розраховується за формулою (1.1).

$$I = \log_2 n. \tag{1.1}$$

Отже, міра інформації I відображає кількість інформації, що міститься в об’єкті, і дає оцінку обсягу цієї інформації. Для обчислення міри інформації зазвичай використовують логарифм із основою 2, хоча теоретично можна застосовувати й інші основи. Проте на практиці це трапляється досить рідко.

Якщо для обчислення логарифма використовується основа 2, то міра інформації вимірюється у бітах (*bit*). Біт є зручною одиницею для цифрової логіки, де його можна відобразити різними рівнями напруги або струму в електричному колі.

Якщо об’єкт може приймати лише один із двох станів ($n = 2$), то його інформаційний зміст дорівнює 1 біту:

$$I = \log_2 2 = 1 \text{ біт},$$

якщо 8 станів то 3 біти,

$$I = \log_2 8 = 3 \text{ біта},$$

якщо 10 станів то 3,32 біта,

$$I = \log_2 10 = 3{,}32 \text{ біта.}$$

Для об’єкта інформаційний вміст якого становить 3.32 біта або 10 можливих станів необхідно мінімум 4 ключі, які дозволяють представити 24=16 різних станів.

Наприклад, при передачі інформації про напругу, яка змінюється від 0 до 220 кВ з точністю до 1 кВ необхідно 8 біт інформації або 2^8=256 різних станів.

Головним параметром, що визначає канал зв’язку, є його пропускна здатність — кількість інформації, яку можна передати за одиницю часу. Зазвичай її вимірюють у бітах за секунду (біт/с).Правильно підібраний канал дозволяє передати необхідний обсяг даних за встановлений проміжок часу. Зазвичай, чим вища пропускна здатність каналу, тим більша його вартість. Пропускна здатність фізичного каналу тісно пов’язана з шириною пропускної смуги, потужністю сигналу та рівнем шуму в системі.

Пропускна смуга — це діапазон частот, який канал зв’язку може передавати, при цьому зниження потужності сигналу не перевищує 50 %. Цей параметр зазвичай вимірюють у герцах (Гц), кілогерцах (кГц) або мегагерцах (МГц), залежно від типу каналу. Пропускна смуга визначає здатність каналу передавати інформацію з потрібною якістю і швидкістю. Наприклад, у звичайній телефонній лінії пропускна смуга складає приблизно 3,1 кГц, що достатньо для передачі голосу, тоді як для телевізійного каналу вона значно ширша — близько 5,5 МГц, що дозволяє передавати високоякісне відео. Ширина пропускної смуги безпосередньо впливає на ефективність зв’язку.

Максимальна пропускна здатність каналу вимірюється у біт/с та визначається за виразом (1.2)

$$R_{\max} = 2 \cdot W \cdot \log_2 V, \qquad (1.2)$$

де W – пропускна смуга;

V – кількість рівнів сигналу.

1.3.2. Передача цифрової інформації

При передачі по фізичному середовищі сигнал вразливий до лінійних спотворень і впливу перешкод. Для зменшення впливу спотворень і перешкод послідовність бітової інформації, що передається, перетворюється в лінійний код, який передається по лінії зв'язку.

Залежно від спрямованого середовища (мідні або волоконно-оптичні кабелі, радіоканали) використовуються різні коди, які різною мірою стійкі до впливу лінійних спотворень та перешкод, мають різні властивості самосинхронізації та різні спектральні характеристики. Спектри сигналів під час використання різних кодів різняться. У багатоканальних системах передачі інформації по лінії зв'язку з обмеженою смугою пропускання спектр сигналу повинен бути вузькосмуговим, щоб по одній лінії передати багато повідомлень [15, 18–22].

Важливою характеристикою коду є властивість самосинхронізації. Устаткування на приймальній стороні повинне працювати синхронно з передавальною апаратурою, тому на приймальній стороні сигнал синхронізації виділяють із прийнятого сигналу. Для цього сигнал повинен досить часто змінювати свій стан (переходити з низького рівня до високого і навпаки). Якщо передається довга послідовність нулів або одиниць, синхронізація на приймальній стороні може бути втрачена. Тому вживаються заходи щодо штучної зміни стану сигналу, що передається.

Існують два основних способи передачі бітової послідовності фізичним каналом [15, 18–22]:

– відправлення бітів у лінію безпосередньо або в закодованому вигляді, при цьому зберігається цифровий характер інформації;

– модуляція несучої по амплітуді/частоті/фазі й передача модульованого сигналу.

Найпростіший спосіб передачі цифрових даних — це безпосереднє кодування. Наприклад, при такому кодуванні напруга 0 В відповідає логічному «0», а +10 В — логічній «1». Логічний «0» позначається як спокій (space), а «1» — як

імпульс (mark). Існує також зворотне кодування, коли «0» (спокій) позначається високим рівнем напруги, а «1» — низьким.

Популярним є й полярне кодування, за якого сигнали «0» і «1» мають однакові за величиною, але протилежні за знаком рівні напруги.

Всі ці методи — пряме, зворотне та полярне — відносяться до кодування без повернення до нуля (NRZ, Non-Return to Zero), оскільки сигнал не обов'язково повертається до нульового рівня між бітами. Якщо послідовність містить багато одиниць, то лінія буде тривалий час підтримувати високий або низький рівень відповідно до обраної схеми [15, 18–22].

Метод NRZ простий у реалізації, але чутливий до впливу перешкод і спотворень. Для компенсації загасання сигналу приймач інтерпретує будь-яку напругу нижче +2 В як логічний «0», а рівень вище +5 В — як логічну «1» (рис. 1.5).

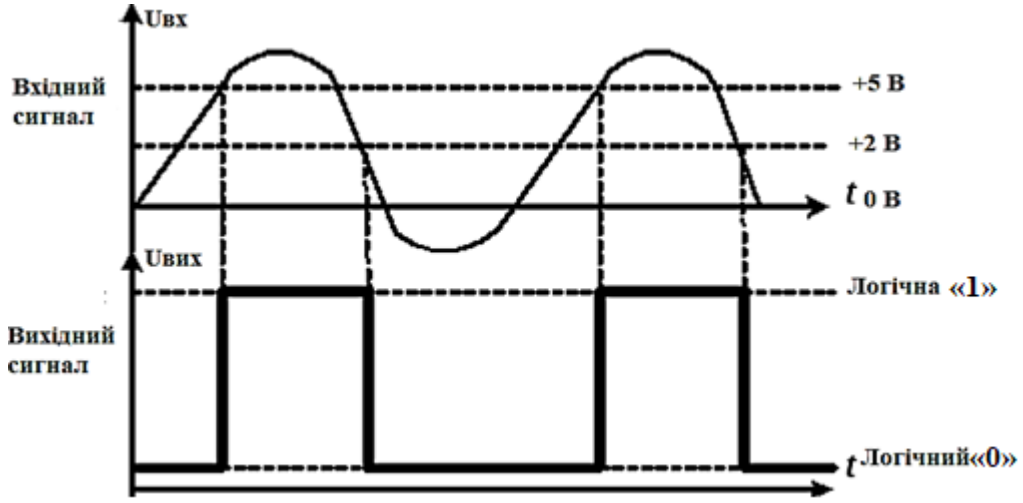

Рисунок 1.5 – Граничні значення для тригера Шмідта

Тригер Шмідта (Schmidt trigger), налаштований на ці рівні, можна використовувати для відновлення цифрового сигналу.

Знання опорного рівня (нуля) є необхідним лише при трирівневому кодуванні; у інших випадках абсолютний рівень сигналу не має значення для розпізнавання даних.

На (рис. 1.6) приведені найбільш розповсюдженні лінійні коди.

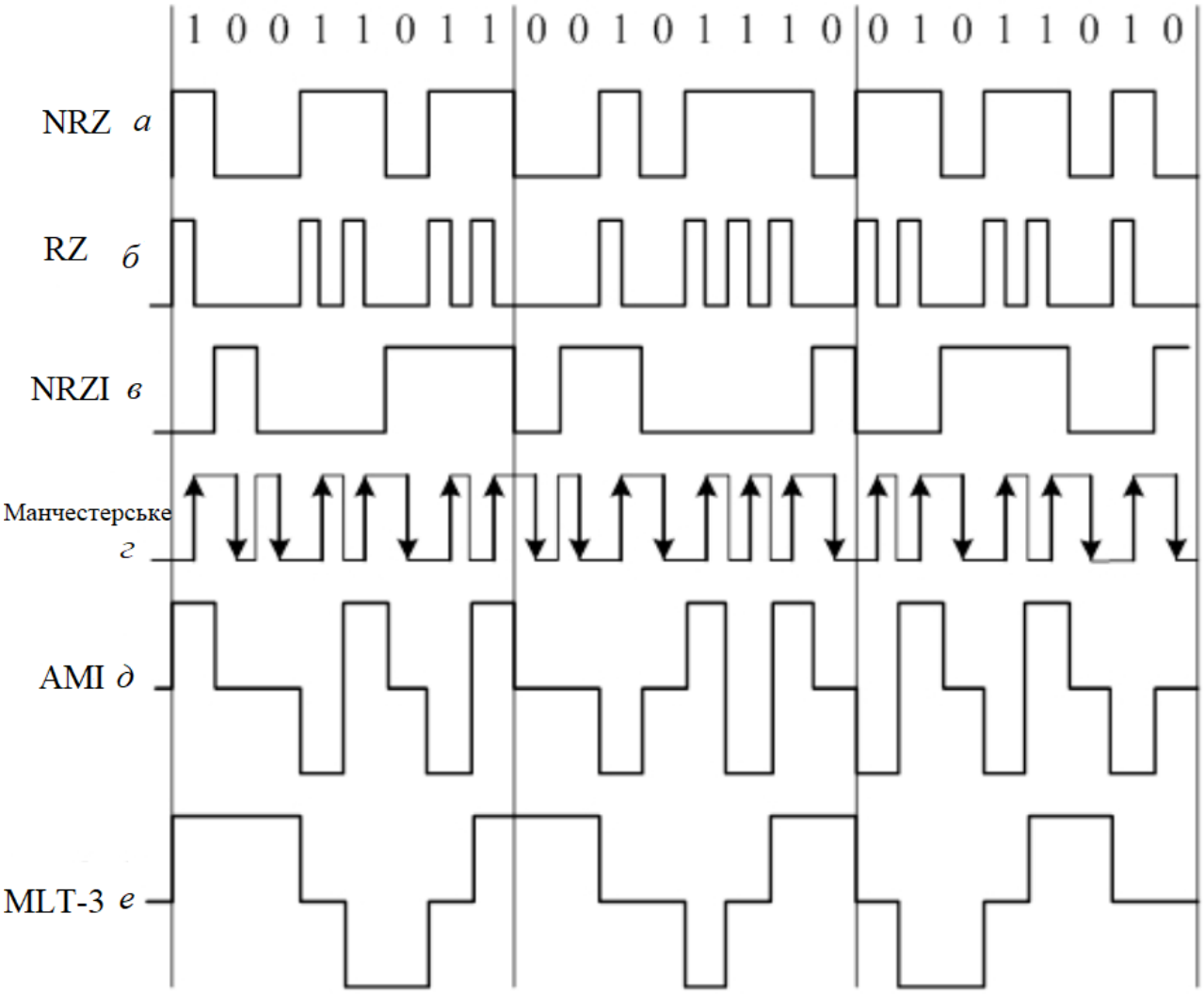

Рисунок 1.6 – Способи цифрового кодування: *а* – без повернення до нуля (NRZ); *б* –з поверненням до нуля (RZ); *в* – інверсне без повернення до нуля (NRZI); *г* – манчестерське кодування; *д* – альтернативна інверсія одиниць (AMI); *е* – трирівневе кодування (MLT-3)

Проте при використанні чистого NRZ-кодування виникає важлива проблема: приймач не може визначити, де починається і де закінчується кожен окремий біт (рис. 1.6, а).

Крім того, якщо передавач працює з різними швидкостями передачі, приймач не зможе одразу на початку сеансу визначити правильну швидкість. Іншими словами, чистий NRZ-код не дає змоги відрізнити відсутність повідомлення, якщо послідовність складається лише з нулів. Одним із рішень є додавання до

кожного повідомлення *преамбули* (спеціальної вставки) — послідовності чергування нулів і одиниць, що дозволяє синхронізувати передавач і приймач.

Проте навіть у цьому випадку існує ризик втрати синхронізації під час передачі, що може призвести до помилкової інтерпретації даних. Крім того, якщо всі імпульси мають однакову полярність, то розподілена ємність лінії може спричинити накопичення постійного електричного потенціалу.

Усі перелічені проблеми усуваються за допомогою кодування з поверненням до нуля (Return to Zero — RZ), як показано на (рис. 1.6, б). При цьому методі вихідні дані поєднуються із сигналом синхронізації. Аналогічно до прямого кодування, використовуються два рівні потенціалу: один відповідає логічному нулю, інший — логічній одиниці. Кожен біт починається з рівня потенціалу, що відповідає його значенню, а в середині імпульсу відбувається перехід до нульового рівня. Фронт цього переходу застосовується для синхронізації приймача.

Хоча RZ-кодування потребує приблизно вдвічі більшої пропускної смуги порівняно з NRZ і вимагає більш складної електроніки для інтерфейсних пристроїв, переваги цього методу значно переважають його недоліки.

Модифікований (інверсний) потенціальний код (Non-Return to Zero Inverted — NRZI) змінює свій стан на протилежний під час передавання нуля і не змінює — під час передавання одиниці (рис. 1.6, в). Його властивості самосинхронізації дещо кращі, ніж у кодування NRZ, тому він застосовується в технології Fast Ethernet за специфікацією 100Base-FX.

Для зменшення впливу перешкод і лінійних спотворень у мідних кабелях однополярні сигнали коду NRZ (RZ) перетворюються на біполярні (двополярні) імпульси. Хорошими властивостями самосинхронізації та стійкістю до дії завад характеризуються біполярні коди: Alternate Mark Inversion (AMI) та Multi-Level Transmission 3 (MLT-3) (рис. 1.6, д, е), відповідно.

Нульові біти коду AMI подаються нульовим рівнем сигналу, а одиничні біти — чергуванням значень +V, –V. Під час передавання нуля в коді MLT-3 значення сигналу не змінюється й залишається таким, як було до цього моменту. При передаванні одиниць сигнал змінюється в такій послідовності: +V, 0, –V, 0,

+V і т. д. Сигнали коду MLT-3 характеризуються вужчою смугою частот порівняно з кодом NRZI, модифікацією якого він є.

Коди AMI, MLT-3, як і інші біполярні коди, застосовуються для передавання інформації по мідних кабелях. Наприклад, код MLT–3 використовується в локальних мережах технології Fast Ethernet за специфікацією 100Base-TX.

Недоліком кодів AMI і MLT–3 є погана самосинхронізація при передаванні довгих послідовностей нулів, тому необхідне використання стаффінгу (вставлення бітів) або блочних кодів.

Найкращими властивостями самосинхронізації характеризується манчестерське кодування (рис. 1.6, г). Однак воно має ширшу смугу спектра частот порівняно з потенційним кодом NRZI і, особливо, — з біполярними кодами AMI, MLT-3. Манчестерський код використовувався в локальних мережах Ethernet за специфікацією 10Base-T. Проте смуга частот його спектра приблизно в 1,5 раза ширша, ніж у згаданих вище кодів.Тому в нових технологіях локальних мереж (Fast Ethernet, Gigabit Ethernet) манчестерське кодування не застосовується.

1.3.3. Перетворення неперервного сигналу в цифрову форму

Зазвичай у телевимірювальних системах передача інформації пов’язана з перетворенням сигналів. Іноді сигнали кілька разів трансформуються з однієї форми в іншу, при цьому більшість проміжних форм необхідна для спрощення та покращення якості передачі, а кінцеві форми мають забезпечувати сприйняття інформації людиною або машиною.

Інформація може бути представлена у вигляді безперервних або дискретних сигналів. Безперервні сигнали містять повідомлення, задані для будь-якого моменту часу, тобто вони є безперервними як у часовій, так і в амплітудній області.

Дискретні сигнали мають амплітуду, що приймає обмежену кількість значень. Перехід від безперервного до дискретного сигналу пов’язаний із округленням або перетворенням величини з безперервної шкали в дискретну. Процес

заміни безперервного сигналу окремими значеннями, рознесеними на певний скінченний інтервал, називається квантуванням за рівнем.

Під час квантування за рівнем значення безперервного сигналу у будь-який момент часу замінюють найближчим дискретним значенням, що називається рівнем квантування – b_i. Інтервал між двома дискретними значеннями називається кроком квантування – h.

На (рис. 1.7, а) ілюструється процес квантування. По осі ординат відкладається величина заздалегідь обраного кроку квантування h і проводяться лінії, паралельні осі часу, що показують рівні квантування. Перехід з одного рівня на інший відбувається, коли значення функції перебуває в середині інтервалу квантування, тому що в цей момент абсолютна похибка квантування виявляється найбільшою формула (1.3).

$$\varepsilon_{y\,\max} = \frac{h}{2}. \tag{1.3}$$

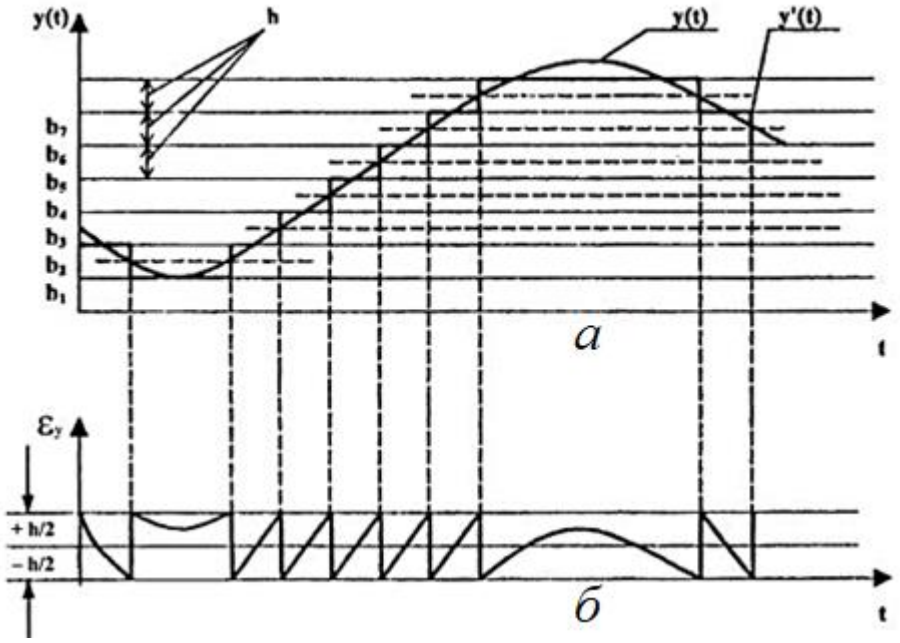

Рисунок 1.7 – Квантування за рівнем

Процес квантування здійснюється в такий спосіб: інтервали квантування діляться навпіл, і проводяться пунктирні горизонтальні лінії до їхнього перетину

із квантованим безперервним сигналом (функцією $y(t)$). У точках перетину значення функції $y(t)$ передається найменш точно і помилка квантування ε_y досягає максимального значення $\frac{h}{2}$. У цих точках відбувається перехід дискретної функції $y'(t)$ з одного рівня квантування на інший. В інших точках квантування виникає похибка квантування ε_y, рівна різниці між значеннями функцій $y(t)$ і $y'(t)$. Абсолютні значення цієї похибки ілюструються на (рис. 1.7, б), де по осі ординат відкладаються помилки квантування за рівнем ε_y, а по осі абсцис час t.

Аналогічно квантуванню за рівнем відбувається квантування за часом, під яким розуміється дискретизація за часом, тобто заміна безперервного в часі сигналу дискретним. Процес квантування показаний на (рис. 1.8, а). Він полягає в наступному: горизонтальна вісь часу ділиться на інтервали, що віддалені один від одного на однаковий інтервал квантування T_0. Далі проводяться вертикальні лінії до перетину із квантованим безперервним сигналом (функцією $y(t)$). У точках перетину визначаються значення функції $y(t_i)$, які зберігаються протягом інтервалу квантування T_0 (до найближчого перетину функції $y(t)$ з вертикальною лінією). Таким чином, утворюється дискретна за часом функція $y'(t)$. Різниця між значеннями функцій $y(t)$ і $y'(t)$дає значення похибки квантування за часом ε_t (рис. 1.8, б).

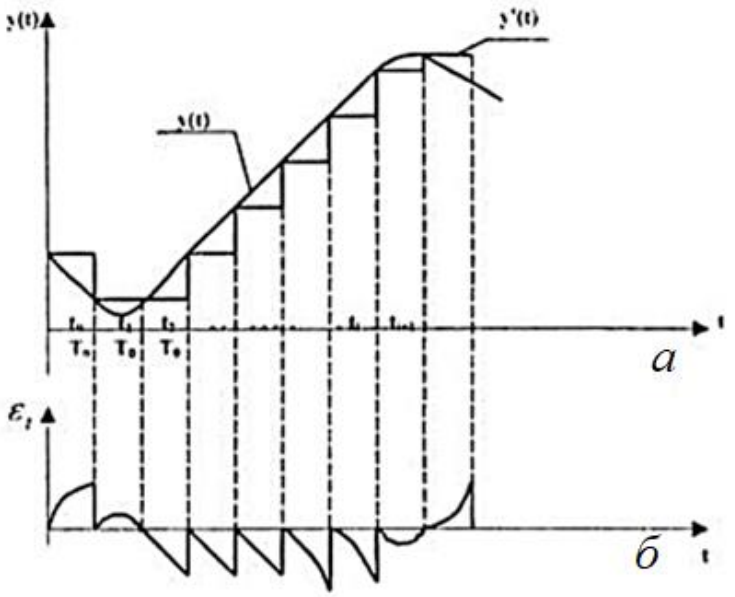

Рисунок 1.8 – Квантування за часом

У реальних системах при перетворенні аналогового сигналу в цифровий відбувається одночасне квантування, як за рівнем, так і за часом. На (рис. 1.9) представлено процес квантування безперервного сигналу $y(t)$ із кроком квантування за рівнем h і із кроком дискретизації за часом T_0. У результаті цього безперервний сигнал заміняється (апроксимується) дискретним сигналом.

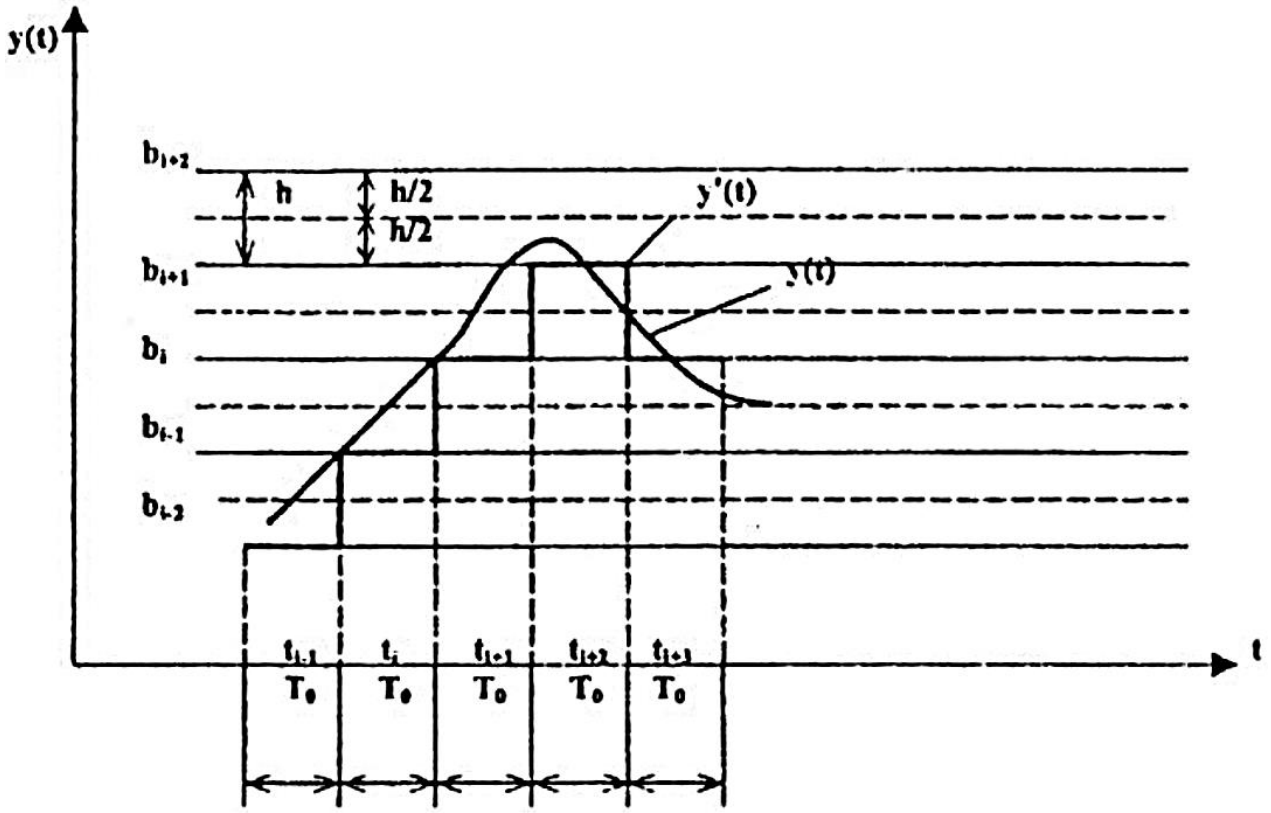

Рисунок 1.9 – Квантування за рівнем та часом

Таким чином, процес перетворення аналогового сигналу в цифровий складається із трьох етапів:

1) квантування за рівнем,

2) квантування за часом,

3) кодування рівня.

Кодування рівня полягає в оцінюванні кожного рівня квантування еквівалентним числом.

Розберемо для прикладу більш детально *похибку квантування за рівнем*.

Ця похибка є випадковою величиною, рівною різниці між фактичним значенням величини $y(t_i)$ і найближчим рівнем квантування (рис. 1.9) та (рис. 1.7, б). Як було зазначено вище, випадкова величина може характеризуватися своїм максимальним значенням формула 1.3 або середньоквадратичним $[\varepsilon_{y,\text{ск.}}]$.

Квадрат середньоквадратичного значення дорівнює математичному очікуванню квадрата випадкових різниць формула (1.4).

$$[\varepsilon_{y,\text{ск.}}]^2 = M[\varepsilon_y]^2. \tag{1.4}$$

Приймаючи розподіл випадкової величини ε_y у межах будь-якого кванта рівномірним одержимо, величину середньоквадратичної помилки квантування формула 1.5

$$[\varepsilon_{y,\text{ск.}}] = \frac{h}{2\sqrt{3}} = \frac{\varepsilon_{y\,\max}}{\sqrt{3}}. \tag{1.5}$$

Отже, максимально приведена похибка квантування за рівнем формула 1.6

$$\delta_{\text{к.}max\,\%} = \frac{\varepsilon_{y\,\max}}{h \cdot N_k} \cdot 100\,\% = \frac{1}{2} \cdot \frac{100\,\%}{N_k}, \tag{1.6}$$

де N_k – число рівнів квантування.

Середньоквадратична приведена похибка за рівнем формула 1.7.

$$\delta_{\text{ск. }\%} = \frac{\varepsilon_{y,\text{ск.}}}{h \cdot N_k} \cdot 100\,\% = \frac{1}{2} \cdot \frac{100\,\%}{N_k}. \tag{1.7}$$

Число рівнів квантування N_k визначається розрядністю кодованих сигналів, а саме — числом інформаційних розрядів кодового слова m формула 1.8

$$N_k = 2^m \tag{1.8}$$

Величина m визначається з виразу (1.8) по заданій величині наведеної похибки квантування за рівнем (1.6). Тривалість між відліком кожного параметра телевимірювань (ТВ), дорівнює кроку дискретизації T_0, визначається тривалістю циклу передачі багатоканальної системи ТВ (рис. 1.10).

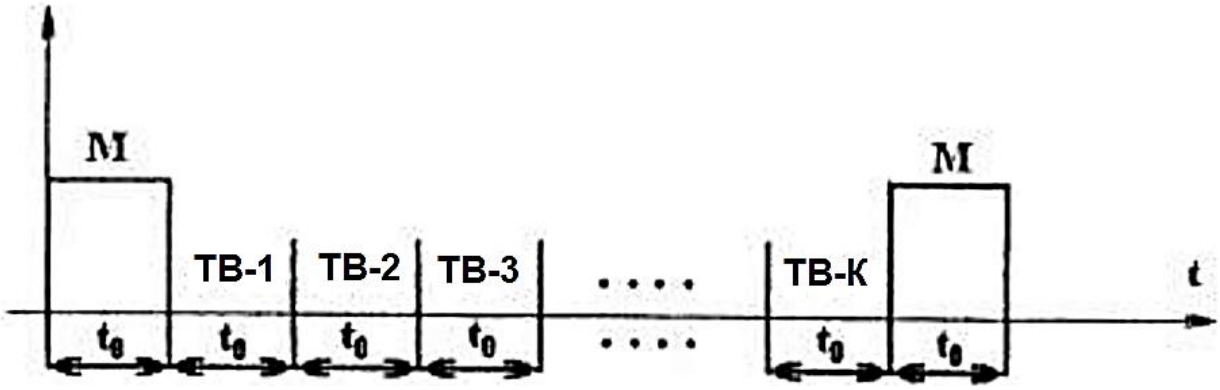

Рисунок 1.10 – Цикл передачі телевимірюваннь

Цикл передачі складається з маркеру синхронізуючого слова, – M і K кодових слів, де K – число каналів, звичайно рівне числу параметрів ТВ, що підлягають передачі. Якщо по тривалості маркерний імпульс дорівнює часу передачі ТВ по одному каналу, то тривалість циклу розраховується по формулі (1.9) або (1.10).

$$T_0 = (k+1) \cdot t_0, \tag{1.9}$$

де t_0 – тривалість передачі кодового слова, що відповідає одному телевимірюванню.

$$T_0 = (m+k) \cdot \tau_0, \tag{1.10}$$

де m і k – число інформаційних і контрольних розрядів у кодовому слові;

τ_0 – тривалість передачі одного розряду (біта) кодового слова.

Тривалість елементарного сигналу (біта) – τ_0 визначається шириною частотного спектра в каналі зв'язку, видом і способом модуляції. У найпростішому випадку наближену величину можна визначити по формулі (1.11) та (1.12).

$$\tau_0 = \frac{K}{\Delta F} \text{ для амплітудної модуляції,} \quad (1.11)$$

$$\tau_0 = \frac{2K}{\Delta F} \text{ для частотної модуляції,} \quad (1.12)$$

де ΔF – пропускна смуга фільтрів у Гц;

K – коефіцієнт, що залежить від припустимої величини викривлення форми переданих імпульсів ($K \approx 3 \div 5$).

Потім величину τ_0 необхідно округлити до величини, що забезпечує стандартну швидкість передачі інформації f_0 = 50; 100; 600; 1200; 2400; 4800; 9600 бод [біт/с]. Швидкість передачі інформації розраховується за формулою (1.13).

$$f_0 = \frac{1}{\tau_0}. \quad (1.13)$$

1.3.4. Модуляція сигналів

Передача інформації здійснюється за допомогою сигналів, які фактично є її фізичним носієм. Однак у деяких випадках сформовані сигнали неможливо без спотворень передати через обрану лінію або канал зв'язку через невідповідність характеристик сигналу та каналу передачі. Одним із способів, який дозволяє передавати первинні інформаційні сигнали без викривлень по заданому каналу, є модуляція.

Модуляція — це процес зміни параметрів певного «переносника» інформації під впливом переданого первинного або закодованого сигналу, тобто сигналу, що містить інформацію [22].

В якості переносника інформації можуть використовуватися гармонічні коливання (змінний струм або напруга змінного струму), імпульсні коливання, зазвичай прямокутної форми, електромагнітні хвилі або постійний струм. Таким чином, модуляція — це метод перетворення первинних сигналів у сигнали іншої форми з певними характеристиками, які забезпечують їх передачу на великі відстані через обрані лінії або канали зв'язку. Сигнал, що утворюється в результаті модуляції, називається *модульованим*, а сигнал, що змінює параметри

переносника, — *модулюючим*. Роль модулюючого сигналу можуть виконувати, наприклад, сигнали з виходів датчиків, таких як датчики вимірювальної інформації, або закодовані сигнали. Важливо, щоб модульований і модулюючий сигнали містили однакову кількість інформації, а процес модуляції не призводив до її спотворення [22].

Види модуляції класифікуються відповідно до типу використовуваного сигналу-переносника. Зазвичай виділяють аналогову (безперервну) та імпульсну модуляцію. У випадку аналогової модуляції носієм сигналу є гармонічні коливання — це може бути змінна напруга, струм або електромагнітні хвилі, іноді — навіть постійний струм. У цифрових системах зв'язку найчастіше застосовується змінний струм або напруга як переносник. Що стосується імпульсної модуляції, то в ній роль носія виконують періодичні імпульси, зазвичай прямокутної форми.

Залежно від параметра переносника, який змінюється під дією модулюючого сигналу, розрізняють наступні види модуляції:

1) Безперервна модуляція:

а) амплітудна модуляція (АМ);

б) частотна модуляція (ЧМ);

в) фазова модуляція (ФМ).

Відповідно в змінному струмі змінюється або амплітуда, або частота, або фаза коливань, інші ж параметри переносника залишаються незмінними [22].

2) Імпульсна модуляція:

а) амплітудно-імпульсна модуляція (АІМ);

б) широтно-імпульсна модуляція (ШІМ);

в) частотно-імпульсна модуляція (ЧІМ);

г) фазо-імпульсна модуляція (ФІМ);

д) кодоімульсна або імпульсно-кодова модуляція (ІКМ).

Розглянемо види безперервної модуляції, коли переносником є гармонічні коливання. Ці види найбільш часто застосовуються і прості для розуміння.

Амплітудна модуляція гармонічних коливань. При АМ модулюючий сигнал змінює амплітуду несучого сигналу, тоді як його частота та фаза залишаються

постійними. Розглянемо найпростіший випадок – модуляцію гармонічним сигналом («чистим тоном»). Припустимо, що переносник описується наступним виразом за формулою (1.14) [22].

$$U_0(t) = U_0 \cos(\omega_0 t), \tag{1.14}$$

де U_0 – початкове значення амплітуди переносника;

ω_0 – початкове значення кутової частоти переносника, розраховується за формулою (1.15).

t – час коливань переносника.

$$\omega_0 = \frac{2\pi}{T_0}, \tag{1.15}$$

де T_0 –початковий період коливань переносника (несучої частоти), розраховується за формулою (1.16).

$$T_0 = \frac{1}{f_0}, \tag{1.16}$$

де f_0 – частота коливань переносника.

Значення модулюючого сигналу розраховуємо за формулою (1.17)

$$U_\Omega(t) = U_\Omega \cos(\omega_\Omega t), \tag{1.17}$$

де U_Ω – амплітуда модулюючого сигналу;

ω_Ω – кутова частота модулюючого сигналу розраховується аналогічно формулі (1.15) де T_0 заміняється на T – період коливань модулюючого сигналу. Відповідно, у формулі (1.16) f_0 замінюється на f – частота модулюючого сигналу.

Сигнал АМ можна описати залежністю (1.18) [22].

$$U_{\text{АМ}}(t) = U_0 \cos(\omega_0 t) + U_\Omega \cos(\omega_\Omega t) \cdot \cos(\omega_0 t). \quad (1.18)$$

Замінимо добуток косинусів відомим у тригонометрії виразом, остаточно отримаємо формулу (1.19).

$$U_{\text{АМ}}(t) = U_0 \cos(\omega_0 t) + 0{,}5U_0 \cdot m_A \cdot \cos\big((\omega_0 + \omega_\Omega) \cdot t\big) + 0{,}5U_0 \cdot m_A \cdot \cos\big((\omega_0 - \omega_\Omega) \cdot t\big). \quad (1.19)$$

де m_A – постійний коефіцієнт, який називають глибиною модуляції, розраховується за формулою (1.20).

$$m_A = \frac{U_\Omega}{U_0}. \quad (1.20)$$

Основними умовами здійснення правильної амплітудної модуляції є 1.20 та (1.21).

$$\omega_0 \gg \omega_\Omega \quad (1.20)$$

$$m_A \leq 1 \quad (1.21)$$

Частота несучої повинна бути в багато разів (5...10) більше частоти модулюючого сигналу, а глибина модуляції – менше або дорівнює одиниці.

Варто відмітити, що в амплітудній модуляції можлива окрема модуляція позитивних (верхніх) і негативних (нижніх) півхвиль амплітуди коливань. Це дозволяє передавати два різні інформаційні сигнали одночасно на одній несучій частоті. Такий вид амплітудної модуляції одержав назву полярної АМ.

Процеси амплітудної модуляції ілюструються тимчасовими діаграмами, наведеними на (рис. 1.11). Огинаюча амплітуди коливань повністю повторює форму, що модулює сигнал $U_\Omega(t)$.

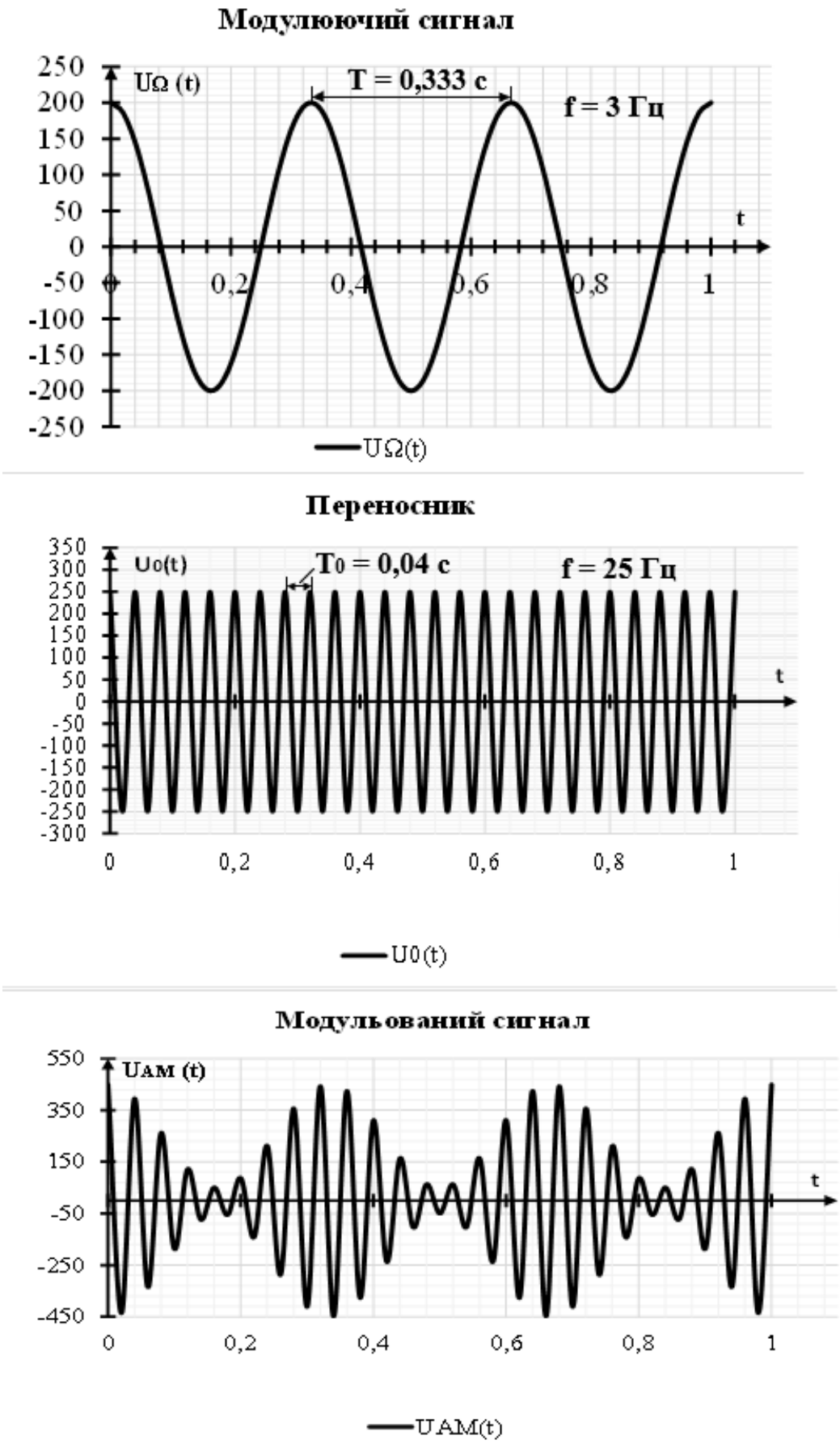

Рисунок 1.11 – Амплітудна модуляція гармонічних сигналів

Частотна й фазова модуляція сигналів. При частотній модуляції під дією модулюючого сигналу змінюється частота переносника, а при фазовій модуляції – фаза коливань переносника. Амплітуда ж переносника залишається незмінною, а при фазовій модуляції і частота переносника повинна залишатися незмінною. Розглянемо приклади модуляції «чистим тоном», тобто коли модулюючий сигнал є гармонічним.

В окремому випадку, коли амплітуда сигналу, що модулює, умовно дорівнює одиниці, його можна описати виразом (1.22).

$$U_\Omega(t) = 1 \cdot \cos(\omega_\Omega t). \tag{1.22}$$

Кутову частоту переносника можна визначити за виразом (1.23).

$$\omega = \omega_0 + \Delta\omega_0 \cdot \cos(\omega_\Omega t), \tag{1.23}$$

де $\Delta\omega_0$ – максимальне відхилення частоти переносника від початкового значення, яке називається девіацією частоти, розраховується за формулою (1.24).

$$\Delta\omega_0 = 2\pi f_{\text{дев}}, \tag{1.24}$$

де $f_{\text{дев.}}$ – частота девіації, Гц.

Частота девіації – це максимальна зміна частоти несучого сигналу відносно його середнього (номінального) значення під впливом модуляційного сигналу. Або наскільки сильно частота сигналу може «відхилятись» вгору або вниз при передачі інформації, формально це $f_{\text{дев.}} = \Delta f =$ максимальне відхилення частоти несучої.

Фазовий кут визначаємо за виразом (1.25).

$$\varphi = \Delta\varphi \cdot sin(\omega_\Omega t). \tag{1.25}$$

Переносник будемо описувати виразом (1.26).

$$U(t) = U_0 \cos(\omega t + \varphi). \tag{1.26}$$

Сигнал ЧМ $U_{\text{ЧМ}}(t)$ та сигнал ФМ $U_{\text{ФМ}}(t)$ знайдемо за виразами (1.27) та (1.28).

$$U_{\text{ЧМ}}(t) = U_0 \cos\big(\omega_0 t + m_f \cdot sin(\omega_\Omega t)\big). \tag{1.27}$$

$$U_{\text{ФМ}}(t) = U_0 \cos(\omega_0 t + \Delta\varphi \cdot sin(\omega_\Omega t)). \tag{1.28}$$

де m_f – коефіцієнт, що називається індексом частотної модуляції, розраховується за формулою (1.29);

де $\Delta\varphi = m_\varphi$ – це індекс фазової модуляції, або фазова девіація (максимальне фазове відхилення, рад.), розраховується за формулою (1.30).

$$m_f = \frac{\Delta\omega_0}{\omega_\Omega}. \tag{1.29}$$

$$m_\varphi = k_\varphi \cdot U_\Omega, \tag{1.30}$$

де k_φ – коефіцієнт фазової модуляції, рад/В, показує, наскільки сильно змінюється фаза несучої в радіанах на кожен вольт модуляційного сигналу, його значення залежить від модулятора який використовується.

Діаграми сигналів, що ілюструють процеси частотної і фазної модуляції переносника, наведені на (рис. 1.12) і на (рис. 1.13), відповідно.

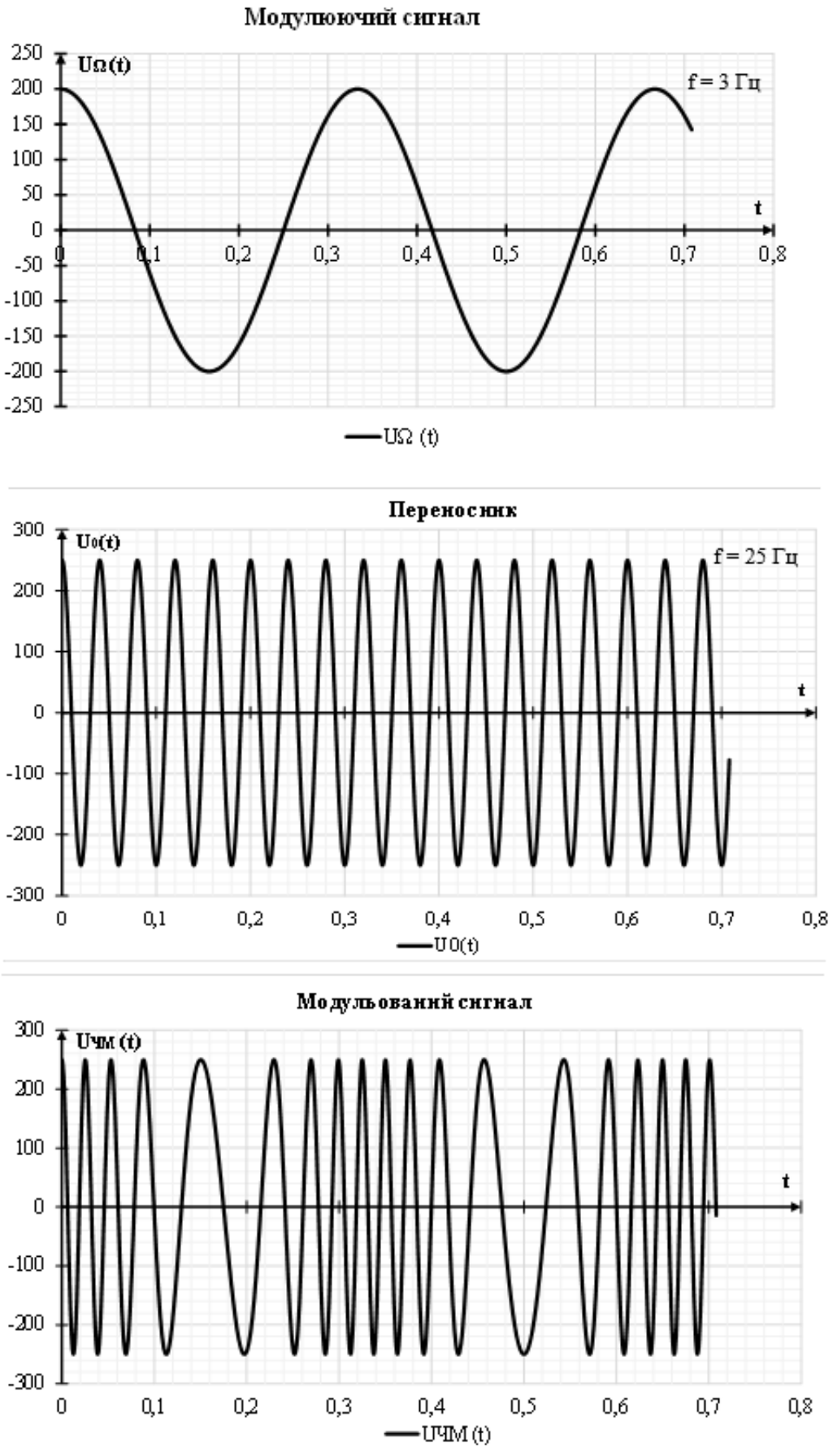

Рисунок 1.12 – Частотна модуляція гармонічних сигналів

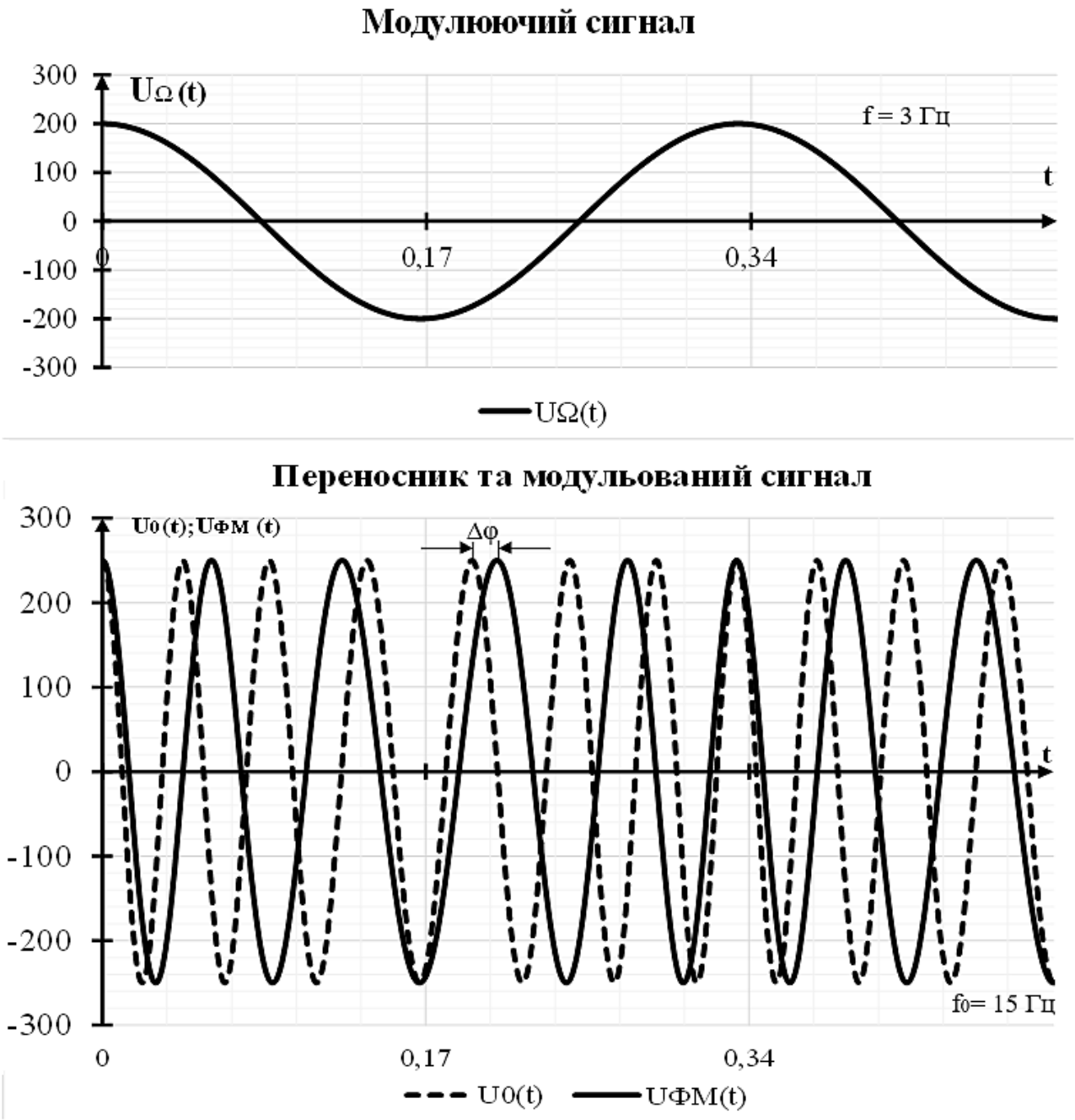

Рисунок 1.13 – Фазна модуляція гармонічних сигналів

1.4. Основні функції систем передачі інформації

Системи передачі інформації (СПІ) в електроенергетиці є критично важливою інфраструктурою, яка забезпечує своєчасне, надійне та точне передавання даних між різними об’єктами енергетичної системи. Вони виконують ключову роль у забезпеченні стабільної роботи енергосистеми, зокрема — в процесах автоматичного керування, диспетчеризації, моніторингу, діагностики та релейного захисту [13–15, 21–24].

Сучасні енергетичні системи функціонують у складних і динамічних умовах, тому функціональність СПІ є багатогранною та охоплює широкий спектр задач. Основні функції СПІ можна поділити на кілька категорій залежно від їхньої ролі в структурі управління та технологічному процесі.

Однією з основних функцій СПІ є передача телеметричних даних — інформації про поточні параметри роботи обладнання та технологічних процесів. Це такі дані, як [13–15, 21–24]:

– напруга, струм, частота;

– потужність (активна, реактивна);

– положення перемикачів, стан обладнання;

– температурні режими, рівень навантаження тощо.

Телеметричні дані передаються у режимі реального часу або з незначною затримкою і є основою для прийняття рішень на всіх рівнях управління енергосистемою.

Передача команд керування. СПІ забезпечують передачу керуючих сигналів від диспетчерських або автоматичних систем до об’єктів управління:

– включення/вимкнення обладнання;

– перемикання комутаційних апаратів;

– зміна режимів регулювання (наприклад, регулювання реактивної потужності трансформаторами з РПН).

Надійність і швидкість виконання цієї функції є критичними, особливо у випадках аварійного керування або релейного захисту.

Забезпечення релейного захисту та протиаварійної автоматики. Для реалізації складних алгоритмів захисту та автоматики, СПІ передають сигнали між різними елементами енергосистеми, у тому числі:

– команди на швидке відключення елементів мережі;

– сигнали синхронізації;

– інформацію про аварійні стани та події.

Такі системи, як IEC 61850 GOOSE, використовуються для високошвидкісного обміну повідомленнями між пристроями захисту.

Синхронізація часу. Точна синхронізація часу є критично важливою для коректного аналізу подій, що відбуваються в енергосистемі, зокрема при роботі автоматизованих систем діагностики, реєстрації аварій, або при роботі ПТК АСУ ТП. Джерелами синхронізації зазвичай виступають GPS або інші точні годинники [13–15, 21–24].

Забезпечення зв'язку між підсистемами SCADA *та* АСУ ТП. SCADA та АСУ ТП (автоматизовані системи управління технологічними процесами) є основними платформами керування в електроенергетиці. СПІ забезпечують:

– передачу інформації з польового рівня (датчики, виконавчі механізми) до верхніх рівнів SCADA;

– збір і обробку даних;

– дистанційний моніторинг і управління об'єктами.

Завдяки цьому забезпечується централізоване управління енергосистемою.

Передача даних на рівень диспетчерських центрів. СПІ забезпечують комунікацію між об'єктами енергетики (електростанціями, підстанціями, РП, ТП) та регіональними або центральними диспетчерськими центрами, які приймають рішення щодо балансування навантаження, планових і аварійних перемикань, роботи генерації [13–15, 21–24].

Ведення протоколів та реєстрація подій. Системи передачі інформації є джерелом інформації для систем реєстрації подій, які фіксують усі зміни стану обладнання та ключові події в мережі. Це дає змогу:

– аналізувати аварії та нештатні ситуації;

– провести технічне обґрунтування дій персоналу;

– визначати причини відмов.

Забезпечення інформаційної безпеки. Сучасні СПІ включають в себе функції захисту переданої інформації від:

– несанкціонованого доступу;

– зовнішніх кібератак;

– модифікації або втрати даних.

Для цього використовуються методи шифрування, цифрового підпису, сегментації мережі, а також протоколи безпеки (наприклад, IEC 62351).

Можливість інтеграції з розумними мережами (Smart Grid). Функції СПІ поступово розширюються відповідно до потреб Smart Grid, що вимагає інтеграції з такими підсистемами як:

– відновлювана генерація;

– зарядні станції для електромобілів;

– smart metering;

– системи прогнозування та оптимізації навантаження.

Це вимагає розширення функціоналу СПІ, підтримки нових стандартів і адаптивної архітектури.

Системи передачі інформації в електроенергетиці виконують широкий спектр функцій, без яких неможливе ефективне управління, забезпечення безпеки, оперативне реагування на аварійні ситуації та інтеграція новітніх технологій. Вони є основою для реалізації концепцій Smart Grid, цифрової трансформації галузі та енергетичної стійкості.

1.5. Структура інформаційної взаємодії в енергетичних системах

Інформаційна взаємодія в енергетичних системах — це сукупність процесів, механізмів і структур, що забезпечують передавання, обробку та використання інформації між різними об’єктами енергетичної інфраструктури. У контексті сучасної цифрової трансформації електроенергетики структура такої взаємодії має ієрархічний, децентралізований та міжмережевий характер, що дозволяє забезпечити високу гнучкість, надійність та масштабованість.

Основні принципи побудови інформаційної взаємодії. Структура інформаційної взаємодії визначається рядом принципів, серед яких:

– ієрархічність — інформаційна система будується у вигляді декількох рівнів: польовий, об’єктовий, регіональний, центральний;

– модульність — кожен рівень виконує окремі функції і взаємодіє з іншими через стандартизовані інтерфейси;

– сумісність — використання єдиних протоколів (IEC 60870, IEC 61850, DNP3, тощо) дозволяє забезпечити обмін між різними виробниками обладнання;

– безперервність обміну — забезпечення постійного зв'язку між елементами для підтримання актуальності інформації;

– безпека та надійність — інформаційна взаємодія передбачає високий рівень захисту від помилок, збоїв і кібератак;

Ієрархічна модель рівнів інформаційної взаємодії. Інформаційна взаємодія в енергетичній системі зазвичай поділяється на такі рівні:

1) Польовий рівень (Field Level). Це базовий рівень, на якому працюють первинні пристрої — датчики, вимірювальні перетворювачі, реле, виконавчі механізми, лічильники. Основні особливості:

а) високочастотне опитування (до мілісекунд);

б) локальні шини Modbus, PROFIBUS, CAN, Ethernet/IP;

в) взаємодія з пристроями PCL, RTU.

2) Об'єктний рівень (Station Level). Розташований на рівні підстанцій або електростанцій. Сюди входять:

а) сервери збору та обробки даних SCADA;

б) інтерфейси оператора HMI;

в) пристрої захисту, автоматики та контролю IED.

Обмін відбувається через шини процесу і станційного рівня (наприклад, відповідно до стандарту IEC 61850).

3) Регіональний рівень (Regional Level). На цьому рівні здійснюється координація роботи групи об'єктів (наприклад, регіонального диспетчерського центру):

а) обробка агрегованих даних;

б) розрахунок режимів;

в) координація роботи підлеглих підстанцій;

г) прогнозування навантажень і генерації.

4) Центральний (національний) рівень (Control Center Level). Національний центр керування енергосистемою (НЕК «Укренерго») здійснює [27]:

а) загальносистемне балансування;

б) обмін інформацією з іншими країнами/операторами мереж;

в) прийняття рішень на основі великомасштабного аналізу даних;

г) інтеграцію відновлюваної генерації, гнучкого споживання, прогнозування аварій.

