УДК 621.396 DOI: 10.31673/2786-8362.2025.015059

**Охрамович М.М.,** к.т.н.; **Коваль М.О.,** PhD;
**Кравченко О.І.,** к.пед.н.; **Шамрай Н.М.**

# МЕТОДИКА ЗАБЕЗПЕЧЕННЯ АДАПТАЦІЇ І САМООРГАНІЗАЦІЇ СЕНСОРНОЇ МЕРЕЖІ В УМОВАХ ПОСТАНОВКИ ЗАВАД ТА КІБЕРВПЛИВУ

**Okhramovych M.M., Koval M.O., Kravchenko O.I., Shamrai N.M. Methodology for ensuring adaptation and self-organization of a sensor network under conditions of interference and cyber influence.** The article examines the functioning process of a sensor network (SN) in which an adaptation and self-organization methodology is applied under conditions of interference and cyber influence. This methodology is based on the use of test diagnostics of the SN, self-organization, and restoration of stable operation.

Sensor networks consist of a large number of multifunctional devices that serve as highly efficient solutions in information collection systems. Ensuring information security in SNs is quite challenging, as it requires key exchange and session maintenance, which affects the number of transactions between network nodes. The reliability of transmitted information is achieved by receiving confirmation after data transmission from properly functioning network sensors. The minimal size of the devices makes sensor technology highly flexible and practical.

**Keywords:** test diagnostics, network self-organization, interference environment, cyber influence, sensor network, sensor

**Охрамович М.М., Коваль М.О., Кравченко О.І., Шамрай Н.М. Методика забезпечення адаптації і самоорганізації сенсорної мережі в умовах постановки завад та кібервпливу.** У статті розглянуто процес функціювання сенсорної мережі (СМ) в якому застосована методика адаптації і самоорганізації мережі коли діють завади та здійснюється кібервплив. Ця методика базується на застосуванні тестового діагностування СМ , самоорганізації та відновлення стійкої роботи.

Сенсорні мережі, мають значну кількість багатофункціональних пристроїв, які використовуються в якості високоефективних рішень в системі збору інформації. Захист інформації в СМ достатньо складно досягнути, оскільки необхідним стає обмін ключами та підтримка сесій, що впливає на кількість транзакцій між вузлами мережі. Достовірність переданої інформації досягається завдяки отриманню підтвердження після передачі даних справними сенсорами мережі. Мінімальні розміри пристроїв роблять сенсорну технологію досить гнучкою і практичною.

**Ключові слова:** тестове діагностування, самоорганізація, завадова обстановка, кібервплив, сенсорна мережа, сенсор

## Вступ

Враховуючи діючу проти України збройну агресію російської федерації, безпека людини, суспільства і держави суттєво залежать від надійного функціонування об’єктів критичної інфраструктури та їх складових. Окрім фізичних впливів на об’єкти летальною зброєю російська федерація не полишає спроб завдавати впливати нелетальними засобами – кіберзброєю на системи управління критичної інфраструктури через кіберпростір. Враховуючи, що об’єкти критичної інфраструктури функціонують в єдиному інформаційному просторі то, всупереч колосальним зусиллям по захисту від несанкціонованого доступу і надалі залишаються вразливими до загроз таких як складна завадова обстановка, кіберзагрози та зміна умов експлуатації. У зв’язку з цим виникає потреба в розробці нових підходів, які забезпечать стійкість, надійність та ефективність СМ у таких умовах.

При цьому стає актуальним питання щодо конфігурування значної кількості вузлів у мережах. Налаштування комунікації в мережах є в певній мірі складним завданням. Датчики як правило мають обмеження за розташуванням, а конфігурація елементів у мережі заздалегідь не відома. При цьому їхнє розміщення у мережі може динамічно змінюватися з перебігом часу за рахунок переміщення наявних вузлів або приєднання нових. Тому однією з вимог, що вису-

вається до сенсорних мереж є самоорганізація, як частина підготовки мережі до застосування [1]. Під конфігурацією розуміють самоорганізовану заміну розташування неструктурованих на структуровані бездротові мережі з ефективним ступнем доступу до середовища.

Для забезпечення ефективної самоорганізації використовують наявні та розробляють нові алгоритми. Переважна кількість їх направлена на зменшення часу ініціалізації, скорочення службового трафіку та побудову оптимальної структури [2]. Таким чином, адаптація та самоорганізація стають ключовими властивостями для таких систем, дозволяючи їм автоматично реагувати на зміни середовища, нейтралізувати небезпечні зовнішні впливи та підтримувати оптимальну працездатність.

