

РОЗДІЛ 3

ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ

УДК 681.518.3:622.691.4

ПРОЄКТУВАННЯ ЗАХИЩЕНИХ ТЕЛЕМЕТРИЧНИХ СИСТЕМ ДЛЯ ГАЗОРОЗПОДІЛЬНИХ МЕРЕЖ

Куцевич Віктор,

здобувач першого (бакалаврського) рівня вищої освіти,

Приватного вищого навчального закладу

«Міжнародний економіко-гуманітарний університет

імені академіка Степана Дем'янчука» (м. Рівне, Україна)

Науковий керівник: Лотюк Юрій,

кандидат педагогічних наук, завідувач кафедри

інформаційних систем та обчислювальних методів

Приватного вищого навчального закладу

«Міжнародний економіко-гуманітарний університет імені

академіка Степана Дем'янчука» (м. Рівне, Україна)

Анотація. У статті розглянуто особливості проектування та захисту телеметричних систем наступного покоління в газорозподільних мережах. Проаналізовано архітектуру пристроїв дистанційної передачі даних, принципи збирання, буферизації та передавання показників споживання газу через мережі GSM/GPRS із використанням TCP/IP та NTP. Окрему увагу приділено засобам підвищення експлуатаційної надійності, антисаботажному захисту, контролю цілісності даних і віддаленій діагностиці. Показано, що впровадження таких рішень сприяє підвищенню точності обліку, безпеки та стійкості енергетичної інфраструктури.

Ключові слова: телеметрична система, газорозподільна мережа, пристрій дистанційної передачі даних, GSM/GPRS, TCP/IP, NTP, Smart Metering, інформаційна безпека, антисаботажний захист, дистанційний облік газу.

Abstract. The article examines the design and protection of next-generation telemetry systems in gas distribution networks. It analyzes the architecture of remote data transmission devices, the principles of data acquisition, buffering, and transmission of gas consumption readings via GSM/GPRS networks using TCP/IP and NTP protocols. Particular attention is paid to operational reliability, anti-tamper protection, data integrity control, and

remote diagnostics. It is shown that the implementation of such solutions improves metering accuracy, information security, and the resilience of energy infrastructure.

Keywords: *telemetry system, gas distribution network, remote data transmission device, GSM/GPRS, TCP/IP, NTP, Smart Metering, information security, anti-tamper protection, remote gas metering.*

Цифрова трансформація газорозподільної галузі зумовлює необхідність переходу від традиційного ручного зняття показників до інтелектуальних телеметричних систем нового покоління, здатних забезпечувати безперервний збір, передавання, збереження та оброблення даних у реальному часі. Водночас функціонування таких систем у розподіленому середовищі, із використанням бездротових каналів GSM/GPRS, стека TCP/IP, часової синхронізації та автономних пристроїв дистанційної передачі даних, висуває підвищені вимоги до надійності, точності, енергоефективності та кіберзахисту. Особливої актуальності набуває проблема забезпечення цілісності телеметричних даних, захисту від несанкціонованого втручання, підміни пристроїв, маніпуляцій із конфігурацією та втрати інформації під час збоїв зв'язку або впливу зовнішніх чинників.

Актуальність теми зумовлена інтенсивною цифровою трансформацією енергетичного сектору та потребою впровадження систем інтелектуального обліку, здатних забезпечити безперервний, точний і захищений збір даних про споживання природного газу. Перехід від ручного зняття показників до автоматизованих телеметричних рішень на базі пристроїв дистанційної передачі даних дає змогу підвищити оперативність оброблення інформації, зменшити вплив людського чинника та забезпечити централізований моніторинг стану вузлів обліку. Водночас використання бездротових каналів GSM/GPRS, протоколів TCP/IP і NTP, автономних контролерів та серверної інфраструктури актуалізує питання надійності передавання даних, часової синхронізації, енергоефективності та захисту від фізичного і логічного втручання [6]. У зв'язку з цим проектування та захист телеметричних систем наступного покоління в газорозподільних мережах є важливим напрямом сучасних науково-прикладних досліджень, орієнтованих на підвищення стійкості, прозорості та безпеки енергетичної інфраструктури.

Метою даної статті є аналіз архітектурних, комунікаційних та безпекових засад побудови телеметричних систем наступного покоління в газорозподільних мережах на основі пристроїв дистанційної передачі даних, а також обґрунтування підходів до забезпечення цілісності, достовірності та захищеності даних у процесі їх збирання, зберігання й передавання до централізованої інформаційної системи підприємства.

