МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ АЕРОНАВІГАЦІЇ,
ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ ТА РАДІОЕЛЕКТРОННИХ СИСТЕМ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри

_____ Віктор ГНАТЮК
“_____”_____2023 р.

КВАЛІФІКАЦІЙНА РОБОТА

(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ МАГІСТР

Тема: «Методика автоматизованого аналізу ризиків інформаційної безпеки»

Виконавець: _____ Євгеній ОЛІЙНИК
(підпис)

Керівник: _____ Володимир КЛИМЧУК
(підпис)

Консультанти з окремих розділів пояснювальної записки:

Консультант розділу «Охорона праці» _____ Батир ХАЛМУРАДОВ
(підпис)

Консультант розділу «Охорона навколишнього середовища» _____
_____ Андріан ЯВНЮК
(підпис)

Нормоконтролер: _____ Денис БАХТІЯРОВ
(підпис)

Київ 2023

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет аеронавігації, електроніки та телекомунікацій .
Кафедра телекомунікаційних та радіоелектронних систем .
Спеціальність 172 «Телекомунікації та радіотехніка» .
Освітньо-професійна програма «Телекомунікаційні системи та мережі» .

ЗАТВЕРДЖУЮ
Завідувач кафедри

Віктор ГНАТЮК
“_____”_____2023 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

Олійника Євгенія Олексійовича
(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема кваліфікаційної роботи: «Методика автоматизованого аналізу ризиків інформаційної безпеки»

затверджена наказом ректора від «28» вересня 2023 р. №1965/ст

2. Термін виконання роботи: з 02.10.2023 р. по 31.12.2023 р.

3. Вихідні дані до роботи:.

4. Зміст пояснювальної записки:.

5. Перелік обов'язкового графічного (ілюстративного) матеріалу:.

6. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1	Розробити деталізований зміст розділів кваліфікаційної роботи	02.10.2023-04.10.2023	Виконано
2	Вступ	05.10.2023-08.10.2023	Виконано
3	Бездротові мережі та інформаційна безпека	09.10.2023-22.10.2023	Виконано
4	Методика автоматизованого аналізу ризиків інформаційної безпеки	23.10.2023-05.11.2023	Виконано
5	Розробка методики автоматизованого аналізу ризиків інформаційної безпеки	06.11.2023-30.11.2023	Виконано
6	Охорона праці	01.12.2023-06.12.2023	Виконано
7	Охорона навколишнього середовища	07.12.2023-17.12.2023	Виконано
8	Усунення недоліків та захист кваліфікаційної роботи	18.12.2023-31.12.2023	Виконано

7. Консультанти з окремих розділів

Розділ	Консультант (посада, П.І.Б.)	Дата, підпис	
		Завдання видав	Завдання прийняв
Охорона праці	к.м.н., професор Батир ХАЛМУРАДОВ		
Охорона навколишнього середовища	к.б.н., доц. Андріан ЯВНЮК		

8. Дата видачі завдання: “29" вересня 2023 р.

Керівник кваліфікаційної роботи _____ Володимир КЛИМЧУК
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Євгеній ОЛІЙНИК
(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Кваліфікаційна робота «Методика автоматизованого аналізу ризиків інформаційної безпеки» містить 84 сторінки, 42 рисунки, 9 таблиць, 30 використаних джерел.

ІНФОРМАЦІЙНА БЕЗПЕКА, КОРПОРАТИВНІ МЕРЕЖІ, АВТОМАТИЧНИЙ АНАЛІЗ, МЕРЕЖЕВИЙ ТРАФІК, АНАЛІЗ ТРАФІКУ, ШТУЧНИЙ ІНТЕЛЕКТ, НЕЙРОМЕРЕЖА, МАШИННЕ НАВЧАННЯ, МЕХАНІЗМИ БЕЗПЕКИ, WIRED EQUIVALENT PRIVACY (WEP), WPA (WI-FI PROTECTED ACCESS), WPA2, WPA3, PYTHON, LINUX.

Метою кваліфікаційної роботи є розробка та вдосконалення методик та підходів до автоматичного аналізу ризиків інформаційної безпеки в режимі реального часу з використанням штучного інтелекту на основі аналізу мережевого трафіку в корпоративних мережах.

Об'єктом дослідження є системи безпеки організаційних мереж інформаційного обміну в корпоративних середовищах, що охоплює вивчення принципів функціонування мереж та аналіз факторів які можуть впливати на якість автоматичного аналізу ризиків інформаційної безпеки.

Предметом дослідження є автоматизований аналіз ризиків інформаційної безпеки на основі аналізу мережевого трафіку, що включає в себе аналіз та вдосконалення алгоритмів, які дозволяють аналізувати трафік та виявляти його аномалії.

Наукова новизна дослідження методик автоматичного аналізу ризиків інформаційної безпеки полягає в підвищенні точності та швидкості методик та підходів до автоматичного аналізу ризиків інформаційної безпеки з використанням штучного інтелекту на основі аналізу мережевого трафіку в корпоративних мережах.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

WPA: Захищений доступ Wi-Fi (Wi-Fi Protected Access).

PSK: Фазова маніпуляція (Phase-Shift Keying).

MSK: Головний ключ сеансу (Master Session Key).

PMK: Парний ключ сеансу (Pairwise Master Key).

MAC: Контроль доступу до мережі (Media Access Control).

ОС: Операційна система (Operating System).

WLAN: Безпровідна локальна мережа (Wireless Local Area Network).

IEEE: Інститут інженерів електротехніки і електроніки (Institute of Electrical and Electronics Engineers).

ML: Машинне навчання (Machine Learning).

AI: Штучний інтелект (Artificial Intelligence).

OFDM: Ортогональне частотне мультиплексування (Orthogonal Frequency Division Multiplexing).

MIMO: Множинний вхід та множинний вихід (Multiple-Input and Multiple-Output).

RC4: Шифр Райвеста 4 (Rivest Cipher 4).

SAE: Одночасна автентифікація рівних (Simultaneous Authentication of Equals)

PMF: Захищені кадри управління (Protected Management Frames, PMF).

IoT: Інтернет речей (Internet of Things).

SSID: Символьна назва точки доступу (Service Set Identifier).

віртуальні приватні мережі (VPN).

ВСТУП

Актуальність теми. «Бездротові мережі є однією з найбільш швидкозростаючих областей телекомунікаційної галузі. Бездротові системи, включаючи стільникові, супутникові та бездротові локальні мережі, стали невід'ємною частиною повсякденного життя. У наш час багато людей володіють більш ніж одним пристроєм, здатним підключатися до бездротових систем (як правило, до декількох одночасно).

З підвищенням стандартів і зміною офісної та соціальної культури в цілому бездротові мережі стають не тільки заміною традиційним дротовим мережам, але і помітним поліпшенням їх переваг. Використання бездротової мережі дозволяє не прив'язуватися до конкретного географічного розташування, як в глобальному масштабі при використанні мобільного або супутникового зв'язку, так і в рамках бездротової мережі. У випадку з окремим приміщенням або будівлею важливо відзначити, що це не так. Бездротові технології передачі даних мають значний вплив на продуктивність та ефективність бізнес-процесів, дозволяючи розширити можливості для розвитку та вдосконалення бізнесу за рахунок впровадження мобільних додатків для передачі голосу, даних, відео та інших додатків.

Інфраструктура бездротових мереж є однією з найбільш швидкозростаючих. За прогнозами, до 2024 року кількість точок доступу досягне 628 мільйонів, а середня швидкість бездротового зв'язку локальної мережі досягне 92 МБ/с [6].

Актуальність даної роботи полягає в тому, що підходи до підвищення безпеки локальної бездротової мережі недостатньо описані у відкритих джерелах, що посилює проблему з вразливістю призначених для користувача і, іноді, корпоративних мереж. Недбале ставлення до безпеки бездротової мережі дозволяє легко отримати доступ до конфіденційної інформації, тому питання моніторингу такої мережі є одним з найважливіших на даний момент.

Метою кваліфікаційної роботи є розробка системи аналізу бездротового мережевого трафіку в режимі реального часу, що дозволить підвищити безпеку і

надійність захищеної мережі. Для досягнення поставленої мети необхідно вирішити наступні завдання:

- вивчити та проаналізувати існуючі підходи до аналізу трафіку та їх реалізації;
- розробити структуру аналізатора та варіанти його реалізації;
- розглянути кілька реалізацій сигнатурного аналізу і вибрати найбільш ефективну;
- провести тестування розробленої системи;
- оцінити результати.

Об'єктом дослідження є системи безпеки організаційних мереж інформаційного обміну в корпоративних середовищах, що охоплює вивчення принципів функціонування мереж та аналіз факторів які можуть впливати на якість автоматичного аналізу ризиків інформаційної безпеки.

Предметом дослідження є автоматизований аналіз ризиків інформаційної безпеки на основі аналізу мережевого трафіку, що включає в себе аналіз та вдосконалення алгоритмів, які дозволяють аналізувати трафік та виявляти його аномалії.

Для дослідження та покращення методів аналізу ризиків інформаційної безпеки використовують різноманітні методи та підходи. Основні ***методи дослідження включають:***

- ***Літературний огляд.*** Літературний огляд є важливим етапом дослідження, оскільки він дозволяє зрозуміти поточний стан знань у вибраній області дослідження і визначити прогалини, на які можна звернутися у кваліфікаційній роботі.
- ***Експериментальні дослідження.*** Здійснення експериментів з реальними або симульованими даними для оцінки ефективності запропонованих методів.
- ***Порівняльний аналіз.*** Порівняння результатів розробленої методики з існуючими методиками є важливим етапом дослідження, який допомагає визначити ефективність та конкурентоспроможність вашого підходу.
- ***Використання алгоритмів машинного навчання.*** Інтеграція алгоритмів

машинного навчання для аналізу трафіку в режимі реального часу задля автоматичного реагування на завчасно визначені патерни загроз та задля відслідковування підозрілого трафіку і формування нових патернів відповідно до реальних сценаріїв використання поточної мережі.

- ***Оцінка вартості і ефективності.*** Аналіз вартості розробки та впровадження методики порівняно з потенційними вигодами та ефективністю, розробка стратегії впровадження.

Використання цих методів у науковому дослідженні дає змогу глибше зрозуміти процес автоматизації розпізнавання ризиків інформаційної безпеки та реагування на них в режимі реального часу з допомогою алгоритмів нейромереж та машинного навчання.

Наукова новизна дослідження методики автоматизованого аналізу ризиків інформаційної безпеки полягає у підвищенні точності та швидкості методик та підходів до автоматичного аналізу ризиків інформаційної безпеки з використанням штучного інтелекту на основі аналізу мережевого трафіку в корпоративних мережах які враховують комплексність проблеми та використовують сучасні методи аналізу даних та технології:

- Оптимізація алгоритмів автоматичного розпізнавання аномалій мережевого трафіку що полягає в інтеграції алгоритмів машинного навчання в систему відслідковування трафіку задля автоматизації сценаріїв реагування на тригери та правила які свідчать про можливу атаку.
- Розробка алгоритму відслідковування трафіку для найшвидшого та найефективнішого «прослуховування» пакетів даних, їх аналізу та прийняття рішень щодо підозрілості трафіку.

Отримані результати досліджень з автоматизації ризиків інформаційної безпеки має значуще **практичне значення у багатьох сферах:**

- **Корпоративна інформаційна безпека.** У великих корпораціях, де обробка великого обсягу інформації відбувається щоденно, автоматичний аналіз ризиків може допомагати виявляти потенційні загрози та слабкі місця в системах

безпеки.

- **Фінансовий сектор.** У фінансовому секторі, де конфіденційність та цілісність даних є одними із найважливіших факторів, автоматичний аналіз може допомагати виявляти шахрайство, аномалії у фінансових транзакціях та інші ризики.
- **Органи державного управління.** Для державних установ, які зберігають та обробляють важливу інформацію, автоматичний аналіз ризиків може бути важливим елементом для забезпечення національної безпеки та захисту важливих інфраструктур.
- **Постачання хмарних послуг.** В компаніях, що надають послуги зв'язку та хмарні рішення, автоматичний аналіз може допомагати відслідковувати та захищати дані користувачів від потенційних загроз.
- **Медичний сектор.** У сфері охорони здоров'я, де конфіденційність інформації пацієнтів та доступ до медичних систем є критично важливими, автоматичний аналіз може слідкувати за безпекою та інтегрітетом медичних даних.
- **Розробка програмного забезпечення.** У процесі розробки програмного забезпечення автоматичний аналіз може допомагати виявляти вразливості та помилки безпеки ще на етапі розробки.

Апробація отриманих результатів. Основні положення роботи доповідалися та обговорювалися на таких конференціях:

- Міжнародна науково-практична конференція молодих учених і здобувачів вищої освіти «Політ. Сучасні проблеми науки», м. Київ, 2023 р. .

РОЗДІЛ 1
БЕЗДРОТОВІ МЕРЕЖІ ТА ІНФОРМАЦІЙНА БЕЗПЕКА

1.1. Бездротові мережі

Коли ми говоримо про бездротові мережі, то найчастіше маємо на увазі локальні мережі (WLAN). Цей тип бездротової мережі описаний Інститутом інженерів з електротехніки та електроніки (IEEE) як набір стандартів 802.11 і більш відомий під брендом Wi-Fi. Тут і далі під бездротовою мережею ми будемо мати на увазі локальну мережу Wi-Fi. Відмінність такої мережі від радіомосту, наприклад, полягає в архітектурі. У мережі Wi-Fi завжди є центральна точка – точка доступу, і один або кілька клієнтських пристроїв. Передача даних від клієнта можлива тільки в точку доступу, клієнти не можуть спілкуватися один з одним безпосередньо. Існують також мережі Ad-Hoc, які не мають централізованої точки доступу, а пристрої в такій мережі передають інформацію безпосередньо. Ці мережі організовуються швидко і часто для екстреної передачі інформації, тому безпека в таких мережах є другорядним пріоритетом. Мережі Ad-Hoc зустрічаються набагато рідше, тому в подальшій частині цього дослідження ми зосередимося в основному на звичайних мережах Wi-Fi з точками доступу та клієнтами.

Точка доступу в бездротовій мережі, в найпримітивнішому вигляді, здатна передавати тільки бездротовий клієнтський трафік в дротову мережу, де він і маршрутизується. Практично всі сучасні точки доступу здатні самі маршрутизувати трафік, що дозволяє створити замкнуту локальну мережу за допомогою всього одного пристрою. Виняток становлять мережі, які включають додаткові датчики для розширення зони покриття.

Передача даних в мережах Wi-Fi здійснюється в діапазонах 2,4 ГГц і 5 ГГц. Для роботи точка доступу налаштовується на один конкретний канал в цьому діапазоні і веде мовлення строго по цьому каналу. Ширина такого каналу коливається від 20 до 160 М. Гц.

Дані в бездротовій мережі передаються у вигляді пакетів, як і в класичній

дротовій мережі. На канальному рівні ці пакети інкапсульовані в додатковий заголовок 802.11, який описує параметри передачі та фізичну адресацію пристроїв, що беруть участь у транзакції.

