УДК 004.05:62-1(045) DOI: 10.31673/2786-8362.2025.011058

Іванченко Є.В., д.т.н.; **Тарасенко Я.В.,** д.т.н.;
Туровський О.Л., д.т.н.; **Кихтенко Є.М.;**
Трухан Д.В.

МЕТОДИ КІБЕРЗАХИСТУ МЕРЕЖІ ІНТЕРНЕТУ РЕЧЕЙ У СФЕРІ ПЕРЕДАЧІ ДАННИХ ЛАБОРАТОРНИХ ДОСЛІДЖЕНЬ

Ivanchenko Y.V., Tarasenko Y.V., Turovsky O.L., Kykhtenko E.M., Trukhan D.V. Cybersecurity methods for the Internet of Things network in the field of laboratory research data transmission. The paper analyzed methods of protecting sensor networks of the Internet of Things in the field of laboratory tests. The role of methods of protecting sensor networks in the context of existing threats to the sensor network was studied, taking into account different types of attacks with the probable use of different types of sensor connections and actuators. The considered network-level protection methods were grouped, which can be used to solve laboratory test tasks by using sensor networks based on IoT technology, into five categories: network segmentation, intrusion identification, secure routing, protection of actuators, protection of the MQTT protocol. A system of methods for protecting IoT networks in the field of laboratory testing has been formed, which takes into account both general methods for protecting wireless networks and a group of special methods for protecting IoT sensor networks, as well as the influence of methods for protecting the perception, support and application levels and the network level in the general security model. The interrelationships of individual methods within the framework of interaction with different groups to solve the problem of protecting wireless sensor IoT networks when used in laboratory tests have been studied. A number of advantages and disadvantages that the groups of considered methods provide for laboratory test tasks have been formed and the path for further development of these methods has been outlined in order to increase the level of efficiency and quality of laboratory tests and the accuracy of laboratory measurements. The practical significance of the work lies in the possibility of using a system of interconnected methods to achieve the maximum level of protection when using sensor networks in the laboratory for the further implementation of existing methods in real conditions and the development of new methods to increase the effectiveness of protection.

Keywords: sensor network, IoT, laboratory testing, automated laboratories, network layer security, wireless sensor networks

Іванченко Є.В., Тарасенко Я.В., Туровський О.Л., Кихтенко Є.М., Трухан Д.В. Методи кіберзахисту мережі інтернету речей у сфері передачі даних лабораторних досліджень. У роботі було проведено аналіз методів кіберзахисту сенсорних мереж Інтернету речей у сфері передачі даних лабораторних досліджень. Проведено аналіз та визначено роль методів кіберзахисту сенсорних мереж у контексті існуючих кіберзагроз з урахуванням різних типів атак при імовірному використанню різних типів з'єднань датчиків та виконавчих пристроїв. Проведено групування розглянутих методів захисту мережевого рівня, які можуть бути використані для вирішення задач передачі даних лабораторних досліджень шляхом застосування сенсорних мереж на основі IoT технології за п'ятьма категоріями: сегментація мережі, ідентифікація вторгнень, захищена маршрутизація, захист виконавчих пристроїв, захист MQTT протоколу. Сформовано систему методів кіберзахисту IoT мереж у сфері передачі даних лабораторних досліджень, яка враховує як загальні методи захисту бездротових мереж та групи спеціальних методів захисту сенсорних мереж IoT, так і вплив методів захисту рівнів сприйняття, підтримки та застосунків та мережевий рівень в загальній моделі безпеки. Досліджено взаємозв'язки окремих методів в рамках взаємодії з різними групами для вирішення задачі захисту бездротових сенсорних IoT мереж при їх використанні в лабораторних випробуваннях. Сформовано ряд переваг та недоліків, які надають групи розглянутих методів для задач передачі даних лабораторних досліджень та окреслено шлях подальшого розвитку цих методів з метою підвищення рівня ефективності та якості проведення передачі даних лабораторних досліджень та точності лабораторних вимірювань. Практичне значення роботи полягає в можливості застосування системи взаємопов'язаних методів для досягнення максимального рівня захисту при застосування сенсорних мереж в лабораторії для подальшого впровадження існуючих методів в реальних умовах і розробки нових методів з метою підвищення ефективності захисту.

Ключові слова: безпроводові сенсорні мережі, кібератака, IoT, лабораторні дослідження, кіберзахист мережевого рівня

Вступ

Технології Інтернету речей (IoT) стрімко розвиваються та залучаються до багатьох сфер повсякденного життя і професійної діяльності. У мережі IoT об'єднуються датчики та виконавчі пристрої для використання у різних професійних напрямках. Одним з таких напрямків є автоматизовані лабораторні дослідження та випробування нових методів, способі та пристроїв, створених на їх основі. У роботі [1] зазначається, що в установах НАН України вже діють програми з використання сенсорних приладів нового покоління, які надають змогу вдосконалення лабораторних баз, а в деяких випадках виступають як альтернативне рішення для передачі даних лабораторних досліджень. Такий напрямок розвитку пояснюється тим фактом, що все більшої актуальності набуває проблема контролю якості продукції вітчизняного виробництва та імпортованих товарів.

Постановка завдання. Підтвердження безпечності та надійності сенсорних мереж на основі IoT технологій важлива та актуальна задача, а застосування їх для контролю та передачі даних лабораторних досліджень може забезпечити оперативне та повне одержання найбільш точних результатів за рахунок відтворення умов максимально наближених до умов експлуатації виробу. Актуальність подібних сенсорних мереж на основі IoT технологій та ефект від їх використання в процесі передачі даних лабораторних досліджень не викликає сумнівів. Недоліком виступає проблема захисту таких мереж.

