МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки

ВОЛОШИН Віктор Олексійович

СИСТЕМА ВИЯВЛЕННЯ ВТОРГНЕНЬ ДЛЯ ІНТЕРНЕТ – РЕЧЕЙ / AN INTRUSION DETECTION SYSTEM FOR THE INTERNET OF THINGS

спеціальність: 125 – Кібербезпека та захист інформації
освітньо-професійна програма – Кібербезпека

Кваліфікаційна робота

Виконав студент групи
КБм -21
В.О.Волошин

Науковий керівник
к.т.н., доцент Н.Г.Яцків

Кваліфікаційну роботу допущено
до захисту:

«____» _____ ___2024 р.

Завідувач кафедри
_____ В.В.Яцків

ТЕРНОПІЛЬ - 2024

Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки
Освітній ступінь «магістр»
спеціальність: 125 - Кібербезпека та захист інформації
освітньо-професійна програма – Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ В.В.Яцків
«____» _____ 2023 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
ВОЛОШИНУ Віктору Олексійовичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи:
Система виявлення вторгнень для Інтернет – речей /
An Intrusion Detection System for the Internet of Things
керівник роботи к.т.н., доцент Н.Г.Яцків
затверджені наказом по університету від 12 грудня 2023 року № 753

2. Строк подання студентом закінченої випускної кваліфікаційної роботи 12 грудня 2024 року.

3. Вихідні дані до кваліфікаційної роботи: завдання на випускну кваліфікаційну роботу студента, наукові статті, технічна література.

4. Основні питання, які потрібно розробити:

- провести аналіз існуючих методів шифрування та захисту для IoT;
- дослідити типи атак і їхні вразливості, розробити алгоритми для виявлення загроз із застосуванням сигнатурного та поведінкового аналізу;
- адаптувати систему для ефективної роботи в середовищах з обмеженими ресурсами.

5. Перелік графічного матеріалу у роботі:

- Типи систем виявлення вторгнень.
- Схема роботи виявлення аномалій.
- Концепція IDS на основі підпису.
- Гібридна система виявлення вторгнень.
- Категорії методів виявлення вторгнень.
- Виявлення шкідливого ПЗ на основі ML.
- Приклад графа атаки.
- Загальна структура системи моделі захисту.
- Таксономія атак IoTID20.
- ROC-крива Дерево рішень.
- ROC-крива K-NN.
- ROC-крива Ада Буст.
- ROC-крива SVM.

6. Консультанти розділів кваліфікаційної роботи

	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 12 грудня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строки виконання етапів кваліфікаційної роботи	Примітка
1	Огляд криптографічних методів для забезпечення безпеки в IoT	12.2023 р. – 03.2024 р.	
2	Теоретичні основи систем виявлення вторгнень	03.2024 р. – 06.2024 р.	
3	Практична реалізація алгоритму машинного навчання для системи виявлення вторгнень в IoT	06.2024 р. – 11.2024 р.	

Студент _____ ВОЛОШИН В.О.
(підпис)

Керівник роботи _____ к.т.н., доцент Н.Г. ЯЦКІВ
(підпис)

АНОТАЦІЯ

Кваліфікаційна робота на тему «Система виявлення вторгнень для Інтернет – речей» на здобуття освітнього ступеня «Магістр» зі спеціальності 125 «Кібербезпека та захист інформації» освітньо-професійної програми «Кібербезпека» написана обсягом 64 сторінки і містить 15 рисунків, 13 таблиць та 48 джерел за переліком посилань.

Метою кваліфікаційної роботи є розробка ефективної системи виявлення вторгнень для IoT, здатної виявляти загрози в реальному часі, враховуючи обмеження ресурсів пристроїв IoT.

Для розв’язання поставлених задач у даній кваліфікаційній роботі використано такі методи дослідження: аналіз літературних джерел з безпеки IoT, моделювання, порівняльний аналіз, інструменти для тестування та оцінки ефективності IDS систем у реальному середовищі.

Результати дослідження. Результати дослідження включають аналіз та систематизацію криптографічних алгоритмів, розробку та адаптацію системи виявлення вторгнень для IoT, а також оцінку її ефективності в умовах обмежених ресурсів пристроїв.

Ключові слова: ІНТЕРНЕТ РЕЧЕЙ, СИСТЕМА ВИЯВЛЕННЯ ВТОРГНЕНЬ, ПОШУК ВРАЗЛИВОСТЕЙ, МАШИННЕ НАВЧАННЯ.

ABSTRACT

Qualification work on the topic of "Identifying Internet-Things" for a Master's degree in the specialty 125 "Cybersecurity and Information Protection" of the Educational and Professional Program "Cybersecurity" is written in volume of 66 pages and contains 15 drawings, 13 tables and 48 sources. According to the list of references.

The purpose of the qualification work is to develop an effective system of detection of IoT invasion that can identify real -time threats, taking into account the limitation of IoT devices. The following research methods were used to solve the tasks in this qualification work: analysis of literary sources for IOT safety, modeling, comparative analysis, tools for testing and evaluating the efficiency of IDS systems in the real environment.

Results of the study. The results of the study include the analysis and systematization of cryptographic algorithms, the development and adaptation of the IOOT invasion system, as well as to evaluate its efficiency in the conditions of limited resources of devices.

Keywords: INTERNET THINGS, SYSTEM OF DETECTION OF INVASION, SEARCH FOR VULNERABILITY, MACHINE LEARNING.

.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

IoT - Internet of Things.

AES - Advanced Encryption Standard.

IDS - Intrusion Detection System.

ML - Machine learning.

DL - Deep learning.

ROC - receiver operating characteristic (робоча характеристика приймача).

HTTP/HTTPS - HyperText Transfer Protocol /Secure.

SVM - Support Vector Machine.

DoS/DDoS - (distributed) denial-of-service attack.

IEEE - Institute of Electrical and Electronics Engineers.

CVE - Common Vulnerabilities and Exposures.

NIST - National Bureau of Standards.

ВСТУП

Актуальність теми. Актуальність теми цього дослідження зумовлена стрімким розвитком Інтернету речей (IoT) та його проникненням у різні сфери – від промислових систем до побутових пристроїв. Розширення мережі IoT створює значні можливості для автоматизації, підвищення ефективності роботи та покращення якості життя. Проте, водночас це робить такі системи вразливими до різного роду кіберзагроз, оскільки пристрої IoT мають обмежені обчислювальні ресурси та часто не підтримують традиційні методи захисту, такі як шифрування даних та багатофакторна автентифікація [1].

Це значно підвищує ризики вторгнень, перехоплення даних, несанкціонованого доступу та зловживання підключеними пристроями, що призводить до зростання кількості атак та вимагає створення ефективних систем виявлення вторгнень (IDS), здатних працювати в умовах обмежених ресурсів. З огляду на специфіку IoT-середовища, традиційні методи забезпечення безпеки часто є надто ресурсомісткими, що унеможливлює їх застосування. Тому необхідність розробки спеціалізованих рішень для виявлення вторгнень та захисту інформації в IoT є надзвичайно актуальною, а їх впровадження дозволить зменшити ризики для користувачів та забезпечити належний рівень безпеки в умовах сучасного кіберсередовища.

Мета і завдання дослідження. Метою дослідження є розробка ефективної системи виявлення вторгнень для IoT, здатної виявляти загрози в реальному часі, враховуючи обмеження ресурсів пристроїв IoT. Для досягнення поставленої мети необхідно вирішити наступні завдання:

– провести аналіз існуючих методів шифрування та захисту для IoT;

– дослідити типи атак і їхні вразливості, розробити алгоритми для виявлення загроз із застосуванням сигнатурного та поведінкового аналізу;

– адаптувати систему для ефективної роботи в середовищах з обмеженими ресурсами.

Об'єктом дослідження є процеси забезпечення кібербезпеки в середовищі Інтернету речей.

Предметом дослідження є методи та алгоритми виявлення і запобігання вторгненням у мережах Інтернету речей, які забезпечують захист пристроїв та інформації від несанкціонованого доступу та різноманітних кіберзагроз в умовах обмежених ресурсів пристроїв IoT.

Методи дослідження. Для досягнення результатів у роботі використано такі методи дослідження: аналіз літературних джерел з безпеки IoT, моделювання, порівняльний аналіз, інструменти для тестування та оцінки ефективності IDS систем у реальному середовищі.

Наукова новизна. Наукова новизна дослідження полягає в розробці IDS системи, оптимізованої для обмежених ресурсів IoT-пристроїв, яка поєднує різні методи аналізу для підвищення ефективності виявлення атак.

Практичне значення. Практичне значення дослідження полягає в можливості застосування розробленої системи в реальних IoT-мережах.

Результати дослідження. Результати дослідження включають аналіз та систематизацію криптографічних алгоритмів, розробку та адаптацію системи виявлення вторгнень для IoT, а також оцінку її ефективності в умовах обмежених ресурсів пристроїв.

Публікації та апробація до магістерської роботи.

1. Волошин В. Адаптивні системи виявлення вторгнень для Інтернету речей. Матеріали науково-практична конференція молодих вчених, аспірантів та студентів «Кібербезпека та комп'ютерно-інтегровані технології» (КБКІТ - 2024), Тернопіль, 2024. – С. 52-56.

2. Волошин В. Моделі систем виявлення вторгнень у мережах Інтернету речей. Матеріали науково-практичного симпозіуму «Захист інформації», Тернопіль, 2024. – С. 28-31.

1 ОГЛЯД КРИПТОГРАФІЧНИХ МЕТОДІВ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В ІНТЕРНЕТІ РЕЧЕЙ

1.1. Симетричне та асиметричне шифрування

Шифрування даних у системах IoT є компонентом забезпечення безпеки та конфіденційності інформації, А її розвиток створює необхідність впровадження ефективних методів криптографічного захисту, що забезпечать належний рівень безпеки при обмежених ресурсах пристроїв [1, 2].

Симетричне шифрування виступає основним методом захисту даних у пристроях IoT через свою обчислювальну ефективність та швидкодію. Алгоритми симетричного шифрування, , використовують єдиний ключ для шифрування та дешифрування, що суттєво зменшує навантаження на ресурси системи. Практика показує, що реалізація AES-128 на мікроконтролерах IoT потребує 10 КБ пам'яті та забезпечує швидкість шифрування до 1 Мбіт/с, та робить його оптимальним вибором для застосування [3].

Впровадження симетричного шифрування в IoT системах вимагає ретельного планування процесу розподілу ключів між пристроями. Проблема безпечного обміну ключами стає особливо гострою в масштабних IoT мережах, де кількість пристроїв може досягати тисяч одиниць. Практичний досвід демонструє ефективність використання протоколів розподілу ключів на основі довіреного центру, який виконує роль координатора та зберігає майстер-ключі для всіх пристроїв мережі [4].

Асиметричне шифрування відіграє критичну роль у забезпеченні механізмів автентифікації та встановлення захищених каналів зв'язку між пристроями IoT. Алгоритми RSA та ECC застосовуються для створення цифрових підписів та обміну ключами симетричного шифрування. Дослідження показують, що використання ECC є більш доцільним для IoT пристроїв, оскільки при однаковому рівні безпеки потребує значно менших ключів порівняно з RSA (табл. 1.1) [5].

Таблиця 1.1 – Параметри безпеки та ефективності алгоритмів RSA і ECC

Рівень безпеки (біт)	Розмір ключа RSA (біт)	Розмір ключа ECC (біт)	Час генерації ключа (мс)
80	1024	160	15
112	2048	224	25
128	3072	256	30
192	7680	384	45
192	15360	512	60

Реалізація гібридних систем шифрування, що поєднують переваги симетричних та асиметричних алгоритмів, дозволяє досягти оптимального балансу між безпекою та продуктивністю IoT систем.

Розробка протоколів безпеки для IoT систем вимагає врахування специфічних характеристик пристроїв та мереж. Обмеження за енергоспоживанням, обчислювальною потужністю та пам'яттю потребують оптимізації криптографічних операцій. Практика показує, що використання спеціалізованих криптографічних співпроцесорів може значно підвищити ефективність шифрування без суттєвого збільшення енергоспоживання.

Методи оптимізації криптографічних операцій включають використання попередніх обчислень, кешування проміжних результатів та застосування апаратних прискорювачів. Експериментальні дослідження демонструють, що впровадження таких оптимізацій може знизити енергоспоживання на криптографічні операції до 40% без зниження рівня безпеки [6].

Процес впровадження криптографічних механізмів у IoT системах потребує комплексного підходу до управління ключами. Необхідно забезпечити надійні механізми генерації, розподілу, зберігання та оновлення криптографічних ключів. Дослідження показують, що використання апаратних модулів безпеки (HSM) для зберігання критичних ключових матеріалів суттєво підвищує загальний рівень захищеності системи.

Аналіз вразливостей криптографічних систем в IoT демонструє необхідність регулярного оновлення криптографічних параметрів та

протоколів. Поява нових методів криптоаналізу та збільшення доступних обчислювальних потужностей вимагають періодичного перегляду довжин ключів та використовуваних алгоритмів. Як показано в таблиці 1.1, вибір параметрів криптосистеми повинен враховувати не тільки поточні, але й перспективні вимоги до рівня безпеки [7].

Розробка механізмів безпечного оновлення програмного забезпечення IoT пристроїв включає використання цифрових підписів для верифікації автентичності оновлень. Практика показує ефективність застосування схем групового підпису, які дозволяють оптимізувати процес перевірки автентичності для великої кількості пристроїв. Дослідження показників продуктивності різних криптографічних алгоритмів на типових IoT платформах демонструє відмінності в ефективності їх реалізації. Результати досліджень підтверджують, що симетричні алгоритми забезпечують вищу швидкодію при менших витратах ресурсів, тоді як асиметричні алгоритми надають необхідну функціональність для вирішення задач безпеки [8].

Застосування сучасних методів оптимізації криптографічних обчислень, таких як еліптичні криві Монтгомері та криві Едвардса, дозволяє значно підвищити ефективність асиметричного шифрування в IoT системах. Експериментальні дослідження демонструють можливість досягнення прийнятної продуктивності навіть на пристроях з обмеженими ресурсами [9].

Впровадження механізмів захисту від атак на криптографічні протоколи вимагає комплексного підходу до проектування систем безпеки. Необхідно враховувати можливості атак на побічні канали, часові атаки та інші види криптоаналізу. Практика показує ефективність застосування додаткових захисних механізмів, таких як рандомізація обчислень та маскування даних.

Перспективи розвитку криптографічних методів захисту в IoT системах пов'язані з впровадженням постквантових алгоритмів та розробкою нових протоколів безпеки. Дослідження показують необхідність завчасної підготовки до можливої появи квантових комп'ютерів, здатних зламати сучасні асиметричні криптосистеми. Розробка та стандартизація постквантових

алгоритмів створює основу для забезпечення довгострокової безпеки IoT систем.

Інтеграція криптографічних механізмів у протоколи зв'язку IoT вимагає ретельного балансування між рівнем захисту та ефективністю передачі даних. Експериментальні дослідження демонструють, що застосування полегшених версій протоколів TLS, спеціально оптимізованих для IoT пристроїв, дозволяє знизити накладні витрати на встановлення захищеного з'єднання до 30% порівняно зі стандартними реалізаціями (табл. 1.2) [10].

Таблиця 1.2 – Аналіз характеристик продуктивності

Алгоритм	Розмір блоку (біт)	Швидкість шифрування (Мбіт/с)	Енергоспоживання (мДж/блок)	Використання пам'яті (КБ)
AES-128	128	89.5	0.38	8.2
AES-256	256	65.3	0.52	12.4
ChaCha20	512	95.2	0.35	6.8
PRESENT	64	78.6	0.25	4.5
SIMON	128	82.4	0.31	5.6

Моніторинг продуктивності криптографічних операцій в реальних IoT системах показує критичну важливість оптимізації процесів управління ключами. Впровадження ієрархічних схем розподілу ключів дозволяє ефективно масштабувати систему безпеки при збільшенні кількості пристроїв. Практичні результати підтверджують зниження навантаження на центральний вузол розподілу ключів до 60% при використанні дворівневої ієрархії [11].

Проектування безпечних IoT систем потребує врахування специфіки різних класів пристроїв та їх обмежень. Результати тестування демонструють, що для пристроїв з батарейним живленням оптимальним є використання полегшених версій криптографічних алгоритмів. Використання спеціалізованих реалізацій AES-128 з оптимізованими S-блоками дозволяє знизити енергоспоживання на операції шифрування до 25% [12].

Розробка механізмів відновлення після компрометації ключів є критичним аспектом безпеки IoT систем. Дослідження показують ефективність застосування схем порогового розподілу секрету для забезпечення відмовостійкості системи управління ключами. Практична реалізація схеми Шаміра (t, n) для розподілу майстер-ключів демонструє можливість відновлення системи навіть при втраті частини ключових серверів [13].

Архітектура системи безпеки IoT повинна передбачати можливість гнучкого масштабування та адаптації до змін у структурі мережі. Експериментальні дослідження підтверджують ефективність використання децентралізованих протоколів узгодження ключів, які дозволяють автоматично встановлювати захищені з'єднання між новими пристроями без участі центрального сервера [14].

Методологія оцінки захищеності IoT систем включає аналіз стійкості криптографічних протоколів до різних типів атак. Практика показує необхідність проведення регулярного тестування на проникнення для виявлення потенційних вразливостей. Використання автоматизованих інструментів аналізу криптографічних протоколів дозволяє значно підвищити ефективність процесу верифікації безпеки.

Дослідження ефективності різних схем автентифікації в IoT системах демонструє перспективність використання полегшених протоколів на основі еліптичних кривих. Модифіковані версії протоколу ECDSA з оптимізованими параметрами кривих забезпечують достатній рівень безпеки при значно менших обчислювальних витратах порівняно з класичними реалізаціями [15].

Механізми захисту від атак на відмову в обслуговуванні повинні враховувати обмежені ресурси IoT пристроїв. Практичні результати показують ефективність застосування адаптивних схем автентифікації, які динамічно регулюють рівень захисту залежно від поточного навантаження на систему та виявлених загроз. Розробка стратегій оновлення криптографічних параметрів враховує життєвий цикл IoT пристроїв. Дослідження показують, що регулярне оновлення фізичних матеріалів та параметрів алгоритмів є критичним для підтримки належного рівня безпеки протягом терміну їх експлуатації [16].

Реалізація механізмів безпечного зберігання ключів в IoT пристроях вимагає використання спеціалізованих апаратних рішень. Експериментальні дослідження демонструють ефективність застосування захищених елементів пам'яті та криптографічних співпроцесорів для захисту критичних даних від несанкціонованого доступу.