У межах згаданих рівнів відбувається кілька основних типів інформаційної взаємодії:

1) горизонтальна взаємодія — між пристроями одного рівня (наприклад, між IED на підстанції);

2) вертикальна взаємодія — між різними рівнями (наприклад, між SCADA і датчиками або центральним сервером і об'єктом);

3) зовнішня взаємодія — з іншими системами: системи ринку електроенергії, телекомунікаційні оператори, інформаційні платформи;

Ефективність взаємодії значною мірою залежить від застосування відповідних протоколів та IT–платформ:

– IEC 60870–5–101/104 — передача даних з RTU до SCADA;

– IEC 61850 — обмін на рівні підстанції (високошвидкісний і стандартний GOOSE, MMS);

– DNP3 — альтернативний протокол, що широко використовується у США та Канаді;

– OPC UA — стандартизований протокол для промислової взаємодії;

– MQTT/REST API — в сучасних IoT-інтегрованих енергосистемах.

На рисунку 1.14 представлена типова схема взаємодії в сучасній енергосистемі, побудованій за принципами Smart Grid.

На рисунку 1.14 показана взаємодія між:

– інтелектуальними пристроями обліку;

– системою керування навантаженням;

– розподіленою генерацією;

– системою управління енергомережами;

– системами балансування (автоматичне регулювання генерації);

– інформаційно-аналітичними центрами.

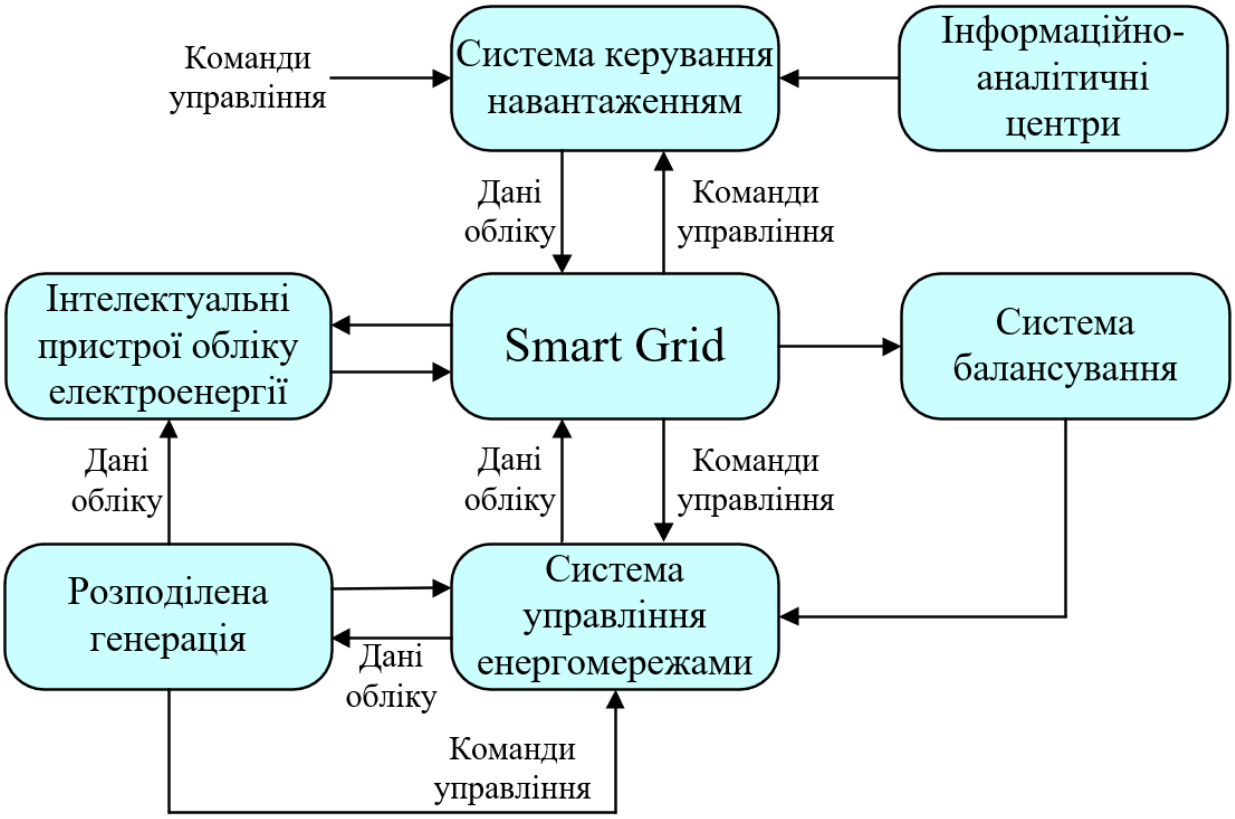

Рисунок 1.14 – Типова структура інформаційної взаємодії в енергетичній системі

З розвитком Smart Grid структура інформаційної взаємодії може ускладнюватися. До неї можуть входити нові елементи:

– енергетичні хаби;

– IoT-сенсори в мережі;

– прогнозні модулі (на основі штучного інтелекту);

– децентралізовані блокчейн-системи обліку.

Це потребує інтеграції з хмарними платформами, адаптивними протоколами і високошвидкісними каналами зв’язку (LTE, 5G, оптика). Побудова інтелектуальної взаємодії. Побудова такої складної інформаційної взаємодії не обходиться без проблем так викликів. До основних з них належать:

– несумісність устаткування різних виробників;

– кібератаки та загрози безпеці даних;

– недостатня швидкість каналів зв’язку;

– складність інтеграції нових технологій;

– висока вартість модернізації існуючих систем.

Структура інформаційної взаємодії є критично важливим елементом сучасної енергетичної системи. Вона забезпечує збирання, передавання, обробку та захист інформації, необхідної для надійної та ефективної роботи енергосистеми. З розвитком цифрових технологій структура постійно ускладнюється, трансформуючись у сторону децентралізованих, інтелектуальних та масштабованих рішень, орієнтованих на інтеграцію в Smart Grid.

1.6. Класифікація систем передачі інформації

У сучасних електроенергетичних системах передача інформації є ключовим елементом функціонування всієї інфраструктури. Завдяки ефективним системам передачі забезпечується диспетчерське управління, контроль за параметрами мережі, реалізація протиаварійних алгоритмів, автоматизація обліку електроенергії, обмін даними з об’єктами генерації, розподілу та споживання. Враховуючи багатофункціональність, різноманітність технічних рішень, середовищ та технологій передачі, виникає потреба в систематизації знань через класифікацію систем передачі інформації.

Класифікація систем передачі дозволяє структурувати інформацію про існуючі технології, полегшує вибір оптимального рішення для конкретного випадку, а також служить основою для навчання та стандартизації галузі. У цьому підрозділі наведено розгорнуту класифікацію за різними ознаками: функціональним призначенням, середовищем передачі, способом модуляції та обробки сигналів, рівнем взаємодії, топологією, середовищем застосування та інноваційними критеріями.

Класифікація систем передачі інформації поділяється на такі основні елементи:

1) Класифікація за функціональним призначенням:

а) системи моніторингу. Використовуються для безперервного або періодичного зчитування даних з елементів електроенергетичної інфраструктури. Основні приклади:

– SCADA-системи — забезпечують збирання, обробку та передачу даних до диспетчерських центрів;

– WAMS — забезпечують моніторинг у режимі реального часу на великій території, з використанням фазометричних вимірювальних пристроїв (PMU);

– системи діагностики обладнання — надають інформацію про технічний стан трансформаторів, вимикачів, кабелів тощо.

б) системи керування. Призначені для реалізації команд управління об’єктами енергосистеми:

– дистанційне керування комутаційною апаратурою;

– автоматичне регулювання генерації;

– системи автоматичного відновлення живлення.

в) системи захисту. Це найвідповідальніші системи, що реагують на аварійні ситуації:

– релейний захист із цифровими каналами зв’язку;

– протиаварійна автоматика (ПА), зокрема централізовані системи ПА із координацією дій між об’єктами.

г) системи обліку:

– інтелектуальні лічильники;

– автоматизовані системи комерційного обліку електроенергії (АСКОЕ).

– системи побутового обліку з віддаленим доступом.

2) Класифікація за середовищем передачі:

а) провідникові системи:

– оптоволоконні системи (FOC);

– виті пари (Ethernet, RS-485);

– PLC (Power Line Communication).

Переваги: стійкість до перешкод, висока швидкість, безпека. Недоліки: складність монтажу, залежність від фізичної цілісності кабелів.

б) бездротові системи:

– радіозв’язок;

– мобільний зв’язок: GSM, 3G, 4G, 5G;

– Low Power Wide Area Network (LPWAN) технології: LoRaWAN, NB-IoT;

– супутниковий зв’язок для віддалених об’єктів.

Переваги: мобільність, швидке розгортання, гнучкість. Недоліки: залежність від умов зовнішнього середовища, потреба в електроенергії.

в) гібридні системи. Поєднують провідні й бездротові технології, наприклад, SCADA з (GSM-зв’язком), або DER (розподілена генерація) із дублюючим зв’язком через LTE й оптоволокно.

3) Класифікація за способом обробки та кодування сигналів:

а) аналогові системи. Використовувалися у перших системах автоматики. Характеризуються високою чутливістю до шумів і обмеженою функціональністю. Зараз майже не використовуються.

б) цифрові системи. Працюють з дискретними сигналами. У таких системах можливе кодування, стискання та шифрування даних, що значно підвищує ефективність і безпеку.

в) системи з протокольним обміном:

– IEC 61850 (для підстанцій);

– IEC 60870-5-104 (віддалене керування);

– DNP3 (переважно в Північній Америці).

Протоколи гарантують сумісність пристроїв різних виробників.

4) Класифікація за рівнем охоплення:

а) локальні системи. Функціонують в межах одного об’єкта (електропідстанції, електростанції). Зазвичай мають високу швидкодію і надійність;

б) регіональні системи. Охоплюють декілька об’єктів. Наприклад, диспетчерський центр регіонального рівня обмінюється даними з 20–50 підстанціями;

в) загальнонаціональні системи. Інтегрують дані з усієї енергосистеми країни. Зазвичай передбачають використання резервування, VPN, централізованих дата-центрів;

г) наднаціональні системи. Наприклад, взаємодія між енергосистемами країн ENTSO-E або між Україною та Європою після синхронізації з ENTSO-E.

5) Класифікація за топологією:

а) радіальна. Центральний вузол координує всі периферійні. Недолік — вразливість до відмови центрального елемента;

б) кільцева. Забезпечує резервування. При виході з ладу однієї ділянки інформація йде в протилежному напрямку;

в) мережева. Має найвищу відмовостійкість. Використовується в Smart Grid, IoT та розподілених системах.

6) Класифікація за середовищем використання:

а) магістральні електричні мережі. Системи для синхронізації, протиаварійної автоматики. Висока пропускна здатність і надійність;

б) розподілені мережі. Контроль якості електроенергії, керування розподіленням генерації, розумні лічильники;

в) побутові та комерційні об’єкти. Smart Home, керування навантаженням, побудова мікромереж, інтеграція з енергетичними спільнотами.

7) Класифікація за сучасним підходом:

а) інтелектуальні системи. Здатні до самонавчання, використання штучного інтелекту. Наприклад, прогнозування навантажень, виявлення аномалій;

б) Кіберфізичні системи. Об’єднують фізичні пристрої та цифрові моделі, зокрема — цифрові двійники об’єктів електроенергетики;

в) IoT-платформи. Платформи на основі хмарних технологій, що обслуговують мільйони пристроїв у режимі реального часу.

Класифікація систем передачі інформації є критично важливою для розуміння ієрархії, функціональності та технічних особливостей засобів інформаційного забезпечення енергетичних об’єктів. Вона дозволяє здійснювати обґрунтований вибір архітектури системи, оцінювати ризики, підвищувати ефективність управління, захисту та обліку.

1.7. Еволюція технологій: від телемеханіки до цифрових мереж

Сучасна електроенергетика є складною, багаторівневою та високотехнологічною системою, ефективне функціонування якої неможливе без надійної передачі інформації. Системи зв'язку та обміну даними в енергетиці пройшли тривалий еволюційний шлях — від перших механічних та аналогових рішень до сучасних цифрових мереж, що охоплюють Інтернет речей, хмарні технології та штучний інтелект. Цей розвиток зумовлений необхідністю підвищення гнучкості, надійності, безпеки та швидкодії управління енергетичними об'єктами на всіх рівнях.

Перші кроки в напрямку автоматизації енергетики були зроблені ще на початку XX століття. Телемеханіка стала основою дистанційного керування технологічними процесами, дозволяючи передавати сигнали «вмикання/вимикання» на великі відстані. Основною метою було забезпечення оперативного управління об'єктами електропостачання та оперативного контролю стану обладнання.

Основні риси телемеханічних систем:

– аналогова передача сигналів — використання електричних імпульсів або струмів для передачі інформації;

– електромеханічні реле — для фіксації та виконання команд;

– дротові лінії зв'язку — як основний канал передачі;

– обмежена функціональність — відсутність зворотного зв'язку, вузький

– спектр керованих параметрів.

Попри свою простоту, телемеханіка дозволила значно підвищити ефективність енергосистем, скоротивши час реагування диспетчерів та покращивши контроль за роботою об'єктів у віддалених регіонах.

1.7.1. Системи телемеханіки

Система телемеханіки — це об'єднання технічних засобів, до складу якого входять датчики, пристрої для приймання та передавання телемеханічної інформації, а також канали зв'язку, що забезпечують передачу даних між об'єктами управління і центром керування [22].

Системи телемеханіки забезпечують автоматичний обмін інформацією між диспетчерським пунктом (ДП) або пунктом керування (ПК) та контрольованими пунктами (КП) енергопідприємства. На ДП і КП встановлюють телемеханічні пристрої: симплексні — для передачі інформації в одному напрямку (наприклад, від КП до ДП) або дуплексні — для двонаправленої передачі даних (від КП до ДП і навпаки). Зв'язок здійснюється через симплексний канал зв'язку (СКС) або дуплексний канал зв'язку (ДКС), які й називають каналами телемеханіки [22].

У енергетичних системах пристрої телемеханіки дають змогу диспетчеру контролювати стан обладнання та режими роботи енергомережі, оперативно отримувати інформацію про зміни в електричній схемі і навіть дистанційно керувати обладнанням. Впровадження телемеханічних систем спрощує роботу оперативного персоналу та підвищує ефективність і якість управління енергетичним комплексом.

За характером функції системи телемеханіки підрозділяються на [22]:

а) телесигналізаційні системи (ТС) використовуються для передачі з контрольного пункту (КП) на диспетчерський пункт (ДП) інформації про стан обладнання, що знаходиться на КП. За допомогою таких систем контролюють положення вимикачів потужності, роз'єднувачів, стан автоматичних пристроїв, а також здійснюють контроль об'єкта;

б) телевимірювальні системи (ТВ) передають диспетчеру дані про параметри виробничих процесів, які контролюються, зокрема струм, напругу, потужність і частоту;

в) системи телекерування або телеуправління (ТК, ТУ) забезпечують передачу команд управління від диспетчерського пункту (ДП) або пункту контролю (ПК) до виконавчих пристроїв об'єкта;

г) система телерегулювання (ТР) виконує передачу команд регулювання типу «більше-менше», «збільшити-зменшити» та інших від диспетчера до автоматичного регулятора, розташованого безпосередньо на об'єкті;

д) автоматичні системи телекерування (АТК) передають керуючу інформацію між автоматичними пристроями. Наприклад, система телевідключення, де автомат, що управляє вимикачем живильної підстанції, отримує команду від автомата, розташованого на віддаленій підстанції без власного вимикача потужності;

е) системи автоматичного телерегулювання (АТР) забезпечують передачу інформації між автоматами, які контролюють роботу об'єкта та керують регулятором у різних пунктах енергосистеми;

ж) аварійно-попереджувальна сигналізація (АПС) — це спрощена форма телесигналізації, яка передає обмежений набір сигналів, таких як «аварія» чи «попередження», з об'єкта на диспетчерський пункт.

Системи АПС, як правило, виконуються за симплексною схемою, що передбачає передачу інформації тільки в одному напрямку.

Системи ТС і ТВ також можуть бути виконані за симплексною схемою, як і багатофункціональні системи типу ТС – ТВ. Системи ТК й АТК в більшості випадків суміщаються із системами ТС, щоб одержати в ПК інформацію про правильність роботи автоматичних пристроїв, які виконують команди телекерування [22].

Такі системи ТУ–ТС або АТУ–ТС виконуються з використанням багатофункціональної апаратури телемеханіки дуплексної схеми. Системи ТР і АТР сполучають із системами ТВ в дуплексній апаратурі телемеханіки ТР – ТВ, АТР –ТВ. Є й інші дуплексні багатофункціональні системи телемеханіки: ТК – ТС – ТВ, ТК – ТР – ТС – ТВ й т.д [22].

На (рис. 1.15) наведено функціональні схеми симплексної й дуплексної систем телемеханіки. Основні елементи цих систем-датчик інформації (ДІ), передаючий пристрій телемеханіки (ППТ), прийомний пристрій телемеханіки (ПРПТ), одержувач інформації (ОІ) та каналу зв'язку. У симплексній системі телемеханіки використовується канал симплексного зв'язку (СКЗ), а в дуплексній системі телемеханіки – дуплексний канал зв'язку (ДКЗ). У симплексній системі використовуються ППТ і ПРПТ, у дуплексній системі — пристрої телемеханіки,

які мають у своєму складі як вузол передачі ППТ, так і вузол прийому ПРПТ телемеханічної інформації. У симплексній системі телемеханіки інформація передається в одному напрямку, наприклад від пункту А до пункту Б, у дуплексній системі інформація передається як з пункту А в пункт Б, так і у зворотному напрямку [22].

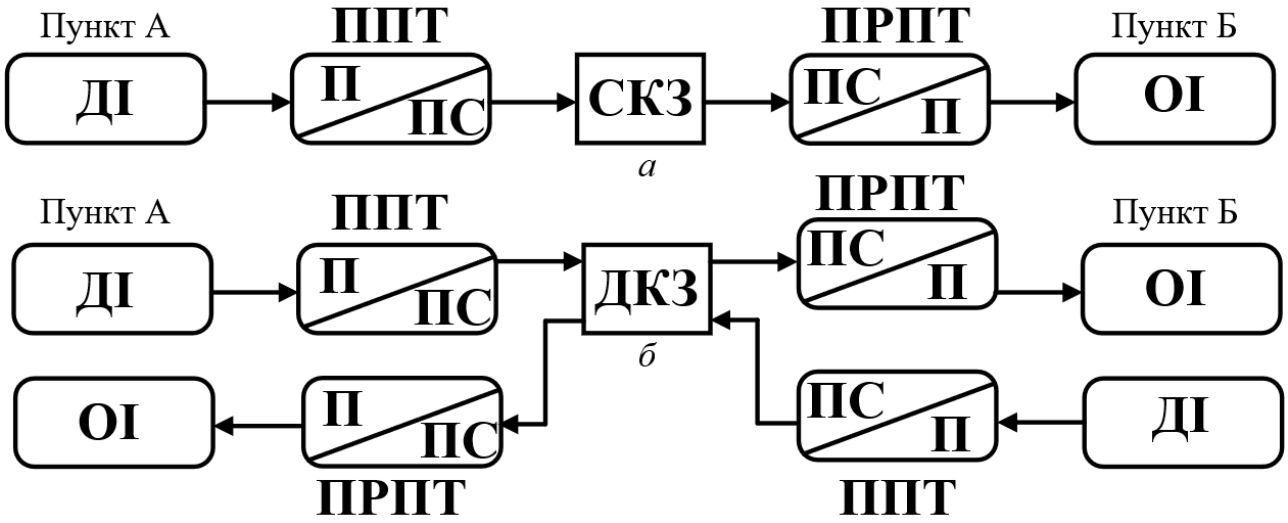

Рисунок 1.15 – Структурні схеми систем телемеханіки: *а* – симплексна; *б* – дуплексна

Розглянемо процес передачі телемеханічної інформації на прикладі симплексної системи телемеханіки (рис. 1.15, а). *Інформацією* називаються відомості про який-небудь процес або явище, які раніше не були відомі одержувачеві інформації ОІ. Ця інформація формується датчиком інформації ДІ, що видає інформацію у вигляді повідомлення [22].

У загальному розумінні, *повідомлення* — це фізичний вплив (механічний, світловий, звуковий, тепловий, магнітний або електричний), певний параметр якого однозначно відповідає переданій інформації. Форма повідомлення визначається видом застосовуваного ДІ. У системах телемеханіки застосовуються переважно ДІ, що виробляють повідомлення у вигляді механічного або електричного впливу. З виходу з ДІ повідомлення (П) надходить на інформаційний вхід ППТ. У ППТ здійснюється перетворення повідомлення П у первинний електричний сигнал (ПС), що потім передається по каналах зв’язку СКЗ із пункту А в

пункт Б. Таким чином, повідомлення є об'єктом передачі, а сигнал — засобом передачі повідомлення на далекі відстані. Обов'язковою умовою якісної передачі інформації є однозначна відповідність значення інформаційного параметра первинного сигналу інформаційному змісту повідомлення. На прийомному кінці системи телемеханіки (пункту Б) ПС із виходу СКЗ надходить у ПРПТ, у якому сигнал перетвориться в повідомлення, передане одержувачеві інформації (ОІ).

Процес передачі інформації в кожному напрямку передачі дуплексної системи телемеханіки (рис. 1.15, б) здійснюється аналогічно розглянутому.

За структурою побудови системи телемеханіки розділяються на однооб'єктні та багатооб'єктні. Однооб'єктні системи забезпечують телемеханічний (симплексний або дуплексний) зв'язок пункту прийому (ПП) з одним КП. Прикладами таких систем є системи на (рис. 1.15, а, б). Багатооб'єктна система телемеханіки забезпечує зв'язок пунктів прийому з декількома КП.

У таких системах на ПП розташовують спеціальні багатооб'єктні приймальнопередаючі пристрої телемеханіки, спільні для всіх КП системи. Залежно від структури використовуваних каналів зв'язку багатооб'єктні системи телемеханіки розділяють на радіальні, послідовні, розгалуджені (деревоподібні) й змішані. У радіальній системі (рис. 1.16) зв'язок ПП з кожним КП здійснюється по своєму незалежному каналу зв'язку. Загальний пристрій станції передавання телемеханіки (СПТ), який є частиною обладнання управління та телемеханіки (ОУТ), з'єднується з каналами через дуплексні лінійні адаптери 1—4, що забезпечують передачу сигналів по дуплексному каналі зв'язку. Кількість адаптерів СПТ відповідає кількості каналів зв'язку й кількості КП у даній системі телемеханіки [22].

Інформація із блоків передачі 5 і 6 надходить через лінійний адаптер і канал зв'язку на КП, зворотна інформація із КП, передана по зворотному каналі зв'язку через адаптер СПТ, надходить на блок прийому 7 і 8 [22].

Наявність незалежних каналів зв'язку в даній системі забезпечує незалежний обмін інформацією ПП з кожним КП.

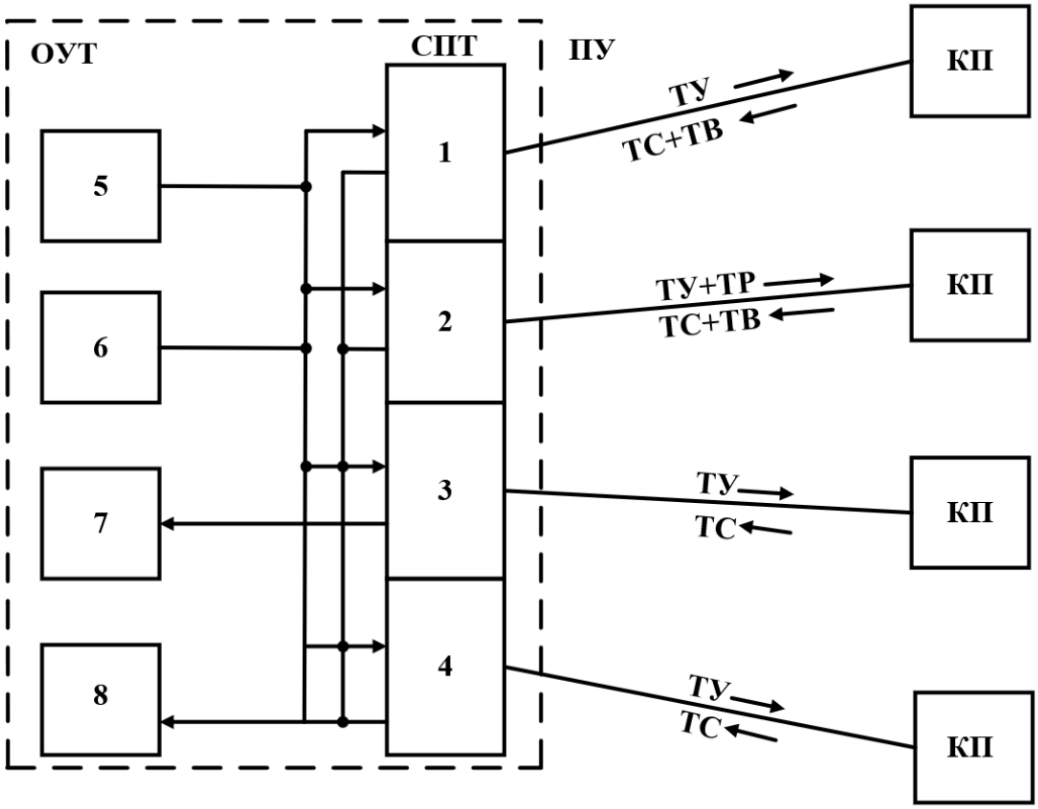

Рисунок 1.16 – Структурна схема радіальної системи телемеханіки

На (рис. 1.17) наведена функціональна схема багатооб’єктної системи телемеханіки, розрахованої для роботи по послідовним а) та розгалудженим (деревоподібним) б) каналам зв’язку. В обох випадках декілька КП включені в один канал зв’язку [22].

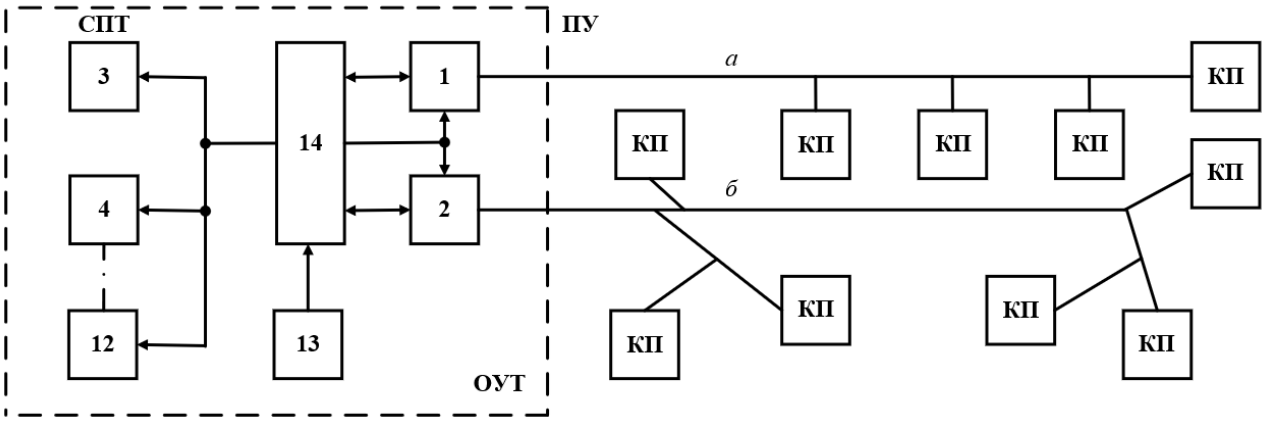

Рисунок 1.17 – Багатооб’єктні системи телемеханіки з каналами зв’язку:
а – послідовними; *б* – змішаними (деревоподібними)

Передача інформації між ПП й КП у цьому випадку можлива тільки шляхом часового ущільнення каналів зв'язку. До складу СПТ входять два лінійних адаптери 1 і 2, блоки прийому інформації 3—12, число яких відповідає числу КП у системі телемеханіки, блок передачі 13 і керуючий розподільний пристрій (КРП) 14. Процес передачі інформації зводиться до наступного. Контрольовані пристрої телемеханіки, розташовані на КП, не передають у канал зв'язку сигнали до одержання від СПТ відповідного дозволу [22]. З передавача СПТ через лінійні адаптери 1 і 2 у відповідні канали зв'язку а), б) для кожного КП по черзі передається сигнал, що містить у собі адресу відповідного КП і інформацію, яку необхідно передати цьому КП від блоку передачі 13. Всі КП одержують зазначений сигнал, але сприймає його тільки контрольований пристрій телемеханіки, чия адреса міститься в даному сигналі. Передавач викликаного пристрою підключається до каналу зв'язку й починає передавати запитану інформацію. Якщо передача ведеться по каналу а), лінійний адаптер сприймає сигнали, і вони через КРП 14 передаються на вхід блоку приймача 3—12, що відповідає пристрою телемеханіки даного КП. Після закінчення циклу обміну інформацією з одним КП КРП формує адресу іншого КП і відповідно підготовляє робочі мережі СПТ для передачі й прийому інформації цього КП. Оскільки КРП працює безупинно, то всі КП даної системи телемеханіки по черзі й циклічно здійснюють обмін інформацією з ПП. Найбільше застосування циклічні багатооб'єктні системи телемеханіки знайшли в розподільних електричних мережах ПЕМ і РЕМ, а також у міських теплових і електричних мережах [22].

Сучасні СПТ з багатьма об'єктами побудовані на основі промислових комп'ютерів, оснащених інтелектуальними лінійними адаптерами та інтерфейсом для виводу інформації на диспетчерський щит або пункт. Інтелектуальний лінійний адаптер включає мікропроцесорний модуль, який відповідає за прийом і передачу первинних сигналів, контроль їхньої коректності, обробку сигналів під час приймання, а також передачу вже обробленої інформації до промислових комп'ютерів. Завдяки впровадженню таких пристроїв, межа між телемеханічним обладнанням та обчислювальною технікою поступово зникає.

1.7.2. Цифрові мережі

З другої половини XX століття енергетика почала активно впроваджувати цифрові технології. З'явилися перші SCADA-системи (Supervisory Control and Data Acquisition) — комплекси збору, обробки та візуалізації даних у реальному часі. Вони дали змогу перейти від простої передачі дискретних сигналів до повноцінного контролю та управління енергетичними процесами.

Впровадження SCADA-систем дало змогу:

– збирати великі обсяги даних від розподілених пристроїв;

– відображати інформацію на диспетчерських екранах у графічному вигляді;

– реалізовувати логіку автоматичного управління на основі сценаріїв;

– архівувати дані для подальшого аналізу.

SCADA-системи стали важливим кроком у побудові ієрархічної системи управління електроенергетикою. Основними елементами стали RTU — термінальні пристрої, встановлені безпосередньо на енергооб'єктах, та HMI — операторські панелі для візуального контролю.

Зі зростанням кількості виробників обладнання виникла потреба у створенні єдиних стандартів протоколів зв'язку, які забезпечили б сумісність пристроїв. Найбільше поширення отримали такі протоколи:

– IEC 60870–5–101/104 — основні телемеханічні протоколи для обміну між диспетчерськими пунктами та об'єктами енергетики;

– DNP3 — поширений у Північній Америці, має розширені функції надійності;

– IEC 61850 — універсальний стандарт для цифрових підстанцій. Забезпечує структуровану модель даних, синхронізацію, інтеграцію IED.

IEC 61850 став проривом: він дозволив об'єднати всі функції релейного захисту, автоматики, обліку та управління в єдину цифрову платформу.

Початок XXI століття ознаменувався новим етапом розвитку — впровадженням концепції Smart Grid (розумної електромережі). Ця концепція базується на ідеї двосторонньої комунікації між усіма учасниками енергетичного процесу:

генераторами, споживачами, операторами систем розподілу та зберігання енергії.

Основні компоненти Smart Grid:

– інтелектуальні лічильники (Smart Meters);
– розподілена генерація (DER);
– системи управління навантаженням та балансування (DR/AGC);
– централізовані та хмарні платформи моніторингу (EMS, DMS);
– цифрові підстанції з повністю програмованою логікою.

Smart Grid використовує оптоволоконні канали, бездротові технології (Wi-Fi, LTE, 5G), мережеві протоколи TCP/IP. Високий рівень автоматизації, прогнозування та інтеграції з цифровими системами дозволяє оптимізувати витрати, зменшити втрати енергії та підвищити надійність.

Останнє десятиліття відзначається впровадженням технологій Інтернету речей (IoT) та аналітики Big Data в енергетику. Це стало можливим завдяки здешевленню сенсорів, зростанню обчислювальних потужностей і появі хмарних сервісів.

Приклади використання:

– моніторинг трансформаторів у реальному часі за допомогою
– IoT-сенсорів;
– прогнозування попиту з використанням штучного інтелекту;
– оптимізація схем навантаження на основі історичних даних;
– виявлення аномалій та кібератак.

Інформаційна інфраструктура сучасної енергосистеми поступово перетворюється на кіберфізичну систему, де відбувається тісне поєднання фізичних процесів і цифрового керування.

У (табл. 1.2) зібрані ключові етапи розвитку технологій передачі інформації в енергетиці: від становлення телемеханіки до розгортання цифрових інтелектуальних систем. Розглянуто технічні особливості кожного етапу, вплив технологічних змін на архітектуру систем управління та перспективи майбутнього розвитку інформаційної інфраструктури енергосистеми (IoT та AI).

Таблиця 1.2 – Порівняльна таблиця етапів розвитку

№	Етап	Роки впровадження	Технології	Особливості
1	Телемеханіка	~1920–1970	Реле, аналогові сигнали	Дискретна передача, вузька функціональність
2	SCADA-системи	~1970–2000	Мікропроцесори, HMI, RTU	Графіка, логіка, архівація даних
3	Протоколи передачі	~1990–дотепер	IEC 101/104, DNP3, IEC 61850	Стандартизація, сумісність, IED
4	Smart Grid	~2005 – дотепер	Smart Meters, DER, EMS	Інтелектуальне керування, двосторонній обмін
5	IoT та AI	~2015–дотепер	Сенсори, хмари, машинне навчання	Прогнозування, автономія, кібербезпека

Процес еволюції технологій передачі інформації в енергетиці демонструє тенденцію до зростаючої інтеграції цифрових технологій у всі рівні управління. Від аналогової телемеханіки до Smart Grid і Інтернету речей — цей розвиток відкриває нові горизонти для ефективності, стабільності та безпеки енергетичних систем. Найближчі роки обіцяють ще більшу цифровізацію, розширення можливостей кіберфізичних систем, гнучке управління попитом і впровадження інтелектуальних платформ підтримки прийняття рішень.

Більш детально про SCADA-системи та протоколи передачі даних буде розглянуто в наступних розділах навчального посібника.

Висновки до розділу 1

У першому розділі навчального посібника закладаються фундаментальні уявлення про системи передачі інформації в електроенергетиці, підкреслюється їхня критична роль у забезпеченні надійного, безпечного та ефективного функціонування енергосистем. Поглиблене ознайомлення з базовими поняттями, структурними елементами, фізичними принципами та математичними основами формує необхідну базу для розуміння більш складних інженерних рішень у наступних розділах.

У цьому розділі був поставлений акцент на природі інформації, повідомлень, сигналів і перешкод. Визначено основні об’єкти інформаційного обміну: джерела, приймачі та канали зв’язку. Зосереджено увагу на властивостях інформації, її вразливості до спотворень і способах її захисту під час передачі. Таке бачення дозволяє усвідомити, чому якість, точність і цілісність даних критично важливі для функціонування енергетичної системи.

Далі було розглянуто загальну модель комунікаційної мережі. Підкреслено функціональний поділ на передавачі та приймачі, особливості фізичного середовища (лінії зв’язку) і вимоги до каналів передачі. Деталізовано проблеми, пов’язані з перешкодами, синхронізацією і необхідністю ефективного кодування. Така модель є ключовою основою для побудови систем SCADA, АСУ ТП та інших інструментів диспетчеризації.

Окремий підрозділ було присвячено моделі взаємодії відкритих систем (OSI), яка є базовим еталоном структурування інформаційного обміну. Вивчення її семи рівнів дозволяє зрозуміти, як розподіляються функції обробки даних, починаючи від фізичного сигналу і закінчуючи прикладними завданнями. Також було зазначено використання спрощеної архітектури EPA в галузевих стандартах, що актуалізує адаптивність систем під особливості електроенергетики.

У підрозділі, присвяченому інформації як об’єкту передачі, акцент зроблено на типології даних: оперативні, аварійні, аналітичні, діагностичні. Розглянуто класифікацію за джерелом, способом передачі, частотою оновлення. Підкреслено важливість відповідності інформації актуальності, точності, цілісності, надійності та безпеці. Такі вимоги є основою для побудови стійких до загроз та адаптивних енергетичних систем.

Значна увага приділялася технічному аспекту цифрової передачі інформації. Вивчено основні методи кодування та способи представлення бітової інформації у фізичному середовищі. Порівняння NRZ, RZ, манчестерського та інших методів дозволяє оцінити компроміси між простотою, стійкістю до шуму та ефективністю використання пропускної здатності каналу.

Наступні підрозділи ознайомили з процесами перетворення аналогових сигналів у цифрову форму через квантування за рівнем і часом. Пояснено вплив дискретизації на точність та швидкість передачі, визначено похибки та способи їх зменшення. Це критично важливо для систем вимірювання, де точність визначає якість керування.

Також було розглянуто модуляцію як спосіб адаптації сигналу до каналу зв'язку. Описано основні види безперервної та імпульсної модуляції, їхні характеристики та особливості застосування. Це дозволяє зрозуміти, як забезпечити передачу даних на великі відстані або через середовища з обмеженими характеристиками.

У наступному підрозділі визначено основні функції систем передачі інформації: передача телеметричних даних, команд керування, реалізація релейного захисту, синхронізація часу, ведення журналів подій, забезпечення безпеки та підтримка Smart Grid. Такий підхід підкреслює багатофункціональність СПІ та їхню роль у всіх процесах енергетичного керування.

Останній підрозділ описав структуру інформаційної взаємодії та класифікацію систем передачі за різними критеріями. Вивчення польового, об'єктного, регіонального та центрального рівнів забезпечує системне розуміння інформаційних потоків. Це знання необхідне для проєктування масштабованих, сумісних і надійних інформаційних систем енергетики.

Таким чином, перший розділ забезпечує базову теоретичну підготовку, необхідну для розуміння принципів побудови, функціонування та розвитку систем передачі інформації в електроенергетиці. Саме ці знання стають відправною точкою для подальшого вивчення мереж, протоколів, архітектур і цифрових рішень сучасної енергосистеми.

Загалом, перший розділ формує системне уявлення про місце, роль та принципи функціонування інформаційних систем в енергетиці. Він підкреслює взаємозв'язок технічних, організаційних і інформаційних компонентів та готує читачів до вивчення більш конкретних прикладних аспектів у наступних розділах.

Запитання для контролю знань за першим розділом

1. У чому полягає роль систем передачі інформації в енергосистемах?
2. Які основні становлять складають типову інформаційну систему передачі?
3. Що таке повідомлення, сигнал та перешкода в контексті інформаційного обміну?
4. Які основні властивості інформації мають особливе значення для електроенергетики?
5. Чому інформація в енергосистемах вважається вразливою до спотворень?
6. Назвіть основні об’єкти інформаційного обміну та їхню роль.
7. Які проблеми виникають при синхронізації сигналів і як їх вирішують?
8. У чому полягає значення моделі OSI для структурування процесу передачі інформації?
9. Які рівні моделі OSI найбільш критичні для енергетичних застосувань і чому?
10. Чим спрощена архітектура EPA відрізняється від моделі OSI і де вона застосовується?
11. Які типи інформації передаються в енергосистемах і чим вони відрізняються?
12. Поясніть різницю між NRZ, RZ та манчестерським кодуванням. Які з них краще протидіють шуму?
13. Як процес дискретизації впливає на точність передачі аналогових сигналів?
14. Які основні функції виконують системи передачі інформації в електроенергетиці?
15. Як класифікуються рівні інформаційної взаємодії в енергетичних системах і яка їхня роль?
16. Яким чином кодування сприяє захисту інформації від спотворень у каналі зв’язку?
17. Що таке модуляція, і чому вона потрібна в системах передачі інформації?

18. Як тип фізичного середовища впливає на вибір методу передачі даних?

19. Які вимоги висуваються до каналів зв’язку в енергетичних системах?

20. Чому точність і швидкість обробки даних мають вирішальне значення для систем керування в енергетиці?

2. ОСНОВНІ ЕЛЕМЕНТИ ТА СТРУКТУРА ІНФОРМАЦІЙНИХ СИСТЕМ

Інформаційні процеси в електроенергетиці є основою ефективного функціонування всієї енергетичної інфраструктури. У центрі цих процесів знаходяться джерела та приймачі інформації — пристрої, які забезпечують формування, передачу, прийом і первинну обробку інформаційних сигналів. Саме з них починається і завершується інформаційний ланцюг, який дозволяє приймати управлінські рішення, контролювати параметри системи, реагувати на аварійні ситуації та забезпечувати надійне функціонування електроенергетичної системи в цілому.

У цьому підрозділі розглядаються класифікація, технічні характеристики, принципи дії та особливості використання джерел і приймачів інформації в умовах сучасних енергетичних об’єктів. Розуміння цих компонентів є критично важливим для майбутніх інженерів-енергетиків, фахівців з автоматизації, розробників SCADA-систем, проєктантів та операторів систем передачі й розподілу електроенергії.

2.1. Джерела і приймачі інформації

Джерела інформації. Джерелом інформації в енергетичній системі вважається будь-який генеруючий елемент, формує або надає інформацію про стан певного процесу або об’єкта. Це можуть бути як фізичні пристрої (наприклад, датчики струму), так і програмно-апаратні комплекси (наприклад, Smart Meter або PMU) [8, 12–14].

Інформація, яку генерують джерела, може мати різну природу: аналогову, цифрову, імпульсну, частотну, часову. Основна задача — забезпечити достовірне й стабільне представлення фізичного процесу у вигляді сигналу, придатного для подальшої обробки та передачі.

Джерела інформації можна класифікувати так:

1) За фізичною природою сигналу:

а) аналогові: формують безперервні сигнали (датчики температури, струму, тиску);

б) цифрові: видають двійкову інформацію або дискретні сигнали (реле стану, енкодери).

2) За функціональним призначенням:

а) контрольні. Фіксують стан елемента (включено/вимкнено, відкрито/закрито);

б) вимірювальні. Генерують дані для кількісного аналізу (наприклад, амперметри, вольтметри);

в) керуючі. Здатні самостійно приймати рішення на основі локальних алгоритмів.

3) За способом взаємодії з середовищем:

а) прямої дії. Безпосередньо вимірюють параметри (термометри, манометри);

б) непрямої дії. Визначають параметри на основі похідних значень або розрахунків (розрахунок потужності за напругою та струмом).

До типових джерел інформації в енергетиці належать:

– трансформатори струму (ТС) і напруги (ТН): забезпечують ізоляцію і масштабування сигналу для систем контролю;

– датчики температури: термопари, термістори, RTD для контролю температури обмоток трансформаторів, шин, кабелів;

– датчики тиску: використовуються в гідроелектростанціях, газових установках, охолоджувальних системах;

– Smart Meter: передають дані про споживання, навантаження, якість електроенергії;

– фазометри (PMU): вимірюють фазові кути, частоту, миттєві значення напруги й струму з точністю до мілісекунд;

– RTU: збирають дані з кількох джерел одночасно та передають їх до диспетчерських центрів.

Приймачі інформації — це елементи, що сприймають сигнали від джерел, інтерпретують їх, а іноді також реагують на них у вигляді логічного сигналу, команд або збереження в базі даних. Приймачі можуть бути простими (наприклад, індикаторний дисплей) або складними (сервер SCADA) [8, 12–14].

Приймачі інформації класифікуються:

1) За функцією:

а) візуалізаційні. Передають дані у зручній формі (HMI-панелі, дисплеї);

б) керуючі. Використовують інформацію для формування команд (логічні контролери);

в) аналітичні. Здійснюють складну обробку (сервери SCADA, АСКОЕ).

2) За рівнем системної інтеграції:

а) польовий рівень. Отримують сигнали безпосередньо з джерел (локальні контролери);

б) системний рівень. Приймають дані з різних підстанцій, генеруючих станцій, аналізують та передають команди.

3) За типом інтерфейсу:

а) аналогові входи: 4–20 мА, 0–10 В;

б) цифрові входи: імпульсні, двійкові сигнали;

в) мережеві інтерфейси: RS-485, Ethernet, Wi-Fi, GSM.

До типових приймачів в енергетиці належать:

– PLC (програмовані логічні контролери). Здійснюють обробку сигналів

– від датчиків та формують відповідні команди;

– SCADA-сервери. Забезпечують моніторинг і диспетчеризацію енергетичних процесів;

– HMI-панелі. Інтерфейси для оператора;

– системи РЗА. Отримують сигнали про коротке замикання, перенавантаження, здійснюють миттєве відключення;

– сервери АСКОЕ. Збирають і зберігають комерційні показники споживання.

– PMU-приймачі: синхронізовані з GPS, збирають фазові координати, частоту, потужність.

Інтеграція джерел і приймачів у системах передачі інформації. Для забезпечення надійного обміну даними між джерелами та приймачами інформації використовуються стандартизовані протоколи

– Modbus RTU/TCP, простий протокол для опитування контролерів;

– IEC 60870–5–101/104, стандарт для телемеханіки в енергетиці;

– IEC 61850, комплексний протокол для цифрових підстанцій;

– DNP3, особливо поширений у Північній Америці.

Відповідність протоколу забезпечує сумісність між різними пристроями незалежно від виробника. Багато сучасних джерел і приймачів підтримують одночасно кілька протоколів.

Часова точність є критично важливою в системах релейного захисту та у фазометричних комплексах. Використовується синхронізація за GPS або PTP відповідно до стандарту IEEE 1588.

В (табл. 2.1) наведені приклади джерел і приймачів інформації в електроенергетиці.

Таблиця 2.1 – Джерела і приймачі інформації в електроенергетиці

№	Джерело інформації	Тип сигналу	Приймач	Протокол	Застосування
1	Трансформатор струму	Аналоговий	PLC	4–20 мА	Контроль навантаження трансформатора
2	Датчик температури	Аналоговий	SCADA	Modbus RTU	Моніторинг охолодження
3	Smart Meter	Цифровий	Сервер АСКОЕ	DLMS/COSEM	Комерційний облік
4	RTU	Збірний	Сервер SCADA	IEC 104	Диспетчеризація
5	PMU	Цифровий	Сервер WAMS	IEEE C37.118	Моніторинг стабільності
6	Датчик тиску	Аналоговий	PLC	0–10 В	Автоматизація ГЕС

Системи передачі інформації мають низку актуальних проблем, що виникають при інтеграції джерел і приймачів, серед яких можна назвати такі:

– гетерогенність пристроїв. Велика кількість пристроїв різних поколінь, що не завжди підтримують сучасні протоколи;

– недостатня захищеність. Стара техніка не підтримує шифрування, що створює кіберзагрози;

– складність технічного обслуговування. Потреба в постійному налагодженні, модернізації;

– висока вартість заміни застарілого обладнання.

Інтеграція джерел та приймачів у системи передачі відкриває також і нові можливості, серед яких можна виокремити наступні:

– розвиток Smart Grid. Підключення тисяч інтелектуальних пристроїв;

– IoT-сенсори. Дешеві та енергоефективні джерела даних;

– Big Data та AI. Розширення аналітичних функцій приймачів;

– квантова передача інформації. Дослідження у сфері надзахищених каналів.

Успішне функціонування будь-якої системи передачі інформації в електроенергетиці неможливе без чіткого розуміння особливостей роботи джерел та приймачів інформації. Від коректної взаємодії цих елементів залежать точність, надійність та оперативність інформаційного потоку в системі. Сучасні вимоги до кіберзахисту, стандартизації, масштабованості та швидкості обміну диктують необхідність інтеграції лише сумісних та адаптованих до цифрової епохи пристроїв. Для фахівців галузі важливо володіти знаннями про типи, характеристики, способи інтеграції та новітні технології в області джерел і приймачів інформації.

2.2. Канали зв’язку: середовище передачі, типи сигналів

У сучасних енергетичних системах передача інформації від джерел до приймачів є критично важливою для забезпечення ефективного управління, моніторингу та автоматизації. Однією з ключових складових цієї передачі є канали

зв’язку, які забезпечують фізичне або логічне середовище для переміщення сигналів. Розуміння різновидів каналів зв’язку, їх характеристик, можливостей та обмежень є основою для побудови надійних і ефективних інформаційних систем в електроенергетиці.

Канал зв’язку — це сукупність технічних засобів та середовищ, які забезпечують передавання інформаційного сигналу від передавача до приймача. Він може бути як фізичним, так і логічним, охоплювати дротові, бездротові, оптичні та комбіновані середовища.

Основні характеристики каналів зв’язку:

– пропускна здатність — кількість інформації, що може бути передана за одиницю часу;

– швидкість передачі даних — визначає, скільки біт або байт передається щосекунди;

– затримка (latency) — час, який потрібен сигналу для проходження каналу;

– достовірність — ймовірність передачі інформації без помилок;

– захищеність — здатність каналу протистояти несанкціонованому доступу або втраті інформації.

Середовище передачі визначає фізичну основу, по якій передаються сигнали. У контексті енергетичних об’єктів середовище повинно бути адаптованим до високих електромагнітних завад, великих відстаней та суворих умов експлуатації.

Види середовищ передачі:

1) Провідникові канали:

а) мідний кабель:

– найбільш поширений у низьковольтних мережах;

– має відносно невисоку вартість;

– обмежена дальність передачі (~100 м для Ethernet).

б) коаксіальний кабель:

– краще екранування від завад, ніж у скручених пар;

– використовувався у старих мережах SCADA;

– частково зберігає актуальність у підстанційних системах.

в) польові шини (Fieldbus):

– використовуються для зв’язку між польовими пристроями;

– приклади: Profibus, CAN, Foundation Fieldbus.

2) Волоконно-оптичні лінії зв’язку.

Оптичне волокно — це середовище, що забезпечує надзвичайно високу швидкість передачі та стійкість до електромагнітних перешкод.

– використовується у міжпідстанційному зв’язку;

– надає можливість передавати сигнали на великі відстані (десятки кілометрів) без значних втрат;

– підтримує технології SDH, DWDM, Ethernet.

Переваги використання:

– висока пропускна здатність (до терабіт/с);

– електромагнітна нечутливість;

– безпека — складно підслухати без фізичного доступу.

Недоліки використання:

– вартість прокладання;

– необхідність в специфічному обладнанні.

3) Бездротові канали:

а) радіоканал:

– використовується для резервного зв’язку та передачі на об’єктах без дротового доступу;

– протоколи: Wi-Fi, ZigBee, LoRaWAN, 4G/5G.

б) супутниковий зв’язок:

– застосовується на важкодоступних об’єктах;

– висока затримка — до 600 мс;

– не залежить від місцевої інфраструктури.

в) мобільний зв’язок:

– інтеграція з публічними мережами операторів;

– актуально для AMI.

До типів сигналів у передачі інформації належать сигнали, що передаються через канали зв’язку, вони можуть бути класифіковані за різними критеріями:

а) аналогові сигнали:

– неперервні у часі;

– відображають зміни фізичних величин (напруга, струм);

– піддаються впливу шумів і завад;

– у минулому широко використовувались для вимірювальної техніки;

б) цифрові сигнали:

– представляють інформацію у вигляді дискретних значень (0 або 1);

– менш чутливі до шумів;

– придатні для обробки мікропроцесорними пристроями;

– підтримують складні протоколи зв’язку (Modbus, DNP3).

в) імпульсні сигнали:

– використовуються для передачі дискретної інформації;

– наприклад, сигнали стану «увімкнено/вимкнено».

У сучасній електроенергетиці спостерігається тенденція до переходу від ізольованих каналів зв’язку до інтегрованих мультисервісних мереж, які здатні передавати одночасно різні типи інформації — диспетчерські дані, телеметрію, відео, голосові повідомлення тощо.

Технології сучасних каналів зв’язку:

– MPLS;

– IP/MPLS мережі;

– SDH;

– Ethernet та індустріальні версії (Industrial Ethernet);

– VPN-тунелі для захищеного обміну.

Вибір типу каналу залежно від завдань є одним із ключових факторів, які враховуються під час проєктування систем передачі інформації:

– призначення каналу — чи це канал для телеметрії, сигналізації, відеоспостереження;

– дальність — на які відстані потрібно передавати інформацію;

– середовище експлуатації — рівень електромагнітних завад, температура, вологість;

– надійність — вимоги до відмовостійкості та резервування.

Приклади використання каналів зв’язку в енергетиці:

а) АСУ ТП (Автоматизовані системи керування технологічними процесами):

– використання польових шин (Profibus, CAN);

– інтеграція з SCADA.

б) цифрові підстанції:

– оптичні лінії для зв’язку між IED-пристроями;

– використання стандартів IEC 61850.

в) AMR/AMI-системи (облік):

– GSM, NB-IoT, LoRa для передачі даних лічильників.

г) системи відеоспостереження:

– Ethernet, Wi-Fi, 4G для IP-камер на об’єктах.

д) релейний захист та автоматика (РЗА):

– жорсткі вимоги до затримок;

– використання оптичного зв’язку з пріоритетною маршрутизацією.

Розуміння принципів роботи каналів зв’язку є фундаментальним для побудови ефективної, надійної та масштабованої інформаційної інфраструктури в енергетиці. Від вибору середовища передачі, типу сигналу та протоколу залежать швидкодія, точність, надійність та безпека всієї системи управління. Урахування специфіки енергетичних об’єктів — їх розподіленості, електромагнітного впливу та вимог до резервування — робить завдання проєктування каналів зв’язку особливо складним і відповідальним.

2.2.1. Фізичні канали зв'язку

Як уже розглядалося в попередньому розділі, фізичний рівень моделі OSI являє собою фізичне середовище передачі – електричне або оптичне – з відповідними інтерфейсами до з'єднуваних об'єктів.

Як фізичне середовище передачі виступає лінія зв'язку, яка складається з одного або більше шляхів передачі інформації. Шлях передачі є матеріальним середовищем, по якому поширюються сигнали від передавача до приймача деякої системи передачі інформації.

У якості інтерфейсу виступає блок узгодження, який перетворює послідовність інформаційних бітів з форми необхідної на канальному рівні пристрою телемеханіки у форму необхідну для шляху передачі інформації.

Блок сполучення (узгодження) з лінією зазвичай виконує такі функції:

– перетворення сигналу;

– забезпечення гальванічного поділу між апаратурою телемеханіки і каналом зв'язку;

– контроль якості сигналу;

– забезпечення побітної синхронізації;

– додавання або усунення ознак синхронізації кадру якщо ця функція не виконується на канальному рівні;

– визначення станів зайнятості каналу зв'язку, очікування та ушкодження.

В електричних системах використовуються провідні лінії («повітряні» або кабельні), волоконнооптичні лінії й радіолінії (лінії радіозв'язку, радіорелейні й супутникові).

Каналом зв'язку (каналом передачі інформації) називають шлях передачі, що забезпечує незалежну передачу інформації на відстань від різних джерел до відповідних приймачів. Цей шлях утворюється сукупністю технічних пристроїв і ліній зв'язку. Таким чином, лінії зв'язку того або іншого типу є складовими частинами каналів зв'язки. Крім наведених у (табл. 2.2) типів ліній зв'язку, в енергетиці широко використовуються канали передачі інформації, які

організовуються по високовольтних лініях, розподільним силовим мережам, зайнятим лініям телефонного зв'язку [22].

Використовувані в енергосистемах лінії зв'язку (ЛЗ) і діапазони застосовуваних при цьому частот наведені в (табл. 2.2).

Таблиця 2.2 – Діапазони частот

№	Тип лінії зв'язку	Використовувані для передачі інформації коливання	Діапазон частот
1	Повітряна	Електричні	$(0…2)\cdot10^5$, Гц
2	Кабельна (симетричний кабель та коаксіальний кабель	Електричні	$(0…15)\cdot10^6$, Гц
3	Радіозв'язок	Електромагнітні	Від 10^4 до $3\cdot10^9$, Гц
4	Радіорелейна	Електромагнітні	Від $3\cdot10^4$ до $3\cdot10^{10}$, Гц
5	Супутникова	Електромагнітні	$(2…8)\cdot10^9$, Гц
6	Волоконно-Оптична	Електромагнітні видимого спектра (оптичні)	$(3…8)\cdot10^{14}$, Гц

Провідні (повітряні й кабельні) лінії зв'язку. Повітряні лінії зв'язку (ПЛЗ) складаються з металевих проводів, які кріпляться на стовпах (дерев'яних або залізобетонних) за допомогою ізоляторів та спеціальних елементів арматури, таких як штирі, гаки і траверзи. Кабельні лінії зв'язку (КЛЗ) представляють собою кабель — ізольовані електропровідники, укладені у загальну вологозахисну оболонку, іноді додатково захищені металевою стрічкою для запобігання механічним пошкодженням. Такий кабель може прокладатися в землі, по дну водойми або бути підвішеним на стовпах ПЛЗ чи опорах ліній електропередачі [22].

Провідні лінії телефонного зв'язку. Телефонний зв'язок призначений для двонаправленої (дуплексної) передачі голосових сигналів на великі відстані. Як показано на (рис. 2.1), мікрофон (ВМ) перетворює звукові коливання у змінні електричні сигнали тональних частот у діапазоні від 300 Гц до 3400 Гц, а телефон (BF) здійснює зворотне перетворення цих електричних сигналів назад у звук.

Схеми двостороннього зв'язку будуються системою з місцевою батареєю (GB) чи центральної батареєю (рис. 2.1). Мікрофони на станціях А та Б отримують живлення від місцевих батарей GB1 та GB2. Мікрофони ВМ1 та ВМ2 включені в коло обмоток I трансформаторів Т1 та Т2. У коло обмоток цих трансформаторів II включені телефони BF1 і BF2. При передачі мови зі станції А на станцію Б і навпаки схема працює як і схема односторонньої передачі. Недоліком схеми, наведеної на (рис. 2.1, а), є те, що мова одночасно відтворюється телефонами обох станцій, тобто, абонент, що говорить, чує власну розмову у своєму телефоні. Це явище носить назву «місцевий ефект» [22].

У телефонних мережах, організованих за системою місцевої батареї, часто використовувалися штучні (фантомні) мережі. Вони дозволяють одночасно передавати сигнали постійного струму телеграфного або телемеханічного зв'язку та змінні струми телефонного зв'язку по одній парі проводів.