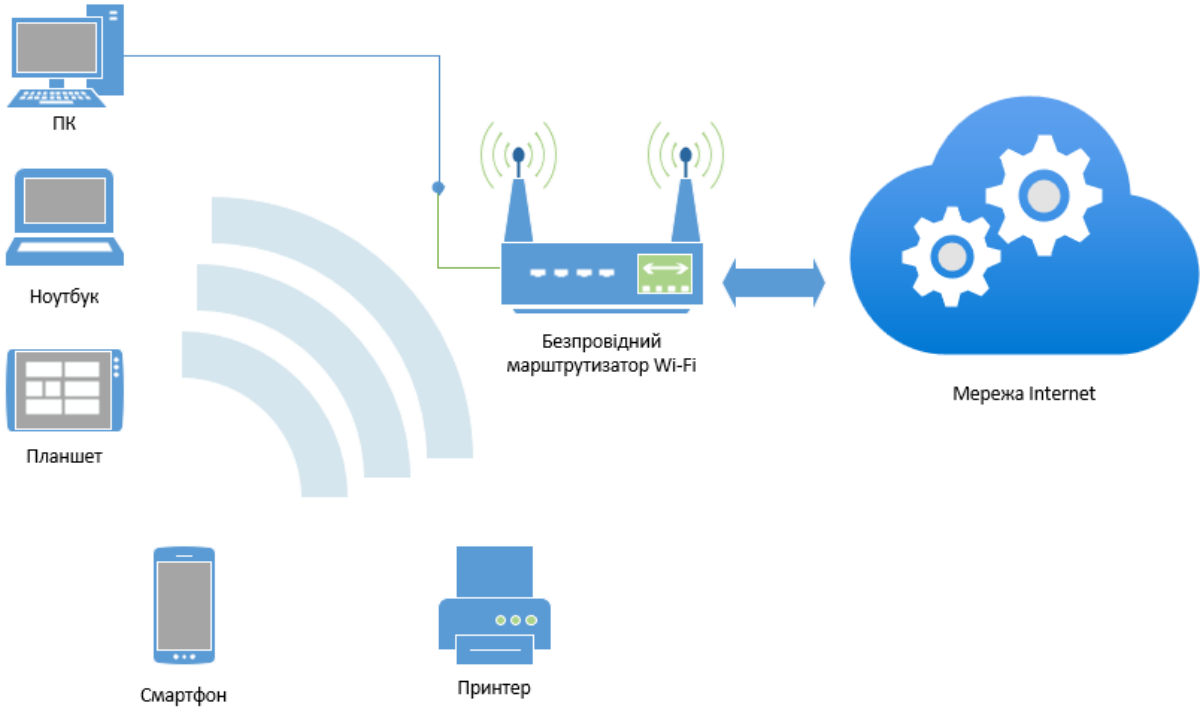


Рис. 1.1. Схема бездротової мережі

Передача даних в бездротових мережах відбувається у відкритому середовищі. Це значно полегшує перехоплення трафіку та втручання в роботу мережі – зловмиснику потрібно лише перебувати в межах чутності атакованої мережі. Тому виникає потреба в дослідженні мережі з метою виявлення шкідливої активності.

Двома основними загальноприйнятими підходами до аналізу мережевого трафіку є сигнатурний аналіз і статистичний аналіз.

Суть сигнатурного аналізу полягає в тому, що існує певна база даних попередньо відомих описів атак (сигнатур) та перевірочний агент що просто порівнює аналізовані пакети з цією базою даних. Якщо пакет або послідовність пакетів збігається, вважається, що відбувається атака, і приймається рішення про відповідь на цю атаку (наприклад, блокування атакуючого пристрою). Перевагою такого підходу є його надійність, передбачуваність і швидкість, але він не може виявити нові

невідомі атаки і атаки, для яких не створено сигнатур (оскільки список сигнатур зазвичай поповнюється вручну розробником системи).

Статистичний аналіз передбачає визначення «норми» трафіку для мережі на основі деяких показників, після чого аналізований трафік порівнюється з цією «нормою» і, якщо є достатнє відхилення, вважається, що здійснюється атака. Великою перевагою цього підходу перед сигнатурним аналізом є те, що він може виявляти атаки «нульового дня» - таки, які ще не досліджені та не описані. Однак статистичний аналіз має і ряд недоліків: точність виявлення атак далека від ідеалу, деякі складні атаки не відрізняються від звичайного трафіку, а система дуже чутлива до неякісних або неправильних навчальних вибірок. Як наслідок, статистичний аналіз наразі не використовується в рішеннях для аналізу трафіку В повній мірі, але тільки примітивно із заздалегідь заданими параметрами або для визначення якісних характеристик мережі.

На даний момент існує безліч програмно-апаратних рішень, що забезпечують сигнатурний аналіз мережевого трафіку в цілому: Snort, Suricata, Cisco Firepower та інші. Однак не існує рішень з відкритим вихідним кодом, які б зосереджувалися на аналізі бездротового трафіку. У даній кваліфікаційній роботі розглянуто етапи розробки такого рішення, а також загальні питання аналізу мережевого трафіку.

1.2. Стандарти сімейства IEEE 802.11

Сімейство стандартів IEEE 802.11 включає в себе ряд стандартів, що описують організацію передачі даних і взаємодії в бездротових мережах. Мережі Wi-Fi включають стандарти IEEE 802.11a, b, g, n, ac і ax. Вони визначають бездротові мережі в діапазонах 2,4 ГГц і 5 ГГц.

Робочий діапазон стандарту IEEE 802.11b (2,4 ГГц), заснований на методі Direct Sequence Spectrum (DSSS), розділений на 14 каналів, які рознесені на 25 МГц для усунення взаємних перешкод. Один з 14 каналів передає дані. Одночасно можна використовувати лише 3 канали, що не перекриваються. При зміні рівня перешкод і відстані від передавача до приймача автоматично змінюється швидкість передачі

даних.

Прийнятий у 1999 році, стандарт IEEE 802.11a був введений у практику лише через два роки. Він описує організацію бездротової мережі в діапазоні 5 ГГц. Цей стандарт частіше використовується в США і Японії, в той час як в Україні і Європі він не набув популярності. У цьому стандарті використовується ортогональне мультиплексування з частотним поділом, OFDM - схема модуляції сигналу. Спочатку основний потік потім розбивається на паралельні підпотоки з відносно низькою швидкістю передачі, після чого для модуляції цих підпотоків використовується відповідна кількість носіїв. Стандарт такий: три обов'язкові – 6, 12 і 24 Мбіт/с, і п'ять додаткових – 9, 18, 24, 48 і 54 Мбіт/с. Крім цього швидкість передачі даних може бути збільшено за рахунок використання декількох каналів одночасно.

Прийнятий у 2003 році, стандарт IEEE 802.11g є вдосконаленням специфікації IEEE 802.11b і реалізує передачу даних у тому ж частотному діапазоні. Перевагою стандарту IEEE 802.11g є підвищена пропускна здатність, в порівнянні з швидкістю передачі даних в радіоканалі 11 Мбіт/с для попереднього стандарту, швидкість стандарту 2003 року становить 54 Мбіт/с. Робочий діапазон специфікації такий самий, як і стандарт 802.11b на частоті 2,4 ГГц. Однак схема модуляції сигналу використовується уже з ортогональним частотним мультиплексуванням. Використання цієї схеми дозволяє збільшити швидкість передачі даних. Цей стандарт відповідає стандарту IEEE 802.11b. Старіші адаптери можуть працювати в мережах 802.11g зі швидкістю до 11 Мбіт/с, тоді як адаптери 802.11g можуть працювати зі швидкістю передачі даних до 11 Мбіт/с для мереж 802.11b.

Стандарт IEEE 802.11n, ратифікований у 2009 році, визначає мережі для обох діапазонів, що використовуються (2,4 ГГц і 5 ГГц). Він реалізує передачу відразу по декількох антенах (до 4 антен), через що максимальна теоретична швидкість передачі за цим стандартом становить 600 Мбіт/с. Така швидкість досягається за рахунок розширення каналу передачі з 20 до 40 МГц і використання технології Multiple-input and Multiple-output (MIMO).

Мережі IEEE 802.11ac працюють виключно в діапазоні 5 ГГц і визначають більш широкі радіоканали 80 і 160 МГц. Також додана більш складна модуляція 256-

QAM і можливість використання MIMO відразу з декількома користувачами (Multi-user MIMO, MU-MIMO). Максимальна кількість одночасних антен збільшено до 8.

Стандарт IEEE 802.11ax був опублікований у 2019 році. Якщо раніше стандарти позиціонувалися як «мережі з високою пропускною здатністю (і дуже високою пропускною здатністю), то цей стандарт позиціонується як «високоефективна мережа». Збільшення швидкості в цьому стандарті досягається не за рахунок використання більш широкого радіоканалу, як в попередніх, а за рахунок використання ортогональної частоти мультиплексування (OFDMA) і більш складна модуляція 1024-QAM. Крім того в стандарті визначені міри тимчасового ущільнення передачі, що дозволяє здійснювати передачу даних великій кількості клієнтів в одному часовому слоті.

1.3. Визначення розв'язуваних завдань

Мережі Wi-Fi забезпечують високу мобільність клієнтів і гнучкість розгортання, жертвуючи при цьому мережевою безпекою. Механізми безпеки, реалізовані в стандартах IEEE 802.11, не вирішили всіх проблем безпеки, що виникають в бездротових мережах. Навіть найновіші стандарти, що впроваджуються, виявляються вразливими, тому інформаційна безпека мереж Wi-Fi -Fi залишається відкритим питанням. Далі ми обговоримо основні існуючі механізми безпеки IEEE 802.11.

1.3.1. WEP

Wired Equivalent Privacy (WEP) був єдиним механізмом захисту в першій версії протоколу 802.11. На практиці з'ясувалося, що він не забезпечує достатнього рівня захисту, і вразливий до безлічі різних атак, в тому числі і тих, які дозволяють швидко При цьому важливо відзначити, що це не так. З появою стандарту IEEE 802.11i у 2004 році WEP вважається застарілим і не рекомендується до використання. Незважаючи на це, існує велика кількість мереж, які дозволяють використовувати WEP як механізм безпеки.

Авторизація в WEP може працювати в двох режимах: відкритому або із загальним ключем. При відкритій авторизації від клієнта не потрібно автентифікаційних даних, такі мережі найчастіше працюють з «білим списком» дозволених MAC-адрес. При роботі з відкритим ключем аутентифікація вписується в 4 повідомлення: клієнт відправляє запит на аутентифікацію з MAC-адресами себе і точки доступу; точка доступу відповідає тестом – 128-бітне випадкове число; клієнт шифрує цей номер відкритим ключем і відправляє його назад, після чого точка доступу розшифровує повідомлення своїм ключем, і якщо отриманий номер збігається з надісланим раніше, клієнт вважається автентифікованим. Точка доступу надсилає відповідь на автентифікацію з результатом. Описаний механізм є одностороннім – клієнт не може автентифікувати точку доступу таким чином.

Для шифрування WEP використовує потоковий шифр RC4 (шифр Rivest 4). Майстер-ключ (40 або 104 біт залежно від версії) використовується для генерації сеансового ключа, який відрізняється для кожного пакета. Цей ключ подається в RC4, а отриманий потік ключів додається за модулем 2 до двійкового пакету.

1.3.2. Wi-Fi Protected Access (WPA) і WPA2

WPA (2003) і незабаром після цього WPA2 (2004) замінили оригінальний механізм безпеки. Уразливості WEP стали доступними для використання навіть користувачами без особливих знань або навичок, тому багато мережевих адміністраторів почали використовувати сторонні рішення безпеки, включаючи 802.1X і віртуальні приватні мережі (VPN). WPA використовує безпечніший протокол Temporal Key Integrity Protocol (TKIP) для шифрування та покращеної перевірки цілісності. WPA впровадила взаємну автентифікацію за допомогою механізмів 802.1X і розширеного протоколу автентифікації (EAP). WPA використовує централізовані сервери автентифікації (наприклад, RADIUS), але існує версія з уже відомим ключем WPA-PSK, яка частіше використовується в приватних мережах.

WPA2 був ратифікований в 2004 році і повністю включений в стандарт IEEE802.11-2007. WPA2 підтримує TKIP, а також CCMP, який базується на Advanced Encryption Standard (AES), який вважається глобальним стандартом шифрування.

WPA2 має сувору ієрархію ключів. На найвищому рівні є завчасно відомий ключ - Pre Shared Key (PSK), якщо автентифікація виконується з використанням механізмів 802.1X. Цей ключ використовується для створення парного майстер-ключа (Pairwise Master Key, PMK), який потім використовується для попарного перехідного ключа (Pairwise Transient Key, PTK) і групового перехідного ключа Group Transient Key (GTK), коли сеанс встановлюється з клієнтом. Ці ключі є унікальними для кожної пари клієнт-точка доступу, оскільки генеруються на основі випадкових чисел, переданих під час встановлення сесії. Потім PTK розбивається на 5 коротших ключів, які знаходяться на найнижчому рівні ієрархії ключів. Тимчасовий ключ (TK) використовується для шифрування одноадресного ключа (unicast) трафіку. EAPOL-ключ для підтвердження ключа (EAPOL-Key KeyConfirmation Key, KCK) і ключ шифрування ключа (EAPOL-Key Key Encryption Key, KEK) використовується для захисту кадрів розширеного протоколу автентифікації в локальній мережі (Extensible Authentication Protocol over LAN, EAPOL). GTK розділяється на два ключі для шифрування/розшифрування і перевірки цілісності групового і широмовного трафіку.і

До виявлення атаки Key Reinstallation Attacks (KRACK) у 2016 році WPA2 вважався безпечним.

1.3.3. WPA3

WPA3, опублікований у 2018 році, вирішує проблеми безпеки, порушені в WPA2, і замінює етап автентифікації на більш безпечну одночасну автентифікацію рівних (Simultaneous Authentication of Equals, SAE). В результаті рукостискання по методу бабки (dragonfly handshake) генерується PMK, який потім використовується в стандартній схемі WPA2 [5]. Крім того, WPA3 також використовує технологію на базі Wi- Fi Enhanced Open, який реалізує шифрування у відкритих мережах без аутентифікації. Ця технологія призначена для запобігання перехоплення трафіку в мережах загального користування.

WPA3 також представляє захищені кадри керування (PMF). Ця технологія застосовує шифрування до певних типів службових кадрів, що унеможливлює

надсилання зловмисником цих кадрів від імені бездротового пристрою без попереднього проникнення в мережу та злому шифрування.

Також є обмеження на кількість спроб підбору пароля в рамках рукостискання, таким чином захищаючи від атак методом перебору за допомогою відомого словника. Це дозволить вам безпечніше використовувати навіть короткі та прості паролі, але більш складні паролі забезпечать кращий захист.

WPA3 було реалізовано в стандарті IEEE 802.1ax. Цей стандарт також визначає кілька технологій для підвищення продуктивності та відмовостійкості мережі.

По-перше, швидкість передачі була збільшена за рахунок використання технології Orthogonal frequency-division multiple access (OFDMA). Це дозволяє передавати інформацію відразу на 9 пристроїв в один часовий проміжок (проти 1 без використання даної технології).

По-друге, WPA3 використовує Base Service Set Coloring (BSS) для підвищення стійкості до перешкод у середовищі передачі. Це додаткова інформація, що передається на фізичному і канальному рівні, що визначає «колір» базової станції. Якщо клієнт отримує дані з декількох точок доступу, він проігнорує їх усі, крім точки з правильним «кольором», з якою він зараз працює.

На даний момент не так багато пристроїв підтримують WPA3, але протокол відкритий для постачальників і, ймовірно, з часом буде прийнятий повсюдно.

1.3.4. IEEE 802.11w

Стандарт IEEE 802.11i зосереджується на конфіденційності та цілісності, але нічого не робить для забезпечення доступності. З моменту появи протоколу IEEE 802.11 сервісні кадри ніяк не захищені, що відкриває перед зловмисником широкий спектр DoS-атак. Стандарт IEEE 802.11w, прийнятий у 2009 році, реалізує шифрування для деяких типів службових кадрів. Крім того, запроваджено новий ключ групового шифрування для шифрування кадрів широкомовних служб. Для захисту від атак запиту асоціації було реалізовано механізм Security Association Query (SA Query). Він полягає в наступному: у відповідь на запит асоціації точка доступу надсилає запит SA Query, і якщо відповідь на цей запит не була підтверджена точкою

доступу, процедура асоціації припиняється. Якщо кінцева станція вже асоційована, але точка отримує новий доступ для асоціації, то вона починає блокувати такі запити на певний час.

Хоча Wi-Fi Alliance вимагає сертифікованих пристроїв для підтримки цього стандарту, багато реалізацій включають його як опцію або як такий, що працює лише з WPA3. Особливо це проявляється на прикладі пристроїв IoT (Internet of Things), які в деяких випадках можуть просто не розуміти захищені кадри управління, що надходять до них, і відмовлятися їх обробляти.

1.4. Існуючі дослідження в області аналізу бездротового трафіку

Описані механізми захисту і той факт, що не всі з них використовуються в реальних мережах, залишають досить багато можливостей для атак зловмисників. На даний момент існує велика кількість готових інструментів, доступних для атак різного рівня складності на бездротові мережі [26]. Багато рекомендацій щодо підвищення безпеки бездротової мережі спирається на оновлення прошивки використовуваних точок доступу, однак, це не завжди можна застосувати у великих мережах, і багато користувачів не вважають за потрібне це робити. Доступність інструментів, недбале використання механізмів безпеки, а також нерозуміння багатьма користувачами принципів роботи бездротової мережі породжує велику кількість загроз безпеці. Глибокий аналіз атак на Wi-Fi мережі представлений в роботі Kolias C та ін [4]. Автори оцінюють описані атаки з точки зору застосовності та завданої шкоди.