Процес сертифікації криптографічних модулів IoT пристроїв потребує розробки спеціалізованих методик тестування. Практика показує необхідність врахування специфічних вимог до енергоефективності та продуктивності при проведенні сертифікаційних випробувань. Розробка стандартизованих процедур оцінки відповідності дозволяє забезпечити єдиний підхід до верифікації безпеки IoT систем. Методи прискорення криптографічних обчислень на базі спеціалізованих апаратних платформ демонструють значний потенціал для підвищення ефективності IoT систем. Використання програмовних логічних матриць (FPGA) для реалізації критичних криптографічних операцій дозволяє досягти оптимального балансу між продуктивністю та енергоспоживанням [17].

Розвиток технологій квантових обчислень створює нові виклики для безпеки IoT систем. Дослідження показують необхідність розробки гібридних криптосистем, які поєднують класичні та постквантові алгоритми для забезпечення довгострокової безпеки. Експериментальні реалізації демонструють можливість ефективного впровадження базових постквантових примітивів навіть на обмежених платформах IoT.

1.2. Полегшені криптографічні алгоритми для обмежених пристроїв IoT

Стрімкий розвиток інтернету речей призвів до необхідності розробки спеціалізованих криптографічних алгоритмів, оптимізованих для роботи на пристроях з обмеженими обчислювальними ресурсами. Технічні характеристики типових IoT пристроїв, наведені в таблиці 1.3, демонструють суттєві обмеження щодо доступної пам'яті та обчислювальної потужності.

Практична реалізація криптографічних механізмів захисту на таких обмежених платформах вимагає застосування спеціальних підходів до оптимізації як на алгоритмічному рівні, так і на рівні програмної реалізації.

Таблиця 1.3 – Технічні характеристики типових IoT пристроїв

Клас пристрою	Процесор	ОЗП (КБ)	Флеш-пам'ять (КБ)	Енергоспоживання (мВт)
Клас 0	8-bit	1-4	32-64	1-10
Клас 1	16-bit	4-16	64-128	15-30
Клас 2	32-bit	16-64	128-512	30-50

Дослідження показують, що класичні криптографічні алгоритми, розроблені для повнофункціональних обчислювальних систем, виявляються надто ресурсоємними для використання в IoT пристроях, що призводить до необхідності розробки нових, полегшених варіантів існуючих алгоритмів та створення принципово нових криптографічних примітивів, спеціально призначених для обмежених платформ [18].

Алгоритм AES, який став світовим стандартом симетричного шифрування, потребує значних модифікацій та оптимізації для ефективного впровадження в IoT пристроях. Базова структура AES, що включає операції SubBytes, ShiftRows, MixColumns та AddRoundKey, може бути оптимізована різними способами для зменшення вимог до ресурсів. Найбільш ефективними виявились методи оптимізації на основі попередніх обчислень та зберігання проміжних результатів, що дозволяє суттєво знизити обчислювальне навантаження за рахунок додаткового використання пам'яті. Експериментальні дослідження показують, що застосування техніки T-таблиць, де попередньо обчислені результати комбінацій операцій SubBytes та MixColumns зберігаються в пам'яті, дозволяє досягти значного прискорення шифрування. При цьому розмір T-таблиць може бути оптимізований шляхом зберігання лише критично необхідних значень та обчислення інших на льоту. Додаткові оптимізації включають використання спеціалізованих інструкцій процесора,

якщо такі доступні, та застосування технік розгортання циклів для зменшення накладних витрат на керування виконанням програми [19].

Алгоритм PRESENT представляє собою принципово новий підхід до проектування полегшених блокових шифрів, спеціально розроблений з урахуванням обмежень апаратної реалізації. Структура алгоритму базується на мережі SPN з оптимізованими S-блоками розміром 4 біти та простим шаром перестановок, що забезпечує мінімальні вимоги до апаратних ресурсів при збереженні достатнього рівня криптографічної стійкості. Порівняльний аналіз характеристик апаратних реалізацій різних полегшених алгоритмів, представлений у таблиці 1.4, демонструє суттєві переваги PRESENT щодо ефективності використання апаратних ресурсів.

Таблиця 1.4 – Порівняльний аналіз характеристик апаратних реалізацій алгоритмів

Алгоритм	Площа кристала (GE)	Пропускна здатність (Кбіт/с)	Енергія на блок (нДж)
AES-128	2400	57.1	8.15
PRESENT	1570	200.0	2.31
SPECK	1280	237.8	1.95
SIMON	1350	198.6	2.15

Архітектура алгоритму оптимізована для апаратної реалізації шляхом мінімізації складності логічних операцій та зменшення кількості необхідних регістрів. Використання малих S-блоків дозволяє реалізувати їх у вигляді простих логічних схем, а операція перестановки бітів може бути реалізована простим перепризначенням сигнальних ліній без додаткових логічних елементів. Процес генерації раундових ключів також оптимізований для мінімізації апаратних витрат та забезпечує достатній рівень дифузії ключового матеріалу [20].

Розробка алгоритмів SPECK та SIMON відбувалась з урахуванням необхідності оптимізації як для програмної, так і для апаратної реалізації.

SPECK, орієнтований на програмну реалізацію, використовує модифіковану структуру мережі Фейстеля з операціями додавання за модулем 2^n, циклічного зсуву та побітового XOR. Вибір цих операцій обґрунтований їх ефективною реалізацією на більшості процесорних архітектур, включаючи 8-бітні мікроконтролери. Особливістю алгоритму є використання двох різних значень для циклічних зсувів, що забезпечує кращі криптографічні властивості при збереженні високої ефективності реалізації. SIMON, оптимізований для апаратної реалізації, використовує подібну структуру, але з заміною операції модульного додавання на побітове AND, що суттєво спрощує апаратну реалізацію (табл. 1.5).

Таблиця 1.5 – Технічні характеристики програмних реалізацій алгоритмів

Алгоритм	Розмір коду (bit)	Використання ОЗП (bit)	Цикли на блок
AES-128	2160	256	1458
PRESENT	1886	432	1886
SPECK	1236	196	1096
SIMON	1348	216	1248

Технічні характеристики програмних реалізацій досліджуваних алгоритмів, наведені в таблиці 1.5, демонструють високу ефективність SPECK та SIMON на програмному рівні, особливо щодо розміру коду та використання оперативної пам'яті [21].

Реалізація механізмів захисту від атак на побічні канали для полегшених криптографічних алгоритмів вимагає особливого підходу через обмеженість доступних ресурсів. Класичні методи протидії атакам за споживанням потужності та часовим атакам, такі як маскування даних та вирівнювання часу виконання операцій, повинні бути адаптовані з урахуванням обмежень IoT пристроїв. Експериментальні дослідження показують ефективність застосування спрощених схем маскування, де критичні операції захищаються від аналізу побічних каналів при мінімальних додаткових витратах ресурсів. Додатково, застосування технік рандомізації порядку виконання операцій та

введення випадкових затримок дозволяє суттєво ускладнити проведення часових атак. Практична реалізація цих захисних механізмів вимагає ретельного балансування між рівнем захисту та додатковими витратами ресурсів, що особливо критично для пристроїв з батарейним живленням [22].

Методологія оцінки криптографічної стійкості полегшених алгоритмів шифрування вимагає комплексного підходу до аналізу можливих векторів атак. Результати криптоаналізу показують, що PRESENT з 80-бітним ключем забезпечує рівень безпеки, достатній для більшості застосувань в IoT системах. Найкращі відомі атаки на повну версію алгоритму мають складність, що перевищує повний перебір ключа. Диференціальний та лінійний криптоаналіз PRESENT демонструє стійкість алгоритму до класичних методів криптоаналізу, що підтверджується відсутністю практично реалізованих атак після тривалого періоду дослідження спільнотою криптоаналітиків. Аналогічні дослідження алгоритмів SPECK та SIMON також підтверджують їх стійкість до відомих методів криптоаналізу, хоча деякі варіанти цих алгоритмів з меншою кількістю раундів можуть бути вразливими до специфічних атак. Експериментальні результати демонструють, що вибір кількості раундів для цих алгоритмів забезпечує достатній запас міцності для протистояння потенційним атакам, які можуть бути розроблені в майбутньому [23].

Розробка ефективних протоколів розподілу ключів для полегшених криптографічних алгоритмів становить окрему проблему в контексті IoT систем. Обмеження обчислювальних ресурсів та енергоспоживання унеможливлюють використання традиційних протоколів узгодження ключів на основі асиметричної криптографії. Практичні дослідження демонструють ефективність гібридних схем, де початкове розгортання ключового матеріалу здійснюється через захищений фізичний канал або під час виробництва пристроїв, а подальше оновлення ключів відбувається з використанням полегшених протоколів на основі симетричної криптографії.

Такий підхід дозволяє мінімізувати обчислювальні витрати на управління ключами при збереженні необхідного рівня безпеки. Додатково, використання ієрархічних схем розподілу ключів, де пристрої групуються за

функціональними або географічними ознаками, дозволяє оптимізувати процес оновлення ключового матеріалу та знизити навантаження на центральні вузли управління ключами [24].

Процес інтеграції полегшених криптографічних алгоритмів у програмне забезпечення IoT пристроїв вимагає розробки спеціалізованих програмних інтерфейсів та бібліотек. Експериментальні дослідження показують, що використання уніфікованих інтерфейсів для різних алгоритмів суттєво спрощує процес розробки та підтримки програмного забезпечення. Розробка оптимізованих бібліотек для конкретних апаратних платформ дозволяє максимально ефективно використовувати доступні ресурси та забезпечити необхідну продуктивність криптографічних операцій. Важливим аспектом є також забезпечення можливості динамічної зміни параметрів алгоритмів та режимів роботи в залежності від поточних вимог до безпеки та доступних ресурсів. Реалізація механізмів моніторингу продуктивності та автоматичної адаптації параметрів криптографічних алгоритмів дозволяє оптимізувати використання ресурсів в реальному часі [25].

Методи оптимізації енергоспоживання при виконанні криптографічних операцій набувають критичного значення для пристроїв з батарейним живленням. Експериментальні дослідження демонструють можливість значного зниження енергоспоживання шляхом застосування комплексу оптимізаційних технік на різних рівнях реалізації. На апаратному рівні ефективним є використання режимів зниженого енергоспоживання процесора між криптографічними операціями та оптимізація частоти роботи відповідно до поточного навантаження. На алгоритмічному рівні можливе застосування адаптивних схем, де складність криптографічних операцій змінюється в залежності від вимог до безпеки та доступного заряду батареї. Додатково, використання технік кешування та попередніх обчислень дозволяє знизити кількість енергоємних операцій за рахунок додаткового використання пам'яті, що особливо ефективно для пристроїв з обмеженим енергоспоживанням [26].

Перспективи подальшого розвитку полегшених криптографічних алгоритмів пов'язані з декількома напрямками досліджень. Розробка нових

архітектурних рішень, що дозволяють ще більше знизити вимоги до ресурсів при збереженні необхідного рівня безпеки, залишається актуальним завданням.

Дослідження показують перспективність використання гібридних підходів, що поєднують переваги різних криптографічних примітивів. Розвиток технологій виробництва мікроелектроніки та поява нових обчислювальних платформ створюють можливості для розробки спеціалізованих апаратних прискорювачів, оптимізованих для виконання криптографічних операцій. Додатково, зростання загроз з боку квантових обчислень стимулює дослідження в області постквантових полегшених криптографічних алгоритмів, здатних забезпечити захист від атак з використанням квантових комп'ютерів при збереженні прийнятних вимог до ресурсів [27].

1.3 Методи обміну ключами та протоколи захисту комунікацій в IoT

Розвиток Інтернету речей створює нові виклики для інформаційної безпеки, оскільки величезна кількість пристроїв обмінюється чутливими даними через незахищені мережі. Проблема захисту комунікацій між пристроями IoT стає критично важливою для забезпечення конфіденційності та цілісності даних. Методи обміну криптографічними ключами та протоколи захисту відіграють ключову роль у побудові безпечної інфраструктури IoT.

Розглядаючи специфіку IoT пристроїв, необхідно враховувати їх обмежені обчислювальні ресурси та енергоспоживання. Традиційні криптографічні методи часто виявляються занадто ресурсомісткими для застосування в IoT середовищі. Це спонукає до розробки легких криптографічних протоколів, які забезпечують достатній рівень безпеки при мінімальних витратах ресурсів.

Протокол Діффі-Хеллмана (DH) залишається одним з фундаментальних методів обміну ключами, який знаходить застосування в IoT системах. Його модифікації, зокрема еліптична криптографія (ECDH), дозволяють значно

зменшити обчислювальне навантаження при збереженні криптографічної стійкості (табл. 1.6).

Таблиця 1.6 – Порівняння довжин ключів для різних методів обміну

Метод	Довжина ключа (біт)	Рівень безпеки (біт)
DH	3072	128
ECDH	256	128
NTRU	2048	128

Як показано в таблиці 1.6, ECDH забезпечує аналогічний рівень безпеки при менших розмірах ключів порівняно з класичним DH [28].

На практиці протоколи захисту в IoT повинні забезпечувати не лише конфіденційність даних, але й автентифікацію пристроїв та захист від атак типу "людина посередині". Протокол TLS 1.3 пропонує комплексне рішення для захисту комунікацій, включаючи взаємну автентифікацію та узгодження ключів. Його полегшена версія DTLS адаптована для роботи через ненадійні транспортні протоколи, що характерно для IoT мереж [28].

Дослідження показують, що впровадження криптографічних протоколів в IoT системах стикається з низкою технічних викликів. Обмежена пропускна здатність мережі та затримки при передачі даних можуть суттєво впливати на ефективність протоколів захисту. В таблиці 1.7 наведено порівняльний аналіз основних протоколів за ключовими характеристиками.

Впровадження квантово-стійких алгоритмів стає актуальним напрямком розвитку методів захисту IoT комунікацій. Решіткові криптосистеми, такі як NTRU, розглядаються як перспективні кандидати для постквантової криптографії в IoT середовищі. Їх головною перевагою є висока обчислювальна ефективність порівняно з традиційними асиметричними алгоритмами [29].

Таблиця 1.7– Характеристики протоколів захисту для IoT

Протокол	Накладні витрати	Енергоспоживання	Стійкість до атак
TLS 1.3	Середні	Високе	Висока
DTLS	Низькі	Середнє	Висока
MQTT-TLS	Низькі	Низьке	Середня

Протоколи групового обміну ключами набувають особливого значення в контексті IoT, де множина пристроїв повинна встановлювати захищені з'єднання одночасно. Механізми broadcast-шифрування дозволяють ефективно розповсюджувати ключовий матеріал серед великої кількості пристроїв при мінімальних накладних витратах.

Програмна реалізація криптографічних протоколів в IoT системах вимагає ретельної оптимізації та врахування специфіки цільових платформ. Використання спеціалізованих бібліотек та апаратних модулів безпеки дозволяє досягти прийнятної продуктивності навіть на обмежених пристроях, а вбудовані криптографічні акселератори стають стандартним компонентом сучасних IoT чіпсетів.

Забезпечення масштабованості системи управління ключами є критичним фактором для великих IoT мереж. Централізовані схеми розподілу ключів можуть створювати вузькі місця та єдині точки відмови. Децентралізовані протоколи на основі технології блокчейн пропонують альтернативний підхід до управління криптографічними ключами в IoT середовищі.

Методи легкої криптографії активно розвиваються для задоволення специфічних вимог IoT пристроїв. Симетричні блочні шифри, такі як PRESENT та CLEFIA, оптимізовані для апаратної реалізації та забезпечують прийнятний рівень безпеки при мінімальному споживанні ресурсів. Потокові шифри знаходять широке застосування в IoT завдяки їх високій швидкодії [30].

Протоколи автентифікації в IoT повинні забезпечувати надійну перевірку ідентичності пристроїв з урахуванням можливих атак. Механізми взаємної автентифікації на основі відкритих ключів дозволяють встановлювати довірені з'єднання між пристроями без необхідності попереднього розподілу секретних

ключів. Аналіз вразливостей та атак на протоколи захисту IoT комунікацій показує важливість комплексного підходу до безпеки. Сучасні методи криптоаналізу дозволяють виявляти потенційні слабкості в протоколах та своєчасно вносити необхідні корективи. Формальна верифікація протоколів стає невід'ємною частиною процесу їх розробки та впровадження.

Стандартизація протоколів безпеки для IoT залишається важливим напрямком роботи міжнародних організацій. Розробка та прийняття єдиних стандартів сприяє забезпеченню сумісності різних IoT платформ та спрощує процес інтеграції систем безпеки. Регулярне оновлення стандартів дозволяє враховувати нові загрози та вимоги до безпеки [30]. З розвитком технологій з'являються нові виклики для безпеки IoT комунікацій.

Атаки з використанням квантових комп'ютерів, експлуатація вразливостей в протоколах та апаратних реалізаціях вимагають постійного вдосконалення методів захисту. Дослідження в галузі постквантової криптографії та розробка нових протоколів продовжують залишатися актуальними напрямками. Експериментальні дослідження показують, що вибір оптимального набору криптографічних примітивів та протоколів значно впливає на загальну продуктивність IoT системи. Результати тестування різних конфігурацій безпеки на реальних пристроях дозволяють визначити найбільш ефективні рішення для конкретних сценаріїв застосування.

1.4. Стандарти безпеки в IoT

Розробка та впровадження стандартів безпеки для Інтернету речей являє собою складний багаторівневий процес, який координується провідними міжнародними організаціями. Стандартизація охоплює широкий спектр технічних аспектів: від фізичного рівня безпеки до прикладних протоколів та архітектурних рішень. Аналіз існуючих стандартів демонструє різноманітність підходів до забезпечення безпеки IoT систем.

Міжнародна організація зі стандартизації (ISO) розробила серію стандартів ISO/IEC 27001, які встановлюють базові вимоги до систем управління інформаційною безпекою. Специфічні вимоги для IoT систем викладені в стандарті ISO/IEC 27402, який визначає методологію оцінки ризиків та впровадження заходів безпеки. Як показано в таблиці 1.8, стандарти ISO охоплюють різні аспекти безпеки IoT систем [32].

Таблиця 1.8 – Стандарти ISO для безпеки IoT

Стандарт	Область застосування	Ключові вимоги
ISO/IEC 27001	Загальна безпека	Управління ризиками
ISO/IEC 27402	IoT безпека	Специфічні контролі
ISO/IEC 29192	Легка криптографія	Енергоефективність
ISO/IEC 30141	IoT архітектура	Референсна модель

Європейський інститут телекомунікаційних стандартів розробив набір специфікацій для IoT безпеки. Стандарт ETSI TS 103 645 визначає вимоги до споживчих IoT пристроїв, включаючи механізми автентифікації, оновлення програмного забезпечення та захисту даних. Методологія оцінки відповідності, представлена в ETSI, дозволяє проводити верифікацію безпеки IoT рішень [15].

Національний інститут стандартів і технологій США опублікував серію рекомендацій щодо безпеки IoT систем. Документ NIST SP 800-183 представляє концептуальну модель IoT та визначає основні компоненти безпеки [21].