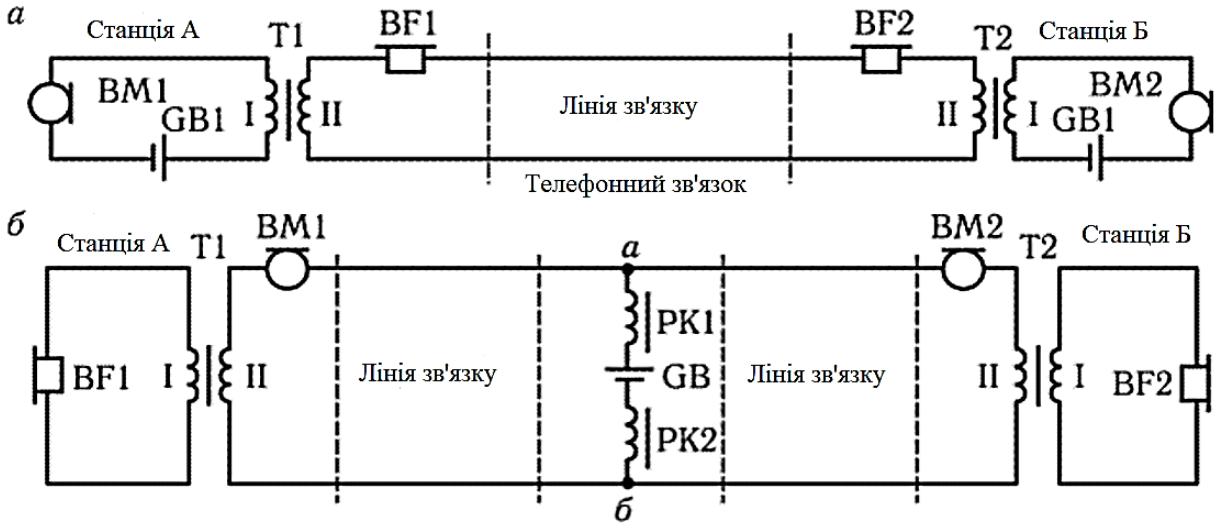

Рисунок 2.1 – Схеми організації телефонного зв'язку: *а* – з місцевою батареєю; *б* – з центральною батареєю

На схемі, що наведена на (рис. 2.1, б), мікрофони включені в обмотки II трансформаторів Т1 і Т2, а телефони – в обмотки I. Така схема включення мікрофонів дозволяє здійснювати їх живлення від однієї центральної батареї GB, що встановлюється на телефонній станції. Батарея GB є спільною для станцій А та Б та підключається до мікрофонних кіл через дроселі РК1 та РК2. Вони мають незначний опір до постійного струму, що протікає від батареї GB через кола мікрофонів ВМ1 і ВМ2, і в той же час перешкоджають замиканню змінної складової розмовного струму через GB батарею. Описана схема двосторонньої телефонної передачі також має місцевий ефект. Для усунення місцевого ефекту у телефонних апаратах застосовуються спеціальні протимісні схеми включення мікрофона та телефону. Головною вимогою до телефонної передачі є забезпечення заданої якості передачі мови. Критеріями оцінки якості є розбірливість, гучність, натуральність відтворюваного звуку та ін.

Високочастотні канали зв'язку по ЛЕП і розподільним силовим мережам

Для забезпечення надійної передачі голосу, команд релейного захисту (РЗ) та протиаварійної автоматики (ПА) в енергетичній сфері широко застосовується високочастотний зв'язок (ВЧЗ) по лініях електропередачі (ЛЕП). Зазвичай використовується метод частотного або частотно-часового ущільнення каналів. Канали функціонують у високочастотному діапазоні з несучими частотами від 300 до 500 кГц, що дозволяє уникнути впливу гармонік промислового змінного струму та перешкод, які виникають через «коронний» розряд на проводах високої напруги. Для цього застосовується спеціалізована апаратура для високочастотної обробки ЛЕП, що включає елементи підключення та обладнання ВЧ-зв'язку (рис. 2.2).

До елементів приєднання належать високочастотний загороджувач (ВЧЗ), високовольтний конденсатор зв'язку (КЗв) та фільтр приєднання (ФП) (рис. 2.2). ВЧЗ забезпечує безперешкодний прохід струму частотою 50 Гц і розраховується на мінімально можливий безперервний струм у ЛЕП, при цьому має витримувати короткочасні максимальні струми короткого замикання в місці встановлення.

Крім того, загороджувач повинен створювати значний опір для високочастотного струму зв’язку.

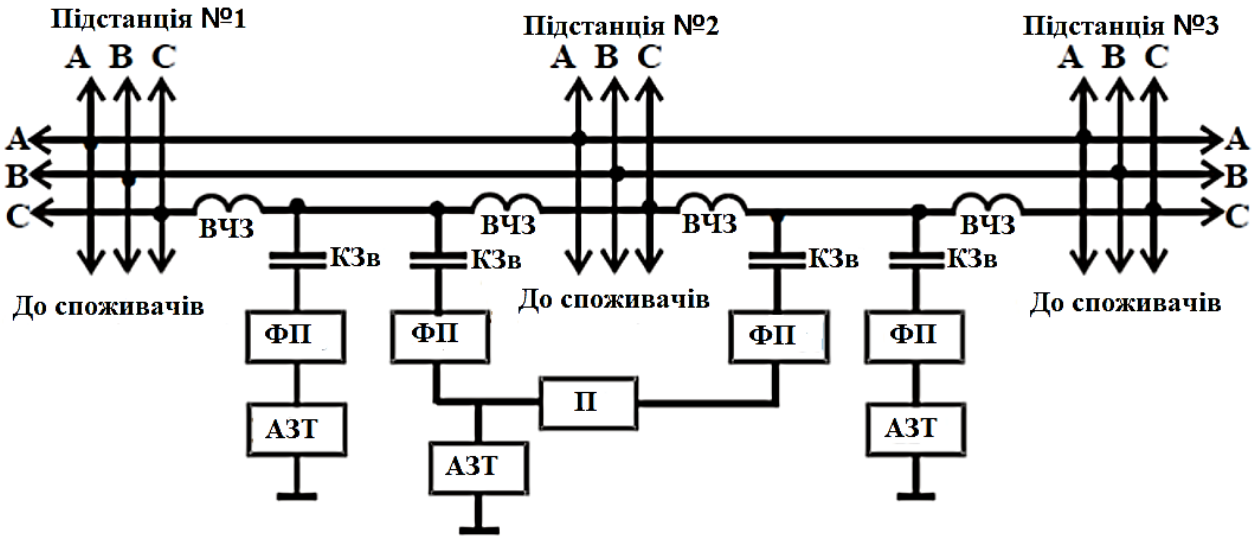

Рисунок 2.2 – Створення каналів зв’язку по ЛЕП

Конденсатори зв’язку постійно працюють під високою напругою промислової частоти, мають відносно невелику ємність — від 2200 до 35000 пФ. Вони виготовляються в порцелянових корпусах для ЛЕП із напругою понад 25 кВ або в металевих корпусах при напрузі від 6 до 35 кВ і мають паперово-масляну ізоляцію.

Фільтри приєднання забезпечують узгодження апаратури високочастотного зв’язку з лінією електропередачі. На (рис. 2.2) відображений випадок створення каналів зв’язку по системі «фаза-земля» між підстанціями №1 і №3, а на підстанції №2 організовано обхідний шлях із проміжним посиленням струмів зв’язку з підсилювачем (П).

Окрім високовольтних ліній, для організації каналів зв’язку можуть використовуватися розподільні мережі електроживлення 6/0,4 кВ, що застосовуються в електрифікованому міському та залізничному транспорті. У таких мережах зазвичай використовується спосіб приєднання «фаза-фаза» (рис. 2.3) [22].

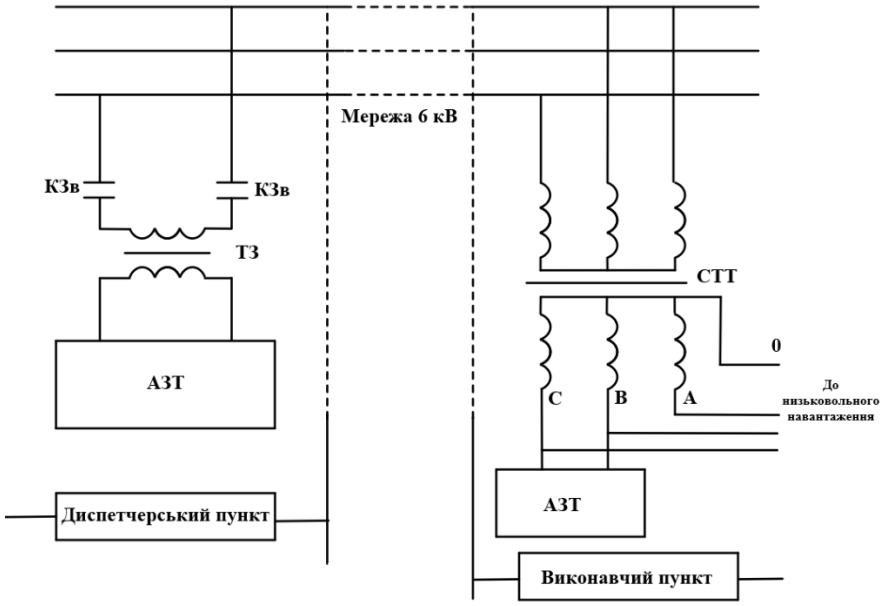

Рисунок 2.3 – Створення каналів телемеханіки по розподільній мережі 6/0,4 кВ

На диспетчерському пункті (рис. 2.3) апаратура зв’язку й телемеханіки (АЗТ) підключається до фаз В і С через конденсатори зв’язку (КЗв) та високочастотний трансформатор зв’язку (ТЗ). На виконавчому пункті для зняття високочастотних сигналів, як показує досвід експлуатації, можуть застосовуватися вторинні обмотки силового трифазного трансформатора (СТТ) [22].

Кращі можливості забезпечує передача сигналів за допомогою струмів «нульової послідовності» (рис. 2.4). Для цього використовуються трансформатори напруги (ТН), які значно надійніші за конденсатори зв’язку і мають вищу ремонтопридатність. Вторинні обмотки ТН з’єднані у відкритий трикутник, що утворює фільтр нульової послідовності, а канал зв’язку організовується одночасно по трьом проводах (А, В і С), які підключені паралельно для проходження струмів зв’язку [22].

Зазвичай на основі цього методу формуються частотні канали: аварійно-попереджувальна сигналізація працює в діапазоні 20–400 Гц, телеграфний і телемеханічний зв’язок — від 400 до 1400 Гц, службовий телефонний зв’язок — у межах 1400–3200 Гц, а надтональний телеграф — при частотах вище 3400 Гц.

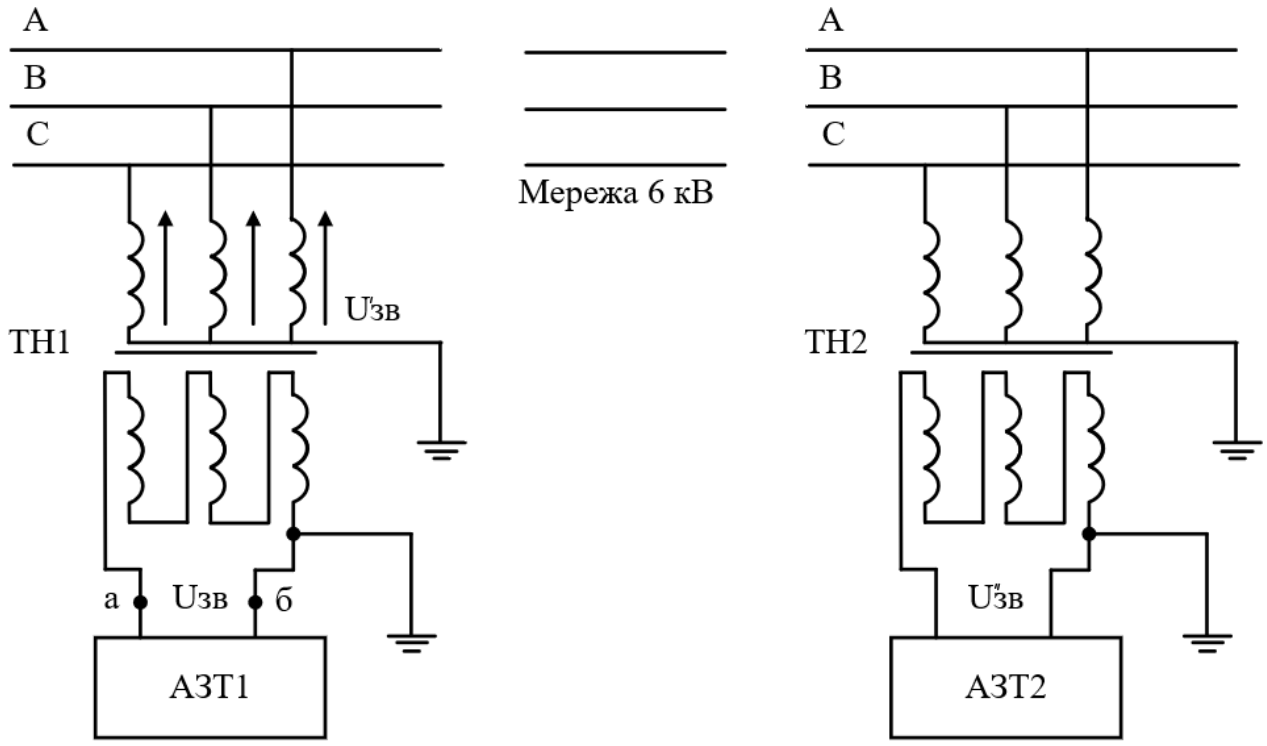

Рисунок 2.4 – Канали зв’язку на струмах нульової послідовності [22]

Відомо, що в схемі «відкритий трикутник» при симетричній системі напруг сума миттєвих значень напруг (або струмів промислової частоти) в будь-який момент часу дорівнює нулю. Тому, якщо між точками розриву трикутника (а і б) подати сигнал зв’язку з частотою значно вищою за частоту промислового струму, в первинних обмотках трансформатора, наприклад ТН1, виникнуть струми зв’язку, які будуть однакові за фазою. Ці струми, протікаючи по фазових проводах високовольтної лінії, на прийомній стороні, у вторинних обмотках трансформатора (ТН2) створять напругу сигналу зв’язку ($U»_{зв}$). При такій схемі досить просто організовується дуплексний канал зв’язку між АЗТ1 і АЗТ2 [22].

Канали зв’язку по радіо. Заміна провідних каналів зв’язку радіоканалами приваблює своєю простотою — для них не потрібні лінійні споруди, а час на організацію таких зв’язків значно скорочується. Проте через вплив часу доби, погодних умов та інших факторів якість радіозв’язку, особливо в довгохвильовому і короткохвильовому діапазонах, часто погіршується. Саме тому використання радіозв’язку в енергосистемах не отримало широкого розповсюдження.

Набагато частіше використовувалися *радіорелейні лінії* (РРЛ), що представляють собою ряд радіостанцій і споруджень зі спрямованими приймально-передавальними антенами (рис. 2.5) [22].

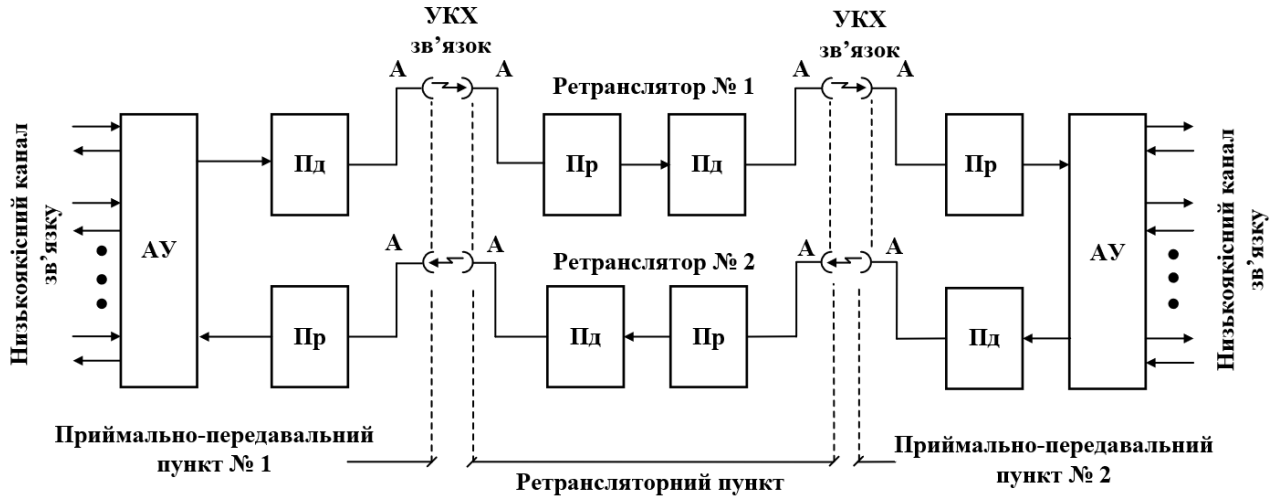

Рисунок 2.5 – Спрощена структурна схема радіорелейної лінії

Антени ретрансляторів розміщують на відстані прямої видимості — приблизно 40–60 км при висоті антен до 70 м. Передача та прийом здійснюються в діапазоні ультракоротких хвиль (УКХ) на частотах від 1,6 до 3,9 ГГц. Канали організовуються за допомогою методів частотного та тимчасового ущільнення. Зазвичай усі канали працюють у симплексному режимі, при цьому «прямий» і «зворотний» канали рознесені по частоті, що запобігає взаємному впливу між ними. Сукупність каналів одного напрямку формує високочастотний «ствол» радіорелейної лінії (РРЛ). Зазвичай у РРЛ є два стволи, але їх може бути і більше. Передача та прийом УКХ сигналів відбуваються за допомогою параболічних антен (А), які виконують функції передавальних і приймальних, як показано на (рис. 2.5). На структурній схемі зображено, що в приймально-передавальних пунктах №1 і №2 знаходяться апаратура ущільнення (АУ), передавач (Пд) і приймач (Пр) УКХ сигналів, а також склад ретрансляційних пунктів. Ретранслятори виконують посилення прийнятих і переданих УКХ сигналів, а також можуть здійснювати корекцію сигналів, що зазнають впливу перешкод. Таким чином, збільшення кількості ретрансляційних пунктів дозволяє забезпечити більшу дальність передачі і високу стійкість сигналу до перешкод.

Як зазначалося раніше, надійна робота радіорелейних ліній (РРЛ) забезпечується за умови, що ретранслятори розташовані в зоні прямої видимості між антенами передавача і приймача. Для зменшення кількості ретрансляторів їх можна розміщувати на стаціонарних супутниках, які знаходяться нерухомо над поверхнею Землі на висоті близько 36 000 км — на геостаціонарній орбіті. Це дозволяє забезпечувати безперервний зв'язок із наземними станціями на частотах від 2 до 8 ГГц.

Досвід використання супутникового зв'язку в енергосистемах є досить позитивним. Проте через широке впровадження волоконно-оптичних ліній зв'язку інтерес енергетиків до супутникових технологій поступово знижується.

Волоконно-оптичні кабелі, що підвішуються на ЛЕП. Основні елементи волоконно-оптичної лінії зв'язку (ВОЛЗ) КП – кодувальний пристрій, ДВ – джерело випромінювання, М – модулятор, Р – ретранслятор, ПВ – приймач випромінювання, П – підсилювач, ДКП – декодувальний пристрій (рис. 2.6).

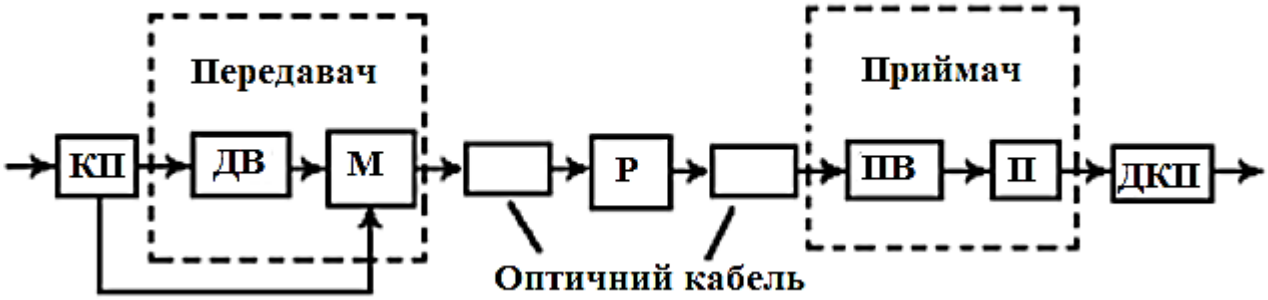

Рисунок 2.6 – Структура волоконно-оптичної лінії зв'язку

Передавач здійснює перетворення електричного сигналу у світловий (оптичний). По суті, у передавачі відбувається перенесення низькочастотного електричного сигналу в діапазон видимого спектра — тобто модуляція електромагнітних коливань видимого (оптичного) спектра. Приймач приймає світловий сигнал, що надходить через волоконно-оптичний кабель, і демодулює його, перетворюючи назад в електричний сигнал.

У структурі ВОЛЗ також знаходяться ще з’єднувачі (коннектори) які виконують важливу роль у забезпеченні узгодженості характеристик оптичного сигналу на виході передавача і на вході приймача з параметрами волоконно-оптичного кабелю. Вони також відповідають за стикування окремих компонентів волоконно–оптичної системи з мінімальними втратами сигналу.

В енергосистемах найбільш часто використовуються волоконно-оптичні або, просто, оптичні кабелі, що підвішуються на ЛЕП. Відомо кілька способів підвіски оптичних кабелів (ОК) на ЛЕП (рис. 2.7).

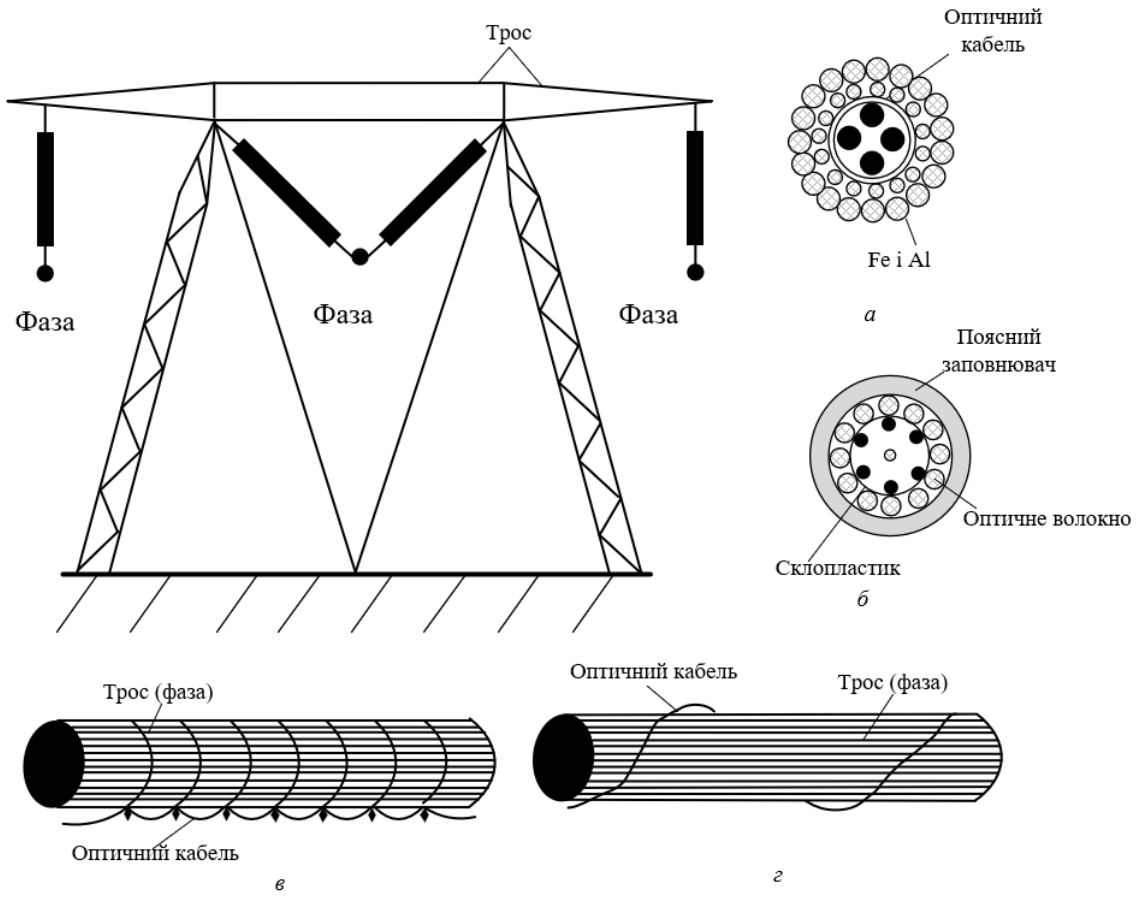

Рисунок 2.7 – Варіанти підвішування оптичних кабелів на ЛЕП: *а* – ОК, вбудований в блискавкозахисний трос або у фазу; *б* – самонесучий ОК; *в* – ОК на підвісках; *г* – спіральне намотування ОК на трос або фазу [22]

За першими двома варіантами ОК розташовується в центрі грозозахисного троса або фази. Самонесучий оптичний кабель має посилену броню, що гарантує необхідну механічну міцність при підвісці на лініях електропередачі (ЛЕП) з

великими прольотами. Кріплення ОК здійснюється за допомогою підвісок до грозозахисного троса або спеціально встановленого троса.

Підвісні оптичні кабелі можуть містити від 4 до 32 оптичних волокон. На (рис. 2.8) представлена конструкція оптичного кабелю, вмонтованого в трос. Кабель складається з чотирьох модулів, кожен з яких може містити 8 або 16 волокон. Оболонка виготовлена з алюмінію товщиною 1 мм, діаметр кабелю становить 8 мм. Трос має два повиви зі сталевих дротів діаметром 1,6 мм і зовнішній повив з алюмінієвих дротів діаметром 2 мм. Загальний діаметр троса — 18,4 мм, а маса підвіски на 1 км — близько 1 тонни.

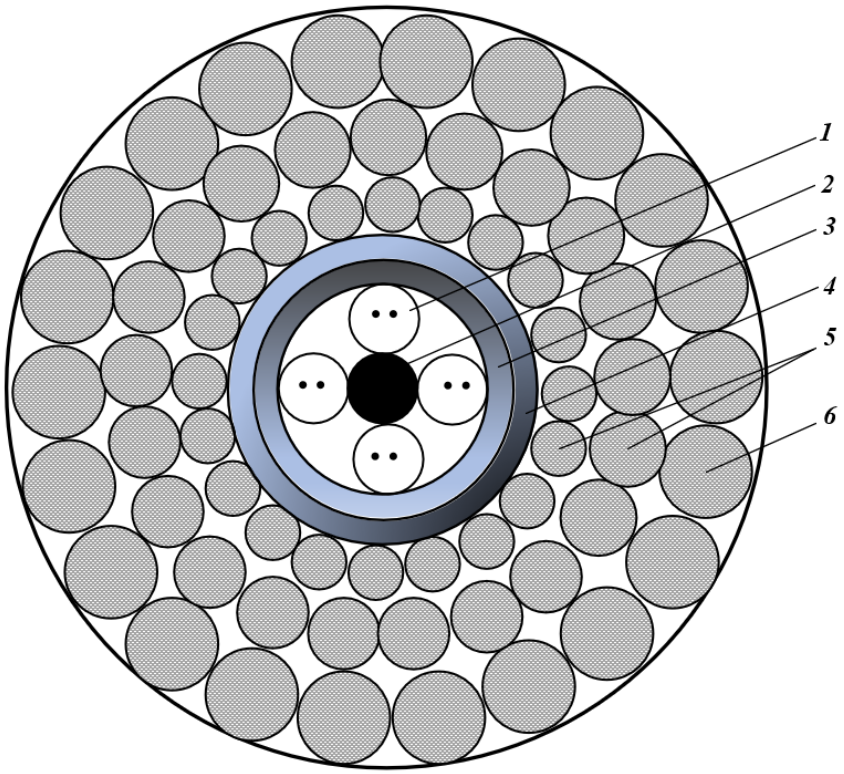

Рисунок 2.8 – Оптичний кабель вбудований у трос: *1* – волокно; *2* – силовий елемент; *3* – поліетилен; *4* – алюмінієва оболонка; *5* – сталеві дроти; *6* – алюмінієві дроти [22]

Варіант конструкції самонесучого кабелю наведено на (рис. 2.9). Кабель містить 6 або 12 волокон, для механічної міцності є два повиву стрижнів зі скловолокон діаметром по 2 мм. Зовні – поліетиленова оболонка. Загальний діаметр кабелю – 11 мм, маса – 296 кг/км.

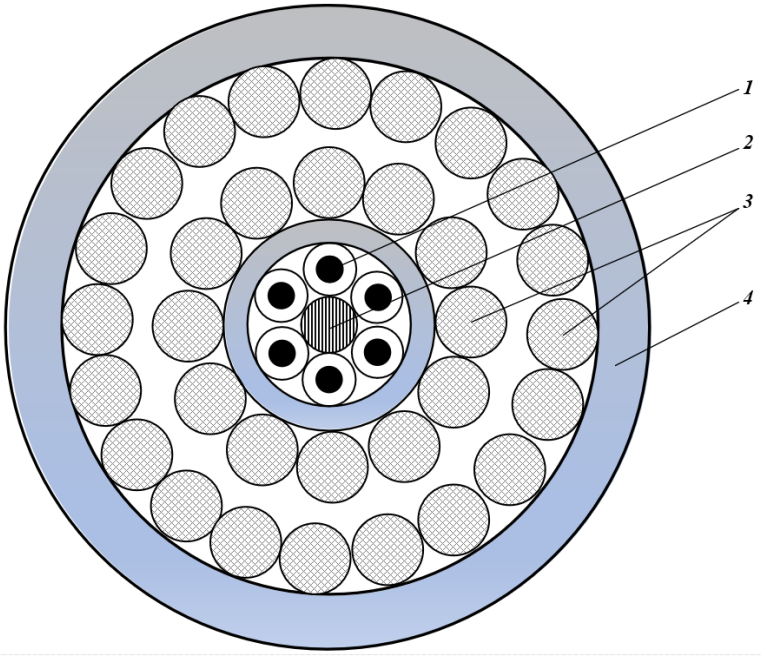

Рисунок 2.9 – Самонесучий оптичний кабель: *1* – волокно; *2* – силовий елемент; *3* – стрижні з склопластику; *4* – поліетиленова оболонка [22]

На (рис. 2.10) представлена типова конструкція багатомодульного оптичного кабелю з центральним силовим елементом.

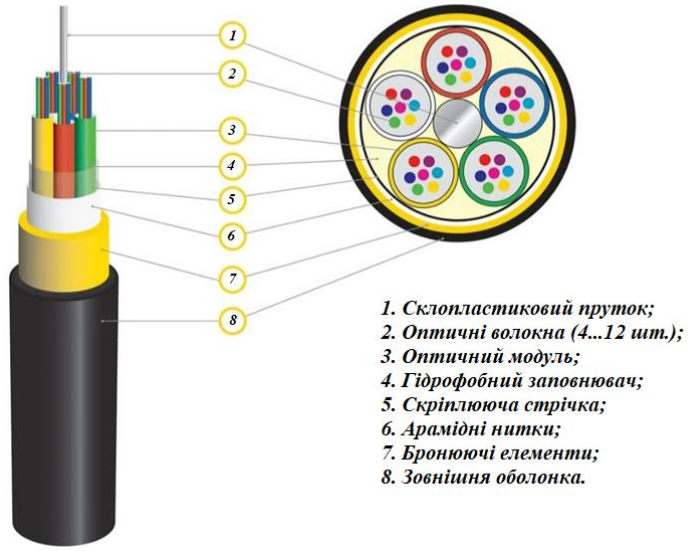

Рисунок 2.10 – Будова оптичного кабелю

Кожен елемент конструкції виконує свою функцію, забезпечуючи надійність передачі даних та захист волокон:

1) Склопластиковий пруток – центральний силовий елемент, що забезпечує механічну міцність кабелю та стійкість до розтягування.

2) Оптичні волокна (4…12 шт.) – основні елементи для передавання інформації у вигляді світлового сигналу. Кількість волокон у модулі може варіюватися залежно від потреб.

3) Оптичний модуль – захисна оболонка, в якій розміщені оптичні волокна. Захищає їх від механічних впливів і забезпечує гнучкість.

4) Гідрофобний заповнювач – речовина, що заповнює простір між волокнами й елементами модуля, запобігаючи проникненню вологи.

5) Скріплююча стрічка – елемент, що утримує внутрішні компоненти кабелю у фіксованому положенні та сприяє збереженню структури при монтажі.

6) Арамідні нитки – додаткові армуючі елементи, які підвищують міцність кабелю на розрив і забезпечують захист від деформацій.

7) Бронюючі елементи – шар із металевих або неметалевих матеріалів, що забезпечує захист кабелю від механічних пошкоджень і гризунів.

8) Зовнішня оболонка – захисний покрив кабелю, виготовлений із полімерного матеріалу, що забезпечує стійкість до впливу навколишнього середовища.

Супутникова навігаційна система. GPS, або Глобальна система позиціонування, зокрема її космічний сегмент, складається з сузір’я 24 супутників. Система, офіційно відома як NAVSTAR, була створена за замовленням і перебуває під контролем Міністерства оборони США. У 1980-х роках її відкрили для цивільного користування. GPS функціонує цілодобово по всьому світу незалежно від погодних умов. За допомогою цієї системи можна з високою точністю визначати координати та швидкість руху різних об’єктів. Для користування GPS не потрібно платити абонентську плату чи плату за підключення — достатньо лише придбати спеціальний GPS-приймач [22].

Супутники GPS рухаються навколо Землі по кругових орбітах, здійснюючи два оберти на добу, і передають навігаційні радіосигнали. GPS-приймачі отримують ці сигнали і визначають місцезнаходження за допомогою методу тріангуляції. Вони порівнюють час, коли сигнал був відправлений, з часом його

прийому, що дозволяє обчислити відстань до супутника. Маючи інформацію про відстані до кількох супутників, приймач може точно визначити своє положення і показати його на електронній карті.

Отримуючи сигнали мінімум від трьох супутників, GPS-приймач здатен визначити двовимірні координати користувача — широту та довготу. Якщо ж сигнали надходять від чотирьох і більше супутників, можна визначити тривимірне положення — широту, довготу та висоту. Крім цього, отримавши місцезнаходження, пристрій може розрахувати швидкість, напрямок руху, пройдений шлях, відстань до пункту призначення, а також час сходу та заходу сонця й інші корисні параметри.

Супутники GPS передають два малопотужних сигнали на частотах L1 і L2. Цивільні GPS – приймачі працюють на частоті L1=1575,42 МГц. Сигнали можна приймати лише від супутників, які знаходяться в зоні прямої видимості. При цьому хмари, скло та пластик не заважають передачі сигналу, тоді як більшість щільних перешкод, таких як будівлі, рельєф місцевості, металеві конструкції та люди, можуть його блокувати.

Сигнал, який передають супутники GPS, складається з трьох основних компонентів — псевдовипадкового коду, ефемеридних даних та альманаху. Псевдовипадковий код включає у себе унікальний номер супутника, що надсилає сигнал. У GPS-приймачах GARMIN цей номер можна побачити на сторінці супутників. Ефемеридні дані, які супутник постійно передає, містять важливу інформацію про стан супутника (активний він чи ні), а також актуальні дату і час. Саме ця частина сигналу широко використовується у сфері енергетики.

Застосування GPS у енергетиці пов’язане з контролем електроенергетичних систем. Завдяки GPS можна у реальному часі визначати кути зсуву фаз за формою кривої напруги у вузлах мережі, оскільки GPS забезпечує точну синхронізацію за часом. Розміщення GPS-приймачів у контрольних точках електричних мереж дозволяє здійснювати ефективний моніторинг їхньої стійкості [22].

Ще однією важливою задачею оперативного управління є оцінка стану електричної мережі на основі виміряних параметрів. Часто отримані дані не містять

інформації про кути зсуву фаз уздовж ліній електропередачі через проблеми синхронізації телевимірювань. Використання GPS у цій сфері допомогло подолати ці труднощі і сприяло створенню пристроїв, які можуть точно вимірювати кути зсуву фаз.

2.3. Комунікаційне обладнання

У сучасних енергетичних системах, побудованих за принципами цифровізації, важливу роль відіграє комунікаційне обладнання, яке забезпечує ефективну передачу, маршрутизацію, агрегацію та фільтрацію даних. Серед основних елементів цієї інфраструктури виділяють концентратори (хаби), маршрутизатори (роутери) та шлюзи. Всі вони виконують свої функції у складі мереж передачі інформації — як у межах підприємства, так і при інтеграції з вищими рівнями диспетчерських систем, зокрема SCADA, АСКОЕ, EMS тощо.

Концентратори є базовими пристроями, які використовуються для збирання інформації з кількох джерел (наприклад, лічильників електроенергії або сенсорів) та подальшої її передачі до головного сервера або іншого обладнання в мережі. Основна функція концентратора — агрегувати сигнали або дані від кількох пристроїв нижчого рівня та передавати їх через канал зв’язку на вищий рівень управління.

У сфері енергетики концентратори найчастіше використовуються в АСКОЕ. Вони розміщуються в розподільних пунктах або трансформаторних підстанціях і приймають дані з великої кількості розумних лічильників (Smart Meters), які встановлені в споживачів.

До основних функцій концентраторів належать:

– збір даних із лічильників через дротові (RS-485, PLC) або бездротові інтерфейси (ZigBee, LoRaWAN, Wi-Fi);

– тимчасове зберігання інформації у внутрішній пам’яті;

– шифрування, перевірка достовірності та цілісності даних;

– передача інформації через GSM, GPRS, Ethernet або оптичні лінії до серверів обліку;

– синхронізація часу та обробка запитів від центральної системи.

Розвиток технологій призвів до створення так званих «розумних концентраторів» — пристроїв, які мають вбудовані елементи аналізу даних, здатні самостійно ідентифікувати аномалії, визначати втрати електроенергії, виявляти маніпуляції зі споживанням та інше.

Маршрутизатор — це мережевий пристрій, що виконує функцію вибору оптимального маршруту для передачі даних між сегментами мережі. У контексті енергетичних систем маршрутизатори забезпечують зв'язок між локальними пристроями (системами керування, вимірювання, захисту) та глобальними інформаційними системами. Вони є критичним елементом у забезпеченні надійної та безперервної комунікації, особливо в умовах розгалуженої структури Smart Grid.

Маршрутизатори можуть працювати як у дротових, так і в бездротових мережах. Типові інтерфейси — Ethernet, LTE, 5G, Wi-Fi, а також промислові стандарти — RS-232/485, CAN, Modbus TCP/RTU, IEC 60870–5–104, IEC 61850.

Основні завдання маршрутизаторів:

– визначення маршруту для пакетів даних (routing);

– фільтрація трафіку згідно із заданими правилами (access control);

– забезпечення QoS — пріоритезація критичних повідомлень;

– перенаправлення трафіку у разі відмови основного каналу;

– шифрування даних (VPN, IPsec) для захисту інформації;

– сумісність з протоколами промислової автоматизації та мереж передачі даних.

Маршрутизатори можуть мати вбудовані функції моніторингу мережі, ведення логів, управління віддаленою конфігурацією (через веб-інтерфейс, SSH, SNMP), що особливо важливо для централізованих систем управління.

Шлюз — це пристрій, що виконує функцію зв'язку між двома мережами, які використовують різні протоколи або архітектури. У енергетичних системах шлюзи необхідні для інтеграції обладнання, яке не має єдиного стандарту обміну даними, в єдину інформаційну систему.

Наприклад, на одній підстанції можуть працювати пристрої з підтримкою Modbus RTU, DNP3, IEC 61850, OPC UA — шлюз дозволяє усім цим пристроям обмінюватися даними, використовуючи протоколи перетворення.

Шлюзи часто реалізуються у вигляді вбудованих пристроїв або програмно-апаратних комплексів. У сучасних умовах дедалі популярнішими стають шлюзи з підтримкою IIoT, які дозволяють підключати до енергетичних систем датчики, виконавчі пристрої та аналітичні платформи.

Функціональність шлюзів включає:

– перетворення протоколів (наприклад, з Modbus на IEC 104);

– буферизація даних у разі втрати зв'язку;

– встановлення зв'язку з хмарними платформами або SCADA-серверами;

– агрегація даних з кількох пристроїв;

– забезпечення інформаційної безпеки через шифрування та автентифікацію.

Шлюзи можуть також виконувати функції виявлення подій, інтеграції з системами відеоспостереження, передачі сигналів тривоги та навіть прийняття автономних рішень у випадку втрати централізованого керування.

У зв'язку з активним розвитком концепції Smart Grid, комунікаційне обладнання постійно вдосконалюється. З'являються пристрої з вбудованим штучним інтелектом, можливістю автономного прийняття рішень, підтримкою хмарних сервісів. Такі пристрої забезпечують не лише передачу даних, а й їхню попередню обробку, аналіз, а також прогнозування можливих відмов чи аномалій у системі.

Також набувають популярності програмно-конфігуровані шлюзи SDG дозволяють динамічно змінювати логіку взаємодії пристроїв залежно від режимів роботи енергосистеми або поточних потреб споживача.

У (табл. 2.3) наведена порівняльна характеристики комунікаційного обладнання.

Таблиця 2.3 – Порівняльна характеристика пристроїв

Тип пристрою	Основна функція	Приклад використання в енергетиці	Інтерфейси	Особливості
Концентратор	Збір та передача даних	АСКОЕ, Smart Metering	RS-485, PLC, GPRS	Об’єднання даних, тимчасове зберігання
Маршрутизатор	Передача даних між мережами	SCADA, EMS	Ethernet, LTE, Wi-Fi	QoS, VPN, моніторин
Шлюз	Протокольна конверсія	РЗА, АСКТП	Modbus, IEC 104, OPC UA	Інтеграція різних систем

Комунікаційне обладнання — це невід’ємна частина сучасних інформаційних систем в електроенергетиці. Концентратори, маршрутизатори і шлюзи забезпечують ефективну взаємодію між енергетичними об’єктами, сприяють надійності, масштабованості та безпеці обміну даними. Розуміння функціональних можливостей кожного з цих пристроїв дозволяє оптимізувати побудову мережі зв’язку, скоротити витрати на обслуговування та підвищити загальну ефективність управління енергетичною системою.

2.4. Принципи побудови мереж: топології, сегментація, адресація

У сучасних інформаційних системах, зокрема в системах передачі інформації в електроенергетиці, надійність, швидкодія та безперебійна взаємодія між пристроями значною мірою залежать від правильного проєктування мережевої інфраструктури. Принципи побудови мереж, що включають топології, сегментацію та адресацію, визначають логіку функціонування всієї системи, її здатність до масштабування, відмовостійкість і рівень безпеки. У цьому підрозділі

розглянемо ключові принципи побудови інформаційних мереж в енергетиці, а також особливості реалізації мережевих рішень у контексті АСУ ТП, SCADA, АСКОЕ та цифрових підстанцій.

Топологія мережі — це спосіб фізичного або логічного з'єднання вузлів мережі, що визначає схему їх взаємодії. У контексті енергетичних систем найбільш поширені такі топології:

1) Шинна топологія. Шинна топологія передбачає підключення всіх пристроїв до одного комунікаційного каналу (шини). Переваги — простота реалізації, мінімальні витрати кабелю. Недоліки — низька надійність (вихід з ладу шини зупиняє всю мережу), труднощі масштабування;

2) Радіальна топологія. У зіркоподібній топології всі пристрої підключені до центрального вузла (наприклад, маршрутизатора або комутатора). Це підвищує керованість та локалізацію несправностей. Широко використовується в локальних мережах енергетичних об'єктів;

3) Кільцева топологія. Пристрої з'єднані послідовно, утворюючи замкнуте кільце. Перевагою є можливість організації резервування: при порушенні одного сегмента зберігається зв'язок за рахунок зворотного напряму. Часто застосовується в системах промислової автоматизації (наприклад, на базі протоколу ProfiBus);

4) Сітчаста (mesh) топологія. Передбачає з'єднання кожного вузла з кількома іншими, що забезпечує високу надлишковість і стійкість до відмов. У Smart Grid ця топологія забезпечує найвищу надійність і гнучкість взаємодії, особливо для розподілених об'єктів;

5) Ієрархічна (деревоподібна) топологія. Поєднує кілька рівнів підмереж, часто організованих за принципом «об'єкт — район — регіон — центр». Відповідає структурі енергетичних компаній, що мають диспетчерське управління на кількох рівнях.

Сегментація мереж. Сегментація — це розподіл великої мережі на менші логічні або фізичні частини для підвищення продуктивності, безпеки та керованості. Види сегментацій:

1) Сегментація за функціональним призначенням. В енергетиці прийнято виділяти сегменти для:

– оперативного управління (SCADA);

– комерційного обліку (АСКОЕ);

– захисту та автоматики (РЗА);

– корпоративного IT-середовища;

– відеонагляду та безпеки.

Такий поділ дозволяє мінімізувати ризики поширення збоїв та кібератак, а також встановити різні політики доступу.

2) VLAN-сегментація. Віртуальні локальні мережі VLAN дають змогу створювати логічно ізольовані сегменти в межах однієї фізичної мережі. Це особливо актуально в розподілених системах, де немає можливості фізично відокремити підсистеми.

3) DMZ та між мережеві екрани. У системах, що мають вихід в інтернет (наприклад, для віддаленого моніторингу), застосовують зони демілітаризованого доступу DMZ, де розміщуються сервери, які приймають зовнішні запити. Між мережеві екрани контролюють трафік між зонами.

Одним із принципів побудови інформаційної мережі є її адресація вона поділяється на:

– IP-адресація. Основою ідентифікації пристроїв у мережах є IP-адреси (IPv4 або IPv6). У великих енергетичних підприємствах практикується чітке структурування адресного простору, з поділом за регіонами, об’єктами, підсистемами;

– MAC-адресація. На канальному рівні кожен пристрій має унікальну MAC-адресу. Вона використовується для локальної маршрутизації в межах одного сегмента мережі;

– Адресація в польових мережах. У SCADA або АСКОЕ застосовуються логічні адреси пристроїв (наприклад, об’єкти IEC 61850 — Logical Node, Functional Constraint). Вони дозволяють визначати структуру даних, відповідно до функціонального призначення;

– DNP3, Modbus, IEC 60870–5–104. Ці протоколи мають власні схеми адресації даних. Наприклад, у Modbus кожному регістру присвоєно унікальний номер; в DNP3 — це об’єктна адреса (Object Group, Variation, Index).

Вимоги до побудови інформаційних мереж в енергетиці. Побудова мереж в енергетичних об’єктах повинна відповідати ряду вимог:

– надійність. Резервування каналів, мережна структура, захищені протоколи;

– безпека. Сегментація, фаєрволи, контроль доступу;

– продуктивність. Достатня пропускна здатність, низька затримка;

– масштабованість. Можливість розширення без зміни архітектури;

– сумісність. Підтримка галузевих стандартів (IEC 61850, 104, DNP3, Modbus TCP тощо);

– керованість. Централізований моніторинг, звіти, засоби конфігурації.

У сучасній практиці проєктування мережевої інфраструктури для електростанцій, підстанцій та розподільчих мереж широко застосовуються:

– Redundant Ring Ethernet для забезпечення безперервного обміну;

– IP/MPLS мережі для магістральних каналів передачі в операторських компаніях;

– SD-WAN технології для динамічного керування трафіком між об’єктами;

– польові шини (наприклад, ProfiNet, EtherCAT) у системах автоматизації.

Усе це забезпечує ефективну інформаційну взаємодію на всіх рівнях енергосистеми: від польового рівня до центру управління.

Розуміння принципів побудови мереж — ключовий етап у проєктуванні надійних інформаційних систем в електроенергетиці. Вибір топології, правильна сегментація та ефективна адресація визначають продуктивність, масштабованість і безпеку мережі. В умовах зростання цифрових технологій та вимог до оперативності обміну даними, роль грамотної мережевої архітектури постійно зростає. Енергетичні об’єкти, зокрема підстанції, диспетчерські центри та

розподілені джерела генерації, мають працювати у єдиному інформаційному просторі, що можливе лише за умови застосування сучасних підходів до побудови мереж.

2.5. Надійність, затримка, швидкодія систем

У сучасних умовах стрімкого розвитку цифрових технологій та автоматизованих систем управління, особливо у галузі енергетики, надзвичайно важливою є надійна передача інформації між усіма компонентами інформаційної системи. Надійність, затримка та швидкодія — це три основоположні характеристики, що визначають ефективність функціонування інформаційних систем і прямо впливають на безпеку, стабільність та економічну доцільність їх використання. У даному підрозділі буде детально розглянуто сутність кожного з цих понять, фактори, що впливають на них, та способи забезпечення оптимальних параметрів роботи систем передачі даних.

Надійність — це властивість системи безперебійно функціонувати впродовж визначеного проміжку часу при дотриманні встановлених умов експлуатації. У контексті енергетичних інформаційних систем, таких як АСКОЕ, SCADA, РЗА (релейний захист і автоматика), EMS, надійність означає здатність системи постійно і коректно передавати, приймати та обробляти інформацію. Основні характеристики надійності:

– безвідмовність — відсутність помилок або збоїв протягом експлуатаційного періоду;

– доступність — здатність системи функціонувати у будь-який момент часу, коли є запит на інформацію;

– цілісність даних — захист від спотворення або втрати інформації під час передачі;

– відновлюваність — можливість швидко повернути систему у робочий стан після збоїв.

На практиці розраховують такі показники надійності:

– MTBF — середній час між відмовами;

– MTTR — середній час відновлення після відмови;

– Availability (%) (доступність) = MTBF / (MTBF + MTTR) × 100 %.

До методів підвищення надійності належать:

– резервування обладнання і каналів передачі даних;

– використання перевірених протоколів з механізмами виявлення і виправлення помилок;

– постійний моніторинг стану систем;

– проєктування з урахуванням принципів відмовостійкості.

Затримка або latency — це часовий інтервал між моментом ініціації передачі даних та моментом їх отримання. У критичних енергетичних системах допустимі значення затримок дуже низькі: від мілі секунд до кількох секунд, залежно від типу застосування.

Види затримок:

– затримка передачі (Transmission delay) — обумовлена довжиною кабелю, швидкістю сигналу та пропускною здатністю мережі;

– затримка обробки (Processing delay) — викликана обробкою даних на пристроях (модеми, комутатори, маршрутизатори);

– затримка черги (Queuing delay) — час очікування даних у черзі перед передачею;

– затримка ретрансляції (Propagation delay) — залежить від відстані та середовища передачі (мідь, оптоволокно, радіо).

Приклади критичних значень затримок для передачі інформації в електроенергетиці:

– системи РЗА: ≤ 10 мс;

– GOOSE-повідомлення в IEC 61850: ≤ 3 мс;

– диспетчерське управління: до 100 мс;

– системи обліку (АСКОЕ): допустима затримка — хвилини або години.

Способи мінімізації затримки:

– оптимізація маршрутизації;

– використання Quality of Service для пріоритетного трафіку трафіку;

– впровадження оптичного середовища передачі;

– пряме підключення без використання непотрібних вузлів.

Швидкодія — це здатність інформаційної системи оперативно виконувати завдання з передачі, обробки та реагування на інформацію. Часто її вимірюють у кількості транзакцій на одиницю часу або у бітах за секунду. До чинників що впливають на швидкодію належать:

– пропускна здатність каналу — кількість інформації, яка може бути передана за одиницю часу;

– навантаження на мережу — збільшення кількості пристроїв або даних призводить до зниження швидкодії;

– протокол передачі — TCP (надійний, але повільніший), UDP (швидший, але ненадійний);

– якість обладнання — процесори маршрутизаторів, буферизація, кешування.

До способів підвищення передачі інформації належать:

– модернізація фізичної інфраструктури (оптика, комутатори рівня 3);

– використання сучасних протоколів і стандартів;

– мінімізація надмірної маршрутизації;

– розвантаження каналів передачі через сегментацію мережі.

Варто розуміти, що між трьома параметрами — надійністю, затримкою та швидкодією — існує певний *компроміс*. Наприклад, підвищення надійності шляхом використання TCP може призвести до збільшення затримки. А спроби досягти максимальної швидкодії через UDP можуть поставити під загрозу цілісність переданих даних. Тому системи енергетики проєктуються з урахуванням необхідного *балансу*:

– для аварійних систем — пріоритет затримки;

– для комерційних — пріоритет цілісності;

– для аналітичних — пріоритет обсягу даних та швидкодії.

Прикладні аспекти у галузі енергетики відносно надійності та швидкодії інформаційних систем. Прикладні аспекти цих систем безпосередньо впливають

на ефективність функціонування енергетичних об’єктів, таких як електростанції, мережі передачі електричної енергії та інші критично важливі інфраструктури. Висока надійність забезпечує безперервність енергопостачання, а швидкодія сприяє оперативному реагуванню на зміни та аварійні ситуації.

SCADA-системи використовуються для моніторингу та управління обладнанням енергомереж. Вони вимагають високої надійності та прийнятної швидкодії. При втраті даних або їх затримці можлива невчасна реакція на аварійну ситуацію.

Релейний захист — це одна з найбільш критичних сфер. Для GOOSE-повідомлень, що ініціюють дію захисту, затримка повинна бути мілісекундною. Всі елементи — комутатори, мережеві карти, трансивери — повинні бути сертифіковані на відповідність стандарту IEC 61850.

АСКОЕ комерційний облік енергії потребує достовірності, а не швидкості. Проте і тут надмірна затримка може призводити до похибок у балансах, особливо в режимі реального часу.

*Smart Grid***.** Інтелектуальні енергосистеми інтегрують велику кількість сенсорів, контролерів, IoT-пристроїв. Тут кожна ланка повинна мати високу швидкодію і здатність до самовідновлення — при цьому без втрати цілісності даних.

Надійність, затримка та швидкодія — це не ізольовані поняття, а взаємозалежні параметри, що впливають на функціонування інформаційних систем в енергетиці. Їх оптимальне поєднання забезпечує стійкість, безпеку та ефективність всієї інфраструктури. Важливою умовою успішного впровадження і експлуатації таких систем є дотримання міжнародних стандартів, використання якісного обладнання, резервування каналів і постійний моніторинг.

Висновки до розділу 2

У другому розділі навчального посібника було комплексно розглянуто фундаментальні складові інформаційних систем, що функціонують у контексті електроенергетики. Вивчення структури таких систем, основних елементів та

принципів їх побудови створює основу для ефективного опанування спеціалізованих рішень, які застосовуються в автоматизованих енергетичних комплексах.

Розгляд починається з джерел і приймачів інформації — базових елементів, що формують і споживають інформаційні сигнали. Було встановлено, що функціональне призначення, фізична природа сигналів та способи взаємодії із середовищем визначають класифікацію цих компонентів, а також впливають на їх ефективність у різних технологічних контекстах. Знання про сучасні типи джерел — від аналогових трансформаторів струму до цифрових Smart Meter і фазометрів — є основою для побудови достовірної системи збору даних. Аналогічно, приймачі, які виконують функції аналізу, візуалізації та управління, мають різний рівень інтеграції та інтерфейсної реалізації. Такий підхід дозволяє забезпечити надійне та гнучке реагування на зміни в режимі реального часу, що критично для керування енергосистемою.

Подальше дослідження було присвячене каналам зв’язку — невід’ємному елементу передачі інформації між джерелами і приймачами. Увагу зосереджено на класифікації каналів за типом середовища, що включає провідникові, волоконно-оптичні та бездротові рішення. Розглянуто особливості їх використання в умовах енергетичних об’єктів, зокрема в аспектах протидії електромагнітним завадам та забезпечення безперервного обміну. Було підкреслено значення розуміння відмінностей між аналоговими, цифровими й імпульсними сигналами, а також важливість вибору оптимального середовища передачі, виходячи з технічних, економічних та експлуатаційних умов.

Окремий акцент зроблено на фізичних каналах зв’язку — лініях, що фактично утворюють інфраструктурну основу інформаційного обміну. Практичні приклади організації каналів по високовольтних лініях, розподільчих мережах і з використанням спеціалізованих ВОЛЗ-рішень демонструють широке різноманіття інженерних підходів до вирішення завдань телемеханіки, зв’язку та синхронізації. Важливе значення має також розгляд способів організації зв’язку через супутникові канали та радіорелейні лінії — у тих випадках, коли фізична прокладка неможлива чи економічно необґрунтована.

Комунікаційне обладнання розглядається як інтелектуальна ланка системи: концентратори, маршрутизатори та шлюзи забезпечують агрегацію, маршрутизацію і перетворення протоколів, що дозволяє інтегрувати різнорідні компоненти системи в єдине інформаційне середовище. Важливо розуміти функціональне розмежування між цими пристроями, їх здатність до масштабування, віддаленої конфігурації, резервування та підключення до хмарних рішень — особливо в умовах розвитку концепції Smart Grid.

Принципи побудови мереж — ще один визначальний аспект, що був розглянутий у межах розділу. Було охарактеризовано поширені топології (шинна, зіркова, кільцева, сітчаста, ієрархічна), кожна з яких має свої переваги та обмеження щодо масштабування, стійкості до відмов та експлуатаційної зручності. Вивчення підходів до сегментації, у тому числі через VLAN, DMZ і зонування за функціональними ознаками, дає змогу проєктувати безпечні і логічно ізольовані мережі, придатні до роботи в умовах підвищених вимог до безпеки. Адресація в мережах — як фізична, так і логічна — підтримує ефективну маршрутизацію та диспетчеризацію, що особливо актуально для великих розподілених систем.

Нарешті, ключовими критеріями, які формують технічну оцінку систем, були визначені надійність, затримка та швидкодія. Вивчення взаємозв’язку між цими параметрами дозволяє розуміти компроміси, які виникають при проєктуванні систем — наприклад, між часом реакції в системах релейного захисту та гарантіями цілісності даних у комерційних облікових комплексах. Важливим є вміння адаптувати параметри мережевої інфраструктури під потреби кожної конкретної підсистеми, враховуючи характер навантаження, критичність затримок і вимоги до відмовостійкості.

Таким чином, розділ формує цілісне уявлення про інформаційні системи в енергетиці: від фізичних сенсорів до логічної інфраструктури мережі. Практичне розуміння описаних концепцій є фундаментом для подальшого вивчення специфічних технологій передачі даних, управління об’єктами енергетики та проєктування сучасних цифрових систем енергоконтролю.

Запитання для контролю знань за другим розділом

1. Які основні складові формують структуру інформаційних систем в електроенергетиці?

2. Чим відрізняються джерела інформації за фізичною природою сигналів?

3. Які сучасні типи джерел інформації використовуються в енергетичних системах?

4. Які функції виконують приймачі інформації в автоматизованих енергетичних системах?

5. Чому інтеграція і гнучкість приймачів важливі для реагування в реальному часі?

6. Які типи каналів зв’язку розглядаються у контексті енергетики?

7. Які особливості використання волоконно-оптичних ліній зв’язку на енергетичних об’єктах?

8. Які переваги і недоліки мають бездротові канали зв’язку в умовах енергетики?

9. У чому полягає відмінність між аналоговими, цифровими та імпульсними сигналами?

10. Як вибір типу середовища передачі залежить від технічних та економічних умов?

11. Яке значення мають фізичні канали зв’язку у побудові телемеханічних систем?

12. Які приклади практичного застосування каналів зв’язку у високовольтних мережах?

13. Коли доцільне використання супутникового або радіорелейного зв’язку?

14. Яку роль відіграють маршрутизатори, шлюзи та концентратори в інформаційних системах?

15. Чому важливо розуміти функціональне розмежування між комунікаційними пристроями?

16. Які топології мереж застосовуються в енергетиці та які їхні ключові властивості?

17. Що таке сегментація мережі та які методи її реалізації використовуються?

