**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ «ДНІПРОВСЬКА ПОЛІТЕХНІКА»**
**НАЦІОНАЛЬНА МЕТАЛУРГІЙНА АКАДЕМІЯ УКРАЇНИ**

Кваліфікаційна наукова
праця на правах рукопису

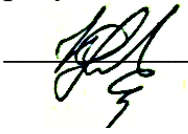
Ковальова Юлія Вікторівна

УДК 004.7: 004.932

# ДИСЕРТАЦІЯ
# МАТЕМАТИЧНІ МОДЕЛІ ТА МЕТОДИ БЕЗДРОТОВОЇ ПЕРЕДАЧІ ДАНИХ В МЕРЕЖАХ ЕНЕРГОМОНІТОРИНГУ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

01.05.02 – Математичне моделювання та обчислювальні методи
Технічні науки

Подається на здобуття наукового ступеня кандидата технічних наук. Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело


Ю. В. Ковальова

Науковий керівник Бабенко Тетяна Василівна, доктор технічних наук, професор

ДНІПРО – 2021

# АНОТАЦІЯ

**Ковальова Ю.В. Математичні моделі та методи бездротової передачі даних в мережах енергомоніторингу на об'єктах критичної інфраструктури.** – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 01.05.02 – Математичне моделювання та обчислювальні методи (12 – Інформаційні технології). – Національний технічний університет «Дніпровська політехніка», Національна металургійна академія України, Дніпро, 2021.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 01.05.02 – математичне моделювання та обчислювальні методи. Національний технічний університет «Дніпровська політехніка». Національна металургійна академія України, Дніпро, 2021.

В дисертації розв'язано важливу науково-прикладну задачу підвищення якості функціонування бездротових сенсорних мереж енергомоніторингу та збільшення часу їх життя за рахунок розробки відповідних математичних моделей і методів дослідження режимів енергоспоживання.

За результатами проведеного аналізу системно обґрунтовано, що з огляду на енергоємність процесу передачі даних, саме управління розмірами повідомлень є основним резервом збільшення терміну життя пристроїв і системи в цілому, а оптимізація енергоспоживання польових пристроїв бездротової мережі з автономним живленням на рівні користувальницького додатка дозволяє застосовувати приймально-передавачі різних виробників в пристроях збору і передачі даних.

В роботі розроблено математичну модель функціонування великомасштабних мереж на базі запитів БСМ, чиї вузли виявляють і ретранслюють події, які потрібні тільки протягом обмеженого часу. Це дозволило підвищити точність оцінки затримок передачі даних, розрахунку енергоємності та терміну служби мережі. Модифіковано протокол SCTMex,

який інкапсульовано в транспортний протокол ZigBee, що дозволило підвищити рівень захисту інформації на рівні польових пристроїв системи. Розроблено спеціалізовану програмно-апаратну платформу «Smart Utility Web» на базі бездротового модуля XBEE S2. Експериментальна експлуатація системи показала коректність підходу до побудови бездротової системи моніторингу на основі технології «роутерів, що прокидаються». Простота інсталяції обладнання системи і надійність захисту даних забезпечує високий рівень достовірності даних та експлуатаційних характеристик. Управління розміром блоків даних і шифруванням на рівні користувальницького додатка дозволяє домогтися оптимального з точки зору терміну життя системи енергоспоживання при збереженні необхідного рівня якості обслуговування.

**Ключові слова:** бездротова сенсорна мережа, енергомоніторинг, об’єкти критичної інфраструктури, математична модель, енергоспоживання, протокол.

# ABSTRACT

**Kovalova Yu. V. Mathematical models and methods of wireless data transmission in energy monitoring networks at critical infrastructure facilities.** – Qualifying scientific work. Manuscript.

A thesis for obtaining a scientific degree of the Candidate of Technical Sciences in the specialty 01.05.02 – Mathematical Modeling and Computational Methods. Dnipro University of Technology. National Metallurgical Academy of Ukraine, Dnipro, 2021.

This dissertation work is concerned with the important scientific and applied problem of increasing the quality of functioning of wireless sensor networks (WSN) for energy monitoring and increasing their life time was solved through the development of appropriate mathematical models and methods for studying energy consumption modes.

The analysis of research in the field of building distributed autonomous wireless monitoring systems showed that wireless sensor networks are a promising technology in the field of creating household and industrial data collection and control systems, and the key indicator of WSN that determines their applicability in practice is their lifetime. Based on the analysis results it was systematically substantiated that, taking into account the energy consumption of the data transmission process, the very control of message sizes is the main reserve for increasing the life of devices and the system as a whole, and optimization of the energy consumption of self-powered wireless field devices at the user application level allows the use of transceivers of various manufacturers in data collection and transmission devices.

The work developed a mathematical model of the functioning of large-scale networks based on requests from the wireless sensor network, which made it possible to increase the accuracy of estimating data transmission delays, calculating the power consumption and service life of the network. Relationships are given for determining the transmission time of messages taking into account the network and retransmission

delays, as well as the average time spent on the transmission of a frame in conditions of retransmissions. It should be noted that in general, the power consumption of network field devices depends on the characteristics of the hardware, the physical and link layer protocols, the routing protocol, and the network topology. This dissertation work formulates requirements to increase the WSN protection from attacks on field equipment and the system as a whole, which will not only protect the monitoring network, but also increase the guaranteed life of the network.

The SCTMex protocol has been modified. It is encapsulated in the ZigBee transport protocol, which made it possible to increase the level of information security at the level of system field devices. The SCTMex protocol is an extension of the SCTM protocol due to the few initial bytes of the data block. Analysis of the resistance of wireless monitoring networks to external attacks indicated their critical vulnerability due to the centralized architecture, so the most effective and efficient mechanism for protecting information in wireless monitoring networks is the transition to decentralized systems, including those based on blockchain technology. It is concluded that the most acceptable solution for WSN is a service or private blockchain, which allows the identification of field devices under the control of designated users.

In this work, a computer simulation of a wireless sensor network was carried out using the XCTU 6.3.5 platform for XBee/RF solutions from DIGI Int. This platform allows not only to perform all the module settings, scan a network of any configuration, but also perform network testing with the measurement of specific signal levels and delays that occur. A specialized software and hardware platform “Smart Utility Web” based on the XBEE S2 wireless module has been developed. The ease of installation of the system hardware and the reliability of data protection ensure a high level of data reliability and performance. By managing block size and encryption at the user application level, you can achieve optimal power consumption in terms of system lifespan while maintaining the required level of quality of service.

***Keywords:*** wireless sensor network, energy monitoring, critical infrastructure objects, mathematical model, power consumption, protocol.

# СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

*Роботи, в яких опубліковані основні наукові результати дисертації:*

1. **Почта Ю.В.,** Бабенко Т.В. Water supply systems in settlements of Ukraine. Науковий вісник НГУ, м. Дніпропетровськ, 2012 № 2. С. 105-108. ISSN: 2071-2227.

*(Наукове фахове видання, індексується в міжнародній реферативній наукометричній базі **Scopus**, National Library of Ukraine (Vernadsky), Index Copernicus).*

2. **Почта Ю.В.** Интеллектуальные информационно-управляющие системы водоснабжения и водопотребления. Регіональний міжвузівський збірник наукових праць «Системні технології», м. Дніпропетровськ, 2013, №3’(86). С.93-96. ISSN: 1562-9945.

*(Наукове фахове видання, індексується в національному електронному інформаційному ресурсі “Україна наукова”, National Library of Ukraine (Vernadsky), Index Copernicus).*

3. **Kovalova Y.**, Babenko T., Oksiiuk O., Myrutenko L. Optimization of Lifetime In Wireless Monitoring Networks. International Journal of Computing. Research Institute for Intelligent Computer Systems, 2020 № 19 (2), Pp. 267–272. ISSN: 2312-5381.

*(Індексується в міжнародній реферативній наукометричній базі **Scopus**, National Library of Ukraine (Vernadsky), Index Copernicus**, Google Scholar)**.*

4. **Ковальова Ю.В.** Математичне моделювання процесу бездротової передачі даних в мережах енергомоніторингу. Регіональний міжвузівський збірник наукових праць «Системні технології». м. Дніпро, 6 (131) 2020. С.186-195. ISSN: 1562-9945.

*(Наукове фахове видання, індексується в національному електронному інформаційному ресурсі “Україна наукова”, National Library of Ukraine (Vernadsky), Index Copernicus*).

5. **Ковальова Ю.В.** Моделювання топології бездротових сенсорних мереж. Регіональний міжвузівський збірник наукових праць «Системні технології», м. Дніпро, 1 (132) 2021. С.92-98. ISSN: 1562-9945.

*(Наукове фахове видання, індексується в національному електронному інформаційному ресурсі "Україна наукова", National Library of Ukraine (Vernadsky), Index Copernicus).*

6. **Kovaleva Yuliia**, Babenko Tetiana, Ignisca Vira. Models And Methods Of Wireless Decentralized Networks for Energy Monitoring of Critical Infrastructure Facilities. Scientific and practical cyber security journal. Georgia. **Issue No:** 4, December, 2020. P.74-78. ISSN: 2587-4667.

*(Закордонне періодичне видання).*

7. ***Kovalova Y.**, Babenko T.* The representative of national problems in the field of cybersecurity. Power engineering and information technologies in technical objects control. / London: Taylor & Francis Group: CRC Press / Balkema. London, UK 2016. P. 151-155. DOI: https://doi.org/10.1201/9781315197814.

*(Закордонне видання).*

8. Ковальова Ю.В. Технологические аспекты беспроводных сетей мониторинга. Монографія «Innovative Technologies in the Formation and Development of Human Capital», Вища Технічна Школа, м. Катовіца, Польша, 2018. С. 27-37.

9. **Почта Ю.В.**, Система дистанционного считывания показаний и управления энергопотреблением «EnergyWeb-XB». Международный электротехнический журнал «Электрик», м. Київ, 2009 №9. С. 31-33.

10. **Почта Ю.В.**, Ленда І.В. Интеллектуальные системы энергоучета. Журнал «Мир Автоматизации», м. Київ №2, 2010. С. 48-51.

*Роботи, які засвідчують апробацію матеріалів дисертації:*

11. Babenko T., Toliupa S., **Kovalova Y.** LVQ models of DDOS attacks identification. 14 th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), Lviv, 2018, pp. 510-513, doi: 10.1109/TCSET.2018.8336253.

*(Індексується в міжнародній реферативній наукометричній базі **Scopus**).*

12. **Почта Ю.В.** Захист та впровадження бездротових систем моніторингу, II Всеукраїнська науково-практична конференція «Системний аналіз. Інформатика. Управління. САІУ-2011, м. Запоріжжя, 10-11 березня 2011. С. 162-163.

13. **Kovalova Y.**, Oksiiuk O., Babenko T. The Optimization of Lifetime in Wireless Monitoring Network. The 4th IEEE International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems. Lviv Polytechnic National University. Lviv 20-21 September 2018.

14. Бабенко Т.В., Толюпа С.В., **Ковальова Ю.В.** Моделі ідентифікації мережевих аномалій на основі карти самоорганізації. VII міжнародна науково-технічна конференція «ITSEC». Київ, 16 травня 2017.

15. **Ковальова Ю.В.**, Бабенко Т.В. Аналіз вразливостей інтелектуальних лічильників в бездротовій мережі моніторингу енергоресурсів. Київський національний університет імені Тараса Шевченка, Збірник матеріалів доповідей та тез I Міжнародна науково-практична конференція «Проблеми кібербезпеки інформаційно-телекомунікаційних систем». М. Київ 5-6 квітня 2018. С. 24-26.

16. **Ковальова Ю.В.**, Бабенко Т.В. Нейромережеві моделі ідентифікації DDoS атак. XX Ювілейна Міжнародна науково-практична конференція «Безпека інформації в інформаційно-телекомунікаційних системах», Буча, 22-24 травня 2018.

17. **Ковальова Ю.В.**, Бабенко Т.В. Застосування технології блокчейн в енергетичних системах. VII Міжнародна науково-практична конференція «Фізико-технологічні проблеми передавання, оброблення та зберігання інформації в інфокомунікаційних системах». М. Чернівці, 8-10 листопада 2018.

18. **Kovalova Y.**, Babenko T. The Discrete Model of Dynamic Energy Systems and Reliability of Data Consumption. VI MIĘDZYNARODOWA KONFERENCJA STUDENTÓW ORAZ DOKTORANTÓW «INŻYNIER XXI WIEKU». Bielsko-Biała, 2016. P. 181-184. ISBN 978-83-65182-51-7.

19. **Почта Ю.В.**, Кузнецов Г.В. Исследование беспроводной технологии ZigBee в области защиты информации. V miedzynarodowej naukowi-praktycznej konferecji «Europejska nauka XXI powieka», Przemysl, 5-15 травня 2009. С. 60-61. ISBN: 978-966-8736-05-6.

20. **Почта Ю.** Управление энергоресурсами на базе беспроводных технологий передачи данных. VIII mezinarodni vedecko-prakticka conference “Moderni vymozenosti vedy”, Publishing House “Education and Science”, Praha, 27 січня – 5 лютого 2012. С. 78-81. ISBN: 978-966-8736-05-6

21. **Kovalova Y.**, Mieshkov V. Information protection in communication networks. Virtual conference «Information Technologies in Science & Education», India, Ukraine, Spain, Italy.

22. **Почта Ю.** Новітні технології у сфері ЖКГ. Вісник Дніпропетровської міської ради. М. Дніпропетровськ 2009 №009.

23. **Почта Ю.В.** Интеллектуальные информационно-управляющие системы, Научно-техническая конференция «Информационные технологии в металлургии и машиностроении. ІТММ-2013», м. Дніпропетровськ, 26-28 березня 2013.

24. **Ковальова Ю.В.** Особливості використання протоколу SCTM в інтелектуальних мережах Smart Grid. Збірник матеріалів доповідей та тез XVIII Міжнародної науково-практичної конференції «Безпека інформації у інформаційно-телекомунікаційних системах», м. Київ, 2016, стор. 54.

25. **Ковальова Ю.В.** Проблеми в сфері забезпечення кібернетичної безпеки об’єктів критичної інфраструктури. Збірник матеріалів доповідей та тез VII Науково-практична конференція «Актуальні проблеми управління інформаційною безпекою держави», м. Київ 2016.

26. **Ковальова Ю.В.**, Бабенко Т.В. Забезпечення кібербезпеки об’єктів енергетичної інфраструктури. Збірник матеріалів доповідей та тез II науково-практична конференція «Проблеми безпеки інформаційно-телекомунікаційних систем», м. Київ, 23-24 березня 2017. С. 121-123.

27. **Ковальова Ю.В.** Моделі ідентифікації мережевих аномалій на основі карти самоорганізації. Збірник матеріалів доповідей та тез VII міжнародної науково-технічної конференції «ITSEC», м. Київ 2017.

28. Твердохліб І.С., **Ковальова Ю.В.** Управління інцидентами кібербезпеки на малих комерційних підприємствах. Збірник матеріалів доповідей та тез. П’ята всеукраїнська науково-технічна конференція студентів, аспірантів і молодих учених «Молодь: наука та інновації 2017». Національний технічний університет «Дніпровська політехніка», м. Дніпро, 2017. Т.12. С.9-10.

29. **Ковальова Ю.В.** Інформаційна безпека бездротових мереж моніторингу. Збірник матеріалів доповідей та тез. П’ята всеукраїнська науково-технічна конференція студентів, аспірантів і молодих учених «Молодь: наука та інновації 2017». Національний технічний університет «Дніпровська політехніка», м. Дніпро, 2017. Т.12. С.40-42.

30. Доколяса О.С., **Ковальова Ю.В.** Кібербезпека в інформаційному просторі України. Збірник матеріалів доповідей та тез. П’ята всеукраїнська науково-технічна конференція студентів, аспірантів і молодих учених «Молодь: наука та інновації 2017». Національний технічний університет «Дніпровська політехніка», м. Дніпро, 2017. Т.12. С.34-35.

31. **Ковальова Ю.В.**, Бабенко Т.В. Нейромережеві моделі ідентифікації DDoS атак. Збірник матеріалів доповідей та тез XX Міжнародної науково-практичної конференції «Безпека інформації в інформаційно-телекомунікаційних системах», м. Буча, 2018. С. 32-33.

32. Кручінін О.В., Тимофєєв Д.С., **Ковальова Ю.В.** Інформаційна безпека бездротових мереж моніторингу. Збірник матеріалів доповідей та тез XX Міжнародної науково-практичної конференції «Безпека інформації в інформаційно-телекомунікаційних системах», м. Буча, 2018. С. 247.

# ЗМІСТ

# ПЕРЕЛІК СКОРОЧЕНЬ

БММ – бездротова мережа моніторингу;

БСМ – бездротова сенсорна мережа;

ПЗПД – пристрій збору та передачі даних;

СУБД – системи управління базами даних;

AODV – Ad Hoc On-Demand Distance Vector;

BFT – Bytantine Fault Tolerant;

DNP – Distributed Networking Protocol;

EPA – Enhanced Performance Architecture;

ERPI – Electric Power Research Institute;

FFD – Full Function Device;

HAN – home area network;

IEEE – Institute of Electrical and Electronics Engineers;

IoT – Internet of Things;

ISDN – Integrated Services Digital Network – Цифрова Мережа з Інтегрованими Послугами;

ISM – industrial, scientific and medical – є частиною радіочастотного спектра загального призначення, яка може бути використана без ліцензування;

MEPS – Minimum Energy Performance Standard;

PAN ID – personal area network ID;

PWAN – Low-power Wide-area Network;

RFD – Reduced Function Device;

SCTM – Serial Coded Tele-Metering;

QoS – Quality of Service;

UCA – Utility Communications Architecture;

WSN – Wireless Sensor Networks.

# ВСТУП

Розробка інтелектуальних систем обліку та управління споживанням енергетичних ресурсів на об’єктах критичної інфраструктури, зокрема в сфері житлово-комунального господарства є актуальним і складним завданням. В його вирішенні зацікавлені споживачі і постачальники ресурсів, а також компанії, що займаються їх розподілом [21]. Останні досягнення технологічного прогресу зробили можливим створення мініатюрних приймачів з надзвичайно малим енергоспоживанням, здатних об’єднуватися в мережу і взаємодіяти один з одним за допомогою бездротових каналів зв’язку. Мережі таких пристроїв отримали назву бездротових мереж моніторингу (БММ), що, зокрема, підкреслює їх основне призначення – збір даних з датчиків (лічильників) для подальшого аналізу і передачі керуючих команд. Незважаючи на видимі переваги і потенційні можливості бездротових мереж, вони ще далекі від використання в повсякденному житті. На сьогоднішній день розроблено велику кількість різних реалізацій бездротових мереж, однак всі вони оптимізовані для вирішення окремих прикладних завдань і для оцінки продуктивності тієї чи іншої мережі необхідно розробляти методики, що дозволяють оцінити функціонування мережі у цілому. Таким чином, завдання розробки моделей і алгоритмів просторової організації зони покриття бездротових мереж є центральною при підвищенні якості обслуговування і скороченні часу передачі даних.

Під бездротовою сенсорною мережею (БСМ) розуміється розподілена мережа сенсорів (інтелектуальних автономних електронних пристроїв), кожен з яких оснащений елементом живлення обмеженої потужності, втрати якої в одиницю часу залежать від значень параметрів сенсорів в активному стані. Основним критерієм якості БСМ є час її життя, збільшення якого досягається, зокрема, мінімізацією енерговитрат БСМ. Однією з проблем, що перешкоджають підвищенню енергоефективності БСМ, є проблема нерівномірного споживання енергії вузлами мережі. Для збільшення часу життя

БСМ необхідно вирішити цілий ряд задач, зокрема оптимальне розміщення сенсорів, визначення зони дії, а також дальності передачі і пошук оптимального розкладу активності кожного сенсора. Внесок у вирішення зазначених задач внесли В.М. Вишневський, В.С. Жданов, А.П. Кулешов, А.І. Ляхов, І.А. Мізін, О.Е. Кучерявий, Е.А. Саксонов, S. Borst, O. Boxma, M. Conti, R.G. Gallager, L. Kleinrock, P. Kyasanur, M. Neuts, C. Perkins, E. Royer, H. Takagi, W. Willinger, P. Abry та ін. дослідники. Завдяки роботам вчених існує ряд методів, спрямованих на вирішення зазначених завдань. До них відносяться програмна оптимізація канального рівня протоколу мережі, індивідуальний підбір ємності батарей, щільності розміщення вузлів, потужності передавачів, позиціонування вузлів мережі. Разом з тим, ефективному вирішенню цих завдань перешкоджає як відсутність математичних моделей, що описують зміну енергоспоживання пристроїв в динаміці при зовнішньому втручанні в роботу мережі на фізичному і канальному рівнях, так і існуючі припущення про критичну важливість часу активного режиму роботи приймально-передавального тракту польових пристроїв. У зв’язку з цим завдання дослідження режимів енергоспоживання та розробка математичних моделей бездротової передачі даних в мережах енергомоніторингу, що дозволяють не тільки оцінити час життя автономних мереж, але і оптимізувати їх роботу за критерієм максимізації часу життя, є актуальною.

**Зв’язок роботи з науковими програмами, планами, темами.** Тематика роботи відповідає вимогам, встановленим Законом України «Про пріоритетні напрями розвитку науки і техніки» (від 16 січня 2016 року, №848-VIII), у тому числі розділам «Фундаментальні наукові дослідження з найбільш важливих проблем розвитку науково-технічного, соціально-економічного, суспільно-політичного, людського потенціалу для забезпечення конкурентоспроможності України у світі та сталого розвитку суспільства і держави».

**Метою роботи** є підвищення якості функціонування бездротових сенсорних мереж енергомоніторингу та збільшення часу їх життя за рахунок

розробки відповідних математичних моделей і методів дослідження режимів енергоспоживання.

**Об’єктом дослідження** є процеси мережевої взаємодії, характеристики елементів в інфраструктурі автономної системи моніторингу управління енергоспоживанням.

**Предметом дослідження** є математичні моделі передачі трафіку та продуктивності мереж; методи аналізу інформаційних потоків, дослідження яких дозволяє розробити найбільш ефективні засоби моніторингу та управління енергоспоживанням.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

1. Провести системний аналіз досліджень в області побудови розподілених автономних бездротових систем моніторингу. Проаналізувати існуючі апаратно-програмні платформи децентралізованих бездротових мереж енергомоніторингу, що самоорганізуються. Виконати аналіз чинників, що впливають на час життя бездротових мереж моніторингу з автономним живленням. Дослідити енергоспоживання польових пристроїв при номінальних режимах експлуатації і в разі зміни умов функціонування мережі.
2. Розробити математичну модель для оцінки ефективності великомасштабних мереж на базі запитів бездротових сенсорних мереж, чиї вузли виявляють і ретранслюють події, які корисні тільки протягом обмеженого часу.
3. Встановити фактори, що зумовлюють надійність та якість обслуговування автономних бездротових систем моніторингу за час їх життя впродовж міжповірочного інтервалу.
4. Модифікувати та адаптувати транспортний протокол SCTM для врахування перешкод розповсюдженню радіосигналу і затримок в мережі передачі даних у відкритому ISM-діапазоні.

5. Розробити комплекс програм параметризації, обліку та управління польовими пристроями бездротової системи енергомоніторингу об’єктів комунального господарства.

**Методи дослідження** базуються на теорії систем і мереж масового обслуговування, теорії математичного моделювання, теорії графів, теорії обробки експериментальних даних, теорії прийняття рішень та оптимізації, теорії дослідження операцій, теорії ймовірності та математичної статистики.

**Наукова новизна одержаних результатів.**

1. Вперше розроблено математичну модель функціонування великомасштабних мереж на базі запитів БСМ, чиї вузли виявляють і ретранслюють події, які потрібні тільки протягом обмеженого часу. Це дозволило підвищити точність оцінки затримок передачі даних, розрахунку енергоємності та терміну служби мережі.

2. Вперше запропоновано механізм динамічної адресації польових пристроїв бездротової Інтернет-системи збору даних і управління енергоспоживанням, що унеможливлює віддалене стороннє втручання в роботу сегментів системи.

3. Вперше модифіковано протокол SCTMex, який інкапсульовано в транспортні протоколи ZigBee і LoRa, що дозволяє підвищити рівень захисту інформації на рівні польових пристроїв системи.

4. Удосконалено математичну модель оцінки працездатності польових пристроїв з автономним живленням і модернізовано архітектуру системи, в результаті чого час життя системи перевищив нормативний період повірки приладів обліку.

5. Дістала подальшого розвитку методика побудови захищеної мережі передачі даних і системи в цілому, що базується на розроблених автором вимогах і моделях, в тому числі перехід до децентралізованої архітектури систем, побудованих на принципах технології блокчейн. Зокрема, це дозволяє проводити ідентифікацію польових пристроїв під контролем призначених користувачів.

**Практична цінність одержаних результатів.** Практичне значення дисертації підтверджується впровадженнями результатів роботи у практику робіт АТ «ДТЕК Дніпровські електромережі» (м. Дніпро) при побудові системи комерційного обліку електроенергії компанії, в ПрАТ «Дніпрополімермаш» під час побудови системи комерційного обліку води, газу та електроенергії товариства, в ТОВ «ЛЕД Азімут» (м. Кам'янське) під час адаптації системи моніторингу та управління загальним освітленням «Smart Lighting Web-ZB», у Департаменті екологічної політики Дніпровської міської ради (м. Дніпро) під час побудови системи моніторингу якості поставок води промисловим і побутовим споживачам.

Практична значущість одержаних результатів полягає у наступному:

- Розроблено апаратну платформу і програмне забезпечення бездротової Інтернет-системи енергомоніторингу. Платформа дозволяє в рамках єдиної системи застосувати стандартні апаратні засоби провідних виробників, які працюють на різних частотах безліцензійного ISM діапазону.
- З метою підвищення рівня захищеності мережі модернізований протокол SCTMex інкапсульовано в протокол транспортного рівня.

**Достовірність та обґрунтованість результатів** дисертації підтверджуються коректним використанням методів математичного та імітаційного моделювання, теорії випадкових процесів з використанням сучасних уявлень про механізм передачі трафіка у бездротових мережах, їхнім узгодженням з відомими з літератури результатами. Отримані наукові результати є достовірними, забезпечуються коректним використанням математичного апарату та методами обробки інформації, а також шляхом валідації отриманих результатів на незалежних тестових даних. Матеріали дисертації неодноразово обговорювалися на міжнародних конференціях.

**Впровадження одержаних результатів.** Результати досліджень, виконаних у кандидатській дисертації, впроваджено:

1) в АТ «ДТЕК Дніпровські електромережі» (м. Дніпро) при побудові системи комерційного обліку електроенергії компанії.

2) в ПрАТ «Дніпрополімермаш» (м. Дніпро) під час побудови системи комерційного обліку води, газу та електроенергії товариства.

3) в ТОВ «ЛЕД Азімут» (м. Кам'янське) під час адаптації системи моніторингу та управління загальним освітленням «Smart Lighting Web-ZB».

4) Департамент екологічної політики Дніпровської міської ради (м. Дніпро) під час побудови системи моніторингу якості поставок води промисловим і побутовим споживачам.

5) в навчальний процес Національного технічного університету «Дніпровська політехніка».

**Особистий внесок здобувача.** Результати дисертаційної роботи, що виносяться на захист і складають наукову новизну виконаних досліджень, отримані особисто здобувачем. Усі одноосібні публікації за темою дослідження [2, 4, 5, 8, 9, 12, 20, 22-25, 27, 29 Додатку А] виконано авторкою самостійно. У роботах, написаних у співавторстві, авторці належать такі наукові результати: [1] – аналіз проблем водопостачання / водоспоживання з метою синтезу моделей для прогнозування параметрів технологічної системи, [3] – визначено основні вимоги до побудови бездротової моніторингової мережі з автономним живленням, що гарантує термін її функціонування, [6] – новий підхід до процесу управління енергоспоживанням польового обладнання, який враховує стохастичність змінних і адаптує прогнозні моделі для компенсації запізнювання передачі даних та затримки сигналів, [7] – виявлені характерні ознаки проблемних питань в існуючій законодавчій базі України в сфері кібербезпеки об'єктів критичної інфраструктури, [10] – метод перетворення мереж енергопостачання в інтелектуальні мережі, [11] – загальний підхід до синтезу ідентифікаційних моделей на основі нейронних мереж, [13] – модель бездротової мережі, що дозволяє оцінювати час її життя за енергетичними

параметрами, [14] – математичні моделі ідентифікації мережевих аномалій, [15] – аналіз вразливостей інтелектуальних лічильників в бездротовій мережі моніторингу енергоресурсів, [16] – побудовано моделі ідентифікації DDoS атак, [17] – вивчення можливості та ефективності використання технології блокчейн до вирішення проблем безпеки об'єктів критичної інфраструктури, [18] – визначення динамічних властивостей системи енергопостачання і структурування рішень в термінах апаратного і програмного забезпечення, [19] – використання безпровідної системи передачі даних енергоносіїв з використанням протоколу Zigbee, [21] – розглянуто ступінь уразливості інтелектуальної мережі обліку та моніторингу електроенергії та проведено аналіз основних видів загроз, [26] – розробка механізмів захисту від APT-атак в системах енергомоніторингу, [28] – метод управління інцидентами в інтелектуальних мережах передачі даних, [30, 32] – аналіз уразливості безпровідної інтелектуальної мережі обліку та моніторингу електроенергії, [31] – побудова моделей на основі нейронних мереж для управління системами в кіберпросторі (Додаток А).

**Апробація результатів дисертації.** Результати дисертаційної роботи доповідались і обговорювались на наукових семінарах кафедри безпеки інформації та телекомунікацій Національного технічного університету «Дніпровська політехніка»; на наукових семінарах кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка; на 14 International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET) (Україна, Львів, 2018); на Всеукраїнській науково-практичній конференції «Системний аналіз. Інформатика. Управління. САІУ-2011» (Україна, м. Запоріжжя, 10-11 березня 2011); на «The 4$^{th}$ IEEE International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems» (Україна, м. Львів, 20-21 вересня 2018); на VII міжнародній науково-технічній конференції «ITSEC» (Україна, м. Київ, 16 травня 2017); на I

Міжнародній науково-практичній конференції «Проблеми кібербезпеки інформаційно-телекомунікаційних систем» (Україна, м. Київ 5-6 квітня 2018); на XX Ювілейній Міжнародній науково-практичній конференція «Безпека інформації в інформаційно-телекомунікаційних системах» (Україна, м. Буча, 22-24 травня 2018); на VII Міжнародній науково-практичній конференції «Фізико-технологічні проблеми передавання, оброблення та зберігання інформації в інфокомунікаційних системах» (Україна, м. Чернівці, 8-10 листопада 2018); на VI MIĘDZYNARODOWA KONFERENCJA STUDENTÓW ORAZ DOKTORANTÓW «INŻYNIER XXI WIEKU». (Польша, Бяско Бяла, 2016); на V miedzynarodowej naukowi-praktycznej konferecji «Europejska nauka XXI powieka», (Чехія, Прземісл, 5-15 травня 2009); на VIII mezinarodni vedecko-prakticka conference «Moderni vymozenosti vedy», (Чехія Прага, 27 січня – 5 лютого 2012); на Virtual conference «Information Technologies in Science & Education» (Україна, Іспанія, Індія, Італія, 2018); на научно-технічній конференції «Інформаційні технології в металургіі та машинобудівництві ITMM-2013» (Україна, м. Дніпропетровськ, 26-28 березня 2013); на XVIII Міжнародній науково-практичній конференція «Безпека інформації у інформаційно-телекомунікаційних системах» (Україна, м. Київ, 2016); на VII Науково-практичній конференції «Актуальні проблеми управління інформаційною безпекою держави» (Україна, м, 2016); на II науково-практичній конференції «Проблеми безпеки інформаційно-телекомунікаційних систем». (Україна, м. Київ, 23-24 березня 2017); на VII міжнародній науково-технічній конференції «ITSEC» (Україна, м. Київ 2017); на 5 Всеукраїнській науково-технічній конференція студентів, аспірантів і молодих учених « Молодь: наука та інновації 2017» (Україна, м. Дніпро, 2017); на XX Міжнародній науково-практичній конференція «Безпека інформації в інформаційно-телекомунікаційних системах» (Україна, м. Буча, 22-24 травня 2018).

**Публікації.** Основні результати дисертаційної роботи опубліковано у 32 наукових робітах, 13 з яких – без співавторів. П’ять статей опубліковано в наукових фахових виданнях України, 3 статті – у закордонних виданнях, 3 роботи індексуються в міжнародній наукометричній базі Scopus; 22 роботи опубліковано у збірниках матеріалів і тез міжнародних та всеукраїнських конференцій.

**Структура та обсяг роботи.** Дисертація складається із вступу, чотирьох розділів, висновків, списку використаних джерел, що налічує 110 найменувань, трьох додатків. Загальний обсяг дисертації – 165 сторінок, обсяг основної частини – 135 сторінок. Робота проілюстрована 62 рисунками та містить 19 таблиць.

# РОЗДІЛ 1 ОГЛЯД ІСНУЮЧИХ РІШЕНЬ ЗБІЛЬШЕННЯ ЧАСУ ЖИТТЯ БЕЗДРОТОВИХ МЕРЕЖ МОНІТОРИНГУ

## 1.1. Основні поняття бездротових мереж моніторингу

Бездротові мережі знаходять своє застосування в системах моніторингу та управління об’єктами житлово-комунального господарства. Вони є однією з базових технологій інтернету речей, що дозволила розвинути на їх базі концепцію Smart City.

Бездротова сенсорна мережа (БСМ) моніторингу енергоспоживання являє собою розподілену самостійну конфігурацію бездротову мережу, що складається з інтелектуальних пристроїв збору та передачі даних. Кожний пристрій оснащений мікроконтролером, прийомо-передавачем, елементом живлення і через відповідний інтерфейс підключено до лічильника або датчику.

БСМ є окремим випадком ситуаційних (в англомовній літературі – ad hoc) мереж, що представляють собою розподілені системи рівноправних вузлів, в яких кожен вузол може обмінюватися даними з кожним зі своїх сусідів. Виходячи з цього, виділяються три основні типи мережевих вузлів: кінцевий пристрій, маршрутизатор, координатор. Кінцеве пристрій виконує функції збору даних з лічильників і датчиків з подальшою передачею їх в мережу. Як правило, більшу частину часу він знаходиться в режимі зниженого енергоспоживання, в якому основні споживачі енергії – приймачі вимкнені. Маршрутизатор представляє собою елемент мережі, що виконує функції ретрансляції даних, що приходять з кінцевих пристроїв, до точки збору даних (координатору). Координатор (шлюз) є елементом, який приймає дані з усієї мережі і передає їх по провідному або бездротовому інтерфейсу. Як правило, координатор має постійне джерело живлення і, на відміну від інших вузлів мережі, не обмежений в ресурсах. Такий поділ використовується для побудови централізованих систем моніторингу та управління, в яких координатор або сам

обробляє інформацію з усієї мережі, або передає її на пристрій з великою кількістю ресурсів (наприклад, сервер системи).

### 1.1.1. Основні стандарти в області бездротових сенсорних мереж

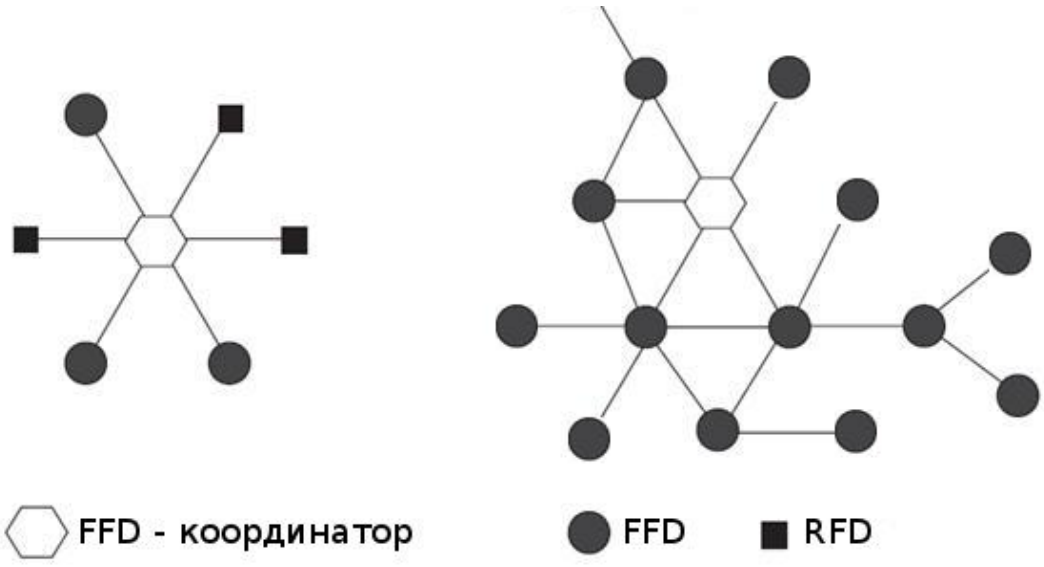
В Європейському Союзі і в Україні діє стандарт бездротової шини WM-Bus EN 13757-4 «Системи зв'язку для лічильників і дистанційне зчитування лічильників. Частина 4. Бездротове зчитування показань лічильника (читання показань лічильника в SRD – Short Range Device діапазоні 868 Мгц)» [14]. Цей стандарт визначає вимоги до параметрів фізичного і канального рівнів для систем, що використовують приймач для дистанційного зчитування лічильників. Типовим застосуванням WM-Bus є організація збору показників лічильників споживання ресурсів на стаціонарний або мобільний концентратор, який згодом передає їх для подальшої обробки. Основна топологія мережі WM-Bus – «точка-точка» або «зірка». WM-Bus застосовується переважно для приладів обліку електричної енергії (електролічильники), теплової енергії (теплолічильники), витратомірів води та газу. Дані передаються на комп'ютерну станцію (сервер) безпосередньо або через концентратори шини WM-Bus, а також підсилювачі-повторювачі сигналу. Це накладає певні обмеження на розмір системи в кількісному, з точки зору застосування комутаційного обладнання на максимально можливий адресний простір однієї мережі, і якісному (можливий обсяг переданих даних) аспектах.

Однією з основних проблем при впровадженні інтелектуальних лічильників енергоресурсів є інтеграція окремих лічильників в мережу для централізованого збору даних. Єдиного рішення цього завдання не існує – крім технічних проблем, виникає безліч інших. В якості носія даних зручніше вибрати радіоканал, що дозволяє не залежати від розташування датчиків і центрального вузла. При цьому можлива робота в так званому ISM-діапазоні частот [33]. На даний момент для організації систем обліку або окремих їх частин можливе застосування таких технологій як ZigBee [105, 106], Wi-Fi,

Bluetooth Low Energy. Бездротові мережі на сьогоднішній день є досить добре стандартизовані.

Основним з існуючих стандартів, на якому засновані мережі, що мають практичне і комерційне значення є IEEE 802.15.4. Стандарт IEEE 802.15.4 [30] Описує фізичний і канальний рівні еталонної моделі OSI. Більш високі рівні доповнюються в специфікаціях, наприклад, ZigBee [74, 75]. Стандарт передбачає роботу в трьох частотних діапазонах: один канал 868,0-868,6 МГц, 10 каналів в діапазоні 902-928 МГц і 16 каналів в діапазоні 2400-2483,5 МГц.

Мережа стандарту IEEE 802.15.4 містить два типи пристроїв – повнофункціональні (FFD – Full Function Device) і пристрої зі зменшеною функціональністю (RFD – Reduced Function Device). За принципом FFD працюють координатор і маршрутизатори мережі, по принципу RFD – кінцеві пристрої. Кожна мережа має свій ідентифікатор (PAN ID – personal area network ID) [5,8, 9, 49, 52, 60]. Мережа, що складається з одного FFD і декількох RFD, утворює топологію типу «зірка» (рис.1.1а) [17]. У загальному випадку вона має вигляд мережі P2P (peer-to-peer) (рис.1.1б). З точки зору досліджуваного питання практичне значення має Mesh-мережа з однотипними пристроями – роутерами (рис.1.2).




а) б)

Рисунок 1.1 – Види толологій мереж стандарту IEEE 802.15.4

У кожного пристрою мережі є унікальна 64-розрядна MAC-адреса, що, як правило, записується в пам’ять виробником. Для спрощення обміну всередині мережі координатор може призначати пристроям коротші 16-розрядні адреси. Інформаційний обмін в мережі відбувається за допомогою послідовності суперфреймів (superframe). У загальному випадку суперфрейм включає керуючий інтервал (beacon), за ним йде інтервал конкурентного доступу відповідно до механізму CSMA/CA (випадковий множинний доступ з контролем несучої і запобіганням колізій) [45] і період призначеного доступу. Останній містить набір часових інтервалів, призначених певним пристроям, чутливим до затримок, для передачі даних (гарантовані тайм слоти, GTS).

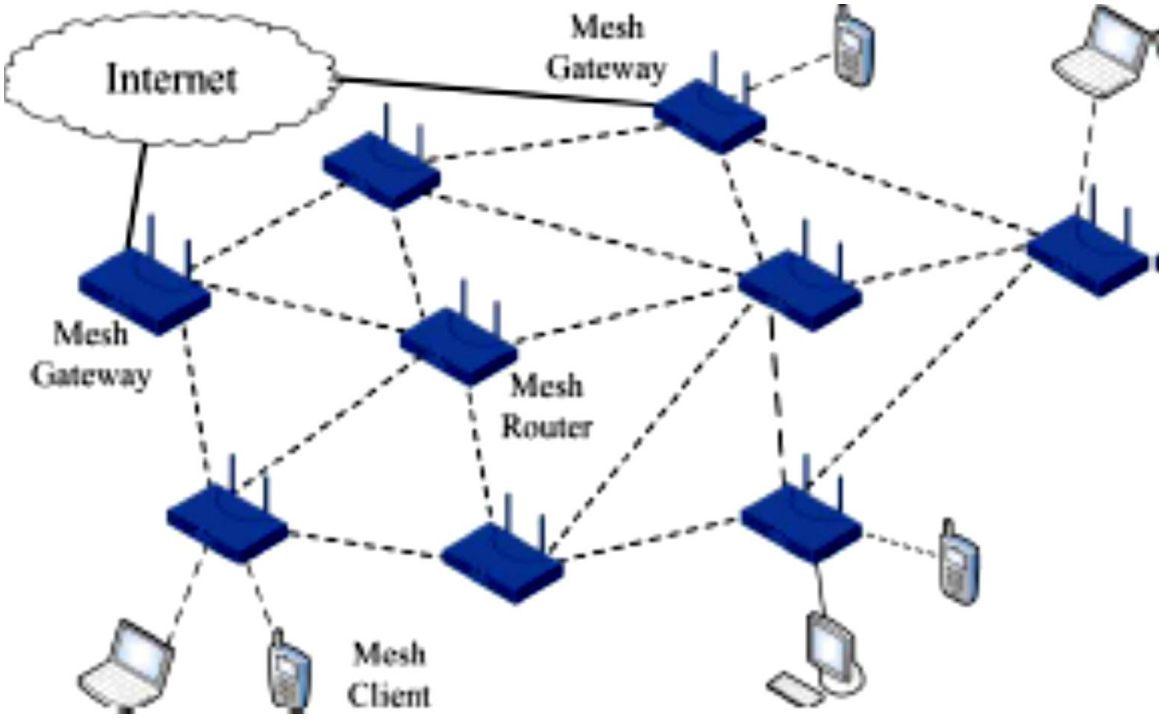



Рисунок 1.2 – Mesh-топологія

Кожен пристрій передає інформацію за допомогою фреймів (пакетів). Вони можуть бути чотирьох типів – керуючі, фрейми даних, фрейми підтвердження прийому даних і фрейми команд MAC-рівня. Більш докладно формати фреймів розглядаються у другому розділі дисертації з точки зору розрахунку споживаної потужності пристроїв.

ZigBee / ZigBee Pro

Специфікація ZigBee [74, 75] доповнює верхні рівні еталонної моделі OSI, використовуючи IEEE 802.15.4 в якості своєї основи. Зокрема, специфікація визначає алгоритми маршрутизації в комірчастій мережі, коли між парою вузлів може бути кілька маршрутів. З огляду на сильну обмеженість в ресурсах сенсорних вузлів і невелику пропускну здатність каналу зв'язку, що виключають можливість регулярного обміну службовою інформацією, використовується спеціальний протокол маршрутизації AODV [11, 53] з обчисленням маршруту на вимогу. Відповідно до даного протоколу, перед тим, як відправити дані віддаленого вузла, відбувається виявлення найкращого шляху через розсилку спеціального запиту на передачу. Це дозволяє уникнути постійного зберігання великих за обсягом таблиць маршрутизації в пам’яті вузлів. Іншою особливістю специфікації ZigBee є детальний опис сервісів користувальницького рівня, спрямований на забезпечення сумісності обладнання різних виробників. З огляду на критичну уразливість базових профілів їх застосування в системах моніторингу не є виправданим.

ZigBee PRO Green Power

Розвитку специфікації на енергоефективні застосування сприяли два основні чинники: створення мікроконтролерів і приймачів з дуже малою споживаною потужністю і створення перетворювачів альтернативної енергії малих розмірів (Micro Energy Harvesters, MEH). На даний момент найбільш ефективними є конвертори на основі п’єзомеханічних генераторів, фотоелементів, термоелектричних перетворювачів. Як наслідок, стало можливим створення повністю автономних пристроїв збору даних, які споживають не більше 200 мікроджоулів на годину. Таким чином, при моделюванні процесу прийому-передачі даних можна застосовувати розроблені раніше моделі. БСМ розраховані на передачу невеликих обсягів даних малої частоти – це дозволяє переводити пристрої в режим низького споживання енергії для збільшення часу їх автономної роботи. Тому актуальним завданням

є дослідження і розробка моделей, що описують мережу з точки зору потужності, споживаної пристроями.

### 1.1.2. Моделі передачі даних у бездротових сенсорних мережах

Прийнято виділяти чотири базові моделі збору даних в БСМ: подієва, передача за розкладом, передача на вимогу, передача за запитом [81].

1. Подієва модель використовується в мережах, які фіксують деякі події в певній галузі, наприклад спрацьовування датчика, вихід фізичного параметра за допустимий діапазон, близькість розряду акумулятора і ряд інших. Важливою особливістю є те, що в загальному випадку точний час настання подій ніяк не можна передбачити, тому при дослідженні мереж використовуються імовірнісні характеристики виникнення подій як випадкового процесу. Як правило, до самої мережі пред'являються деякі вимоги за максимальною затримки передачі інформації про подію в центр збору даних.

2. При передачі за розкладом, так само як і в подієвій моделі, процес відправки повідомлень ініціюється елементами системи, а не центром збору даних, проте він прив'язаний до певного розкладу, що дає можливість синхронізувати роботу вузлів мережі.

3. Збір даних за запитом застосовується в системах, що накопичують інформацію про графік споживання, щоб потім на вимогу передати її на сервер.

4. Часто застосовується гібридна модель, що поєднує в собі особливості перших трьох. Наприклад, повідомлення про добові енергоспоживання абонентів можуть передаватися через фіксовані інтервали, в той же час інформація про виникаючі події передається згідно подієвої моделі [81].

Далі в дисертаційній роботі розглядаються мережі, що працюють за першими двома моделями, тобто будь-яка передача даних ініціюється елементами системи, а не центром збору даних.

## 1.2. Час життя бездротової мережі моніторингу

Концепція сенсорних мереж передбачає, що будь-який вузол працює від автономного джерела живлення. Якщо таким джерелом є звичайний акумулятор (типорозміри AAA, AA і 18650), то в певний момент часу він розряджається і автономний пристрій перестає працювати. Оскільки будь-який елемент мережі виконує певний набір завдань, вихід з ладу може означати наступне: в разі, якщо набір завдань, що виконується вузлом некритичний, то можна говорити про падіння якості обслуговування мережі; якщо вузол є ключовою ланкою системи, виконуючи завдання маршрутизації потоків даних, то його відмова і неможливість заміни маршруту означає відмову всієї мережі.

Поняття якості обслуговування (QoS), в тому числі стосовно БСМ, детально досліджується в роботах [4, 12, 34, 59, 66, 69].

Якість обслуговування визначає, чи може мережа надати необхідний сервіс з передачі даних при заданих умовах [62]. Іншими словами, якість обслуговування є інтегральною характеристикою і описується набором параметрів. У класичних мережах в якості таких параметрів використовують смугу пропускання, затримки при передачі пакетів, а також ймовірність доставки пакета. На відміну від класичних мереж бездротові мережі моніторингу надають сервіс не тільки з передачі даних, але також і зі збору та їх обробці. Відповідно якість обслуговування в бездротових сенсорних мережах і його показники будуть відрізнятися від класичного уявлення. До характеристик якості обслуговування в бездротових сенсорних мережах відносять такі параметри як: затримка, пропускна здатність, втрати, час життя мережі, покриття заданої області, стійкість до зміни топології [4, 66]. Параметри якості обслуговування найчастіше пов’язані між собою. У табл. 1.1 наведені фактори, що впливають на характеристики якості обслуговування, що відносяться до того чи іншого рівня мережевої моделі [4].