Аналіз сучасних досліджень у сфері інтелектуального обліку енергоресурсів і телеметричних мереж свідчить, що основна увага науковців і розробників зосереджується на питаннях підвищення точності дистанційного збору даних, забезпечення надійності функціонування автономних вимірювальних пристроїв, оптимізації бездротових каналів передавання інформації та посилення кіберзахисту критичної інфраструктури. У низці праць розглядаються принципи побудови Smart Metering-систем, архітектури пристроїв дистанційної передачі даних, застосування енергонезалежної пам'яті для буферизації архівів, а також засоби моніторингу технічного стану обладнання. Окремий напрям досліджень стосується використання APN-з'єднань і NTP-синхронізації як базових засобів забезпечення стабільного та масштабованого обміну даними в розподілених мережах обліку [7].

З наукового погляду зазначена проблема пов'язана з розробленням архітектурних принципів побудови захищених телеметричних мереж, вибором ефективних протоколів передавання даних, методів автентифікації, механізмів антисаботажу, буферизації та віддаленої діагностики. У практичному вимірі її розв'язання має важливе значення для підвищення достовірності комерційного обліку газу, зменшення експлуатаційних витрат, своєчасного виявлення аварійних і позаштатних ситуацій, а також для формування стійкої, прозорої та безпечної цифрової інфраструктури підприємств газорозподільної сфери. Саме тому проектування і захист телеметричних систем наступного покоління є важливим науково-прикладним завданням, спрямованим на підвищення ефективності та безпеки енергетичної інфраструктури.

Проблема дистанційного обліку енергоресурсів розглядається переважно в межах концепцій Smart Metering та Advanced Metering Infrastructure [1]. Дослідження Gaggero [2] показують, що ефективність систем розумного обліку суттєво залежить від правильно обраної комунікаційної технології, яка має поєднувати низьке енергоспоживання, достатню дальність зв'язку, пропускну здатність і засоби безпеки. У праці Kippke Salomón [4] smart meter подано вже не як пасивний засіб фіксації показників, а як активний вузол цифрової розподільної мережі, придатний для майже реального часу спостереження, керування й автоматизації. Водночас Koukouvinos [5] експериментально підтверджують переваги інтелектуальних лічильників над традиційними за точністю вимірювання, можливостями передавання даних і підтримкою енергоменеджменту. Для газорозподільної галузі узагальнювальний огляд Yadav [8] окреслює роль IoT, GIS, SCADA, AI та машинного навчання у формуванні підходів до smart gas distribution, однак цей напрям переважно висвітлюється на рівні загальної цифрової трансформації галузі.

Процес цифрової трансформації енергетичного сектору потребує впровадження надійних систем інтелектуального обліку (Smart Metering). Основним завданням при проектуванні мереж наступного покоління є перехід від ручного зняття показників до автоматизованих систем телеметрії, що базуються на пристроях дистанційної передачі даних (ПДПД). У даній роботі розглядається архітектура, канали зв'язку та протоколи безпеки на прикладі модема 104.UA Smart (Рис.1), який інтегрує фізичні прилади обліку в єдину інформаційну базу даних підприємства [9].

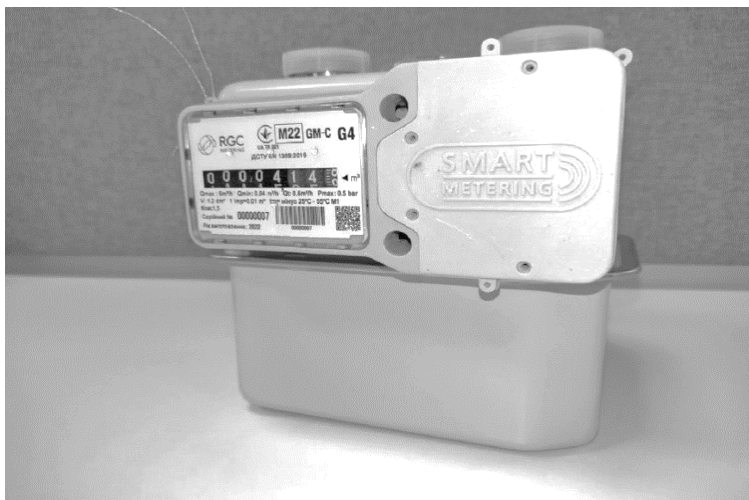


Рис. 1. Модем 104.UA Smart, встановлений на газовому лічильнику

Пристрій дистанційної передачі даних є автономним контролером, розробленим для роботи в агресивних середовищах (клас захисту IP66). Його апаратна частина спроектована з урахуванням тривалого життєвого циклу без зовнішнього живлення, що забезпечується літієвою батареєю з розрахунковим терміном служби до 10 років.