Загрози безпроводових сенсорним IoT мережам багато в чому схожі до загроз звичайних інформаційно-комунікаційних мереж з урахуванням вищої складності захисту безпроводових мереж [2] та особливостей організації і функціонування мережі в процесі передачі даних лабораторних досліджень.

За даними звіту [3] 89% організацій, які використовують IoT системи зазнали кібератак за 12 місяців на суму збитків у 250 мільйонів доларів. Більше половини організацій (56%) вважають свій захист недостатнім. Такий стан речей доводить, що безпека сенсорних мереж є ключовою умовою якості і надійності проведення передачі даних лабораторних досліджень та точності лабораторних вимірювань, а наявних методів та засобів недостатньо для повноцінного забезпечення захисту сенсорних мереж.

Аналіз останніх досліджень. На сьогоднішній день існує значна кількість методів та моделей захисту IoT систем, які спрямовані на забезпечення безпеки різних рівнів та етапів функціонування елементів системи. У роботі [4] пропонується застосування комплексного підходу до організації безпеки IoT систем від виявлення вторгнень до організації безпеки постачання компонентів системи, але не мало уваги приділяється взаємозв'язкам різних методів захисту. Робота [5] присвячена захисту від загроз, спричинених вразливостями бездротових мереж, однак захист бездротових мереж не враховує специфіку використання їх у вигляді сенсорних мереж для задач передачі даних лабораторних досліджень. Обидві роботи приділяють увагу загальним підходам захисту IoT систем та не враховують специфіку організації захисту в сенсорних мережах.

Роботи [6-7] присвячені безпосередньо методам захисту бездротових сенсорних мереж. У роботі [6] розглядає методи захисту бездротових сенсорних мереж на основі криптографічних процедур. Робота [7] присвячена розгляду ряду методів захисту сенсорних мереж: виявлення вторгнень, розподілу доступу, управління ключами. Сучасні роботи в напрямку захисту бездротових сенсорних мереж розглядають методи різного спрямування та не досліджують застосування системи методів для забезпечення захисту безпосередньо мережі. У роботах відсутні результати аналізу взаємодії методів захисту мережі та концептуального представлення взаємодії методів захисту мережі з методами захисту іншого спрямування. Варто наголосити на відсутності пропозицій по системному представленні групи методів для забезпечення захисту сенсорних мереж, які використовують технологію IoT при організації передачі даних лабораторних досліджень. Сучасні праці, що присвячені методам за засобам захисту спрямовані на вирішення задач побутових користувачів та промислових IoT мереж. Методи захисту сенсорних мереж на базі IoT технологій, які використовуються в науково-дослідних випробувальних лабораторіях потребують додаткового розгляду.

Така потреба зумовлена тим фактом, що застосування мереж IoT в специфічних сферах як лабораторні випробування вимагає особливого підходу до організації кіберзахисту з урахуванням характерних характеристик напрямку та формулювання шляхів удосконалення існуючих технологій та окремих методів для використання в сенсорних мережах при автоматизації передачі даних лабораторних досліджень.

Метою роботи є підвищення ефективності кіберзахисту мереж IoT, у сфері автоматизації передачі даних лабораторних досліджень.

Для досягнення поставленої мети в роботі необхідно вирішити наступні задачі:

1). Провести аналіз наявних методів захисту та структурування за класифікаційними ознаками для задач передачі даних лабораторних досліджень;

2). Сформувати систему методів кіберзахисту IoT мереж у сфері передачі даних лабораторних досліджень;

3). Провести дослідження взаємозв'язків представників різних груп методів кіберзахисту мереж IoT;

4). Оцінити переваг і недоліків розглянутих методів кіберзахисту мереж IoT та обґрунтування напрямків їх подальшого розвитку при вирішення завдань передачі даних лабораторних досліджень.

Виклад основного матеріалу дослідження

Дослідження методів кіберзахисту вимагає проведення аналізу вразливостей мережі IoT з метою всебічного та повноцінного врахування системи кіберзагроз та типів кібератак та ораний тип мережі передачі даних. У роботі [8] наводиться класифікація загроз безпеки в системах IoT. Згідно наведеної класифікації, загрози безпеці є однією, але не єдиною загрозою безпеки систем IoT. Окрім загроз мережевого рівня (атаки на протокол, атаки при передачі даних, атаки маршрутизації), виділяють загрози рівня сприйняття (спуфінг, глушіння сигналу чи захоплення вузла), загрози рівня підтримки (підробка даних, несанкціонований доступ) та загрози рівня застосунків (ін'єкція шкідливого коду, цілісність, перехоплення сеансу).

У роботі [2] конкретизуються загрози мережевого рівня у випадку потенційних атак на безпроводові сенсорні мережі. Такі мережі є основним об'єктом у випадку розгляду використання мереж IoT в лабораторних випробуваннях, тому вимагають особливої уваги. До загроз відносять пасивні атаки (моніторинг і прослуховування, аналіз трафіку), активні атаки (атаки маршрутизації) та фізичні атаки.

Ґрунтуючись на представлених у роботі [9] варіантах підключення мережі з використанням різних топологій, сформовано графічне представлення моделі загроз при використанні сенсорної мережі в лабораторних випробуваннях (рис. 1).

Заштрихований прямокутний елемент на рисунку позначає пристрій, прямокутний елемент без заливки – шлюз. Позначення "a" має тип з'єднання з допомогою шлюзу, "b" – тип з'єднання без посередників, "c" – з'єднання без використання мережі по типу "точка-точка".

