УДК: 621.396.4
DOI: **10.33099/2311-7249/2025-52-1-85-92**

АРТЮХ Сергій Григорович,
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна,
https://orcid.org/0000-0003-2142-1552

ФУНКЦІОНАЛЬНА МОДЕЛЬ ПІДСИСТЕМИ БЕЗПЕКИ СИСТЕМИ УПРАВЛІННЯ БЕЗПРОВОДОВИМИ СЕНСОРНИМИ МЕРЕЖАМИ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

Розвиток сучасних інформаційно-комунікаційних технологій у військовій сфері потребує вдосконалення систем управління безпроводовими сенсорними мережами. Ефективне поєднання процесів моніторингу та телекомунікації із гарантуванням конфіденційності, цілісності, доступності та автентифікації інформації можливе лише за наявності комплексної системи управління безпроводовими сенсорними мережами, важливою складовою якої є підсистема безпеки.

***Метою статті** є розроблення функціональної моделі підсистеми безпеки системи управління безпроводовими сенсорними мережами військового призначення для забезпечення безпеки їх функціонування та оптимізації її впливу на інші підсистеми системи управління на всіх рівнях мережі.*

***Методи дослідження.** Під час написання статті використано методи аналізу та синтезу. Зазначений методологічний підхід дає змогу визначити цільові функції підсистеми безпеки та математично формалізувати процес забезпечення безпеки системи управління безпроводових сенсорних мереж військового призначення.*

***Отримані результати дослідження.** Проведено аналіз наукових публікацій та визначено, що модель системи безпеки з повним перекриттям (модель Клементса – Хоффмана), що спирається на теорію графів, нечітких множин, ймовірностей вважається основою для формалізації процесу функціонування систем безпеки. Розроблено функціональну модель підсистеми безпеки, що складається з таких модулів: аутентифікації й управління доступом, шифрування, виявлення і запобігання вторгненням, управління політиками безпеки та оновлення програмного забезпечення й відновлення. Наведена модель, що забезпечує повне перекриття загроз, формалізована у вигляді математичного опису, що підвищує рівень стійкості мережі до атак.*

***Елементи наукової новизини.** Науковою новизною роботи є синтез існуючих методів захисту і механізмів безпеки в єдину підсистему, що дає змогу комплексно оцінювати та мінімізувати ризики від атак для безпроводової сенсорної мережі військового призначення. Запропонований підхід забезпечує адаптивність та інтегрується в існуючі системи управління.*

***Теоретична й практична значущість.** Теоретичною значущістю дослідження є розвиток методів математичного моделювання загроз та побудова стійкої архітектури управління безпекою безпроводових сенсорних мереж. Практична цінність результатів дослідження полягає у можливості їх впровадження у військових і спеціальних системах зв'язку, що забезпечує підвищену захищеність критичних інформаційно-комунікаційних систем у сучасних умовах.*

***Ключові слова:** безпроводові сенсорні мережі, система управління, підсистема безпеки, функціональна модель управління, атака, виявлення вторгнень, управління безпекою.*

Вступ

Постановка проблеми. Сучасний розвиток інформаційно-комунікаційних технологій та їх активне застосування у військовій сфері зумовлює необхідність удосконалення систем управління безпроводовими сенсорними мережами (далі – БСМ). БСМ є невід'ємною частиною сучасних тактичних систем моніторингу, спостереження та збору даних у реальному часі. Однак зростання складності архітектури мереж, розширення спектру завдань і посилення загроз кібернетичної безпеки ставлять нові виклики перед розробниками таких систем.

Безпроводові сенсорні мережі є ключовим компонентом сучасних інформаційно-комунікаційних систем, що забезпечують моніторинг, збір та передачу даних у режимі реального часу. Військове та спеціальне призначення таких мереж вимагає не лише ефективного управління ресурсами, а й високого рівня безпеки, надійності та адаптивності до змінних умов експлуатації [1].

Призначення системи управління БСМ полягає в координації роботи сенсорних вузлів, оптимізації використання ресурсів, забезпеченні безперервного зв'язку та захисті від зовнішніх загроз. Основні завдання містять моніторинг стану мережі, балансування навантаження, адаптивну маршрутизацію даних, управління енергоспоживанням та інтеграцію механізмів безпеки.

Тому координація функціонування підсистем моніторингу та телекомунікації з одночасним забезпеченням вимог безпеки (конфіденційність, цілісність, доступність, автентифікація) БСМ військового призначення не можливе без ефективної системи управління у складі якої передбачається реалізація підсистеми безпеки.

Аналіз останніх досліджень і публікацій. Функціональна модель системи управління БСМ для забезпечення оптимального використання ресурсів, адаптивності до змін умов експлуатації, високої надійності й безпеки функціонування запропоновано у статті [1]. Наведена удосконалена модель передбачає структуризацію системи на рівні сенсорів, обробки даних та передачі інформації й складається з відповідних підсистем, зокрема, введеної підсистеми управління безпекою. Однак, в зазначеній роботі не розглянуто архітектуру підсистеми безпеки та не визначено функції її елементів.

