КОМП'ЮТЕРНІ ЗАСОБИ, МЕРЕЖІ ТА СИСТЕМИ

УДК 004.75

В.О. РОМАНОВ, І.Б. ГАЛЕЛЮКА, В.О. ОСТАПЕНКО

ВИМОГИ ДО ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ

V. Romanov, I. Galelyuka, V. Ostapenko

REQUIREMENTS TO FUNCTIONAL AND INFORMATIONAL SAFETY OF WIRELESS SENSOR NETWORKS

Basic safety applicable functional and information principles of wireless sensor network are considered in the article.
Key words: functional safety, informational safety, wireless sensor network.

Рассмотрены особенности применения базовых принципов в организации функциональной и информационной безопасности беспроводных сенсорных сетей.
Ключевые слова: функциональная безопасность, информационная безопасность, беспроводная сенсорная сеть.

Розглянуті особливості застосування базових принципів організації функціональної та інформаційної безпеки бездротових сенсорних мереж.
Ключові слова: функціональна безпека, інформаційна безпека, бездротова сенсорна мережа.

Вступ. Функціональна безпека бездротових сенсорних мереж (БСМ) є комплексом заходів, спрямованих на захист мереж від аварій з метою запобігання нанесення шкоди людям, зовнішньому середовищу та матеріальним цінностям. Високий рівень функціональної безпеки забезпечується у разі, коли функція безпеки в аварійних ситуаціях працює надійно. В автоматизованих системах управління технологічними процесами (АСУ ТП), наприклад, до характерних функцій безпеки відносяться наступні запобіжні функції: аварійна зупинка, контроль тиску котла, аварійне відкриття/закриття клапану котла, утримання від закриття шлюзних воріт і т. п. [1].

Загальна частина. Основні норми функціональної безпеки створюваних електричних, електронних та електронних програмованих пристроїв та систем наведені у стандартах МЕК 61508 та МЕК 61511. Особливістю цих стандартів є ризик-орієнтований підхід. Залежно від шкоди, яка може бути завдана техногенними об’єктами (до яких відносяться БСМ) життю або здоров’ю людини чи зовнішньому середовищу, встановлюються відповідні рівні ризику (рис. 1). Для зменшення рівня ризику передбачено комплекс заходів, які регламентовано стандартами МЕК 61508 та МЕК 61511.

Сімейство стандартів МЕК 61508 містить сім частин (рис. 2). Як випливає з рис. 2, перша частина стандартів МЕК 61508 охоплює загальні вимоги до систем, які відповідають за безпеку системи. Друга частина охоплює пов'язані з безпекою вимоги до електричних,

електронних та електронних програмованих систем. Третя частина визначає вимоги до ПЗ. Четверта частина містить основні терміни та визначення, які стосуються функціональної безпеки. П'ята частина включає приклади методів визначення рівнів повноти безпеки (safety integrity level – SIL). Шоста частина є настановою застосування методів, які викладені в другій та третій частинах. В сьомій частині наведено огляд і приклади технічних і організаційних заходів, спрямованих на забезпечення функціональної безпеки створюваного виробу (у нашому випадку БСМ).

Слід зазначити, що всі системні функції, які регламентовано цими стандартами, підтримуються БСМ.

БСМ – це багаторівневі розподілені мережі, побудовані за принципами самоорганізації, з великою кількістю сенсорів та виконавчих механізмів, які об’єднані радіоканалом (рис. 3) [2]. На основі БСМ реалізуються проекти, які виконані за технологією Інтернету речей, тобто об’єктів, які взаємодіють один з одним без участі людини. Широке впровадження технології Інтернету речей у