Як видно з представленої графічної моделі, усі розглянуті в [9] варіанти топологій сенсорної мережі як шлюзове з'єднання, безшлюзове з'єднання та пряме з'єднання на основі моделі "точка-точка" є вразливими до атак мережевого рівня. При цьому варто відмітити загрози немережевого рівня, які також опосередковано впливають на процеси передачі даних в мережі. Така ситуація дає підстави вважати неможливим розгляд методів захисту мережі IoT окремо від методів захисту на рівнях сприйняття, підтримки і застосунків. Робота присвячена методам захисту мережевого рівня, однак слід враховувати, що на ефективність застосування методів захисту мережевого рівня впливає ефективність методів захисту інших рівнів. Така ситуація вимагає врахування впливу методів захисту інших рівнів при виконанні систематизації методів захисту мережі IoT.

Вищезазначена теза підтверджується аналізом представлених механізмів забезпечення безпеки в [2]. Результати аналізу доводять, що використання механізмів як низького рівня (управління ключами, аутентифікація, відмовостійкість, захист маршрутизації), так і високого рівня (захист керування групою вузлів, ідентифікація вторгнень, захищена агрегація даних)

передбачає опосередкований розгляд захисту на рівнях сприйняття, підтримки чи застосунків. Даний факт доводить не лише взаємозв'язок різних рівнів, але і виділяє мережевий рівень як такий, що об'єднує у собі всі інші рівні.

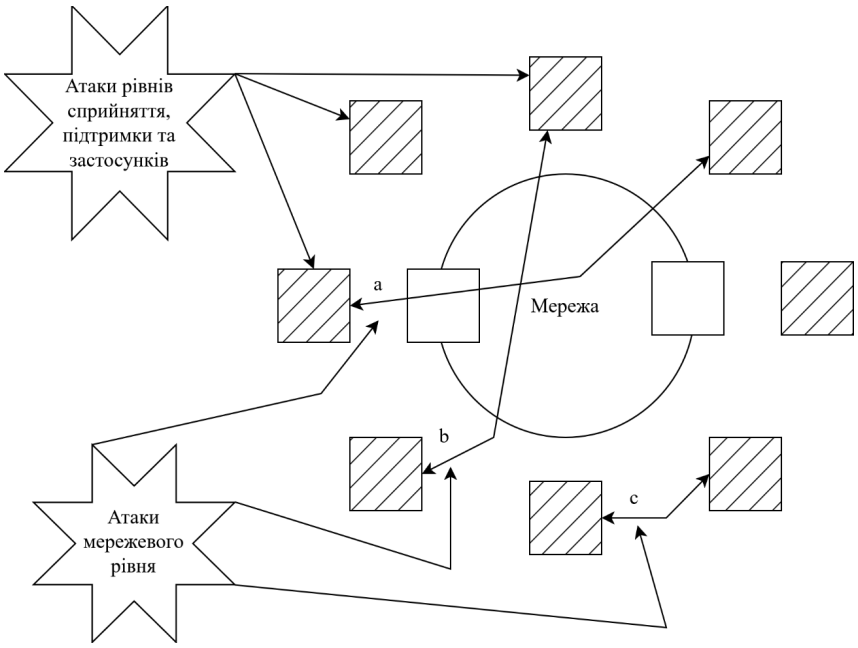

Рис. 1. Загрози сенсорній мережі

Методологічне представлення комплексного захисту системи IoT на усіх рівнях забезпечується існуючими моделями безпеки IoT.

Існує значна кількість моделей безпеки різного походження та призначення.

Модель представлена у роботі [10] пов'язана з пошуком нових наукових підходів захисту систем IoT і представляє інноваційний підхід.

Існує ряд еталонних моделей IoT, проаналізованих в роботі [8], які в своїй структурі розглядають заходи безпеки як елемент реалізації систем IoT.

Моделі безпеки мають спільні властивості їх побудови. Виділяють 2 напрямки побудови моделей:

1) формування рівня кібербезпеки в системі рівнів архітектури;

2) реалізація кіберзахисту на кожному вузлі функціонування IoT системи.

Із напрямків побудови моделей кібербезпеки можна визначити, що для кожної задачі використання IoT систем визначається власна модель безпеки.

Для задачі передачі даних лабораторних досліджень за рахунок сенсорних мереж на основі технології IoT найкраще підходить другий варіант побудови моделі безпеки. Захист бездротової сенсорної мережі повинен бути реалізований як окрема складова мережевого рівня паралельно із захистом на рівнях сприйняття, підтримки та застосунків. Модель безпеки надає можливість об'єднати різні методи захисту в єдину ефективну систему з урахуванням взаємного впливу для максимальної ефективності захисту.

Жодна модель безпеки при цьому не позбавлена недоліків. Так, в умовах розгляду моделі безпеки IoT з точки зору захисту мережевого рівня можна виділити вразливість протоколу передачі даних, що потребує використання додаткових методів захисту спеціалізованих протоколів, які використовуються в сенсорних мережах. Варто відмітити відсутність спеціалізованих моделей захисту сенсорних мереж, які можна використати для проведення передачі даних лабораторних досліджень.

Мережевий рівень кіберзахисту потребує більш детального розгляду в контексті використання системи методів організації безпеки. Важливою умовою формування системи методів захисту IoT мереж є диференціація спеціалізованих методів, призначених для кіберзахисту сенсорної мережі та загальних методів захисту бездротових мереж в контексті використання технології Інтернету речей.

Загальні методи призначені для запобігання описаних в роботі [11] вразливостей, що полягають у захисті від моніторингу трафіку, неавторизованого доступу, атаки типу “людина всередині”, DoS/DDoS атакам. Такі методи можливо використовувати при організації захисту сенсорної мережі для передачі даних лабораторних досліджень за умови адаптації механізмів їх застосування. У даному випадку мається на увазі, що рекомендації повинні включати використання методів: ідентифікації та контролю користувачів (криптографічні сертифікати), організації безпеки зв’язку (криптографічне хешування), контролю незалежних з’єднань (криптографічне шифрування).

