УДК 621.396

к.т.н., с.н.с. **Охрамович М.М.** (ВІКНУ)
к.т.н., с.н.с. **Гахович С.В.** (ВІКНУ)
док. філ. **Коваль М.О.** (ВІКНУ)
к. пед. н. **Кравченко О.І.** (ВІКНУ)

DOI: http://doi.org/10.17721/2519-481X/2024/84-11

АНАЛІЗ І ОЦІНКА ФУНКЦІОНУВАННЯ СЕНСОРНИХ МЕРЕЖ В УМОВАХ ЗАВАДОВОЇ ОБСТАНОВКИ ТА КІБЕРВПЛИВУ

У статті здійснено аналіз сучасних сенсорних мереж і розглянуто базові принципи побудови та застосування у системах військового призначення. Особлива увага приділена бездротовим сенсорним мережам (БСМ), як перспективної технології, для реалізації важливого напряму воєнної політики.

Це стало можливим завдяки мініатюризації компонентів та зростанню потужності обчислень. Сенсорні мережі, складаються з великої кількості малопотужних багатофункціональних пристроїв, які розгортаються в певній географічній зоні. Хоч більшість з елементів такої мережі мають обмежені фізичні ресурси, об'єднані разом, вони швидко конфігуруються до виконання цілого ряду функціональних завдань захисту критичної інфраструктури та моніторингу навколишнього середовища тощо. Однак з розвитком та трансформацією все активніше досліджується й питання інформаційної безпеки, оскільки ризики несанкціонованого доступу або втручання можуть серйозно підірвати ефективність і надійність цих технологій. Слід зауважити, що саме через відкрите середовище передачі інформації, необхідно здійснювати оновлення методів шифрування та автентифікації

Запропоновано опис особливостей функціонування сенсорних мереж в умовах завадової обстановки та кібервпливу, застосуванню їх в якості високоефективних і перспективних рішень в системі збору інформації. Можливість розгортання мережі в складних умовах, відсутність провідних комунікацій і мінімальні розміри сенсорних пристроїв роблять технологію сенсорних мереж надзвичайно гнучкою і практичною. Вона передбачає максимальне використання інформаційних систем, що надають доступ до інформації в будь-який час незалежно від місцезнаходження користувача.

Ключові слова: бездротова сенсорна мережа, координатор мережі, датчики, маршрутизатори, інформаційні системи.

Вступ та постановка проблеми.

Стратегічним оборонним бюлетенем України, схвалено що одним із першорядних напрямів реалізації воєнної політики України є побудова системи об'єднаного керівництва силами оборони та військового управління у Збройних Силах України відповідно до передового досвіду, принципів і стандартів держав-членів НАТО [1]. Для реалізації важливого напряму воєнної політики, доцільно максимально використати основні функцій інформаційних систем, що надають доступ до інформації в будь-який час незалежно від місцезнаходження користувача. Завдяки цьому виникає необхідність застосовувати системи зв'язку для безперебійного обміну інформацією, своєчасної передачі наказів, розпоряджень, що забезпечить якісне та безперебійне управління військовими підрозділами.

Збір, оцінка і передача інформації є життєво важливими під час ведення бойових дій. Дані сенсорів, забезпечують точку входу для тих, хто може захотіти втрутитися в сприйняття військового персоналу і командирів, вставляючи неправдиві дані або взагалі відключаючи ці дані в рамках плану обману.

Кожна одиниця військової техніки має свій слід. Він може бути візуальним, звуковим або електромагнітним. Він може мати всі ці ознаки, а також володіти такими ознаками, як

вихлопні гази транспортних засобів чи літаків. Військові підрозділи різного масштабу також мають характерні ознаки. Основна ідея полягає у використанні сенсорних мереж і датчиків,

які дозволять виявити зазначені сліди військової діяльності і проінформувати командирів про виявлені ознаки.