18. Як здійснюється адресація в енергетичних мережах і для чого вона потрібна?

19. Які параметри оцінюють технічну ефективність інформаційної системи?

20. Які компроміси виникають між швидкодією, надійністю та затримкою в енергетичних мережах?

3. ПРОТОКОЛИ ТА СТАНДАРТИ ПЕРЕДАЧІ ДАНИХ В ЕЛЕКТРОЕНЕРГЕТИЦІ

3.1. Роль протоколів у передачі енергетичних даних

У сучасних енергетичних системах, де передача інформації відіграє ключову роль у забезпеченні ефективної, безпечної та стабільної роботи, особливе значення мають протоколи передачі даних. Саме вони визначають, як дані кодуються, передаються, приймаються та інтерпретуються в системах автоматизації, обліку, керування та моніторингу в електроенергетиці.

Протокол — це набір правил, які регламентують формат, структуру і послідовність передавання повідомлень між пристроями, що взаємодіють через інформаційні канали. У контексті енергетики, де йдеться про управління обладнанням високої критичності, ці правила повинні забезпечувати не тільки точність і швидкість, але й високий рівень надійності, синхронності та захищеності.

Перехід до цифрових енергосистем на базі концепції Smart Grid, широке використання відновлюваних джерел енергії, розвиток технологій зберігання електроенергії та зростаюча кількість енергонезалежних об’єктів зумовили потребу у стандартизованому обміні даними між великою кількістю різнорідного обладнання. Протоколи забезпечують:

– уніфікацію обміну даними між пристроями різних виробників;

– скорочення часу розробки та впровадження систем керування;

– сумісність пристроїв в межах однієї або кількох мереж;

– інтеграцію елементів автоматизації, обліку, релейного захисту, SCADA та інших систем;

– надійність у ситуаціях, коли необхідна оперативність рішень (наприклад, аварійне вимкнення).

Протоколи можна класифікувати за кількома ознаками:

а) за рівнем моделі OSI:

– канальні (наприклад, Modbus RTU);

– мережеві (наприклад, IP);

– транспортні (TCP/UDP);

– прикладні (наприклад, IEC 60870–5–104, DNP3, IEC 61850);

б) за призначенням:

– для моніторингу та диспетчерського управління (SCADA);

– для автоматизації підстанцій;

– для релейного захисту та автоматики;

– для інтелектуального обліку (Smart Metering).

в) за типом передачі:

– серійні протоколи (Modbus RTU, IEC 60870–5–101);

– мережеві IP–протоколи (IEC 60870–5–104, IEC 61850, DNP3 over TCP/IP).

Протоколи передачі даних у системах енергетики виконують широкий спектр функцій:

– формування кадрів (кадрування). Чітке розмежування початку і кінця повідомлення;

– адресація. Вказівки, до якого пристрою направлено повідомлення;

– управління потоком. Контроль за кількістю переданих даних;

– виявлення і корекція помилок. Контрольні суми, підтвердження отримання;

– синхронізація. Забезпечення часової узгодженості між даними;

– безпека. Шифрування, автентифікація, цифрові підписи;

– керування доступом до середовища передачі. Запобігання конфліктам у мережі.

До найрозповсюдженіших протоколів в енергетиці належать:

а) IEC 60870–5–101/104. Один з найпоширеніших протоколів в енергетиці. Версія 101 — для серійного обміну (RS-232, RS-485), версія 104 — для мереж IP. Протокол забезпечує [26]:

– передачу технологічних сигналів (станів, вимірів, аварій);

– дистанційне керування обладнанням;

– синхронізацію часу;

– роботу в реальному часі.

б) IEC 61850. Сучасний високорівневий стандарт, орієнтований на автоматизацію підстанцій. Його особливості [26]:

– об’єктно-орієнтований підхід до представлення пристроїв;

– підтримка високошвидкісних повідомлень GOOSE;

– масштабованість і гнучкість;

– підтримка віртуальних пристроїв, які об’єднують функціональність різного устаткування.

в) Modbus. Простий, широко поширений протокол, що використовується для взаємодії з контролерами, датчиками та приводами. Випускається у версіях RTU, ASCII та TCP. Підтримується практично всіма PLC;

г) DNP3. Розроблений для використання у віддалених об’єктах. Має високу стійкість до збоїв і можливість пакетного накопичення даних з подальшою передачею.

Одним із викликів у галузі залишаються розбіжності між протоколами, які застосовуються на різних рівнях управління. Для усунення цієї проблеми активно використовуються шлюзи протоколів та конвертери форматів, що дозволяють інтегрувати:

– IEC 61850 ↔ Modbus;

– IEC 60870–5–104 ↔ DNP3;

– OPC UA ↔ SCADA-протоколи.

Розробка єдиних інтерфейсів передачі даних сприяє побудові гетерогенних (різнорідних) інформаційних систем, що охоплюють елементи від датчика до центру диспетчеризації.

У контексті енергетичних систем до протоколів висуваються такі основні вимоги:

– реальний час: мінімальна затримка при передаванні критичних команд;

– надійність: підтвердження доставки, повторна передача при збої;

– масштабованість: підтримка великої кількості пристроїв;

– сумісність: можливість взаємодії пристроїв від різних виробників;

– безпека: автентифікація користувачів, шифрування каналів.

В (табл. 3.1) наведений порівняльний аналіз перерахованих протоколів.

Таблиця 3.1 – Порівняння стандартів передачі даних в енергетиці

№	Характеристика	IEC 60870–5–104	IEC 61850	Modbus TCP	DNP3
1	Призначення	Телемеханіка, диспетчерське управління	Цифрові підстанції, автоматизація	Простий обмін даними між пристроями	Телемеханіка, SCADA-системи
2	Передача по TCP/IP	Так	Так	Так	Можливо через DNP3 over TCP
3	Структура даних	Проста, ієрархічна	Об’єктно-орієнтована	Реєстри, регістри та біти	Ієрархічна, з типізацією
4	Масштабованість	Середня	Висока	Обмежена	Середня
5	Інтероперабельність (здатність взаємодіяти різні системи	Обмежена	Висока	Низька	Середня
6	Швидкість реакції	Висока	Дуже висока (особливо GOOSE)	Висока	Середня
7	Підтримка подій у реальному часі	Часткова	Повна (GOOSE, Sampled Values)	Немає	Обмежено
8	Підтримка часової синхронізації	Зовнішня	Вбудована (SNTP, PTP)	Залежить від реалізації	Часткова (часові мітки)
9	Безпека	Базова	Висока (із розширеннями)	Низька	Покращена в DNP3 Secure
10	Тип обміну	Клієнт-сервер	Клієнт-сервер + публікація/підписка	Клієнт-сервер	Клієнт-сервер

Продовження таблиці 3.1

№	Характеристика	IEC 60870–5–104	IEC 61850	Modbus TCP	DNP3
11	Тип даних	Дискретні та аналогові	Уніфіковані об’єкти даних	Дискретні, аналогові	Дискретні, аналогові
12	Стандартизація	IEC	IEC	Де-факто (не формальний стандарт)	IEEE та IEC
13	Головна перевага	Простота, надійність	Універсальність, швидкодія	Простота реалізації	Підтримка широких мереж SCADA
14	Головний недолік	Застаріла модель даних	Складність впровадження	Відсутність безпеки	Обмежена масштабованість
15	Застосування	SCADA, диспетчерські центри	Цифрові підстанції, Smart Grid	Промислові мережі, лічильники	SCADA, телеметрія, підстанції

У сучасній цифровій підстанції часто поєднуються кілька протоколів. Наприклад:

– мережа процесів (Process Bus) використовує IEC 61850 Sampled Values;

– для обміну з контролерами застосовується GOOSE (IEC 61850);

– для підключення до SCADA — IEC 104;

– для резервного обліку — Modbus TCP.

Ця архітектура дозволяє реалізувати розподілену інтелектуальну автоматизацію, де кожен пристрій обмінюється даними з іншими в режимі реального часу.

З розвитком технологій штучного інтелекту, інтернету речей (IoT), хмарних обчислень та 5G, зростає потреба у нових протоколах:

– MQTT — для IoT-сенсорів;

– OPC UA — для інтеграції з корпоративними IT-системами;

– TLS/HTTPS — для безпечного обміну;

– REST API — для веб-сервісів.

Усе це свідчить про еволюцію протоколів від вузькоспеціалізованих до гнучких, платформо-незалежних рішень, що легко масштабується.

Протоколи передачі даних є ключовим елементом цифрової трансформації енергетики. Вони забезпечують уніфіковану мову взаємодії між пристроями, сприяють підвищенню ефективності управління, точності обліку, швидкості реагування систем автоматики та рівню безпеки. Впровадження протоколів типу IEC 61850, IEC 104, DNP3 та Modbus дозволяє створювати інтегровані, масштабовані й захищені енергетичні інфраструктури, які відповідають сучасним викликам і перспективам розвитку галузі.

3.2. Протоколи IEC 60870–5–101/104, DNP3, Modbus

У світі енергетичних інформаційних систем ключову роль відіграють протоколи обміну даними, які забезпечують передачу, інтерпретацію, контроль і зберігання великої кількості інформації між численними пристроями. Серед найбільш поширених і визнаних стандартів у галузі автоматизації енергетики — IEC 60870–5–101, IEC 60870–5–104, DNP3 та Modbus. Кожен з них має унікальні характеристики, призначення, особливості реалізації та сферу застосування.

Стандарт IEC 60870–5–101 був розроблений як частина великого набору протоколів для телемеханіки. Його основна мета — забезпечити надійну комунікацію між об’єктами управління RTU та центрами диспетчерського керування SCADA. Протокол орієнтований на асинхронні серійні лінії зв’язку. До його основних особливостей належать:

– підтримує контрольну суму CRC, що забезпечує надійність передачі;

– орієнтований на одночасну роботу з кількома типами інформаційних об’єктів: змінні, команди, індикатори подій;

– має низьку смугу пропускання, що робить його придатним для використання в умовах обмежених ресурсів зв’язку, як-от радіомодемні мережі або аналогові канали зв’язку.

Технічні параметри:

– швидкість передачі: 300–9600 біт/с;

– архітектура: Master-Slave (односпрямований обмін);

– підтримка функціональних груп: моніторинг, управління, синхронізація годинника, тестування зв’язку.

Переваги:

– простота реалізації;

– стійкість до завад у мережі;

– довготривала експлуатація, перевірена часом.

Недоліки:

– обмежена швидкодія;

– відсутність підтримки IP-протоколів;

– складність масштабування та інтеграції з новітніми технологіями.

Протокол IEC 60870–5–104 (IEC 104). Цей протокол є розширенням IEC 101, адаптованим для мереж TCP/IP, що суттєво розширює можливості стандарту. Основна відмінність — використання мережевих протоколів передачі як транспорту даних. Основні особливості:

– підтримує швидкісні Ethernet–мережі;

– відкритий протокол, сумісний із мережею Інтернет;

– підтримка одночасної передачі даних у реальному часі.

Переваги:

– вища швидкість передачі даних;

– легкість інтеграції в існуючу IP-інфраструктуру;

– підтримка шифрування та авторизації;

– підтримка асинхронного обміну інформацією.

Недоліки:

– більші вимоги до стабільності мережі;

– ускладнене конфігурування;

– залежність від надійності TCP-з’єднання.

IEC 104 широко використовується в цифрових підстанціях, диспетчерських центрах енергокомпаній, системах аварійного управління, віддаленого моніторингу та управління електромережами.

Протокол DNP3. Був розроблений у 1990-х роках у США для потреб SCADA-систем. Він був створений як більш сучасна альтернатива протоколам IEC, із фокусом на буферизацію даних, збереження часових міток і підтримку надійної передачі навіть за умов втрати зв'язку.

До його особливостей можна віднести:

– власна ієрархічна архітектура;

– підтримка оптимізації трафіку через класифікацію даних: статичні, події, пріоритети;

– буферизація подій в разі розриву зв'язку з можливістю їх відновлення після відновлення каналу.

Технічні параметри:

– підтримує як серійне з'єднання, так і TCP/IP;

– мітки часу використовуються для реєстрації змін стану;

– підтримує захищену автентифікацію, шифрування, контроль доступу (у новітніх реалізаціях).

Переваги:

– надійна передача даних;

– буферизація подій із мітками часу;

– відкритість і підтримка багатьма виробниками.

Недоліки:

– складність конфігурації та аналізу;

– різні версії можуть бути несумісні між собою;

– не є нативним IP-протоколом (але підтримує TCP).

DNP3 використовується переважно в розподілених системах управління, особливо у США, Канаді та Австралії. У Європі він менш поширений, але часто присутній у системах автоматизації розподілу енергії, водопостачання, нафтових та газових трубопроводах.

Протокол Modbus. Один із найстаріших промислових протоколів, який досі широко використовується в різних галузях, включаючи енергетику, водопостачання, HVAC та автоматизацію виробництва. Існує кілька версій: Modbus RTU, Modbus ASC II, Modbus TCP. Має таку структуру та формати :

– Modbus RTU використовує компактний формат кадрів із CRC-контролем і працює в серійних мережах;

– Modbus TCP — адаптація до Ethernet, що використовує той самий протокол прикладного рівня, але працює через TCP-порт 502.

Архітектура Modbus:

– модель master-slave (головний – підлеглий) або клієнт-сервер (TCP);

– кожен пристрій має унікальну адресу;

– команди надсилаються майстром, а підлеглі відповідають лише на запити.

Переваги:

– простота протоколу;

– відкритість стандарту;

– широка підтримка в пристроях нижнього рівня (датчики, лічильники, PLC).

Недоліки:

– відсутність міток часу;

– відсутність підтвердження доставки на прикладному рівні;

– не підходить для критично важливих завдань з високою надійністю.

Протокол Modbus широко застосовується в автоматизації для вирішення різних завдань. Зокрема, його використовують для моніторингу та керування генераторами, що дозволяє віддалено відстежувати їхній стан і параметри роботи. Крім того, Modbus забезпечує контроль температури, тиску та споживання ресурсів у промислових системах, сприяючи точному регулюванню технологічних процесів. Ще одним важливим напрямом застосування є інтеграція обладнання з HMI-панелями та SCADA-системами через OPC-сервери, що забезпечує

візуалізацію та централізоване управління об’єктами в режимі реального часу. В (табл. 3.2) наведено порівняльну характеристику протоколів.

Таблиця 3.2 – Порівняння протоколів

№	Критерій	IEC 60870–5–101	IEC 60870–5–104	DNP3	Modbus RTU/TCP
1	Тип зв’язку	Серійний	Ethernet TCP/IP	Серійний / TCP/IP	Серійний / TCP/IP
2	Наявність міток часу	Частково	Так	Так	Ні
3	Буферизація подій	Обмежена	Часткова	Повна	Відсутня
4	Надійність	Середня	Висока	Дуже висока	Середня
5	Швидкодія	Низька	Висока	Середня	Висока
6	Гнучкість	Обмежена	Середня	Висока	Низька
7	Підтримка безпеки	Обмежена	Так	Так (IEC 62351)	Ні
8	Тип архітектури	Master-Slave	Client-Server	Client-Server	Master-Slave

Кожен із розглянутих протоколів має своє специфічне місце в архітектурі автоматизованих енергетичних систем. IEC 60870–5–101 забезпечує надійний зв’язок для старих мереж. IEC 104 — ідеальне рішення для IP-мереж із сучасною інфраструктурою. DNP3 виділяється своєю надійністю, гнучкістю і буферизацією, роблячи його найкращим вибором для розподілених систем. Modbus, хоча й простий, залишається актуальним завдяки простоті й відкритості, особливо в пристроях польового рівня. Вибір протоколу залежить від вимог до надійності, швидкості, гнучкості та масштабованості системи.

3.3. Стандарт IEC 61850 та цифрова підстанція

У сучасних електроенергетичних системах дедалі більшого значення набуває впровадження цифрових технологій, що забезпечують вищу ефективність, керованість і надійність енергетичної інфраструктури. Одним із ключових

елементів цього процесу є цифрові підстанції, які функціонують на основі протоколу IEC 61850 — міжнародного стандарту для автоматизації електричних підстанцій.

Цей стандарт забезпечує уніфіковану платформу для обміну даними між пристроями релейного захисту, автоматики, вимірювального обладнання та SCADA-системами. Він встановлює моделі даних, механізми передачі, формати повідомлень та інші засади, необхідні для ефективної взаємодії пристроїв різних виробників у межах однієї енергетичної системи.

Головна мета стандарту IEC 61850 полягає у забезпеченні інтероперабельності між різними інтелектуальними електронними пристроями (IED), спрощенні їх інтеграції, пришвидшенні процесів налаштування та обслуговування систем автоматизації підстанцій. Це досягається за допомогою:

– єдиної моделі даних;
– уніфікованого формату опису системи — SCL;
– високошвидкісної передачі повідомлень GOOSE, SV;
– відкритої платформи для розширення та інтеграції.

Цифрова підстанція відповідно до концепції IEC 61850 складається з трьох основних функціональних рівнів (рис. 3.1 – 3.2):

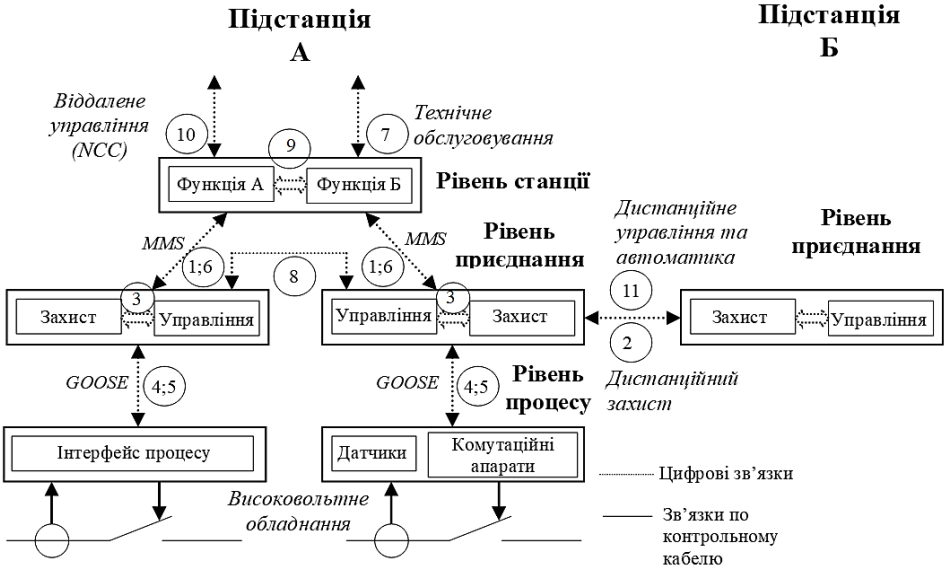

Рисунок 3.1 – Архітектура системи зв'язку між двома цифровими підстанціями

1) Рівень процесу (Process Level). Це найнижчий рівень, де розташовані вимірювальні трансформатори струму (CT), трансформатори напруги (VT), пристрої збору зразків (Merging Units), виконавчі механізми та сенсори. Дані з процесуального рівня оцифровуються та передаються далі.

2) Рівень приєднань (Bay Level). Тут розміщуються інтелектуальні електронні пристрої (IED), які реалізують функції релейного захисту, автоматики, вимірювання та управління. Саме тут GOOSE і Sampled Values активно використовуються для міжпристроєвої комунікації.

3) Рівень станції (Station Level). Цей рівень включає станційний сервер, HMI, SCADA-сервер та засоби управління підстанцією. Він забезпечує оператору доступ до інформації, отриманої з байєсного рівня.

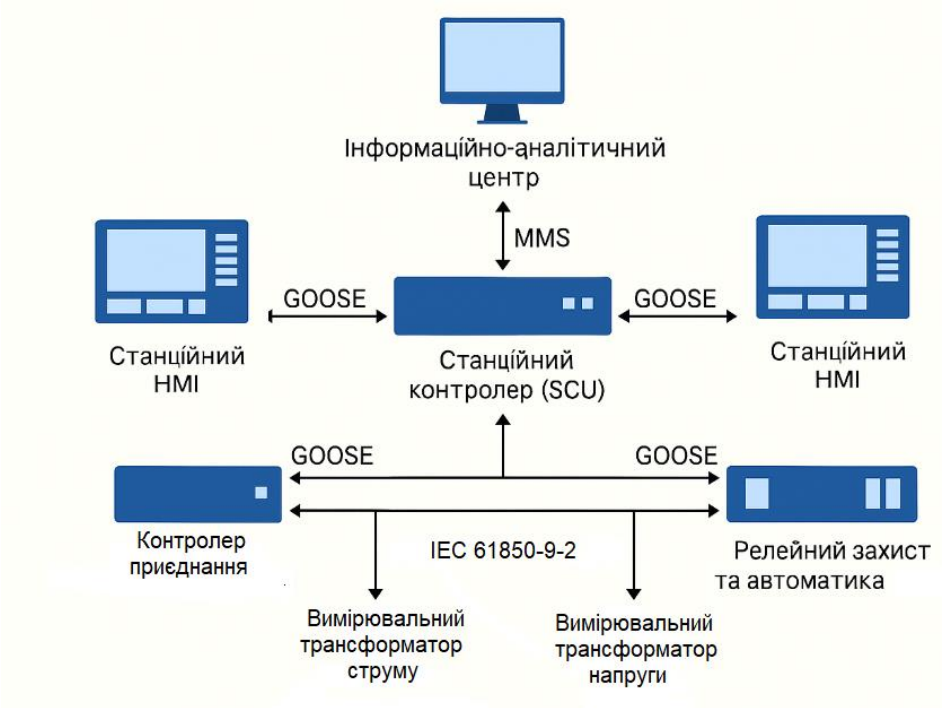

Рисунок 3.2 – Схема взаємодії пристроїв за протоколом IEC 61850

Комунікації між цими рівнями здійснюються через Ethernet-мережу із використанням сервісів MMS, GOOSE, SV згідно з IEC 61850.

Модель даних у стандарті IEC 61850 побудована на основі ієрархії:

– Physical Device (PD): реальний пристрій;

– Logical Device (LD): логічне представлення функціонального блоку в межах PD;

– Logical Node (LN): базовий функціональний елемент, наприклад захист, автоматика або вимикач;

– Data Object (DO): структурований набір атрибутів, які описують фізичний стан або змінні;

– Data Attribute (DA): конкретна величина або стан (наприклад, статус ввімкнення).

Приклад логічного вузла: XCBR (Breaker Control) – керування вимикачем. Має DO: Pos (позиція), OpCnt (лічильник операцій), Health (стан пристрою) тощо.

Для опису конфігурації всієї підстанції використовується SCL — XML-подібна мова, що описує:

– розташування пристроїв;

– мережеві з’єднання;

– структуру моделей;

– маршрути обміну повідомленнями GOOSE та SV.

Це забезпечує стандартизоване планування, моделювання, конфігурацію та інтеграцію систем.

IEC 61850 підтримує чотири основні типи комунікаційних сервісів:

1) MMS (Manufacturing Message Specification). Протокол прикладного рівня, що забезпечує:

– зчитування/запис даних;

– керування командами;

– логування подій;

– управління файлами (конфігурація, архіви).

2) GOOSE. Передача подій між пристроями з мінімальною затримкою (до 3 мс), застосовується для реалізації функцій релейного захисту та сигналізації. Передає стани та команди без участі серверів;

3) SV. Передача оцифрованих аналогових вимірювань (струм, напруга) у вигляді пакунків Ethernet. Це дозволяє обійтися без аналогових проводів;

4) Web Services (у нових редакціях). Додаткові засоби для інтеграції з хмарними сервісами, SCADA та іншими системами управління в контексті Smart Grid.

Мережі для IEC 61850 мають відповідати низці вимог:

– Gigabit Ethernet або Fast Ethernet;

– підтримка VLAN та приоритезації (IEEE 802.1Q та 802.1p);

– Redundancy protocols: PRP, HSR для безперервності передачі;

– Точна синхронізація часу (PTP/IEEE 1588) для Sampled Values.

IEC 61850 має механізми взаємодії з іншими протоколами:

– IEC 60870–5–104 – через шлюзи;

– DNP3 – через перетворення моделей;

– Modbus – інтеграція з неінтелектуальними пристроями;

– IEC 62351 – забезпечення кібербезпеки.

До переваг стандарту IEC 61850 можна віднести:

– масштабованість. Можливість розширення систем без зміни загальної архітектури;

– інтероперабельність. Спрощення інтеграції пристроїв різних виробників;

– зменшення кабельних витрат. Передача по Ethernet, а не аналоговими проводами;

– швидка реакція. Критичні команди передаються за 2–4 мс;

– автоматизоване конфігурування. За допомогою SCL.

Недоліки та виклики:

– високі вимоги до IT-кваліфікації персоналу;

– складність налаштування. Конфігурація SCL вимагає досвіду;

– кібербезпека. Необхідність впровадження механізмів шифрування та автентифікації;

– висока початкова вартість впровадження.

Приклади реалізації протоколу IEC 61850:

а) Digital Substation Siemens (Німеччина). Застосування IEC 61850 для повної інтеграції IED, PRP-мережі, GOOSE, SV;

б) GE Digital Energy (США). Комплексні рішення з використанням MMS, підтримки SCL, повної інтеграції в SCADA;

в) Укренерго (Україна). Пілотні проєкти з цифровізації підстанцій у рамках переходу до Smart Grid.

Перспективи розвитку використання протоколу IEC 61850:

– розширення на інші сфери — Smart Grid, DER (розподілені джерела), енергозберігаючі будівлі;

– впровадження кіберзахисту згідно з IEC 62351;

– поява профілів для нових протоколів (Web Services, REST, MQTT).

Стандарт IEC 61850 відіграє ключову роль у цифровій трансформації енергетичної галузі. Його гнучка модель даних, підтримка високошвидкісних сервісів, здатність до масштабування та інтеграції робить його незамінним інструментом для створення надійних та ефективних цифрових підстанцій. Успішне впровадження IEC 61850 сприяє зменшенню експлуатаційних витрат, покращенню обслуговування та підвищенню рівня автоматизації в умовах динамічної модернізації електроенергетичних систем.

3.4. Інтероперабельність і конвергенція протоколів

У сучасних енергетичних системах, де взаємодіють безліч пристроїв програмного забезпечення та комунікаційних платформ, забезпечення надійної взаємодії між ними є критично важливим. Поняття інтероперабельності та конвергенції протоколів стали ключовими в умовах швидкої цифровізації енергетики, що передбачає інтеграцію інформаційних та операційних технологій, забезпечення гнучкого реагування на зміну попиту, розподілену генерацію, автоматизоване керування тощо.

Інтероперабельність означає здатність різних систем, технологій і протоколів ефективно працювати разом без необхідності радикальних змін в їхній

архітектурі. Конвергенція протоколів — це процес уніфікації та інтеграції різних протоколів у спільну інформаційну інфраструктуру. Разом ці два поняття дозволяють створювати надійні, масштабовані та ефективні системи передачі та обробки енергетичних даних.

Інтероперабельність охоплює кілька рівнів взаємодії, кожен з яких має свої особливості та виклики:

а) фізичний рівень — забезпечує сумісність обладнання на рівні інтерфейсів. Наприклад, використання стандартних мережевих інтерфейсів Ethernet, RS-232 або RS-485;

б) комунікаційний рівень — гарантує, що пристрої можуть передавати дані однаковим способом. Сюди входять протоколи зв'язку, які регламентують структуру, синхронізацію та логіку обміну (наприклад, TCP/IP, UDP, IEC 60870–5–104) [26];

в) синтаксичний рівень — забезпечує узгодженість форматів даних, які передаються. Це стосується, зокрема, кодування, ідентифікації змінних, структури повідомлень;

г) семантичний рівень — надає значення переданим даним. Це важливо для того, щоб дві сторони не просто обмінювалися символами, а розуміли, про що йде мова. Наприклад, повідомлення про аварію має бути однаково зрозумілим для обох систем;

д) прикладний рівень — дозволяє системам виконувати узгоджені функції на основі обміну даними. Це стосується взаємодії SCADA з релейним захистом, автоматизованими вимикачами, датчиками тощо.

Конвергенція протоколів у сфері енергетики передбачає поєднання різноманітних мережевих технологій у єдину інформаційну екосистему. У більшості випадків, це зведення до IP-базованої платформи, де працюють різні протоколи — Modbus TCP, IEC 61850, DNP3, OPC UA тощо (рис. 3.3) [26].

Переваги конвергенції:

– зниження вартості експлуатації мереж;

– зменшення кількості обладнання;

– централізація моніторингу та керування;

– підвищення масштабованості та гнучкості системи;

– уніфікація каналів зв’язку та зменшення кількості дублюючих протоколів.

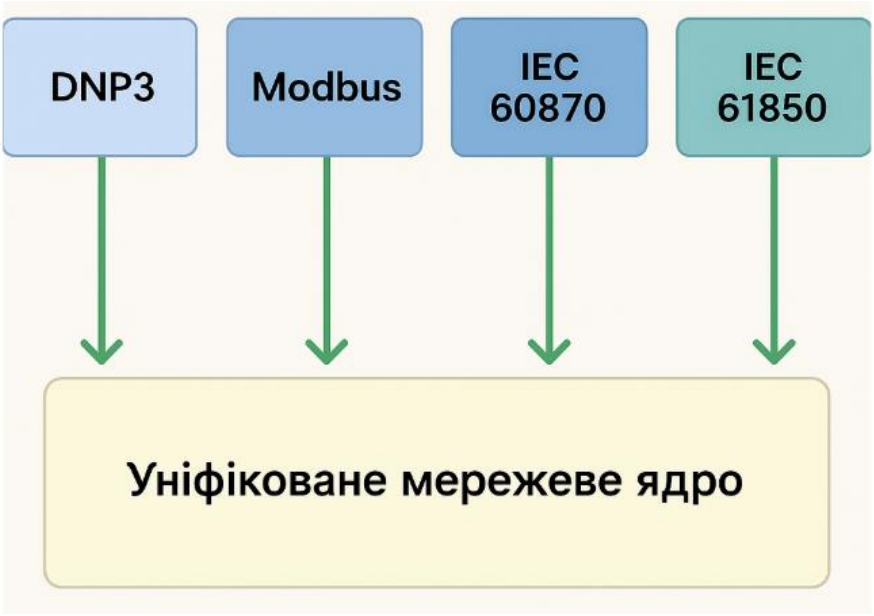

Рисунок 3.3 – Конвергенція протоколів

В електроенергетиці інтероперабельність застосовується:

1) на цифровій підстанції — платформа, де використовуються пристрої різних виробників, що підтримують стандарт IEC 61850. Завдяки цьому, IED можуть обмінюватися повідомленнями GOOSE, MMS, а також синхронізовано працювати через SV;

2) на шлюзах між протоколами — у багатьох випадках дані, зібрані з допомогою Modbus RTU, передаються до диспетчерського пункту через протокол IEC 60870–5–104. Тут використовуються спеціальні шлюзи–конвертори, які дозволяють зберегти єдину логіку управління;

3) на SCADA-системах нового покоління — підтримують багатопротокольний обмін, що дозволяє інтегрувати старі системи з новими технологіями, поступово модернізуючи інфраструктуру без повної її заміни.

Рисунок 3.4 – Ключові компоненти інтероперабельності цифрових систем

До засобів забезпечення інтероперабельності можна віднести:

– стандартизовані моделі об'єктів. В IEC 61850 всі пристрої представлені у вигляді логічних вузлів (LN), кожен з яких відповідає за певну функцію (захист, вимірювання, керування).

– описові мови (SCL). Дозволяють описати конфігурацію підстанції незалежно від виробника, що значно спрощує інтеграцію.

– протокол OPC UA. Служить універсальним інтерфейсом для передачі даних між різними системами. Підтримує сучасні вимоги до безпеки, масштабованості та семантичної інтеграції.

– профілі стандартів. Наприклад, профілі IEC 61850 Edition 2 деталізують реалізацію стандарту і підвищують сумісність між продуктами [26].

До викликів з якими стикається конвергенція протоколів можна віднести:

а) несумісність реалізацій одного і того ж протоколу — наприклад, різні інтерпретації GOOSE-повідомлень від різних виробників можуть мати відмінності в таймінгах, структурі повідомлень.

б) відсутність зворотної сумісності. Нові версії протоколів не завжди підтримують старі пристрої, що ускладнює модернізацію;

в) складність налаштування шлюзів. Протокол-конвертори вимагають складної конфігурації та тестування;

г) проблеми масштабування. Зі збільшенням кількості пристроїв зростають вимоги до обчислювальної потужності систем управління;

д) кібербезпека. Деякі протоколи, особливо старі (як Modbus), не мають вбудованих механізмів шифрування або автентифікації.

Роль міжнародних організацій. IEC — формує основні стандарти (IEC 61850, 60870, 61970, 61968 тощо). IEEE — пропонує специфікації для інтероперабельності в Smart Grid (наприклад, IEEE 2030). NIST — створює рамкові документи для побудови інтероперабельної енергетичної інфраструктури. OPC Foundation — розвиває універсальні протоколи взаємодії, які можуть інтегрувати промислові, енергетичні та IT-рішення.

До перспектив розвитку інтерперабельності можна віднести:

а) поглиблення семантичної уніфікації. Впровадження CIM для опису об’єктів та процесів в енергосистемах;

б) розвиток платформи OPC UA FX. Як наступний кроку у забезпеченні промислової та енергетичної конвергенції;

в) штучний інтелект та машинне навчання. Автоматична адаптація шлюзів і оптимізація протоколів обміну;

г) інтеграція енергетики з іншими галузями. У майбутньому, протоколи Smart Grid мають взаємодіяти з транспортом (електромобілі), промисловістю (Industry 4.0), житловим сектором (розумні будинки).

Інтероперабельність і конвергенція протоколів є наріжними каменями побудови сучасної, ефективної, безпечної та масштабованої енергетичної

інфраструктури. Забезпечення можливості взаємодії між різними системами та платформами дозволяє зменшити витрати, покращити надійність обміну даними та створити єдину інформаційну екосистему. Технічні рішення на основі відкритих стандартів, підтримка міжнародних ініціатив та постійне вдосконалення інструментів конфігурації — ключ до стійкого розвитку цифрової енергетики.

3.5. Приклади побудови систем з використанням протоколів

Сучасна енергетична інфраструктура функціонує на основі комплексних автоматизованих систем, де обмін інформацією між пристроями відбувається за допомогою різноманітних протоколів зв'язку. Для забезпечення надійності, масштабованості та безпеки інформаційного середовища в енергетиці, критично важливою є правильна побудова архітектури системи, відповідний вибір протоколів, врахування особливостей застосування кожного з них.

Цей підрозділ присвячено розгляду конкретних прикладів реалізації систем передачі даних у енергетиці з використанням широко визнаних промислових протоколів — Modbus, DNP3, IEC 60870–5–104 та IEC 61850. Кожен із них має свої переваги, призначення, обмеження і використовується залежно від завдань, які вирішуються в межах об'єкта.

Система автоматизованого контролю енергоспоживання на базі Modbus TCP/IP.

Сфера застосування:

– облік споживання електроенергії в промислових підприємствах;

– контроль навантаження;

– управління розподільними щитами.

Опис реалізації:

У даній системі контролери типу PLC (програмовані логічні контролери), цифрові лічильники електроенергії та сенсори струму підключаються до єдиної Ethernet-мережі. Кожен пристрій підтримує протокол Modbus TCP/IP (рис. 3.5).

Періодично головний контролер або SCADA-сервер здійснює опитування всіх пристроїв через Modbus-запити, зчитуючи значення регістрів. Дані

відображаються в реальному часі на HMI або SCADA, а також зберігаються в архів для аналізу споживання енергії.

Переваги рішення:

– простота реалізації;

– висока сумісність з обладнанням різних виробників;

– відкрита специфікація протоколу.

Недоліки:

– відсутність вбудованих механізмів безпеки;

– обмежені можливості з точки зору часової синхронізації;

– не підходить для критично важливих систем.

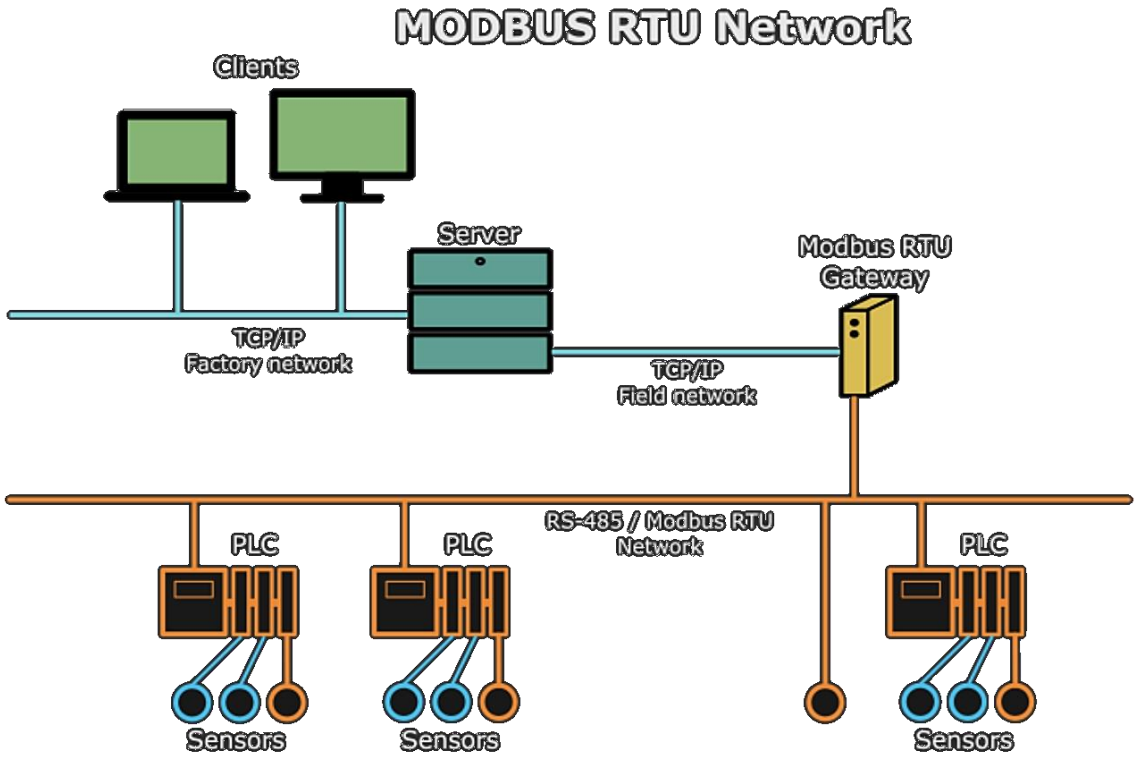

Рисунок 3.5 – Система автоматизованого контролю енергоспоживання на базі Modbus TCP/IP

Побудова системи телемеханіки із використанням IEC 60870–5–104 (через Ethernet). На базовому рівні встановлено RTU — пристрої збору та передачі інформації. До них підключені сигнали стану, вимірювальні трансформатори, лічильники та пристрої керування (рис. 3.6).

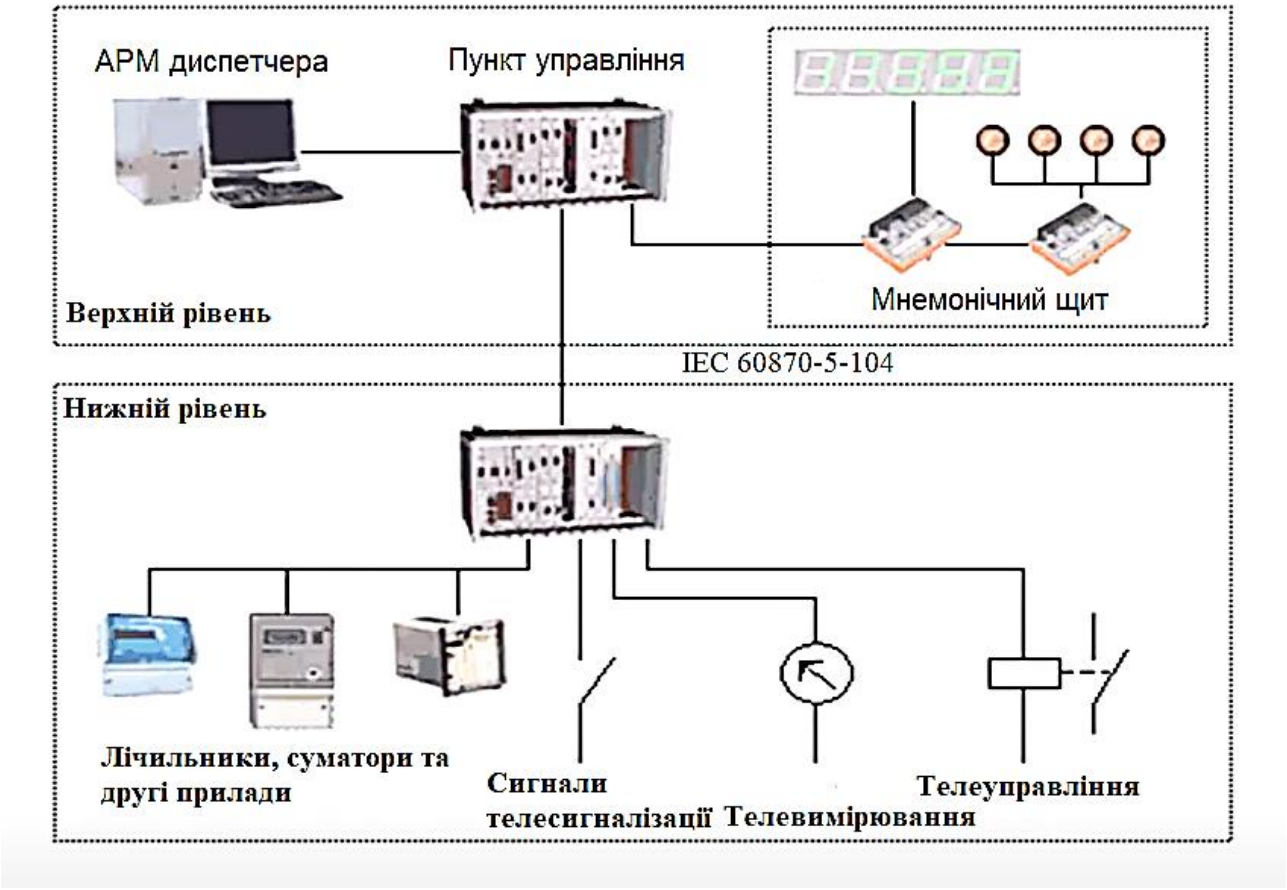

Рисунок 3.6 – Побудова системи телемеханіки із використанням IEC 60870–5–104 (через Ethernet)

RTU–комунікують з центром управління SCADA через IP–мережу, використовуючи протокол IEC 60870–5–104. Передача включає як спонтанні повідомлення про зміну стану, так і періодичні опитування.

Сфера застосування:

– передача інформації з підстанцій на диспетчерські центри;

– контроль стану обладнання енергосистем.

Переваги рішення:

– підтримка асинхронної передачі;

– можливість пріоритезації сигналів;

– сумісність з енергетичними диспетчерськими системами.

Недоліки:

– обмежена підтримка розширених функцій безпеки;

– обмежена масштабованість порівняно з IEC 61850.

Енергетична підстанція з використанням IEC 60870–5–104. Підстанція 110/35/10 кВ має кілька RTU, які збирають дані з реле, трансформаторів струму і напруги, вимірювальних приладів. Передача інформації до диспетчерського центру реалізується по протоколу IEC 60870–5–104 через VPN-канал на базі GPRS/3G (рис. 3.7).

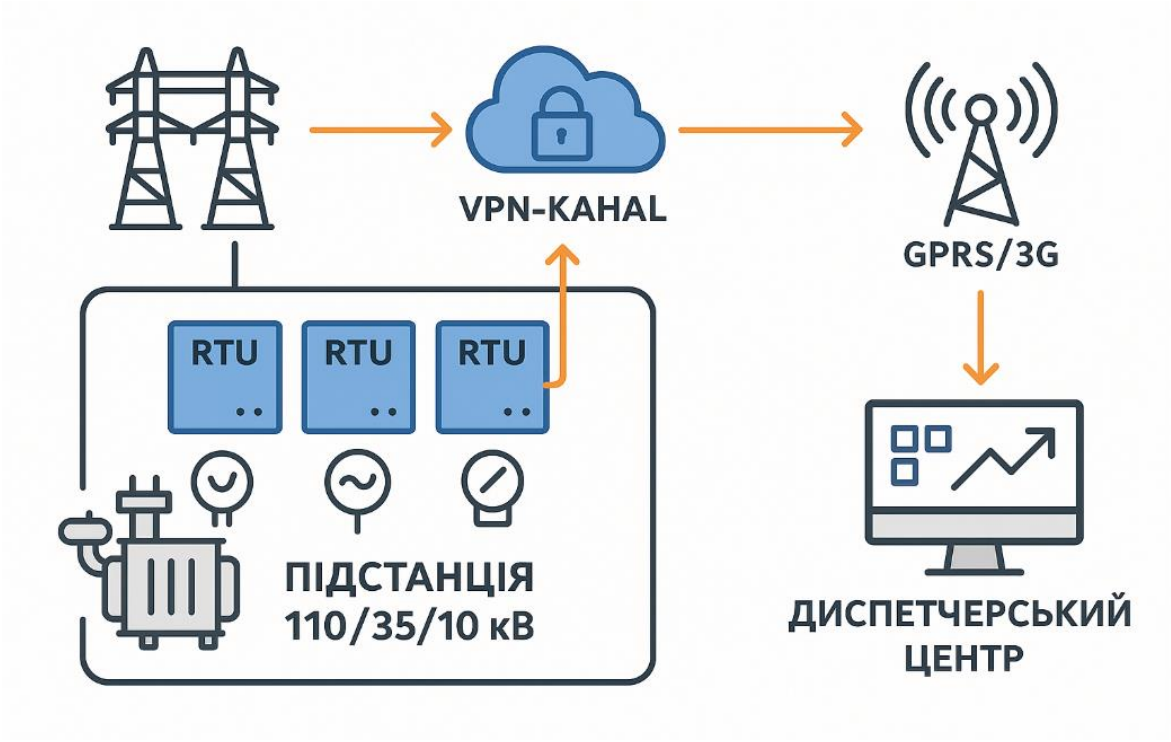

Рисунок 3.7 – Підстанція з використанням IEC 60870–5–104

Функціональність:

– сигнали аварій та попереджень;
– значення струму, напруги, потужності;
– стан комутаційного обладнання;
– команди керування (наприклад, увімкнення/вимкнення вимикачів).

Архітектура:

– SCADA в центрі управління виконує періодичне опитування RTU;
– RTU передають також спонтанні повідомлення при зміні стану;
– забезпечується двосторонній зв’язок для дистанційного керування.

Інтеграція з іншими протоколами:

– через протокольні шлюзи можливий обмін даними з Modbus та DNP3-пристроями;

– дані зберігаються у централізованій базі для аналізу аварій.

Автоматизована система управління енергією з DNP3 (рис. 3.8). Протокол DNP3 має розширені можливості порівняно з Modbus і часто використовується в розподілених системах, де важлива точність даних та їх синхронізація в часі.

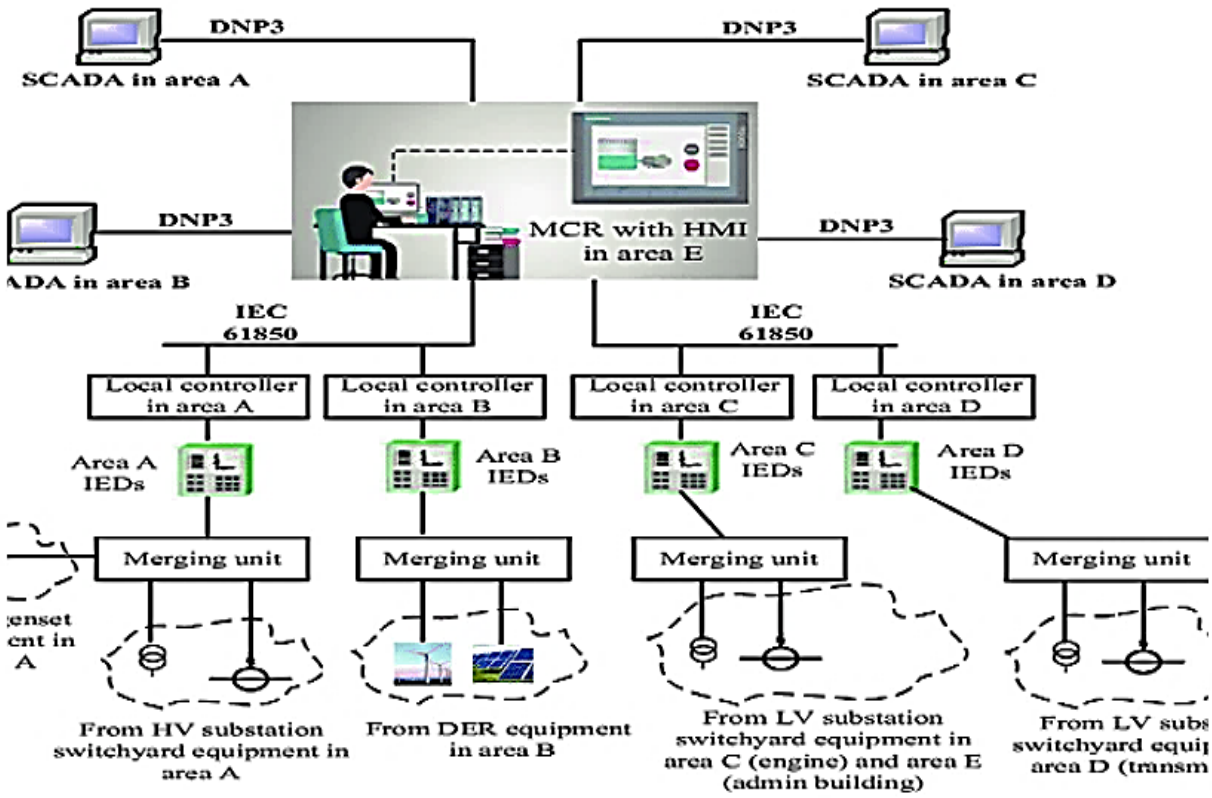

Рисунок 3.8 – Автоматизована система управління енергією з DNP3

На базі розподіленої сонячної електростанції (рис. 3.9) реалізовано систему управління станом сонячних інверторів, моніторинг погодних умов та контроль точок підключення до мережі. Кожна точка обладнана контролером з підтримкою DNP3, що комунікує з головним сервером SCADA через мобільний інтернет із захищеним VPN-з’єднанням.

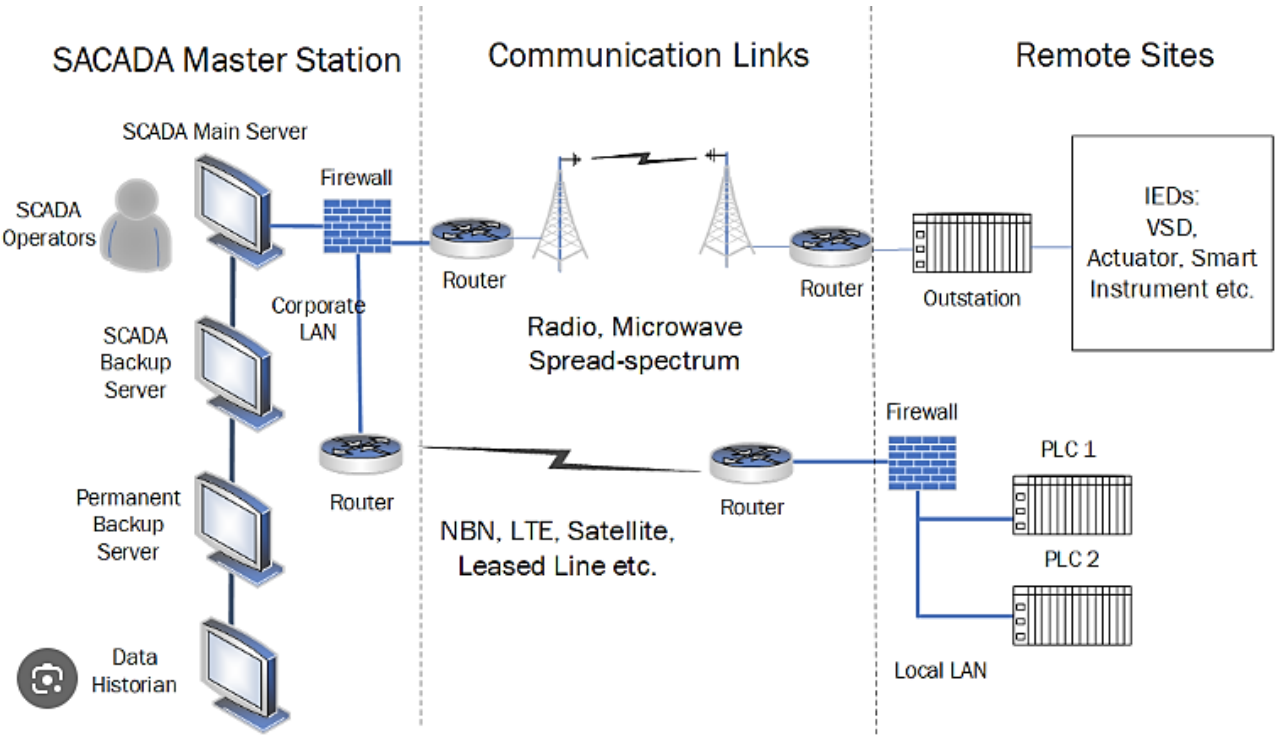

Рисунок 3.9 – Приклад використання DNP3 SCADA

Функціональні можливості:

– збір даних про поточну генерацію;

– контроль температури панелей та інверторів;

– отримання інформації з датчиків вологості, освітлення, швидкості вітру;

– управління станом реле навантаження.

Переваги:

– вбудовані часові мітки подій;

– буферизація даних при розриві зв’язку;

– надійна передача по нестабільних каналах.

Архітектура:

– SCADA-сервер — головний контролер (Master);

– польові пристрої — підлеглі (Slave);

– передача даних у форматі DNP3 із використанням TLS-шифрування.

Цифрова підстанція з IEC 61850. Це найсучасніший стандарт, який реалізує повністю цифрову взаємодію між пристроями у підстанції без фізичного підключення вхідних/вихідних сигналів (рис. 3.10).

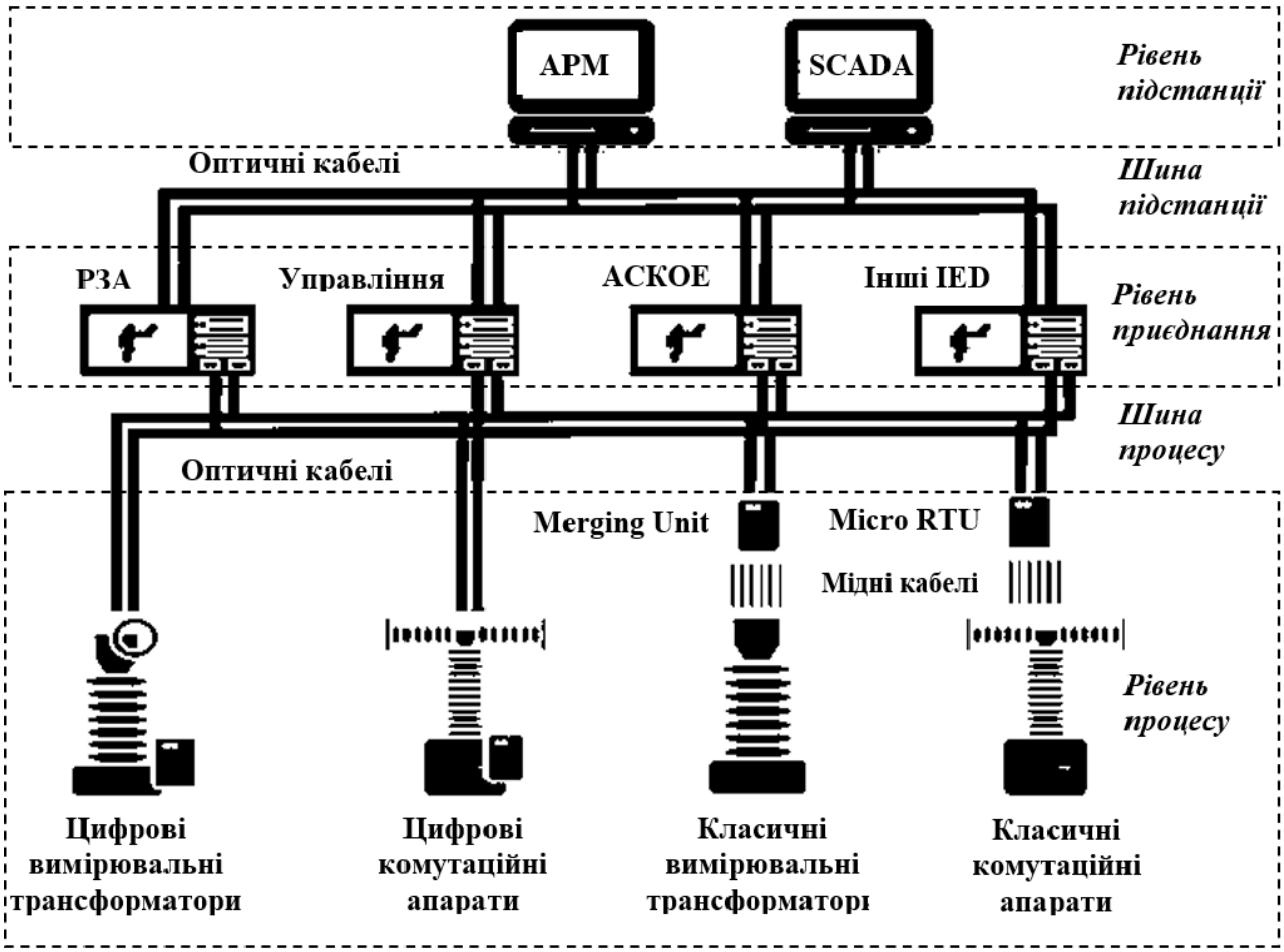

Рисунок 3.10 – Цифрова підстанція з IEC 61850

На підстанції впроваджено повноцінну систему на базі IEC 61850:

– IED пристрої (інтелектуальні електронні пристрої) здійснюють вимірювання, захист, автоматику;

– Дані між пристроями передаються у вигляді GOOSE-повідомлень та Sampled Values;

– Комунікація відбувається через оптоволоконну мережу з використанням Ethernet–комутаторів, що підтримують IEEE 1588 (PTP).

Переваги:

– швидкодія (реакція на подію <4 мс);

– повна відмова від дротового з’єднання між реле;

– висока надійність через дублювання та резервування.

Додаткові елементи:

– SCL-файли для конфігурації всієї підстанції;

– MMS-протокол для взаємодії SCADA з IED;

– синхронізація часу за допомогою PTP.

Система керування мікромережею (Microgrid). У контексті зростання популярності мікромереж (microgrid), особливо в критично важливих об'єктах (аеропорти, лікарні), забезпечення безперебійної роботи передбачає інтеграцію кількох типів джерел енергії: мережа, дизель-генератори, акумулятори, сонячні станції (рис. 3.11).