Таблиця 1.1 – Взаємозв’язок характеристик якості обслуговування відповідно мережевої моделі

| Характеристика якості обслуговування | Фізичний рівень | Канальний рівень | Мережевий рівень |
|---|---|---|---|
| затримка | спосіб кодування | розклад доступу до каналу | час визначення маршруту, довжина шляху |
| пропускна спроможність | розмір повідомлень | синхронізація доступу до каналу, надлишкові пакети | маршрутизація по декількох шляхах, додаткові дані маршрутизації в пакеті |
| втрати | рівень шуму | колізії | тупикові маршрути, зациклення |
| час життя мережі | спосіб кодування, потужність передачі | час активного або пасивного режимів, повторна передача пакетів | використання одних і тих же вузлів при побудові маршруту |
| покриття | потужність передачі | - | - |
| стійкість | потужність передачі | Період зміни режимів | динамічна маршрутизація |

У табл.1.2 наведені пріоритетні показники якості обслуговування для виділених класів задач бездротових мереж по топології і за моделлю передачі даних:

Таблиця 1.2 – Пріоритетні показники якості обслуговування для різних класів задач бездротових сенсорних мереж

| | Мережі зі статичними вузлами |
|---|---|
| періодичний вимір показника | час життя |
| постійне вимір показника | затримка, пропускна здатність |
| детектування події | гарантія доставки (надійність) за передбачуваний період часу |
| вимірювання показника за запитом | втрати, затримка |

Оскільки в загальному випадку всі елементи БСМ є автономними, обов’язково настає момент, коли мережа більш не може вирішувати покладені на неї завдання. Час від початку роботи мережі до даного моменту називається часом життя або часом автономної роботи мережі (network lifetime). Проблема полягає в тому, що в кожному окремому випадку момент виходу мережі з ладу може визначатися по-різному, в залежності від вимог до якості обслуговування.

Важливо також відзначити дві ключові функції бездротових мереж моніторингу – самоорганізація і самовідновлення. Самоорганізація – це процес самостійного налаштування і підтримки роботи бездротової мережі з динамічним регулюванням параметрів і логіки її роботи в залежності від зовнішніх факторів [65]. Самовідновлення тісно пов’язане з самоорганізацією і передбачає, що при виході з ладу окремих вузлів мережі через певний інтервал часу мережа перебудовується і знову починає виконувати покладені на неї функції.

Функції самоорганізації і самовідновлення, як правило, описуються в стандартах мережевого рівня еталонної моделі OSI.

При вирішенні практичних завдань на базі автономних БСМ виникають дві основні задачі, пов’язані з показником часу життя:

1. Оцінка передбачуваного часу життя мережі при заданих характеристиках апаратних засобів і алгоритмах її роботи.

2. Збільшення часу життя за рахунок застосування ряду методів і алгоритмів.

Дослідження часу життя мережі і пов’язані з ним завдання, є одним з ключових питань цієї дисертаційної роботи.

Зокрема, слід згадати про зв’язок часу життя з енергоефективністю (energy efficiency) бездротової мережі [8, 73]. Енергоефективність часто вживається в якості характеристики стандартів, алгоритмів і протоколів, а її досягнення ставиться в якості однієї із завдань технічних проектів в самих різних областях, тобто вважається, що більший час автономної роботи БСМ за умови повної передачі реєстрованих даних забезпечує більшу

енергоефективність. Тому час життя мережі включає в себе вимоги щодо забезпечення якості обслуговування, яким мережа повинна задовольняти.

### 1.3. Методи збільшення часу життя бездротових сенсорних мереж

Для бездротових мереж моніторингу з автономним живленням актуально забезпечення гарантованого часу життя мережі протягом міжповірочного терміну експлуатації приладів обліку, що утворюють дану мережу. До найбільш простих з можливих методів збільшення часу автономної роботи БСМ відносяться зменшення енергоспоживання апаратних пристроїв, оптимізація топології мережі, збільшення ємності батарей.

Слід зазначити, що існують як фізичні (передача даних по радіоканалу вимагає певних енергетичних витрат) так і цінові обмеження (використання більш енергоефективних компонентів призводить до подорожчання систем). Крім того, використання великих по ємності батарей неминуче призводить до збільшення розміру пристроїв, в той час як сама концепція БСМ передбачає їх мініатюрність.

З точки зору програмних алгоритмів обробки даних на вузлах системи оптимізація енергоспоживання здійснюється шляхом стиснення даних і передачі даних великими блоками. Метод заснований на тому, що в сучасних бездротових стандартах будь-яка передача цифрового пакету пов’язана з додатковими накладними витратами. Тому вигідніше передавати дані великими блоками в одному пакеті. Останні дослідження в області мініатюрних перетворювачів альтернативної енергії (МЕН, Micro-Energy Harvesters) [65] відкрили ряд можливостей для створення повністю автономних вузлів. На сьогоднішній день жодне з рішень по збору і перетворенню альтернативної енергії ще не знайшло масового застосування в реальних мережах збору даних. Але в перспективі даний підхід може стати одним з провідних і, в кінцевому рахунку, вирішити проблему обмеженого часу життя БСМ.

### 1.3.1. Методи енергетичного балансування

Як було зазначено вище, бездротові мережі моніторингу головним чином призначені для збору даних. Це означає, що існує один виділений вузол, до якого надходить інформація з усієї мережі. Даний вузол, як правило, має постійне джерело живлення, інтерфейси сполучення з локальними та/або глобальними мережами.

Сучасні технологічні досягнення дозволили зробити мікропроцесор з дуже малою споживаною потужністю, здатний виконувати широкий спектр завдань. Для проведення натурного експерименту обрані модулі виробництва DIGI і REXENSE [57, 68]. Параметри їх енергоспоживання представлені в таблиці 1.3.

Таблиця 1.3 – Параметри енергоспоживання

| Специфікація | XBEE | XBEE S2C | REX3D |
|---|---|---|---|
| Робочий струм (передача) | 45 мА | 45 мА | 43 мА |
| Робочий струм (прийом) | 50 мА | 31 мА | 29 мА |
| Струм в режимі сну | 10 мкА | <1 мкА | 0.4 мкА |
| Потужність передачі | 1 мВт (0 дБм) | 6.3 мВт (+ 8дБм) | 4,5 мВт (+ 7дБм) |

З даних таблиці видно, що енергоспоживання модулів в режимі сну на два порядки нижче, ніж в активному режимі. Відправлення/прийом повідомлень збільшує енергоспоживання в порівнянні з базовим режимом. Але в будь-якому випадку очевидно те, що сплячий режим вимагає найменшої кількості енергії.

У бездротовій мережі є переважний напрямок рух корисного трафіку, що приводить до того, що через вузли маршрутизації, що знаходяться поруч з координатором, проходить на порядок більший обсяг трафіку. Чим більше даних проходить через вузол бездротової мережі, тим більше енергії їм споживається. Як наслідок, в мережі виникає проблема дисбалансу

енергоспоживання [70], що призводить до того, що автономні елементи, розташовані поруч з центральним вузлом збору даних (координатором), раніше інших виходять з ладу через розряд власних акумуляторів, і, як наслідок, зменшується час автономної роботи сенсорної мережі.

Для вирівнювання споживаної потужності всіх вузлів мережі використовують різні методи енергетичної балансування (energy balancing) [70]. Побудова гомогенної мережі передбачає використання ряду можливостей [63]:

1. Індивідуальний підбір ємності батарей в залежності від положення пристроїв в структурі мережі і виконуваних ними функцій [66]. В цьому випадку ключові ретранслюючі пристрої можуть забезпечуватися великими по ємності акумуляторами. Даний підхід є одним з найбільш простих, але водночас призводить до низької масштабованості мережі і її поганої адаптації до зміни умов функціонування.

2. Різна щільність розміщення вузлів мережі в залежності від передбачуваної інтенсивності трафіку в конкретній зоні [56]. Це рішення спрямоване на забезпечення надмірності в структурі мережі і дублювання функцій окремих вузлів. Так при виході з ладу чергового маршрутизатора його функції будуть перекладені на сусідній елемент.

Відомо, що в протоколах маршрутизації традиційних мереж використовуються метрики, спрямовані на збільшення пропускної здатності мережі або зменшення затримок переданих даних. У бездротових мережах часто застосовується метрика залишкової енергії вузлів на шляху до координатора.

### 1.3.2. Програмні методи енергетичного балансування

Для ZigBee БСМ механізм агрегатування є найбільш ефективним механізмом маршрутизації для мереж збору даних, в яких безліч віддалених вузлів пересилають повідомлення на один центральний вузол. Говорячи про маршрутизації маються на увазі тільки комірчасті мережі, оскільки в ZigBee-мережі з іншою топологією маршрути жорстко задані і зберігаються в пам’яті

координатора, і, отже, маршрутизація в таких мережах не потрібна. Стандартний алгоритм пошуку маршруту передбачає розсилку широкомовного повідомлення ініціалізації. Всі вузли, які чують це повідомлення, ретранслюють його, додаючи інформацію про те, з яким рівнем сигналу вони отримали повідомлення. Таким чином, вибирається оптимальний маршрут. При цьому мінімізується кількість ретрансляції і враховується якість сигналу при кожній пересилці. Кожен проміжний вузол при цьому зберігає в своїй таблиці маршрутизації відповідний запис. Зі сказаного, що процедура пошуку маршруту, що представляє собою трансляцію розсилки, сильно завантажує мережу. Для мереж збору даних, в яких безліч віддалених вузлів пересилають повідомлення на один центральний вузол-координатор, механізм агрегатування дозволяє замінити безліч широкомовних розсилок від віддалених вузлів, призначених для пошуку маршруту до центрального вузла, на всього одну трансляцію розсилку, ініційовану самим координатором.

Ще однією проблемою мереж збору даних є те, що вузли, близько розташовані до координатора і беруть участь у великій кількості маршрутів, витрачають багато пам’яті на зберігання записів в своїх таблицях маршрутизації. Механізм агрегатування дозволяє скоротити обсяг необхідної пам’яті за рахунок того, що зберігаються тільки записи для маршрутів в напрямку від віддаленого вузла до центрального. Передбачається, що в системах збору даних повідомлення від центрального вузла до віддалених здійснюються рідше і для них створюються тільки тимчасові (всього на одне повідомлення) маршрути в той момент, коли повідомлення від віддаленого вузла направляється до центрального вузла. Таким чином, центральний вузол для того, щоб послати своє повідомлення, повинен спочатку дочекатися повідомлення від віддаленого вузла, що приймає, центральний вузол отримує також тимчасовий маршрут для передачі одного свого повідомлення в зворотному напрямку. Центральний вузол може використовувати цей тимчасовий маршрут для того, щоб разом з підтвердженням послати якусь додаткову інформацію. З огляду на те, що широкомовлення не дозволяє ввести

обмеження на кількість адресатів, вона дуже сильно завантажує мережу. Для зниження цього ефекту транспортний рівень бере на себе турботу про відстеження відповідності між 64-бітними ідентифікаторами і 16-розрядними адресами в мережі. При пересиланні адресних повідомлень транспортний рівень надає дві можливості: пересилка одиночних пакетів з підтримкою підтвердження доставки повідомлення; і пересилання великої кількості пакетів. У тому випадку, коли потрібно послати велику кількість пакетів і важливо, щоб на приймальній стороні зберігся порядок надходження пакетів, до повідомлення додається номер пакета. Ця функція подібна обміну TCP в мережах Ethernet і вимагає попередньої установки з'єднання між двома адресатами і закриття з'єднання після того, як обмін буде завершено. Транспортний рівень надає можливість виконання широкомовних розсилок, тобто розсилку повідомлень групі вузлів без обмеження або з обмеженням на кількість ретрансляції відповідно [18].

Таким чином, програмне керування трафіком в системі бездротового моніторингу дозволяє ефективно управляти енергоспоживанням мережевих пристроїв. В цьому випадку з безлічі альтернативних маршрутів вибирається той, на якому вузли мають велику залишкову енергію.

### 1.3.3. Контроль доступу до середовища

Специфікація ZigBee передбачає передачу інформації з максимальною швидкістю 250 кБіт/с [74, 75]. За стандартом ZigBee закріплені 27 каналів в трьох частотних діапазонах – 2.4 ГГц, 915 МГц і 868 МГц. Максимальна швидкість передачі даних для цих ефірних діапазонів становить відповідно 250 кБіт с, 40 кбіт/с і 20 кБіт/с. По суті, ZigBee – це не один протокол: специфікація ZigBee [74, 75] регламентує стек протоколів, в якому протоколи верхніх рівнів використовують сервіси, що надаються протоколами нижчих рівнів. В якості двох нижніх рівнів (фізичного рівня PHY і рівня доступу до середовища MAC) використовується стандарт IEEE 802.15.4 [16, 30]. MAC-рівень в мережі ZigBee реалізує механізм CSMA-CA (прослуховування несучої і усунення колізій),

мережевий рівень (NWK) відповідальний за маршрутизацію повідомлень, а рівень APS (підтримки додатків) забезпечує інтерфейс з рівнем додатки. З точки зору енергоефективності розглянутих мереж інтерес представляють канальний рівень (MAC) і мережевий рівень (NWK) [45].

**Протокол канального рівня**

Специфікація IEEE 802.15.4 описує два режими роботи мережі: маячковий і без маяків. У режимі без маяків маршрутизатори постійно прослуховують ефір, тому не можна побудувати мережу з наднизьким енергоспоживанням.

У маячковому режимі всі пристрої з певним періодом посилають в ефір спеціальні кадри, звані маяками. Інтервал між маяками (BI) включає в себе активний період, званий суперфреймом, і неактивний період. Протягом суперфрейма можлива передача кадрів даних. Під час неактивного періоду вузли засипають. Протягом періоду конкурентного доступу (CAP) вузли змагаються за отримання доступу до фізичного середовища, використовуючи механізм слотного CSMA-CA (Slotted Carrier Sense Multiple Access with Collision Avoidance) доступу [45]. У протоколі IEEE 802.15.4 також передбачений період неконкурентного доступу до середовища (CFP), про який буде сказано нижче.

**Протокол мережевого рівня**

Специфікація ZigBee пропонує використання одного з двох протоколів мережевого рівня. Перший підхід – реактивний протокол динамічної маршрутизації AODV (Ad hoc On-Demand Distance Vector) [11, 53]. Другий – протокол HERA (HiErarchical Routing Algorithm), який використовує дерево асоціації вузлів, яке будується і підтримується на канальному рівні [13]. На відміну від AODV, вирішуються зв'язки тільки одного виду «координатор-вузол». Протокол HERA є проактивним, тому не потрібно ніяких додаткових службових повідомлень для побудови маршрутів. У мережах енергомоніторингу мають пористу структуру інформація передається з нерухомих джерел на нерухомий приймач. При цьому кожен вузол є маршрутизатором, що

встановлює зв'язок з найближчими сусідами. Тому в даних мережах традиційно застосовується протокол AODV [11, 53].

### 1.3.4. Енергоефективна передача даних в БСМ

Через все зростаючу популярність бездротового доступу до локальних мереж зросла актуальність технологій бездротових комірчастих (mesh)-мереж і мереж типу «зірка», що застосовуються в сучасних рішеннях. Mesh-мережі дозволяють збільшувати область бездротового покриття за рахунок залучення самих вузлів, що передають дані, в процес маршрутизації. Це дозволяє скоротити кількість необхідних точок доступу і збільшити територію бездротового доступу. Модель пересилання даних містить в собі три види транзакцій. Перший вид – передача даних координатору, другий – передача від координатора, третій вид – передача між рівними пристроями. У топології типу «зірка» застосовується тільки перші два види транзакцій, оскільки дані йдуть між координатором і пристроєм. У топології «рівноправних вузлів» можливі всі три види транзакцій.

Механізм кожного типу транзакцій (обмінів) залежить від того, чи підтримує мережа передачу маяків. Мережі PAN з підтримкою маяків використовуються в мережах, які або вимагають синхронізації, або підтримують мережеві пристрої, що вимагають малої затримки відгуку. Якщо мережа не потребує синхронізації або малих затримок, вона може не використовувати кадри-маяки для стандартних обмінів. Однак маяки в будь-якому випадку потрібні для відновлення мережі.

**Механізм CSMA-CA**

IEEE 802.15.4 [30] використовує два типи механізмів доступу до каналу, в залежності від конфігурації мережі. Мережі PAN (Personal Area Network) без маяків використовують бездоменний механізм доступу до каналу CSMA-CA. У бездротовій мережі комунікації встановлюються між окремими пристроями і центральним контролером, званим координатор PAN. Мережевий пристрій зазвичай асоціюється з одним з додатків і в процесі комунікацій є або

відправником, або одержувачем даних. Мережі PAN с маяками (beacon) використовують доменний механізм доступу до каналу CSMA-CA. Успішний прийом і верифікація кадрів даних або MAC-команд може бути підтверджений відправкою пакетів підтвердження. Якщо приймаючий пристрій з якоїсь причини не може обробити вхідний кадр, отримання повідомлення не підтверджується.

**Передача даних координатору**

Коли мережевий пристрій хоче передати дані координатору в мережі PAN з підтримкою кадрів-маяків, він спочатку намагається детектувати кадр-маяк (beacon). Коли маяк виявлений, пристрій синхронізуються зі структурою суперкадра. У відповідний момент часу пристрій передає свій інформаційний кадр, використовуючи доменний алгоритм CSMA-CA, координатору. Дана послідовність дій відображена на рис. 1.3.


Рисунок 1.3 – Передача даних координатору в PAN з використанням маяків

Коли мережевий пристрій хоче передати дані в мережі PAN без підтримки маяків, він просто посилає інформаційний кадр координатору, використовуючи схему CSMA-CA. Координатор підтверджує успішну доставку даних посилкою кадру підтвердження. Дана послідовність операцій відображена на рис. 1.4.

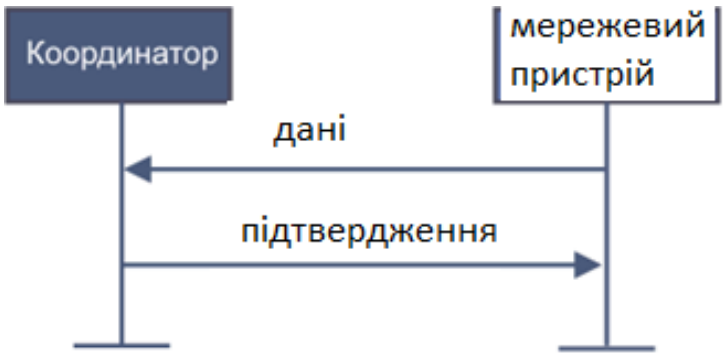



Рисунок 1.4 – Комунікації з координатором в PAN без міток

**Передача даних з координатора**

Коли координатор хоче передати дані мережевого пристрою в мережі PAN з підтримкою маяків, він визначає з мережевого маяка, які дані очікують відправки. Пристрій періодично прослуховує мережеві маяки (beacon), і якщо є очікувані відправки повідомлення, передається MAC-команда запиту даних з використанням доменного механізму CSMA-CA. Координатор підтверджує отримання запиту даних за допомогою відповідного кадру (ACK). Пристрій може підтвердити успішне отримання даних шляхом відправки кадру підтвердження. На цьому транзакція завершується. Послідовність описаних дій представлена на рис. 1.5.

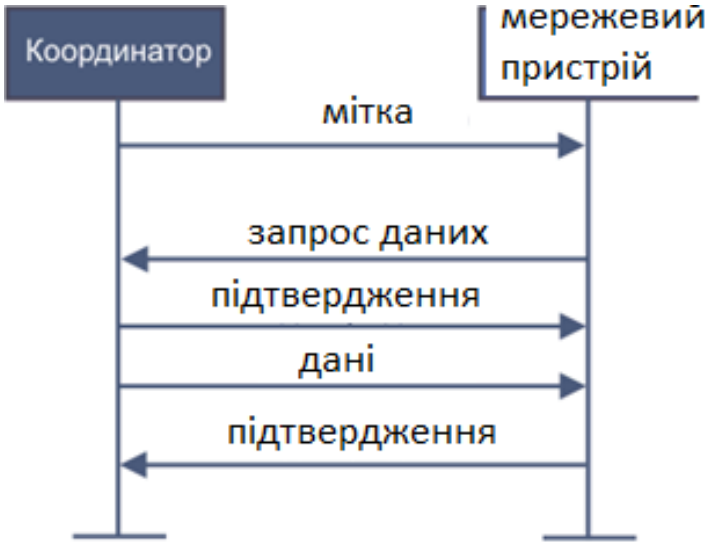



Рисунок 1.5 – Передача даних з комунікатора мережі PAN, що використовує маяки

Мережевий пристрій може встановити контакт з координатором шляхом відправки MAC-команди запиту даних, використовуючи механізм бездоменного CSMA-CA, зі швидкістю обміну, заданої додатком. Координатор підтверджує успішне отримання інформаційного запиту за допомогою кадру підтвердження. Якщо інформаційний кадр чекає відправки, координатор посилає пристрою кадр даних, використовуючи механізм CSMA-CA. Якщо кадру даних, що чекає відправки, немає, координатор фіксує цей факт або в пакеті підтвердження, наступного за запитом даних, або в інформаційному кадрі з нульовою довжиною поля даних. Якщо потрібно, пристрій підтверджує успішне отримання кадру даних. Послідовність дій для даної схеми відображена на рис. 1.6.

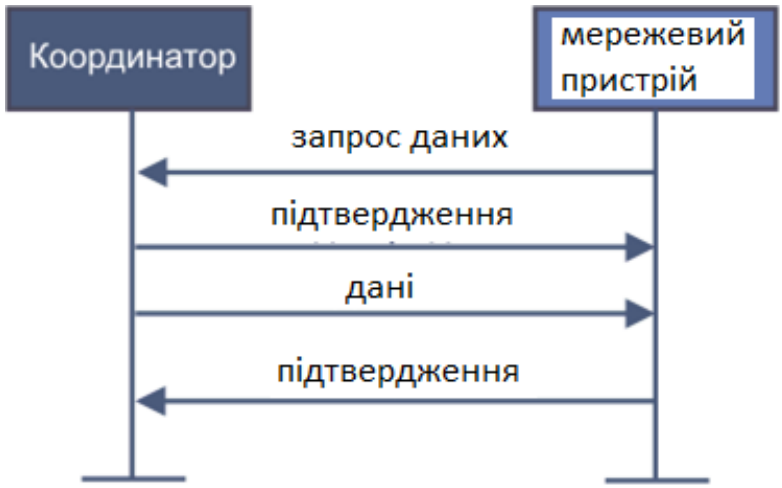



Рисунок 1.6 – Телекомунікації з координатора в мережу PAN без маяків

**Передача даних в режимі P2P**

У P2P PAN, кожен пристрій може обмінюватися даними з будь-яким іншим пристроєм в межах радіодоступності. З огляду на сильну обмеженість в ресурсах сенсорних вузлів і невелику пропускну здатність каналу зв’язку, що виключають можливість регулярного обміну службовою інформацією, використовується спеціальний протокол маршрутизації AODV [11, 14]. AODV

(Ad Hoc On-Demand Distance Vector) – це протокол динамічної маршрутизації, заснований на побудові таблиць маршрутизації на кожному вузлі мережі для мінімізації часу передачі інформації між вузлами. У таблиці міститься довжина найкоротшого шляху до кожного вузла в мережі через кожен сусідній вузол. Після обчислення маршруту починається передача даних по найкоротшому знайденому шляху. Невикористані записи в таблицях маршрутизації стираються. Перевага AODV полягає в тому, що він не створює додаткового трафіку при передачі даних за встановленим маршрутом. Маршрутизація AODV дозволяє будь-якого пристрою спілкуватися з будь-яким іншим пристроєм в мережі, що самовідновлюється мережу без єдиної точки відмови.

**Маршрутизація в комірчастій мережі**

З практичної точки зору в розподілених мережах енергообліку широкого поширення набули сіткові (mesh) структури, в яких маршрутизація підтримується координатором і роутерами. Алгоритм сіткової маршрутизації дозволяє створити односпрямований шлях, виконати групову маршрутизацію або прокласти маршрут типу «багато до одного». Це дозволяє мінімізувати ризик можливої нестабільності великих мереж. Комірчаста мережа – проста і гнучка технологія. Маршрут складається від одного вузла до іншого і в передачі задіються тільки вузли, що входять в маршрут, що значно знижує навантаження мережі і прискорює передачу. Також вузол-відправник точно знає, чи було доставлено повідомлення.

Алгоритм маршрутизації заснований на публічно доступному алгоритмі динамічної маршрутизації AODV. В алгоритмі AODV інформація про маршрут розподілена – кожен вузол мережі містить таблицю маршрутизації. Спочатку комірчаста мережа не містить ніякої інформації про маршрути. Маршрути зазвичай односпрямовані і існують, поки можуть використовуватися. В даному алгоритмі мережа являє собою зважений граф. Визначення маршруту починається з широкомовного повідомлення від вузла-відправника. Наприклад, координатор (вузол 0) відправляє запит вузлу 10 (рис.1.7). Вузол 10 не є сусідом вузла 0, і маршрут до нього невідомий, тому починається визначення

маршруту. Повідомлення ретранслюється в усіх напрямках і на кожному вузлі в тіло пакету додається вага пройденого ребра графа. Відповідно до специфікації, довгий маршрут з більш якісним зв’язком краще, так як на повторну передачу зниклого пакету піде більше часу, ніж на проходження зайвого вузла в маршруті [70].

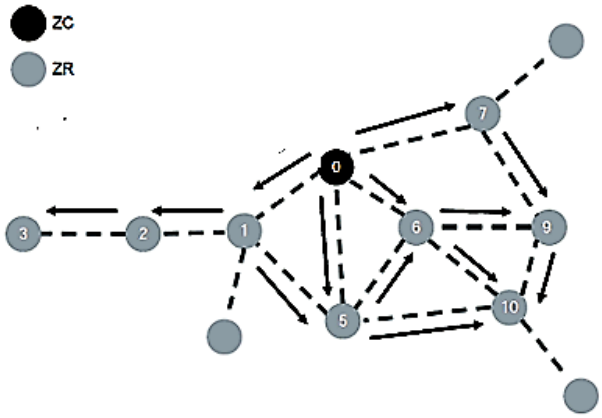



Рисунок 1.7 – Прокладка маршруту в mesh-мережі

Порівняльний аналіз бездротових сенсорних мереж показує, що цілісність і гарантована якість обслуговування вузлів мережі потенційно досяжні тільки у двох топологій – зірка і комірчаста архітектура. При цьому топологія зірка дозволяє отримати гарантований час опитування вузлів мережі, а комірчаста архітектура – високу живучість бездротової мережі [10, 22, 25, 44, 54]. За результатами аналізу топологій бездротових мереж можна зробити висновок про те, що єдиною топологією мережі, яка має в повній мірі властивість самоорганізації, є комірчаста архітектура [10, 27]. Тільки така топологія мережі дозволяє забезпечити відмовостійкість. З практичної точки зору для задач моніторингу енергоспоживання в житлово-комунальному господарстві найбільш придатними є пористі структури мереж для випадку щільної міської багатоповерхової забудови і топологія зірки для малоповерхової забудови, властивою околиць міст і сільських населених пунктів. У зв'язку з цим сформульовані вимоги до основних завдань досліджень цієї роботи – забезпечення максимальної тривалості життя бездротової мережі моніторингу з автономними джерелами живлення.

### 1.4. Апаратні методи оптимізації енергоспоживання БСМ

Методики і моделі енергоефективних мереж стандарту 802.15.4 / ZigBee досить широко представлені в роботах [20, 23-28, 80]. Автори [23] пропонують метод для налаштування конкурентного доступу до каналу CSMA/CA з метою максимізації енергозбереження та пропускної здатності. Однак пропонована модель не враховує споживання енергії в неактивному режимі. У дослідженні [80] пропонується використовувати заряд батареї в вузлах 802.15.4 / ZigBee як метрику для алгоритму маршрутизації AODV. У статті [27] досліджується вплив використання криптографічного механізму на енергоспоживання мереж з підтримкою маяка, а в [24] моделюються потужності, споживані пристроями, що використовують фізичний рівень 802.15.4 і стеки. З огляду на те, що розмір суперфрейма, переданого в бездротовій мережі, також впливає на енергоспоживання пристроїв, цей ефект вимагає додаткового вивчення. Зі структури пакетів стека ZigBee випливає, що кожен рівень стека додає до даних свій заголовок зі службовою інформацією. В сумі додаткова службова інформація всього стека в пакеті при передачі даних становить 33 байта. При цьому для даних рівня додатки в пакеті залишається 100 байт. Тому розмір переданих пакетів даних (наприклад, добовий графік навантаження/витрати) і їх частота в значній мірі визначають час життя системи. Це необхідно враховувати при розробці моделі, яка б дозволяла прогнозувати час життя батареї в бездротовій сенсорній мережі. Щоб передбачити тривалість роботи батареї в практичній реалізації мережі 802.15.4/ZigBee, ми повинні охарактеризувати цикли активності при передачі даних, а також струм, який генерується з батареї під час різних операцій, виконуваних в динаміці, особливо тих, які мають на увазі активацію приймача (основного джерела споживання енергії в пристроях).

Технологія ZigBee/802.15.4 була розроблена для мінімізації енергоспоживання пристроїв, що підтримують цей стандарт. Для цієї мети активність пристроїв повинна бути зменшена до мінімуму, щоб вони могли

залишатися якомога довше в стані малої потужності (сну). Таким чином, пристрій просто має «прокидатися» (бути активним), щоб передавати (або отримувати) дані за невеликий проміжок часу. Основна мета досліджень дисертаційної роботи – максимізувати термін служби батареї в польових пристроях бездротової системи енергомоніторингу і, отже, оптимізувати час життя самої бездротової мережі.

### 1.5. Аналіз моделей і постановка задачі

Продовження терміну служби мережі є спільною метою досліджень бездротових мереж, оскільки вузол мережі зазвичай обмежений ємністю джерела живлення, яка визначає час його життя. Автори [8, 9, 11] проаналізували час життя бездротових сенсорних мереж. У роботах [8, 11] було введено поняття енергетичної цінності вузла, яка визначається як відношення повної споживаної енергії до вихідної початкової енергії батареї. Цінність вузла тим вище, чим менше відношення енергії, що витрачається вузлом при роботі в мережі, до його початкової енергії. Відповідно до цієї моделі загальна енергія споживання включає в себе енергію, яка витрачається на передачу і прийом пакетів, режим сну і зондування. Однак, автори не врахували додаткові джерела енергетичних витрат, таких як управління пакетами в режимі GTS і повторними передачами, викликаними перешкодами в мережі. Останнє є визначальним, оскільки при інтенсивному трафіку повторна передача «невдалих» пакетів веде до суттєвих додаткових витрат енергії, що призводить до скорочення часу життя мережі. Модель, запропонована в [73], усуває цей недолік, але не пропонує аналітичного методу обчислення ймовірності невдалої передачі. В роботі [72] аналізується режим доступу до середовища CSMA/CA і визначається затримка передачі відповідно до довжини кадру, а автори [49] запропонували модель прогнозування затримок зв’язку в режимі GTS.

З огляду на безліч моделей [31, 50, 51], що описують залежність енергоспоживання від режимів роботи пристроїв стандарту 802.15.4/ZigBee на MAC і NWK рівнях специфікації певний практичний інтерес представляє

розробка реалістичної аналітичної моделі для прогнозування часу життя і затримки зв'язку в мережах IEEE 802.15.4 з урахуванням можливого зовнішнього впливу на мережу.

### 1.6. Висновки до першого розділу

1. Проведений аналіз відкритих джерел показав, що бездротові мережі моніторингу є перспективною технологією в області створення побутових і промислових систем збору даних і управління. Ключовим показником БСМ, визначальним їх застосовність на практиці, є час їхнього життя. Завдання його збільшення є актуальною.
2. У літературі описаний ряд моделей, що описують вплив режимів роботи канального і мережевого рівня на енергоефективність бездротових мереж, однак всі вони розглядають окремі випадки. Необхідна більш загальна модель, яка дозволяла б оцінювати час життя мережі і вирішувати завдання максимізації даного часу шляхом зміни різних параметрів роботи мережі. Також необхідно провести більш детальний аналіз можливих підходів до оптимізації структури мережі за часом життя як комплексної системи.
3. Маршрутизатори бездротової мережі є найбільш залежними від енергоспоживання пристроями, які критично визначають час життя мережі. Тому завдання збільшення часу їх життя розглядається в якості основної при побудові автономних бездротових мереж моніторингу. У даній роботі розглядається концепція моделі «роутерів, що прокидаються» в комірчастій мережі меш-топології. Використання керованих «роутерів, що прокидаються» як польових пристроїв бездротової мережі моніторингу є одним з найбільш перспективних методів збільшення часу життя комірчастої мережі.

Результати даного розділу опубліковано в роботах автора [92, 96, 97, 99, 100, 103].

# РОЗДІЛ 2. МОДЕЛЮВАННЯ БЕЗДРОТОВОЇ ПЕРЕДАЧІ В МЕРЕЖАХ ЕНЕРГОМОНІТОРИНГУ

Розділ присвячений моделюванню роботи бездротової сенсорної мережі з оцінюванням часу її життя за енергетичними параметрами. Наведено методику розрахунку ключових параметрів моделі. Сформульовано задачу дослідження, яка полягає в оптимізації енергоспоживання польових пристроїв бездротової мережі з автономним живленням на рівні користувальницького додатка. Для організації систем обліку обрано технологію ZigBee стандарту IEEE 802.15.4, який описує фізичний і канальний рівні еталонної моделі OSI.

## 2.1. Математична модель

В роботі запропоновано енергетичну модель відповідно до основних завдань, які вузли виконують в мережі. Ця модель враховує всі компоненти енергії, які впливають на загальне енергоспоживання в активному режимі. Перш за все, у початковий момент вузол готовий до включення. Потім потрібен час перемикання для зміни статусу перед відправкою пакету у середовище. Тут вузол спочатку запускає відповідний алгоритм (наприклад CSMA), а потім передає інформаційний пакет, збільшуючи час передачі. Тепер вузлу потрібен час перемикання для зміни дій, він залишається неактивним і знову змінює задачу. Крім того, потрібен час перемикання, щоб почати прийом інформації та повідомити час прийому. Вузол виконує послідовність дій потрібну кількість разів, скільки відправляє і отримує інформацію (повідомлення) протягом періоду вибірки. Нарешті, вузол вимикається, «витрачаючи» час вимикання. Все це поки мікроконтролер залишається в активному режимі. В ході цього процесу вимірюється енергія, необхідна для роботи кожного основного вузла в мережі. Залежно від завдання і часу, який потрібен вузлу для її виконання, це відповідає заданим напрузі і току, тому загальна енергія, яка використовується

кожним вузлом, може бути отримана підсумовуванням енергій для кожної з дій.

Основними джерелами енергоспоживання для вузла бездротової мережі є [81]:

• Передача та прийом пакетів.

• Технологічні втрати енергії, обумовлені процедурами управління: оскільки пакети управління не містять даних, вони розглядаються як додаткове джерело технологічних витрат.

• Зіткнення: якщо відбувається зіткнення, вузли повинні повторно передавати одні й ті ж дані, при цьому різко зростає споживання енергії.

• Прослуховування: коли вузол збирає пакети, призначені для інших вузлів, він споживає більше енергії.

• Безперервне прослуховування: прослуховування прийому трафіку веде до збільшення споживання енергії.

Ці параметри є визначальними для оцінки затримок передачі даних і розрахунку енергоємності мережі.

Фактично, час життя мережі залежить від програми і режиму роботи мережі. Це означає, що час життя мережі повинен розглядатися з точки зору її функціональних станів:

• Час до вичерпання енергії будь-якого одного вузла мережі.

• Час до вичерпання енергії в декількох вузлах, що викликає втрату зв'язку на одному або більше ділянках мережі.

• Час, протягом якого до 50% вузлів вийде з ладу.

У всіх цих випадках час життя сильно залежить від залишкової енергії. Відповідно, фокусування уваги на споживанні енергії вузлами для оцінки тривалості їх життя і, отже, тривалості життя мережі є визначальним при розробці математичної моделі.

В роботі розглядаються наступні початкові умови:

1) Енергоємність $C_i(t)$ вузла $N_i$ в момент часу $t$, визначається як відношення повної енергії $E$, що споживається вузлом в момент часу $t$, до початкової енергії автономного джерела живлення $E_{\text{поч } i}$:

$$C_i(t) = \frac{E_i\,(t)}{E_{\text{поч } i}}. \tag{2.1}$$

2) Рівні енергії спочатку задані з різними значеннями, тому розрахунок енергоємності проводиться в інтервалі [0, 1]:

• $\mathrm{C}_i(t) = 0$, тобто батарея вузла $N_i$ в момент часу $t$ повністю заряджена.

• $\mathrm{C}_i(t) = 1$, тобто батарея вузла $N_i$ в момент часу $t$ розряджена.

Якщо в момент часу $t$ батарея найбільш енергоємного вузла вичерпана, то це визначає час життя усієї мережі.

В моделі прогнозування тривалості життя мережі враховується енергоспоживання польових пристроїв з урахуванням стартових екранів, прослуховування, управління пакетами в режимі GTS і повторними передачами, викликаними перешкодами в мережі.

Загальна енергія E, споживана в одиницю часу вузлом БСМ, включає в себе енергію, яка витрачається на передачу $E_{\text{пер}}$ і прийом $E_{\text{пр}}$ пакетів даних, при передачі і прийомі керуючих пакетів $E_{\text{кер}}$, при прослуховуванні каналу $E_{\text{прос}}$ і при прийомі пакетів сусідів $E_{\text{сусід}}$:

$$\mathrm{E} = E_{\text{пер}} + E_{\text{пр}} + E_{\text{кер}} + E_{\text{прос}} + E_{\text{сусід}}\,. \tag{2.2}$$

Оскільки передача пакетів може завершитися невдачею, то в роботі використовується поняття середнього значення невдалих передач пакета перед успішної передачею $N_{\text{сер}}$.

Енергія, що витрачається вузлом $N_i$ при передачі пакетів в часовому інтервалі [0, $t$], може бути обчислена як сума кількості енергії, споживаної при пересиланні повідомлень в мережі і при відправці підтверджень:

$$E_{\text{пер } i}(t) = t \cdot P_{\text{пер}}\left(1 + N_{\text{сер}}N_i\right)\left(v_i \cdot T_{\text{підтв}} + T_{\text{пер}}(v_i + w_i)\right), \tag{2.3}$$

де $P_{\text{пер}}$ – споживана потужність при передачі одного пакета,

$T_{\text{пер}}$ – час передачі пакета даних,

$T_{\text{підтв}}$ – час передачі підтвердження,

$w_i$ – швидкість генерації пакета для вузла $N_i$,

$v_i$ – швидкість пересилання пакетів вузлом $N_i$.

Аналогічно енергія, що витрачається вузлом $N_i$ при прийомі пакетів в інтервалі часу [0, $t$], може бути визначена:

$$E_{\text{пр}\,i}(t) = t \cdot P_{\text{пр}}(1 + N_c N_i)\left(v_i \cdot T_{\text{пер}} + T_{\text{підтв}}(v_i + w_i)\right), \quad (2.4)$$

де $P_{\text{пр}}$ – споживана потужність при отриманні одного пакета.

На додаток до енергії, що витрачається на передачу і прийом пакетів даних, вузол датчика споживає енергію, надсилаючи та приймаючи керуючі пакети, такі як маяки і командні кадри:

$$E_{\text{кер}\,i}(t) = t\left(W \cdot T_{\text{кер}} \cdot \left(P_{\text{пер}} + P_{\text{пр}}\right)\right), \quad (2.5)$$

де $W$ – середня швидкість генерації керуючих пакетів,

$T_{\text{кер}}$ – час передачі керуючого пакета.

Енергія, що витрачається на прослуховування каналу, пов'язана з періодами часу очікування доступу. За аналогією з IEEE 802.11 стосовно стандарту IEEE 802.15.4 енергія, що витрачається на прослуховування каналу в часовому інтервалі [0, t], визначається як:

$$E_{\text{прос}\,i}(t) = t_{\text{слот}} \cdot P_{\text{прос}} \cdot R \cdot K(t), \quad (2.6)$$

де $P_{\text{прос}}$ – споживання енергії в режимі очікування,

$t_{\text{слот}}$ – час слота,

$K(t)$ – це кількість пакетів, отриманих за час t,

$R$ – оцінка каналу, яка використовується вузлом для перевірки, чи вільний канал або зайнятий.

Енергія, що витрачається на прослуховування, залежить від швидкості генерації трафіку $w_l$ і швидкості пересилання $v_l$ сусідів $Z(N_i)$ та визначається наступним співвідношенням:

$$E_{\text{сусід}}(t) = t \cdot P_{\text{пр}} \sum_{k \in Z(N_i)} \left[ \left( N_{\text{сер}} N_l + 1 \right) \left( v_l \cdot T_{\text{підтв}} + T_{\text{пер}}(v_l + w_l) \right) \right], \quad (2.7)$$

де $Z(N_l)$ – множина вузлів, розташованих в околиці вузла $N_l$ і передаючих трафік, призначений для інших вузлів,

$w_l$ – швидкість генерації пакета для вузла $N_l$,

$v_l$ – швидкість пересилання пакетів вузлом $N_l$.

Моделювання можна спростити згідно припущення, що всі повідомлення мають однаковий розмір і, отже, один і той самий час прийому-передачі. Відповідно до стандарту IEEE 802.15.4, підрівень MAC вимагає часу для обробки даних, отриманих на фізичному рівні [16]. Відповідно, два послідовних кадри, що передаються з вузла, повинні бути розділені, щонайменше, одним періодом IFS. Довжина періоду IFS залежить від розміру переданого кадру.

Час обслуговування – це сума часу затримки, оцінки каналу $R$, передачі кадру і прийому підтвердження після міжфазного інтервалу IFS.

При зовнішніх впливах в мережах можуть статися помилки передачі. Аналіз ґрунтується на $N_{\text{сер}}$, який є середнім числом невдалих передач пакета перед успішної передачею. Згаданий вище механізм CSMA/CA працює за принципом прослуховування частот протягом певного часу і виявлення вільної частоти для передачі даних. Якщо канал зайнятий, то вузол «відсторонюється» і чекає певну кількість часу, перш ніж знову почати спробу відправки пакета. Уникнення колізій використовується для того, щоб поліпшити продуктивність CSMA. Поліпшення продуктивності досягається за рахунок зниження ймовірності колізій і повторних спроб передачі.

Для обчислення середньої потужності вузла, необхідно визначити, скільки часу вузол займає кожний стан. На додаток до середнього споживання

енергії можна обчислити загальну ймовірність відмови передачі. Помилка передачі може бути пов'язана з відмовою доступу до каналу. Стандартом IEEE 802.15.4 [30] визначається чотири типи пакетів:

- сигнальний пакет (beacon frame);
- пакет даних (data frame);
- пакет підтвердження (acknowledgment frame);
- командний пакет.

На додаток до даних корисного навантаження передається пакет, що складається з послідовності: преамбули (4 байта даних), роздільник кадру (1 байт) і 1 і 8 байтів даних служби PHY і MAC, відповідно. Оскільки різні вузли відчувають різні втрати, для досягнення максимальної енергоефективності їм доводиться адаптувати свою потужність передачі. Щоб визначити оптимальні за енергією порогові значення для перемикання між рівнями потужності передачі, загальна енергія кожного переданого біта обчислюється для повного діапазону втрат в тракті. У відповідність стандарту, якщо стався збій передачі в даному суперфреймі, додаток буде повторювати передачу в наступному суперфреймі.

У стандарті 802.15.4 для частот в діапазоні 2,4 ГГц визначена максимальна швидкість передачі 250 Кбіт/с. У стандарті визначено алгоритм доступу до середовища передачі даних CSMA/CA. При передачі даних пристрій чекає випадковий проміжок часу з визначеного діапазону, після чого визначає зайнятість каналу. Якщо канал вільний, пристрій передає дані, якщо канал зайнятий, то він чекає випадковий проміжок часу.

Розмір корисного навантаження залежить від довжини службових полів. У разі використання короткої 16 бітної адреси, що використовується в розробленій в роботі системі, максимальний обсяг пакета даних буде дорівнює 114 байтам. Якщо прийняти швидкість на вході 250 Кбіт/с, то час передачі пакета даних складе 4,1 мс. Кадр підтвердження прийому даних складається з 11 байт, а час його передачі складе 350 мкс.

Перед відправкою підтвердження стандартом визначена затримка в 192 мкс, що пов'язано з тим, що пристрій має перейти з режиму прийому в режим передачі. Крім того, в стандарті визначені мінімальні затримки, які слідують після кадру підтвердження:

- для кадрів довжиною до 18 байт – 18 символьних періодів.
- для кадрів довжиною понад 18 байт – 40 символьних періодів.

При передачі даних між рівноправними пристроями дані передаються після синхронізації.

### 2.2. Метод вимірювання середніх значень енергоспоживання

Основні причини енергетичних втрат в БСМ були описані І. Демірколом і ін. [16]. З огляду на характеристики радіозв’язку, найбільш значущими є втрати енергії на прослуховування і повторні передачі. Прослуховування в режимі очікування полягає в тому, що приймач активний, коли не приймаються вхідні пакети, і існує необхідність повторної передачі пакета, адресованої конкретному вузлу. Активний приймач споживає кількість енергії незалежно від того, відбувається передача чи ні. Якщо одночасно передається велика кількість кадрів, відбуваються зіткнення. Загалом, все конфліктуючі пакети повинні бути повторно передані. Це веде до збільшення потужності споживання і завантаження мережі. У випадках з великим трафіком і поганим механізмом планування, це може стати серйозною проблемою, що ускладнює характеристики всієї системи.

Інша причина енергетичних втрат – підслуховування, тобто прийом пакетів, які призначені для інших вузлів. Для уникнення переповнення вхідних пакетів необхідно ввести механізм адресації, який вказує всі вузли призначення наступної передачі.

Це досягається шляхом передачі пакетів управління, але вони призводять до додаткових енергетичних втрат через витрати на керуючі пакети. Очевидно,

що з метою енергозбереження, протокол MAC повинен використовувати мінімальну кількість пакетів управління.

Для режиму «прокидаються роутерів», використовуваного в розробленій системі енергомоніторингу, робота мережі складається з етапів:

- прокидання і виходу в мережу (sleep up & start up);
- побудови мережі;
- передачі даних.

Для випадку стаціонарної мережі з усталеною «комірчастою» конфігурацією основні витрати енергії обумовлюються режимом передачі даних. У той же час енергетичні витрати на перші два механізми є постійними фіксованими величинами, що мають другорядне значення з точки зору часу життя мережі.

Загальна ідея полягає в тому, щоб контролювати потужність, необхідну польовому пристрою, що діє в якості дочірнього вузла 802.15.4, при спілкуванні з пристроєм FFD (координатором мережі). Для оцінки струму, споживаного ПЗПД, запропонований стенд, в якому резистор з відомим значенням розміщений між джерелом опорного напруги і відповідним контактом модуля. Тим самим визначається струм споживання пристроїв протягом робочого циклу. Модернізована методика визначення енергетичних параметрів застосована для вивчення енергоспоживання ПЗПД, побудованих на модулях DIGI XBEE S2 і REX3. Детально опис експериментальної частини представлено в наступному розділі.

### 2.3. Розрахунок споживаної потужності і часу життя БСМ

Метод енергетичної балансування цікавий з практичного боку, оскільки являє випадок передачі тривожних повідомлень в комірчастій мережі. У цьому випадку кожен вузол може працювати в двох режимах передачі – ближньому і далекому. У ближньому режимі он передає інформацію своєму найближчому

сусіду, в далекому – координатору мережі без ретрансляції. Вважається, що кожен вузол вибирає свій режим незалежно від інших.

Координатор мережі, що має постійне зовнішнє живлення, представляє собою спеціальний тип ідеального вузла, для якого початкова енергія необмежена, а характеристики споживаної потужності не є важливими. Останнім важливим елементом моделі є зміна конфігурацій, обумовлених виходом з ладу окремих вузлів, що призводить до зміни маршруту доставки повідомлень в мережі.

Дана модель може бути застосована для мереж зі стійким характером функціонування вузлів, вираженим в незмінною споживаної потужності в кожній з можливих конфігурацій. Споживана потужність безпосередньо залежить від трафіку, що генерується і ретранслюється вузлом. В цілому зрозуміло, що вузол бездротової мережі збору даних можна вважаються найманими працівниками, поки він може безпомилково зчитувати показання з датчиків і передавати дані в мережу. При розробці та встановлення мережі важливо заздалегідь оцінити приблизний час роботи кожного вузла до моменту, коли буде необхідна заміна його батарей. Для цього важливо розуміти, які фактори впливають на тривалість часу його автономної роботи.

Відомо, що енергоспоживання окремих елементів мережі залежить від наступних факторів, які необхідно брати до уваги при моделюванні БСМ:

· Характеристики апаратних засобів (ємність батарей, споживана потужність мікроконтролера і приймача).

· Частота збору і передачі даних.

· Протоколи фізичного і канального рівнів, що визначають, перш за все, механізми контролю доступу до середовища [61].

· Топологія мережі, яка визначає обсяг інформації, що проходить через кожен елемент (з урахуванням ретрансляції повідомлень) [80, 89].

· Використовуваний протокол маршрутизації, який додає в мережу додатковий службовий трафік [6, 15].

Формалізуємо наведені вище твердження у вигляді методики розрахунку часу життя. У розробленій бездротової мережі моніторингу застосовуються два типи вузлів – маршрутизатори (ретранслятори) і координатор. Координатори не уявляють інтерес з точки зору часу автономної роботи, так як вони підключені до джерел живлення, які мають на порядок більшу ємність.

Розрахунок часу життя кінцевих пристроїв і ретрансляторів ґрунтується на наступних припущеннях:

· Алгоритм роботи пристрою є строго детермінованим, для зовнішніх чинників, які є випадковими величинами, відомо математичне очікування.