У [2] проведений аналіз безпеки мобільних радіомереж або Mobile Ad-Hoc Networks (MANET), визначені основні вразливості, проведено класифікацію існуючих атак та оцінювання загроз для таких мереж, а також проаналізовано механізми забезпечення безпеки. Також у статті [3] на основі аналізу існуючих вразливостей та вимог із безпеки авторами запропоновано удосконалену класифікацію атак на складові (підсистеми) системи управління (далі – СУ) БСМ, що дає змогу запропонувати методи захисту, які спрямовані на запобігання визначеним видам атак і механізмам протидії загрозам під час проєктування БСМ.

У статті [4] проведений аналіз варіантів побудови систем виявлення атак у мобільних радіомережах, сформовані вимоги до їх функціональності та наведено варіанти архітектури. Такий підхід може бути використаний і для підсистем управління безпекою СУ БСМ з урахуванням особливостей функціонування таких мереж.

У роботі [5–7] проаналізовано переваги й недоліки різних методів і механізмів захисту БСМ, зокрема, алгоритмів шифрування й розподілу ключів, механізмів довіри та автентифікації й інших контрзаходів для протидії атакам на БСМ. Проте, авторами не враховуються специфіка застосування БСМ у військовій сфері.

За результатами аналізу наукових публікацій [1–7] можна зробити висновок, що невирішеними залишаються питання стосовно функціонування підсистеми безпеки системи управління БСМ, а розроблення функціональної моделі такої підсистеми є важливим науковим завданням.

Для вирішення зазначеної проблематики пропонується використати підхід розглянутий у [8], де розглядається модель системи безпеки з повним перекриттям (модель Клементса – Хоффмана), що спирається на теорію графів, нечітких множин, ймовірностей та вважається основою для формалізації функціонування систем безпеки. Основним положенням зазначеної моделі є вимога, що система, спроєктована на її основі, має як мінімум один реалізований механізм (метод, спосіб) для забезпечення безпеки на кожному можливому шляху проникнення зловмисником у систему.

Метою статті є розроблення функціональної моделі підсистеми безпеки системи управління безпроводовими сенсорними мережами військового призначення для забезпечення безпеки їх функціонування та оптимізації її впливу на інші підсистеми системи управління на всіх рівнях мережі.

Виклад основного матеріалу дослідження

У моделі системи безпеки з повним перекриттям (Клементса – Хоффмана) розглядається взаємодія «області загроз», «області, що захищається» та «системи захисту». Вважається, що несанкціонований доступ (як будь-який доступ, що порушує заявлену політику безпеки) до кожного з набору об’єктів області, що захищається, пов’язаний з деякою величиною збитку, що може бути визначений кількісно (інакше його вважають рівним певній умовній величині). Водночас, кількісна категорія збитків може бути виражена у вартісному еквіваленті (сума фінансових втрат), або в термінах, пов’язаних із цільовою функцією системи (наприклад, часу, необхідного для відновлення функціональних можливостей БСМ після зловмисного впливу) [8].

Для опису підсистеми безпеки СУ БСМ на основі моделі системи безпеки з повним перекриттям використаємо множину об’єктів захисту (підсистеми системи управління БСМ) $O=\{o_j\}$, $j=1, ..., J$), характерною для об’єктів множиною атак ($A=\{a_i\}$, $i=1, ..., I$) та множину заходів забезпечення безпеки заходів безпеки ($M=\{m_k\}$, $k=1, ..., K$), які можуть бути реалізовані в підсистемі безпеки.

Слід зазначити, що пасивні атаки не мають впливу на СУ БСМ, водночас активні атаки можуть бути спрямовані на такі підсистеми управління [3]:

моніторингом – впливають на розгортання, покриття, виявлення та ідентифікацію об’єктів та якість моніторингу;

топологією – перешкоджають побудові та підтримці топології БСМ відповідно до потенційних можливостей та наявних ресурсів мережі;

маршрутизацією – впливають на побудову та підтримку маршрутів передачі заданої якості за виконання вимог до їх функціонування, типу трафіка, цільових функцій управління;

радіоресурсом – порушують розподіл часового, просторового, частотного, кодового ресурсів для забезпечення інформаційного обміну між сусідніми вузлами;

якістю обслуговування – перешкоджають передачі певних класів трафіка із заданою якістю обслуговування (Quality of Service, QoS);

енергоресурсом вузлів – збільшують споживання енергії вузлами мережі на будь-якому рівні еталонної моделі взаємодії відкритих систем.