Крім вивчення загроз бездротових мереж, Kolias C та ін. пропонують описи основних атак, достатні для їх виявлення. Ці дані будуть використовуватися в даній роботі при написанні підписів для розроблюваної системи.

Існують рішення, які забезпечують аналіз трафіку та функціональність захисту бездротового зв'язку (наприклад, Cisco Adaptive Wireless IPS, HP Mobility Security IDS/IPS, HP Software RFProtect, Zebra Technologies AirDefense), але майже у всіх випадках їх функціональність обмежена менш ніж 10 виявленими атаками. Крім того,

на відкритій платформі наразі немає рішень.

1.5. Атаки на бездротові мережі

1.5.1. Атаки на WEP

Атака PTW названа на честь її творців, Pyshkin, Tews, Weinman, і була виявлена у 2007 році. Вона спрямований на злом ключа WEP за допомогою методів, які були більш ефективними, ніж відомі на той час статистичні методи. PTW сьогодні є стандартною атакою в утилітах для злому WEP.

Як і PTW, атака Hirte зосереджена на зламі секретного ключа WEP, але в цьому випадку вам не потрібна точка доступу, тільки клієнтський пристрій. Для здійснення атаки клієнтський пристрій повинен активно шукати мережі, до яких він був підключений раніше (сьогодні цей механізм увімкнено за замовчуванням у всіх пристроях із адаптерами бездротового зв'язку.) Перехоплюючи пакети, які клієнт використовує для пошуку мережі, зловмисник може прикинутися точкою доступу в цій мережі, а потім клієнт автентифікується та асоціює себе з підробленою точкою, оскільки WEP не перевіряє легітимність точки доступу. Потім зловмиснику потрібно отримати зашифрований ARP або IP-пакет. Потім отриманий пакет розбивається на фрагменти і перетворюється в ARP-запит, після якого багато з цих повідомлень можуть бути використані для складання векторів ініціалізації WEP для відомих атак зі зламом ключів.

Атаки злому секретних ключів в основному пов'язані з WEP, так як ключ для цього протоколу є обчислюваним, і для цього існують ефективні інструменти. Для протоколів WPA, WPA2 і WPA3 таких атак набагато менше, і частіше вони складаються з перебору ключових фраз в словнику, а не обчислення ключа безпосередньо. Далі в цій статті ми не будемо розглядати атаки, які є націлювання на WEP, оскільки протокол офіційно вважається вразливим і не рекомендований до використання. Замість цього розроблювана система може контролювати використання WEP в захищеній мережі, і в разі виявлення видавати попередження про необхідність використання більш безпечних протоколів.

1.5.2. Атаки типу «відмова в обслуговуванні»

Атаки типу «відмова в обслуговуванні» (DoS) на бездротові мережі найчастіше реалізуються за допомогою механізмів управління та контролю стандартів IEEE 802.11. У мережах, які використовують стандарти, старіші за IEEE 802.11n, такі атаки є тривіальними, оскільки кадри керування не шифруються.

Найнебезпечнішою з таких атак є атака фреймів деаутентифікації. У стандартах IEEE 802.11 фрейми деаутентифікації вважаються не запитами, а повідомленнями, і будь-який пристрій, який отримує такий кадр, повинен на нього реагувати. Тому ця атака проста в реалізації і має сильний ефект. Будь-який клієнт, який отримує такий кадр від імені точки доступу, повинен негайно відключитися від бездротової мережі без будь-яких додаткових дій. Після цього ініціюється процедура повторної аутентифікації та асоціювання клієнта, під час якої він не може надсилати трафік. Постійне надсилання фреймів деаутентифікації (флуд) не дозволить клієнту використовувати цю мережу. При використанні широкомовних кадрів ефект поширюється на всі клієнтські пристрої мережі в зоні досяжності слуху зловмисника, а їх одночасна повторна аутентифікація на точці доступу може викликати стрибок навантаження на мережу. Типова схема DoS-атак показана на рис. 1.2.

При використанні фреймів дисоціації час, необхідний клієнту для повторного підключення до мережі, стає вищим [4]. Це пов'язано з тим, що, всупереч стандарту, який після дисоціації зобов'язує пройти тільки процедуру реасоціації, для відновлення роботи всі вивчені авторами клієнтські пристрої після отримання рамки дисоціації розривали зв'язок, відправляли кадри деаутентифікації, а потім знову проходили процедури аутентифікації і асоціації. Флуд з фреймами дисоціації більш ефективний, ніж з фреймами деаутентифікації.

В роботах Mayank Agrwal та ін. приводяться системи для захисту від DoS-атак з фреймами деаутентифікації [7] і кадрами управління енергозбереженням PS-Poll [2]. Однак механізми, представлені в цих роботах, не можуть бути використані для захисту від інших атак.

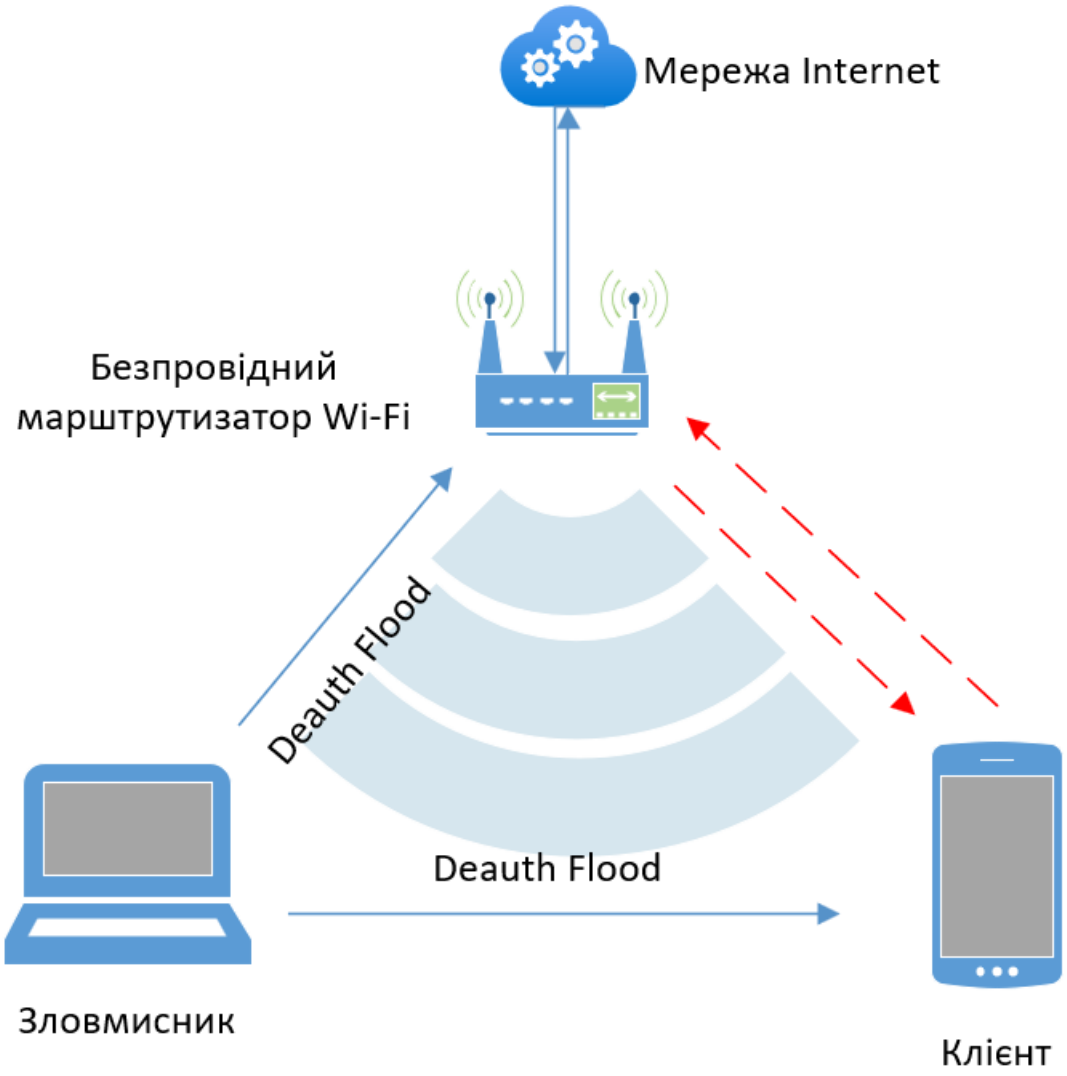


Рис. 1.2. Типовий сценарій DoS-атаки

1.5.3. Фальшиві мережі

Фальшиві мережі створюються кіберзлочинцями для залучення користувачів з метою здійснення на них різних атак. Зазвичай вони мають привабливі ESSID (назви), (наприклад, «Free WiFi», «Open»). Коли користувач підключається до такої мережі, весь його трафік буде доступний зловмиснику. Крім того, це дозволить йому запускати атаки на більш високих рівнях (наприклад, втручання в інтернет-сесію). На канальному рівні неможливо визначити, чи підробна мережа чи ні, а вторгнення в трафік користувача може бути виявлено лише системами безпеки, які аналізують вищі рівні. Користувач зобов'язаний підключатися тільки до довірених мереж.

1.5.4. Злий двійник

Злий двійник (англ. «Evil Twin») — це тип підробленої мережі, яка носить назву ESSID реальної мережі. Точка доступу зловмисника імітує сусідню точку в реальній мережі. Такі мережі використовують механізм, за допомогою якого клієнтські пристрої зазвичай працюють із точкою доступу з сильнішим сигналом. Найчастіше такі атаки здійснюються у відкритих мережах (наприклад, мережі в кафе або аеропорту) або мережах, до яких зловмисник вже має доступ (наприклад, мережа в готелі). Після того, як клієнт підключений до підробленої точки, зловмисник також отримує доступ до трафіку клієнта та можливість здійснювати більш складні атаки.

1.5.5. Неконтрольована точка доступу

Шахрайські точки доступу (англ. «Rogue Access Point») зазвичай забезпечують несанкціонований доступ у корпоративній або домашній мережі та використовуються людьми, які вже мають доступ до мережі та даних компанії (інсайдерами). Такі точки доступу можуть бути встановлені для того, щоб отримати доступ до трафіку інших користувачів або обійти певні механізми безпеки корпоративної мережі (наприклад, використання корпоративної автентифікації). Виявлення та вимкнення цих точок доступу є складним завданням для захищеної мережі.

У разі атаки MitM, Zhendong Wu [3] пропонує змінити метод аутентифікації для пристроїв, відмінних від MitM, що не завжди застосовно.

На рис. 1.3 показана типова схема атак, заснованих на фальшивих мережах, атаках Evil Twin і атаках з неконтрольованими точками доступу.

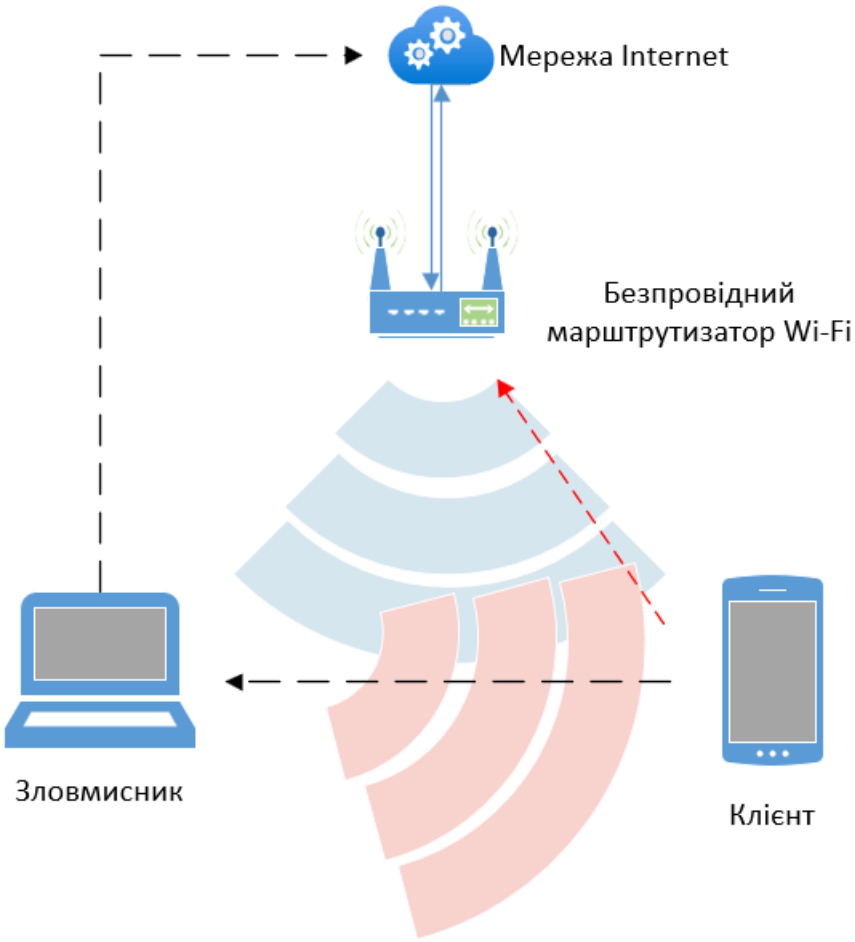


Рис. 1.3. Типова схема атаки MitM

1.5.6. Атаки перевстановлення ключа

Атаки перевстановлення ключа (KRACK) — це кілька атак на WPA2, виявлених у 2016 році Mathy Vanhoef и Frank Piessens [29]. Вони стали основним каталізатором створення більш безпечного стандарту WPA3. Існує кілька різних способів здійснення цієї атаки, але суть її полягає в тому, що клієнт перевстановлює ключі, скидаючи вектор ініціалізації, що дозволяє зловмиснику, який вже перехопив повідомлення з таким же вектором, прочитати надіслане повідомлення. У випадку з WEP і WPA також можлива ін'єкція трафіку зловмисником.

1.6. Визначення завдань для системи аналізу бездротового трафіку

На підставі наведених вище досліджень робимо висновок, що розроблювана система повинна виявляти:

1. аномалії мережевого трафіку (нерегульована поведінка бездротових пристроїв);
2. використання нерекомендованих (застарілих, вразливих) протоколів і механізмів в мережі;
3. конкретний список атак, застосовних до захищеної мережі , що налаштовується і налаштовується адміністратором мережі;
4. інші нешкідливі ситуації, які адміністратори мережі можуть налаштувати самостійно.

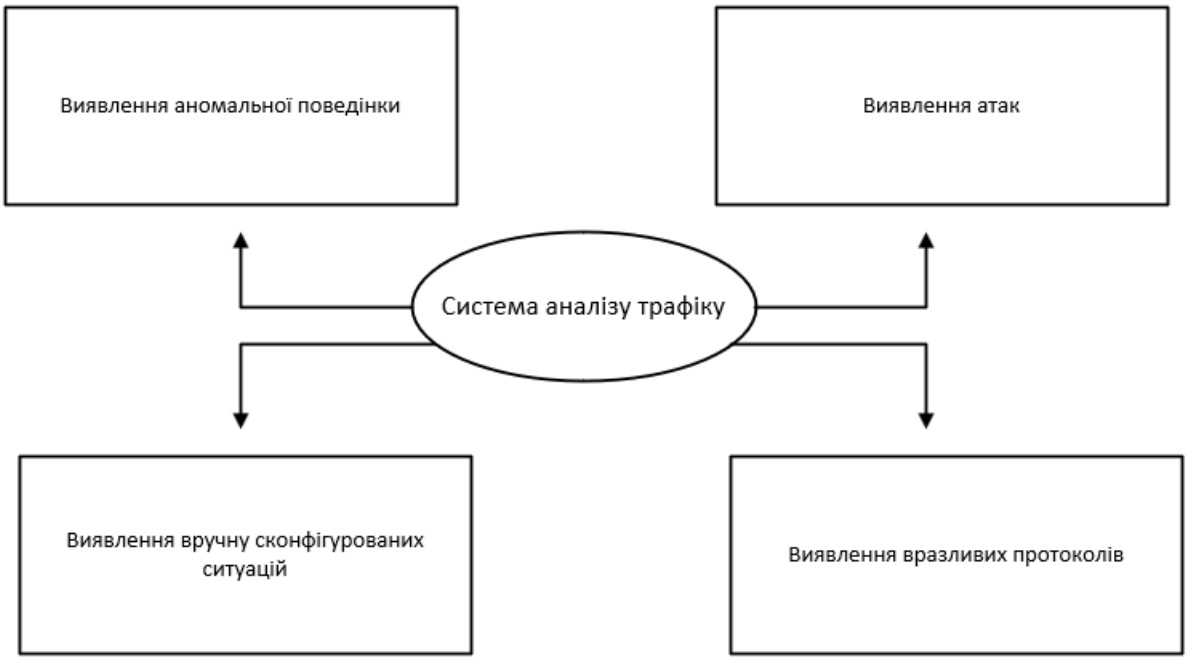


Рис. 1.4. Завдання, які виконує система

Вивчення і тестування атак і мережевих аномалій тягне за собою необхідність використання існуючих або створення нових наборів даних. Ці набори можуть бути представлені як вибірки конкретних полів трафіку в певному форматі, або як дампи мережевого трафіку у форматі pcap. Другий варіант краще вивчити, так як в

майбутньому він може виявити невідомі залежності мережевого трафіку в різних умовах.