У роботі [11] висувається пропозиція від’єднання пристроїв, які на даний момент не використовуються, але задачі застосування сенсорів та виконавчих пристроїв при лабораторних випробуваннях передбачають невизначеність стану об’єкта випробувань на різних етапах. Вимірювання стану об’єкта за допомогою різних датчиків на етапах передачі даних лабораторних досліджень може вимагати використання різних виконавчих механізмів, що зумовлює необхідність включення усіх наявних вимірювальних засобів та виконавчих механізмів впродовж усього циклу випробувань.

Використання базових методів кіберзахисту бездротових мереж недостатньо для досягнення максимальної повноти організації безпеки бездротових сенсорних мереж в ході передачі даних лабораторних досліджень. Необхідним є розгляд груп методів, які враховують специфіку застосування IoT технології в лабораторних випробуваннях. Такі методи можна назвати спеціальними.

Виходячи з вище поданих результатів аналізу пропонується спеціальні методи кіберзахисту сенсорних IoT мереж під час передачі даних лабораторних досліджень в загальній системі методів захисту розподілити на п’ять груп:

1) сегментація мережі;
2) ідентифікація вторгнень;
3) захищена маршрутизація;
4) захист виконавчих пристроїв;
5) захист MQTT протоколу.

Для кожної групи існує значна кількість методик та моделей кіберзахисту, що ґрунтуються на різних принципах та функціонують за рахунок різних підходів. Обирались лише ті методи, які найбільш повно задовольняють потреби використання сенсорних мереж у сфері передачі даних лабораторних досліджень.

Виокремлення першої групи методів, а саме сегментації мережі при вирішенні завдань передачі даних лабораторних досліджень за допомогою сенсорних мереж на основі IoT технології зумовлено важливістю підвищення безпеки та оптимізації продуктивності мережі, що описано в роботі [10]. Продуктивність важлива при проведенні випробувань різного типу зовнішніх впливів у лабораторних умовах.

Є ряд висвітлених наукових джерелах методів для сегментації сенсорних мереж. Серед цих методів для задач передачі даних лабораторних досліджень найкраще підходять методи сегментації: на основі ролей [12], на основі довіри [13] та з інтеграцією систем виявлення вторгнень [14]. Сегментація на основі ролей підвищує рівень безпеки та забезпечує різнопланові випробування, де кожен сегмент може відповідати за окрему перевірку в лабораторних умовах. Кожному вузлу мережі відводиться своя роль як групи випробувальних вимірювань, зумовлені різними зовнішніми впливами на об’єкт випробувань (кліматичні, механічні чи інші фактори), різні типи впливів виконавчих механізмів, маршрутизація тощо. Такий метод пояснює властивість емерджентності моделі безпеки, оскільки дозволяє підвищити ефективність забезпечення захисту одночасно і для інших груп методів, таких як захищена маршрутизація на основі кластерів. Сегментація на основі довіри забезпечує значну гнучкість, що є важливою умовою при лабораторних випробуваннях. Сегментація з інтеграцією систем виявлення вторгнень важлива для інтеграції з іншими групами методів, зокрема з групою ідентифікації вторгнень. Висока складність проєктування таких сегментованих мереж накладає певні обмеження на ефективність їх використання.

Пр представлення сенсорної мережі в вигляді функціональної моделі [15] можна виділити наступну групу методів кіберзахисту – ідентифікацію вторгнень як таку, що забезпечує захист системи управління бездротовими сенсорними мережами. До другої групи варто віднести методи: глибинного аналізу даних [16], глибинного навчання [17], неглибокі нейромережі [18] та аналіз великих масивів данних [19]. Лабораторні випробування передбачають опрацювання великих обсягів даних що надходять в режимі реального часу та зберігаються з попередніх випробувань. У рамках цих задач найкраще відповідають методи захисту, які ґрунтуються на засадах аналізу великих масивів даних та глибинному аналізі. Машинне навчання важливо використовувати при аналізі вторгнень, але на різних рівнях доцільно застосовувати різні методи: на рівні аналітики – глибинне навчання, на рівні – сенсорів та виконавчих пристроїв – неглибокі нейромережі. Одночасне функціонування двох типів методів машинного навчання дозволяє забезпечити різноспрямованість виявлення вторгнень. Обчислювальна потужність мікроконтролерів датчиків та виконавчих пристроїв накладає обмеження на прикладне застосування методів.

У роботі [2] наводяться механізми забезпечення безпеки бездротових сенсорних мереж, серед яких виділяється ще одна група методів – захищена маршрутизація як така, що забезпечує захист передачі даних між датчиками та виконавчими механізмами в сенсорних мережах лабораторій. До третьої групи методів варто віднести методи маршрутизації: на основі кластерів [20], з розосередженим контролем [21] та на основі довіри [21]. Маршрутизація на основі кластерів органічно поєднується із бездротовими сенсорними мережами, до яких застосована сегментація, а також надає можливість врахування різних типів випробувань. Маршрутизація з розосередженим контролем та на основі довіри підвищує гнучкість сенсорної мережі при різних умовах випробувань. Технічні параметри існуючого лабораторного обладнання не завжди можна використати для захищеної маршрутизації, що накладає відповідні обмеження.