Отже, за рівнями моделі взаємодії відкритих систем, визначимо перелік атак a_i, спрямованих на наведені вище підсистеми СУ БСМ [4]:

a_1 – шкідливе програмне забезпечення. Впровадження вірусів або інших зловмисних програм для саботажу мережі;

a_2 – DoS-атака на маршрутизацію. Навмисне спрямування трафіку на певні вузли для їхнього перевантаження;

a_3 – перенавантаження. Надсилання надмірної кількості трафіку для зниження якості обслуговування всієї мережі;

a_4 – десинхронізація. Порушення роботи механізмів синхронізації мережі;

a_5 – затоплення. Надсилання великої кількості запитів для перевантаження мережі;

a_6 – визначення топології мережі. Аналіз широкомовних запитів для ідентифікації важливих вузлів у мережі;

a_7 – модифікація маршрутної інформації. Вузол порушує обмін маршрутною інформацією між іншими вузлами для створення петель або інших проблем у мережі;

a_8 – тунелювання. Створення прихованого каналу зв'язку між різними сегментами мережі для обходу захисних механізмів маршрутизації;

a_9 – атака чорної діри. Вузол заявляє, що має найкоротший маршрут, а потім поглинає весь трафік;

a_{10} – вибіркова передача. Скомпрометований вузол навмисно ігнорує певні пакети або змінює;

a_{11} – атака Hello Флуд. Відправлення підроблених Hello-пакетів для зміни топології мережі;

a_{12} – атака воронки. Вузол діє як базова станція та концентрує на собі якомога більше трафіку;

a_{13} – атака Сивілли. Вузол маскується під кілька пристроїв, щоб отримати більше можливостей у мережі;

a_{14} – нерівномірність доступу. Надсилання великої кількості пріоритетних запитів для зниження пропускної здатності та блокування каналу для інших вузлів;

a_{15} – колізії. Навмисне створення конфліктів у мережі для зменшення її пропускної здатності;

a_{16} – виснаження ресурсів. Генерування та надсилання надмірної кількості трафіку для примусового виснаження батарей сенсорів;

a_{17} – створення завад. Випромінювання сигналів високої потужності для глушіння зв'язку між вузлами. Надсилання шкідливого трафіку для порушення роботи мережі;

a_{18} – фізичні атаки. Захоплення або підміна вузла фальшивим пристроєм для отримання конфіденційних даних. Фізичне знищення (пошкодження) вузла для порушення топології мережі.

Складові системи управління БСМ [1] позначимо як об'єкти захисту $o_j \in O$:

o_1 – підсистема управління моніторингом;

o_2 – підсистема управління топологією;

o_3 – підсистема управління маршрутизацією;

o_4 – підсистема управління енергоресурсу вузлів;

o_5 – підсистема управління радіоресурсом;

o_6 – підсистема управління якістю обслуговування.

У разі відсутності підсистеми безпеки безпосередній вплив атак на підсистеми СУ можна навести у вигляді дводольного графа (рис. 1). Слід зазначити, що елементи наведених вище множин $O=\{o_j\}$ та $A=\{a_i\}$ перебувають між собою у певних відношеннях, водночас зв'язки між атаками і об'єктами захисту не є однолінійними. Атака $a_i \in A$ може поширюватися на будь-яку кількість об'єктів O, а на об'єкт $o_j \in O$ може здійснювати більше ніж одна атака a_i. Їх взаємозв'язок наведено у вигляді множини дуг $\{a_i, o_j\}$, існуючих тільки тоді, коли a_i є атакою, спрямованою на порушення безпеки об'єкта $o_j \in O$.

За результатами аналізу існуючих механізмів (методів, способів) безпеки БСМ, методів [4-7] протидії атакам та впливів атак на систему управління БСМ (рис. 1) пропонується до підсистем безпеки віднести такі модулі:

аутентифікації та управління доступом – здійснює перевірку ідентичності користувачів та пристроїв, забезпечує їх доступ до ресурсів мережі;

шифрування забезпечує шифрування даних, які передаються між вузлами та базовою станцією, для захисту конфіденційності й цілісності інформації;

виявлення та запобігання вторгненням (IDS/IPS) – виявляє атаки на мережу та спроби несанкціонованого доступу, автоматично блокує зловмисні дії та/або сповіщає адміністраторів для подальшого реагування;

управління політиками безпеки – здійснює централізоване керування політиками безпеки, правилами і налаштуваннями мережі (маршрутизацією, зміною радіочастот тощо);

оновлення програмного забезпечення та відновлення – відповідає за оновлення програмного забезпечення (далі – ПЗ) вузлів та базової станції, що забезпечує своєчасне усунення вразливостей, резервне копіювання даних, здійснює швидке відновлення мережі після збоїв або інцидентів.

Для розроблення функціональної моделі підсистеми безпеки СУ БСМ розглянемо взаємодію модулів підсистеми безпеки з відповідними підсистемами системи управління.

