Хмельницький національний університет
Факультет інформаційних технологій
Кафедра комп'ютерної інженерії та інформаційних систем

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

Галузь знань 12 – Інформаційні технології

Спеціальність 123 – Комп'ютерна інженерія

на тему «Метод забезпечення безпечного функціонування пристроїв Інтернету речей на основі алгоритму евристичного пошуку»

КвРКІП. 2301151.23.01.25 ПЗ

Виконав: студент 2 курсу, група КІ2м-23-1 Вадим ДІДУХ
Підпис Ім'я, прізвище

Керівник д-р. техн. наук, професор Сергій ЛИСЕНКО
Науковий ступінь, вчене звання Підпис Ім'я, прізвище

До **захисту** допускаю:
Зав. кафедри КІІС, доктор філософії, доцент
Ольга ПАВЛОВА
09 04 2025 р.

Хмельницький, 2025

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

Освітній рівень МАГІСТР

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 123 КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

Освітня програма ОСВІТНЬО-НАУКОВА ПРОГРАМА «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ ТА ПРОГРАМУВАННЯ»

ЗАТВЕРДЖУЮ

Зав. кафедри Ольга ПАВЛОВА

" 01 " 09 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ МАГІСТРА

ДІДУХУ Вадиму Анатолійовичу

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Метод забезпечення безпечного функціонування пристроїв Інтернету речей на основі алгоритму евристичного пошуку

Керівник проекту (роботи) Сергій ЛИСЕНКО, д.т.н., професор

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 08.01.2025 №8

2. Строк подання студентом проекту (роботи) на кафедру 01.05.2025 р.

3. Вихідні дані до проекту (роботи) Завдання на дипломне проектування

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)

Аналіз відомих методів забезпечення безпечного функціонування пристроїв інтернету речей

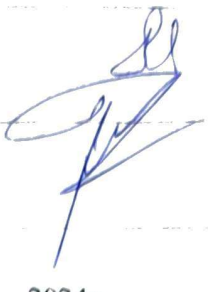
Модель процесу забезпечення безпечного функціонування пристроїв інтернету речей на основі алгоритму евристичного пошуку

Метод забезпечення безпечного функціонування пристроїв інтернету речей на основі алгоритму евристичного пошуку

Реалізація та експериментальні дослідження системи забезпечення безпечного функціонування пристроїв інтернету речей на основі алгоритму евристичного пошуку

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

6. Консультанти розділів кваліфікаційної роботи магістра

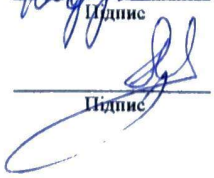
Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Сергій ЛИСЕНКО, професор кафедри КІС		
Антиплагіат	Андрій НІЧЕПОРУК, доцент кафедри КІС		

7. Дата видачі завдання «_01_»_____09_____2024р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) кваліфікаційної роботи магістра	Термін виконання етапів проекту (роботи)	Примітка
1	Вибір напряму дослідження та узгодження тематики КвРМ з керівником	01.09.2024	виконано
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	01.10.2024	виконано
3	Робота над розділом 1 – аналіз відомих моделей, методів за темою; постановка задачі	01.11.2024	виконано
4	Робота над розділом 2 – розробка моделей для вирішення поставленої задачі	01.12.2024	виконано
5	Робота над науковою статтею	01.02.2025	виконано
6	Робота над розділом 3 – розробка методів для вирішення поставленої задачі	15.02.2025	виконано
7	Робота над розділом 4 – проектування та розробка ПЗ для вирішення поставленої задачі, експериментальна частина	01.04.2025	виконано
8	Оформлення пояснювальної записки згідно вимог	18.04.2025	виконано
9	Попередній захист ДРМ	29.04.2025	виконано
10	Захист ДРМ на засіданні ЕК	До 15.05.2025	

Студент  Вадим ДІДУХ
Підпис Ім'я, прізвище

Керівник роботи  Сергій ЛИСЕНКО
Підпис Ім'я, прізвище

РЕФЕРАТ

Тема кваліфікаційної роботи магістра: Метод забезпечення безпечного функціонування пристроїв Інтернету речей на основі алгоритму евристичного пошуку.

Автор роботи: Дідух Вадим Анатолійович.

Керівник роботи: Лисенко Сергій Миколайович.

Пояснювальна записка: 72 с., 10 рис., 10 табл., 2 дод., 104 джерел.

ЕВРИСТИЧНИЙ ПОШУК, АЛГОРИТМ, ПРИСТРОЇ ІНТЕРНЕТУ РЕЧЕЙ, ГРАФИ, IoT, HARM, ЛОГІКА ПОШУКУ, БД.

Об’єктом дослідження є методи забезпечення безпечного функціонування пристроїв Інтернету речей.

Предметом дослідження є метод та система забезпечення безпечного функціонування пристроїв інтернету речей на основі алгоритму евристичного пошуку.

Метою кваліфікаційної роботи магістра є забезпечення безпечного функціонування пристроїв Інтернету речей.

Для розв’язання поставлених задач використовувалися методи забезпечення функціонування систем з IoT, методи математичного моделювання.

Наукова новизна отриманих результатів:

− набув подальшого розвитку метод забезпечення безпечного функціонування пристроїв Інтернету речей, який реалізовано на основі удосконаленого евристичного алгоритму пошуку. На відміну від відомих рішень, запропонований метод враховує принципи повного розгортання з мінімальним ризиком і максимальною корисністю без погіршення рівня безпеки, що дозволяє більш ефективно приймати рішення в умовах невизначеності та загроз;

− набула подальшого розвитку інформаційна технологія забезпечення безпечного функціонування пристроїв Інтернету речей, в якій удосконалено систему захисту шляхом застосування евристичного алгоритму пошуку.

На основі проведених досліджень було реалізовано систему забезпечення безпечного функціонування пристроїв інтернету речей на основі алгоритму евристичного пошуку.

Практична значимість отриманих результатів полягає у можливості ефективного застосування розробленої інформаційної технології для підвищення рівня безпеки пристроїв Інтернету речей у реальних умовах експлуатації. Запропонована система, що базується на удосконаленому евристичному алгоритмі пошуку, забезпечує динамічне виявлення та оцінку потенційних загроз із урахуванням критичних факторів ризику та рівня корисності реагування. Це дозволяє своєчасно приймати обґрунтовані рішення щодо захисту IoT-пристроїв без надмірного навантаження на обчислювальні ресурси. Практична реалізація системи підтвердила її здатність адаптуватися до змін у середовищі, оперативно реагувати на небезпечні події та забезпечувати стабільне функціонування пристроїв у складних умовах. Результати можуть бути впроваджені в системах розумного дому, промислового Інтернету речей, транспортній інфраструктурі та інших сферах, де важлива безперервна робота IoT-рішень з підвищеним рівнем безпеки.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

IoT - антивірусне Інтернет речей

БД - база даних

СППР – система підтримки та прийняття рішень

ОС - операційна система

ПЗ - програмне забезпечення

ЕС - експертна система

ВСТУП

Інтернет речей (IoT, Internet of Things) – це технологія, що забезпечує взаємодію фізичних пристроїв через інтернет для збору, обробки та обміну даними. За останні десятиліття ця концепція знайшла широке застосування у різних галузях: промисловості (Industrial IoT), охороні здоров'я (eHealth), транспорті (Connected Vehicles), розумних містах (Smart Cities), сільському господарстві (Smart Agriculture) тощо. Очікується, що до 2030 року кількість IoT-пристроїв перевищить 50 мільярдів, а їхня роль у критичних інфраструктурах значно зросте [1].

Пристрої, такі як Інтернет речей (IoT), займають важливе місце у нашому повсякденному житті завдяки технологічній революції, бездротовим пристроям та комунікаційним системам. IoT став невід'ємною частиною цифрової ери Індустрії 4.0. Завдяки розвитку технологій все частіше можливо перетворювати фізичні об’єкти на цифрові [1]. Мережі IoT впливають на різні сфери, зокрема, на домашній моніторинг та повсякденний моніторинг пацієнтів. IoT поєднує переваги обробки даних, аналітики та використання потужностей вебу для прийняття рішень щодо фізичних об’єктів реального світу. Це система, де розумні об’єкти з’єднані між собою і використовують Інтернет як основу для взаємодії, збору та обміну інформацією за допомогою «речей». IoT став одним із основних напрямків досліджень у світі.

Термін «Інтернет речей» (IoT) також іноді позначають як «мережу підключених пристроїв». Пристрої IoT різного розміру та функціональних можливостей -– це електричні чи електронні пристрої, здатні підключатися до Інтернету. Вони можуть використовуватися в різних середовищах: у житлових будинках, на виробництві, у сфері навколишнього середовища, охороні здоров’я, енергетиці та зв’язку.

IoT можна визначити з декількох точок зору. З погляду орієнтації на об’єкти, мета IoT полягає в тому, щоб зробити їх «розумними» за допомогою співпраці віртуальних та фізичних суб’єктів. Ці пристрої бачать, чують, мислять, обмінюються інформацією та виконують завдання, координуючи прийняття

рішень [2]. Інша концепція зосереджена на розвитку IP-мереж, щоб об’єкти могли підключатися та взаємодіяти між собою [3]. У системах IoT, де виникає потреба у високому обсязі даних від сенсорів або розумних сутностей, формується семантичний підхід [4]. Сервіс-орієнтована концепція IoT об’єднує розумні сервіси та додатки, засновані на цих підходах [5].

Пристрої IoT часто мають обмежені обчислювальні ресурси, що ускладнює впровадження традиційних механізмів захисту. Низький рівень безпеки таких пристроїв робить їх вразливими до атак різного типу.

На сьогодні існують різні підходи до забезпечення безпечного функціонування IoT-пристроїв, включаючи криптографічні алгоритми, механізми аутентифікації, сегментацію мережі та впровадження політик безпеки. Проте більшість існуючих рішень є або занадто ресурсоємними, або не враховують специфіку малопотужних пристроїв.

Таким чином, постає завдання розробки ефективних методів забезпечення безпеки IoT-мереж.

Метою даного дослідження є забезпечення безпечного функціонування пристроїв Інтернету речей.

Для досягнення цієї мети необхідно вирішити такі завдання:

- Проаналізувати сучасні загрози для забезпечення безпечного функціонування пристроїв Інтернету речей.

- Дослідити існуючі методи забезпечення безпечного функціонування пристроїв Інтернету речей.

- Розробити модель процесу забезпечення безпечного функціонування пристроїв інтернету речей на основі алгоритму евристичного пошуку.

- Розробити метод забезпечення безпечного функціонування пристроїв інтернету речей на основі алгоритму евристичного пошуку.

- Реалізувати та виконати експериментальні дослідження системи забезпечення безпечного функціонування пристроїв інтернету речей на основі алгоритму евристичного пошуку.

Об'єкт дослідження – методи забезпечення безпечного функціонування пристроїв Інтернету речей.

Предмет дослідження – метод та система забезпечення безпечного функціонування пристроїв інтернету речей на основі алгоритму евристичного пошуку.

Актуальність теми зумовлена стрімким розвитком технологій Інтернету речей (IoT) та зростанням кількості підключених пристроїв у різних сферах, оскільки з кожним підключенням зростає кількість потенційних вразливих точок. Метод, заснований на евристичних алгоритмах, може допомогти знизити ризики кібератак, зокрема, шляхом виявлення вразливостей або аномальних поведінок, що є критично важливим для безпеки IoT-систем. Актуальність цієї теми полягає також у необхідності інтеграції новітніх підходів у розробку ефективних, адаптованих до реальних умов IoT-мереж методів забезпечення безпеки.

Для розв’язання поставлених задач використовувалися методи забезпечення функціонування систем з IoT, методи математичного моделювання.

Наукова новизна дослідження полягає в:

- розробленні удосконаленого метод та система забезпечення безпечного функціонування пристроїв інтернету речей на основі алгоритму евристичного пошуку, який на відміну від відомих використовує принципи повного розгортання з мінімальним ризиком та максимальної корисності без погіршення ризику;
- удосконалено систему забезпечення безпечного функціонування пристроїв інтернету речей на основі алгоритму евристичного пошуку.

Практичне значення роботи включає: в результаті проведених досліджень було реалізовано систему забезпечення безпечного функціонування пристроїв інтернету речей на основі алгоритму евристичного пошуку.

За темою кваліфікаційної роботи опубліковано одну публікацію у фазовому виданні Computer systems and information technologies [101].

1 АНАЛІЗ ВІДОМИХ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОГО ФУНКЦІОНУВАННЯ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ

1.1 Огляд та поняття Інтернету речей

IoT має значний вплив на повсякденне життя, що стимулює активні дослідження з метою отримання користі для людини. З цієї причини було проведено численні опитування щодо екосистеми IoT та її особливостей. Деякі роботи присвячувалися огляду викликів, з якими стикається IoT, зокрема питань безпеки [11, 12], де обговорювалися різні типи атак. У [13] показано вразливості Bluetooth і можливі атаки на IoT через недоліки цього протоколу. Виклики IoT також розглядаються в [14]. У [15] подано рекомендації щодо безпеки, а вплив 5G на системи IoT було обговорено в [16]. Архітектуру IoT та її рівні аналізували в [17], а різні протоколи -– в [18]. Різноманітні застосування IoT описані, зокрема, у [19], де розглянуто вплив розумної логістики на промисловість. Оскільки IoT є пристроями з обмеженими ресурсами, необхідні ефективні та легкі операції. Для цього у роботах [20] продемонстровано, як периферійні обчислення можуть допомогти обробляти сервіси IoT, наприклад, у розумному сільському господарстві чи логістиці. Важливо також забезпечити безпечну передачу даних та захист від атак. Системи автентифікації можуть бути побудовані як централізовано, так і децентралізовано. Рішення на базі блокчейну та децентралізованих механізмів розглянуто в оглядових статтях [21]. Також було розглянуто мобільні IoT-архітектури з різноманітними механізмами безпеки, а рішення для виявлення вторгнень на основі машинного навчання -– у [22]. Проте жодне з них не розглядало таксономію атак IoT, поверхні атак, механізми безпеки та методи безпечної передачі даних, як це зроблено у даному дослідженні. Таблиця 2 підсумовує внесок різних оглядових робіт і показує, чим підхід цього дослідження відрізняється від інших.

Застосування IoT можуть використовуватися для спрощення, вдосконалення, автоматизації та контролю процесів у системах і бізнесі. IoT також може забезпечувати передачу важливих даних, контроль ефективності роботи або

моніторинг довкілля, що здійснюється безперервно та дистанційно. Таким чином, застосування IoT сприяє створенню нових систем і бізнес-стратегій, забезпечуючи компаніям доступ до даних для розробки продуктів і послуг.

Розумне місто -– це технологічно просунута агломерація, яка збирає інформацію за допомогою різноманітних електронних технологій, технологій розпізнавання голосу та сенсорів. Отримані дані використовуються для ефективного управління активами, послугами та програмами, що забезпечує безперебійне функціонування міста. Дані, зібрані від мешканців, обладнання, будівель та інших ресурсів, аналізуються для моніторингу та обслуговування транспортної інфраструктури, енергетичних установ, комунальних послуг, систем водопостачання, управління відходами, профілактики злочинності, управління даними, навчальних закладів, бібліотек, медичних установ та інших міських програм. Розумне місто -– це система, що складається з різноманітних сенсорів та пристроїв для моніторингу, звітності та обробки даних задля ефективного управління інфраструктурними ресурсами. Інформація, отримана з бездротових сенсорів, дозволяє системі навчатися і приймати рішення, що приносять користь населенню. Порівняно з нинішнім моніторингом охорони здоров’я, водопостачання та стану довкілля, розумне місто дозволить краще інтегрувати мешканців із необхідними послугами [23]. Водночас необхідно забезпечити захист як конфіденційності мешканців, так і цілісності інформаційної системи, адже зібрана сенситивна інформація вразлива до кібернетичних атак.

Інтеграція функцій охорони здоров’я в IoT-пристрої перетворює середовище на IoMT. Завдяки розвитку технологій використання IoMT-пристроїв зростає. Крім того, пандемія COVID-19 обмежила особисті зустрічі між пацієнтами та лікарями, створивши нову еру IoMT для надання медичної допомоги [24]. IoMT створює мережу людей та медичних пристроїв (бездротових та імплантованих), використовуючи технології бездротового зв’язку (Bluetooth, Wi-Fi, 3G, 4G, 5G, ZigBee тощо) для обміну медичними даними з лікарнями, експертами та іншими медичними установами [25]. Завдяки досягненням у сфері мікроелектроніки, медичні пристрої стають інтелектуальними, здатними моніторити та повідомляти

про фізичні показники, такі як артеріальний тиск, серцебиття, рівень кисню тощо. Такі пристрої можуть носитися як годинники, ремені, взуття, одяг, намиста тощо [26].

Розумна електромережа -– це енергетична система, що містить численні ефективні функції, такі як інтелектуальне вимірювання, розумні електросхеми, спеціалізоване обладнання, системи управління та альтернативні/відновлювані джерела енергії. Термін «розумна мережа» охоплює всю систему генерації та розподілу електроенергії в єдиній структурі. Це система, побудована на основі цифрових технологій, що використовує двосторонню цифрову комунікацію для постачання електроенергії споживачам, роблячи систему більш ефективною та екологічно чистою. Зростаючий попит на чисту енергію у всьому світі підкреслює актуальність впровадження розумних мереж. Перший раз термін «розумна мережа» було використано в 2003 році [27]. Технологія розумної мережі дозволяє здійснювати моніторинг, координацію та контроль електричної мережі в режимі реального часу за допомогою комунікаційних мереж між фізичними компонентами, що забезпечує ефективне та економічне управління. Широке розповсюдження Інтернет-з’єднання робить впровадження розумної мережі ще більш доцільним. Розумна мережа включає системи SCADA, системи енергетичного управління, мережеві комунікаційні системи та розподілені джерела енергії (DER). Забезпечення конфіденційності та безпеки даних користувачів у такій мережі є надзвичайно важливим, адже кібер-фізичні атаки можуть порушити фізичну безпеку системи.

1.2 Вразливості пристроїв та обмеження безпеки

Підключені пристрої зазнають різноманітних загроз, кількість яких зростає щодня. Пристрої з низьким енергоспоживанням не завжди можуть задовольнити вимоги традиційних методів безпеки. Щоб зберегти безпеку пристроїв та конфіденційність користувачів, необхідно унеможливити доступ зловмисників до

пристроїв або мережі. У цьому розділі проілюстровано можливі загрози та заходи захисту [28-32].

Застосування традиційних механізмів безпеки до мереж IoT чи окремих пристроїв є складним завданням через обмежені ресурси цих пристроїв.

Зі збільшенням кількості та різноманітності пристроїв IoT площа поверхні атаки зростає багаторазово [33-39].

До того ж, ця площа збільшується через зростання кількості пристроїв, ускладнення архітектури, гетерогенність, різноманітність, сумісність, портативність, мобільність, розташування, топологію та розподіл об'єктів (пристрої, контролери, з'єднання, користувачі та сервіси). Поверхня атаки формується завдяки елементам мережі (протоколам) та сутностям (пристроям, методам, інформації), а також визначається з'єднанням компонентів системи та політиками доступу.

IoT-пристрої утворюють численні будівельні блоки системи, тому важливо враховувати всі можливі точки атаки [40-45]. До таких точок можна віднести адміністративний інтерфейс, веб-інтерфейс пристроїв/хмарних сервісів, механізми оновлення, мобільні додатки, фізичні інтерфейси, мікропрограми та пам'ять пристроїв [41-46].

Виявлення цих точок дозволяє оцінити ризики безпеки та визначити вразливі ділянки, де потрібен поглиблений захист. Велика кількість потенційних векторів атак стимулює розробку ефективних засобів захисту, адже традиційні методи часто не підходять для ресурсозалежних IoT-пристроїв.

Прикладом є ботнет Mirai, який демонструє можливість захоплення пристроїв та проведення потужних DDoS-атак.

Пристрої IoT створюють зручний досвід для користувачів, але їх розповсюдження супроводжується зростанням загроз безпеки, оскільки зловмисникам відкривається можливість маніпулювати великими обсягами даних у взаємозв'язаному світі [47-52].

Без належних заходів безпеки IoT-пристрої стають вразливими до витоку конфіденційної інформації. Крім того, кіберзлочинність, пов'язана з IoT, може

виникнути раптово. Через низьку ціну, мінімальне енергоспоживання та обмежені обчислювальні можливості, а також через гетерогенність мережі, IoT-пристрої вразливі як з технічної точки зору, так і через дії користувачів.

1.3 Дослідження методів забезпечення безпечного функціонування пристроїв інтернету речей

Розглянемо відомі методи забезпечення безпечного функціонування пристроїв інтернету речей.

Усі задачі безпеки поділено на загрози програмного та апаратного рівнів. Атаки програмного рівня, такі як злом, витік інформації, несанкціонований доступ та інші, спрямовані на виклик збою системи та отримання конфіденційних даних (наприклад, даних кредитних карток чи паролів) [53-56]. Використання міжмережевого екрана, оновленої вірусної бази даних та сучасного програмного забезпечення може знизити ризик таких атак. Атаки апаратного рівня також становлять значну загрозу, адже для створення повністю безпечного апаратного забезпечення необхідно розробляти захищені інтегральні схеми або системи на кристалі (SoC). Це ускладнюється наномасштабним дизайном, розподілом виробництва VLSI-чіпів та використанням сторонніх ядер інтелектуальної власності. Навіть невелика шкідлива схема, вставлена під час виробництва, може призвести до компрометації системи, що залишиться непомітним для розробників [57-59].

Недоліки компонентів системи розширюють площу атаки, оскільки зловмисник може скористатися вразливостями як апаратного, так і програмного забезпечення для здійснення своїх атак. За даними одного звіту, у 50% комерційно доступних IoT-пристроїв було виявлено суттєві вразливості. Запобігання та реагування на ці вразливості є критично важливими, адже вони можуть призвести до витоку конфіденційної інформації та зловживання системою IoT. Враховуючи численні типи атак, аналіз безпеки IoT є надзвичайно складним завданням, що

вимагає впровадження комплексних захисних заходів. Проте великий обсяг даних, що генерується, стимулює підвищення загального рівня безпеки системи.

З метою захисту обладнання необхідно чітко визначити цілі безпеки. Традиційно використовують триаду CIA -– конфіденційність, цілісність і доступність. Конфіденційність встановлює критерії доступу до інформації для уповноважених осіб. Цілісність гарантує надійність послуг, забезпечуючи отримання IoT-пристроями лише легітимних команд та даних. Доступність забезпечує, щоб функції IoT були доступні уповноваженим користувачам у будь-який час та з будь-якого місця. Розширений набір цілей з інформаційної безпеки (IAS-octave) усуває недоліки триади CIA [60-63].

У статті [64] розглядається критично важливе питання споживання енергії в екосистемі Інтернету речей (IoT), що швидко розширюється. Визнаючи, що розгортання величезної кількості взаємопов'язаних пристроїв може призвести до значних потреб в електроенергії та впливу на навколишнє середовище, автори пропонують нову схему, яка надає пріоритет енергоефективності при збереженні функціональної надійності мереж IoT. Їхня робота є внеском у нову галузь «Зеленого Інтернету речей», яка наголошує на сталому та енергоефективному проектуванні систем. Автори досліджують обмеження традиційних методів розгортання IoT, особливо з точки зору використання енергії та довговічності мережі. Вони стверджують, що традиційні підходи часто ігнорують енергетичні витрати, пов'язані з надлишковими вузлами і неефективною маршрутизацією даних. Щоб вирішити ці проблеми, вони пропонують структуру розгортання, яка динамічно коригує щільність вузлів і стратегії передачі даних на основі умов навколишнього середовища і мережі в реальному часі. Ця адаптивна стратегія ґрунтується на теорії оптимізації та використовує імовірнісні моделі, щоб збалансувати якість покриття з економією енергії. Основним компонентом їхнього підходу є формулювання задачі оптимізації енергетичного покриття, яку вони вирішують за допомогою евристичного алгоритму, пристосованого для масштабованої реалізації. Автори аналізують, як їхня схема може розумно зменшити кількість активних вузлів, не жертвуючи при цьому покриттям мережі

або зв'язком. Їх модель враховує не тільки просторовий розподіл і точність зондування, а й можливості збору енергії, що робить її особливо придатною для зовнішніх або великомасштабних застосувань. Щоб підтвердити ефективність запропонованої ними схеми, автори провели серію симуляцій за різних сценаріїв розгортання. Результати демонструють значне підвищення енергоефективності та тривалості життя мережі порівняно з традиційними рівномірними або випадковими методами розгортання. Крім того, дослідження показує, що їхня схема є надійною в різних випадках використання Інтернету речей, таких як моніторинг навколишнього середовища та інтелектуальна інфраструктура, де підтримка стабільної продуктивності протягом тривалого періоду часу має вирішальне значення. Також в статті представлено перспективне рішення для розгортання енергоефективних систем Інтернету речей, що поєднує в собі теоретичну строгість з практичними міркуваннями. Зменшуючи втрати енергії та подовжуючи термін експлуатації сенсорних мереж, автори роблять значний внесок у сталий розвиток технологій IoT.

У статті [65] розглядаються нагальні проблеми безпеки та конфіденційності в Інтернеті речей (IoT), які виникають через значну гетерогенність, динамічний характер і масштаб екосистем IoT. Автори стверджують, що традиційні централізовані моделі безпеки погано підходять для середовищ Інтернету речей через їхні обмеження в масштабованості, стійкості та гнучкості. Натомість вони пропонують децентралізовану архітектуру безпеки, яка розподіляє прийняття рішень і контроль ближче до межі мережі.

Автори починають з опису вразливостей, притаманних системам Інтернету речей, наголошуючи на труднощах в управлінні ідентифікацією, аутентифікації пристроїв та забезпеченні конфіденційності і цілісності даних у високорозподілених середовищах. Ці проблеми ускладнюються тим, що багато пристроїв Інтернету речей мають обмежені ресурси, обмежену обчислювальну потужність і енергоспоживання, що робить впровадження стандартних криптографічних протоколів проблематичним.