Ключові компоненти системи:

- Інтерфейс збору даних: Модем взаємодіє з лічильниками газу через низькочастотний імпульсний вихід (геркон). Контролер реєструє кожне замикання контакту, що відповідає певному об'єму газу (наприклад, 0.01 м³ для лічильників з коефіцієнтом 100 імпульс/м³).
- Модуль пам'яті: Вбудована енергонезалежна пам'ять (EEPROM) виконує роль буфера. Це критично важливо для збереження цілісності

даних при тимчасовій відсутності зв'язку. Пристрій здатний зберігати погодинні звіти протягом 90 діб та добові протягом 12 місяців.

- Датчики контролю стану: ПДПД оснащений вбудованим температурним датчиком та системою моніторингу напруги батареї для прогнозування технічного обслуговування.

Технології передачі даних та мережеві протоколи

- Проектування мереж наступного покоління передбачає використання надійних бездротових каналів. У модемах серії Smart реалізовано технологію пакетної передачі даних GPRS (Class 10/8 B).

Рівні мережевої взаємодії:

- Мережеві стандарти: Передача інформації реалізується через бездротові мережі стандарту GSM/GPRS у діапазонах 850/900/1800/1900 МГц. Вибір цієї технології обумовлений широкою зоною покриття та високою проникаючою здатністю сигналу, що критично для лічильників, встановлених у підвальних або металевих нішах.

- Синхронізація та часові мітки: Важливим елементом мереж наступного покоління є часова цілісність даних. Пристрої використовують протоколи синхронізації часу (NTP), що дозволяє фіксувати показники споживання з точністю до секунди, формуючи погодинні та добові архіви.

У системах захисту мереж наступного покоління безпека поділяється на фізичну стійкість та логічну захищеність каналів зв'язку [10].

Захист від несанкціонованого втручання (Anti-tamper):

- Магнітний моніторинг: Пристрій обладнаний датчиком магнітного поля, який реєструє спроби впливу на лічильник газу зовнішнім магнітом. Будь-яка аномалія фіксується як подія «Тривога магнітного сенсора» (MagSensor Alarm) і миттєво передається на сервер.

- Датчик розтину: Конструкція передбачає реєстрацію відкриття кришки корпусу. Це запобігає маніпуляціям з SIM-картою або внутрішніми ланцюгами пристрою.

Мережевий захист та верифікація [3]:

- Автентифікація пристроїв: Кожна сесія передачі даних супроводжується ідентифікацією за IMEI модема та серійним номером лічильника. Це унеможливує підміну даних або атаку типу «Man-in-the-middle» шляхом імітації пристрою.

- Захищене конфігурування: Зміна критичних параметрів (IP-адреса сервера, порти, графік виходу на зв'язок) можлива лише через спеціалізоване ПЗ «Configurator-104.ua-SMART» за умови фізичного підключення або через захищений сервісний канал.

- Цілісність даних: Система використовує механізми перевірки контрольних сум пакетів. При виявленні помилок у внутрішній пам'яті (наприклад, збій EEPROM), пристрій має алгоритми самовідновлення або

аварійного вимкнення модуля зв'язку для збереження енергії та запобігання передачі недостовірних даних.

- Ідентифікація та авторизація: Кожен пристрій має унікальний IMEI та серійний номер, які використовуються як первинні ідентифікатори при встановленні з'єднання. Серверна частина виконує сувору автентифікацію, відсікаючи будь-які спроби підключення стороннього обладнання.

- Захист конфігураційних даних: Налаштування критичних параметрів (IP-адреси сервера, порти, ліміти споживання) здійснюється через спеціалізоване захищене ПЗ Configurator-104.ua-SMART. Це виключає можливість віддаленої перенастроюки модема зловмисниками.

Процес проектування включає розробку алгоритмів обробки позаштатних ситуацій. Модем веде постійний журнал станів, що дозволяє адміністраторам мережі віддалено відстежувати рівень сигналу GSM, напругу живлення та статус реєстрації в мережі оператора. Це мінімізує витрати на виїзди технічних бригад, оскільки більшість проблем (наприклад, помилки оновлення прошивки або збої реєстрації) можна діагностувати через інтерфейс сервера телеметрії.