Методи створення набору даних, описані Vilela, Douglas W. F. L. та ін. можуть бути застосовні в даній роботі [1].

Виходячи з вивчених мов програмування, вибір основної мови розробки складається з C++ і Python. У таблиці 1.1 наведені основні критерії для порівняння.

Таблиця 1.1

Порівняння основних можливостей C++ та Python

	Python	C++
Спосіб виконання	Інтерпретований	Компільований
Швидкість виконання	Низька	Висока
Швидкість розвитку	Висока	Низька
Кросплатформеність	Так	Ні

В результаті порівняння розробка системи буде здійснюватися на мові програмування Python3.8. Python – це інтерпретована, об'єктно-орієнтована, високорівнева мова. Динамічна семантика і вбудовані складні структури даних роблять його найбільш придатним для прототипування розроблюваного рішення. Крім того, Python широко використовується для взаємодії з мережевою інфраструктурою, що може вплинути на застосовність рішення в майбутньому [15].

У даній роботі під аномалією розуміється вплив на мережу, який може привести до небажаних наслідків для користувача, наприклад, неможливості передачі даних. Оскільки розглядаються аномалії трафіку, то до нього не відносять перешкоди в каналі і фізичний вплив на елементи мережі. В першу чергу оцінюється аномальна поведінка бездротового пристрою (що може свідчити про помилку програмного забезпечення) і навмисні шкідливі впливи, включаючи різні DoS-атаки, а також атаки типу "людина посередині".

Для успішного захоплення бездротового трафіку має бути виконано кілька умов:

1. Сумісна операційна система

Для захоплення можна використовувати будь-яку UNIX-подібну операційну систему. Windows теж можна використовувати, але дуже мало бездротових адаптерів, драйвери яких будуть працювати для цієї ОС.

2. Адаптер бездротового зв'язку з підтримкою режиму монітора

Мікросхеми бездротового адаптера можуть працювати в декількох режимах: Infrastructure (бути кінцевою станцією для точки доступу), Ad-hoc (для участі в одноранговій бездротовій мережі), Master (бути точкою доступу), Monitor (для пасивного прослуховування всіх пакетівв каналі). Перші два режими стандартні для багатьох чіпів, але для багатьох чіпів, захоплення трафіку необхідне для того, щоб чіп міг перейти в режим моніторингу. Драйвери, що дозволяють адаптерам працювати в цьому режимі, найчастіше створюються сторонніми розробниками, а тому таких драйверів для Linux набагато більше. Однак, незважаючи на те, що існують робочі драйвери для конкретного адаптера, іноді він може бути занадто повільним, непередбачуваним або нестабільним у режимі монітора.

Адаптер повинен працювати в тому ж діапазоні, що й захищена точка доступу. Тому, якщо основна захищена мережа працює в діапазоні 5 ГГц, адаптер також повинен підтримувати цей діапазон.

3. Фізична платформа

Передбачається, що датчик буде окремим пристроєм, інтегрованим в мережу. Для розгортання такої системи можна використовувати платформу Raspberry Pi. Він являє собою невеликий пристрій з власним процесором, оперативною і постійною пам'яттю, а також додатковими слотами для розширення. Це дозволить, в тому числі, підключити до нього бездротовий адаптер.

4. Інформація про захищену точку доступу

Зокрема, для успішної роботи необхідно знати канал, в якому веде мовлення ця точка і слухати трафік тільки в цьому каналі. Якщо в мережі є кілька точок доступу потрібно буде встановлювати адаптери для кожної окремої точки. Якщо для мережі відома тільки назва (ESSID), досить легко автоматично шукати точки доступу по декількох каналах і встановлювати їх на каналі з більш сильним сигналом. Так як в

деякихточках (частіше домашніх) для вибору каналу виставлений режим «авто», необхідно періодично перевіряти наявність точки в каналі, що прослуховується.

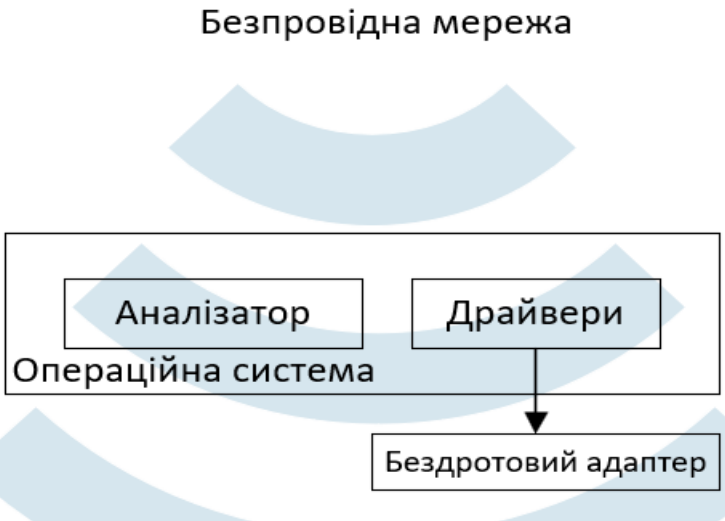


Рис. 1.5. Основними елементами системи, що розробляється

Основним об'єктом, що аналізується, будуть системні кадри (канальний рівень OSI Model Layer). Також буде розглянуто додатковий заголовок Radiotap, в який пакет інкапсульовується приймальним адаптером. Далі розглянемо основні протоколи, що застосовуються в досліджуваній системі.

1.6.1. Radiotap

Radiotap – це протокол, який передає додаткову інформацію про отриманий кадр [27]. Якщо драйвер приймального адаптера підтримує цей протокол, кадр буде інкапсульований у нього під час отримання. Поля в цьому протоколі надають додаткову інформацію, таку як рівень шуму та сигналу, номер антени, частота каналу, бітрейт, чи фрагментований кадр, чи приєднана до нього контрольна сума та часова прийому кадру. Крім того, протокол дозволяє розширити цей заголовок і додатково визначити власні поля.

```
Radiotap Header v0, Length 18
   Header revision: 0
   Header pad: 0
   Header length: 18
 > Present flags
 > Flags: 0x10
   Data Rate: 1.0 Mb/s
   Channel frequency: 2432 [BG 5]
 > Channel flags: 0x00a0, Complementary Code Keying (CCK), 2 GHz spectrum
   Antenna signal: -34 dBm
   Antenna: 0
 > RX flags: 0x0000
```

Рис. 1.6. Приклад заголовка Radiotap

1.6.2. Заголовок IEEE 802.11

Заголовок канального рівня в бездротових мережах Wi-Fi визначається стандартами IEEE 802.11. Він визначає тип і підтип кадру, що передається, його напрямок, а також те, чи ретранслюється кадр і шифрується. Цей заголовок містить MAC-адреси пристроїв, що беруть участь у передаванні (у деяких випадках до чотирьох адрес). Це основний заголовок, який потрібно перевірити на наявність службових кадрів, таких як фрейми деавтентифікації. Оскільки різні сценарії передають серію різних підтипів кадрів у безпроводових мережах, можна відстежувати це поле, наприклад, коли новий пристрій підключається до мережі або переміщується до найближчої точки доступу.

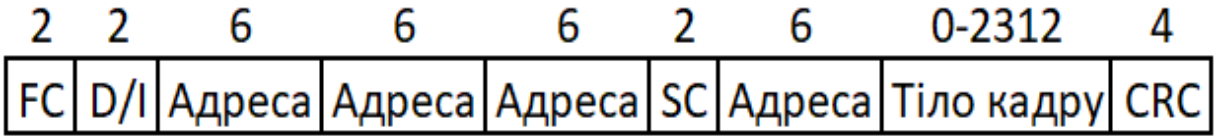


Рис. 1.7. Структура кадру Wi-Fi

На рис. 1.7 наведена структура кадру Wi-Fi, де:

- (Frame Control) Керування кадром: Це поле містить інформацію про тип кадра, підтип та інші управляючі прапори;
- ID (Duration/ID) Тривалість: Це поле містить інформацію про час, протягом якого канал буде зайнятий для передачі поточного кадра, а

також ідентифікатор.

- (Address 1, 2, 3, 4): Адреса 1, 2, 3, 4 Ці поля містять MAC-адреси пристроїв, які беруть участь у взаємодії. Які адреси використовуються, залежить від типу та підтипу кадра.
- (Sequence Control) Керування послідовністю: Це поле містить інформацію про послідовність кадрів для управління порядком доставки.
- (Frame Body) Тіло кадра: Це поле містить непосреджньо дані, які передаються в кадрі. Формат та вміст цього поля залежать від типу кадра.
- FCS (Frame Check Sequence) (Контрольна послідовність кадра): Це поле містить контрольну суму (CRC), яка використовується для перевірки цілісності даних в кадрі.

1.6.3. Кадри управління IEEE 802.11

Кадри керування — це тип кадру 802.11, який визначає такі сценарії, як зв'язок і повторне зв'язування з точкою доступу, дисоціація, автентифікація та деавтентифікація, а також дії, які відповідають за інші транзакції служби в безпроводовій мережі. Весь заголовок ділиться на дві частини – фіксовані параметри, які містять різну інформацію в залежності від типу кадру, а також теговані параметри. Вони визначають, наприклад, ім'я мережі (SSID), що транслюється точкою доступу, доступні швидкості передачі, інші можливості пристрою, а також інформація про виробника, яка визначається довільно. Ці кадри визначають взаємодію між точкою доступу та клієнтом у мережі. Наприклад, фрейми деаутентифікації надсилаються точкою доступу клієнту, коли точка доступу чомусь відключає клієнта. Крім того, такий кадр може бути відправлений клієнтом на точку доступу, щоб сповістити її про розірвання з'єднання. Маячкові кадри періодично надсилаються точкою доступу, сповіщаючи про її присутність у мережі та можливі параметри підключення. Коли клієнт шукає певну мережу, він надсилає запити на зондування (англ. Probe Request). Якщо такі кадри будуть відправлені без конкретної адреси на трансляцію, клієнт буде знати про всі точки, що знаходяться поблизу.

1.6.4. Кадри моніторингу IEEE 802.11

Кадри моніторингу в бездротових мережах керують доступом пристроїв до середовища передачі. Цей тип включає в себе наступні підтипи кадрів: Запит на відправку (Request to Send, RTS), вільно для відправки (Clear to Send), Підтвердження (Acknowledgement), управління енергозбереженням (Power-Save Poll). Наприклад, коли RTS/CTS механізм увімкнено, клієнт повинен надіслати RTS-кадр і запросити дозвіл зайняти радіосередовище перед передачею кадру даних. Якщо кінцевий пристрій підтримує механізм PS-Poll, точка доступу збереже кадри, спрямовані на нього до буфера, поки він неактивний. Як тільки пристрій вийде з режиму енергозбереження, він направить кадр PS-Poll на точку доступу, запитуючи кадри, адресовані йому. Інтервали, через які пристрій вимикається і включається, визначаються виробником пристрою.

ВИСНОВКИ ДО РОЗДІЛУ 1

Були вивчені основні механізми захисту і атак на бездротові мережі, а також дослідження, що описують сигнатури атак і прийоми створення наборів даних для вивчення сигнатур. Оскільки на даний момент не існує відкритих рішень з необхідним функціоналом, розробку власної системи можна вважати доцільною. Висуваються вимоги до розроблюваної системи і визначаються основні інструменти створення системи.

РОЗДІЛ 2
МЕТОДИКА АВТОМАТИЗОВАНОГО АНАЛІЗУ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

В даний час важливим завданням в області інформаційної безпеки є виявлення атак на комп'ютерні системи і мережі. Успішна комп'ютерна атака може призвести до втрати інформації, несанкціонованого використання інформаційних ресурсів, спотворення критично важливих даних. Це актуалізує необхідність розробки та використання ефективних методів і засобів виявлення мережевих атак для захисту інформації в комп'ютерних системах і мережах.

Під системою виявлення атак зазвичай розуміють програмно-апаратні або апаратно-програмні засоби, призначені для виявлення несанкціонованого доступу до комп'ютерної системи або мережі або управління ними [17]. Системи виявлення атак використовуються для виявлення певних видів зловмисної діяльності, які можуть поставити під загрозу безпеку комп'ютерної системи. Це включає мережеві атаки на вразливі служби, атаки підвищення привілеїв, несанкціонований доступ до конфіденційних файлів і шкідливе програмне забезпечення. Прикладом мережевої атаки є сканування портів комп'ютера для виявлення вразливостей, які можуть бути використані для отримання несанкціонованого доступу.

Існує велика кількість методів реагування на мережеву атаку. Всі вони вимагають точності, щоб своєчасно її виявити. Поширеність розподілених мережевих систем і незахищених мереж, таких як Інтернет, істотно актуалізувала необхідність розробки і вдосконалення систем виявлення атак.

Всі мережеві атаки можна звести до аномалій і зловживань. Виявлення аномалій виявляє дії, які відрізняються від шаблонів, установлених для користувачів. При цьому, як правило, створюється база даних, що містить профілі контрольованих видів діяльності.

Виявлення зловживань передбачає порівняння активності користувача з відомими моделями поведінки зловмисника, який намагається проникнути в систему. У той час як виявлення аномалій зазвичай використовує пороговий моніторинг, щоб

визначити, коли досягнуто певного встановленого ліміту, методи виявлення зловживань часто використовують підхід, заснований на правилах, який описує сценарії атак. Ядро виявлення реагує на потенційні атаки, якщо дії користувача відповідають встановленим правилам. Наявність вичерпних баз знань з такими правилами є найважливішим аспектом для систем виявлення атак. Такі системи вимагають постійного оновлення баз знань, щоб залишатися актуальними. Вони часто не в змозі виявити сценарії атак, які можуть відбуватися протягом тривалого періоду часу. Незначні зміни в послідовності дій під час атаки можуть вплинути на процес порівняння правил активності до такої міри, що атака не буде виявлена.

2.1. Можливості використання нейронних мереж для аналізу трафіку

Мінливий характер мережевих атак вимагає розробки гнучкої, адаптивної системи захисту, здатної аналізувати великі обсяги мережевого трафіку при постійно мінливих умовах мережевої активності. Альтернативою системам, заснованим на правилах, є нейронні мережі [18]. На відміну від експертних систем [8], які можуть дати користувачеві однозначну відповідь щодо того, чи відповідають розглянуті характеристики атаки характеристикам, закладеним в базу знань, нейронна мережа аналізує інформацію і дає можливість оцінити, чи відповідають аналізовані дані тим характеристикам, які вона навчилася розпізнавати [14].

Розглянемо властивості нейронних мереж, що визначають їх переваги при виявленні мережевих атак [10]:

- гнучкість нейронної мережі (мережа здатна аналізувати дані мережевого трафіку в умовах їх спотворення або неповноти);
- висока швидкість обробки (оскільки захист обчислювальних ресурсів вимагає оперативної ідентифікації атак, швидкість обробки в нейронній мережі може бути достатньою для реагування в режимі реального часу на атаки, що відбуваються, до того, як в системі виникне непоправна шкода);
- передбачуваність (вихід нейронної мережі можна інтерпретувати у вигляді ймовірності, що дає можливість спрогнозувати подальший розвиток атаки;

нейромережева система виявлення вторгнень може визначати ймовірність того, що окрема подія або серія подій вказує на атаку, і вживати захисних заходів до успішної реалізації атаки);

- здатність аналізувати характеристики навмисних атак і виявляти елементи, не схожі на ті, що спостерігалися в мережі при її навчанні (нейромережу можна навчити розпізнавати відомі підозрілі події з високим ступенем точності, а також можна використовувати ці знання для виявлення атак, які не точно збігаються з характеристиками попередніх вторгнень).