У роботі [22] піднімається питання вразливості актуаторів у технологіях IoT, що дає підстави виокремити ще одну групу методів, які забезпечують захист виконавчих пристроїв, що використовуються в сенсорних мережах для управління процесами передачі даних лабораторних досліджень. До четвертої групи методів можна віднести методи: моніторинг поведінки виконавчих пристроїв [23] та end-to-end шифрування команд [24]. Моніторинг поведінки виконавчих пристроїв є необхідною умовою для управління процесами випробувань у лабораторії та забезпечення безпеки сенсорної мережі за рахунок зв’язку із системою виявлення вторгнень, яка реалізується другою групою методів безпеки. Шифрування дозволяє захистити дані, які передаються в сенсорній мережі до виконавчих пристроїв та обґрунтовує зв’язок з методів захисту виконавчих пристроїв з методами захисту протоколу MQTT. Шифрування даних та аналіз вторгнень зумовлює необхідність виконання додаткових дій мікропроцесорними системами контролерів та датчиків, що збільшує час виконання команд та може негативно вплинути на точність автоматизованих лабораторних вимірювань.

Головним елементом передачі даних у сенсорних мережах у роботі [25] визначають протокол, що дає підстави виокремити наступну групу методів, які забезпечують захист MQTT протоколу як такого, що є центральним елементом технології зв’язку в бездротових сенсорних мережах. До четвертої групи методів можна віднести методи: end-to-end шифрування [26] та захист брокера [27]. Шифрування є базовим способом захисту передачі інформації та пов’язане із шифруванням при маршрутизації. Брокер виступає основною складової технології передачі даних та забезпечує зв’язок з усіма пристроями мережі, що дозволяє забезпечити зв'язок методів захисту протоколу із методами сегментації. Такі процеси забезпечують можливість захищеної взаємодії вузлів при дослідженні різних етапів випробувань в лабораторних умовах. Велика кількість обчислень не дозволяє використовувати ряд лабораторного обладнання, що також накладає певні ситуативні обмеження.

На основі аналізу було сформовано систему методів захисту IoT мереж у сфері передачі даних лабораторних досліджень (рис. 2).

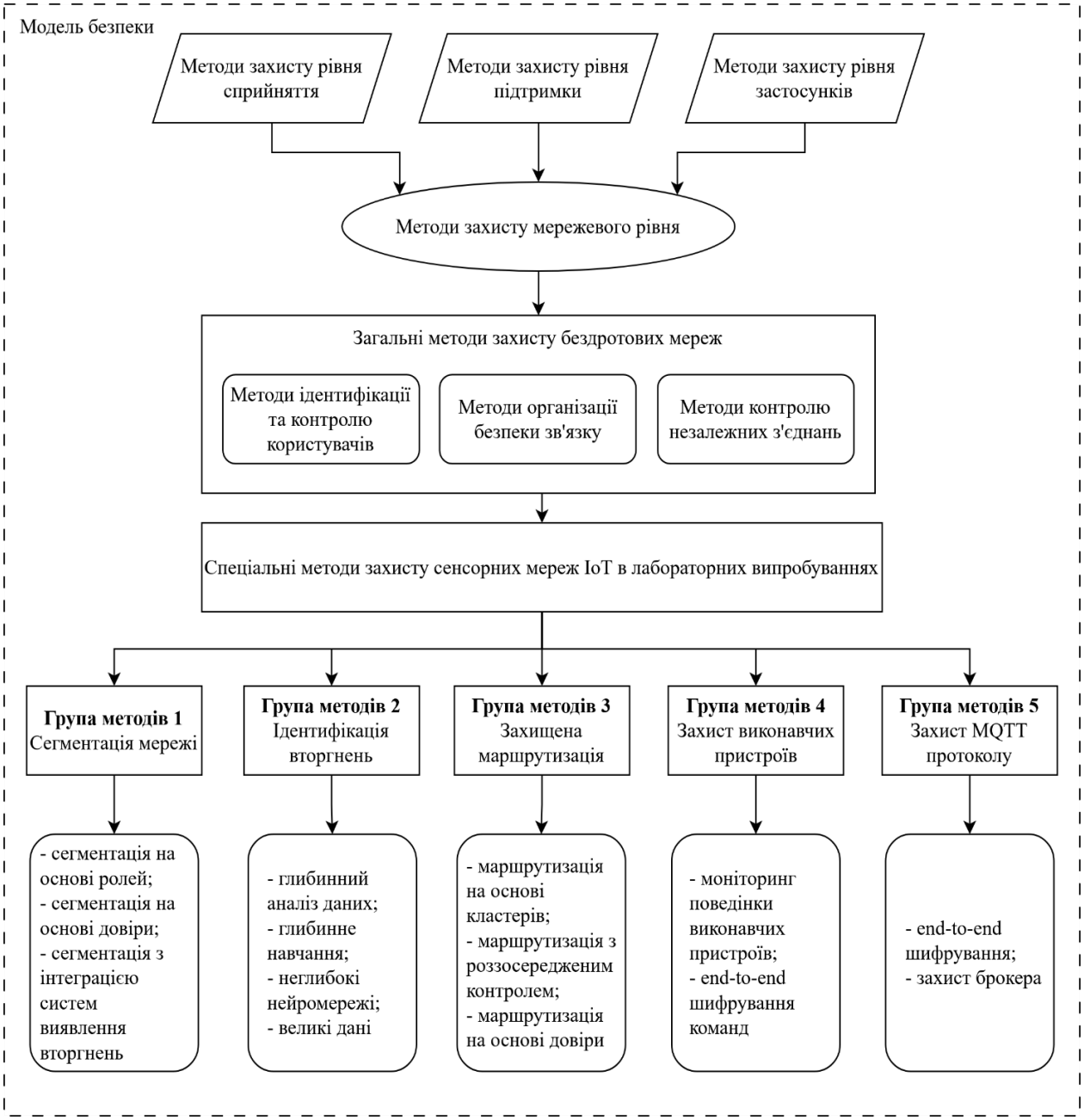

Рис. 2. Система методів захисту IoT мереж у сфері передачі даних лабораторних досліджень

Представлена система методів стосується лише мережевий рівень, але враховує вплив методів захисту рівнів сприйняття, підтримки та застосунків. Система враховує взаємозв’язок загальних методів захисту бездротових мереж із спеціальними групами методів захисту сенсорних мереж IoT в лабораторних випробуваннях в рамках загальної моделі безпеки.