Система дистанційної передачі даних на базі модемів 104.UA Smart є прототипом проектування захищених мереж наступного покоління. Поєднання автономності, багатодіапазонного зв'язку та багаторівневої системи антисаботажу забезпечує високу точність обліку газу та захист даних від фізичних та програмних маніпуляцій. Впровадження таких систем є необхідним кроком для створення стійкої та прозорої енергетичної інфраструктури.

Ефективне функціонування телеметричних систем у газорозподільних мережах потребує комплексного поєднання надійних каналів передавання даних, засобів автентифікації, контролю цілісності інформації та механізмів антисаботажного захисту. Використання модемів 104.UA Smart дає змогу забезпечити безперервний дистанційний облік газу, підвищити достовірність даних і зменшити ризики фізичного та логічного втручання. Практичне значення таких рішень полягає у підвищенні експлуатаційної надійності, спрощенні віддаленої діагностики та формуванні стійкої цифрової інфраструктури газорозподільних підприємств.

ЛІТЕРАТУРА

1. Abdullah A. A., El-den B. M., Abo-Al-Ez K. M., Hassan T. M. Security Management for an Advanced Metering Infrastructure (AMI) System of Smart Electrical Grids // Applied Sciences. 2023. Vol. 13, no. 15. Article 8990. DOI: 10.3390/app13158990.
2. Gaggero G. B., Marchese M., Moheddine A., Patrone F. A Possible Smart Metering System Evolution for Rural and Remote Areas Employing Unmanned Aerial Vehicles and Internet of Things in Smart Grids // Sensors. 2021. Vol. 21, no. 5. Article 1627. DOI: 10.3390/s21051627.

- 3.Kohout D., Lieskovan T., Mlynek P. Smart Metering Cybersecurity–Requirements, Methodology, and Testing // *Sensors*. 2023. Vol. 23, no. 8. Article 4043. DOI: 10.3390/s23084043.
- 4.Kippke Salomón M. A., Carou Álvarez J. M., Suárez Ramón L., Arboleya P. Self-Diagnostic Advanced Metering Infrastructure Based on Power-Line Communication: A Study Case in Spanish Low-Voltage Distribution Networks // *Energies*. 2025. Vol. 18, no. 7. Article 1746. DOI: 10.3390/en18071746.
- 8.Koukouvinos K. G., Koukouvinos G. K., Chalkiadakis P., Kaminaris S. D., Orfanos V. A., Rimpas D. Evaluating the Performance of Smart Meters: Insights into Energy Management, Dynamic Pricing and Consumer Behavior // *Applied Sciences*. 2025. Vol. 15, no. 2. Article 960. DOI: 10.3390/app15020960.
- 9.Nambundo J. M., de Souza Martins Gomes O., de Souza A. D., Machado R. C. S. Cybersecurity and Major Cyber Threats of Smart Meters: A Systematic Mapping Review // *Energies*. 2025. Vol. 18, no. 6. Article 1445. DOI: 10.3390/en18061445.
- 10.Szczepaniuk E. K., Szczepaniuk H. Cybersecurity of Smart Grids: Requirements, Threats, and Countermeasures // *Energies*. 2025. Vol. 18, no. 18. Article 5017. DOI: 10.3390/en18185017.
- 11.Yadav K., Sircar A., Bist N. A Comprehensive Review on Role of Information Technology in City Gas Distribution Industry // *Unconventional Resources*. 2025. Vol. 7. Article 100202. DOI: 10.1016/j.unres.2025.100202.
- 12.Вілянський А. В., Позняк А. А. Організаційні аспекти впровадження моделі Zero Trust у корпоративному середовищі // Актуальні питання забезпечення кібербезпеки та захисту інформації : матеріали XI Міжнародної науково-практичної конференції, м. Київ, 24 квітня 2025 р. Київ, 2025. С. 20–21.
- 13.Дудикевич В. Б., Микитин Г. В., Мурак Т. Є. Комплексна система безпеки регіональної корпоративної мережі на основі еталонної моделі OSI та моделі «глибокого захисту» // *Комп'ютерні системи та мережі*. 2025. Т. 7, № 1. С. 119–131. DOI: 10.23939/csn2025.01.119.