У кваліфікаційній роботі розглядаються можливості та ефективність використання нейронної мережі для діагностики аномальної мережевої активності [16]. Мережева активність штучно імітується шляхом сканування портів локального комп'ютера. Такі атаки можуть бути реалізовані різними сканерами безпеки для виявлення вразливостей атакованого хоста.

2.2. Розробка методики автоматизованого аналізу ризиків інформаційної безпеки

Для збору даних про мережеву активність та формування навчальної вибірки для нейронної мережі була розроблена наступна методика:

- виділення сегмента локальної мережі;
- розробка програмного забезпечення ;
- моніторинг мережі в умовах нормальної мережевої активності;
- моніторинг мережі в умовах аномальної мережевої активності;
- обробка даних та формування навчальної вибірки;

На першому етапі методології вибирається сегмент локальної мережі, в рамках якого будуть збиратися дані про мережеву активність. Для цього знадобляться два комп'ютери з виходом в локальну мережу. Перший комп'ютер використовується як «жертва». На ньому встановлюється аналізатор мережевого трафіку. На другому комп'ютері встановлюється сканер безпеки для сканування портів першого хоста і таким чином імітації аномальної мережевої активності.

На другому етапі методології розробляється програмне забезпечення, необхідне для збору та аналізу мережевого трафіку, сама нейронна мережа, а також програмне забезпечення для моделювання аномальної мережевої активності.

Третій етап призначений для збору даних про звичайну мережеву активність. При цьому використовується тільки перший комп'ютер, на базі якого здійснюється спостереження за мережею. Дані про мережеві пакети зберігаються в спеціальному файлі журналу. Потім ця інформація використовується для формування навчальної вибірки.

На четвертому етапі використовується другий комп'ютер, на якому встановлюється сканер безпеки, що імітує атаки на аномальну мережеву активність. Сніффер першого комп'ютера аналізує перехоплені пакети і збирає дані про аномальну мережеву активність, які також входять в навчальну вибірку.

П'ятий етап використовується для обробки даних і формування навчальної вибірки. Обробка потрібна, щоб привести дані в форму, придатну для навчання нейронної мережі.

Розглянемо застосування описаної методики для збору даних і формування навчальної вибірки для нейронної мережі. Для моніторингу мережі при нормальній мережевій активності потрібен один комп'ютер, підключений до локальної мережі (див. рис. 2.1).

Рис. 2.1. Схема моніторингу сегмента локальної мережі при нормальній мережевій активності

Мережевий аналізатор, встановлений на комп'ютері, перехоплює і аналізує мережевий трафік з метою визначення наступних параметрів: часу отримання пакета, його протоколу (TCP-пакет, UDP-пакет, ARP-пакет і т.д.), порту джерела і призначення пакета, а також розміру даних в пакеті. В результаті роботи мережевого аналізатора формується спеціальний файл, який містить значення параметрів пакета наступного вигляду:

Рис. 2.2. Значення параметрів пакета

Отримані дані формують статистику нормальної мережевої активності, яка в майбутньому буде включена в навчальну вибірку.

Для збору даних про аномальну мережеву активність потрібно мати два комп'ютери, підключені до мережі, як показано на рисунку 2.3.

Рис. 2.3. - Схема моніторингу сегмента локальної мережі в умовах аномальної мережевої активності

Мережевий аналізатор, встановлений на першому комп'ютері, вирішує ті ж проблеми, що і при його використанні для збору даних про звичайну мережеву активність. Сканер безпеки проводить сканування портів першого комп’ютера. Разом з цим аналізатор виконує сканування і виявляє кожен факт виконування сканування та зберігає ці дані в журнал тривог у наступному вигляді:

```
13:39:01:109 > IP-233.167.11.213 was probed by IP-162.244.119.172 on port 6600
13:39:01:109 > IP-233.167.11.213 was probed by IP-162.244.119.172 on port 6601
13:39:01:140 > IP-76.137.207.238 was probed by IP-162.244.119.172 on port 6969
13:39:01:156 > IP-81.78.20.43 was probed by IP-162.244.119.172 on port 7000
13:39:29:859 > IP-155.27.173.238 was probed by IP-162.244.119.172 on port 80
13:39:31:906 > IP-155.27.173.238 was probed by IP-162.244.119.172 on port 80
13:39:33:953 > IP-155.27.173.238 was probed by IP-162.244.119.172 on port 80
```

Рис. 2.4. Дані в файлі журналу тривог

У цьому журналі дані представлені в форматі «час» - «відсканована адреса» - «адреса, з якої було виконано сканування» - «порт сканування». Ці дані дозволяють ідентифікувати з точністю до 0.001 секунди ті пакети, які становлять загрозу для комп'ютера і характеризують аномальну мережеву активність.

Для формування навчальної вибірки необхідно звести отримані дані про мережеву активність до форми, придатної для навчання нейронної мережі. Входами мережі є такі параметри мережевого трафіку:

- тип протоколу PType (TCP, UDP і т. д.);
- вихідний порт Port1;
- порт призначення Port2;
- розмір пакета Size

Виходом мережі є єдиний параметр Activity.

Оскільки нейронні мережі здатні обробляти числову інформацію, значення вхідних і вихідних параметрів мережі повинні бути закодовані як цілі числа. Для кодування типу протоколу використовуються TCP = 0, UDP = 1, ICMP = 2 і Unknown = 3. Значення полів Source Port, Destination Port і Packet Size без змін. Значення вихідних параметрів «Індикатор аномальної мережевої активності» кодуються як 0 для нормальної активності та 1 для аномальної активності.

В результаті дані про мережеву активність можуть бути представлені в наступному вигляді (див. Таблицю 2.1).

Таблиця 2.1

Дані про мережеву активність

Вхідні параметри				Вихідний параметр
Ptype	Port1	Port2	Size	Activity
1	53	3943	164	0
0	1609	352	62	1
…	…	…	…	…

Отримані дані являють собою вибірку для навчання нейронної мережі і визначення умов перебігу норми і виникнення аномальної мережевої активності. Виходячи з умови завдання, нейронна мережа повинна класифікувати простір вхідних ознак на два класи: нормальна (0) і аномальна (1) мережева активність. В якості мережевої моделі була обрана багатошарова нейронна мережа прямого поширення [9,11]. На рисунку 2.5 представлена архітектура моделі нейронної мережі діагностика аномальної мережевої активності.

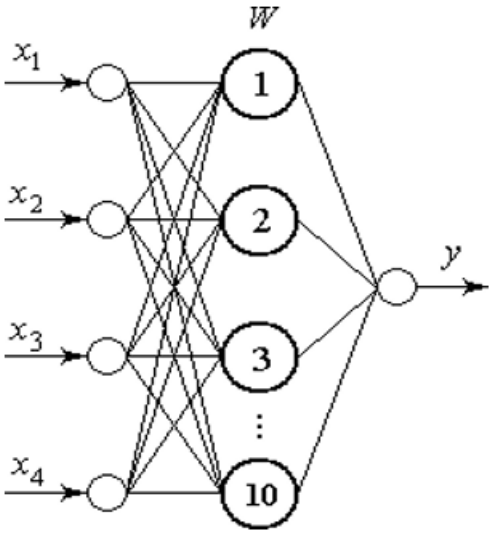


Рис. 2.5. Архітектура моделі нейронної мережі

Як видно з цього малюнка, мережа складається з чотирьох вхідних нейронів, заданих вхідною ознакою вектора X = {x1, x2, x3, x4}, і одного вихідного нейрона, значеннями якого є числа «0» або «1». Нейронна мережа має один прихований шар, що складається з десяти нейронів, що обробляють вхідні дані. Вектор W радає набір ваг нейронів прихованого шару.

Для побудови моделі нейронної мережі ,було задіяно бібліотеку TensorFlow для роботи з нейронними мережами та scikit-learn для роботи з даними [13,19]. Для оцінки точності моделі діагностики аномальної мережевої активності були проведені експерименти на тестовій вибірці даних, за результатами яких були розраховані два види похибок:

- помилка типу 1, коли мережева активність є ненормальною, але не

діагностується нейронною мережею як аномалія.

- другий тип помилок, коли мережева активність не є аномальною, а помилково діагностується нейронною мережею як аномалія.

Для обчислення першого типу похибок використовувалася наступна формула:

$$E_1 = \frac{n_1}{N_1}, \tag{2.1}$$

де n_1 – кількість випадків аномальної мережевої активності, класифікованих як нормальна; N_1 – загальна кількість екземплярів у тестовій вибірці, які ідентифікують аномальну мережеву активність.

Для обчислення другого типу похибок використовувалася наступна формула:

$$E_2 = \frac{n_2}{N_2}, \tag{2.2}$$

де n_2 - кількість прикладів нормальної мережевої активності, класифікованих як аномалія; N_2 - загальна кількість прикладів у тестовій вибірці, що визначають нормальну мережеву активність. Результати експериментів з оцінки точності нейромережевої моделі для діагностики аномальної мережевої активності були зафіксовані в таблицях 2.2 і 2.3.

Таблиця 2.2

Результати діагностики для розрахунку помилки першого роду

№	Еталонне вихідне значення	Розраховане вихідне значення	Результат діагностики
1	1	0,99	Вірно
2	1	0,06	Помилка I роду
…	…	…	…

Таблиця 2.3

Результати діагностики для розрахунку помилки другого роду

№	Еталонне вихідне значення	Розраховане вихідне значення	Результат діагностики
1	0	0,0000021	Вірно
2	0	0,86	Помилка II роду
…	…	…	…

Похибки першого та другого типів склали 0,04 та 0,06 відповідно, що доводить ефективність використання нейронної мережі для вирішення задачі діагностики аномальної мережевої активності. Практична цінність запропонованого підходу полягає в можливості побудови ефективних систем виявлення вторгнень на основі нейромережевих моделей. На рис. 2.6 показана принципова схема використання нейронної мережі в складі інтелектуальної системи діагностики аномальної мережевої активності. Як видно з рис. 2.6, значення параметрів мережевих пакетів, що складають трафік локальної мережі, надходять на вхід інтелектуальної системи, ядром якої є навчена нейронна мережа. Модуль прийняття рішень аналізує вхідні значення і формує відповідь системи про тип мережевої активності. В рамках цього алгоритму розв'язується задача нейромережевої діагностики аномальної мережевої активності.

2.3. Адаптивність методики

Слід зазначити, що інтелектуальна система діагностики аномальної мережевої активності, побудована на базі нейронної мережі, є адаптивною. У разі некоректного виявлення активності в локальній мережі, інформація про помилки може накопичуватися в спеціальній базі даних. З певною періодичністю система може перенавчати нейронну мережу з урахуванням даних помилкової класифікації мережевих пакетів.

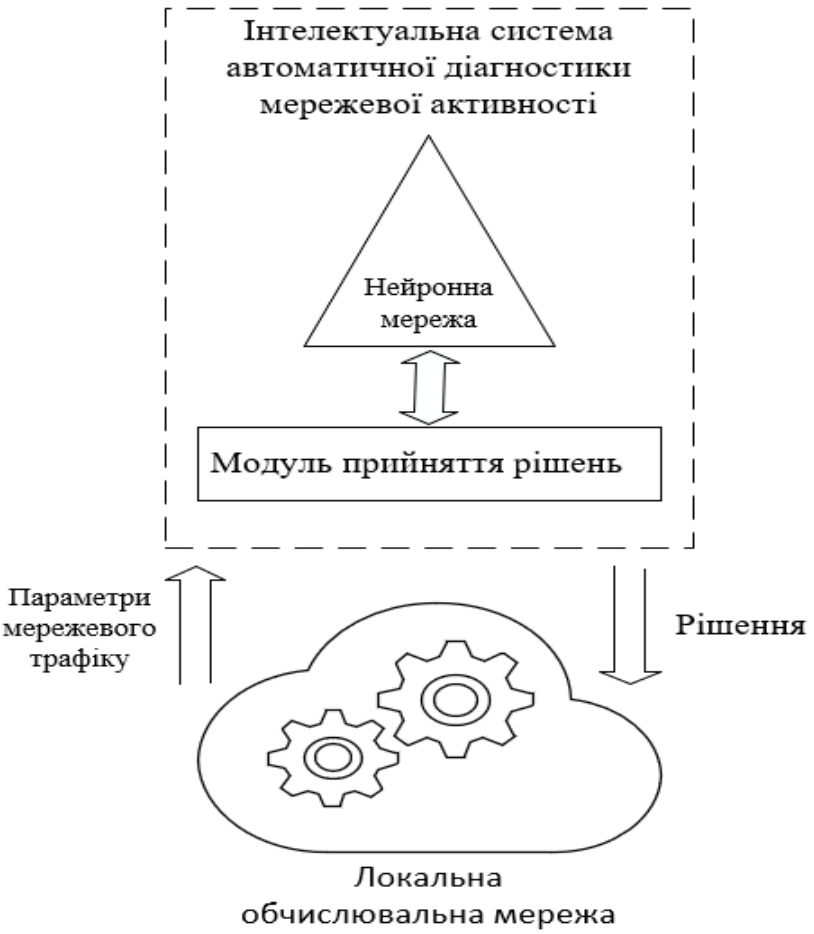


Рис. 2.6. Схема використання нейронної мережі в складі системи діагностики аномальної мережі

Таким чином, отримана модель є адаптивною системою штучного інтелекту, що дозволяє з високим ступенем точності вирішити завдання діагностики аномальної мережевої активності

РОЗДІЛ 3
РОЗРОБКА МЕТОДИКИ АВТОМАТИЗОВАНОГО АНАЛІЗУ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1. Структури системи аналізу аномалій

У дротовій мережі пристрій фільтрації безпеки зазвичай розміщується перед шлюзом, через який спрямовується трафік. Таким чином, шкідливий і небажаний трафік не покидає локальну мережу. Однак у бездротовій мережі неможливо встановити фільтруючий пристрій між клієнтським пристроєм і маршрутизатором, оскільки вони не з'єднані обмеженим фізичним середовищем. Передані радіохвилі, навіть якщо їх чує фільтруючий пристрій, все одно досягнуть клієнтського пристрою кілька разів пізніше. Це унеможливлює проактивне реагування на шкідливий трафік у бездротовій мережі. Для аналізу трафіку в мережі пропонується використовувати окремий пристрій з бездротовими інтерфейсами для захоплення трафіку, який би міг управляти точкою доступу і маршрутизатором мережі, а також відправляти дані на контролер бездротової мережі, якщо він є.

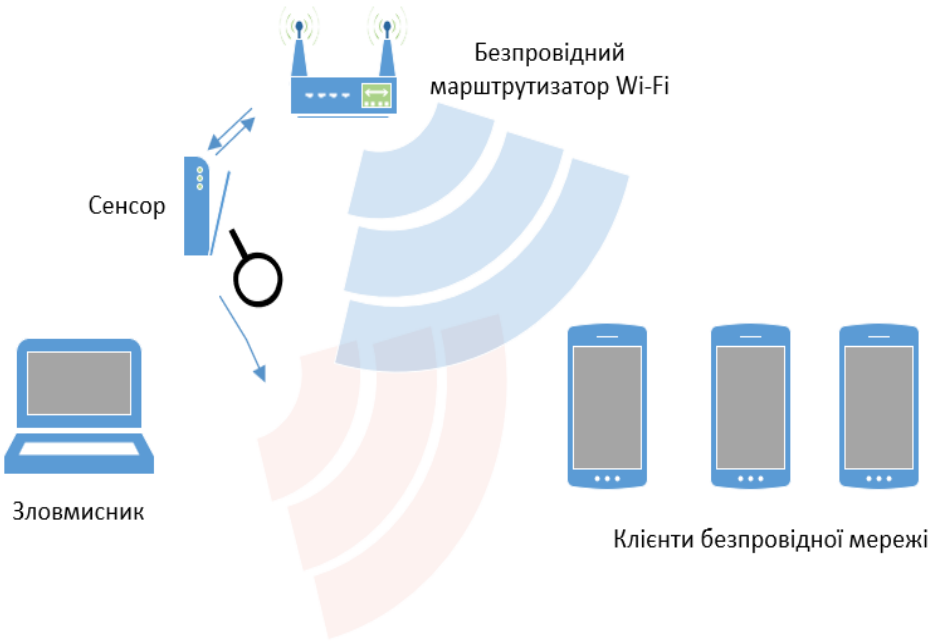


Рис. 3.1. Приклад інтеграції датчика в мережу

Розроблювана система ділиться на апаратну частину, що включає в себе платформу Raspberry Pi і адаптер бездротового зв'язку, і програмну частину, що включає в себе операційну систему, драйвери бездротового адаптера, розроблену програму на мові Python.