Представлена система характеризується взаємозв’язком методів різних груп, що зумовлює комплексний характер її використання для одночасного охоплення різних напрямків захисту сенсорних IoT мереж для задач передачі даних лабораторних досліджень.

Взаємозв’язок методів різних груп представлено у вигляді організаційної структури спеціальних методів захисту сенсорних мереж IoT в лабораторних випробуваннях (рис. 3).

Характерною ознакою організаційної структури є повне охоплення усіх груп методів захисту при їх взаємодії для досягнення максимальної ефективності захисту сенсорних мереж лабораторій. Методи сегментації мережі та методи захисту виконавчих пристроїв залежать від методів ідентифікації вторгнень. Захищена маршрутизація та захист MQTT протоколу залежать від сегментації мережі. Методи захисту актуаторів взаємозалежні із методами захисту MQTT протоколу.

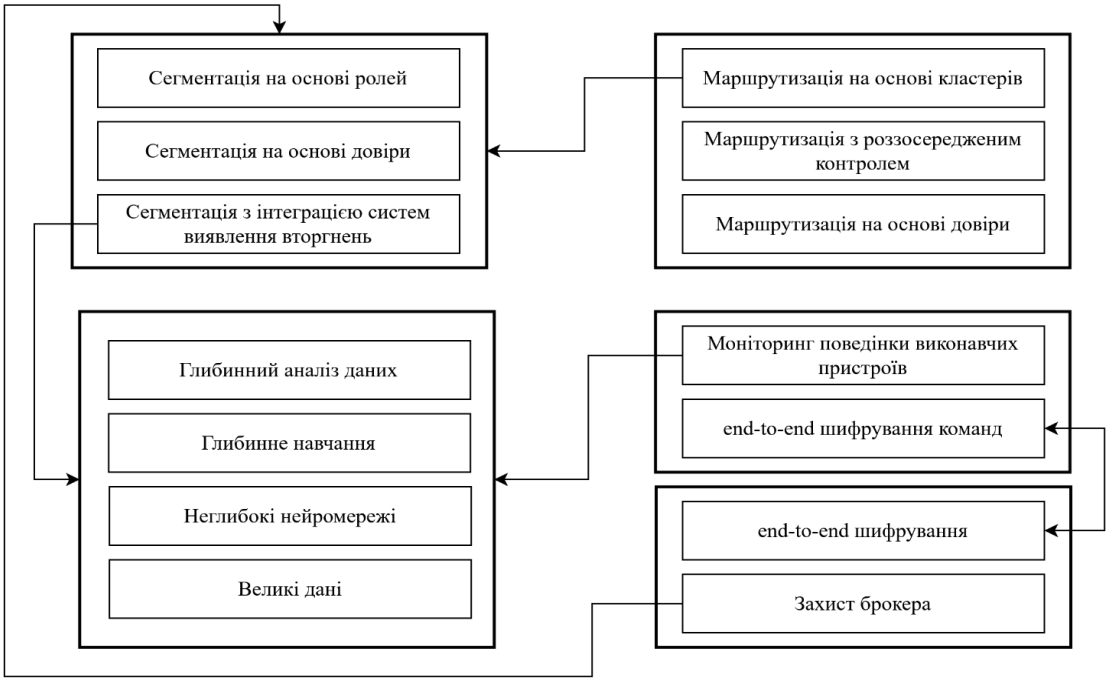

Рис. 3. Організаційна структура спеціальних методів захисту сенсорних мереж IoT в лабораторних випробуваннях

Проведений диференційований аналіз методів захисту мережевого рівня, які можуть бути використані для організації безпеки сенсорних мереж, які функціонують на основі IoT технологій для задач передачі даних лабораторних досліджень дозволив визначити групи методів для виконання цієї задачі. Кожна група методів володіє як рядом переваг, так і недоліків в контексті організації захисту сенсорних мереж у сфері передачі даних лабораторних досліджень. Усунення недоліків при збереженні переваг основна мета застосування запропонованої системи методів на практиці. Усунути виявлені недоліки можливо з урахуванням напрямків подальшого розвитку існуючих та потенціалу розробки нових методів захисту сенсорних мереж в рамках зазначених груп методів. Порівняльна таблиця характеристик груп методів захисту з урахуванням їх подальшого розвитку представлена у таблиці 1.

Таблиця 1

Порівняльна таблиця характеристик груп методів захисту для використання в сенсорних мережах лабораторій.

Група методів	**Переваги**	**Недоліки**	**Перспективи розвитку**
Група 1. Сегментація мережі	Оптимізація продуктивності, зручний розподіл сегментів по досліджуваному впливу на об’єкт випробувань	Висока імовірність помилки проєктування та налаштування, що може знизити точність результатів випробувань	Впровадження автоматизованої сегментації в реальному часі
Група 2. Ідентифікація вторгнень	Можливість аналізу великих обсягів даних для точного та різноспрямованого виявлення вторгнень в мережу	Обмеження обчислювальних можливостей обладнання, потреба введення додаткових обчислювальних вузлів, необхідність наявності великої вибірки даних	Спрощення алгоритмів машинного навчання на основі використання неглибоких нейромереж

Продовження таблиці 1

Порівняльна таблиця характеристик груп методів захисту для використання в сенсорних мережах лабораторій.