Протягом багатьох років армії Заходу прагнули такого способу ведення війни, де б сукупність «датчиків» – відеокамер, тепловізорів, радіоантен тощо – виявляла цілі, передавала дані найкращому «стрільцю» – гаубиці, ракеті чи військовому кораблю, – і в такий спосіб утворювався б «ланцюг знищення» або ж, як зараз кажуть, «павутина знищення» безпрецедентної швидкості та ефективності.

Радіо, комп'ютерні мережі, супутникові сузір'я і наземні станції, технології шифрування, штучний інтелект і високопродуктивні обчислення – ось деякі з технологій, які зараз інтегровані в сенсорні та комунікаційні мережі.

На сьогодні, однією із технологічних інновацій є штучний інтелект (ШІ). Його розвиток та активне впровадження, здається, не оминули жодну сферу життя людини. Проте для армій, особливо західних демократій, штучний інтелект уже не новинка. У низці оборонних відомств департаменти давно розвивають та впроваджують ШІ. Для українських Сил оборони розвиток систем машинного навчання тільки починається. Тим не менш, в зоні бойових дії вже існують зразки озброєння, які працюють за допомогою ШІ. Одного дня їх кількість та системний вплив можуть стати настільки вагомими, що дозволить переломити позиційну форму війни.

В умовах активних боїв головним завданням для українських розробників є забезпечення ШІ-рішень для фронту. Одним з них є система Griselda, яка використовує ШІ для збору розвідувальних даних і підвищення ситуаційної обізнаності військ. Вона здатна обробляти тисячі повідомлень із супутників, безпілотників, соцмереж, ЗМІ та зламаних баз даних ворога [https://www.griselda.com.ua/].

Griselda за місяць обробляє понад 25 тис цілей, а рекорд за часом з моменту отримання інформації про ворога до її появи в системі становив 28 сек. Технологія інтегрована із системою ситуаційної обізнаності Delta, застосунками для артилеристів і танкістів "Броня", "Кропива", "Укроп" та "ГісАрта".

Аналіз досліджень та публікацій. Нові можливості сенсорних мереж при виконанні складних, стратегічних завдань, дають змогу спостерігати, за бойовими цілями, фіксувати їх у просторі та передавати розвідувальну інформацію для планування бойових дій [2].

У роботі [4], проведено аналіз завдань управління сенсорними мережами, а також запропоновано функціональну модель системи управління сенсорною мережею, обґрунтовані принципи її побудови, структура та функції. У статті [7] розглядаються перспективи розвитку тактичних сенсорних мереж, здійснено класифікацію і вимоги, що висуваються до них. Крім того, стаття містить результати аналізу проблем розроблення таких мереж і їх розвитку в сучасних умовах. У дослідженні [3] виконано аналітичний огляд сучасних наукових праць стосовно стану мобільних бездротових сенсорних мереж (далі – БСМ), а також надано загальне визначення бездротових сенсорних мереж з мобільними сенсорами та наводиться класифікація їхньої архітектури.

Побудові технічних засобів виявлення різноманітних датчиків сенсорних мереж присвячена багато робіт 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. [8,9].

Побудовою, розгортанням сенсорних мереж, а також кодуванням даних досліджували науковці, серед яких: А.О. Дружинін, О.В. Жук, С.В. Лєнков, В.О. Романов, В.А. Романюк та інші [11,12].

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 забезпечення: сталого функціонування бездротових сенсорних мереж в умовах складної завадової обстановки; можливостей захисту від кібервпливів в процесі подальшого відновлення функціонування.

Метою статті є аналіз особливостей функціонування і прикладного застосування бездротових сенсорних мереж, а також реалізації необхідних заходів безпеки при функціонування в умовах завадової обстановки та кібервпливу.

Викладення основного матеріалу. 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.

Використання сенсорних мереж у військовій сфері, обумовлена необхідністю виконувати базові функції під впливом дестабілізуючих факторів,

при складній завадовій обстановці та в умовах кібервпливу.

Одним із варіантів для вирішення завдань наземної розвідки є розгортання сітчастих сенсорних мереж.