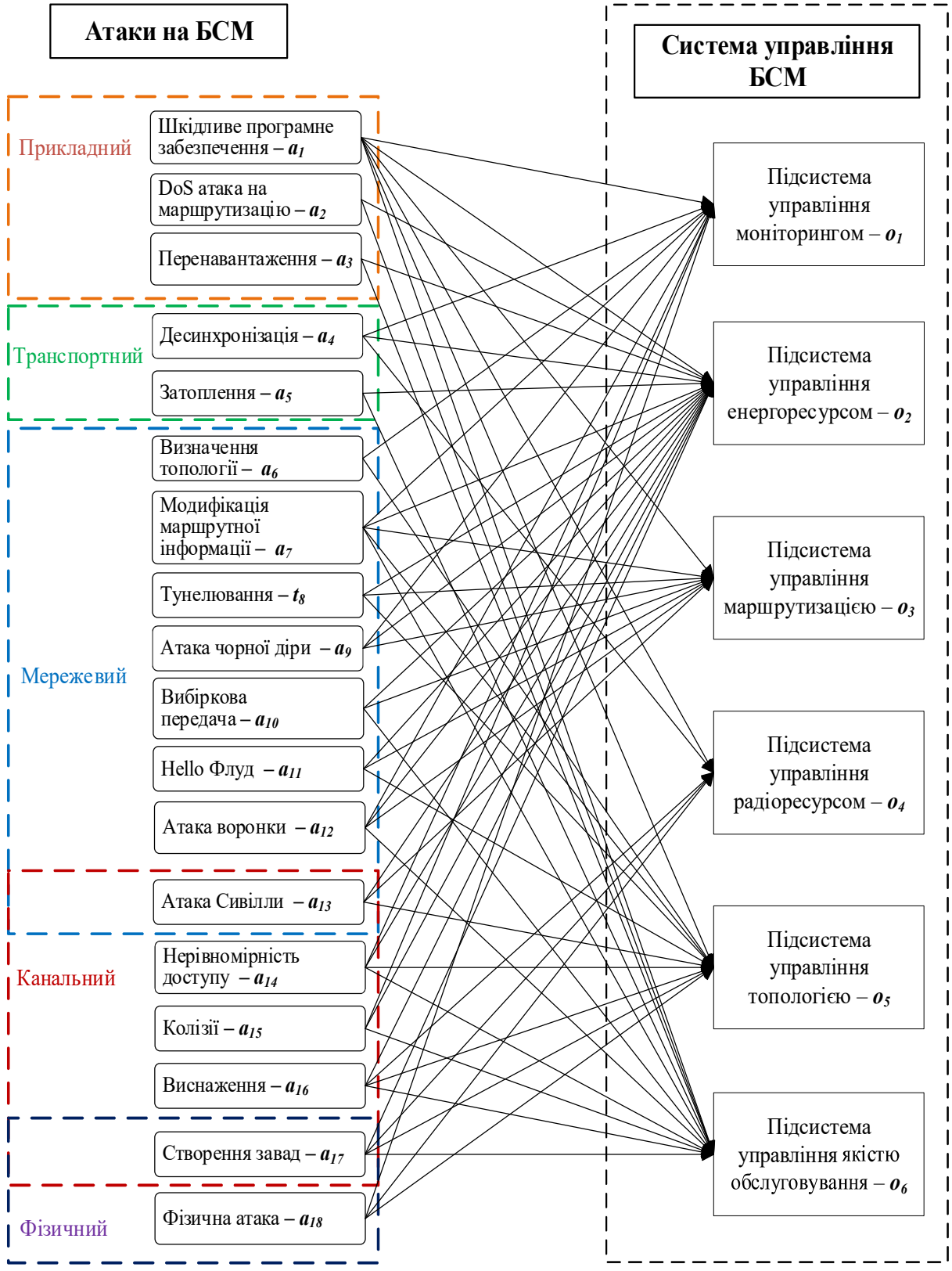

Рисунок 1 – Безпосередній вплив атак на систему управління безпроводових сенсорних мереж військового призначення

Модуль аутентифікації та управління доступом може обмежити кількість вузлів, що беруть участь у маршрутизації, оскільки неавторизовані вузли не допускаються до передачі трафіку. Це зменшує кількість доступних маршрутів і може впливати на надійність передачі даних (підсистема управління маршрутизацією). Перевірка відповідності цифрових підписів та надання доступу вимагають додаткових

обчислювальних ресурсів та збільшення енергоспоживання (підсистема управління витратами енергоресурсу вузлів). Процеси аутентифікації можуть створювати додаткові затримки при встановленні з'єднань, що впливає на QoS-критичні сервіси, такі як передача відео та голосових даних (підсистема управління якістю обслуговування). Якщо процес аутентифікації займає багато часу, це може спричинити затримки у зборі даних, що є критичним для функціонування у реальному часі (підсистема управління моніторингом).