· Відсутній ефект відновлення батареї.

Формула потужності споживання пристрою має вигляд:

$$P = \frac{P_{\text{сну}}(t_{\text{цикл}} - t_1 - t_2) + P_1 t_1 + P_2 t_2}{t_{\text{цикл}}}, \quad (2.8)$$

де $P_1$ – середня потужність в процесі передачі даних і подальшого прийому підтвердження [Вт];

$P_2$ – потужність споживання в режимі обробки даних (зчитування показників) [Вт];

$P_{\text{сну}}$ – споживана потужність в режимі сну [Вт];

$t_{\text{цикл}}$ – тривалість одного циклу роботи пристрою [с];

$t_1$ – час, що витрачається на передачу даних та прийом підтвердження [с];

$t_2$ – сумарний час, що витрачається на зчитування показань з датчиків, їх обробку і підготовку до передачі [с];

Тоді знаючи початкову енергію батареї $E_0$ і потужність $P$, споживану пристроєм, можна приблизно оцінити час його життя по формулі [81]:

$$T = \frac{E_0}{P}. \quad (2.9)$$

Слід зазначити, що енергія, яка використовується мікроконтролером, залежить від режиму роботи вузла. Наприклад, методи відключення вузлів знижують споживання енергії за рахунок установки мікроконтролера в режим

очікування на певні проміжки часу. Однак можна припустити, що SoC на кожному вузлі працює в безперервному активному режимі на частоті 32 МГц (тактова частота мікроконтролера). Таким чином, загальна енергія, яка використовується мікроконтролером, буде дорівнювати:

$$E_{\text{МК}} = I_{\text{МК}} \cdot V_{\text{МК}} \cdot T_{\text{МК}} \ , \tag{2.10}$$

де $I_{\text{МК}}$ – струм мікроконтролера, А;

$V_{\text{МК}}$ – напруга мікроконтролера, В;

$T_{\text{МК}}$ – час енергоспоживання мікроконтролера.

Вихідна енергія оцінюється на основі напруги, струму і часу, необхідних для включення і готовності мережі:

$$E_{\text{гот}} = I_{\text{гот}} \cdot V_{\text{гот}} \cdot T_{\text{гот}} \ , \tag{2.11}$$

де $I_{\text{гот}}$, $V_{\text{гот}}$, $T_{\text{гот}}$ – відповідні параметри, необхідні для готовності мережі.

Модель також описує енергію, споживану при відключенні вузлів, коли закінчився час мережі (період вибірки). Ця енергія задається формулою (2.12), і називається енергією відключення:

$$E_{\text{відк}} = I_{\text{відк}} \cdot V_{\text{відк}} \cdot T_{\text{відк}} \ . \tag{2.12}$$

Як і в режимі передачі, вузол витрачає енергію, коли отримує пакети. Ця енергія визначається наступним чином:

$$E_{\text{відк}} = L \cdot I_{\text{пак}} \cdot V_{\text{пак}} \cdot T_{\text{пак}} \ . \tag{2.13}$$

де $L$ – довжина пакета (байтів),

$T_{\text{пак}}$ – час (сек), протягом якого вузол приймає байт при відповідних напрузі $V_{\text{пак}}$ (вольт) та струмі $I_{\text{пак}}$ (ампер).

Для цієї моделі вузол споживає енергію від мікроконтролера в активному режимі протягом усього часу дискретизації. Наприкінці цього періоду вузол витрачає загальну енергію, спожиту всіма функціями, які він виконував під час мережевих процесів.

Описана енергетична модель має деякі обмеження. Ця модель включає в себе основні види енергії, необхідні вузлу для виконання функцій в мережі. Однак ця модель безпосередньо не описує конкретні енергії, пов'язані з аномальною поведінкою вузлів, але вона здатна передбачати дивну поведінку в мережі через зміну типових функцій вузлів. Така поведінка виникає через ситуації, таких як з'єднання і роз'єднання через перебої в каналах. Тобто це можна представити як результат інших видів енергії. Наприклад, ця ситуація відбивається в збільшенні кількості повторних передач, повторних спроб аудиту каналу і конфліктів пакетів. Ці зміни збільшують передачу, прийом, переключення і т.і. Таким чином, пропонована модель може ідентифікувати аномальну поведінку, що спостерігається в цих типах енергії, і робити висновки щодо зон ризику або потенційних атак. Тобто є періоди часу, в які певна кількість вузлів переходить в пасивний режим, споживаючи менше енергії, ніж зазвичай. З цих причин пропоновану модель легко можна масштабувати відповідно до вимог аналізу.

## 2.4. Висновки до другого розділу

1. Вперше розроблено математичну модель функціонування великомасштабних мереж на базі запитів БСМ, чиї вузли виявляють і ретранслюють події, які потрібні тільки протягом обмеженого часу. Це дозволило підвищити точність оцінки затримок передачі даних, розрахунку енергоємності та терміну служби мережі.
2. Основний шлях скорочення енергоспоживання заснований на балансі робочого циклу бездротового пристрою. Ефективна передача використовує не менше 50% від загальної енергії. 25% енергії витрачається під час

конкурентного доступу до середовища. Механізм виявлення використовує 15% енергії, головним чином через необхідність активації приймача під час очікування підтвердження. 20% енергії витрачається на прослуховування маяків.

3. Ґрунтуючись на енергетичному балансі трансивера, визначено кілька ключових способів підвищення загальної енергоефективності бездротових мереж. Конкретні методи включають в себе скорочення часу переходу між станами та створення приймача на фізичному рівні пристрою, що вимагає зміни фірмової прошивки стандартного приймача-передавача. При цьому, скорочення часу переходу між станами в два рази призводить до зменшення загальної середньої потужності на 12%. Приймач, який пропонує режим малої потужності для визначення каналу і очікування кадру підтвердження, має потенціал зменшення загальної середньої потужності на додаткові 15%.
4. З огляду на енергоємність процесу передачі даних саме управління розмірами повідомлень є основним резервом збільшення терміну життя пристроїв і системи в цілому.

Результати даного розділу опубліковано в роботах автора [37, 38, 40, 42, 76, 87, 88, 89, 103].

# РОЗДІЛ 3. ЕНЕРГОСПОЖИВАННЯ ТА ІНФОРМАЦІЙНА БЕЗПЕКА БЕЗДРОТОВОЇ СЕНСОРНОЇ МЕРЕЖІ

## 3.1. Експериментальна установка для вимірювання витрати енергії батарей

Для фактичного визначення енергоспоживання пристрою збору та передачі даних застосована схема побудови випробувального стенду з використанням цифрового осцилографа УНІПРО В-121. За своєю суттю осцилограф є вольтметром, що показує графік напруги. Однак з його допомогою можна спостерігати і форму струму. Для цього послідовно з досліджуваної ланцюгом включають резистор $R_C$ (тут індекс «*c*» означає струмовий), рис. 3.1. На резисторі за законом Ома виникає падіння напруги:

$$u(t) = i(t)R_C. \tag{3.1}$$

Ця напруга і вимірюється осцилографом. А знаючи величину $R_C$ можна перевести напругу, що показується осцилографом, в струм.

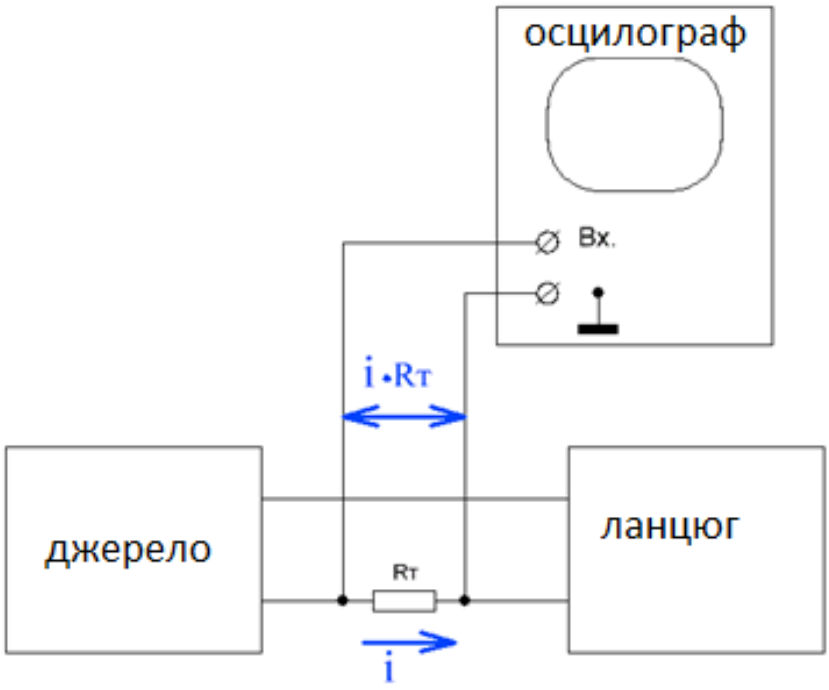



Рисунок 3.1 – Схема випробувального стенду

Як джерело живлення обраний літій-іонний акумулятор 18650. Вибір даного джерела обумовлений тим, що ми повинні мати джерело з гарантованими параметрами напруги і ємності, які контролюється мікропроцесорним зарядним пристроєм IMAX B-6. Резистор $R_C$ потужністю 10 Вт має номінал 3,3 Ом. Опір резистора $R_C$ набагато менше, ніж опір ланцюга вимірювання осцилографа, який становить 1 МОм. У цьому випадку резистор не впливає на роботу приладу і його включення не призводить до змін режиму роботи ланцюга живлення досліджуваного ПЗПД.

На рисунку 3.2 представлена схема вимірювання параметрів енергоспоживання польових пристроїв «Сигма ZB», обладнаних трансиверами фірм DIGI і REXENSE, в режимі робочої експлуатації.

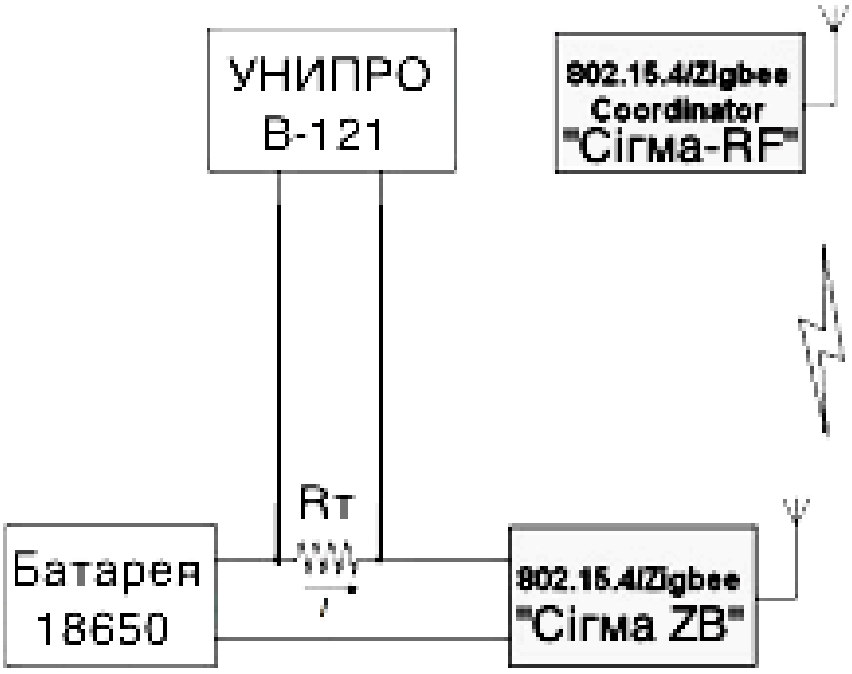



Рисунок 3.2 – Схема експерименту

Згідно з теоремою Найквіста-Шенона (Котельникова), оскільки мінімальне часове вікно спостереження становить 200 мс, , то максимальна частота дискретизації повинна дорівнювати 50 КГц. Саме зазначені значення застосовані для проведення вимірювань в рамках цієї роботи.

Експериментальне визначення розряду батареї в режимі побудови мережі представлено нижче.

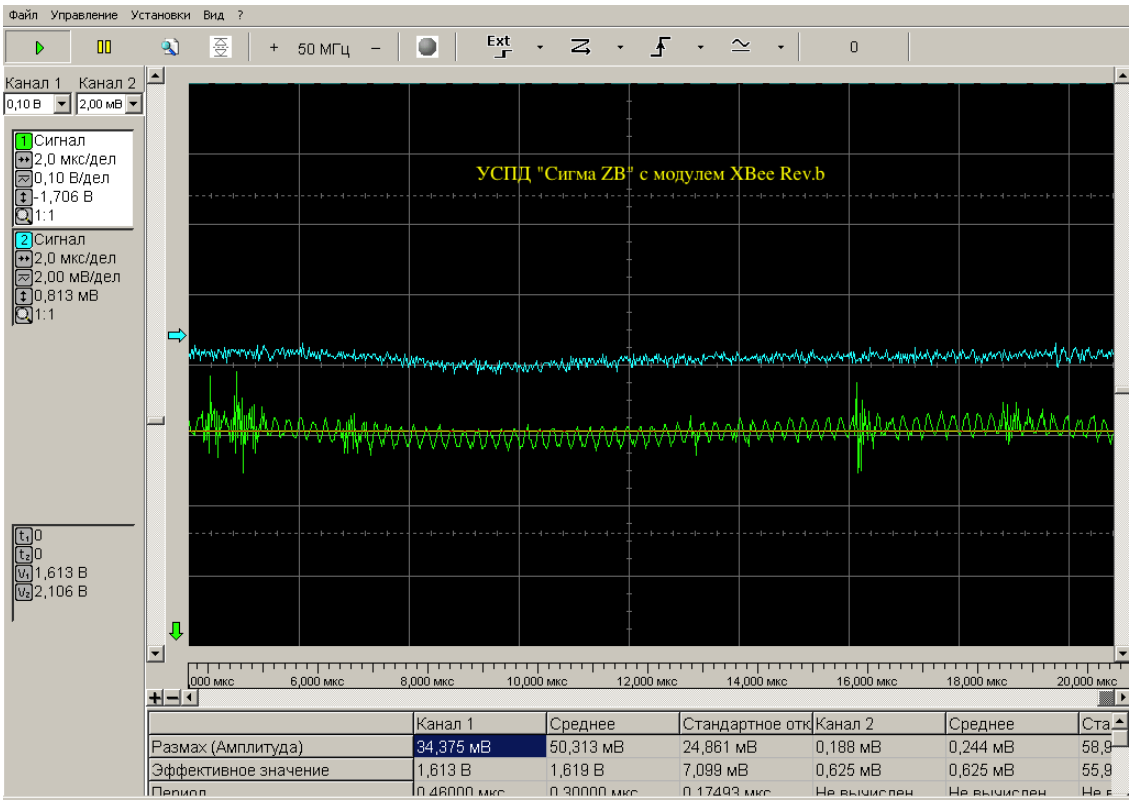



Рисунок 3.3 – Вид сигналу на моніторі (модульXBee rev.b)

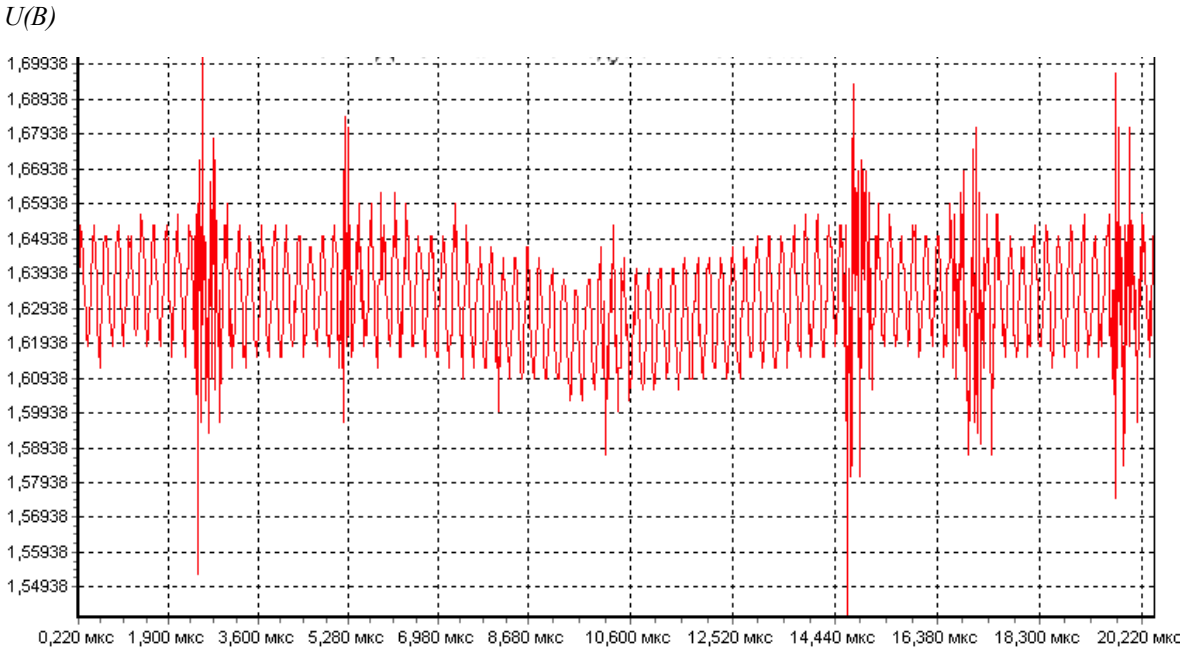



Рисунок 3.4 –Значення напруги на резисторі-шунті

Наведені вище графіки відносяться до вимірювання параметрів енергоспоживання ПЗПД «Сигма-ZB» з встановленим модулем XBee rev.b потужністю 1 мВт.

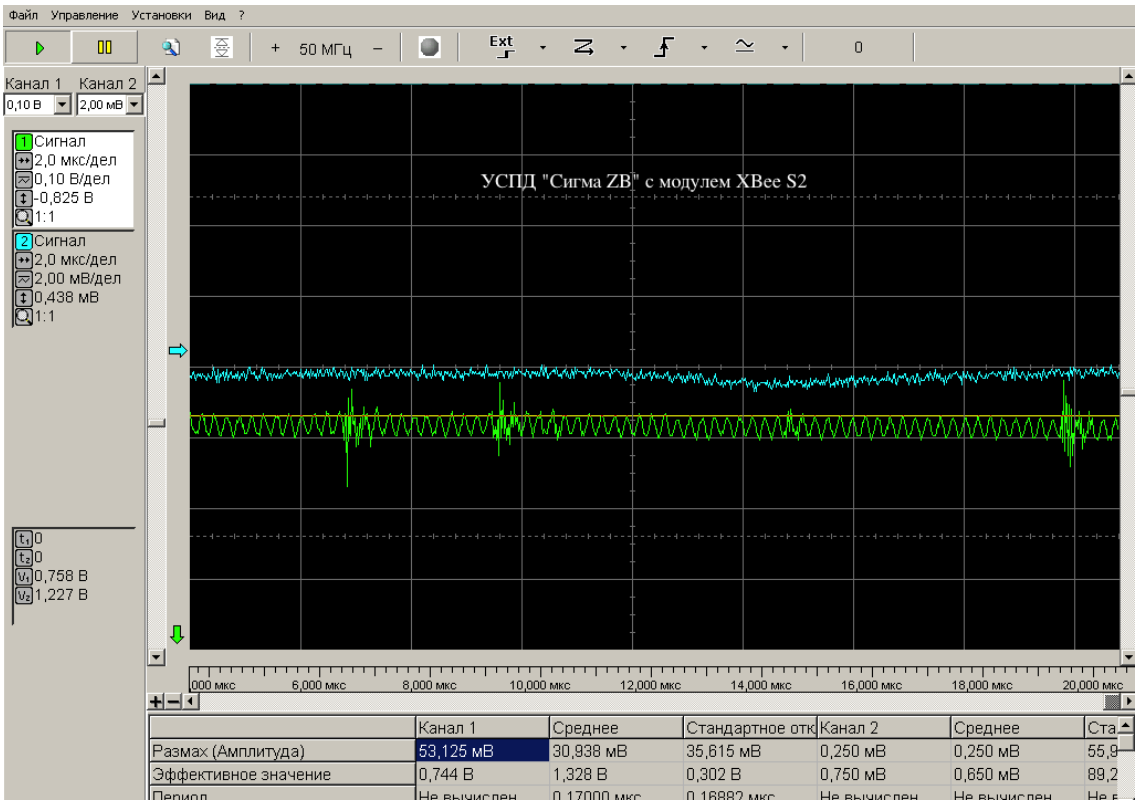



Рисунок 3.5 – Вид сигналу на моніторі (модульXBee S2)

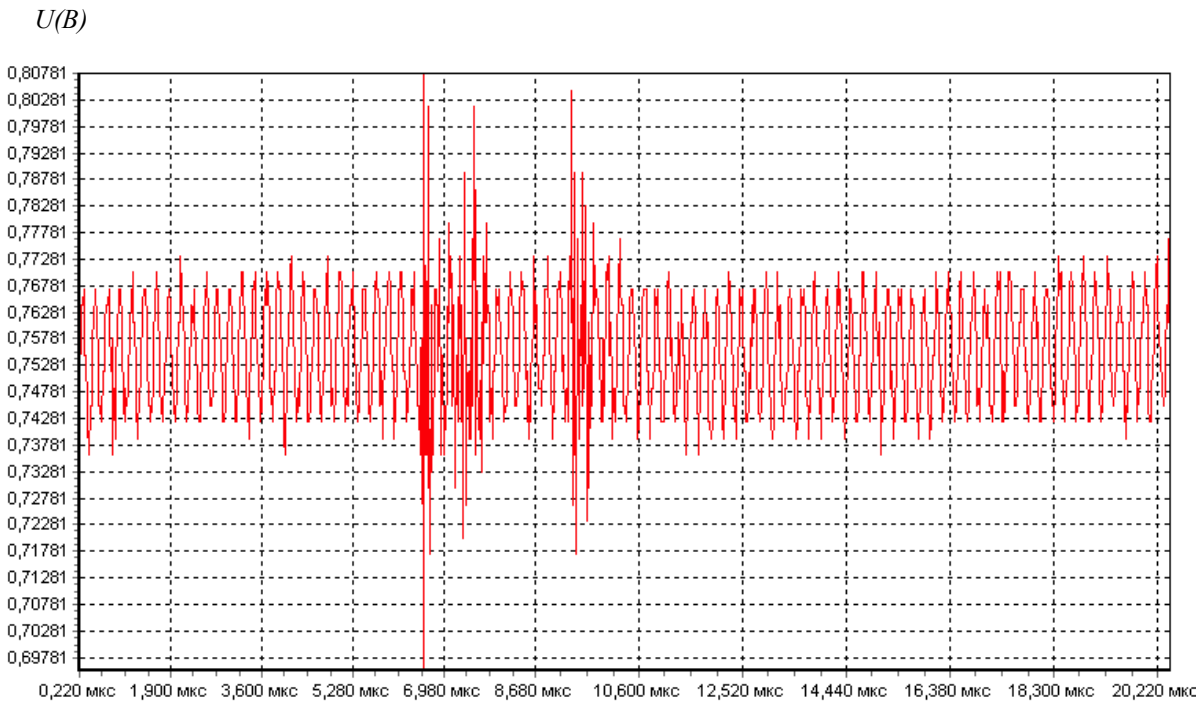



Рисунок 3.6 – Значення напруги на резисторі

Наведені вище на рисунках 3.5 і 3.6 графіки відносяться до вимірювання параметрів енергоспоживання ПЗПД «Сигма-ZB» з встановленим модулем SMT XBee S2 потужністю 4 мВт.

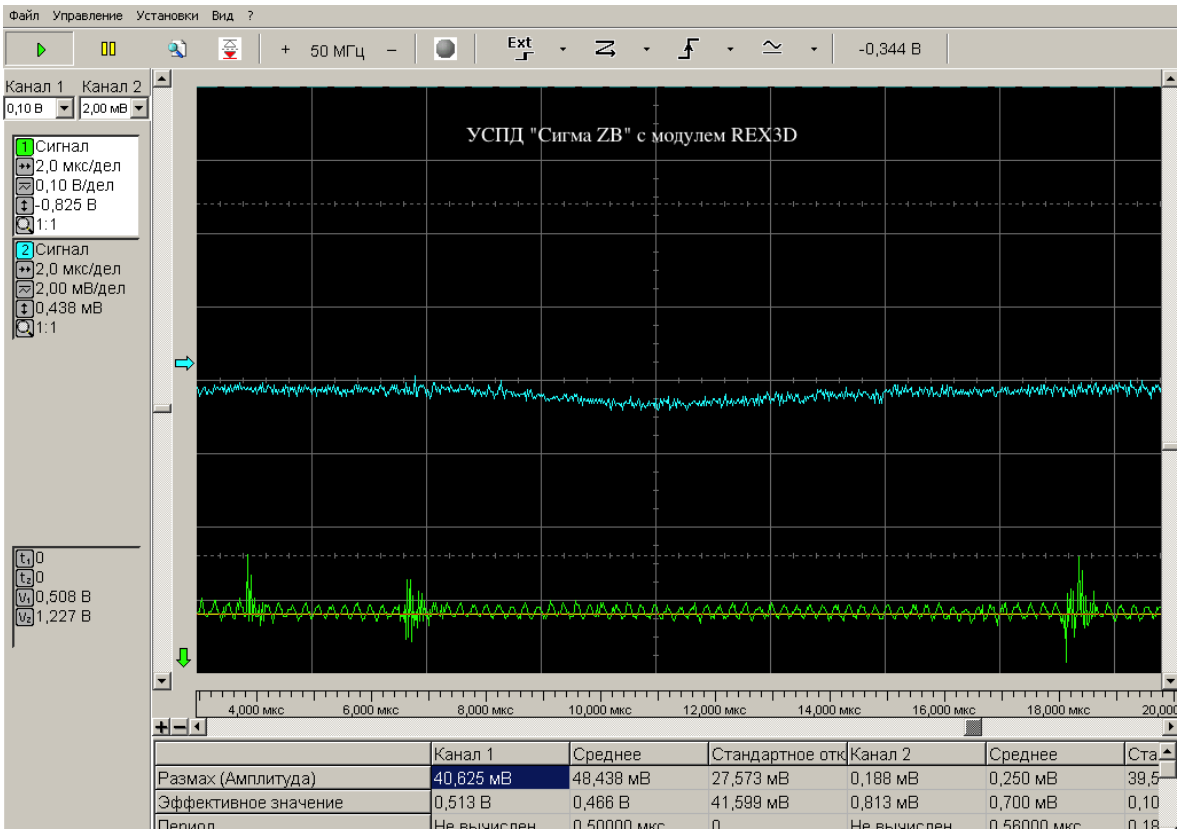



Рисунок 3.7 – Вид сигналу на моніторі (модуль REX3D)

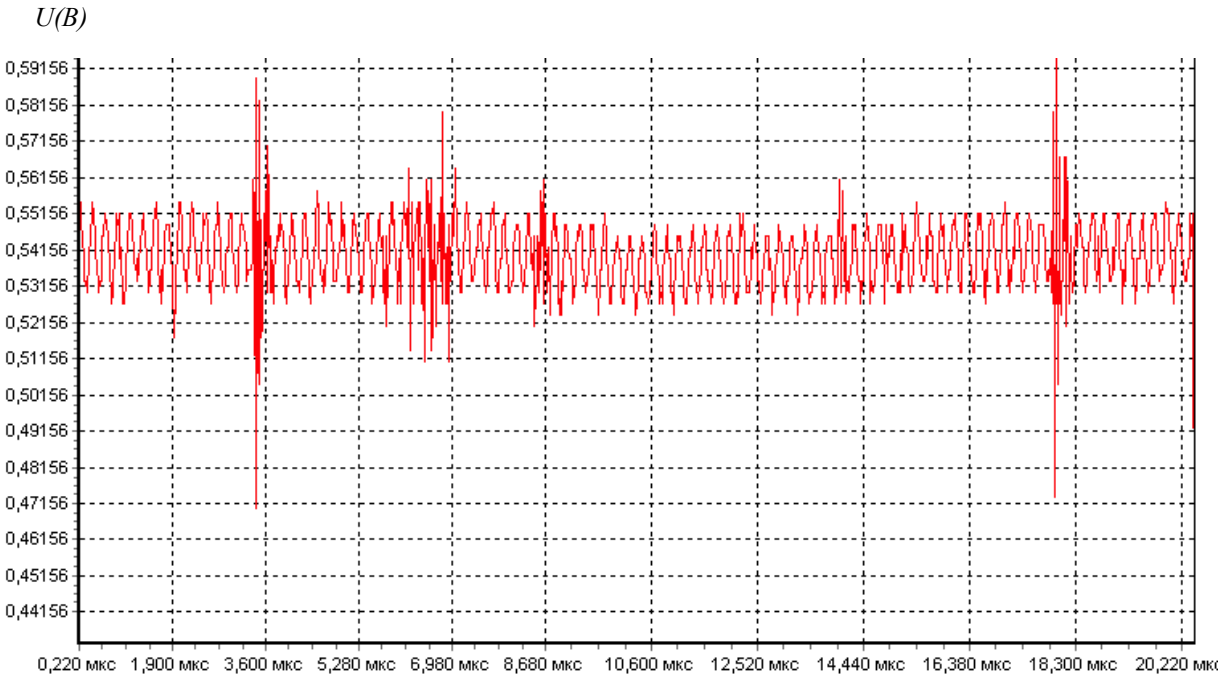



Рисунок 3.8 – Значення напруги на резисторі

Наведені вище на рисунках 3.7 і 3.8 графіки відносяться до вимірювання параметрів енергоспоживання ПЗПД «Сигма-ZB» з встановленим модулем REX3D потужністю 6 мВт. Виходячи з відомих значень ефективного значення стандартного відхилення і опору резистора можна визначити ефективне значення середнього струму споживання пристроїв «Сигма-ZB».

Таблиця 3.1 – Експериментальні значення в режимі робочої експлуатації

| Тип модуля | Потужність, мВт | Стандартне відхилення, мВ | Середнє значення ефективного струму, мА |
|---|---|---|---|
| XBee rev.b | 1,0 | 7,099 | 2.151 |
| XBee S2 | 4.0 | 302,0 | 91,515 |
| REX3D | 6,0 | 41,599 | 12,606 |

### 3.2. Енергоспоживання польових пристроїв в робочих режимах

З огляду на очікувану залежність енергоспоживання польових пристроїв від розміру переданих по мережі даних пакетів виконано визначення параметрів при різних режимах роботи мережевих пристроїв, обладнаних трансиверами DIGI (S1 і S2) і REXENSE (REX3D). Експеримент проводився в середовищі SCTM-Dialog з фіксуванням характеристик переданих та отриманих пакетів.

#### 3.2.1. Енергоспоживання ПЗПД з трансивером XBee

Режим синхронізації часу в мережі. Структура пакета представлена на рис.3.9.

Скрін екрану осцилограми і графік представлені на рисунках 3.10 і 3.11, відповідно.

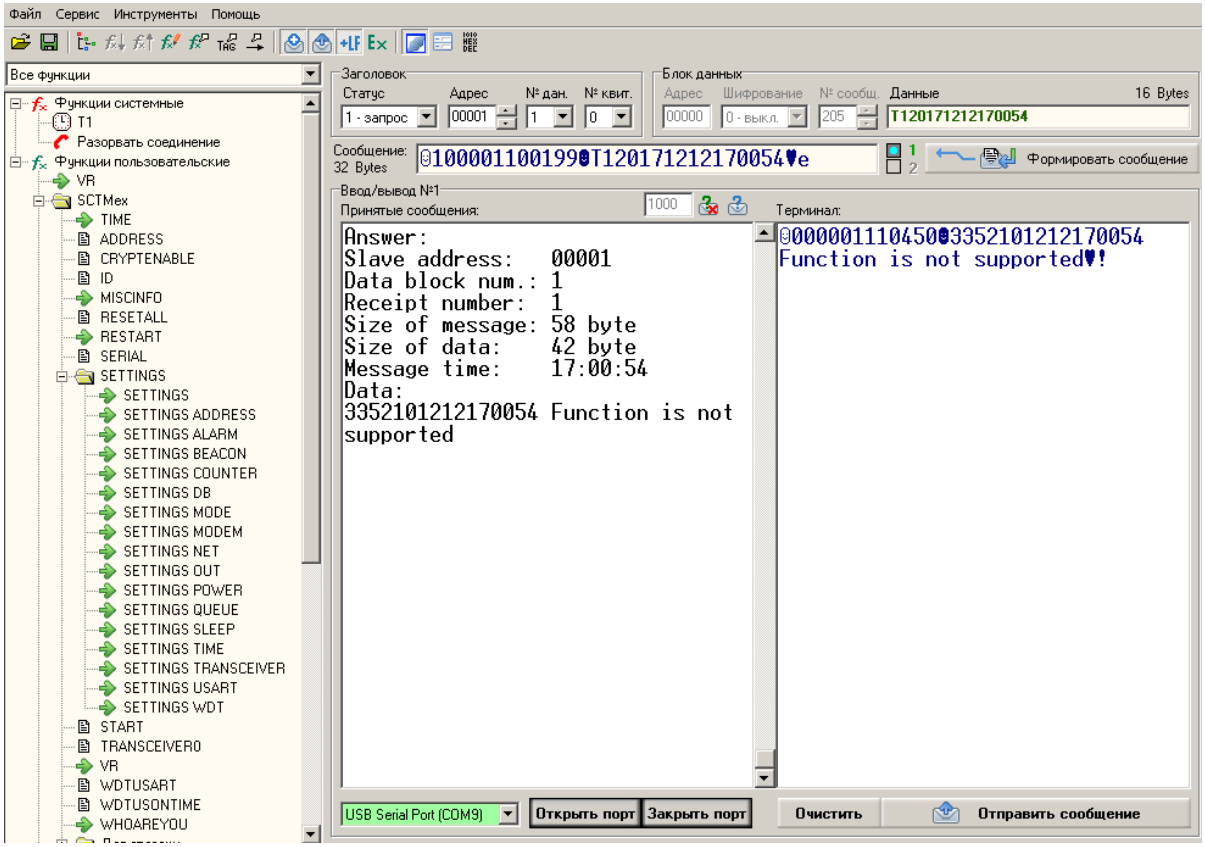



Рисунок 3.9 – Формат пакета встановлення часу

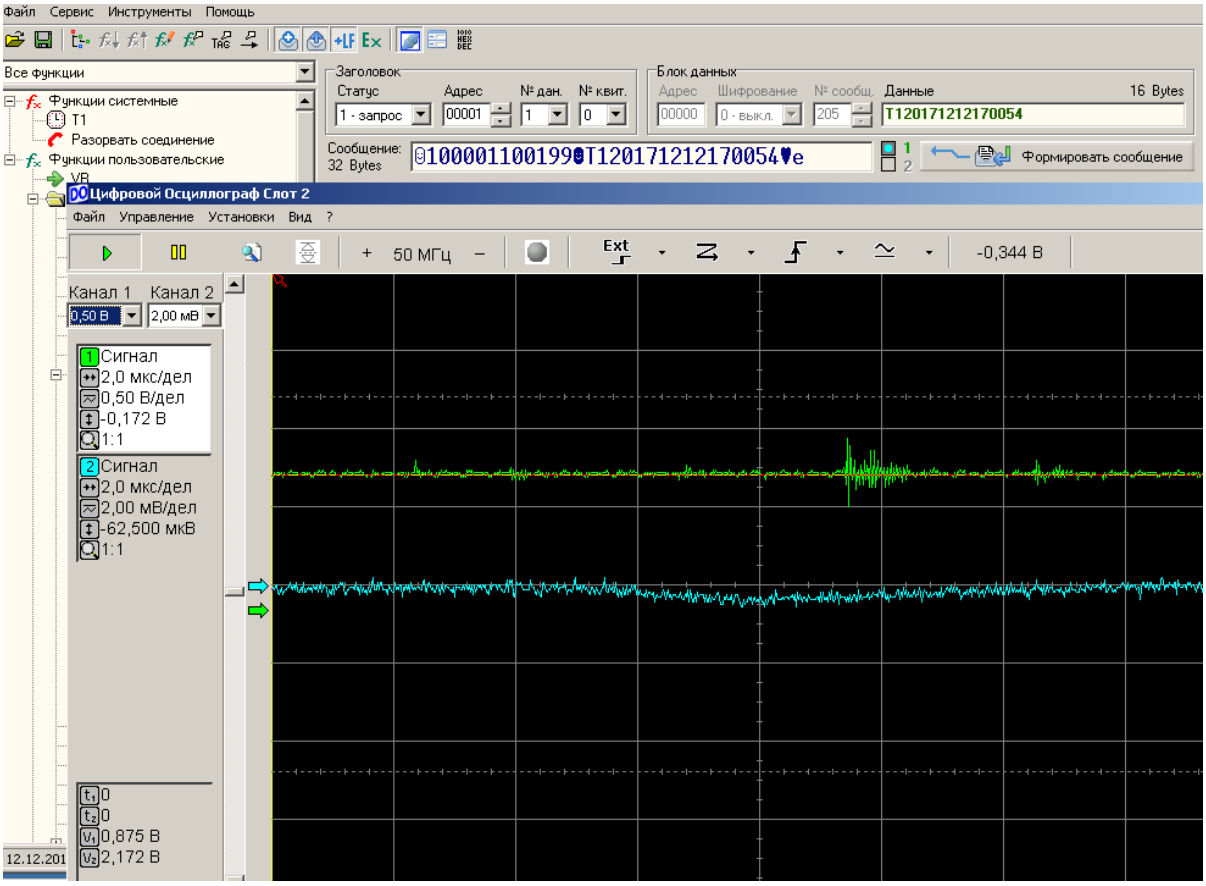



Рисунок 3.10 – Осцилограма пакета (скрін екрану)

*U(B)*

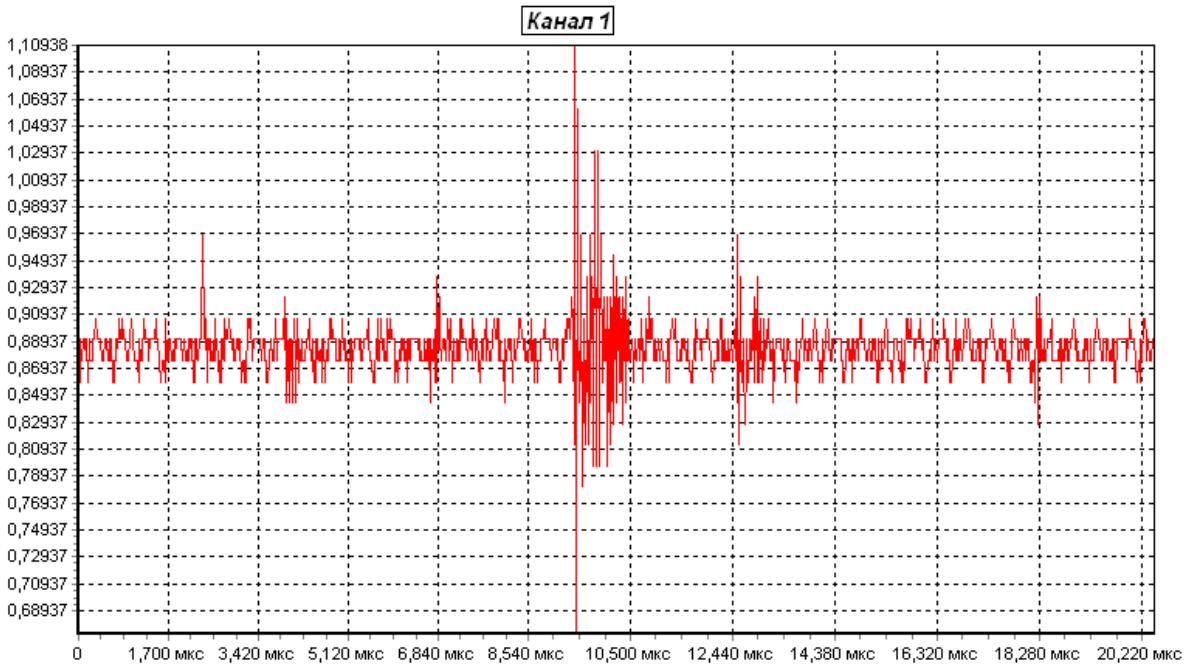



Рисунок 3.11 – Вид сигналу синхронізації часу на вимірювальному шунті

### 3.2.2. Енергоспоживання ПЗПД з трансивером XBee S2

Режим синхронізації часу в мережі. Структура пакета представлена на рис.3.12.

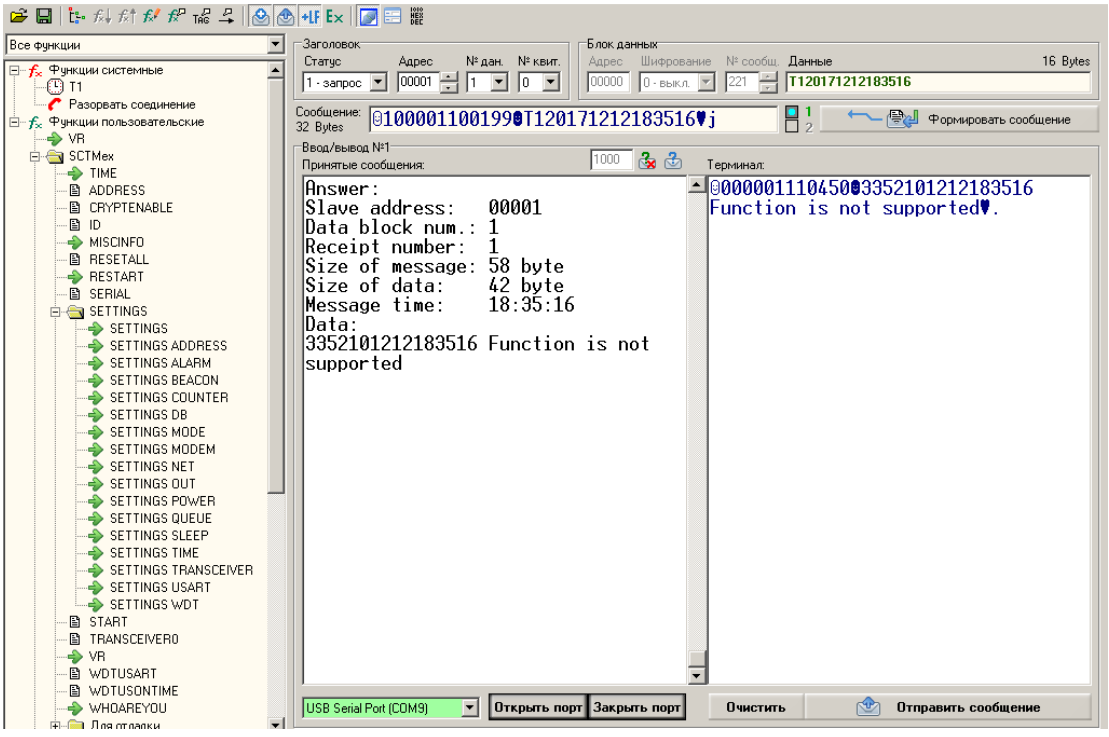



Рисунок 3.12 – Формат пакета встановлення часу

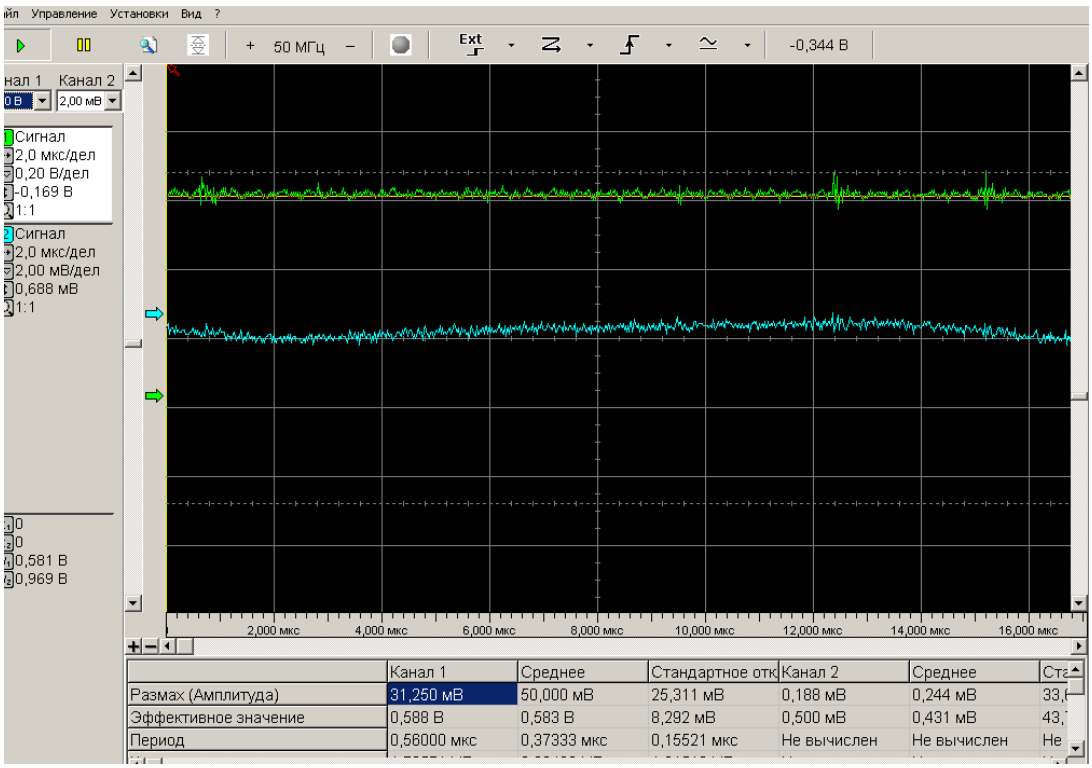



Рисунок 3.13 – Осцилограма пакета (скрін екрану)

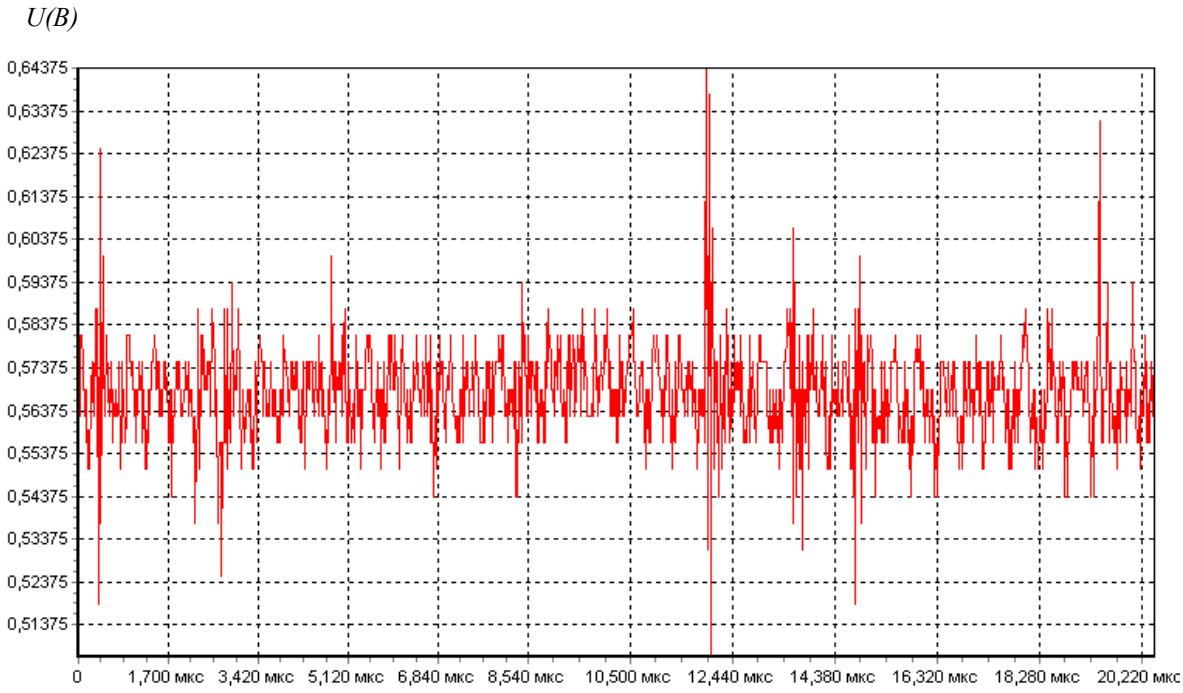



Рисунок 3.14 – Вид сигналу синхронізації часу на вимірювальному шунті

### 3.2.3. Енергоспоживання ПЗПД з трансивером REX3D

Режим синхронізації часу в мережі. Структура пакета представлена на рис.3.15.