Можна запропонувати наступну систему організації сітчастих сенсорних мереж, що складаються з шести елементів, кожен з яких все більше спирається на підтримку штучного інтелекту:

- сенсорні елементи, які збирають дані про те, що відбувається;
- елемент зв'язку, який передає інформацію між системами та операторами;
- елемент безпеки, який гарантує, що дані, а також лінії зв'язку, які з'єднують датчики та аналітиків, захищені від підробки, пошкодження або крадіжки даних;
- елемент/елементи обробки, які агрегують і аналізують дані з багатьох джерел для прийняття рішень;
- елемент прийняття рішень, на сьогодні людський, де інформація перетворюється на дію;
- компонент впливу, де інформація і рішення перетворюються на кінетичні та некінетичні ефекти на полі бою або в інших стратегічних заходах.

Одним із ключових наслідків цього є інтеграція різних сфер у спільних операціях, краща взаємодія і синтез військової та невійськової діяльності у загальнонаціональній структурі.

Така будова сенсорної мережі дозволяє виявляти розташування людей на підконтрольній території, вистежування їх переміщення, а також здійснювати моніторинг екології, погоди, обстановки, а головне сприяє запобіганню втрат серед особистого складу під час вирішення бойових завдань.

Термін «сенсорна мережа» (Sensor Network), з'явившись порівняно недавно, але є вже досить усталеним поняттям, що характеризується, стійкістю до відмови окремих елементів мережі. Мережа складається із великої кількості, компактних і дешевих напівпровідникових пристроїв, що об'єднані між собою бездротовим зв'язком. Елементи мережі не обслуговуються і не вимагають спеціальної установки. Кожен вузол мережі може містити вбудовані датчики фізичних параметрів навколишнього середовища, наприклад, руху, рівня вологості повітря, світла, температури, тиску тощо, а також мікросхеми для первинної обробки інформації і зберігання отриманих даних.

Для протидії новим сенсорним технологіям необхідно буде розробити нові види адаптивного камуфляжу, зміни форми транспортних засобів, кібернетичної війни і перешкод.

Загалом, бездротову сенсорну мережу можна охарактеризувати як мережу сенсорів, які спільно контролюють навколишнє середовище та збирають інформацію. Ці мережі забезпечують взаємодію між людьми або комп'ютерами та навколишнім середовищем [3, 4]. Існує три типи пристроїв, які утворюють бездротову сенсорну мережу [5]. Сюди входить координатор мережі (КМ) – у будь-якій мережі може бути лише один. Він розташований у корені дерева мережі. Наступний пристрій – це вузли датчиків або FFD (Fully Function Device – пристрій з повним набором функцій). Вони повністю функціональні і можуть функціонувати як маршрутизатори. Найменші – це сенсори або RFD (Reduced Function Device – пристрій з обмеженим набором функцій). Вони є кінцевими пристроями і не можуть бути маршрутизаторами (рис. 1).