Модуль шифрування впливає на ефективність маршрутизації через додаткові затримки під час обробки пакетів. Це може спричинити збільшення часу передачі даних та вплинути на вибір маршрутів.(підсистема управління маршрутизацією). Крім того, шифрування збільшує час передачі даних, що може вплинути на критичні сервіси в реальному часі або команд управління (підсистема управління якістю обслуговування). Процес шифрування даних потребує додаткових обчислювальних ресурсів, що призводить до підвищеного споживання енергії сенсорами. (підсистема управління витратами енергоресурсу).

Модуль виявлення та запобігання вторгненням (IDS/IPS) постійно аналізує мережевий трафік і поведінку вузлів, що потребує додаткових обчислювальних ресурсів і, відповідно, збільшує споживання енергії сенсорами(підсистему управління витратами енергоресурсу вузлів). Якщо він виявляє зловмисний вузол або атаку на маршрутизацію, модуль може блокувати або змінювати маршрути для обходу потенційної загрози (підсистему управління маршрутизацією). У разі виявлення нормальних потоків даних, він може обмежити їхню швидкість або заблокувати підозрілі вузли. Це може зменшити пропускну здатність для легітимного трафіку та викликати затримки (підсистема управління якістю обслуговування). Модуль IDS/IPS може погіршити точність моніторингу шляхом блокування зловмисних або підозрілих вузлів (підсистема управління моніторингом). Також блокування цих вузлів може перебудувати структуру мережі (підсистема управління топологією). У разі виявлення глушіння сигналу або перехоплення радіоканалів мережа може автоматично змінювати частоти або зменшувати потужність передачі, що впливає на ефективність використання радіоресурсів (підсистема управління радіоресурсом).

Модуль управління політиками безпеки може змінювати критерії вибору маршрутів, оминаючи вузли з низьким рівнем довіри та створювати більш безпечні, але довші шляхи (підсистема управління маршрутизацією). Цей модуль може обмежувати певні типи трафіку або накладати додаткові перевірки, що впливає на затримки та пропускну здатність (підсистема управління якістю обслуговування). Політики безпеки можуть вимагати зниження потужності передачі для зменшення ризику перехоплення сигналу, що впливає на радіус покриття мережі (підсистема управління радіоресурсом). Модуль визначає, які вузли вважаються довіреними та можуть формувати топологію та зв'язність мережі(підсистема управління топологією).

Функціонування *модуля оновлення програмного забезпечення та відновлення* може тимчасово знижувати продуктивність мережі через завантаження великих обсягів даних або перезапуск вузлів(підсистема управління якістю обслуговування та підсистема управління топологією). Процес оновлення ПЗ потребує завантаження, перевірки, встановлення та перезапуску вузлів, що спричиняє додаткові витрати енергії (підсистема управління витратами енергоресурсу вузлів).

З урахуванням наведеної взаємодії модулів підсистеми безпеки з відповідними підсистемами системи управління БСМ цільову функцію підсистеми безпеки, що максимізує рівень загальної безпеки системи за гарантованого виконання мінімальних вимог до кожної її складової не знижуючи загальну продуктивність мережі доцільно визначити через зважену суму рівнів безпеки всіх підсистем:

$$max\ S_{заг} = w_1 S_{аут} + w_2 S_{шифр} + w_3 S_{СВВ} + w_4 S_{пб} + w_5 S_{онов}, \quad (1)$$

де $S_{аут}$ – рівень успішної аутентифікації пристроїв;

$S_{шифр}$ – рівень захисту шифруванням;

$S_{СВВ}$ – ефективність виявлення атак;

$S_{пб}$ – рівень відповідності політикам безпеки;

$S_{онов}$ – рівень оновлення ПЗ та відновлення;

w_1, w_2, w_3, w_4, w_5 – вагові коефіцієнти, що характеризують важливість кожної підсистеми та визначаються експертним шляхом.

За аналогією з моделлю з повним перекриттям (Клементса–Хоффмана) визначимо модулі безпеки для СУ БСМ:

m_1 – модуль аутентифікації та управління доступом;

m_2 – модуль шифрування;

m_3 – модуль виявлення та запобігання вторгненням (IDS/IPS);

m_4 – модуль управління політиками безпеки;

m_5 – модуль оновлення програмного забезпечення та відновлення.

Захист СУ БСМ забезпечується перекриттям всіх можливих дуг графа, завдяки використанню відповідного засобу захисту. У результаті дводольний граф (рис. 1) перетворюється в тридольний, що відображає функціональну модель підсистеми безпеки СУ БСМ (рис. 2).