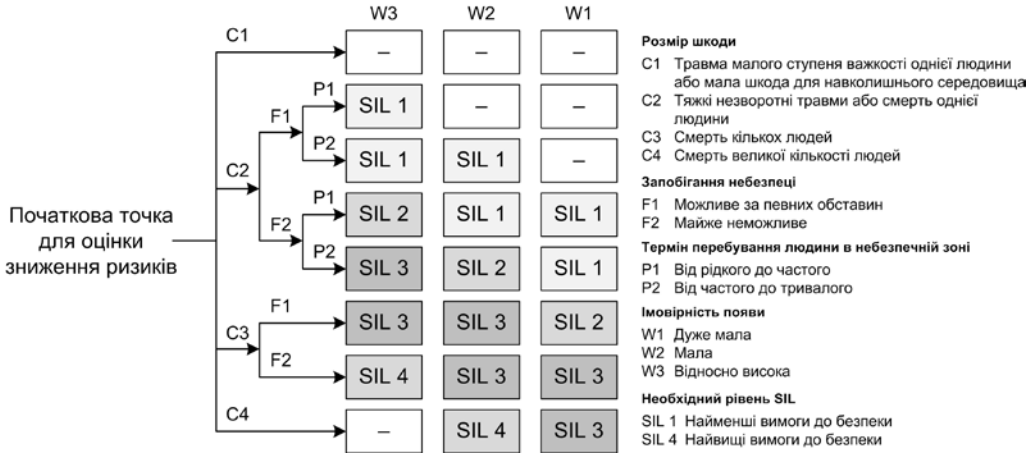

РИС. 1. Діаграма рівнів ризиків для оцінки функціональної безпеки

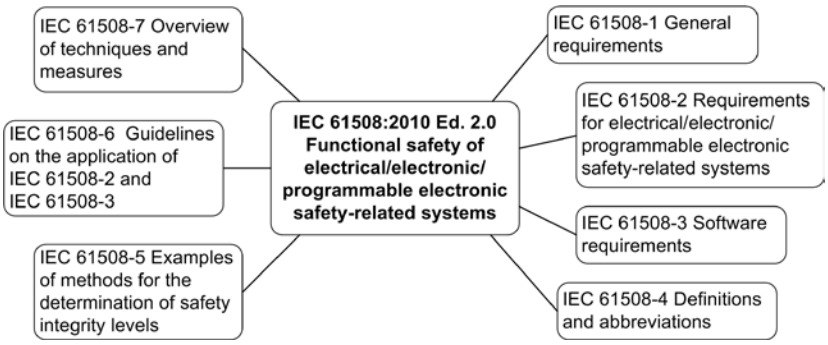

РИС. 2. Перелік міжнародних стандартів з функціональної безпеки сімейства МЕК 61508

глобальні міжнародні проекти протягом останніх трьох років [3] свідчить про появу нового класу, так званих, кібер-фізичних об'єктів. У цих об’єктах засоби забезпечення надійності, функціональної та інформаційної безпеки повинні бути об’єднані у єдину систему. Зв'язок атрибутів, що відповідають за надійність, функціональну та інформаційну безпеку, показано на діаграмі (рис. 4) [4].

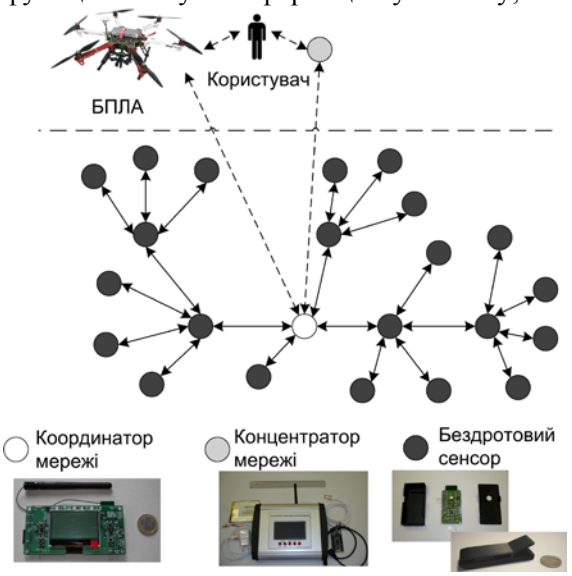

РИС. 3. Структурна організація бездротових сенсорних мереж

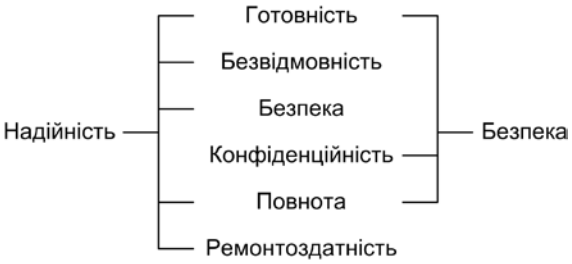

РИС. 4. Взаємозв'язок атрибутів надійності

Базовим показником функціональної безпеки є ризик. Ризики за міжнародними стандартами можна оцінювати якісно або кількісно. Методи оцінки ризиків або оцінки рівнів повноти безпеки (SIL) наведені в стандарті МЕК 61508-5. Відповідно до цього стандарту функціональна безпека є ознакою систем, для яких відмова функції безпеки може привести до суттєвих втрат для людей та/або зовнішнього середовища. Властивість системи забезпечувати функцію безпеки визначається рівнем повноти безпеки SIL. Як випливає з рис. 1, стандарт МЕК 61508 визначає чотири рівня повноти безпеки SIL – це рівні SIL 1, SIL 2, SIL 3 та SIL 4. Найвищим рівнем безпеки є рівень SIL 4, найменшим – рівень SIL 1. Для того, щоб присвоїти створюваному виробу відповідний рівень безпеки SIL, використовують методи розрахунку, наведені в стандартах МЕК 61508 та МЕК 61511. Якщо необхідний рівень безпеки SIL визначено, то здійснюють вибір засобів, які дозволяють забезпечити необхідну функцію безпеки у цілому.