Технічна реалізація стандартів безпеки вимагає врахування специфіки різних класів IoT пристроїв. В таблиці 1.9 наведено порівняльний аналіз вимог стандартів для різних категорій пристроїв, що демонструє диференційований підхід до забезпечення безпеки.

Інститут інженерів електротехніки та електроніки розробив стандарт IEEE 2413, який визначає архітектурну структуру для IoT систем.

Таблиця 1.9 − Порівняльний аналіз вимог стандартів для різних категорій пристроїв

Клас пристроїв	Критичність	Рівень захисту	Основні стандарти
Промислові	Висока	Максимальний	IEC 62443, NIST SP 800-82
Споживчі	Середня	Базовий	ETSI EN 303 645
Медичні	Висока	Розширений	ISO 80001, FDA guidance
Транспортні	Висока	Максимальний	ISO 26262, SAE J3061

Документ описує механізми безпеки на різних рівнях архітектури та встановлює вимоги до взаємодії компонентів. Стандарт IEEE 1363 визначає специфікації для криптографічних алгоритмів, які можуть застосовуватися в IoT пристроях [11].

Механізми криптографічного захисту, визначені в стандартах, повинні враховувати обмеження IoT пристроїв щодо обчислювальних ресурсів та енергоспоживання. Стандарт ISO/IEC 29192 специфікує алгоритми легкої криптографії, оптимізовані для використання в обмежених середовищах. Реалізація цих алгоритмів дозволяє забезпечити необхідний рівень безпеки при мінімальних витратах ресурсів [14].

Протоколи комунікації в IoT системах повинні відповідати вимогам стандартів щодо конфіденційності та цілісності даних. Стандарт ETSI TS 103 858 визначає механізми захисту для протоколів прикладного рівня, включаючи MQTT та CoAP. Специфікації IEEE 802.15.4 встановлюють вимоги до безпеки на фізичному та канальному рівнях для бездротових сенсорних мереж [15].

Методологія оцінки відповідності стандартам безпеки передбачає проведення тестування IoT систем. NIST розробив набір сценаріїв та метрик для верифікації механізмів захисту. Процес сертифікації згідно з ISO/IEC 27001 включає регулярний аудит та оновлення системи управління безпекою [17].

Аналіз вразливостей та загроз для IoT систем є важливою складовою процесу стандартизації. ETSI публікує регулярні звіти про виявлені вразливості та рекомендації щодо їх усунення. База даних CVE, підтримувана MITRE,

містить структуровану інформацію про відомі вразливості в IoT продуктах та їх відповідність стандартам безпеки [18].

Процес гармонізації стандартів між різними організаціями сприяє створенню єдиного підходу до безпеки IoT. Спільні робочі групи ISO/IEC JTC 1 координують розробку взаємопов'язаних стандартів та забезпечують їх узгодженість. Міжнародне співробітництво дозволяє враховувати регіональні особливості та вимоги при розробці глобальних стандартів [12].

Впровадження стандартів безпеки в промислових IoT системах вимагає особливої уваги через високі ризики та потенційні наслідки порушень безпеки. IEC 62443 встановлює специфічні вимоги для промислових систем управління та визначає рівні безпеки для різних компонентів. Методологія оцінки ризиків, представлена в стандарті, дозволяє визначити необхідні заходи захисту [23].

Експериментальні дослідження показують практичну застосовність стандартів безпеки в реальних IoT системах. Тестування конфігурацій безпеки, проведене відповідно до вимог стандартів, дозволяє оцінити їх ефективність та визначити оптимальні рішення для конкретних застосувань. Результати досліджень використовуються для вдосконалення та оновлення стандартів.

2 ТЕОРЕТИЧНІ ОСНОВИ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ

2.1. Визначення та класифікація систем виявлення вторгнень

Першу концепцію систем виявлення вторгнень виклав у 1980 році Джеймс Андерсон з АНБ у своєму звіті "Моніторинг і спостереження за загрозами комп'ютерній безпеці". Потім, у 1986 році, Дороті Деннінг написала "Модель виявлення вторгнень" - наукову статтю, яка стала основою для багатьох систем, що використовуються і сьогодні [25]. Модель, представлена в роботі, була використана для розробки експертної системи виявлення вторгнень.

Модель IDES виявляє моделі поведінки потенційного зловмисника, використовуючи статистику для виявлення аномалій на основі профілів користувачів, хост-систем і цільових систем. З 1980-х і до початку 2000-х років IDS вважалися найкращою практикою безпеки. Але в той час галаслива і турбулентна природа мереж призводила до багатьох хибних спрацьовувань IDS, що робило їх ненадійними в очах багатьох людей. Однак в останні роки їх домінування і проблеми хмарних обчислень пролили нове світло на системи виявлення вторгнень, які вже давно стали основою корпоративної безпеки. І хоча багато організацій інвестують в проактивні заходи безпеки та інші превентивні стратегії, вони все одно можуть зазнати невдачі. Виявлення атак, які можуть статися після цього, залишається критично важливим.

Термін IDS відноситься до процесів, що використовуються для виявлення несанкціонованого доступу до мережі та зловмисних дій в мережі. Таким чином, IDS система - це інструмент, який відстежує мережевий трафік на предмет потенційних вторгнень, які можуть свідчити про зловмисну діяльність або порушення політик. Вторгнення в цьому сенсі можна визначити як будь-який тип несанкціонованого доступу, що може завдати шкоди конфіденційності, цілісності та доступності даних. IDS видає попередження при виявленні такої активності, які потім або повідомляються адміністратору, або збираються за допомогою системи управління інформацією та подіями безпеки (SIEM) [26].

IDS часто порівнюють і плутають з брандмауером, але IDS не сидить на периметрі мережі і не відстежує трафік з метою визначення того, що має бути допущено в мережу, як це робить брандмауер. В ідеалі IDS розміщується в стратегічних точках мережі, де він відстежує і аналізує трафік до і з кінцевих точок мережі, щоб виявити будь-яку шкідливу активність. Це дозволяє IDS діяти як другий рівень безпеки, якщо загроза проникає через брандмауер, а також у випадках загроз, які виникли всередині мережі. Хорошою аналогією буде уявити брандмауер як вхідні двері вашого будинку, що дозволяють або блокують вхід і вихід, а IDS - як камеру безпеки, що спостерігає за дверима. Важливо також розрізняти IDS і IPS, або системи запобігання вторгненням. У той час як IDS займається інформативним і реактивним виявленням вторгнень, IPS є превентивним заходом, який запобігає загрозам до того, як вони потраплять в мережу.

Системи виявлення вторгнень бувають різних варіацій і можуть виявляти підозрілу активність за допомогою різних методів і можливостей. Зазвичай, різні різновиди IDS можна класифікувати за п'ятьма типами (рис. 2.1).

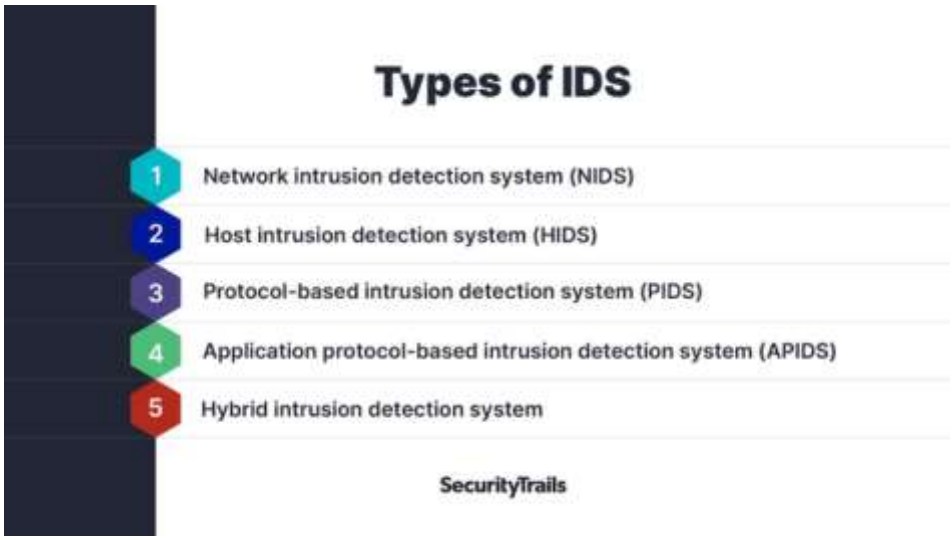

Рисунок 2.1 – Типи систем виявлення вторгнень

Система виявлення мережевих вторгнень (NIDS) встановлюється по всій мережі, в тактичних точках, де вона відстежує вхідний і вихідний трафік на всі пристрої в мережі. Вона досліджує трафік і порівнює його з індикаторами

відомих атак. При виявленні аномальної активності генерується сповіщення для подальшого вивчення інциденту.

Система виявлення вторгнень на основі протоколів (PIDS) зазвичай розгортається на веб-сервері і використовується для моніторингу та аналізу зв'язку між пристроями в мережі та онлайн-ресурсами, оскільки вона сканує дані, що передаються через HTTP/HTTPS.

Система виявлення вторгнень на основі прикладних протоколів (APIDS) контролює зв'язок між користувачами та додатками. Вона відстежує пакети, що передаються за специфічними для додатків протоколами, і ідентифікує інструкції, відстежуючи їх до окремих користувачів.

Гібридна система виявлення вторгнень визначається саме так, як випливає з її назви: це комбінація двох або більше типів IDS. У гібридному типі об'єднуються можливості двох систем – наприклад, хост- і мережевих IDS, що робить його більш ефективним, ніж будь-який окремий тип IDS.

Системи виявлення вторгнень також поділяються на активні та пасивні:

1. Активна IDS також відома як система виявлення та запобігання вторгнень (IDPS). Вона не тільки налаштована на моніторинг трафіку та виявлення аномальної поведінки, але й автоматично блокує будь-які підозрювані атаки, блокуючи IP-адреси або обмежуючи доступ до важливих ресурсів без участі адміністратора.

2. Пасивна IDS лише відстежує та аналізує мережевий трафік і сповіщає адміністратора про потенційну атаку. Він не має можливості самостійно здійснювати блокування або превентивні дії.

IDS виявляє підозрілу активність за допомогою двох методів.

1. Система виявлення вторгнень на основі сигнатур (SIDS), також відома як IDS, заснована на знаннях, виявляє активні інструкції шляхом моніторингу пакетів, що проходять через мережу, і порівняння їх з базою даних відомих вразливостей системи та їх атрибутів. SIDS шукають певні шаблони, такі як кількість байт або відомі послідовності шкідливих інструкцій, а виявлені шаблони (щось, що походить від антивірусного програмного забезпечення) називаються сигнатурами. Оскільки IDS можуть виявляти лише відомі атаки,

важливо постійно оновлювати сигнатури, але це все одно не забезпечить захист від загроз «нульового дня».

2. Система виявлення вторгнень на основі аномалій (AIDS) – або поведінкова система – була створена, щоб заповнити прогалини, залишені SIDS, і представити новішу технологію, яка виявляє невідомі атаки, щоб не відставати від швидкості, з якою розробляються нові шкідливі програми та загрози. Замість моніторингу мережевого трафіку і порівняння його з базою даних відомих атак, AIDS встановлює базовий рівень нормальної і надійної мережевої активності і порівнює його з трафіком для виявлення аномалій.

Хоча в порівнянні з IDS на основі сигнатур вони можуть адаптуватися до мінливого внутрішнього IT-ландшафту і зовнішніх загроз, вони можуть страждати від своїх власних проблем. Ці проблеми проявляються у вигляді хибних спрацьовувань: випадкове віднесення невідомої та легітимної активності до зловмисної, що призводить до марних витрат часу та ресурсів, виділених на її розслідування.

Щодня розробляються нові технології та шкідливе програмне забезпечення для проникнення в системи та мережі, отримання, крадіжки та витоку конфіденційної інформації, а кіберзлочинці постійно знаходять нові способи подолання наших захисних систем. Ось чому впровадження IDS є важливою і фундаментальною частиною будь-якої ефективної інфраструктури безпеки.

Поєднання різних типів IDS і різних методів виявлення може дозволити їй розвиватися разом з IT-середовищем, яке вона контролює, а також загрозами і атаками, що підстерігають ззовні. IDS мають ряд очевидних переваг.

− Виявлення ризиків безпеки. Інструмент IDS, виявляючи вторгнення та інциденти безпеки, може допомогти вам зрозуміти ризики безпеки, з якими стикається ваша організація, а також їх кількість і рівень складності. Він також може виявити проблеми з конфігурацією мережевих пристроїв і надати цінні показники, які можуть бути використані для подальшого інформування політики реагування на інциденти.

− Вдосконалення засобів контролю безпеки. Підтримувати здоровий рівень знань і розуміння ризиків кібербезпеки необхідно для створення і вдосконалення політик і стратегій кібербезпеки, які розвиваються в міру зміни ландшафту загроз. Аналіз кількості та типів атак, з якими стикається ваша організація, може допомогти їй впровадити більш ефективні засоби контролю безпеки та ефективніше запобігати майбутнім атакам.

− Відповідність нормативним вимогам. Оскільки кількість нормативних політик, яким повинні відповідати організації, зростає, причому в широкому спектрі галузей, наявність інструменту, який розширює можливості та спрощує процес дотримання цих норм, має вирішальне значення. IDS можуть допомогти, забезпечуючи прозорість мережі, створюючи і зберігаючи журнали, які є важливою частиною будь-якої документації, що ведеться для аудиту відповідності.

− Покращення часу реагування. Хоча ми вже згадували, що рішення IDS можуть бути використані для покращення практики реагування на інциденти, важливо також підкреслити їхню здатність збільшувати час реагування на інциденти безпеки. Система IDS не тільки негайно генерує сповіщення, коли виявляє аномальну поведінку під час моніторингу мережевих пакетів на хостах і пристроях, але й може перевіряти інформацію в цих пакетах, збираючи цінні дані ефективно і швидко [26].

2.2. Ключові принципи роботи IDS

IDS використовує різні методи виявлення потенційних загроз.

− Виявлення на основі сигнатур метод який спирається на базу даних відомих сигнатур або шаблонів атак. IDS порівнює вхідний мережевий трафік або дії системи з цими сигнатурами для виявлення відомих атак. Хоча виявлення на основі сигнатур є ефективним проти відомих загроз, воно може бути неефективним при виявленні нових атак або атак нульового дня.

− Виявлення аномалій передбачає встановлення базової лінії нормальної поведінки мережі або системи, а потім виявлення відхилень від цієї базової

лінії. Система аналізує шаблони трафіку, продуктивність системи, поведінку користувачів та інші показники, щоб виявити аномалії, які можуть свідчити про потенційне порушення безпеки.

Коли IDS виявляє вторгнення або підозрілу активність, вона генерує попередження або сповіщення для адміністраторів безпеки. Ці сповіщення містять інформацію про характер інциденту, уражену систему або мережу, а також будь-які додаткові деталі, які допоможуть у процесі реагування та мінімізації наслідків інциденту.

Важливо зазначити, що IDS не є самостійним рішенням, а працює в поєднанні з іншими заходами безпеки, такими як брандмауери, антивірусне програмне забезпечення та політики безпеки. Крім того, системи запобігання вторгненням (IPS) часто використовуються разом з IDS, щоб не тільки виявляти, але й активно блокувати або запобігати виявленим загрозам. Таким чином, IDS системи відіграють вирішальну роль у виявленні та реагуванні на потенційні інциденти безпеки в режимі реального часу. Відстежуючи мережеву та системну активність, IDS допомагає організаціям посилити загальний рівень безпеки та мінімізувати потенційний вплив кіберзагроз [26]. На рисунку 2.2 наведено методи виявлення аномалій з їхніми перевагами та недоліками.

Статистичні підходи для виявлення аномалій. Статистичні підходи широко використовуються для виявлення аномалій в IDS. Ці методи передбачають використання статистичних методів для встановлення базових значень нормальної поведінки та виявлення відхилень від цих базових значень. Алгоритми виявлення відхилень, такі як метод статистичного виявлення відхилень або метод Z-рахунку, використовуються для виявлення точок даних, які значно відхиляються від очікуваної поведінки.

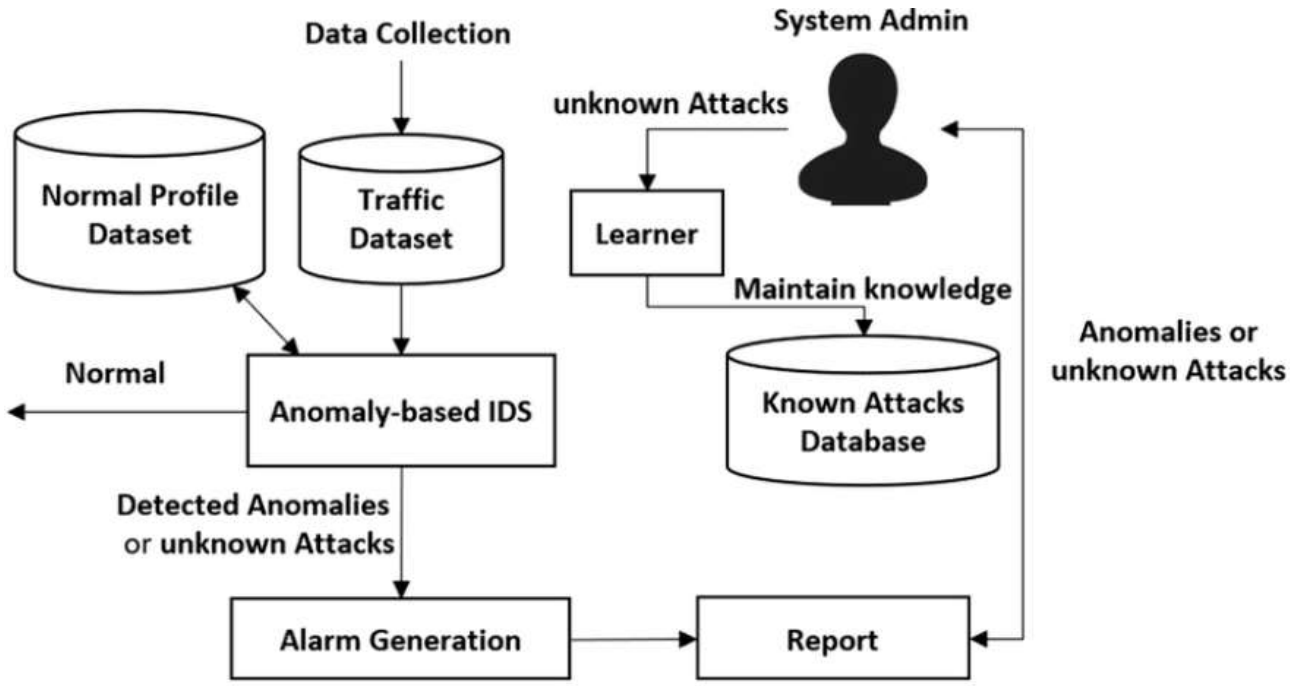

Рисунок 2.2 – Схема роботи виявлення аномалій

Методи аналізу часових рядів, такі як моделі авторегресійного інтегрованого ковзного середнього, використовуються для виявлення аномалій у часових даних. Підходи статистичного моделювання, такі як моделі гауссової суміші або приховані марковські моделі, використовуються для фіксації статистичних характеристик нормальної поведінки та виявлення аномалій на основі відхилень від вивчених моделей.