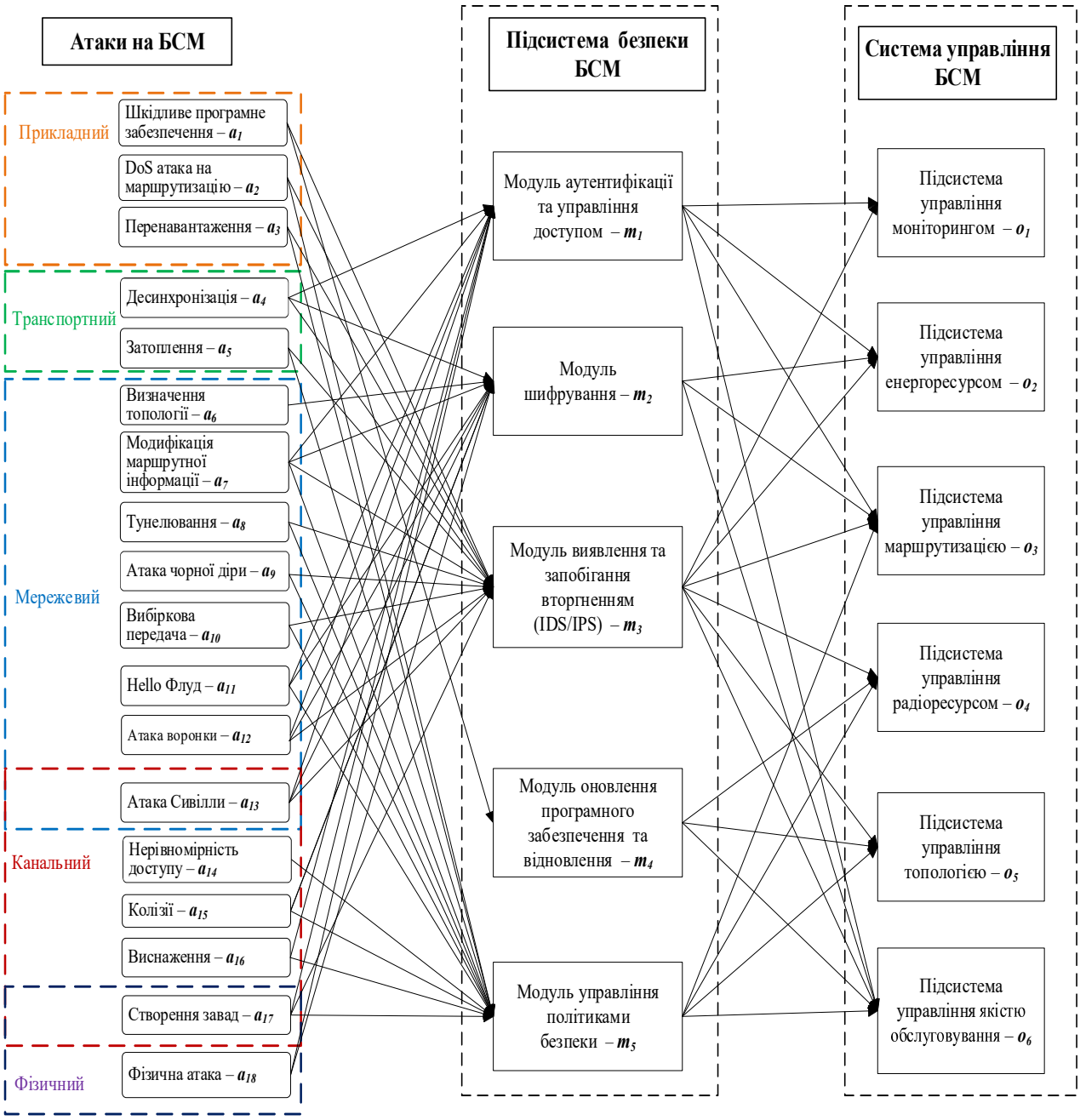

Рисунок 2 – Функціональна модель підсистеми безпеки системи управління безпроводових сенсорних мереж військового призначення

У захищеній системі всі дуги моделі видаються у вигляді (t_i , m_k) і (m_k, o_j). За таких умов слід зазначити, що один і той же модуль підсистеми безпеки може перекривати більше ніж одну атаку та/або захищати більше ніж один об'єкт. Для формалізації базового рівня безпеки СУ БСМ використаємо 5-мірний кортеж (п'ятірки) [8]:

$$S = \{O, A, M, V, B\}, \qquad (2)$$

де $O=\{o_j\}$, $j=1, ..., 6$ – множина об'єктів захисту СУ БСМ;

$A=\{a_i\}$, $i=1, ..., 18$ – множина атак на систему управління БСМ;

$M=\{m_k\}$, $k=1, ..., 5$ – множина заходів безпеки (кількість модулів підсистеми безпеки СУ БСМ).