Група методів	**Переваги**	**Недоліки**	**Перспективи розвитку**
Група 3. Захищена маршрутизація	Можливість гнучко змінювати мережеву структуру для адаптації до нових умов	Складність інтеграції в існуюче лабораторне обладнання, обмеження кількості кластерів	Розробка динамічних моделей розміщення вузлів, розробка когнітивних технологій маршрутизації
Група 4. Захист виконавчих пристроїв	Можливість контролю виконавчих пристроїв, що унеможливлює ряд потенційних атак	Зростання часу виконання команд виконавчими пристроями	Впровадження адаптивних технологій контролю параметрів виконання команд
Група 5. Захист MQTT протоколу	Зручність аналізу взаємодії вузлів системи для дослідження різних типів впливів об’єкта випробувань	Мікропроцесори лабораторного обладнання мають обмеження по обчислювальним можливостям	Розробка легких криптографічних моделей шифрування

Висновки

У роботі було сформовано систему методів кіберзахисту IoT сенсорних мереж на основі моделі IoT за рахунок аналізу структурованих за класифікаційними ознаками методів кіберзахисту. Це в роботі досягнуто шляхом побудови взаємопов’язаних груп методів захисту спеціального призначення, яке, шляхом удосконалення методології розбудови системи кіберзахисту мережі IoT, надає можливість підвищити ефективність кіберзахисту сенсорної мережі на базі технології IoT, яка використовується для задач проведення передачі даних лабораторних досліджень.

Наведено організаційну структуру спеціальних методів кіберзахисту сенсорних мереж IoT в лабораторних випробуваннях.

Сформовано порівняльну таблицю характеристик груп методів захисту для використання в сенсорних мережах лабораторій та наведено шляхи подальшого розвитку існуючих та розробки нових методів захисту.

Теоретичне значення полягає у сформованому напрямку подальшого розвитку існуючих методів кіберзахисту сенсорних мереж IoT та розробки нових методів захисту.

Практичне значення отриманих у роботі результатів полягає у застосуванні описаної системи методів при організації кіберзахисту сенсорних мереж в лабораторіях.

Подальших досліджень потребує формалізація оцінювання впливу методів захисту рівнів сприйняття, підтримки та застосунків на ефективність методів захисту мережевого рівня на основі вагових коефіцієнтів.

Список використаної літератури:

1. Бездротові мережі “розумних” мультисенсорів та біосенсорних приладів для експрес-діагностики стану виноградних і плодоягідних культур та контролю якості продуктів виноробства / В.О. Романов та ін. *Кібернетика та комп’ютерні технології*. 2023. № 1. С. 58-73. URL: https://doi.org/10.34229/2707-451X.23.1.6.

2. Волошко С.В., Курца Д.О. Інформаційна безпека в безпроводових сенсорних мережах. *Новітні інформаційні системи та технології*. 2018. Вип. 9. URL: https://journals.nupp.edu.ua/mist/article/view/1039.

3. Digital trust in a connected world: navigating the state of IoT secutity. Keyfactor, VansonBourne, 2023. URL: https://www.keyfactor.com/state-of-iot-security-report-2023

4. Прокопович-Ткаченко Д.І., Звєрєв В.П., Козаченко І.М. Кіберзагрози та методи захисту фізичної інфраструктури промислового Інтернету речей (ILOT). Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки. 2025. Том 36 (75), № 1. С. 218-225. URL: https://doi.org/10.32782/2663-5941/2025.1.2/32.

5. Методи захисту інформації в технологіях IoT / Я. Олійник та ін. *Кібербезпека: освіта, наука, техніка*. 2025. Том 3, № 27. С. 100-108. URL: https://doi.org/10.28925/2663-4023.2025.27.705.

6. Kardi A., Zagrouba R. Attacks classification and security mechanisms in wireless sensor networks. *Advances in Science, Technology and Engineering Systems Journal*. 2019. Vol. 4, № 6. P. 229-243. URL: https://dx.doi.org/10.25046/aj040630.

7. Complete security framework for wireless sensor networks / Sharma K. et al. *arXiv*. 2009. URL: https://doi.org/10.48550/arXiv.0908.0122.

8. Коваленко О.Є. Моделі безпеки Інтернету речей. *Математичні машини і системи*. 2023. № 4. С. 43-50. URL: https://doi.org/10.34121/1028-9763-2023-4-43-50.

9. Стервоєдов М.Г., Терьохін В.Л. Розробка мережевої інфраструктури IoT на базі сенсорної мережі розподілених датчиків для вимірювання радіаційного забруднення з використанням багаторівневої архітектури. *Вісник Харківського національного університету імені В.Н. Каразіна серія "Математичне моделювання. Інформаційні технології. Автоматизовані системи управління"*. 2020. № 48. С. 89-97. URL: https://doi.org/10.26565/2304-6201-2020-48-09.

10. Модель забезпечення кібербезпеки Інтернету речей / Г.І. Гайдур та ін. *Телекомунікаційні та інформаційні технології*. 2024. № 2(83). С. 4-13. URL: https://doi.org/10.31673/2412-4338.2024.020515.

11. Лісовий І.В., Войтович О.П., Волинець О.Ю. Рекомендації забезпечення безпеки бездротових з'єднань Інтернету речей. Матеріали LIII науково-технічної конференції підрозділів ВНТУ Вінниця 20-22 березня 2024 р. URL: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2024/paper/view/20423.