Для вирішення цих проблем у статті представлено децентралізовану систему управління ідентифікацією та доступом, що базується на принципах розподіленої авторизації та контекстно-орієнтованої системи. Ядро запропонованого рішення використовує модель автентифікації, авторизації та обліку (AAA), але розширює її за рахунок включення політик, орієнтованих на користувача та пристрій, які застосовуються локально. Система використовує цифрові облікові дані та підтримує динамічні довірчі відносини між суб'єктами, що дозволяє більш гнучко та адаптивно забезпечувати безпеку. Ключовим нововведенням у цьому підході є делегування завдань автентифікації периферійним пристроям або локальним шлюзам, які можуть підтверджувати ідентичність і впроваджувати політики доступу, не покладаючись на центральний орган. Це не лише зменшує затримки та вузькі місця, але й покращує конфіденційність, мінімізуючи кількість конфіденційних даних, які необхідно передавати або зберігати централізовано. Запропонована архітектура також підтримує федеративні моделі ідентичності, що забезпечує безпечну взаємодію між різними адміністративними доменами. Автори підтверджують свій підхід на прикладі використання у сфері «розумного дому», демонструючи, як децентралізований контроль доступу може безпечно керувати взаємодією між пристроями, користувачами та зовнішніми сервісами. Тематичне дослідження ілюструє переваги запропонованого фреймворку з точки зору адаптивності, масштабованості та покращеного збереження конфіденційності. На завершення в статті представлено переконливе бачення децентралізованої безпеки в системах IoT. Переносячи контроль на периферію мережі і забезпечуючи локальне застосування політики, автори пропонують надійну і масштабовану альтернативу традиційним централізованим моделям. Їх робота є внеском у постійні зусилля по розробці безпечних екосистем IoT, що зберігають конфіденційність і враховують інтереси користувачів.

У статті [62] пропонується інноваційний підхід до оцінки ризиків безпеки в Інтернеті речей (IoT), натхненний біологічною імунологією. Визнаючи, що середовище Інтернету речей є дуже динамічним, гетерогенним і схильним до широкого спектру нових загроз, автори стверджують, що статичні або традиційні

моделі оцінки ризиків є недостатніми. Натомість вони виступають за динамічний та адаптивний механізм, який відображає самонавчання та захисні властивості імунної системи людини. Автори починають з аналізу обмежень існуючих моделей оцінки безпеки в контексті IoT. Вони вказують на те, що різноманітність пристроїв, різноманітність протоколів зв'язку та постійні зміни в топології мережі і станах пристроїв вимагають більш чутливої і стійкої системи оцінки. Проводячи паралелі з біологічними імунними системами - зокрема, їх здатністю виявляти, адаптуватися і реагувати на нові патогени - автори пропонують модель на основі штучної імунної системи (ШІС), пристосовану для аналізу ризиків безпеки в середовищах IoT. Їх модель включає ключові імунологічні концепції, такі як дискримінація «я/не-я», імунна пам'ять та теорія небезпеки. Запропонована система безперервно моніторить середовище Інтернету речей, виявляє аномальну або потенційно зловмисну поведінку та коригує рівні ризику в режимі реального часу. Вона оцінює ризики безпеки на основі як історичних даних, так і поточних поведінкових моделей, уможливлюючи проактивні механізми захисту, а не реактивне реагування. Фреймворк складається з декількох модулів, які імітують компоненти імунної системи: детектори, які відстежують аномалії, комірки пам'яті, що зберігають шаблони минулих загроз, та адаптивні механізми, які покращують можливості виявлення з часом. Така архітектура дозволяє системі динамічно оцінювати стан безпеки пристроїв і мереж, враховуючи контекст і часові фактори. За допомогою моделювання та аналізу автори демонструють, що модель, натхненна імунологією, може ефективно виявляти потенційні загрози та оцінювати ризики безпеки у більш гнучкий та адаптивний спосіб, ніж традиційні підходи. Вони підкреслюють здатність моделі розвиватися з часом, вчитися на нових моделях атак і реагувати на нові загрози з мінімальним втручанням людини. Таким чином, стаття представляє біологічно натхненну парадигму для динамічної оцінки ризиків безпеки в середовищах IoT. Імітуючи адаптивну і розподілену природу імунної системи, запропонована модель пропонує перспективний напрямок для підвищення стійкості та інтелектуальності систем безпеки IoT.

У статті [67] представлено формальну структуру, розроблену для проведення кількісного і модельного аналізу ризиків безпеки в системах Інтернету речей (IoT). Автори звертають увагу на гостру потребу в строгих, математично обґрунтованих інструментах для оцінки та управління ризиками безпеки в складних і динамічних середовищах IoT. На відміну від традиційних методів оцінки ризиків, які покладаються на якісні оцінки або спеціальні підходи, цей метод використовує перевірку ймовірнісних моделей, щоб забезпечити формальний і систематичний засіб оцінки ризиків. Автори підкреслюють, що системи Інтернету речей складаються з дуже взаємопов'язаних і різнорідних компонентів, що робить оцінку ризиків особливо складною через невизначеність, складність і динамічну поведінку. Система моделює ці системи за допомогою дискретно-часових марковських ланцюгів (DTMC) і застосовує імовірнісну часову логіку для вираження і перевірки властивостей безпеки. Цей підхід до моделювання враховує як імовірнісну природу виникнення загроз, так і різний вплив цих загроз на різні компоненти. Одним з ключових внесків статті є інтеграція поведінки системи, моделей загроз і параметрів ризику в єдину формальну модель. Автори визначають «ризик» не лише з точки зору ймовірності, але й з точки зору потенційних втрат, що дозволяє отримати комплексні показники оцінки. Підхід дозволяє аналітикам формулювати точні запитання (наприклад, ймовірність того, що загроза спричинить збій у роботі сервісу протягом певного часу) і обчислювати точні відповіді за допомогою інструментів перевірки моделей, таких як PRISM. Фреймворк також підтримує модульність і масштабованість, дозволяючи моделювати складні системи Інтернету речей по компонентах, а потім компонувати їх для загального аналізу. За допомогою набору експериментальних оцінок і тематичних досліджень, включаючи сценарій системи «розумного будинку», автори демонструють, як інструмент може бути використаний для оцінки конфігурацій безпеки, виявлення критичних вразливостей і порівняння стратегій пом'якшення наслідків на основі формальної кількісної оцінки ризиків. По суті, стаття пропонує формальну, відтворювану і підтримувану інструментами методологію для аналізу ризиків Інтернету речей, яка заповнює прогалину між

високорівневою оцінкою ризиків і низькорівневим моделюванням поведінки системи. Поєднуючи імовірнісні міркування, формальну верифікацію та практичні демонстрації кейсів використання, цей підхід є значним кроком до більш надійного та науково обґрунтованого управління безпекою IoT.

У статті [63] досліджується структурований і кількісний метод аналізу ризиків безпеки в корпоративних мережах за допомогою використання імовірнісних графів атак. Визнаючи складність і взаємозалежність, притаманні сучасним корпоративним системам, автори стверджують, що традиційні якісні методи оцінки ризиків є недостатніми для відображення динамічної та багатоетапної природи кіберзагроз. Натомість вони пропонують формальну модель, яка відображає можливі шляхи атак, кількісно оцінює пов'язані з ними ризики та підтримує прийняття рішень щодо захисту мережі. В основі їхнього підходу лежить граф атак - графічне представлення всіх можливих послідовностей експлойтів, які зловмисник може використовувати для компрометації мережевих активів. На відміну від базових дерев атак, граф атак враховує взаємозалежності між вразливостями та конфігураціями мережі, що дозволяє більш комплексно та реалістично моделювати багатоетапні атаки. Новизна цього звіту полягає у включенні імовірнісних міркувань в аналіз графів атак. Призначаючи ймовірності успіху окремих експлойтів (на основі історичних даних, експертних оцінок або оцінок вразливостей, таких як CVSS), модель уможливлює кількісну оцінку ризику. Це дозволяє аналітикам з безпеки розрахувати ймовірність того, що зловмисник досягне конкретних цінних цілей і виявити найбільш критичні вразливості з точки зору їхнього внеску в загальний ризик. У звіті також обговорюється, як ця імовірнісна структура підтримує аналіз «що, якщо», що дозволяє моделювати різні стратегії захисту або зміни в системі. Наприклад, аналітики можуть оцінити, як виправлення певних вразливостей, додавання сегментації мережі або розгортання систем виявлення вторгнень вплине на ймовірність успішної атаки. Це допомагає визначити пріоритети інвестицій у безпеку та ефективно розподілити ресурси. Крім того, автори наголошують на автоматизації та масштабованості, зазначаючи, що їхній метод можна інтегрувати в реальні корпоративні середовища за допомогою

інструментів, які аналізують мережеві конфігурації та автоматично генерують графіки атак. Поєднуючи дані сканування вразливостей зі структурованим моделюванням, система пропонує можливості аналізу ризиків у режимі, близькому до реального часу, що має вирішальне значення для динамічних мережевих інфраструктур, які розвиваються. У статті представлено потужну основу для аналізу ризиків безпеки на основі ймовірнісних графів атак, що пропонує баланс теоретичної строгості та практичної застосовності. Забезпечуючи кількісну оцінку мережевих ризиків на основі сценаріїв, автори надають фахівцям з безпеки практичні рекомендації щодо посилення кібербезпеки підприємств. Ця робота мала тривалий вплив на розвиток інструментів моделювання безпеки та формальної аналітики ризиків.

Графи атак були використані для оцінки ризику безпеки організаційних мереж [64]. Ці дослідження намагаються подолати різні задачі та покладаються на численні інструменти, представляючи різні моделі для аналізу ризиків, однак конкретні характеристики пристроїв IoT у цих статтях не розглядалися. У всіх цих дослідженнях аналізується структура звичайної IT-мережі з урахуванням вразливостей робочих станцій і серверів. Пристрої IoT створюють додаткові задачі для моделювання ризиків безпеки за допомогою графів атак, таких як різноманітні фізичні розташування, різноманітність протоколів зв’язку малого радіусу дії, кіберфізичні можливості пристроїв, мобільність тощо.

У цьому дослідженні ми доповнили модель графа атак організації, щоб врахувати розташування та зв’язок малого радіусу дії пристроїв IoT, і використали розширену модель графа атак для оптимізації розгортання пристроїв IoT у всій організації.

Зокрема в [65] запропонували загальну оцінку безпеки мережі шляхом комбінування вразливостей окремих осіб щодо їхніх стосунків у графах атак. В [66] визначили оцінку ризику як ймовірність атаки, яка була отримана з ймовірності окремих експлойтів.

В [67] описано чотири групи показників для вимірювання ризику безпеки в графі атак. Кожна родина була представлена одним записом у чотиривимірному

векторі. Евклідова норма цього вектора була використана як загальна оцінка ризику.

В [68] обчислено кількість найкоротших планів в графі планування, отриманому з графу атак, як спосіб вимірювання безпеки мережі.

В [69] використано три метрики оцінки ризику, метрику найкоротшого шляху, метрику кількості шляхів і середню довжину шляху та об'єднали їх, щоб визначити, яка з двох мереж є більш безпечною.

Автори стверджували, що кожна оцінка ризику сама по собі може призвести до оманливих результатів, і запропонували алгоритм комбінування використання метрик безпеки на основі графів атак. Вони використовували метрики прийняття рішень, коли дві метрики створювали конфлікти щодо того, яка мережа безпечніша. Їхній алгоритм допомагає прийняти рішення, створюючи загальний порядок пріоритетів питань щодо цих конфліктів.

Усі наведені вище показники ризику можна використовувати для оптимізації розгортання IoT після того, як визначення графа атак було доповнено для врахування специфікацій пристроїв IoT.

Ризики безпеки можна зменшити шляхом виправлення вразливостей. Однак не завжди можливо виправити всі вразливості відразу через експлуатаційні витрати (виправлення часто вимагає значного простою). Різноманітні недорогі підходи до зміцнення мережі можуть бути використані для визначення пріоритетності вразливостей (наприклад, [70]).

В [71] стверджує, що більшість із цих методів не є масштабованими. Вони запропонували евристичні алгоритми для прискорення оптимізації патча.

В [72] використано алгоритм оптимізації мурашиної колонії для виявлення мінімального критичного набору експлойтів.

В [73] досліджено ефект додавання фальшивих вразливостей у графі атак і використовували комбінаторну оптимізацію, щоб знайти оптимальне призначення цих вразливостей.

В [74] використано послідовне лінійне програмування в графах атак, щоб знайти оптимальне розміщення продуктів безпеки (наприклад, брандмауер на

основі хоста) в мережі. Автори використали імовірнісну модель, яка використовує Бернуллі, і перетворили граф атаки на систему лінійних і нелінійних рівнянь.

В [75] використовано граф атак для оптимізації розміщення датчиків системи виявлення вторгнень (IDS), щоб дозволити контролювати шкідливу активність на критичних шляхах.

В [76] зазначив, що деякі пристрої IoT використовують більше одного протоколу зв'язку. Автори стверджували, що якщо такий пристрій скомпрометовано шляхом злому одного з протоколів зв'язку, хакер може скористатися цим і використовувати інші протоколи як точки входу в мережу. У документі використовували HARM (ієрархічні моделі представлення атак), які є моделями графів атак, що використовуються, для покращення масштабованості [77]. Автори представили реальний сценарій і показали, як ним може скористатися зловмисник.

У сценарії деякі пристрої мають як протоколи зв'язку Wi-Fi, так і ZigBee. Також присутні розумні пристрої, такі як планшет і телевізор, які можна підключити до системи освітлення Philips Hue (Hue Bridge) через Wi-Fi. Ця система освітлення також має ZigBee, який дозволяє їй керувати розумними лампочками в будинку.

Використовуючи планшет, який запускає програму Hue, зловмисник може отримати контроль над системою Hue Bridge і використовувати її для керування всіма розумними світильниками. Автори відзначили, що концентратор освітлення може складатися з будь-якого іншого розумного концентратора, і сценарій також можна використовувати для злому будь-якого розумного пристрою, а не лише лампочок.

В [78] використовували графи атак для впровадження системи оцінки ризиків для промислових систем Інтернет речей (IIoT). Такі системи можна знайти в охороні здоров'я, сільському господарстві, на транспорті тощо. Автори відзначили багато вразливостей в пристроях IoT і стверджували, що це може призвести зловмисника до проникнення в систему за допомогою слабкого пристрою IoT. Їхню

структуру надихнули графи атак, що дозволило їм пропонувати стратегії зменшення ризику для зниження загального рівня загрози в мережі.

В [79] запропонували COBANOT, евристично засноване на витратах і бюджеті рішення зміцнення мережі для систем IoT, яке використовує компактні графи атак.

1.4 Постановка задачі

Таким чином, для досягнення мети дослідження необхідно вирішити такі науково-технічні завдання:

1. Розробити модель процесу забезпечення безпечного функціонування пристроїв Інтернету речей на основі алгоритму евристичного пошуку. Побудувати формалізовану модель, яка описує динаміку функціонування IoT-середовища з урахуванням можливості виникнення загроз та впровадження захисних заходів. В основі моделі має лежати використання алгоритмів евристичного пошуку для вибору оптимальних стратегій реагування на потенційні інциденти безпеки.

2. Розробити метод забезпечення безпечного функціонування пристроїв Інтернету речей на основі алгоритму евристичного пошуку. Запропонувати новий метод, який забезпечує проактивний захист пристроїв Інтернету речей за рахунок аналізу поточного стану системи та прогнозування ймовірних сценаріїв порушення безпеки. Метод повинен базуватися на евристичному підході до прийняття рішень у реальному часі щодо протидії кіберзагрозам.

3. Реалізувати та виконати експериментальні дослідження системи забезпечення безпечного функціонування пристроїв Інтернету речей на основі алгоритму евристичного пошуку. Реалізувати запропонований метод у вигляді програмного прототипу або симуляційного середовища. Провести експериментальні дослідження для оцінки ефективності запропонованого підходу з точки зору швидкості реагування, точності виявлення загроз, рівня захищеності системи та впливу на обчислювальні ресурси. Провести порівняльний аналіз з іншими існуючими методами.

1.5 Висновки до першого розділу

Проведений аналіз сучасних досліджень у сфері безпечного розгортання пристроїв Інтернету речей виявив низку обмежень та викликів, що залишаються невирішеними.

Переважна більшість робіт зосереджується або на питаннях розгортання, або на аспектах безпеки, часто розглядаючи ці проблеми ізольовано.

Навіть ті дослідження, які інтегрують концепції безпеки, здебільшого орієнтовані на аналіз окремих пристроїв чи специфічних доменів (наприклад, розумні міста, системи охорони здоров’я), не враховуючи взаємодію IoT-пристроїв із традиційними IT-компонентами (робочими станціями, серверами) в єдиній системній конфігурації.

Встановлено, що існуючі підходи до оцінки ризиків і моделювання загроз, засновані на графах атак, мають обмежену здатність враховувати специфічні характеристики IoT-середовищ: мобільність пристроїв, гетерогенність протоколів зв’язку, фізичне розташування та кіберфізичну природу пристроїв.

Попри деякі зусилля щодо адаптації графових моделей до IoT (наприклад, HARM, компактні графи атак), відсутні масштабовані, уніфіковані рішення, які б ефективно поєднували вразливості різнотипових компонентів мережі й дозволяли оптимізувати розгортання пристроїв з урахуванням безпеки.

Таким чином, сформувалася чітка потреба у розробці нових методів забезпечення безпечного функціонування пристроїв IoT.

2 МОДЕЛЬ ПРОЦЕСУ ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОГО ФУНКЦІОНУВАННЯ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ НА ОСНОВІ АЛГОРИТМУ ЕВРИСТИЧНОГО ПОШУКУ

2.1 Аспекти безпеки в Інтернеті речах

Для забезпечення безпечного функціонування пристроїв Інтернету речей, такі компоненти як брандмауери, IDS, антивіруси та програмні патчі.

Розглянемо основні причини.

Типи політик, де одна програма може використовувати кілька пристроїв IoT, спілкуючись явно (наприклад, через Wi-Fi або Bluetooth) або неявно (наприклад, лампочка IoT може ініціюється датчиком світла IoT).

Результатом є складна та динамічна мережа, яку може бути важко захистити за допомогою єдиної політики безпеки (наприклад, за допомогою брандмауерів).

Деякі методи безпеки зберігають аномалії та сигнатури на пристрої для розпізнавання та виявлення загроз.

Через різноманітність пристроїв IoT і виробників ці методи будуть неадекватними, головним чином через постійну потребу оновлювати та підтримувати пристрій для підтримки цих інструментів.

Пристрої IoT мають низьку обчислювальну здатність, низьке енергоспоживання та не працюють із повноцінними операційними системами. Для роботи більшості поширених методів безпеки потрібно все перераховане вище, тому їх неможливо застосувати на пристроях IoT.

Довговічність пристроїв IoT може призвести до розгортання пристроїв, які постачальники більше не підтримують. Таким чином уразливі пристрої (з паролями за замовчуванням або невиправленими помилками) можуть залишатися в організації.

Крім того, конкурентний ринок пристроїв Інтернет речей змушує постачальників намагатися випустити свої продукти якомога швидше, віддаючи пріоритет функціональності та взаємодії з користувачем, ігноруючи аспект безпеки.

Загалом більшість продуктів майже не борються з ризиками безпеки та конфіденційності, що робить їх найслабшою ланкою з точки зору безпеки та мішенню для зловмисників, зацікавлених у проникненні в мережі.

Таким чином, незважаючи на те, що безпека є центральною задачею ринку IoT, це все ще продовжує залишатися викликом сьогодні.

У сучасних умовах стрімкого зростання кількості пристроїв Інтернету речей (Internet of Things, IoT) в інфраструктурах критичного та бізнес-призначення зростає актуальність розроблення ефективних механізмів захисту таких пристроїв та систем.

Проблематика ускладнюється високим ступенем гетерогенності мереж, обмеженими обчислювальними ресурсами пристроїв, а також частою фізичною досяжністю вузлів для потенційного зловмисника.

Для вирішення зазначеної проблеми було запропоновано модель процесу забезпечення безпечного функціонування IoT-пристроїв, що ґрунтується на використанні механізмів евристичного пошуку.

Запропонована модель охоплює весь життєвий цикл аналізу та прийняття рішень щодо безпечного розгортання пристроїв: від аналізу поточного стану мережі до формування та вибору оптимального розгортання з урахуванням ризиків безпеки.

Модель побудована як формалізований процес, що реалізує послідовність перетворень вхідних даних (мережева топологія, набір IoT-пристроїв, обмеження на розгортання, відомості про вразливості) у вихідні дані – варіанти безпечного розміщення пристроїв з мінімальним ризиком.

2.2 Загальні положення моделі

У сучасних умовах стрімкого зростання кількості пристроїв Інтернету речей (Internet of Things, IoT) в інфраструктурах критичного та бізнес-призначення зростає актуальність розробки ефективних механізмів захисту таких цифрових пристроїв.

Вирішення задачі ускладнюється високим ступенем гетерогенності мереж, обмеженими обчислювальними ресурсами пристроїв, а також частою фізичною досяжністю вузлів для потенційного зловмисника.

Для вирішення зазначеної задачі було запропоновано модель процесу забезпечення безпечного функціонування IoT-пристроїв, що ґрунтується на використанні механізмів евристичного пошуку.

Зокрема, запропонована модель охоплює весь життєвий цикл аналізу та прийняття рішень щодо безпечного розгортання пристроїв: від аналізу поточного стану мережі до формування та вибору оптимального розгортання з урахуванням ризиків безпеки.

Модель побудована як формалізований процес, що реалізує послідовність перетворень вхідних даних (мережева топологія, набір IoT-пристроїв, обмеження на розгортання, відомості про вразливості) у вихідні дані – варіанти безпечного розміщення пристроїв з мінімальним ризиком.

2.3 Вхідні параметри

Модель процесу забезпечення безпечного функціонування пристроїв IoT реалізується як послідовність взаємопов’язаних етапів, кожен з яких виконує окрему функцію в рамках загального циклу безпеки.

Схематично модель можна представити як багатоетапну систему обробки даних, що включає ключові компоненти (таблиця 2.1).

Таблиця 2.1 – Опис компонентів багатоетапної обробки даних

№ етапу	Етап	Обробка даних	Компоненти
1	Модуль збору даних про мережу	Вхідні дані	топологія мережі, список хостів, доступних пристроїв IoT, конфігурації брандмауерів
		Засоби	сканери мережі (Nmap), вразливостей (Nessus)
		Вихідні дані	структурований опис мережі, вразливостей та підключень
2	Модуль формування графа атак	Вхідні дані	результати сканування
		Засоби	система моделювання MulVAL, PDDL-представлення
		Вихідні дані	логічний граф атак, що відображає можливі шляхи досягнення цілей зловмисника
3	Модуль моделювання розгортань IoT-пристроїв	Вхідні дані	список IoT-пристроїв, можливі місця розміщення, функціональні обмеження
		Функція	створення множини допустимих розгортань, з урахуванням фізичних і логічних обмежень
4	Модуль оцінки ризику	Вхідні дані	граф атак, розгортання пристроїв
		Вихідні дані	числовий показник ризику, що враховує кількість планів атак, довжину шляху, експлойти і привілеї

Продовження таблиці 2.1.

№ етапу	Етап	Обробка даних	Компоненти
5	Модуль оптимізації розгортання	Мета	знаходження оптимального розгортання згідно з обраною цільовою функцією: FDMR (повне розгортання з мінімальним ризиком); MURD (максимізація кількості пристроїв без збільшення ризику).
		Засіб	евристичний пошук DFBnB з обрізанням та допустимою евристичною функцією
6	Модуль формування рішення	Вихідні дані	остаточне рекомендоване розгортання пристроїв IoT, що забезпечує заданий рівень безпеки

2.4 Формалізація моделі

Для побудови формалізованої моделі процесу забезпечення безпечного функціонування пристроїв IoT введемо наступні позначення:

$H = \{h_1, h_2, \ldots, h_n\}$ -– множина хостів організації.

$D = \{d_1, d_2, \ldots, d_m\}$ -– множина доступних пристроїв IoT.

$T = \{t_1, t_2, \ldots, t_k\}$ -– множина типів IoT-пристроїв.

$L = \{l_1, l_2, \ldots, l_q\}$ -– множина можливих точок розгортання пристроїв.

$C = \{c_1, c_2, \ldots, c_r\}$ -– множина обмежень на розгортання пристроїв.

Функцію розгортання пристроїв визначимо як відображення:

$$\delta : D \to L \cup \{\emptyset\}, \tag{2.1}$$

де $\delta(d_i) = l_j$ означає, що пристрій d_i розгорнуто у місці l_j, а $\delta(d_i) = \emptyset$ означає, що пристрій не розгорнуто.

Кожне обмеження $c \in C$ визначається кортежем:

$$c = \langle T(d), P_d, D_t \rangle, \tag{2.2}$$

де:

$T(d) \subseteq L$ – множина допустимих місць для розгортання наявних в мережі пристроїв типу t;

$P_d \leq |T(d)|$ – кількість місць, у яких необхідно розгорнути наявні в мережі пристрої типу t;

$D_t \subseteq D$ – множина пристроїв типу t.

Оцінку ризику для кожного варіанту розгортання δ задаємо як функцію:

$$R(\delta) = \frac{1}{4}\left(\frac{OptLen(\delta)}{OptLen(\emptyset)} + \frac{OptCnt(\delta)}{OptCnt(\emptyset)} + \frac{OptExp(\delta)}{OptExp(\emptyset)} + \frac{OptPrv(\delta)}{OptPrv(\emptyset)}\right), \tag{2.3}$$

де:

$OptLen(\delta)$ – довжина найкоротшого плану атаки;

$OptCnt(\delta)$ – кількість найкоротших планів атаки;

$OptExp(\delta)$ – середня кількість експлойтів;

$OptPrv(\delta)$ – середня кількість привілеїв;

$\emptyset$ -– порожнє розгортання (еталон базового рівня безпеки).

Задамо цільову функцію для вирішення задачі повного розгортання з мінімальним ризиком:

$$\min_{\delta \in \Delta_C} R(\delta), \tag{2.4}$$

де Δ_C -– множина допустимих повних розгортань, що задовольняють усім обмеженням C.

Для вирішення задачі визначення максимальної корисність без погіршення ризику:

$$\max_{\delta \in \Delta_C, R(\delta) \leq R(\emptyset)} |\{d \in D | \delta(d) \neq \emptyset\}|. \quad (2.5)$$

2.5 Побудова простору рішень та логіка пошуку

Оптимізація розгортання IoT-пристроїв із урахуванням безпеки вимагає розгляду великої кількості комбінацій, обмежених технічними, фізичними та логічними умовами.

З метою ефективного перебору можливих рішень модель формує двоїсте дерево пошуку, в якому:

- кожна вершина представляє часткове розгортання пристроїв,
- кожне ребро – бінарне рішення щодо включення або виключення конкретного пристрою у певне місце.

Розглянемо структуру простору пошуку, де кореневий вузол – це порожнє розгортання δ_0, де всі пристрої нерозгорнуті; кожен внутрішній вузол – це часткове рішення, яке включає деякі пристрої; кожен перехід між вузлами – це бінарне рішення (ліва гілка – пристрій розгорнуто в певному місці, права гілка – пристрій не розгортається в цьому місці).