$V=A\times O=\{v_r=(a_i, o_j), r=1, ..., R\}$ – множина вразливостей, що являють собою декартовий добуток впорядкованих пар та характеризують шляхи реалізації атак A відповідно до об'єктів O;

$B=V\times M=A\times O\times M=\{b_l=(a_i, o_j, m_k), l=1, ..., \Lambda\}$ – множина механізмів захисту, що являють собою декартовий добуток упорядкованих трійок та відображають у яких точках потрібно здійснити захист.

Для формалізованої моделі (2) умову повного перекриття можна визначити за таким виразом:

$$\forall (v_r = (a_i , o_j)) \in V, \exists (b_l = (a_i , o_j, m_k))) \in B. \qquad (3)$$

Умова (3) означає, що для кожної реалізації атаки a_i відносно множини об'єктів захисту O засобом безпеки m_k створюється механізм захисту b_l, що нейтралізує атаку для конкретного об'єкта o_j. Тому, рис 2 відображає розроблену функціональну модель підсистеми безпеки системи управління БСМ, а вирази (2) та (3) математично формалізують запропоновану модель, що забезпечує базовий рівень безпеки такої системи.

Висновки й перспективи подальших досліджень

Функціональна модель підсистеми безпеки системи управління безпроводовими сенсорними мережами військового призначення базується на відомій концепції повного перекриття (Клементса – Хоффмана), що забезпечує комплексний підхід до захисту всіх рівнів системи управління такими мережами. Розроблена модель враховує існуючі механізми (методи, способи) захисту й складається з модулів аутентифікації та управління доступом, шифрування, виявлення та запобігання вторгненням, управління політиками безпеки, а також оновлення програмного забезпечення та відновлення. Впровадження цих модулів у підсистему безпеки системи управління дає змогу підвищити стійкість безпроводової сенсорної мережі військового призначення до атак, забезпечуючи надійність передачі даних та стійкість системи до змінних умов експлуатації.

Формалізовано базовий та загальний рівень безпеки системи управління, що дасть змогу в подальшому оцінювати ефективність запропонованих засобів захисту. Математично обґрунтована модель підсистеми безпеки для безпроводових сенсорних мереж військового призначення може бути використана під час розроблення та вдосконалення систем управління такими мережами.

Основними напрямами подальшого дослідження є розроблення (удосконалення) методів і методик автоматичного виявлення аномалій та вторгнень із використанням технологій штучного інтелекту для адаптивного управління безпекою в умовах динамічної зміни мережевої топології та загроз.

Список бібліографічних посилань

1. Жук О. В., Машталір В. В., Грозовський Р. І., Чекан А. Ю. Функціональна модель системи управління бездротовими сенсорними мережами військового призначення. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2024. № 3(51). С. 146–154. DOI: https://doi.org/10.33099/2311-7249/2024-51-3-146-154.

2. Міночкін А. І., Романюк В. А. Безпека мобільних радіомереж. *Збірник наукових праць ВІТІ НТУУ «КПІ».* 2004. Вип. № 5. С. 116–126. **3. Артюх С. Г., Жук О. В., Чернега В. М.** Класифікація атак у безпроводових сенсорних мережах тактичної ланки управління військами. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2023. № 3(48). С. 11–19. DOI: https://doi.org/10.33099/2311-7249/2023-48-3-11-19. **4. Міночкін А. І., Романюк В. А., Шаціло П. В.** Виявлення атак в мобільних радіомереж. *Збірник наукових праць ВІТІ НТУУ «КПІ».* 2005. Вип. № 1. С. 102–111. **5. Gautam A. K., Kumar R.** A comprehensive study on key management, authentication and trust management techniques in wireless sensor networks. *SN Applied Sciences*. 2021. №1(3). DOI: https://doi.org/10.1007/s42452-020-04089-9 (accessed: 17.03.2025). **6. Rehman A. U. et al.** A Survey on MAC-Based Physical Layer Security over Wireless Sensor Network. *Electronics*. 2022. № 16(11). P. 2529. DOI: 10.3390/electronics11162529 . **7. Jain U., Hussain M.** Wireless Sensor Networks: Attacks and Countermeasures. *SSRN Electronic Journal*. 2018. DOI: 10.2139/ssrn.3170185. **8. Hoffman L. J., Clements D.** Fuzzy computer security metrics: A preliminary report. Memorandum No. ERLM77/6. 27 January 1977. Electronics research laboratory. College of Engineering University of California, Berkeley. 20 p. URL: https://www2.eecs.berkeley.edu/Pubs/TechRpts/1977/ERL-m-77-6.pdf. (accessed: 17.03.2025).