ЇЇ можна розділити на кілька логічних компонентів: джерело трафіку, аналізатор трафіку, перевірочний агент і правила безпеки.

3.2. Джерело трафіку

Для захоплення трафіку бездротовий інтерфейс необхідно перевести в режим моніторингу. Для цього виконуються такі команди:

```
ifconfig wlan0 down #  вимкнути радіоінтерфейс
ifconfig wlan0 mode monitor # перевод радіоінтерфейсу в режим монітору
ifconfig wlan0 up # ввімкнути радіоінтерфейс
```

Рис. 3.2 Команди для активації режиму моніторингу

Для успішного налаштування можуть знадобитися додаткові команди (наприклад, перезапуск мережевої служби), залежно від використовуваного адаптера та операційної системи.

Після цього інтерфейс слід встановити в тому ж каналі, в якому працює точка, що захищається. Дізнатися його можна з налаштувань точки, коли вона встановлена вручну, або за допомогою таких команд:

```
netsh wlan show all # на windows
iwlist wlan0 scanning # в Linux
```

Рис. 3.3. Команди для визначення каналу роботи точки доступу

Встановити інтерфейс на потрібний канал можна за допомогою команди:

```
...
>>> iwconfig wlan0 channel <номер каналу>
```

Рис. 3.4. Встановлення інтерфейсу на потрібний канал

Потім програма створює "сирий" сокет, який приймає пакети без їх обробки в мережевому стеку:

```
s = socket.socket(socket.AF_PACKET, socket.SOCK_RAW,
socket.htons(ETH_P_ALL))
s.bind(('wlan0', 3)) # привязка сокета к интерфейсу
```

Рис. 3.5. Створення сирого сокета

Тут:

socket.AF_PACKET — це сімейство адрес у Linux, яке дозволяє відкритому сокету передавати дані безпосередньо до програми без обробки мережевим стеком операційної системи.

socket.SOCK_RAW – тип сокета, що забезпечує доступ до даних нижчого рівня;SockeT.Htons(ETH_P_ALL)) – тип протоколів, які нам потрібні отримувати. В даному випадку він позначає всі вхідні протоколи.

В подальшому виклик функції recv() на цьому сокеті поверне необроблені мережеві пакети, включаючи канальний рівень, який використовує адаптер. У нашому випадку почнеться обробка пакета протоколом Radiotap для отримання додаткової інформації про приймальний носій.

3.3. Аналізатор трафіку

Всі мережеві пакети можуть бути розкладені на набір протоколів і полів цих протоколів. Крім того, часто зустрічаються складні поля, наприклад, прапорцеві поля. Кожен такий атрибут може бути представлений у вигляді маршруту по пакету – від протоколу до імені поля – і його значення. В результаті кожен мережевий пакет може бути представлений у вигляді набору пар шлях-значення.

Декомпозиція двійкових даних, захоплених в мережі, на логічні структури, описані вище або аналогічні, є парсингом. Відповідно, мова йде про вибір парсера з готових або створення свого.

3.3.1. Scapy

Перш за все, було найпопулярніший модуль python для взаємодії з мережевими пакетами, включаючи їх парсинг і створення. Scapy — це програма та бібліотека для маніпулювання пакетами, яка може декодувати велику кількість протоколів, надсилати та перехоплювати пакети, а також контролювати сеанси.

Пакетний клас в scapy має складну структуру з безліччю додаткових полів, включаючи вкладене передбачення протоколу, посилання на вищележачий протокол, поля за замовчуванням, словник з іменами полів і так далі. Весь клас імітує словник, на протоколи якого можна посилатися як за ім'ям протоколу, так і за назвою протоколу. Доступ до деяких полів у вкладених протоколах також можна отримати безпосередньо, якщо поля мають унікальне ім'я.

```
>>> packet.summary()
'RadioTap / Dot11 / Dot11QoS / LLC / SNAP / IP / UDP 0.0.0.0:bootpc > 255.255.255.255:bootps / BOOTP / DHCP'
```

Рис. 3.6. Короткий опис пакета в scapy

3.3.2. DPKT

DPKT - це модуль для python, який позиціонується творцями як швидкий і легкий інструмент для парсингу і створення пакетів, що підтримує базові протоколи стека TCP/IP. Класи DPKT дійсно простіші, ніж у Scapy, і використовують слоти для реєстрації полів, на відміну від словників, як у Scapy. Слоти – механізм python, який замінює динамічну реєстрацію атрибутів класів на основі словника списком попередньо визначених атрибутів. Ця технологія дає різний приріст у часі залежно від версії використовуваного python. Крім того, в класах DPKT майже немає додаткових полів, крім поля даних, в якому зберігаються вкладені дані протоколу або двійкового вкладення. Через цю особливість немає можливості прямого доступу до вкладених протоколів та їх полів при використанні DPKT. Тому для роботи з DPKT подібно до класів модулів, було створено шаблонний клас пакетів, який розкриває всі протоколи, присутні в пакеті, в однорівневу структуру, таким чином надаючи доступ безпосередньо до вкладених протоколів.

```
class IEEE80211(dpkt.Packet):
    __hdr__ = (
        ('framectl', 'H', 0),
        ('duration', 'H', 0)
    )
```

Рис. 3.7. Приклад заголовка 802.11 в dpkt

3.3.3. Власна розробка користувацьких класів

Вивчивши підходи до парсингу пакетів сторонніх модулів, було прийнято рішення написати власний парсер. У першій версії використовувалися прості класи з вкладеними підкласами для складних полів. Після парсингу всі протоколи зберігаються у вигляді атрибутів основного пакетного класу. Доступ до полів здійснюється через атрибути класу. Реалізовано такі протоколи: Radiotap, IEEE802.11, IEEE802.11 Management, LLC, ARP, IPv4, UDP, DHCP, IEEE802.1x, EAP. Цей набір протоколів реалізований в більш пізніх версіях парсера.

```
>>> packet.summary()
'[2020-10-16 15:14:42.937715] 2.4 GHz ch 6 -74 dbm | QoS Data cc:5d:4e:fc:b9:3e -> 88:a4:79:e4:56:12 | EAPOL RSN Key |'
```

Рис. 3.8. Короткий опис пакету

3.3.4. Користувацькі класи з використанням слотів

Згодом створені класи були модернізовані за допомогою слотів для суворого обмеження можливих атрибутів кожного класу. За замовчуванням кожен клас у python використовує прихований словник для зберігання власних атрибутів, який ініціалізується під час створення екземпляра класу. Однак, якщо для класу оголошені слоти, такий словник не буде створено. Натомість, python виділятиме ресурси для фіксованої кількості атрибутів, які перелічені в об'єкті Слоти. Ця реалізація буде називатися «custom_slots».

3.3.5. Безкласові словники

Реалізовані класи виявилися громіздкими і погано масштабованими, тому було прийнято рішення створити уніфіковані протоколи з більш простим присвоєнням

атрибутів. Оскільки розробка ведеться на python, то в якості основного типу даних був обраний словник. Словники на python дуже оптимізовані, пошук елемента за ключем має складність O(1) і не залежить від розміру словника [28]. Тому було прийнято рішення створити функції для кожного окремого протоколу, які б приховували всі поля і їх підполя в однорівневий словник. Те ж саме відбувається і на рівні пакетів – всі поля всіх протоколів об'єднані в один загальний словник, в якому ключем є повний шлях до поля пакета. З точки зору перевірки полів такі підграфіки набагато простіше, ніж класові – немає необхідності перевіряти наявність атрибутів полів для класу перед перевіркою їх значення. У випадку зі словником ми просто перевіряємо наявність поля в об'єкті і можемо відразу отримати значення поля, яке шукаємо.

У цій реалізації в якості загальної точки використовується пакетний клас зі слотами, в межах якого у вигляді окремих атрибутів містяться час пакета, список протоколів, номер протоколу канального рівня та основний словник. Це полегшує обробку хибних атрибутів. Однак всі ці елементи також можуть бути переміщені всередині словника без використання класів.

```
>>> for k, v in packet.fields.items():
...     print(k, v)
...
radiotap.version 0
radiotap.pad 0
radiotap.length 18
radiotap.present 18478
radiotap.flags.short_gi 0
radiotap.flags.bad_fcs 0
radiotap.flags.data_pad 0
radiotap.flags.fcs_at_end 0
radiotap.flags.fragmentation 0
radiotap.flags.wep 0
radiotap.flags.preamble 0
radiotap.flags.cfp 0
radiotap.data_rate 2
radiotap.channel_frequency 2437
```

Рис. 3.8. Приклад пакета, розкладеного в словник

Порівняння різних властивостей досліджуваних реалізацій представлено в таблиці 3.1.

Таблиця 3.1

Порівняння різних реалізацій аналізаторів

Критерій	Scapy	Dpkt	Custom_class	Custom_slots	Custom_dict
Кількість підтримуваних протоколів	916	67	11	11	11
Додавання нових протоколів	Так	Ні	Так	Так	Так
Типи значень	Користувацькі класи залежно від розміру поля	int або bytes	int або bytes	int або bytes	int або bytes
Передбачуваність парсингу	Нові поля залежно від вкладення	Нові поля залежно від вкладення	Вкладення завжди в полі payload	Вкладення завжди в полі payload	Вкладення та протокол в явному вигляді
Доступність протоколу	Необхідна перевірка наявності	Протоколи вкладені один в одного	Протоколи в окремому списку	Протоколи в окремому списку	Протоколи в окремому списку
Доступність полів	Потрібна перевірка наявності	Потрібна перевірка наявності	Порожнє значення при відсутності	Порожнє значення при відсутності	Порожнє значення при відсутності
Обробка пошкоджених пакетів	До пошкодження протоколу	Ні	Ні	До пошкодження протоколу	До пошкодженого протоколу інформація зберігається

З розглянутих реалізацій неможливо однозначно вибрати одну для подальшого розвитку, грунтуючись лише на основних характеристиках. Тому потрібне більш глибоке вивчення та тестування продуктивності представлених реалізацій.

3.3.6. Тестування парсерів

Щоб протестувати швидкість роботи парсерів без впливу сторонніх факторів (швидкість повітряного інтерфейсу, мережева активність і т.д.), тестування буде проводитися на дампах. Для цього у відкритій мережі був зібраний дамп і розділений на окремі файли розміром від 20 до 50 тисяч кадрів. Потім п'ять різних реалізацій зчитували кожен з дампів і аналізували пакети без додаткового аналізу. Вимірювався час кожного запуску, обчислювалися середні значення отриманих результатів, нормувалися показники. Середні значення результатів випробувань представлені в таблиці 3.2.

Таблиця 3.2.

Середні значення результатів тестування

	Середній час обробки дампа	Середні втрати відносно мінімального	Середня кількість пакетів на секунду	Середній виграш відносно мінімального
Scapy	35.05	33.76	1423.76	1.00
Dpkt	15373	12451	20062.91	14.41
Custom_class	12420	47119	36263.61	45133
Custom_slots	44986	1.00	46721.83	33.76
Custom_dict	32509	30317	25507.84	18.37

Згідно з результатами, нативний парсер на класах зі слотами виявився найшвидшим (пікова швидкість обробки парсера на слотах досягає 50 000 пакетів в секунду), а парсер scapy - майже в 34 рази повільніше. Така різниця пояснюється тим, що складні конструкції скапі пропонують широкий спектр застосування, в тому числі і для створення пакети з класу та прості мережеві дії, коли користувацький парсер створюється лише для розкладання пакета на структури класів. Крім того, кількість

підтримуваних протоколів набагато нижча, ніж у обох сторонніх модулів.

Крім тестування швидкості створення класу (або словника) та ініціалізації його атрибутів, необхідно також протестувати швидкість доступу до значень пакета.

3.4. Розробка структури сигнатур

Щоб система сигнатурного аналізу працювала, вона повинна мати базу даних описів атак, на виявлення яких налаштована система. Такі описи називаються підписами. Залежно від атаки вони можуть включати різні дані і відстежувати цілий спектр ознак. Збіг однієї або декількох з цих ознак з списком відомих правил вкаже на атаку.

Кожен об'єкт правил містить ім'я для ідентифікації, список умов, які будуть перевірені в досліджуваному пакеті, і список дій, які будуть виконані, коли пакет відповідатиме всім умовам. Кожна умова містить шлях, оператор і значення. Шлях описує поле в пакеті, значення якого буде порівнюватися з правилом, і складається з протоколу, поля і його вкладених полів за необхідності.

Оператор записує дію яка може бути застосована при порівнянні, і може набувати значень: «==» (строго рівно), «!=» (не рівно), ">" (більше), ">=" (більше або дорівнює), "<" (менше), "<=" (менше або дорівнює), а також "y" (наявність поля або протоколу в пакеті) і "n" (відсутність поля або протоколу в пакеті). При необхідності список операторів може бути розширений. Третє поле умови – значення - записується у вільній, але максимально уніфікованій формі. Завдання інтерпретації цієї величини перед порівнянням покладається на перевіряючого агента.

Для запису була обрана мова розмітки json, так як вона досить уніфікована, щоб сприйматися різними системами. Це накладає обмеження на тип даних, які можуть бути перевірені. Так, наприклад, не можна без перетворення напряму використовувати вбудований тип python byte в якому оброблюються бінарні дані. В json є цілі числа та дроби, рядки, списки, словники, булеві значення та порожній нульовий об'єкт.

Прикладом умов, що описують кадр протоколу IEEE802.11 з типом 0, підтип 12, є кадр деаутентифікації:

Рис. 3.9. Вигляд кадру деаутентифікації

Кожного разу, коли пакет відповідає набору правил, виконуватимуться дії, визначені для цього правила. Список дій в рамках прототипу обмежується підрахунком тригерів і відображенням короткого опису тригерного кадру, але в реальній системі цей список можна легко розширити. Наприклад, пропонується відправляти інформацію на сервер журналу подій, відправляти команди або попередження на контролер бездротової мережі і пристрій безпеки, відправляти команди безпосередньо в точку доступу (наприклад, занести в чорний список певну MAC-адресу), і надсилання фреймів деаутентифікації зловмиснику, коли є вільний бездротовий інтерфейс. Крім того, деякі мережеві пакети можуть бути збережені для подальших досліджень.

Після того, як була розроблена структура правил, система була протестована з різною кількістю активних правил. Для тестування були використані прості правила з єдиною умовою, яка перевіряє єдине поле конкретного протоколу. Агент валідації влаштований таким чином, що при першому збої умови валідація всього правила переривається, так що більш складні правила потягли за собою більш неточні дані. Результати випробувань представлені в таблицях 4 і 5.

Виходячи з отриманих даних, можна зробити висновок, що реалізації з

власними класами мають найбільший виграш у часі при реалізації перевірки пакетів. Це означає, що посилання на атрибути цих класів є неефективним.

Таблиця 3.3

Середній час обробки залежить від кількості правил

	при 1 правилі	при 10 правилах	при 100 правилах	при 1000 правилах
Scapy	35.12	39.80	87.07	546.66
Dpkt	2.54	2.88	6.24	39.10
Custom_class	1.42	1.75	5.18	41.30
Custom_slots	1.12	1.46	5.02	42.17
Custom_dict	1.98	2.18	4.04	22.40

Таблиця 3.4

Середній приріст часу перевірки пакетів

	при 1 правилі	при 10 правилах	при 100 правилах	при 1000 правилах
Scapy	99.80%	112.86%	239.36%	1483.07%
Dpkt	104.89%	119.20%	260.35%	1649.34%
Custom_class	106.18%	131.17%	391.83%	3148.01%
Custom_slots	108.06%	141.56%	490.32%	4145.62%
Custom_dict	104.61%	115.14%	214.63%	1199.03%

Незважаючи на те, що при невеликій кількості правил, реалізація на Scapy показує найнижчий приріст, а при великій кількості правил програє тільки реалізації на словниках, сумарний час обробки цієї реалізації все одно в десятки разів вище, ніж інших, тому дана реалізація не буде брати участь в подальшому тестуванні. Реалізація DPKT також показує відносно невеликий приріст, і якщо немає можливості створити свій модуль, його можна використовувати. Однак складність додавання нових протоколів і досить низька продуктивність роблять його менш застосовним, ніж

нативні реалізації.