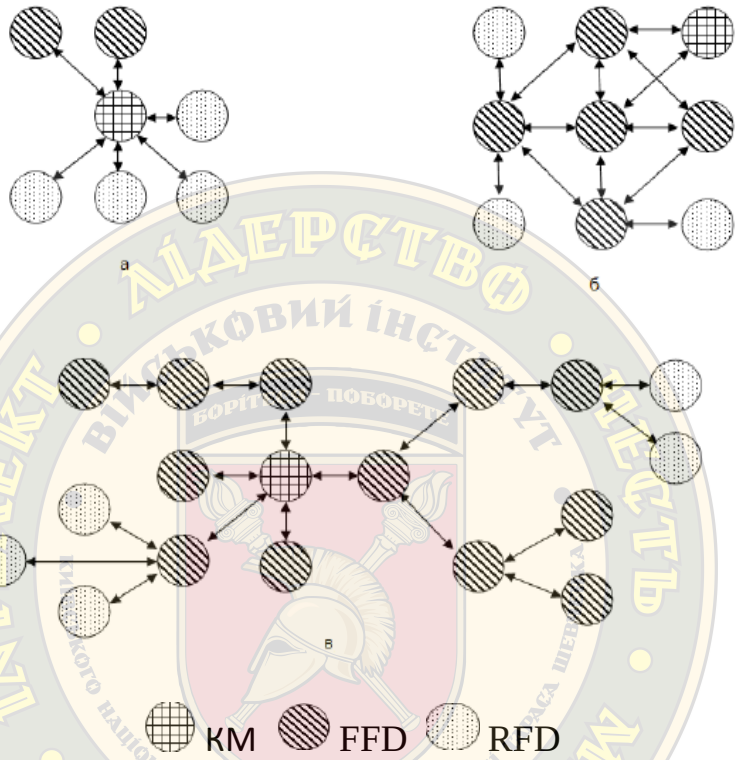

Рисунок 1- Приклади топологій сенсорних мереж

Велика кількість датчиків, випадковим чином розташованих всередині контрольованої зони або поблизу неї, утворюють мережі на основі використання функції самоорганізації. Основним завданням датчиків є контроль фізичних параметрів середовища та передача інформації до інших датчиків за допомогою послідовного методу передачі. Тобто вузли сенсорної мережі є одночасно передавачем і приймачем.

Протягом періоду передачі, дані можуть оброблятися кількома датчиками, щоб перейти до вузла шлюзу після багато каскадної маршрутизації і, нарешті, досягти датчика управління. Користувач здійснює конфігурацію та управління БСМ за допомогою блоку управління. Він встановлює завдання моніторингу та збирає контрольовані дані [6].

Розглядаючи заходи технічного захисту інформації, що циркулює в бездротовій сенсорній мережі, необхідно виявити потенційні загрози безпеці, які поділяються на внутрішні та зовнішні.

До внутрішніх факторів відносяться ненавмисні помилки викликані неправильним налаштування пристроїв, помилки в обслуговуванні або управлінні мережами, збої в живленні, недоліки в програмному забезпеченні, кліматичні умови.

Оскільки БСМ часто розгортаються в неконтрольованих або незахищених фізичних умовах, важливо окремо приділити увагу впливу атак і загроз на вузли та сенсори мережі. Виток інформації через фізичний доступ до вузлів може знищити цілісність і конфіденційність даних, що обробляються. Це ставить під загрозу не тільки окремі компоненти мережі, але й загальну безпеку системи в цілому [7]

До зовнішніх факторів слід віднести фактори штучного впливу такі як DDoS-атаки, MITM-атаки пов'язані з перехопленням та модифікацією даних, що передаються між пристроями. Також противник може здійснювати перехоплення і підробку сигналів змінюючи цілісність інформації або використовувати потужні джерела радіохвиль на тих же частотах, що й мережа, для створення завад у передачі даних.

Розглянемо можливі заходи для захисту сенсорної мережі військового призначення від зовнішніх факторів.

Першим і дуже ефективним способом протидії зовнішнім факторам у бездротовій сенсорній мережі датчиків розвідувального призначення є використання шифрування даних (наприклад AES) для захисту інформації, що передається. Використання нових підходів в методах шифрування, а також покращенні наявних алгоритмів безпеки на мережевому рівні може допомогти уникнути підміни даних маршрутизації та забезпечити додаткову цілісність і конфіденційність даних, тим самим успішно протидіяти атакам типу Black Hole і Selective Forwarding [8].

Також доцільно використовувати потенціал штучного інтелекту (ШІ) для організації кіберзахисту. Системи ШІ мають здійснювати постійний моніторинг трафіку для виявлення аномалій, що можуть вказувати на атаки. Це дасть змогу виявити уразливі місця та виконати певні дії, необхідні для самостійного виправлення. Якщо врахувати високу швидкість, необхідну для проведення будь-якої кібер-операції, очевидно, що тільки механізми ШІ здатен ефективно реагувати на початкових стадіях серйозних кібер-атак. Таким чином, ШІ може впоратися із недоліками традиційних інструментів кібербезпеки. Інший аспект, що має значення для побудови систем кібербезпеки із застосування ШІ – у майбутньому може бути залученний у квантових обчисленнях або високопродуктивних комп'ютерах [9,10].