Таким чином, кожен шлях від кореня до листа дерева відображає повне розгортання $\delta \epsilon \Delta_C$, яке або задовольняє обмеження, або відкидається в процесі пошуку.

Розглянемо властивості дерева пошуку.

Коефіцієнт розгалуження складає 2 для кожного пристрою в певному місці мережі.

Максимальна глибина дерева дорівнює загальній кількості можливих рішень ($|D| \cdot |L|$).

Кількість листів: експоненційно залежить від кількості наявних пристроїв та місць.

У моделі було використано евристичний алгоритм DFBnB (Depth-First Branch and Bound), який забезпечує пошук з обрізанням гілок, що не мають потенціалу до кращого рішення.

Розглянемо основні кроки алгоритму.

Алгоритм 2.1

Ініціалізація: стек із кореневим вузлом.

Ітерація:

Витягується вузол зі стеку.

Генеруються два нащадки (розгортання / нерозгортання).

Для кожного розгортання формується відповідний граф атак G^{δ}.

Обчислюється оцінка ризику $R(\delta)$ та евристична функція $h(\delta)$.

Обрізання гілок:

Якщо $f(\delta) = g(\delta) + h(\delta)$ перевищує поточне найкраще знайдене рішення, гілка відкидається.

Зберігається найкраще допустиме розгортання з мінімальним ризиком або максимальною кількістю пристроїв.

Особливості алгоритму подано в таблиці 2.2.

Розглянемо використані евристичні функції.

Для вирішення задачі повного розгортання з мінімальним ризиком $h_{FDMR}(\delta) = \min$ (оцінка приросту ризику від решти потенційних пристроїв)

Для Визначення максимальної корисність без погіршення ризику $h_{MURD}(\delta) = \max$ (кількість пристроїв, які можна ще безпечно розгорнути)

Таблиця 2.2 - Особливості алгоритму

№	Задача	Особливість
1	Повного розгортання з мінімальним ризиком	обрізання базується на заниженій оцінці ризику в піддереві
2	Визначення максимальної корисність без погіршення ризику	обрізання базується на переоцінці кількості пристроїв, які ще можна розгорнути без підвищення ризику

2.6 Інтеграція з графами атак і підсистемами моделі

В основі моделі процесу забезпечення безпечного функціонування IoT-пристроїв лежить динамічна взаємодія між обраним варіантом розгортання пристроїв та графом атак, який відображає змінений стан загроз у комп'ютерній мережі організації.

Після кожного розгортання δ, яке включає хоча б один IoT-пристрій, виконується оновлення базового графа атак G_0 шляхом:

Процес додавання нових вузлів включає компоненти:

1. Фактичні вузли (facts), які є станом пристрою в певному місці та його можливості підключення.
2. Вузли експлойтів (exploits), які є потенційними вразливостями, характерними для конкретного пристрою та протоколу.
3. Вузли привілеїв (privileges), які є правами доступу, які може отримати зловмисник.

Процес створення нових ребер між доданими вузлами та існуючими компонентами графа здійснюється на основі топології мережі, специфікацій протоколів (наприклад, ZigBee, BLE, ad-hoc Wi-Fi) та досяжності в межах радіуса зв'язку.

Це дає змогу формувати новий граф атак G^{δ}, що відображає зміни у загрозах через інтеграцію нових пристроїв.

Кожен варіант розгортання δ породжує окремий екземпляр графа G^{δ}.

Далі цей граф використовується для :

- виявлення планів атак (attack paths), що стали можливими після розгортання;
- обчислення показників ризику: довжини атак, кількості привілеїв, кількості експлойтів, тощо;
- евристичної оцінки потенційного впливу подальших розгортань.

Модель підтримує модульну реалізацію, де кожен компонент (збір даних, побудова графа, оцінка, пошук) функціонує автономно, але узгоджено в межах загального процесу.

Дані від Nessus/Nmap надходять до модуля графа атак. PDDL-граф формується у MulVAL та передається до модуля ризику.

Значення ризику надсилається до модуля оптимізації.

Модуль пошуку формує нові δ, які повертаються у зворотний цикл.

2.7 Візуальна інтерпретація моделі

Для полегшення розуміння запропонованої моделі процесу доцільно представити її у вигляді структурної блок-схеми, що відображає послідовність дій та взаємозв’язки між компонентами.

Така схема дозволяє чітко ідентифікувати основні модулі, потоки даних, точки прийняття рішень та місця використання евристичних методів.

Блок-схема моделі подано на рисунку 2.1.

2.8 Мета експерименту та сценарії розгортання

Метою експериментальної перевірки є демонстрація практичної застосовності запропонованої моделі процесу забезпечення безпечного функціонування IoT-пристроїв у реальних або змодельованих умовах. Основний акцент зроблено на:

– аналізі змін у графах атак унаслідок різних сценаріїв розгортання;

- обчисленні показників ризику для кожного з варіантів;
- оцінці ефективності алгоритму DFBnB у задачах повного розгортання з мінімальним ризиком та визначення максимальної корисність без погіршення ризикута MURD.

Рисунок 2.1 – Блок-схема моделі

Для моделювання була сформована умовна мережева топологія організації з такими характеристиками:

$|H|$ =10 хостів (робочі станції, сервери, гостьові пристрої);

$|D|$ =8 IoT-пристроїв: IP-камери, детектори диму, смарт-ТВ, холодильники;

$|L|$ =7 можливих точок розміщення в приміщеннях;

Підтримувані протоколи зв’язку: ZigBee, BLE, Wi-Fi (ad hoc);

Глибина охоплення протоколів: ShortRange, MediumRange;

Використано Nmap та Nessus для отримання симульованих даних про підключення і вразливості.

Було реалізовано та протестовано три основні сценарії:

− Порожнє розгортання, у якому жодного IoT-пристрою не розгорнуто (еталон).

− Випадкове розгортання, у якому пристрої розміщуються без врахування ризику.

− Оптимізоване розгортання, у якому використано алгоритм DFBnB (коли усі пристрої розгорнуто з мінімальним ризиком; а також розгорнуто найбільшу кількість пристроїв без погіршення ризику).

2.9 Технічна реалізація та результати

Реалізація графа атак: MulVAL + PDDL, автоматизовано генерацію графів із вхідних сканів.

Платформа: Python 3.11, бібліотеки -– networkx, scikit-learn (для аналізу структур графів).

Евристика зберігалась у вигляді таблиць $H_{risk}[d][l]$, які оновлювались у реальному часі під час пошуку.

Модель дозволила ефективно відкинути небезпечні варіанти розгортання ще на ранніх етапах пошуку.

Повне розгортання з мінімальним ризиком показало незначне зростання ризику, при цьому забезпечивши повне розгортання.

Найбільша кількість пристроїв без погіршення ризику зберегла рівень безпеки базової мережі, розгорнувши 5 із 8 пристроїв.

Витрати часу на DFBnB – у середньому в 3 рази менші за повний перебір.

Оцінка ризиків подано в порівняльній таблиці 2.3.

Таблиця 2.3 – Порівняльна таблиця оцінки ризиків

Сценарій	OptLen	OptCnt	OptExp	OptPrv	$R(\delta)$
Порожнє розгортання	4	6	3.2	2.5	1.000
Випадкове розгортання	3	10	4.5	4.1	1.478
Повне розгортання з мінімальним ризиком	4	7	3.4	2.8	1.078
Максимальна корисність без погіршення ризику	4	6	3.2	2.5	1.000

2.10 Висновки до другого розділу

У другому розділі було здійснено комплексне дослідження проблем забезпечення безпечного функціонування пристроїв Інтернету речей (IoT) у сучасних інформаційних інфраструктурах.

Показано, що традиційні підходи до кіберзахисту, орієнтовані на використання брандмауерів, антивірусів, IDS/IPS та механізмів оновлення, виявляються малоефективними або непридатними у випадку IoT-середовищ. Це зумовлено низькою обчислювальною потужністю пристроїв, обмеженим енергоспоживанням, гетерогенністю архітектур і відсутністю централізованого адміністрування.

З метою подолання зазначених викликів у роботі було запропоновано нову модель процесу забезпечення безпечного функціонування пристроїв IoT на основі алгоритму евристичного пошуку. Вона охоплює повний цикл прийняття рішень – від збору вхідних даних про мережу до формування оптимального варіанту розгортання пристроїв із мінімальним ризиком. У моделі було формалізовано структуру вхідних параметрів, описано обмеження та введено математичне

представлення функцій ризику, що враховують кількість, довжину та складність потенційних планів атак, а також рівень привілеїв і наявність експлойтів.

Особливу увагу приділено побудові простору рішень, який моделюється у вигляді дерева перебору з бінарними рішеннями для кожного пристрою. У якості оптимізаційного механізму застосовано алгоритм евристичного пошуку з обмеженням гілок DFBnB, що дозволяє ефективно здійснювати пошук навіть у великих просторах рішень.

Інтеграція моделі з динамічними графами атак дозволяє відобразити зміну стану мережевої безпеки при кожному новому варіанті розгортання, забезпечуючи адаптивність та актуальність оцінки ризику.

Було запропоновано два сценарії використання моделі: повне розгортання з мінімальним ризиком (FDMR) та максимізація кількості розгорнутих пристроїв без погіршення показників ризику (MURD).

Для кожного з цих сценаріїв розроблено відповідні евристичні функції, що враховують особливості оптимізаційних цілей.

Таким чином, запропонована модель не лише вирішує актуальну проблему безпечного розгортання пристроїв IoT, а й формує основу для побудови адаптивних систем керування безпекою в умовах високої динамічності та гетерогенності сучасних мереж.

Вона є масштабованим та гнучким інструментом, який може бути інтегрований у процеси проектування, моніторингу та експлуатації IoT-інфраструктур.

3 МЕТОД ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОГО ФУНКЦІОНУВАННЯ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ НА ОСНОВІ АЛГОРИТМУ ЕВРИСТИЧНОГО ПОШУКУ

3.1 Основи методу забезпечення безпечного функціонування пристроїв Інтернету речей на основі алгоритму евристичного пошуку

Для досягнення поставленої мети було удосконалено метод забезпечення безпечного функціонування пристроїв Інтернету речей на основі алгоритму евристичного пошуку.

З цією метою було використано апарат графу атак - моделі комп'ютерної мережі, яка охоплює зв'язок комп'ютера, уразливості, активи та експлойти.

Він використовується для представлення набору складних багатоетапних шляхів атаки (надалі плани атаки) і може використовуватися для оцінки та кількісного визначення ризику безпеки.

У дослідженні запропонований метод доповнює аналіз графів атак для врахування фізичного розташування пристроїв IoT та їхніх комунікаційних можливостей.

Спираючись на нові графи атак, можна кількісно оцінити ризик додавання пристрою IoT до певної мережі та показати, що він може зрости через розгортання лише шести пристроїв IoT на малому та середньому підприємстві.

Метод також уможливлює оптимізувати розгортання пристроїв IoT, щоб зменшити негативні наслідки такого розгортання для безпеки.

Метод включає дві шляхи оптимізації:

- розгортання з мінімальним ризиком (FDMR), де всі необхідні пристрої IoT повинні бути розгорнуті з мінімальними наслідками для безпеки
- досягнення максимальної корисності без погіршення ризику (MURD), де має бути максимальна кількість пристроїв IoT розгорнутий без збільшення ризику безпеки мережі.

Удосконалений метод використову алгоритм евристичного пошуку з розгалуженням у глибину та межами (DFBnB), щоб вирішити обидві задачі

оптимізації та запропонувати прийнятну евристичну функцію для прискорення пошуку.

3.2 Графи атак

Для вирішення поставлених задач було застосовано граф атак -– це модель комп’ютерної мережі, яка охоплює комп’ютерне підключення, уразливості, активи та експлойти.

Графи атак використовуються для представлення наборів складних багатоетапних сценаріїв атак, що проходять через організацію від початкової точки входу до найбільш критичних активів IoT.

Аналізуючи граф атак, аналітик безпеки може оцінити ризики потенційних вторгнень і розробити ефективні стратегії захисту.

Методологія аналізу графа атак містить три основні етапи:

(1) сканування мережі та вразливостей;

(2) моделювання графа атак;

(3) аналіз графа атак.

На першому етапі сканер вразливостей Nessus [102] використовується для відображення вразливостей усіх хостів в організації.

З’єднання між хостами може бути ідентифіковано системними адміністраторами вручну на основі топології мережі організації та конфігурацій брандмауера. Nessus, Nmap або інші мережеві сканери можуть допомогти в процесі оцінки підключення.

Звіти про підключення до мережі та вразливості обробляються MulVAL [103] для створення представлення графа атак мовою визначення домену планування (PDDL).

Граф атак складається з вузлів привілеїв, вузлів експлойтів/дій і вузлів фактів.

У графі атаки вузол привілеїв представляє отриману інформацію або привілеї доступу, які отримує потенційний зловмисник (на графі представлено трикутниками).

Вузол експлойт/дія представляє дію, необхідну зловмиснику для використання вразливості (позначено овалами).

Краї побудованих вузлів експлойту призначені для передумов і постумов експлойту.

Фактичний вузол представляє стан мережі, який повинен існувати, щоб зловмисник міг використати вразливість (представлено прямокутниками). Щоб отримати привілей, зловмисник повинен виконати дій, що призводять до цього (логічне АБО).

Щоб використовувати експлойт, зловмиснику потрібні всі привілеї та факти, які призводять до експлойту (логічне І).

Експлойт-вузол потребує всіх цих попередніх умов, що призводять до його виконання, і після виконання зловмисник отримує всі постумови, до яких призводить експлойт-вузол.

Після побудови графа атак представлення графа PDDL було використано як модель предметної області для різноманітних планувальників.

Типовим завданням є пошук оптимального плану атаки або оцінка ймовірності успішного атаки на основі графа атаки організації.

Отже, графи атак було використано для посилення безпеки мережі за допомогою різноманітних оптимізацій графів атак.

3.3 Евристичний пошук

Наступним кроком розв’язку було залучення евристичного пошуку – сімейства методів, які використовуються для вирішення складних задач штучного інтелекту.

У цьому випадку кожна задача представлена станами, де кожен стан представляє поточний стан задачі.

Кожна задача також має початковий стан і один або більше досліджуваних цільових станів.

Простір пошуку – це середовище, в якому відбувається пошук, де мета пошуку – знайти шлях від початкового стану до одного з цільових станів у просторі пошуку.

Кожне рішення представляє один цільовий стан.

Якість рішення вимірюється вартістю цільового стану.

Алгоритми пошуку розрізняють мінімум і максимум задач.

У задачі мінімуму необхідно знайти рішення з найменшою вартістю, а в задачі максимуму бажане рішення з найвищою вартістю.

Більшість задач – це мінімум задач, наприклад, необхідно найдешевше або найшвидше рішення.

Якщо не зазначено інакше, мається на увазі мінімальну задачу.

У дослідженні було використано алгоритм розгалуження в глибину та зв’язку, який використовує евристичну функцію для більш ефективного вирішення задач.

Евристика – це оцінка вартості досліджуваного шляху від вузла n до цільового вузла.

Евристична функція використовується для спрямування алгоритму пошуку в напрямку мети.

У поінформований спосіб евристика допомагає алгоритму здогадатися, який дочірній елемент з усіх дочірніх вузлів приведе до мети.

Якщо для будь-якого n евристична функція ніколи не переоцінює вартість найкращого шляху від вузла n до цільового вузла, тоді ця функція називається допустимою евристичною функцією .

В задачі знаходження максимуму (де необхідно отримати рішення з максимальною вартістю) це навпаки, тобто евристична функція, яка ніколи не недооцінює вартість найкращого шляху.

Нехай потрібно знайти найкоротший шлях від точки А до точки Б.

Це мінімальна задача, де ціною є відстань між двома точками.

Хорошою допустимою евристичною функцією може бути відстань у повітрі, оскільки фактичний шлях між обома точками ніколи не буде меншим за відстань у повітрі.

У більшості пошукових алгоритмів, а також в алгоритмі DFBnB однією з найважливіших умов для евристичної функції є те, що вона повинна бути допустимою.

Розглянемо алгоритми пошуку, A ∗ , IDA ∗ та DF BNB [26].

Базовий алгоритм – A*, який знаходить оптимальний шлях, якщо евристична функція допустима.

Його перевага полягає в тому, що він розширює найменшу кількість необхідних вузлів.

Його основним недоліком є потреба в пам’яті, як і будь-які алгоритми пошуку найкращим, і тому він не може вирішити більшість складних задач, які потрібно вирішити.

IDA* – це A* з ітеративним поглибленням, і він усуває задачу пам’яті A*, не завдаючи шкоди оптимальності.

Кожна ітерація алгоритму є пошуком у глибину, який відстежує вартість, яка обчислюється як в алгоритмі A*.

Коли вартість перевищує певний поріг, вона обривається, а пошук повертається назад, а потім продовжується.

Початковий поріг –це евристична оцінка початкового вузла, коли в кожній наступній ітерації він збільшується на найменшу вартість, яка була відрізана на попередній ітерації.

Вимоги до пам'яті IDA* є лінійними при пошуку максимальної глибини, і його рішення є оптимальним, якщо евристична функція допустима.

Він є асимптотично оптимальним у часі та просторі над A* і його легше реалізувати.

IDA* добре підходить для розсувних головоломок або кубиків Рубіка.

Алгоритм DFBnB – це алгоритм пошуку в глибину [26, 65].

Алгоритм використовується для навігації в просторі пошуку та пошуку оптимального рішення.

Під час процесу пошуку DFBnB підтримує найкраще знайдене рішення.

Для того, щоб виконувати скорочення частіше і таким чином прискорити процес пошуку, DFBnB використовує евристичну функцію.

Вартість вузла визначається як:

$$f(e) = m(e) + n(e), \tag{3.1}$$

де $f(e)$ є сумою поточної вартості вузла $m(e)$;

евристична функція для цілі $n(e)$, яка є оцінкою вартості від вузла x до цілі.

Таким чином, f (x) оцінює найменшу загальну вартість будь-якого шляху рішення, що проходить через вузол x .

Якщо знайдено гілку з вищою вартістю, її можна обрізати, щоб не було потреби продовжувати розширення до неї.

Алгоритм повертає оптимальне рішення з лінійним простором пам’яті, припускаючи, що евристична функція допустима.

Це рішення залежить від типу задачі (тобто мінімальна чи максимальна), яка визначається вартістю цільового стану.

DFBnB підходить для задач, коли максимальна глибина пошуку відома заздалегідь або дерево пошуку кінцеве, як у задачі комівояжера (TSP) або як у нашій задачі, тому що кожен вузол має двох дітей.

У дослідженні було обрано евристичний алгоритм DFBnB, оскільки він відповідає задачі.

3.4 Графи атак IoT. Розгортання IoT

У типовій організації всі хости (робочі станції та сервери) підключені до організаційної мережі через дротове або бездротове з'єднання.

Нехай $N = \{ n_1, n_2, \dots, n_w \}$ – набір хостів, які є частиною комп'ютерної мережі організації.

Окрім звичайних хостів, комп'ютерна мережа організації може містити пристрої IoT.

Нехай $T = \{ t_1, t_2, \dots, t_w \}$ – вказує на набір унікальних пристроїв IoT, присутніх в мережі.

Кожен пристрій IoT мережі t_i має унікальний ідентифікатор (зазвичай це IP-адреса).

Пристрої IoT відрізняються за своїм функційним призначенням і можливостями.

Наприклад, холодильник здатний підтримувати низьку температуру, а смарт-телевізор здатний показувати фільми високої чіткості.

Таким чином, було здійснено групування пристроїв IoT за типом, наприклад, холодильник, телевізор, камера, детектор диму тощо.

$D = \{ d_1, d_2, \dots, d_h \}$ – це набір усіх типів пристроїв IoT.

Позначимо набір усіх пристроїв типу d як T (d), а окремий пристрій типу t як d (t).

Припустимо, що кожен пристрій комп'ютерної мережі IoT є частиною лише однієї групи.

Деякі пристрої IoT можна розгортати лише в певних заздалегідь визначених місцях.

Наприклад, кухня зазвичай є призначеним місцем для холодильника, тоді як великі телевізійні екрани або проектори знаходяться в кімнатах для нарад.

Деякі пристрої IoT, такі як камери або детектори диму, можуть бути розгорнуті в різних місцях організації.

Нехай $S = \{ s_1,\ s_2,\ \dots ,\ s_n \}$ вказує набір унікальних точок розташування, де можна розгорнути пристрої IoT.

Позначимо набір місць, де можна розгорнути пристрій IoT певного типу $d \in D$ як $S(d) \subseteq S$.

У кожній точці розташування може бути розгорнуто лише один тип пристроїв IoT, тобто $S(d)$ визначається таким чином, що перетин кожної пари наборів $S(d_e)$ є порожнім, $\cap_{d \in S(d)} = \emptyset$.

Тому що місце розташування повинно бути бути пов'язаним з деяким типом пристроїв IoT, об'єднання $S(d)$ дорівнює S, $\cup_{d \in S(d)} = S$.

Організації можуть мати обмеження щодо розгортання пристроїв IoT в мережі.

Було визначено два основних обмеження для типу пристрою d.

Перший – це кількість місць (із загальної кількості доступних), які повинні містити розгорнутий пристрій цього типу.

Наприклад, є чотири можливі місця для камер у коридорі, але організації потрібно розгорнути лише дві з них.

Другим обмеженням є кількість пристроїв кожного типу. Наприклад, для одного місця, де можна розгорнути холодильник, існує три можливих холодильники, які організація може придбати.

Нехай B – множина всіх обмежень.

$B(d)$ – це кортеж, який представляє обмеження для типу d:

$$B(d) = \big(S(d),\ h(d),\ T(d)\big). \tag{3.2}$$

де:

$S(d)$ – це набір місць, де можна розгорнути пристрій IoT певного типу $d \in D$ (як визначено у визначенні 1);

$h(d)$ – це кількість місць, які необхідно було розгорнути з усіх місць у $S(d)$;

$T(d)$ – це набір усіх пристроїв IoT типу d.

Нехай організація має три можливі місця, у яких можна розгорнути телевізор ($S(TV) = \{ s_{TV1},\ s_{TV2},\ s_{TV3} \}$), але потрібно розгорнути телевізор лише в двох із цих місць ($h\ (TV) = 2$).

Крім того, існує чотири різні телевізори, які можна розгорнути:

$$T(TV) = \{t_{TV1},\ t_{TV2},\ t_{TV3,}\ t_{TV4}\}. \quad (3.3)$$

Формально обмеження $B(TV)$ буде визначено таким чином:

$$B(TV) = \left(\{ s_{TV1},\ s_{TV2},\ s_{TV3,} \},\ 2,\ \{ t_{TV1},\ t_{TV2},\ t_{TV3,}\ t_{TV4} \} \right) . \quad (3.4)$$

$s \in S$ можна розгорнути не більше одного пристрою IoT .

Розгортання пристроїв IoT визначається як функція d: $T \longrightarrow S\ Y\ \{\perp\}$, яка відображає кожен пристрій у певному місці.

Спеціальний символ розташування $\perp$ означає, що пристрій в мережі не розгорнуто.

Будемо вважати, що розгортання дійсне, якщо воно не порушує обмежень вищевказаних обмежень.

Нехай $d: T \longrightarrow S\ Y\ \{\perp\}$ буде розгортанням пристроїв IoT. d дійсний, якщо $\forall t \in T, d(t) \in S(d\ (t)\ ) Y\{\perp\}$.

Позначимо d_{full} як розгортання, яке задовольняє всі обмеження B, і d_{empty} як порожнє розгортання без розгорнутих пристроїв IoT.

Зауважимо, що умова $h(d) \leq |T(d)|$ має бути виконано для повного розгортання мережі.

Багато пристроїв IoT, розгорнутих у приміщеннях організації, ймовірно, зможуть спілкуватися з сусідніми хостами через протоколи зв’язку малого радіусу дії (SRC), такі як ZigBee, Bluetooth, ad hoc Wi-Fi тощо.

Деякі хости в організації також можуть підтримувати протоколи SRC , що може дозволити супротивнику переходити між мережами.

Визначаємо набір протоколів зв'язку малої дальності

$$\mathcal{R} = \{p_1, p_2, \ldots\}. \quad (3.3)$$

Нехай $r: T\ Y\ N \longrightarrow 2^{\mathcal{R}}$ бути функцією, яка відображає пристрій IoT або хост на підмножину протоколів SRC, які він підтримує.

У дослідженні будемо використовувати термін «пристрій» для позначення як пристроїв IoT, так і хостів.

Будь-які два пристрої в комп'ютерній мережі, підключені за допомогою протоколу SRC, повинні знаходитися на певній відстані один від одного (тобто в радіусі зв'язку).

Наприклад, нехай $t \in T$ – деякий пристрій IoT, який підтримує протокол SRC $g \in \mathcal{R}$, і нехай $n \in N$ – деякий хост, який підтримує той самий протокол. Якщо t розгорнуто в місці s , а n знаходиться в радіусі зв'язку s , тоді t може спілкуватися з n і навпаки.

Визначаємо діапазон як $S\ Y\ \perp^{2\ T\ \cup\ N}$ певного місця як набору хостів, які можуть спілкуватися з розгорнутим там пристроєм IoT.

Важливо зазначити, що дальність $s,\ s \in S$ – це оцінка на основі специфікації радіозв'язку різних пристроїв IoT.

Фактичний набір пристроїв у діапазоні розгортання пристрою IoT у місці l може змінюватися залежно від потужності радіо, перешкод тощо.

Для зручності обговорення було зроблено абстракцію такого діапазону.

Було визначено три різні діапазони:

- ShortRange;
- MediumRange;
- LongRange.

Два пристрої можуть мати однаковий протокол зв'язку малого радіусу дії, але різні діапазони.

Кожному пристрою IoT було призначено діапазон, який залежить від його SRC .

Для кожного розташування, для кожного SRC ми визначили набір хостів , які знаходяться в діапазоні від цього розташування l.

Якщо пристрій IoT розгорнуто в певному місці, він може підключитися до всіх хостів у цьому місці, які мають той самий SRC і той самий діапазон.

Набір хостів у ShortRange є підмножиною MediumRange , яка є підмножиною LongRange .

Пристрій може перебувати в діапазоні кількох місць і що жоден пристрій не знаходиться в діапазоні нелокації $\pm$ (тобто діапазон $(\pm) = \emptyset$).

3.5 Визначення графа атак

Потенційні місця розташування пристроїв Інтернету речей і протоколів SRC інтегровані в методологію аналізу графа атаки після етапу сканування та перед моделюванням графа атаки.

Для кожного можливого розгортання пристроїв IoT, яке буде розглянуто під час оптимізації, здійснюється доповнення карти підключення пристроїв, щоб включити гіпотетичні зв'язки між будь-яким пристроєм IoT $t \in T$, розгорнутим у розташуванні $d\ (t)$, і всіма пристроями в діапазон t : діапазон $\big(d(t)\big)$.