Стандарт МЕК 61508 регламентує три режими роботи системи, яка підтримує функцію безпеки: з низькою частотою запитів (low demand mode), тобто частота запитів на здійснення функції безпеки у цьому режимі не перевищує одного на рік; з високою частотою запитів (high demand mode), тобто частота запитів на здійснення функції безпеки є більшою, ніж раз на рік; безперервний режим (continuous mode). Залежність рівня SIL від значення середньої імовірності небезпечної відмови у разі здійснення системою функції безпеки на запит для режиму з низькою частотою запитів (Average of the safety function – PFD_{AVG}) наведена

у табл. 1. Одиницею виміру функції безпеки системи в режимі з високою частотою запитів є значення середньої інтенсивності небезпечних відмов функції безпеки (Average frequency of dangerous failure of the safety function [h^{-1}] – PFH). Залежність рівня SIL від цього параметра наведена у табл. 1.

ТАБЛИЦЯ 1. Залежність рівня SIL від значення PFD_{AVG} і PFH

Рівень SIL	Значення PFD_{AVG}	Значення PFH[h^{-1}]
4	від 10^{-5} до 10^{-4}	від 10^{-9} до 10^{-8} (одна відмова за 11 400 років)
3	від 10^{-4} до 10^{-3}	від 10^{-8} до 10^{-7} (одна відмова за 1 140 років)
2	від 10^{-3} до 10^{-2}	від 10^{-7} до 10^{-6} (одна відмова за 114 років)
1	від 10^{-2} до 10^{-1}	від 10^{-6} до 10^{-5} (одна відмова за 11,4 років)

Звичайно, забезпечувати рівень безпеки SIL 4 для однієї конкретної БСМ немає сенсу, але враховуючи те, що в світі працюють тисячі однотипних мереж, то навіть при такій низькій частоті відмов, які відповідають рівню безпеки SIL 4, небезпечні відмови є досить імовірними подіями.

Слід зазначити, що рівень безпеки SIL є функцією всієї БСМ, тому треба враховувати середню частоту небезпечних відмов усіх елементів мережі.

Розраховувати рівень SIL функції безпеки можна за методикою, яку викладено у стандарті МЕК 61508. У цьому стандарті запропоновано такі показники, як імовірності відмов для оцінки функції безпеки. Спочатку визначають долю небезпечних відмов (Dangerous Failure Fraction – DFF), яка доповнює долю безпечних відмов до одиниці та обчислюється як відношення інтенсивності небезпечних недіагностованих відмов до сумарної інтенсивності відмов. Діагностичне покриття (Diagnostic Coverage – DC) відповідно до МЕК 61508 розраховують на основі визначення інтенсивності небезпечних відмов. Діагностичне покриття є відношенням інтенсивності небезпечних діагностованих відмов до інтенсивності небезпечних відмов. Звідси випливає, що діагностичне покриття свідчить про долю зменшення імовірності тільки небезпечних відмов за рахунок вбудованих, наприклад, у БСМ засобів діагностики.

Виходячи з розрахункового значення долі безпечних відмов (Safe Failure Fraction – SFF), визначають максимальний рівень безпеки SIL як для резервованих, так і нерезервованих конфігурацій БСМ. Приклад розрахованих таким чином рівнів SIL наведено у табл. 2.

Як випливає з табл. 2, для долі безпечних відмов 90–99 % (БСМ нерезервована, тобто HFT = 0) максимальний рівень безпеки не перевищує SIL 2. Якщо елементи БСМ дубльовані (HFT = 1), то рівень безпеки для елементів складає SIL 3. Для тройованих елементів мережі (HFT = 2) рівень безпеки елементів сягає значення SIL 4. Для розрахунку рівня безпеки усієї БСМ недостатньо враховувати PFD_{AVG} окремих компонентів. Для цього треба визначити сумарне значення PFD_{AVG}, після чого сумарне значення PFD_{AVG} треба порівняти з допустимою загальною імовірністю відмов відповідного рівня SIL. Відзначимо, що рі-

вень безпеки SIL можна підвищити за рахунок додаткового резервування надійних елементів БСМ або вбудованими засобами діагностики.