Крім можливостей ШІ також треба використовувати традиційні інструменти кібербезпеки такі як системи систем виявлення вторгнень (Intrusion Detection System, IDS), система запобігання вторгнень (Intrusion Prevention System, IPS), система захисту кінцевих точок (Endpoint Detection and Response, EDR), система управління інформацією і подіями безпеки (Security Information and Event Management, SIEM) [11]. Їх можливості по виявленню та моніторингу вхідних подій у мережі, таких як нові підключення, потенційні проблеми або незвична активність дають уявлення фахівцю з кібербезпеки своєчасно відстежувати події, виявляти потенційні загрози та реагувати на них [12].

Також необхідно передбачити застосування механізмів автентифікації для підтвердження ідентичності пристроїв у мережі, а також здійснення автентифікації даних, що забезпечує достовірність повідомлень шляхом ідентифікації його походження. Противник не обмежується лише зміною пакета даних. Він може змінити весь пакетний потік, ввівши додаткові пакети. Тому одержувачу необхідно забезпечити, щоб дані, які у будь-якому процесі прийняття рішень, виходили з правильного джерела. З іншого боку, при побудові мережі датчиків автентифікація даних дозволяє одержувачу перевірити, чи дані відправлені заявленим відправником. У разі двостороннього зв'язку автентифікація даних може бути досягнута за допомогою суто симетричного механізму: відправник та одержувач

спільно використовують секретний ключ для обчислення коду автентифікації повідомлення всіх переданих даних [13].

Управління ключами в БСМ є достатньо складним завданням через значну кількість вузлів та обмежені ресурси кожного з них. Розробка механізмів розподілу та оновлення ключів, які адаптуються до змін у топології та управлінню вузлами, є важливою умовою підтримання безпеки мережі в динамічних умовах.

Для захисту від постановки радіозавад слід застосовувати Використання технологій, які підтримують декілька частот або каналів для передачі даних, щоб зменшити вплив інтерференції.

Збільшення кількості сенсорів у мережі додатково створює проблеми з отриманням, зберіганням і передачею даних, оскільки традиційні методи можуть не справлятися із значними об’ємами даних, що постійно генеруються. Використання закодованої передачі сигналів - шифрування, звуження або навпаки розширення спектру сигналів, що передаються - найбільш ефективний спосіб захисту бездротової сенсорної мережі. Застосування технологій стиснення даних та розробка алгоритмів для вибіркової передачі інформації може частково допомогти зменшити навантаження на мережу та оптимізувати її продуктивність. Однак в цьому випадку заходи щодо протидії атакам на бездротові сенсорні мережі, вимагають більш жорстких кроків щодо удосконалення зазначеного підходу [14].

Висновки. Технологія бездротових сенсорних мереж на сьогодні є надзвичайно гнучкою і практичною. Вона використовує інформаційні систем, що надають доступ до інформації в будь-який час незалежно від місця знаходження користувача.

Відсутність провідних комунікацій і мінімальні розміри сенсорних пристроїв дають змогу розгортати мережу в складних умовах. Невизначна структура мережі, зумовлює необхідність передавання маршрутної інформації. Легкість доступу до каналів зв‘язку як вправило може викликати ряд специфічних загроз для БСМ. Для забезпечення надійного функціонування БСМ необхідно застосовувати заходи по захисту даних на всіх рівнях.

Значна кількість атак здійснюється на мережевому рівні, тому при розробці засобів захисту БСМ необхідно враховувати цю особливість. Крім цього, засоби забезпечення безпеки у БСМ мають бути енергоефективним. Під цією вимогою розуміється те, що вузол не повинен виконувати складних обчислень, а також необхідно скоротити часові і енергетичні витрати на обмін повідомленнями.

Робоче середовище БСМ з точки зору надійності має певні недоліки. Складні умови середовища з вузькосмуговим багаточастотним шумом перешкоджають надійному зв'язку через обмежений ресурси каналів.