Підходи машинного навчання для виявлення аномалій. Алгоритми машинного навчання відіграють вирішальну роль у виявленні аномалій для IDS. Ці алгоритми можуть вивчати шаблони і поведінку з історичних даних і застосовувати ці знання для виявлення аномалій в режимі реального часу. Алгоритми кластеризації, такі як k-середні або DBSCAN, групують схожі екземпляри разом і позначають екземпляри, які не вписуються в жодний кластер, як аномалії. Алгоритми класифікації, такі як машини опорних векторів (SVM) або випадкові ліси, навчаються на основі маркованих даних, щоб класифікувати екземпляри як нормальні або аномальні. Нейронні мережі, включаючи моделі глибокого навчання, такі як згорткові нейронні мережі (CNN) або рекурентні нейронні мережі (RNN) [27], можуть фіксувати складні

патерни і взаємозв'язки для виявлення аномалій. На рисунку 2.3 показано підходи до машинного навчання в IDS.

Виявлення на основі сигнатур, також відоме як виявлення на основі правил, покладається на заздалегідь визначені сигнатури або шаблони відомих атак для виявлення вторгнень. Однак виявлення на основі сигнатур має обмеження, оскільки воно може виявляти лише відомі атаки, для яких були визначені сигнатури.

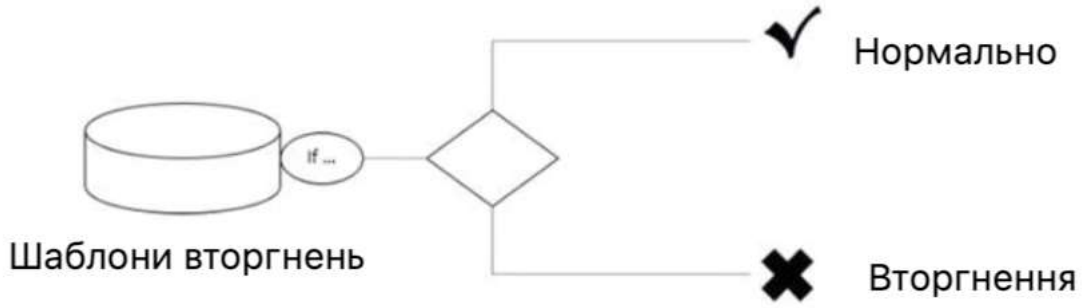

Рисунок 2.3 – Концепція IDS на основі підпису

Нові або невідомі атаки можуть легко вислизнути від сигнатурного виявлення. Методи виявлення аномалій, з іншого боку, зосереджені на виявленні відхилень від нормальної поведінки, не покладаючись на заздалегідь визначені сигнатури. Це робить виявлення аномалій більш ефективним при виявленні невідомих або нових атак, які не мають специфічних сигнатур. На рисунку 2.3 показано концепцію IDS на основі сигнатур.

Виявлення на основі сигнатур, як правило, найкраще підходить для виявлення відомих загроз. Він працює за допомогою попередньо запрограмованого списку відомих загроз та їхніх індикаторів компрометації (IOK). Індикатором може бути певна поведінка, яка зазвичай передує зловмисній мережевій атаці, хеші файлів, зловмисні домени, відомі послідовності байт або навіть вміст заголовків тем електронних листів.

Оскільки системи виявлення вторгнень на основі сигнатур відстежують пакети, що проходять через мережу, вони порівнюють ці пакети з базою даних

відомих IOC або сигнатур атак, щоб відмітити будь-яку підозрілу поведінку. З іншого боку, системи виявлення вторгнень на основі аномалій можуть попередити вас про підозрілу поведінку, яка невідома. Замість того, щоб шукати відомі загрози, система виявлення на основі аномалій використовує машинне навчання, щоб навчити систему розпізнавати нормалізовану базову лінію. Базовий рівень показує, як система зазвичай поводиться, а потім вся мережева активність порівнюється з цим базовим рівнем. Замість того, щоб шукати відомі IOC, IDS на основі аномалій просто ідентифікує будь-яку незвичну поведінку, щоб викликати оповіщення.

З розвитком різноманітних атак дві класичні IDS, згадані вище, не можуть ефективно захищати наші інформаційні системи. Були запропоновані нові методи комбінування різних систем виявлення вторгнень для підвищення їх ефективності. Дослідження показали, що комбіновані алгоритми працюють краще, ніж окремі алгоритми [28].

Метою гібридних систем виявлення вторгнень є поєднання декількох моделей виявлення для досягнення кращих результатів. Гібридна система виявлення вторгнень складається з двох компонентів. Перший компонент обробляє несекретні дані. Другий компонент приймає оброблені дані і сканує їх, щоб виявити активність вторгнення. Гібридні системи виявлення вторгнень засновані на поєднанні двох алгоритмів. Кожен алгоритм навчання має унікальні особливості, які допомагають підвищити продуктивність гібридної системи. Гібридні СППР можна поділити на каскадні гібридні, гібридні на інтегрованій основі та гібридні на основі кластерів і одиночних СППР.

Гібридні підходи поєднують в собі як статистичні методи, так і методи машинного навчання для підвищення точності та ефективності виявлення аномалій в IDS. Використовуючи сильні сторони різних підходів, гібридні моделі можуть забезпечити розширені можливості виявлення. Наприклад, гібридний підхід може використовувати статистичні методи для визначення базової поведінки та алгоритми машинного навчання для класифікації випадків як нормальних або аномальних. Така комбінація дозволяє створити більш комплексну та надійну систему виявлення аномалій (рис. 2.4).

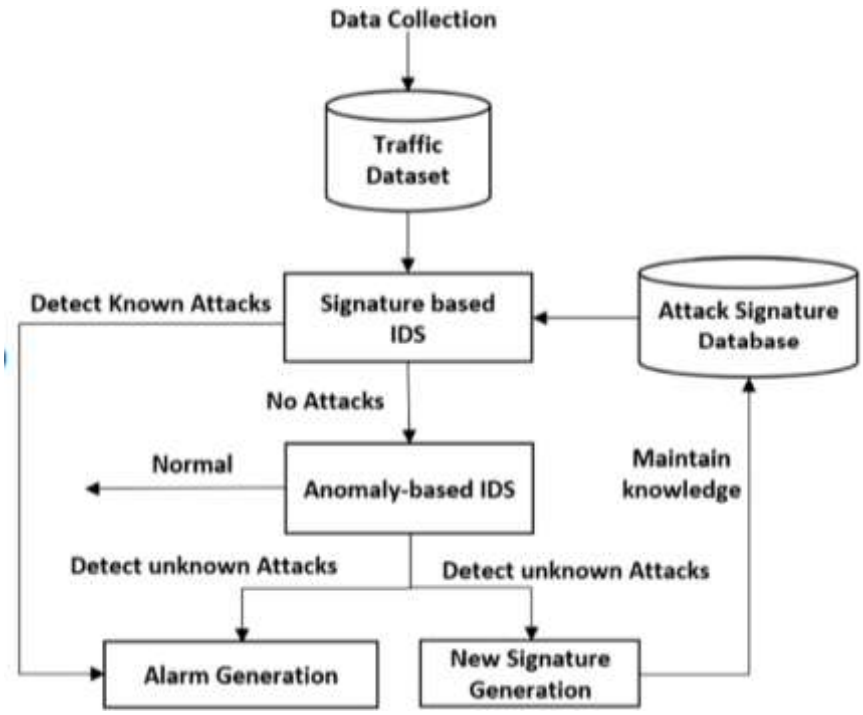

Рисунок 2.4 - Гібридна система виявлення вторгнень

Моделлю, яка часто використовується є гібридна система виявлення вторгнень на основі компонентів виявлення сигнатур та аномалій. На першому етапі моделі застосовувався компонент виявлення зловживань для виявлення відомих атак на основі захоплених шаблонів. Цей компонент базувався на алгоритмі дерева рішень. Другий етап складався з компонента виявлення аномалій, який використовував недоліки компонента виявлення зловживань. Для розробки другого компонента моделі було використано декілька однокласних алгоритмів SVM. Продуктивність моделі було протестовано за допомогою набору даних KDD Cup 99. Модель показала кращі результати, ніж один традиційний IDS.

Дослідники об'єднують методи виділення ознак і класифікації, щоб підвищити рівень виявлення і водночас знизити рівень хибних спрацьовувань. На першому етапі гібриду для виділення ознак використовувався метод хі-квадрат. Метою цього етапу було зменшити кількість ознак у наборі даних, але зберегти важливі ознаки, які фіксують атаки. На другому етапі для класифікації використовувався алгоритм багатокласової машини опорних векторів (SVM). Багатокласова машина опорних векторів була використана в цій моделі для

покращення швидкості класифікації. Модель було оцінено за допомогою набору даних NSL-KDD, і результати показали, що модель демонструє високий рівень виявлення з низьким рівнем хибних спрацьовувань.

2.3 Особливості застосування IDS в контексті Інтернету Речей

Інтернет речей - це динамічна екосистема, що складається з розумних пристроїв різних можливостей і розмірів, пов'язаних між собою через інтернет. Ці пристрої автономно збирають та обмінюються даними і приймають рішення на основі зібраної інформації. Екосистема побудована на декількох основних компонентах: пристроях, датчиках, виконавчих механізмах, варіантах підключення, блоках обробки даних, хмарній інфраструктурі, а також різних додатках і сервісах. Сфера застосування Інтернету речей розширюється і виходить за рамки простого зв'язку між машинами, і, незважаючи на різні цілі додатків і сервісів Інтернету речей, вони мають фундаментальну схожість. Зокрема, очікується, що кожен підключений інтелектуальний пристрій повинен підтримувати функціональність, пов'язану з кожним архітектурним рівнем IoT, щоб ефективно функціонувати в IoT.

Архітектура Інтернету речей забезпечує структуровану основу, яка описує взаємодію і зв'язок пристроїв і систем Інтернету речей через Інтернет, яка може бути адаптована до конкретних додатків, доменів і сценаріїв використання. В даний час не існує загальноприйнятої еталонної архітектури для IoT, і розробка такого стандарту є складним завданням, незважаючи на постійні зусилля в напрямку стандартизації. Більше того, з часом були запропоновані різні архітектури IoT, включаючи тришарові, чотиришарові, п'ятишарові та семишарові моделі. Як правило, типова чотирирівнева архітектура IoT складається з чотирьох основних рівнів: рівня сприйняття / зондування, мережевого рівня, рівня обробки даних і прикладного рівня, як показано на рисунку 2.5, де кожен рівень виконує певні функції для реалізації колективних цілей екосистеми IoT.

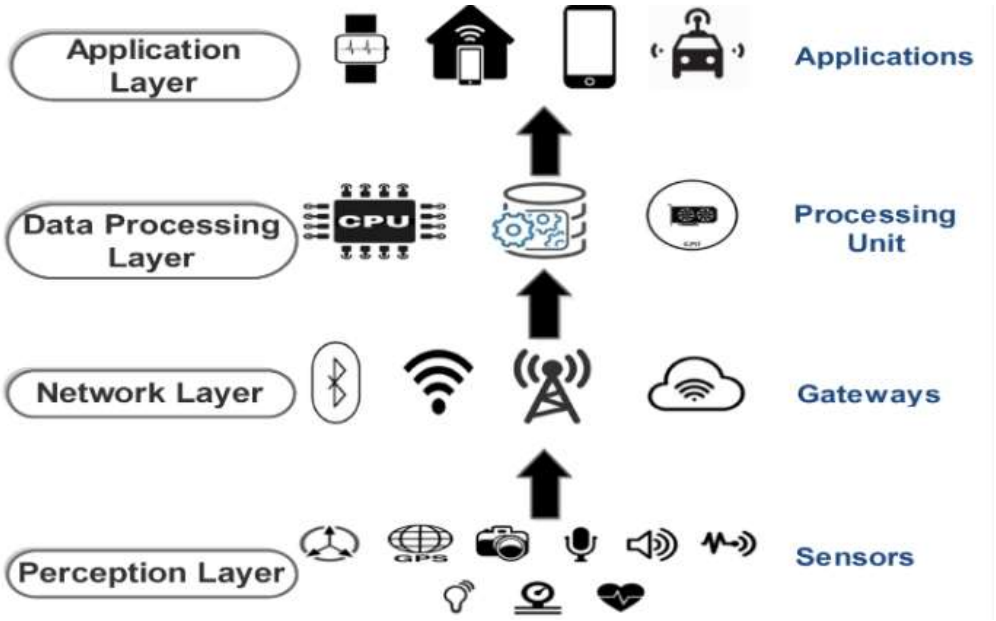

Рисунок 2.5 - Типова архітектура IoT

IDS в IoT слугує механізмом безпеки, який відстежує та аналізує мережевий трафік і поведінку пристроїв IoT для виявлення та запобігання зловмисним діям або порушенням в екосистемі IoT. Такі дії спрямовані на незаконне проникнення в пристрої та мережі IoT, тим самим ставлячи під загрозу їх конфіденційність, цілісність та доступність. Ці порушення можуть походити від супротивників як всередині, так і за межами організації.

Отже, IDS покликана підвищити рівень безпеки, відстежуючи зловмисні дії в мережевому трафіку, і в разі виявлення чогось, що порушує мережеві політики, негайно надсилає сповіщення адміністратору.

Поширення різних типів атак в мережі і зростаюче збільшення обміну даними між пристроями ставлять вимогу до захисту мереж і пристроїв IoT.

В даний час існують різні методи виявлення таких атак і на рисунку 2.6 представлені методи, пов'язані з розгортанням і виявленням вторгнень в IDS.

У сфері Інтернету речей IDS реалізуються аналогічно традиційним мережам і поділяються на мережеві, хост-орієнтовані та гібридні. Завданням мережевих IDS є ретельний аналіз мережевого трафіку для виявлення зловмисних дій, в той час як хост-орієнтовані IDS контролюють діяльність пристроїв і датчиків IoT.

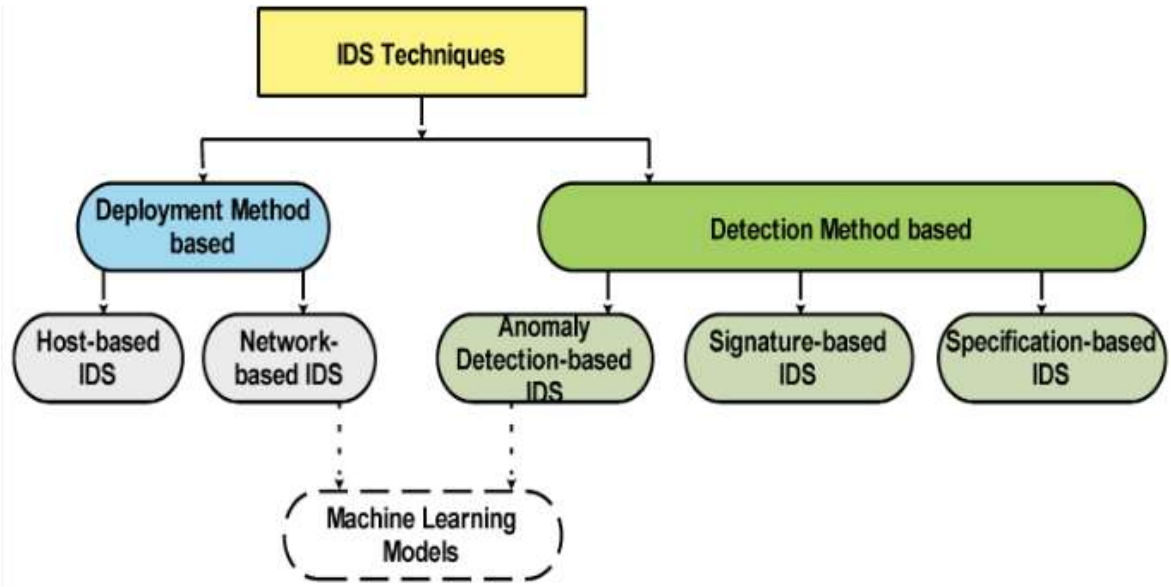

Рисунок 2.6 - Категорії методів виявлення вторгнень

Гібридні IDS поєднують в собі можливості як мережевих, так і хост-систем. Ці системи можуть бути розгорнуті в різних конфігураціях в пристроях і мережах IoT, включаючи централізовані, розподілені, ієрархічні або спільні підходи. Крім того, для розробки ефективної IDS вирішальне значення мають такі фактори, як ресурси, що підлягають захисту, моделі для визначення типової поведінки цих ресурсів, методи порівняння діяльності цих ресурсів з їх очікуваною поведінкою і, зрештою, методи визначення того, що є аномальною поведінкою або поведінкою вторгнення.

Стрімке розширення та повсюдна інтеграція Інтернету речей у поєднанні зі стрімким розвитком технологій та недостатніми протоколами безпеки підвищили ризики безпеки, зробивши Інтернет речей вразливим до широкого спектру кібератак. Ці атаки спрямовані на те, щоб обійти, вивести з ладу або погіршити функціональність і продуктивність пристроїв IoT.

Таким чином, пріоритетність безпеки є обов'язковою умовою для захисту бізнесу та приватних осіб від потенційних витоків даних та пов'язаних з ними збитків. Всебічне вивчення вразливостей, систем безпеки та потенційних загроз є життєво важливим для безпечної та успішної реалізації передбачуваного IoT. Сплеск зловмисних атак, спрямованих на пристрої Інтернету речей, викликає

тривогу і продовжує зростати в геометричній прогресії. Такі атаки можуть серйозно порушити роботу додатків Інтернету речей і завдати шкоди, включаючи катастрофічні інциденти, такі як збої в електромережі, що призводять до відключення електроенергії і людських жертв.