Після того, як зв'язок між усіма пристроями визначено, ми використовуємо стандартну структуру MulVAL для створення графа атак, який враховує певне розгортання пристроїв IoT.

Кожне розгортання має інший граф атак, залежно від розгорнутих пристроїв в мережі.

Якщо жоден пристрій IoT не розгорнуто, розгортання буде порожнім $\big(d_{empty}\big)$, а граф атак є просто вихідним графом атак організації.

Нехай d – це розгортання пристроїв IoT в організації. Граф логічної атаки M_d є кортежем:

$$M_d = \left(H_k, H_x, H_j, X, G, m \right), \tag{3.4}$$

де H_k, H_x і H_j – набори вузлів привілеїв, вузлів експлойту та фактичних (листових) вузлів відповідно;

X – набір орієнтованих ребер.

При цьому :

$$X \subseteq (H_k \; e \; H_x) \; Y \; \Big(H_x \; e \; \big(H_x \; Y \; H_j \big) \Big). \tag{3.5}$$

У графі атак є два типи ребер. Перехід $(x,\ k) \in X$ від вузла експлойту $x \in H\ x$ до вузла привілеїв $k \in H\ k$ означає, що зловмисник може отримати привілей k, виконавши exploit e.

Щоб отримати привілей, зловмиснику потрібно виконати один із експлойтів, які ведуть до нього.

Перехід $(j,\ x) \in X$ від вузла фактів або вузлів привілеїв $j \in H_j \; U \; H_k$ до вузла експлойту $x \in H_x$ означає, що вузол j є передумовою для виконання досліджуваного експлойту x.

Наприклад, вузол фактів може бути вразливістю в протоколі Bluetooth, якою можна скористатися, якщо зловмисник знаходиться в зоні дії Bluetooth вразливого пристрою.

Щоб запустити експлойт, зловмиснику потрібні всі привілеї та факти, які ведуть до експлойту.

У дослідженні орієнтації ребер слідують напрямку неявної логічної операції.

Подамо формально план атаки як:

$\wp(x) = \{q \in H_k \; Y \; H_j \; (q,\ x) \in X\}$ – усі передумови вузла x .

$\mathcal{b}(k) = \{x \in H_x \mid q \in H_k \ \& \ (x,\ q) \in X\}$ – це набір експлойтів, які призводять до вузла привілеїв p (набору привілеїв, отриманих зловмисником).

Предствимо план атаки як це підграф M_d деякого графа атаки M_d, який представляє сценарій, за яким зловмиснику вдається досягти мети, а саме $m \in M\ tk$.

Отже, у плані атаки всі попередні умови експлойту $x \in M_d$ і задовольняються, і кожен привілей $k \in M\ tk$ отримується експлойтом.

Нехай AP (M_d) – усі плани атаки графа M_d.

Кожен план атаки $M_d \in X\ \mathcal{A}\ (M_d)$ повинен задовольняти таким трьом умовам:

$$m \in M_d$$
$$\forall\ r \in H_x : \mathcal{p}(r) \subseteq M_d \mid H_x \in M_d$$
$$\forall\ k \in H_k : \exists\ r \in \mathcal{b}(k) \subseteq M_d \mid H_k \in M_d\ . \qquad (3.6)$$

Розглянемо довжину плану атаки як кількість вузлів, які він містить.

OptLen (M_d) – це довжина найкоротшого плану атаки на графі G.

Тоді OptCnt (M_d) вказує, скільки найкоротших планів атаки є на графі G.

Розглянемо також середню кількість експлойтів у найкоротших планах атаки на графі G як OptExp (M_d) та середню кількість привілеїв у найкоротших планах атаки як OptPrv (M_d) .

3.6 Оцінка ризику

Безпеку мережі можна оцінити за показником ризику, де чим вищий показник ризику, тим нижча безпека мережі.

У середовищі, в якому розгортаються пристрої IoT, є кілька аспектів, які слід враховувати під час вибору методу обчислення оцінки ризику.

По-перше, метод повинен дати відповідь, що розгортання пристроїв IoT може створити нові плани атак.

Відповідно, вартість атаки може знизитися, а ймовірність атаки може зрости через додаткові вразливості та можливості для бокового руху, якими може скористатися зловмисник.

Нарешті, метод має вказувати на зміни в різних розгортаннях і бути достатньо чутливим, щоб виявити зміни, викликані розгортанням навіть одного додаткового пристрою IoT.

Розглянемо розгортання пристроїв IoT, які поєднують кілька аспектів комп'ютерної мережі.

В дослідженні розраховуються всі найкоротші плани атак, враховуючи їх довжину, кількість, середню кількість експлойтів і середню кількість наявних привілеїв.

Головна мета – порівняти різні розгортання, намагаючись визначити між двома мережами, яка з них є більш безпечною.

Для цього було розраховано всі наведені вище параметри для мережі, у якій не було розгорнуто пристроїв Інтернету речей, і на основі цього було отримано оцінку ризику для кожного розгортання.

Таким чином, метою є порівняння різних розгортань.

Задамо оцінку ризику.

Нехай $A(d)$ – це число, яке представляє показник ризику розгортання, а $A(d_{empty})$ – це показник ризику розгортання без розгорнутих пристроїв IoT:

$$A(d) = \frac{\mathcal{T}Len(M_d)}{\mathcal{T}Len\left(M_{d_{empty}}\right)} - 1 +$$

$$\frac{\mathcal{T}Cnt(M_d)}{\mathcal{T}Cnt\left(M_{d_{empty}}\right)} - 1 +$$

$$\frac{\mathcal{T}Exp(M_d)}{\mathcal{T}Exp\left(M_{d_{empty}}\right)} - 1 +$$

$$\frac{\mathcal{J}Prv(M_d)}{\mathcal{J}Prv\left(M_{d_{empty}}\right)} - 1 \ . \tag{3.7}$$

Оцінка ризику – це загальна сума відносного збільшення кожного параметра. Мінімальне значення $A(\mathcal{d})$ дорівнює нулю, як і порожнє розгортання мережі:

$$A\left(\mathcal{d}_{empty}\right) = 0. \tag{3.8}$$

Значення один означає, що в середньому значення кожного параметра подвоїлося.

3.7 Оптимізація розгортання задачі

Розглянемо питання оптимізація розгортання задачі. З цією метою було використано поняття, які використовуються для визначення двох задач оптимізації розгортання IoT:

- Повне розгортання з мінімальним ризиком (FDMR);
- Максимальна корисність без погіршення ризику (MURD).

Маючи граф атак організації G , набір пристроїв IoT D типів T і обмеження розташування C, знайдіть розгортання $\left(\mathcal{d}_{full}\right)$ пристроїв IoT таким чином, щоб усі пристрої IoT розгорталися відповідно до обмежень розташування, а оцінка ризику $A\left(\mathcal{d}_{fun}\right)$ зведена до мінімуму.

Опишемо задачу повного розгортання з мінімальним ризиком (FDMR).

Враховуючи кортеж < G, D, T, C >, необхідно знайти $\mathcal{d}_{full}$ так, щоб $A\left(\mathcal{d}_{fun}\right)$ було мінімізоване

$$\mathcal{g}_{min}\left\{A\left(\mathcal{d}_{full}\right)\right\}.$$

Маючи граф атак організації G , набір пристроїв IoT D типів T і обмеження розташування C, необхідно знайти розгортання, яке складається з найбільшої кількості пристроїв IoT без збільшення оцінки ризику R.

Опишемо задачу максимальної корисності без погіршення ризику (MURD).

Дано кортеж < G, D, T, C >. Необхідно знайти d такий, що $|A(d)|$ максимізується і $A\ (d) = A\left(d_{empty}\right)$

$$g_{max}\left\{\ |A\ (d)|\ :\ A\ (d) = A\left(d_{empty}\right)\right\} \tag{3.9}$$

Визначимо простір пошуку для FDMR і MURD.

У кожному випадку стан простору пошуку організовано як бінарне дерево, де в кожному стані приймається рішення розгортати (лівий дочірній елемент) або не розгортати (правий дочірній) певний пристрій IoT у певному місці.

Кореневий стан – це порожнє розгортання $\left(\ A\left(d_{empty}\right)\ \right)$, де ще не прийнято жодних рішень.

Кожен шлях від кореневого вузла простору пошуку відповідає набору рішень.

Це означає, що шлях від кореня до будь-якого стану визначає, де розгортаються деякі пристрої IoT і де інші пристрої мережі IoT не можуть бути розгорнуті.

Набір дочірніх елементів уздовж шляху є частковим розгортанням пристроїв IoT.

Таким чином, було розглянуто всі можливі розгортання з урахуванням обмежень щодо розташування.

Для кожного вузла простору пошуку ми отримуємо відповідний граф атак G_{depl} і обчислюємо оцінку ризику $A\ (d)$.

Цільові вузли залежать від конкретної задачі.

У задачі FDMR цільові вузли включають усі стани з розгортанням, яке відповідає всім обмеженням, d_{full}, і метою є визначення цільового стану з найнижчим показником ризику.

У задачі MURD цільові стани включають всі стани з розгортанням, яке має такий самий показник ризику, як початковий стан.

Використовуючи наведені вище визначення, здійснюється обчислення розміру простору пошуку, тобто кількість можливих повних розгортань.

Необхідно знайти загальну кількість різних розгортань залежно від існуючих обмежень, обчислюючи кількість можливих розгортань для кожного типу розташування та множачи всі результати один на одного.

Щоб обчислити кількість усіх можливих розгортань у t, використовуємо перестановку і поєднання 2, де перестановка n P k означає, що для n елементів ми хочемо знайти кількість способів упорядкування k елементів.

Перестановка визначається як: $K\ p = \frac{h!}{(h-p)!}$, і комбінація визначається як:

$$\binom{h}{p} = \frac{h!}{p!\ (h-p)!}. \tag{3.10}$$

Нехай необхідно обчислити кількість можливих розгортань типу TV,

$$B(TV) = (\{\ s_{TV1},\ s_{TV2},\ s_{TV3}\ \},\ 2,\ \{\ t_{tv1},\ t_{tv2},\ t_{tv3},\ t_{tv4}\ \}).$$

По-перше, здійснюється обчислення перестановки кількості пристроїв типу t ($|\ T(TV)\ | = 4$) поза місцями для розгортання ($h\ (TV) = 2$).

Було використано перестановку, оскільки в цьому випадку порядок має значення, оскільки кожен пристрій унікальний, а розташування кожного пристрою означає різне розгортання.

Якщо обрати два пристрої та розгорнемо їх у двох місцях, і якщо обрати ті самі два пристрої, але поміняти їх розташування, розгортання будуть різними, $| T(TV) | K_h = 4K_2 = 12$.

Далі здійснюється обчислення комбінації кількості місць, які необхідно розгорнути в типі t ($h\ (TV) = 2$) із місць для розгортання ($| S\ (TV) | = 3$).

У цьому випадку використовується комбінація, оскільки порядок не має значення.

Всього є три локації, і нам потрібно розгорнути лише дві з них:

$$\binom{| S\ (TV) |}{h\ (TV)} = \binom{3}{2} = 3.$$

Отже, кількість можливих різних розгортань у типі TV дорівнює 36, 3 • 12 = 36.

Формула для обчислення розміру можливих розгортань, який також визначається як розмір простору пошуку, виглядає наступним чином:

$$K_{d \in D}\left(\binom{| S\ (TV)|}{h\ (TV)}\right) | T(d) | K_{h\ (d)}$$

Тут виконується множення кількості усіх можливих розгортань кожного типу.

3.8 Евристичний пошук

Запропонований метод застосовує евристичний пошук на основі алгоритму DFBnB.

Пошук за алгоритмом DFBnB дозволяє скорочувати час роботи.

Крім того, у спосіб, яким побудовано простір пошуку, коефіцієнт розгалуження дорівнює двом (кожен вузол має рівно двох дочірніх елементів), і алгоритм підходить для задач із низьким коефіцієнтом розгалуження.

Кожен стан у дереві пошуку стосується двох дочірніх елементів (лівого та правого).

В одному випадку було додано пристрій IoT до розгортання в певному місці, а в іншому не дозволено розгортати пристрій IoT у цьому місці.

На практиці кожна держава має різні варіанти щодо того, які пристрої IoT розгорнути.

Було використано впорядкування вузлів, щоб вибрати один пристрій d і одне розташування l , де d все ще можна розгорнути, і створити двох дочірніх елементів: розгортати d в l і не розгортати d в l.

Для лівого дочірнього елемента, що відповідає рішенню про розгортання, ми створюємо новий граф атак і перераховуємо показник ризику.

Для представлення виконання методу було ініціалізовано змінні, включаючи додавання порожнього розгортання без розгорнутих пристроїв IoT до стека.

Для кожного стану, який ми витягли зі стеку, було згенеровано двох нащадків:

- l_s відповідає лівому згенерованому дочірньому елементу;
- l_a відповідає правому.

Було обчислено f -значення для кожної дитини (якщо немає евристичної функції, $f(x) = m(e)$).

Розрахунок ризику безпеки базується лише на лівій дочірній системі.

Коли досягається цільовий вузлол (повного розгортання), здійснюється його збереження як найкраще рішення та оновлюється альфа-версія.

Далі здійснюється додавання до стеку дочірній елемент, лише якщо його f -значення менше за a.

Показаний псевдокод підходить для виконуваної задачі FDMR.

Щоб обчислити евристичні функції, було створено таблицю оцінок ризиків Table ($\mathcal{d}_h$), яка містить оцінки ризиків для кожного пристрою IoT у кожному можливому місці.

Іншими словами, кожного разу моделюється розгортання одного пристрою IoT.

Для кожного розгортання ми оновлюємо таблицю, видаляючи пристрій IoT, який було розгорнуто або заборонено розгортати.

Для задачі FDMR евристична функція недооцінює найменшу можливу зміну ризику в кожному піддереві.

Тоді, коли оцінка ризику найкращого повного розгортання, знайденого на даний момент, нижча за оцінку ризику будь-якого повного розгортання, яке можна знайти в піддереві, це піддерево скорочується.

Алгоритм 3.1 - Алгоритм DFBnB

```
procedure DFBnB ( a, b )
alpha ← ∞
bestSolution ← null
stack ← { root }
while stack ≠ 0 do
state ← stack.pop
l_s, l_a ← getTwoSons (state )
f l_s, f l_a ← calcF ( l_s , l_a)
a ← calcSecurityRisk ( l_s )
if isGoal (l_s) then
alpha ← fs i bestSolution ← r
if f l_s ≤ alpha  then
stack ← { l_s }
if f l_a) ≤ alpha  then
 stack ← { l_a) }
```

```
return bestSolution
```

Для FDMR нехай $n_{FDMR}(d_h)$ буде евристикою depln. $n_{FDMR}(d_h)$ -– мінімальний $A(d_t)$ і $A(d_t) \in$ Таблиця (d_h).

$$n_{FDMR}\,(d_h) = \mathcal{g}_{min}\,\{\,A\,(d_t) \in Table\,(d_h)\,\}$$

Інтуїтивно зрозуміло, n_{FDMR} занижує оцінку ризику, оскільки (1) окремо кожен розгорнутий пристрій збільшує ризик відповідно до таблиці (d_h), але (2) разом кілька розгорнутих пристроїв можуть призвести до планів атак, які ще не були враховані.

Для задачі MURD евристична функція переоцінює найбільшу можливу зміну в кількості пристроїв IoT, які можна розгорнути без збільшення ризику.

Тоді, коли кількість пристроїв, розгорнутих відповідно до поточного рішення Bent, знайденого на даний момент, перевищує кількість пристроїв, які можливо розгорнути, продовжуючи пошук у піддереві, це піддерево скорочується.

Необхідно розгорнути якомога більшу кількість пристроїв IoT, тому евристична функція підраховує кількість пристроїв IoT у таблиці (d_h) з тим самим показником ризику, що й кореневий стан.

Нехай h (d_h) буде евристикою d_h. h MURD (d_h)є кількість пристроїв із показником ризику, що дорівнює початковому стану $A\left(d_{empty}\right)$, таким чином, що:

$$\left|\, A\,(d_t) = A\left(d_{empty}\right)\,\right| and\; A\,(d_t) \in Table\,(d_h).$$

$$n_{MURD}(d_h) = \left|\, A\,(d_t) \in Table\,(d_h) :\; A\,(d_t) = A\left(d_f\right)\,\right| = \qquad (3.11)$$

Інтуїтивно зрозуміло, h MURD переоцінює кількість пристроїв, які можна розгорнути, тому що) будь-який пристрій loT, який збільшує ризик відповідно до таблиці (d_h), не може бути розгорнуто, і навіть якщо окремий набір розгорнутих пристроїв робить не підвищувати оцінку ризику, разом вони можуть призвести до плану атаки, який раніше не був доступним.

Щоб швидко знайти оптимальний цільовий вузол, щойно згенеровані дочірні вузли слід шукати в порядку зростання їх вартості. З цією метою було в методі було застосовано принцип node-ordering, що прискорює пошук [104].

У дослідженні було використано евристичну функцію також як упорядкування вузлів. З цією метою було згенеровано нащадка з найнижчою евристикою. Коли не використовується евристичну функцію, здійснюється випадковий вибір дочірньої функції для генерації.

3.9 Висновки до третього розділу

У розділі було розроблено та удосконалено метод забезпечення безпечного функціонування пристроїв Інтернету речей (IoT) на основі алгоритму евристичного пошуку, що дозволяє враховувати не лише логічні, а й фізичні аспекти функціонування IoT-систем у комп'ютерних мережах.

На основі апарату графу атак було здійснено моделювання потенційних сценаріїв компрометації інформаційної безпеки, що виникають при інтеграції нових IoT-пристроїв у наявну мережеву інфраструктуру.

Запропонована модель графа атак була доповнена критично важливими параметрами – фізичним розташуванням пристроїв та їх комунікаційними можливостями, що дозволило значно підвищити точність оцінки безпекових ризиків.

Такий підхід дозволяє глибше зрозуміти взаємозв'язки між пристроями IoT, активами та можливими векторами атак, а також виявити латентні загрози, які можуть бути неочевидними в класичних мережах.

У рамках дослідження були сформульовані два сценарії оптимального розгортання пристроїв IoT, що ґрунтуються на принципах зменшення ризику та збереження мережевої безпеки:

- FDMR (розгортання з мінімальним ризиком) – передбачає інфраструктурне впровадження повного набору необхідних пристроїв IoT з мінімальним впливом на загальний рівень безпеки;

- MURD (максимальна корисність без зростання ризику) – орієнтоване на максимальне використання можливостей IoT без збільшення рівня загроз.

Для розв’язання зазначених задач було використано модифікований алгоритм евристичного пошуку з розгалуженням у глибину з межами (DFBnB), що дозволив ефективно та в прийнятні часові межі знаходити наближену оптимальну конфігурацію розгортання IoT-пристроїв.

Крім того, була розроблена відповідна евристична функція, яка враховує як топологічні, так і безпекові характеристики мережі, що дозволяє пришвидшити процес пошуку та зменшити обчислювальні витрати.

Таким чином, запропонований у розділі метод є універсальним інструментом підтримки прийняття рішень при впровадженні пристроїв IoT в існуючу мережеву інфраструктуру. Він дозволяє одночасно досягти високої функціональної ефективності та забезпечити високий рівень захищеності, що є критично важливим у сучасних умовах зростання кількості кіберзагроз.

4 РЕАЛІЗАЦІЯ ТА ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОГО ФУНКЦІОНУВАННЯ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ НА ОСНОВІ АЛГОРИТМУ ЕВРИСТИЧНОГО ПОШУКУ

4.1 Експериментальні дослідження системи забезпечення безпечного функціонування пристроїв інтернету речей

Для апробації ефективності запропонованої системи забезпечення безпечного функціонування пристроїв Інтернету речей було реалізовано комплекс експериментальних досліджень, спрямованих на розв’язання двох ключових задач: знаходження повного розгортання з мінімальним ризиком (FDMR) та максимізації корисності без погіршення рівня ризику (MURD). В обох випадках було застосовано модифікований алгоритм глибини-пошуку з відсіченням гілок (DFBnB), що використовує евристичні функції, розроблені в межах запропонованого підходу.

Програмно-технічні засоби проведення дослідження включали застосування Nessus Vulnerability Scanner (версія 10.x) для автоматизованого сканування інформаційно-технічної інфраструктури реальної організації з метою виявлення вразливостей, які можуть бути використані під час атак на пристрої IoT.

Також було використано MulVAL (Multi-host, Multi-stage Vulnerability Analysis) для побудови графа атак (attack graph) на основі результатів сканування, що дозволило формалізувати можливі шляхи експлуатації вразливостей у мережі.

Тестове середовище склало комп’ютерну мережу організації, що містить 30 вузлів (хостів), серед яких - як звичайні IT-сервери, так і пристрої IoT.

Віртуалізаційне середовище було Oracle VirtualBox для моделювання топологій та ізоляції тестових сегментів.

Було застосовано сервер із ОС Ubuntu Server 22.04 LTS як система для запуску MulVAL та реалізації серверної частини експериментального модуля.

Реалізація алгоритмічного ядра була здійснена за допомогою мови програмування Python 3.11 з використанням бібліотек networkx (для представлення

графових структур), numpy (для обчислень), heapq (для ефективної реалізації черги з пріоритетом в DFBnB).

Було розроблено модулі: реалізовано окремі програмні модулі для:

a. побудови евристичних функцій на основі ризиків;
b. пошуку рішень за допомогою алгоритму DFBnB;
c. інтеграції з MulVAL для автоматичного завантаження графів атак.

Системи візуалізації та аналізу результатів включала:

1. Graphviz: візуалізація побудованих графів атак.
2. Jupyter Notebook: оформлення, запуск та верифікація результатів кожного етапу дослідження.
3. Matplotlib/Seaborn: побудова графіків та діаграм для порівняльного аналізу ефективності рішень, зокрема залежності рівня ризику та корисності від вибраного маршруту захисту.

Порівняльна оцінка була проведена між базовими (рандомізованими) підходами та запропонованим методом за ключовими метриками:

a. рівень залишкового ризику;
b. корисність розгортання;
c. кількість вузлів у маршруті атаки;
d. час обчислення рішення.

Для здійснення апробації ефективності розробленої системи забезпечення безпечного функціонування пристроїв інтернету речей було проведено експеримент для кожної з задач, які необхідно вирішити: знайти повне розгортання з мінімальним ризиком (FDMR) і знайти максимальну корисність без погіршення ризику (MURD).

Для обох задач було використано запропонований алгоритм DFBnB з евристикою.

Щоб оцінити запропонований метод, було проведено ряд експериментів, використовуючи граф атак, отриманий із мережі реальної організації.

Мережа організації - це справжня мережа, що складається з 24 хостів. Мережу організації було просканово за допомогою засобу Nessus Scanner, а потім за допомогою MulVAL сформували граф атак за результатами сканування комп'ютерної мережі.

На рисунку 4.1 зображено з'єднання хостів у мережі, виведене з топології VLAN.

На рисунку 4.1 різні кольори представляють різні VLAN.

Сині вузли – це DMZ VLAN, а помаранчеві вузли – мережа внутрішньої організації. Кожен вузол представляє хост, а ребро вказує на з'єднання між двома хостами.

Кожен вузол представляє хост, а ребро вказує на з'єднання між двома хостами.

Організація може мати більше ніж один хост, який вона бажає захистити, і це означає кілька цілей для зловмисника.

Щоб спростити речі, усі цільові хости підключені до абстрактного goalHost, а мета графу атак полягає у виконанні коду на цьому хості.

Виконання коду на цільовому хості доводить, що зловмиснику вдалося контролювати один із цільових хостів, який призвів до цілі.

У рамках експериментальної установки було зроблено припущення, що організація вільна від внутрішніх противників і що потенційний зловмисник знаходиться в Інтернеті.

Граф атак має хост, який представляє Інтернет.

Мережа організації, яка використовується в експерименті, не включала пристрої IoT.

Тому було вирішено симулювати пристрої IoT, їхні протоколи зв'язку та обмеження, необхідні для їх розгортання.

Для цього було змодельовано три типи IoT (детектор, холодильник, камера), дев'ять різних пристроїв IoT (чотири детектори, дві камери та три холодильники) і вісім місць для розгортання пристроїв IoT.

Під час симуляції було розгорнуто три детектори, для яких є чотири можливі місця розташування, одну камеру, для якої є два можливі місця розташування, і два холодильники, для яких є два можливі місця розташування.

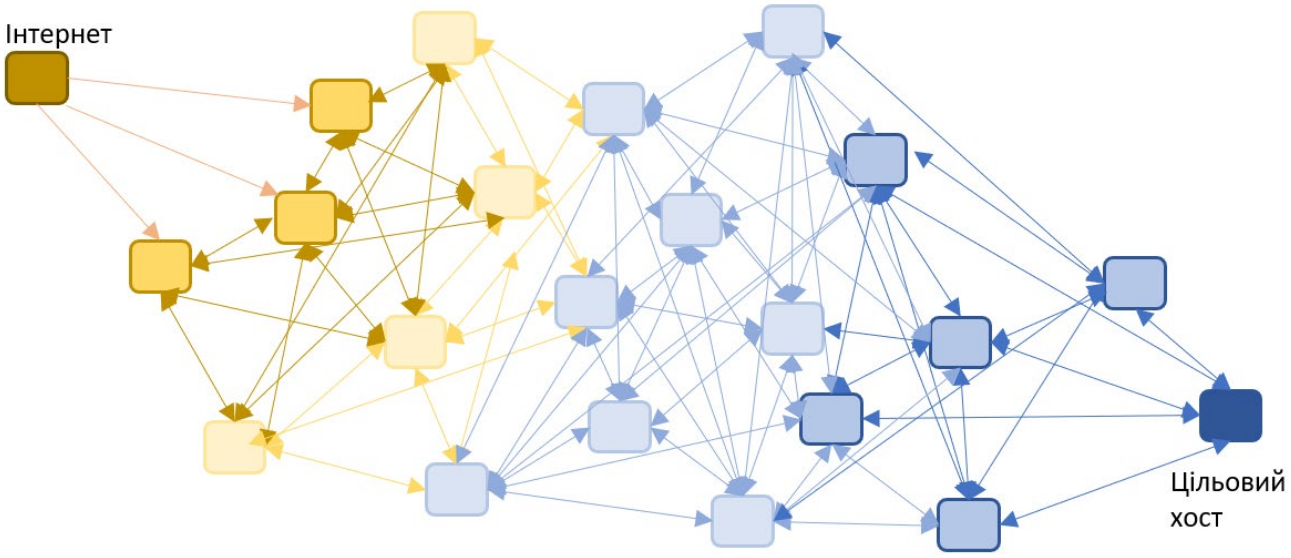


Рисунок 4.1 - Граф підключення хостів в організаційній мережі, отриманий на основі топології VLAN

Таким чином, загалом потрібно було розгорнути шість пристроїв IoT.