ТАБЛИЦЯ 2. Максимальний рівень SIL в залежності від значення SFF та показника апаратної відмовостійкості (Hardware Fault Tolerance – HFT)

Доля безпечних відмов на елемент БСМ, або SFF	Допустима кількість апаратних відмов БСМ або HFT		
	0	1	2
>60 %	—	SIL 1	SIL 2
від 60 % до 90 %	SIL 2	SIL 2	SIL 3
від 90 % до 99 %	SIL 2	SIL 3	SIL 4
≥99 %	SIL 3	SIL 4	SIL 4

Приклад розрахунку загального показника PFD для БСМ показано на рис. 5. Як свідчить цей приклад, для мережі, яка містить 100 сенсорів, один координатор та один концентратор, середня імовірність небезпечної відмови $PFD_{AVG} = 4.46 \cdot 10^{-1}$, що нижче рівня безпеки SIL 1. З цього випливає, що для підвищення рівня безпеки SIL БСМ необхідно, перш за все, дублювати сенсори, які вносять найбільший вклад у долю небезпечних відмов або обладнати елементи мережі вбудованими засобами діагностики.

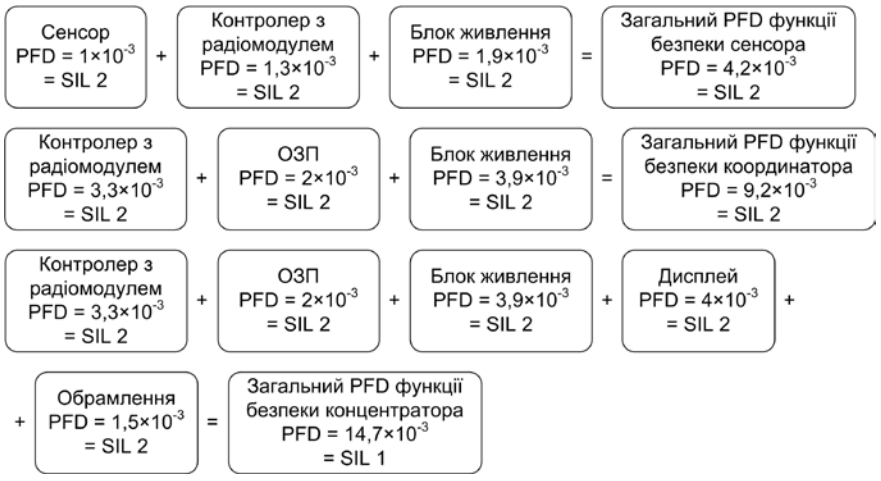

РИС. 5. Розрахунок значень функції безпеки PFD елементів БСМ у складі сенсора, координатора та концентратора

У БСМ однаково важливо застосовувати методи, спрямовані на забезпечення як функціональної безпеки, так й інформаційної безпеки. Треба відзначити, що в стандартах сімейства МЕК 61508 практично не йде мова про інформаційну безпеку, відсутні підходи до її забезпечення.

Високі вимоги як до інформаційної безпеки, так і безпеки в цілому бездротових сенсорних мереж у першу чергу зумовлені тим, що бездротові технології та бездротові сенсорні мережі все глибше та ширше проникають у виробничі процеси багатьох галузей промисловості та повсякденне життя пересічних громадян. Відповідно до [5] ризики, які супроводжують впровадження та застосування системи інформаційної безпеки телекомунікаційної системи, можна визначити як імовірність загрози безпеці та реалізація цієї загрози.

Забезпечення інформаційної безпеки бездротових мереж – досить складне завдання і на даний час не існує чітких та беззаперечних рекомендацій щодо побудови системи гарантування безпеки.

Більшість загроз інформаційній безпеці БСМ мають більш складний характер ніж подібні загрози дротовим комп'ютерним мережам, оскільки бездротові мережі набагато складніше захистити із-за загальнодоступного середовища передавання даних та широкосмугового характеру бездротових з'єднань. Забезпечення безпеки в бездротових сенсорних мережах є складною та комплексною задачею через цілий ряд причин.

1. Масштабованість БСМ, тобто мережа може складатися як з кількох вузлів, так і з кількох тисяч. Відповідно алгоритми та механізми гарантування інформаційної безпеки повинні також масштабуватися до обсягів мережі.