Використання у методах шифрування нових підходів разом з покращенням наявних алгоритмів безпеки на мережевому рівні дасть змогу уникнути підміни даних та забезпечити їх захищеність від несанкціонованого доступу. Тому в більшості випадків це забезпечить надійне спілкування в режимі реального часу.

Щодо подальших рекомендацій для інноваційного розвитку вітчизняних бездротових сенсорних мереж в секторі безпеки та оборони України слід відмітити можливість досліджень по впровадженню та експлуатації бездротових сенсорних мереж для забезпечення їхньої сумісності з іншими сенсорними системами, та гнучкими автоматизованими системами управління у військовій сфері.

ЛІТЕРАТУРА:

1. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року "Про Стратегічний оборонний бюлетень України"» від 17 вересня 2021 року № 473/2021 URL: https:// https://zakon.rada.gov.ua/laws/show/473/2021#Text (дата звернення:23.06.2023).

2. Опенько П.В., Довженко Н. М. Оріховський П. В., Ікаєв Д. Р. Забезпечення надійності та безпеки у сучасних безпроводових сенсорних мережах на основі впровадження метрики RSS., «Повітряна міць України», Науково практичний журнал, Національний університет оборони, № 1 (6). 2024 С.131-135. Дата звернення: 12 липня 2024. [Онлайн]. Доступно http://sap.nuou.org.ua/issue/view/18099/10998.

3. Прищепа Т.О., Лисенко О.І. Безпроводові сенсорні мережі із мобільними сенсорами. Перспективи телекомунікацій: зб. матер. Міжнар. наук.-техн. конф., м. Київ, 21–25 квітня 2015 року. Київ: НТУУ «КПІ», 2015. URL:http://conferenc.its.kpi.ua/proc/article/view/104177 (дата звернення: 23.06.2023).

4. 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.

5. Tewari N., Bhardwaj A. Flow Statistics Based Detection of Low Rate and High Rate DDoS Attacks // International Journal of Scientific & Engineering Research. 2013. Vol. 4, № 5. P. 348 – 353.

6. Xiao P., He J., Chen Y., Fu Y. A new trusted roaming protocol in wireless mesh networks // International Journalof Sensor Networks. 2013. Vol. 14, Issue 2. P. 109 – 119. doi: 10.1504/IJSNET.2013.056610 89

7. 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.

8. Лепіх Я.І., Гордієнко Ю.О, Дзядевич С.В., Дружинін А.О., Євтух А.А.,. Лєнков С.В., Мельник В.Г., Романов В.О. Створення мікроелектронних датчиків нового покоління для інтелектуальних систем: монографія. Одеса: «Астропринт», 2010. 296 с.

9. 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.

10. Про рішення Ради національної безпеки і оборони України від 20 травня 2016 року "Про Стратегічний оборонний бюлетень України": Указ Президента України від 06.06.2016 № 240/2016. URL: https://www.president.gov.ua/documents/ 2402016-20137 (дата звернення: 23.06.2023).

11. 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.

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

13. Жуковський П.С. Аналіз уразливостей бездротових сенсорних мереж, Державний університет телекомунікаційй «Сучасний захист інформації» № 4(48), 2021 р. С 59-63.

14. Собчук А.В., Коваль М.О., Кравченко Ю.В., Барабаш О.В. Математична модель функціонально стійкої безпровідної сенсорної мережі. Наукове періодичне видання «Системи управління, навігації та зв'язку». Полтава, ПНТУ, 2017. Вип. 6 (46). С. 122 – 126.

REFERENCES:

1. Ukaz Prezydenta Ukrainy (2021) «Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy "Pro Stratehichnyi oboronnyi biuleten Ukrainy"» № 473/2021 Available at: https:// https://zakon.rada.gov.ua/laws/show/473/2021#Text . (accessed 23 January 2023). (in Ukrainian)

2. Openko P.V., Dovzhenko N. M. Orikhovskyi P. V., Ikaiev D. R.(2024) Zabezpechennia nadiinosti ta bezpeky u suchasnykh bezprovodovykh sensornykh merezhakh na osnovi vprovadzhennia metryky RSS. [Ensuring reliability and security in modern wireless sensor networks based on the implementation of the RSS metric.]. *Povitriana mits Ukrainy», Naukovo praktychnyi zhurnal, Natsionalnyi universytet oborony*, -1