Формально, обмеження розташування в моделюванні визначаються таким чином:

$$C(detector) = (\{l_{det1}, l_{det2}, l_{det3}, l_{det4}\}, 3, \{d_{det1}, d_{det2}, d_{det3}, d_{det4}\})$$
$$C(camera) = (\{l_{cam1}, l_{cam2}\}, 1, \{d_{cam1}, d_{cam2}\})$$
$$C(refrigerator) = (\{l_{ref1}, l_{ref2}\}, 1, \{d_{ref1}, d_{ref2}, d_{ref3}\}) \quad (4.1)$$

Тепер можна обчислити розмір простору пошуку:

$$\binom{4}{3}_4P_3 * \binom{2}{1}_2P_1 * \binom{2}{2}_2P_2,$$

що свідчить про те, що існує більше 2000 можливих розгортання.

Також було змодельовано два протоколи зв’язку малого радіусу дії (ZigBee і Bluetooth) і випадковим чином розподілили їх між усіма пристроями IoT і мережними хостами.

Співвідносшення склало:

- 75% хостів мали Bluetooth і 20% з них мали Zigbee;

- 40% пристроїв IoT мали Bluetooth і 80% з них мають Zigbee.

Шанс для Zigbee не залежить від шансу Bluetooth, і навпаки.

Для кожного пристрою для кожного з його протоколів зв’язку короткого радіусу дії було випадковим чином обирано діапазон протоколу.

Як правило, Bluetooth-пристрої мають більший радіус дії порівняно з пристроями, що працюють за протоколом ZigBee.

У зв’язку з цим, для ZigBee-пристроїв передбачено два варіанти радіуса дії: ShortRangeз ймовірністю 50% або MediumRange з ймовірністю 50%.

Натомість Bluetooth-пристрої могли отримати MediumRange з ймовірністю50% або LongRange з ймовірністю 50%.

Щоб створити потенційні плани атак, які включають пристрої IoT, було змоделювали наявні вразливості, які можна використати наступним чином.

Для кожного пристрою IoT і для кожного хоста, окрім відомих вразливостей (за результатами сканування), було створено вразливість на основі використовуваного протоколу.

Фактичне фізичне розташування справжніх мережних хостів було недоступним.

Розташування хостів важливе для імітації близькості пристроїв IoT до хосту та, отже, створення потенційних планів атак із залученням пристроїв IoT.

Тому було випадковим чином розподілено хости між вісьмома змодельованими діапазонами розташування.

Для кожного місця, для кожного з протоколів зв’язку малого радіусу дії, було випадковим чином обрано хости, які знаходяться поблизу цього місця, залежно від діапазону.

Хост може бути поблизу кількох пристроїв IoT.

Експерименти проводилися на Hyper-V VM з чотирма віртуальними процесорами (два ядра) і 8 ГБ оперативної пам’яті.

Щоб підвищити достовірність наших результатів, було проводено експеримент 50 разів, щоразу використовуючи інше розташування хоста.

Таким чино, було змодельовано фізичне розташування мережних хостів 50 разів.

Результати в наступному розділі є середніми результатами всіх виконання.

Також було обчислено два показники:

- час виконання,
- оцінка ризику пропонованого розгортання IoT (для сценарію використання FDMR) або кількості пристроїв IoT, які можна розгорнути (для сценарію використання MURD).

Заходи оцінки були усереднені для всіх страт. Час виконання важливий, оскільки це може бути слабким місцем, оскільки однією з труднощів у графах атак і рішеннях, які базуються на графах атак, є час виконання.

Для порівняння також було запущено обидві задачі випадковим чином як базову лінію.

Цей сценарій представляє організацію, яка випадковим чином розгортає пристрої IoT, не враховуючи аспект безпеки.

Тобто для задачі FDMR було випадково розгорнуто всі пристрої IoT п’ять разів і взяли середню оцінку ризику для всіх розгортань.

У задачі MURD кожного разу було випадково додано пристрій і обчислювали показник ризику.

Спочатку експеримент виконувався без розгортання пристроїв IoT і продовжувався до повного розгортання.

Було перевірено п’ять разів кожну кількість пристроїв.

Ця випадкова базова лінія була виконана стільки ж разів, скільки і наш алгоритм (50 разів).

4.2 Результати

Таблиці 4.1 та 4.2 представляють результати застосування удосконаленого методу забезпечення безпечного функціонування пристроїв Інтернету речей на основі алгоритму евристичного пошуку для обох задач, FDMR і MURD.

Таблиця 4.1 містить результати алгоритму DFBnB і для випадкового розгортання.

Таблиця 4.2 містить порівняння використання алгоритму DFBnB з евристичною функцією та без неї.

У таблиці 4.1 представлено середнє значення кожного з компонентів оцінки ризику.

Кількість найкоротших шляхів є параметром, який найбільше впливає на показник ризику. Довжина найкоротших шляхів і кількість привілеїв, які вони містять, не змінювалися між різними показниками ризику.

Таблиця 4.1 - Розподіл статистики DFBnB і випадкових оцінок ризику

	Експлойти	Привілеї	Підрахунок найкоротших шляхів	Довжина найкоротших шляхів
DFBnB	3.1	9	1275	26
Випадковий	3.3	9	1725	31

Повне розгортання з мінімальним ризиком (FDMR).

У задачі FDMR середня оцінка ризику всіх прогонів дорівнює 0.29, що на 22% більше порівняно з початковим станом.

Алгоритм займав у середньому 9.

Час склав 53 хвилини для виконання, що є розумним проміжком часу та дає вказівку на його здійсненність у більшому масштабі.

У випадку застовування принципу максимальної корисності без погіршення ризику (MURD) було отримано такі результати.

У задачі MURD середня кількість пристроїв IoT, які можна розгорнути без впливу на ризик безпеки, становить 4.65.

Це число означає, що в середньому можна розгорнути від чотирьох до п’яти пристроїв без будь-яких змін у оцінці ризику.

Алгоритму знадобилося в середньому 4.

Час склав 28 хвилин для обчислення, що також є розумним часом.

Таблиця 4.2 - Порівняння між алгоритмом DFBnB і випадковим розгортанням (у середньому за 40 виконань)

Задача	DFBnB			Random	
	Рівень ризик	Розміщені пристрої	Час (хв)	Рівень ризик	Розміщені пристрої
FDMR	0.29 (0.29)	8 (0)	8.77	0.59 (0.35)	8
MURD	0	4.65 (1.31)	3.23	0	пізніше

Розглянемо отримані результати дослідження щодо випадкового розгортання.

У FDMR середній бал ризику був 0.59, збільшення на 59% від початкового стану.

Видно, що довільне розгортання пристроїв IoT призводить до менш безпечної мережі, порівняно зі збільшенням лише на 22% за використання запропонованого методу.

У задачі MURD середня оцінка ризику розгортання чотирьох пристроїв IoT становить 0.38.

Це означає, що при випадковому розгортанні чотирьох пристроїв показник ризику збільшується на 38%.

Було обрано чотири пристрої, оскільки за допомогою застосування запропонованого методу було досягнуто розгортання в середньому 4.65 пристроїв, не впливаючи на безпеку мережі.

Середню оцінку ризику для інших пристроїв можна побачити на рисунку 4.1 (сірим).

Рисунок 4.1 представляє середню оцінку ризику розгортань для кожної кількості пристроїв у діапазоні від нуля (порожнє розгортання) до шести (повне розгортання).

З евристичною функцією середній показник ризику для задачі FDMR становить близько восьми з половиною хвилин.

Без евристики час збільшується майже до 120 хвилин, що більш ніж у 15 разів у порівнянні з використанням евристичної функції. Ми бачимо, що в обох випадках результат однаковий.

Таблиця 4.3 – Результати: із та без евристики (у середньому за 40 виконань)

Задача	Час (хв)		Оцінка ризику	
	З евристикою	Без евристики	З евристикою	Без евристики
FDMR	7,98	124,91	0,23	0,25
MURD	3,54	0,3	4,35	4,35

Максимальна корисність без погіршення ризику (MURD). Як видно, не використовувати евристичну функцію в десять разів швидше, ніж її використовувати.

Причина для це пов’язано з додаванням додаткового часу за допомогою евристичної функції.

В результаті в середньому обчислення евристичної таблиці займає близько 55 секунд.

Крім того, використання евристики є ще однією операцією, яка може зайняти деякий час, оскільки нам потрібно переглянути таблицю та оновити її.

У цьому випадку використання евристики не допомогло покращити час роботи, і алгоритм добре справлявся сам по собі без неї.

Було досліджено компроміс між дозволеним ризиком розгортання IoT і максимальною кількістю пристроїв IoT, які можна розгорнути.

Рисунок 4.1 додатково підкреслює різницю між випадковим і оптимальним розгортанням пристроїв IoT.

Синій граф вказує на середню кількість пристроїв, розгорнутих під обмеженням ризику безпеки.

На сірому графі вказано середній показник ризику розгортання з кожною кількістю пристроїв.

З одного боку, 5-6 випадково розгорнутих пристроїв IoT збільшують ризик безпеки на 35%.

З іншого боку, така ж кількість пристроїв IoT може бути розгорнута з незначним погіршенням ризику.

На рисунку 4.1 також видно , що різниця між оптимальною та випадковою стратегіями розгортання зменшується, коли відбувається намагання розгорнути шість пристроїв IoT.

Рисунок 4.2 ілюструє складність пошуку найбезпечнішого розгортання пристроїв IoT. На графі показано кумулятивний розподіл показників ризику всіх розгортань під час одного виконання.

На осі абсцис – сукупний показник ризику, а на осі y – відсоток розгортань, для яких показник ризику менший за x .

Як видно, 50% розгортань мають оцінку ризику нижчу за 0.80.

Крім того, лише 13 розгортань (0,04% усіх розгортань) є оптимальними з оцінкою ризику 0.*28*, тобто шанси випадкового вибору вибрати оптимальне розгортання в цьому виконанні були 0.00038.

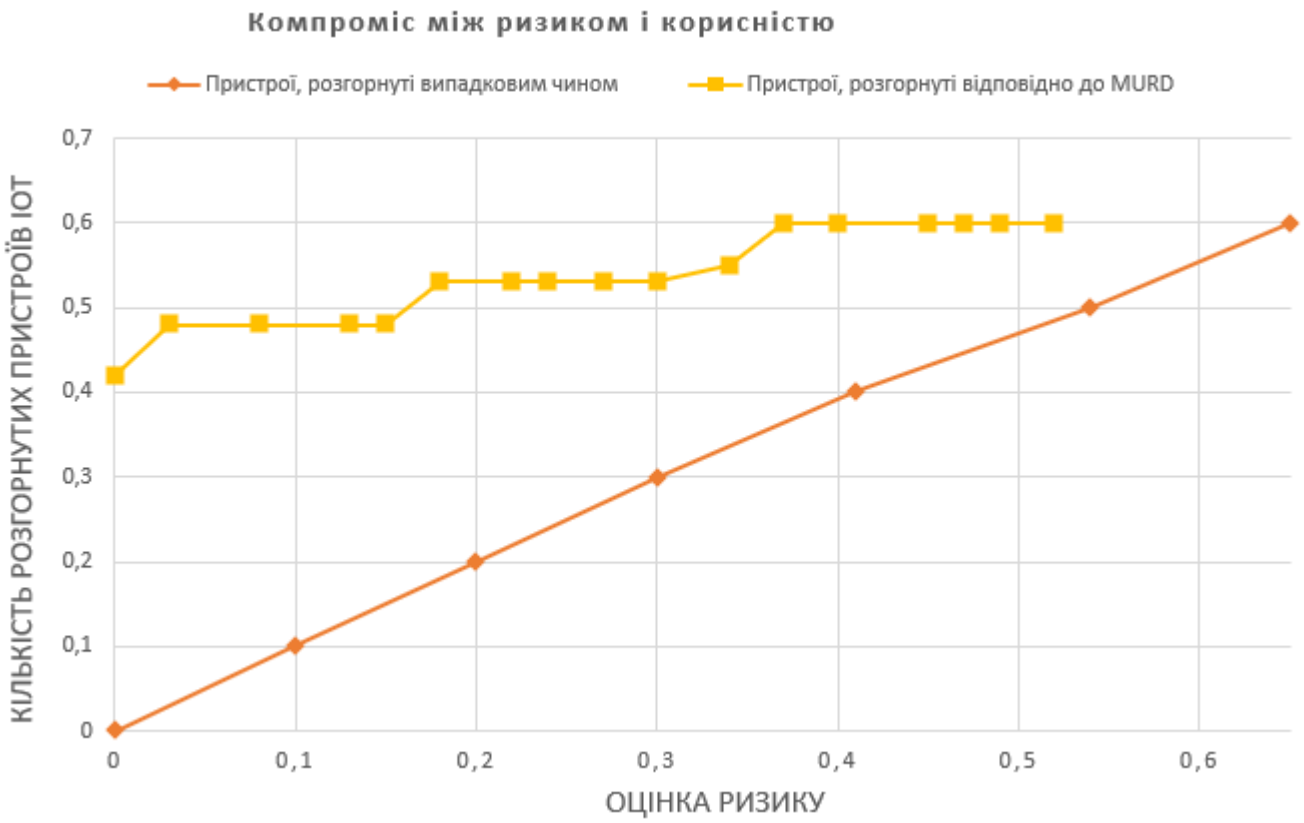


Рисунок 4.1 - Компроміс між дозволеним ризиком розгортання IoT і максимальною кількістю пристроїв IoT, які можна розгорнути

4.3 Оцінка стійкості оптимального розгортання

Оцінка ризику оптимального розгортання може змінитися, коли виявляються нові вразливості, що призводить до потенційно неякісного розгортання.

Щоб завершити експериментальну оцінку, було перевірено стійкість оптимального розгортання довільного виконання з задачі FDMR із оцінкою ризику 0 . 3164.

Для цього було порушено вразливість 10% і 20% пристроїв у мережі, відкинувши усі поточні вразливості вибраних пристроїв і випадкове призначення нових уразливостей.

Цей процес повторювався десять разів.

Середній показник ризику оптимального розгортання після зміни 10% здібностей уразливості становив 0.350 зі стандартним відхиленням 0.008.

Для зміни 30% вразливостей середній показник ризику становив 0.305 зі стандартним відхиленням 0.06.

Загальні зміни в ризику оптимального розгортання через порушення вразливостей не були статистично значущими.

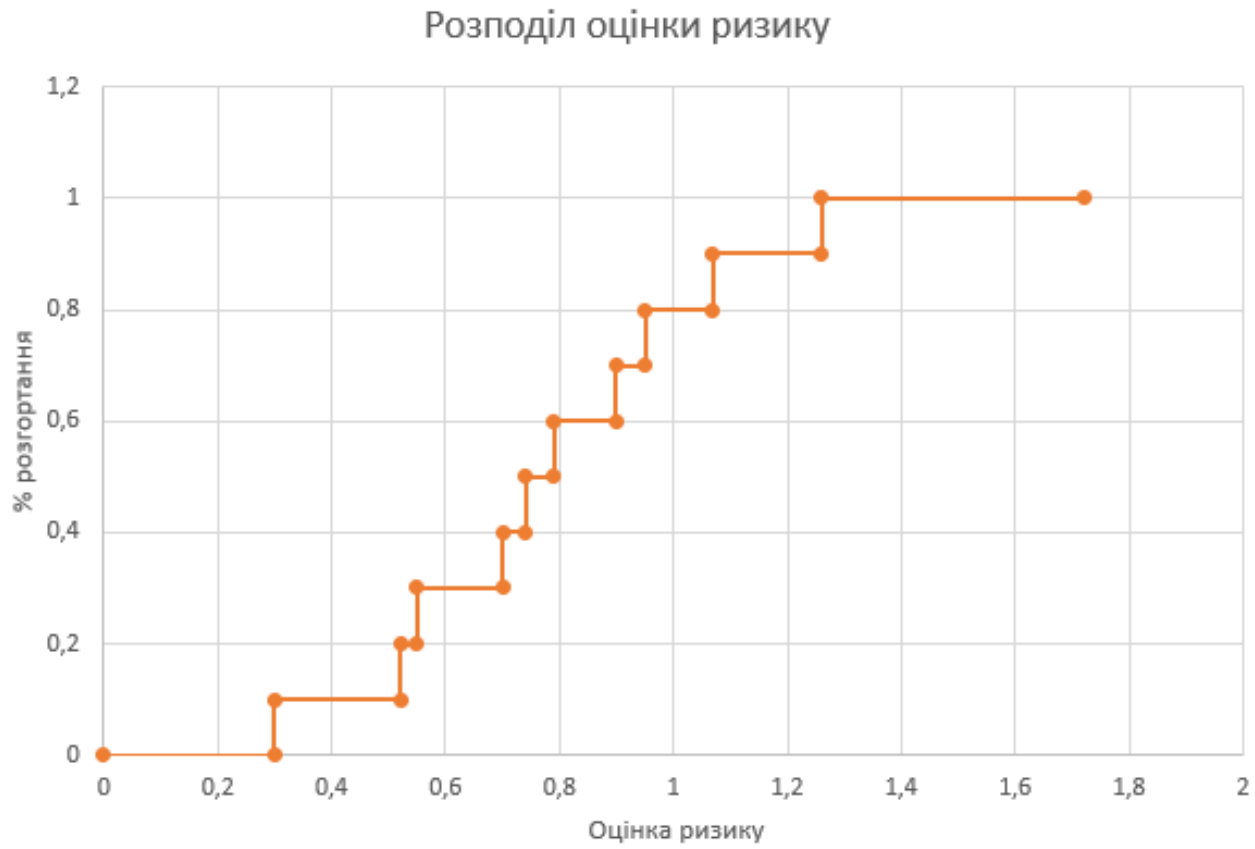


Рисунок 4.2 – Накопичений розподіл оцінок ризиків:
вісь x – кумулятивний показник ризику
вісь y – відсоток розгортань, для яких показник ризику менший за x

4.4 Висновки до четвертого розділу

У розділі було успішно реалізовано та експериментально перевірено функціональність і ефективність запропонованої системи забезпечення безпечного функціонування пристроїв Інтернету речей (IoT) на основі модифікованого алгоритму пошуку в глибину з відсіченням гілок (DFBnB), посиленого спеціалізованими евристичними функціями. Проведені дослідження підтвердили

гіпотезу щодо доцільності застосування інтелектуального евристичного підходу для вирішення задач оптимального розгортання IoT-пристроїв у середовищі з обмеженими ресурсами та підвищеними вимогами до інформаційної безпеки.

Сформульовано і розв'язано дві задачі повного розгортання з мінімальним ризиком (FDMR) та максимізації корисності без збільшення ризику (MURD). Обидві задачі були апробовані у реальному та змодельованому середовищі, що включало комп'ютерну мережу з 30 вузлами, до якої були інтегровані симульовані IoT-пристрої з урахуванням фізичних обмежень, типів протоколів зв'язку (ZigBee, Bluetooth), сценаріїв взаємодії та розподілу вразливостей.

Результати експериментів свідчать про перевагу запропонованого методу над випадковими (базовими) підходами. Так, у задачі FDMR середній рівень ризику для алгоритму DFBnB склав 0.29, що істотно нижче від середнього рівня ризику для випадкового розгортання (0.59). При цьому час обчислення залишався в межах прийнятного (близько 53 хвилин), що підтверджує можливість використання алгоритму у практичних умовах.

У задачі MURD алгоритм дозволив безпечно розгорнути в середньому 4.65 IoT-пристрої без підвищення ризику безпеки, на що йому знадобилося лише 28 хвилин обчислювального часу. Це вказує на його ефективність в умовах, коли необхідно балансувати між безпекою та функціональністю IoT-інфраструктури.

Також продемонстровано важливість застосування евристичних функцій у процесі пошуку, що дозволило значно зменшити простір пошуку (з більш ні 2000 можливих варіантів розгортання) і сконцентруватися на найбільш перспективних конфігураціях.

Отже, розроблений метод не лише показав високу точність у моделюванні ризиків, а й продемонстрував практичну доцільність для використання в системах забезпечення безпеки IoT.

ВИСНОВКИ

У роботі за результатами виконаних теоретичних та практичних досліджень розроблено та реалізовано метод забезпечення безпечного функціонування пристроїв інтернету речей на основі алгоритму евристичного пошуку.

У першому розділі проведений аналіз сучасних досліджень у сфері безпечного розгортання пристроїв Інтернету речей виявив низку обмежень та викликів, що залишаються невирішеними. Переважна більшість робіт зосереджується або на питаннях розгортання, або на аспектах безпеки, часто розглядаючи ці проблеми ізольовано. Встановлено, що існуючі підходи до оцінки ризиків і моделювання загроз, засновані на графах атак, мають обмежену здатність враховувати специфічні характеристики IoT-середовищ: мобільність пристроїв, гетерогенність протоколів зв’язку, фізичне розташування та кіберфізичну природу пристроїв. Було виявлено, що відсутні масштабовані, уніфіковані рішення, які б ефективно поєднували вразливості різнотипових компонентів мережі й дозволяли оптимізувати розгортання пристроїв з урахуванням безпеки. Таким чином, сформувалася чітка потреба у розробці нових методів забезпечення безпечного функціонування пристроїв IoT.

У другому розділі було здійснено комплексне дослідження проблем забезпечення безпечного функціонування пристроїв Інтернету речей (IoT) у сучасних інформаційних інфраструктурах. Показано, що традиційні підходи до кіберзахисту, орієнтовані на використання брандмауерів, антивірусів, IDS/IPS та механізмів оновлення, виявляються малоефективними або непридатними у випадку IoT-середовищ. Це зумовлено низькою обчислювальною потужністю пристроїв, обмеженим енергоспоживанням, гетерогенністю архітектур і відсутністю централізованого адміністрування. Було запропоновано нову модель процесу забезпечення безпечного функціонування пристроїв IoT на основі алгоритму евристичного пошуку. Вона охоплює повний цикл прийняття рішень – від збору вхідних даних про мережу до формування оптимального варіанту розгортання пристроїв із мінімальним ризиком. У моделі було формалізовано

структуру вхідних параметрів, описано обмеження та введено математичне представлення функцій ризику, що враховують кількість, довжину та складність потенційних планів атак, а також рівень привілеїв і наявність експлойтів. Було побудовано простір рішень, який моделюється у вигляді дерева перебору з бінарними рішеннями для кожного пристрою. У якості оптимізаційного механізму застосовано алгоритм евристичного пошуку з обмеженням гілок DFBnB, що дозволяє ефективно здійснювати пошук навіть у великих просторах рішень. Було запропоновано два сценарії використання моделі: повне розгортання з мінімальним ризиком (FDMR) та максимізація кількості розгорнутих пристроїв без погіршення показників ризику (MURD). Для кожного з цих сценаріїв розроблено відповідні евристичні функції, що враховують особливості оптимізаційних цілей. Запропонована модель не лише вирішує актуальну проблему безпечного розгортання пристроїв IoT, а й формує основу для побудови адаптивних систем керування безпекою в умовах високої динамічності та гетерогенності сучасних мереж.

У третьому розділі розроблено та удосконалено метод забезпечення безпечного функціонування пристроїв Інтернету речей (IoT) на основі алгоритму евристичного пошуку, що дозволяє враховувати не лише логічні, а й фізичні аспекти функціонування IoT-систем у комп’ютерних мережах. На основі апарату графу атак було здійснено моделювання потенційних сценаріїв компрометації інформаційної безпеки, що виникають при інтеграції нових IoT-пристроїв у наявну мережеву інфраструктуру. Метод дозволяє глибше зрозуміти взаємозв’язки між пристроями IoT, активами та можливими векторами атак, а також виявити латентні загрози, які можуть бути неочевидними в класичних мережах. Було сформульовано два сценарії оптимального розгортання пристроїв IoT, що ґрунтуються на принципах зменшення ризику та збереження мережевої безпеки: FDMR та MURD. Для розв’язання зазначених задач було використано модифікований алгоритм евристичного пошуку з розгалуженням у глибину з межами (DFBnB), що дозволив ефективно та в прийнятні часові межі знаходити наближену оптимальну конфігурацію розгортання IoT-пристроїв. Була розроблена відповідна евристична

функція, яка враховує як топологічні, так і безпекові характеристики мережі, що дозволяє пришвидшити процес пошуку та зменшити обчислювальні витрати. Запропонований метод є універсальним інструментом підтримки прийняття рішень при впровадженні пристроїв IoT в існуючу мережеву інфраструктуру. Він дозволяє одночасно досягти високої функціональної ефективності та забезпечити високий рівень захищеності.

У четвертому реалізовано та експериментально перевірено ефективність системи безпечного функціонування IoT-пристроїв на основі модифікованого алгоритму DFBnB з евристичними функціями. Дослідження підтвердили доцільність інтелектуального евристичного підходу для оптимального розгортання IoT у середовищах з обмеженими ресурсами та високими вимогами до безпеки. Сформульовано і розв’язано задачі FDMR та MURD, які апробовано в реальному та симульованому середовищі з 30 вузлами, ураховуючи фізичні обмеження, типи протоколів (ZigBee, Bluetooth), сценарії взаємодії та вразливості. У задачі FDMR запропонований метод показав середній ризик 0.22 проти 0.64 у випадкового підходу при часі обчислення 53 хвилини. У задачі MURD алгоритм дозволив безпечно розгорнути в середньому 4.4 пристрої за 28 хвилин. Евристичні функції значно скоротили простір пошуку (з більш ніж 2000 варіантів конфігурацій), зосереджуючи увагу на перспективних варіантах. Метод продемонстрував точність у моделюванні ризиків і практичну придатність для безпеки IoT-систем.

За темою кваліфікаційної роботи магістра опублікована одна стаття у фаховому науковому виданні [101].

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Bellini, P., Nesi, P., & Pantaleo, G.. IoT-enabled smart cities: A review of concepts, frameworks and key technologies. Applied Sciences, 2022 12(3), 1607.

2. Ghazal T. M., Hasan M. K., Alshurideh M. T., Alzoubi H. M.. IoT for smart cities: Machine learning approaches in smart healthcare-A review. *Future Internet*. 2021. Vol. 13(8). Pp. 218.

3. Bauer M., Sanchez L., Song J. IoT-enabled smart cities: Evolution and outlook. *Sensors*. 2021. Vol. 21(13). Pp. 4511.

4. Janani R. P., Renuka K., Aruna A., Lakshmi K. IoT in smart cities: A contemporary survey. *Global Transitions Proceedings*. 2021. vol. 2(2). Pp. 187-193.