12. Pribadi: A decentralized privacy-preserving authentication in wireless multimedia sensor networks for smart cities / R. Goyat et al. *Cluster Computing*. 2023. Vol. 26, №6. P. 4567-4583. URL: https://doi.org/10.1007/s10586-023-04211-7.

13. A secure clustering protocol with fuzzy trust evaluation and outlier detection for industrial wireless sensor networks / L. Yang et al. *arXiv*. 2022. URL: https://doi.org/10.48550/arXiv.2207.09936.

14. Clustering objectives in wireless sensor networks: A survey and research direction analysis / A. Shahraki et al. *Computer Networks*. 2020. Vol. 180. URL: https://doi.org/10.1016/j.comnet.2020.107376.

15. Артюх С.Г. Функціональна модель підсистеми безпеки системи управління безпроводовими сенсорними мережами військового призначення. *Сучасні інформаційні технології у сфері безпеки і оборони*. 2025. № 1 (52). С. 85-92. URL: https://doi.org/10.33099/2311-7249/2025-52-1-85-92.

16. Buczak A.L., Guven E. A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*. 2016. Vol. 18, № 2. P. 1153-1176. URL: https://doi.org/10.1109/COMST.2015.2494502.

17. Evolving machine intelligence toward tomorrow's intelligence network traffic control systems / G. Nikitha et al.. *International Journal of Engineering Research in Computer Science and Engineering*. 2018. Vol. 5, № 4. P. 566-569.

18. Shallow and deep networks intrusion detection system: A taxonomy and survey / E. Hodo et al. *arXiv*. 2017. URL: https://doi.org/10.48550/arXiv.1701.02145.

19. Wang L., Jones R. Big data analytics for network intrusion detection: A survey et al. *International Journal of Networks and Communications*. 2017. Vol. 7, № 1. P. 24-31. URL: https://doi.org/10.5923/j.ijnc.20170701.03.

20. A fuzzy logic and DEEC protocol-based clustering routing method for wireless sensor networks / N. Subramani et al. *AIMS Mathematics*. 2023. Vol. 8, № 4. P. 8310-8331. URL: https://doi.org/10.3934/math.2023419.

21. Trust and energy-aware routing protocol for wireless sensor networks based on secure routing / G. Muneeswari et al. *International Journal of Electrical and Computer Engineering Systems*. 2023. Vol. 14, № 9. P. 1015-1022. URL: https://doi.org/10.32985/ijeces.14.9.6.

22. Тіхонов С.В. Питання кібербезпеки в базових технологіях Інтернету речей. *Current challenges of science and education* : proceedings of XII International Scientific and Practical Conference, Berlin, Germany, 29-31 July 2024 / MDPC Publishing, Berlin : 2024. С. 165-171.

23. Prasad P.B.N., Gopalan K.D.R.S. Exploiting physical dynamics to detect actuator and sensor attacks in mobile robots. *arXiv*. 2017. URL: https://doi.org/10.48550/arXiv.1708.01834.

24. Secure and authenticated data communication in wireless sensor networks / Alfandi O. et al. *Sensors*. 2015. Vol. 15, № 8. P. 19560-19585. URL: https://doi.org/10.3390/s150819560.

25. Белей О.І., Логутова Т.Г. Безпека передачі даних для Інтернету речей. *Кібербезпека: освіта, наука, техніка*. 2019. № 2 (6). С. 6-18. URL: doi.org/10.28925/2663-4023.2019.6.618.

26. Winarno A., Sari R.F. A novel secure end-to-end IoT communication scheme using lightweight cryptography based on block cipher. *Applied Science*. 2022. Vol. 12, №17. URL: https://doi.org/10.3390/app12178817.

27. Paolo E.D., Bassetti E., Spognardi A. Security assessment of common open source MQTT brokers and clients. *arXiv*. 2023. URL: https://doi.org/10.48550/arXiv.2309.03547.

Автори статті

Іванченко Євгенія – доктор технічних наук, професор, Державний університет інформаційно-комунікаційних технологій, Київ. Україна.
ORCID: 0000-0002-6613-068X

Тарасенко Ярослав – доктор технічних наук, доцент, Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки, Черкаси, Україна.
ORCID: 0000-0002-5902-8628

Туровський Олександр – доктор технічних наук, професор, Державний університет інформаційно-комунікаційних технологій, Київ. Україна.
ORCID: 0000-0002-4961-0876

Кихтенко Євген – аспірант, Державний університет інформаційно-комунікаційних технологій, Київ. Україна.
ORCID: 0009-0008-1696-1048

Трухан Денис – аспірант, Державний університет інформаційно-комунікаційних технологій, Київ. Україна.
ORCID: 0009-0001-9321-5099

Authors of the article

Ivanchenko Yevheniya – Doctor of Sciences (technical), Professor, State University of Information and Communication Technologies, Kyiv, Ukraine.
ORCID: 0000-0002-6613-068X

Tarasenko Yaroslav – Doctor of Sciences (technical), Associate Professor, State Scientific Research Institute of Armament and Military Equipment Testing and Certification, Cherkasy, Ukraine.
ORCID: 0000-0002-5902-8628

Turovsky Oleksandr – Doctor of Sciences (technical), Professor, State University of Information and Communication Technologies, Kyiv, Ukraine.
ORCID: 0000-0002-4961-0876

Kykhtenko Yevhen – postgraduate, State University of Information and Communication Technologies, Kyiv, Ukraine.
ORCID: 0009-0008-1696-1048

Trukhan Denys – postgraduate, State University of Information and Communication Technologies, Kyiv, Ukraine.
ORCID: 0009-0001-9321-5099