2. Змінна топологія бездротової мережі, що супроводжується додаванням нових вузлів або видаленням існуючих. Це вимагає використання складних алгоритмів маршрутизації та механізмів підтримання цілісності мережі.

3. Уразливість бездротових каналів, оскільки передавання даних здійснюється в загальнодоступному середовищі. Доступ до бездротового каналу можна отримати значно легше, ніж до дротових мереж передавання даних.

4. Уразливість вузлів мережі, оскільки вузли можуть переміщатися обслуговуючим персоналом або в інший спосіб, та не існує можливості завжди гарантувати фізичний захист будь-якого вузла мережі. Це робить імовірним фізичний доступ до незахищеного вузла мережі.

5. Обмежені енергетичні та обчислювальні можливості вузла, що зумовлює ситуацію, коли на рівні вузла майже неможливо реалізувати надійні механізми та алгоритми безпеки, оскільки вони є досить ресурсо- та енергозатратними.

6. Системні помилки в роботі вузла і мережі, зокрема, втрати пакетів даних при передаванні, відсутність зв'язку з центральним вузлом, вихід з ладу вузла або розрядження батареї. Оскільки такі помилки можуть виникати в мережі часто, то навмисні дії, які маскують під системні збої, досить важко виявити.

Аналізуючи вище наведене, можна зробити висновок, що заходи по забезпеченню інформаційної безпеки бездротової сенсорної мережі (рис. 6) можна розділити на основні та другорядні [6]. До основних слід віднести гарантування конфіденційності, цілісності мережі, аутентифікації та доступності даних. Другорядними є гарантування самоорганізації мережі, часової синхронізації та актуальності даних.

Конфіденційність, зазвичай, в основному і визначає рівень безпеки бездротової мережі. Мережа з високим рівнем конфіденційності захищає дані, що пе-

редаються по мережі, та закриває до них доступ для потенційних загроз. Конфіденційність досягається застосуванням механізмів контролю доступу, шифруванням тощо.

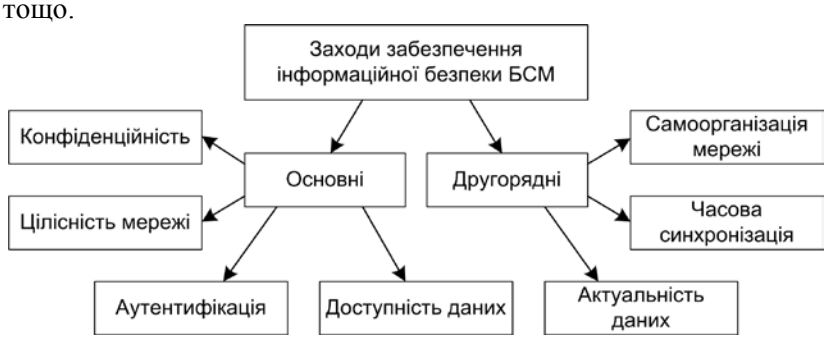

РИС. 6. Заходи по забезпеченню інформаційної безпеки БСМ

Аутентифікацію даних в бездротовій мережі реалізовують з метою підтвердження автентичності даних, що передаються, через застосування механізмів ідентифікації їх походження або, іншими словами, джерела передавання даних. Через механізм аутентифікації можна підтвердити справжність джерела та приймача даних, що реалізується, зазвичай, через обмін таємними ключами.

Механізми цілісності даних необхідні для гарантування того, що дані, які передаються через бездротовий канал, не будуть замінені чи модифіковані під час транспортування від одного вузла до іншого. Цей механізм, зазвичай, дозволяє виявити пошкоджене повідомлення або фальшиві дані, які були вбудовані в автентичне повідомлення або передані скомпрометованим вузлом.

Доступність даних передбачає, що бездротова сенсорна мережа виконує одну з основних своїх функцій, передавання даних між вузлами. Зумовити загрозу доступності даних можна виведенням з ладу центрального вузла мережі. При відсутності можливості передавати дані виникає питання в доцільності мережі.

Актуальність даних дозволяє гарантувати, що передаються дані, які є актуальними на даний момент. Це дозволяє уникнути пересилання застарілих даних або повторного пересилання даних, що може зумовити конфлікти в мережі.

Механізми самоорганізації дозволяють вузлу мережі бути функціонально гнучким та незалежним з метою самовідновлення свого місця в топології мережі при різних умовах довкілля або при виникненні різних ситуацій. Реалізувати цей механізм з дотриманням усіх вимог інформаційної безпеки досить складно.