Створення методики, дозволить інтегрувати ці властивості в сенсорних мережах (СМ), забезпечуючи їхню стабільність і стійкість до викликів сучасного кібернетичного середовища.

**Аналіз останніх досліджень.** Бездротові сенсорні мережі збору і передачі даних можуть бути легко адаптовані до вирішення багатьох завдань практично в будь-яких сферах діяльності. Найбільш очевидна область застосування подібних мереж – це організація різних систем контролю і моніторингу, створення систем швидкого реагування в надзвичайних ситуаціях. В якості найбільш очевидних можна відзначити наступні завдання: протипожежні системи, організація систем безпеки – контроль периметру, визначення вторгнення, віддалене спостереження, контроль навколишнього середовища поблизу місць зберігання радіоактивних матеріалів, хімічних або біологічних речовин.

Нові можливості сенсорних мереж при виконанні широкого спектра завдань, а також використання останніх наукових та технологічних досягнень дають змогу спостерігати, за бойовими цілями, фіксувати їх у просторі та передавати розвідувальну інформацію для планування бойових дій [3]. Однак існує ряд проблем технологічного та експлуатаційного характеру, які вимагають пильного розгляду.

У статті [4] здійснено огляд перспективних можливостей розвитку тактичних сенсорних мереж, здійснено класифікацію та проведений аналіз проблем розроблення таких мереж у сучасних умовах.

У роботі [5] розглянуто спосіб оцінки ефективності методів керування бездротовими сенсорними мережами, який дозволяє виділити допустимий набір методів управління, що відповідають конкретній бездротовій сенсорної мережі та визначення діапазонів їх ефективного використання.

Дослідженню засобів виявлення різноманітних датчиків сенсорних мереж присвячені роботи науковців: О.В. Барабаша, Ю.О. Гордієнко, С.В. Дзядевич, А.А. Євтух, Я.І. Лепіх , В.Г. Мельник, В.А. Мокрицький, О.В. Сєлюков [6-7].

Вивченню будови, розгортанню та кодуванню даних у сенсорних мережах присвячені роботи науковців, серед яких: А.О. Дружинін, О.В. Жук, С.В. Лєнков, В.О. Романов, В.А. Романюк та інші [8-9].

Вчені звертають увагу на можливість проектування та оптимізації складних технічних систем залежно від наступних показників: обраного показника якості, середнього часу затримки повідомлення в мережі, надійності елементів системи та вартості проектування системи. На теперішній час значні зусилля спрямовані на проблему життєздатності і надійності мереж для збереження здатності виконувати базові функції навіть під впливом дестабілізуючих факторів та в умовах кібервпливу.

Таким чином, враховуючи особливості будови та експлуатації бездротових сенсорних мереж виникає необхідність досягти сталого функціонування сенсорних мереж завдяки забезпеченню властивості самоорганізації в умовах коли діють завади та здійснюється кібервплив.

**Постановка завдання.** Визначення етапів діагностування сенсорної мережі за допомогою методики адаптації і самоорганізації мереж в умовах коли діють завади та здійснюється кібервплив.

**Метою роботи** є підвищення ефективності функціонування сенсорної мережі умовах постановки завад та кібервпливу.

**Виклад основного матеріалу дослідження**

Процес вистежування бойових цілей, їх фіксування у просторі та передача розвідувальних даних про противника, став невід'ємною основою для планування та виконання заходів по відбиттю агресії, яка викликана прямим застосуванням збройних сил російською федерацією проти України. Важливу роль у виконанні таких завдань відіграють сенсорні мережі (СМ), які знаходять широке застосування в різних галузях. Їхнє функціонування частіше піддається впливу зовнішніх факторів, таких як завадова обстановка, кіберзагрози та зміна умов експлуатації. У зв'язку з цим виникає потреба в розробці нових підходів, які забезпечать стійкість, надійність та ефективність СМ у таких умовах.

Для якісної самоорганізації таких систем, необхідно нейтралізувати зовнішні впливи та підтримувати оптимальну працездатність. Ця робота спрямована на створення методики, який дозволить елементам СМ забезпечити їхню стабільність та стійкість до викликів сучасного кібернетичного середовища.