Реалізація:

– сонячні інвертори спілкуються через Modbus TCP;

– акумулятори — через CAN-шину з конвертацією в Modbus RTU;

– генератори — через DNP3;

– центральний контролер керує всією мікромережею, розподіляючи навантаження;

– комунікація з мережею — через IEC 104.

Цей приклад показує важливість інтероперабельності протоколів та гнучкості програмного забезпечення.

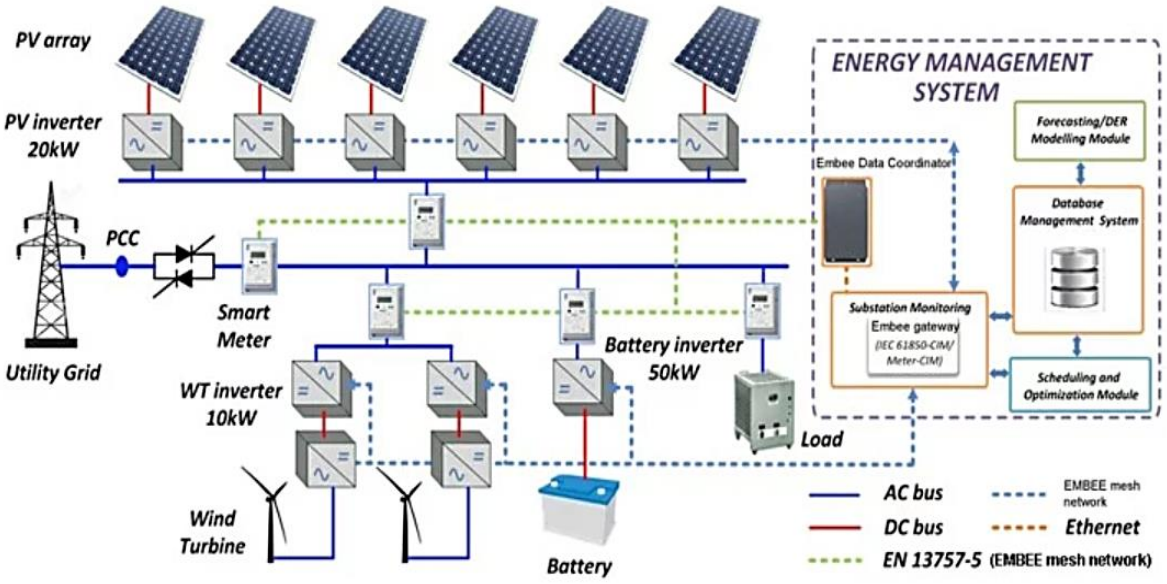

Рисунок 3.11 – Класична мікромережа

На (рис. 3.11) показана класична мікромережа. Потужність Microgrid становить 10 кВт і включає 1 х 3 кВт, 1 х 2 кВт фотоелектричні станції, сонячну станцію 0,3 кВт, двигун Стірлінга з водяним тепловим резервуаром та 5 кВт накопичувач. Платформа Embee IoT дозволяє контролювати Teslacamp Microgrid у реальному часі. Баланс між генерацією та споживанням становив 2–3 % втрат.

У контексті зростаючого попиту на енергонезалежні рішення та підвищення енергоефективності, сонячні електростанції розглядаються як базовий етап у впровадженні автономних енергетичних систем. Однак, за умови роботи виключно на власне споживання, середній коефіцієнт корисного використання електроенергії (ККД) таких установок зазвичай не перевищує 10 %. Це обумовлює необхідність переходу до більш комплексних енергетичних рішень.

Одним із перспективних напрямів є створення розумної мікромережі — децентралізованої енергосистеми, що забезпечує інтеграцію різних джерел генерації, накопичувачів енергії та систем автоматизованого управління. Поетапне впровадження такої інфраструктури дозволяє досягати рівня ефективності енергоспоживання до 55 %, що значно перевищує показники традиційної автономної генерації.

Початковим етапом побудови мікромережі є впровадження систем моніторингу енергоспоживання. Збір та аналітична обробка даних щодо навантажень і споживання електроенергії дає змогу ідентифікувати критичні точки втрат, оптимізувати використання наявних ресурсів та обґрунтувати подальші інвестиційні рішення. Надалі система може бути масштабована шляхом інтеграції додаткових джерел генерації та елементів накопичення, що сприяє підвищенню загальної стабільності та економічної доцільності енергопостачання.

Таким чином, перехід від простої сонячної генерації до комплексної мікромережі є стратегічно обґрунтованим рішенням, яке забезпечує вищий рівень енергоефективності, гнучкості та енергетичної безпеки. Приклад такої мережі показаний на (рис. 3.12).

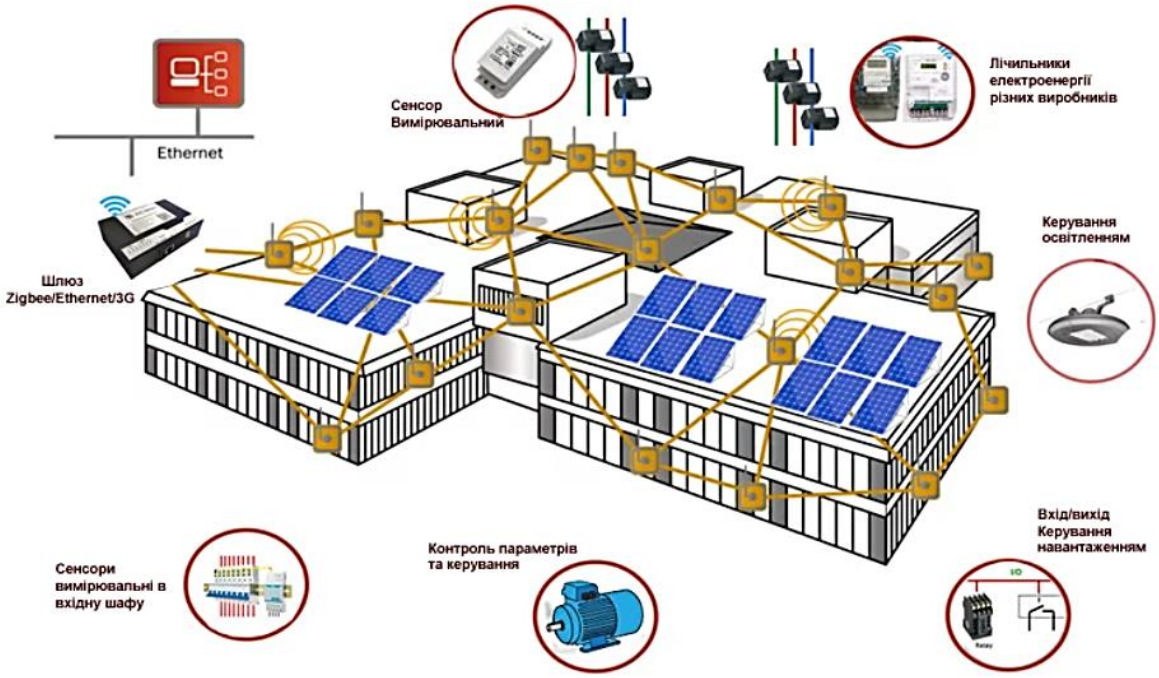

Рисунок 3.12 – Мікромережа будівлі

Побудова систем у сучасній енергетиці потребує не тільки знання конкретного протоколу, а й розуміння загальної архітектури, можливостей конвергенції, масштабованості та майбутнього розвитку. Навіть у рамках одного об’єкта, як ми побачили, можуть використовуватися різні протоколи для різних завдань. Важливим фактором успішної реалізації є правильне проєктування шлюзів, управління часом (синхронізація), врахування кібербезпеки та підтримка стандартів.

Висновки до розділу 3

У третьому розділі навчального посібника було комплексно висвітлено ключову роль протоколів та стандартів у процесах передачі даних в електроенергетичних системах. Систематичний огляд архітектур, підходів та конкретних реалізацій дав змогу сформувати практичне уявлення про те, як цифрова взаємодія пристроїв стає основою ефективного, безпечного і стабільного функціонування сучасної енергетичної інфраструктури.

Розглянуто загальну роль протоколів у забезпеченні уніфікованої взаємодії між пристроями та системами. Було наголошено на важливості відповідності сучасним вимогам енергетики: реальному часу, надійності, безпеці та масштабованості. Через огляд класифікацій за моделлю OSI, призначенням та типами передачі закладено основи для подальшого розуміння специфіки галузевих протоколів. Вивчення основних функцій передачі — кадрування, адресації, синхронізації, управління потоком, шифрування — дозволяє оцінити складність і глибину організації енергетичних мереж зв'язку.

Було приділено увагу характеристикам і порівнянню базових протоколів, таких як IEC 60870–5–101/104, DNP3 та Modbus. Вони широко застосовуються в автоматизованих системах телемеханіки, SCADA, контролю та обліку. Описано переваги кожного з них у відповідних умовах: надійність при нестабільному зв'язку, підтримка часових міток, простота інтеграції, гнучкість або масштабованість. Сформовано практичне уявлення про відповідність протоколів до задач систем диспетчеризації, збору даних, релейного захисту або польового рівня керування.

Особливу увагу було приділено стандарту IEC 61850 як основі для побудови цифрової підстанції. Описана структурна модель взаємодії пристроїв на різних рівнях — процесуальному, байєсному, станційному — дозволяє сформувати системне бачення побудови сучасної підстанції. Ієрархічна модель даних, логічні вузли, мовні засоби конфігурації (SCL), сервіси обміну (GOOSE, SV, MMS) демонструють потенціал стандарту для уніфікації, автоматизації та прискорення розгортання нових рішень в енергетиці. Висвітлено також вимоги до інфраструктури мережі, синхронізації, безпеки та механізмів взаємодії з іншими протоколами.

У підрозділі, що розглядав питання інтероперабельності та конвергенції, проаналізовано підходи до поєднання різних протоколів в одній інфраструктурі. Було наголошено на важливості забезпечення взаємодії на фізичному, комунікаційному, синтаксичному, семантичному та прикладному рівнях. Підкреслено значення шлюзів, описових мов, об'єктно-орієнтованих моделей і відкритих

протоколів для підтримки гетерогенних систем. Питання уніфікації, масштабування, модернізації та кібербезпеки проілюстровано прикладами застосування в реальних інфраструктурах. Було також окреслено глобальні тенденції, включно з переходом до платформ OPC UA, використанням профілів стандартів та роллю міжнародних організацій у підтримці сумісності рішень.

Розглянуто приклади практичного впровадження систем із використанням згаданих протоколів. Було подано опис реальних архітектур з урахуванням різних технічних і функціональних вимог — від простих рішень на Modbus TCP до високонадійних систем із IEC 61850. Продемонстровано можливості комбінування протоколів у рамках мікромереж, телемеханічних систем, цифрових підстанцій і автономних енергетичних об'єктів. Це дозволяє зрозуміти, як на практиці реалізується інтеграція, як досягається гнучкість, і які виклики виникають на шляху до цифрової трансформації енергетики.

Таким чином, третій розділ навчального посібника формує не лише теоретичну основу, а й практичне бачення сучасної архітектури інформаційного обміну в енергетиці. Розуміння стандартів і протоколів дозволяє ефективно проєктувати, інтегрувати та модернізувати енергетичні системи з урахуванням вимог часу, технічного прогресу та міжсистемної сумісності.

Запитання для контролю знань за третім розділом

1. Яку роль відіграють протоколи у забезпеченні взаємодії між пристроями в енергетичних системах?
2. Чому важливо, щоб протоколи відповідали вимогам реального часу, безпеки та масштабованості?
3. Які основні функції передачі реалізуються в протоколах електроенергетики?
4. Чим відрізняються протоколи IEC 60870–5–101 та IEC 60870–5–104?
5. Які переваги має DNP3 у нестабільних умовах зв'язку?
6. У чому полягає простота та ефективність протоколу Modbus?

7. Які завдання вирішуються за допомогою кожного з базових протоколів у SCADA-системах?

8. Яку архітектуру взаємодії пристроїв описує стандарт IEC 61850?

9. Що таке логічні вузли та які їх функції в IEC 61850?

10. Які типи повідомлень використовуються у стандарті IEC 61850?

11. Чому конфігураційна мова SCL є важливою для впровадження стандарту IEC 61850?

12. Які рівні взаємодії враховуються для забезпечення інтероперабельності між різними протоколами?

13. Яку роль відіграють шлюзи та описові мови у поєднанні протоколів?

14. Чим відрізняються синтаксичний та семантичний рівні взаємодії?

15. Які приклади реальних архітектур з комбінуванням протоколів були розглянуті в розділі?

16. Як використовується OPC UA для забезпечення гнучкості та масштабування систем?

17. Які виклики виникають при інтеграції протоколів у мікромережах і цифрових підстанціях?

18. Яке значення мають міжнародні організації у підтримці сумісності протоколів?

19. Як забезпечується безпека в системах, що використовують різні протоколи передачі даних?

20. Як третій розділ допомагає у формуванні практичної компетентності щодо проєктування сучасних енергетичних мереж?

4. АВТОМАТИЗОВАНІ СИСТЕМИ ДИСПЕТЧЕРСЬКОГО УПРАВЛІННЯ SCADA

4.1. Функціональне призначення та структура SCADA-систем

В сучасному світі автоматизація стала невід'ємною складовою енергетичних, промислових та інфраструктурних об'єктів. Важливою складовою автоматизованих систем керування є SCADA-системи — диспетчерські системи управління та збору даних, які забезпечують спостереження, збір, обробку, збереження та аналіз інформації у режимі реального часу, а також дають можливість дистанційного керування об'єктами.

Цей розділ присвячений вивченню призначення SCADA-систем, їх базової та розширеної архітектури, а також основним принципам роботи і взаємодії між компонентами системи.

SCADA-системи розроблені для централізованого контролю, моніторингу та управління технологічними процесами, які часто охоплюють великі території — наприклад, енергетичні мережі, системи водопостачання, транспортні мережі та нафтогазову галузь.

Основні функції SCADA-систем включають:

1) Моніторинг. SCADA дозволяє в режимі реального часу відслідковувати параметри об'єктів:

– напруга, струм, температура, тиск тощо;
– стан обладнання (вимикачі, клапани, насосні агрегати);
– аварійні чи передаварійні ситуації.

2) Керування. Оператор може дистанційно:

– вмикати/вимикати обладнання;
– змінювати режими роботи;
– запускати алгоритми автоматичного регулювання.

3) Архівація даних. Система зберігає дані про:

– вимірювальні параметри;
– події, тривоги;

– дії операторів;

– зміни конфігурації.

4) Аналіз та оптимізація. На основі даних SCADA здійснюється:

– оцінка ефективності роботи об’єкта;

– прогнозування навантаження чи споживання;

– оптимізація витрат;

– технічне обслуговування за станом.

5) Забезпечення безпеки. SCADA інтегрується з системами кіберзахисту та фізичної охорони, зокрема:

– контроль доступу;

– реєстрація входу/виходу користувачів;

– виявлення вторгнень.

Архітектура SCADA-систем. Сучасні SCADA-системи мають модульну, багаторівневу архітектуру рис 4.1, Основними рівнями архітектури є:

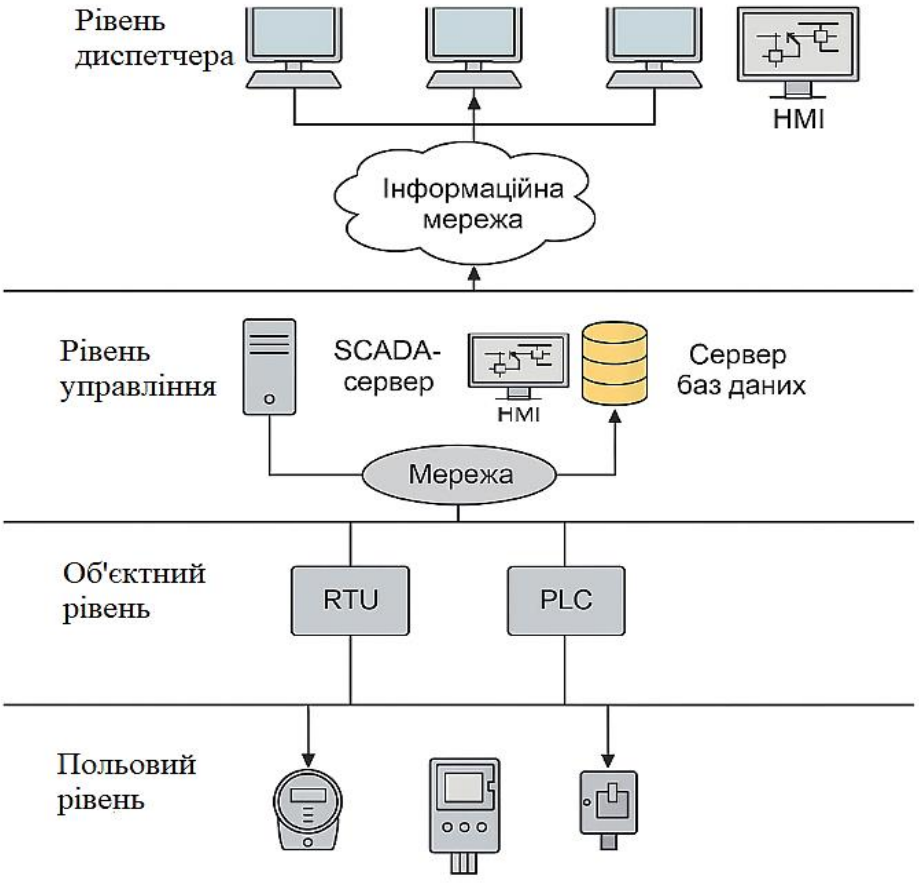

Рисунок 4.1 – Архітектура SCADA-систем

1) Польовий рівень (Field Level). Цей рівень включає сенсори, приводи, виконавчі механізми, лічильники, датчики та реле, які безпосередньо взаємодіють з фізичними об’єктами. Пристрої цього рівня зазвичай підключаються до локальних контролерів через протоколи:

– Modbus RTU/TCP;

– Profibus/Profinet;

– HART;

– IEC 61850 (у цифрових підстанціях);

– DNP3, IEC 60870–5–101/104.

2) Рівень контролерів (Control Level). На цьому рівні працюють:

– PLC;

– RTU;

– IED;

– PAC.

Контролери збирають дані з польових пристроїв, обробляють їх локально, а також передають у вищі рівні SCADA-системи. Вони також можуть виконувати алгоритми автоматичного регулювання.

3) Комунікаційний рівень. Цей рівень забезпечує обмін даними між польовими пристроями, контролерами та серверами. Він включає:

– промислові Ethernet-мережі;

– оптоволоконні канали;

– радіоканали, GSM/3G/4G/5G;

– захищені VPN-з’єднання;

– протоколи передачі даних: TCP/IP, UDP, MQTT, IEC 104, OPC UA, SNMP.

4) Серверний рівень (SCADA-сервер). Центральним елементом системи є SCADA-сервер, який виконує:

– збір та архівацію даних;

– обробку подій;

– керування логікою взаємодії;

– надання даних клієнтам;

– взаємодію з іншими IT-системами (ERP, CMMS, GIS).

Часто реалізується кластер серверів для забезпечення відмовостійкості та безперервної роботи (hot-standby або active-active моделі).

5) Рівень інтерфейсу користувача (HMI – людино машинний інтерфейс). Оператори взаємодіють із системою через людино-машинний інтерфейс:

– графічні мнемосхеми;

– табличні уявлення;

– тривожні повідомлення;

– звіти та графіки.

Можливий доступ через:

– локальні термінали;

– мобільні пристрої;

– веб-браузери (завдяки Web HMI).

Розглянемо приклад дворівневої системи (рис. 4.2), де безпосереднє керування технологічними процесами відбувається саме на цих рівнях. Особливості конкретної системи керування залежать від програмно-апаратної платформи, що застосовується на кожному з рівнів.

Нижній рівень, або рівень об’єкта (контролерний), включає різноманітні датчики (вимірювальні перетворювачі), які збирають дані про перебіг технологічного процесу, а також електроприводи і виконавчі механізми для виконання регулюючих і керуючих дій. Дані з датчиків надходять до програмованих логічних контролерів (PLC/ПЛК) або віддалених термінальних пристроїв (RTU), які здатні виконувати такі функції:

– збір, первинна обробка й зберігання інформації про стан устаткування й параметрах технологічного процесу;

– автоматичне логічне керування й регулювання;

– виконання команд із пункту керування;

– самодіагностика роботи програмного забезпечення й стану самого контролера;

– обмін інформацією з пунктами керування.

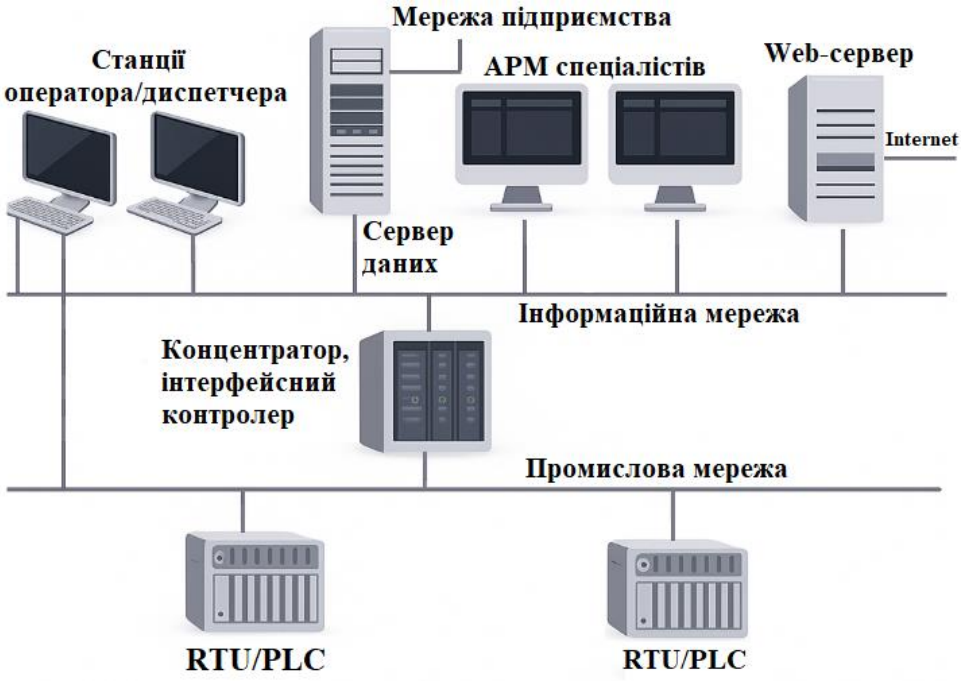

Рисунок 4.2 – Узагальнена структурна схема системи керування SCADA

Оскільки інформація в контролерах попередньо обробляється і частково використовується безпосередньо на місці, це значно знижує вимоги до пропускної здатності каналів зв’язку.

Дані з логічних контролерів можуть передаватися у мережу диспетчерського пункту як напряму, так і через контролери вищого рівня (рис. 4.2). Відповідно до конкретних завдань, контролери верхнього рівня — такі як концентратори або комунікаційні контролери — виконують різноманітні функції. Деякі з них наведені нижче:

– збір даних з логічних контролерів;
– обробка даних, включаючи масштабування;
– підтримка єдиного часу в системі;
– синхронізація роботи підсистем;
– організація архівів по обраних параметрах;
– обмін інформацією між логічними контролерами й верхнім рівнем;
– робота в автономному режимі при порушеннях зв’язку з верхнім рівнем;

– резервування каналів передачі даних і ін.

Верхній рівень — диспетчерський пункт (ДП) — включає одну або декілька станцій керування, які є автоматизованими робочими місцями (АРМ) диспетчера або оператора. На цьому рівні також може розташовуватися сервер бази даних. Крім того, тут можуть бути створені робочі місця для спеціалістів, зокрема для інженера з автоматизації.

Станції керування призначені для відображення поточного стану технологічного процесу та оперативного управління ним. Ці задачі виконує програмне забезпечення SCADA, яке розроблене для забезпечення інтерфейсу між диспетчером або оператором і системою керування, а також для організації взаємодії з зовнішніми системами.

Всі апаратні компоненти системи керування з'єднані каналами зв'язку. На нижньому рівні контролери взаємодіють із датчиками та виконавчими пристроями через фізичні лінії, а з блоками вилученого та розподіленого введення/виводу — через спеціалізовані мережі.

Зв'язок між контролерами нижнього рівня та контролерами верхнього рівня (концентраторами) часто здійснюється за допомогою радіо або телефонних каналів. При невеликих відстанях логічні контролери можуть бути з'єднані між собою та з верхнім рівнем через керуючі мережі на основі витої пари або оптоволокна.

Взаємозв'язок між робочими місцями оперативного персоналу та фахівців, контролерами верхнього рівня і вищими рівнями здійснюється за допомогою інформаційних мереж, найчастіше — на базі оптоволоконних технологій.

Залежно від обсягів об'єкта, географії, надійності та потреб безпеки застосовуються різні типи архітектур SCADA:

а) централізована SCADA

– один сервер, декілька операторських станцій;

– використовується на компактних об'єктах.

б) розподілена SCADA:

– декілька серверів і контрольних центрів;

– застосовується в енергетичних системах, транспорті, водоканалах.

в) гібридна SCADA:

– поєднання централізованого моніторингу з автономною роботою локальних вузлів;

– підвищена стійкість до збоїв та кіберзагроз.

г) хмарна SCADA:

– дані зберігаються та обробляються в хмарних серверах;

– переваги: масштабованість, доступність, зниження витрат на IT-інфраструктуру;

– недоліки: потреба в захищеному інтернет-з'єднанні.

Особливості побудови SCADA в енергетиці. У галузі енергетики SCADA має додаткові вимоги:

– підтримка спеціалізованих протоколів (IEC 61850, 104, DNP3);

– висока швидкодія та надійність;

– можливість реалізації схем резервування та «гарячого» дублювання;

– інтеграція з АСКОЕ, RPA, системами захисту.

В енергетиці SCADA використовується для:

– моніторингу стану мереж 35/110/220/330/750 кВ;

– диспетчеризації електропідстанцій;

– управління режимами навантаження;

– обміну даними між обласними та національними центрами диспетчеризації.

Безпека SCADA-систем. Системи SCADA є критично важливими об'єктами інфраструктури, тому питання кібербезпеки відіграє ключову роль. Основні заходи:

– сегментування мереж (використання DMZ);

– фаєрволи, IDS/IPS;

– автентифікація користувачів та управління доступом;

– шифрування протоколів (TLS, IPsec);

– аудит дій користувачів;

– резервне копіювання.

SCADA повинна відповідати стандартам:

– IEC 62443 — кібербезпека в автоматизації;

– NERC CIP — критична інфраструктура в енергетиці (США);

– ISO/IEC 27001 — інформаційна безпека.

Інтеграція з іншими системами. SCADA не є ізольованою — вона інтегрується з:

– ERP — обмін даними про виробництво та енергоспоживання;

– CMMS — для управління обслуговуванням;

– GIS — для візуалізації на картах;

– MES — на виробництві;

– EMS — в енергетиці.

Це досягається завдяки використанню відкритих стандартів і протоколів, таких як:

– OPC UA;

– REST API;

– MQTT.

SCADA-системи є ключовими у цифровізації енергетики та промисловості. Вони виконують критичні функції моніторингу, керування, архівації, безпеки та аналітики, дозволяючи підвищити ефективність, безпеку та прозорість роботи технологічних процесів.

Архітектура SCADA повинна враховувати потреби конкретного об’єкта: масштаб, кількість даних, географічну розподіленість, вимоги до надійності та безпеки. Водночас варто передбачати гнучкість для майбутньої модернізації та інтеграції з іншими цифровими платформами.

4.1.1. Організація SCADA-систем клієнт-серверної взаємодії

На початковому етапі розвитку мікропроцесорних систем керування у 1980-х роках кожен виробник створював власні SCADA-програми. Ці програми працювали лише з обмеженим набором контролерів і були закритими системами

— вони не мали універсальних драйверів для роботи з пристроями різних виробників, а також не підтримували стандартні методи інтеграції з іншими програмними продуктами.

З появою концепції відкритих систем на початку 1990-х програмне забезпечення для операторських станцій стало самостійним продуктом. Одним із головних завдань розробників SCADA стало створення багатокористувацьких систем керування, здатних одночасно підтримувати значну кількість автоматизованих робочих місць (АРМ) користувачів. В результаті виникла клієнт-серверна технологія або архітектура.

Клієнт-серверна архітектура передбачає наявність двох незалежних процесів — клієнта і сервера, які можуть працювати на різних комп'ютерах і обмінюватися даними через мережу (рис. 4.3). За такою схемою можуть будуватися системи керування технологічними процесами, системи обробки даних на базі СУБД та інші подібні рішення.

Рисунок 4.3 – Клієнт-серверна архітектура SCADA

У цій архітектурі станція-сервер — це комп'ютер із спеціалізованим програмним забезпеченням, яке відповідає за збір, збереження та подальшу передачу даних по каналах зв'язку оперативному персоналу для контролю та керування технологічним процесом, а також зацікавленим фахівцям і керівникам. За своєю суттю сервер виступає як постачальник інформації, тоді як клієнт — її споживач. Відповідно, робочі станції операторів, диспетчерів, спеціалістів і керівників є клієнтськими станціями. Зазвичай клієнтом є настільний ПК, на якому працює прикладне програмне забезпечення кінцевого користувача. Програмне забезпечення клієнта — це будь-яка програма або пакет, здатні відправляти запити серверу через мережу та обробляти отриману у відповідь інформацію. Функції клієнтських станцій, а отже і програмне забезпечення, різняться залежно від завдань конкретного робочого місця.

Кількість операторських станцій, серверів введення/виводу (серверів баз даних) визначається під час проєктування системи і залежить насамперед від обсягу інформації, що обробляється в системі. У невеликих системах керування функції сервера введення/виводу та оператора HMI можуть бути поєднані в одному комп'ютері.

У мережевих розподілених системах із використанням засобів SCADA/HMI стало можливим створювати вузли з різним функціональним призначенням: станції операторів або диспетчерів, сервери з функціями HMI, «сліпі» сервери без HMI, станції моніторингу для перегляду інформації без права керування, призначені для фахівців і керівників, а також інші типи вузлів.

SCADA-програми складаються з двох взаємопов'язаних модулів: Development (середовище розробки проєкту) і Runtime (середовище виконання). З метою оптимізації вартості проєкту ці модулі можуть бути встановлені на різні комп'ютери. Зазвичай станції операторів є вузлами Runtime (або View) із повним набором функцій людино-машинного інтерфейсу. Водночас принаймні один комп'ютер у мережі має бути типу Development, де проєкт створюється, редагується і, за потреби, виконується. Деякі SCADA-системи дозволяють вносити зміни до проєкту без зупинки роботи всієї системи. Програмне забезпечення

SCADA-серверів забезпечує можливість розробки повного проєкту системи керування, включно з базою даних і HMI.

Важливою складовою у структурі мережевих систем керування є організація бази даних реального часу — вона може бути централізованою або розподіленою. Різні розробники SCADA/HMI-систем по-різному реалізують ці структури, що істотно впливає на ефективність підтримки цілісності та єдності бази даних, її стабільність і можливості внесення змін.

Іноді для доступу до інформації на комп'ютерах-клієнтах створюють локальні копії бази даних, які синхронізуються з віддаленими серверами. Проте дублювання даних може призводити до труднощів із забезпеченням цілісності бази та знижувати продуктивність системи керування. Наприклад, при додаванні нової змінної необхідно оновлювати всі мережні копії, які її використовують.

Інший підхід полягає в тому, що комп'ютери-клієнти не зберігають копії бази даних, а отримують необхідну інформацію безпосередньо від сервера, який відповідає за її підтримку. Зазвичай таких серверів небагато, і кожен фрагмент даних зберігається лише в одному місці — на відповідному сервері. Внесення змін у базу відбувається виключно на сервері, що забезпечує її цілісність і унікальність. Цей метод зменшує навантаження на мережу та має низку інших переваг.

З погляду структурної побудови SCADA-пакетів розрізняють:

– системи, що забезпечують повний набір базових функцій HMI;

– системи, що полягають із модулів, що реалізують окремі функції HMI.

Системи, що включають повний набір базових функцій, можуть доповнюватися додатковими модулями, які реалізують необов'язкові функції контролю та керування.

У другому випадку система формується як повністю модульна структура — з окремими серверами для введення/виведення, обробки сигналів (alarms), аналізу трендів тощо. Для невеликих проєктів усі ці модулі можуть працювати на одному комп'ютері. У більших системах модулі можуть бути розподілені між

кількома комп’ютерами в різних комбінаціях. Приклад клієнт-серверної архітектури такої системи наведено на (рис. 4.3).

У клієнт-серверній архітектурі системи керування, зображеній на (рис. 4.4), обробка та зберігання даних, управління сигналами тривоги (alarms) і аналіз трендів розподілені між трьома окремими серверами. Інтерфейс людина-машина HMI реалізується на станціях-клієнтах.

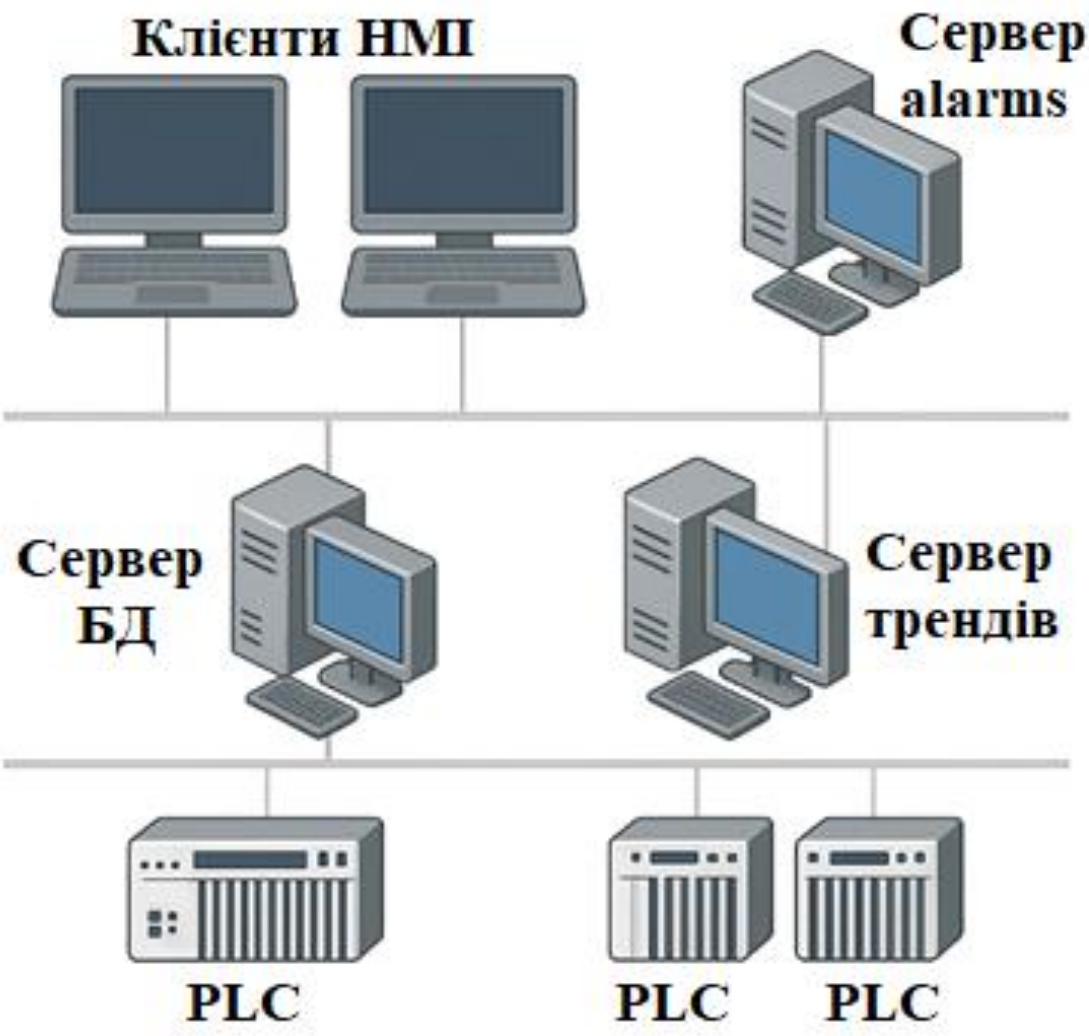

Рисунок 4.4 – Архітектура модульної SCADA

Наприклад, SCADA Citect має у своєму складі п’ять функціональних модулів (серверів або клієнтів):

– i/o – сервер вводу/виводу. Забезпечує передачу даних між фізичними пристроями введення/виводу й іншими модулями Citect;

– display – клієнт візуалізації. Забезпечує операторський інтерфейс: відображення даних, що надходять від інших модулів Citect, і керування виконанням команд оператора;

– alarms – сервер сигналів. Відслідковує дані, порівнює їх з припустимими межами, перевіряє виконання заданих умов і відображає сигнали на відповідному вузлі візуалізації;

– trends – сервер трендів. Збирає й реєструє трендову інформацію, дозволяючи відображати розвиток процесу в реальному масштабі часу або в ретроспективі;

– reports – сервер звітів. Генерує звіти після закінчення певного часу, при виникненні певного події або по запиту оператора.

В одній мережі можна використовувати тільки один сервер alarms, сервер трендів і сервер звітів. У той же час допускається використання декількох серверів уведення/виводу (i/o server). Кількість комп'ютерів із установленим модулем display (що забезпечують операторський інтерфейс) у мережі практично не обмежене.

4.1.2. Концепція відкритої системи в SCADA-технологіях

Розповсюдження архітектури «клієнт-сервер» стало можливим завдяки розвитку та впровадженню концепції відкритих систем. Основною причиною виникнення цієї концепції були складнощі у забезпеченні сумісної роботи програмно-апаратних компонентів у локальних комп'ютерних мережах. Вирішити ці проблеми дозволила міжнародна стандартизація програмних і апаратних інтерфейсів.

Концепція відкритих систем передбачає вільну взаємодію SCADA-програм із програмно-технічними засобами різних виробників. Це особливо важливо, оскільки сучасні автоматизовані системи відзначаються високим рівнем інтеграції численних компонентів. Окрім самого об'єкта керування, система включає комплекс різноманітних програмно-апаратних пристроїв: датчики, виконавчі механізми, контролери, сервери баз даних, робочі місця операторів, а також АРМ

спеціалістів і керівників (рис. 4.5). При цьому в межах однієї системи можуть використовуватись обладнання та програмне забезпечення від різних виробників.

Для забезпечення ефективної роботи в такому гетерогенному середовищі SCADA-система повинна мати високий рівень мережевої сумісності.

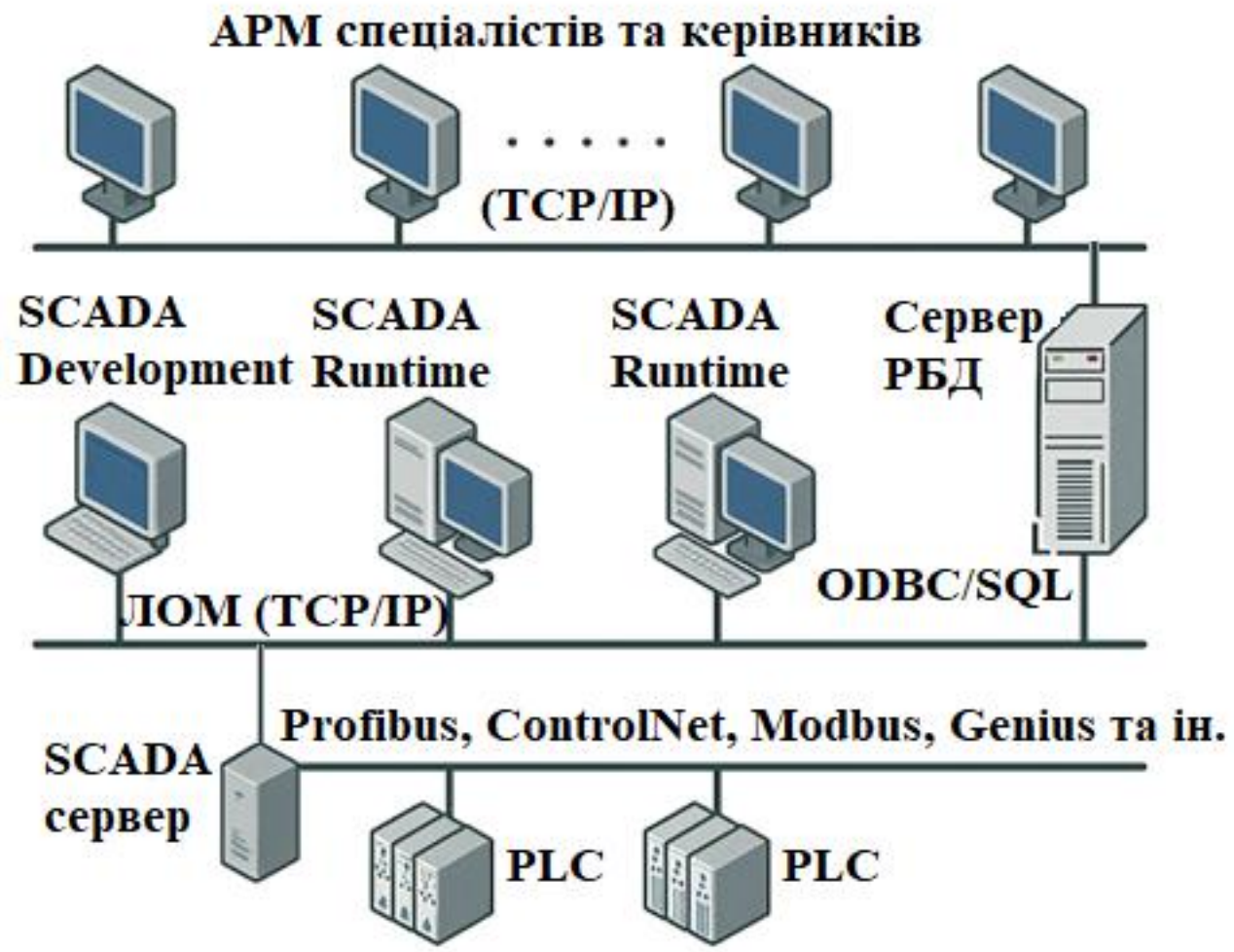

Рисунок 4.5 – Інтеграція SCADA у систему керування

З іншого боку, SCADA-системи повинні підтримувати інтерфейси зі стандартними інформаційними мережами, такими як Ethernet, із використанням стандартних протоколів передачі даних, наприклад TCP/IP, для забезпечення обміну інформацією з компонентами розподіленої системи керування.

Практично будь-яка SCADA-система містить базу даних реального часу та підсистему архівування даних. Однак підсистема архівування не призначена для

тривалого зберігання великих обсягів інформації (місяці чи роки). Дані в архіві регулярно оновлюються, адже для зберігання необмеженого обсягу інформації місця не вистачить. Основне завдання SCADA-програмного забезпечення — забезпечити оперативний персонал актуальною та архівною інформацією, необхідною для безпосереднього управління технологічними процесами.

Інформація, яка відображає господарську діяльність підприємства (наприклад, для складання матеріальних балансів установок, виробництв або підприємства загалом), зберігається у реляційних базах даних (РБД) типу Oracle, Sybase тощо. Дані до цих баз потрапляють або через ручне введення, або автоматично за допомогою SCADA-систем. Тому до SCADA-програмного забезпечення висувається ще одна важлива вимога — наявність протоколів обміну, сумісних із типовими базами даних.

4.1.3. Забезпечення стабільної роботи SCADA-систем

Поняття стабільності SCADA-пакетів включає два основні аспекти: надійність самого програмного забезпечення і можливість програмного резервування різних компонентів системи.

Стабільність SCADA визначається кількома факторами: стабільністю операційної системи, наявністю засобів збереження даних і конфігурації під час збоїв, а також можливістю автоматичного перезапуску системи.

За стабільністю сучасні SCADA-продукти мало чим відрізняються один від одного, як і за функціональністю. Однак при виборі пакета варто звернути увагу на перелік його можливостей. Наприклад, підтримка проєктів для небезпечних і відповідальних виробництв, робота з великим числом параметрів і територіально розподіленими сигналами тривоги свідчать про високу стабільність пакета.

Варто пам’ятати, що система керування може вийти з ладу не лише через програмні збої, а й через несправність обладнання. Найпоширенішою є розподілена система керування (рис. 4.6), але вона також може вийти з ладу, якщо один із компонентів, наприклад сервер, вийде з ладу.

Для запобігання таким ситуаціям SCADA-системи підтримують функції резервування. Це дозволяє усувати відмови без втрати працездатності і продуктивності системи. Резервування реалізується як через архітектуру системи, так і за допомогою вбудованих механізмів програмного забезпечення.

Для підвищення надійності системи керування широко застосовується резервування серверів (рис. 4.6). Існують два основні варіанти організації резервування.

У першому випадку основний і резервний сервери одночасно працюють із пристроями введення/виводу, що подвоює навантаження на промислову мережу і знижує загальну продуктивність системи. При нормальній роботі клієнти звертаються до основного сервера, а у разі його відмови – перенаправляють запити на резервний сервер.

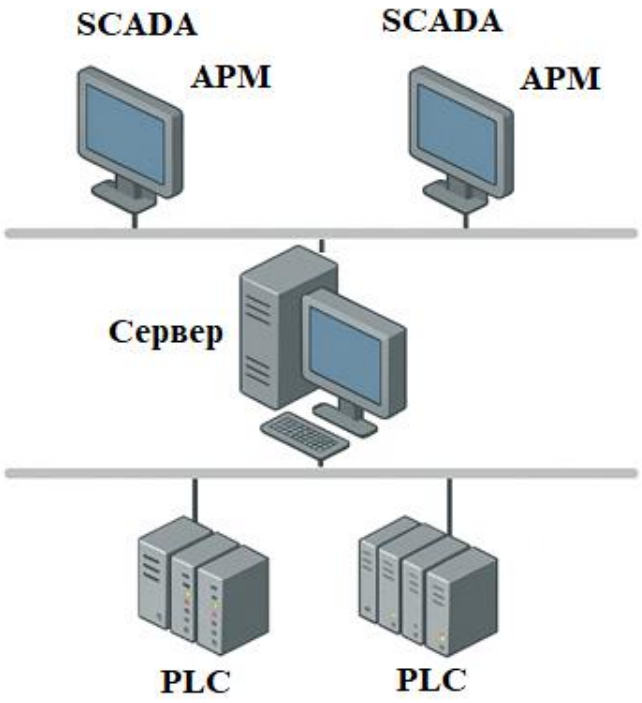

Рисунок 4.6 – Мережева архітектура SCADA

У розподіленій клієнт-серверній архітектурі SCADA-систем (рис. 4.7) лише один основний сервер безпосередньо взаємодіє з контролерами. При цьому основний сервер постійно оновлює базу даних резервного сервера, підтримуючи його в постійній готовності.

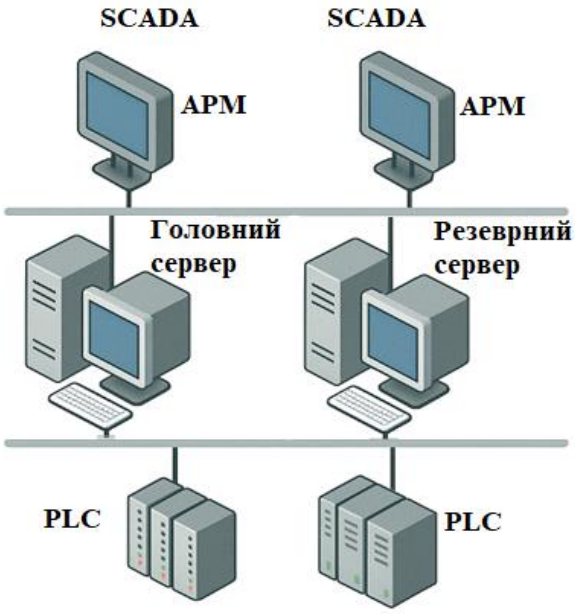

Рисунок 4.7 – Резервування сервера

Така структура підвищує стабільність системи, усуваючи одне з головних слабких місць – відмову сервера. Проте іншим потенційним слабким місцем є мережа: якщо вона виходить з ладу, станції операторів та диспетчерів втрачають зв’язок із системою, і керування порушується.

Підвищення надійності системи керування забезпечується додатковою мережею (рис. 4.8).

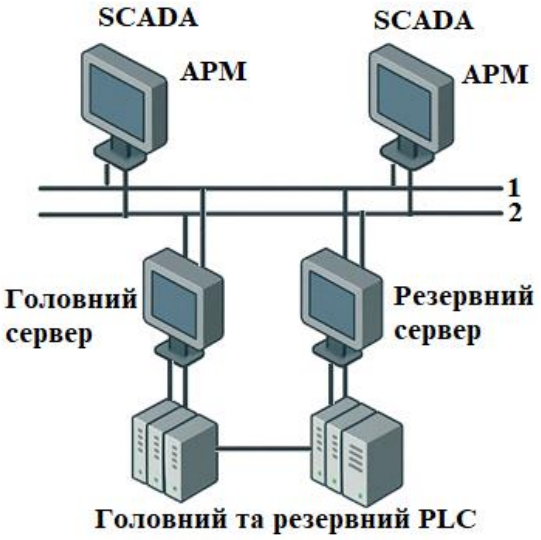

Рисунок 4.8 – Варіанти резервування

Більшість контролерів підтримують додатковий (резервний) канал зв’язку з сервером введення/виводу, що забезпечує обмін даними навіть при відмові основного каналу. Повне резервування досягається дублюванням контролерів (рис. 4.8).

Важливо, що вбудовані в SCADA-систему механізми дозволяють на етапі проєктування налаштовувати основні та резервні пристрої. Під час роботи система автоматично виявляє несправність компонентів, виконує перемикання на резервне обладнання і повідомляє про це оперативному персоналу.

4.2. Основні компоненти SCADA: RTU, PLC, HMI

Системи диспетчерського управління та збору даних SCADA є ключовими в інфраструктурі автоматизації енергетики, промисловості, транспорту та багатьох інших галузей. У своїй основі SCADA-системи складаються з кількох важливих компонентів, кожен із яких виконує унікальні функції у загальній архітектурі управління. До основних компонентів SCADA належать: віддалені термінальні пристрої RTU, програмовані логічні контролери PLC та інтерфейси людина-машина HMI.

RTU (Віддалений термінальний пристрій). RTU є ключовим елементом у SCADA-системах, який забезпечує зв’язок між фізичними об’єктами в польовому середовищі (наприклад, трансформаторними підстанціями, лініями електропередач, вимикачами тощо) та центром керування. Його основна функція — збір даних із сенсорів та виконавчих механізмів, а також передача команд керування з SCADA-системи.

Основні функції RTU:

– збір аналогових і дискретних сигналів (наприклад, струм, напруга, положення вимикачів);

– перетворення фізичних параметрів у цифрові сигнали;

– передача даних до SCADA-серверів за допомогою протоколів (наприклад, IEC 60870–5–101/104, DNP3);

– отримання команд керування та передача їх виконавчим пристроям;

– ведення журналів подій у разі втрати зв’язку з диспетчерським центром.

Особливості RTU:

– висока надійність і робота в жорстких кліматичних умовах;

– підтримка резервування каналів зв’язку;

– автономна робота при розриві з’єднання із центром керування;

– часто працюють на вбудованих операційних системах реального часу.

PLC (Програмований логічний контролер). PLC призначений для локального управління обладнанням. Його можна вважати мозком локальної автоматизації, який реагує на вхідні сигнали (запуски, аварії, зміни стану) і видає керуючі сигнали в реальному часі.

Основні функції PLC:

– виконання логіки керування на основі запрограмованих алгоритмів;

– реагування на події з низькою затримкою (у мілісекундах);

– підключення до RTU або безпосередньо до SCADA-системи;

– прийняття даних з аналогових та цифрових входів;

– формування керуючих впливів на вихідних каналах.

Переваги PLC:

– гнучкість — програмування можливе під конкретну задачу;

– висока швидкодія;

– широка підтримка інтерфейсів зв’язку;

– надійність у промислових умовах;

– можливість створення модульних та масштабованих систем.

У багатьох випадках PLC та RTU працюють у парі. Наприклад, PLC виконує швидке локальне управління, а RTU забезпечує зв’язок із SCADA. У сучасних системах часто один пристрій виконує функції обох (так звані інтегровані пристрої) (рис. 4.9).

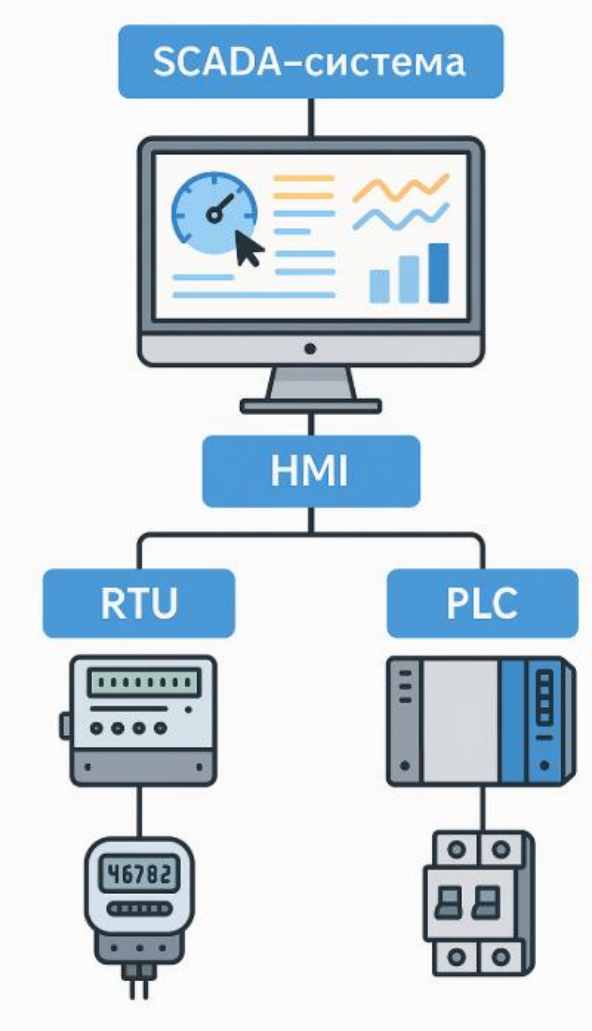

Рисунок 4.9 – Схема взаємодії RTU, PLC та HMI у SCADA

HMI (Інтерфейс людина-машина). HMI забезпечує взаємодію оператора з SCADA-системою, дозволяючи переглядати дані, вводити команди, виявляти несправності, спостерігати за тенденціями та вести звітність. Це графічний інтерфейс, який спрощує сприйняття складних технологічних процесів.

Основні компоненти HMI:

– графічні дисплеї: відображення структурних схем, панелей керування, сигналізацій;

– панелі подій і тривог: інформування про критичні ситуації;

– тренди та графіки: відстеження змін параметрів у часі;

– інтерактивні елементи: кнопки, повзунки, розкривні списки для керування параметрами або функціями системи.

Переваги HMI:

– висока наочність та інтуїтивність;
– зручність для навчання персоналу;
– гнучке конфігурування та кастомізація;
– підтримка різних мов інтерфейсу.

Існують локальні HMI, що розташовані безпосередньо на об’єктах (наприклад, сенсорна панель на шафі керування), та централізовані HMI, інтегровані в SCADA-сервери або робочі станції диспетчерів. Централізовані HMI зазвичай мають більший функціонал: від моніторингу всієї мережі до аналітики даних. В (табл. 4.1) наведена порівняльна характеристика RTU, PLC та HMI.

Таблиця 4.1 – Порівняння RTU, PLC та HMI

№	Компонент	Призначання	Основна функція	Особливість
1	RTU	Збір/передача даних з об’єкта	Комунікація між SCADA і польовими пристроями	Автономна робота, адаптований до зовнішніх умов
2	PLC	Локальне керування	Виконання логіки на об’єкті	Реакція в режимі реального часу
3	HMI	Взаємодія з людиною	Графічне представлення інформації	Інтуїтивність, налаштування інтерфейсів

У типовій SCADA-інфраструктурі (рис. 4.9) RTU та/або PLC встановлюються на об’єкті, де вони зчитують дані з лічильників, трансформаторів, реле захисту тощо. Зібрана інформація передається по мережі (наприклад, через Ethernet або радіоканал) до серверів SCADA, де дані обробляються та візуалізуються через HMI. Оператор через HMI може відправляти команди назад на об’єкт, наприклад, увімкнути або вимкнути вимикач.

Також важливо розуміти, що практична реалізація може мати гібридну архітектуру, де одна частина функцій реалізується PLC, інша — RTU, а керування здійснюється через HMI в межах одного пристрою.

Впровадження у енергетиці. У енергетиці ці компоненти є критично важливими для забезпечення надійного моніторингу та керування електромережами:

– RTU встановлюються на розподільчих підстанціях, де зчитують дані про навантаження, температуру, аварії;

– PLC керують логікою ввімкнення резервного живлення, перемикання між лініями;

– HMI дозволяє оператору диспетчерського пункту миттєво реагувати на зміну стану енергосистеми.

У складних сценаріях, наприклад, при роботі з цифровими підстанціями, ці компоненти можуть також обмінюватися даними по протоколах IEC 61850, що забезпечують гнучку й стандартизовану комунікацію.

Сучасні SCADA-системи частіше переходять:

– на віртуалізовані середовища — де всі компоненти SCADA розгортаються як віртуальні машини;

– на кібербезпеку — RTU, PLC та HMI тепер мають сертифікацію безпеки, шифрування зв’язку;

– на IoT-інтеграцію — нові RTU та PLC можуть працювати як пристрої Інтернету речей;

– на веб-інтерфейси HMI — замість стаціонарних клієнтів, доступ до SCADA можна отримати через браузер.

Компоненти RTU, PLC та HMI утворюють «трикутник» функціональності SCADA-систем. Вони забезпечують збір, обробку, аналіз і передачу інформації, дозволяючи здійснювати централізоване або децентралізоване управління технологічними процесами. Глибоке розуміння їхніх функцій та взаємодії є запорукою надійної та ефективної автоматизації, зокрема в енергетичній галузі, де точність, швидкодія та безперервність мають вирішальне значення.

4.3. Збір і обробка телеметричної інформації

У сучасних енергетичних системах ефективне диспетчерське управління можливе лише за умови наявності оперативної, достовірної та точної інформації про стан об’єктів енергетичної інфраструктури. Цю інформацію надає телеметрія — система, що забезпечує дистанційний збір, передавання та аналіз параметрів, таких як напруга, струм, частота, стан обладнання, рівень споживання та інші показники. У контексті SCADA-систем телеметрія є ключовим функціональним компонентом, що дозволяє реалізовувати централізоване управління, контроль та прогнозування.