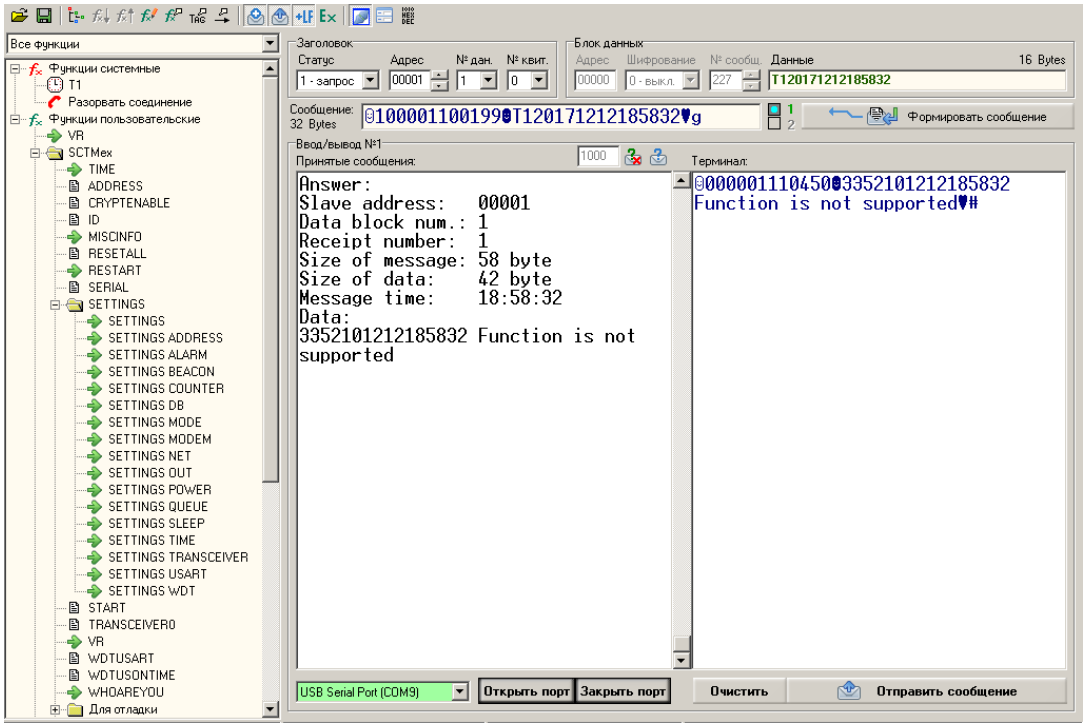



Рисунок 3.15 – Формат пакета встановлення часу

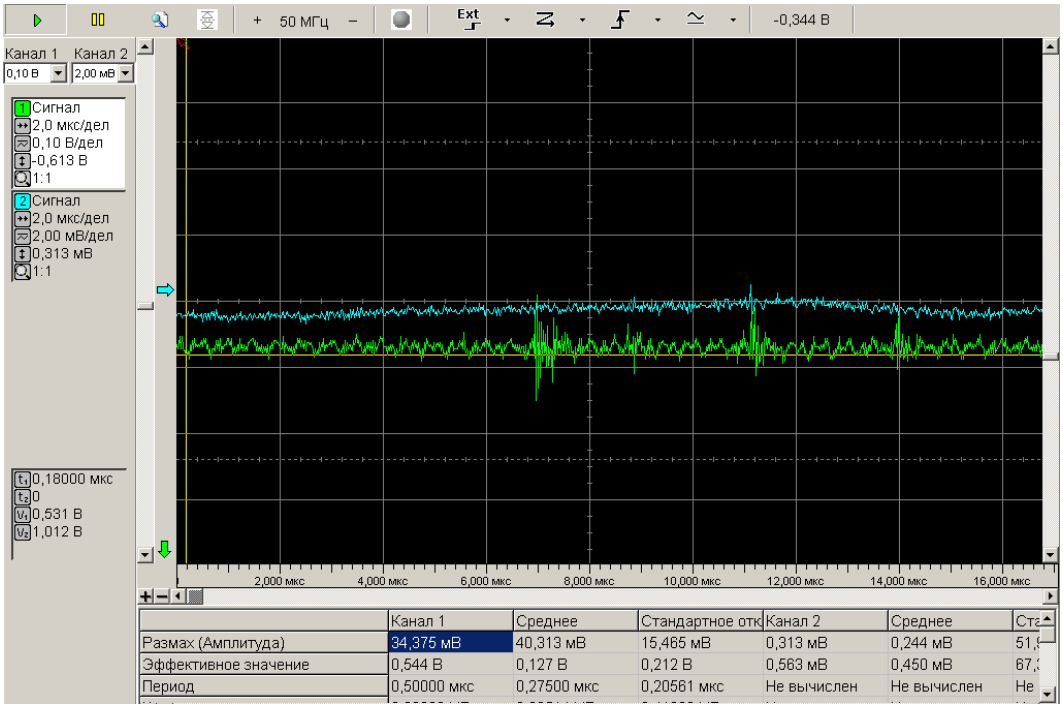



Рисунок 3.16 – Осцилограма пакета (скрін екрану)

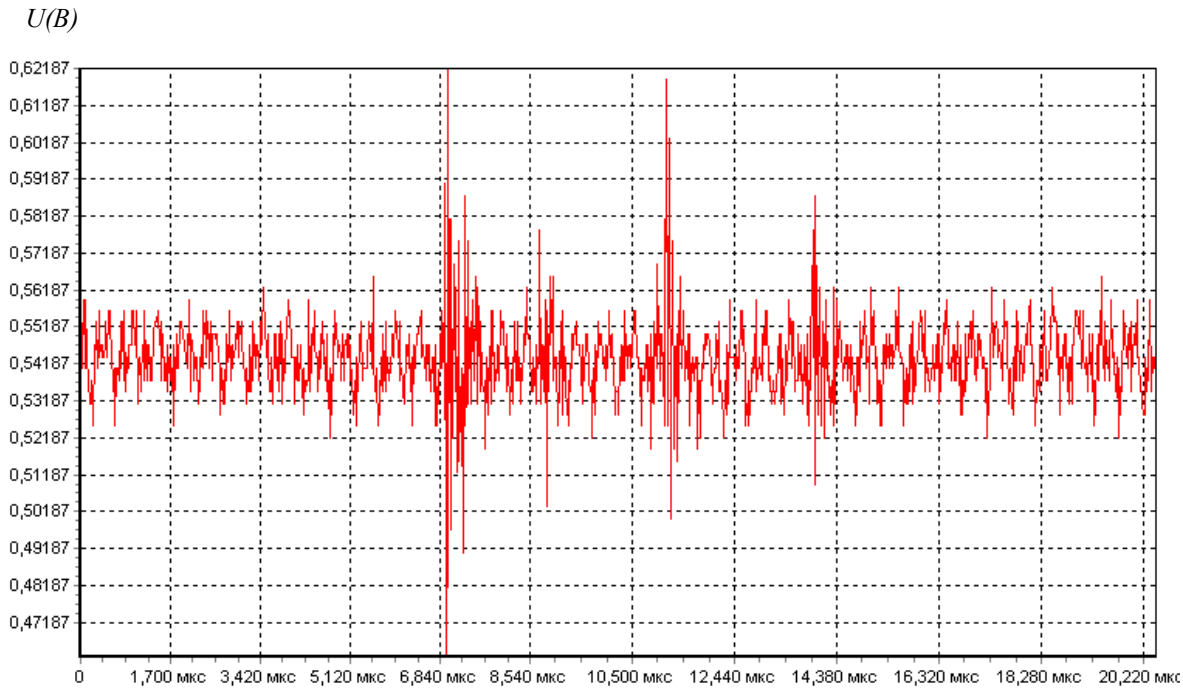



Рисунок 3.17 – Вид сигналу синхронізації часу на вимірювальному шунті

Виходячи з відомих значень ефективного значення стандартного відхилення і опору резистора-шунта визначено ефективне значення середнього струму споживання пристроїв «Сигма-ZB» в режимі синхронізації часу мережі і розмірі пакета 58 байт.

Таблиця 3.2 – Експериментальні значення в режимі синхронізації часу мережі

| Тип модуля | Потужність, мВт | Стандартне відхилення, мВ | Середнє значення ефективного струму, мА |
|---|---|---|---|
| XBee rev.b | 1,0 | 2,51 | 4,14 |
| XBee S2 | 4.0 | 25,31 | 41,77 |
| REX3D | 6,0 | 15,47 | 25,52 |

### 3.2.4. Енергоспоживання ПЗПД з трансивером XBee

Режим установки адреси польового пристрою. Розмір пакета 34 байта.

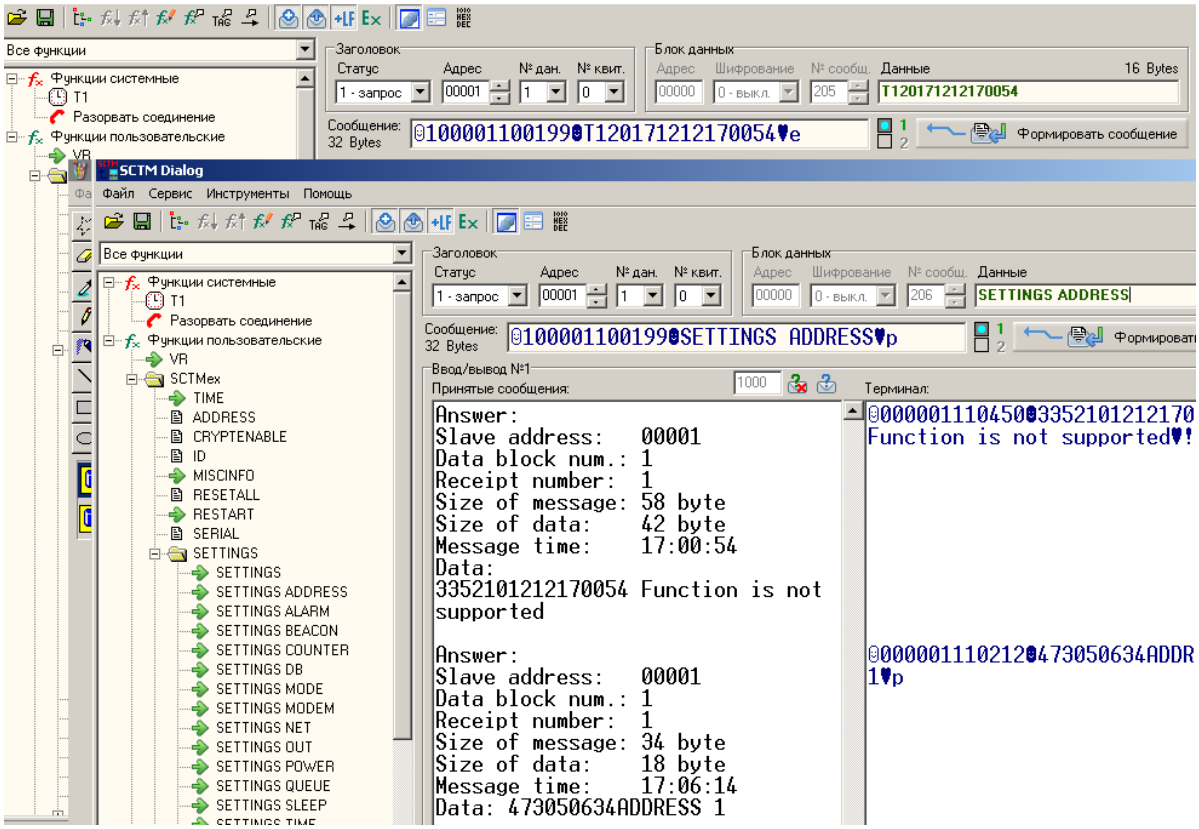



Рисунок 3.18 – Формат пакета адресації

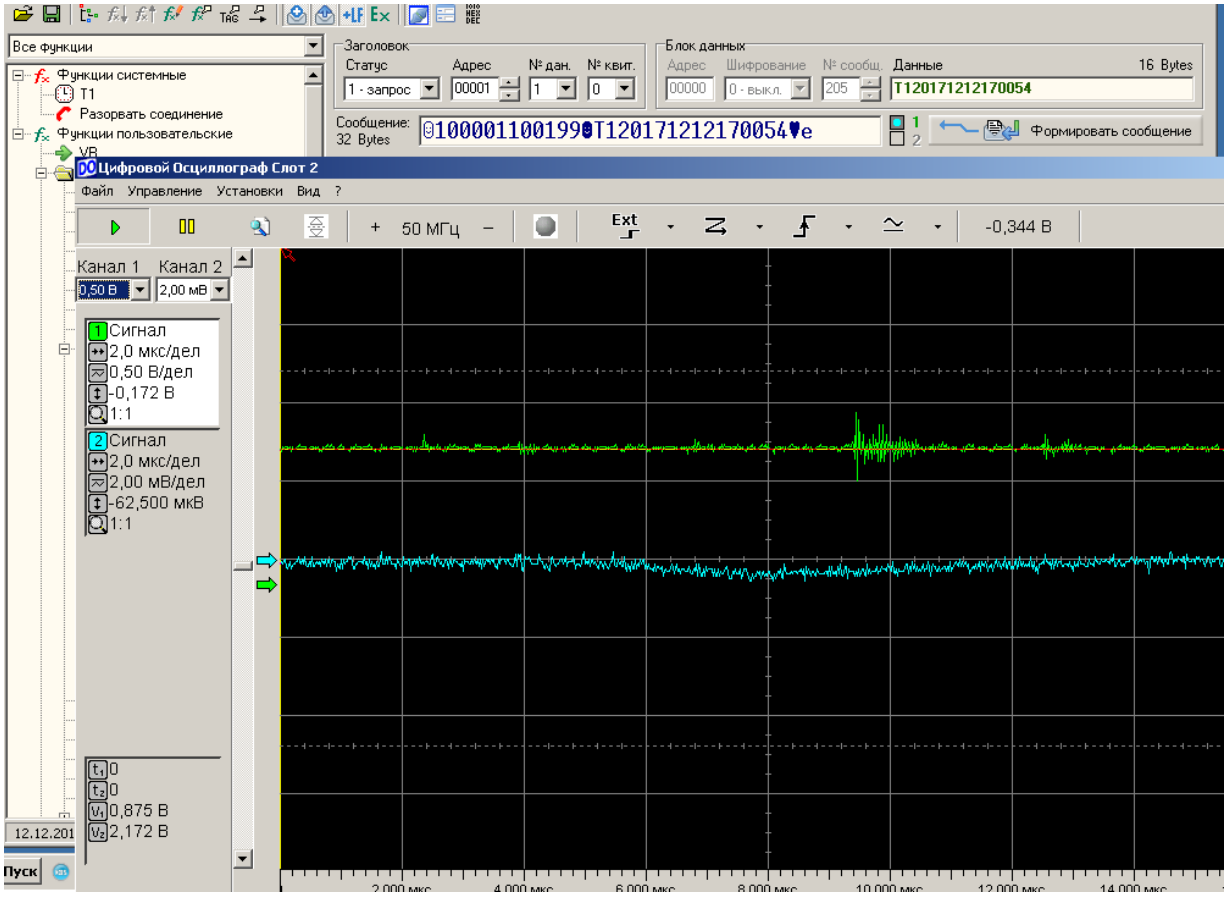



Рисунок 3.19 – Осцилограма пакета адресації

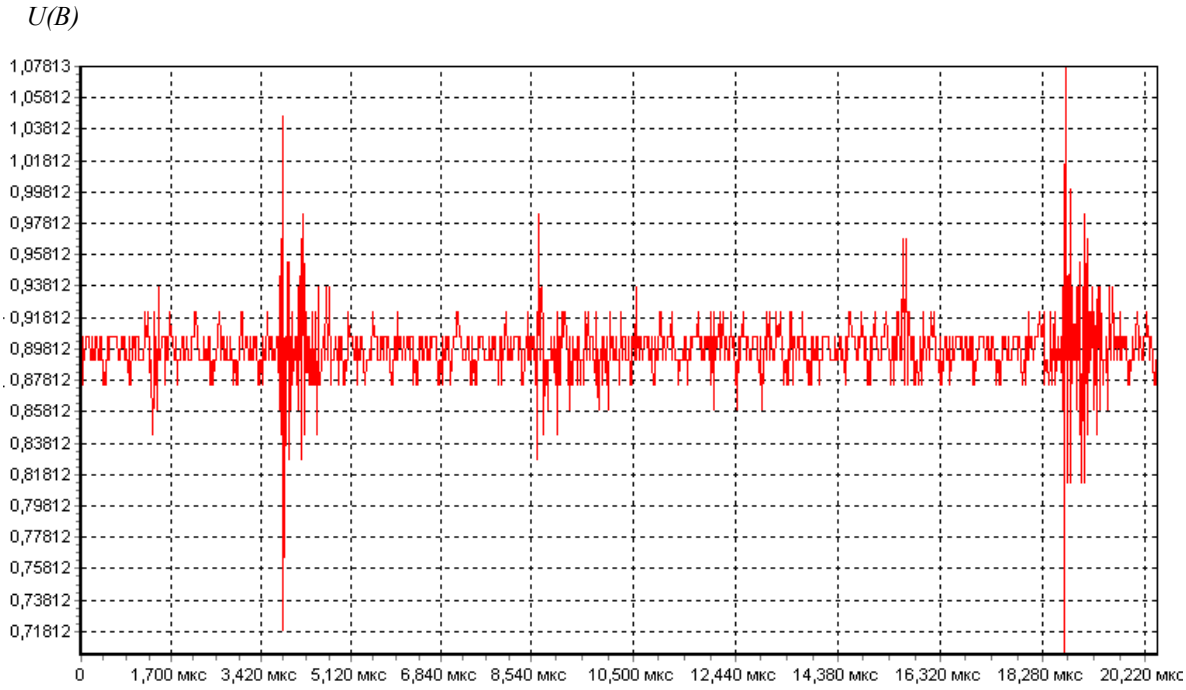



Рисунок 3.20 – Вид сигналу адресації на вимірювальному шунті

### 3.2.5. Енергоспоживання ПЗПД з трансивером XBee S2

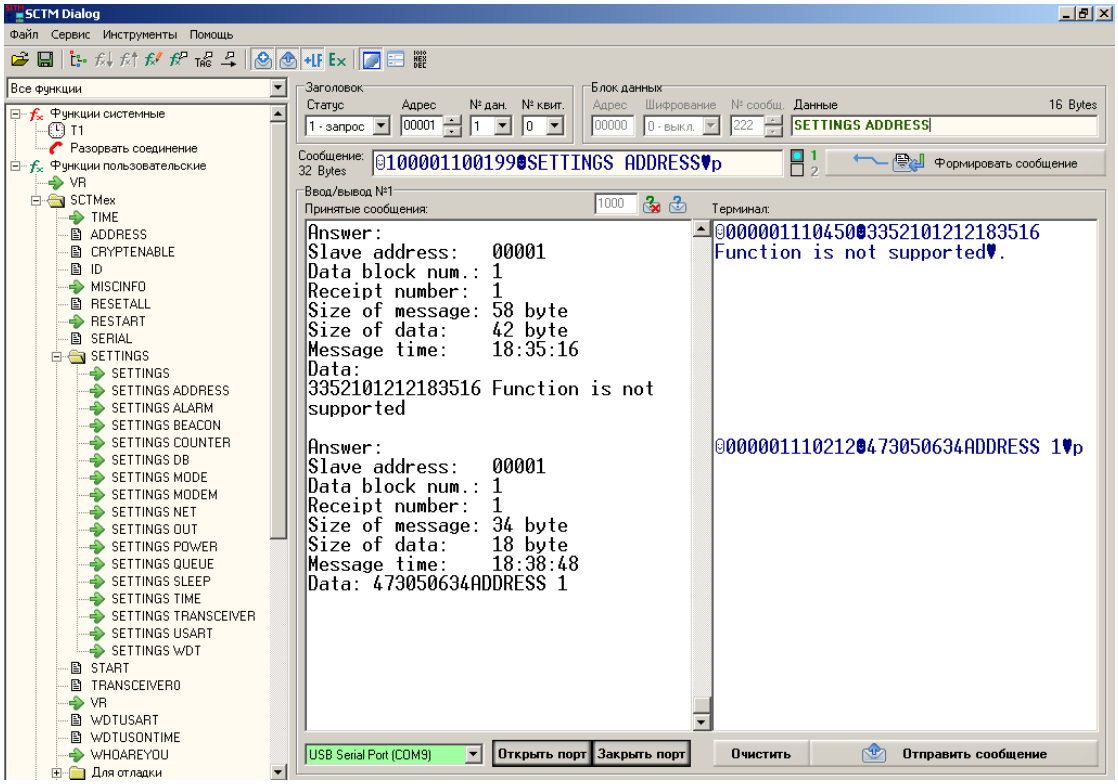



Рисунок 3.21 – Формат пакета адресації

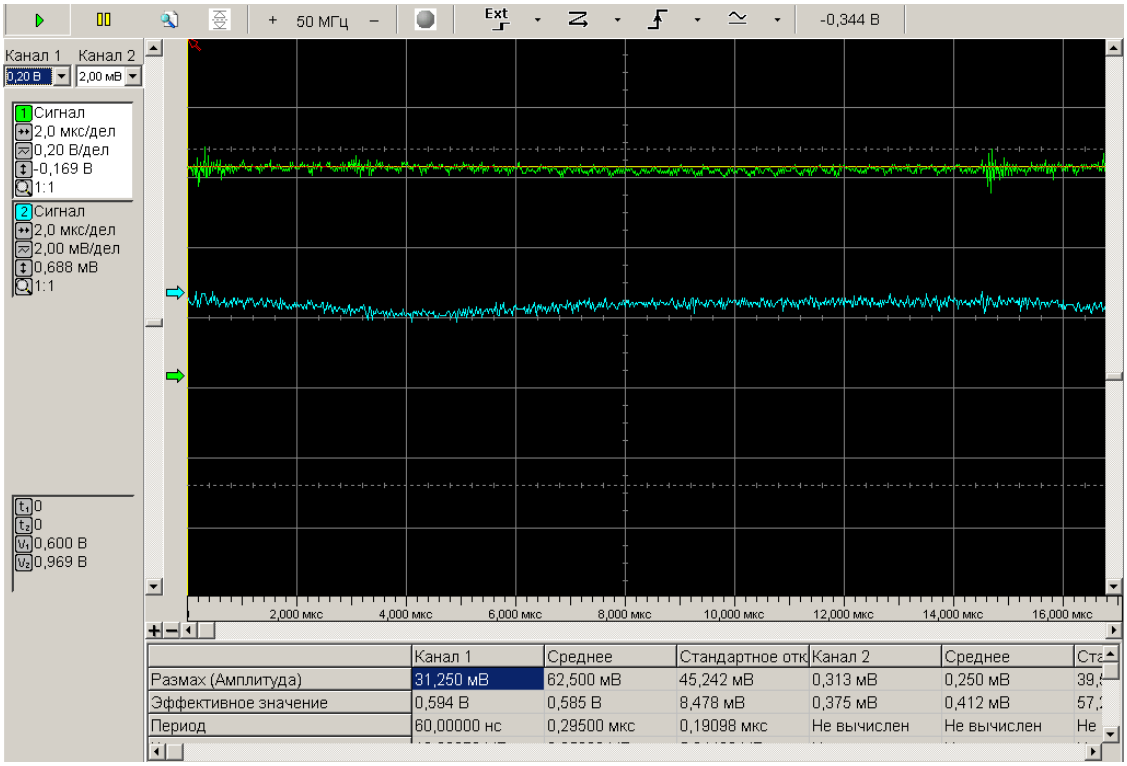



Рисунок 3.22 – Осцилограма пакета адресації

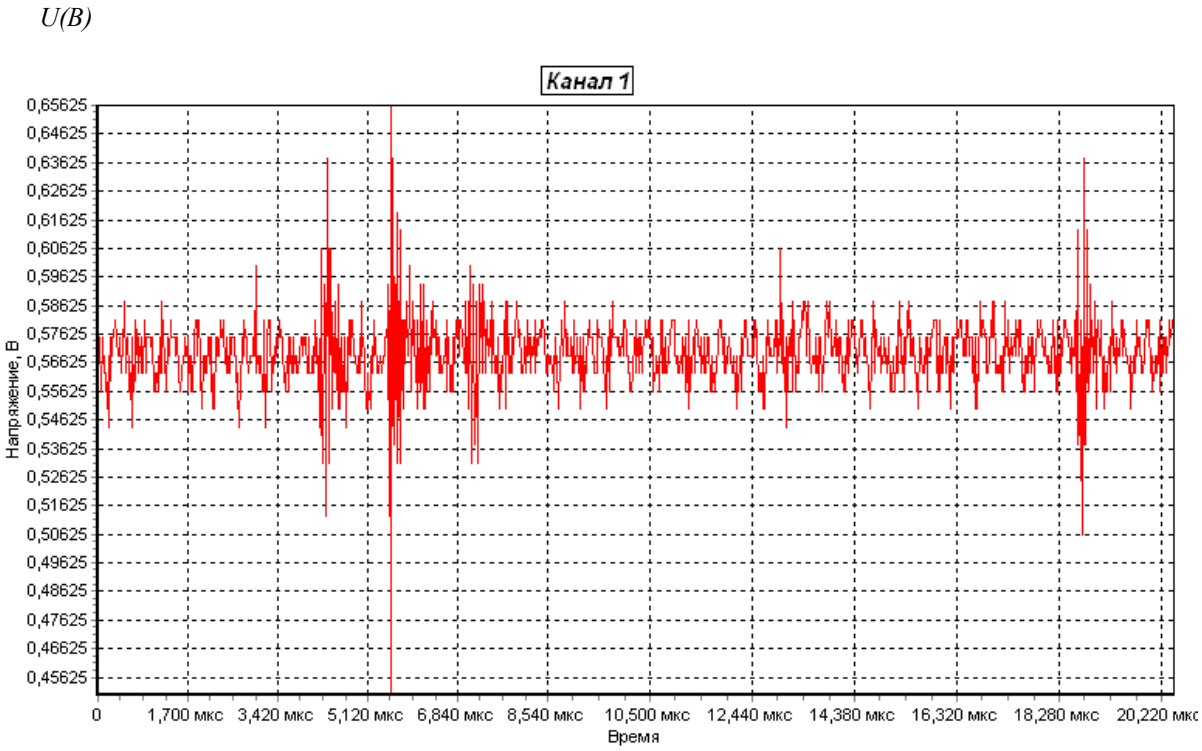



Рисунок 3.23 – Вид сигналу адресації на вимірювальному шунті

### 3.2.6. Енергоспоживання ПЗПД з трансівером REX3D

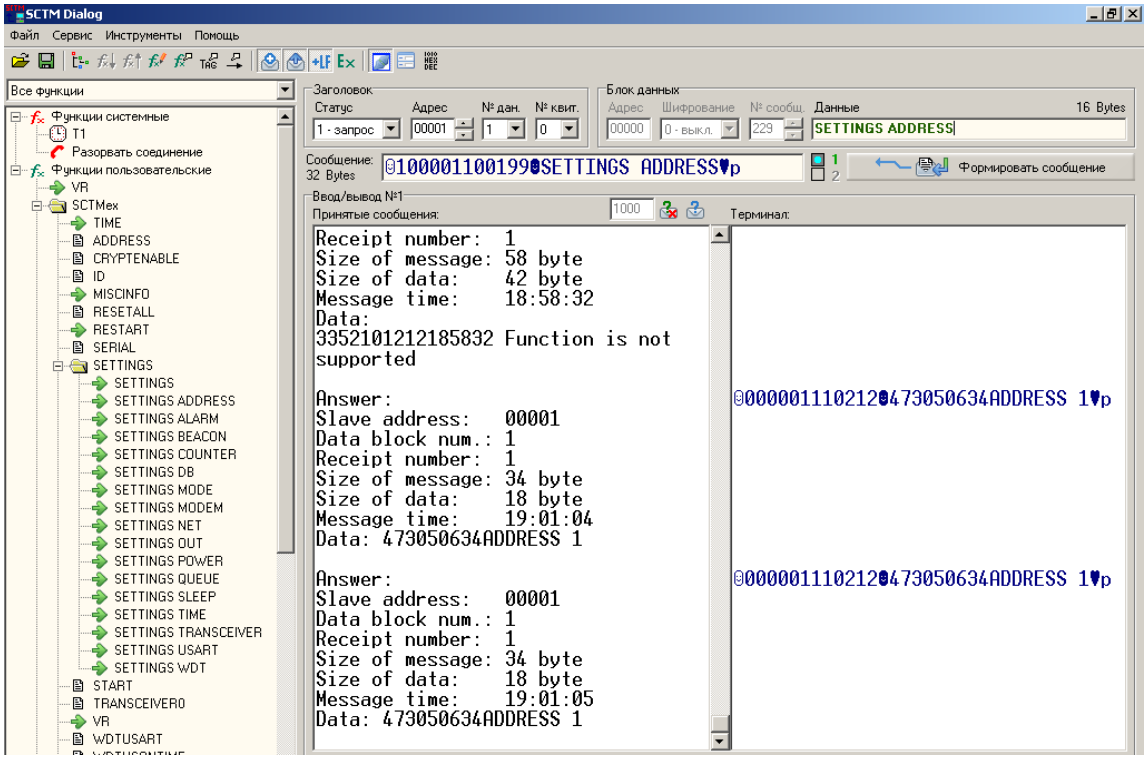



Рисунок 3.24 – Формат пакета адресації

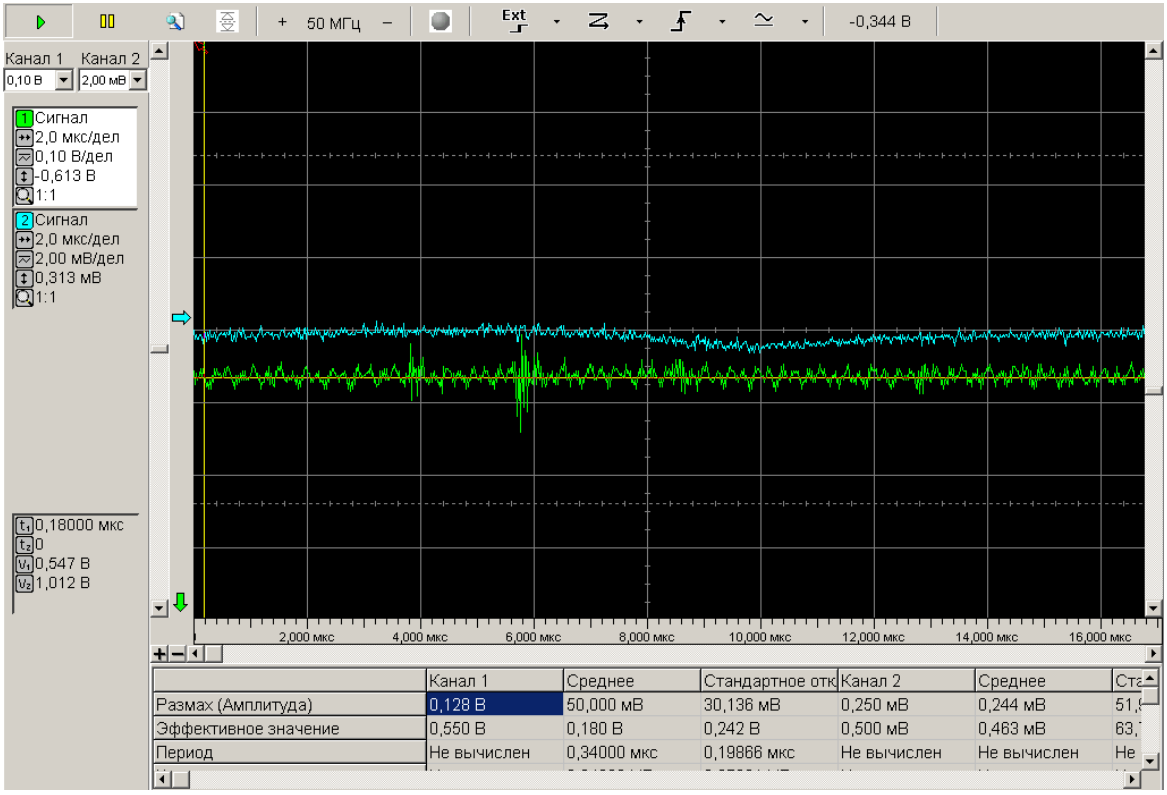



Рисунок 3.25 – Осцилограма пакета адресації

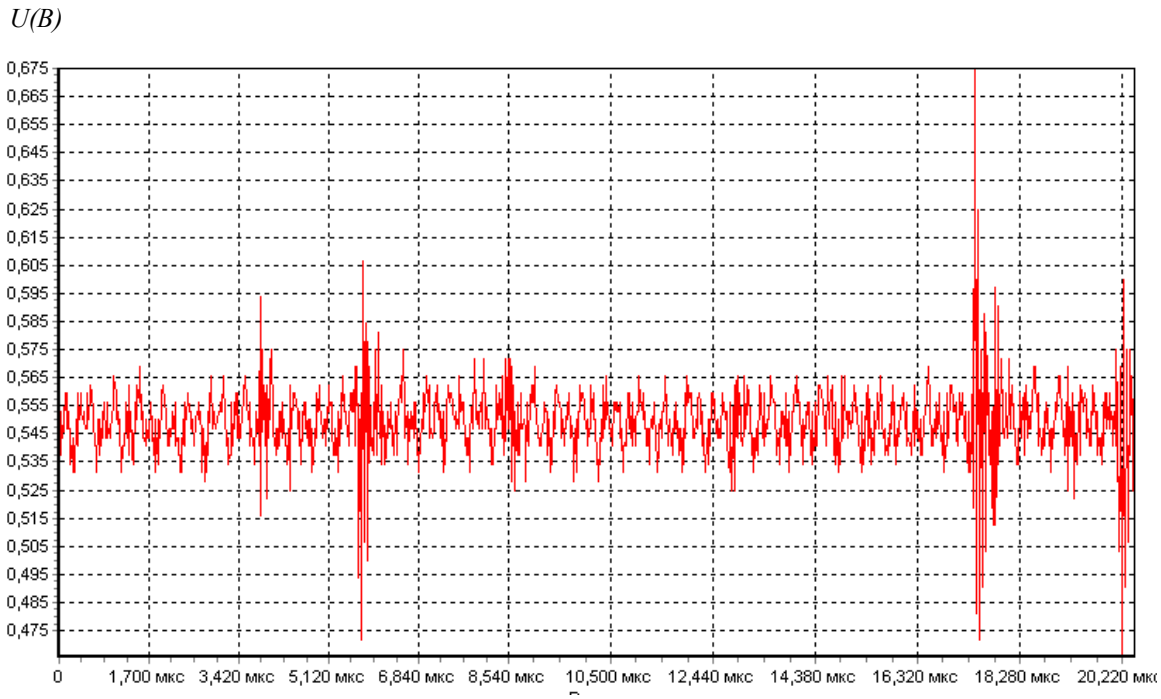



Рисунок 3.26 – Вид сигналу адресації на вимірювальному шунті

Виходячи з виміряних значень ефективного значення стандартного відхилення і опору резистора визначено ефективне значення середнього струму споживання пристроїв «Сигма-ZB» в режимі адресації мережі і розмір пакета 34 байта.

Таблиця 3.3 – Експериментальні значення в режимі встановлення адреси і розмірі пакету 34 байта

| Тип модуля | Потужність, мВт | Стандартне відхилення, мВ | Середнє значення ефективного струму, ма |
|---|---|---|---|
| XBee rev.b | 1,0 | 5,22 | 8,62 |
| XBee S2 | 4.0 | 45,24 | 74,66 |
| REX3D | 6,0 | 30,14 | 49,73 |

### 3.2.7. Енергоспоживання ПЗПД з трансивером XBee

Режим активації приймально-передавача. Розмір пакета 62 байта.