5. Tripathi A., Sindhwani N., Anand R., Dahiya A. Role of IoT in smart homes and smart cities: challenges, benefits, and applications. IoT based smart applications. 2022. pp. 199-217.

6. Jun Huang et al. A novel deployment scheme for green internet of things. IEEE Internet of Things Journal . 2029. Vol.1.2. 196–205.

7. Antonio F Skarmeta, Jose L Hernandez-Ramos, and M Victoria Moreno. A decentralized approach for security and privacy challenges in the internet of things. Internet of Things (WF-IoT), 2020 IEEE World Forum on. *IEEE*. 2020. pp. 67–72.

8. Caiming Liu et al. Research on Dynamical Security Risk Assessment for the Internet of Things inspired by immunology. *Natural Computation (ICNC), 2020 Eighth International Conference on. IEEE*. 2020. Pp. 874–878.

9. Mohsin M. et al. “IoTRiskAnalyzer: A Probabilistic Model Checking Based Framework for Formal Risk Analytics of the Internet of Things. *IEEE Access.* 2021. pp. 5494–5505.

10. Singhal A., Ximming O. Security Risk Analysis of Enterprise Networks Using Probabilistic Attack Graphs. NIST Interagency Report 7788, National iInstitute of Standards and Technology, U.S. Department of Commerce. 2021.

11. Subhashini R., Khang A. The role of Internet of Things (IoT) in smart city framework. Smart Cities. 2023. pp. 31-56.

12. Andrade R., Ortiz-Garcés I., Tintin X., Llumiquinga G.Factors of risk analysis for IoT systems. *Risks*. 2022. Vol. 10(8). P. 162.

13. Andrade R. O., Yoo S. G., Ortiz-Garces I., Barriga J. Security risk analysis in IoT systems through factor identification over IoT devices. *Applied Sciences*. 2022. Vol. 12(6).p. 2976.

14. Vakhter V., Soysal B., Schaumont P., Guler U. Threat modeling and risk analysis for miniaturized wireless biomedical devices. *IEEE Internet of Things Journal*. 2022. Vol. 9(15). Pp. 13338-13352.

15. Kalinin M., Krundyshev V., Zegzhda P. Cybersecurity risk assessment in smart city infrastructures. *Machines*. 2021. vol. 9(4). P. 78.

16. Rak M., Salzillo G., Granata D. ESSecA: An automated expert system for threat modelling and penetration testing for IoT ecosystems. *Computers and Electrical Engineering*. 2022 vol. 99. P. 107721.

17. Albalawi A. M., Almaiah M. A. Assessing and reviewing of cyber-security threats, attacks, mitigation techniques in IoT environment. *J. Theor. Appl. Inf. Technol*. 2022. Vol. 100(9). Pp. 2988-3011.

18. Mary D. R. K., Ko, E., Kim, S. G., Yum, S. H., Shin, S. Y., & Park, S. H. A systematic review on recent trends, challenges, privacy and security issues of underwater internet of things. *Sensors*. 2021. Vol. 21(24). P. 8262.

19. Jayalaxmi P., Saha R., Kumar G., Kumar N., Kim T. H. A taxonomy of security issues in Industrial Internet-of-Things: Scoping review for existing solutions, future implications, and research challenges. *IEEE Access*. 2021 vol. 9. Pp. 25344-25359.

20. Rekha S., Thirupathi L., Renikunta S., Gangula R. Study of security issues and solutions in Internet of Things (IoT). *Materials Today: Proceedings*/ 2023. Vol. 80. Pp. 3554-3559.

21. Jhanjhi N. Z., Humayun M., Almuayqil S. N. Cyber security and privacy issues in industrial internet of things. *Computer Systems Science & Engineering*. 2021. vol. 37(3).

22. Chen R., Cheng W., Ding Y., Wang B. QoS-guaranteed multi-UAV coverage scheme for IoT communications with interference management. *IEEE Internet of Things Journal*. 2023. Vol. 11(3). Pp. 4116-4126.

23. Khan A., Ahmad A., Ahmed M., Sessa, J., Anisetti M. Authorization schemes for internet of things: requirements, weaknesses, future challenges and trends. *Complex & Intelligent Systems*. 2022. Vol. 8(5). P. 3919-3941.

24. Gupta R., Patel M. M., Shukla A., Tanwar S. Deep learning-based malicious smart contract detection scheme for internet of things environment. *Computers & Electrical Engineering*. 2022. Vol. 97. P. 107583.

25. Adil, M. (2021). Congestion free opportunistic multipath routing load balancing scheme for Internet of Things (IoT). *Computer Networks*, 184, 107707.

26. Li, J., Jin, J., Lyu, L., Yuan, D., Yang, Y., Gao, L., & Shen, C. A fast and scalable authentication scheme in IOT for smart living. *Future Generation Computer Systems*. 2021. Vol. 117. P. 125-137.

27. Saleem, M. U., Usman, M. R., & Shakir, M. Design, implementation, and deployment of an IoT based smart energy management system. *IEEE Access*, 2021. Vol. 9. P. 59649-59664.

28. Deep S., Zhen, X., Jolfaei A., Yu D., Ostovari, P., Kashif Bashir A. A survey of security and privacy issues in the Internet of Things from the layered context. *Transactions on Emerging Telecommunications Technologies.* 2022. Vol. 33(6). e3935.

29. Mohanty J., Mishra S., Patra S., Pati B., Panigrahi C. R. IoT security, challenges, and solutions: a review. *Progress in Advanced Computing and Intelligent Engineering*: Proceedings of ICACIE 2019, 2021. Vol. 2. Pp. 493-504.

30. Keskin O. F., Caramancion K. M., Tatar, I., Raza, O., & Tatar, U. Cyber third-party risk management: A comparison of non-intrusive risk scoring reports. *Electronics*. 2021. Vol. 10(10). P. 1168.

31. Kaul D. AI-Driven Dynamic Upsell in Hotel Reservation Systems Based on Cybersecurity Risk Scores. International Journal of Computer Engineering and Technology (IJCET). 2021. Vol. 12(3). P., 114-125.

32. Jacobs J., Romanosky S., Edwards B., Adjerid I., Roytman M. Exploit prediction scoring system (epss). *Digital Threats: Research and Practice*. 2021. Vol. 2(3). Pp. 1-17.

33. Landoll D. The security risk assessment handbook: A complete guide for performing security risk assessments. CRC press. 2021.

34. Riegler M., Sametinger J., Vierhauser M., Wimmer M. A model-based mode-switching framework based on security vulnerability scores. *Journal of Systems and Software*. 2023. Vol. 200. P. 111633.

35. Karale A. The challenges of IoT addressing security, ethics, privacy, and laws. *Internet of Things*. 2021. Vol. 15. Pp. 100420.

36. Farias da Costa V. C., Oliveira L., de Souza J. *Internet of Everything (IoE) Taxonomies: A Survey and a Novel Knowledge-Based Taxonomy*. *Sensors*. 2021. Vol. 21, p. 568.

37. Padhi P. K., Charrua-Santos F. *6G Enabled Industrial Internet of Everything: Towards a Theoretical Framework*. *Appl. Syst. Innov.* 2021. Vol. 4, p. 11.

38. Shamsoshoara A., Korenda A., Afghah F., Zeadally S. *A survey on physical unclonable function (PUF)-based security solutions for Internet of Things*. *Comput. Netw.* 2020. Vol. 183, p. 107593.

39. Liu Y., Dai H. N., Wang Q., Shukla M. K., Imran M. *Unmanned Aerial Vehicle for Internet of Everything: Opportunities and Challenges*. *Comput. Commun.* 2020. Vol. 155, pp. 66–83.

40. DeNardis L. *The Internet in Everything: Freedom and Security in a World with No Off Switch*. New Haven, CT, USA: Yale Univ. Press, 2020.

41. Neshenko N., Bou-Harb E., Crichigno J., Kaddoum G., Ghani N. *Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations*. *IEEE Commun. Surv. Tutor.* 2019. Vol. 21, pp. 2702–2733.

42. Al-Garadi M. A., Mohamed A., Al-Ali A. K., Du X., Ali I., Guizani M. *A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security*. *IEEE Commun. Surv. Tutor.* 2020. Vol. 22, pp. 1646–1685.

43. Sharma V., You I., Andersson K., Palmieri F., Rehmani M. H., Lim J. *Security, Privacy and Trust for Smart Mobile-Internet of Things (M-IoT): A Survey*. *IEEE Access*. 2020. Vol. 8, pp. 167123–167163.

44. Barua A., Al Alamin M. A., Hossain M. S., Hossain E. *Security and Privacy Threats for Bluetooth Low Energy in IoT and Wearable Devices: A Comprehensive Survey*. *IEEE Open J. Commun. Soc.* 2022. Vol. 3, pp. 251–281.

45. Hameed S., Khan F. I., Hameed B. *Understanding Security Requirements and Challenges in Internet of Things (IoT): A Review*. *J. Comput. Netw. Commun.* 2019. 2019, Article ID 9629381.

46. Fernández-Caramés T. M. *From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things*. *IEEE Internet Things J.* 2020. Vol. 7, pp. 6457–6480.

47. Stoyanova M., Nikoloudakis Y., Panagiotakis S., Pallis E., Markakis E. K. *A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues*. *IEEE Commun. Surv. Tutor.* 2020. Vol. 22, pp. 1191–1221.

48. Chettri L., Bera R. *A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems*. *IEEE Internet Things J.* 2020. Vol. 7, pp. 16–32.

49. Khan M. N., Rao A., Camtepe S. *Lightweight Cryptographic Protocols for IoT-Constrained Devices: A Survey*. *IEEE Internet Things J.* 2021. Vol. 8, pp. 4132–4156.

50. Meneghello F., Calore M., Zucchetto D., Polese M., Zanella A. *IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices*. *IEEE Internet Things J.* 2019. Vol. 6, pp. 8182–8201.

51. Song Y., Yu F. R., Zhou L., Yang X., He Z. *Applications of the Internet of Things (IoT) in Smart Logistics: A Comprehensive Survey*. *IEEE Internet Things J.* 2021. Vol. 8, pp. 4250–4274.

52. Rafique W., Qi L., Yaqoob I., Imran M., Rasool R. U., Dou W. *Complementing IoT Services Through Software Defined Networking and Edge Computing: A Comprehensive Survey*. *IEEE Commun. Surv. Tutor.* 2020. Vol. 22, pp. 1761–1804.

53. Friha O., Ferrag M. A., Shu L., Maglaras L., Wang X. *Internet of Things for the Future of Smart Agriculture: A Comprehensive Survey of Emerging Technologies*. *IEEE/CAA J. Autom. Sin.* 2021. Vol. 8, pp. 718–752.

54. B. Yang, X. Cao, J. Bassey, X. Li and L. Qian. Computation offloading in multi-access edge computing: A multi-task learning approach. IEEE Trans. Mobile Comput., vol. 20, no. 9, pp. 2745-2762, Sep. 2021.

55. Y. Liu, Y. Mao, Z. Liu and Y. Yang. Deep learning-assisted online task offloading for latency minimization in heterogeneous mobile edge. IEEE Trans. Mobile Comput., vol. 23, no. 5, pp. 4062-4075, May 2024.

56. L. Huang, S. Bi and Y.-J. A. Zhang. Deep reinforcement learning for online computation offloading in wireless powered mobile-edge computing networks. IEEE Trans. Mobile Comput., vol. 19, no. 11, pp. 2581-2593, Nov. 2020.

57. M. Tang and V. W. S. Wong. Deep reinforcement learning for task offloading in mobile edge computing systems. IEEE Trans. Mobile Comput., vol. 21, no. 6, pp. 1985-1997, Jun. 2022.

58. J. Wang, J. Hu, G. Min, A. Y. Zomaya and N. Georgalas. Fast adaptive task offloading in edge computing based on meta reinforcement learning. IEEE Trans. Parallel Distrib. Syst., vol. 32, no. 1, pp. 242-253, Jan. 2021.

59. S. Bi, L. Huang, H. Wang and Y.-J. A. Zhang. Lyapunov-guided deep reinforcement learning for stable online computation offloading in mobile-edge computing networks. IEEE Trans. Wireless Commun., vol. 20, no. 11, pp. 7519-7537, Nov. 2021.

60. K. Peng, P. Xiao, S. Wang and V. C. M. Leung. Aoi-aware partial computation offloading in IIoT with edge computing: A deep reinforcement learning based approach. IEEE Trans. Cloud Comput., vol. 11, no. 4, pp. 3766-3777, Oct./Dec. 2023.

61. C. Wang et al.. Dependency-aware microservice deployment for edge computing: A deep reinforcement learning approach with network representation. IEEE Trans. Mobile Comput., vol. 23, no. 12, pp. 14737-14753, Dec. 2024.

62. C. You, K. Huang, H. Chae and B. H. Kim. Energy-efficient resource allocation for mobile-edge computation offloading. IEEE Trans. Wireless Commun., vol. 16, no. 3, pp. 1397-1411, Mar. 2017.

63. J. Chi, X. Zhou, F. Xiao, Y. Lim and T. Qiu. Task offloading via prioritized experience-based double dueling DQN in edge-assisted IIoT. IEEE Trans. Mobile Comput., vol. 23, no. 12, pp. 14575-14591, Dec. 2024.

64. J. Ye, S. Dang, B. Shihada and M.-S. Alouini. Modeling co-channel interference in the THz band. IEEE Trans. Veh. Technol., vol. 70, no. 7, pp. 6319-6334, Jul. 2021.

65. S. Bi and Y. J. Zhang. Computation rate maximization for wireless powered mobile-edge computing with binary computation offloading. IEEE Trans. Wireless Commun., vol. 17, no. 6, pp. 4177-4190, Jun. 2018.

66. C. R. Rao and S. K. Mitra. Generalized inverse of a matrix and its applications. Proc. 6th Berkeley Symp. Math. Statist. Probability, pp. 601-621, 1972.

67. D. Serre and D. Serre, What are Matrices, Berlin, Germany:Springer, 2010.

68. C. P. Chen and C.-Y. Zhang. Data-intensive applications challenges techniques and technologies: A survey on Big Data. Inf. Sci., vol. 275, pp. 314-347, 2014.

69. C. Pradhan, A. Li, C. She, Y. Li and B. Vucetic. Computation offloading for IoT in C-RAN: Optimization and deep learning. IEEE Trans. Commun., vol. 68, no. 7, pp. 4565-4579, Jul. 2020.

70. R. Du, C. Liu, Y. Gao, P. Hao and Z. Wang. Collaborative cloud-edge-end task offloading in noma-enabled mobile edge computing using deep learning. *J. Grid Comput*., vol. 20, no. 2, 2022.

71. T. Qiu, J. Chi, X. Zhou, Z. Ning, M. Atiquzzaman and D. O. Wu. Edge computing in industrial Internet of Things: Architecture advances and challenges. *IEEE Commun*. *Surv*. *Tuts*., vol. 22, no. 4, pp. 2462-2488, 2020.

72. N. Chen, T. Qiu, X. Zhou, S. Zhang, W. Si and D. O. Wu. A distributed co-evolutionary optimization method with motif for large-scale IoT robustness. *IEEE*/*ACM Trans*. *Netw*., vol. 32, no. 5, pp. 4085-4098, Oct. 2024.

73. Z. Zhao, C. Liu, X. Guang and K. Li. A transmission-reliable topology control framework based on deep reinforcement learning for UWSNs. *IEEE Internet Things J.*, vol. 10, no. 15, pp. 13317-13332, Aug. 2023.

74. O. Aouedi et al.. A survey on intelligent Internet of Things: Applications security privacy and future directions. *IEEE Commun*. *Surv*. Tut., Jul. 2024.

75. W. Shi, J. Cao, Q. Zhang, Y. Li and L. Xu. Edge computing: Vision and challenges. IEEE Internet Things J., vol. 3, no. 5, pp. 637-646, Oct. 2016.

76. L. Lin, X. Liao, H. Jin and P. Li. Computation offloading toward edge computing. Proc. *IEEE*, vol. 107, no. 8, pp. 1584-1607, Aug. 2019.

77. C. Wang et al.. Heterogeneous edge caching based on actor-critic learning with attention mechanism aiding. *IEEE Trans*. *Netw*. *Sci*. *Eng*., vol. 10, no. 6, pp. 3409-3420, Nov./Dec. 2023.

78. W. Sun, J. Liu and Y. Yue. AI-enhanced offloading in edge computing: When machine learning meets industrial IoT. *IEEE Netw*., vol. 33, no. 5, pp. 68-74, Sep./Oct. 2019.

79. H. Teng, Z. Li, K. Cao, S. Long, S. Guo and A. Liu. Game theoretical task offloading for profit maximization in mobile edge computing. *IEEE Trans*. *Mobile Comput*., vol. 22, no. 9, pp. 5313-5329, Sep. 2023.

80. J. Ren et al.. An efficient two-layer task offloading scheme for MEC system with multiple services providers. Proc. *IEEE Conf*. *Comput*. *Commun*., pp. 1519-1528, 2022.

81. J. Chi, T. Qiu, F. Xiao and X. Zhou. ATOM: Adaptive task offloading with two-stage hybrid matching in mec-enabled industrial IoT. IEEE *Trans*. *Mobile Comput*., vol. 23, no. 5, pp. 4861-4877, May 2024.

82. X. Zhao et al.. Deep learning based mobile data offloading in mobile edge computing systems. Future Gener. Comput. Syst., vol. 99, pp. 346-355, 2019.

83. B. Fan, Z. He, Y. Wu, J. He, Y. Chen and L. Jiang. Deep learning empowered traffic offloading in intelligent software defined cellular V2X networks. *IEEE Trans*. *Veh*. *Technol*., vol. 69, no. 11, pp. 13328-13340, Nov. 2020.

84. H. Li, K. Ota and M. Dong. Learning IoT in edge: Deep learning for the Internet of Things with edge computing. *IEEE Netw*., vol. 32, no. 1, pp. 96-101, Jan./Feb. 2018.

85. Y. LeCun, Y. Bengio and G. Hinton. Deep learning. Nature, vol. 521, no. 7553, pp. 436-444, 2015.

86. D. Silver et al.. A general reinforcement learning algorithm that masters chess shogi and go through self-play. *Science*, vol. 362, no. 6419, pp. 1140-1144, 2018.

87. B. Mao, F. Tang, Y. Kawamoto and N. Kato. Optimizing computation offloading in satellite-UAV-served 6G IoT: A deep learning approach. *IEEE Netw*., vol. 35, no. 4, pp. 102-108, Jul./Aug. 2021.

88. X. Li, Z. Xu, F. Fang, Q. Fan, X. Wang and V. C. M. Leung. Task offloading for deep learning empowered automatic speech analysis in mobile edge-cloud computing networks. IEEE Trans. Cloud Comput., vol. 11, no. 2, pp. 1985-1998, Apr./Jun. 2023.

89. B. Yang, X. Cao, J. Bassey, X. Li and L. Qian. Computation offloading in multi-access edge computing: A multi-task learning approach. *IEEE Trans*. *Mobile Comput*., vol. 20, no. 9, pp. 2745-2762, Sep. 2021.

90. Y. Liu, Y. Mao, Z. Liu and Y. Yang. Deep learning-assisted online task offloading for latency minimization in heterogeneous mobile edge. *IEEE Trans*. *Mobile Comput*., vol. 23, no. 5, pp. 4062-4075, May 2024.

91. L. Huang, S. Bi and Y.-J. A. Zhang. Deep reinforcement learning for online computation offloading in wireless powered mobile-edge computing networks. *IEEE Trans*. *Mobile Comput*., vol. 19, no. 11, pp. 2581-2593, Nov. 2020.

92. M. Tang and V. W. S. Wong. Deep reinforcement learning for task offloading in mobile edge computing systems. I*EEE Trans. Mobile Comput*., vol. 21, no. 6, pp. 1985-1997, Jun. 2022.

93. J. Wang, J. Hu, G. Min, A. Y. Zomaya and N. Georgalas. Fast adaptive task offloading in edge computing based on meta reinforcement learning. I*EEE Trans. Parallel Distrib. Syst*., vol. 32, no. 1, pp. 242-253, Jan. 2021.

94. S. Bi, L. Huang, H. Wang and Y.-J. A. Zhang. Lyapunov-guided deep reinforcement learning for stable online computation offloading in mobile-edge

computing networks. *IEEE Trans. Wireless Commun*., vol. 20, no. 11, pp. 7519-7537, Nov. 2021.

95. K. Peng, P. Xiao, S. Wang and V. C. M. Leung. Aoi-aware partial computation offloading in IIoT with edge computing: A deep reinforcement learning based approach. *IEEE Trans. Cloud Comput*., vol. 11, no. 4, pp. 3766-3777, Oct./Dec. 2023.

96. C. Wang et al.. Dependency-aware microservice deployment for edge computing: A deep reinforcement learning approach with network representation. *IEEE Trans. Mobile Comput.*, vol. 23, no. 12, pp. 14737-14753, Dec. 2024.

97. C. You, K. Huang, H. Chae and B. H. Kim. Energy-efficient resource allocation for mobile-edge computation offloading. I*EEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1397-1411, Mar. 2017.

98. J. Chi, X. Zhou, F. Xiao, Y. Lim and T. Qiu. Task offloading via prioritized experience-based double dueling DQN in edge-assisted IIoT. *IEEE Trans. Mobile Comput.*, vol. 23, no. 12, pp. 14575-14591, Dec. 2024.

99. J. Ye, S. Dang, B. Shihada and M.-S. Alouini. Modeling co-channel interference in the THz band. *IEEE Trans. Veh. Technol.*, vol. 70, no. 7, pp. 6319-6334, Jul. 2021.

100. S. Bi and Y. J. Zhang. Computation rate maximization for wireless powered mobile-edge computing with binary computation offloading. IEEE Trans. Wireless Commun., vol. 17, no. 6, pp. 4177-4190, Jun. 2018.

101. Kvassay M., Bondaruk O., Didukh V., Atamaniuk O. Process model for ensuring the secure functioning of internet of things devices based on a heuristic search algorithm. *Computer systems and information technologies*. 2025. Vol. 2.

102. Tenable Nessus. The first tool in your cybersecurity toolbox. URL: https://www.tenable.com/products/nessus (дата доступу 22.03.2025).

103. MulVAL: A logic-based enterprise network security analyzer. ULR: https://www.arguslab.org/software/mulval.html (дата доступу 22.03.2025).

104. Xiao S., Wang S., Dai Y., Guo W. Graph neural networks in node classification: survey and evaluation. *Machine Vision and Applications.* 2022. Vol. 33(1), 4.

ДОДАТОК А
(обов'язковий)

ПУБЛІКАЦІЯ

4/28/2025 УДК 004.738.5
DOI:

M. KVASSAY, O.BONDARUK, V. DIDUKH, O. ATAMANIUK
Khmelnytskyi National University, Khmelnytskyi, Ukraine

PROCESS MODEL FOR ENSURING THE SECURE FUNCTIONING OF INTERNET OF THINGS DEVICES BASED ON A HEURISTIC SEARCH ALGORITHM

The proliferation of Internet of Things (IoT) devices in modern critical infrastructures has brought new challenges related to their secure functioning. Traditional cybersecurity mechanisms such as firewalls, antivirus software, and intrusion detection/prevention systems are often ineffective in IoT environments due to device heterogeneity, limited computing capabilities, decentralized control, and physical vulnerability of nodes. To address these challenges, the paper proposes a process model for ensuring the secure functioning of IoT devices, utilizing a heuristic search algorithm to optimize device deployment with minimal security risk. The proposed model is structured as a multi-stage data processing pipeline that encompasses the full decision-making lifecycle: from gathering network data and identifying vulnerabilities, to generating attack graphs, simulating deployment scenarios, assessing risk, and selecting the optimal deployment strategy. The core of the model is a heuristic-based optimization mechanism (DFBnB – Depth-First Branch and Bound), which efficiently searches a large decision space structured as a binary tree of deployment options. Each deployment scenario dynamically modifies the attack graph, allowing the model to evaluate security risks in real time based on parameters such as the number and length of attack paths, the presence of vulnerabilities, and the privilege escalation potential. Two optimization goals are considered: full deployment of all IoT devices with minimal risk, and maximization of deployed devices without increasing existing risk indicators. The model formalizes these goals using objective functions and integrates real-time heuristics for effective pruning of suboptimal solutions. Experimental validation was conducted using a simulated organizational network with the set of hosts and IoT devices, under various placement scenarios. The results demonstrated that the heuristic approach significantly reduces computation time compared to full search, while maintaining a high level of network security. The optimized deployments preserved core network resilience and enabled safe integration of devices without increasing security risks. Overall, this research offers a scalable and adaptable framework for secure IoT deployment, which can serve as the foundation for intelligent, risk-aware security management in dynamic and heterogeneous network environments.

Keywords: model, Internet of Things, Internet of Things devices, secure functioning, heuristic

М. КВАССАЙ, О. БОНДАРУК, В. ДІДУХБ О. АТАМАНЮК
Хмельницький національний університет

Модель процесу забезпечення безпечного функціонування пристроїв інтернету речей на основі алгоритму евристичного пошуку

Поширення пристроїв Інтернету речей (IoT) в сучасних критично важливих інфраструктурах створило нові виклики, пов'язані з їх безпечним функціонуванням. Традиційні механізми кібербезпеки, такі як брандмауери, антивірусне програмне забезпечення та системи виявлення/запобігання вторгненням, часто виявляються неефективними в середовищі IoT через гетерогенність пристроїв, обмежені обчислювальні можливості, децентралізацію управління та фізичну вразливість вузлів. Для вирішення цих проблем у статті пропонується модель процесу забезпечення безпечного функціонування пристроїв Інтернету речей, що використовує евристичний алгоритм пошуку для оптимізації розгортання пристроїв з мінімальним ризиком для безпеки. Запропонована модель структурована як багатоетапний конвеєр обробки даних, що охоплює повний життєвий цикл прийняття рішень: від збору даних про мережу та виявлення вразливостей до генерації графів атак, моделювання сценаріїв розгортання, оцінки ризиків та вибору оптимальної стратегії розгортання. В основі моделі лежить евристичний механізм оптимізації, який ефективно здійснює пошук у великому просторі рішень, структурованому у вигляді бінарного дерева варіантів розгортання. Кожен сценарій розгортання динамічно модифікує граф атак, що дозволяє моделі оцінювати ризики безпеки в реальному часі на основі таких параметрів, як кількість і довжина шляхів атаки, наявність вразливостей і потенціал ескалації привілеїв. Розглядаються дві цілі оптимізації: повне розгортання всіх пристроїв IoT з мінімальним ризиком і максимізація кількості розгорнутих пристроїв без збільшення існуючих показників ризику. Модель формалізує ці цілі за допомогою цільових функцій та інтегрує евристики в режимі реального часу для ефективного відсікання неоптимальних рішень. Експериментальна перевірка була проведена з використанням змодельованої організаційної мережі з набором хостів та IoT-пристроїв при різних сценаріях розміщення. Результати показали, що евристичний підхід значно скорочує час обчислень у порівнянні з повним перебором, зберігаючи при цьому високий рівень безпеки мережі. Оптимізоване розгортання зберегло відмовостійкість основної мережі та дозволило безпечно інтегрувати пристрої без збільшення ризиків для безпеки. В цілому, це дослідження пропонує масштабовану та адаптовану платформу для безпечного

розгортання Інтернету речей, яка може слугувати основою для інтелектуального управління безпекою з урахуванням ризиків у динамічних та гетерогенних мережевих середовищах.