Алгоритми часової синхронізації необхідні для встановлення загальної шкали часу для усіх вузлів мережі з метою синхронізації вбудованих механізмів.

Аналізуючи заходи забезпечення інформаційної безпеки бездротових сенсорних мереж, можна чітко розділити атаки мереж (рис. 7) на пасивні та активні.

При пасивних атаках відсутні втручання в процес маршрутизації, а виконується лише моніторинг мережі та прослуховування трафіку для отримання інформації про топологію мережі, розташування вузлів, взаємодію між вузлами тощо. Пасивний моніторинг мережі дозволяє отримати інформацію про інтенсив-

ність обміну в мережі. Якщо з певним вузлом ведеться інтенсивний обмін даними, то це може свідчити про важливість вузла, а отже він може стати ціллю атаки. Зазвичай від пасивних атак дуже важко захиститися, а виявити їх у багатьох випадках неможливо. При цьому виді атак не порушується цілісність мережі та доступність даних, зате страждає конфіденційність.

РИС. 7. Атаки проти інформаційної безпеки БСМ

Активні атаки передбачають втручання в роботу протоколів маршрутизації через зміну полів повідомлень керування, інформації про маршрутизацію або, одним з найпоширеніших способів, спричиненням відмови в обслуговуванні. Найчастіше зустрічаються активні атаки на мережевому рівні, а саме атаки маршрутизації:

1) підміна ідентифікатора, коли скомпрометований вузол може використовувати кілька псевдо ідентифікаторів та видавати себе за декілька вузлів. Такі атаки, зазвичай, використовують для порушення механізмів маршрутизації, агрегації даних, розподіленого зберігання даних тощо. Чим більш рівноправних вузлів у мережі, тим більше мережа є схильною до такого типу атаки;

2) вибіркове видалення, яке полягає у тому, що скомпрометований вузол може вибірково видаляти певні пакети. Це призводить до порушення цілісності мережі та доступності даних;

3) модифікація інформації про маршрутизацію. Найбільш схильні до такої атаки мережі з певною децентралізацією, де прості вузли можуть виконувати функції маршрутизації та, відповідно, змінювати дані маршрутизації. Як наслідок такої атаки може відбуватися збільшення часу на передавання маршруту із-за спотворених даних про маршрут, закільцювання маршруту тощо;

4) атаки типу "воронка", коли скомпрометований вузол починає концентрувати на собі весь трафік мережі. В цьому разі скомпрометований вузол слухає запити на маршрути та відповідає, що знає короткий маршрут до центрального вузла. Через деякий час такому вузлу вдається сконцентрувати на собі велику частину трафіку мережі, що дозволяє йому модифікувати пакети даних;

5) атака через переповнення, яка являє собою широкосмугову атаку та націлена на спрямування у БСМ великої кількості непотрібних повідомлень. Така атака є ресурсозатратною для атакованої мережі, що спричинює зниження пропускної здатності, зменшення енергетичних та обчислювальних ресурсів тощо;

6) атаки типу "червоточина" передбачають, що в мережі є два або більше скомпрометованих вузлів. При цьому між такими вузлами створюється маршрут для передавання перехоплених пакетів, які стають недоступними для атакованої системи [7]. Така атака впливає на мережу загалом через передавання фальшивих пакетів, які спричиняють спотворення маршрутних таблиць сусідніх вузлів.

Іншим типом активної атаки є відмова в обслуговуванні. Така атака може бути результатом ненавмисного виходу з ладу будь-якого вузла мережі або результатом навмисних дій. Атака направлена на швидку трату всіх ресурсів скомпрометованого вузла шляхом розсилання непотрібних пакетів даних. При цьому користувачі мережі не можуть у повній мірі використовувати ресурси мережі із-за значної завантаженості [8]. Атаки такого типу направлені на руйнування мережі, розірвання бездротових каналів, створення подій у мережі, які унеможливлюють виконання мережею закладених у неї функцій тощо.

До активних атак відносять захоплення вузла, що може зумовити розкриття важливої інформації, наприклад, криптографічних ключів. При успішній атаці цього типу може бути скомпрометовано цілу бездротову сенсорну мережу [9].

Активною загрозою бездротовій мережі є також несправність будь-якого вузла або вихід його з ладу. Несправний вузол може генерувати некоректні дані, що може зумовити порушення цілісності мережі. При виході з ладу вузла з функціями маршрутизації може бути порушена маршрутизація мережі.