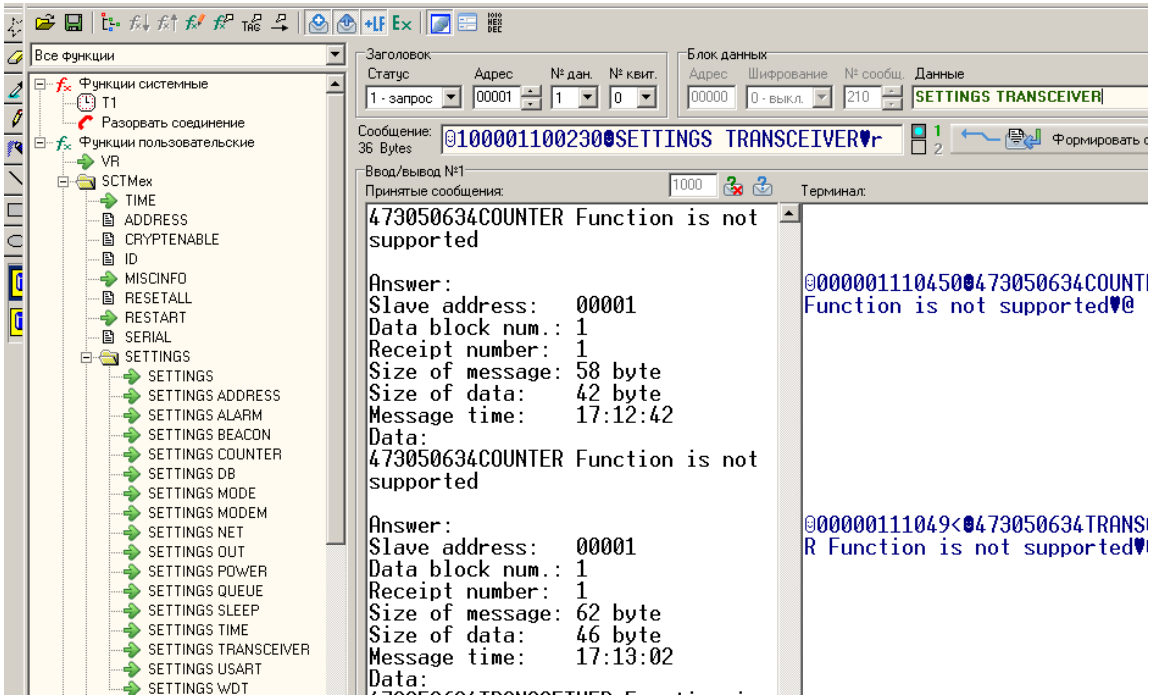



Рисунок 3.27 – Формат пакета активації трансивера

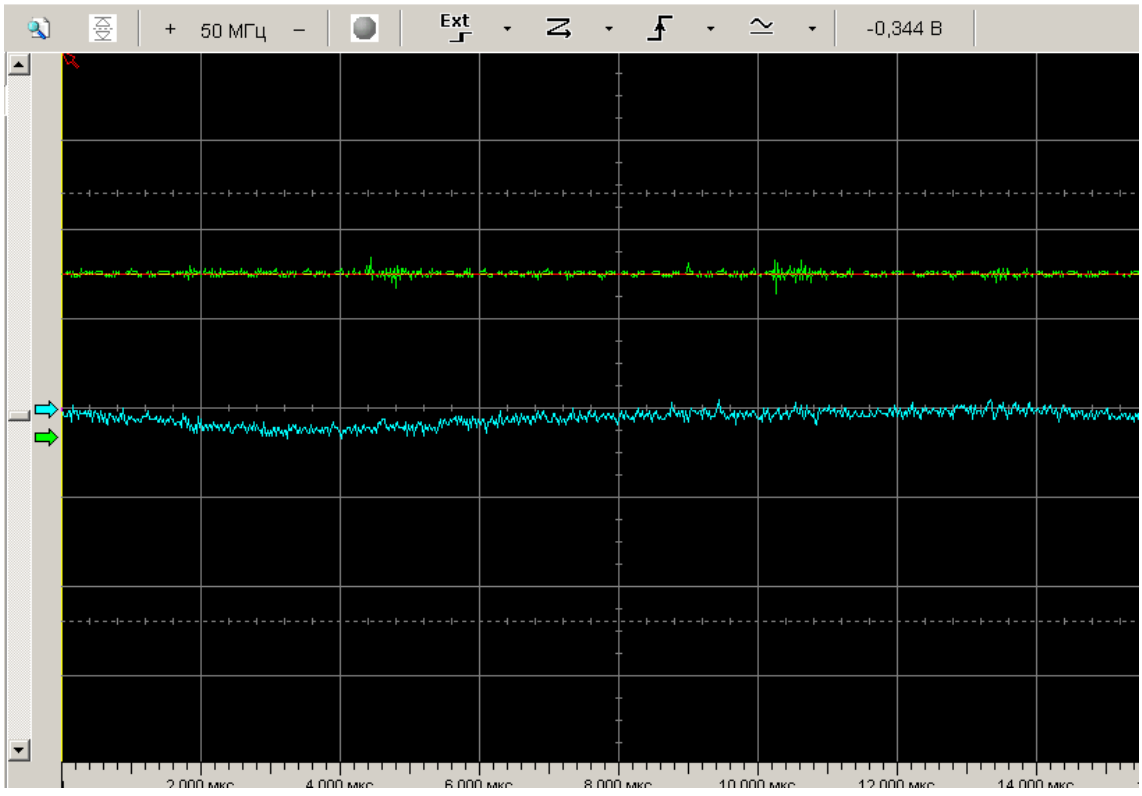



Рисунок 3.28 – Осцилограма пакета адресації

*U(B)*

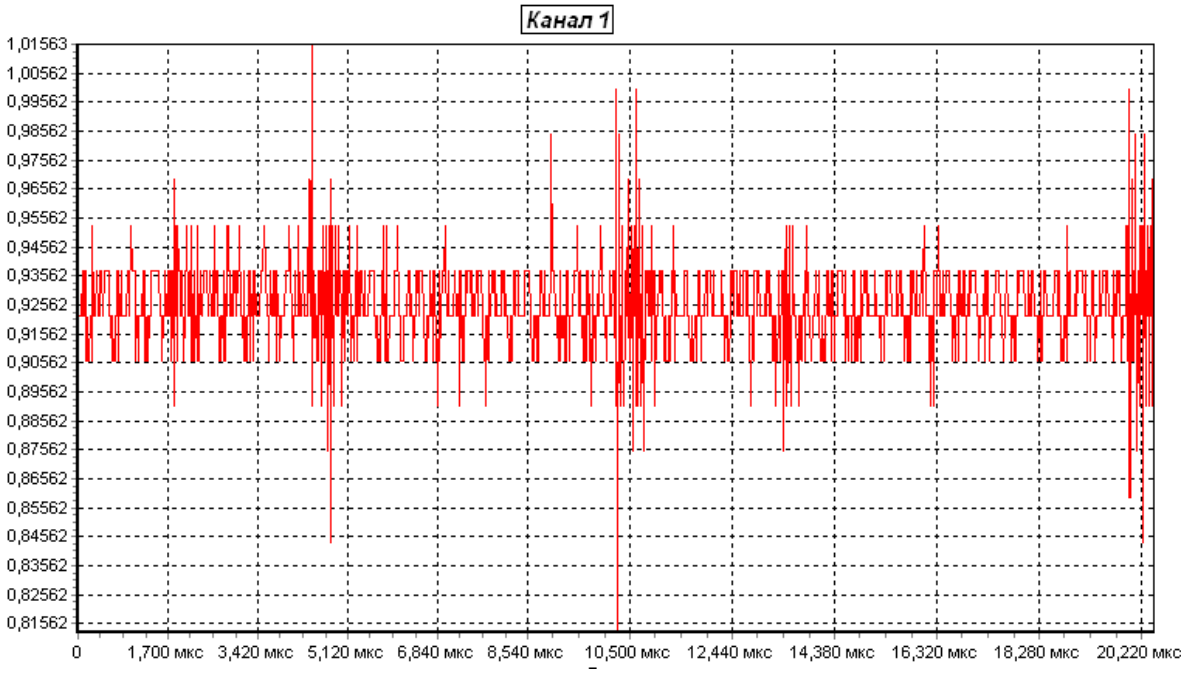



Рисунок 3.29 – Вид сигналу адресації на вимірювальному шунті

### 3.2.8. Енергоспоживання ПЗПД з трансивером XBee S2

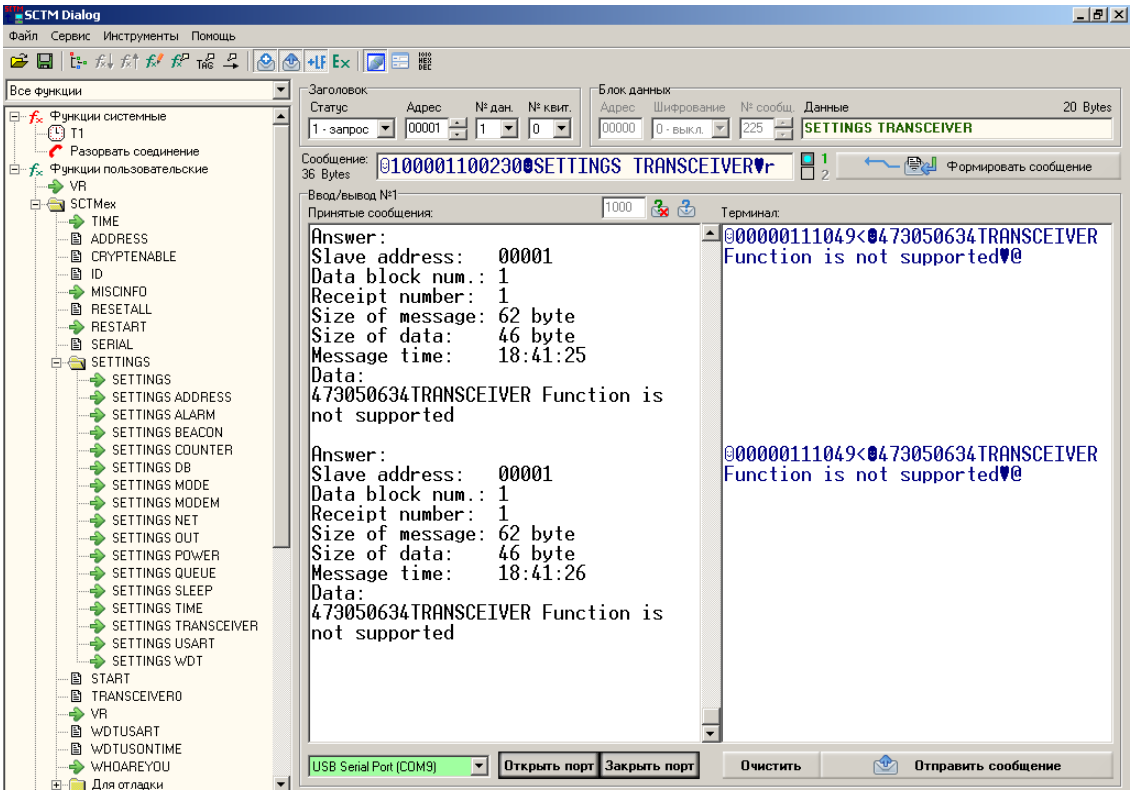



Рисунок 3.30 – Формат пакета активації трансивера

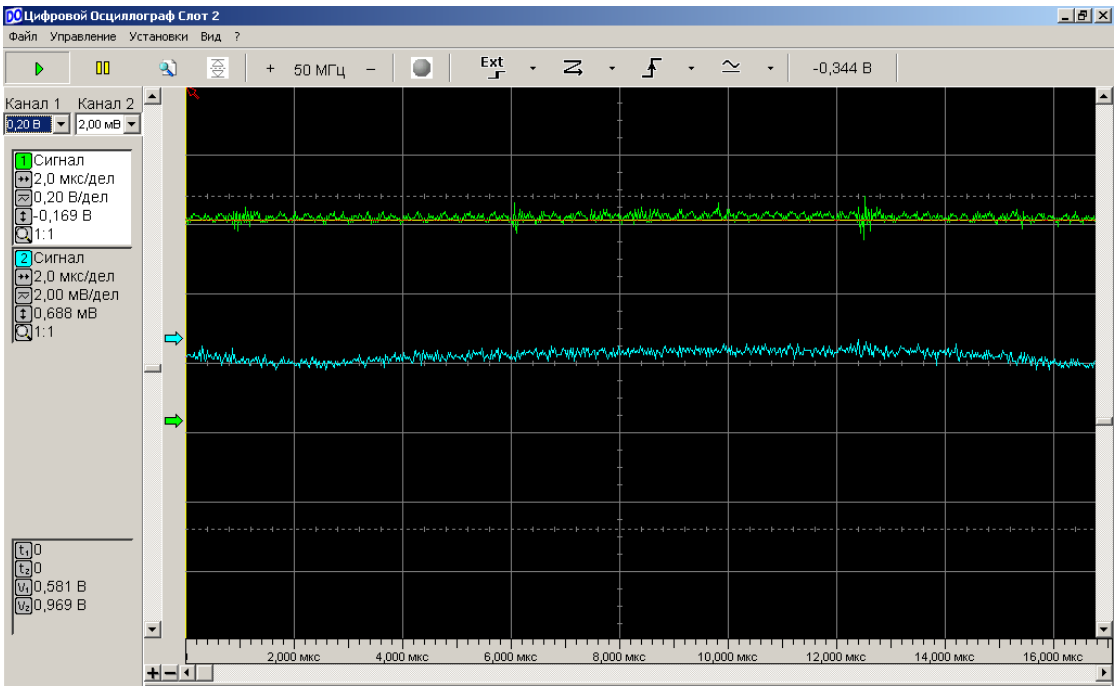



Рисунок 3.31 – Осцилограма пакета активації трансивера

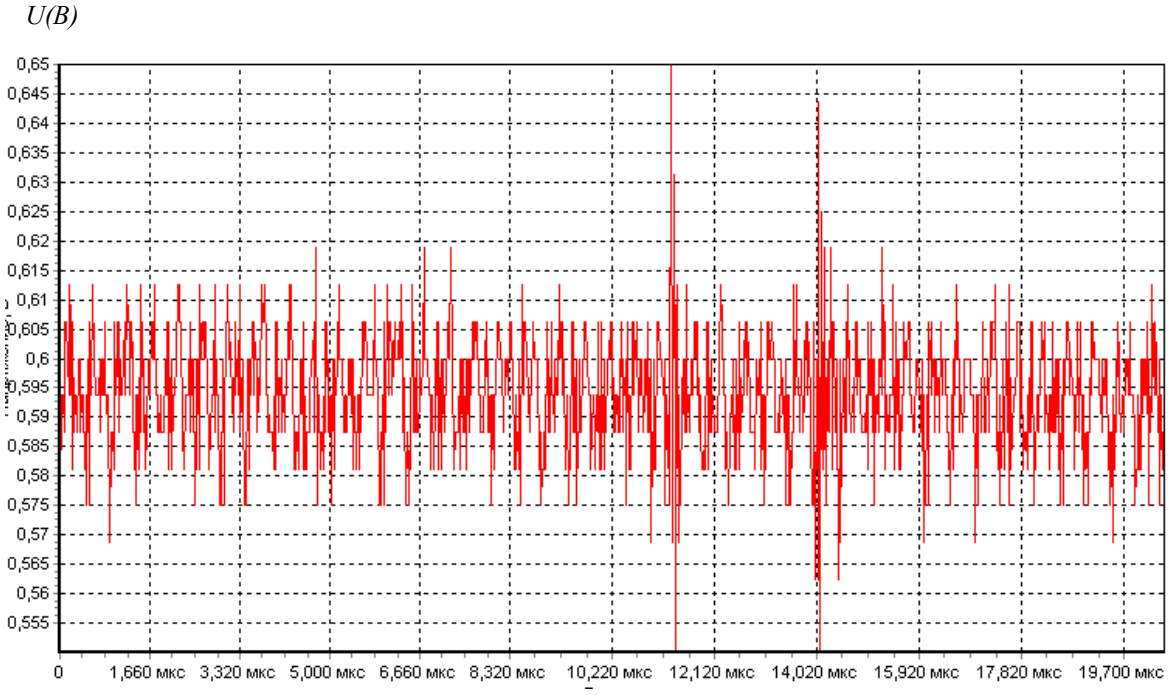



Рисунок 3.32 – Вид сигналу активації трансивера на вимірювальному шунті

### 3.2.9. Енергоспоживання ПЗПД з трансивером REX3D

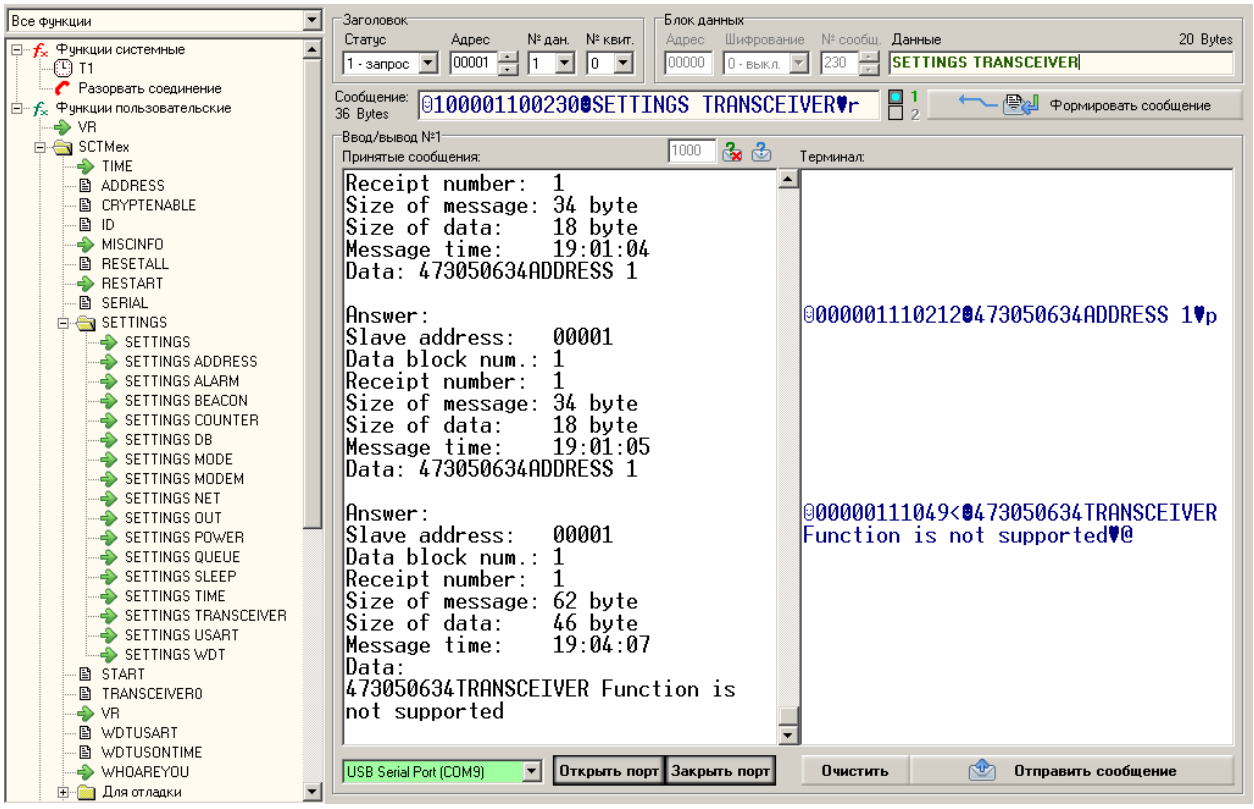



Рисунок 3.33 – Формат пакета активації трансивера

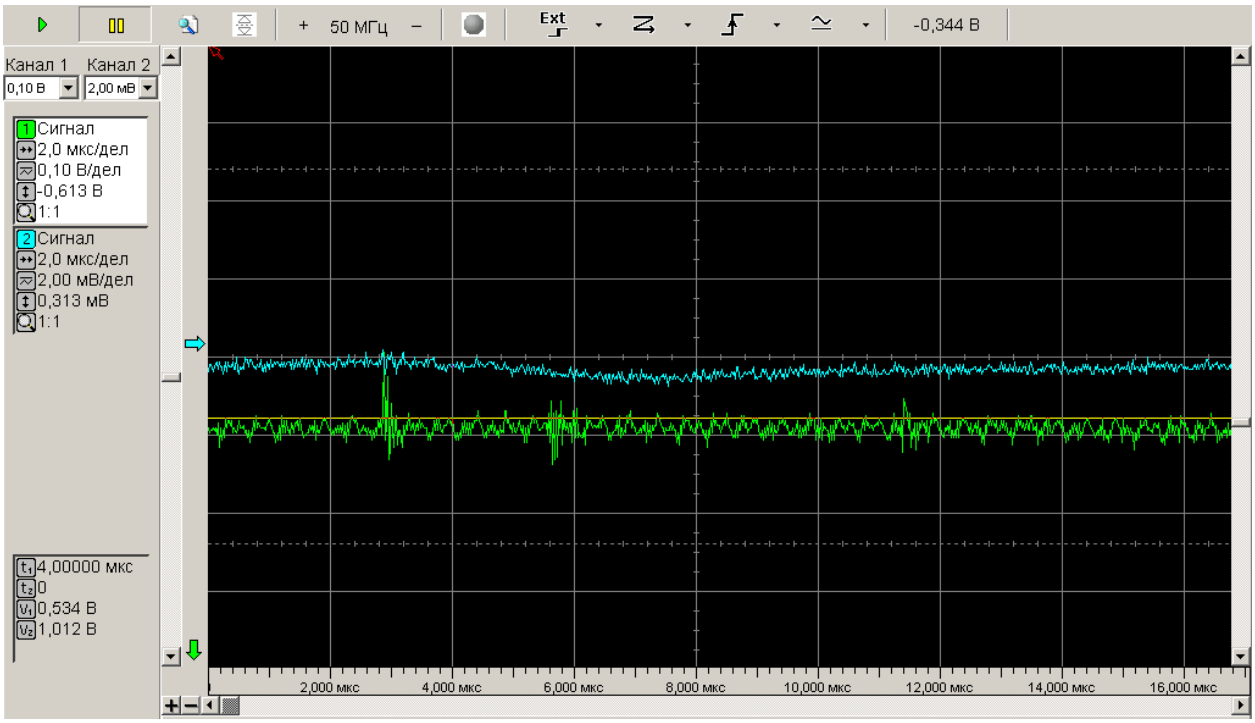



Рисунок 3.34 – Осцилограма пакета активації трансивера

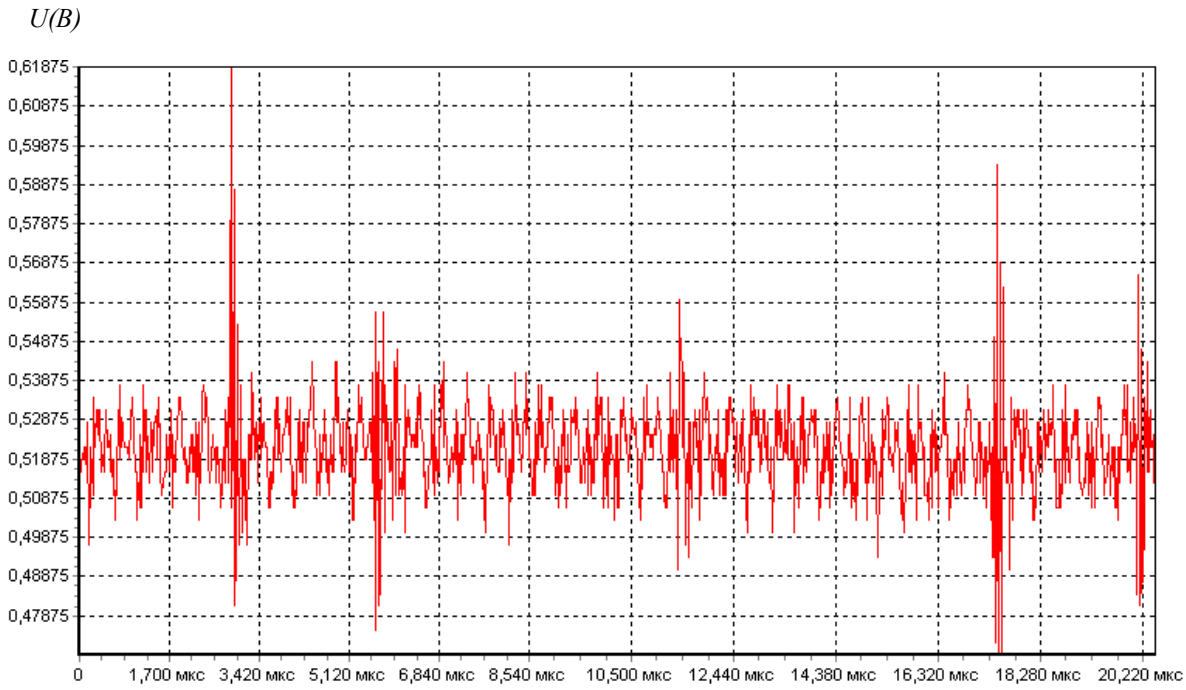



Рисунок 3.35 – Вид сигналу активації трансивера на вимірювальному шунті

Виходячи з виміряних значень ефективного значення стандартного відхилення і опору резистора визначено ефективне значення середнього струму споживання пристроїв «Сигма-ZB» в режимі адресації мережі і розмірі пакета 62 байта.

Таблиця 3.4 – Експериментальні значення в режимі адресації мережі і розмірі пакету 62 байта

| Тип модуля | Потужність, мВт | Стандартне відхилення, мВ | Середнє значення ефективного струму, мА |
|---|---|---|---|
| XBee rev.b | 1,0 | 3,44 | 5,68 |
| XBee S2 | 4.0 | 33,89 | 55,92 |
| REX3D | 6,0 | 20,66 | 34,09 |

Виходячи з експериментальних даних, наведених в таблицях 3.1, 3.2, 3.3, 3.4, можна зробити важливий висновок: енергоспоживання польового пристрою залежить не стільки від потужності прийомо-передавача, але визначається взаємодією трансивера з керуючим мікроконтролером,

встановленим в польовому пристрої для виконання призначених для користувача функцій. Іншими словами, енергоспоживання визначається верхнім рівнем додатків стека протоколу ZigBee, і є критично залежним від фізичного і канального рівня протоколу 802.15.4.

Подальший розвиток системи шляхом інтеграції існуючого рішення в блокчейн з урахуванням викладених вище вимог передбачає модернізацію програмної і апаратної частини [19, 32, 46-48]. У міру розвитку технології перспективним рішенням є RadixDLT [108], оскільки це рішення позбавлене недоліків IOTA в частині громіздкого механізму реалізації «смарт контрактів» і не таке вимогливе до апаратних ресурсів як IBM Hyperledger [67]. У частині апаратних рішень найбільш імовірним є заміна ПЗПД «Сигма RF» на більш продуктивні «легкі» ноди на малопотужних пристроях, наприклад Raspberry Pi. На стороні сервера може використовуватися Raspberry Pi 3, що керує майстер-нодою на основі Radix. Дана імплементація відрізняється від оригінальної тим що, що не передбачає встановлення центрального сервера системи, а її синхронізація здійснюється майстер-нодами, що розосереджені територіально. Додатково підтримка мережі TOR забезпечить кращу синхронізацію і підвищену загальну продуктивність.

### 3.3. Моделювання мережі енергомоніторингу

Комп’ютерне моделювання мереж відіграє важливу роль. Для швидкої і якісної побудови мережі, розрахунку складових елементів використовуються різні пакети моделювання.

Затримка пакетів є важливою характеристикою мережі, вона визначається як затримка між моментом надходження пакету на вхід якого-небудь мережевого пристрою або частини мережі і моментом появи його на виході цього пристрою. Цей параметр характеризує мережеві етапи обробки даних. Згідно [110], в глобальних мережах затримка розподілена за експоненціальним законом. При моделюванні мережі необхідно найбільш точно відтворювати всі

її характеристики, тому розподіл затримки пакетів в моделі повинно збігатися з розподілом затримки в реальній мережі. Тому нами застосована версія платформи XCTU 6.3.5 для XBee / RF рішень від DIGI Int. Дана платформа дозволяє не тільки виконати всі настройки модуля (рис.3.36), провести сканування мережі будь-якої конфігурації, але і виконати тестування мережі з виміром конкретних рівнів сигналу і затримок, що виникають (рис.3.37-3.38).

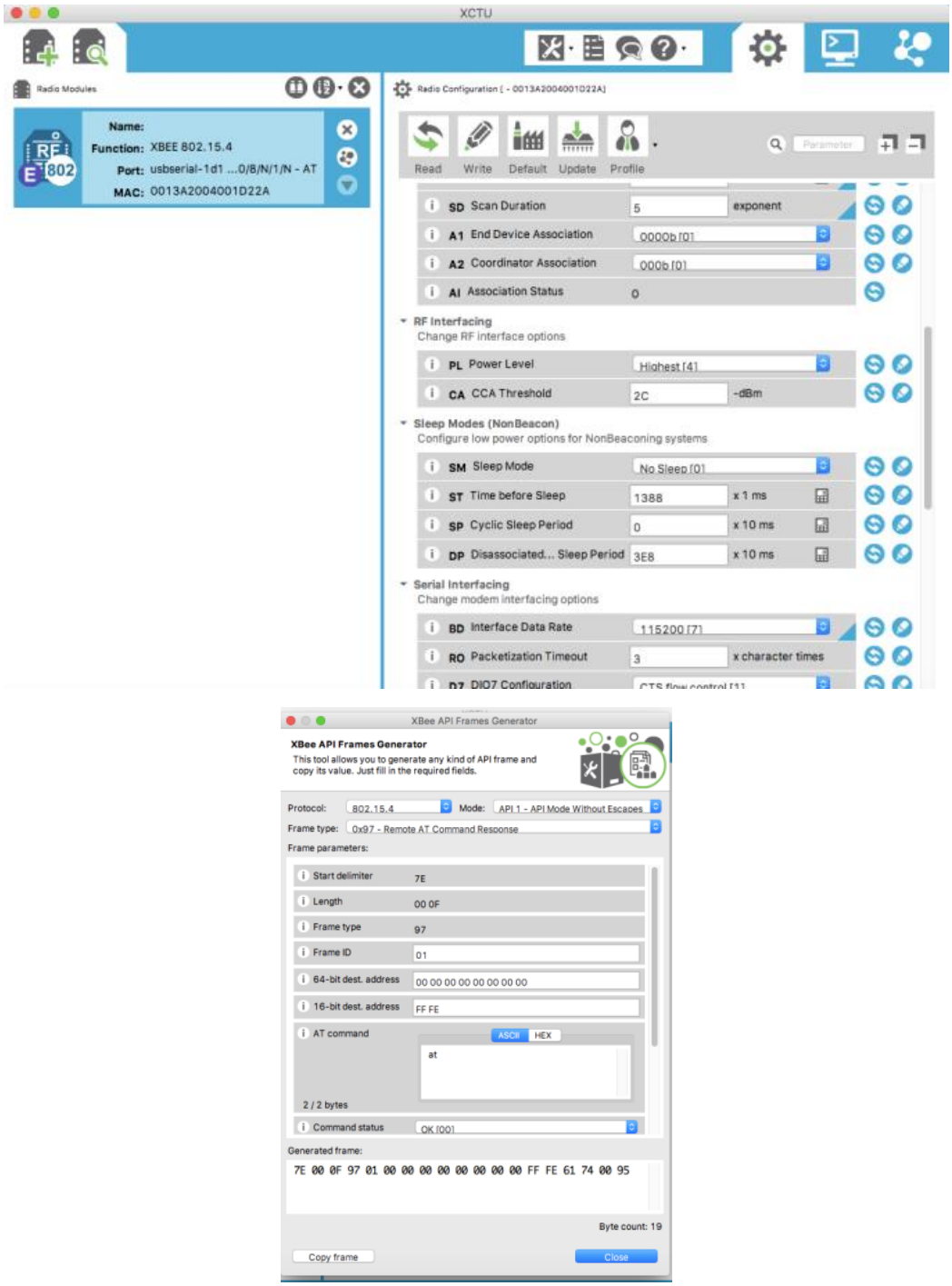



Рисунок 3.36 – Інтерфейс програми XCTU 6.3.5

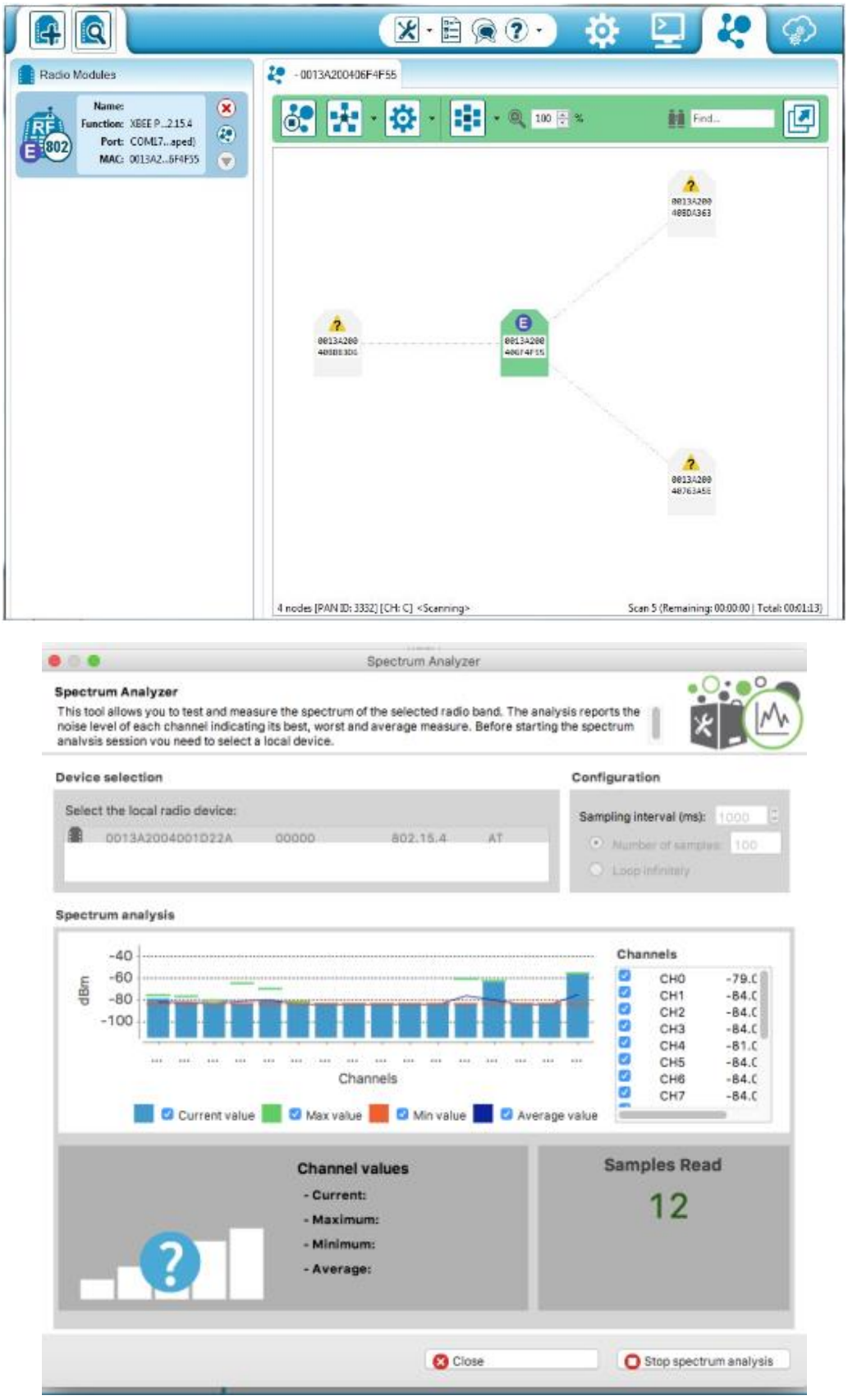



Рисунок 3.37 – Сканування мережі

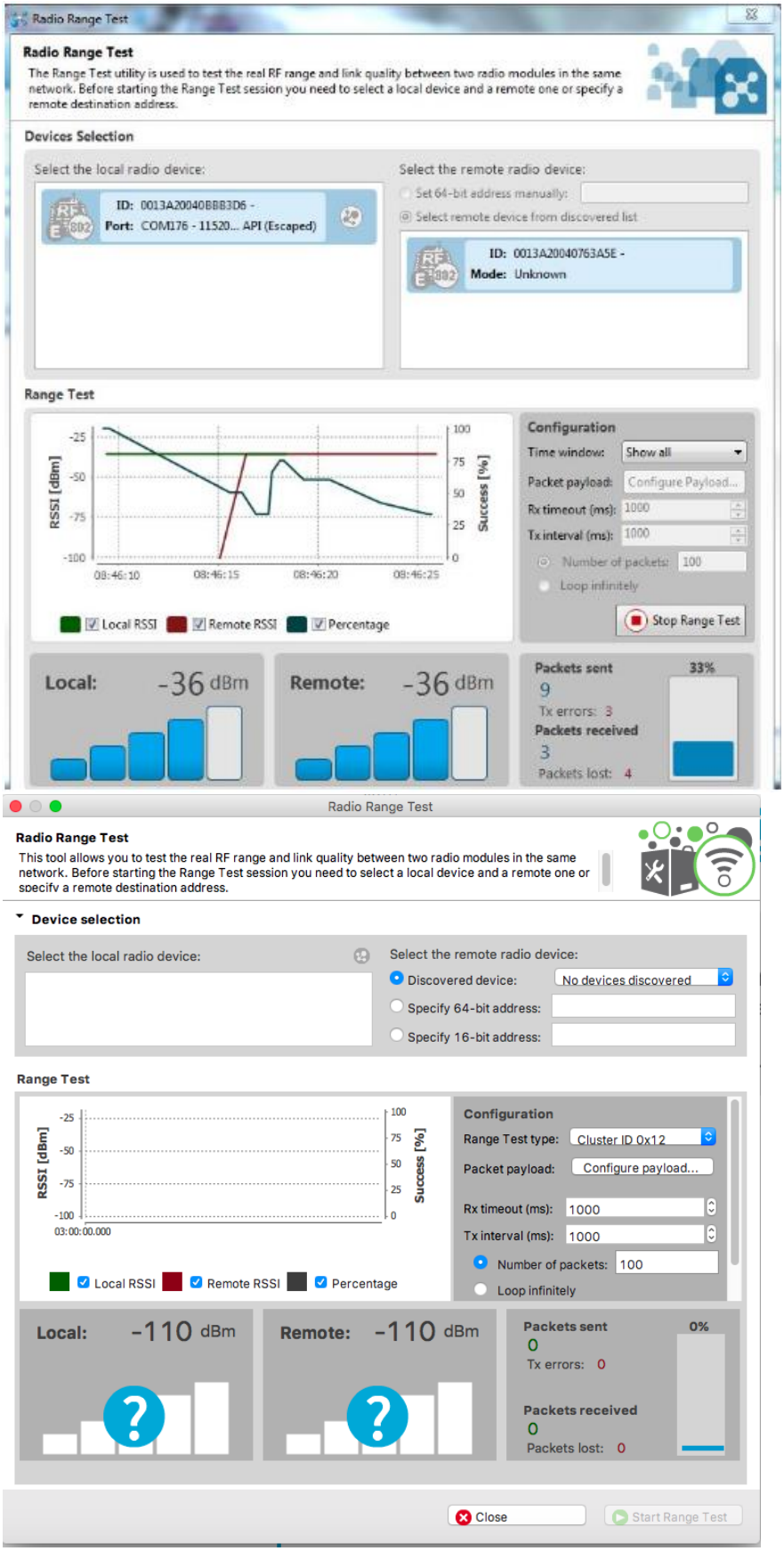



Рисунок 3.38 – Результат тестування

Для валідації розробленої моделі в якості об’єкту обрано під’їзд типового 9-ти поверхового житлового будинку. Максимальна затримка для цих умов оцінюється виходячи з цих початкових умов в такий спосіб:

1. Максимальна відстань від координатора до віддаленого вузла - 12 ретрансляцій (хопів), мінімальне - 1 хоп.

2. Час передачі пакета між двома вузлами ≈ 0,03 с.

3. Число ретрансляцій на рівні 802.15.4 - 3 (фіксована величина).

Максимальний час передачі повідомлення між сусідніми вузлами становить ≈ 0,09 сек., стільки ж буде потрібно для підтвердження на рівні додатку. Таким чином, в маршруті з 12 ретрансляцій максимальна затримка передачі одного повідомлення складе 12 × 0,09 × 2 = 2,16 секунд на відправку одного повідомлення. При відсутності зв’язку додаток повторює відправку максимум 3 рази, для підтвердження або фіксування недоступності вузла одержувача, що займає приблизно 7 секунд. При одній ретрансляції максимальний час ідентифікації вузла становить 0,54 секунди. Отже, середній час повної ідентифікації системи, що складається з 36 вузлів, становить 118,26 сек. або приблизно 2 хвилини.

Успішність формування мережі перевіряється програмою XCTU, в якій через віддалену конфігурацію відкривається вікно, в якому відображаються всі вузли MESH-мережі. З огляду на пакетний режим передачі даних в системі, приймемо середній розмір переданого пакета 120 байт. З огляду на те, що повний розмір добового пакета даних ПЗПД в форматі протоколу SCTMex становить 837 байт, для його передачі необхідно 7 сеансів зв’язку з вузлом. Таким чином, з урахуванням ймовірності передачі інформаційного пакету, що дорівнює 0,42, розрахунковий максимальний час тривалості сеансу зв’язку в системі, що моделюється, з 36 ПЗПД становить приблизно 6 хв.

Само по собі це значення не критично і залежить від додатку, який використовує MESH-мережу для передачі даних. При зміні обсягу переданих даних ця величина може варіюватися.


Рисунок 3.39 – Відображення мережі в програмі XCTU

Для системи енергомоніторингу, в якій пакети даних передаються всередині мережі один раз на годину, затримки в 7 секунд не є критичними. У той же час, саме затримки при ретрансляції пакету є головним обмежувачем при побудові масштабних ZigBee- мереж. Саме з цих міркувань в специфікації DIGI MESH максимальна глибина ZigBee-мережі обмежена 15 ретрансляціями і 500+ пристроями.

У модулях XBee S2 максимальний час очікування відповідей для команд ND (пошук вузлів) і DN (прокладка маршруту) не може перевищувати 25 секунд (параметр NT). Хоча при використанні модулів XBee S2 глибина мережі формально не обмежена, однак число ретрансляцій при розсилці широкомовних повідомлень не може бути більше 15. Це означає, що

конкретний вузол просто не зможе виявити інші вузли, розташовані на відстані більше 15 хопів від нього.

Експериментально було визначено оптимальний розмір мереж з MESH-топологією виходячи з доцільності застосування автономних джерел живлення ємністю 2800 мА·г. Для режиму роботи з побудовою мережі в 20 ПЗПД, час активного режиму становить близько 3 хвилин, а при 40 ПЗПД – 6 хвилин. Цей алгоритм роботи з щоденним режимом передачі даних забезпечить безперебійну роботу обладнання протягом понад 4 роки, що відповідає міжповірочному інтервалу більшості лічильників, які використовуються в якості датчиків системи, що розробляється.

### 3.4. Інформаційна безпека бездротових систем моніторингу

З огляду на архітектурні особливості, БСС мають обмежені обчислювальні можливості, малу ємність пам’яті, низьку пропускну здатність, обмежені енергоресурси і малі розміри апаратних засобів, що накладає жорсткі обмеження на методи забезпечення безпеки в мережах і роблять застосування деяких з них неможливим [77-79]. Основні обмеження в БСС, що накладаються на засоби захисту інформації, можна класифікувати наступним чином:

1. Обмеженість ресурсів:
    - Обмеженість обчислювальних ресурсів;
    - Обмеженість енергетичних ресурсів.
2. Ненадійність зв’язку
    - Ненадійна передача
    - Конфлікти
    - Затримки
3. Непередбачені випадки

Розглянемо більш детально. Будучи мініатюрними ЕОМ, сенсори оснащені процесором, модулем оперативної пам’яті, урізаною операційною системою з мінімальним набором інструкцій і дуже невеликою доступною

вільною пам’яттю, тому алгоритми забезпечення безпеки не можуть вимагати від сенсорів виконання обчислювально складних і витратних по пам’яті операцій без ризику перешкоджання виконанню основної конструктивної задачі – збору та передачі даних.

*Обмеженість енергетичних ресурсів.* Енергія в сенсорах витрачається на три основних компоненти: модуль датчика, трансивер і мікропроцесор. Складні алгоритми додатково завантажують процесор, при виконанні безлічі обчислень, і модуль зв'язку, при необхідності інтенсивного обміну даними. При цьому мікропроцесор виконує близько 800-1000 операцій в секунду, але енергетичні витрати на передачу даних набагато більше в порівнянні з її обробкою в ЦП. Практика застосування сенсорів передбачає їх установку і використання на протязі довгих часових проміжків зі збільшеним періодом заміни батареї, тому методи забезпечення безпеки, що помітно скорочують цей період, непрактичні.

*Ненадійна передача.* БСС - велика кількість пов'язаних в мережу сенсорів, де передача даних найчастіше відбувається у вигляді мережевих пакетів від одного сенсора до іншого. З огляду на природи бездротової комунікації та структури мережі, пакети можуть бути або пошкоджені через помилки і перешкод в каналі передачі, або відкинуті надмірно завантаженими вузлами. У мережі, побудованої без застосування протоколів виявлення і виправлення таких помилок, зростають ризики втратити критично важливі пакети, що містять особливо цінну інформацію про середовище або інформацію, необхідну для здійснення процедур безпеки, наприклад, криптографічні ключі.

*Конфлікти.* У мережах з високою кількістю сенсорів на одиницю площі можуть виникати конфлікти бездротового зв’язку, що призводять до неповної передачі пакета або її припинення, що ускладнює застосування методів забезпечення безпеки, покладаються на стабільність зв'язку та повноту даних, що передаються.

*Затримки.* Найчастіше через особливості розгортання БСС неможливо побудувати таку архітектуру мережі, де була б можлива глобальна адресація одного вузла іншим. Більш того, в таких мережах, як правило, передбачається

потік інформації через кілька вузлів до одного загального вузла збору даних. Все це призводить до спеціального проектування топології мережі, де мають значення розташування вузлів в просторі і їх зв'язки один з одним.

Топологічні особливості, такі як різна віддаленість від вузла збору інформації, непередбачені виходи з ладу окремих вузлів, різна завантаженість, неминуче призводять до пересилання пакетів, перебудові маршрутів їх передачі та затримки в доставці. Робота деяких систем захисту в таких умовах може виявитися нестійкою і неефективною.

*Непередбачені ситуації.* БСС безпосередньо взаємодіють з навколишнім їх середовищем, тому вони часто застосовуються в відкритих, великомасштабних просторах, де неможливо контролювати будь-які незначні зміни. Звідси випливає ряд проблем, пов’язаних з фізичною цілісністю сенсорів як пристроїв, серед яких випадковий вихід з ладу, фізичний збиток, різка зміна умов середовища і ін. Отримання надійних даних в складних умовах від фізично віддалених сенсорів до кінцевого користувача буває саме по собі непростим завданням.

Забезпечення інформаційної безпеки в БСС через поставлені обмеження має ряд особливостей:

1) Складні криптографічні протоколи є ресурсовитратними і погано підходять для концепції малопотужних пристроїв без постійного джерела живлення.

2) Ресурсоємні надбудовані протоколи також привносять додаткове навантаження і впливають на передачу інформації між пристроями.

3) Процес забезпечення інформаційної безпеки мережі безпосередньо залежить від кваліфікації адміністратора. Більш того, в деяких випадках при великій кількості пристроїв в мережі практично неможливо забезпечити необхідний рівень безпеки вбудованими засобами.

4) Непристосованість пристроїв до агресивного зовнішнього середовища.

Як показує історія розвитку бездротових технологій і тенденції на ринку – всі рішення в області БСМ рухаються в напрямку IP-складових рішень. Інтернет стає масовою сукупністю стандартів і протоколів розвитку локальних мереж. При цьому бездротові технології будуть займати більше 80% ринку. У тому зв'язку питання безпеки мереж безпосередньо пов'язані з часом їх життя [1, 2, 7].

Як було зазначено вище, не дивлячись на те, що енергоспоживання визначається верхнім рівнем додатків стека протоколу ZigBee, і є критично залежним від фізичного і канального рівня протоколу 802.15.4, саме управління розмірами повідомлень є основним резервом збільшення терміну життя пристроїв і системи в цілому. Розвиток технологій бездротових мереж збору та передачі даних, зниження енергоспоживання і мініатюризація сенсорних датчиків і необхідність встановлення зворотного зв'язку з контрольованими об'єктами породили нову парадигму еволюції стандартних AMR / AMI / AMM рішень в область «інтернету речей» (Internet of Things, IoT). Це призвело до переосмислення стандартних підходів до технологічних рішень, програмного забезпечення, енергоспоживанню, безпеки [43].

Централізація збору даних про енергоспоживання і необхідність особистого контролю за витратами сприяють поширенню рішень HAN (home area network) або PWAN (Low-power Wide-area Network – «енергоефективна мережу далекого радіусу дії). З точки зору безпеки, «інтернет речей» схильний до нового типу загроз, яким піддаються самі пристрої, їх апаратні платформи, інформаційні системи і системи зв’язку, а також самі системи, до яких підключені пристрої IoT. Захист БСМ є актуальною проблемою, оскільки вузли мережі мають невелику обчислювальну потужність, обмежений заряд батареї, розташовуються в незахищених місцях, а інформація передається по бездротових каналах. Будь-яке порушення роботи мережі може призвести до небажаних наслідків.

На сьогоднішній день для статичних БСМ розроблено велику кількість методів захисту та систем виявлення вторгнень. Виходячи з викладеного вище,

сформульована задача і основна вимога до розроблюваних пристроїв IoT, що полягає в можливості поновлення апаратного і програмного забезпечення в період життєвого циклу системи без порушення її цілісності. Ця вимога піддається реалізації для дворівневих систем IoT, що складаються з взаємодіючих вузлів-роутерів і шлюзу-координатора мережі. Подібна архітектура вказує на основну відмінність горизонтальних систем, побудованих за топологією «сітки» або «зірки», від структурованих ієрархічних систем попереднього покоління, побудованих на «шині».

### 3.4.1. Типи можливих атак на БСМ

В даний час існує велика кількість можливих атак на БСМ, більшість з яких спрямовані на виведення з ладу вузлів мережі, на дезорієнтацію протоколів маршрутизації, а також збій роботи мережі в цілому. Огляд публікацій, присвячених безпеці розподілених систем управління, показав, що в них недостатня увага приділяється питанням захисту та безпеки бездротових мереж моніторингу. Для того щоб вжити заходів для захисту розгорнутої мережі необхідно провести оцінку основних видів загроз безпеки: конфіденційності, цілісності та доступності. Загрози конфіденційності на рівні передачі комерційної та технологічної інформації можуть принести серйозної шкоди. Формування неправдивих команд локальної автоматики, в загальному випадку, може привести до аварійної ситуації, так як віддалене управління в більшості випадків зводиться тільки до зміни налаштувань, що призводить до неоптимального режиму роботи обладнання.

Найбільш вірогідними є загрози трафіку, що полягають у введенні шкідливої зайвої інформації в мережу, поява «лавини» повідомлень. Даний вид погроз може привести до збільшення затримок при передачі даних або до втрат пакетів, що призведе до недостовірної оцінки стану об’єкта і, відповідно, призведе до можливості прийняття катастрофічних рішень.

Втрата пакетів від кінцевих вузлів досягається зловмисником двома основними способами:

- введення сенсора SD рівня кінцевих вузлів, який проводить DDoS-атаку;

- введення сенсора SM рівня маршрутизаторів, який порушує роботу механізму маршрутизації.

Введення в систему зловмисником вузла SD призводить до збільшення навантаження на маршрутизатор і нездатності виконувати задані функції. Поява вузла SM призводить до втрати даних кінцевих сенсорів, підключених до даного маршрутизатора. Одним з ефективних способів боротьби з даними видами атак є використання шифрування даних на різних рівнях і механізмів аутентифікації. При цьому необхідно враховувати обмеження, пов’язані з невеликими обчислювальними ресурсами вузлів і невеликим об’ємом пам’яті. Це не дозволяє використовувати асиметричні алгоритми шифрування. Симетричні алгоритми шифрування володіють такими перевагами, як низькі вимоги до продуктивності вузлів і енергоспоживання, але вони мають низьку захищеність, пов’язану з тим, що, дізнавшись ключ, зловмисник може отримати доступ до всіх вузлів мережі.

Зростання кількості пристроїв малої обчислювальної потужності, що підключаються через Інтернет, викликало значне зростання інцидентів кібербезпеки, зумовленими нової вразливістю пристроїв, що не існувала раніше. Щоб належним чином забезпечити безпеку системи моніторингу, необхідно враховувати забезпечення безпеки окремих пристроїв, зв’язку між пристроями, мережею і всіма цими системами з плином часу. Захист польових пристроїв має пріоритетний характер, так як уразливі саме вони, а не встановлені на них додатки. Цим покладено новий етап в індустрії захисту інформації – захист мереж збору даних інтелектуальних датчиків і пристроїв обліку енергоресурсів, що володіють обмеженими обчислювальними ресурсами.

Основні моделі інтелектуальних лічильників, присутніх на ринку, не підтримують жодних алгоритмів шифрування, що робить їх уразливими до хакерських атак. Несанкціоноване віддалене зчитування даних з лічильників може використовуватися в кримінальних цілях з метою доступу до

конфіденційної інформації. Вбудовування засобів забезпечення безпеки в самі об'єкти поки обмежене з технологічних причин. Саме критична уразливість польового пристрою вказала на необхідні заходи щодо зміни не тільки методологічного підходу до інформаційного захисту бездротових мереж, але і до зміни їх архітектури та алгоритму роботи. Основна вимога полягає в тому, що кібербезпека повинна враховуватися вже на стадії проектування системи. Кращим способом отримання впевненості в тому, що інтелектуальна мережа захищена належним чином, є розробка єдиних вимог в частині кібернетичної безпеки для всіх пристроїв.

### 3.4.2. Види вразливостей БСМ

В останні роки в багатьох країнах світу в житлових будинках впроваджують так звані інтелектуальні лічильники. Вони відрізняються від традиційних лічильників розширеними можливостями, дозволяють вести облік часу споживання ресурсів, а також оснащуються комунікаційними засобами для автоматичної передачі показників. Як і будь-які бездротові електронні пристрої, інтелектуальні лічильники електроенергії, а разом з ними і самі «розумні» електромережі уразливі для хакерів. Після того, як зловмисник отримав доступ до кодів, він може підключатися до лічильника і віддавати йому команди, причому цим командам будуть підкорятися всі лічильники певної марки в межах мережі. Дослідниками з Університету Південної Кароліни та Rutgers University, було встановлено, що в поширених інтелектуальних лічильниках досить легко провести реверс-інжиніринг комунікаційних протоколів, використовуваних в AMR, а також атаки типу «маскарад» (spoofing). Зловмисники можуть віддалено контролювати, чи є хто в квартирі, шляхом знімання інформації про рівень енергоспоживання лічильника. Також можлива атака, яка веде до розряду акумулятора лічильника. При отриманні сигналу активації він відразу ж передає пакет, тому при безперервному подаванні безлічі таких сигналів лічильник може швидко розрядитися. Атаки типу «маскарад» призводять до втрати цілісності даних і їх

спотворення. Як виявилося, в системах інтелектуального обліку не передбачена аутентифікація. Крім того, перевірка на вході також відсутня. При отриманні кількох пакетів з однаковим ID і різними показниками лічильника, зчитувач приймає пакет з найсильнішим сигналом. При використанні більш сучасної моделі зчитувача, який виробляє таку перевірку, існує можливість простого блокування пакетів з легітимного лічильника і перенаправлення зчитувача на прийом пакетів з підставного пристрою.

Одним з можливих рішень захисту інтелектуальних лічильників є Smartsynch Universal Communications Model – модель інтелектуального лічильника в збірці, що дозволяє замінювати застарілі контролери на нові, що підтримують аутентифікацію і шифрування, без необхідності видалення з мережі лічильника. Для бездротових мереж основні цілі безпеки залишаються такими ж, як і для провідних мереж: збереження конфіденційності, гарантія недоторканності і забезпечення доступності інформації. Таким чином, визначення ризиків для конфіденційності сенсорних мереж являє собою ступінь доступності даних, що передаються, які представляють найвищу цінність. За ступенем важливості способи, за допомогою яких зловмисник може скомпрометувати конфіденційність даних, виділяються атаки, за допомогою яких визначається несуча частота, розмір повідомлення, рівень сигналу і відомості про маршрутизації інформації. При вивченні схеми проходження трафіку сенсорної мережі можна простежити розташування базової станції або іншого стратегічно розташованого вузла.

Більшість бездротових атак підпадають під одну з наступних категорій [54]:

- Атаки на конфіденційність: ці атаки намагаються перехопити секретну інформацію, що надсилається засобами бездротової передачі.
- Атаки на недоторканність: дані атаки посилають фрейми (структурні одиниці інформації) помилкового контролю, управління або містять дані для виникнення збою на одержувача, або використовуються для полегшення проведення іншого типу атак.

- Атаки на доступність: ці атаки перешкоджають доставці бездротових повідомлень для легалізації користувачів за допомогою виводу з ладу мережевих ресурсів.

Природа організації зв’язку в бездротовій мережі відкриває шляхи для чотирьох основних атак: перехоплення, зміна, руйнування і ін’єкція коду або пакета. Більшість атак мережевого рівня проти таких мереж підпадають під одну з цих категорій.

**Повторне відтворення даних.** Атака повторного відтворення – це форма мережевої атаки, при якій передача валідних даних навмисно або шляхом обману повторюється. Оскільки зловмисник може прослухати будь-яке повідомлення, передане за допомогою мережі, він може вставити «нові» повідомлення або маніпулювати будь-яким повідомленням, що відправлене уповноваженим відправником мережі.

**Атака воронки.** Атака воронки перешкоджає базовій станції отримувати повні та коректні дані з сенсорів, таким чином створюючи серйозну загрозу додатків високого рівня. Зазвичай атаки воронки проводяться зі створенням шкідливого вузла, спеціально спрямованого для найближчих вузлів згідно з алгоритмом маршрутизації.

**Вибіркове пересилання.** При атаці вибіркового пересилання зловмисник може перенаправляти певні повідомлення і просто залишати їх, перебуваючи в упевненості, що вони не будуть далі поширюватися.

**Флудинг.** В атаці флуда зловмисник має на меті порушення основного дерева маршрутизації.

**Ін'єкція шкідливого коду.** Використовуючи переваги вразливостей щодо пам’яті на сенсорних вузлах, такі як переповнення буфера, зловмисник може відправити спеціально створені пакети, щоб здійснити переповнення стека і запустити на виконання довільний код на цільовій системі.

**Пінгування** – визначення того, чи знаходиться вузол в даний момент на зв’язку і поширення програмного образу. Поширення програмного способу – це базисний сервіс в сенсорних мережах, за допомогою якого здійснюється

передача оновлень образів. Однак це призводить до загроз, оскільки зловмисник може легко зруйнувати його за допомогою модифікації або заміни справжнього образу коду, який поширюється на сенсорні вузли.

Наведені вище уразливості вимагають особливого підходу до проектування бездротової мережі енергомоніторингу. Бажано, щоб польовий вузол системи підтримував процедури аутентифікації, кодування і не підтримував можливість здійснення флудингу і пінгування зовнішніми пристроями.

### 3.4.3. Модель захисту БСМ

Посилення інтенсивності кібератак, здійснених в останні роки на об’єкти інфраструктури веде до необхідності розробки нових підходів до реалізації політики кібернетичної безпеки. Комплексна система захисту інформації зазвичай будується з урахуванням чотирьох рівнів інформаційної системи:

1. Рівень прикладного програмного забезпечення (ПЗ), що відповідає за взаємодію з користувачем.

2. Рівень системи управління базами даних (СУБД), що відповідає за зберігання і обробку даних інформаційної системи.

3. Рівень операційної системи (ОС), що відповідає за обслуговування СУБД і прикладного програмного забезпечення.

4. Рівень мережі відповідає за взаємодію вузлів інформаційної системи.

Найбільш прогресивним в даний час є підхід, запропонований XSeed Capital. Цей похід заснований на дворівневому аналізі: перший рівень фіксує можливість, надану технологією безпеки, в той час як другий оцінює зв’язок рішення з шаром IT стека, на якому розгорнута технологія. Аналіз безпеки проводиться за трьома основними критеріями:

1. Профілактика – здатність рішення системи захисту на виявлення можливих атак і їх блокування.
2. Виявлення уразливості системи захисту, спрямоване на скорочення часу виявлення і фіксації атаки, а також на збільшення часу

ексфільтрації (час, необхідний зловмиснику для крадіжки конфіденційних даних).

3. Ретроспектива – можливості оперативного усунення можливих інцидентів, обумовлених виявленими уразливими.

З огляду на обмеженість ресурсів польового пристрою і цінові обмеження для БСМ, виправданим рішенням є зміна загальноприйнятого алгоритму роботи ПЗПД, що полягає в перешкоджанні прозорого доступу зловмисника до польового пристрою.

Розроблений алгоритм передбачає два етапи формування мережі – побудова мережі і прийом/передача даних. Етап побудови мережі полягає в побудові мережі координатором за розкладом, після чого координатор починає виконувати роль шлюзу між комірчастою мережею і зовнішнім додатком. При цьому ініціатором обміну даними стають польові пристрої, які надсилають запити координатору. Аналогічно координатор-шлюз відправляє запит серверу додатків. При виявленні команди для виконання вона передається відповідному польовому пристрою, адреса якого міститься в даній команді. Таким чином реалізується механізм, в якому ініціатором завжди виступає польовий пристрій відповідно до налаштувань, встановлених при інсталяції обладнання. Цим вирішується питання авторизації пристроїв як в локальній бездротовій мережі моніторингу, так і в інтернет просторі. Подібний алгоритм роботи системи істотно підвищує її стійкість до можливих DDoS атак, атак типу воронки, вибіркового пересилання і т.д. Всі ці моменти сприяють збільшенню терміну життя системи в цілому, оскільки здійснюється блокування несанкціонованого втручання в роботу системи на рівні польових пристроїв.

## 3.5. Обґрунтування застосування технології блокчейн для модернізації бездротових мереж моніторингу

Вночі 18 грудня 2016 р. в енергосистемі Київської області сталося раптове відключення споживачів правобережжя Києва і прилеглих районів.

Оперативний персонал «Укренерго», з огляду на досвід аналогічної аварії в Прикарпаття-обленерго, перевели обладнання в ручний режим управління і за годину п’ятнадцять хвилин відновили живлення в повному обсязі. Українська компанія ISSP, яка розслідувала для «Укренерго» грудневий інцидент, вказує на взаємозв’язок між нападами. За твердженням компанії, хакерські напади на електропостачання 2015 і 2016 років взаємопов’язані, а також пов’язані з аналогічними нападами в грудні на інші об’єкти інфраструктури, в тому числі на "Укрзалізницю", ряд міністерств і Пенсійний фонд. Кібератаки в 2015 і 2016 роках мало відрізнялися одна від оіншої, використовувався інструментарій BlackEnergy2 – шахрайське програмне забезпечення, пристосоване для проведення APT-атак. Єдина різниця полягала в тому, що напад 2016 року був більш складним і краще організованим. Саме цей факт потрапляє під парадигму APT-атаки (advanced persistent threat – «розвинена стійка загроза»). Атака APT перевершує звичайні кіберзагрози, тому що орієнтується на злом конкретної цілі і готується на підставі інформації про неї, яка збирається протягом тривалого часу. APT здійснює злом цільової інфраструктури за допомогою експлуатації програмних вразливостей і методів «соціальної інженерії».