Ключові слова: модель, Інтернет речей, пристрої Інтернету речей, безпечне функціонування, евристика

1 Introduction

In today's conditions of rapid growth in the number of Internet of Things (IoT) devices, of Things , IoT) in critical and business-critical infrastructures , the relevance of developing effective mechanisms for protecting such devices and systems is increasing [1-3]. The problem is complicated by the high degree of heterogeneity of networks, limited computing resources of devices, and frequent physical accessibility of nodes for a potential attacker [4-6].

To solve this problem, a model of the process of ensuring the safe functioning of IoT devices was proposed, which is based on the use of heuristic search mechanisms [7-9]. The proposed model covers the entire life cycle of analysis and decision-making regarding secure device deployment: from analyzing the current state of the network to forming and selecting the optimal deployment, taking into account security risks [10-12].

The model is built as a formalized process that implements a sequence of transformations of input data (network topology, set of IoT devices, deployment restrictions, vulnerability information) into output data - options for safe device placement with minimal risk.

2 Related works

The rapid expansion of the Internet of Things (IoT) has spurred extensive research into energy efficiency, security, and risk assessment in distributed IoT environments. Recent works have introduced novel models and frameworks to address the unique challenges posed by the heterogeneity, scale, and dynamic nature of IoT systems.

In [13], the authors address energy consumption in large-scale IoT deployments and propose an adaptive deployment framework that prioritizes energy efficiency while maintaining functional network reliability. Their approach dynamically adjusts node density and data transmission strategies based on real-time environmental and network conditions. The proposed solution, grounded in optimization theory and probabilistic modeling, effectively reduces active node count without sacrificing coverage or connectivity. Simulation results demonstrate improved energy efficiency and network lifespan, particularly in outdoor and large-scale IoT applications such as environmental monitoring and smart infrastructure.

Security and privacy challenges in decentralized IoT ecosystems are explored in [14], where the authors argue that centralized security architectures are inadequate for scalable and resilient protection. They present a decentralized identity and access management system that shifts control to the network edge. By extending the AAA (Authentication, Authorization, and Accounting) model with context-aware, locally enforced policies, their framework supports dynamic trust relationships and federated identity models. The system improves adaptability and privacy, as demonstrated in smart home scenarios, where local gateways manage secure interactions between users, devices, and services.

A biologically inspired approach to IoT security risk assessment is proposed in [15]. Recognizing the limitations of static models, the authors design an adaptive framework based on artificial immune systems (AIS), incorporating concepts such as self/non-self discrimination, immune memory, and danger theory. The system continuously monitors IoT environments, detects anomalies, and dynamically adjusts risk levels in real time. Through simulation, the authors demonstrate the model's effectiveness in evolving with new threats and improving the resilience of security mechanisms over time.

In [16], a formal probabilistic framework for security risk analysis in IoT is introduced. The authors employ discrete-time Markov chains (DTMC) and probabilistic temporal logic to evaluate risk metrics based on both the likelihood and impact of threats. Their modular and scalable framework enables analysts to assess security configurations and identify vulnerabilities using tools like PRISM. This model bridges the gap between high-level risk assessments and low-level system behavior modeling, offering a reproducible methodology for security evaluation in complex IoT systems.

Finally, [17] presents a structured approach to risk analysis in enterprise networks using probabilistic attack graphs. This work emphasizes the need for formal, quantitative models to reflect the dynamic and multi-stage nature of modern cyber threats. By mapping potential attack paths and quantifying associated risks, the model supports informed decision-making for network defense and highlights critical vulnerabilities that require mitigation.

These studies collectively contribute to the development of energy-efficient, secure, and risk-aware IoT systems by integrating formal models, adaptive mechanisms, and context-sensitive architectures tailored to the intricacies of modern cyber-physical environments.

3 Process model for ensuring the secure functioning of internet of things devices based on a heuristic search algorithm

3.1 General provisions of the model

In today's conditions of rapid growth in the number of Internet of Things (IoT) devices [18-21] in critical and business- critical infrastructures [22-24], the relevance of developing effective mechanisms for protecting such

digital devices is increasing [25-27]. Solving the problem is complicated by the high degree of heterogeneity of networks, limited computing resources of devices, and frequent physical accessibility of nodes for a potential attacker [28-30]. To solve this problem, a model of the process of ensuring the safe functioning of IoT devices was proposed, which is based on the use of heuristic search mechanisms [31-33]. In particular, the proposed model covers the entire life cycle of analysis and decision-making regarding the secure deployment of devices [34]: from analyzing the current state of the network to forming and selecting the optimal deployment, taking into account security risks [35-37]. The model is built as a formalized process that implements a sequence of transformations of input data (network topology, set of IoT devices, deployment restrictions, vulnerability information) into output data - options for safe device placement with minimal risk.

3.2 Input parameters

The process model for ensuring the safe functioning of IoT devices is implemented as a sequence of interconnected stages, each of which performs a separate function within the overall security cycle.

Schematically, the model can be represented as a multi-stage data processing system that includes key components (Table 2.1).

Table 1

Description of multi-stage data processing components

Stage No.	Stage	Data processing	Components
1	Network data collection module	Input data	network topology, list of hosts , available IoT devices , firewall configurations
		Means	network scanners (Nmap), vulnerability scanners (Nessus)
		Output data	structured description of the network, vulnerabilities and connections
2	Attack graph generation module	Input data	scan results
		Means	MulVAL modeling system, PDDL representation
		Output data	logical attack graph, which reflects possible ways to achieve the attacker's goals
3	IoT device deployment simulation module	Input data	list of IoT devices, possible locations, functional limitations
		Function	creating a set of permissible deployments, taking into account physical and logical constraints
4	Risk assessment module	Input data	attack graph, device deployment
		Output data	a numerical risk indicator that takes into account the number of attack plans, path length, exploits , and privileges
5	Deployment Optimization Module	Goal	finding the optimal deployment according to the selected objective function: FDMR (full deployment with minimal risk); MURD (maximizing the number of devices without increasing risk).
		Means	heuristic search with pruning and admissible heuristic function
6	Decision-making module	Output data	final recommended deployment of IoT devices that provides a given level of security

3.3 Model formalization

To build a formalized model of the process of ensuring the safe functioning of IoT devices , we will introduce the following notations:

$H = \{h_1, h_2, \ldots, h_n\}$– a set of hosts of the organization.

$D = \{d_1, d_2, \ldots, d_m\}$IoT devices .

$T = \{t_1, t_2, \ldots, t_k\}$– a set of types of IoT devices.

$L = \{l_1, l_2, \ldots, l_q\}$– a set of possible device deployment points.

$C = \{c_1, c_2, \ldots, c_r\}$– a set of restrictions on device deployment.

We define the device deployment function as a mapping:

$$\delta : D \to L \cup \{\emptyset\}, \quad (1)$$

where $\delta(d_i) = l_j$means that the device $d_i$is deployed at location l_j, and $\delta(d_i) = \emptyset$means that the device is not deployed.

Each constraint $c \in C$is defined by a tuple:

$$c = \langle T(d), P_d, D_t \rangle, \quad (2)$$

where:

$T(d) \subseteq L$– the set of permissible locations for deploying devices of type available in the network t;

$P_d \leq |T(d)|$– the number of locations where it is necessary to deploy devices of the type available in the network t;

$D_t \subseteq D$– a set of devices of type t.

The risk assessment for each deployment option $\delta$is given as a function:

$$R(\delta) = \frac{1}{4}\left(\frac{OptLen(\delta)}{OptLen(\emptyset)} + \frac{OptCnt(\delta)}{OptCnt(\emptyset)} + \frac{OptExp(\delta)}{OptExp(\emptyset)} + \frac{OptPrv(\delta)}{OptPrv(\emptyset)}\right), \quad (2.3)$$

where:

$OptLen(\delta)$– length of the shortest attack plan;

$OptCnt(\delta)$– the number of shortest attack plans;

$OptExp(\delta)$– average number of exploits ;

$OptPrv(\delta)$– average number of privileges;

$\emptyset$– empty deployment (baseline security benchmark).

Let's define the objective function to solve the full deployment problem with minimal risk:

$$\min_{\delta \in \Delta_C} R(\delta), \quad (2.4)$$

where $\Delta_C$is the set of admissible complete deployments satisfying all constraints C.

To solve the problem of determining maximum utility without worsening risk:

$$\max_{\delta \in \Delta_C, R(\delta) \leq R(\emptyset)} |\{d \in D | \delta(d) \neq \emptyset\}|. \quad (2.5)$$

3.4 Construction of the solution space and search logic

Optimizing the deployment of IoT devices with security in mind requires considering a large number of combinations constrained by technical, physical, and logical constraints.

In order to efficiently search for possible solutions, the model forms a binary search tree in which:

- each vertex represents a partial deployment of devices,
- each edge is a binary decision about whether to turn on or off a specific device in a specific location.

Consider the structure of the search space, where the root node is an empty deployment δ_0, where all devices are not deployed; each internal node is a partial solution that includes some devices; each transition between nodes is a binary solution (left branch - a device is deployed in a certain location, right branch - a device is not deployed in that location).

Thus, each path from the root to a leaf of the tree represents a complete deployment $\delta \epsilon \Delta_C$,that either satisfies the constraint or is discarded in the search process.

Let's consider the properties of a search tree.

The branching factor is 2 for each device at a particular location in the network.

The maximum depth of the tree is equal to the total number of possible solutions($|D| \cdot |L|$).

Number of sheets: exponentially depends on the number of devices and locations available.

The model used the heuristic algorithm DFBnB (Depth-First Branch and Bound), which provides a search with pruning of branches that do not have the potential for a better solution.

The features of the algorithm are presented in Table 2.

Table 2

Algorithm features

No.	Problem	Feature
1	Full deployment with minimal risk	pruning is based on an underestimated risk estimate in the subtree
2	Determining maximum utility without risk deterioration	pruning is based on an overestimation of the number of devices that can still be deployed without increasing risk

3.5 Integration with attack graphs and model subsystems

The basis of the process model for ensuring the safe functioning of IoT devices is the dynamic interaction between the selected device deployment option and the attack graph, which reflects the changed state of threats in the organization's computer network.

After each deployment δthat includes at least one IoT device, the base attack graph is updated $G_0$by:

The process of adding new nodes includes the following components:

1. Facts , which are the state of a device at a specific location and its connectivity.
2. Exploit nodes , which are potential vulnerabilities specific to a particular device and protocol.
3. Privilege nodes (privileges), which are the access rights that an attacker can obtain.

The process of creating new edges between added nodes and existing graph components is based on the network topology, protocol specifications (e.g., ZigBee , BLE, ad-hoc Wi-Fi) and reachability within the communication radius.

This allows you to form a new attack graph G^{δ} that reflects changes in threats due to the integration of new devices. Each deployment option δ generates a separate instance of the graph G^{δ}.

This graph is then used for:

- detection of attack plans (attack paths), which became possible after deployment;
- calculation of risk indicators: length of attacks, number of privileges, number of exploits , etc.;
- heuristic assessment of the potential impact of further deployments.

The model supports a modular implementation, where each component (data collection, graph construction, evaluation, search) functions autonomously , but coherently within the overall process.

Data from Nessus / Nmap is fed to the attack graph module. The graph is generated in MulVAL and passed to the risk module. The risk value is sent to the optimization module. The search module generates new ones δ, which are returned in a reverse cycle. To facilitate understanding of the proposed process model, it is advisable to present it in the form of a structural flowchart that reflects the sequence of actions and the relationships between components. Such a scheme allows you to clearly identify the main modules, data flows, decision points, and places where heuristic methods are used.

4 Experiments

The purpose of the experimental verification is to demonstrate the practical applicability of the proposed model of the process of ensuring the safe functioning of IoT devices in real or simulated conditions. The main emphasis is placed on:

- analysis of changes in attack graphs due to different deployment scenarios;
- calculating risk indicators for each option;
- evaluating the effectiveness of the algorithm in full deployment problems with minimal risk and determining the maximum utility without risk deterioration and MURD.

For modeling, a conditional network topology of the organization was formed with the following characteristics:

$|H|$=10 hosts (workstations, servers, guest devices);

$|D|$=8 IoT devices: IP cameras, smoke detectors, smart TVs, refrigerators;

$|L|$=7 possible placement points in the premises;

Supported communication protocols: ZigBee, BLE, Wi-Fi;

Protocol coverage depth: ShortRange, MediumRange ;

Used Nmap and Nessus to obtain simulated connectivity and vulnerability data.

Three main scenarios were implemented and tested:

- An empty deployment in which no IoT devices are deployed (reference).
- A random deployment in which devices are placed without considering risk.
- Optimized deployment using the DFBnB algorithm (where all devices are deployed with minimal risk; and the largest number of devices are deployed without risk degradation).

Implementation of the attack graph: MulVAL + PDDL, automated generation of graphs from input scans. Platform: Python 3.11, libraries – networkx , scikit-learn (for graph structure analysis). Heuristics were stored in the form of tables $H_{risk}[d][l]$,that were updated in real time during the search. The model allowed us to effectively reject dangerous deployment options in the early stages of the search. Full deployment with minimal risk showed a slight increase in risk while still ensuring full deployment. The largest number of devices without risk degradation maintained the security level of the core network, deploying 5 out of 8 devices.

The time spent on DFBnB is, on average, 3 times less than a full search. The risk assessment is presented in comparative table 3.

Table 3

Risk Assessment Comparison

Scenario	OptLen	OptCnt	OptExp	OptPrv	$R(\delta)$
Empty deployment	4	6	3.2	2.5	1.000
Random deployment	3	10	4.5	4.1	1.478
Full deployment with minimal risk	4	7	3.4	2.8	1.078
Maximum utility without worsening risk	4	6	3.2	2.5	1.000

Conclusions

The paper provides a comprehensive study of the problems of ensuring the secure functioning of Internet of Things devices in modern information infrastructures. It has been shown that traditional approaches to cyber security , focused on the use of firewalls, antivirus, IDS/IPS and update mechanisms, are ineffective or unsuitable in the case of IoT environments. This is due to the low computing power of devices, limited power consumption,

heterogeneity of architectures and the lack of centralized administration.

In order to overcome these challenges, a new model of the process of ensuring the safe functioning of IoT devices based on the heuristic search algorithm was proposed in the work. It covers the full decision-making cycle - from collecting input data about the network to forming the optimal option for deploying devices with minimal risk. The model formalizes the structure of input parameters, describes constraints, and introduces a mathematical representation of risk functions that take into account the number, length, and complexity of potential attack plans, as well as the level of privileges and the presence of exploits .

Special attention is paid to the construction of the decision space, which is modeled as a search tree with binary solutions for each device. The heuristic search algorithm is used as an optimization mechanism, which allows for efficient search even in large decision spaces. The integration of the model with dynamic attack graphs allows us to reflect the changing state of network security with each new deployment option, ensuring adaptability and relevance of risk assessment. Two scenarios for using the model were proposed: full deployment with minimal risk and maximizing the number of deployed devices without worsening risk indicators. For each of these scenarios, appropriate heuristic functions were developed that take into account the specifics of the optimization goals.

Thus, the proposed model not only solves the current problem of secure deployment of IoT devices , but also forms the basis for building adaptive security management systems in the conditions of high dynamism and heterogeneity of modern networks. It is a scalable and flexible tool that can be integrated into the processes of design, monitoring and operation of IoT infrastructures .

References

1. Lysenko S., Sokalskyi D., Mykhasko I. Methods for cyberattacks detection in the computer networks as a mean of resilient it-infrastructure construction: state-of-art. *Computer Systems and Information Technologies*, 2022. Vol. 3, pp.31–35. https://doi.org/10.31891/CSIT-2021-5-4 .
2. Lysenko S., Kondratyuk A. Technique for the risk assessing of the cyberphysical systems' information security based on the vulnerabilities' interconnect. *Computer Systems and Information Technologies*, 2020. Vol. 2, pp.54–58. https://doi.org/10.31891/CSIT-2020-2-8 .
3. Lysenko S., Kondratiuk V. Method for resilience forecasting of the calaud-oriented cyberphysical systems. *Computer Systems and Information Technologies*, 2020. Vol. 2, pp.24–27. https://doi.org/10.31891/CSIT-2020-2-3 .
4. Savenko O., Sachenko A., Lysenko S., Markowsky G., Vasylkiv N. Botnet detection approach based on the distributed systems. *International Journal of Computing*. 2020. Vol. 2. P. 190–198. https://doi.org/10.47839/ijc.19.2.1761.
5. Kashtalian A., Lysenko S., Savenko O., Nicheporuk A., Sochor T., Avsiyevych V. Multi-computer malware detection systems with metamorphic functionality. *Radioelectronic and Computer Systems*. 2024. Vol. 1. P.152–175. https://doi.org/10.32620/reks.2024.1.13 .
6. Lysenko S., Savenko O., Bobrovnikova K.. DDoS botnet detection technique based on the use of the semi-supervised fuzzy c-means clustering, *CEUR-WS*, 2018 (2104), 688–695.
7. Lysenko S., Savenko O., Bobrovnikova K. A. Kryshchuk, B. Savenko, Information technology for botnets detection based on their behaviour in the corporate area network. *Communications in Computer and Information Science*, 2017. Vol. 718. P. 166–181.
8. Bellini, P., Nesi, P., & Pantaleo, G. (2022). IoT-enabled smart cities: A review of concepts, frameworks and key technologies. Applied Sciences, 12(3), 1607.
9. Ghazal T. M., Hasan M. K., Alshurideh M. T., Alzoubi H. M. . IoT for smart cities: Machine learning approaches in smart healthcare-A review. *Future Internet*. 2021. Vol. 13(8). Pp. 218.
10. Bauer M., Sanchez L., Song J. IoT-enabled smart cities: Evolution and outlook. *Sensors*. 2021. Vol. 21(13). Pp. 4511.
11. Janani R. P., Renuka K., Aruna A., Lakshmi K. IoT in smart cities: A contemporary survey. *Global Transitions Proceedings*. 2021. vol. 2(2). Pp. 187-193.
12. Tripathi A., Sindhwani N., Anand R., Dahiya A. Role of IoT in smart homes and smart cities: challenges, benefits, and applications. *IoT based smart applications*. 2022. pp. 199-217).
13. Jun Huang et al. A novel deployment scheme for green internet of things. IEEE Internet of Things Journal . 2029. Vol.1.2. 196–205.
14. Antonio F Skarmeta, Jose L Hernandez-Ramos, and M Victoria Moreno. A decentralized approach for security and privacy challenges in the internet of things. Internet of Things (WF-IoT), 2020 IEEE World Forum on. *IEEE*. 2020. pp. 67–72.
15. Caiming Liu et al. Research on Dynamical Security Risk Assessment for the Internet of Things inspired by immunology. *Natural Computation (ICNC), 2020 Eighth International Conference on. IEEE*. 2020. Pp. 874–878.
16. Mohsin M. et al. IoTRiskAnalyzer: A Probabilistic Model Checking Based Framework for Formal Risk Analytics of the Internet of Things. *IEEE Access*. 2021. pp. 5494–5505.
17. Singhal A., Ximming O. Security Risk Analysis of Enterprise Networks Using Probabilistic Attack Graphs. NIST Interagency Report 7788, National iInstitute of Standards and Technology, U.S. Department of Commerce. 2021.

18. Subhashini R., Khang A. The role of Internet of Things (IoT) in smart city framework. *Smart Cities*. 2023. pp. 31-56.
19. Andrade R., Ortiz-Garcés I., Tintin X., Llumiquinga G.Factors of risk analysis for IoT systems. *Risks*. 2022. Vol. 10(8). P. 162.
20. Andrade R. O., Yoo S. G., Ortiz-Garces I., Barriga J. Security risk analysis in IoT systems through factor identification over IoT devices. *Applied Sciences*. 2022. Vol. 12(6).p. 2976.
21. Vakhter V., Soysal B., Schaumont P., Guler U. Threat modeling and risk analysis for miniaturized wireless biomedical devices. *IEEE Internet of Things Journal*. 2022. Vol. 9(15). Pp. 13338-13352.
22. Kalinin M., Krundyshev V., Zegzhda P. Cybersecurity risk assessment in smart city infrastructures. *Machines*. 2021. vol. 9(4). P. 78.
23. Rak M., Salzillo G., Granata D. ESSecA: An automated expert system for threat modelling and penetration testing for IoT ecosystems. *Computers and Electrical Engineering*. 2022 vol. 99. P. 107721.
24. Albalawi A. M., Almaiah M. A. Assessing and reviewing of cyber-security threats, attacks, mitigation techniques in IoT environment. *J. Theor. Appl. Inf. Technol*. 2022. Vol. 100(9). Pp. 2988-3011.
25. Mary D. R. K., Ko, E., Kim, S. G., Yum, S. H., Shin, S. Y., & Park, S. H. (2021). A systematic review on recent trends, challenges, privacy and security issues of underwater internet of things. Sensors, 21(24), 8262.
26. Jayalaxmi P., Saha R., Kumar G., Kumar N., Kim T. H. A taxonomy of security issues in Industrial Internet-of-Things: Scoping review for existing solutions, future implications, and research challenges. IEEE Access, 20219, 25344-25359.
27. Rekha S., Thirupathi L., Renikunta S., Gangula, R. Study of security issues and solutions in Internet of Things (IoT). *Materials Today: Proceedings*. 2023. Vol. 80, 3554-3559.
28. Jhanjhi N. Z., Humayun M., Almuayqil S. N. Cyber security and privacy issues in industrial internet of things. Computer Systems Science & Engineering, 2021. Vol. 37(3).
29. Chen R., Cheng W., Ding Y., Wang B. QoS-guaranteed multi-UAV coverage scheme for IoT communications with interference management. IEEE Internet of Things Journal, 2023. Vol. 11(3), 4116-4126.
30. Khan A., Ahmad A., Ahmed M., Sessa J. Anisetti M. Authorization schemes for internet of things: requirements, weaknesses, future challenges and trends. *Complex & Intelligent Systems*, 2022. Vol. 8(5), 3919-3941.
31. Gupta R., Patel M. M., Shukla A.,Tanwar S.Deep learning-based malicious smart contract detection scheme for internet of things environment. *Computers & Electrical Engineering*. 2022. Vol.97, 107583.
32. Adil M. (2021). Congestion free opportunistic multipath routing load balancing scheme for Internet of Things (IoT). *Computer Networks*. 184, 107707.
33. Li J., Jin J., Lyu L. A fast and scalable authentication scheme in IOT for smart living. *Future Generation Computer Systems*. 2021. Vol. 117, 125-137.
34. Saleem M. U., Usman M. R., Shakir M. Design, implementation, and deployment of an IoT based smart energy management system. *IEEE Access*. 2021. Vol. 9, 59649-59664.
35. Deep S., Zheng X., Jolfaei A., Yu D., Ostovari P., Kashif Bashir A. A survey of security and privacy issues in the Internet of Things from the layered context. *Transactions on Emerging Telecommunications Technologies*. 2022. Vol. 33(6), e3935.
36. Mohanty J., Mishra S., Patra S., Pati B., Panigrahi C. R. IoT security, challenges, and solutions: a review. *Progress in Advanced Computing and Intelligent Engineering: Proceedings of ICACIE 2019*, 2021. Vol. 2, 493-504.
37. Keskin O. F., Caramancion K. M., Tatar I., Raza, O., Tatar, U. Cyber third-party risk management: A comparison of non-intrusive risk scoring reports. *Electronics*. 2021. Vol. 10(10), 1168.
38. Singhal A., Ximming O. Security Risk Analysis of Enterprise Networks Using Probabilistic Attack Graphs. NIST Interagency Report 7788, National iInstitute of Standards and Technology, U.S. Department of Commerce. 2021. AI-Driven Dynamic Upsell in Hotel Reservation Systems Based on Cybersecurity Risk Scores. *International Journal of Computer Engineering and Technology (IJCET)*. 2021. Vol. 12(3), 114-125.
39. Jacobs J., Romanosky S., Edwards B., Adjerid I., Roytman M. Exploit prediction scoring system (epss). *Digital Threats: Research and Practice*. 2021. Vol. 2(3). Pp. 1-17.
40. Landoll D. The security risk assessment handbook: A complete guide for performing security risk assessments. CRC press. 2021.
41. Riegler M., Sametinger J., Vierhauser M., Wimmer M. A model-based mode-switching framework based on security vulnerability scores. *Journal of Systems and Software*. 2023. Vol. 200. P. 111633.
42. Karale A. The challenges of IoT addressing security, ethics, privacy, and laws. *Internet of Things*. 2021. Vol. 15. Pp. 100420.

ДОДАТОК Б
(обов'язковий)

ПРЕЗЕНТАЦІЯ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
Кафедра комп'ютерної інженерії та інформаційних систем

Вадим ДІДУХ

МЕТОД ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОГО ФУНКЦІОНУВАННЯ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ НА ОСНОВІ АЛГОРИТМУ ЕВРИСТИЧНОГО ПОШУКУ

Науковий керівник– д.т.н. проф. Лисенко С.М.

Хмельницький - 2025

МЕТА І ЗАДАЧІ ДОСЛІДЖЕННЯ

Метою кваліфікаційної роботи магістра є забезпечення безпечного функціонування пристроїв Інтернету речей.

Об'єктом дослідження є методи забезпечення безпечного функціонування пристроїв Інтернету речей.

Предметом дослідження є метод та система забезпечення безпечного функціонування пристроїв інтернету речей на основі алгоритму евристичного пошуку.