До активних атак, крім того, слід віднести фальшування або копіювання вузла. Впровадження в мережу фальшивого вузла дозволяє такому вузлу розсилати некоректні дані, що може призвести, в певних випадках, до руйнування цілої мережі через розсилання зловмисного коду. При атаці копіюванням у мережу впроваджується завчасно підготовлений вузол, який використовує ідентифікатор існуючого в мережі вузла. Далі конфігураційні дані, які зібрані вузлом-копією, використовуються для маніпулювання сусідніми вузлами, що може призвести до захоплення керування цілим сегментом бездротової сенсорної мережі.

Для протидії атакам використовуються механізми забезпечення інформаційної безпеки. Зазвичай, такі механізми призначені для ідентифікації, попередження та відновлення БСМ після атак різного типу. В залежності від рівня використання механізми забезпечення безпеки можна розділити на механізми високого та низького рівня.

До механізмів забезпечення безпеки низького рівня можна віднести такі:

1) керування ключами та використання центрів довіри. Оскільки вузли БСМ обмежені в обчислювальних та енергетичних ресурсах, то застосування шифрування асиметричними ключами недоцільне і нераціональне у БСМ. Краще використовувати симетричне шифрування. Механізми встановлення та керування ключами мають бути придатними та масштабованими для використання в мережах, які складаються з сотень або тисяч вузлів. Деякі принципи побудови БСМ передбачають, що вузли мають встановлювати ключі з сусідніми вузлами;

2) захищена маршрутизація. Як відомо, маршрутизація є основним процесом, без якого неможлива комунікація між вузлами взагалі. Але сучасні протоколи маршрутизації при своїй, часто надмірній складності, містять багато враз-

ливостей інформаційній безпеці мережі в цілому. Найпростіші атаки передбачають включення неправдивих маршрутних даних в БСМ, що може порушити канали передавання даних як між певними вузлами, так і у межах цілої мережі. Застосування нових методів аутентифікації та захищених протоколів маршрутизації дозволить захиститися від подібних атак;

3) секретність та аутентифікація. БСМ гостро потребують захисту від прослуховування, вбудування та модифікування пакетів даних. Криптографія є стандартним механізмом захисту. Для певних типів БСМ виникають проблеми при застосуванні криптографії. Наприклад, для бездротових мереж з рівноправними вузлами криптографія дає високий рівень захисту, але потребує встановлення ключів між всіма вузлами мережі та є несумісною з широкосмуговим розсиланням повідомлень. Застосування криптографії на канальному рівні дозволяє легко встановлювати ключі та підтримує широкосмугове розсилання, але проміжні вузли зможуть перехоплювати та змінювати повідомлення;

4) захист від захоплення вузла. Така атака є досить серйозною проблемою, оскільки вузли не завжди знаходяться у недоступних для фізичного впливу місцях. З викраденого вузла можна отримати криптографічну інформацію, перепрограмувати вузол або замінити викрадений вузол фальшивим вузлом з зловмисною програмою. Найбільш простими методами захисту від подібних атак є застосування захищених від злому корпусів, удосконалених алгоритмічних рішень або техніки хешування.

5) стійкість до відмов в обслуговуванні. Причинами відмов в обслуговуванні можуть бути неполадки апаратних ресурсів, помилки прикладних програм, параметри довкілля або сукупність вказаних факторів. Причиною, наприклад, може бути потужний сигнал, яким намагалися заглушити всі комунікаційні канали та вивести БСМ з ладу. Протидією може бути використання механізму розширеного спектру, який дозволяє штучно розширити діапазон частот.

До механізмів забезпечення безпеки високого рівня можна віднести такі:

1) захищене агрегування даних. Зазвичай, дані, які збираються з вузлів, агрегуються на рівні базових станцій, які мають бути надійно захищені за допомогою захищених протоколів маршрутизації та надійних схем аутентифікації;

2) захищене керування групою. Кожний вузол має обмежені комунікаційні можливості, енергетичні та обчислювальні ресурси. Але певні функції, такі як агрегування та аналіз мережевих даних, можуть здійснюватися групою вузлів. Отже, необхідні захищені протоколи для керування групами вузлів БСМ, які виконують спільні функції. Такі протоколи повинні дозволяти приймати нові вузли у функціональні групи та підтримувати захищену комунікацію між вузлами-членами такої групи;

3) ідентифікація вторгнень. БСМ схильні до різних вторгнень. Тому необхідна наявність механізмів ідентифікації вторгнень, які б проводили моніторинг стану мережі, ідентифікували можливі спроби проникнення та повідомляли користувача про такі спроби. При захисті від таких атак корисним буде використання захищених груп вузлів.