Додатки на основі Інтернету речей схильні до різних форм атак, включаючи активні, пасивні та спеціально розроблені атаки. Ці питання безпеки обговорювалися в багатьох дослідженнях. Наприклад, у [29] провели глибокий аналіз безпеки Інтернету речей, запропонувавши класифікацію загроз і атак на різних архітектурних рівнях Інтернету речей, а також оцінку загроз, підходи до пом'якшення наслідків і передові заходи безпеки, а також визначивши напрямки майбутніх досліджень. У той же час, в [30] розглянули виявлення вторгнень і, таким чином, класифікували атаки IoT на фізичні, програмні та мережеві, а також представили таксономію методів IDS IoT. Існує кілька викликів, що впливають на екосистему IoT, серед яких домінують ключові проблеми безпеки, а саме:

1. Характеристики та розмірність даних. Складність управління даними мережевого трафіку підвищується через їхню високу розмірність і велику кількість точок доступу в рамках підключених до Інтернету сервісів. Крім того, класифікація вторгнень бот-мереж в мережі IoT за допомогою алгоритму KNN стає особливо складною, коли доводиться стикатися з об'ємними наборами даних. Аналогічно, поширеність дисбалансу класів в IDS IoT негативно впливає на ефективність і точність моделей ML, які розробляються на основі цих викривлених наборів даних.

2. Вразливості та атаки. Усунення вразливостей і атак в мережах Інтернету речей є складним завданням, особливо в тих, що використовують хмарні технології, оскільки вони схильні до різноманітних атак. Завдання забезпечення безпеки і конфіденційності інфраструктур на основі IoT в середовищі "розумного міста" також є складним, особливо в частині захисту команд в промисловому IoT від підробки і неправильної маршрутизації. Завдання ще більше ускладнюється необхідністю протистояти все більш витонченим і різноманітним загрозам, які переслідують IoT, особливо в mesh-

мережах. Також значною проблемою є навмисне подовження часу передачі пакетів за допомогою кібератак, спрямованих на виснаження мережевих ресурсів. Крім того, нагальною проблемою є розробка протоколів безпеки, які аутентифікують сенсорні вузли та захищають їхню анонімність у мобільних БСМ, чутливих як до перекриття сенсорних полів, так і до атак з внутрішніх та зовнішніх джерел. Ці багатогранні виклики підкреслюють складність захисту середовищ Інтернету речей від широкого спектру загроз.

3. Методи ML та DL для виявлення вторгнень в мережах IoT. Ключовим викликом є впровадження мережевих IDS з використанням стратегій ML та DL, які потребують окремих наборів даних для роботи. Крім того, ще одним викликом є розробка високоякісних сценаріїв атак для тренування рішень з кібербезпеки для промислових КСЗІ, враховуючи їхню підвищену вразливість до вдосконалених мережевих та обчислювальних технологій.

4. Збереження конфіденційності та методи машинного навчання в мережах IoT. Збереження конфіденційності даних у мережах IoT при навчанні моделей за допомогою методів ФЛ є багатогранним завданням. Це включає в себе необхідність захисту від зловмисників, які можуть використовувати спільні параметри для компрометації додатків. Існує нагальна потреба у підвищенні ефективності, стійкості та безпеки методів, орієнтованих на ФЛ, для покращення виявлення та забезпечення збереження приватності.

5. Обмеженість та доступність ресурсів. Проблеми, пов'язані з обмеженістю та доступністю ресурсів, пов'язані з кількома викликами. Однією з таких проблем є отримання загальнодоступних наборів даних, які точно відображають нещодавню поведінку мережі та специфічні характеристики мережі IoT для дослідницьких цілей. Крім того, виявлення вторгнень в такі системи, як пристрої "розумного будинку", де самі по собі мережеві сліди можуть бути ненадійними, є ще однією проблемою [41]. Дуже важливо ефективно використовувати стратегії виявлення вторгнень в умовах обмежених ресурсів мережевих пристроїв IoT.

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ АЛГОРИТМУ МАШИННОГО НАВЧАННЯ ДЛЯ СИСТЕМИ ВИЯВЛЕННЯВТОРГНЕНЬ В ІОТ

3.1 Методології та алгоритми виявлення вторгнень в IoT

3.1.1. Використання алгоритмів машинного навчання та штучного інтелекту в IDS для IoT

Такі технології, як хмарні обчислення, хмарні границі та програмно-визначені мережі (SDN) значно підвищили залежність користувачів від своєї інфраструктури. Відповідно, зросла і кількість загроз, з якими стикаються ці користувачі. Як наслідок, управління безпекою під час розробки систем IoT стає дедалі складнішим і складнішим. IoT можна описати як електричну мережу, яка з'єднує фізичні об'єкти, такі як датчики, з програмним забезпеченням, що дозволяє їм обмінюватися, досліджувати і збирати дані. Додатки Інтернету речей використовуються в різних секторах, включаючи військову сферу, особисту охорону здоров'я, побутову техніку та інфраструктуру сільськогосподарського виробництва.

Загалом, методи машинного навчання застосовуються в різних завданнях, включаючи машинний переклад, регресію, кластеризацію, транскрипцію, виявлення, класифікацію, масову функцію ймовірності, вибірку і оцінку щільності ймовірності. Методи та алгоритми ML застосовуються у багатьох сферах, таких як ідентифікація спаму, розпізнавання зображень і відео, сегментація клієнтів, аналіз настроїв, прогнозування попиту, віртуальні персональні асистенти, виявлення шахрайських транзакцій, автоматизація обслуговування клієнтів, автентифікація, виявлення шкідливого програмного забезпечення та розпізнавання мови. Крім того, інтеграція IoT і ML може підвищити рівень безпеки пристроїв IoT, тим самим збільшуючи їх надійність і доступність. Передові методи дослідження даних ML відіграють важливу роль у підвищенні рівня безпеки IoT від забезпечення безпеки лише пристроїв зв'язку до інтелектуальних систем з високим рівнем безпеки.

Моделі на основі ML з'явилися як відповідь на кібератаки в екосистемі Інтернету речей, а поєднання підходів глибокого навчання (DL) і ML є новим і

важливим досягненням. Численні сфери застосування, включаючи носяться смарт-пристрої, розумні будинки, охорону здоров'я і транспортні мережі (VANET), вимагають впровадження надійних заходів безпеки для захисту приватності користувачів і особистої інформації. Успішне використання Інтернету речей очевидне в багатьох сферах сучасного життя. Результати досліджень показують, що методи ML і DL є ключовими рушіями автоматизації роботи зі знаннями, що сприяє економічному ефекту.

Методи машинного навчання відіграють важливу роль в аналізі та вилученні інформації з величезної кількості даних, що генеруються пристроями Інтернету речей. Ось деякі популярні методи ML та їх застосування в IoT:

1. Контрольоване навчання. Цей тип алгоритму навчається на основі маркованих навчальних даних. Різні додатки Інтернету речей можуть використовувати контрольоване навчання, наприклад:

1) виявлення аномалій. Навчивши моделі ML розпізнавати аномальні шаблони або поведінку в даних датчиків Інтернету речей, ми можемо виявити аномалії або потенційні порушення безпеки;

2) прогнозне обслуговування. Аналізуючи минулі дані датчиків, алгоритми контрольованого навчання можуть передбачити збої в роботі обладнання або потреби в технічному обслуговуванні. Це дозволяє впроваджувати проактивні заходи з технічного обслуговування, що призводить до скорочення часу простою;

3) моніторинг навколишнього середовища. Моделі машинного навчання можуть навчатися на основі даних з датчиків, щоб прогнозувати стан навколишнього середовища, наприклад, якість повітря, забруднення води або погодні умови.

2. Неконтрольоване навчання. Алгоритми неконтрольованого навчання витягують шаблони або структури з немаркованих даних без попередньо визначених категорій. В IoT методи неконтрольованого навчання знаходять такі застосування, як:

1) кластеризація моделей. ML може групувати подібні пристрої IoT або точки даних, полегшуючи розподіл ресурсів, балансування навантаження

або ідентифікацію сегментів мережі;

2) зменшення розмірності. Методи неконтрольованого навчання, такі як автокодери або аналіз головних компонент (PCA), полегшують аналіз даних IoT;

3) поведінкове профілювання. Неконтрольоване навчання може допомогти в розумінні нормальної поведінки пристроїв IoT або користувачів, дозволяючи виявляти відхилення або аномалії.

ML є перспективним підходом для захисту пристроїв Інтернету речей від кібератак. Він пропонує унікальну стратегію для запобігання атакам і надає ряд переваг, включаючи розробку сенсорно-залежних систем, забезпечення оцінки в режимі реального часу, підвищення безпеки, зменшення потоку даних і використання великої кількості даних в Інтернеті для всіх індивідуальних користувацьких додатків.

Останнім часом ML привертає увагу науковців і застосовується для забезпечення безпеки Інтернету речей, а також для розвитку багатьох інших галузей. Ефективними методами дослідження даних для виявлення "аномальних" і "нормальних" компонентів IoT і поведінки пристроїв в екосистемі IoT є DL і ML. Отже, щоб трансформувати безпеку систем IoT від забезпечення безпечного зв'язку "пристрій-пристрій" до створення систем, заснованих на інтелектуальній безпеці, необхідні методи ML/DL33 (рис. 3.1).

Підвищення безпеки IoT за допомогою алгоритмів підходів ML, таких як ансамблеве навчання, кластеризація k-середніх, правило асоціацій (AR), дерево рішень (DT), AdaBoost, машина опорних векторів (SVM), XGBoost і KNN мають свої переваги, недоліки і застосування в сфері безпеки IoT. DT нагадує дерево з гілками і листям, які слугують вузлами моделі. При класифікації SVM максимізує відстань між найближчими точками і гіперплощиною для класифікації класу. У виявленні DoS-атак RF працює краще, ніж SVM та KNN.

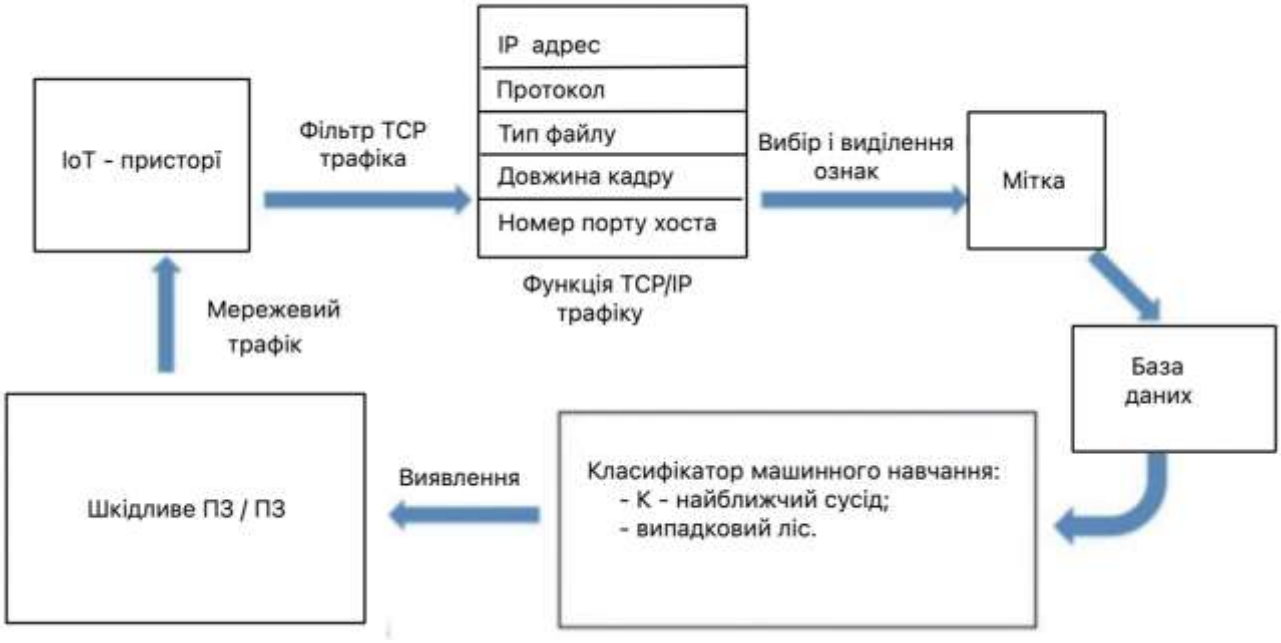

Рисунок 3.1 - Виявлення шкідливого ПЗ на основі ML

Використання підходів ML для мереж IoT має обмеження через виділену обчислювальну потужність і обмежену енергію машин IoT. Мережі IoT генерують дані з різноманітними структурами, формами та значеннями, а традиційні алгоритми погано пристосовані для обробки цих безперервних потоків даних у реальному часі. ML припускає, що всі статистичні атрибути набору даних є постійними, і дані повинні спочатку пройти попередню обробку та очищення, перш ніж вписуватися в певну модель. Однак у реальному світі дані надходять з багатьох вузлів і мають різне представлення з різним форматуванням, що створює труднощі для алгоритмів ML.

3.1.2 Сучасні підходи до моделювання вторгнень IoT

Для вирішення деяких проблем, з безпекою вторгнень у IoT, у цьому підрозділі представлено аналіз існуючих рішень для виявлення вторгнень на основі IoT. Методи IDS, засновані на машинному навчанні, з контролем та напівконтролем Методи IDS, засновані на SL, дозволяють алгоритму навчатися на маркованому наборі даних, де кожен алгоритм вивчає відображення від входів до виходів, що дозволяє йому робити прогнози або класифікувати нові, невідомі атаки. З іншого боку, SSL поєднує в собі елементи як SL, так і USL, де

алгоритм спочатку навчається на мічених даних, а потім допрацьовується або адаптується з використанням немічених даних для підвищення загальної продуктивності. У дослідженнях, розглянутих у цій статті, методи IDS, засновані на контрольованому або напів контрольованому навчанні.

Для підвищення безпеки смарт-пристроїв від загроз у [42] запропонували трирівневу IDS з використанням SL, де рівень I класифікує нормальну поведінку пристроїв IoT на основі типу і профілю, рівень II виявляє шкідливі пакети під час атак з використанням моделі ML, а рівень III класифікує виявлений тип атаки. Ефективність рішення було перевірено на тестовому стенді "розумного будинку", де воно протистояло 12 атакам, зокрема DoS, MitM, розвідувальним та повторним атакам, а також чотирьом багатоетапним сценаріям атак. Отримані результати показують високі показники F-міри 96,2%, 90,0% та 98,0% для різних мережевих атак, що підтверджує здатність запропонованого IDS розрізняти пристрої Інтернету речей, класифікувати мережеву активність та ідентифікувати конкретні атаки.

Аналогічно, для пом'якшення проблеми великих маркованих наборів даних в SL для підвищення точності в мережах IoT запропонували IDS, засновану на моделі SSL, DNNs і техніці неконтрольованої кластеризації, k-середніх. В результаті з'явилася модель SDRK - комбінація нейронної мережі глибокого прямого поширення SSL (DFNN), повторної випадкової вибірки (RRS) і k-середніх (K).

При розміщенні у вузлах туману між шарами Інтернету речей і хмари ці алгоритми виявляють і пом'якшують мережеві вторгнення без істотного впливу на затримку в мережі. Запропонований IDS був експериментально оцінений з використанням набору даних NSL-KDD, і результати показали, що він перевершує існуючі рішення з точки зору високої точності виявлення порушень безпеки і подолання проблем з маркуванням у великих наборах даних. SDRK досягнув точності, оцінки F1 та MCC 99,78%, 99,72% та 99,44%, відповідно, для виявлення атаки "потоку даних".

Завдяки використанню ШНМ з гіперпараметрами та п'ятикратній перехресній перевірці метод продемонстрував надійність, але зіткнувся з

проблемами при виявленні в реальному часі з різними розмірами записів у наборі даних. Він ефективно виявив DoS-атаки, атаки типу Probe, User to Root та Remote Local, досягнувши найкращих результатів у виявленні DoS-атак з точністю 99,61%, відкликання - 99,92% та F-міри - 99,17%. Загальна точність виявлення чотирьох атак склала 98,87%, що перевершило існуючі підходи.

У цьому ж ключі у [43] запропонували структуру IDS для протидії значним загрозам в екосистемі IoT з фокусом на DoS/DDoS-атаках. Використовуючи багаторівневий персептрон, керований алгоритм ШНМ, модель навчалася на трасі інтернет-пакетів, щоб класифікувати нормальні та загрозливі патерни в мережі. Її ефективність була оцінена за допомогою імітаційних експериментів, досягнувши 99,4% точності у виявленні DoS/DDoS-атак. Аналогічно, , виявлення типів атак і автоматичної генерації набору правил, що представляють безпечну поведінку пристроїв. Вони створили тестовий стенд для збору мережевого трафіку з реальних "розумних" будинків, а продуктивність як IDS, так і системи була оцінена на основі семи моделей для класифікації цих атак і декількох показників продуктивності. Результати показали, що GBDT перевершив інші моделі з точністю 99,53%, точністю 99,57%, відгуком 99,55% і оцінкою F1 99,56%.

Рішенням є багаторівнева розподілена IDS, розташована в кожному вузлі екосистеми "розумного будинку", яка використовує співпрацю між різними пристроями Інтернету речей за допомогою розподіленої хеш-таблиці (DHT), де вузли обмінюються мережевою та системною інформацією. Він виявляє неочікувану поведінку мережевих компонентів за допомогою бінарного класифікатора, аналізуючи та агрегуючи характеристики вхідного трафіку як з мережі, так і з DHT.

Були проведені експериментальні оцінки та порівняння з різними класифікаторами, які показали, що AdaBoost перевершив інші моделі з точністю 99,39%, 99,36% точності та 99,33% повторюваності в плані виявлення бот-мереж шкідливого програмного забезпечення Mirai. Крім того, для вирішення проблем з обчислювальними накладними витратами та масштабуванням, пов'язаних з відомими сигнатурами атак.

Пом'якшити проблему високої розмірності даних при виявленні аномалій в динамічних і різноманітних середовища, можна завдяки вдосконаленій системі виявлення аномалій, яка інтегрує традиційні методи з алгоритмом поліпшеної динамічної оптимізації рою двійкових частинок (IDSBPSO). Цей алгоритм призначений для ефективного відбору ключових ознак, тим самим удосконалюючи процес виявлення. IDSBPSO, який використовує ймовірність перевертання, а не швидкість, слугує технікою оптимізації ознак на основі обгортки. Він динамічно зменшує простір пошуку і відбирає релевантні, не надлишкові ознаки для IDS. IDS використовує статистичні та ML-алгоритми для виявлення та класифікації зловмисного мережевого трафіку.

Під час тестування на наборах даних IoTID20 і UNSW-NB15 IDS продемонстрував чудову продуктивність порівняно з традиційними методами відбору на основі PSO, досягнувши 89,52% точності у виявленні різних атак, а також зменшивши обчислювальні вимоги і кількість необхідних ознак. Також важливо вирішувати проблеми, притаманні системам Інтернету речей, такі як екстремальні умови навколишнього середовища, низькі обчислювальні ресурси та обмежена енергія, які роблять їх вразливими до кіберзагроз.