FUNCTIONAL MODEL OF THE SECURITY SUBSYSTEM OF THE CONTROL SYSTEM OF WIRELESS SENSOR NETWORKS FOR MILITARY PURPOSES

ARTIUKH Serhii, Military Institute of Telecommunications and Information Technologies named after Heroes of Kruty, Kyiv, Ukraine, https://orcid.org/0000-0003-2142-1552

Formulation of the problem in general. *The development of modern information and communication technologies in the military requires improving wireless sensor network management systems. An effective combination of monitoring and telecommunication processes with the guarantee of confidentiality, integrity, availability and authentication of information is possible only if there is a comprehensive wireless sensor network management system, an essential component of which is the security subsystem. The aim is to develop a functional model of the security subsystem of the military wireless sensor network management system to ensure the security of its operation and optimise its impact on other subsystems of the management system at all levels of the network.*

Analysis of recent research and publications*. The scientific sources analyse the security of mobile radio networks, options for building attack detection systems, and identify the advantages and disadvantages of various methods and mechanisms for protecting wireless sensor networks. Based on the results, it is concluded that there are still unresolved issues regarding the functioning of the security subsystem of these networks.*

Presenting the primary material. *An analysis of scientific publications is carried out, and it is determined that the model of a security system with complete overlap (Clements-Hoffman model), based on the theory of graphs, fuzzy sets, and probabilities, is considered the basis for formalising the description of the functioning of security systems. A*

functional model of the security subsystem has been developed, consisting of the following modules: authentication and access control, encryption, intrusion detection and prevention, security policy management, and software update and recovery. This model, which provides complete overlap of threats, is formalised in the form of a mathematical description, increasing network resistance to attacks.

Elements of scientific novelty. *The scientific novelty of the work lies in synthesising existing protection methods and security mechanisms into a single subsystem that allows for a comprehensive assessment and minimisation of the risks of attacks on a wireless sensor network for military purposes. The proposed approach provides adaptability and integrates into existing control systems.*

Practical significance of the article. *The study's theoretical significance lies in developing methods for mathematical modelling of threats and constructing a sustainable security management architecture for wireless sensor networks. The practical value of the research results lies in the possibility of their implementation in military and special communication systems, which provides increased security of critical information and communication systems in modern conditions.*

Conclusion and the perspectives of future research. *For military purposes, the functional model of the security subsystem of the control system of wireless sensor networks provides an integrated approach to protection at all control system levels. The basic and general level of security of the control system is formalised, which will allow further evaluation of the effectiveness of the proposed security measures Directions for further research are the development of methods and techniques for automatic detection of anomalies and intrusions using artificial intelligence technologies for adaptive security management in the face of dynamic changes in network topology and threats.*

Keywords: *wireless sensor networks, management system, security subsystem, functional management model, attack, intrusion detection, security management.*

References

1. Zhuk, O. V., Mashtalir, V. V., Hrozovskyi, R. I., Chekan, A. Y., (2024). Functional model of the control system of wireless sensor networks for military purposes. *Modern Information Technologies in the Sphere of Security and Defence.* 3(51), 146-154. DOI: https://doi.org/10.33099/2311-7249/2024-51-3-146-154. **2. Minochkin, A. I., Romaniuk, V. A.,** (2004). Mobile Radio Network Security. *Collection of Scientific Works of VITI NTUU «KPI». 5*, 116-126. **3. Artiukh, S. G., Zhuk, O. V., Cherneha, V. M.,** (2023). Classification of attacks in wireless sensor networks of troops' tactical command and control. *Modern Information Technologies in the Sphere of Security and Defence.* 3(48), 11-19. DOI: https://doi.org/10.33099/2311-7249/2023-48-3-11-19. **4. Minochkin, A. I., Romaniuk, V. A., Shatsilo, P. V.,** (2005). Detecting attacks on mobile radio networks. *Collection of Scientific Works of VITI NTUU «KPI».* 1, 102-111. **5. Gautam, A. K., Kumar, R.,** (2021). A comprehensive study on wireless sensor networks' key management, authentication and trust management techniques. *SN Applied Sciences*. 1(3). DOI: https://doi.org/10.1007/s42452-020-04089-9 [Accessed: 17 March 2025]. **6. Rehman, A., Mahmood, M., Zafar, S., Raza, M., Qaswar, F., Aljameel, S., Khan, I. and Aslam, N.,** (2022). A Survey on MAC-Based Physical Layer Security over Wireless Sensor Networks. Electronics. 11(16), 2529. DOI: 10.3390/electronics11162529. **7. Jain, U. and Hussain, M.,** (2018). Wireless Sensor Networks: Attacks and Countermeasures. *SSRN Electronic Journal*. DOI: 10.2139/ssrn.3170185. **8. Hoffman, L. J., Clements D.** (1977). Fuzzy computer security metrics: A preliminary report. Memorandum No. ERLM77/6 [online]. Electronics research laboratory. College of Engineering University of California, Berkeley. 20 . Available at: https://www2.eecs.berkeley.edu/Pubs/TechRpts/1977/ERL-m-77-6.pdf [Accessed: 17 March 2025].

Рукопис надійшов до редакції *19.03.2025*
Рукопис прийнято до друку після рецензування *25.03.2025*
Дата публікації *30.04.2025*