Узагальнене представлення загроз та відповідних рішень наведено у табл. 3.

ТАБЛИЦЯ 3. Узагальнене представлення загроз і рішень

	Загроза	Вразливість	Рішення
1	Пасивний моніторинг мережі	Конфіденційність	Криптографія, шифрування
2	Прослуховування та аналіз трафіку	Конфіденційність	Криптографія, шифрування
3	Атаки маршрутизації	Цілісність мережі, маршрутизація, доступність даних	Захищена маршрутизація, аутентифікація, керування ключами, центр довіри
3.1	Підміна ідентифікатора	Механізми маршрутизації, агрегація даних	Захищена маршрутизація, захищене агрегування даних
3.2	Вибіркове видалення	Цілісність мережі, доступність даних	Захищена маршрутизація
3.3	Модифікація інформації про маршрутизацію	Таблиці маршрутизації	Захищена маршрутизація
3.4	Атаки типу "воронка"	Маршрутизація, цілісність мережі	Захищена маршрутизація
3.5	Атака через переповнення	Пропускна здатність каналів мережі, енергетичні та обчислювальні ресурси	Захищена маршрутизація
3.6	Атаки типу "червоточина"	Цілісність мережі, таблиці маршрутизації	Захищена маршрутизація
4	Відмова в обслуговуванні	Цілісність мережі, енергетичні та обчислювальні ресурси	Стійкість до відмов в обслуговуванні, зокрема механізм розширеного спектру
5	Захоплення вузла	Цілісність мережі, криптографічні ключі, конфіденційна інформація	Ідентифікація вторгнень
6	Несправність вузла або вихід його ладу	Цілісність мережі	Альтернативні маршрути, вбудована діагностика
7	Фальшування або копіювання вузла	Цілісність мережі, конфіденційна інформація	Ідентифікація вторгнень

Висновки. 1. Бездротові сенсорні мережі – основа технології Інтернету речей. Широке застосування технології Інтернету речей неможливе без забезпечення функціональної та інформаційної безпеки бездротових сенсорних мереж.

2. Основні вимоги до функціональної безпеки бездротових сенсорних мереж регламентовані сімейством міжнародних стандартів МЕК 61508 та МЕК 61511. Головна особливість цих нормативних документів – ризик-орієнтований підхід.

3. Нормативні документи, спрямовані на регламентацію вимог до інформаційної безпеки, поки що не розроблені, що стримує розвиток технології Інтернету речей та її впровадження у різні сфери людської діяльності.

4. Проаналізовані підходи до забезпечення інформаційної безпеки бездротових сенсорних мереж. Проаналізовано види атак на бездротові сенсорні мережі, наслідки дії цих атак і основані методи та засоби боротьби з загрозами та наслідками цих атак.

1. AUMA – функциональная безопасность – SIL. https:www.auma/ru/reshenija/service-conditirus functional-safety-sil/.
2. Palagin O.V., Romanov V.O., Galelyka I.B., Voronenko O.V., Brayko Yu.O., Imamutdinova R.G. Wireless sensor network for precision farming and environmental protection. *Information theories and applications.* 2017. Vol. 24, N 1. P. 19–34.
3. Функциональная безопасность часть 5 из 6. Жизненный цикл информационной и функциональной безопасности. https://habrahabr.ru/post/322428/
4. Функциональная безопасность часть 6 из 6. Оценивание показателей функциональной безопасности и надежности. https://habrahabr.ru/post/323776
5. ITU-T Recommendation E.408. Telecommunication Network Security Requirement, 2004.
6. Walters J.P., Liang Z., Shi W., Chaudhary V. Wireless Sensor Network Security: A Survey. Security in Distributed, Grid and Pervasive Computing. Yang Xiao (Eds), 2006.
7. Hu Y., Perrig C., Johnson D.B. Packet leashes: a defense against wormhole attacks in wireless networks. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies, Vol. 3. 3 April 2003. P. 1976–1986.
8. Blackert W.J., Gregg D.M., Castner A.K., Kyle E.M., Hom R.L., Jokerst R.M. Analyzing interaction between distributed denial of service attacks and mitigation technologies. Proc. DARPA Information Survivability Conference and Exposition. Vol. 1. 24 April 2003. P. 26–36.
9. Pathan A.S.K., Hyung-Woo Lee, Choong Seon Hong. Security in wireless sensor networks: issues and challenges. Advanced Communication technology (ICACT). 2006.

Одержано 20.09.2017