Телеметрія (від грец. «теле» — далеко, і «метрео» — вимірюю) — це технологія вимірювання фізичних параметрів на віддалених об’єктах з подальшою передачею даних до центрального вузла збору і аналізу. У сфері енергетики телеметрична інформація включає як аналітичні, так і дискретні дані. Аналітичні дані можуть бути представлені значеннями струму, напруги, температури трансформатора, частоти мережі тощо, тоді як дискретні — це інформація про спрацьовування реле, відкриття чи закриття вимикачів, зміни стану приладів обліку.

Сучасні SCADA-системи автоматизовано збирають телеметричну інформацію за допомогою пристроїв збору даних, таких як RTU та PLC, після чого дані передаються до серверної частини SCADA для візуалізації та обробки.

Телеметричні дані можуть надходити з різноманітних пристроїв та систем, встановлених на об’єктах енергетичної інфраструктури.

Основні джерела телеметрії в енергетиці:

– сенсори напруги і струму — вимірюють змінні або постійні електричні величини;

– трансформатори струму і напруги (ТТ, ТН) — використовуються для вимірювання параметрів високовольтних ліній;

– лічильники електроенергії (Smart Meters) — забезпечують дані щодо обсягу споживання електроенергії та її якості;

– автоматичні вимикачі з функцією моніторингу — інформують про аварійні ситуації або відключення;

– температурні, вібраційні, тискові датчики — оцінюють стан обладнання, наприклад трансформаторів, генераторів.

– GPS/RTC годинники — забезпечують точну синхронізацію даних, що особливо важливо при подієвому аналізі.

На практиці збір телеметричної інформації відбувається через наступні етапи [6, 27]:

– первинне вимірювання — значення фізичних параметрів знімаються із сенсорів або трансформаторів;

– передача на польовий рівень — дані надходять до RTU або PLC, які працюють як локальні контролери;

– попередня обробка — RTU здійснює перетворення аналогових сигналів у цифрові, може здійснювати фільтрацію шуму або базову логіку;

– передача в SCADA — канали зв'язку (Ethernet, оптика, 4G, LTE, RS-485) передають інформацію на сервер або в хмару;

– обробка та зберігання — SCADA-сервер аналізує та архівує дані, виводить їх на HMI-панелі або термінали диспетчерів.

Реалізація повного циклу збору телеметричної інформації залежить як від типу обладнання, так і від обраного протоколу зв'язку — наприклад, Modbus, IEC 60870–5–104, DNP3 чи IEC 61850 [6, 27].

Обробка зібраних даних полягає не лише у зберіганні їх у базах даних, а й у перетворенні в аналітичну інформацію для прийняття рішень. Це включає:

– обчислення середніх, пікових та інтегрованих значень;

– виявлення тенденцій, аномалій та аварій;

– логічний аналіз послідовностей подій;

– обробку дискретних сигналів для визначення станів елементів;

– автоматичне формування звітів та журналів подій.

На етапі обробки активно застосовуються алгоритми цифрової фільтрації, агрегування даних, логічні та тригерні функції, а також системи тривог.

Основні функції програмного забезпечення для обробки телеметричних даних:

– формування трендів — графічне представлення змін параметрів у часі;

– сигналізація — автоматичне виявлення відхилень від допустимих значень і сповіщення диспетчера;

– архівація — збереження телеметричних даних у базах для подальшого аналізу;

– інтеграція — передача даних в інші системи (ERP, EMS, DMS);

– віддалений доступ — можливість моніторингу через вебінтерфейси або мобільні додатки;

– калібрування — автоматичне або ручне коригування значень за еталонами.

Щоб SCADA-система могла ефективно виконувати функції моніторингу та управління, її телеметрична частина повинна відповідати наступним вимогам:

– надійність — здатність забезпечити безперервний зв’язок і точні вимірювання;

– швидкодія — мінімальні затримки передачі, особливо для критичних сигналів;

– скалованість — можливість розширення кількості контрольованих точок;

– інтероперабельність — підтримка відкритих протоколів для обміну з іншими системами;

– стійкість до збоїв — можливість резервування каналів і дублювання даних.

Ці характеристики є критично важливими для об’єктів генерації, трансформації і розподілу енергії, де збій в передачі навіть одного сигналу може призвести до втрат або аварій.

Приклади практичного застосування. Розглянемо типову ситуацію в роботі диспетчерського пункту обленерго (рис. 4.10). RTU, розташований на підстанції 110/35/10 кВ, збирає дані з трансформаторів напруги, силових вимикачів, пристроїв релейного захисту. Через оптоволоконний канал дані надходять до SCADA-сервера, де оператор спостерігає на HMI відображення режимів роботи.

У разі виникнення аварійної ситуації — наприклад, короткого замикання на одній із ліній — система фіксує сигнал спрацювання, відображає повідомлення про аварію, активує тривогу і створює запис у журналі подій [6, 27].

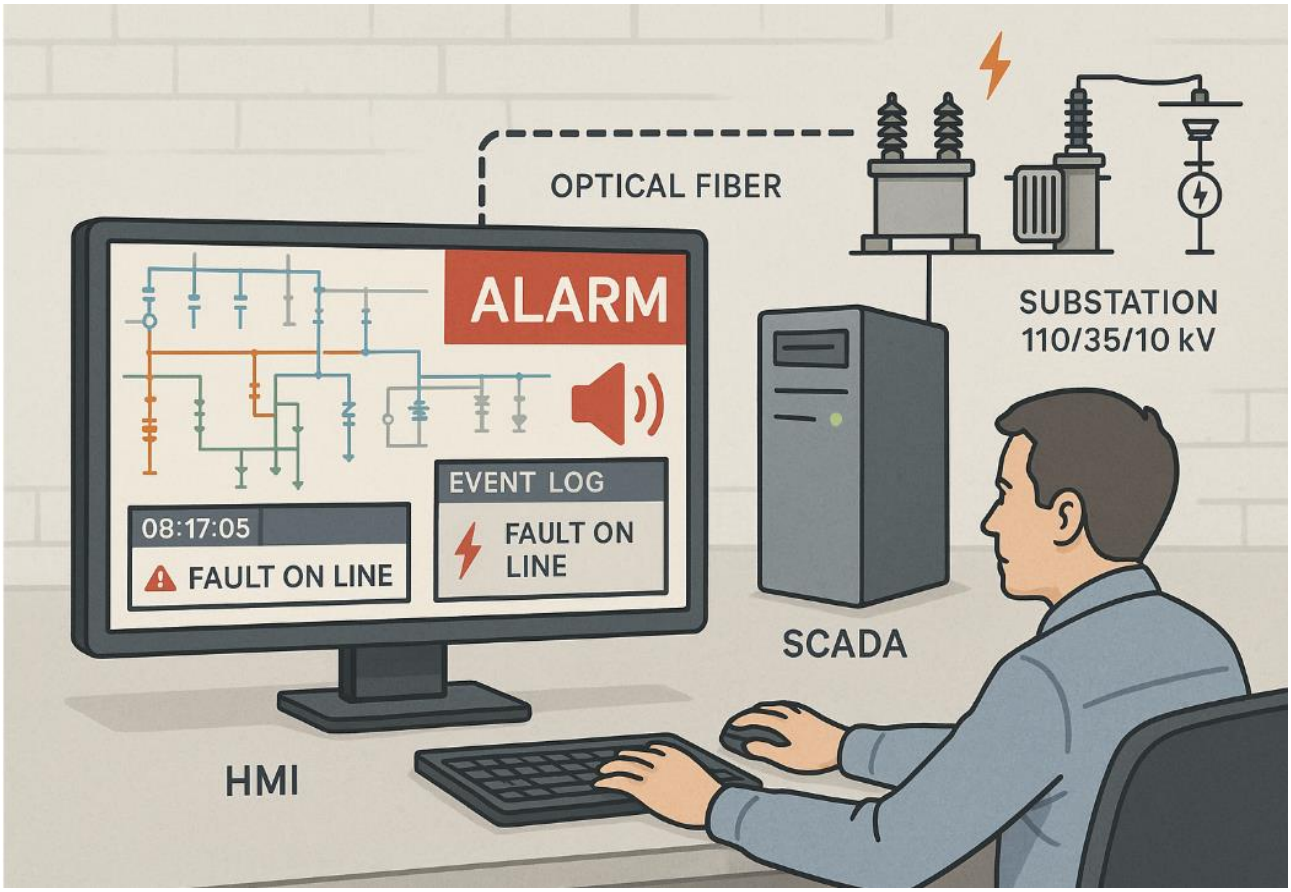

Рисунок 4.10 – Робота диспетчерського пункту обленерго

Також телеметричні дані можуть використовуватися для побудови прогнозних моделей навантаження, балансування потужностей та оптимізації роботи мереж. Завдяки телеметрії реалізуються функції «розумної мережі» (Smart Grid) — автоматичного управління споживанням, інтеграції відновлюваних джерел, виявлення неполадок у режимі реального часу.

Отже, телеметрична інформація є основою для повноцінного функціонування SCADA-систем в енергетиці. Її збір і обробка дозволяють підтримувати безперервний контроль над критично важливою інфраструктурою, забезпечують оперативне реагування на зміни в мережі та сприяють підвищенню надійності і ефективності енергетичних процесів. В умовах розвитку цифрових технологій

роль телеметрії тільки зростає — вона перетворюється з інструменту моніторингу у джерело цінних аналітичних даних, що формують основу для інтелектуальних рішень у сфері енергоменеджменту [6, 27].

4.4. Передача команд управління

У структурі систем диспетчерського управління, таких як SCADA, функція передачі команд управління займає центральне місце. Саме вона забезпечує реалізацію ключового принципу — не лише моніторинг, але й активний вплив на стан об’єктів управління (рис 4.11). Це стосується як дій з боку оператора, так і автоматичних алгоритмів, що активуються внаслідок певних подій, порогових значень чи збоїв. Передача команд управління — складний процес, який охоплює як технічні, так і логічні аспекти.

Рисунок 4.11 – Передача команди

Передача команд управління — це зворотний напрямок у потоці даних у SCADA-системі. Якщо телеметрія передає дані від об’єкта до диспетчерського центру (uplink), то команди управління — навпаки, прямують від SCADA-центру до обладнання (downlink). Ці команди можуть мати різну природу: включення або відключення лінії, зміна режиму трансформатора, регулювання напруги, зміна налаштувань захисту тощо.

Команди управління можуть бути реалізовані у вигляді дискретних сигналів (наприклад, включення/відключення), аналогових значень (встановлення уставки), або як серії команд, які виконуються у певній послідовності. Важливо

зазначити, що передача команд несе у собі потенційний ризик — помилкова або несвоєчасна дія може мати серйозні наслідки. Тому в системах SCADA ця функція максимально захищена, верифікована і структурована.

Архітектурна побудова передачі команд. Процес передачі команд має чітко визначену архітектуру. У загальному випадку вона включає кілька ключових етапів:

– генерація команди — команда формується в SCADA-сервері на основі дій оператора або автоматичних алгоритмів;

– передача по мережі — команда надходить через мережеві шляхи (Ethernet, LTE, MPLS) до віддаленого пристрою — RTU або PLC;

– прийом і декодування — RTU приймає команду, розпізнає її та запускає відповідний виконавчий механізм (наприклад, включає контактор);

– зворотний зв'язок (feedback) — після виконання команди об'єкт генерує підтвердження або інформує про стан, який фіксується на SCADA.

Весь процес зазвичай виконується за дуже короткий час — від кількох мілісекунд до кількох секунд, залежно від відстані, типу з'єднання і критичності функції.

Передача команд управління повинна відповідати ряду вимог, серед яких особливо виділяються точність, затримка, автентичність та захист від несанкціонованого доступу. Через високу критичність цієї функції, багато SCADA-рішень передбачають механізми попереднього підтвердження команди (select-before-execute), які дозволяють оператору двічі підтвердити дію перед її виконанням на обладнанні.

Крім того, протоколи зв'язку, що використовуються у SCADA-системах (таких як DNP3, IEC 60870–5–104, IEC 61850), забезпечують високий рівень захисту через:

– використання контрольних сум і CRC для перевірки цілісності даних;

– механізми шифрування на рівні кадрів;

– логування усіх переданих команд;

– контроль часових міток для виключення «відкладених» чи «повторно зіграних» команд.

Особливо варто підкреслити важливість використання віддаленої аутентифікації і ролевих моделей доступу, щоб жоден оператор або процес не міг вплинути на критичні вузли системи без відповідного дозволу.

Команди управління в SCADA-системах можуть бути класифіковані за різними ознаками: за типом дії, за механізмом реалізації або за рівнем критичності. Найбільш поширеними є наступні типи:

а) дискретні команди (ON/OFF). Вмикання або вимикання обладнання, наприклад, запуск генератора або роз'єднувача;

б) команди аналогового регулювання. Встановлення певного значення уставки — наприклад, встановлення напруги на трансформаторі або обмеження потужності;

в) секвенційні (послідовні) команди. Виконання серії дій, які повинні бути запущені у визначеному порядку — наприклад, запуск автоматизованого режиму.

г) автоматичні команди. Такі команди генеруються самою системою SCADA за умови досягнення критичних порогів або виникнення надзвичайної ситуації (наприклад, захисне відключення).

Усі ці типи команд можуть бути взаємопов'язаними. Наприклад, команда на підвищення потужності може супроводжуватись обмеженням на інші гілки навантаження, що вимагає додаткового аналізу з боку оператора або автоматизованого ПЗ.

Ключові фактори ефективної передачі команд:

– низька затримка передачі — особливо важливо для аварійних дій;

– достовірність — запобігання фальсифікації або помилкової передачі;

– синхронізація у часі — команди повинні виконуватись лише у точний момент;

– зворотній зв'язок — підтвердження виконання дій.

Роль людини та автоматизації в управлінні. Передача команд в SCADA не завжди є повністю автоматизованим процесом. Оператор у диспетчерському центрі залишається ключовим елементом у багатьох сценаріях, особливо коли йдеться про нестандартні або критичні ситуації. Сучасні HMI (інтерфейси людина-машина) дозволяють диспетчеру у зручному форматі бачити всі параметри системи, стан обладнання, і візуально контролювати виконання команд.

Однак, з розвитком технологій автоматизації, усе частіше управлінські рішення приймаються без участі людини. У таких випадках велику роль відіграє релейний захист і автоматика (РЗА), який працює в парі зі SCADA і в ряді ситуацій діє автономно, реалізуючи «швидкі команди» ще до того, як оператор отримає повідомлення.

Збалансована система, в якій автоматизація і диспетчерський контроль гармонійно співіснують, є найбільш ефективною і безпечною моделлю реалізації команд управління.

Попри прогрес у технологіях зв'язку та автоматизації, передача команд в SCADA-системах все ще стикається з низкою викликів:

– мережеві затримки — в умовах використання мобільного або супутникового зв'язку виникає затримка, що неприпустимо в критичних системах;

– збої в RTU/PLC — поломка польових пристроїв може унеможливити виконання команд;

– кібербезпека — зовнішнє втручання або хакерська атака може спровокувати подання помилкових команд;

– людський фактор — оператори можуть помилитися або не встигнути вчасно відреагувати на подію.

Для вирішення цих проблем впроваджуються резервні канали зв'язку, дублювання RTU, застосування антивірусного захисту, аудит команд управління та глибокий моніторинг усіх подій у SCADA.

Приклад із практики. На об'єкті генерації енергії, наприклад ГЕС, диспетчер може віддалено передати команду на закриття одного з клапанів турбіни у разі виявлення витоку або несправності. Ця команда надходить на центральний

сервер SCADA, звідти — до RTU, розташованого безпосередньо у машинному залі. RTU інтерпретує команду та активує електропривід клапана. Після виконання подається підтвердження — зворотна телеметрична інформація. Усі дії логуються і можуть бути перевірені в разі розслідування або аудиту (рис. 4.12).

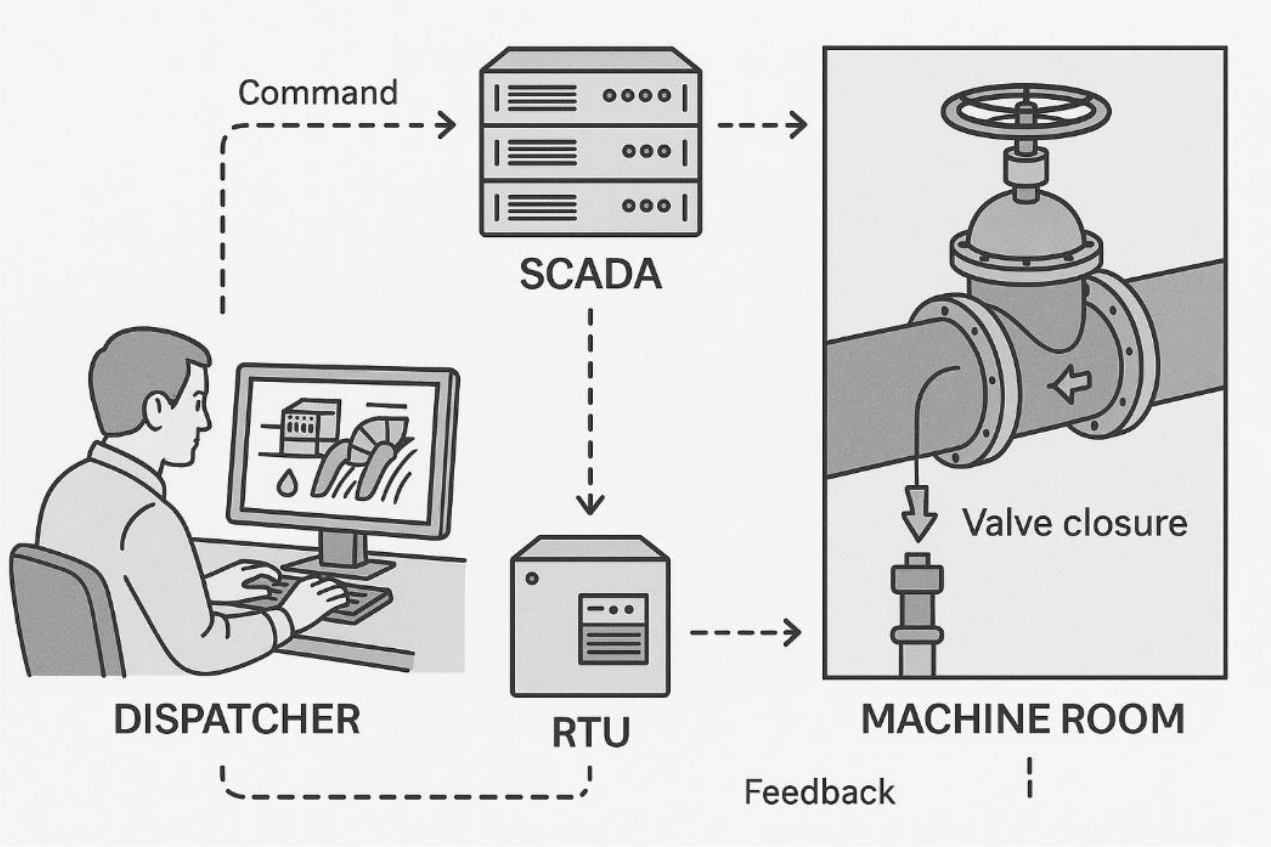

Рисунок 4.12 – Приклад застосування SCADA — RTU на ГЕС

Передача команд управління — це одна з найвідповідальніших функцій SCADA-систем, яка забезпечує не просто спостереження, а активне управління процесами в енергетичних системах. Вона вимагає високої надійності, захисту, чіткого регламенту виконання та глибокого інтегрування з іншими функціями системи. У майбутньому, зі зростанням ролі штучного інтелекту і глибокої автоматизації, ця функція стане ще більш інтелектуальною, але водночас потребуватиме ще вищих вимог до безпеки та контролю.

4.5. Приклади впровадження SCADA в енергетиці України та світу

Інтеграція SCADA-систем у сферу енергетики відкриває новий рівень ефективності, надійності та гнучкості управління інфраструктурою енергопостачання. З огляду на масштабність енергетичних систем, необхідність у моніторингу, контролі та автоматизації процесів є вирішальною. У цьому контексті SCADA виступає не просто як програмний інструмент, а як стратегічна складова цифрової трансформації галузі.

У цьому підрозділі розглянемо реальні приклади впровадження SCADA-систем в енергетиці України та світу, проаналізуємо досягнуті переваги, виклики, а також зосередимось на практичних аспектах, таких як адаптація до існуючої інфраструктури, взаємодія з іншими системами та специфіка комунікацій.

Впровадження SCADA у диспетчерському управлінні обласних електромереж (рис. 4.10). Одним із найбільш поширених прикладів в Україні є впровадження SCADA-систем у обласних РЕМ (районних електромережах), які відповідають за розподіл електроенергії на регіональному рівні. Такі системи забезпечують безперервний моніторинг та управління станом трансформаторних підстанцій, ліній електропередач, комутаційного обладнання.

У багатьох випадках SCADA-системи інтегрувались у вже наявну інфраструктуру. Наприклад, у «Хмельницькобленерго» було реалізовано SCADA на базі програмного забезпечення з підтримкою протоколів IEC 60870–5–104. Це дало змогу диспетчерам оперативно реагувати на нештатні ситуації, перемикати навантаження, дистанційно вимикати обладнання для ремонту.

Зокрема, однією з основних переваг стало скорочення часу виявлення аварій. Якщо раніше для з’ясування місця відключення могли проходити години, то з SCADA інформація надходить у режимі реального часу. Крім того, віддалене керування значно підвищило безпеку для ремонтного персоналу.

SCADA в об’єднаній енергосистемі України (ОЕС) (рис. 4.13). На рівні національного масштабу SCADA-системи використовуються для керування балансом генерації та споживання електроенергії. Системний оператор НЕК

«Укренерго» впровадив єдину систему диспетчерського управління, яка об'єднує елементи телемеханіки, SCADA, EMS.

Така система має декілька рівнів — регіональні диспетчерські центри, національний центр, а також підключення до європейської системи ENTSO-E. Здійснюється не лише передача оперативних команд, але й постійний збір аналітичних даних, що використовуються для прогнозування попиту, балансування енергосистеми, управління резервами.

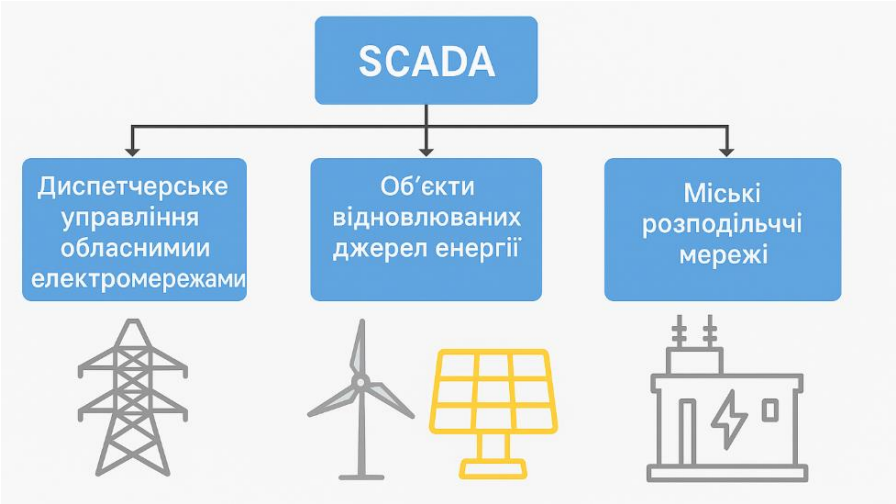

Рисунок 4.13 – Впровадження SCADA в енергетиці

Ключові особливості SCADA у ОЕС України:

– висока ступінь резервування каналів зв'язку;

– підтримка протоколів IEC 61850 та OPC UA;

– інтеграція з геоінформаційними системами (ГІС) для візуалізації розташування об'єктів;

– автоматичне оновлення даних у випадку втрати з'єднання.

Ця система пройшла випробування під час критичних ситуацій, зокрема після пошкоджень інфраструктури внаслідок надзвичайних ситуацій, і довела свою стійкість до відмов.

SCADA на об'єктах ВДЕ (відновлюваних джерел енергії).

Зі зростанням частки відновлюваних джерел енергії в енергобалансі, інтеграція SCADA-систем у СЕС (сонячні електростанції) та ВЕС (вітрові електростанції) стає критично важливою.

На СЕС у Миколаївській області встановлено SCADA-систему, яка забезпечує:

– моніторинг вироблення потужності з кожної сонячної панелі;

– контроль за температурою інверторів;

– управління кутом нахилу панелей для підвищення ефективності;

– підключення до центральної SCADA обласної мережі.

У вітровій генерації SCADA дозволяє не лише здійснювати контроль за швидкістю вітру та продуктивністю турбін, а й керувати «розумним обмеженням» у випадку перевищення дозволеного навантаження в енергосистемі.

Міські мережі. Приклад автоматизації підстанцій у Києві (рис. 4.14). У Києві реалізовано проєкт автоматизації розподільчих підстанцій середньої напруги із застосуванням SCADA, що дозволяє моніторити кожен етап електропостачання міських мікрорайонів. Усі підстанції оснащені RTU, які передають інформацію до центрального серверу, де диспетчер може бачити у візуальному інтерфейсі стан кожного роз'єднувача, трансформатора, аварійні сигнали, поточні навантаження.

Проєкт відзначається тим, що підстанції були модернізовані без повної заміни старого обладнання — тобто впроваджено принцип коли нова електроніка інтегрується в наявні системи.

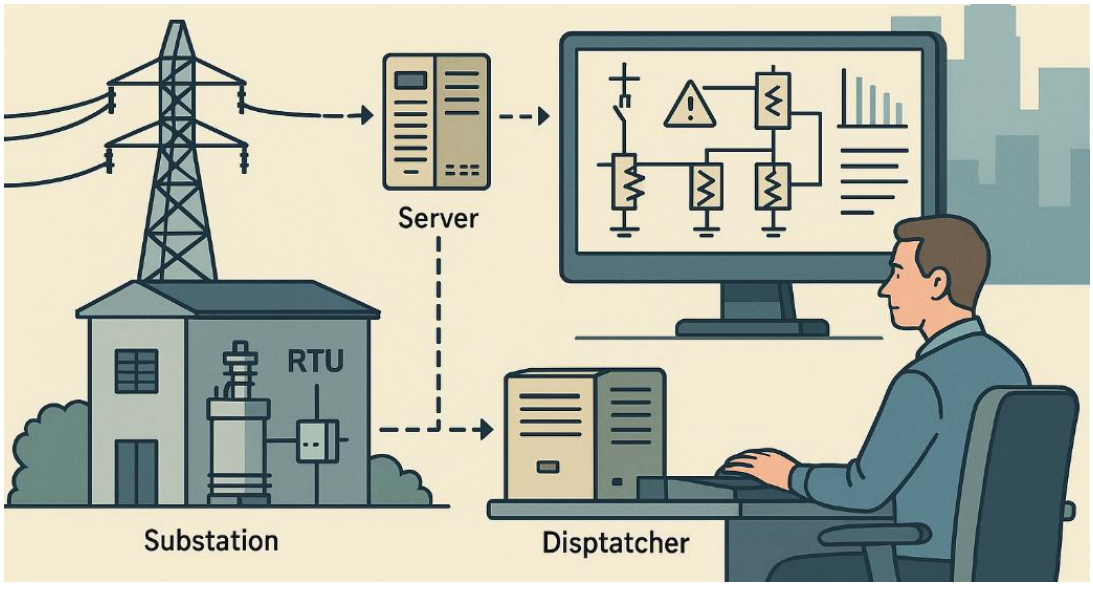

Рисунок 4.14 – Застосування SCADA-систем на підстанціях Києва

Успішні приклади з-за кордону. Варто також розглянути приклади впровадження SCADA за межами України. Зокрема, у Німеччині компанія *E.ON* впровадила масштабну SCADA-систему, що охоплює понад 7000 розподільчих підстанцій і використовує протокол IEC 61850. Усі підстанції взаємодіють із головним центром управління через захищені VPN-канали з резервуванням.

Також у США компанія *Duke Energy* використовує SCADA як частину загальної стратегії Smart Grid. Інформація від тисяч датчиків, RTU і PLC надходить до єдиного аналітичного центру, що дозволяє не лише реагувати на події в режимі реального часу, але й будувати прогнозні моделі навантаження.

Незважаючи на загальну архітектурну подібність SCADA-систем, кожне впровадження має свої особливості. Щоб проєкт був успішним, необхідно враховувати кілька факторів:

а) аналіз існуючої інфраструктури — визначення можливості інтеграції без повної заміни обладнання;

б) вибір протоколів зв'язку — відповідно до підтримки пристроїв (IEC 60870–5, DNP3, IEC 61850);

в) резервування каналів та елементів SCADA — особливо критично для об'єктів ОЕС;

г) підготовка персоналу — навчання диспетчерів, інженерів і техніків;

д) інтеграція з іншими системами — ERP, GIS, системами кібербезпеки.

Основні переваги, які забезпечує впровадження SCADA в енергетиці:

– підвищення оперативності управління;
– зниження витрат на технічне обслуговування;
– збільшення надійності електропостачання;
– прозорість у зборі статистичних даних;
– оптимізація режимів роботи обладнання.

SCADA-системи є критично важливими для сучасної енергетики. Їхнє впровадження не лише підвищує надійність і стабільність роботи мереж, а й створює основу для подальшого розвитку Smart Grid технологій, інтеграції ВДЕ, автоматизації реагування на аварії. Приклади, наведені в цьому підрозділі,

демонструють широкі можливості адаптації SCADA до потреб як регіональних мереж, так і централізованих систем керування.

Висновки до розділу 4

У межах четвертого розділу було розкрито багатовимірну роль SCADA-систем у сучасних енергетичних структурах, підкреслюючи їх важливість як інструменту, що забезпечує цілісність, надійність та керованість технологічних процесів. Аналіз архітектури, компонентів і функціональних можливостей SCADA дав змогу сформувати системне уявлення про те, як реалізується диспетчерське управління в електроенергетиці.

Розглянуто архітектуру SCADA-систем, включаючи польовий рівень, рівень контролерів, комунікаційний сегмент, серверну інфраструктуру та HMI. Було розкрито ключові принципи ієрархії, взаємодії між рівнями та типи функцій, які виконує кожен сегмент — від збору первинних даних до їх обробки, архівації та візуалізації. Важливе значення має диференціація архітектур — централізованої, розподіленої, гібридної та хмарної — що дозволяє гнучко адаптувати SCADA до різних умов об’єктів енергетики.

Розглянута клієнт-серверна архітектура дала змогу зрозуміти логіку взаємодії між центральним сервером і численними клієнтами — як робочими місцями операторів, так і інженерними станціями. Було показано, як структура баз даних, модульність та функціональне розділення впливають на гнучкість і масштабованість системи. Питання централізації або розподілення даних розкриває важливі аспекти продуктивності, цілісності та надійності SCADA-рішень.

У підрозділі, що розглядає питання відкритості систем, акцент зроблено на міжсистемній взаємодії та здатності SCADA інтегруватися з широким спектром апаратно-програмних рішень. Визначено переваги використання відкритих протоколів, підтримки промислових і корпоративних мереж, а також механізмів інтеграції з базами даних і сторонніми системами. Таке розуміння критично важливе в умовах мультивендорного середовища.

Окремо було розглянуто стабільність SCADA-систем. Було охарактеризовано підходи до резервування серверів, мережевих каналів, контролерів і функціональних модулів. Вивчено концепцію «дублювання», резервних ліній зв'язку та механізмів автоматичного перемикання, що забезпечують безперервність управління навіть у разі відмов. Це дозволяє проєктувати стійкі до збоїв системи з високим рівнем готовності.

В окремому підрозділі розглянуто основні компоненти SCADA: RTU, PLC та HMI. Розкрито їхню функціональну взаємодію, переваги й межі застосування. Глибоке розуміння ролі кожного з елементів дозволяє правильно розподіляти навантаження між пристроями, забезпечуючи баланс між локальним керуванням та централізованим контролем. Також висвітлено сучасні тенденції, пов'язані з віртуалізацією, веб-доступом і IoT-інтеграцією.

Значну увагу було приділено збору та обробці телеметричної інформації. Систематизовано підходи до вимірювання, перетворення, передачі, архівації та аналітики даних. Важливою є підтримка вимог до точності, швидкодії та стійкості до збоїв, що забезпечує можливість впровадження Smart Grid-рішень.

Розглянуто зворотній інформаційний потік — від оператора чи автоматичного алгоритму до виконавчого пристрою. Проаналізовано архітектуру, рівні захисту, підтвердження виконання та вимоги до протоколів. Підкреслено, що ефективна реалізація цієї функції вимагає не лише технологічної досконалості, але й чітких регламентів, а також захисту від помилок і зовнішніх впливів.

Наведені приклади впровадження SCADA в енергетиці дозволили побачити практичну реалізацію їх в різних умовах: регіональні мережі, об'єкти ОЕС, ВДЕ, міські системи. Показано, як інтеграція SCADA дозволяє покращити моніторинг, оптимізувати керування, скоротити аварійність і підвищити ефективність. Це демонструє не лише технічну, але й стратегічну роль SCADA-систем у цифровізації енергетики.

Таким чином, четвертий розділ навчального посібника дає комплексне уявлення про SCADA як інструмент управління в енергетиці: від фізичного рівня до бізнес-інтеграції. Знання, отримані в цьому розділі, формують основу для

практичного проєктування, впровадження та обслуговування сучасних енергетичних систем.

Запитання для контролю знань за четвертим розділом

1. Яке місце займає SCADA у структурі сучасних енергетичних систем і яку роль вона виконує?
2. Які основні рівні архітектури SCADA і які функції виконує кожен із них?
3. Чим відрізняються централізована, розподілена, гібридна та хмарна архітектури SCADA?
4. Як функціонує клієнт-серверна архітектура в SCADA-системах?
5. У чому полягають переваги модульного підходу до побудови SCADA?
6. Як впливає структура бази даних на ефективність роботи SCADA?
7. Які переваги надає використання відкритих протоколів у SCADA?
8. Чому відкритість SCADA є критично важливою для сучасної енергетики?
9. Як забезпечується стабільність і безперервність функціонування SCADA?
10. Які існують методи резервування в SCADA-системах?
11. У чому полягає роль RTU, PLC та HMI у складі SCADA-системи?
12. Як взаємодіють між собою основні компоненти SCADA для досягнення ефективного управління?
13. Які переваги надає віртуалізація та IoT-інтеграція у SCADA-системах?
14. Які етапи охоплює процес збору та обробки телеметричної інформації в SCADA?
15. Які вимоги висуваються до точності та швидкодії телеметричних даних?
16. Як реалізується передача команд управління в SCADA-системах?
17. Які заходи застосовуються для захисту команд управління від помилок і зовнішніх впливів?
18. Як виглядає зворотний інформаційний потік у системі SCADA?
19. Які переваги дає впровадження SCADA для моніторингу та управління енергетичними об’єктами?
20. Як SCADA сприяють цифровій трансформації енергетичної галузі?

5. АВТОМАТИЗОВАНІ СИСТЕМИ ОБЛІКУ ЕЛЕКТРОЕНЕРГІЇ

Автоматизовані системи комерційного обліку електроенергії (АСКОЕ) є ключовими інструментами сучасної енергетичної інфраструктури. Їх впровадження забезпечує точний, своєчасний та надійний збір даних про споживання електроенергії, що необхідно як для обґрунтованого тарифоутворення, так і для ефективного енергоменеджменту. У цьому підрозділі розглянемо основні завдання АСКОЕ, а також принципи, що лежать в основі побудови цих систем.

5.1. Завдання та принципи побудови АСКОЕ

Основне призначення АСКОЕ — забезпечення об’єктивного й достовірного комерційного обліку електричної енергії в автоматизованому режимі. На відміну від технічного обліку, комерційний має юридичну силу в розрахунках між постачальниками і споживачами енергії. Завдяки цьому АСКОЕ виконує кілька ключових завдань:

1) автоматизований збір та обробка даних. Система забезпечує регулярне отримання даних про споживання електроенергії з точних вимірювальних приладів без необхідності людського втручання;

2) передача даних у реальному часі. АСКОЕ передає зібрану інформацію до центрів обробки даних через канали зв’язку (GSM, GPRS, Ethernet, LoRaWAN тощо);

3) забезпечення енергетичної прозорості. Система дозволяє точно відслідковувати втрати в мережі, виявляти несанкціоновані підключення чи крадіжки електроенергії;

4) оптимізація енергоспоживання. Дані, зібрані АСКОЕ, дозволяють аналізувати профілі навантаження, що сприяє впровадженню енергоефективних заходів;

5) підтримка розумних мереж (Smart Grid). АСКОЕ є основою для подальшого розвитку інтелектуальних електромереж, які дозволяють гнучко реагувати на зміну попиту та пропозиції енергії.

Концепція побудови АСКОЕ базується на ряді принципів, які забезпечують функціональність, надійність та безпеку системи. До основних принципів належать:

а) Ієрархічність архітектури. АСКОЕ реалізуються у вигляді багаторівневої системи, де кожен рівень виконує специфічну функцію. Зазвичай виділяють три рівні:

– об'єктовий рівень — включає електролічильники, які встановлені на об'єктах споживання (підстанції, трансформаторні пункти, об'єкти споживачів);

– рівень збору та концентрації даних — реалізується за допомогою пристроїв збору та обробки інформації (концентраторів, шлюзів);

– центральний (диспетчерський) рівень — серверне ПЗ, яке виконує збір, збереження, обробку та візуалізацію даних. Часто тут реалізується інтерфейс користувача.

б) безперервність та надійність вимірювання. Використання електролічильників класу точності не нижче 0.5S або 1.0, що мають функції архівування та самодіагностики, є обов'язковим. У разі зникнення зв'язку лічильники повинні зберігати дані у внутрішній пам'яті до моменту відновлення каналу передачі;

в) гнучкість і масштабованість. АСКОЕ повинна легко адаптуватися до змін структури об'єктів обліку, дозволяти розширення кількості вузлів, зміну тарифів, інтеграцію з іншими системами (ERP, SCADA тощо);

г) відповідність нормативній базі. Системи повинні відповідати вимогам чинних стандартів, таких як:

– ДСТУ EN 62056 (серія для обміну даними);

– IEC 62052 / 62053 (вимоги до лічильників);

– ISO/IEC 27001 (інформаційна безпека).

д) захищеність інформації. Системи АСКОЕ повинні гарантувати цілісність і конфіденційність даних. Для цього використовуються протоколи з шифруванням (TLS, HTTPS), багаторівнева авторизація користувачів, контроль доступу та запис подій.

Щоб ефективно виконувати функції комерційного обліку, АСКОЕ включає низку ключових компонентів:

– інтелектуальні електролічильники — з функцією зчитування та архівування даних за часовими інтервалами;

– концентратори/шлюзи — агрегують дані з кількох лічильників та передають їх на сервер;

– мережеві пристрої зв'язку — забезпечують передачу даних через Ethernet, GSM/3G/4G, радіоканали або оптоволокно;

– сервер збору даних (Head-End System) — програмне забезпечення, яке приймає та зберігає дані від усіх вузлів обліку;

– аналітичне програмне забезпечення — виконує обробку інформації, формування звітів, аналіз споживання тощо.

Обмін даними в АСКОЕ може здійснюватися за допомогою різних технологій, таких як:

– DLMS/COSEM — міжнародний стандарт обміну даними з лічильниками;

– Modbus, IEC 60870–5–104 — промислові протоколи, які можуть використовуватися у шлюзах для передачі даних на диспетчерські рівні;

– MQTT, HTTP API — використовуються для взаємодії з хмарними платформами або мобільними застосунками.

Типова схема роботи АСКОЕ (рис. 5.1). Зазвичай система працює наступним чином: інтелектуальні лічильники на об'єктах фіксують споживання енергії з заданою періодичністю (наприклад, кожні 15 хвилин), після чого дані передаються на концентраційний рівень. Потім інформація централізовано надходить до серверної частини, де вона обробляється, архівується та візуалізується через інтерфейс користувача.

Впровадження АСКОЕ має суттєвий економічний та операційний ефект:

– зниження небалансів у мережах і контроль втрат;

– оптимізація розрахунків із споживачами, завдяки детальній та прозорій інформації;

– можливість прогнозування попиту, що важливо для стабільності енергосистеми;

– інтеграція з системами Smart Grid — перехід до автоматичного реагування на навантаження;

– віддалене управління вузлами обліку — оновлення тарифів, перезавантаження пристроїв, контроль стану лічильників.

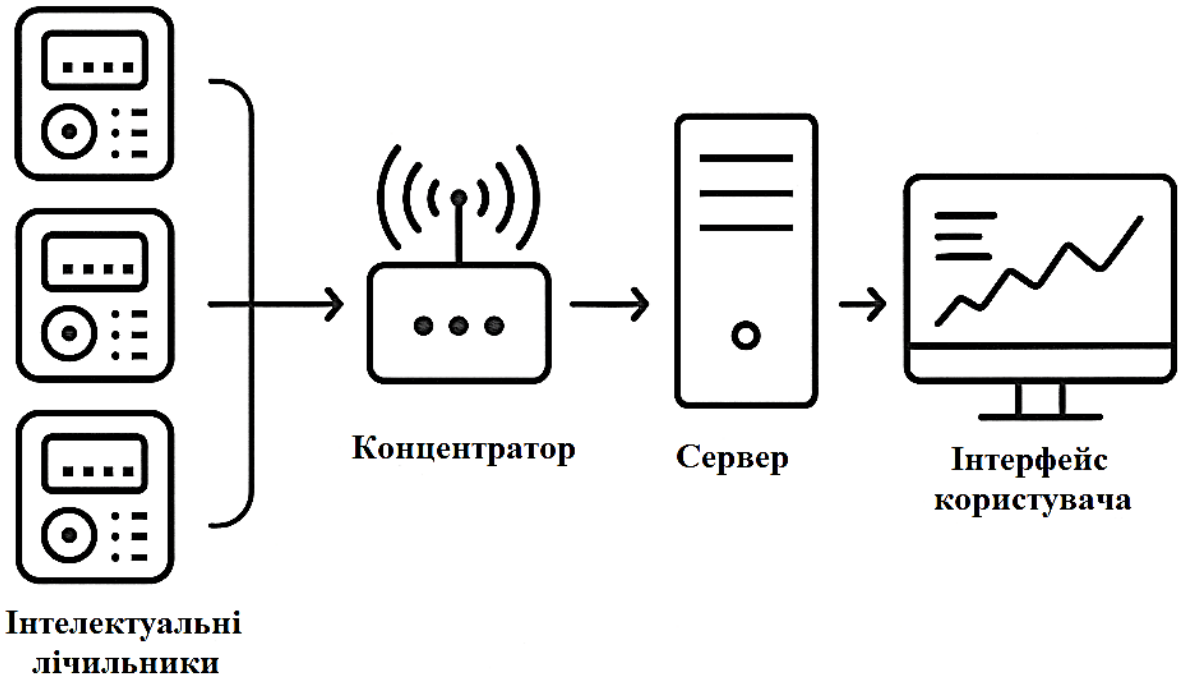

Рисунок 5.1 – Типова схема роботи АСКОЕ

Переваги від використання АСКОЕ:

– підвищення прозорості взаємин між енергопостачальником і споживачем.

– зменшення операційних витрат завдяки автоматизації.

– підвищення енергетичної безпеки.

– надання можливості інтеграції в системи управління енергоефективністю.

Попри очевидні переваги, впровадження АСКОЕ пов’язане з певними викликами:

– висока вартість обладнання та інфраструктури;

– необхідність захисту інформації від кіберзагроз;

– інтеграція з застарілими системами обліку на об’єктах, де ще не реалізовано Smart-обладнання;

– організаційні бар’єри, зокрема опір зміні традиційних підходів до обліку.

Автоматизовані системи комерційного обліку електроенергії є критично важливим елементом сучасної енергетичної інфраструктури. Завдяки автоматичному збору, передачі та обробці даних, АСКОЕ забезпечують ефективне управління споживанням енергії, мінімізацію втрат, об’єктивність розрахунків і підвищення надійності енергопостачання. Побудова таких систем вимагає врахування багатьох технічних, організаційних і безпекових аспектів, однак їх ефективність цілком виправдовує витрати на впровадження.

5.2. Структура інформаційного обміну в АСКОЕ

Інформаційний обмін у системах автоматизованого комерційного обліку електроенергії (АСКОЕ) є одним із ключових компонентів, що визначає ефективність, достовірність і надійність функціонування всієї системи. Він охоплює взаємодію між усіма елементами — від інтелектуальних лічильників на польовому рівні до центрального сервера, який забезпечує аналітичну обробку, архівацію і виведення даних через користувацький інтерфейс.

Попри те, що зовнішньо АСКОЕ може виглядати як простий ланцюг «лічильник – сервер – диспетчер», насправді за цим стоїть складна багаторівнева система, що має дотримуватись як технічних, так і нормативних вимог. Структура інформаційного обміну в АСКОЕ повинна забезпечувати не лише передачу даних, а й їх перевірку, синхронізацію, збереження та доступність у реальному часі.

Основна логіка побудови інформаційного обміну. Незалежно від конфігурації конкретної АСКОЕ, структура інформаційного обміну зазвичай має ієрархічну організацію. Дані спершу збираються на рівні польових пристроїв (інтелектуальні лічильники), потім передаються до пристроїв концентрації, з яких надходять до центрального сервера або хмарної інфраструктури. У кожній точці

обміну виконуються додаткові завдання — від перевірки автентичності джерела до архівації в резервних сховищах.

Щоб забезпечити цілісність цієї структури, особлива увага приділяється таким елементам:

– синхронізації даних у часі;

– можливості ретрансляції та повторної передачі при збоях;

– автоматичному розпізнаванню аномалій у даних;

– шифруванню інформації при передачі.

– адаптації до нових пристроїв без потреби у повній перебудові архітектури.

Ці принципи втілюються через логічне розділення системи на функціональні рівні (рис. 5.2).

Рисунок 5.2 – Структура інформаційного обміну АСКОЕ

Функціональні рівні структури обміну:

1) Польовий рівень. Початковий рівень складається з інтелектуальних лічильників, що здійснюють безперервний або періодичний збір показників електроспоживання. Залежно від специфікації, лічильники фіксують:

– активну та реактивну електроенергію;

– максимальні значення навантаження;

– події (відключення, спроби втручання тощо);

– якість електроенергії (гармоніки, перекоси напруги).

Ці дані зберігаються у внутрішній пам'яті пристрою до моменту передачі. Щоб забезпечити відповідність часових позначок, лічильники синхронізуються за допомогою локального або глобального джерела часу (GPS, NTP).

2) Рівень концентрації. Цей рівень виконує агрегування даних із кількох лічильників і діє як буфер між польовими пристроями та сервером. Концентратор виконує базову фільтрацію, шифрує інформацію, перевіряє достовірність підключених лічильників і забезпечує адаптацію форматів даних до стандартів системи. У разі втрати з'єднання з сервером, концентратор зберігає дані тимчасово, запобігаючи втратам.

3) Комунікаційний рівень. Передача інформації між концентраторами та сервером реалізується різними каналами — від мобільних мереж (2G-5G, LTE-M, NB-IoT), PLC, Ethernet, до спеціалізованих VPN-з'єднань. Особливу увагу тут приділяють питанням:

– стійкості до втручань;

– криптографічного захисту;

– визначення пріоритетності пакетів даних (QoS);

– підтримки відкладеної доставки у разі непередбачуваних обставин.

Однією з головних переваг сучасних технологій зв'язку є можливість гнучкої маршрутизації, що дозволяє мінімізувати затримки навіть у великих енергетичних мережах.

4) Серверний рівень. Центральна серверна частина виконує ключову функцію – довготривале зберігання, обробку, обчислення та вивід даних для користувача. Обчислювальні потужності серверу дозволяють:

– здійснювати валідацію і нормалізацію отриманих даних;

– побудову аналітичних моделей для виявлення тенденцій;

– генерацію звітів для енергетичних компаній, регуляторів та кінцевих споживачів;

– інтеграцію з іншими системами (ERP, CRM, SCADA тощо).

У великих мережах застосовуються сервери з розподіленими базами даних, резервними кластерами та хмарною інфраструктурою.

5) Інтерфейсний рівень. Остання ланка — інтерфейс користувача — дає змогу споживачам та операторам взаємодіяти з даними в зручній формі. Сучасні інтерфейси забезпечують:

– вебдоступ до інформації з різних пристроїв;

– налаштування сповіщень про події (через email, SMS, push);

– фільтрацію, сортування, побудову графіків;

– налаштування прав доступу залежно від ролі користувача.

Сучасні виклики для інформаційного обміну. З розвитком технологій та ускладненням енергетичних систем, структура обміну в АСКОЕ повинна адаптуватися до нових викликів. Зокрема, необхідно враховувати такі аспекти:

а) кібербезпека. У зв’язку з дедалі більшою кількістю атак на енергетичні системи (включно з SCADA та АСКОЕ), виникає потреба у реалізації захисту даних не лише на рівні шифрування, а й у створенні механізмів виявлення аномалій у трафіку та сегментації мереж;

б) інтероперабельність. Враховуючи різноманіття виробників лічильників та іншого обладнання, виникає потреба у створенні єдиної платформи з підтримкою стандартів типу DLMS/COSEM;

в) масштабованість. Зі зростанням кількості точок обліку (особливо у містах), система повинна бути здатною розширюватися без порушення надійності;

г) обробка великих даних. Відповідь на виклик Big Data — застосування технологій паралельної обробки, хмарних платформ та штучного інтелекту.

Приклад інформаційного потоку даних в АСКОЕ. Кожні 15 хвилин (рис. 5.3) інтелектуальний лічильник записує значення електроспоживання і надсилає його через GPRS-модем на концентраційний пристрій, який агрегує інформацію з десятків або сотень інших точок. Потім ці дані передаються через VPN-тунель на головний сервер, де верифікуються, аналізуються й архівуються. Користувач у веб-інтерфейсі може переглядати графіки споживання, аналізувати пікові періоди або формувати звіт для виставлення рахунків.

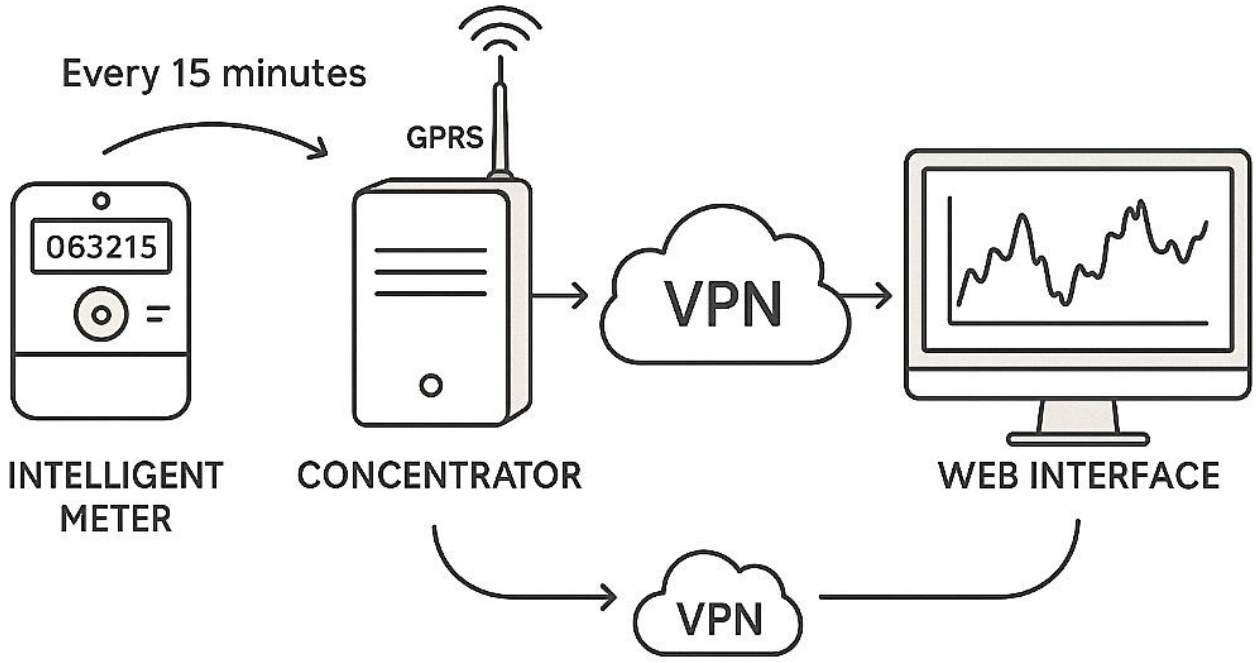

Рисунок 5.3 – Інформаційний потік даних в АСКОЕ

Інформаційний обмін — це артерія, через яку циркулює життєво важлива інформація для функціонування АСКОЕ. Його структура визначає, наскільки точно, своєчасно та безпечно система реагує на події, приймає рішення і забезпечує прозорість взаємодії між енергокомпаніями та споживачами. В умовах діджиталізації енергетики, побудова гнучкої, стійкої та масштабованої структури обміну стає запорукою ефективного управління ресурсами.

5.3. Захист і шифрування даних

У сучасних умовах цифровізації енергетичних систем питання інформаційної безпеки набуває стратегічного значення. Автоматизовані системи комерційного обліку електроенергії (АСКОЕ) є ключовими компонентами енергетичних підприємств, і забезпечення цілісності, конфіденційності та доступності інформації у таких системах є критично важливим для стабільної роботи енергетичної галузі.

Із розвитком кіберзагроз, появою нових способів вторгнення та злому інформаційних систем, зростають вимоги до захищеності АСКОЕ. У цій підсистемі циркулює інформація, що може мати комерційне, технічне або навіть стратегічне значення. Мова йде не лише про обсяг споживання електроенергії, а й про структуру навантаження, профілі споживання окремих підприємств, регіональні особливості споживання, що можуть бути використані як для аналітики, так і для кібершпигунства чи маніпуляцій у разі втручання зловмисників.

Проблематика захисту інформації в АСКОЕ. Почати варто з глибшого розуміння специфіки обігу інформації в АСКОЕ. Дані тут мають, як правило, циклічний характер — лічильники формують пакети з показниками у певні інтервали (від хвилин до годин), які передаються через канали зв’язку до концентраційного рівня (збір даних) і надалі — до центрального архіву та обробки. На всіх цих етапах дані зазнають потенційних загроз: перехоплення, фальсифікація, видалення, зміна або блокування. У той же час, підключення великої кількості пристроїв, розподілених по географії країни, створює умови для множинних точок входу для атак.

Ще одна важлива особливість — це обмежені ресурси частини пристроїв, що беруть участь в АСКОЕ. Деякі інтелектуальні лічильники або модеми не мають достатньої обчислювальної потужності для реалізації складних криптографічних алгоритмів, що змушує обирати компромісні рішення: або знижувати рівень захисту, або впроваджувати гібридні схеми.

Архітектура безпеки АСКОЕ. Сучасна архітектура безпеки АСКОЕ базується на стандартах, зокрема IEC 62351, ISO/IEC 27001, рекомендаціях NIST та

реальних вимогах енергетичних компаній. Як правило, вона включає фізичний, мережевий, криптографічний і організаційно-адміністративний рівні захисту. Така багаторівнева модель дозволяє реалізовувати принцип оборони в глибину (defense in depth), коли навіть при прориві одного рівня безпеки загальний захист системи зберігається.

Розглянемо один з таких рівнів — криптографічний — більш детально. У контексті АСКОЕ шифрування даних використовується під час:

– передавання інформації по каналах зв'язку (від лічильника до концентратора, від концентратора до сервера);

– зберігання даних на сервері;

– автентифікації користувачів і пристроїв у системі;

– передачі команд керування, наприклад, команд на відключення або зміну конфігурації.

Реалізація цього шифрування зазвичай базується на симетричних та асиметричних алгоритмах. Симетричне шифрування, як-от AES, є оптимальним для високошвидкісного кодування великих обсягів даних, тоді як асиметричні алгоритми, як RSA або ECC, застосовуються для автентифікації або обміну ключами (рис. 5.4 – 5.5).

Рисунок 5.4 – Захист даних в АСКОЕ

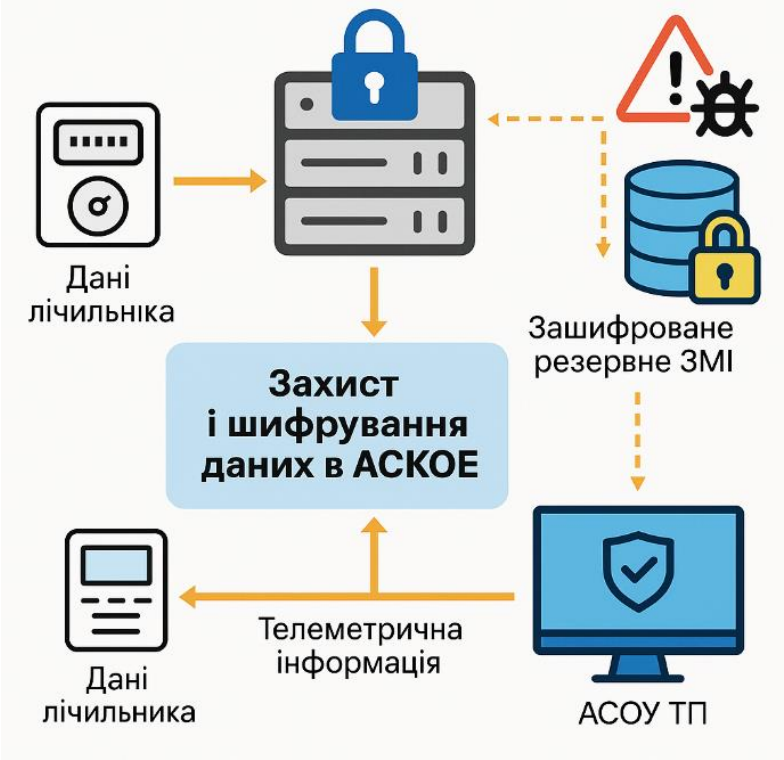

Рисунок 5.5 – Захист та шифрування даних в АСКОЕ

Управління ключами є одним з найскладніших аспектів інформаційної безпеки. У масштабній системі АСКОЕ можуть бути сотні тисяч пристроїв, кожен з яких має мати унікальний або захищений ключ. Необхідно забезпечити:

– генерацію надійних ключів;

– їх безпечне зберігання та розподіл;

– регулярне оновлення або заміну;

– можливість відкликання у разі компрометації.

Найпоширенішим рішенням є впровадження PKI (інфраструктура відкритих ключів), де сертифікати X.509 забезпечують ідентифікацію пристроїв і користувачів. Також використовуються протоколи OCSP або списки відкликаних сертифікатів CRL, які дозволяють блокувати скомпрометовані ключі в реальному часі.

Безпечна автентифікація користувачів і пристроїв. Питання автентифікації — не менш важливе, ніж шифрування. Необхідно впевнено знати, що користувач чи пристрій, який надсилає дані чи запити, є довіреним елементом системи.

Для цього застосовуються:

– токени;

– сертифікати;

– багатофакторна автентифікація (наприклад, пароль + код з мобільного додатку);

– криптографічні підписи, що дозволяють перевірити джерело запиту.

Ці засоби повинні бути адаптовані під реальні умови експлуатації — включаючи нестабільне покриття мобільних мереж, віддалені локації об’єктів і обмежені обчислювальні ресурси польових пристроїв.