Розглянемо СМ, що складається з $N$ сенсорів і коли діють завади та здійснюється кібервплив.

Під час своєї роботи кожний сенсор проводить вимірювання показників середовища в якому він знаходиться. Згодом він виконує попередню обробку, зберігає і передає отримані данні до оператора. Виміряна інформація передається не лише операторам, але при необхідності іншим сенсорам СМ. Такі варіанти застосування СМ можуть викликати певні обмеження в структурі і функціонуванні сенсорів. Приміром, вартість сенсора повинна бути недорогою, розміри мінімальні та мати можливість працювати автономно на протязі тривалого часу. Варто звернути увагу, що надійність переданої інформації здійснюється не за допомогою стійкого каналу зв'язку, а завдяки підтвердженню справними сенсорами мережі отримання переданого пакету даних. Розглянемо методику самоорганізації СМ для забезпечення адаптації і самоорганізації сенсорної мережі в умовах постановки завад та кібервпливу. Досліджувану методику представимо у вигляді етапів:

1. Діагностування СМ здійснюється за допомогою адаптації тестового діагностування. Сутність методики полягає у наступному. Мережевий сенсор, що здійснює діагностування після перевірки може відправити зібрану діагностичну інформацію в сенсор мережі, який він перевірив або залишати її у себе. У випадку коли сенсор СМ $v_i$ оцінює $v_j$ як коректний, коли: $(r_{ij}=0)$, то $v_i$ надсилає у сенсор $v_j$ підсумок елементарної перевірки $\{r_{ij}\}$ та слово яке є ключове і містить інформацію про діагностичні зв'язки у СМ. В іншому випадку, якщо $v_i$ оцінює сенсор $v_j$ некоректним, коли: $(r_{ij}=1)$, то $v_i$ не передає інформацію про зміни у структурі та підсумки перевірок, залишить собі. Сенсор $v_j$, зокрема, здійснює передачу інформації в сенсор $v_l$, у випадку коли оцінює його коректним. Інформація, що передається містить в собі підсумки всіх попередніх перевірок та ключове слово про будову діагностичних зв'язків у мережі.

2. За час виконання перевірок, сенсор СМ, який отримав діагностичну інформацію щодо поточної структуру та синдром, робить визначення власних індикаторів структури $C_k$, $k=1,2,...,N$ застосовуючи які, обчислює властивість достатності структури для діагностування. Вказаний методика здійснює збір діагностичної інформації та зберігає в пам'яті коректних сенсорів СМ. Збір інформації виконаний після того, коли підсумки елементарних перевірок передаються в сенсори СМ, що отримав результат, який дорівнює нулю [10].

Коли за результатами перевірки $r=1$, то передача діагностичної інформації не здійснюється, а залишається в пам'яті сенсора, що виконує функції перевірки. Дана методика дає змогу коректним сенсорам мережі значно швидше накопичити необхідний об'єм

даних щоб провести діагностування. Така умова потрібна для того, щоб діагностування проводився лише коректним сенсором. В противному випадку при виконанні діагностування некоректним сенсором мережі може бути неправильне визначення семантичного стану СМ. При отриманні правильного підсумку діагностування із найбільш високою достовірністю необхідно, щоб підсумки перевірок накопичувалися тільки в коректних сенсорах мережі.

3. Сенсор, який після діагностування містить найбільший обсяг інформації вважають діагностичним сенсором (ДС).

4. Діагностичний сенсор активує роботу *першого алгоритму*. Перевагою його у порівнянні з відомими алгоритмами, які використовують взаємну інформаційну є те що, *перший алгоритм* потребує меншої надмірності у мережі і має два раунди для обміну інформаційними повідомленнями серед сенсорів СМ. Цей алгоритм дає змогу діагностувати мережу коли є відмови значної кількості сенсорів або є в наявності складні "блимаючі" відмови. Якщо після роботи *першого алгоритму* отримано неоднозначні результати, то починається виконання *другого алгоритму*. Він має декілька фаз роботи та використовує в ролі критерію час виконання цих фаз. В процесі роботи *другий алгоритм* визначає сенсор, який виконує діагностування. У випадку коли результат обробки буде неправильний чи час обробки не відповідає часовому ліміту, то сенсор буде вважатися таким, що відмовив та виключається з розгляду.

5. Після виявлення сенсорів які відмовили, починається процес самоорганізації СМ.