З великою кількістю правил стає явно помітною перевага безкласової реалізації на словниках, вона демонструє найнижчий рівень приросту часу. На рис. 3.10 показано динаміку росту часу обробки для різних реалізацій. Видно, що реалізація на словниках стає швидшою, ніж реалізація на класах зі слотами на 50 правил, і швидшою, ніж реалізація на звичайних класах на 36.

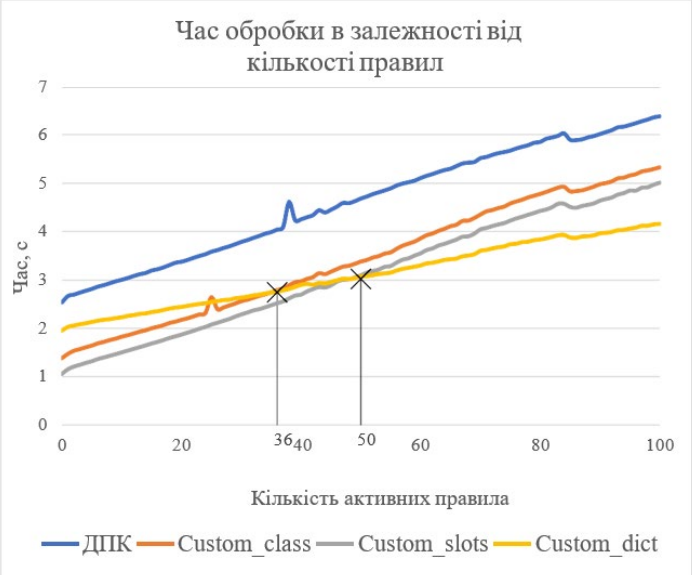


Рис.3.10. Ефективність обробки різних реалізацій

За результатами тестування було прийнято рішення про подальший розвиток системи на основі реалізації парсера зі словниками, так як зростання латентності з ним відбувається повільніше за інших, що в майбутньому сильно вплине на масштабованість і застосовність рішення.

Крім простої перевірки полів пакетів, для деяких атак необхідно також враховувати статистичні параметри пакета. У найпростішій реалізації можна враховувати кількість пакетів за часовий інтервал. При такому підході межі того, скільки пакетів, що відповідають правилу, вважаються нормальними, а які ні, встановлюються вручну на основі вивчених досліджень. та лабораторних досліджень. Наприклад, виявлення 100 кадрів дисоціації за хвилину вкаже на можливу DoS-атаку.

Крім того, в деяких ситуаціях правило може знадобитися відключити на деякий час після його спрацьовування. Для цього введено параметр timeout. Коли правило

спрацьовує, воно стане неактивним протягом кількості секунд, заданих цим параметром.

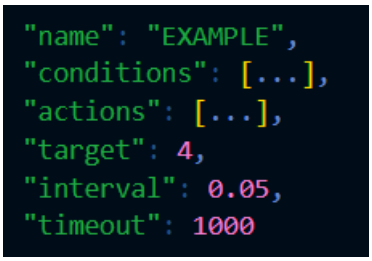


Рис.3.11. Приклад правила з додатковими параметрами

Це правило спрацьовує, коли за 0,05 секунди приймаються 4 пакети, що відповідають правилам, після чого відключається на 1000 секунд.

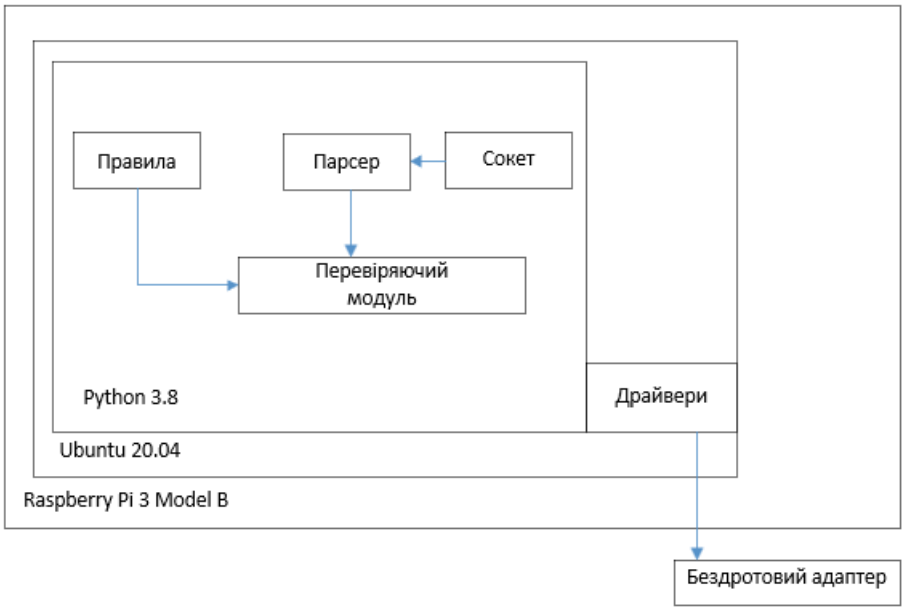
Нижче наведено приклад повного правила для DoS-атаки з дисоціаційними кадрами. Бажані кадри протоколу 802.11: тип 0 (контроль), підтип 10 (дисоціація). Якщо протягом хвилини буде виявлено 100 таких кадрів, правило відобразить інформацію про тригер в консолі і відключиться на 5 хвилин:

Рис3.12. Приклад повного правила для DoS-атаки з дисоціаційними кадрами

3.5. Робоче середовище системи

Для захоплення низькорівневого мережевого трафіку потрібні спеціальні драйвери. В рамках випробувального стенду використовується бездротовий адаптер TP Link Archer T4U. Останні кілька версій драйверів для цього чіпсета підтримуються спільнотою [25].

В якості операційної системи для тестового стенду буде використовуватися Ubuntu. З додаткового програмного забезпечення, крім драйверів бездротового адаптера, встановлюється версія Python версії 3.9. Надалі планується реалізація програмного ядра системи з використанням технологій контейнеризації з використанням Docker.



Малюнок 3.13. Схема організованої системи

3.6. Функціональне тестування системи аналізу

Для тестування використовуються правила, які виявляють:

- DoS-атаки з фреймами деаутентифікації;
- DoS-атаки з PS-Poll-кадрами;
- маяки для точок доступу, які використовують WEP.

Формалізований опис цих правил представлено на рис. 3.16.

Для тестування був організований стенд з наступною архітектурою:

- Вразливою точкою доступу стала точка Tenda AC6. Для перших двох атак вона працювала в режимі WPA2-PSK без додаткових механізмів захисту, потім була переведений в режим WEP для тестування третього правила.
- Клієнтом був телефон з операційною системою Android 12.
- Зловмисником виявився ноутбук на базі Kali Linux з бездротовим адаптером. Для проведення DoS-атаки з кадрами деаутентифікації використовувалася утиліта aireplay-ng, вбудована в дистрибутив Kali Linux . Для DoS-атаки PS Poll був написаний скрипт на python за допомогою модуля scapy для ін'єкційних пакетів.
- Датчиком послужив Raspberry Pi з бездротовим адаптером TP Link Archer T4U.

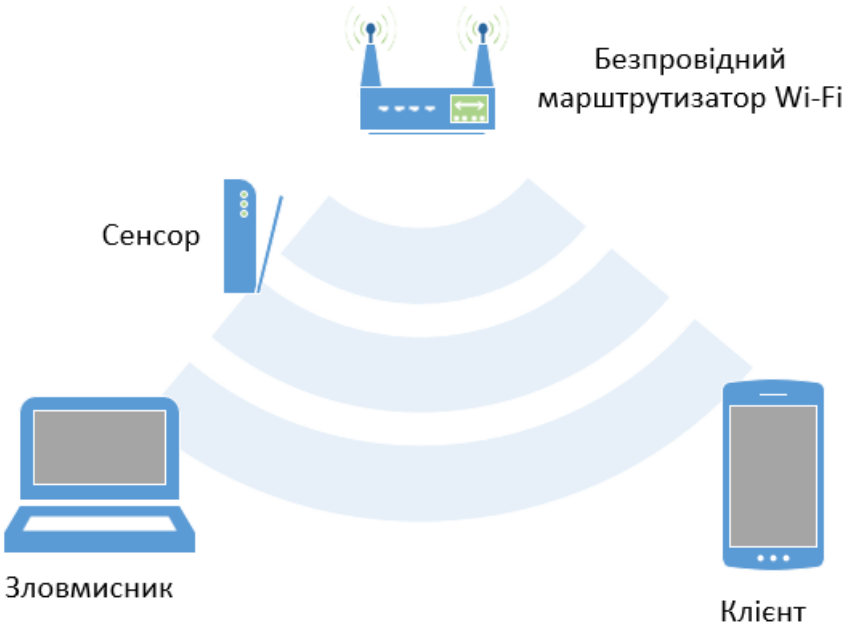


Рис.3.14. Структура випробувального стенду

Фотографія датчика випробувального стенду показана на рис. 3.15. На цій платі була встановлена ОС Ubuntu 20.04, додаткові драйвери мережевого адаптера, дистрибутив програми. Управління датчиком здійснюється через SSH.

Рис.3.15. Фото датчика, який використовується в складі випробувального стенду Sensor Launch:

Запуск сенсора:

```
>start
Starting system...
Rules active:
DEAUTH_FLOOD: dot11.type==0 dot11.subtype==12; 100 in 60s; timeout 300s;
PSPOLL_FLOOD: dot11.type==1 dot11.subtype==10; 100 in 5s; timeout 300s;
WEP_AP: dot11.type==0 dot11.subtype==8 dot11mgmt.fixed.capabilities.privacy==1
 !dot11mgmt.tagged.rsn_information; 5 in 1s; timeout 3600s;
Capturing on wlan0...
```

Рис.3.16. Скріншот запуску датчика

Aireplay-ng під час DoS-атаки з фреймами деаутентифікації надсилає ці кадри клієнту від імені точки доступу та точки доступу від імені

Клієнт. Таким чином, обидва пристрої вважають, що з'єднання було перервано з іншого боку. Для запуску атаки використовується наступна команда:

aireplay-ng -0 0 -a 04:95:e 6:97:9a:a5 -c 88:46:04:f5:55:98 wlan0

Тут:

-0 – атака з фреймами деаутентифікації;

0 — кількість надісланих кадрів.

0 – надсилати безстроково;

-a <MAC> - адреса точки доступу в мережі;

-with <MAC> – адреса атакованого пристрою;

wlan0 — інтерфейс , який використовується для надсилання кадрів.

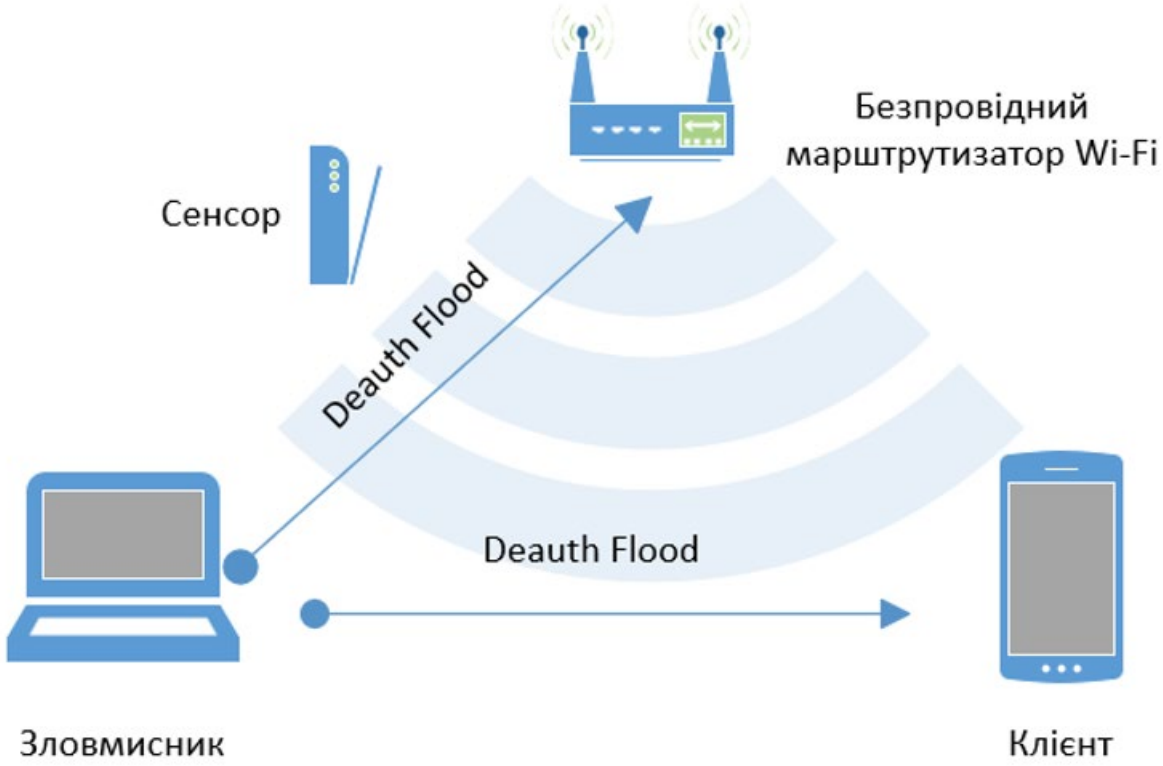


Рис.3.17. Схема DoS-атаки з фреймами деаутентифікації

Виявлення сенсорної атаки:

```
DEAUTH_FLOOD ringed at 2021-06-13 16:30:13.775462: 100 pkts at -78 dBm
DEAUTH_FLOOD ringed at 2021-06-13 16:35:14.459382: 38628 pkts at -82 dBm
```

Рис.3.18. Спрацьовування правила DEAUTH_FLOOD

На рис. 3.18 ми бачимо, що правило спрацьовує знову через 5 хвилин (параметр тайм-ауту) після першого. В якості додаткової інформації, він також відображає загальну кількість пакетів, які були спрацьовані, а також останнє значення потужності

сигналу з заголовка Radiotap.

Суть DoS-атаки з кадрами PS-Poll полягає у використанні енергозберігаючого механізму клієнта. Зловмисник може змусити точку доступу передати незавершені кадри пробудження клієнта до того, як клієнт буде готовий їх прийняти. Для здійснення кадрової атаки PS-Poll використовується програма на python. Для ін'єкції використовується модуль scapy [12]. Вихідний код програми зображено на рис.3.19 .

```
from scapy.all import *
frame = RadioTap()/Dot11FCS(type=1,
subtype=10,
addr1='04:95:e6:97:9a:a5',
addr2='88:46:04:f5:55:98')
sendp(frame, iface='wlan0', inter=0.050, loop=1, monitor=True)
```

Рис. 3.19.Вихідний код програми

Тут addr1 – це MAC-адреса точки доступу, addr2 – MAC-адреса клієнта.

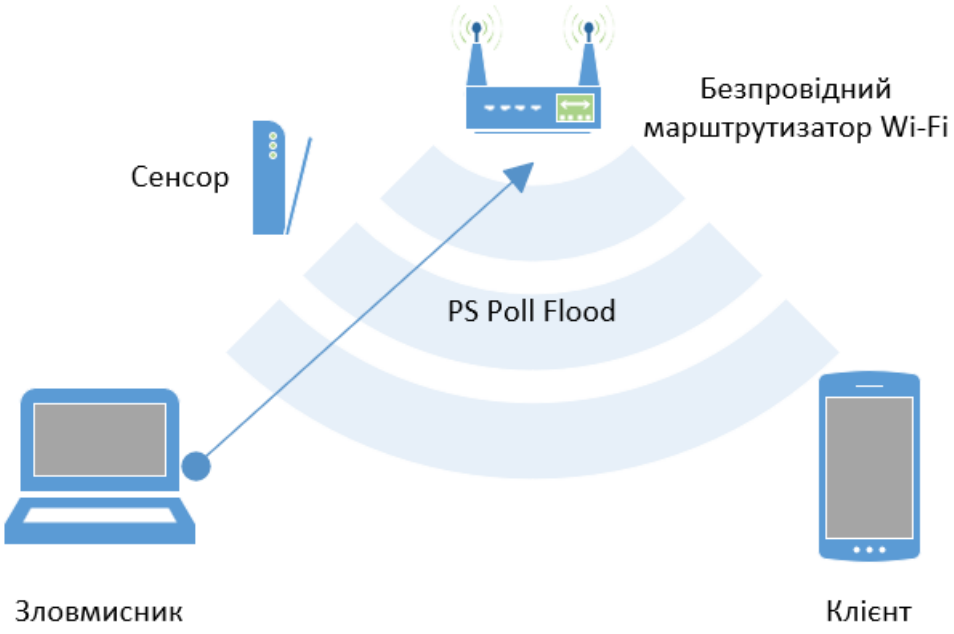


Рис. 3.20. Схема здійснення атаки кадрами PS-Poll

Виявлення атаки датчика:

```
PSPOLL_FLOOD ringed at 2021-06-13 16:36:48.129443: 100 pkts at -72 dBm
PSPOLL_FLOOD ringed at 2021-06-13 16:41:53.965996: 6200 pkts at -72 dBm
```

Рис. 3.21. Активація правила PSPOLL_FLOOD

Додаткові відомості відображаються так само, як і правило DEAUTH_FLOOD.