Без сумніву, ці суб’єкти дійсно є силою, з якою треба рахуватися, проте так звані інсайдери, зокрема діючі та колишні співробітники компанії, є найбільш часто згадуваними винуватцями кіберзлочинів. Це зовсім не означає, що всі співробітники демонструють зловмисну поведінку. У багатьох випадках вони можуть стати мимовільними винуватцями витоку інформації, втративши свої мобільні пристрої або ставши жертвою фішингу.

Виділяють 4 стадії цільової атаки (підготовка, проникнення, поширення, досягнення мети), кожна з яких супроводжується діяльністю, спрямованою на приховування слідів присутності в системі.

На стадії підготовки здійснюється виявлення слабких місць в системі безпеки, здійснюється розробка стратегії досягнення необхідного результату з використанням методів соціальної інженерії, підбираються засоби проникнення з раніше створених або створюються нові. Оскільки технічні засоби, що

використовуються для захисту інформаційної мережі організації, є конфіденційною інформацією, структуру інформаційної системи і її слабкості намагаються дізнатися будь-яким доступним методом, в тому числі і методами соціальної інженерії. Таким чином інсайдерська інформація і соціальна інженерія є найбільш дієвими прийомами на стадії підготовки до APT.

Проникнення в систему організації стає тривіальним процесом при якісно проведеному етапі підготовки. На цьому етапі використовуються уразливості нульового дня, а так само всі можливі техніки соціальної інженерії. Після посвідчення в проникненні на потрібний хост, зловмисник дає команду на інсталяцію шкідливого коду. Основним інструментом проникнення є експлойт (використовує уразливість Adobe PDF, Microsoft Office та ін.) і валідатор (програма для збору і перевірки інформації з зараженого хоста і передачі її в центр управління). Саме фішинг через вкладення в пошті, привів до інциденту в Прикарпаття-обленерго в 2015р.

В останні роки популярність флешок і інших знімних USB-накопичувачів, які використовують функції автозапуску для виконання шкідливих програм, значно зросла при виконанні цільових атак на системи підприємств.

На етапі поширення здійснюється максимальне поширення коду з інформаційної мережі, орієнтуючись на ключові точки – робочі станції і сервери, необхідні для здійснення цілей атаки. Зазвичай це здійснюється через віддалений доступ з використанням легітимних прав адміністратора системи підприємства. Після досягнення мети атаки слід приховування слідів і, при необхідності, залишення точок повернення в систему. Саме тому виявлення джерела кібератаки і її замовника є вкрай складним завданням. Тому основною проблемою ефективної протидії кіберзагрозам є ретельно спланована і розроблена політика інформаційної безпеки, і алгоритм її реалізації на підприємстві. Основним способом протистояння цільовим атакам є недопущення їх початку, оскільки активну атаку вкрай складно помітити.

Важливою частиною запобігання APT-атак є навчання персоналу правильній політиці інформаційної безпеки.

Успішна політика в області інформаційної безпеки організації, спрямована на мінімізацію ризику критичного пошкодження інфраструктури інформаційної мережі, повинна враховувати той факт, що цільові атаки йдуть пліч-о-пліч з соціальною інженерією. APT – це атаки, спрямовані проти конкретних організацій або державних відомств. Як правило, такі атаки не мають масового характеру і готуються досить тривалий період. Об'єктами атаки є дуже обмежені певними рамками або цілями конкретні інформаційні системи. Ефективність захисту від націлених атак не може визначатися тільки застосовуваними технічними засобами. Подібно будь-яким рішенням продукти із захисту від націлених атак мають як свої сильні сторони, так і слабкі. Надійність системи захисту інформації визначається можливістю оперативного реагування на таргінг атаки, моніторингом фактів компрометації і витоку інформації, сукупним аналізом інформаційної системи. Додаткову складність надають тривалість та інтенсивність атаки. Підготовка може займати місяці, а активна фаза – хвилини. Шкідливе програмне забезпечення спеціально розробляється для атаки, щоб штатні антивіруси і засоби захисту, які використовуються об'єктом і досить добре вивчені зловмисниками, не змогли виявити загрозу.

Технології захисту від націлених атак виходять на новий рівень. В першу чергу мова йде про різні інструменти для виявлення аномалій – як на локальних комп'ютерах, так і на рівні мережевої активності. Завданням таких систем є пошук всього незвичайного, що відбувається, а не пошук шкідливого року. Це дозволяє побачити схожі ознаки аномалій в різних сегментах інформаційної системи. До цих систем додається активно розвивається клас SIEM - «Security information and event management», що дозволяє агрегувати разом системні події, що надходять від різних систем захисту, і бачити в реальному часі всі зміни, що відбуваються. Всі нові технології передбачають аналіз поведінки. У цьому випадку помилки 1-го (false positives) і 2-го роду (false negatives)

неминучі, тому ефективність сильно залежить від кваліфікації співробітників, які налаштовують і експлуатують ці рішення. Таким чином вимоги до професійності персоналу та його відповідальності є основними, при реалізації політики інформаційної безпеки підприємства або організації [36].

Для успішної роботи додатків БСМ потрібно злагоджена робота і управління великою кількістю розподілених і слабо пов'язаних польових смарт-пристроїв, які ідентифікують і довіряють один одному. Хоча обрана платформа ZigBee забезпечує інтеграцію пристроїв в мережу і орієнтується на децентралізовану апаратно-програмну платформу, поточні рішення засновані на централізованій інфраструктурі. До недоліків централізованої інфраструктури відносяться, серед іншого, високі експлуатаційні витрати, низька сумісність з іншими централізованими інфраструктурами, і реальні загрози національній безпеці в окремих точках відмови.

Децентралізація інфраструктури БСМ дає переваги, в тому числі скорочення обсягу даних, переданих в Інтернет для обробки і аналізу, поліпшення безпеки та конфіденційності інформації. Забезпечення достовірності цих операцій означає досягнення розподіленого консенсусу з польовим пристроїв БСМ. Зараз сформувалося три принципово різних підходи до вирішення завдання передачі та обробки інформації різними платформами існуючих рішень – рішення IBM Research на базі технології Hyperledger Fabric [67], рішення консорціуму IOTA на базі протоколу Tangle, в основі якого лежить DAG (Directed Acyclic Graph), та технології Qubic і перспективний підхід проекту Radix, заснований на Tempo Ledger технології. Ці підходи об'єднує можливість роботи на різних апаратних засобах, а функціональна мова програмування дозволяє спростити аналіз, щоб довести правильність коду і надає великого значення паралелізму, що означає, що різні частини великої програми можуть запускатися одночасно, щоб використовувати переваги декількох процесорів або навіть декількох пристроїв.

Proof-of-work (PoW) – механізм консенсусу вважається вельми енерговитратною технологією. З огляду на важливість PoW IBM Research

розробляє новий метод реалізації цього механізму використовуючи обчислювальні потужності пристроїв Інтернету речей [58]

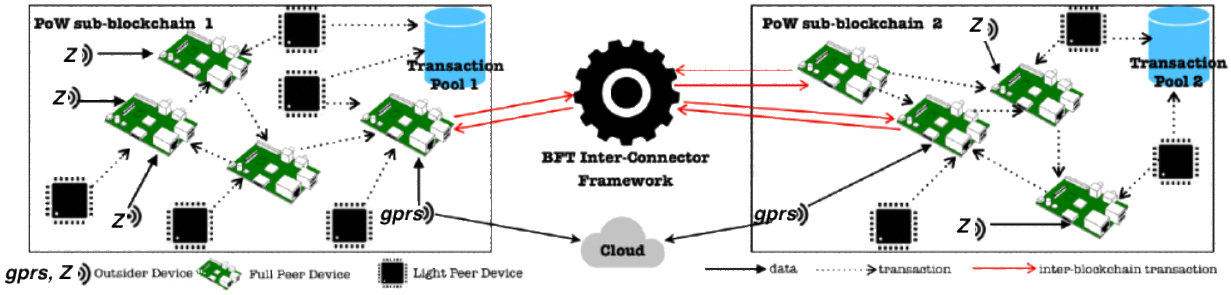



Рисунок 3.40 – Гібридний БСМ-блокчейн

Однією з найбільших проблем в інтеграції блокчейну в IoT є масштабованість. Через велику кількість пристроїв і обмежень ресурсів розгортання блокчейн є особливо складним. Оптимальна архітектура блокового ланцюга повинна масштабуватись для багатьох пристроїв введення-виведення (вони стають одноранговими вузлами в ланцюжку блокчейна), і вона повинна обробляти високу пропускну здатність транзакцій. Hybrid-IoT, платформа, розроблена IBM Research, використовує як блок-схеми PoW, так і протоколи Bytantine Fault Tolerant (BFT) для досягнення масштабованості.

По-перше, блок-схеми PoW забезпечують розподілений консенсус серед багатьох пристроїв, рівноправних вузлів блокового ланцюга в кластерному суб-блокчейні. Hybrid-IoT використовує структуру міжкластерних з'єднань BFT для забезпечення взаєморозуміння між блоковими ланцюжками.

Обрана структура віртуалізованих пристроїв введення-виведення, представлених одноранговими вузлами Hybrid-IoT з різними ролями в рамках окремого блок-ланцюга PoW, доводить ефективність конструкції блокового ланцюга PoW, яка також запобігає уразливості системи безпеки.

Пристрої мережі IoT мають вкрай широкий діапазон обчислювальної потужності і енергоресурсів, а деякі з них не можуть вирішувати складні завдання, передбачені PoW. Поділ вузлів по групах дозволяє алгоритму вирішувати, яка пропорція в кожній групі повинна здійснювати майнінг, в

залежності від обсягу енергії, використовуваної кожним вузлом. У цій моделі тільки деякі ноди (вузли) здійснюють повне PoW. IBM виявила, що при розміщенні вузлів в кластерах по 250 од., тільки 7% цих підблокчейнів виконували PoW, досягаючи найкращого результату з точки зору економічності, масштабування і безпеки. IOTA, розроблена з урахуванням концепції масштабованості, представила концепцію спеціальної платформи смарт-контрактів під назвою Qubic, що працює поверх основного протоколу IOTA. Індивідуальні Qubic – це, по суті, розподілені на основі кворумі обчислювальні завдання. Qubic використовує IOTA Tangle для упаковки і поширення кубиків від їх власників до оракулів, які будуть їх обробляти. Технічно метод Tangle є ациклічним графом – це метод циклічної передачі, при якому цикли можуть виконуватися паралельно. Кубики можуть жити на Tangle в сплячому стані. Коли конкретні вхідні дані стають доступними або змінюються, вони «прокидаються» і починають обробку, що може привести до того, що каскад інших кубиків прокидається в міру появи нових результатів. Це дозволяє створити дуже динамічне середовище програмування, що дозволяє додавати нові кубики в будь-який час і прив’язувати їх до будь-яких вхідних даних. Після обробки кубика, досягнутого кворуму і результатів, відправлених в Tangle, відбуваються дві речі: 1) кубик знову переходить в сплячий режим, очікуючи наступної зміни входів, і 2) спрацьовує каскадний ефект, так що залежний кубик починає обробку з новими входами. Технологія передбачає економний режим функціонування і оптимізована під низьке енергоспоживання і невеликий обсяг пам’яті польових пристроїв.

RADIX запропонував однорангові з’єднання вузлів з логічними годинами. Radix домігся рішення для обох проблем таким чином, що йому не потрібен PoW (майнінг), йому не потрібно PoS (доказ частки) і йому не потрібні головні вузли для підтвердження транзакцій. Система є безпечною, надаючи вузли з історичним записом згенерованих часових доказів. RADIX DLT має лінійну масштабованість. Це означає, що чим більше вузлів додано в мережу, тим більше вона буде масштабуватися. На відміну від поточних

рішень, кожен вузол, що додається, збільшує пропускну здатність Radix-мережі. Radix дозволяє навіть обмеженим ресурсами пристроям брати участь в якості вузлів в мережі. Вузол Radix можна запускати на пристрої з розміром пам’яті 16 МБ і процесором 100 МГц. Це робить децентралізацію ще більш досконалою.

Маркери Radix (RAD) використовують децентралізовану технологію leger (DLT) для запису транзакцій. RadixDLT пропонує систему, яка покращує, хоча і відрізняється, технологію блокування з точки зору масштабованості. RadixDLT зберігає всі транзакції і замовлення в протоколі в глобальній розподіленій книзі Tempo Ledger. Ця книга складається з трьох основних компонентів: мережного кластера вузлів, глобальної бази даних регістрів, розподіленої по вузлах, і алгоритму для генерації криптографічно безпечної записи тимчасово упорядкованих подій.

### 3.6. Висновки до третього розділу

1. Виходячи з експериментальних даних зроблено наступні висновки: енергоспоживання польового пристрою залежить не стільки від потужності прийомо-передавача, але визначається взаємодією трансивера з керуючим мікроконтролером, встановленим в польовому пристрої для виконання призначених для користувача функцій. Іншими словами, енергоспоживання визначається верхнім рівнем додатків стека протоколу ZigBee, і є критично залежним від фізичного і канального рівня протоколу 802.15.4.

2. Удосконалено математичну модель оцінки працездатності польових пристроїв з автономним живленням і модернізовано архітектуру системи, в результаті чого час життя системи перевищив нормативний період повірки приладів обліку.

3. Проведені дослідження підтвердили перспективність використання технології ZigBee для побудови бездротових систем енергомоніторингу об’єктів комунальної інфраструктури. З точки зору енергоефективності та часу

життя системи встановлені основні вимоги до обладнання та організації системи. Найкращі результати досягаються при використанні технології ZigBee в системах енергомоніторингу в районах щільної багатоповерхової забудови і складної завадової обстановки. Оптимальні результати досягаються для MESH-мереж, які об’єднують в своєму складі близько 40 ПЗПД, з’єднаних одним координатором, який виконує роль шлюзу.

4. З огляду на необхідність розробки системи енергомоніторингу сформульовані вимоги до програмного забезпечення рівня користувальницького додатка.

5. Вперше запропоновано механізм динамічної адресації польових пристроїв бездротової Інтернет-системи збору даних і управління енергоспоживанням, що унеможливлює віддалене стороннє втручання в роботу сегментів системи.

6. Аналіз стійкості бездротових мереж моніторингу до зовнішніх атак вказав на їх критичну уразливість, обумовлену централізованою архітектурою, тому найбільш дієвим і ефективним механізмом захисту інформації в бездротових мережах моніторингу є перехід до децентралізованих систем, зокрема побудованих на принципах технології блокчейн. Зроблено висновок, що найбільш прийнятним рішенням для БСМ є сервісний або приватний блокчейн, що дозволяє проводити ідентифікацію польових пристроїв під контролем призначених користувачів.

Основні результати розділу опубліковано в роботах автора: [3, 39, 41, 76, 79, 83-86, 88, 91, 93-95, 98, 102, 104, 107].

# РОЗДІЛ 4. ПРАКТИЧНА РЕАЛІЗАЦІЯ БЕЗДРОТОВОЇ ПЕРЕДАЧІ ДАНИХ В МЕРЕЖАХ ЕНЕРГОМОНІТОРИНГУ

## 4.1. Комунікаційний протокол бездротової мережі передачі даних

Наведені вище результати вказують на визначальне значення рівня додатку стека ZigBee для стійкості бездротової мережі моніторингу до хакерських атак і, як наслідок до збільшення терміну життя системи в цілому. З огляду на енергоємність процесу передачі даних, саме управління розмірами повідомлень є основним резервом збільшення терміну життя пристроїв і системи в цілому. У розділі 3 зроблений важливий висновок про те, що енергоспоживання польового пристрою визначається взаємодією трансивера з керуючим мікроконтролером, встановленим в польовому пристрої для виконання призначених для користувача функцій. Іншими словами, енергоспоживання визначається верхнім рівнем додатків стека протоколу ZigBee, і критично залежною від фізичного і канального рівня протоколу 802.15.4.

Згідно з визначенням протокол – це набір правил, встановлених для однозначного подання інформації, переданої в цифровому вигляді. З кінця 80-х років XX століття почали розроблятися уніфіковані відкриті протоколи для пристроїв і систем автоматизації. Рушійною силою цього процесу була необхідність упорядкування ситуації паралельного використання безлічі несумісних протоколів різних виробників. Потреба у створенні уніфікованого відкритого протоколу для пристроїв і систем автоматизації, що дозволяє працювати з усім розмаїттям об'єктів, привела до створення протоколів, найбільш відомими з яких стали DNP3, UCA і стандарти серії IEC 60870.

Протокол DNP (Distributed Networking Protocol) розроблявся з 1990 року. У 1993 році вийшла третя версія протоколу – DNP 3.0, яка спочатку позиціонувалася як протокол для послідовних каналів, але з 1998 року він став підтримувати роботу Ethernet (TCP або UDP). DNP3 базується на варіанті

протоколу IEC 60870-5 і використовує ряд рішень з IEC 60870-5-1 і -2 [82].

Протокол UCA (Utility Communications Architecture, http://www.ucaiug.org/aboutUCAIug / default.aspx) розроблений в 1988 році ERPI (Electric Power Research Institute, США) і IEEE (Institute of Electrical and Electronics Engineers). Згодом протокол UCA ліг в основу стандарту IEC 61850 «Мережі і системи зв'язку на підстанціях».

IEC 60870 – це серія стандартів, розроблена Технічним комітетом 57 (Робоча група 03) Міжнародної Електротехнічної Комісії (МЕК, IEC - International Electrotechnical Commission) з метою забезпечити відкритий протокол для передачі керуючих та інформаційних даних телеметрії [82, 109]. Перші базові стандарти в рамках IEC 60870 почали з'являтися з 1988 року і вилилися в публікацію в 1995 році профілю IEC 60870-5-101, який «поширюється на пристрої та системи телемеханіки з передачею даних послідовними двійковими кодами для контролю і управління територіально розподіленими процесами». У міру розвитку мережевих технологій IEC 60870-5 став передбачати використання протоколу TCP / IP. Усередині TCP / IP можуть бути використані різні типи мереж, включаючи Ethernet 802.3, X.25, ATM (режим асинхронної передачі) та ISDN (Цифрова мережа інтегрованого обслуговування) [64]. Положення цього стандарту служили базою для фірми Landis & Gyr, при розробці протоколу SCTM (Serial Coded Tele-Metering), призначеного для передачі даних по вимірювальним каналам з реалізацією процедури поблочного виявлення помилок з використанням методу контролю циклічним надлишковим кодом (CRC) і підтвердження прийому. Незважаючи на появу нових протоколів систем енергомоніторингу, таких як VDEW і DLMS, на наш погляд, надійність і простота інсталяції дозволяють рекомендувати протокол SCTM для застосування в радіомережах передачі даних, що мають значні затримки і наявність перешкод [109]. Це обумовлено перевантаженістю і ненадійністю функціонування протоколів VDEW і DLMS в масштабних системах енергомоніторингу з використанням передачі даних по каналах GSM /

GPRS. Використання протоколу SCTM в мережах стандарту ZigBee є актуальним і виправданим рішенням, що буде показано нижче.

### 4.1.1. Протокол обміну даними SCTM

Протокол SCTM використовує рекомендації IEC 60870-5 і розроблений для додатків телеметричного збору вимірювальних даних з метою забезпечення надійного і достовірного обміну даними по лініях зв'язку низької якості (низьке співвідношення сигнал/шум, підвищений рівень шумів і імпульсних перешкод, високі фазові спотворення) [55]. Протокол заснований на трирівневій моделі «Архітектура підвищеної продуктивності» (EPA – Enhanced Performance Architecture), визначеній в IEC 60870-5, що є спрощеним варіантом семирівневої моделі ISO / IEC 7498-1. Архітектура EPA була розроблена з метою отримання більш швидкого часу реакції для критичної інформації, але з обмеженими послугами. Зазвичай в модель EPA додають ще один рівень – «Процес користувача». Даний рівень додається, щоб представити різні функції або процеси, які повинні бути обов’язково визначені, щоб передбачити здатність до взаємодії між обладнанням системи.

На канальному рівні слід звернути увагу на такі поняття:

Первинна (ведуча, майстер) і вторинна (відома, slave) станції. Термін «первинна станція» означає, що вона (і тільки вона) ініціює взаємодію на канальному рівні. Відома станція чекає запиту від первинної станції і тільки після отримання посилає у відповідь будь-які дані. Однак відома станція може виступати як первинна для станцій наступного рівня в ієрархічній системі. Процедури передачі – небалансна і балансна. При небалансній процедурі передачі одна зі станцій завжди виступає як первинна станція, а всі інші станції як вторинні. При балансній передачі кожна станція може бути як первинною, так і вторинною. Сервісні процедури і примітиви – функції канального рівня, що надають послуги більш високих рівнів. Існує три основних типи сервісів на канальному рівні: Send/no reply, Send/confirm, Request/respond.

Send/no reply використовується для розсилки широкомовних повідомлень, send / confirm для посилки команд управління, request / respond для отримання даних від відомої станції.

Протокол телеметрії IEC-60870 представляє собою широко поширений стандарт, призначений для моніторингу та управління розподіленими процесами за допомогою локальних інтелектуальних пристроїв для зв'язку центральної ЕОМ з віддаленими пристроями управління і для збору даних. Протокол IEC-60870 поєднує деякі можливості символьних протоколів в форматі UART з біт- орієнтованим форматом кадру типу HDLC.

В IEC-60870 одиницею передачі інформації є телеграма, що складається з байтових послідовностей по 8 біт. Кожен байт передається відповідно до формату UART у вигляді 11-бітової послідовності (1 стартовий біт, 8 біт даних, 1 біт парності, 1 столовий біт). Октети передаються послідовно в кожній телеграмі в наступному порядку:

- заголовок (1 або 4 байти);
- призначені для користувача дані (змінна довжина, до 253 байт);
- контрольна сума (1 байт);
- символ кінця повідомлення (1 байт).

Завдяки своїй простоті протокол IEC-60870 легко вбудовується в різноманітні пристрої і в основу багатьох промислових рішень світових лідерів, таких як Landis & Gyr, Siemens і ін. [55]

Протокол SCTM заснований на загальній трирівневій моделі:

1. фізичний рівень використовує стандарти Міжнародного союзу електрозв'язку, Т - телеметрія, (RS232 / V.24, RS485, V.21; V.22; V.22bis; V.23 та ін.), які забезпечують передачу даних методом поблочного кодування на канальному рівні.

2. канальний рівень (IEC-60870-5-1: Формат телеграми; IEC-60870-5-2: Процедури передачі канального рівня) містить процедури передачі, які використовують однозначну інформацію про управління протоколом

канального рівня, за допомогою яких передаються модулі службових даних рівня додатків (ASDU) в якості службових даних канального рівня. Канальний рівень використовує формат телеграми FT1.2, яка забезпечує необхідну цілісність, високу достовірність, ефективність і надійність передачі даних.

Цей стандарт визначає однозначну адреса (номер) для кожного з'єднання. Кожна адреса може бути єдиною всередині даної системи або єдиним всередині групи каналів, що використовують загальний канал. Останнє вимагає меншого адресного поля, але ПУ повинен встановлювати відповідність між адресами і номером каналу.

3. рівень додатків (IEC-60870-5-3: Загальна структура даних користувача; IEC-60870-5-4: Опис і кодування інформаційних елементів) включає опис передачі модулів службових даних рівня додатків.

Основні характеристики SCTM:

- Клас організації обміну даними: клас S3 «запит / відповідь» (операція «читання RTU»).
- Процедура передачі даних: незбалансований режим (запити посилає тільки ЦС).
- Режим роботи: полудуплекс.
- Вид з'єднання: точка - точка, лінія.
- Тип передачі: асинхронний старт / стоп.
- Формат знаку: 1 стартовий біт, 7 біт даних, 1 біт парності, 1 стоповий біт.
- Формати телеграм: кадр класу FT1.2 з постійною і змінною довжиною.
- Виявлення помилок: контроль циклічним надлишковим кодом по слову і по кадру.
- Захист доступу до RTU: ідентифікаційний номер і пароль.
- Захист від втрати інформації:

  - позитивне квитування відповіді від RTU,

  - повтор запиту при виявленні помилки або відсутності відповіді від RTU

  - система порядкових номерів і форматів телеграм.

Основні дані по реалізації протоколів:

**МЕК 870-5-101**

- Передача по каналу зв'язку - небалансна
- Кадр - FT1.2
- Швидкість від 100 до 115200 бод
- Інтерфейс RS-232 (можливо RS-485)
- Адресний поле канального рівня 1 байт
- Максимальна довжина прийнятого кадру 120 байт
- Максимальна довжина переданого кадру 120 байт
- Запит даних класу 1 і 2 обробляються ідентично

**МЕК 870-5-104**

- Установка з’єднання по TCP пасивна (контролер чекає з’єднання з боку центру)
- Активізація обміну очікується з боку центру
- Підтримується тестові кадри (з ініціативи центру)
- Максимальна довжина прийнятого кадру 120 байт
- Максимальна довжина переданого кадру 250 байт
- Підтримується режим передачі групи інформаційних кадрів на одну квитанцію (потрібно для каналів з тривалою буферизацією).

### 4.1.2. Опис повідомлення по протоколу SCTM

Повідомлення запиту по протоколу SCTM завжди складається з заголовка і блоку даних, які мають власні контрольні суми. Тема містить в собі такі базові службові поля [55]:

- стан ( «запит», «відповідь» або «відповідь довга»
- адреса (slave)
- № блоку даних
- № квитанції

- довжина блоку даних
- контрольна сума заголовка

Стан «відповідь довга» на відміну від «відповідь» має на увазі, що всі запитувані дані не вміщуються в дане повідомлення і після квитування даної відповіді, буде передана відповідь з наступними даними.

Адреса (slave) – це адреса веденого пристрою, кому призначений запит (або від кого відповідь). Номер блоку даних в запитах завжди дорівнює 1, а у відповідях змінюється від 1 до 9 (і т.д. по колу), якщо відповідь довга.

Номер квитанції у відповідях завжди дорівнює 1, а в запитах (квитанціях довгої відповіді) змінюється згідно з номером блоку даних отриманого повідомлення. При первинному запиті номер квитанції дорівнює 0. Максимальна довжина блоку даних 255.

Повідомлення відповіді може бути як з заголовка і блоку даних, так і тільки з одного заголовка (квитанція). Квитанція, як відповідь на запит означає, що остання передана команда виконана. Квитанція довгої відповіді означає, що був прийнятий відповідний блок даних і очікується передача наступного блоку даних (повідомлення).

При описі протоколу SCTM під відповідну систему слід враховувати, що початком повідомлення (заголовка) завжди є байт з кодом 1 (SOH по таблиці ASCII), крім випадку, коли даний байт потрапляє на контрольну суму блоку даних (оскільки блок даних може бути довільної довжини, то і контрольна сума може бути будь-який). Контрольна сума заголовка з кодом 1 бути не може.

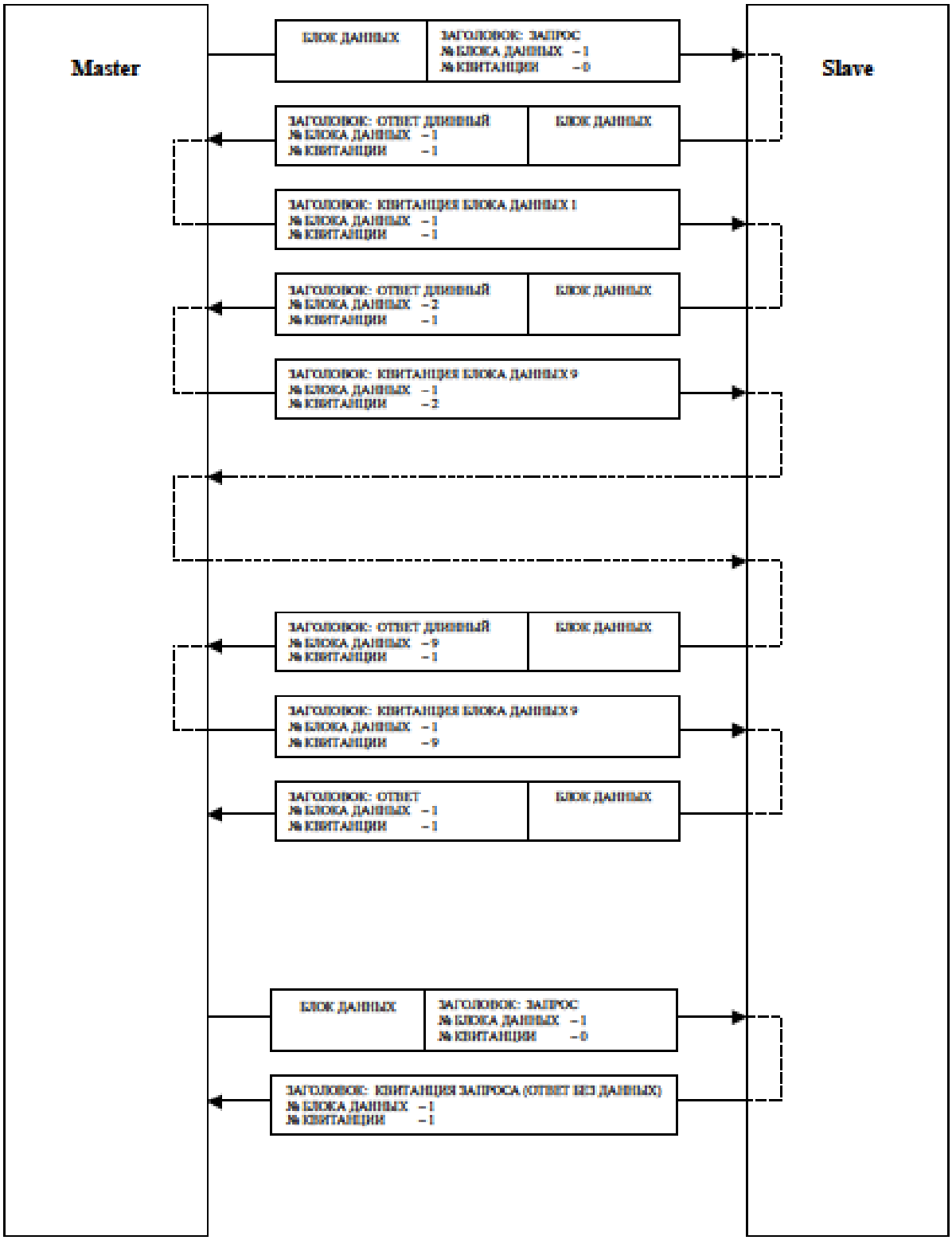



Рисунок 4.1 – Процедура передачі даних

ЗАПИТ

| | Заголовок - 13 байт | | | | | | Блок данных | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Состояние | | | | | | | | | |
| Старт SOH | 0 - ответ<br>1 - запрос<br>2 - ответ длинный | Адрес Slave<br>0 - 65535 | № блока данных<br>1-1 | № квитанции<br>0 - начало данных<br>1-9 - след. данные | Длина блока данных<br>0 - 255 | Контр. сумма загол. | Начало текста STX | Поле данных | Конец текста ETX | Контр. сумма данных |
| 1 | 1 | 0 0 0 1 2 | 1 | 0 | 0 0 5 | 54 | 2 | V R | 3 | 7 |
| DEC | ASCII | ASCII | ASCII | ASCII | ASCII | DEC | DEC | ASCII | DEC | DEC |
| | Данные для подсчета контр. суммы (через XOR) | | | | | | | Данные для XOR | | |

ВІДПОВІДЬ

| | Заголовок - 13 байт | | | | | | Блок данных | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Состояние | | | | | | | | | |
| Старт SOH | 0 - ответ<br>1 - запрос<br>2 - ответ длинный | Адрес Slave<br>0 - 65535 | № блока данных<br>1-9 | № квитанции<br>1-1 | Длина блока данных<br>0 - 255 | Контр. сумма загол. | Начало текста STX | Поле данных | Конец текста ETX | Контр. сумма данных |
| 1 | 0 | 0 0 0 1 2 | 1 | 1 | 0 0 8 | 59 | 2 | H 0 7 0 1 | 3 | 77 |
| DEC | ASCII | ASCII | ASCII | ASCII | ASCII | DEC | DEC | ASCII | DEC | DEC |
| | Данные для подсчета контр. суммы (через XOR) | | | | | | | Данные для XOR | | |

Квитанція (відповідь без даних)

| | 14 байт | | | | | | |
|---|---|---|---|---|---|---|---|
| | Состояние | | | | | | |
| Старт SOH | 0 - ответ<br>1 - запрос<br>2 - ответ длинный | Адрес Slave<br>0 - 65535 | № блока данных<br>1-9 | № квитанции<br>1-1 | Длина блока данных<br>0 - 255 | Контр. сумма загол. | Конец текста ETX |
| 1 | 0 | 0 0 0 1 2 | 1 | 1 | 0 0 0 | 51 | 3 |
| DEC | ASCII | ASCII | ASCII | ASCII | ASCII | DEC | DEC |
| | Данные для подсчета контр. суммы (через XOR) | | | | | | |

Квитанція довгого відповіді

| | 14 байт | | | | | | |
|---|---|---|---|---|---|---|---|
| | Состояние | | | | | | |
| Старт SOH | 0 - ответ<br>1 - запрос<br>2 - ответ длинный | Адрес Slave<br>0 - 65535 | № блока данных<br>1-1 | № квитанции<br>0 - начало данных<br>1-9 - след. данные | Длина блока данных<br>0 - 255 | Контр. сумма загол. | Конец текста ETX |
| 1 | 1 | 0 0 0 1 2 | 1 | 7 | 0 0 0 | 52 | 3 |
| DEC | ASCII | ASCII | ASCII | ASCII | ASCII | DEC | DEC |
| | Данные для подсчета контр. суммы (через XOR) | | | | | | |

Рисунок 4.2 – Формат повідомлення по протоколу SCTM (приклади)

### 4.1.3. Опис повідомлення по протоколу SCTMex

З огляду на, що протокол SCTM розроблявся для дротових мереж, його імплементація для роботи в радіомережах стандарту 802.15.4 / ZigBee зажадала деякої модифікації для забезпечення надійної роботи пристроїв в бездротових мережах складної архітектури [55].

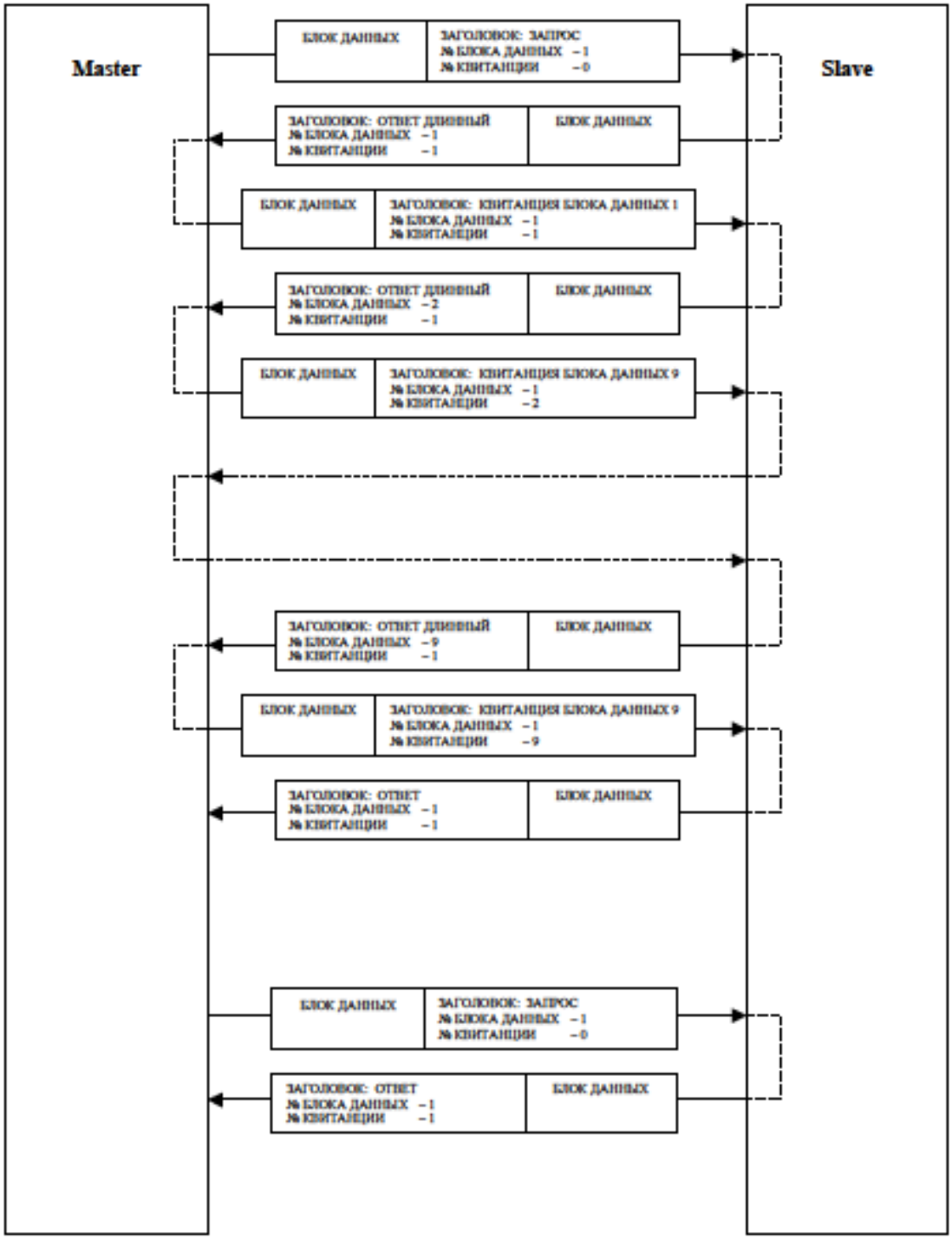



Рисунок 4.3 – Процедура передачі даних

**Основні характеристики SCTM (ex):**

- Клас організації обміну даними: «запит / відповідь»
- Тип передачі: асинхронний
- Режим роботи: підлозі дуплекс

- Формат кадру фізичного рівня: 8 біт даних, 1 стартовий біт, 1 стоповий біт
- Формати повідомлення канального рівня: кадр класу FT1.2 з постійною і змінною довжиною
- Виявлення помилок: контроль циклічним виключає АБО (XOR)
- Захист від втрати інформації:
  - відповідь від RTU (квитанція);
  - повтор запиту при виявленні помилки або відсутності відповіді від RTU
  - система нумерації повідомлень (для SCTMex)

**ЗАПИТ**

| | Заголовок - 13 байт | | | | | | | Блок данных | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Состояние | | | | | | | | | | | | | |
| Старт | 0 - ответ<br>1 - запрос | Адрес Slave | № блока данных | № квитанции<br>0 - начало данных | Длина блока данных | Контр. сумма загол. | Начало текста | Адрес Master | Шифр.<br>0 - выкл. | Номер сообщ. | Поле данных | Конец текста | Контр. сумма данных |
| SOH | 2 - ответ длинный | 0 - 65534 | 1-1 | 1-9 - след. данные | 0 - 255 | | STX | 0 - 65534 | 1 - вкл. | | | ETX | |
| 1 | 1 | 00012 | 1 | 0 | 019 | 59 | 2 | 00001 | 0 | 123 | POWER0 | 3 | 125 |
| DEC | ASCII | ASCII | ASCII | ASCII | ASCII | DEC | DEC | ASCII | ASCII | ASCII | ASCII | DEC | DEC |
| | Данные для подсчета контр. суммы (через XOR) | | | | | | | Данные для XOR | | | | | |

**ВІДПОВІДЬ**

| | Заголовок - 13 байт | | | | | | Блок данных | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Состояние | | | | | | | | | | | | |
| Старт | 0 - ответ<br>1 - запрос | Адрес Slave | № блока данных | № квитанции | Длина блока данных | Контр. сумма загол. | Начало текста | Адрес Master | Шифр.<br>0 - выкл. | Номер сообщ. | Поле данных | Конец текста | Контр. сумма данных |
| SOH | 2 - ответ длинный | 0 - 65534 | 1-9 | 1-1 | 0 - 255 | | STX | 0 - 65534 | 1 - вкл. | | | ETX | |
| 1 | 0 | 00012 | 1 | 1 | 019 | 59 | 2 | 00001 | 0 | 123 | POWER0 | 3 | 125 |
| DEC | ASCII | ASCII | ASCII | ASCII | ASCII | DEC | DEC | ASCII | ASCII | ASCII | ASCII | DEC | DEC |
| | Данные для подсчета контр. суммы (через XOR) | | | | | | | Данные для XOR | | | | | |

Рисунок 4.4 – Формат повідомлення по протоколу SCTMex (приклади)

Протокол SCTMex є розширенням протоколу SCTM, за рахунок декількох початкових байт блоку даних. Отже, призначення всіх полів заголовка протоколу SCTMex ідентично протоколу SCTM. Різниця полягає в конструкції повідомлень. У повідомленні протоколу SCTMex відпадає таке поняття, як квитанція (без блоку даних). У будь-якому повідомленні запиту і відповіді є заголовок і блок даних. Поняття "квитанція" в протоколі SCTMex означає той же запит, тільки з іншим номером квитанції в заголовку.

Протокол SCTMex щодо SCTM розширено трьома службовими полями:

- адреса (master)
- шифрування
- номер повідомлення

Адреса (master) - це адреса ведучого пристрою, від кого надійшов запит (або для кого відповідь). Дане поле дозволяє відстежувати і однозначно ідентифікувати повідомлення в умовах бездротових мереж, а також виключити помилки при накладенні радіоканалів різних мереж.

Поле «шифрування» може мати два стани: 1 - включено або 0 - вимкнено. Якщо отримано повідомлення з активованим шифруванням – це означає, що вся інформація в поле даних буде зашифрована за алгоритмом на рівні додатку. Поле «номер повідомлення» може змінюватися в межах від 1 до 999. Номер повідомлення в запиті і відповіді на цей запит повинен бути один і той же. Після кожної сесії (запит / відповідь) необхідно змінювати номер повідомлення. Це необхідно для правильної ідентифікації повідомлення при передачі в умовах затримок бездротових мереж, а також для маршрутизації повідомлень на рівні додатку.

### 4.2. Система енергомоніторингу

З точки зору обладнання для стаціонарної частини мережі, існує величезний вибір пристроїв для різних завдань [35]. Можна умовно розбити весь спектр обладнання на три групи:

1. Електронні компоненти – мікроконтролери, приймачі і т.і., що є основою для розробки рішень, починаючи з самого низького рівня.

2. Проміжні платформи, як правило, розробляються дослідницькими університетами з метою проведення експериментів.

3. Вбудовувані системи, створювані для вирішення конкретних завдань.

Теоретично можна провести натурний експеримент, зібравши з окремих компонентів спеціалізовану платформу на базі одного з безлічі доступних бездротових модулів, вироблених такими компаніями як Texas Instruments,

Atmel, REXENES, Freescale/DIGI і ін.

В ході роботи була розроблена спеціалізована програмно-апаратна платформа «SmartUtility Web» (Додаток В) на базі бездротового модуля XBEE S2 [57, 58]. Дані модулі на момент розробки володіли найкращими характеристиками з точки зору простоти використання, побудови мереж меш-топології, підтримки режимів. Автор дисертаційної роботи брав участь у проекті зі створення бездротової системи моніторингу споживання води побутовими абонентами КП «Водоканал» Запоріжжя.

Система Інтернет-моніторингу споживання і управління споживанням енергоресурсів «Smart Utility Web» призначена для простого і легкого використання на об'єктах житлово-комунального господарства. Система включає прилади обліку, пристрої збору і передачі даних (ПЗПД) «Сигма ZB», модем-координатор системи «Сигма RF», хмарний SaaS сервіс.

Програмно-апаратна платформа «Smart Utility Web» включає:

- лічильники води (холодної та гарячої);
- Перетворювачі імпульсів у вигляді герконового датчика або транзистора з відкритим колектором;
- Польові пристрої збору і передачі інформації «СІГМА ZB»
- Модем-координатор ПЗПД «СІГМА RF»
- INTERNET.

ПЗПД «Сигма ZB» володіє унікальними технологічними характеристиками, до яких відносяться:

- висока стійкість до електромагнітних завад;
- високу швидкодію (періодичність вимірювань від 10 мс);
- розширені можливості синхронізації по мережі ZigBee або Ethernet (по протоколах NTP і МЕК 60870-5-104);
- призначення міток часу виміряним параметрам в самому пристрої безпосередньо в момент вимірювання;
- простота конфігурації і програмування по мережі;
- можливість одночасного підключення до 2-х клієнтів за протоколом

МЕК 60870-5-104.

Ключова особливість полягає в тому, що він поєднує в собі функції:

1. Облік імпульсів по 2-м каналам. ПЗПД підключаються безпосередньо до імпульсних виходів приладів обліку (лічильники електроенергії, теплової енергії, води, газу). Для зв’язку з верхнім рівнем всі пристрої мають на вибір: радіоінтерфейс 433, 868 МГц і 2,4 ГГц (специфікації ZigBee); 2-дротовий інтерфейс RS485, що дозволяє легко організувати розподілену систему збору даних в рамках підприємства або комунального об'єкту.

2. Облік енергоресурсів. При конфігуруванні задаються тип енергоносія, коефіцієнти перетворення, інтервал вимірювання та інші параметри. Ведеться архів споживання енергоресурсу по двох незалежних каналах з прив’язкою кожного запису до мітках часу кратними 15, 30 або 60-хвилинним інтервалом. Глибина зберігання архіву 2-8 діб. Формується кумулятивний архів добових і місячних показань з глибиною зберігання 3 роки. Підтримується перехід на літній та зимовий час.

3. Реєстрація аварійних подій. ПЗПД має незалежне введення контролю цілісності ланцюга. При розмиканні контакту формується повідомлення про порушення нормального режиму з фіксацією часу події. Можливо управління станом споживання абонента при навмисному впливі спрямованим магнітним полем, створюваним постійним магнітом з магнітною індукцією на поверхні більше 50 мТл і загальною площею до 60 см².

4. Управління навантаженням споживання. Ця функція дозволяє проводити перевірку поточного стану споживання та його порівняння з заданим параметром. При перевищенні заданого порогу формується керуюча команда на реле (клапан відсікання або кульовий кран з електроприводом) на повне або часткове обмеження споживання до відновлення параметра в заданому діапазоні.

5. Підтримується режим автономного живлення ПЗПД від літієвих батарей. При цьому виконується вимога енергоефективності, зафіксована стандартом MEPS (Minimum Energy Performance Standard).

Устаткування автоматизованої системи «Smart Utility Web» призначене для простого і швидкого розгортання систем моніторингу та управління водоспоживанням на об’єкті автоматизації.

Функціональність «Smart Utility Web» полягає в:

- Забезпеченні одноразового знімання показань з усіх приладів обліку;
- Контролі режиму споживання і сигналізація про виникнення аварійних ситуацій;
- Проактивному управлінні режимами поставки;
- Виявленні витоків і аномальних витрат на ранній стадії;
- Веденні балансу споживання і виявлення розкрадань;
- Дистанційному контролі якості води;
- Дистанційному моніторингу і управлінні.

Доступ до даних здійснюється через будь-який Web-браузер або мобільний додаток (iOS, Android, Win).

Модем-координатор (рис.4.5) є основним пристроєм системи, що забезпечує побудову і підтримання працездатності радіомережі, а також передає інформацію, зчитану з лічильників до іншої програми по каналах мобільного зв’язку.

ПЗПД «Сигма ZB» підключається безпосередньо до лічильника за допомогою штатного інтерфейсу лічильника.

ПЗПД «Сигма ZB» (рис.4.6) підтримує передачу через себе по мережі даних, одержуваних від інших пристроїв в мережі. Тому, після установки всіх абонентських модулів і при наявності між ними зв’язку світлодіоди на всіх модулях повинні горіти безперервно. Система перейде в режим автономної роботи.


а)

б)

Рисунок 4.5 – Модем-координатор «Сигма RF»

Внесення початкових налаштувань на місці установки польового пристрою здійснюється за допомогою спеціально розробленого термінального пристрою «Інсталлер». Дистанційне керування польовими пристроями здійснюється через розроблену за участю дисертанта програму параметризації «SCTM-Dialog» (див. п.4.3.).


а)


б)

в)

Рисунок 4.6 – ПЗПД «Сигма ZB»

Наведені нижче скріншоти екранних форм системи «Smart Utility Web» (Додаток В) демонструють результати, отримані при експлуатації системи за адресою: м.Запоріжжя, вул.40-років Радянської України, будинок № 84-б під'їзд 4 (1 квартира без урахування – перекрита каналізація).