Самоорганізація СМ виконується за допомогою поступової деградації: сенсори, які відмовили, не приймають участь у діагностичному процесі, вирішення завдань перерозподіляється між справними сенсорами, які залишилися. Проте, деградація СМ може виконуватися до певного рівня, який залежить від обсягу завдань, які здійснює СМ та фактичної кількісті вільних ресурсів Для бездротової сенсорної мережі, яка застосовує методику адаптації пошуком несправностей та подальшою самоорганізацією мережі до певного рівня буде: $t_{max}=\left[\frac{N-2}{2}\right]$. Виходячи з цього в системі виділяється п'ять наступних станів: *S0* − усі сенсорі справні; *S1* − один сенсор несправний, інші справні; *S2* − два сенсорі несправні, інші справні; *S3* − три сенсорі несправні, інші справні; *S4* − повна відмова системи. Стан повної відмови, коли сенсорна мережа не може виконувати своїх функцій, може настати при умовах: виникнення в мережі кількості несправностей що більша за допустиму; невиявлення несправностей; невідновлення працездатності мережі; виникнення помилок в роботі методики адаптації та самоорганізації. Самоорганізація мережі дає змогу забезпечити заданий рівень функціональної стійкості (ФС) СМ.

Згідно з мережевим стандартом IEEE 802.15.4. [11] перерозподіл завдань між сенсорами повинен відповідати таким обмеженням:

$$80\ м \le d_{ij} \le 100\ м;$$

$$0 < w_{ij} \le 5\ dBm;$$

$$\rho_{ij} \le 250\ кбіт/с;$$

$$E_i \le 60\ \ мВт.$$

де $d_{ij}$ – визначає відстань між двома сенсорами $(i, j)$;

$w_{ij}$ – потужність передавача, який здійснює передачу інформації між двома сенсорами $(i, j)$;

$\rho_{ij}$ – пропускна здатність визначеного каналу зв'язку;

$E_i$ – енергоспоживання сенсора.

Після закінчення процесу самоорганізації СМ продовжує працювати в штатному режимі. Методику застосування і самоорганізації СМ для забезпечення їх зв'язності в умовах постановки завад та кібервпливу можна представити схематично, рисунок 1.