Тому було запропоновано нову, ресурсоефективну IDS та метод подвійного вибору ознак під назвою MI2G. Цей метод надає пріоритет ознакам з високою взаємною інформацією та низькою ентропією, оптимізуючи обчислювальну ефективність. Стратегія використовує модель USL для аналізу мережевого трафіку та виявлення аномалій, що вказують на кібервторгнення. Тестування на наборі даних CICIDS2018, а також порівняння з іншими дослідженнями, що використовували той самий набір даних і еталонний набір даних UNSW-NB15, показали, що класифікатор DT перевершив альтернативні класифікатори ML. Він досяг 99,5% точності, достовірності та частоти згадування, довівши свою ефективність для середовищ IoT з обмеженими обчислювальними можливостями.

3.1.3 Використання графових алгоритмів для моделювання атак

Аналіз графів атак - це модельний підхід до аналізу мережевої безпеки. Він аналізує орієнтований граф, який називається графом атак. Зазвичай кожна вершина в ньому відповідає шкідливій події, спричиненій зловмисниками, а ребра відповідають причинно-наслідковим зв'язкам між подіями. Ми можемо отримати граф атак з топології мережі, її конфігурації та розподілу вразливостей. Граф атак дає нам різну інформацію, що стосується мережевої безпеки. Крім того, існує кілька відповідних алгоритмів для пошуку бажаних засобів контролю безпеки, застосовних до мережі такі як залежність від експлойтів, граф І/АБО, монотонність та обробка циклів (рис. 3.2).

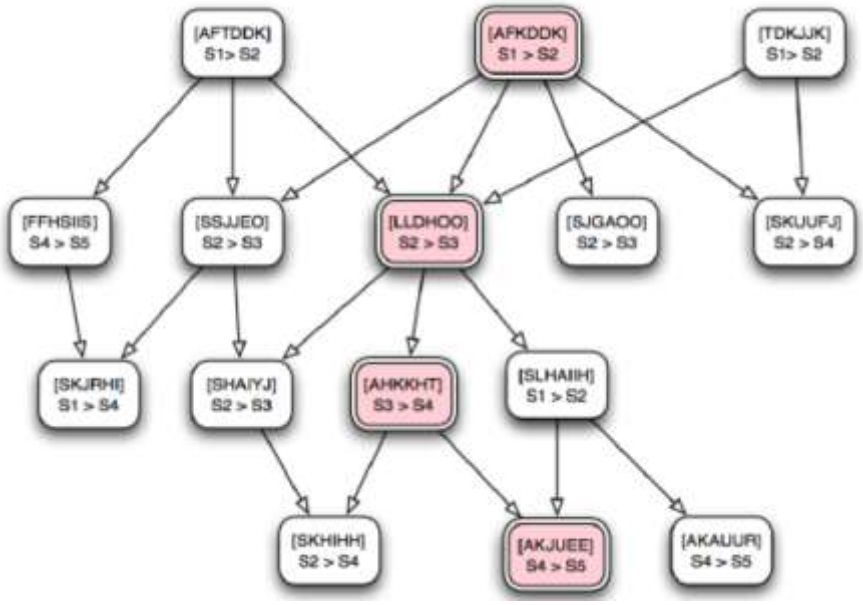

Рисунок 3.2 - Приклад графа атаки

У [24] автори запропонували перший комплексний підхід до аналізу графів атак. З того часу було досягнуто значного прогресу. Він включає представлення графів атак і припущення про монотонність, два типи комбінацій вузлів, ієрархічну техніку візуалізації, відображення в пропозиційну логіку та алгоритм наближеної оптимізації для засобів контролю безпеки. Історія дослідження також підкреслює кілька проблем, таких як масштабованість, складність у розробці метрик та робота з структурами.

За цим прогресом стоять різні визначення графів атак. На ранньому етапі

їх визначали як скінченні автомати, які називали графами перебору станів. Пізніше з'явилося визначення циклічних спрямованих графів І/АБО, які отримали назву графів залежності від експлойтів [25]. Зараз деякі дослідники узагальнюють його як окремий випадок байєсівських мереж, які називають байєсівськими графами атак [26].

Для вирішення багатьох проблем з мережевими атаками активно вивчається технологія графів атак, яка прогнозує шлях атаки зловмисника. Її основною метою є прогнозування шляху атаки та визначення потенційного шляху атаки з точки зору зловмисника. Завдяки визначенню шляху атаки вона може допомогти адміністратору визначити ціль, яку необхідно захистити, зосередивши увагу в першу чергу на різних інформаційних активах в системі.

Однак для того, щоб створити граф атак, необхідно заздалегідь створити не тільки топологію мережі та системну інформацію, а й базу даних вразливостей, що є дорогим і трудомістким завданням. Крім того, для створення графа атак потрібен великий обсяг обчислень, оскільки перехресна кореляція повинна бути розрахована для всіх систем (вузлів), підключених до мережі. Тому необхідне дослідження нового методу генерації графів атак для прогнозування можливих шляхів атак і виявлення потенційних шляхів атак шляхом генерації графа атак за низькою вартістю на основі методів штучної розвідки. Дослідження і розробка системи, яка генерує граф атак за низькою вартістю шляхом впровадження методів штучного інтелекту, все ще перебуває на стадії розвитку.

Загалом граф атак і дерево атак представляють кібератаки з точки зору візуального синтаксису. Вони показали, що хоча є багато переваг відображення кібератак у вигляді графа атак або дерева атак, існує неузгодженість щодо способу представлення кібератак на графах атак і деревах атак. Через це було пояснено необхідність візуальної стандартизації. Це перша робота, в якій представлено детальний критичний аналіз візуального синтаксису методів моделювання атак. Важливими механізмом оцінки основних вузлів IoT-систем на основі графа атак. Оцінка основного вузла включає в себе дві частини: одна - це відношення використання між вузлами, а інша - вплив на систему після того,

як вузол буде атакований. Вони кількісно оцінюють ці дві частини, використовуючи значення важливості вузла Electronics 2022,11, 1332 3 of 25 та значення ризику вузла.

По-перше, значення важливості вузла обчислюється з урахуванням шляху атаки через вузол і ймовірності того, що зловмисник відмовиться від атаки. По-друге, вони запропонували два кількісні показники для комплексної оцінки впливу вузла на безпеку системи на додаток до вразливості вузла та результатів атаки, а також розрахувати значення ризику вузла на основі методу аналізу сірої кореляції. По-третє, основний вузол системи IoT може бути отриманий шляхом інтеграції значення важливості вузла і значення ризику.

Вона вчиться генерувати шлях атаки на основі існуючих графів атак, використовуючи машинне та глибинне навчання. Навчена модель генерує граф атаки, використовуючи лише топологію мережі та системну інформацію, системної інформації та інформації про шлях атаки. Задача генерації графа атак переформульована як задача навчання з багатьма виходами та бінарної класифікації, після чого ми застосовуємо моделі машинного навчання та глибокого навчання для генерації графа атак.

3.2. Методи попередньої обробки та методології машинного навчання для оцінювання моделі безпеки

Для порівняння ефективності різних алгоритмів машинного навчання для побудови системи виявлення вторгнень (IDS), включаючи дерево рішень (DT), випадковий ліс (RF), k-Nearest Neighbor (k-NN), Ada Boost та опорні вектори (SVM). (SVM), використовуючи набір даних IoTID20, ми будемо дотримуватися методології, описаної нижче:

1) попередня обробка. Очистіть і підготуйте набір даних для використання в алгоритмах машинного навчання. Це може включати обробку пропущених значень, вибір ознак або інжиніринг, а також масштабування або нормалізацію даних за потреби;

2) відбір ознак використовується для визначення найбільш релевантних змінних для прогнозної моделі;

3) поділ даних. Дані розділяють на навчальний і тестовий набори. Навчальний набір буде використано для навчання моделей, тоді як тестовий набір буде використано для оцінки їхньої продуктивності;

4) навчання та оцінка алгоритмів: Для кожного з цих алгоритмів (DT, RF, k-NN, Ada Boost та SVM), ми навчимо модель на навчальних даних, а потім оцінимо її роботу на тестових даних. Існують різні метрики, які ми будемо використовувати для оцінки роботи алгоритмів, такі як точність, точність швидкість запам'ятовування та F1-міра;

5) порівняння результатів. Після того, як ми отримаємо метрики продуктивності для кожного з алгоритмів, ми порівняємо результати, щоб визначити, який алгоритм працює найкраще. Загальна структура системи показана на рисунку 3.3.

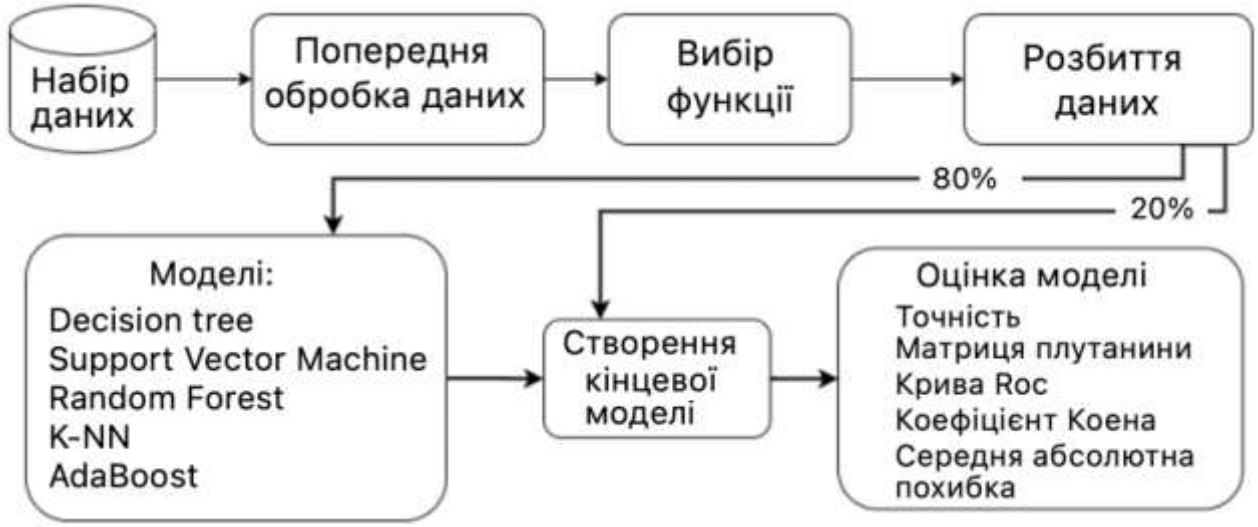

Рисунок 3.3 - Загальна структура системи моделі захисту

У експерименті використовується набір даних IoTID20 для мережевих систем виявлення вторгнень (IDS). Цей набір даних з відкритим вихідним кодом, зібраний з IEEE Data Port і наданий Huy Kang Kim [27], має маркування і включає комплексну мережу з різними характеристиками на основі потоків і загальними характеристиками, характерними для бездротових середовищ.

Цей набір даних дозволяє нам оцінити здатність виявляти аномальну активність в мережах IoT. Він буде служити в якості еталоном для виявлення аномальної активності в мережах IoT і стане цінним ресурсом для розробки нових методів IDS для середовищ IoT. Набір даних IoTID20 був згенерований за допомогою домашнього підключеного смарт-пристрою, оснащеного НГУ SKT та Wi-Fi Smart-камерою EZVIZ (пристрій-жертва IoT), а також інших пристроїв, включаючи ноутбуки, смартфони та планшети (пристрої, що атакують IoT). Цей набір даних забезпечує реалістичне представлення мережевої активності IoT, включаючи як нормальну, так і аномальну поведінку.

Цей набір даних містить 625 783 екземпляри з 83 характеристиками мережі IoT та трьома мітками [27]: бінарний код, категорія та підкатегорія, деталі наведені в таблиці 3.1.

Таблиця 3.1 – Набір даних

Мітка	Кількість (міток)	Відносна частота (міток)	Категорія	Кількість (категорій)	Відносна частота
Аномальна	585680	92,8%	Mirai	420331	65,80%
Нормальна	40082	7,2%	Scan	76012	12%
			DoS	60187	9,50%
			Нормальна	39871	6,40%
			MITM ARP Spoofing	34172	5,70%

Також була представлена таксономія атак IoTID20 (рис. 3.4).

1. Попередня обробка даних передбачає підготовку вихідних даних для моделі машинного навчання. Це важливий крок у створенні моделі машинного навчання створення моделі машинного навчання і включає такі завдання, як очищення даних, кодування міток, нормалізація функціональна інженерія та розділення даних. Виконуючи ці кроки, ми можемо гарантувати, що дані готові до використання в моделі машинного навчання.

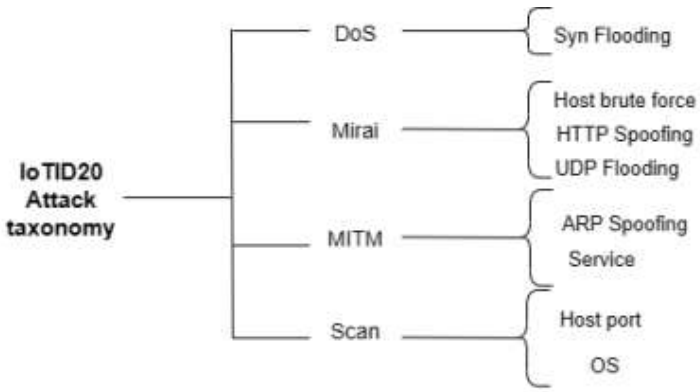

Рисунок 3.4 - Таксономія атак IoTID20

2. Очищення даних передбачає виявлення та виправлення або видалення неправильних, неповних і неточних даних з наборів даних. Це також може включати заміну відсутніх значень. У цьому експерименті ми виконали кілька завдань з очищення даних, включаючи видалення дубльованих рядків, видалення несуттєвих стовпців (таких як «Мітка часу»), заміну нескінченних значень нулями та перетворення нечислових ознак на числа.

3. Кодування міток передбачає перетворення категоріальних міток у числову форму, яка може бути зрозумілою для алгоритмів машинного алгоритми машинного навчання. У цьому дослідженні ми використали підхід кодування міток для перетворення категоріальних ознак 'Flow_Bytes/s', 'Flow_Pkts/s', 'Src_IP' та 'Dst_IP' у числові значення.

4. Відбір ознак - це процес визначення найбільш релевантних вхідних змінних для прогнозної моделі. Зменшуючи кількість вхідних змінних, ми можемо зменшуючи кількість вхідних змінних, ми можемо зменшити обчислювальні витрати на моделювання і потенційно покращити продуктивність моделі. У цьому дослідженні ми використовували фільтр низької дисперсії для усунення ознак, дисперсія яких не досягала порогового значення від 0,0 до 0,5. Початковий набір даних містив 83 ознаки, а після застосування підходу фільтрації ознак, було відібрано 62 ознаки. Вибір саме цього порогу був мотивований бажанням досягти балансу між збереженням інформативних ознак та виключенням між збереженням інформативних ознак

та виключенням тих, що мають обмежену дискримінативну силу.

5. Нормалізація - це процес масштабування стовпчиків у наборі даних до однакового діапазону зі збереженням відносної варіації в діапазонах значень. У нашому випадку набір даних IoTID20 має різноманітні значення, з деякими особливостями від'ємні значення, а інші обчислюються тисячами. Щоб вирішити цю проблему, ми застосували метод min-max для нормалізації даних між 0 та 1.

6. Розбиття даних - це процес поділу набору даних на дві або більше підмножин. Одна підмножина зазвичай використовується для навчання моделі, в той час як інша використовується для оцінки ефективності моделі. У цьому дослідженні ми розділили дані на 80% навчальної навчальний набір і 20% тестовий набір.

3.3 Результати аналіз і побудови моделей

У цій секції представлено результати аналізу даних. Для того, щоб застосувати та оцінити наші класифікатори, ми дотримувалися методів попередньої обробки та підготовки, описаних у минулому розділі. Ми візуально проаналізували результати та використали різні критерії оцінки для порівняння ефективності різних класифікаторів.

Всі експерименти з алгоритмом машинного навчання, описані в цій роботі, були проведені з використанням аналітики KNIME. KNIME Analytics Platform - це безкоштовне програмне забезпечення з відкритим вихідним кодом для науки про дані. Воно дозволяє розкривати інсайти, приховані у ваших даних приховані у ваших даних, видобувати нові знання та робити прогнози щодо майбутніх тенденцій. Завдяки інтуїтивно зрозумілому інтерфейсу та потужними інструментами, KNIME дозволяє легко досліджувати та аналізувати ваші дані [30]. KNIME надає графічний інтерфейс для всього процесу розробки, він містить різні заздалегідь визначені вузли для завдань машинного навчання, таких як попередня обробка даних, класифікація, кластеризація та візуалізація

даних.

Для оцінки ми розглядаємо наступні метрики.

Точність - це відсоток правильних прогнозів, поданий у відсотках:

$$\text{Точність} = \frac{\text{Кількість правильних передбачень}}{\text{Загальна кількість передбачень}}.$$

Матриця плутанини табулює правильні та неправильні прогнози, зроблені класифікаційною моделлю.

Точність обчислює відношення правильно передбачених позитивних результатів до загальної кількості передбачених позитивних результатів:

$$P_r = \frac{TP}{TP+FP}.$$

Recall обчислює відношення правильно передбачених позитивних результатів до всіх результатів у певному класі:

$$R_c = \frac{TP}{TP+FN}.$$

Оцінка F_1 - це комбінований показник точності та пригадування, що змінюється від 0 до 1 і визначається наступним чином:

$$F_1 = \frac{2\times(R_c+P_r)}{(R_c+P_r)}.$$

ROC графік показує ефективність моделі при різних прогнозуваннях, використовуючи частоту істинних спрацьовувань (TPR) і частоту хибних спрацьовувань (FPR),і обчислюється наступним:

$$TPR = \frac{TP}{TP+FN},$$

$$FPR = \frac{FP}{FP+FN}.$$

Ми оцінюємо всі класифікатори з точки зору точності, правильно класифіковані та неправильно класифікованих екземплярів. Результати наведені в таблиці 3.2.

Щоб перевірити ефективність класифікаторів, ми порівняли показники

точності, що базуються на точності, прогнозованості, швидкості TP та FP для DT, RF, Ada Boost, K-NN та SVM, як показано в таблиці 3.3.

Таблиця 3.2 – Ефективність класифікаторів

Критерії оцінювання	Класифікатори				
	DT	RF	K-NN	Ada Boost	SVM
Точність (%)	99,80	99,79	99,60	97,26	95,48
Правильно класифіковані екземпляри	55902	55897	55803	54482	53483
Неправильно класифіковані екземпляри	113	118	212	1533	2532

Таблиця 3.3 – Порівняння міри точності для класифікаторів

	TP	FP	Точність	Rc	F - міра
DT	50478	65	0,999	0,999	0,999
	5424	48	0,991	0,988	0,990
RF	50517	109	0,998	0,999	0,999
	5380	9	0,998	0,980	0,989
K-NN	50454	140	0,997	0,999	0,998
	5349	72	0,987	0,974	0,981
Ada Boost	50401	1408	0,973	0,998	0,985
	4081	125	0,97	0,743	0,842
SVM	49355	1361	0,973	0,977	0,975
	4128	1171	0,779	0,752	0,765

Щоб краще зрозуміти ефективність, для оцінки наших моделей ML використовується матриця плутанини. У таблиці 3.4 кожен рядок відповідає фактичним показникам класів, тоді як кожен стовпчик відображає прогнози.