Встановлені лічильники: DN20 CDTRP. Абонентський облік: DN15 CD OneTRP класу «С» (1 л / імп.).

| Дата | Витрата по під'їзду, куб.м | Баланс, куб.м | Баланс,% |
|---|---|---|---|
| 26.Лют | 2,213 | 0,06 | 2,71 |
| 27.Лют | 2,45 | 0,074 | 3,02 |
| 28.Лют | 2,332 | 0,15 | 6,43 |
| 01.Бер | 2,306 | 0,052 | 2,69 |
| 02.Бер | 1,694 | -0,027 | -1,59 |
| 03.Бер | 1,791 | -0,003 | -0,17 |
| 04.Бер | 2,035 | 0,034 | 1,67 |
| 05.Бер | 2,284 | 0,143 | 6,26 |
| 06.Бер | 2,735 | 0,409 | 14,95 |
| 07.Бер | 2,497 | 0,153 | 6,13 |
| 08.Бер | 2,056 | 0,131 | 6,37 |
| 09.Бер | 2,332 | 0,175 | 7,5 |
| 10.Бер | 2,488 | 0,22 | 8,84 |
| 11.Бер | 2,146 | 0,105 | 4,89 |

Рисунок 4.7 – Середній відсоток небалансу - 6%

| Квартира | № лічил. | Попер. пок. | Наст. пок. | Споживання води |
|---|---|---|---|---|
| 30 (юр.) | 1210156774 | 29.795 | 33.162 | 3.367 |
| 31 | 1210156775 | 1.043 | 1.677 | 0.634 |
| 32(юр.) | 1210156772 | 7.539 | 8.743 | 1.204 |
| 33 | 1210156778 | 8.275 | 9.538 | 1.263 |
| 34 | 1210156785 | 32.16 | 39.056 | 6.896 |
| 35 | 1210156782 | 1.258 | 2.103 | 0.845 |
| 36 | 1210156786 | 18.891 | 21.639 | 2.748 |
| 37 | 1210156783 | 3.46 | 4.946 | 1.486 |
| 38 | 1210156777 | 41.959 | 46.968 | 5.009 |
| 40 | 1210156781 | 9.115 | 10.313 | 1.198 |
| Общедомовый учет | 1211213464 | 67.257 | 93.466 | 26. 209 |
| Небаланс | | | | 1.559 (5.95%) |

Рисунок 4.8 – Звіт про фактичне споживання води за період

| Квартира | № лічил. | Попер. пок. | Наст. пок. | Споживання води |
|---|---|---|---|---|
| 30 (юр.) | 1210156774 | 29.795 | 29.795 | 0 |
| 31 | 1210156775 | 1.122 | 1.204 | 0.082 |
| 32(юр.) | 1210156772 | 7.593 | 7.691 | 0.098 |
| 33 | 1210156778 | 8.388 | 8.561 | 0.173 |
| 34 | 1210156785 | 32.741 | 33.361 | 0.62 |
| 35 | 1210156782 | 1.334 | 1.428 | 0.094 |
| 36 | 1210156786 | 19.083 | 19.313 | 0.23 |
| 37 | 1210156783 | 3.663 | 3.823 | 0.16 |
| 38 | 1210156777 | 42.24 | 42.487 | 0.247 |
| 40 | 1210156781 | 9.257 | 9.347 | 0.09 |
| Общедомовый учет | 1211213464 | 68.951 | 70.742 | 1.791 |
| Небаланс | | | | -0.00299999999999999 (-0.17%) |

Рисунок 4.9 – Звіт про фактичне споживання води за період (норма)

Зафіксоване приладове розкрадання (при встановленій заглушці на каналізацію) становить 6%.

| Кварт. | № лічил. | 01.03 | 10.03 | Спожи-вання води 1 дек., м.куб | 20.03 | Спожи-вання води 2 дек., м.куб | 31.03 | Спожи-вання води 3 дек., м.куб | Сумарне спожи-вання води, м.куб. |
|---|---|---|---|---|---|---|---|---|---|
| 30 (юр.) | 1210156774 | 29.795 | 32.32 | 2.525 | 34.283 | 1.963 | 36.028 | 1.745 | 6.233 |
| 31 | 1210156775 | 1.043 | 1.561 | 0.518 | 1.993 | 0.432 | 2.625 | 0.632 | 1.582 |
| 32(юр.) | 1210156772 | 7.539 | 8.306 | 0.767 | 9.626 | 1.32 | 10.561 | 0.935 | 3.022 |
| 33 | 1210156778 | 8.275 | 9.269 | 0.994 | 10.356 | 1.087 | 11.685 | 1.329 | 3.41 |
| 34 | 1210156785 | 32.16 | 37.374 | 5.214 | 42.701 | 5.327 | 48.301 | 5.6 | 16.141 |
| 35 | 1210156782 | 1.258 | 1.907 | 0.649 | 2.678 | 0.771 | 3.646 | 0.968 | 2.388 |
| 36 | 1210156786 | 18.891 | 20.959 | 2.068 | 23.4 | 2.441 | 26.032 | 2.632 | 7.141 |
| 37 | 1210156783 | 3.46 | 4.554 | 1.094 | 5.787 | 1.233 | 7.14 | 1.353 | 3.68 |
| 38 | 1210156777 | 41.959 | 45.786 | 3.827 | 50.443 | 4.657 | 55.724 | 5.281 | 13.765 |
| 40 | 1210156781 | 9.115 | 10.136 | 1.021 | 11.084 | 0.948 | 12.189 | 1.105 | 3.074 |
| Общедомовый учет | 1211213464 | 67.257 | 87.169 | 19.912 | 108.148 | 20.979 | 87.169 | 22.33 | 63.221 |
| Небаланс | - | - | - | 1.235 | - | 0.8 | - | 0.75 | 2.785 (4.41%) |

Рисунок 4.10 – Використання води за березень

Зафіксований місячний небаланс (при встановленій в кв.39 заглушці на каналізацію) становить 4,41%.

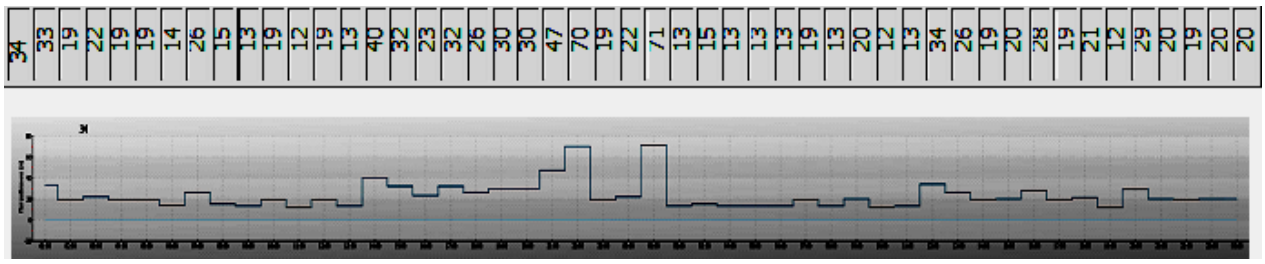



Рисунок 4.11 – Графік споживання (витік води)

Аномально висока витрата по кв.№34 – висновок: постійний витік більше 12 літрів на годину.

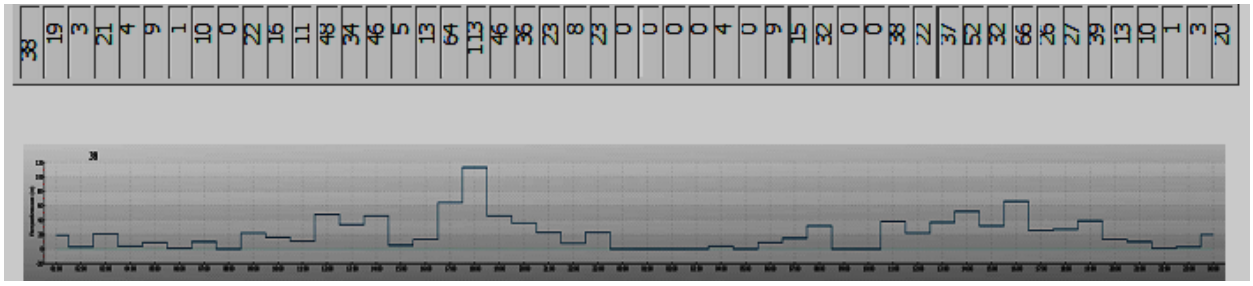



Рисунок 4.12 – Графік споживання (норма)

Висновок: Наявність «нульового споживання» – свідчить про справність арматури.

### 4.3. Програма SCTM DALOG

#### 4.3.1. Призначення

Програма SCTM Dialog призначена для організації обміну даними між комп'ютером і віддаленим пристроєм по протоколу SCTM і призначена для настройки обладнання та розробки програм і пристроїв на основі згаданого протоколу. У даній програмі також реалізований протокол SCTMex (розширення протоколу SCTM за рахунок блоку даних). В основі створення програми закладені принципи інтуїтивно зрозумілого інтерфейсу, інформативності, максимальної зручності та гнучкості користування, а також

найменшої кількості виконуваних дій для побудови і відправки протокольного повідомлення.

### 4.3.2. Характеристика

SCTM Dialog має можливість працювати одночасно з двома пристроями введення / виведення. Вибір використання другого «входу» здійснюється через меню програми. Кількість використовуваних COM портів задається в параметрах програми. За допомогою даної програми може бути передана прошивка мікроконтролера на віддалений пристрій для перепрограмування за умови підтримки даної можливості в віддаленому пристрої.

У програмі є можливість встановлення мови інтерфейсу на російську, українську та англійську. SCTM Dialog може видавати повідомлення про підключення пристрою на віртуальний COM порт, із зазначенням його номера, якщо дана можливість дозволена в параметрах програми.

При необхідності, можна змінити розміри основного вікна і дерева функцій.

Налаштування програми і створені дані зберігаються у файлі SCTM Dialog.ini, що знаходяться в одній директорії з програмою, що дозволяє переносити і використовувати дану програму на іншому комп’ютері з усіма основними настройками і створеними даними.

При закритті програми стан її дерева функцій буде збережено, і, при її повторному відкритті, вона буде мати вигляд, як при останньому сеансі роботи.

### 4.3.3. Опис основних можливостей

У лівому верхньому кутку (під панеллю інструментів) знаходиться спадаючий список тегів функцій, а під ним дерево функцій. Праворуч розташовані дві групи параметрів, що складають одне повідомлення – Тема і Блок даних. У цих групах і формується повідомлення у вигляді рядка, яке, після формування, поміщається в відповідне поле трохи нижче. Праворуч від поля повідомлення знаходяться перемикачі введення / виведення, в які і буде

відправлено сформоване повідомлення, якщо на панелі завдань буде відповідною кнопкою дозволено відправляти повідомлення відразу, після його формування. Праворуч від перемикачів розташована кнопка формування повідомлення. Повідомлення буде сформовано так само, при натисканні на кнопку "Enter" (далі - введення) в будь-якому полі заголовка і блоку даних, яке має клавіатурне введення. Нижче розташована група введення / виведення №1 і група введення / виведення №2, якщо остання дозволена в меню програми. У системному вікні програми зліва направо відображається: системний час і дата комп'ютера, параметри введення / виведення №1 і №2.

Якщо введення / виведення встановлено на COM порт, то відображається його швидкість передачі. Якщо введення / виведення встановлено на сокет, то відображається IP адреса і номер порту віддаленого пристрою.

### 4.3.4. Опис групи введення-виведення

Дана група має в складі вікно прийнятих повідомлень і терміналу. У вікні терміналу відображаються введені дані з клавіатури і прийняті дані, як є – з відображенням спец. символів. У вікні прийнятих повідомлень відображається структурована інформація службових полів отриманого повідомлення і ефективні дані, після висловлення – «Data:». В параметрах програми можна вибрати, які з службових даних будуть відображатися у вікні отриманих повідомлень. У складі цієї групи так само присутній: спадаючий список портів, кнопки відкриття і закриття порту, кнопка очищення вікна терміналу і прийнятих повідомлень, кнопка відправки повідомлення, поле оперативного введення паузи очікування відповіді на запит, після закінчення якого запит буде повторений, якщо відповідною кнопкою праворуч цей режим буде дозволений; кнопка дозволу автоматичного запиту наступних даних, якщо відповідь не вміщається в одну посилку (далі – довга відповідь). При натиснутому стані двох останніх кнопок праворуч з'являються таймера зворотного відліку заданого часу очікування, які можна скинути, натиснувши на відповідний таймер. При натисканні на кнопку «Відправити повідомлення», буде

відправлено в обраний порт або сокет попередньо сформоване повідомлення з поля, що знаходиться під групою заголовка і блоку даних. У спадаючому списку портів задіяні COM порти будуть відображатися в дужках.

### 4.3.5. Дерево функцій

Дерево функцій складається з двох основних гілок: системних функцій і функцій користувача. В системні функції входить функція установки часу з підстановкою поточного часу комп'ютера в момент побудови повідомлення і функція, призначена для розриву зв'язку модемного з'єднання. В гілку призначених для користувача функцій можна додавати наступні об'єкти: папки, функції і команди. Функції і команди можна додавати в папки. Функції можуть бути з автоматичним формуванням повідомлення і вимагають додаткового введення параметрів. Команди відрізняються від функцій тим, що відправляються в порт або сокет, як є – без формування в оболонку протоколу SCTM (ex). Якщо ім'я функції задається безпосередньо підписом відповідного об'єкта дерева функцій, то команда, яка буде відправлятися, знаходиться в описі даного об'єкта дерева функцій. Об'єкти дерева, що додаються, можуть мати свій опис (підказку) і перелік тегів для зручного їх угруповання. Відображення підказки та / або переліку тегів, при наведенні курсору миші на відповідний об'єкт дерева функцій, включається через меню програми або відповідною кнопкою на панелі управління. При запуску програми дерево функцій працює в режимі формування повідомлень при виборі відповідної функції. Для редагування об'єктів дерева необхідно вибрати відповідний пункт в меню програми. У режимі редагування стає доступним контекстне меню і можливість переміщення об'єктів дерева за допомогою відповідних кнопок на панелі управління. За допомогою контекстного меню можна створити, видалити, копіювати і вставити будь-який об'єкт гілки призначених для користувача функцій, а також редагувати опис вибраного об'єкту. В опис об'єкта дерева функцій входить підказка і перелік тегів.

### 4.3.6. Робота з тегами

Теги призначені для компактного відображення використовуваних об’єктів дерева функцій. Для кожного об’єкта може бути створено не обмежену кількість тегів. Перелік всіх тегів будь-якого об’єкта дерева функцій знаходиться у відповідному вікні опису об’єкта.

Додавання і видалення тегів можна робити безпосередньо в описі об’єкта і за допомогою контекстного меню дерева функцій. Другий спосіб дозволяє додавати і видаляти теги одночасно декількох об'єктів і забезпечує гнучкий вибір вкладеності об’єктів із зазначенням їх типів. За допомогою контекстного меню списку тегів (над деревом функцій) можна виробляти глобальні зміни тегів (перейменування і видалення).

### 4.3.7. Робота з додатками

При запуску SCTM Dialog, всі налаштування програми залишаються такими, як перед закриттям цього додатка, за винятком поля статусу, номера даних, номера квитанції і режиму відображення списків тегів в підказці дерева функцій. Зазначені поля приймають значення за замовчуванням, відповідні побудови повідомлення запиту. Режим відображення списку тегів відключено. Прі кліці миші на об’єкті функції дерева з дозволом формування повідомлення при виборі (зелена стрілочка вправо), дана функція поміщується в поле даних і автоматично відбувається формування повідомлення з усіма службовими полями і контрольними сумами. Сформоване повідомлення поміщається в відповідне поле нижче. Якщо на панелі управління дозволений режим «автоматично відправляти повідомлення при формуванні», то повідомлення буде відправлено в зазначений пункт введення / виведення, якщо в ньому буде відкритий обраний порт. Так само сформоване повідомлення може бути відправлено натисканням на відповідну кнопку будь-якого «пункту» введення / виведення. Прі кліці миші на об’єкті функції дерева без дозволу формування повідомлення при виборі, функція так само поміщається в поле даних, але автоматичної побудови повідомлення не відбувається, а курсор поміщається в

поле даних за функцією для введення необхідних даних. Даний об’єкт дерева функцій застосовується, якщо функція вимагає введення параметрів.

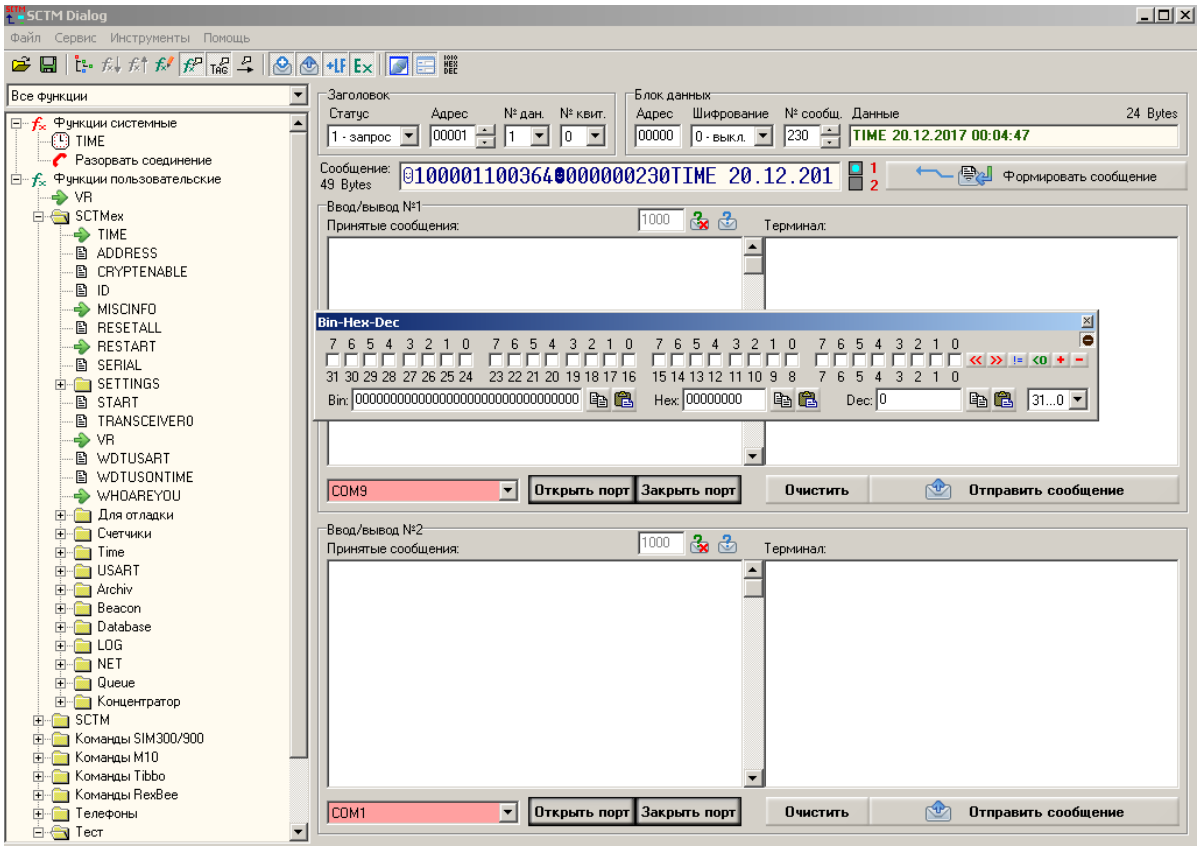



Рисунок 4.13 – Інтерфейс  SCTM Dialog

При натисканні на введення в поле даних або на кнопку «Формувати повідомлення», сформоване повідомлення буде поміщено в відповідне поле нижче і, якщо дозволено налаштуваннями, відправлено далі в зазначений порт вказаного введення-виведення. Прі кліці миші на об’єкті команди дерева функцій (синя стрілочка вправо), дана команда (яка перебуває в описі цього об’єкта) буде передана в зазначений порт вказаного вводу / виводу, як є (без оболонки SCTM протоколу). Для передачі будь-яких ASCII символів, необхідно використовувати наступну конструкцію: #hh, де # - символ, за яким розташований код переданого ASCII символу в шістнадцятковому вигляді, а hh – безпосередньо код символу. Команди, в основному, застосовуються для параметризації різного устаткування (модеми та ін.).

### 4.3.8. Робота з портами

Перед відправкою даних необхідно відкрити відповідний порт або сокет. Дані можна відправляти у вигляді повідомлення з поля «Повідомлення» шляхом натискання на відповідну кнопку в обраному «порті» введення / виведення, натисканням на кнопку «Формувати повідомлення» або натисканням на введення в будь-якому полі заголовка або блоку даних, які мають клавіатурне введення, за умови, що дозволена в настройках програми автоматична відправка повідомлення при формуванні, а також в порт відправляються всі введені дані у вікні терміналу. Всі отримані повідомлення через COM порт або сокет з обраним протоколом SCTM будуть розкладені на складові (дані системних полів і ефективні дані) і будуть відображені у вікні «Отримані повідомлення» відповідного введення/виведення. Необхідні дані системних полів для відображення можна вибрати в параметрах програми. При використанні сокета з протоколом HTTP, прийняті дані будуть відображені, як є, у вікні отриманих повідомлень. Якщо натиснути на введення в вікні «Повідомлення» при обраному сокеті з протоколом SCTM, то повідомлення відправитися в тому вигляді, як є, а якщо обраний протокол HTTP то в кінець повідомлення буде додано символ повернення каретки.

### 4.3.9. Синхронізація часу

У даній програмі здійснена можливість синхронізації часу сервера і комп’ютера, на якому запущена програма SCTM Dialog. Для цього необхідно відкрити відповідний сокет і в головному меню програми вибрати пункт – «Скорегувати час по серверу».

Після цього в сокет буде відправлений рядок, що вказано в налаштуваннях програми, як «рядок запиту часу з сервера». Якщо відповідь сервера буде відповідати допустимим значенням часу, то час в комп’ютері буде переведено на отриманий від сервера.

### 4.3.10. Вікно параметрів

Вікно параметрів SCTM Dialog містить наступні вкладки: отримані повідомлення, Порт, Socket, Налаштування та Загальні.

На вкладці прийнятих повідомлень здійснюється вибір тих параметрів (системних полів оболонки протоколу), які необхідно відображати при отриманні повідомлення. Вкладка «Порт» містить налаштування COM порту за відповідним веденням/виведенням і кількість використовуваних портів.

За допомогою вкладки "Socket" здійснюється додавання, видалення і редагування використовуваних сокетів. Для кожного сокета вказується протокол, який буде використовуватися при відправленні й одержанні повідомлень.

## 4.4. Висновки до четвертого розділу

1. Підбір та оптимізація протоколу з метою його інкапсулювання в стек ZigBee є визначальним з точки зору вирішення завдань і досягнення цілей дисертаційної роботи.
2. З огляду на, що стандарт IEC-60870-5 розроблявся для дротових мереж, його імплементація для роботи в радіомережах стандарту 802.15.4/ZigBee зажадала модифікації для забезпечення надійної роботи пристроїв в бездротових мережах складної архітектури. З цією метою протокол був модифікований на канальному рівні. Розширення канального рівня виконано за рахунок рівня додатків і містить додаткові службові дані, необхідні для збільшення надійності, достовірності та моніторингу повідомлень в умовах бездротової передачі даних.
3. Експериментальна експлуатація системи «Smart Utility Web» показала коректність підходу до побудови бездротової системи моніторингу на основі технології «роутерів, що прокидаються». Простота інсталяції (Додаток В) обладнання системи і надійність захисту даних забезпечує високий рівень достовірності даних та експлуатаційних характеристик.

Управління розміром блоків даних і шифруванням на рівні користувальницького додатка дозволяє домогтися оптимального, з точки зору терміну життя системи, енергоспоживання при збереженні необхідного рівня якості обслуговування.

4. Внесення початкових налаштувань на місці установки польового пристрою здійснюється за допомогою спеціально розробленого термінального пристрою «Інсталлер». Дистанційне керування польовими пристроями здійснюється через розроблену за участю дисертанта програму параметризації «SCTM-Dialog» (п.4.3.).

Основні результати розділу опубліковано в роботах автора [37, 90, 92, 96, 97, 99, 101, 103, 104].

# ВИСНОВКИ

В дисертаційному дослідженні розв’язано важливу науково-прикладну задачу підвищення якості функціонування бездротових сенсорних мереж енергомоніторингу та збільшення часу їх життя за рахунок розробки відповідних математичних моделей і методів дослідження режимів енергоспоживання. У роботі запропоновано новий підхід до вирішення проблеми енергозбереження в сенсорних мережах енергомоніторингу, що дозволяє одночасно скоротити енергоспоживання мережевих пристроїв і час доставки повідомлень.

Отримано наступні основні результати, які мають наукову новизну та практичну цінність:

1. Проведений аналіз досліджень в області побудови розподілених автономних бездротових систем моніторингу показав, що БММ є перспективною технологією в області створення побутових і промислових систем збору даних і управління, а ключовим показником БСМ, визначальним їх застосовність на практиці, є час їхнього життя. За результатами проведеного аналізу обґрунтовано необхідність розробки математичних моделей і методів дослідження режимів енергоспоживання з метою збільшення часу життя автономних БММ.
2. Системно обґрунтовано, що використання керованих «роутерів, що прокидаються» в якості польових пристроїв БММ є одним з найбільш перспективних методів збільшення часу життя комірчастої мережі. З огляду на енергоємність процесу передачі даних, саме управління розмірами повідомлень є основним резервом збільшення терміну життя пристроїв і системи в цілому, а оптимізація енергоспоживання польових пристроїв бездротової мережі з автономним живленням на рівні користувальницького додатка, дозволяє застосовувати приймо-передавачі різних виробників в пристроях збору і передачі даних.

3. На підставі проведеного аналізу сформульована задача розробки бездротової системи моніторингу з автономним живленням, що володіє гарантованим терміном життя зі забезпеченням захищеності інформації, переданої в публічних мережах передачі даних. З огляду на необхідність розробки системи енергомоніторингу сформульовані вимоги до програмного забезпечення рівня користувальницького додатка.
4. Вперше розроблено математичну модель функціонування великомасштабних мереж на базі запитів БСМ, чиї вузли виявляють і ретранслюють події, які потрібні тільки протягом обмеженого часу. Це дозволило підвищити точність оцінки затримок передачі даних, розрахунку енергоємності та терміну служби мережі.
5. Удосконалено математичну модель оцінки працездатності польових пристроїв з автономним живленням і модернізовано архітектуру системи, в результаті чого час життя системи перевищив нормативний період повірки приладів обліку.
6. Вперше запропоновано механізм динамічної адресації польових пристроїв бездротової Інтернет-системи збору даних і управління енергоспоживанням, що унеможливлює віддалене стороннє втручання в роботу сегментів системи.
7. Вперше модифіковано протокол SCTMex, який інкапсульовано в транспортні протоколи ZigBee і LoRa, що дозволило підвищити рівень захисту інформації на рівні польових пристроїв системи.
8. Розроблено спеціалізовану програмно-апаратну платформу «Smart Utility Web» на базі бездротового модуля XBEE S2. Експериментальна експлуатація системи показала коректність підходу до побудови бездротової системи моніторингу на основі технології «роутерів, що прокидаються». Простота інсталяції обладнання системи і надійність захисту даних забезпечує високий рівень достовірності даних та експлуатаційних характеристик. Управління розміром блоків даних і шифруванням на рівні користувальницького додатка дозволяє домогтися

оптимального з точки зору терміну життя системи енергоспоживання при збереженні необхідного рівня якості обслуговування.

9. Аналіз стійкості бездротових мереж моніторингу до зовнішніх атак вказав на їх критичну уразливість, обумовлену централізованою архітектурою, тому найбільш дієвим і ефективним механізмом захисту інформації в бездротових мережах моніторингу є перехід до децентралізованих систем, зокрема побудованих на принципах технології блокчейн. Зроблено висновок, що найбільш прийнятним рішенням для БСМ є сервісний або приватний блокчейн, що дозволяє проводити ідентифікацію польових пристроїв під контролем призначених користувачів.
10. Результати роботи впроваджені в навчальний процес Національного технічного університету «Дніпровська політехніка» та ряді організацій різних форм власності.

# СПИСОК ПОСИЛАНЬ

1. A Framework for Assessing and Improving the Security Posture of Industrial Control Systems (ICS) and Network Analysis Center Released: August 20, 2010 Version:1.1. National Security Agency, USA.

2. Ayadi H., Zouinkhi A., Val T., Bassche A., Abdelkrim M. N. Network lifetime management in wireless sensor networks. IEEE Sensors Journal, vol. 18, no. 15, pp. 6438-6445, 2018.

3. Babenko T., Toliupa S., Kovalova Y. LVQ models of DDOS attacks identification. 14 th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), Lviv, 2018, pp. 510-513, doi: 10.1109/TCSET.2018.8336253.

4. Balen J., Zagar D., Martinovic G. Quality of service in wireless sensor networks: a survey and related patents // Recent Patents on Computer Science. 2011. V.4. P. 188–202.

5. Benoît Latré, Pieter De Mil, Ingrid Moerman, Bart Dhoedt and Piet Demeesterю Throughput and Delay Analysis of Unslotted IEEE 802.15.4, Journal of networks, vol. 1, no. 1, May 2006.

6. Bha, G.; Sreenivasan A. Review on energy optimization and cluster based routing protocol in WSN. Int. Res. J. Eng. Technol. (IRJET) 2019, 6, 101–103.

7. Bouabdallah F., Bouabdallah N. The Tradeoff Between Maximizing the Sensor Network Lifetime and the Fastest Way to Report Reliably an Event Using Reporting Nodes' Selection. Computer Communications Journal (Elsevier), Vol. 31, Issue 9, pp. 1763 – 1776, June 2008.

8. Bougard Catthoor Bruno, Daly Francky, Denis C., Chandrakasan Anantha, Dehaene Wim. Energy Efficiency of the IEEE 802.15.4 Standard in Dense Wireless Microsensor Networks: Modeling and Improvement Perspectives // Proceedings of the Design, Automation and Test in Europe Conference and Exhibition (DATE'05) Munich, Germany, 2005; pp.196-201.

9. Casilari Eduardo, Cano-García Jose M. and Campos-Garrido Gonzalo. Modeling of Current Consumption in 802.15.4/ZigBee Sensor Motes// Sensors 2010, 10, 5443-5468; доступ: www.mdpi.com/journal/sensors.

10. CEN-CENELEC-ETSI Smart Grid Coordination Group. Smart Grid Reference Architecture; 2012. [Online] Available at: https://ftp.cencenelec.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/FrameworkDocument.pdf

11. Chakeres Ian D., Belding-Royer Elizabeth M.: AODV Routing Protocol Implementation Design. http://moment.cs.ucsb.edu/pub/wwan_chakeres_i.pdf

12. Chen D., Varshney P. K. QoS Support in Wireless Sensor Networks: A Survey // Proc. of the 2004 International Conference on Wireless Networks (ICWN 2004), Las Vegas, Nevada, USA. 2004. P. 227–233.

13. Chen J. et al. “Rapidly-Exploring Tree With Linear Reduction : A Near-Optimal Approach for Spatiotemporal Sensor Deployment in Aquatic Fields Using Minimal Sensor Nodes. IEEE Sens. J., vol. 18, no. 24, pp. 10225–10239, 2018.

14. CSN EN 13757-4 -2013 Communication systems for meters and remote reading of meters - Part 4: Wireless meter readout (Radio meter reading for operation in SRD bands) –[Электронный ресурс]. Доступ: https://www.en-standard.eu/csn-en-13757-4-communication-systems-for-meters-and-remote-reading-of-meters-part-4-wireless-meter-readout-radio-meter-reading-for-operation-in-srd-bands/. (Дата звернення: 11.2017).

15. Del-Valle-Soto C., Mex-Perera C., Nolazco-Flores J. A., Velázquez R., & Rossa-Sierra A. (2020). Wireless Sensor Network Energy Model and Its Use in the Optimization of Routing Protocols. Energies, 13(3), 728. doi:10.3390/en13030728

16. Demirkol I., Ersoy C. and Alagoz F. MAC Protocols for Wireless Sensor Networks: A Survey. IEEE Communication Magazine, Vol. 44, No. 4, April 2006, pp. 115-121.

17. Dunlop J., Smith D.G. Telecommunications Engineering. 3rd edition, p.508. Cheltenham, 1994.

18. EmberZNet Application Developer's Guide, 21 July, 2008, http://www.wless.ru/files/ZigBee/EM260/120-4028-000_EmberZNetAppDevGuide.pdf

19. Energy Futures Initiative. Policy paper Promising Blockchain Applications for Energy: Separating the Signal from the Noise JULY 2018:- 900 17 TH ST. NW, SUITE 1100, WASHINGTON, D.C. 2006

20. Ergen S.C., Varaiya P. Energy Efficient Routing with Delay Guarantee for Sensor Networks, ACM Wireless Networks Journal, 13(5):679-690, October 2007.

21. EWEA: Wind in Power 2015 European Statistics. Available online: https://windeurope.org/wp-content/uploads/files/about-wind/statistics/EWEA-Annual-Statistics-2015.pdf (accessed on 15 November 2017).

22. Guerrero, J.M.; Chandorkar, M.; Lee, T.L. Advanced control architectures for intelligent microgrids – Part I:Decentralized and hierarchical control. Trans. Ind. Electron. 2014, 60, 1254–1262.

23. Gun M., Kosar R., Ersoy C. Lifetime optimization using variable battery capacities and nonuniform density deployment in wireless sensor networks // Computer and information sciences, 2007. iscis 2007. 22nd international symposium on. 2007. P. 1–6.

24. Halder S., Ghosal A., Chaudhuri A., DasBit S. A probability density function for energy-balanced lifetime-enhancing node deployment in WSN // Proceedings of the 2011 international conference on Computational science and its applications - Volume Part IV. ICCSA'11. Berlin, Heidelberg: Springer-Verlag, 2011. P. 472–487.

25. Hatziargyriou, N. (Ed.) Microgrids: Architectures and Control; Wiley/IEEE Press: Hoboken, NJ, USA, 2014;ISBN 978-1-118720-68-4.

26. Horalek, Josef & Sobeslav, Vladimir. (2015). Analysis of communication protocols for smart metering. ARPN Journal of Engineering and Applied Sciences. 10. 1438-1446.

27. Hossain E., Leung K. Wireless Mesh Networks Architectures and Protocols // Springer. 2007.

28. Huang Yu-Kai, Kuo Chin-Fu, Pang Ai-Chun, and Zhuang Weihua. Stochastic Delay Guarantees in ZigBee Cluster-Tree Networks. IEEE International Conference on Communications (ICC) 2012.

29. Hui J. W., Culler D. The dynamic behavior of a data dissemination protocol for network programming at scale. In SenSys '04: Proceedings of the 2nd international conference on Embedded networked sensor systems, pages 81-94, New York, NY, USA, 2004. ACM.

30. IEEE 802.15.4d-2009 standard [Електронний ресурс] / Institute of Electrical and Electronics Engineers. 2009. Доступ: http://standards.ieee.org/ getieee802/download/802.15.4d-2009.pdf (дата звернення: 10.2010).

31. IEEE-TG15.4 (2006). Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for low-rate Wireless Personal Area Networks (LR-WPANs). IEEE standard for information technology, 2006.

32. Ishtiaq Rouf, Hossen Mustafa, Miao Xu, Wenyuan Xu, Rob Miller: Neighborhood Watch: Security and Privacy Analysis of Automatic Meter Reading Systems.- Proceeding CCS '12 Proceedings of the 2012 ACM conference on Computer and communications security. Pages 462-473 . ACM New York, USA, 2012.

33. Iturri P. L., Aguirre E., Azpillicueta L., and Astrain J.J. Implementation and analysis of ISM 2.4 GHz wireless sensor network systems in Judo training venues," in Sensors, vol. 16 (8), 2016.

34. Jesus G., Casimiro A., and Oliveira A. A survey on data quality for dependable monitoring in wireless sensor networks. Sensors, vol. 17 (9), 2017.

35. Karavas C.S.; Kyriakarakos G.; Arvanitis K.G.; Papadakis G. A multi-agent decentralized energy management system based on distributed intelligence for the design and control of autonomous polygeneration microgrids. Energy Convers. Manag. 2015, 103, 166–179.

36. Kathryn Cave. The IoT “time bomb” report: 49 security experts share their views.- http://www.idgconnect.com/abstract/12744/the-iot-bomb-report-49-security-experts-share-views

37. Kovaleva Yuliia, Babenko Tetiana, Ignisca Vira. Models And Methods Of Wireless Decentralized Networks for Energy Monitoring of Critical Infrastructure Facilities. Scientific and practical cyber security journal. Georgia. Issue No: 4, December, 2020. P.74-78. ISSN: 2587-4667.

38. Kovalova Y., Babenko T. The Discrete Model of Dynamic Energy Systems and Reliability of Data Consumption. VI MIĘDZYNARODOWA KONFERENCJA STUDENTÓW ORAZ DOKTORANTÓW «INŻYNIER XXI WIEKU». Bielsko-Biała, 2016. P. 181-184. ISBN 978-83-65182-51-7.

39. Kovalova Y., Babenko T. The representative of national problems in the field of cybersecurity. Power engineering and information technologies in technical objects control. / London: Taylor & Francis Group: CRC Press / Balkema. London, UK 2016. P. 151-155. DOI: https://doi.org/10.1201/9781315197814.

40. Kovalova Y., Babenko T., Oksiiuk O., Myrutenko L. Optimization of Lifetime In Wireless Monitoring Networks. International Journal of Computing. Research Institute for Intelligent Computer Systems, 2020 № 19 (2), Pp. 267–272. ISSN: 2312-5381.

41. Kovalova Y., Mieshkov V. Information protection in communication networks. Virtual conference «Information Technologies in Science & Education», India, Ukraine, Spain, Italy.

42. Kovalova Y., Oksiiuk O., Babenko T. The Optimization of Lifetime in Wireless Monitoring Network. The 4th IEEE International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems. Lviv Polytechnic National University. Lviv 20-21 September 2018.

43. Krebs on Security. 01 Source Code for IoT ‘Mirai’ Released / https://krebsonsecurity.com/2016/10

44. Kurt, S.; Yildiz, H.U.; Yigit, M.; Tavli, B.; Gungor, V.C. Packet size optimization in wireless sensor networks for smart grid applications. IEEE Trans. Ind. Electron. 2017, 64, 2392–2401.

45. Kwon H., Seo H., Kim S., Lee B. G. Generalized CSMA/CA for OFDMA systems: protocol design, throughput analysis, and implementation issues // Wireless Communications, IEEE Transactions on. 2009. Vol. 8, no. 8. P.p.4176–4187.

46. Lee Thomas, Chao Long, Pete Burnap, Jianzhong Wu, Nick Jenkins. Automation of the supplier role in the GB power system using blockchain-based smart contracts.- CIRED, Open Access Proc. J., 2017, Iss. 1, pp. 2619–2623.

47. Marcelo Manjon. A framework to help make sense of cybersecurity tools.- 17.01.2017 http://www.networksasia.net/article/framework-help-make-sense-cybersecurity-tools.1433516707).

48. Mauri G. et al. State-of-the-Art Technologies & Protocols – Description of State-of-the-Art Comm. Protocols and Data Structures: D 2.1/Part 4. Jun 2009.

49. Mišić J. Traffic and energy consumption of an IEEE 802.15.4 network in the presence of authenticated, ECC Diffie-Hellman ephemeral key exchange. Comput. Netw. 2008, 52, 2227-2236.

50. Nassef L., Elhebshi R., and Jose L. Evaluating performance of Wireless Sensor Network in realistic smart grid environment. International Journal of Wireless & Mobile Networks (IJWMN), vol. 10, no. 3, 2018.

51. Othman F., Bouabdallah N., Boutaba R. Load-Balanced Routing Scheme for Energy-Efficient Wireless Sensor Networks. IEEE GLOBECOM 2008, New Orleans, LA, USA, December 2008.

52. Ouni, S., & Trabelsi Ayoub, Z. (2013). Predicting Communication Delay and Energy Consumption for IEEE 802.15.4/Zigbee Wireless Sensor Networks. International Journal of Computer Networks & Communications, 5(1), 141–152. doi:10.5121/ijcnc.2013.5110

53. Perkins C. Ad hoc On-Demand Distance Vector (AODV) Routing/C.E. Perkins, C.E. Belding-Royer // RFC 3561. - July 2003.

54. Pop Claudia, Cioara Tudor, Antal Marcel, and etc. Blockchain Based Decentralized Management of Demand Response Programs in Smart Energy Grids: Sensors 2018, 18, 162; doi:10.3390/s18010162 pp. 1-21 Доступ: www.mdpi.com/journal/sensors.

55. Protocol: Landis & Gyr - SCTM Communication. - LIAN 98 Protocol Router, Simulator and Analyzer© Copyright 2001, 2006, 2011 by Werner Mayr.

56. Ramassamy C., Fouchal H., Hunel P. Impact of application layers over wireless sensor networks // Lecture Notes in Informatics. Bonn, Germany. 2012.

57. RF-модули _XBee Series 2 OEM - _ZigBee - _v1.x2x [2007.07.019] 90000866_B © 2007 _Digi International, Inc.

58. Sagirlar Gokhan, Carminati Barbara, Ferrari Elena, Sheehan John D., Ragnoli Emanuele. Hybrid-IoT: Hybrid Blockchain Architecture for Internet of Things - PoW Sub-blockchains.- IEEE International Conference on Blockchain (Blockchain-2018), July 30 - August 03, 2018 Halifax, Canada https://arxiv.org/abs/1804.03903.

59. Sofiane Ouni, Salsabil Gherairi, Farouk Kamoun. Real-time quality of service with delay guarantee in sensor networks. International Journal of Sensor Networks, Volume 9 Issue 1, 2011.

60. Sofiane Ouni, Zayneb Trabelsi Ayoub. Predicting communication delay and energy consumption for ieee 802.15.4/zigbee wireless sensor networks.- International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.1, January 2013. Pp. 141-152

61. Szabo N.: ‘The god protocols’. Available at https://web.archive.org/web/20160306022606/http://szabo.best.vwh.net/msc.html, accessed on 07 September 2018.

62. The Value of the Engaged Energy Consumer, Quantifying theValue of Strong Customer Relationshipsfor European Utilities. Available online: http://energypost.eu/wp-content/uploads/2014/12/COM-WP_Value-CE-EMEA-141017-PRINT-2.pdf (accessed on 2 September 2018).

63. Trevisan Jefferson Antonio Zeni, Mariano Andre´ Augusto, Ribeiro Eduardo Parente / Average Power Consumption Model For Wireless Sensor Networks.- Universidade Federal do Paraná. Av. Coronel Francisco Heráclito dos Santos, 210. Curitiba - PR - 81531-970 - Brazil. Доступ: www.inatel.br/.../82-averagepowerconsumptionmodelforwir...

64. Trigunait C.K.; Prabha S. A Novel Energy Efficient Security Protocol In WSN. Int. J. Inf. Technol. (IJIT) 2019, 5, 1–4.

65. Vullers R., van Schaijk R., Doms I. et al. Micropower energy harvesting // Solid-State Electronics. 2009. Vol. 53, no. 7. P. 684 – 693.

66. Wang Y., Liu X., Yin J. Requirements of quality of service in wireless sensor network // Proceedings of the International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies. Washington, DC, USA. 2006.

67. What is Hyperledger Fabric? URL: https://www.ibm.com/blockchain/hyperledger (дата звернення: 15.11.2017).

68. XCTU-Next Generation Configuration Platform for XBee/RF Solutions.- Доступ: https://www.digi.com/products/xbee-rf-solutions/xctu-software/xctu

69. Xia F. QoS challenges and opportunities in wireless sensor/actuator networks // Sensors. 2008. V. 8. № 2. P. 1099–1110.

70. Zhang H., Shen H. Balancing Energy Consumption to Maximize Network Lifetime in Data-Gathering Sensor Networks // IEEE Trans. Parallel Distrib.Syst. 2009. Vol. 20, no. 10. P. 1526–1539.

71. Zhang Z., Mehmood A., Shu L., Huo Z., Zhang Y., Mukherjee M. A survey on fault diagnosis in wireless sensor networks. IEEE Access, vol. 6, pp. 11349-11364, 2018.

72. Zhang, F.; Zhou, H.; Zhou, X. A routing algorithm for ZigBee network based on dynamic energy consumption decisive path. In Proceedings of International Conference on Computational Intelligence and Natural Computing (CINC’09), Wuhan, China, June 2009; pp. 429-432.

73. Zhang, Y.; Xu, P.; Bi, G.; Bao, F.S. Analysis of energy efficiency and power saving in IEEE 802.15.4. In Proceedings of Wireless Communications and Networking Conference (WCNC 2007), Hong Kong, China, March 2007; pp. 3330-3334.

74. ZigBee Alliance. ZigBee Specification. Q4/2007 // www.zigbee.org/en/spec_download/ zigbee_downloads.asp

75. ZigBee specification overview [Електронный ресурс] / ZigBee Alliance. 2012. Дост: http://www.zigbee.org/Specifications/ZigBee/Overview. aspx (дата обращения: 10.2012).

76. Бабенко Т.В., Толюпа С.В., Ковальова Ю.В. Моделі ідентифікації мережевих аномалій на основі карти самоорганізації. VII міжнародна науково-технічна конференція «ITSEC». Київ, 16 травня 2017.

77. Галимов Р.Р. Вопросы безопасности беспроводной сенсорной сети распределенной системы управления технологическими объектами нефтегазодобычи.: НАУКА И СОВРЕМЕННОСТЬ – 2013, с.137-143.

78. Гианнетсос Т. Беспроводные сети как оружие: Утилита для совершения атак против сенсорных сетей [Электронный документ] / Танассис Гианнетсос, Тассос Димитриоу, Неели Р. Прасад. – Режим доступа: http://www.securitylab.ru/analytics/406876.php.

79. Доколяса О.С., Ковальова Ю.В. Кібербезпека в інформаційному просторі України. Збірник матеріалів доповідей та тез. П’ята всеукраїнська науково-технічна конференція студентів, аспірантів і молодих учених «Молодь: наука та інновації 2017». Національний технічний університет «Дніпровська політехніка», м. Дніпро, 2017. Т.12. С.34-35.

80. Евдокимов Е.В. Сравнение топологий беспроводных сенсорных сетей // Вестник компьютерных и информационных технологий. – 2008. – № 8. – С. 240.

81. Ефремов Сергей Геннадьевич. Моделирование времени жизни динамически реконфигурируемых сенсорных сетей с мобильным стоком.- Диссертация на соискание ученой степени кандидата технических наук /.- Москва, 2013.

82. Золотарев С.В. Некоторые особенности реализации стандарта IEC-60870-5-104 в системе программирования контроллеров ISAGRAF: от теории к практике.- Журнал “ИСУП” № 4(28)_2010, с.36-31.

83. Ковальова Ю.В., Бабенко Т.В. Аналіз вразливостей інтелектуальних лічильників в бездротовій мережі моніторингу енергоресурсів. Київський національний університет імені Тараса Шевченка, Збірник матеріалів доповідей

та тез І Міжнародна науково-практична конференція «Проблеми кібербезпеки інформаційно-телекомунікаційних систем». М. Київ 5-6 квітня 2018. С. 24-26.

84. Ковальова Ю.В., Бабенко Т.В. Застосування технології блокчейн в енергетичних системах. VII Міжнародна науково-практична конференція «Фізико-технологічні проблеми передавання, оброблення та зберігання інформації в інфокомунікаційних системах». М. Чернівці, 8-10 листопада 2018.

85. Ковальова Ю.В., Бабенко Т.В. Нейромережеві моделі ідентифікації DDoS атак. XX Міжнар. науково-практ. конференція «Безпека інформації в інформаційно-телекомунікаційних системах», Буча, 22-24 травня 2018.

86. Ковальова Ю.В. Інформаційна безпека бездротових мереж моніторингу. Збірник матеріалів доповідей та тез. П’ята всеукраїнська науково-технічна конференція студентів, аспірантів і молодих учених «Молодь: наука та інновації 2017». Національний технічний університет «Дніпровська політехніка», м. Дніпро, 2017. Т.12. С.40-42.

87. Ковальова Ю.В. Математичне моделювання процесу бездротової передачі даних в мережах енергомоніторингу. «Системні технології». м. Дніпро, 6 (131) 2020. С.186-195. ISSN: 1562-9945.

88. Ковальова Ю.В. Моделі ідентифікації мережевих аномалій на основі карти самоорганізації. Збірник матеріалів доповідей та тез VII міжнародної науково-технічної конференції «ITSEC», м. Київ 2017.

89. Ковальова Ю.В. Моделювання топології бездротових сенсорних мереж. Регіональний міжвузівський збірник наукових праць «Системні технології», м. Дніпро, 1 (132) 2021. С.92-98. ISSN: 1562-9945.

90. Ковальова Ю.В. Особливості використання протоколу SCTM в інтелектуальних мережах Smart Grid. Збірник матеріалів доповідей та тез XVIII Міжнародної науково-практичної конференції «Безпека інформації у інформаційно-телекомунікаційних системах», м. Київ, 2016, стор. 54.

91. Ковальова Ю.В. Проблеми в сфері забезпечення кібернетичної безпеки об’єктів критичної інфраструктури. Збірник матеріалів доповідей та тез VII Науково-практична конференція «Актуальні проблеми управління інформаційною безпекою держави», м. Київ 2016.

92. Ковальова Ю.В. Технологические аспекты беспроводных сетей мониторинга. «Innovative Technologies in the Formation and Development of Human Capital», Вища Технічна Школа, м. Катовіца, Польша, 2018. С. 27-37.

93. Ковальова Ю.В., Бабенко Т.В. Забезпечення кібербезпеки об'єктів енергетичної інфраструктури. Збірник матеріалів доповідей та тез II науково-практична конференція «Проблеми безпеки інформаційно-телекомунікаційних систем», м. Київ, 23-24 березня 2017. С. 121-123.

94. Ковальова Ю.В., Бабенко Т.В. Нейромережеві моделі ідентифікації DDoS атак. Збірник матеріалів доповідей та тез XX Міжнародної науково-практичної конференції «Безпека інформації в інформаційно-телекомунікаційних системах», м. Буча, 2018. С. 32-33.