Окремої уваги заслуговує аналіз реальних кіберінцидентів. Наприклад, у випадках із атаками BlackEnergy, Industroyer, Sandworm, які були спрямовані проти української енергетики, використовувались як соціальна інженерія, так і вразливості SCADA-компонентів. Усі вони показали, що навіть найкраще захищена система є вразливою, якщо не реалізовано моніторинг, резервне копіювання, оновлення ПЗ та регулярні аудити безпеки.

В Україні деякі енергетичні компанії, особливо національного масштабу (наприклад, НЕК «Укренерго»), реалізували захищені канали зв’язку для передавання даних АСКОЕ на базі IPsec-VPN, використовують сертифіковані засоби криптографії, цифрові підписи та багаторівневу аутентифікацію. У той же час в умовах війни спостерігається зростання уваги до розподіленої архітектури систем, де дані не зберігаються централізовано, що дозволяє мінімізувати ризик єдиного вузла відмови.

Перелік ключових заходів захисту даних у АСКОЕ:

– шифрування трафіку та даних;

– автентифікація користувачів і пристроїв;

– ведення журналів дій;

– застосування цифрових підписів;

– розподілене резервне копіювання.

Хоча цей перелік є коротким, у практиці захисту головне не кількість технологій, а узгодженість їх використання — кожен компонент має підсилювати інші, не створюючи “слабких ланок”.

5.4. Інтеграція АСКОЕ з іншими системами підприємства

Автоматизовані системи комерційного обліку електроенергії самі по собі є потужним інструментом для моніторингу та аналізу споживання електроенергії. Проте справжню цінність вони розкривають тоді, коли інтегруються з іншими інформаційними та управлінськими системами підприємства. Така інтеграція дозволяє не тільки підвищити ефективність використання ресурсів, але й сприяє оптимізації виробничих процесів, зменшенню витрат, покращенню планування та підвищенню загальної конкурентоспроможності підприємства.

У цьому підрозділі буде детально розглянуто завдання інтеграції АСКОЕ, типи систем, з якими вона може взаємодіяти, а також ключові аспекти успішної інтеграції.

Потреба в інтеграції АСКОЕ з іншими системами обумовлена кількома факторами. По-перше, сучасні підприємства прагнуть до централізації інформації для кращої аналітики та прийняття обґрунтованих рішень. По-друге, окреме функціонування систем створює ризики дублювання даних, втрат інформації та зниження оперативності роботи. Нарешті, розвиток концепцій Industry 4.0 та цифрової трансформації вимагає створення інтегрованих інформаційних екосистем.

Без інтеграції навіть найкраща АСКОЕ може залишитися ізольованим рішенням, яке обмежено виконує тільки завдання обліку, не роблячи вагомого внеску у стратегічне управління підприємством.

Інтеграція АСКОЕ може здійснюватися у кількох ключових напрямах (рис. 5.6):

– фінансові системи: передача даних про споживання електроенергії для розрахунків витрат, тарифікації, підготовки бюджетів та фінансового прогнозування;

– системи енергоменеджменту (EMS): використання інформації АСКОЕ для розробки енергоефективних заходів, виявлення втрат та оптимізації споживання;

– АСУ ТП (автоматизовані системи управління технологічними процесами): використання даних обліку для оперативного керування виробничими процесами залежно від рівня енергоспоживання;

– ERP-системи: інтеграція для комплексного управління ресурсами, включаючи енергетичні ресурси поряд із матеріальними, фінансовими та людськими.

Рисунок 5.6 – Інтеграція АСКОЕ з іншими системами підприємства

Процес інтеграції супроводжується певними труднощами, серед яких варто відзначити:

– різноманітність протоколів передачі даних: системи можуть використовувати різні протоколи та формати даних, що ускладнює об’єднання інформації без проміжних рішень;

– несумісність обладнання: лічильники та інші пристрої можуть підтримувати обмежений набір функцій інтеграції;

– проблеми кібербезпеки: інтеграція підвищує ризики несанкціонованого доступу до критичної інформації;

– високі вимоги до точності та своєчасності даних: будь-які затримки або викривлення інформації можуть призвести до серйозних наслідків у виробничих і фінансових процесах.

Для забезпечення надійної взаємодії між АСКОЕ та іншими системами використовуються такі підходи:

– стандартизовані протоколи обміну даними (наприклад, IEC 60870–5–104, Modbus TCP/IP, OPC UA);

– використання проміжного програмного забезпечення (middleware) для адаптації різних форматів даних;

– розробка API для організації безпечного доступу до даних АСКОЕ сторонніми системами;

– реалізація сервісно-орієнтованої архітектури SOA для гнучкої побудови інтеграційних рішень.

Інтеграція АСКОЕ із системою ERP дозволяє автоматично підставляти дані про витрати електроенергії у фінансову звітність підприємства, що значно спрощує аналіз собівартості продукції та планування енергоспоживання (рис. 5.7).

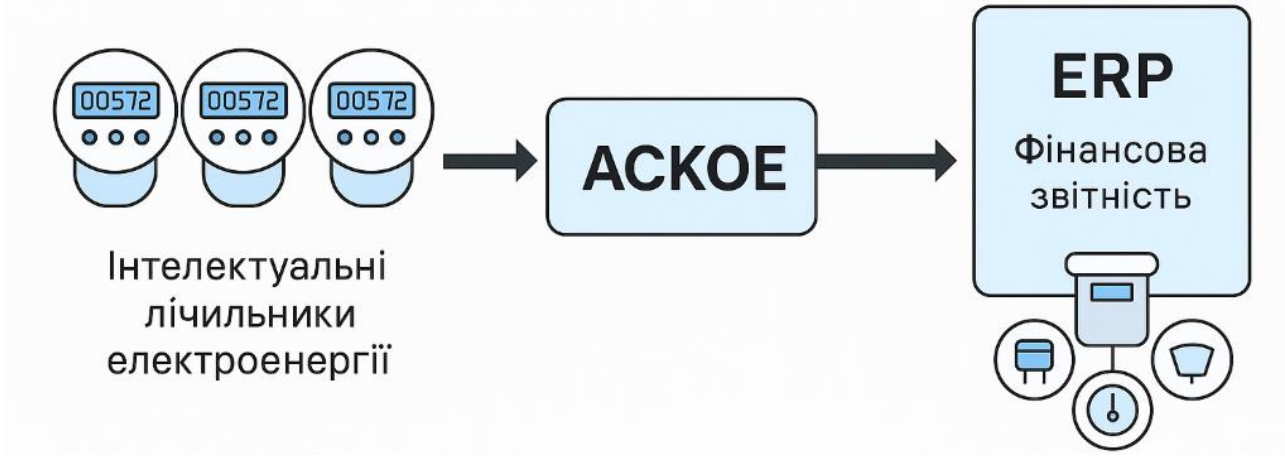

Рисунок 5.7 – Інтеграція АСКОЕ із системою ERP

Інтеграція АСКОЕ з іншими системами дає низку переваг:

– скорочення витрат на енергоресурси через своєчасне виявлення неефективного споживання;

– поліпшення точності фінансового обліку і можливість оперативного формування звітності;

– підвищення загальної енергоефективності підприємства;

– створення умов для глибокого аналізу енергоспоживання у розрізі підрозділів, технологічних процесів або обладнання;

– можливість автоматизації процесів планування закупівель енергії.

Інтеграцію АСКОЕ можна провести із системами, які уже згадувалися в попередніх розділах навчального посібника: ERP-системи (наприклад, SAP, Oracle E-Business Suite), системи енергоменеджменту EMS, АСУ ТП.

Існує кілька моделей побудови інтегрованих рішень з системою АСКОЕ:

– точкові інтеграції. Створення окремих каналів обміну даними між АСКОЕ та кожною системою;

– централізована інтеграція через шину даних (Enterprise Service Bus). Усі системи обмінюються даними через єдиний комунікаційний центр;

– хмарна інтеграція. Передача даних у централізоване хмарне середовище, де дані обробляються та поширюються до зацікавлених систем.

Сучасні тенденції в інтеграції систем обліку електроенергії передбачають ширше використання хмарних технологій, що забезпечують масштабованість, відмовостійкість і можливість аналітики у реальному часі. Зростає попит на рішення, які підтримують інтеграцію за допомогою інтелектуальних агентів, що автоматично узгоджують формати даних і оптимізують потоки інформації без участі людини.

Особлива увага приділяється питанням безпеки інтегрованих систем: усе частіше застосовуються технології шифрування даних при передачі та автентифікації користувачів через багатофакторні механізми.

Інтеграція АСКОЕ з іншими інформаційними системами підприємства — це не просто технічний проєкт, а стратегічна ініціатива, яка сприяє цифровій

трансформації виробництва. Розумно організована інтеграція дозволяє перетворити дані обліку електроенергії на потужний інструмент управління, що допомагає підприємству досягати високої енергоефективності, знижувати витрати та підвищувати гнучкість у реагуванні на зміни ринку.

5.5. Нормативне забезпечення функціонування АСКОЕ

Автоматизовані системи комерційного обліку електроенергії є ключовим компонентом у структурі сучасного енергетичного господарства. Їх впровадження та ефективне функціонування нерозривно пов'язані з розвиненою нормативно-правовою базою, яка регулює всі аспекти створення, впровадження, експлуатації, технічного обслуговування та модернізації таких систем. Забезпечення відповідності міжнародним і національним стандартам є обов'язковою умовою для інтеграції АСКОЕ у загальну систему енергетичного менеджменту країни та участі на конкурентному ринку електроенергії.

Нормативне забезпечення виконує кілька критично важливих функцій. По-перше, воно встановлює загальні технічні вимоги до засобів обліку електроенергії та інформаційних систем. По-друге, формує єдині правила взаємодії між різними учасниками ринку електроенергії — операторами систем передачі, постачальниками, споживачами, органами державного регулювання. По-третє, забезпечує довіру до результатів обліку, завдяки чітко визначеним процедурам верифікації та сертифікації (рис. 5.8).

Крім того, нормативне регулювання має вирішальне значення для впровадження інновацій в галузі обліку та енергоменеджменту. Зокрема, розвиток «розумних мереж» (Smart Grids), впровадження динамічного тарифоутворення, інтеграція з інформаційно-аналітичними системами підприємств потребують постійного оновлення вимог та адаптації стандартів.

В Україні функціонування АСКОЕ регулюється низкою законів, підзаконних актів та стандартів. Базовим документом є Закон України «Про ринок електричної енергії», який визначає засади організації обліку електричної енергії в умовах лібералізованого ринку. У цьому законі передбачено обов'язковість

комерційного обліку, його незалежність, а також відповідальність за достовірність даних обліку.

Рисунок 5.8 – Нормативне забезпечення АСКОЕ

Іншим важливим документом є Закон України «Про енергозбереження», який формує нормативну базу для підвищення ефективності використання енергії, у тому числі шляхом впровадження АСКОЕ як інструменту моніторингу та оптимізації споживання енергії.

Не менш важливою є постанова Національної комісії, що здійснює державне регулювання у сферах енергетики та комунальних послуг (НКРЕКП) щодо Правил роздрібного ринку електричної енергії, в якій визначені вимоги до побудови систем обліку, вимоги до засобів вимірювальної техніки та процесів взаємодії між учасниками ринку.

Технічне регулювання функціонування АСКОЕ базується на міжнародних і національних стандартах. Зокрема, важливим є застосування сімейства стандартів DLMS/COSEM (ДСТУ EN 62056), які регулюють формат передачі даних між лічильниками та системами збору інформації. Ці стандарти забезпечують інтероперабельність різного обладнання незалежно від виробника, що критично важливо для функціонування ринку.

Крім того, застосовуються стандарти IEC 61850, що стосуються автоматизації енергетичних об’єктів і забезпечують можливість обміну даними між різними системами в реальному часі.

На національному рівні діють стандарти, наприклад, ДСТУ 7113:2009, який визначає вимоги до точності та функціональних характеристик засобів комерційного обліку електроенергії.

Ще одним важливим напрямком нормативного забезпечення є процедура сертифікації обладнання та метрологічного контролю. Усі прилади обліку електроенергії, що використовуються в системах АСКОЕ, повинні пройти державну метрологічну атестацію та бути внесені до відповідного реєстру.

Процес сертифікації включає в себе:

– оцінку відповідності технічним вимогам;

– перевірку на відповідність стандартам захисту даних;

– випробування в умовах експлуатації.

Лише після успішного проходження всіх етапів обладнання може бути використане для комерційного обліку.

АСКОЕ працює з критично важливою інформацією — даними про споживання енергії, які мають як економічну, так і стратегічну цінність. Тому нормативне забезпечення обов’язково охоплює вимоги до інформаційної безпеки.

В Україні діють вимоги щодо захисту інформації в автоматизованих системах відповідно до законодавства про захист інформації та персональних даних. Зокрема, йдеться про необхідність впровадження:

– технологій шифрування даних при передачі;

– систем автентифікації та авторизації доступу;

– засобів виявлення та реагування на несанкціоновані дії.

Актуальними є також вимоги стандарту ISO/IEC 27001, який визначає принципи побудови системи управління інформаційною безпекою в організації.

Приклад системного підходу до нормативного регулювання:

– встановлення базових принципів функціонування обліку електроенергії у законах;

– деталізація технічних вимог у підзаконних актах та стандартах;

– створення процедур сертифікації та контролю якості;

– розробка вимог до інформаційної безпеки та захисту даних.

Попри наявність значної нормативної бази, функціонування АСКОЕ стикається з низкою викликів. Одним із головних є застарілість окремих нормативних актів, що не враховують новітніх технологічних рішень у галузі енергетики та цифровізації. Часто нормативи відстають від реального розвитку індустрії на кілька років, що стримує впровадження інноваційних підходів до обліку.

Ще однією проблемою є недостатня деталізація вимог до захисту даних в автоматизованих системах обліку, що створює ризики кіберзагроз. Окремі підприємства впроваджують АСКОЕ без належної сертифікації обладнання, що ускладнює забезпечення точності обліку і може призводити до фінансових суперечок.

Для подолання цих викликів необхідно:

– провести ревізію чинної нормативної бази з метою її актуалізації;

– активніше впроваджувати міжнародні стандарти у національне законодавство;

– створити механізми постійного моніторингу відповідності систем АСКОЕ вимогам нормативних актів;

– посилити державний контроль за впровадженням АСКОЕ через акредитацію та сертифікацію.

Найближчим часом можна очікувати подальшу інтеграцію української нормативної бази із європейською. Зокрема, йдеться про гармонізацію з вимогами Регламенту (ЄС) № 2016/679 (GDPR) у частині захисту персональних даних та директивами ЄС щодо функціонування енергетичних ринків.

Крім того, очікується розробка нових стандартів щодо інтеграції АСКОЕ з системами «розумного дому», розподіленої генерації, системами накопичення енергії, що потребуватиме відповідної адаптації вимог безпеки, інтероперабельності та енергетичної ефективності.

Іншою перспективною тенденцією є перехід до цифрових нормативних актів — формалізованих електронних стандартів, які зможуть автоматично інтерпретуватися програмним забезпеченням, що забезпечить ще вищий рівень сумісності між різними системами.

Висновки до розділу 5

У п’ятому розділі було комплексно розглянуто автоматизовані системи комерційного обліку електроенергії як невід’ємну складову сучасної цифрової енергетики. Поступовий перехід до автоматизованого, точного та безперервного контролю за електроспоживанням вимагає не лише технічного вдосконалення, а й системного підходу до інтеграції, захисту та нормативного супроводу. Розділ сформував цілісне уявлення про функціональність, архітектуру та перспективи таких систем у контексті розвитку Smart Grid і цифрової трансформації енергетичного сектору.

Було висвітлено ключові функції систем — від збору й обробки даних до передачі їх у реальному часі та підтримки енергетичної прозорості. Значну увагу приділено ієрархічній архітектурі, що включає об’єктовий, концентраційний і центральний рівні. Підкреслено важливість надійності вимірювань, масштабованості, відповідності нормативам і захищеності інформації. Ознайомлення з ключовими компонентами, протоколами передачі даних та типами мережевої взаємодії створює фундамент для подальшого вивчення практичної реалізації таких систем.

Деталізовано багаторівневу модель взаємодії між польовими лічильниками, концентраторами, каналами передачі, серверною частиною та користувацькими інтерфейсами. Підкреслено значення синхронізації даних, безперервності зв’язку, стійкості до збоїв і здатності до адаптації. Увага зосереджена на вимогах до функціонального поділу, маршрутизації, шифрування та інтелектуальної обробки інформації в реальному часі. Така структура визначає ефективність, достовірність і швидкодію всієї системи обліку.

При розгляді аспектів захисту й шифрування даних у центрі уваги була багаторівнева архітектура безпеки, що поєднує фізичний, мережевий, криптографічний і адміністративний рівні. Розглянуто проблеми, пов’язані з обмеженими ресурсами пристроїв, управлінням криптографічними ключами, автентифікацією користувачів і запобіганням несанкціонованому доступу. Підкреслено значення відповідності міжнародним стандартам безпеки, зокрема щодо шифрування трафіку, цифрових підписів, багатофакторної аутентифікації та систем моніторингу подій. Практичні приклади вказують на стратегічну важливість інформаційного захисту для безпеки енергосистем.

При розгляді інтеграції АСКОЕ з іншими інформаційними системами підприємств, було показано, що ізольована робота системи обліку обмежує її потенціал, тоді як інтеграція з ERP, EMS, АСУ ТП або фінансовими платформами дозволяє створити єдину інформаційну екосистему. Розглянуто варіанти реалізації обміну даними, використання API, middleware, стандартних протоколів і хмарних платформ. Було наголошено на технічних і організаційних викликах — сумісності, кібербезпеці, точності інформації. У результаті сформовано уявлення про переваги інтегрованого підходу до управління енергоресурсами підприємства.

Також було розглянуто нормативне забезпечення функціонування АСКОЕ. Проаналізовано чинну нормативну базу на національному та міжнародному рівнях, що регламентує технічні вимоги до лічильників, процеси обліку, вимоги до захисту інформації та процедури сертифікації. Підкреслено важливість оновлення нормативних актів у відповідь на розвиток цифрових технологій, зокрема щодо Smart Grid, Big Data та цифрових нормативів. Увага до сертифікації, метрологічного контролю та правового регулювання формує основу довіри до систем комерційного обліку.

Таким чином, п’ятий розділ навчального посібника комплексно висвітлив технічні, інформаційні, організаційні та нормативні аспекти АСКОЕ. Цей розділ є ключовим для розуміння того, як сучасні енергетичні підприємства можуть

забезпечити прозорий, точний і безпечний облік електроенергії, інтегруючи його у загальну систему енергетичного та корпоративного управління.

Запитання для контролю знань за п’ятим розділом

1. Які основні завдання автоматизованих систем комерційного обліку електроенергії в умовах цифрової енергетики?
2. Чому важлива ієрархічна архітектура АСКОЕ та які рівні вона включає?
3. Яким чином забезпечується надійність вимірювань в АСКОЕ?
4. Які типи мережевої взаємодії використовуються в АСКОЕ і чому?
5. Як впливають протоколи передачі даних на ефективність системи обліку електроенергії?
6. Що становить основу структури інформаційного обміну в АСКОЕ?
7. Які вимоги висуваються до синхронізації даних в АСКОЕ?
8. Як забезпечується стійкість системи АСКОЕ до збоїв?
9. У чому полягає значення функціонального поділу компонентів АСКОЕ?
10. Які підходи застосовуються до маршрутизації інформації в АСКОЕ?
11. Як реалізується шифрування даних в автоматизованих системах обліку?
12. Які рівні охоплює архітектура інформаційної безпеки в АСКОЕ?
13. Які загрози виникають при обмежених ресурсах облікових пристроїв?
14. Чому важливе управління криптографічними ключами в системах обліку?
15. Які заходи забезпечують автентифікацію користувачів у АСКОЕ?
16. Яке значення має відповідність міжнародним стандартам у сфері кіберзахисту АСКОЕ?
17. Чому ізольоване функціонування АСКОЕ обмежує її потенціал?
18. Як інтегрується АСКОЕ з ERP, EMS або фінансовими системами?
19. Які технічні та організаційні виклики виникають при інтеграції АСКОЕ з іншими платформами?
20. Які основні напрями регулювання охоплює нормативна база для функціонування АСКОЕ?

6. СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЕНЕРГЕТИЦІ

Енергетична сфера перебуває на порозі великої технологічної революції. Збільшення попиту на електроенергію, поширення відновлюваних джерел енергії, електрифікація транспорту, а також глобальні цілі декарбонізації енергетики змушують переглядати традиційні принципи побудови електричних мереж. У відповідь на ці виклики з'явилася концепція Smart Grid — нова парадигма розвитку енергетичних систем, орієнтована на гнучкість, інтегрованість, автоматизацію та інтелектуальне управління.

6.1. Концепція Smart Grid

Концепція Smart Grid передбачає створення високотехнологічних енергетичних мереж, що поєднують в собі засоби традиційної енергетики, інформаційно-комунікаційних технологій, автоматизації та аналітики великих даних. Ці системи повинні забезпечити оптимальне використання ресурсів, підвищити надійність енергопостачання, забезпечити ефективну інтеграцію децентралізованої генерації та зменшити негативний вплив на навколишнє середовище.

Основні риси та суть концепції. Традиційні електричні мережі працюють за принципом односторонньої передачі енергії — від великих електростанцій до кінцевих споживачів. У системі Smart Grid цей процес стає двостороннім: споживач може не тільки отримувати енергію, але й самостійно її генерувати, зберігати, продавати або споживати залежно від поточних потреб ринку.

Суть концепції Smart Grid полягає в максимальній автоматизації та саморегулюванні енергетичної системи. Всі компоненти мережі оснащуються сенсорами, контролерами та комунікаційними пристроями, які забезпечують безперервний моніторинг стану системи та прийняття оперативних рішень без участі людини (рис. 6.1).

На практиці це означає, що енергосистема зможе:

– самостійно балансувати навантаження між генерацією і споживанням;
– оперативно реагувати на зміни у споживанні енергії;

– ідентифікувати та локалізовувати аварії у режимі реального часу;

– інтегрувати відновлювані джерела енергії без втрати стабільності мережі.

Рисунок 6.1 – Концепція Smart Grid

Таким чином, Smart Grid трансформує звичайну енергосистему на комплексну «енергетичну екосистему», де кожен учасник може брати активну участь у виробництві, розподілі та споживанні енергії.

Технічна архітектура Smart Grid. Будова «розумної» мережі передбачає інтеграцію декількох ключових рівнів:

– польовий рівень — включає інтелектуальні пристрої: сенсори, реле, інтелектуальні лічильники, контролери мікромереж;

– комунікаційний рівень — забезпечує безпечний та надійний обмін даними між усіма елементами системи за допомогою різних мережевих технологій (наприклад, Wi-Fi, LTE, 5G);

– аналітичний рівень — обробляє зібрані дані за допомогою хмарних платформ, великих даних та алгоритмів машинного навчання для прогнозування споживання, управління попитом і виявлення аномалій;

– рівень взаємодії з користувачами — дозволяє кінцевим споживачам контролювати споживання енергії, брати участь у програмах управління попитом та вільно продавати надлишки енергії.

Важливо зазначити, що ефективність Smart Grid залежить не тільки від технологічного обладнання, але й від якості комунікаційної інфраструктури та безпеки обробки інформації.

Використання інформаційних технологій. Інформаційні технології є «нервовою системою» концепції Smart Grid. Вони забезпечують збір, передавання, обробку та аналіз величезного обсягу даних, який генерується мережею. Зокрема, такі технології, як Інтернет речей IoT, штучний інтелект AI та великі дані Big Data, дозволяють не просто збирати інформацію, а й використовувати її для:

– оптимізації режимів роботи обладнання;

– прогнозування пікових навантажень;

– планування ремонтних робіт;

– прогнозування виробництва від відновлюваних джерел енергії.

Використання таких технологій дозволяє забезпечити максимально ефективне, екологічне та економічно вигідне функціонування енергосистеми.

Переваги впровадження Smart Grid. Концепція Smart Grid відкриває перед енергетикою нові можливості, серед яких можна виділити три основні переваги:

– підвищення надійності енергопостачання — автоматизоване виявлення і локалізація аварій значно зменшує час простою;

– економічна ефективність — оптимізація розподілу навантажень дозволяє зменшити втрати енергії та витрати на обслуговування;

– екологічна сталість — інтеграція відновлюваних джерел сприяє зменшенню викидів вуглекислого газу.

Проблеми та виклики. Попри величезні перспективи, впровадження Smart Grid супроводжується низкою складних викликів:

– висока вартість впровадження — модернізація інфраструктури потребує значних капіталовкладень;

– необхідність зміни законодавчої бази — чинні нормативи часто не враховують нові моделі генерації та споживання енергії;

– проблеми сумісності — необхідна стандартизація протоколів обміну даними між різними виробниками обладнання;

– ризики кібербезпеки — цифровізація мереж робить їх потенційною мішенню для кібератак;

– опір користувачів — відсутність розуміння переваг Smart Grid серед кінцевих споживачів може гальмувати процес впровадження.

Аналітики вказують на те, що успішне вирішення цих проблем вимагає не тільки технічних інновацій, а й комплексних змін у стратегіях розвитку енергетики, бізнес-моделях операторів ринку, а також активної участі держави у стимулюванні цифровізації.

Перспективи впровадження Smart Grid в Україні. В Україні перші кроки до цифровізації енергетики вже зроблено: з'являються інтелектуальні лічильники, реалізуються пілотні проєкти з автоматизації підстанцій. Однак національна енергетична система залишається застарілою і потребує глибокої модернізації. Основними завданнями для реалізації Smart Grid в Україні є:

– розробка національної стратегії цифрової трансформації енергетики;

– стандартизація протоколів та обладнання;

– залучення інвестицій у модернізацію мереж;

– підвищення обізнаності споживачів та стимулювання участі у програмах розподілу попиту.

При належному підході Україна має всі шанси стати частиною глобального тренду переходу до «розумних» енергосистем, що дозволить не тільки підвищити енергоефективність, а й зміцнити енергетичну безпеку держави.

6.2. IoT-рішення в електроенергетиці

Сучасний розвиток електроенергетичної галузі тісно пов'язаний із використанням інноваційних технологій. Однією з таких революційних технологій є Інтернет речей IoT. Концепція IoT передбачає мережеве об'єднання великої

кількості фізичних об’єктів, які здатні взаємодіяти між собою та із зовнішнім середовищем через цифрові канали обміну даними. У контексті електроенергетики ця технологія дозволяє оптимізувати всі процеси — від виробництва до кінцевого споживання енергії, забезпечуючи вищу ефективність, надійність і стійкість енергетичних систем.

Роль IoT у сучасній електроенергетиці не можна переоцінити. Його застосування відкриває нові можливості для автоматизації моніторингу та управління інфраструктурою, зменшення втрат, підвищення якості обслуговування клієнтів і підтримки розвитку відновлюваних джерел енергії. Використання сенсорів, розумних лічильників, модулів збору даних та хмарних обчислювальних технологій забезпечує новий рівень прозорості і гнучкості в енергетичних системах (рис. 6.2).

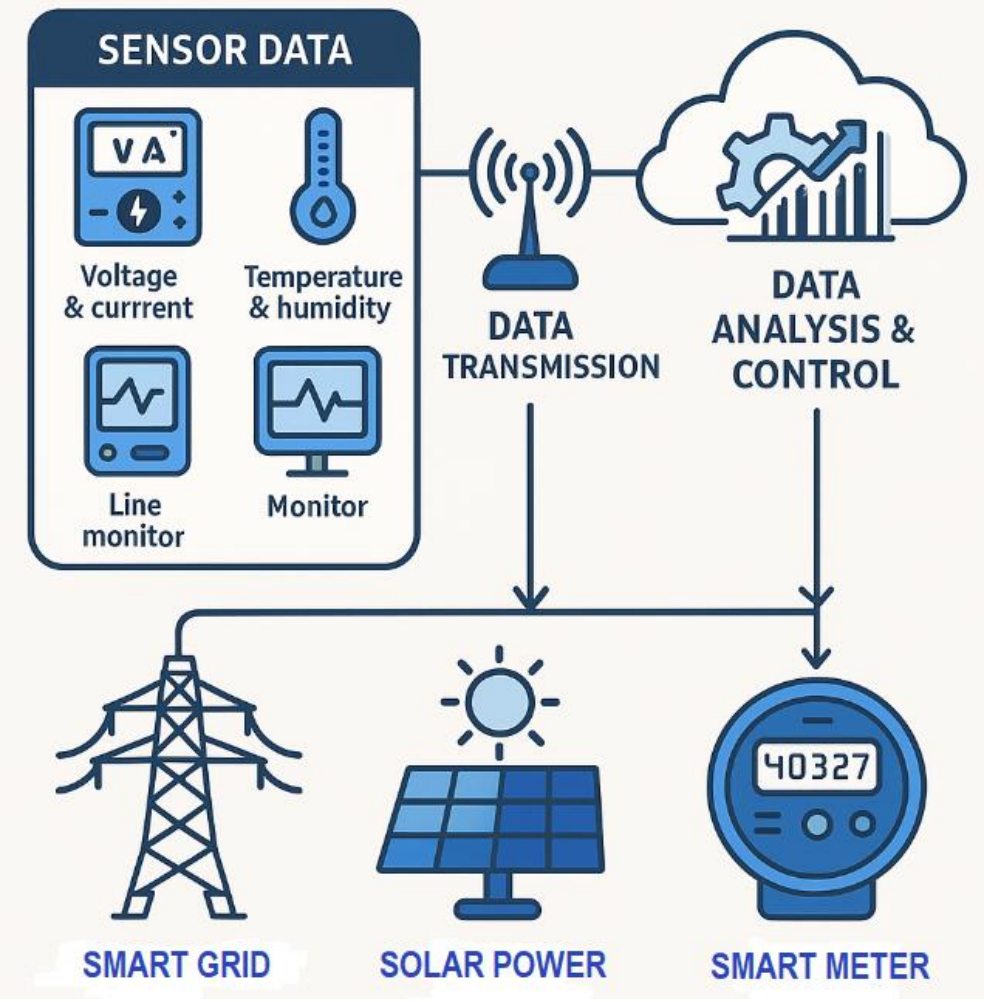

Рисунок 6.2 – IoT-рішення в електроенергетиці

Побудова IoT-рішень для енергетичної галузі базується на декількох рівнях:

1) Пристрої збору даних — сенсори, смарт-лічильники, контролери;

2) Мережа передачі даних — дротові або бездротові комунікаційні канали;

3) Платформи обробки даних — хмарні або локальні сервіси для аналізу великих обсягів інформації;

4) Інтерфейси користувача — панелі моніторингу, мобільні додатки, SCADA-системи.

Кожен з цих рівнів виконує критичну роль у забезпеченні безперервної роботи енергетичних систем, оптимізації виробничих процесів та швидкому реагуванні на зміни або аномалії.

Збір даних. На рівні збору даних IoT-технології застосовуються для безперервного моніторингу різноманітних параметрів: напруги, струму, частоти мережі, температури обладнання, вологості навколишнього середовища, рівня вібрації на механічних вузлах тощо. Отримані дані формують основу для подальшої обробки і прийняття рішень.

Передача даних. Передача даних від сенсорів до обробних платформ може здійснюватися через різні канали, залежно від вимог до швидкості, дальності та енергоспоживання. У енергетиці часто використовуються спеціалізовані протоколи, що забезпечують високу стійкість до завад і низький рівень затримки.

Аналітика і керування. Після надходження даних на аналітичні платформи відбувається їх обробка з використанням алгоритмів машинного навчання, штучного інтелекту або математичного моделювання. Це дозволяє не лише моніторити поточний стан систем, але й здійснювати прогнозування, виявляти аномалії, оцінювати ефективність роботи обладнання та планувати технічне обслуговування.

Основні напрями застосування IoT в енергетиці. IoT-рішення в електроенергетиці застосовуються у багатьох напрямах, кожен з яких сприяє підвищенню надійності та ефективності системи:

– моніторинг стану обладнання. Сенсори на генераторах, трансформаторах, лініях електропередач безперервно збирають дані про параметри їх роботи, виявляючи навіть найменші відхилення від норми;

– управління споживанням енергії. Розумні лічильники дозволяють споживачам і постачальникам енергії бачити реальне споживання, що сприяє економії ресурсів та впровадженню динамічного ціноутворення;

– оптимізація генерації та розподілу. Дані, що надходять від розподілених джерел енергії, дозволяють балансувати генерацію і споживання в режимі реального часу;

– інтеграція відновлюваних джерел енергії. IoT сприяє ефективному управлінню сонячними та вітровими електростанціями, де важливо оперативно реагувати на зміну погодних умов;

Спочатку застосування IoT у енергетиці обмежувалося простим збором і передачею даних. Однак із часом виникла потреба у більш складних функціях: автоматизованому аналізі, прогнозному обслуговуванні, активному управлінні енергоспоживанням.

Сьогодні IoT-рішення не лише інформують користувача, а й здатні самостійно приймати рішення на основі заданих сценаріїв або моделей прогнозування. З’явилися системи, що автоматично відключають обладнання при виявленні несправностей, перенаправляють потоки електроенергії для уникнення перевантаження ліній, або регулюють режим роботи об’єктів розподіленої генерації залежно від загального балансу мережі.

Попри очевидні переваги, розгортання IoT у енергетиці супроводжується низкою серйозних викликів:

– кібербезпека. Підвищення кількості підключених пристроїв збільшує потенційні вразливості системи. Забезпечення безпеки передачі даних та захисту пристроїв є критично важливим завданням.

– масштабованість. Необхідно забезпечити стабільну роботу великої кількості пристроїв навіть при різкому зростанні їх числа.

– інтероперабельність. Різні виробники використовують різні стандарти і протоколи, що ускладнює інтеграцію пристроїв в єдину систему.

Однією з важливих проблем є також питання стандартизації даних. Без єдиних стандартів для обміну інформацією важко забезпечити ефективну взаємодію різних систем.

Завдяки впровадженню IoT електроенергетичні системи стають набагато стійкішими до зовнішніх загроз та внутрішніх збоїв. IoT дозволяє:

– швидко виявляти та локалізувати аварії;

– ефективно управляти аварійними режимами;

– підвищувати ефективність відновлення систем після катастрофічних подій.

Ці переваги особливо важливі в умовах зміни клімату та зростання частоти екстремальних погодних явищ.

Очікується, що у найближче десятиліття роль IoT в енергетиці продовжить стрімко зростати. Інтеграція із штучним інтелектом та машинним навчанням відкриє нові можливості для автоматизації процесів, виявлення прихованих закономірностей у великих обсягах даних та прийняття обґрунтованих рішень у реальному часі.

Водночас розвиток 5G-мереж значно підвищить пропускну здатність і знизить затримки в обміні даними між пристроями, що дозволить ефективніше впроваджувати нові сервіси, такі як автономні енергетичні мікромережі чи «розумні міста» (Smart Cities).

Крім того, поява енергоефективних мікрочипів і сенсорів дозволить збільшити тривалість роботи IoT-пристроїв у польових умовах без необхідності частого обслуговування чи заміни батарей.

6.3. Хмарні сервіси та віртуальні енергетичні платформи

Сучасна енергетика стрімко трансформується під впливом цифрових технологій, серед яких особливу роль відіграють хмарні сервіси та віртуальні енергетичні платформи. Ці технології стають основою для побудови нових бізнес-

моделей, сприяють підвищенню гнучкості систем електропостачання, забезпечують оптимізацію управління енергетичними процесами. З огляду на глобальні виклики, пов'язані зі зростанням попиту на енергоресурси та необхідністю переходу до відновлюваних джерел енергії, впровадження цифрових інструментів набуває особливої актуальності.

Хмарні технології дозволяють енергетичним компаніям відмовитися від традиційних моделей обробки та зберігання даних, замінюючи їх на більш гнучкі, масштабовані рішення. Одночасно віртуальні платформи створюють можливості для інтеграції різноманітних джерел енергії, управління розподіленими ресурсами та формування нових форматів взаємодії між виробниками та споживачами.

Основи хмарних технологій в енергетиці. Хмарні сервіси (Cloud Services) передбачають надання обчислювальних ресурсів, сховищ даних, аналітичних інструментів і програмних рішень через інтернет. У контексті енергетики їх застосування відкриває доступ до потужних інструментів аналізу великих масивів даних, обробки інформації в реальному часі та автоматизації процесів управління.

Серед ключових переваг хмарних сервісів варто відзначити такі: гнучкість масштабування обчислювальних потужностей відповідно до потреб підприємства, зменшення капітальних витрат на розвиток власної IT-інфраструктури, спрощення доступу до інноваційних технологій без необхідності тривалого розгортання локальних систем.

Особливого значення набуває використання хмарних платформ для інтеграції даних із різних джерел: смарт-лічильників, сенсорів моніторингу енергомереж, розподілених енергетичних ресурсів. Завдяки цьому стає можливим комплексний аналіз енергоспоживання, прогнозування попиту та розробка оптимізованих стратегій керування енергією (рис. 6.3).

Одним із важливих аспектів є моделі надання хмарних сервісів, серед яких найпоширенішими є IaaS (Infrastructure as a Service), PaaS (Platform as a Service) та SaaS (Software as a Service). У енергетиці особливо актуальним є використання

PaaS і SaaS для розробки власних програмних рішень для управління енергетичними процесами.

Рисунок 6.3 – Взаємодія хмарних платформ і електроенергетичних систем

Концепція віртуальних енергетичних платформ. Віртуальні енергетичні платформи (Virtual Energy Platforms) — це комплексні цифрові системи, які дозволяють інтегрувати виробників, споживачів, операторів енергетичних ресурсів та постачальників послуг в єдиному цифровому середовищі. Вони об’єднують різні типи енергетичних активів — від традиційних електростанцій до розподілених джерел енергії — у єдину мережу з централізованим або децентралізованим управлінням.

Головною метою віртуальних платформ є створення гнучких, адаптивних систем енергопостачання, здатних швидко реагувати на зміну попиту,

інтегрувати відновлювані джерела енергії та забезпечувати високу ефективність роботи енергомережі.

Функціонал віртуальних платформ зазвичай включає: моніторинг стану енергетичних об'єктів у реальному часі, прогнозування виробництва та споживання енергії, автоматизацію процесів балансування навантажень, оптимізацію взаємодії з енергоринками.

Особливо перспективною є концепція віртуальних електростанцій VPP, які об'єднують безліч розподілених ресурсів — таких як сонячні панелі, вітряки, акумулятори — в єдину керовану мережу. Це дозволяє формувати новий формат участі в енергетичних ринках, підвищуючи доступність та ефективність використання енергії.

Аналітичний аспект застосування хмарних рішень. Один із найбільших потенціалів хмарних технологій у енергетиці полягає в аналітиці даних. Завдяки можливостям обробки великих обсягів інформації в реальному часі, хмарні платформи дозволяють здійснювати детальний аналіз споживання енергії, виявляти неефективності, прогнозувати попит та оптимізувати роботу обладнання.

Аналітичні моделі, що реалізуються на хмарних сервісах, можуть враховувати не лише технічні параметри роботи обладнання, а й зовнішні фактори — погодні умови, динаміку цін на енергоносії, поведінку споживачів. Це створює можливості для побудови більш точних прогнозних моделей, розробки адаптивних стратегій управління ресурсами.

Особливо важливою є інтеграція технологій машинного навчання (Machine Learning) та штучного інтелекту для автоматичного виявлення аномалій, оптимізації схем навантаження, розробки самонавчальних систем керування розподіленою генерацією.

Безпека та виклики при впровадженні хмарних рішень. Одним із ключових викликів для впровадження хмарних сервісів у енергетиці є забезпечення високого рівня інформаційної безпеки. Оскільки енергетичні дані мають критичне значення для національної безпеки, питання захисту інформації від кіберзагроз виходить на перший план.

Серед основних ризиків:

– можливість кібератак на інфраструктуру провайдерів хмарних послуг;

– загроза витоку конфіденційної інформації;

– ризики, пов’язані з недоступністю хмарних сервісів у разі технічних збоїв або кібератак.

Для мінімізації цих ризиків необхідне впровадження багаторівневих стратегій безпеки, серед яких особливу роль відіграють системи шифрування даних, багатофакторна автентифікація, використання приватних або гібридних хмар.

Перспективи розвитку хмарних сервісів та віртуальних платформ. У майбутньому розвиток хмарних технологій у сфері енергетики буде спрямований на ще більшу інтеграцію з технологіями Інтернету речей, штучного інтелекту та блокчейну. Це дозволить створювати повністю автоматизовані енергетичні системи, де обробка даних, прийняття рішень та керування ресурсами здійснюватимуться у реальному часі без прямого втручання людини.

Інтеграція хмарних платформ із технологіями блокчейн створює можливості для децентралізованого управління енергетичними ресурсами, забезпечуючи прозорість і безпеку транзакцій на енергетичних ринках. Це особливо важливо для розвитку локальних енергетичних спільнот і мікроринків.

Очікується також подальше розширення моделей співпраці у форматі «енергія як сервіс» (Energy-as-a-Service, EaaS), де споживачі отримуватимуть не просто енергію, а комплексні послуги з її оптимізації, управління та економії.

Впровадження хмарних сервісів та віртуальних енергетичних платформ відкриває нові горизонти для розвитку енергетичної галузі. Вони стають фундаментом для створення цифрової енергетики майбутнього, де ключовими характеристиками є гнучкість, ефективність, безпека і доступність. Водночас успішна реалізація цих технологій вимагає системного підходу до управління ризиками, розробки нових моделей бізнес-процесів і постійного вдосконалення цифрової інфраструктури.

Таким чином, хмарні сервіси та віртуальні платформи не просто змінюють технічні аспекти енергетики, а формують нову філософію управління енергією у XXI столітті.

6.4. Кібербезпека в інформаційних системах енергетики

У сучасному цифровому світі, де енергетичні підприємства дедалі частіше інтегрують цифрові технології, Інтернет речей (IoT), хмарні сервіси та SCADA-системи, питання кібербезпеки постає не як другорядна, а як ключова вимога до стабільності енергосистеми. Інформаційні системи в енергетиці (ІСЕ) є не лише інструментом автоматизації, а й критичною інфраструктурою, від якої залежать національна безпека, економіка та добробут населення. Їх захист — це не просто технічне завдання, а стратегічний виклик.

З кожним роком ІСЕ дедалі глибше інтегруються в енергетичну інфраструктуру — від лічильників у домогосподарствах до інтелектуальних електромереж, систем керування підстанціями, балансування навантаження, диспетчеризації. Така інтеграція призводить до того, що атака на енергосистему вже не обов'язково передбачає фізичну диверсію — достатньо лише порушити логіку обміну даними або вплинути на критичні вузли керування.

Цифрова трансформація, яка включає впровадження Smart Grid, IoT та хмарних сервісів, відкриває нові можливості для ефективності, однак вона ж створює численні вектори потенційного вторгнення. У 2022–2023 роках у світі фіксувалося зростання цільових атак на енергетичні компанії, при цьому більшість із них мали не лише економічну, а й геополітичну мотивацію.

Особливо вразливими є системи, які поєднують IT-інфраструктуру з оперативними технологіями (OT). Інтеграція SCADA з офісними мережами створює так звану «поверхню атаки» — простір, через який зловмисники можуть проникнути в критичну інфраструктуру.

*Основні види кіберзагроз для енергетичних інформаційних систем***.** Проблематика кібербезпеки в енергетиці охоплює широкий спектр ризиків (рис. 6.4).

Рисунок 6.4 – Кібербезпека в інформаційних системах енергетики

Від шкідливого програмного забезпечення до втручання у протоколи управління. Важливо розрізняти три рівні ризиків:

– операційні атаки, які впливають на працездатність обладнання (відключення підстанції, зміна параметрів навантаження);

– інформаційні атаки, що передбачають перехоплення або спотворення даних (підміна телеметрії, викривлення балансової інформації);

– інфраструктурні атаки, які блокують роботу мережі в цілому (DDoS-атаки, шифрування даних, саботаж комунікацій).

Серед найбільш поширених векторів атак:

– фішинг і соціальна інженерія — через електронну пошту та злам облікових записів персоналу;

– використання вразливостей у ПЗ SCADA-систем;

– несанкціонований доступ через віддалені з’єднання (VPN, RDP);

– шкідливі оновлення прошивок або драйверів контролерів.

Показовим є приклад атаки на енергосистему України у 2015–2016 роках, коли хакери змогли отримати доступ до системи диспетчеризації, викликати фізичне відключення електроенергії у кількох регіонах. Цей інцидент став першим підтвердженим випадком успішної кібератаки на енергомережу і засвідчив серйозність кіберзагроз.

Принципи забезпечення кібербезпеки в енергетиці. Надійна кібербезпека не обмежується встановленням антивірусного захисту. Йдеться про комплексну багаторівневу систему, яка включає інфраструктурні, організаційні, технологічні й правові аспекти. Ключові принципи:

– сегментація мереж. Розділення IT і OT-середовищ для уникнення неконтрольованого доступу;

– принцип мінімального доступу (Least Privilege). Кожен користувач або процес повинен мати лише ті права, які необхідні для виконання функцій;

– контроль автентичності та шифрування трафіку. Використання сертифікатів, VPN, протоколів TLS/SSL;

– періодичний аудит безпеки та тестування на проникнення. Імітація атак для виявлення слабких місць;

– навчання персоналу. Більшість атак розпочинаються з помилки людини.

Особливу увагу приділяють захисту каналів зв’язку між інтелектуальними пристроями (RTU, PLC, розумні лічильники) і центральними системами. Шифрування, багатофакторна автентифікація, цифрові підписи — усі ці елементи стають стандартом де-факто.

У сучасних системах безпеки використовуються як традиційні, так і новітні підходи до технологій та протоколів захисту. Зокрема:

– IDS/IPS (системи виявлення та запобігання вторгненням) — використовуються для моніторингу та реагування на аномальні дії в мережі;

– SIEM-системи — для збору, аналізу та кореляції подій безпеки в реальному часі;

– промислові протоколи з вбудованим захистом — такі як IEC 62351, який доповнює стандартні протоколи (Modbus, DNP3, IEC 60870) функціями шифрування, автентифікації, виявлення підміни.

Також активно впроваджуються блокчейн-рішення, особливо у розподілених енергетичних системах, для гарантування цілісності даних обліку. Ця технологія дозволяє захистити записи від модифікації навіть на рівні фізичного обладнання.

Забезпечення кібербезпеки в енергетиці не можливе без відповідної нормативної бази. В Україні функціонують такі документи та акти:

– Закон України «Про основні засади забезпечення кібербезпеки України» (2017);

– накази Держенергонагляду щодо вимог до безпеки SCADA/АСУ ТП;

– вимоги Національного банку до кіберстійкості критичних об’єктів інфраструктури;

– ISO/IEC 27001 — міжнародний стандарт управління інформаційною безпекою.

На підприємствах також впроваджуються політики кібербезпеки, які визначають відповідальність персоналу, структуру доступу до даних, правила реагування на інциденти.

Загалом організаційна складова має таку ж вагу, як і технічна. Навіть найдосконаліша система захисту буде вразливою, якщо немає чітко визначених процедур реагування, резервування, архівування та планування.

Попри численні технічні інструменти, галузь кібербезпеки стикається з низкою актуальних проблем та викликів:

– швидкість цифровізації випереджає темпи впровадження захисту. Багато підприємств впроваджують нові системи без відповідного аналізу кіберризиків;

– недостатня кваліфікація персоналу. У багатьох компаніях відсутні фахівці з ОТ-безпеки;

– складність у забезпеченні кіберстійкості старого обладнання, яке не підтримує сучасні протоколи захисту.

У перспективі дедалі більшого значення набувають системи машинного навчання, які зможуть автоматично виявляти аномалії поведінки пристроїв у реальному часі. Також посилюється увага до Zero Trust Architecture — концепції повної недовіри до будь-якого пристрою чи користувача до моменту повної перевірки.

Кібербезпека в енергетиці — це не статичний стан, а динамічний процес, що вимагає постійної адаптації. З огляду на стратегічне значення енергосистем, кожен елемент цифрової інфраструктури — від розумного лічильника до серверної ферми SCADA — має бути захищений як потенційна точка вторгнення.

Ефективна кібербезпека можлива лише при поєднанні технологій, чіткої регламентації, кваліфікованого персоналу та культури безпеки. В умовах гібридних загроз енергетична стабільність країни напряму залежить від здатності енергетичних компаній впроваджувати найкращі практики захисту.

6.5. Тенденції розвитку та цифрова трансформація

Цифрова трансформація в енергетичному секторі є не просто модернізацією існуючих технологій, а радикальною зміною способів виробництва, розподілу, управління та споживання енергії. Під впливом інноваційних рішень, нових бізнес-моделей та глобальних викликів, галузь енергетики поступово перетворюється на складну, динамічну систему, у центрі якої — дані, автоматизація та взаємодія з користувачами. Це перетворення називають цифровою трансформацією, і воно охоплює всі рівні функціонування енергетичних підприємств — від виробництва до комерційного обліку та взаємодії з кінцевими споживачами.

Поштовхом до цифрових перетворень стали як технологічні досягнення (IoT, великі дані, штучний інтелект, хмарні обчислення), так і соціально-економічні обставини — зростаючий попит на чисту енергію, потреба у зниженні викидів вуглецю, підвищення енергоефективності та вимоги до прозорості у

взаєминах із користувачем. Енергетика перетворюється з вертикально інтегрованої структури у більш децентралізовану, адаптивну мережу.

Цифровізація дозволяє зробити енергосистеми більш чутливими до змін у режимах роботи, швидше реагувати на аварійні ситуації, забезпечити гнучке управління попитом, інтеграцію відновлюваних джерел енергії, а також розвиток нових послуг — таких як віртуальні електростанції, peer-to-peer торгівля енергією або предиктивне технічне обслуговування.

Основні напрями цифрової трансформації (рис. 6.5). Одним із ключових елементів трансформації є перехід від реактивної до проактивної моделі управління, яка базується на аналітиці даних у реальному часі. Підприємства енергетики дедалі активніше використовують цифрові близнюки (digital twins) — віртуальні моделі об’єктів або процесів, що дозволяють тестувати сценарії без фізичного втручання.

Рисунок 6.5 – Цифрова трансформація в електроенергетиці

Також активно розвивається концепція інтелектуального управління активами, де за допомогою IoT-датчиків та алгоритмів машинного навчання забезпечується прогнозування технічних збоїв, оптимізація термінів обслуговування, а також зниження втрат електроенергії.

Ще одним напрямом є цифровізація взаємодії із клієнтами. Завдяки мобільним додаткам, онлайн-кабінетам та платформам на базі штучного інтелекту, споживачі можуть не лише отримувати рахунки або подавати показники, а й бачити свою енергетичну поведінку, прогнозувати витрати, брати участь у програмах економії та навіть продавати надлишки енергії у мережу.

Роль великих даних та аналітики. Центральним компонентом цифрової трансформації в енергетиці стає аналітика великих даних (Big Data Analytics). Потоки даних, що надходять із тисяч пристроїв обліку, станцій керування, систем SCADA та IoT-сенсорів, аналізуються для виявлення трендів, аномалій, оптимальних режимів функціонування.

Аналітика дозволяє виявляти неочевидні закономірності у роботі обладнання, ефективніше керувати балансом навантаження, оптимізувати виробничі цикли або прогнозувати пік попиту. Застосування машинного навчання та алгоритмів штучного інтелекту в цьому процесі дозволяє створювати автоматизовані системи прийняття рішень, що суттєво зменшують роль людського фактора та ризик помилок.

Віртуалізація та нові бізнес-моделі. Паралельно з розвитком технологій змінюється й сама структура ринку електроенергії. На зміну традиційній централізованій моделі приходять віртуальні електростанції, агрегатори попиту та децентралізовані енергетичні платформи.

Віртуальна електростанція (Virtual Power Plant, VPP) — це сукупність розподілених генеруючих потужностей (сонячні панелі, вітрові турбіни, акумулятори), які координуються як єдиний об’єкт за допомогою цифрових технологій. Це дозволяє зменшити навантаження на мережу, забезпечити стабільність системи, а також надати нові послуги для учасників ринку.

Такі моделі функціонування неможливі без високого рівня цифрової інтеграції, стандартизації протоколів обміну даними, кіберзахисту та застосування блокчейн-технологій для прозорості та довіри між учасниками.

Інтеграція з іншими секторами та технологіями. Цифрова трансформація в енергетиці тісно пов’язана з розвитком суміжних секторів, таких як транспорт,

будівництво та промисловість. Наприклад, електромобілі — це не лише споживачі, а й потенційні енергетичні активи. Концепція V2G (Vehicle-to-Grid) дозволяє використовувати акумулятори авто для балансування навантаження в мережі. Це відкриває нові перспективи для взаємодії між енергетикою і мобільністю.

Водночас автоматизація будівель (smart buildings), які використовують інтелектуальні системи кліматичного контролю, освітлення та вентиляції, інтегрується з платформами енергетичного менеджменту. Завдяки цьому можливо адаптивно змінювати режими роботи обладнання залежно від тарифів, наявності генерації з ВДЕ або рівня навантаження в мережі.

Вплив цифровізації на політику та регуляцію. Цифрова трансформація також вимагає змін у нормативно-правовій базі. Виникає потреба у нових стандартах обміну даними, визначеннях відповідальності сторін, правилах кіберзахисту та сертифікації програмного забезпечення. Регулятори мають адаптуватися до умов, коли інформація стає основним активом, а швидкість реагування систем — критичним чинником безпеки.

Особливої уваги потребує регулювання в частині конфіденційності персональних даних, що збираються з пристроїв обліку або мобільних застосунків. Важливо забезпечити прозорість процедур, права користувача на доступ і видалення своїх даних, а також можливість перевірки дій енергопостачальників.

Попри очевидні переваги, процес цифровізації супроводжується низкою викликів. Найбільш значущими з них є:

– кібербезпека — кожен новий інтерфейс чи пристрій, підключений до мережі, потенційно може стати точкою вразливості. Захист критичної інфраструктури потребує не лише технологічних рішень, але й ретельної стратегії реагування, підготовки персоналу, тестування та відновлення;

– несумісність систем — на багатьох підприємствах досі функціонують застарілі інформаційні системи або обладнання, не здатне підтримувати сучасні цифрові протоколи. Інтеграція таких платформ вимагає додаткових витрат на модернізацію або створення проміжного програмного забезпечення;

– кадрова підготовка — перехід до цифрових технологій змінює вимоги до працівників. Потрібні фахівці, які не лише розуміють енергетику, а й володіють навичками роботи з IT-системами, аналітикою, кібербезпекою. Це вимагає нових програм навчання, перепідготовки кадрів і переосмислення професійних стандартів.

У середньостроковій перспективі цифрова трансформація призведе до появи розумних енергетичних екосистем, де всі учасники взаємодіють у реальному часі на базі прозорих правил, автоматизованих процесів та захищених платформ. Виробники, споживачі, оператори системи передачі, рітейлери та навіть побутові користувачі зможуть спільно створювати цінність за рахунок обміну даними, енергією та послугами.

Країни Європейського Союзу вже зараз реалізують стратегії Digital Energy, в яких пріоритетами є децентралізація, інтеграція ВДЕ, мобільність та прозорість. Україна, в контексті інтеграції до ENTSO-E та виконання Угоди про асоціацію з ЄС, також бере курс на цифровізацію галузі, зокрема через розвиток АСКОЕ, впровадження систем енергетичного менеджменту, реформу ринку електроенергії.

Висновки до розділу 6

У шостому розділі навчального посібника проаналізовано сучасні інформаційні технології, які трансформують підходи до управління, моніторингу та оптимізації енергетичних процесів. У межах цього розділу було розглянуто широкий спектр концепцій, інструментів і технологій, що забезпечують перехід енергетичної галузі до нового етапу — цифрової, адаптивної та інтерактивної інфраструктури, зорієнтованої на ефективність, надійність і сталий розвиток.

Розглянуті питання які, стосуються концепції Smart Grid, окреслено фундаментальні засади побудови інтелектуальних електричних мереж, здатних до саморегуляції, двостороннього обміну енергією, інтеграції розподілених джерел та гнучкого управління попитом. Було акцентовано увагу на багаторівневій архітектурі, включаючи сенсорні системи, мережеві протоколи, аналітичні

платформи та інтерфейси з користувачами. Ці аспекти формують уявлення про ключові структурні елементи сучасної енергетичної системи.

Підкреслено роль Інтернету речей як платформи, що об'єднує фізичні пристрої, канали передачі даних, аналітичні сервіси й користувацькі інтерфейси. Увага приділена багаторівневій організації таких систем — від збору даних до автоматизованого управління. Окреслено напрямки застосування IoT: моніторинг обладнання, оптимізація генерації, управління споживанням і підтримка інтеграції ВДЕ. Також було визначено виклики, пов'язані з масштабованістю, безпекою, стандартизацією та інтероперабельністю.

Також було розглянуто хмарні сервіси та віртуальні енергетичні платформи як рушійні сили нових моделей керування енергетичними процесами. Було показано, як хмарні технології дозволяють масштабувати обчислювальні ресурси, інтегрувати дані з різних джерел, забезпечувати аналітику у реальному часі та підтримувати рішення на основі штучного інтелекту. Віртуальні платформи, зокрема концепція віртуальних електростанцій, розкривають потенціал координації розподілених ресурсів, забезпечення балансування та адаптивності ринку. Увага також приділялася безпековим аспектам впровадження хмарних рішень і необхідності використання гібридних моделей обробки даних.

При розгляді питань кібербезпеки в умовах цифровізації енергетичних систем було проаналізовано загрози для інформаційних систем енергетики, включаючи атаки на SCADA, IoT, комунікаційні платформи та корпоративні мережі. Розділ систематизував типи ризиків — від інформаційних до інфраструктурних — і вказав на необхідність впровадження комплексного багаторівневого захисту. Підкреслено важливість нормативного супроводу, національних стандартів, політик безпеки та навчання персоналу. Таким чином, безпека розглядається як невіддільна складова цифрової стратегії в енергетиці.

Розкрито ключові тенденції цифрової трансформації енергетики. Було визначено, що цифровізація — це не просто оновлення технічної бази, а фундаментальна зміна логіки функціонування галузі: перехід до проактивного управління, розширення ролі споживача, зростання значення аналітики даних і

віртуальних рішень. Особливий акцент зроблено на інтеграції міжсекторальних рішень (транспорт, будівництво, житлово-комунальна сфера) та формуванні нових бізнес-моделей. Також розглянуто проблеми несумісності, кадрового забезпечення, кіберризиків і нормативних бар'єрів.

Таким чином, шостий розділ формує глибоке розуміння цифрової трансформації в енергетиці як багатовимірного процесу, що охоплює технології, інфраструктуру, безпеку, бізнес і користувача. Практичне засвоєння цих знань дозволяє майбутнім фахівцям ефективно впроваджувати новітні інформаційні технології у всі сегменти енергетичної системи, формуючи її стійкість, ефективність і готовність до викликів майбутнього.