Таблиця 3.4 – Матриця плутанини

	Неправильна	Правильна	Клас
DT	50478	48	Неправильний
	65	5424	Правильний
RF	50517	9	Неправильний
	109	5380	Правильний
K-NN	50454	72	Неправильний
	140	5349	Правильний
Ada Boost	50401	125	Неправильний
	1408	4081	Правильний
SVM	49355	1171	Неправильний
	1361	4128	Правильний

На додаток до матриці плутанини, представлено ROC-криву, щоб проілюструвати точність кожного класифікатора.

На рисунках 3.5 - 3.9 представлено ROC-криві класифікаторів.

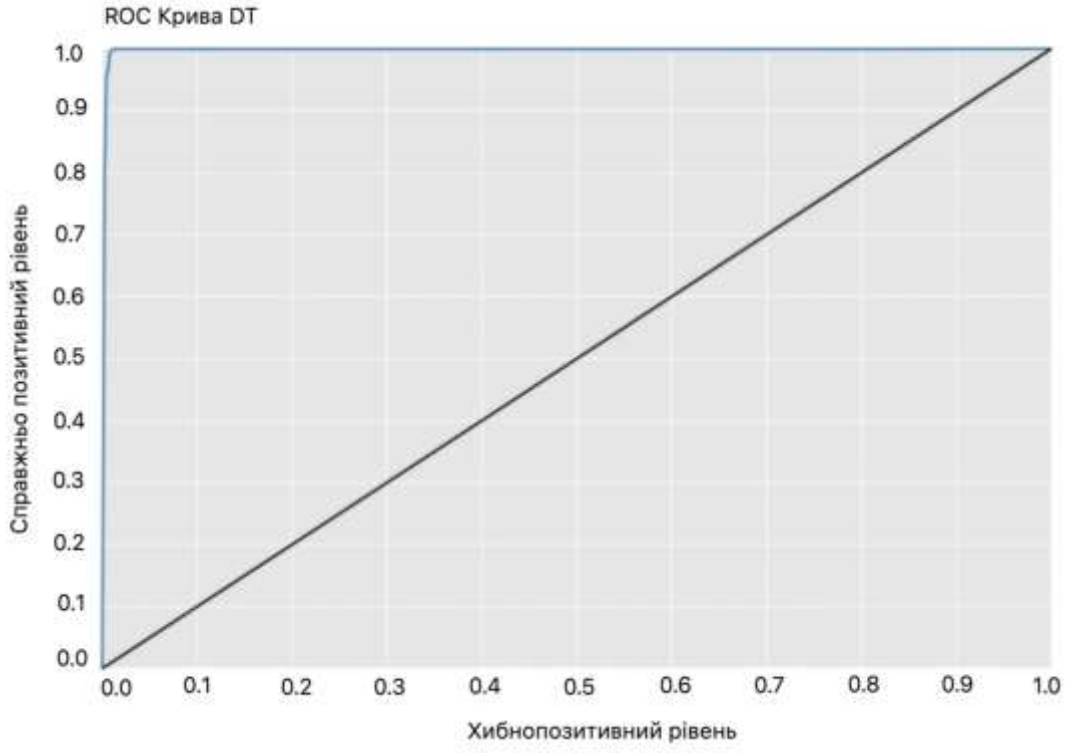

Рисунок 3.5 – ROC-крива Дерево рішень

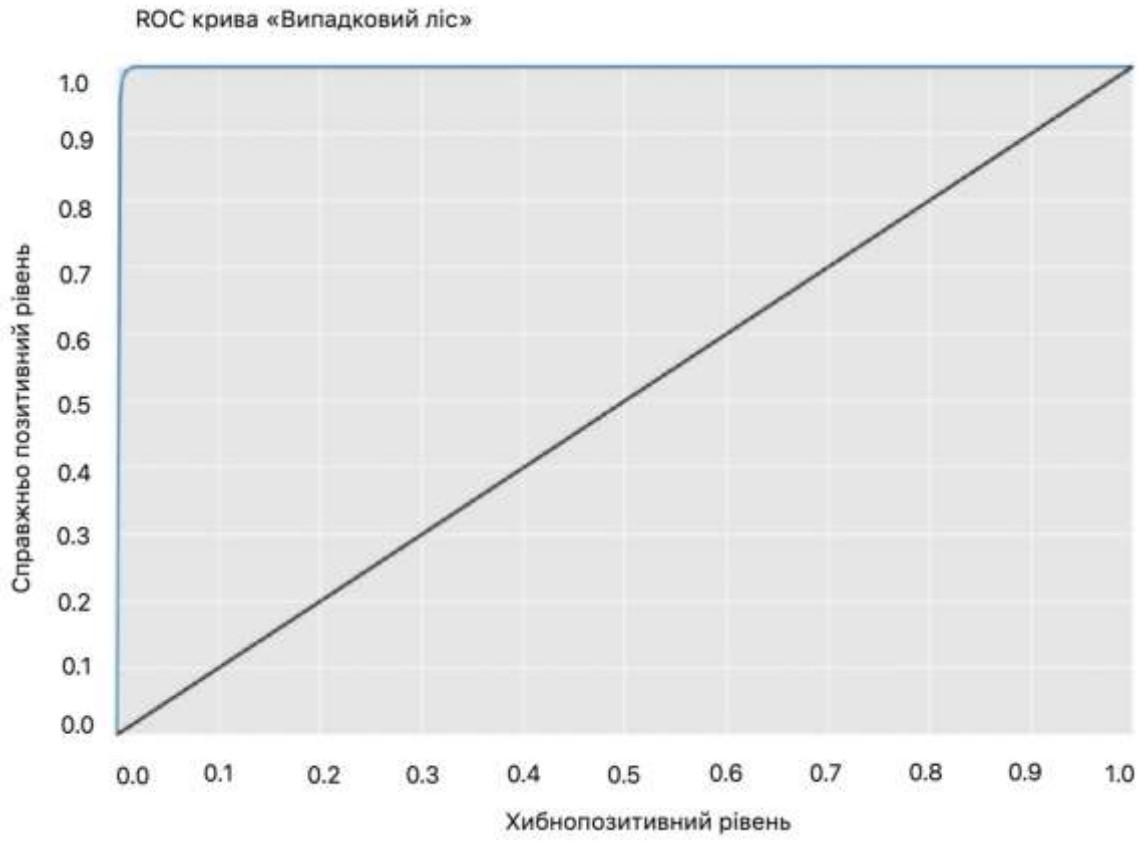

Рисунок 3.6 - ROC-крива “Випадковий ліс”

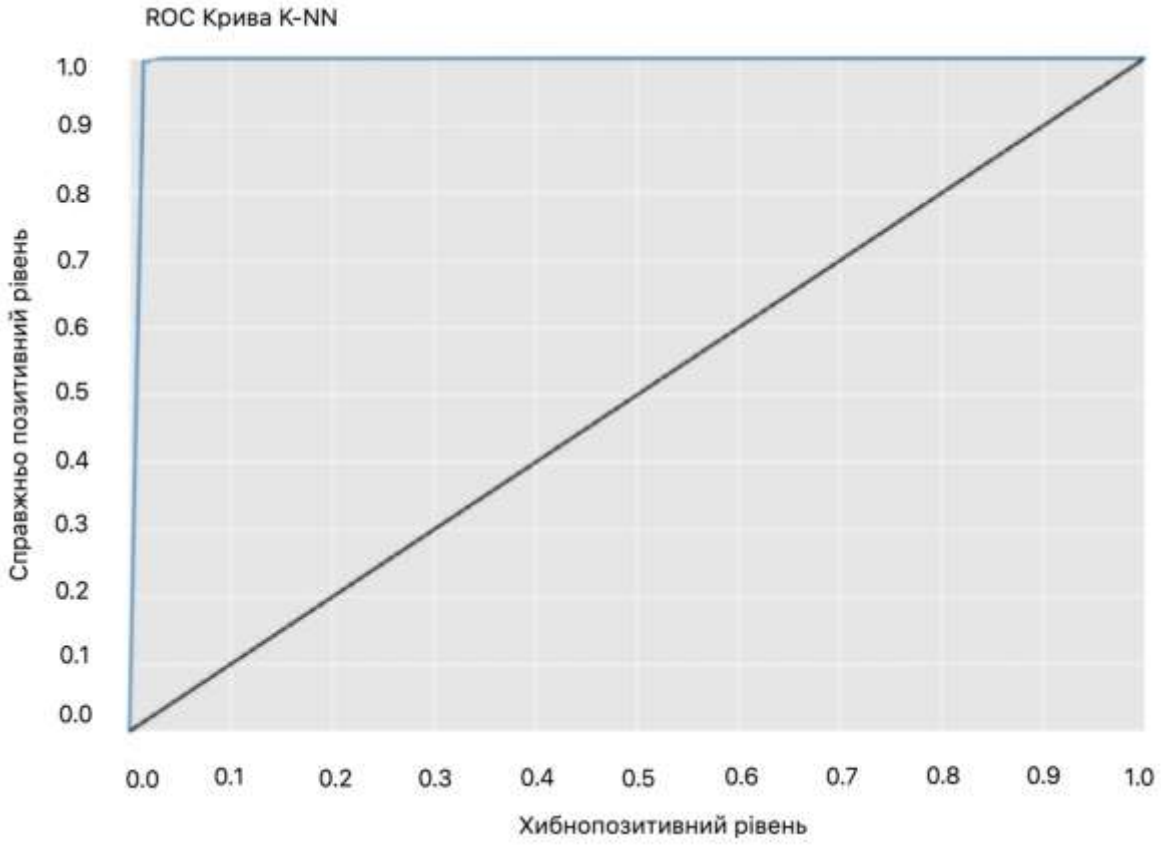

Рисунок 3.7 – ROC-крива K-NN

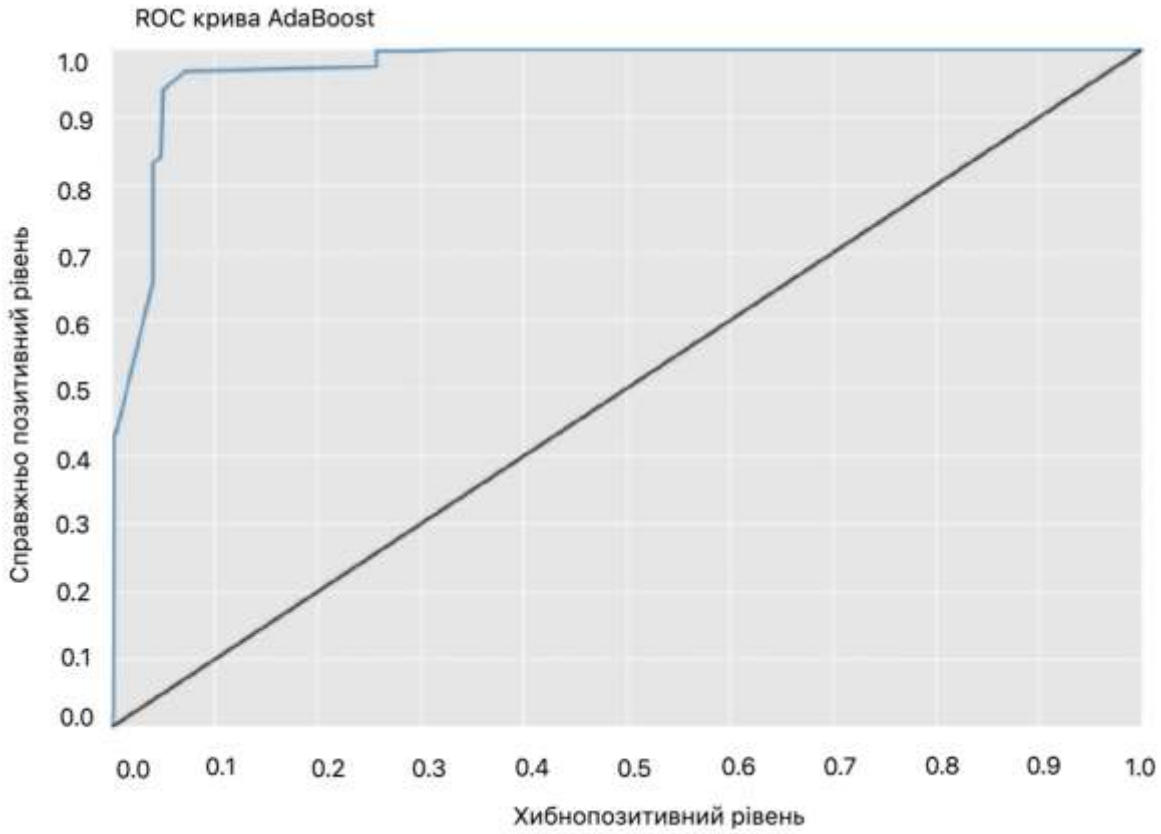

Рисунок 3.8 - ROC-крива AdaBoost

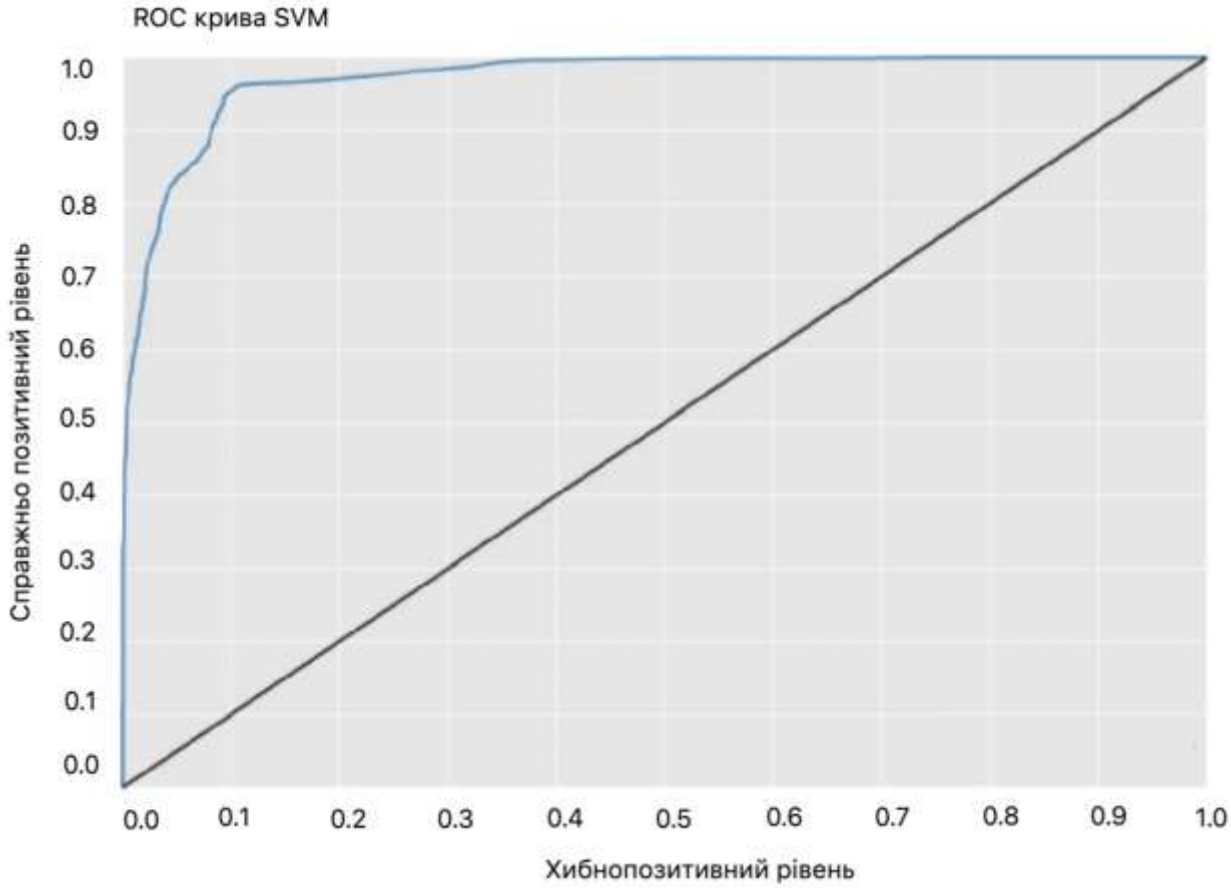

Рисунок 3.9 – ROC-крива SVM

Після побудови прогнозної моделі можемо оцінити ефективність алгоритмів, проаналізувавши результати. Як показано в таблиці 3.2, алгоритми дерева рішень (DT) та випадкового лісу (RF) мали найвищу точність (99.80% та 99,79% відповідно) на наборі даних IoTID 20, причому алгоритм DT працює трохи краще, ніж алгоритм RF. Алгоритм k-найближчих сусідів (K-NN) також мав високу точність, але вона була трохи нижчою, ніж у DT та RF алгоритмів. Алгоритм Ada Boost мав нижчу точність, ніж інші три алгоритми, але вона була все ще відносно висока. Алгоритм машини опорних векторів (SVM) мав найнижчу точність серед п'яти алгоритмів.

Крім того, рисунок 3.5 ілюструє, що класифікатор дерева рішень працює краще, ніж інші класифікатори, з найбільшу кількість правильно класифікованих екземплярів і найменшу кількість неправильно класифікованих екземплярів.

У таблиці 3.4 наведено матрицю плутанини класифікатора, з якої видно, що як випадковий ліс, так і дерево рішень класифікатори мають найвищі значення істинної позитивної оцінки (TP) для класу аномалій - 50517 та 50478 екземплярів відповідно. Однак алгоритм SVM правильно ідентифікує 49355 екземплярів, що належать до класу аномалій. Показник помилкових спрацьовувань (FP) помилкових спрацьовувань (FP) є нижчим для класифікаторів на основі дерева рішень та випадкового лісу (65 та 109 випадків відповідно для класу аномалій, відповідно, для класу аномалій та 48 і 9 випадків, відповідно, для нормального класу), далі йдуть алгоритми K-NN Ada Boost та SVM. Ці результати пояснюють, чому класифікатори дерева рішень та випадкового лісу перевершують інші класифікатори.

Тепер давайте порівняємо фактичний клас і передбачені результати, отримані за допомогою матриці плутанини, зображеної в таблиці 3.4.