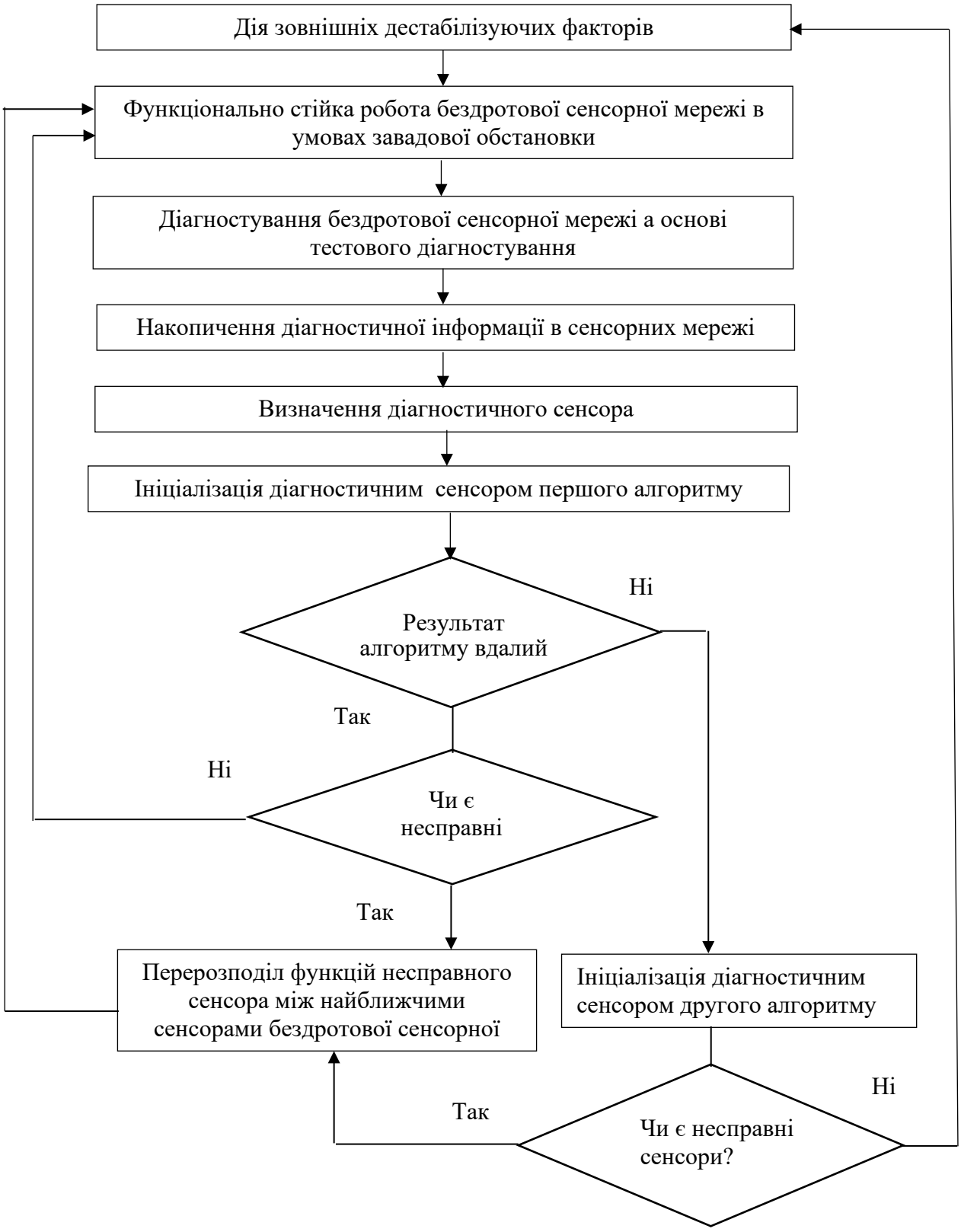


Рис. 1. Методика самоорганізації сенсорної мережі на основі адаптації в умовах постановки завад та кібервпливу

Здійснити надійний захист інформації у бездротових сенсорних мережах, що самоорганізовуються достатньо складно досягнути, оскільки необхідним стає обмін ключами та підтримка сесій. Це суттєво впливає на число транзакцій які здійснюються у мережі і в подальшому впливають на параметри енергоспоживання, що є важливим для СМ. Взагалі здатність до самоорганізації означає, що сенсорні пристрої використовують для роботи: а)

обмежену кількість інформації, періодично оновлюючи її за допомогою різноманітних зворотних зв'язків та взаємодій між сусідніми пристроями; б) використовують показники ймовірнісні в методах для прийняття рішень [12].

**Висновки**

Розроблена метотика адаптації і самоорганізації сенсорної мережі в умовах постановки завад та кібервпливу бере за основу результати тестового діагностування та відмовостійкої. Коли в результаті діагностування виявлено сенсори, які мають відмови, відбувається процес самоорганізації СМ. Самоорганізація СМ здійснюється при поступовій деградації: сенсори, що відмовили, вилучаються з процесу діагностування, розв'язання решти завдань передається на справні сенсори, що залишились. Вони забезпечують самоорганізацію та подальше відновлення працездатного режиму сенсорної мережі. Проте, процес деградації СМ може тривати до певної межі, яка залежить від завдань, які вирішують СМ та наявністю вільних ресурсів.

Завдяки розвитку сучасних бездротових сенсорних мереж, варто відмітити можливість майбутніх досліджень спрямованих на впровадження та експлуатацію бездротових сенсорних мереж в умовах постановки завад та кібервпливу, для досягнення досконалої сумісності із існуючими автоматизованими системами управління, які використовуються в секторі безпеки та оборони України.

**Список використаної літератури:**

1. Зеленін А.М., Власова В.А. Фаза ініціалізації в безпроводових сенсорних мережах // Вісник Національного технічного університету "ХПІ": зб. наук. праць. Тематичний випуск: Нові рішення в сучасних технологіях. 2012. № 26. С. 55–61.

2. Bein D. Self-Organizing and Self-Healing Schemes in Wireless Sensor Networks. London, England: Springer London, 2009. P. 293–304. URL: https://doi.org/10.1007/978–1–84882–218–4_11.

3. Петрушко М. М. Аналіз особливостей позиціонування мобільних об'єктів бездротових сенсорних мереж: пояснювальна записка до атестаційної роботи здобувача вищої освіти на другому (магістерському) рівні, спеціальність 172 Телекомунікації та радіотехніка /М. М. Петрушко; М-во освіти і науки України, Харків. нац. ун-т радіоелектроніки. – Харків, 2019. – 65 с. URL: http://openarchive.nure.ua/handle/document/11169.