95. Кручінін О.В., Тимофєєв Д.С., Ковальова Ю.В. Інформаційна безпека бездротових мереж моніторингу. Збірник матеріалів доповідей та тез XX Міжн. науково-практ. Конф. «Безпека інформації в інформаційно-телекомунікаційних системах», м. Буча, 2018. С. 247.

96. Почта Ю. Новітні технології у сфері ЖКГ. Вісник Дніпропетровської міської ради. М. Дніпропетровськ 2009 №009.

97. Почта Ю. Управление энергоресурсами на базе беспроводных технологий передачи данных. VIII mezinarodni vedecko-prakticka conference "Moderni vymozenosti vedy", Publishing House "Education and Science", Praha, 27 січня – 5 лютого 2012. С. 78-81. ISBN: 978-966-8736-05-6

98. Почта Ю.В. Захист та впровадження бездротових систем моніторингу, II Всеукраїнська науково-практична конференція «Системний аналіз. Інформатика. Управління. САІУ-2011, м. Запоріжжя, 10-11 березня 2011. С. 162-163.

99. Почта Ю.В. Интеллектуальные информационно-управляющие системы водоснабжения и водопотребления. Регіон. міжвузівський збірник наукових праць «Системні технології», м. Дніпропетровськ, 2013, №3'(86). С.93-96.

100. Почта Ю.В. Интеллектуальные информационно-управляющие системы. Научно-техническая конференция «Информационные технологии в

металлургии и машиностроении. ІТММ-2013», м. Дніпропетровськ, 26-28 березня 2013.

101. Почта Ю.В., Бабенко Т.В. Water supply systems in settlements of Ukraine. Науковий вісник НГУ, м. Дніпропетровськ, 2012 № 2. С. 105-108. ISSN: 2071-2227.

102. Почта Ю.В., Кузнецов Г.В. Исследование беспроводной технологии ZigBee в области защиты информации. V miedzynarodowej naukowi-praktycznej konferecji «Europejska nauka XXI powieka», Przemysl, 5-15 травня 2009. С. 60-61. ISBN: 978-966-8736-05-6.

103. Почта Ю.В., Ленда І.В. Интеллектуальные системы энергоучета. Журнал «Мир Автоматизации», м. Київ №2, 2010. С. 48-51.

104. Почта Ю.В., Система дистанционного считывания показаний и управления энергопотреблением «EnergyWeb-XB». Международный электротехнический журнал «Электрик», м. Київ, 2009 №9. С. 31-33.

105. Пушкарев О. Передача данных в ZigBee-сети с помощью модулей XBee ZNet 2.5.- НОВОСТИ ЭЛЕКТРОНИКИ №3, 2008. С.27-31.

106. Семенов Ю.А. (ИТЭФ-МФТИ) Беспроводные сети ZigBee и IEEE 802.15.4. Доступ: http://book.itep.ru/1/intro1.htm (дата обращения : 10.2016)

107. Твердохліб І.С., Ковальова Ю.В. Управління інцидентами кібербезпеки на малих комерційних підприємствах. Збірник матеріалів доповідей та тез. П’ята всеукр. науково-технічна конф. студентів, аспірантів і молодих учених «Молодь: наука та інновації 2017», м. Дніпро, 2017. Т.12. С.9-10.

108. Технологии распределенных баз данных (DLT).-IOSCO Research Report on Financial Technologies (Fintech), February 2017, p.p.1-21

109. Фокин Григорий Алексеевич. Управление самоорганизующимися пакетными радиосетями на основе радиостанций с направленными антеннами./Автореферат диссертации на соискание ученой степени кандидата технических наук. Санкт-Петербург, 2009.

110. Целевая группа Smart Grid – отчет EG1, «Взаимодействие, стандарты и функциональные возможности, применяемые в крупномасштабном развертывании интеллектуального учета», октябрь 2015 г.

# ДОДАТОК А
# СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. **Почта Ю.В.,** Бабенко Т.В. Water supply systems in settlements of Ukraine. Науковий вісник НГУ, м. Дніпропетровськ, 2012 № 2. С. 105-108. ISSN: 2071-2227.

2. **Почта Ю.В.** Интеллектуальные информационно-управляющие системы водоснабжения и водопотребления. Регіональний міжвузівський збірник наукових праць «Системні технології», м. Дніпропетровськ, 2013, №3’(86). С.93-96. ISSN: 1562-9945.

3. **Kovalova Y.**, Babenko T., Oksiiuk O., Myrutenko L. Optimization of Lifetime In Wireless Monitoring Networks. International Journal of Computing. Research Institute for Intelligent Computer Systems, 2020 № 19 (2), Pp. 267–272. ISSN: 2312-5381.

4. **Ковальова Ю.В.** Математичне моделювання процесу бездротової передачі даних в мережах енергомоніторингу. Регіональний міжвузівський збірник наукових праць «Системні технології». м. Дніпро, 6 (131) 2020. С.186-195. ISSN: 1562-9945.

5. **Ковальова Ю.В.** Моделювання топології бездротових сенсорних мереж. Регіональний міжвузівський збірник наукових праць «Системні технології», м. Дніпро, 1 (132) 2021. С.92-98. ISSN: 1562-9945.

6. **Kovaleva Yuliia**, Babenko Tetiana, Ignisca Vira. Models And Methods Of Wireless Decentralized Networks for Energy Monitoring of Critical Infrastructure Facilities. Scientific and practical cyber security journal. Georgia. **Issue No:** 4, December, 2020. P.74-78. ISSN: 2587-4667.

7. ***Kovalova Y.***, *Babenko T.* The representative of national problems in the field of cybersecurity. Power engineering and information technologies in technical objects control. / London: Taylor & Francis Group: CRC Press / Balkema. London, UK 2016. P. 151-155. DOI: https://doi.org/10.1201/9781315197814.

8. Ковальова Ю.В. Технологические аспекты беспроводных сетей мониторинга. Монографія «Innovative Technologies in the Formation and

Development of Human Capital», Вища Технічна Школа, м. Катовіца, Польша, 2018. С. 27-37.

9. **Почта Ю.В.**, Система дистанционного считывания показаний и управления энергопотреблением «EnergyWeb-XB». Международный электротехнический журнал «Электрик», м. Київ, 2009 №9. С. 31-33.

10. **Почта Ю.В.**, Ленда І.В. Интеллектуальные системы энергоучета. Журнал «Мир Автоматизации», м. Київ №2, 2010. С. 48-51.

11. Babenko T., Toliupa S., **Kovalova Y.** LVQ models of DDOS attacks identification. 14 th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), Lviv, 2018, pp. 510-513, doi: 10.1109/TCSET.2018.8336253.

12. **Почта Ю.В.** Захист та впровадження бездротових систем моніторингу, ІІ Всеукраїнська науково-практична конференція «Системний аналіз. Інформатика. Управління. САІУ-2011, м. Запоріжжя, 10-11 березня 2011. С. 162-163.

13. **Kovalova Y.**, Oksiiuk O., Babenko T. The Optimization of Lifetime in Wireless Monitoring Network. The 4th IEEE International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems. Lviv Polytechnic National University. Lviv 20-21 September 2018.

14. Бабенко Т.В., Толюпа С.В., **Ковальова Ю.В.** Моделі ідентифікації мережевих аномалій на основі карти самоорганізації. VII міжнародна науково-технічна конференція «ITSEC». Київ, 16 травня 2017.

15. **Ковальова Ю.В.**, Бабенко Т.В. Аналіз вразливостей інтелектуальних лічильників в бездротовій мережі моніторингу енергоресурсів. Київський національний університет імені Тараса Шевченка, Збірник матеріалів доповідей та тез І Міжнародна науково-практична конференція «Проблеми кібербезпеки інформаційно-телекомунікаційних систем». М. Київ 5-6 квітня 2018. С. 24-26.

16. **Ковальова Ю.В.**, Бабенко Т.В. Нейромережеві моделі ідентифікації DDoS атак. ХХ Ювілейна Міжнародна науково-практична конференція «Безпека інформації в інформаційно-телекомунікаційних

системах», Буча, 22-24 травня 2018.

17. **Ковальова Ю.В.**, Бабенко Т.В. Застосування технології блокчейн в енергетичних системах. VII Міжнародна науково-практична конференція «Фізико-технологічні проблеми передавання, оброблення та зберігання інформації в інфокомунікаційних системах». М. Чернівці, 8-10 листопада 2018.

18. **Kovalova Y.**, Babenko T. The Discrete Model of Dynamic Energy Systems and Reliability of Data Consumption. VI MIĘDZYNARODOWA KONFERENCJA STUDENTÓW ORAZ DOKTORANTÓW «INŻYNIER XXI WIEKU». Bielsko-Biała, 2016. P. 181-184. ISBN 978-83-65182-51-7.

19. **Почта Ю.В.**, Кузнецов Г.В. Исследование беспроводной технологии ZigBee в области защиты информации. V miedzynarodowej naukowi-praktycznej konferecji «Europejska nauka XXI powieka», Przemysl, 5-15 травня 2009. С. 60-61. ISBN: 978-966-8736-05-6.

20. **Почта Ю.** Управление энергоресурсами на базе беспроводных технологий передачи данных. VIII mezinarodni vedecko-prakticka conference “Moderni vymozenosti vedy”, Publishing House “Education and Science”, Praha, 27 січня – 5 лютого 2012. С. 78-81. ISBN: 978-966-8736-05-6

21. **Kovalova Y.**, Mieshkov V. Information protection in communication networks. Virtual conference «Information Technologies in Science & Education», India, Ukraine, Spain, Italy.

22. **Почта Ю.** Новітні технології у сфері ЖКГ. Вісник Дніпропетровської міської ради. М. Дніпропетровськ 2009 №009.

23. **Почта Ю.В.** Интеллектуальные информационно-управляющие системы. Научно-техническая конференция «Информационные технологии в металлургии и машиностроении. ITMM-2013», м. Дніпропетровськ, 26-28 березня 2013.

24. **Ковальова Ю.В.** Особливості використання протоколу SCTM в інтелектуальних мережах Smart Grid. Збірник матеріалів доповідей та тез XVIII Міжнародної науково-практичної конференції «Безпека інформації у інформаційно-телекомунікаційних системах», м. Київ, 2016, стор. 54.

25. **Ковальова Ю.В.** Проблеми в сфері забезпечення кібернетичної безпеки об’єктів критичної інфраструктури. Збірник матеріалів доповідей та тез

VII Науково-практична конференція «Актуальні проблеми управління інформаційною безпекою держави», м. Київ 2016.

26. **Ковальова Ю.В.**, Бабенко Т.В. Забезпечення кібербезпеки об'єктів енергетичної інфраструктури. Збірник матеріалів доповідей та тез II науково-практична конференція «Проблеми безпеки інформаційно-телекомунікаційних систем», м. Київ, 23-24 березня 2017. С. 121-123.

27. **Ковальова Ю.В.** Моделі ідентифікації мережевих аномалій на основі карти самоорганізації. Збірник матеріалів доповідей та тез VII міжнародної науково-технічної конференції «ITSEC», м. Київ 2017.

28. Твердохліб І.С., **Ковальова Ю.В.** Управління інцидентами кібербезпеки на малих комерційних підприємствах. Збірник матеріалів доповідей та тез. П'ята всеукраїнська науково-технічна конференція студентів, аспірантів і молодих учених «Молодь: наука та інновації 2017». Національний технічний університет «Дніпровська політехніка», м. Дніпро, 2017. Т.12. С.9-10.

29. **Ковальова Ю.В.** Інформаційна безпека бездротових мереж моніторингу. Збірник матеріалів доповідей та тез. П'ята всеукраїнська науково-технічна конференція студентів, аспірантів і молодих учених «Молодь: наука та інновації 2017». Національний технічний університет «Дніпровська політехніка», м. Дніпро, 2017. Т.12. С.40-42.

30. Доколяса О.С., **Ковальова Ю.В.** Кібербезпека в інформаційному просторі України. Збірник матеріалів доповідей та тез. П'ята всеукраїнська науково-технічна конференція студентів, аспірантів і молодих учених «Молодь: наука та інновації 2017». Національний технічний університет «Дніпровська політехніка», м. Дніпро, 2017. Т.12. С.34-35.

31. **Ковальова Ю.В.**, Бабенко Т.В. Нейромережеві моделі ідентифікації DDoS атак. Збірник матеріалів доповідей та тез XX Міжнародної науково-практичної конференції «Безпека інформації в інформаційно-телекомунікаційних системах», м. Буча, 2018. С. 32-33.

32. Кручінін О.В., Тимофєєв Д.С., **Ковальова Ю.В.** Інформаційна безпека бездротових мереж моніторингу. Збірник матеріалів доповідей та тез XX Міжнародної науково-практичної конференції «Безпека інформації в інформаційно-телекомунікаційних системах», м. Буча, 2018. С. 247.

# ДОДАТОК Б

# ДОКУМЕНТИ ЩОДО ВПРОВАДЖЕННЯ РЕЗУЛЬТАТІВ ДОСЛІДЖЕНЬ

ДТЕК Дніпровські Електромережі
Оператор системи розподілу

АТ «ДТЕК ДНІПРОВСЬКІ ЕЛЕКТРОМЕРЕЖІ»
шосе Запорізьке, 22
м. Дніпро, 49107, Україна
тел.: +38 056 373 50 59
факс: +38 056 373 50 23

АТ «ПУМБ», м. Київ
МФО 334851
код ЄДРПОУ 23359034
IBAN UA873348510000000002600448085

_____ № КВ 247
На №_____ від 15.10.2020

АКТ
Впровадження наукових результатів дисертаційної роботи
Ковальової Юлії Вікторівни
«МАТЕМАТИЧНІ МОДЕЛІ ТА МЕТОДИ БЕЗДРОТОВОЇ ПЕРЕДАЧІ ДАНИХ В МЕРЕЖАХ ЕНЕРГОМОНІТОРИНГУ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ»,
подану на здобуття наукового ступеня кандидата технічних наук за спеціальністю
01.05.02 – Математичне моделювання та обчислювальні методи

Результати досліджень, виконаних у кандидатській дисертації Ковальової Ю.В., використані під час побудови системи комерційного обліку електроенергії компанії.

Запропонований автором новий підхід до процесу управління енергоспоживанням польового обладнання автономних бездротових систем, та алгоритм, який враховує стохастичність змінних, і використовує адаптацію прогнозуючих моделей для компенсації запізнювання передачі даних, затримки сигналів, і збурень в реальному масштабі часу, дозволить будувати автономні системи енергомоніторінгу з прогнозованим терміном придатності і підвищеної якості. Зміна потоків активної і реактивної потужності, викликане розподіленою генерацією сонячних батарей та вітрогенераторів, має важливі технічні та економічні наслідки для розподільної мережі, що робить очевидною неспроможність централізованих підходів до архітектури автоматизованих систем енергомоніторингу та актуалізує потребу моделювання процесів у децентралізованих системах.

Впровадження автономних локальних бездротових систем моніторингу, та впровадження проактивного керування в вузлах розподілу, дозволить забезпечити якість та надійність надання послуг кінцевим споживачам електроенергії. Застосовані в дисертаційній роботі моделі дозволяють з великою ймовірністю прогнозувати строк ефективної безперебійної експлуатації польового обладнання системи, що позитивно впливає на економічні показники Компанії.

В.о. начальника відділу з капітального будівництва І.В. Слинько

ЗАТВЕРДЖУЮ

Директор Департаменту екологічної політики Дніпровської міської ради
Семенко Олег Борисович

15 грудня 2020 р.

АКТ

Впровадження наукових результатів дисертаційної роботи
Ковальової Юлії Вікторівни
"МАТЕМАТИЧНІ МОДЕЛІ ТА МЕТОДИ БЕЗДРОТОВОЇ ПЕРЕДАЧІ ДАНИХ В МЕРЕЖАХ ЕНЕРГОМОНІТОРИНГУ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ",
подану на здобуття наукового ступеня кандидата технічних наук
за спеціальністю
01.05.02 – Математичне моделювання та обчислювальні методи

Результати досліджень, що виконані у кандидатській дисертації Ковальової Ю.В., використані під час побудови системи моніторингу якості поставок води промисловим і побутовим споживачам.

Запропонований автором підхід до процесу управління енергоспоживанням польового обладнання автономних бездротових систем, та алгоритм адаптації прогнозуючих моделей в реальному масштабі часу, дозволяє будувати автономні системи моніторингу з прогнозованим терміном придатності і підвищеної якості.

Впровадження автономних локальних бездротових систем моніторингу поставок води споживачам, та впровадження проактивного керування в місцях підключення до мережі, дозволить забезпечити якість послуг та надійність їх надання. Тобто, крім найважливішої функції контролю за водоспоживанням абонента, має місце теж дуже важлива функція реального управління його водоспоживанням та якості.

В перспективі це дозволить привести відношення між постачальником та споживачем в цифровий формат. Застосовані в дисертаційній роботі моделі дозволяють з великою ймовірністю прогнозувати строк ефективної безперебійної експлуатації польового обладнання системи, що позитивно впливає на економічні показники і зниження понаднормативних витрат.

Заступник директора департаменту-
начальник управління комунальної
екології департаменту екологічної
політики Дніпровської міської ради І. А. Козлова

ЗАТВЕРДЖУЮ

Директор виконуючий
ПрАТ «Дніпрополімермаш»
Мацюця Сергій Федорович
21 січня 2021р.

# АКТ

Впровадження наукових результатів дисертаційної роботи
Ковальової Юлії Вікторівни
“МАТЕМАТИЧНІ МОДЕЛІ ТА МЕТОДИ БЕЗДРОТОВОЇ ПЕРЕДАЧІ ДАНИХ В МЕРЕЖАХ ЕНЕРГОМОНІТОРИНГУ НА ОБ’ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ”,
подану на здобуття наукового ступеня кандидата технічних наук
за спеціальністю
01.05.02 – Математичне моделювання та обчислювальні методи

Результати досліджень, виконаних у кандидатській дисертації Ковальової Ю.В., використані під час побудови системи комерційного обліку води, газу та електроенергії товариства.

Запропонований автором підхід до процесу управління енергоспоживанням польового обладнання автономних бездротових систем та алгоритм адаптації прогнозуючих моделей в реальному масштабі часу, дозволив збудувати автономні системи моніторингу (вода, газ) з прогнозованим терміном придатності. Зміна потоків активної і реактивної потужності, викликане розподіленою генерацією та наявністю альтернативних джерел генерації, що присутнє на підприємстві, має важливі технічні та економічні наслідки, що робить очевидною неспроможність централізованих підходів до управління енергоспоживанням та актуалізує потребу моделювання процесів у децентралізованих системах.

Впровадження автономних локальних бездротових систем моніторингу поставок води та газу дозволило забезпечити якість управління енергоспоживанням підприємства та посприяло зниженню витрат.

Технічний директор А.І. Галкін

**ТОВ "ЛЕД Азімут"**
вул. Соборна, 16/9,
м. Кам'янське, 51925
**Телефон:**
**+380677036258**
**+380675686125**

http://aled.net.ua
e-mail : info@aled.net.ua

Світлодіодні світильники

Автоматизація і дистанційне керування системами освітлення

АКТ
Впровадження наукових результатів дисертаційної роботи
Ковальової Юлії Вікторівни

"МАТЕМАТИЧНІ МОДЕЛІ ТА МЕТОДИ БЕЗДРОТОВОЇ ПЕРЕДАЧІ ДАНИХ В МЕРЕЖАХ ЕНЕРГОМОНІТОРИНГУ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ",

подану на здобуття наукового ступеня
кандидата технічних наук за спеціальністю

01.05.02 – Математичне моделювання та обчислювальні методи

Результати досліджень, виконаних у кандидатській дисертації Ковальової Ю.В., використані під час адаптації системи моніторингу та управління загальним освітленням "Smart Lighting Web-ZB" згідно вимогам консорціуму TALQ. Проект виконувався нашим підприємством в рамках грантової програми Фонду «Північної ініціативи гуманітарної підтримки та енергоефективності (Україна)» НЕФКО в 2016р. Під час виконання проекту, який є одним з найбільших в Європі, було встановлено шість пунктів управління світлодіодним освітленням, з яких за технологією ZigBee виконувалось бездротове керування 1050 світильниками на відстані 9,6 кілометрів.

Запропонована автором адаптація моделі компенсації запізнювання передачі даних і затримки сигналів в локальній мережі і мережі Інтернет в реальному часі, дозволило здійснити керування автономними системами з прогнозованим терміном управляючих сигналів.

Впровадження автономних локальних бездротових систем моніторингу, та впровадження прогнозованого управління вузлами енергопостачання, дозволить забезпечити якість та надійність надання послуг з освітлення локальних об'єктів, що територіально віддалені.

**Директор** **Скулов С.В.**
02.11.2020р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ «ДНІПРОВСЬКА ПОЛІТЕХНІКА»
просп. Д. Яворницького, 19, м. Дніпро, 49005, Україна
тел./tel. +38 (056) 744 62 19
+38 (0562) 46 40 62
факс/fax +38 (056) 744 62 11
e-mail: rector@nmu.org.ua,
nmu@nmu.org.ua
http://nmu.org.ua

20.10.20 № 04-53/60 на №

# АКТ

Про використання наукових результатів дисертаційної роботи на здобуття наукового ступеня кандидата технічних наук асистента кафедри безпеки інформації та телекомунікацій

**Ковальової Юлії Вікторівни**

в навчальному процесі

Національного технічного університету “Дніпровська політехніка”

Комісія у складі: голова – перший проректор НТУ «Дніпровська політехніка», професор Азюковський О.О., керівник навчального відділу Салова В.О., декан факультету інформаційних технологій, професор Алексєєв М.О., завідувачка кафедрою програмного забезпечення комп’ютерних систем, доцент Удовик І.М. склали цей акт про те, що результати наукової роботи асистента кафедри безпеки інформації та телекомунікацій Ковальової Ю.В. впроваджено в навчальний процес та викладаються у курсі “Математичне моделювання процесів і систем” за освітньою програмою “Комп’ютерні науки” другого (магістерського) рівня вищої освіти спеціальності 122 “Комп’ютерні науки”.

Голова комісії О.О. Азюковський

Члени комісії В.О. Салова

М.О. Алексєєв

І.М. Удовик

# ДОДАТОК В

# ІНСТАЛЯЦІЯ ОБЛАДНАННЯ ТА РОЗРОБЛЕНОЇ СИСТЕМИ «SMART UTILITY WEB»

## ВСТУП

Система Інтернет-моніторингу споживання і управління споживанням енергоресурсів «Smart Utility Web» призначена для простого і легкого використання на об'єктах житлово-комунального господарства. Система включає прилади обліку енергоресурсів (електрична енергія, холодна і гаряча вода, природний газ, теплова енергія), пристрої збору і передачі даних (ПЗПД) «Сигма ZB», модем-координатор системи «Сигма RF», хмарний SaaS сервіс.

«SUW» є бездротовою системою, що працює у неліцензованому радіодіапазоні 2,4 ГГц і використовує сертифікований альянсом ZigBee протокол Digi-Mesh.

«SUW» призначена для використання в складній завадовій обстановці міст і мегаполісів всередині житлових будинків, офісних і виробничих приміщень, технологічних виробництв і закритих майданчиків. Реалізує три режими експлуатації: проактивний, реактивний і гібридний. Дозволяє здійснювати просте масштабування без використання додаткових комутаційних пристроїв.

Архітектура системи дозволяє безпроблемний монтаж при дотриманні простих правил інсталяції, наведених у цій інструкції.

## 1. ОСНОВИ ПОБУДОВИ HAN-МЕРЕЖ

HAN (home area network) або домашні мережі малого радіусу дії розгортаються всередині приміщень, тому ослаблення радіосигналу набуває основне значення при проектуванні і установці систем в реальних умовах. Кожна пара радіопристроїв характеризується енергетичним запасом (потенціалом), який необхідний для компенсації послаблень радіосигналу. Для стійкої роботи повинен бути передбачений енергетичний запас в 20-25 дБ.

Ослаблення за рахунок перешкод (будівельних конструкцій приміщень) відбувається в результаті поглинання ними радіосигналу. В результаті після проходження радіосигналу крізь перешкоди формується вторинна електромагнітна хвиля. В результаті для оцінки придатності радіоінтерфейсу суму зазначених послаблень сигналу (в дБ) необхідно відняти від заявленого виробником енергетичного потенціалу між радіопристроями. Отриманий результат і є розрахунковим енергетичним запасом між радіопристроями. Його рекомендована величина характеризує стабільну радіозв'язок і призначена для компенсації так званих швидких і повільних завмирань сигналу. До швидких завмирань, крім явищ, пов'язаних із самою природою поширення радіохвиль, відносяться ослаблення сигналу, пов'язані з переміщенням в приміщеннях людей, а також багаторазовим перевідбиттів радіохвиль всередині цих приміщень. При поширенні радіохвиль всередині приміщень є деяке обмеження, пов'язане з так званої граничної товщиною перешкоди (стіни), при перевищенні якої вже не відбувається формування вторинної електромагнітної хвилі.

Дальність радіозв'язку визначається чотирма параметрами:

- потужністю передавача;
- чутливістю приймача;
- ослабленням сигналу у вільному просторі;
- ослабленням сигналу при проходженні через стіни приміщень.

### 1.1.Енергетичні параметри радіомодулів

ПЗПД «Сигма ZB» і «Сигма RF» комплектуються радіомодулями XBee і REX3DP виробництва DIGI і REXENSE, відповідно. Характеристики модулів наведені в таблиці 1.

Таблиця 1. Характеристика радіомодулів

| Радіомодуль | Потужність прд, дБм | Потужність прд, мВт | Чутливість ПЗМ, дБм |
|---|---|---|---|
| XBee | 0 | 1 | -92 |
| XBeePRO | 20 | 100 | -100 |
| XBeeS2 | 3 | 2 | -96 |
| XBeeProS2 | 14 | 50 | -102 |
| XBeeSMT | 8 | 6,3 | -102 |
| XBeeSMT_PRO | 18 | 63 | -101 |
| REX3D | 9 | 7,94 | -99 |
| REX3DP | 20 | 100 | -104 |

**Ослаблення сигналу у вільному просторі** визначається робочою частотою системи. У таблиці 2 представлена залежність ослаблення сигналу у вільному просторі від відстані.

Таблиця 2. Ослаблення сигналу 2,4 ГГц у вільному просторі

| **Відстань, м** | **0** | **10** | **50** | **100** |
|---|---|---|---|---|
| **Ослаблення сигналу, дБ** | 40 | 60 | 74 | 80 |

**Значення ослаблення сигналу діапазону частот 2,4 ГГц**при проходженні крізь стіни приміщень і гранична товщина стіни представлені в табл. 3. Якщо товщина стіни перевищує деяку граничну величину, то радіосигнал не буде проходити через неї.

Таблиця3. Ослаблення сигналу при проходженні через стіну під кутом $90^0$

| Матеріал стіни | Ослаблення сигналу, дБ | Гранична товщина, м |
|---|---|---|
| дерево і пінобетон | 3-4 | 1,6 |
| цегла | 6 | 0,8 |
| бетон | 10 | 0,1 |
| залізобетон | 18-30 | 0,09 |

Якщо електромагнітна хвиля на поверхню потрапляє під кутом, відмінним від 90 °, то гранична товщина стіни стає трохи менше, а ослаблення сигналу за рахунок часткового відображення радіохвилі - більше (рис.1).

З метою збільшення дальності радіозв'язку доцільно застосування роутерів. Вони дозволяють створити більш рівномірну енергетичну щільність між пристроями і в повній мірі реалізувати принцип автоматичного написання маршруту доставки сигналів між компонентами радіосистеми (динамічна маршрутизація).

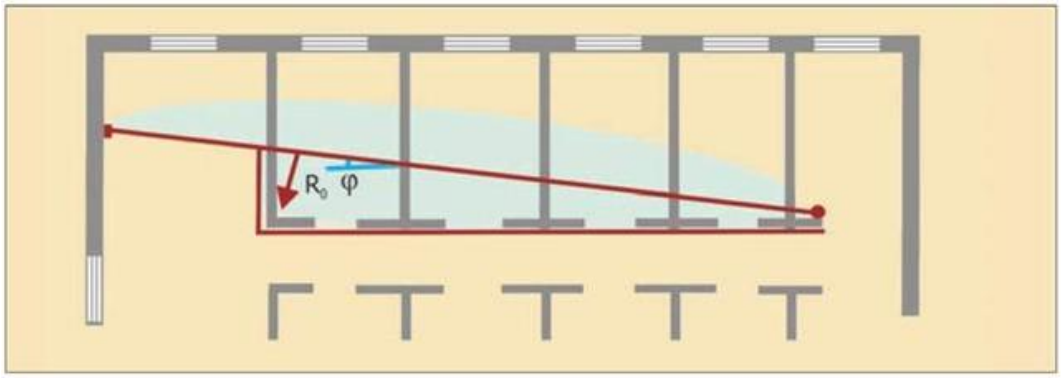



Рис.1. Поширення радіохвиль в приміщенні

*<u>Приклад розрахунку:</u>*

*Відстань 15 м, 2 стіни. Смуга пропускання 2,4 ГГц. Ослаблення сигналу у вільному просторі: Vo=64 дБ. Ослаблення сигналу за рахунок перешкод: Vпр. = 2 х 10 дБ = 20 дБ. Сумарне ослаблення сигналу: VΣ = 64 + 20 = 84 дБ. Енергетичний запас на завмирання дорівнює: 110 - 84 = 26 дБ. Енергетичний запас діапазону більше 20 дБ, що достатньо для стабільної радіозв'язку. Даний оціночний розрахунок застосовується при проектуванні мережі в приміщенні на стадії будівництва. Для існуючих будівель доцільно застосовувати вимір сигналу за допомогою сніфферу.*

У смузі частот (2,4 ГГц) при поширенні радіохвиль всередині будівлі необхідно розглядати вплив таких чинників, як: розташування і тип об'єкта, матеріали стін і перегородок, а також і інші конструктивні характеристики будівлі. Через те, що довжина хвилі в даній смузі частот становить приблизно 12 см, існує досить багато предметів і поверхонь всередині будівлі, що мають розміри порядку половини довжини хвилі (6 см), які могли б взаємодіяти в розглянутій смузі частот. Кожен такий предмет є потенційним джерелом рефракції, дифракції або розсіювання радіочастотної енергії.

### 1.2. Діаграма спрямованості випромінювання

Для пристроїв, що працюють в діапазоні 2,4 ГГц, дальність дії зв'язку між пристроями є однією з найважливіших характеристик радіосистем. Для надійної роботи радіосистеми необхідно, щоб між елементами був забезпечений стійкий радіозв'язок з достатнім енергетичним запасом. При цьому потужність передавача має другорядне значення в порівнянні з чутливістю приймача і має незначний вплив на дальність зв'язку. Радіоканал необхідно планувати таким чином, щоб потужність передавача була якомога нижче, а збільшення рівня сигналу в точці прийому домагатися за рахунок технічних засобів. Саме за забезпечення оптимальних умов роботи приймально-передавального тракту відповідають антени і їх діаграми спрямованості. Відповідно до вимоги нормативної документації (PI 24-6 «Обладнання мереж автоматизованого управління, *від 12.01. 2012 року № 18 )*для пристроїв, що працюють в даному діапазоні, коефіцієнт посилення антен не повинен перевищувати 6 dBi, а сама

антена повинна бути інтегрована в пристрій. Підключення зовнішніх антен заборонено. Тому для роботи в складі пристроїв «Сигма ZB» і «Сигма RF» застосовані модулі XBee і REX3 з вбудованими chip і PCB антенами, діаграма спрямованості (ДС) яких приведена на рис.2.
Такі антени забезпечують однаковий рівень випромінювання в будь-якому напрямку в горизонтальній площині. Для забезпечення радіозв'язку з пристроями, що знаходяться в різних напрямках, слід використовувати антени з круговою ДС.

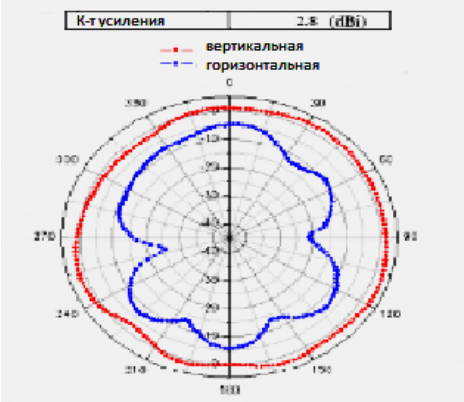



Рис.2. Діаграма спрямованості

## 2. ПРАКТИЧНІ РЕКОМЕНДАЦІЇ

Наведена методика оцінки придатності радіопристроїв бездротових систем не викликає яких-небудь труднощів при розрахунках. Більш того, при внесенні будь-яких змін в планування функціонуючих будівель запропонована методика дозволяє спрогнозувати і своєчасно спланувати необхідні заходи щодо зміни структури радіосистеми без проведення серйозних вишукувальних робіт, для чого іноді досить обмежитися переміщенням одного або двох роутерів. Розуміння фахівцями монтажних підрозділів цієї методики дозволяє значно скоротити час при пошуку місць оптимального розташування радіопристроїв.

**Основні рекомендації по монтажу обладнання радіосистем:**

- ПЗПД і роутери слід монтувати по можливості далі від металевих предметів, металевих дверей, металізованих віконних прорізів, комунікацій та ін.
- Слід уникати установки радіопристроїв поблизу різних електронних приладів, комп'ютерної техніки, струмоведучих кабелів, проводів, для того щоб виключити вплив перешкод на прийом радіосигналів.
- Рекомендована відстань між радіомодулями і електронними пристроями - не менше 1-1,5 м.

## 3. УСТАНОВКА ВОДОМІРІВ НА ОБ'ЄКТІ КОНТРОЛЮ ТА УПРАВЛІННЯ

Устаткування автоматизованої системи «Servic Smart Utility Web-ZB» призначене для простого і швидкого розгортання систем моніторингу та управління водоспоживанням на об'єкті автоматизації. В якості первинних приладів обліку ми рекомендуємо використовувати лічильники води виробництва «Maddalena Spa.», обладнані штатними імпульсними інтерфейсами «reed switch».

### 3.1. Підготовка лічильника до установки.

Лічильники CD..SD-8 і CD One TRP поставляються в заводській упаковці з позначкою про первинну заводську повірку. Маркування і зовнішній вигляд представлені на рис.2 і перевіряються при розпакуванні приладу. Лічильники води CD..SD-8 і CD One TRP поставляються підготовленими для установки імпульсного інтерфейсу. Лічильники води CD..SD-8 мають вбудований магнітний датчик імпульсів з постійною величиною: 10 літрів = 1 імпульс. Установка датчика «Reed switch» і його пломбування зображені на рис.4.

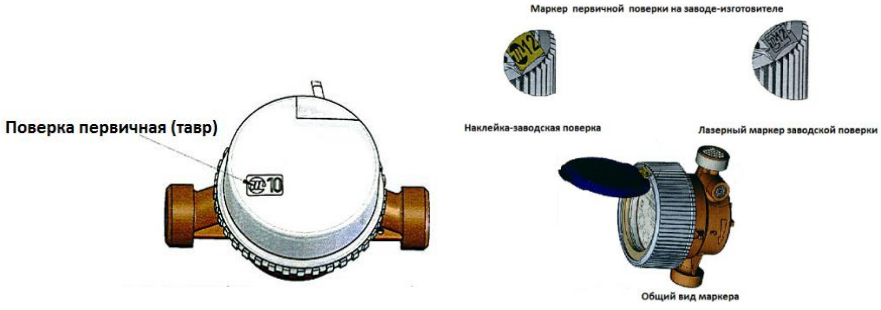



Рис. 3. Заводський тавр водомірів

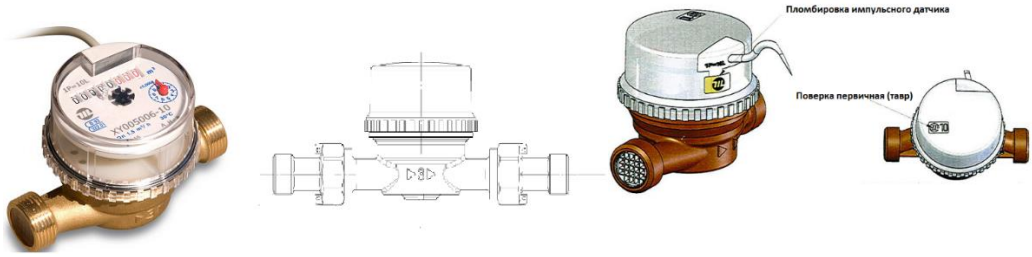
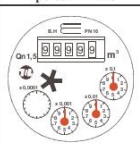
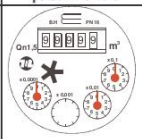
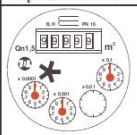
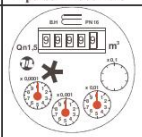



Рис. 4. Підключення імпульсного інтерфейсу лічильників CD..SD-8

Лічильники CD One TRP мають вбудований магнітний датчик, що настроюється на вибране співвідношення відповідно до таблиці 4.

Таблиця 4. Постійна лічильника CD One TRP

| Pulse Factor | 1P=1L K=1<br>1 pulse = 1 litre | 1P=10L K=0.1<br>1 pulse = 10 litre | 1P=100L K=0.01<br>1 pulse = 100 litre | 1P=1000L K=0.001<br>1 pulse = 1000 litre |
|---|---|---|---|---|
| Magnet position |  |  |  |  |
| Sensor position |  |  |  |  |

Імпульсний інтерфейс «Reed switch» дляCD One, DS TRP представлений на рис. 5.

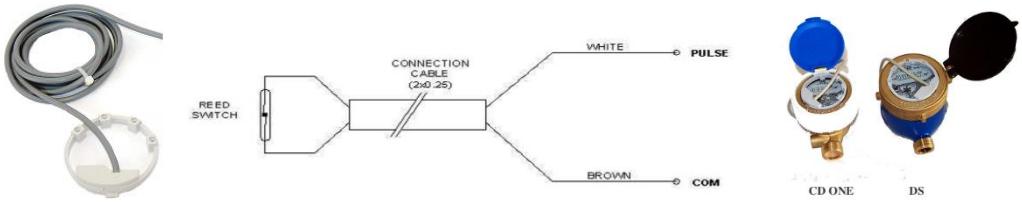



Рис. 5. Зовнішній вигляд і схема інтерфейсу «Reed switch»

Інтерфейс встановлюється на лічильник відповідно до вибраного значення коефіцієнта і пломбується відповідно до рисунка 6.


Рис. 6. Пломбування імпульсного інтерфейсу

### 3.2 Підключення імпульсного інтерфейсу до ПЗПД «Сигма ZB»

#### 3.1.1. ПЗПД «Сигма ZB» версії H08.11 S01.01 (облік)

ПЗПД призначено для підрахунку надходять на нього імпульсів по двом входам, перетворення їх в показання вимірюваних величин і подальшого архівування, контролю пристроїв сигналізації. Даний ПЗПД являє собою пластиковий корпус КМ-52 з електронною платою, на якій встановлені: радіочастотний приймач, роз'єм для параметризації і елементи схеми і холдер з двома літієвими джерелами живлення (3В) типорозміру АА. На платі, зліва від роз'єму для параметризації, розташований клемник для підключення двох імпульсних входів. Призначення висновків: G - загальний висновок (маса); 1 - імпульсний вхід №1; 2 - імпульсний вхід №2. Якщо імпульсний вхід №2 буде використовуватися, як другий вхід сигналізації, то необхідно замість резистора, розташованого в задній частині плати, як показано на рис.7, встановити перемичку.
Зовнішній вигляд ПЗПД наведено на рис. 8.

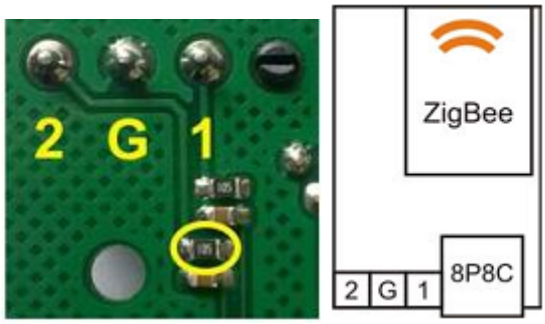



Рисунок 7. Схема підключення ПЗПД

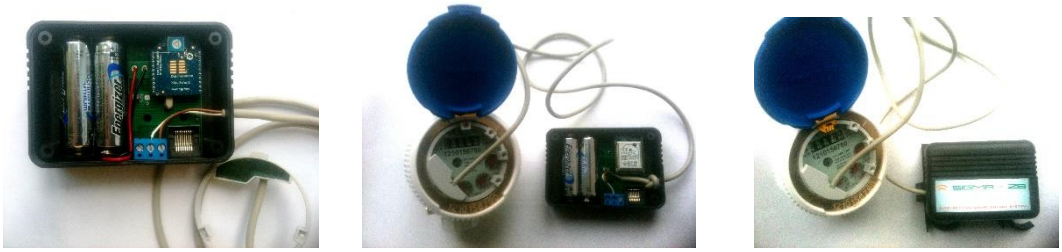


Рис. 8. Загальний вигляд вузла обліку

Установка ПЗПД здійснюється безпосередньо на трубі за допомогою двох штатних монтажних кріплень. При необхідності ПЗПД можна встановлювати на будь-якій ізольованій вертикальній поверхні за допомогою 2-х дюбелів або 2-стороннього монтажного скотча. При необхідності надлишки сигнального кабелю можуть бути пов'язані і закріплені за допомогою монтажних стяжок, як показано на малюнку 8. Вузол обліку поставляється готовим до установки і експлуатації.

Рис. 9. Монтаж вузла обліку

### 3.1.2. ПЗПД «Сигма ZB» версії H09.01 S01.02 (облік і управління)

ПЗПД являє собою пластиковий корпус Z-52 з електронною платою, на якій встановлені: радіочастотний приймач, батарейко- власники (холдери), роз'єм для параметризації, елементи схеми. На платі, знизу від радіомодуля, розташований клемник для підключення двох імпульсних входів і входу сигналізації. Призначення висновків: G - загальний висновок (маса); 1 - імпульсний вхід №1; 2 - імпульсний вхід №2; A - вхід сигналізації


Рис. 10. Схема підключень ПЗПД

У комплект поставки обладнання вузла обліку та регулювання входить:

1. Лічильник води виробництва MADDALENA (Italy).
2. Комплект з'єднань
3. Пристрій для формування імпульсів «Reed Switch»
4. Кульовий кран з електроприводом CWX-15 виробництва TTHigh-TechValveCo., Ltd (PRC)
5. ПЗПД «Сигма ZB» версія H09.01 S01.02.
6. Датчик протікання H09.01 S01.02 LD (рис.11).

Рис. 11. Датчик протікання

ЗБІРКА УЗЛА ОБЛІКУ ТА УПРАВЛІННЯ

1. Розпакувати обладнання і з'єднати лічильник води з кульовим краном згідно схеми (наведено нижче).
2. Встановити адаптер «ReedSwitch» відповідно до обраного діапазоном витрат
3. Зняти задню кришку ПЗПД «Сигма ZB» і встановити 4 батарейки типу АА в штатний утримувач.
4. Підключити вихід адаптера «ReedSwitch» до клеми контактів відповідно до схеми.
5. Підключити кабель кульового крана CWX-15 до керуючих контактам ПЗПД «Сигма ZB» відповідно до схеми і рис. 12.
6. Підключити датчик протікання до входу сигналізації ПЗПД.

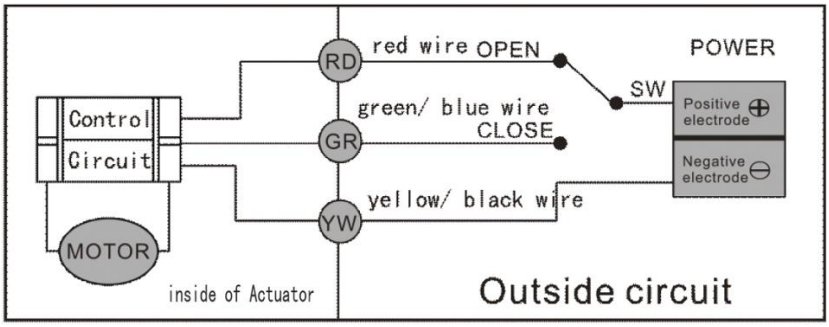




Рис. 12. З'єднання обладнання вузла обліку та управління

**<u>ПРИМІТКИ:</u>**

*При установці вузла обліку в колодязі враховувати напрям поширення радіосигналу: модем-координатор і ПЗПД «Сигма ZB» повинні знаходитися на одній лінії відповідно до схеми і малюнком, наведеними нижче на рис.13.*

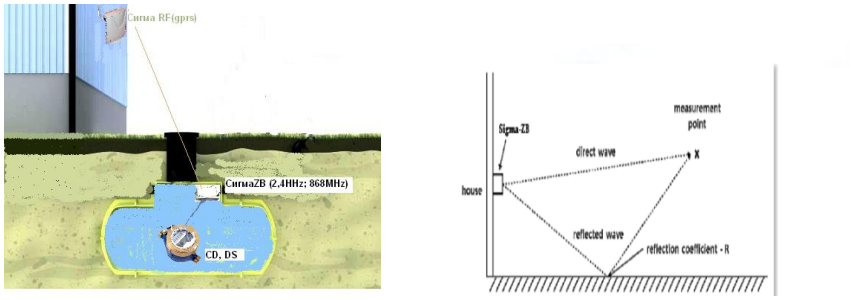



Рис. 13. Установка вузла обліку в розподільному колодязі

*<u>ВАЖЛИВО:</u> Напрямок поширення радіосигналу перпендикулярно лицьової поверхні ПЗПД з нанесеним QR-кодом. ЗВЕРНУТИ УВАГУ НА КОЛІР провідників кульового крана CWX-15 !!!*

7. Закрити кришку на 4 гвинта і закріпити пристрій на вертикальній поверхні за допомогою 2-х дюбелів.

### 3.2. Монтаж вузла обліку

**Абонентський облік.**


Рис. 14. Загальний вигляд

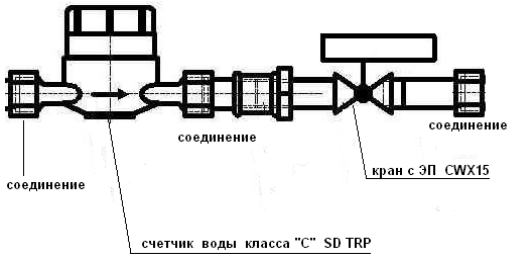



Рисунок 15. Схема абонентського обліку

## 4. ПОРЯДОК РОБІТ З МОНТАЖУ СИСТЕМИ

З огляду на те, що обладнання системи поставляється налаштованим і готовим до використання, установка системи здійснюється наступним чином і в такому порядку (не допускається порушення порядку операцій).

4.1. У будь-якому під'їзді (або квартирі) вибрати місце з упевненим прийомом GSM-оператора, що підтримує gprs-з'єднання. Встановити модем з дотриманням поляризації антени, під поляризацію обраного оператора (за замовчуванням KIYVSTAR GSM). Подати харчування на модем (220В, 50Гц).

У безпосередній близькості від модему (визначається за допомогою «Інсталлер») В квартирі:

4.2. Демонтувати старий лічильник.

4.3. Встановити на його місце новий лічильник з підключеним ПЗПД «Сигма-ZB». Закріпити ПЗПД. Виконати пломбування вузла обліку.

4.4. Повторити дії в суміжних квартирах і поверхах.

4.5. Мережа буде будуватися автоматично.

Схематичне представлення системи обліку представлено на рис.16:

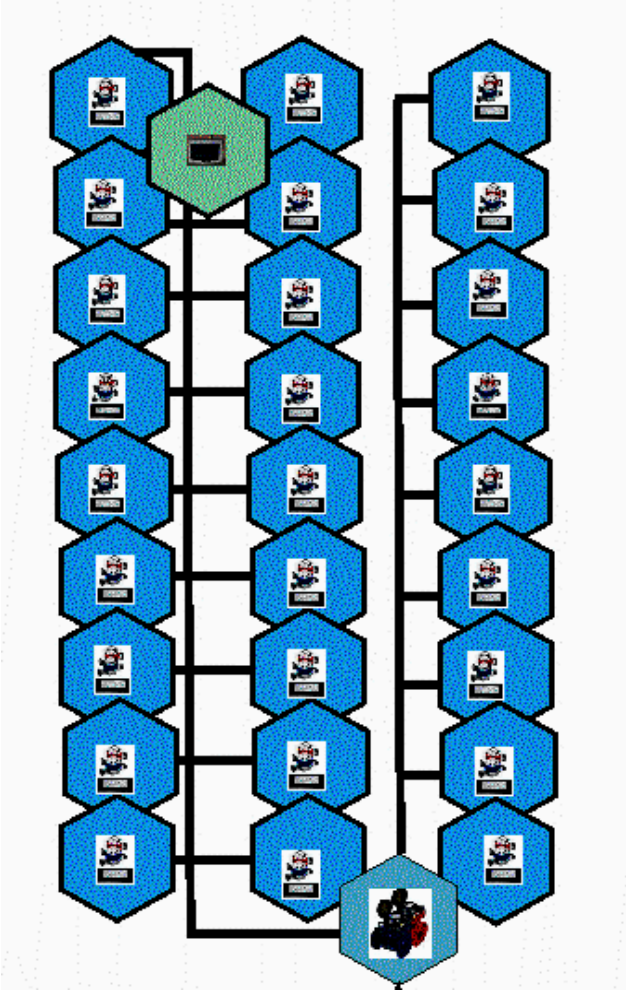


Рис. 16. Схема HAN житлового будинку