Дерево рішень правильно передбачило 55902 екземпляри з 56015 екземплярів і зробило 113 невірних прогнозів. Це пояснює чому точність дерева рішень є кращою, ніж у інших методів класифікації, що використовуються з меншим значенням коефіцієнта помилок. Графік ROC-кривої на рисунках 3.5 - 3.9 ілюструє продуктивність різних алгоритмів машинного навчання.

Очевидно, що алгоритми дерева рішень та випадкового лісу є чудовими класифікаторами, оскільки вони починаються з лівого кута і досягають верхнього лівого і верхнього правого кутів з чутливістю 99% і специфічністю 98%. Алгоритми K-NN та SVM також демонструють хороші результати, але не настільки ефективні, як Decision tree та Random forest. Експериментальні результати показують, що алгоритм дерева рішень досяг найвищої точності - 99.80%. На відміну від нього, алгоритм SVM показав найнижчу точність - 95,48%. У порівнянні з іншими дослідженнями виявлення вторгнень з використанням IoT які оцінювали точність класифікації різних алгоритмів інтелектуального аналізу даних, дані результати показують, що підхід на основі дерева рішень послідовно давав оптимальні результати при порівнянні за точністю, чутливістю, специфічності та метрики точності.

ВИСНОВКИ

В кваліфікаційній роботі розв’язано актуальну задачу підвищення ефективності виявлення вторгнень для Інтернет – речей. При цьому отримано наступні результати.

1. У роботі було проаналізовано основні характеристики IDS, включаючи виявлення на основі сигнатур і виявлення аномалій, і підкреслено переваги використання методів виявлення аномалій над підходами на основі сигнатур.

2. Розглянуто різні методи виявлення аномалій, включаючи статистичні методи, методи на основі кластеризації, методи на основі щільності, методи на основі реконструкції та однокласові машини опорних векторів (SVM).

3. Розглянуто метрики оцінки та продуктивності, які використовуються для оцінки ефективності методів виявлення аномалій, включаючи загальновживані набори даних для оцінки та метрики продуктивності, такі як точність, точність, відгук, F1-рахунок, ROC-крива та AUC.

4. Дослідження показало, що глибинне навчання та ансамблеві методи є найбільш ефективні.

5. Алгоритми дерево Decision та алгоритм випадкового лісу показали найвищу точність 99,80% та 99,79% відповідно, перевершивши інші алгоритми. Результати показали, що дерево рішень і випадковий ліс є ефективні для прогнозування вторгнень в IoT і мають найкращі показники з точки зору точності та достовірності.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. M. Abualkibash. Machine Learning in Network Security Using KNIME Analytics. Int. J. Netw. Secur. Its Appl., 2019, vol. 11, no. 5, pp. 1–14

2. M. Arafat, A. Jain, and Y. Wu, “Analysis of intrusion detection dataset NSL-KDD using KNIME analytics,” Proc. 13th Int. Conf. Cyber Warf. Secur. ICCWS 2018, vol. 2018-March, pp. 573–583.

3. S. B. Kotsiantis. Decision trees: a recent overview. Artif. Intell. Rev., 2013, vol. 39, no. 4, pp. 261–283.

4. W. S. Noble, “What is a support vector machine?,” Nat. Biotechnol., Dec. 2006, vol. 24, no. 12, pp. 1565–1567.

5. Y. Freund and R. E. Schapire, “A Decision-Theoretic Generalization of On-Line Learning and an Application to Boosting,” J. Comput. Syst. Sci., 1997, vol. 55, no. 1, pp. 119–139.

6. M. Hasan, M. M. Islam, M. I. I. Zarif, and M. M. A. Hashem, “Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches,” Internet of Things, Sep. 2019, vol. 7, p.100059.

7. J. Su, S. He, and Y. Wu, “Features selection and prediction for IoT attacks,” High-Confidence Comput., Jun. 2022, vol. 2, no. 2, p.100047.

8. Abeshu, A., Chilamkurti, N.: Deep learning: the frontier for distributed attack detection in fog-to-things computing. IEEE Commun. Mag, 2018, 56(2), pp. 169–175.

9. Abomhara, M., Køien, G.M.: Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. J. Cyber Secur. Mobil. 2015, 4(1), pp. 65–88.

10. Al-Hawawreh, M., Moustafa, N., Sitnikova, E.: Identification of malicious activities in industrial internet of things based on deep learning models. J. Inf. Secur. Appl. 2018, 41, pp. 1–11.

11. Al Jallad, K., Aljnidi, M., Desouki, M.S.: Anomaly detection optimization using big data and deep learning to reduce false-positive. J. Big Data, 2020, 7(1), 1–12.

12. Alaiz-Moreton, H., Aveleira-Mata, J., Ondicol-Garcia, J., Muñoz-Castañeda, A.L., García, I., Benavides, C.: Multiclass classification procedure for detecting attacks on MQTT-IoT protocol. Complexity, 2019, pp.1–11.

13. Amanullah, M.A., Habeeb, R.A.A., Nasaruddin, F.H., Gani, A., Ahmed, E., Nainar, A.S.M., Akim, N.M., Imran, M.: Deep learning and big data technologies for IoT security. Comput. Commun. 2020, 151, 495–517.

14. Bahşi, H., Nõmm, S., La Torre, F.B.: Dimensionality reduction for machine learning based IoT botnet detection. In: 2018 15th International Conference on Control, Automation, Robotics and Vision (ICARCV), 2018, pp. 1857–1862.

15. Bassey, J., Adesina, D., Li, X., Qian, L., Aved, A., Kroecker, T.: Intrusion detection for IoT devices based on RF fingerprinting using deep learning. In: 2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC), 2019, pp. 98–104. IEEE

16. Chowdhury, M.M.U., Hammond, F., Konowicz, G., Xin, C., Wu, H., Li, J.: A few-shot deep learning approach for improved intrusion detection. In: 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), 2017, pp. 456–462. IEEE.

17. Dawoud, A., Shahristani, S., Raun, C.: Deep learning and software-defined networks: towards secure IoT architecture. Internet of Things, 2018, 3, pp. 82–89.

18. Diro, A., Chilamkurti, N.: Leveraging LSTM networks for attack detection in fog-to-things communications. IEEE Commun. Mag. 2018, 56(9), pp.124–130.

19. Diro, A.A., Chilamkurti, N.: Distributed attack detection scheme using deep learning approach for Internet of Things. Fut. Gener. Comput. Syst. 2018, 82, pp. 761–768.

20. Elsaeidy, A., Munasinghe, K.S., Sharma, D., Jamalipour, A.: Intrusion detection in smart cities using restricted Boltzmann machines. J. Netw. Comput. Appl. 135, 76–83.

21. Eswari, T., Vanitha, V.: A novel rule based intrusion detection framework for Wireless Sensor Networks. In: 2013 International Conference on

Information Communication and Embedded Systems (ICICES), 2013, pp. 1019–1022.

22. Ferdowsi, A., Saad, W.: Generative adversarial networks for distributed intrusion detection in the internet of things. In: 2019 IEEE Global Communications Conference (GLOBECOM), 2019, pp. 1–6. IEEE

23. Gül, A., Adalı, E.: A feature selection algorithm for ids. In: 2017 International Conference on Computer Science and Engineering (UBMK), 2017, pp. 816–820.

24. Huda, S., Miah, S., Yearwood, J., Alyahya, S., Al-Dossari, H., Doss, R.: A malicious threat detection model for cloud assisted internet of things (CoT) based industrial control system (ICS) networks using deep belief network. J. Parallel Distrib. Comput. 2018, 120, pp. 23–31.

25. Hussain, F., Hussain, R., Hassan, S.A., Hossain, E.: Machine learning in IoT security: current solutions and future challenges. IEEE Commun. Surv. Tutor., 2020, 22(3), pp.1686–1721.

26. Karimipour, H., Dehghantanha, A., Parizi, R.M., Choo, K.K.R., Leung, H.: A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids. 2019, IEEE Access7, pp. 80778–80788.

27. Khraisat, A., Gondal, I., Vamplew, P., Kamruzzaman, J.: Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity, 2019, 2(1), pp. 1–22.

28. Klambauer, G., Unterthiner, T., Mayr, A., Hochreiter, S.: Self-normalizing neural networks. In: Advances in Neural Information Processing Systems, 2017, pp. 971–980

29. Kolias, C., Kambourakis, G., Stavrou, A., Voas, J.: DDoS in the IoT: Mirai and other botnets. Computer, 2017, **50**(7), pp.80–84.

30. Lee, S.J., Yoo, P.D., Asyhari, A.T., Jhi, Y., Chermak, L., Yeun, C.Y., Taha, K.: IMPACT: impersonation attack detection via edge computing using deep autoencoder and feature abstraction. IEEE Access, 2020, 8, pp. 65520–65529.

31. Волошин В. Адаптивні системи виявлення вторгнень для Інтернету речей. Матеріали науково-практична конференція молодих вчених, аспірантів

та студентів «Кібербезпека та комп’ютерно-інтегровані технології» (КБКІТ - 2024), Тернопіль, 2024. – С. 52-56.

32. Волошин В. Моделі систем виявлення вторгнень у мережах Інтернету речей. Матеріали науково-практичного симпозіуму «Захист інформації», Тернопіль, 2024. – С. 28-31.

ДОДАТОК А

Копії публікацій



ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ПОЛІТЕХНІКА»
ГАЛИЦЬКИЙ ФАХОВИЙ КОЛЕДЖ ІМ. В'ЯЧЕСЛАВА ЧОРНОВОЛА

КІБЕРБЕЗПЕКА ТА КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ (КБКІТ – 2024)

науково-практична конференція
молодих вчених, аспірантів та студентів

26–28 серпня 2024
Тернопіль

БЕЗПЕКА ІНТЕРНЕТ РЕЧЕЙ

КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

УДК 004.056(477)

Віктор ВОЛОШИН

Західноукраїнський національний університет

АДАПТИВНІ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ ДЛЯ ІНТЕРНЕТУ РЕЧЕЙ

Вступ. Сучасний світ стає все більш залежним від технологій, що об'єднують фізичні об'єкти в єдину мережу, відомою як Інтернет речей (IoT). Ця технологія відкриває нові можливості для автоматизації, моніторингу та управління, проте разом із цим виникають серйозні виклики у сфері безпеки. Зростаюча кількість підключених пристроїв створює нові вектори для кібератак, що робить традиційні методи захисту недостатніми. У цьому контексті адаптивні системи виявлення вторгнень (IDS) стають критично важливими для забезпечення безпеки IoT-мереж.

Мета: дослідження адаптивних систем виявлення вторгнень для Інтернету речей, зокрема, аналіз імплементації алгоритмів поведінкового аналізу для динамічного виявлення загроз. У рамках цього дослідження буде розглянуто, як ці алгоритми можуть бути використані для виявлення нових і невідомих атак, а також їх вплив на загальний рівень безпеки IoT-мереж. Важливим аспектом є також вивчення ефективності таких систем у зменшенні кількості хибнопозитивних сповіщень, що є критично важливим для підтримки стабільної роботи мережі та довіри користувачів.

1. Імплементація алгоритмів поведінкового аналізу для динамічного виявлення загроз

Сучасний світ стрімко рухається до повної цифровізації, де IoT відіграє ключову роль у трансформації традиційних систем у розумні та автоматизовані рішення. Проте разом із розширенням мережі IoT-пристроїв зростають і загрози кібербезпеки, що вимагає впровадження ефективних механізмів захисту. Особливу увагу слід приділити адаптивним системам виявлення вторгнень, які здатні динамічно реагувати на нові види загроз через аналіз поведінкових патернів пристроїв [1].

У контексті розвитку IoT-технологій традиційні методи виявлення вторгнень, засновані на сигнатурному аналізі, виявляються недостатньо ефективними. Це пов'язано з тим, що кіберзлочинці постійно розробляють нові методи атак, які не мають відомих сигнатур. Саме тому імплементація алгоритмів поведінкового аналізу стає критично важливим елементом сучасних систем безпеки. Поведінковий аналіз дозволяє виявляти аномалії в роботі пристроїв, які можуть свідчити про потенційні загрози, навіть якщо конкретний тип атаки раніше не був зафіксований. Це особливо актуально для IoT-мереж, де різноманіття пристроїв і їх функцій ускладнює застосування традиційних методів захисту [2].

Крім того, важливо зазначити, що адаптивні системи виявлення вторгнень можуть використовувати машинне навчання для покращення точності виявлення загроз. Завдяки здатності навчатися на основі історичних даних, такі системи

можуть адаптуватися до нових умов і змінювати свої алгоритми в залежності від еволюції атак. Це дозволяє не лише знижувати кількість хибнопозитивних сповіщень, але й підвищувати загальний рівень безпеки IoT-мереж. На рисунку 1 зображено загальну архітектуру адаптивної системи виявлення вторгнень для IoT-мережі, яка включає компоненти збору даних, аналізу поведінки та прийняття рішень.

Рисунок 1 - Архітектура адаптивної системи виявлення вторгнень для IoT-мережі

Основним викликом при розробці адаптивних систем виявлення вторгнень є необхідність забезпечення балансу між точністю виявлення загроз та обчислювальною ефективністю. IoT-пристрої часто мають обмежені ресурси, тому алгоритми аналізу повинні бути оптимізовані для роботи в умовах обмеженої продуктивності. Крім того, важливо забезпечити можливість обробки даних у реальному часі, оскільки затримка у виявленні загрози може призвести до серйозних наслідків.

Для ефективного виявлення аномалій у поведінці IoT-пристроїв використовуються різні методи машинного навчання. Серед них особливо варто відзначити алгоритми кластеризації, які дозволяють групувати схожі поведінкові патерни, та методи глибокого навчання, здатні виявляти складні залежності в даних. На рисунку 2 представлено порівняння ефективності різних алгоритмів машинного навчання для задачі виявлення аномалій.

Важливим аспектом роботи адаптивних систем виявлення вторгнень є здатність до самонавчання та адаптації до нових умов роботи мережі. Система повинна постійно аналізувати нові дані та оновлювати свої моделі виявлення загроз. При цьому необхідно враховувати можливість появи нових типів пристроїв у мережі та зміни характеру їх взаємодії. Це вимагає розробки гнучких

, 2

алгоритмів, здатних адаптуватися до змін у структурі мережі та характері трафіку [3].

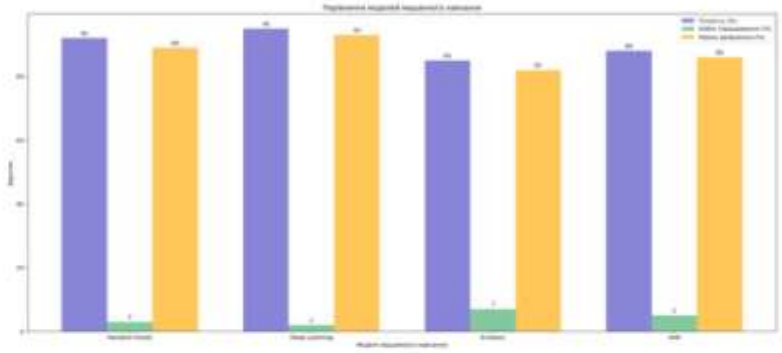

Рисунок 2 - Порівняння ефективності різних алгоритмів машинного навчання

Особливу увагу слід приділити обробці та аналізу мережевого трафіку IoT-пристроїв. На відміну від традиційних комп'ютерних мереж, трафік IoT-пристроїв має свої специфічні характеристики: періодичність передачі даних, обмежений набір протоколів та типів повідомлень, специфічні патерни взаємодії між пристроями. Ці особливості можуть бути використані для більш ефективного виявлення аномалій та потенційних загроз.

На рисунку 3 показано типову структуру аналізу мережевого трафіку в системі виявлення вторгнень для IoT.

Одним з ключових аспектів роботи адаптивних систем виявлення вторгнень є механізм прийняття рішень. Система повинна не тільки виявляти потенційні загрози, але й приймати рішення про відповідні дії для захисту мережі. Це може включати блокування підозрілого трафіку, ізоляцію скомпрометованих пристроїв, сповіщення адміністраторів системи тощо. При цьому важливо забезпечити баланс між безпекою та зручністю використання мережі, уникаючи надмірного блокування легітимного трафіку.

Значну роль у роботі адаптивних систем виявлення вторгнень відіграє процес попередньої обробки даних. Це включає фільтрацію шуму, нормалізацію даних, виділення значущих ознак тощо. Якість попередньої обробки безпосередньо впливає на ефективність роботи алгоритмів аналізу та точність виявлення загроз. Крім того, правильна попередня обробка дозволяє зменшити обсяг даних, що підлягають аналізу, що особливо важливо в умовах обмежених ресурсів IoT-пристроїв.

Важливим аспектом є також забезпечення масштабованості системи. З ростом кількості IoT-пристроїв у мережі зростає і обсяг даних, що потребують аналізу. Система повинна ефективно справлятися зі збільшенням навантаження, зберігаючи при цьому високу точність виявлення загроз. Це може вимагати використання розподілених архітектур обробки даних та оптимізації алгоритмів аналізу.

Окремої уваги заслуговує питання захисту приватності при аналізі поведінки IoT-пристроїв. Системи виявлення вторгнень повинні забезпечувати необхідний рівень безпеки, не порушуючи при цьому конфіденційність даних користувачів. Це особливо актуально для пристроїв, що працюють з чутливими даними, наприклад, медичними чи фінансовими.

,3

Рисунок 3 - Структура аналізу мережевого трафіку.

Імплементація адаптивних систем виявлення вторгнень вимагає також розробки ефективних механізмів зберігання та управління даними. Необхідно забезпечити можливість швидкого доступу до історичних даних для аналізу трендів та паттернів поведінки, при цьому оптимізуючи використання ресурсів пам'яті. Важливо також забезпечити надійне резервне копіювання даних та можливість їх відновлення у випадку збоїв.

Особливу увагу слід приділити питанням інтеграції системи виявлення вторгнень з іншими компонентами інфраструктури безпеки. Це включає взаємодію з системами управління доступом, журналювання подій, моніторингу мережі тощо. Ефективна інтеграція дозволяє створити комплексну систему захисту, здатну протистояти різноманітним загрозам.

У контексті розвитку технологій важливо забезпечити можливість оновлення та модернізації системи виявлення вторгнень. Це включає як оновлення програмного забезпечення, так і модифікацію алгоритмів аналізу відповідно до нових видів загроз та змін у характері мережевого трафіку. Система повинна бути досить гнучкою, щоб адаптуватися до нових вимог безпеки та технологічних змін.

Важливим аспектом є також забезпечення високої доступності системи виявлення вторгнень. Система повинна працювати безперервно, навіть у випадку часткових збоїв або відмов окремих компонентів. Це може вимагати впровадження механізмів резервування та балансування навантаження.

Ефективність роботи адаптивних систем виявлення вторгнень значною мірою залежить від якості початкових даних та правильного налаштування параметрів алгоритмів аналізу. Важливо забезпечити регулярне оновлення бази