4. Міночкін А.І., Романюк В.А., Жук О.В. Перспективи розвитку тактичних сенсорних мереж. // Збірник наукових праць ВІТІ НТУУ "КПІ"– 2007. – № 4. С. 16 – 22.

5. Жук О. В., Романюк В. А., Сова О. Я. Методологічні основи управління перспективними неоднорідними безпроводовими сенсорними мережами тактичної ланки управління військами. Пріоритетні напрямки розвитку телекомунікаційних систем та мережа спеціального призначення // К.: ВІТІ НТУУ «КПІ» 2016. С. 34 – 44.

6. Машталір В.В., Жук О.В., Міненко Л.М., Артюх С.Г. Концептуальні підходи застосування бездротових сенсорних мереж арміями передових країн світу. Сучасні інформаційні технології у сфері безпеки та оборони. 2023. Т. 47, № 2. С. 96– 112.

7. Лепіх Я.І., Гордієнко Ю.О, Дзядевич С.В., Дружинін А.О., Євтух А.А., Лєнков С.В., Мельник В.Г., Проценко В.О., Романов В.О. Інтелектуальні вимірювальні системи на основі мікроелектронних датчиків нового покоління: монографія. Одеса: «Астропринт», 2011. 352 с.

8. Лепіх Я.І., Гордієнко Ю.О, Дзядевич С.В., Дружинін А.О., Євтух А.А.,. Лєнков С.В., Мельник В.Г., Проценко В.О., Романов В.О. Мікроелектронні датчики нового покоління для інтелектуальних систем. монографія. Одеса: «Астропринт», 2011. 92 с.

9. Лєнков С.В., Лепіх Я.І., Мокрицький В.А., Сєлюков О.В., Сминтина В.А. за заг. ред. Мокрицького В.А., Лєнкова С.В. Напівпровідникові оптичні та акустоелектронні сенсори і системи. монографія. Одеса: «Астропринт», 2009. 256 с.

10. System-on-Chip (SoC) Solution for ZigBee/IEEE 802.15.4 Wireless Sensor Network. URL: http://focus.ti.com/docs/prod/ folders/print/cc2431.html. URL: https://oxorona.com/ieee-802-15-4/.

11. Протокол стандарту IEEE 802.15.4. URL: https://oxorona.com/ieee-802-15-4/.

12. М.Ю. Зеляновський, О.В.Тимченко. Інтелектуальна система для бездротових спеціалізованих сенсорних та мереж персонального радіусу дії: програмно-апаратна платформа вузла бездротової мережі // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ НАН України. - Вип.49. - К.: 2008. - С. 185-193.

***Автори статті***

**Охрамович Михайло** – кандидат технічних наук, старший науковий співробітник, Військовий інститут Київського національного університету імені Тараса Шевченка, Київ, Україна.

ORCID: 0000-0002-8776-3937

**Коваль Мирослав** – PhD, старший науковий співробітник, Військовий інститут Київського національного університету імені Тараса Шевченка, Київ, Україна.

ORCID: 0000-0002-8374-7390

**Кравченко Олександр** – кандидат педагогічних наук, старший науковий співробітник, Військовий інститут Київського національного університету імені Тараса Шевченка, Київ, Україна.

ORCID: 0000-0002-7865-5870

**Шамрай Назар** – старший науковий співробітник, Військовий інститут Київського національного університету імені Тараса Шевченка, Київ, Україна.

ORCID: 0000-0001-8387-3277

***Authors of the article***

**Okhramovych Mykhailo –** Candidate of Sciences (technical), Senior Researcher, Military Institute of Taras Shevchenko Kyiv National University, Kyiv, Ukraine.

ORCID: 0000-0002-8776-3937

**Koval Myroslav –** PhD, Senior Researcher, Military Institute of Taras Shevchenko Kyiv National University, Kyiv, Ukraine.

ORCID: 0000-0002-8374-7390

**Kravchenko Oleksandr –** Candidate of Sciences (pedagogical), Senior Researcher, Military Institute of Taras Shevchenko Kyiv National University, Kyiv, Ukraine.

ORCID: 0000-0002-7865-5870

**Shamrai Nazar –** Senior Researcher, Military Institute of Taras Shevchenko Kyiv National University, Kyiv, Ukraine.

ORCID: 0000-0001-8387-3277