(6).131-135. Retrieved from: http://sap.nuou.org.ua/issue/view/18099/10998 (accessed 12 July 2024) (in Ukrainian)

3. PryshchepaT.O., LysenkoO.I. (2015) Bezprovodovi sensorni merezhi iz mobilnymy sensoramy [Wireless sensor networks with mobile sensors]. *Perspektyvy telekomunikatsii*: Materialy naukovo-tekhnichnoi konferentsii. Kyiv: NTUU «KPI». Retrieved from::http://conferenc.its.kpi.ua/proc/article/view/104177 (accessed 23 January 2023)
(in Ukrainian).

4. Zhuk O. V., Romaniuk V. A., Sova O. Y., (2016) Metodolohichni osnovy upravlinnia perspektyvnymy neodnoridnymy bezprovodovymy sensornymy merezhamy taktychnoi lanky upravlinnia viiskamy [Methodological foundations of management of prospective heterogeneous wireless sensor networks of the tactical link of military command]. *Priorytetni napriamky rozvytku telekomunikatsiinykh system ta merezha spetsialnoho pryznachennia* // K.: VITI NTUU «KPI» 2016. 5. 34 - 44. (in Ukrainian)

5. Tewari N., Bhardwaj A. (2013) Flow Statistics Based Detection of Low Rate and High Rate DDoS Attacks *International Journal of Scientific & Engineering Research.* Vol. 4, 5. 348-353. (in English)

6. Xiao P., He J., Chen Y., Fu Y. A(2013) A new trusted roaming protocol in wireless mesh networks .*International Journalof Sensor Networks*,14, Issue 2. P. 109 -119. (in English) https:// doi.org/ 10.1504/IJSNET.2013.056610 89

7. Minochkin A.I., Romaniuk V.A., Zhuk O.V. (2007) Perspektyvy rozvytku taktychnykh sensornykh merezh [Prospects for the development of tactical sensor networks]. *Zbirnyk naukovykh prats VITI NTUU "KPI"* 2007, 4, 16-22. (in Ukrainian)

8. Lepikh Ya.I., Hordiienko Yu.O, Dziadevych S.V., Druzhynin A.O., Yevtukh A.A.,. Lienkov S.V., Melnyk V.H., Romanov V.O. (2010). *Stvorennia mikroelektronnykh datchykiv novoho pokolinnia dlia intelektualnykh system* [Creation of new generation microelectronic sensors for intelligent systems]. Odesa: "Astroprint". (in Ukrainian)

9. Lepikh Ya.I., Hordiienko Yu.O, Dziadevych S.V., Druzhynin A.O., Yevtukh A.A.,. Lienkov S.V., Melnyk V.H., Protsenko V.O., Romanov V.O. (2011). *Intelektualni vymiriuvalni systemy na osnovi mikroelektronnykh datchykiv novoho pokolinnia* [Intelligent measuring systems based on new generation microelectronic sensors]. Odesa: "Astroprint". (in Ukrainian)

10. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy (2016) "Pro Stratehichnyi oboronnyi biuleten Ukrainy": Ukaz Prezydenta Ukrainy vid 06.06.2016 №240/2016. Available at: https://www.president.gov.ua/documents. (accessed 23 January 2023). (in Ukrainian)

11. Lepikh Ya.I., Hordiienko Yu.O, Dziadevych S.V., Druzhynin A.O., Yevtukh A.A.,. Lienkov S.V., Melnyk V.H., Protsenko V.O., Romanov V.O. (2011). *Mikroelektronni datchyky novoho pokolinnia dlia intelektualnykh system.* [New generation microelectronic sensors for intelligent systems.] Odesa: "Astroprint". (in Ukrainian)