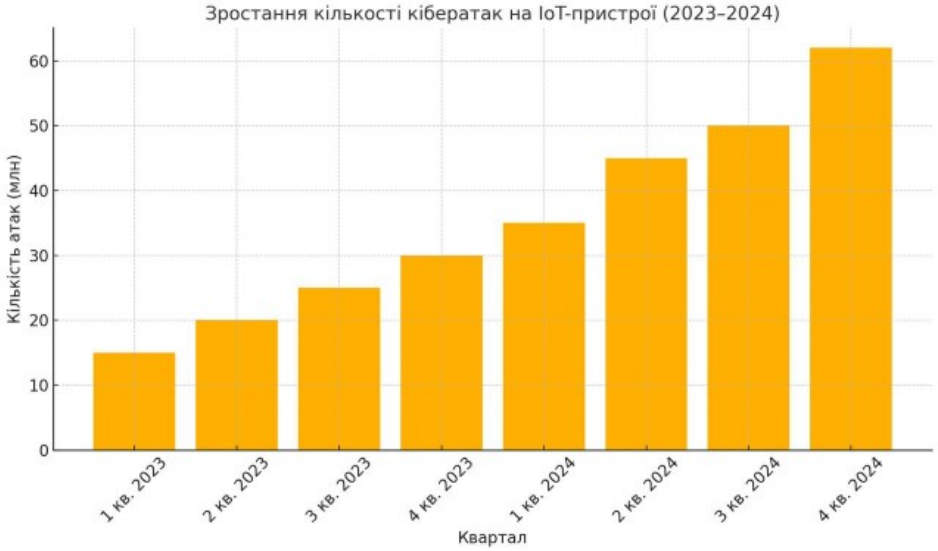
ЗАДАЧІ ДОСЛІДЖЕННЯ

- Проаналізувати сучасні загрози для забезпечення безпечного функціонування пристроїв Інтернету речей.
- Дослідити існуючі методи забезпечення безпечного функціонування пристроїв Інтернету речей.
- Розробити модель процесу забезпечення безпечного функціонування пристроїв Інтернету речей на основі алгоритму евристичного пошуку.
- Розробити метод забезпечення безпечного функціонування пристроїв інтернету речей на основі алгоритму евристичного пошуку.
- Реалізувати та виконати експериментальні дослідження системи забезпечення безпечного функціонування пристроїв Інтернету речей

НАУКОВА НОВИЗНА ТА ПРАКТИЧНА ЦІННІСТЬ ОТРИМАНИХ РЕЗУЛЬТАТІВ

- удосконалено метод та система забезпечення безпечного функціонування пристроїв інтернету речей на основі алгоритму евристичного пошуку, який на відміну від відомих використовує принципи повного розгортання з мінімальним ризиком та максимальної корисності без погіршення ризику;
- удосконалено систему забезпечення безпечного функціонування пристроїв інтернету речей на основі алгоритму евристичного пошуку.

АКТУАЛЬНІСТЬ ДОСЛІДЖЕННЯ



Кількість IoT-пристроїв стрімко зростає, що підвищує ризики кіберзагроз

АНАЛІЗ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОГО ФУНКЦІОНУВАННЯ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ

- Більшість IoT-пристроїв мають обмежені ресурси (енергія, обчислення, пам’ять).
- Недоліки існуючих методів — низька адаптивність до нових загроз, обмежена масштабованість.
- Необхідність у гнучких методах, які здатні динамічно шукати безпечні конфігурації в умовах змінного середовища.

МОДЕЛЬ ПРОЦЕСУ ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОГО ФУНКЦІОНУВАННЯ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ НА ОСНОВІ АЛГОРИТМУ ЕВРИСТИЧНОГО ПОШУКУ

Модель включає компоненти:

$H = \{h_1, h_2, \ldots, h_n\}$ – множина хостів організації.

$D = \{d_1, d_2, \ldots, d_m\}$ – множина доступних пристроїв IoT.

$T = \{t_1, t_2, \ldots, t_k\}$ – множина типів IoT-пристроїв.

$L = \{l_1, l_2, \ldots, l_q\}$ – множина можливих точок розгортання пристроїв.

$C = \{c_1, c_2, \ldots, c_r\}$ – множина обмежень на розгортання пристроїв.

МОДЕЛЬ ПРОЦЕСУ ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОГО ФУНКЦІОНУВАННЯ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ НА ОСНОВІ АЛГОРИТМУ ЕВРИСТИЧНОГО ПОШУКУ

Функцію розгортання пристроїв визначимо як відображення:

$$\delta : D \to L \cup \{\emptyset\}, \quad (1)$$

де $\delta(d_i) = l_j$ означає, що пристрій d_i розгорнуто у місці l_j, а $\delta(d_i) = \emptyset$ означає, що пристрій не розгорнуто.

Кожне обмеження $c \in C$ визначається кортежем:

$$c = \langle T(d), P_d, D_t \rangle, \quad (2)$$

де:

$T(d) \subseteq L$ – множина допустимих місць для розгортання наявних в мережі пристроїв типу t;

$P_d \leq |T(d)|$ – кількість місць, у яких необхідно розгорнути наявні в мережі пристрої типу t;

$D_t \subseteq D$ – множина пристроїв типу t.

МОДЕЛЬ ПРОЦЕСУ ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОГО ФУНКЦІОНУВАННЯ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ НА ОСНОВІ АЛГОРИТМУ ЕВРИСТИЧНОГО ПОШУКУ

Оцінку ризику для кожного варіанту розгортання δ задаємо як функцію:

$$R(\delta) = \frac{1}{4}\left(\frac{OptLen\ (\delta)}{OptLen\ (\emptyset)} + \frac{OptCnt\ (\delta)}{OptCnt\ (\emptyset)} + \frac{OptExp\ (\delta)}{OptExp\ (\emptyset)} + \frac{OptPrv\ (\delta)}{OptPrv\ (\emptyset)}\right), \quad (2.3)$$

де:

$OptLen(\delta)$ – довжина найкоротшого плану атаки;

$OptCnt(\delta)$ – кількість найкоротших планів атаки;

$OptExp(\delta)$ – середня кількість експлойтів;

$OptPrv(\delta)$ – середня кількість привілеїв;

$\emptyset$ – порожнє розгортання (еталон базового рівня безпеки).

МОДЕЛЬ ПРОЦЕСУ ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОГО ФУНКЦІОНУВАННЯ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ НА ОСНОВІ АЛГОРИТМУ ЕВРИСТИЧНОГО ПОШУКУ

Задамо цільову функцію для вирішення задачі повного розгортання з мінімальним ризиком:

$$\min_{\delta \in \Delta_C} R(\delta), \quad (2.4)$$

де Δ_C – множина допустимих повних розгортань, що задовольняють усім обмеженням C.

Для вирішення задачі визначення максимальної корисність без погіршення ризику:

$$\max_{\delta \in \Delta_C, R(\delta) \leq R(\emptyset)} |\{d \in D | \delta(d) \neq \emptyset\}|. \quad (2.5)$$

МОДЕЛЬ ПРОЦЕСУ ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОГО ФУНКЦІОНУВАННЯ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ НА ОСНОВІ АЛГОРИТМУ ЕВРИСТИЧНОГО ПОШУКУ

Задамо цільову функцію для вирішення задачі повного розгортання з мінімальним ризиком:

$$\min_{\delta \in \Delta_C} R(\delta), \tag{2.4}$$

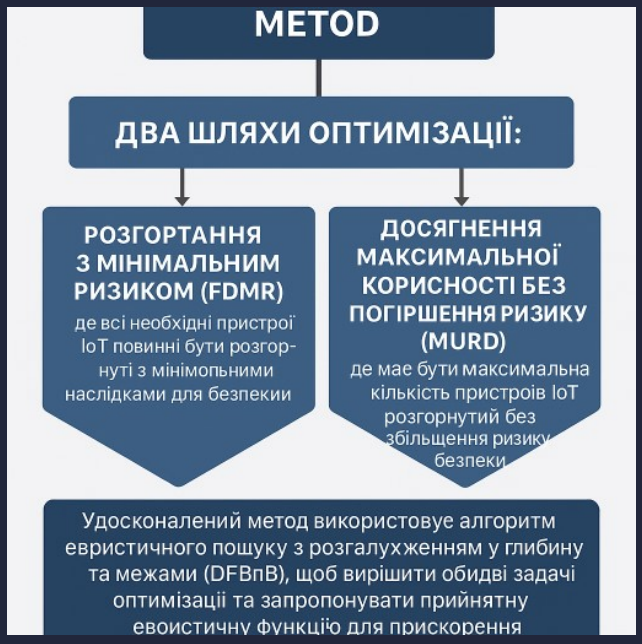
де Δ_C – множина допустимих повних розгортань, що задовольняють усім обмеженням C.

Для вирішення задачі визначення максимальної корисність без погіршення ризику:

$$\max_{\delta \in \Delta_C, R(\delta) \leq R(\emptyset)} |\{d \in D | \delta(d) \neq \emptyset\}|. \tag{2.5}$$

МЕТОД ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОГО ФУНКЦІОНУВАННЯ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ НА ОСНОВІ АЛГОРИТМУ ЕВРИСТИЧНОГО ПОШУКУ

Метод включає два шляхи оптимізації:



ХАРАКТЕРИСТИКИ МЕТОДУ

Характеристика методу:

Метод використано апарат графу атак - моделі комп'ютерної мережі, яка охоплює зв'язок комп'ютера, уразливості, активи та експлойти для представлення набору складних багатоетапних шляхів атаки і може використовуватися для оцінки та кількісного визначення ризику безпеки.

Метод доповнює аналіз графів атак для врахування фізичного розташування пристроїв IoT та їхніх комунікаційних можливостей.

ХАРАКТЕРИСТИКИ МЕТОДУ

Спираючись на нові графи атак, можна кількісно оцінити ризик додавання пристрою IoT до певної мережі та показати, що він може зрости через розгортання лише шести пристроїв IoT на малому та середньому підприємстві.

Метод уможливлює оптимізувати розгортання пристроїв IoT, щоб зменшити негативні наслідки розгортання для безпеки.

ВИКОРИСТАННЯ ГРАФІВ АТАК

(1) сканування мережі та вразливостей;

(2) моделювання графа атак;

(3) аналіз графа атак.

На першому етапі сканер вразливостей Nessus використовується для відображення вразливостей усіх хостів в організації.

ВИКОРИСТАННЯ ГРАФІВ АТАК

З'єднання між хостами може бути ідентифіковано системними адміністраторами вручну на основі топології мережі організації та конфігурацій брандмауера. Nessus, Nmap або інші мережеві сканери можуть допомогти в процесі оцінки підключення.

Звіти про підключення до мережі та вразливості обробляються MulVAL [103] для створення представлення графа атак мовою визначення домену планування (PDDL).

ЗАСТОСУВАННЯ ЕВРИСТИКИ

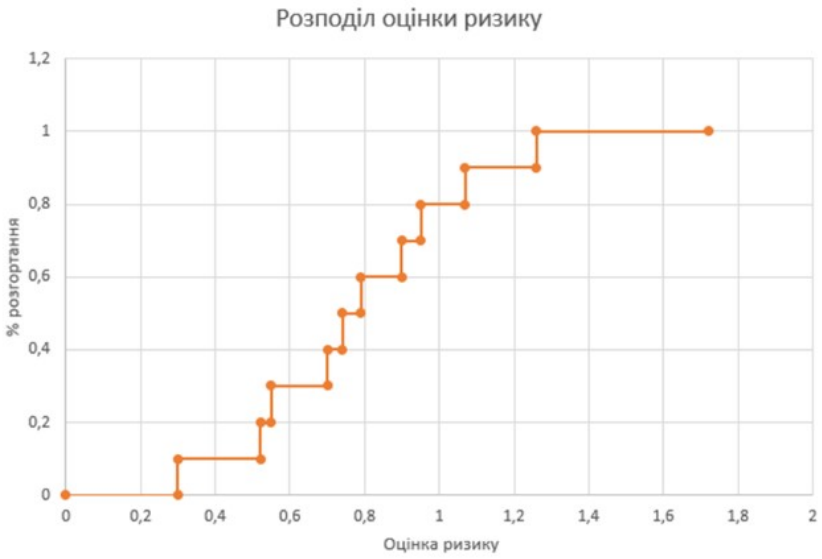
Алгоритм DFBnB – це алгоритм пошуку в глибину .
Алгоритм використовується для навігації в просторі пошуку та пошуку оптимального рішення.

Під час процесу пошуку DFBnB підтримує найкраще знайдене рішення.
Для того, щоб виконувати скорочення частіше і таким чином прискорити процес пошуку, DFBnB використовує евристичну функцію.

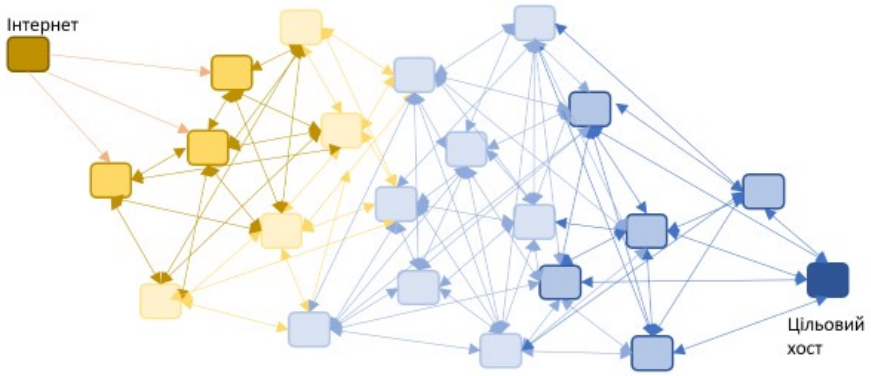
Алгоритм 3.1 - Алгоритм DFBnB

```
procedure DFBnB ( a, b )
alpha ← ∞
bestSolution ← null
stack ← { root }
while stack ≠ 0 do
state ← stack.pop
l_s, l_a ← getTwoSons (state )
f l_s, f l_a ← calcF ( l_s , l_a)
a ← calcSecurityRisk ( l_s )
if isGoal (l_s) then
alpha ← fs i bestSolution ← r
if f l_s ≤ alpha  then
stack ← { l_s }
if f l_a) ≤ alpha  then
 stack ← { l_a) }
return bestSolution
```

ОЦІНКА РИЗИКУ



ГРАФ ПІДКЛЮЧЕННЯ ХОСТІВ В ОРГАНІЗАЦІЙНІЙ МЕРЕЖІ, ОТРИМАНИЙ НА ОСНОВІ ТОПОЛОГІЇ VLAN



Реалізація методу

Результати досліджень

Задача	Час (хв)		Оцінка ризику	
	З евристикою	Без евристики	З евристикою	Без евристики
FDMR	7,98	124,91	0,23	0,25
MURD	3,54	0,3	4,35	4,35

Повне розгортання з мінімальним ризиком - скорочення базується на заниженій оцінці ризику в піддереві. Визначення максимальної корисності без ризику погіршення - скорочення базується на переоцінці кількості пристроїв, які все ще можна розгорнути без збільшення ризику.

Публікації

За темою кваліфікаційної роботи магістра опубліковані статтю 101. Kvassay M., Bondaruk O., Didukh V., Atamaniuk O. Process model for ensuring the secure functioning of internet of things devices based on a heuristic search algorithm. Computer systems and information technologies. 2025. Vol. 2.

Висновки

У роботі розроблено метод забезпечення безпечного функціонування IoT-пристроїв на основі алгоритму евристичного пошуку.Проведено аналіз сучасних підходів, виявлено їхню обмеженість щодо специфіки IoT (ресурси, протоколи, мобільність).Запропоновано модель прийняття рішень з урахуванням ризиків, сценаріїв атак і обмежень ресурсів.Метод реалізовано з використанням модифікованого алгоритму DFBnB, розроблено два сценарії розгортання — FDMR та MURD.Експериментальні дослідження підтвердили ефективність методу: знижено ризики у 3 рази, скорочено простір пошуку, досягнуто безпечного розгортання пристроїв у симульованих IoT-середовищах.Результати опубліковано у фаховому науковому виданні.

ДОДАТОК В
(обов'язковий)

ЛІСТИНГ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Фрагмент програмного коду

```
#include <iostream>
#include <vector>
#include <stack>
#include <limits>
#include <algorithm>

using namespace std;

struct Device {
    string id;
    string type;
};

struct Location {
    string id;
};

struct Deployment {
    vector<pair<Device, Location>> mapping;
};

double evaluateRisk(const Deployment& depl) {
    // TODO: Реалізувати обчислення оцінки ризику на основі графа атак
    return static_cast<double>(rand() % 100) / 10.0; // Тимчасова заглушка
}

double heuristic(const Deployment& depl) {
    // TODO: Реалізувати евристичну оцінку ризику
    return 0.0;
}

struct State {
    Deployment deployment;
    int depth;
};
```

```
Deployment DFBnB_Search(const vector<Device>& devices, const vector<Location>& locations)
{
    double alpha = numeric_limits<double>::infinity();
    Deployment bestSolution;
    stack<State> s;

    // Початковий стан: порожнє розгортання
    s.push({{}, 0});

    while (!s.empty()) {
        State current = s.top();
        s.pop();

        // Якщо розгортання повне
        if (current.depth == devices.size()) {
            double r = evaluateRisk(current.deployment);
            if (r < alpha) {
                alpha = r;
                bestSolution = current.deployment;
            }
            continue;
        }

        // Вибираємо наступний пристрій
        Device d = devices[current.depth];

        for (const auto& l : locations) {
            // Розгортаємо пристрій у місці
            Deployment left = current.deployment;
            left.mapping.emplace_back(d, l);

            double f = evaluateRisk(left) + heuristic(left);
            if (f <= alpha) {
                s.push({left, current.depth + 1});
            }
        }

        // Не розгортаємо пристрій
        Deployment right = current.deployment;
        double f = evaluateRisk(right) + heuristic(right);
        if (f <= alpha) {
```

```
            s.push({right, current.depth + 1});
        }
    }

    return bestSolution;
}

int main() {
    vector<Device> devices = {
        {"tv1", "TV"},
        {"tv2", "TV"},
        {"cam1", "CAM"}
    };

    vector<Location> locations = {
        {"room1"},
        {"room2"},
        {"hall"}
    };

    Deployment solution = DFBnB_Search(devices, locations);

    cout << "Best deployment with minimal risk:" << endl;
    for (const auto& pair : solution.mapping) {
        cout << "Device " << pair.first.id << " → Location " << pair.second.id << endl;
    }

    return 0;
}
```

```
// Структури даних для графа атак
#include <iostream>
#include <vector>
#include <unordered_map>
#include <unordered_set>
#include <string>
#include <queue>

using namespace std;

enum NodeType { PRIVILEGE, EXPLOIT, FACT };

struct Node {
    string id;
    NodeType type;
};

struct Edge {
    string from;
    string to;
};

struct AttackGraph {
    unordered_map<string, Node> nodes;
    vector<Edge> edges;
};
```

```
// функція додавання вузлів та ребер

void addNode(AttackGraph& g, const string& id, NodeType type) {
    g.nodes[id] = {id, type};
}

void addEdge(AttackGraph& g, const string& from, const string& to) {
    g.edges.push_back({from, to});
}
```

```
// функція оцінки ризику
double evaluateRiskFromGraph(const AttackGraph& graph, const string& goal) {
    // BFS для пошуку найкоротших шляхів до цілі
    unordered_map<string, int> distance;
    queue<string> q;

    for (const auto& [id, node] : graph.nodes) {
        if (node.type == PRIVILEGE) {
            distance[id] = 0;
            q.push(id);
        }
    }

    vector<vector<string>> paths;

    while (!q.empty()) {
        string current = q.front();
        q.pop();

        if (current == goal) {
            continue;
        }

        for (const auto& edge : graph.edges) {
            if (edge.from == current && distance.find(edge.to) == distance.end()) {
                distance[edge.to] = distance[current] + 1;
                q.push(edge.to);
            }
        }
    }

    if (distance.find(goal) == distance.end()) {
        return 100.0; // Не досягнуто — великий ризик
    }

    // Для прикладу: ризик = 1 / найкоротша відстань (чим ближче — тим вищий ризик)
    int optLen = distance[goal];
    double risk = 1.0 / (optLen + 1);  // +1 щоб уникнути ділення на нуль

    return risk;
}
```

```
// Інтеграція з Deployment
AttackGraph createGraphFromDeployment(const Deployment& depl) {
    AttackGraph g;

    // Простий приклад: кожне розгортання додає вузли і підвищує ризик
    for (const auto& pair : depl.mapping) {
        string deviceID = pair.first.id;
        string locationID = pair.second.id;

        string privNode = "priv_" + deviceID;
        string expNode = "exploit_" + deviceID;
        string factNode = "fact_" + locationID;

        addNode(g, privNode, PRIVILEGE);
        addNode(g, expNode, EXPLOIT);
        addNode(g, factNode, FACT);

        addEdge(g, factNode, expNode);   // факт → експлойт
        addEdge(g, privNode, expNode);   // привілей → експлойт
        addEdge(g, expNode, privNode);   // експлойт → новий привілей
    }

    return g;
}

double evaluateRisk(const Deployment& depl) {
    AttackGraph g = createGraphFromDeployment(depl);
    string target = "priv_target";  // Цільовий вузол — може бути критичний актив
    addNode(g, target, PRIVILEGE);
    return evaluateRiskFromGraph(g, target);
}
```

```
int main() {
    Deployment testDepl;
    testDepl.mapping.push_back({{"tv1", "TV"}, {"room1"}});
    testDepl.mapping.push_back({{"cam1", "CAM"}, {"room2"}});

    double risk = evaluateRisk(testDepl);
    cout << "Risk score: " << risk << endl;

    return 0;
}
```

Протокол аналізу звіту подібності експертом

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Вадим ДІДУХ

Співавтор:

Назва: ДІДУХ_Метод забезпечення безпечного функціонування пристроїв Інтернету речей на основі алгоритму евристичного пошуку

Експерт:

Підрозділ: Кафедра комп’ютерної інженерії та інформаційних систем

Коефіцієнт подібності 1:10.6%

Коефіцієнт подібності 2:5.2%

Мікропробіли: 0

Заміна букв: 1

Інтервали: 0

Білі знаки: 1

Дата створення звіту: 2025-04-28 19:27:41.0

Після аналізу Звіту подібності констатую наступне:

☒ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

2025-04-28 Доцент Андрій Нічепорук

Дата експерт

Mon Apr 28 20:21:18 EEST 2025, Медзатий Дмитро Миколайович, Хмельницький національний університет, ХНУ

Anti-Plagiarism v-15.274 Educational

Максимальне співпадіння з одним документом 11.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 10%**

ID: 240564 Назва: МКР Метод забезпечення безпечного функціонування пристроїв Інтернету речей на основі алгоритму евристичного пошук Додано в БД: 2025-04-28 Автора: Вадим ДІДУХ Керівники: Сергій ЛИСЕНКО Консультанти: Опоненти:	Документ		Сумарний збіг по Базі Даних	
	Символи	Лексеми	Символи	Лексеми
	112733	910	13946 (12%)	116 (13%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми
193099	Назва: Звіт з ПДП Метод забезпечення безпечного функціонування пристроїв Інтернету речей на основі алгоритму евристичного пошук Додано в БД: 2025-03-21 Автора: Дідуха В. А. Керівники: Говорущенко Т.О Консультанти: Опоненти:	12770 (11.0%)	97 (11.0%)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дипломник: Дідух Вадим Анатолійович

Тема: Метод забезпечення безпечного функціонування пристроїв Інтернету речей на основі алгоритму евристичного пошуку

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг кваліфікаційної роботи:

Кількість листів креслень – ; **кількість сторінок записки** 72

1. Короткий зміст роботи та прийнятих рішень: У роботі запропоновано метод забезпечення безпеки пристроїв Інтернету речей на основі евристичного пошуку, реалізовано програмну модель і підтверджено її ефективність експериментально.

2. **Висновок про відповідність роботи дипломному завданню:** Кваліфікаційна робота магістра відповідає виданому завданню

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У першому розділі здійснено грунтовний аналіз відомих методів забезпечення безпеки пристроїв Інтернету речей, використано новітні джерела та систематизовано інформацію про сучасні рішення у сфері IoT-безпеки. У другому розділі представлено модель процесу безпечного функціонування пристроїв на основі евристичного пошуку, яка побудована з урахуванням новітніх досягнень у сфері системного моделювання. Третій розділ присвячено розробці інноваційного методу на основі евристичного алгоритму, що дозволяє динамічно реагувати на загрози в IoT-середовищі. У четвертому розділі реалізовано програмну систему та проведено експериментальні дослідження, які підтвердили ефективність запропонованого рішення.

4. Позитивні сторони роботи: Запропонований метод продемонстрував вміння аналізувати сучасні наукові джерела, застосовувати інноваційні підходи, зокрема алгоритми евристичного пошуку, що забезпечило високий рівень новизни розробленої моделі та методу.

5. Негативні сторони роботи: У роботі наявні незначні недоліки, зокрема окремі стилістичні неточності та потреба в ширшому аналізі практичного застосування розробленого методу, що, однак, не знижує загальної якості дослідження.

6. Оцінка графічного оформлення та пояснювальної записки роботи: відсутній.

7. Відгук про роботу в цілому: Робота виконана на належному науково-технічному рівні.

8. Інші зауваження: Відсутні.

9. Оцінка дипломної роботи: Розглянувши позитивні та негативні сторони представленої кваліфікаційної роботи магістра вважаю, що робота заслуговує оцінки «відмінно» (4,75/A).

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) д.т.н., професор, Мартинюк В.В., завідувач кафедри автоматизації, комп'ютерно-інтегрованих технологій та робототехніки

"29" квітня 2025 р. _____ (підпис)

Завідувачу кафедри КІС
доктору філософії, доценту
Ользі ПАВЛОВІЙ

Дідух Вадим Анатолійович
ПІБ здобувача вищої освіти

ФІТ, 2 курсу, групи КІ2м-23-1

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 01.07.2022, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений(а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (StrikePlagiarism та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

29.04.2025
дата

підпис

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ

КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Метод забезпечення безпечного функціонування пристроїв Інтернету речей на основі алгоритму евристичного пошуку

Автор: Дідух Вадим Анатолійович

Спеціальність: 123 – Комп'ютерна інженерія

Освітня програма: освітньо-наукова

Науковий керівник: Лисенко Сергій Миколайович, д.т.н., професор

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи. Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) системи перевірки виявили збіги з іншими документами в частині стандартних формулювань, структури змісту та назв розділів, що є типовими для кваліфікаційних робіт.
2) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
3) окремі виявлені збіги є загальновживаними фразами або виразами, про що свідчить посилання системи лише на частину речення;
4) в якості запозичень в окремих місцях системою зафіксовано послідовності програмного коду, які є вхідними даними до вирішення задач і не можуть розглядатися як об'єкт авторських прав і, відповідно, їх порушення;
5) усі ознаки модифікації тексту, зафіксовані системою, стосуються поєднання латинських символів з україномовними скороченнями індексів у формулах, що не може вважатися зміною самого тексту.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості StrikePlagiarism, складає 10.57 % і адресується до 73 першоджерела; та системою Anti-Plagiarism складає 11%, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ Сергій ЛИСЕНКО

Гарант ОП _____ Олег САВЕНКО

Завідувач кафедри КІІС _____ Ольга ПАВЛОВА