Запитання для контролю знань за шостим розділом

1. Які ключові технології трансформують сучасну енергетичну галузь у напрямку цифровізації?
2. Що таке Smart Grid і які її основні характеристики?
3. Як багато рівнів архітектури включає концепція Smart Grid?
4. Яку роль у Smart Grid відіграють сенсорні системи та мережеві протоколи?
5. Як забезпечується двосторонній обмін енергією в сучасних енергетичних мережах?
6. Які функції виконує Інтернет речей у сфері електроенергетики?
7. Які основні компоненти формують IoT-систему в енергетиці?
8. У яких напрямах електроенергетики застосовується IoT?
9. Які виклики виникають при впровадженні IoT у великих енергосистемах?
10. Які можливості надають хмарні технології в управлінні енергетичними процесами?
11. У чому полягає суть концепції віртуальної електростанції?
12. Які переваги забезпечує використання гібридних моделей хмарних обчислень?

13. Які загрози для енергетичних інформаційних систем виділяються в умовах цифровізації?

14. Які об’єкти найчастіше стають мішенню кіберзагроз в енергетиці?

15. Чому важливо дотримуватись стандартів та політик безпеки в енергосистемах?

16. Які складові включає багаторівневий підхід до забезпечення кібербезпеки?

17. Які зміни в управлінні енергетикою зумовлені цифровою трансформацією?

18. Як цифровізація впливає на роль споживача в енергетичній системі?

19. Які міжсекторальні рішення інтегруються в сучасну енергетичну інфраструктуру?

20. Які бар’єри гальмують цифрову трансформацію енергетики, і як їх можна подолати?

7. ПРОЄКТУВАННЯ СИСТЕМ ПЕРЕДАЧІ ІНФОРМАЦІЇ

Проєктування систем передачі інформації в енергетиці потребує ґрунтовного аналізу вимог до таких систем на всіх рівнях їх функціонування. Початковий етап створення будь-якої телекомунікаційної чи інформаційної системи передбачає визначення технічних, функціональних, організаційних та нормативних аспектів, які будуть впливати на архітектуру, вибір технологій і методів реалізації. У галузі енергетики, де значна кількість рішень приймається автоматично на основі переданих даних, ці вимоги набувають особливої ваги. Надійність, точність, безперебійність передачі інформації є не лише технічними пріоритетами, а й питанням безпеки критичної інфраструктури.

7.1. Аналіз вимог до систем

Аналіз вимог до СПІ передбачає поетапне вивчення таких ключових компонентів: характеристики джерел і споживачів інформації, типи передавальних даних, частота передачі, вимоги до часу реакції, ступінь доступності, вимоги до масштабування, безпеки та взаємодії з іншими системами (рис. 7.1).

Рисунок 7.1 – Аналіз вимог до систем передачі інформації

Особливість СПІ в енергетиці полягає в тому, що передані дані не є ізольованими — вони постійно впливають на прийняття рішень у режимі реального часу. Це стосується систем диспетчерського управління (наприклад, SCADA), автоматизованих систем комерційного обліку електроенергії (АСКОЕ), захисту та автоматики, а також взаємодії з розподіленими джерелами енергії. Кожна з цих підсистем висуває свої специфічні вимоги до каналів передачі даних.

Узагальнений аналіз вимог можна умовно поділити на три блоки: функціональні, нефункціональні та зовнішні вимоги. Функціональні стосуються безпосередньо тих операцій, які має підтримувати система, нефункціональні — якості цих функцій, а зовнішні — впливу регуляторного, інфраструктурного чи технологічного середовища.

Функціональні вимоги формуються на основі завдань, які має вирішувати система. У контексті енергетики це, зокрема:

– передача технологічної інформації з віддалених об’єктів (підстанцій, генераторів, розподільчих пунктів) у центр управління;

– збір даних з АСКОЕ для розрахунків, аналітики та виставлення рахунків;

– передача команд від диспетчерів на виконавчі механізми;

– забезпечення доступу до даних для аналітичних і планувальних систем підприємства.

Ці вимоги передбачають високу точність переданих сигналів, захист від спотворення або втрати даних, а також синхронізацію подій за часовими мітками.

Серед нефункціональних вимог домінують такі характеристики:

– надійність — система повинна мати мінімальний рівень відмов, можливість резервування каналів зв’язку і миттєвого перемикання у разі збоїв;

– затримка передачі — критично важлива для реального часу. В системах оперативного управління затримка не повинна перевищувати 100 мс, а для деяких реле захисту — й менше;

– пропускна здатність — залежить від кількості каналів, обсягу переданих даних та частоти запитів. Наприклад, для відеоспостереження або систем

машинного зору (які також інтегруються з енергетичними системами) потрібна значно вища пропускна здатність, ніж для SCADA;

– масштабованість — можливість адаптувати систему до зростаючих вимог без повного її переоснащення. Це особливо важливо у зв'язку з розвитком розподіленої генерації та «розумних» електромереж (Smart Grid).

Вимоги до СПІ значною мірою формуються архітектурою системи. У випадку централізованих систем, навантаження концентрується в центральному вузлі, що потребує високої продуктивності серверної частини. У децентралізованих (наприклад, peer-to-peer) системах основна вимога — узгоджена робота вузлів та механізми синхронізації. Сучасні тенденції підтримують гібридну архітектуру — з елементами обробки даних як на периферії (edge computing), так і в хмарних сервісах, що дозволяє зменшити затримки, оптимізувати пропускну здатність та підвищити надійність.

СПІ не функціонують у вакуумі. Усі енергетичні підприємства мають внутрішні IT-системи: ERP, CRM, фінансові платформи, облікові системи персоналу тощо. Системи передачі даних повинні бути інтегровані з ними, або, як мінімум, мати можливість обміну даними за допомогою API чи стандартів інтероперабельності (наприклад, IEC 61850, DLMS/COSEM). Ця взаємодія також вимагає визначення вимог до форматів даних, швидкості їх передачі, а також захисту при міжсистемному обміні.

Захист даних під час передачі є одним із ключових аспектів. Аналіз вимог до безпеки охоплює:

– аутентифікацію пристроїв та користувачів;

– шифрування даних;

– протидію зовнішнім атакам (наприклад, перехоплення, підміна, DDoS);

– захист від внутрішніх загроз, включно з помилками персоналу.

Зростання інтересу до кібербезпеки в енергетиці змушує розробників СПІ орієнтуватися на стандарти, що встановлюють вимоги до інформаційної безпеки інфраструктури, зокрема ISO/IEC 27001, IEC 62351, NERC CIP.

Процес аналізу вимог до СПІ включає кілька етапів:

– вивчення бізнес-процесів підприємства, які потребують автоматизації або передачі даних;

– інвентаризація наявного обладнання та IT-інфраструктури, що може бути інтегроване в нову систему;

– визначення очікувань користувачів, тобто диспетчерів, інженерів, фінансових аналітиків, керівництва;

– оцінка середовища експлуатації — від географічного положення до температурних умов та рівня доступу до інтернету;

– формування технічного завдання (ТЗ), в якому конкретизуються всі типи вимог, строки реалізації, фінансові обмеження, очікувані ризики.

Із розвитком концепцій Smart Grid, Industrial IoT, машинного навчання, змінюються і вимоги до систем передачі даних. З'являються нові сценарії використання: попереджувальна діагностика, гнучке керування навантаженням, інтеграція споживачів у процес балансування енергосистеми. Для таких задач традиційні підходи вже не є достатніми.

Відповідно, сучасні СПІ мають враховувати:

– низьке енергоспоживання (важливо для пристроїв на віддалених об'єктах);

– застосування бездротових технологій (LoRaWAN, NB-IoT, Zigbee) для швидкої побудови;

– інтелектуальну маршрутизацію та динамічну адаптацію маршрутів зв'язку;

– сумісність з хмарними сервісами для аналізу великих обсягів даних.

Таким чином, сучасні системи передачі інформації в енергетиці повинні бути не лише технічно досконалими та здатними ефективно виконувати поставлені завдання відповідно до актуальних вимог, але й мати потенціал до подальшого розвитку та масштабування. Вони мають бути достатньо гнучкими, щоб швидко адаптуватися до нових викликів, зумовлених технологічним прогресом, змінами нормативного середовища, зростаючими вимогами до безпеки та

надійності, а також еволюцією архітектури енергетичних систем у напрямку цифровізації, децентралізації та інтеграції ВДЕ.

7.2. Розробка технічного завдання

Розробка технічного завдання (ТЗ) є ключовим етапом у процесі створення систем передачі інформації, зокрема в галузі енергетики, де будь-які збої в обміні даними можуть призвести до значних втрат або порушення стабільності енергосистеми. ТЗ — це документ, що визначає вимоги замовника до проєкту, включаючи його функціональні, технічні, організаційні та інші характеристики. Саме на основі ТЗ відбувається подальше проєктування, реалізація та приймання інформаційної системи в експлуатацію.

Ретельно складене технічне завдання забезпечує узгоджене розуміння очікувань між усіма учасниками проєкту: замовниками, розробниками, технічними консультантами та підрядниками. Його наявність дозволяє уникнути двозначностей у процесі розробки, прискорює ухвалення рішень, забезпечує нормативну основу для проведення тестування та введення системи в експлуатацію (рис. 7.2).

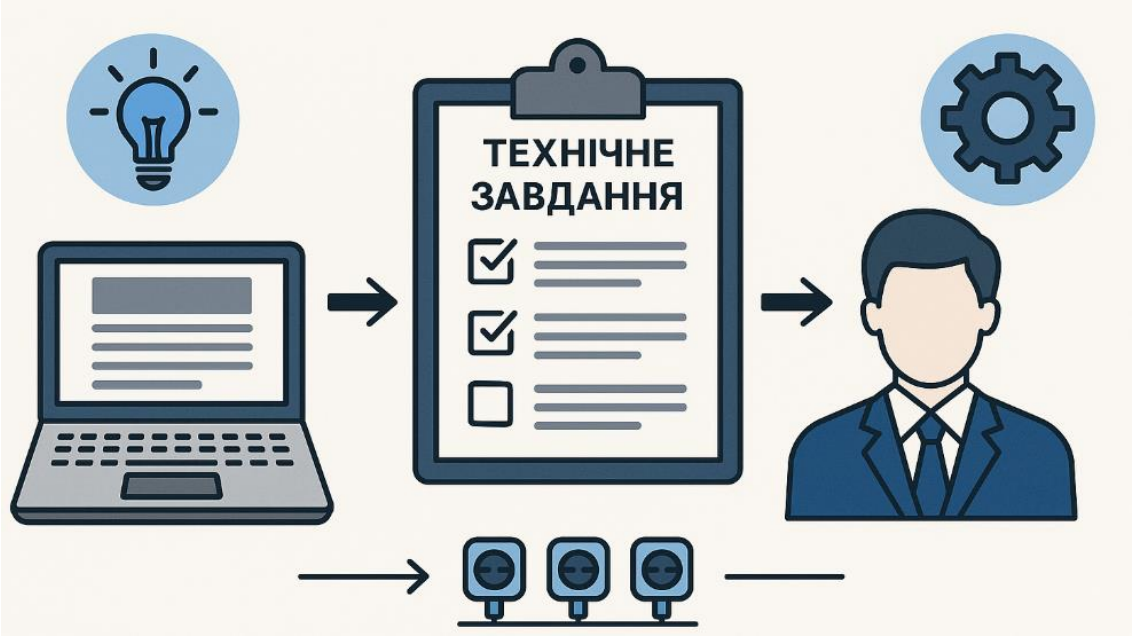

Рисунок 7.2 – Розробка технічного завдання

Зокрема, у сфері передачі інформації в енергетиці технічне завдання повинно враховувати як особливості цифрової інфраструктури підприємства, так і

вимоги з безпеки, надійності, відмовостійкості й масштабованості. Слід враховувати як чинні галузеві стандарти, так і перспективи подальшої цифровізації підприємства.

Підготовка технічного завдання передбачає багатоступеневу роботу, яка включає:

– аналіз потреб і обмежень замовника. Збирання інформації щодо існуючої інфраструктури, наявних ІТ-систем, каналів передачі даних, рівня автоматизації та цілей модернізації;

– формалізація функціональних вимог. Визначення того, яку саме інформацію має передавати система, з якою частотою, затримкою, рівнем точності та безпеки;

– технічне структурування вимог. Встановлення типу необхідних компонентів, технологій зв'язку, програмного забезпечення, стандартів протоколів, інтерфейсів та вимог до резервування;

– узгодження юридичних та нормативних аспектів. Технічне завдання повинне враховувати національні регламенти, стандарти ISO/IEC, правила кібербезпеки, а також внутрішні регламенти підприємства [26, 27].

Згідно з ДСТУ (Державними стандартами України) та міжнародними аналогами, структура технічного завдання повинна бути чітко визначеною, щоб забезпечити повноту опису і логічну послідовність. Типова структура ТЗ для системи передачі даних в енергетиці може містити такі розділи:

– вступ. Короткий опис проєкту, обґрунтування розробки;

– цілі та завдання. Що має досягти система після впровадження;

– технічні вимоги. Параметри передачі даних, інтерфейси, архітектура;

– програмне забезпечення. Платформи, мови програмування, взаємодія з іншими системами;

– безпека. Вимоги до шифрування, ідентифікації користувачів, резервного копіювання;

– етапи реалізації. Календарне планування, етапи приймання, критерії завершення;

– вимоги до експлуатації. Обслуговування, навчання персоналу, супровід.

Зазвичай розділ «Технічні вимоги» є найоб'ємнішим і вимагає міждисциплінарної участі — від ІТ-фахівців до енергетиків, які можуть описати специфіку енергетичних процесів, що потребують передачі інформації.

Розробка технічного завдання може стикатися з низкою труднощів. По-перше, замовник не завжди володіє повною картиною своєї інфраструктури, особливо якщо вона має гібридну структуру або включає застаріле обладнання. По-друге, розробники можуть недостатньо глибоко розуміти галузеву специфіку, що призводить до формального підходу до опису вимог.

Ще однією проблемою є часта зміна вимог у процесі реалізації, що свідчить про недостатньо чітке початкове формулювання потреб. Для цього важливо передбачити в ТЗ механізм контролю змін — тобто порядок, за яким нові вимоги вносяться до проєкту, а їх реалізація документується.

Також варто врахувати ризики, пов'язані з зовнішніми технологічними змінами — наприклад, з переходом на нові стандарти передачі даних або зміну нормативного регулювання. Якісне ТЗ має бути достатньо гнучким для адаптації до змін без необхідності повного перепроєктування системи.

Залежно від того, яка саме система передбачена до впровадження — локальна LAN, регіональна WAN, бездротова (RF, LTE), або побудована на базі IoT — технічне завдання буде відрізнятись. У випадку з розгалуженими промисловими системами, часто необхідно деталізувати взаємодію між польовими пристроями (датчиками, лічильниками), контролерами та центральним вузлом обробки.

Особливо важливо звертати увагу:

– на топологію мережі (радіальна, магістральна, кільцева тощо);
– на тип носія інформації (оптоволокно, радіоканал, Ethernet);
– на вимоги до швидкості обміну, затримок і допустимих втрат даних;
– на надійність (середній час безвідмовної роботи компонентів);
– на енергоспоживання та стійкість до зовнішніх впливів.

Ці параметри напряму впливають на вибір обладнання, підходів до маршрутизації, а також алгоритмів відновлення системи у разі аварійних ситуацій.

Підхід до уніфікації технічних завдань у великих енергетичних компаніях. Для великих організацій доцільно формувати уніфіковані шаблони технічних завдань. Це дозволяє стандартизувати вимоги до систем передачі даних, забезпечити узгодженість проєктів у різних підрозділах та полегшити технічний аудит.

У таких випадках застосовуються системи управління вимогами (Requirements Management Systems), які дозволяють централізовано зберігати, оновлювати та контролювати всі ТЗ, забезпечуючи простежуваність змін і відповідність стандартам ISO 9001 або IEC 61508.

Крім того, сучасні методології, зокрема Agile-підходи, частково адаптовані й до інженерних проєктів, хоча в енергетиці вони застосовуються обмежено. Більш релевантною тут є каскадна (Waterfall) модель, де технічне завдання формується на початковому етапі й лишається основним орієнтиром до завершення проєкту.

7.3. Етапи проєктування та монтажу

Проєктування та монтаж систем передачі інформації в енергетичних об’єктах — це складний, багатоетапний процес, що вимагає ретельного дотримання норм, стандартів та логічної послідовності дій. Розробка ефективної інфраструктури для збору, обробки та передачі даних у сучасних системах автоматизованого обліку та контролю енергоресурсів (АСКОЕ) є критичним фактором забезпечення безперебійного та надійного функціонування енергетичного підприємства.

Основна мета цього підрозділу — розглянути ключові етапи проєктування та монтажу систем передачі інформації, що інтегруються в енергетичну інфраструктуру, включаючи як високорівневі системи керування, так і нижній рівень вимірювання та збору даних (рис. 7.3).

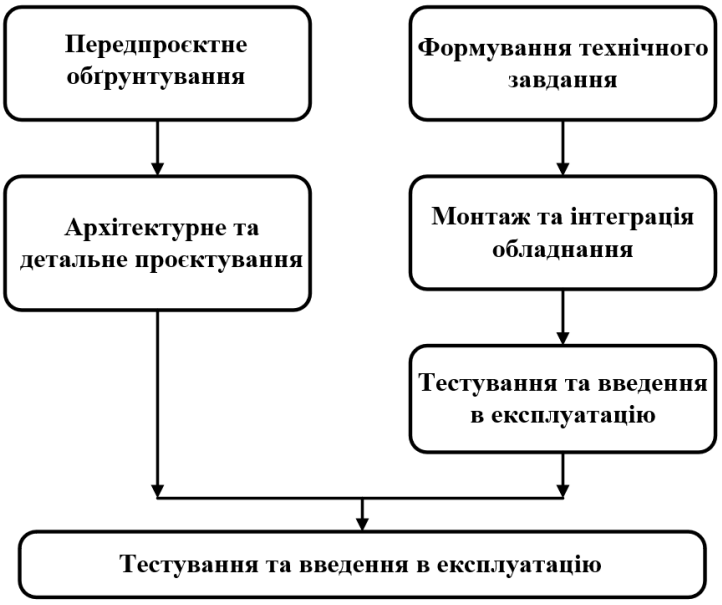

Рисунок 7.3 – Етапи проєктування та монтажу

Розберемо всі етапи по черзі:

1) *Передпроєктне обґрунтування та техніко-економічна оцінка.* Успішне впровадження будь-якої інформаційної системи починається з передпроєктного аналізу. Це період, коли замовник разом із проєктувальниками визначає ключові задачі, проблеми та технічні потреби. Ретельна оцінка наявної інфраструктури дозволяє уникнути помилок на подальших етапах і забезпечити оптимальне співвідношення між вартістю, функціональністю та надійністю системи. У межах цього етапу аналізується:

– поточний стан інформаційної інфраструктури (наявність каналів зв’язку, типи використовуваних лічильників, серверні потужності);

– наявність попередніх систем обліку або моніторингу;

– організаційні потреби підприємства (наприклад, потреба в дистанційному доступі до даних, інтеграції з ERP, CRM чи SCADA);

– нормативні вимоги та галузеві регламенти, які мають бути враховані під час розробки проєкту.

Техніко-економічне обґрунтування (ТЕО) на цьому етапі виконує ключову функцію: воно дозволяє порівняти кілька варіантів технічних рішень, обрати оптимальний і передбачити терміни окупності інвестицій.

2) *Формування технічного завдання*. На основі зібраної аналітичної інформації складається технічне завдання. Воно є базовим документом для подальшого проєктування. У ТЗ фіксується повний перелік вимог до майбутньої системи: обсяг функціональності, архітектура, типи обладнання, вимоги до безпеки, взаємодія з іншими системами підприємства, умови експлуатації тощо.

Цей документ погоджується з усіма зацікавленими сторонами — інженерною службою, ІТ-відділом, керівництвом підприємства, постачальниками рішень. Правильно сформоване ТЗ значно знижує ризики невідповідності очікувань результатам реалізації.

3) *Архітектурне проєктування та вибір технологій*. Архітектурне проєктування передбачає побудову логічної структури майбутньої системи. Визначаються всі ключові елементи — вузли збору даних (інтелектуальні лічильники, датчики, контролери), засоби комунікації (дротові чи бездротові канали), серверна інфраструктура та системи збереження й візуалізації інформації. На цьому етапі критично важливим є вибір технологій передачі даних. Залежно від типу об’єкта та умов експлуатації можуть застосовуватись:

– провідні рішення (Ethernet, RS-485, Modbus);
– бездротові протоколи (LoRaWAN, ZigBee, NB-IoT);
– мобільний зв’язок (2G/3G/4G/5G з використанням VPN);
– комбіновані технології (гібридні мережі).

Кожна технологія має свої переваги й обмеження, які повинні бути оцінені в контексті надійності, енергоефективності, захищеності та вартості реалізації.

4) *Детальне проєктування.* Кожна деталь узгоджується з нормативними вимогами (ДСТУ, ISO, IEC) і враховує особливості об’єкта (промислове підприємство, житловий будинок, інфраструктурний вузол тощо). Також проєктується резервна система живлення, яка дозволить зберегти працездатність елементів збору й передачі даних у разі аварійного знеструмлення. На цьому етапі розробляються:

– технічні креслення прокладання кабельних трас;
– схеми підключення обладнання;

– специфікації та кошториси;

– розрахунки навантажень;

– вимоги до пожежної безпеки та заземлення;

– інструкції з інсталяції.

5) *Підготовка об'єкта до монтажу*. Монтаж системи передбачає не лише встановлення обладнання, а й підготовку відповідної інфраструктури. Це може включати:

– облаштування технічних приміщень (серверних, шаф, стійок);

– забезпечення вентиляції та кліматичного контролю;

– прокладання каналів зв'язку (використання існуючих кабельних лотків або встановлення нових);

– фізичну охорону обладнання (сигналізація, замки, відеоспостереження).

Підготовка виконується з урахуванням вимог електробезпеки, стандартів монтажу слабкострумових систем і рекомендованих практик.

6) *Монтаж та інтеграція обладнання*. Інтеграція з іншими системами підприємства — обов'язковий компонент. Система повинна коректно передавати дані в ERP, SCADA, системи енергетичного моніторингу або бухгалтерського обліку. Усі дії фіксуються в технічній документації та супроводжуються перевіркою на відповідність ТЗ. Процес інсталяції системи включає встановлення та підключення:

– розумних лічильників;

– контролерів збору даних;

– маршрутизаторів і шлюзів;

– серверів або хмарних клієнтів;

– програмного забезпечення.

7) *Тестування та налаштування*. Після монтажу виконується комплексне тестування всієї інфраструктури. Воно охоплює:

– перевірку працездатності всіх вузлів;

– тестування каналів зв'язку на надійність та швидкість;

– перевірку безпеки (включаючи VPN, firewall, автентифікацію);

– перевірку точності збору й обробки даних;

– навантажувальні випробування.

За результатами тестування виконується налагодження системи, зокрема — калібрування лічильників, оптимізація протоколів передачі даних, встановлення автоматичних процедур резервного копіювання, налаштування сповіщень та подій.

8) *Навчання персоналу та введення в експлуатацію*. Успішне функціонування системи залежить не лише від техніки, але й від того, наскільки персонал підприємства вміє з нею працювати. Тому проєкт передбачає:

– підготовку інструкцій користувача та технічної документації;

– навчання інженерного складу (обслуговування, діагностика, усунення несправностей);

– навчання операторів (інтерпретація даних, реагування на інциденти, звітність);

– супровід під час перших місяців експлуатації.

Після завершення навчання система офіційно вводиться в експлуатацію, складається акт приймання-передачі.

9) *Підтримка, обслуговування та оновлення*. Навіть після введення в дію система вимагає періодичного обслуговування: технічні огляди, оновлення програмного забезпечення, модернізація компонентів. Важливо впроваджувати механізми віддаленого моніторингу та автоматичного виявлення несправностей для підвищення ефективності обслуговування.

Проєктування та монтаж систем передачі інформації — це не просто технічний процес, а багатовимірний управлінський та аналітичний виклик. Успішна реалізація залежить від балансу між нормативною відповідністю, технічною доцільністю, економічною ефективністю та адаптацією до потреб конкретного підприємства. Надійна інформаційна інфраструктура в енергетиці — це основа цифрової трансформації галузі, яка забезпечує прозорість, ефективність і гнучкість управління енергоресурсами.

7.4. Тестування, налагодження та технічна підтримка систем

Розгортання систем передачі інформації в енергетичному секторі є складним і багатоступеневим процесом, який не закінчується фізичним монтажем обладнання. Важливою фазою після проєктування й інсталяції є тестування, налагодження та організація системи технічної підтримки. Ці етапи визначають надійність функціонування, відповідність проєктним вимогам і здатність системи адаптуватися до реальних умов експлуатації. Їх значення в умовах зростаючих вимог до енергоефективності, кіберзахисту, масштабованості та інтероперабельності систем не можна недооцінювати.

Значення тестування в процесі впровадження інформаційних систем. Тестування — це перша і одна з найбільш критичних фаз після інсталяції обладнання (рис. 7.4). Воно покликане виявити потенційні відхилення від очікуваної функціональності, апаратні несправності або помилки в програмному забезпеченні. Процедура тестування охоплює як одиничні компоненти (модулі збору даних, комунікаційні шлюзи, сервери, енергетичні контролери), так і функціонування всієї системи в цілому.

Рисунок 7.4 – Фази проєктування

У разі збоїв, виявлених під час тестів, їх усунення відбувається на етапі налагодження. Якісно проведене тестування забезпечує мінімізацію ризиків у майбутній експлуатації, особливо в контексті критичних енергетичних об’єктів, де інформація про енергоспоживання, диспетчеризацію чи аварійні стани має бути максимально точною та доступною в режимі реального часу.

У процесі тестування зазвичай виділяють кілька підетапів:

– функціональне тестування (перевірка відповідності алгоритмів роботи системи до технічного завдання);

– навантажувальне тестування (оцінка поведінки системи під піковим потоком даних);

– інтеграційне тестування (взаємодія окремих підсистем — наприклад, SCADA, ERP, АСКОЕ);

– тестування на безперервність і відмовостійкість.

Крім того, велике значення має тестування безпеки, особливо в умовах активних кіберзагроз. Йдеться не лише про перевірку паролів, брандмауерів чи VPN-з'єднань, а й про моделювання зовнішніх атак із метою оцінити ефективність захисних механізмів системи.

Налагодження систем передачі інформації. Після того як усі компоненти системи протестовані, настає фаза налагодження. Це технічно й аналітично складний етап, під час якого відбувається адаптація параметрів роботи до реальних умов експлуатації. Цей процес передбачає як тонке налаштування обладнання (частоти опитування, інтервали передачі, алгоритми буферизації даних), так і конфігурацію програмного забезпечення (інтеграція з базами даних, хмарними платформами, параметри безпеки).

Налагодження також охоплює:

– калібрування та синхронізацію вимірювальних пристроїв;

– оновлення прошивок та налаштування політик автоматичного резервного копіювання;

– конфігурацію маршрутизаторів, комутаторів, шлюзів передачі даних;

– формування шаблонів звітів, інтерфейсів користувача.

На цьому етапі активно взаємодіють інженери з автоматизації, IT-фахівці, представники замовника та іноді оператори енергетичних об'єктів. Саме ця співпраця дозволяє налаштувати систему максимально ефективно для її подальшого повсякденного використання.

Варто зазначити, що частина процесів налагодження виконується віддалено, особливо у випадках, коли використовуються хмарні рішення. Це знижує витрати, однак вимагає високого рівня підготовки обох сторін: як інтегратора, так і замовника.

Технічна підтримка: запорука безперервного функціонування. Жодна сучасна інформаційна система не може працювати стабільно без належної технічної підтримки. Це особливо актуально для енергетичного сектору, де збої можуть спричинити не лише економічні втрати, а й небезпеку для об'єктів критичної інфраструктури. Технічна підтримка передбачає організацію комплексу сервісних заходів, спрямованих на забезпечення безперебійної роботи, оновлення, захисту і масштабування інформаційних систем.

До основних задач технічної підтримки належать:

– моніторинг працездатності в реальному часі;
– оперативне реагування на інциденти;
– оновлення ПЗ відповідно до змін у регуляторному полі;
– резервне копіювання й аварійне відновлення;
– консультування персоналу підприємства.

У межах ефективної техпідтримки важливо передбачити SLA (угоду про рівень сервісу), в якій фіксуються час реакції на запит, рівень доступності системи (наприклад, 99,9 %), а також відповідальність сторін.

Однією з сучасних тенденцій є використання елементів штучного інтелекту для автоматизації технічної підтримки. Наприклад, системи можуть самостійно прогнозувати потенційні збої на основі статистичних патернів і генерувати відповідні повідомлення для оператора.

Взаємозв'язок тестування, налагодження та технічної підтримки. Ці три етапи не є відокремленими процесами — вони утворюють цілісний цикл, який забезпечує надійність, гнучкість і масштабованість енергетичних інформаційних систем. Тестування дає змогу виявити потенційні проблеми ще до початку експлуатації. Налагодження дозволяє адаптувати систему до конкретного середовища, а технічна підтримка забезпечує її стабільне функціонування впродовж життєвого циклу.

Крім того, ці етапи мають бути документально зафіксовані. Повинні бути створені технічні журнали тестування, протоколи налагодження, а також інструкції користувача та сценарії реагування на інциденти. Це не лише полегшує

обслуговування системи, а й дозволяє оперативно виявляти слабкі місця для подальшої оптимізації.

Ефективне функціонування систем передачі інформації в енергетиці неможливе без належного проходження етапів тестування, налагодження та організації технічної підтримки. Саме ці фази визначають довгострокову надійність, адаптивність і безпечність таких систем. В умовах постійної цифровізації енергетики та зростання обсягів переданих даних, питання правильної організації цих етапів стає особливо актуальним. Компаніям, що впроваджують такі системи, необхідно інвестувати в підготовку кадрів, автоматизовані інструменти моніторингу та сертифіковану підтримку, щоб забезпечити відповідність сучасним технічним і безпековим стандартам.

7.5. Приклади реалізованих проєктів

Проєктування та впровадження систем передачі інформації в енергетичній галузі на практиці супроводжується значною кількістю викликів — від технічних обмежень до організаційних ризиків. Тому аналіз конкретних реалізованих проєктів дає можливість побачити, як теоретичні знання застосовуються в реальних умовах, які технології обирають, на які результати орієнтуються і як долають труднощі.

Впровадження Smart Grid в операторів системи розподілу (ОСР) в Європі. Один з найбільш показових прикладів — реалізація концепції Smart Grid у німецьких та шведських енергетичних компаніях (рис. 7.5). Такі компанії, як *E.ON* та *Vattenfall*, з 2012 року почали впровадження інтелектуальних лічильників і комунікаційних мереж, що поєднують споживачів, генераторів і операторів системи розподілу.

Проєкт передбачав інтеграцію таких елементів:

– мережі передачі даних (переважно за допомогою PLC та LTE);
– централізованої SCADA-системи;
– автоматизованих лічильників з функцією двосторонньої передачі даних;
– платформи аналізу даних (Big Data) для прийняття оперативних рішень.

Рисунок 7.5 – Приклади реалізованих проєктів

Впровадження цієї технології дозволило досягти значного підвищення прозорості в енергоспоживанні, ефективного виявлення втрат у мережах, а також підвищення енергоефективності кінцевих користувачів. У Німеччині, за оцінками Федерального міністерства економіки, було зменшено комерційні втрати енергії до 3 % за перші 2 роки експлуатації системи.

Важливим аспектом проєкту стала модульна архітектура системи, яка дозволяла поступове масштабування без необхідності зупинки основних процесів розподілу. Іншим успішним рішенням стала адаптація стандартів ISO/IEC 61850, що забезпечила високу сумісність між пристроями різних виробників.

Впровадження АСКОЕ в Україні. Національні енергетичні компанії в Україні також впроваджують проєкти цифрової трансформації. Одним із прикладів є автоматизована система обліку електроенергії (АСКОЕ), впроваджена ПАТ «Київобленерго» у 2018–2022 роках. Система охопила як промислових споживачів, так і побутових абонентів у Київській області.

Проєкт передбачав впровадження:

– більше ніж 100 000 інтелектуальних лічильників;

– GSM/GPRS комунікаційних модулів для дистанційної передачі інформації;

– централізованої бази даних для накопичення та аналізу споживання;

– сповіщень про несанкціоноване втручання в мережу.

Головними викликами стали:

– відсутність у частини абонентів покриття стільникового зв’язку;

– низький рівень цифрової грамотності користувачів;

– необхідність адаптації до національних норм та законодавства.

Незважаючи на ці труднощі, система дозволила значно зменшити людський фактор в процесі зняття показів, підвищити точність обліку, а також інтегрувати енергетичні дані у фінансову звітність.

Цікаво, що у цьому проєкті було протестовано концепцію віддаленого відключення та повторного підключення споживачів. Такий функціонал дав змогу оперативніше реагувати на борги чи аварійні ситуації без необхідності виїзду бригад на об’єкт.

Італійський досвід: ENEL та масове впровадження AMI. ENEL — одна з провідних енергетичних компаній Італії — реалізувала масштабний проєкт AMI ще на початку 2010-х років. Було замінено понад 35 мільйонів традиційних лічильників на інтелектуальні пристрої, що підтримують протокол DLMS/COSEM та здатні передавати дані через Power Line Communication (PLC).

Інтеграція з корпоративними системами ERP дала змогу автоматично оновлювати споживання, формувати рахунки, контролювати балансування навантажень і проводити аналіз даних у режимі реального часу.

Цей кейс також демонструє важливість інформаційної безпеки: у ENEL функціонує багаторівнева система захисту, що включає симетричне шифрування, VPN для комунікацій між компонентами інфраструктури та регулярні аудитні перевірки.

Завдяки інвестиціям понад 2 млрд євро, компанія домоглася:

– зниження операційних витрат;

– зменшення втрат енергії;

– підвищення точності прогнозування навантажень.

Локальні мікромережі: проєкт в університетському містечку Стенфорд. У 2015–2018 роках Університет Стенфорда (США) реалізував проєкт створення власної мікромережі з функціоналом Smart Grid, яка включала:

– два сонячні парки сумарною потужністю понад 70 МВт;

– систему зберігання енергії на базі акумуляторних батарей;

– власну систему SCADA для керування споживанням;

– IoT-мережу датчиків для моніторингу споживання в будівлях.

Особливість цього проєкту — реалізація повного енергетичного циклу в межах одного кампусу з мінімальною залежністю від зовнішніх джерел. Було досягнуто 68 % самозабезпечення електроенергією, а споживання викопного палива знижено на 90 %.

Важливим наслідком стало створення навчально-дослідної бази, яка дозволяє тестувати нові технології у реальних умовах, наприклад, прогностичне керування навантаженням або балансування з використанням штучного інтелекту.

З аналізу представлених прикладів можна зробити кілька висновків щодо чинників, що визначають успіх реалізації проєктів у сфері передачі інформації в енергетиці:

а) інтеграція стандартів. Проєкти, що використовували відкриті протоколи зв'язку (IEC 61850, DLMS/COSEM), демонстрували кращу масштабованість та сумісність з різними пристроями;

б) поетапне впровадження. Вдале проєктування передбачає пілотні зони, що дозволяють тестувати рішення та виявляти помилки до повноцінного запуску;

в) пріоритет безпеки. Кожен успішний проєкт включав багаторівневий захист даних та архітектурні підходи до ізоляції критичних сегментів мережі;

г) прозоре фінансування. Державна підтримка або чітке планування інвестицій підвищують шанси на завершення проєкту без затримок;

д) участь користувача. Споживач, як активний елемент системи має бути поінформований, навчений та мати доступ до своїх даних.

Реалізовані проєкти систем передачі інформації в енергетиці підтверджують, що майбутнє цієї галузі за цифровізацією, автоматизацією та інтелектуальним управлінням. Сучасні приклади демонструють, що правильне проєктування, стандартизація та врахування людського чинника дозволяють створювати ефективні, безпечні та масштабовані системи, які не лише підвищують енергоефективність, але й сприяють розвитку сталої енергетики загалом.

Висновок до розділу 7

Останній розділ навчального посібника присвячено всебічному аналізу процесу проєктування та впровадження систем передачі інформації в енергетиці — одного з ключових етапів цифровізації галузі. Розгляд концепцій, методик, етапів і практичного досвіду дозволяє сформувати системне розуміння того, як створюються ефективні, безпечні й масштабовані інформаційні рішення в енергетичному середовищі.

Вивчення функціональних, нефункціональних та зовнішніх вимог дозволяє зрозуміти, як різні категорії задач — від телеметрії до керування — впливають на архітектуру системи. Було розглянуто вимоги до швидкодії, надійності, пропускної здатності, масштабованості та взаємодії з іншими інформаційними платформами. Також було порушено важливі аспекти кібербезпеки, що визначають рівень захисту переданої інформації та надійність системи в умовах кіберзагроз.

Проаналізовано етапи створення технічного завдання як центрального документа, що визначає параметри, функціональність і критерії якості СПІ. Належне формування ТЗ дозволяє узгодити очікування замовника, забезпечити чітке планування та гарантувати відповідність результату початковим вимогам. Було розглянуто структуру ТЗ, вимоги до документації, проблеми узгодження змін та необхідність інтеграції стандартів, включно з ISO/IEC та галузевими нормами. Підкреслено значення уніфікації підходів і стандартизації технічних специфікацій у межах великих підприємств.

Було окреслено логічну послідовність дій — від передпроєктного обґрунтування до розгортання фізичної інфраструктури. Підкреслено, що процес проєктування охоплює не лише вибір технологій, а й створення кабельної інфраструктури, підготовку приміщень, забезпечення енергонезалежності та взаємодію з іншими системами підприємства. Розглядались особливості монтажу польового обладнання, налаштування маршрутизаторів, вибір топології мережі та технічна підготовка до експлуатації. Окремо висвітлено вимоги до навчання персоналу, технічної документації та приймання об’єкта в експлуатацію.

Окрему увагу приділено тестуванню, налагодженню та організації технічної підтримки. Це критичні етапи для забезпечення стабільної та безпечної роботи системи. Висвітлено принципи функціонального, навантажувального, інтеграційного та безпекового тестування. Після цього система проходить процес адаптації до реального середовища — налаштовуються протоколи, алгоритми резервування, параметри опитування пристроїв. Було підкреслено значення організації постійної технічної підтримки, впровадження систем моніторингу, резервного копіювання та обслуговування інфраструктури відповідно до SLA. Окремо згадано можливості використання елементів штучного інтелекту для автоматизації діагностики.

Наведено практичні приклади реалізованих проєктів — як міжнародних, так і національних. Аналіз кейсів реалізації Smart Grid, AMI та АСКОЕ дозволяє виявити фактори успіху: застосування відкритих стандартів, поступове впровадження, пріоритет безпеки, інтеграція з бізнес-процесами та активна участь кінцевих користувачів. Показано, як сучасні СПІ можуть бути гнучко масштабовані, адаптовані до складних умов, зменшувати втрати енергії, підвищувати ефективність управління та сприяти розвитку сталої енергетики.

Отже, останній розділ навчального посібника сформував цілісне уявлення про повний життєвий цикл СПІ — від аналізу потреб до експлуатації. Це знання дозволяє майбутнім фахівцям грамотно проєктувати та впроваджувати інформаційні системи в енергетиці з урахуванням як технічних, так і управлінських, нормативних і економічних аспектів.

Запитання для контролю знань за сьомим розділом

1. Які функціональні та нефункціональні вимоги висуваються до систем передачі інформації в енергетиці?
2. Яке значення мають зовнішні вимоги при проєктуванні СПІ?
3. Як швидкодія і масштабованість впливають на архітектуру СПІ?
4. Чому кібербезпека має вирішальне значення для сучасних СПІ?
5. Які основні етапи формування технічного завдання для СПІ?
6. Чому необхідна інтеграція стандартів ISO/IEC у технічне завдання?
7. Які проблеми можуть виникати під час узгодження змін у ТЗ?
8. Навіщо уніфікувати підходи до технічних специфікацій у межах великих підприємств?
9. Що охоплює процес проєктування СПІ на етапі передпроєктного обґрунтування?
10. Які компоненти фізичної інфраструктури СПІ створюються під час монтажу?
11. Чому важливо враховувати енергонезалежність системи при проєктуванні?
12. Які аспекти монтажу польового обладнання потребують особливої уваги?
13. Як відбувається технічна підготовка об’єкта СПІ до експлуатації?
14. Які види тестування застосовуються для перевірки працездатності СПІ?
15. Які налаштування потрібні під час адаптації СПІ до роботи?
16. Чому важливо організувати постійну технічну підтримку СПІ?
17. Які можливості дає використання AI в обслуговуванні СПІ?
18. Які уроки можна винести з аналізу реалізованих проєктів у сфері Smart Grid, AMI та АСКОЕ?
19. Чому інтеграція СПІ з бізнес-процесами є ключовим чинником успіху?
20. Як знання життєвого циклу СПІ допомагає майбутнім енергетикам?

ВИСНОВОК

Навчальний посібник «Передача інформації в електроенергетиці: засоби, протоколи, стандарти, кібербезпека» охоплює повний спектр питань, пов’язаних із формуванням, функціонуванням і розвитком сучасних інформаційно-комунікаційних технологій в енергетичному середовищі. Вивчення матеріалу всіх розділів дозволяє сформувати системне бачення технологічної, організаційної та нормативної складової інформаційного обміну в галузі, що активно трансформується під впливом цифровізації.

Читач знайомиться з базовими поняттями, принципами та моделями, які лежать в основі побудови систем передачі інформації. Формується фундаментальне уявлення про природу сигналів, шляхи їх передачі, види перешкод, архітектурні моделі комунікації та функції інформаційних систем в енергетиці. Розуміння структури та функціонального призначення СПІ дозволяє читачу впевнено сприймати подальші прикладні аспекти.

Навчальний посібник поглиблює знання про основні елементи інформаційних систем: джерела, приймачі, канали зв’язку, комунікаційне обладнання та топології мереж. Звертається увага на практичну важливість вибору технічних рішень залежно від умов експлуатації та завдань системи. Допомагає розуміти, як формується інформаційна структура енергетичного об’єкта — від фізичної інфраструктури до логічних з’єднань.

У навчальному посібнику систематизовано знання про протоколи та стандарти передачі даних. Через огляд основних технологій комунікації, міжнародних протоколів та вимог до сумісності закладається основа для інтеграції інформаційних систем у єдине технологічне середовище. Порівняння підходів, приклади впровадження та аналіз тенденцій дозволяють сформувати уявлення про стратегії адаптації до вимог сучасної цифрової енергетики.

Один із розділів розглядає SCADA-системи як ключовий елемент диспетчерського управління. Охоплено всі рівні архітектури — від польових пристроїв до центральних серверів — і показано їх взаємодію. Розділ акцентує увагу на

відкритості, масштабованості, стійкості до збоїв та здатності до інтеграції з іншими інформаційними рішеннями. Практичні приклади ілюструють реальні підходи до впровадження SCADA в різних умовах.

Описано роботу автоматизованих систем обліку електроенергії, які стали основою для сучасного енергетичного моніторингу та аналізу. Детально описано архітектуру, принципи взаємодії елементів системи, захист інформації, інтеграцію з іншими платформами та нормативне забезпечення. Підхід до обліку як до інтегрованої інформаційної системи дозволяє сформувати бачення про її стратегічне значення в цифровій енергетиці.

Проаналізована нову парадигму функціонування енергетичних систем — цифрову трансформацію. Вивчення концепцій Smart Grid, IoT, хмарних технологій, кібербезпеки та цифрових платформ формує розуміння майбутнього галузі. Підкреслюється необхідність адаптації до нових вимог і викликів — технічних, організаційних, нормативних — та активна участь усіх учасників ринку у процесі змін.

Розглянуто практичне впровадження систем передачі інформації — від формування вимог і технічного завдання до монтажу, тестування, підтримки та аналізу прикладів реалізації. Він узагальнює матеріал попередніх розділів і дає уявлення про повний життєвий цикл СПІ. Особливу увагу приділено питанням безпеки, відповідності стандартам, ефективному управлінню проєктом і технічній готовності персоналу.

Навчальний посібник формує цілісну картину сучасних інформаційних процесів в енергетиці, охоплюючи базові знання, технології, стандарти, архітектури, захист і практичне впровадження. Його структура дозволяє майбутнім фахівцям послідовно опанувати як теоретичні засади, так і практичні навички, необхідні для проєктування, експлуатації та розвитку ефективних інформаційних систем в електроенергетиці.

ПЕРЕЛІК ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

АСУ ТП	–	Автоматизовані системи управління технологічними процесами;
АСКОЕ	–	Автоматизовані систем комерційного обліку електроенергії;
ВДЕ	–	Відновлювальні джерела енергії;
КП	–	Контрольований пункт;
ОЕС	–	Об’єднана енергетична система;
ПК	–	Пункт керування;
РЕМ	–	Районні електричні мережі;
РЗА	–	Релейний захист та автоматика;
СПІ	–	Системи передачі інформації;
СУБД	–	Система управління базами даних;
AES	–	Advanced Encryption Standard / Стандарт передового шифрування;
AGC	–	Automatic Generation Control / Автоматичне регулювання генерації;
AMI	–	Advanced Metering Infrastructure / Інфраструктура інтелектуального обліку;
AMI	–	Alternate Mark Inversion / Альтернативна інверсія імпульсів;
AMR	–	Automatic Meter Reading / Автоматичне зчитування показників лічильника;
API	–	Application Programming Interface / Програмний інтерфейс прикладного програмування;
CAN	–	Controller Area Network / Мережева система контролерів;
CIM	–	Common Information Model / Загальна інформаційна модель;
CMMS	–	Computerized Maintenance Management System / Комп’ютеризована система управління технічним обслуговуванням;
COSEM	–	Companion Specification for Energy Metering / Супровідна специфікація для енергетичного обліку;

CRC	–	Cyclic Redundancy Check / Контрольна сума з циклічним надмірним кодом;
CRL	–	Certificate Revocation List / Список відкликаних сертифікатів;
DLMS	–	Device Language Message Specification / Специфікація повідомлень мовою пристроїв;
DMZ	–	Demilitarized Zone / Демілітаризована зона;
DMS	–	Distribution Management System / Система управління розподілом;
DNP3	–	Distributed Network Protocol version 3 / Розподілений мережевий протокол версії 3;
DR	–	Demand Response / Управління попитом;
DWDM	–	Dense Wavelength Division Multiplexing / Щільне спектральне мультиплексування з поділом довжин хвиль;
ECC	–	Elliptic Curve Cryptography / Криптографія на еліптичних кривих;
EMS	–	Energy Management System / Система енергетичного менеджменту;
ENTSO-E	–	European Network of Transmission System Operators for Electricity / Європейська мережа операторів систем передачі електроенергії;
EPA	–	Enhanced performance architecture / Архітектура з підвищеною продуктивністю;
ERP	–	Enterprise Resource Planning / Система планування ресурсів підприємства;
FOC	–	Fiber Optic Communication / Волоконно-оптичний зв’язок;
GDPR	–	General Data Protection Regulation / Загальний регламент захисту даних ЄС;
GIS	–	Geographic Information System / Геоінформаційна система;
GOOSE	–	Generic Object Oriented Substation Event / Загальні об’єктно-орієнтовані події підстанцій;

GPRS	–	General Packet Radio Service / Служба пакетної радіопередачі загального користування;
GPS	–	Global Positioning System / Глобальна система позиціонування;
GSM	–	Global System for Mobile Communications / Глобальна система мобільного зв’язку;
HART	–	Highway Addressable Remote Transducer / Адресована шина дистанційних перетворювачів;
HMI	–	Human-Machine Interface / Людино-машинний інтерфейс;
HTTP	–	HyperText Transfer Protocol / Протокол передавання гіпертексту;
HTTPS	–	HyperText Transfer Protocol Secure / Захищений протокол передавання гіпертексту;
HVAC	–	Heating, Ventilation, and Air Conditioning / Опалення, вентиляція та кондиціювання повітря;
IDS	–	Intrusion Detection System / Система виявлення вторгнень;
IEC	–	International Electrotechnical Commission / Міжнародна електротехнічна комісія;
IEEE	–	Institute of Electrical and Electronics Engineers / Інститут інженерів з електротехніки та електроніки;
IED	–	Intelligent Electronic Devices / Інтелектуальні електронні пристрої;
IIoT	–	Industrial Internet of Things / Промисловий Інтернет речей;
IP	–	Internet Protocol / Інтернет-протокол;
IPS	–	Intrusion Prevention System / Система запобігання вторгненням;
IoT	–	Internet of Things / Інтернет речей;
ISO	–	International Organization for Standardization / Міжнародна організація зі стандартизації;
LAN	–	Local Area Network / Локальна (місцева) мережа;

LPWAN – Low Power Wide Area Network / Широкосмугова мережа з низьким енергоспоживанням;

LTE – Long Term Evolution / Технологія мобільного зв'язку четвертого покоління;

MAC – Media Access Control / Керування доступом до середовища;

MLT-3 – Multi-Level Transmit - 3 levels / Трирівнева багаторівнева передача;

MMS – Manufacturing Message Specification / Специфікація повідомлень для виробництва;

MQTT – Message Queuing Telemetry Transport / Протокол телеметрії із чергами повідомлень;

MPLS – Multiprotocol Label Switching / Комутація за багатопротокольними мітками;

MTBF – Mean Time Between Failures / Середній час між відмовами;

MTTR – Mean Time To Repair / Середній час на відновлення;

NAVSTAR – Navigation Signal Timing and Ranging / Система навігаційного сигналу часу та дальності;

NERC CIP – North American Electric Reliability Corporation Critical Infrastructure Protection / Стандарти захисту критичної інфраструктури Північноамериканської корпорації електроенергетичної надійності;

NIST – National Institute of Standards and Technology / Національний інститут стандартів і технологій (США);

NTP – Network Time Protocol / Мережевий протокол синхронізації часу;

NRZ – Non-Return to Zero / Без повернення до нуля;

NRZI – Non-Return-to-Zero Inverted / Інверсне кодування без повернення до нуля;

OCSP – Online Certificate Status Protocol / Протокол онлайн-перевірки статусу сертифіката;

OPC UA	–	OPC Unified Architecture / Уніфікована архітектура OPC;
OSI	–	Open System Interconnection / Відкрита система взаємозв’язку;
PAC	–	Programmable Automation Controllers / Програмовані контролери автоматизації;
PKI	–	Public Key Infrastructure / Інфраструктура відкритих ключів;
PLC	–	Programmable Logic Controllers / Програмовані логічні контролери;
PMU	–	Phasor Measurement Unit / Пристрій вимірювання фазорів;
PROFIBUS	–	Process Field Bus / Польова шина процесів;
PTP	–	Precision Time Protocol / Протокол точного часу;
QoS	–	Quality of Service / Якість обслуговування;
RDP	–	Remote Desktop Protocol / Протокол віддаленого робочого столу;
REST API	–	Representational State Transfer Application Programming Interface / Програмний інтерфейс прикладного рівня на основі REST;
RF	–	Radio Frequency / Радіочастотна передача даних;
RSA	–	Rivest-Shamir-Adleman / Криптосистема Рівеста — Шаміра — Адельмана;
RTC	–	Real-Time Clock / Годинник реального часу;
RTD	–	Resistance Temperature Detector / Датчик температури опору;
RTU	–	Remote Terminal Units / Віддалені термінальні пристрої;
RZ	–	Return to Zero / Повернення до нуля;
SAP	–	Systems, Applications, and Products in Data Processing / Системи, додатки та продукти в обробці даних;
SCADA	–	Supervisory Control and Data Acquisition / Диспетчерське управління і збір даних;
SCL	–	Substation Configuration Language / Мова конфігурації підстанцій;

SD-WAN	–	Software-Defined Wide Area Network / Програмно-визначена глобальна мережа;
SDG	–	Software Defined Gateways / Програмно-визначені шлюзи;
SDH	–	Synchronous Digital Hierarchy / Синхронна цифрова ієрархія;
SIEM	–	Security Information and Event Management / Система управління інформацією та подіями безпеки;
SNMP	–	Simple Network Management Protocol / Протокол простого управління мережею;
SOA	–	Service-Oriented Architecture / Сервісно-орієнтована архітектура;
SSH	–	Secure Shell / Захищена оболонка;
SSL	–	Secure Sockets Layer / Протокол захищених сокетів;
SV	–	Sampled Values / Вибіркові значення;
TCP	–	Transmission Control Protocol / Протокол керування передаванням;
TLS	–	Transport Layer Security / Протокол захисту транспортного рівня;
UDP	–	User Datagram Protocol / Протокол дейтаграм користувача;
VPP	–	Virtual Power Plants / Віртуальні електростанції;
VPN	–	Virtual Private Network / Віртуальна приватна мережа;
WAMS	–	Wide Area Monitoring System / Система моніторингу широкої зони;
WAN	–	Wide Area Network / Глобальна мережа.

СПИСОК ДЖЕРЕЛ ІНФОРМАЦІЇ

1. Автоматизовані системи обліку та якості електричної енергії в оптовому ринку [Текст] / А. В. Праховник, Ю. Ф. Тесік, А. Ф. Жаркін [та ін.] ; за ред. О. Г. Гриба. – Харків : ПП «Ранок–НТ», 2012. – 516 с.

2. Боднар І. Р., Боднар Р. М. Системи автоматичного керування в електроенергетиці : навч. посіб. – Львів : Видавництво Львівської політехніки, 2015.

3. Васюра А. С. Елементи та пристрої систем управління і автоматики : навч. посіб. Ч. 1 / А. С. Васюра. – Вінниця : ВДТУ, 1999. – 157 с.

4. Васюра А. С. Техніка передавання аналогової та дискретної інформації / А. С. Васюра. – Вінниця : ВДТУ, 1998. – 218 с.

5. Воробієнко П. П. Телекомунікаційні та інформаційні мережі : підручник / П. П. Воробієнко, Л. А. Нікітюк, П. І. Резніченко. – Київ : САММІТ–Книга, 2010. – 708 с.

6. Горлач А. І., Клюєв В. М. Автоматизовані системи управління в енергетиці. – Київ : НАУ, 2018.

7. Гунгор В. С., Ламберт Ф. К. Огляд комунікаційних мереж для автоматизації електричних систем. Computer Networks, 2006.

8. Гузій М. М., Олійник М. М. Основи автоматизації в електроенергетиці. – Київ : ІЕЕ НАН України, 2020.

9. Інформаційне та нормативне забезпечення організації мультиагентного керування електроенергетичної системи із активним споживачем [Текст] / О. В. Кириленко, С. П. Денисюк, С. Є. Танкевич, Т. М. Базюк // Інформаційні технології та комп’ютерна інженерія. – 2016. – № 1. – С. 29.

10. Карпалюк І. Т. Комп’ютерні інформаційні технології в енергетиці / І. Т. Карпалюк ; Харків. нац. ун–т міськ. госп–ва ім. О. М. Бекетова. – Харків : ХНУМГ ім. О. М. Бекетова, 2018. – 118 с.

11. Ковальчук С. А. Автоматизовані системи управління технологічними процесами в енергетиці. – Київ : КНУБА, 2020.

12. Коцар О. В. Автоматизовані системи контролю, обліку та управління енерговикористанням : навч. посіб. / О. В. Коцар. – Київ : КПІ ім. Ігоря Сікорського; Дніпро : Середняк Т. К., 2017. – 44 с.

13. Корнієнко Б. Я. Обробка інформації за допомогою динамічного хаосу / Б. Я. Корнієнко, А. В. Устьянцев // Зб. наук. пр. Ін–ту проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України. – К. : ІПМЕ ім. Г. Є. Пухова НАН України, 2009. – Вип. 52. – Бібліогр.: 2 назв.

14. Кузьмінський В. І., Ісаєнко С. О. Інформаційні системи та технології в енергетиці. – Київ : КПІ ім. Ігоря Сікорського, 2020.

15. Мельниченко С. В., Забарний Ю. В. Інформаційно–комунікаційні технології в енергетиці. – Харків : Українська інженерно–педагогічна академія, 2019.

16. Міністерство енергетики України. Концепція впровадження “розумних мереж” в електроенергетиці України : офіц. документ. – Київ, 2021.

17. Міністерство енергетики України. Цифрова трансформація енергетики: аналітичні матеріали, 2021–2024: веб – сайт URL: https://www.mev.gov.ua (дата звернення 04.04.2025)

18. Олійник М. М. Цифрові технології в електроенергетиці. – Київ : ІЕЕ НАН України, 2020.

19. Павлюк А. В. Цифрові технології в електроенергетиці : навч. посіб. – Харків : НТУ «ХПІ», 2021.

20. Рябенький В. М. Цифрова схемотехніка : навч. посіб. / В. М. Рябенький, В. Я. Жуйков, В. Д. Гулий. – Львів : Новий Світ–2000, 2009. – 736 с.

21. Соколов В. Ю. Інформаційні системи і технології : навч. посіб. / В. Ю. Соколов. – Київ : ДУІКТ, 2010. – 138 с.

22. Стаднік М. І. Інтелектуальні системи в електроенергетиці. Теорія та практика : навч. посіб. / М. І. Стаднік, А. А. Видмиш, А. А. Штуць, М. А. Колісник. – Вінниця : ТОВ «ТВОРИ», 2020. – 332 с.

23. Техніка передавання дискретної інформації : навч. посіб. / А. С. Васюра, С. Г. Кривогубченко, А. Я. Кулик, М. М. Компанець, О. І. Худолій ; МОН України. – Вінниця : ВДТУ, 1998. – 101 с.

24. Хаїмзон І. Я. Техніка передачі інформації. Функціональні вузли та схеми. Частина ІІ / І. Я. Хаїмзон. – Вінниця : ВДТУ, 2000. – 112 с.

25. ДСТУ EN 50160:2014. Характеристики напруги в електричних мережах загального призначення. – Київ : УкрНДНЦ, 2014.

26. ДСТУ IEC 60870–5–104:2016. Автоматизовані системи управління. Протоколи обміну даними для телемеханіки. Частина 5-104. Передача по TCP/IP. – Київ : УкрНДНЦ, 2016.

27. Укренерго. Офіційні матеріали і технічна документація. 2023: веб – сайт. URL: https://ua.energy (дата звернення 04.04.2025).

Навчальне видання

ДЯЧЕНКО Олександр Васильович
ГАПОН Дмитро Анатолійович
РУДЕВІЧ Наталія Валентинівна
ШВЕЦЬ Сергій Вікторович
ДОНЕЦЬКА Тетяна Сергіївна
ЛОЖКІН Руслан Сергійович

ПЕРЕДАЧА ІНФОРМАЦІЇ В ЕЛЕКТРОЕНЕРГЕТИЦІ: ЗАСОБИ, ПРОТОКОЛИ, СТАНДАРТИ, КІБЕРБЕЗПЕКА

Навчальний посібник
для бакалаврів та магістрів спеціальності
G3 «Електрична інженерія» усіх форм навчання

Відповідальний за випуск доц. Гапон Д. А.

Роботу до видання рекомендувала проф. Безпрозванних Г. В.

В авторській редакції

Комп’ютерна верстка та оригінал-макет О. І. Линник

План 2025 р., поз. 47

Гарнітура Times New Roman. Ум. друк. арк. 9,1

Видавничий центр НТУ «ХПІ».
Свідоцтво про державну реєстрацію ДК № 5478 від 21.08.2017 р.
61002, Харків, вул. Кирпичова, 2.

Електронне видання