12. Lenkov S.V., Lepikh Ya.I., Mokrytskyi V.A., Sieliukov O.V., Smyntyna V.A V.O. za zah. red. Mokrytskoho V.A., Lienkova S.V. (2009). *Napivprovidnykovi optychni ta akustoelektronni sensory i systemy.* [Semiconductor optical and acoustoelectronic sensors and systems]. Odesa: "Astroprint". (in Ukrainian)

13. Zhukovskyi P.S.(2021) *Analiz urazlyvostei bezdrotovykh sensornykh merezh* [Vulnerability analysis of wireless sensor networks] Derzhavnyi universytet telekomunikatsiii «Suchasnyi zakhyst informatsii» 4(48), 59-63. (in Ukrainian)

14. Sobchuk A.V., Koval M.O., Kravchenko Yu.V., Barabash O.V. (2017) Matematychna model funktsionalno stiikoi bezprovidnoi sensornoi merezhi [Mathematical model of a functionally stable wireless sensor network] *Naukove periodychne vydannia «Systemy upravlinnia, navihatsii ta zviazku»*. Poltava, PNTU, 6 (46) 122-126. (in Ukrainian)

Ph.D. Okhramovych M.M., Ph.D.,Gakhovych S.V., Ph.D. Koval M.O
Ph.D. Kravchenko O.I.

ANALYSIS AND ASSESSMENT OF SENSOR NETWORK FUNCTIONING FEATURES UNDER JAMMING CONDITIONS AND CYBER INFLUENCE

This article analyzes modern sensor networks and examines the basic principles of their construction and application in military systems. Special attention is given to wireless sensor networks (WSNs) as a promising technology for implementing crucial aspects of military policy. This advancement has been made

possible due to the miniaturization of components and increased computational power. Sensor networks consist of a large number of low-power, multifunctional devices deployed in a specific geographical area. Although most elements of such a network have limited physical resources, when combined, they can quickly configure to perform a wide range of functional tasks such as protecting critical infrastructure and monitoring the environment.

However, with their development and transformation, issues of information security are increasingly being researched, as risks of unauthorized access or interference can seriously undermine the effectiveness and reliability of these technologies. It should be noted that due to the open nature of information transmission, there is a need to update encryption and authentication methods.

An overview of the features of sensor network functioning under jamming conditions and cyber influence is proposed, highlighting their application as highly efficient and promising solutions in information collection systems. The ability to deploy networks in challenging conditions, the absence of wired communications, and the minimal size of sensor devices make sensor network technology extremely flexible and practical. It allows for the maximum utilization of information systems, providing access to information at any time, regardless of the user's location.

Keywords: *wireless sensor network, network coordinator, sensors, routers, information systems.*

Ph.D. Okhramovych M.M., Ph.D.,Gakhovych S.V.,
Ph.D. Koval M.O, Ph.D. Kravchenko O.I.

ANALYSIS AND ASSESSMENT OF SENSOR NETWORK FUNCTIONING FEATURES UNDER JAMMING CONDITIONS AND CYBER INFLUENCE

This article analyzes modern sensor networks and examines the basic principles of their construction and application in military systems. Special attention is given to wireless sensor networks (WSNs) as a promising technology for implementing crucial aspects of military policy. This advancement has been made possible due to the miniaturization of components and increased computational power. Sensor networks consist of a large number of low-power, multifunctional devices deployed in a specific geographical area. Although most elements of such a network have limited physical resources, when combined, they can quickly configure to perform a wide range of functional tasks such as protecting critical infrastructure and monitoring the environment.

However, with their development and transformation, issues of information security are increasingly being researched, as risks of unauthorized access or interference can seriously undermine the effectiveness and reliability of these technologies. It should be noted that due to the open nature of information transmission, there is a need to update encryption and authentication methods.

An overview of the features of sensor network functioning under jamming conditions and cyber influence is proposed, highlighting their application as highly efficient and promising solutions in information collection systems. The ability to deploy networks in challenging conditions, the absence of wired communications, and the minimal size of sensor devices make sensor network technology extremely flexible and practical. It allows for the maximum utilization of information systems, providing access to information at any time, regardless of the user's location.

Keywords: *wireless sensor network, network coordinator, sensors, routers, information systems.*