Потім було протестовано правило WEP_AP, яке відстежує кадри-маяки від точки доступу. Для цього точку, що охороняється, перевели в режим WEP.

Рис. 3.22. Схема вразливої мережі

Виявлення датчиком слабозахищеної точки:

```
WEP_AP ringed at 2021-06-13 16:45:02.068328: AP 04:95:e6:97:9a:a5 in net TestWEPNet
```

Рис. 3.23. Спрацьовування правила WEP_AP

В результаті експерименту датчик виявив всі атаки і уразливості, що вивчаються. Функціональне тестування системи можна вважати успішним.

3.7. Навантажувальне тестування розробленої системи

Далі було проведено навантажувальні випробування системи. Воно проходило у 2 етапи. Перший етап здійснювався шляхом захоплення трафіку в реальній мережі з декількома пристроями.

Правила цих тестів є структурами, близькими до реальних правил, але не виявляють жодних конкретних атак. Вони генерувалися автоматично для коригування навантаження на систему.

Рис. 3.24. Схема мережі, що використовується для навантажувального тестування

Було порівняно навантаження на центральний процесор при різній кількості активних правил пошуку (рис. 3.25). Так як реалізоване рішення працює в єдиному процесі, то все навантаження припало на одне з чотирьох ядер станції. Максимальне навантаження (25%) було досягнуто за 1330 активних правил.

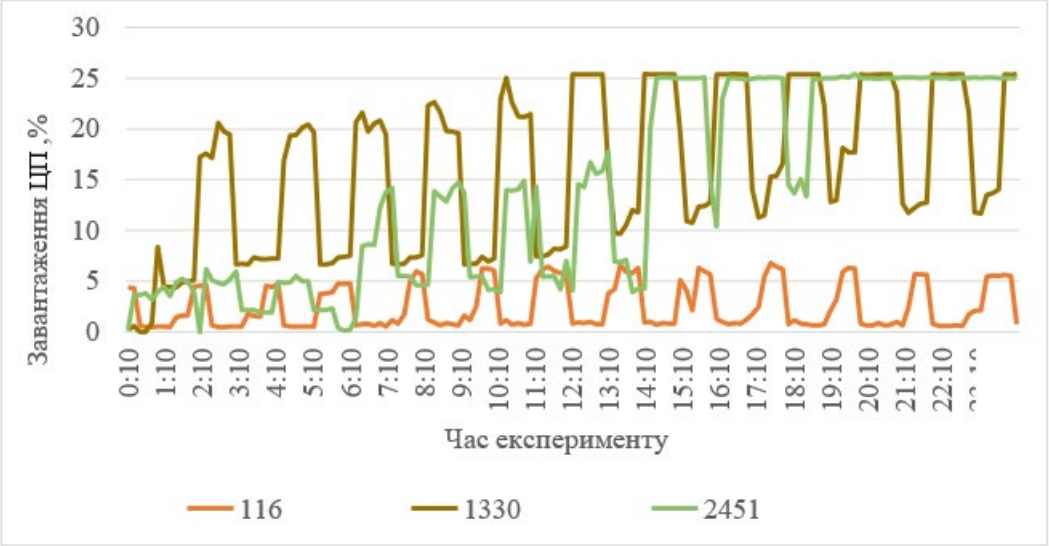


Рис. 3.25. Навантаження на центральний Процесор в залежності від кількості активних правил

На другому етапі тестування вивчалася пропускна здатність системи. Для цього з реальних мереж було зібрано 19 дампів різного розміру. Потім для різної кількості правил визначали середнє число пакетів в секунду і відношення реального часу до часу обробки (табл. 3.5).

Таблиця 3.5

Тестування пропускної здатності системи

	1 правило	10 правил	100 правил	1000 правил
Середня кількість пакетів на секунду	25313	10498	1344	136
Середнє співвідношення реального часу до часу обробки	5198.73	1883.67	228.23	22.30
Мінімальне співвідношення реального часу до часу обробки	23.94417	9.286031	1.27535	0.117607

Система також досягає межі навантаження з великою кількістю правил, але успішно справляється з кількома десятками правил, що робить її застосовною на практиці.

РОЗДІЛ 4
ОХОРОНА ПРАЦІ

4.1. Аналіз умов праці на робочому місці

Організація робочого місця. Системний адміністратор як правило, проводить виробничу діяльність в спеціально обладнаних для цього приміщеннях. Однак час від часу може виникати необхідність проводити час в інших приміщеннях, наприклад в приміщеннях де встановлено серверне або інше мережеве обладнання. Розташування та дизайн робочого місця повинні відповідати психологічним, фізіологічним і антропометричним вимогам від-повідно до ДСТУ 12.2.032-78. Налаштування робочого місця повинно відповідати стандартам, технічним умовам і методичним вказівкам з безпеки праці [21].

Основними елементами робочого місця є персональний комп'ютер, що включає в себе системний блок, декілька моніторів, клавіатуру та маніпулятор типу «миша»; робочий телефон; стіл для телефону та комп'ютера; крісло (стілець) для сидіння; диван для відпочинку, який використовується протягом усього робочого дня.

Відповідно до вимог ДСТУ 12.2.032-78 приміщення має відповідати певним нормам, зокрема має бути проведено теплоізоляцію стелі та стін, також стелі та стіни не повинні затримувати пил. Підлога має бути безпечною, не слизькою, рівною. Організація джерел штучного освітлення компенсує брак природнього. Для працівників передбачено наявність санітарно-побутових приміщень.

Розміри робочої кімнати, яка використовується для організації робочого місця системного адміністратора натупні: ширина – 2.7 метрів, довжина – 3.5 метрів, висота - 3,4 метрів, площа – 9.45 квадратних метрів і загальний об'єм – 32.13 кубічних метрів. Згідно вимог площа та об'єм приміщення на одного співробітника становлять відповідно 9.45 кв. м і 32.13 куб. м. За результатами аналізу можна зробити висновок, що робоче місце відповідає стандартам.

Мікроклімат виробничих приміщень. Робоче місце системного адміністратора згідно ГОСТ 12.1.005-95 вважається комфортним за умови

дотримання таких показників метеорологічних умов: температури повітря 18–23 °С, відносної вологісті повітря 40–60% і швидкісті руху повітря 0,2– 0,7 м/с. У зимовий період було зафіксовано такі метрологічні пара-метри: температура 22 градуси Цельсія, відносна вологість 47% і швидкість повітря 0,2 м/с. Всі параметри відповідають вимогам нормативних документів і в приміщенні дозволено працювати.

4.2. Перелік шкідливих та небезпечних виробничих факторів у робочій зоні

Виробничі чинники, які представляють небезпеку та можуть шкодити здоров'ю працівників, мають вплив на робочий процес. Оцінка ризику та кількість таких технологічних процесів можуть служити критерієм безпеки праці на виробництві. Державний стандарт ДСТУ 12.0.003-74, "Небезпечні та шкідливі виробничі фактори", визначає класифікацію цих факторів, оскільки деякі з них можуть впливати на працівників під час експлуатації та обслуговування обладнання.

Фізичні, хімічні, біологічні та психофізичні виробничі фактори вважаються небезпечними та шкідливими. ДСТУ 12.0.003-74 вказує, що при роботі з радіомаяками можуть виникнути різні небезпечні та шкідливі фактори, такі як електричний струм, електромагнітне випромінювання, недостатнє освітлення робочого місця, неадекватні мікрокліматичні умови та монотонність роботи [22].

Електробезпека. З метою запобігання випадкового дотику зі струмоведучими частинами використовуються різні заходи, які визначені в стандарті [24]. Серед них – використання запобіжників у ланцюзі живлення, застосування низьких напруг, електричне розділення мережі, попереджувальна сигналізація, блокування, застосування знаків безпеки, ізоляція струмоведучих частин, правильне розташування, використання захисних огороджень та інші.

Державний стандарт ДСТУ 12.1.030-81 визначає методи для уникнення поразки електричним струмом при дотику до металевих струмоведучих частин через ушкоджену ізоляцію, такі як контроль ізоляції, електричний поділ мережі, ізоляція неструмоведучих частин та захисна металізація.

Стандарт ДСТУ 12.1.019-79 "Електробезпека" регулює питання безпеки в електроустановках. Він визначає заходи для заземлення електрообладнання та забезпечення електробезпеки на робочому місці шляхом застосування безпечних видів праці та заземлення.

Стандарт ДСТУ 54-71004-85 регулює безпечні види праці, забезпечуючи комфорт та безпеку під час роботи. Електробезпека досягається правильним розташуванням обладнання та енергетичних комунікацій, а також надійним контактним з'єднанням.

Зазначений стандарт також вказує на важливість використання провідних матеріалів для устаткування та одягу працівників для уникнення електростатичної небезпеки, а відносна вологість повітря повинна відповідати нормативам для зменшення електризації.

Раціональне виробниче освітлення на робочому місці вважається одним з ключових аспектів створення сприятливих умов праці. Добре спроектоване та адекватно вибране освітлення виробничих приміщень забезпечує можливість працівникам чітко розрізняти предмети та інструменти протягом тривалого часу. Недостатнє освітлення на заводі може негативно вплинути на якість виробленої продукції. Психоемоційний стан працівника, його працездатність, мотивація, продуктивність та безпека праці – всі ці аспекти залежать від якості освітлення.

Електромагнітні хвилі світла створюють відчуття зору. "Поле зору" – це те місце, на яке спрямовані очі та голова працівника, коли вони не рухаються. Рівень освітлення на робочому місці впливає на гостроту зору, контрастну чутливість, тривалість ясного бачення та здатність бачити на різних відстанях. Для працівників з нормальним зором, освітлення на рівні 50–70 лк забезпечує нормальну гостроту зору та можливість розрізняти дрібні предмети. Освітленість на рівні 600–1000 лк важлива для найкращого розрізнення деталей.

Дослідження в області фізіології показали, що час ясного бачення працівників зменшується при зниженні освітленості. Наприклад, при освітленості 50 лк час ясного бачення зменшується на 72%, при 75 лк – на 55%, при 100 лк – на 26%, а при 200 лк – на 15%. У розглянутому приміщенні використовується комбінований підхід – бічне

природне та загальне штучне освітлення що включає в себе вікно розмірами 2 м шириною та 2.1 м висотою та 3 світильники на стінах відповідно. Ці параметри відповідають вимогам цього приміщення для холодного періоду року.

4.3. Розробка заходів з охорони праці. Електробезпека

Відповідно до вимог ДСТУ 12.1.030-81 "Безпека електроенергетики", для пристроїв із напругою до 1000 В опір заземлення не повинен перевищувати 4 Ом. У випадку трифазної електричної мережі з глухозаземленою нейтраллю, напругою 220 В і частотою 50 Гц, необхідно провести розрахунок повторного заземлення нульового провода [20].

Поновлення заземлення нульового проводу на певній відстані від джерела живлення визначається як повторне заземлення нульового проводу. Це дозволяє знизити напругу нульового проводу та корпусів заземленого обладнання в порівнянні зі землею як у нормальному режимі, так і при обриві нульового проводу між приймачем та джерелом живлення. Для проведення розрахунків було використано програмне середовище Mathcad 15. На рис 4.1 можемо побачити вікно програми з вхідними даними та проведеними розрахунками.

Для розрахунку заземлення використаємо такі дані:
Питомий опір грунту $\rho = 20$ Ом*м
Коефіцієнти кліматичної зони для розрахунку заземлення:
Вертикальний провідник - $\psi_{верт} = 1.4$
Горизонтальний провідник - $\psi_{гор} = 2$
Норма опору - $R_H = 4$
Тип заземлення: вертикальні електроди (сталева труба, діаметр d = 7 мм, товщина стінки h = 4 мм, довжина електрода L = 2,5 м) та горизонтальна смуга (ширина b = 60 мм, товщина стінки h = 4 мм). Глибина траншеї t = 0,7 м, співвідношення відстані між заземлюючими елементами прийнято як α = 1xL.

1. Величина питомого опору грунту з урахуванням кліматичної зони розраховується наступним чином:

$$\rho_{екв} := \psi_{верт} \cdot \rho = 28 \quad \text{Ом·м}$$

2.Опір розтікання струму одиночного вертикального заземлювача:

$$R_0 := \frac{\rho_{екв}}{2\pi \cdot L}\left(\ln\left(\frac{2 \cdot L}{d}\right) + 0.5 \cdot \ln\left(\frac{4T + L}{4T - L}\right)\right) = 8 \text{ Ом}$$

3. Умовна кількість вертикальних заземлюваів:

$$n_0 := \frac{R_0}{R_H} = 2.05$$

4. Дійсна кількість вертикальних заземлювачів:

$$n := \text{floor}\left(\frac{R_0}{R_H \eta_{0в}}\right) = 3 \quad \text{шт}$$

5. Довжина горизонтального

$$L_Г := \alpha \cdot (n - 1) = 5 \quad \text{м}$$

6. Опір розтікання струму горизонтального заземлювача:

$$R_Г := 0.366\left(\frac{\rho \cdot \psi_{гор}}{L_Г \cdot 0.62}\right) \cdot \log\left(\frac{2 \cdot L_Г^{\,2}}{b \cdot t}\right) = 14.525 \text{ м}$$

7. Загальний опір заземлюючого пристрою

$$R_{об} := \frac{R_Г \cdot R_0}{R_0 \cdot 0.62 + R_Г \cdot \eta_в \cdot n} = 3.86 \quad \text{Ом·м}$$

Рис. 4.1. Розрахунок заземлюючого пристрою в програмному середовищі Mathcad

Як видно отримане значення 3,86 Ом*м не перевищує гранично допустимого значення в 4 Ом на м.

4.4. Пожежна безпека

Відповідно до НАПБ А.01.001-2004 "Правила пожежної безпеки в Україні" та ОНТП 24-86 "Визначення категорії приміщень і будівель за вибухопожежною та пожежною небезпекою", робоче місце системного адміністратора віднесено до категорії "Д". Вибір цієї категорії передбачає використання негорючих матеріалів у холодному стані відповідно до характеристик речовин і матеріалів, що перебувають в приміщенні. Крім того, до цієї категорії не включаються приміщення, де горючі рідини знаходяться в системах змащування, охолодження чи гідроприводу обладнання, а також кабельні електропроводки до обладнання та окремі меблі на робочих місцях.

Під час використання персонального комп'ютера чи ноутбука, як правило, відсутні вибухонебезпечні речовини. Проте, існують пристрої та зони, які можуть становити пожежну небезпеку. Серед таких приладів можна виділити персональні робочі пристрої працівника, розетки, що розташовані безпосередньо на робочому місці, а також області чи пристрої, які можуть бути пожежонебезпечними в приміщенні, такі як електрощитові, зони проведення газових чи електрокомунікацій.

Головними причинами виникнення пожеж є порушення технологічних регламентів, несправність використовуваного обладнання або неправильна його експлуатація. Важливо уникати небезпечного поводження з відкритим вогнем та забезпечити безпечні умови роботи з електротехнікою та електронікою в робочих приміщеннях.

Для запобігання та протидії пожежній небезпеці в приміщенні встановлено адресний оптичний димовий сповіщувач, а в беспосередній близькості - порошковий вогнегасники, який можна використовувати для гасіння електроустановок до 1 кВт.

На території в доступних зонах розміщені таблички із зображенням плану приміщення, екстреними виходами, шляхами евакуації та місцями розміщень пожежних кранів. На рис. 4.2 показана дана схема приміщення.

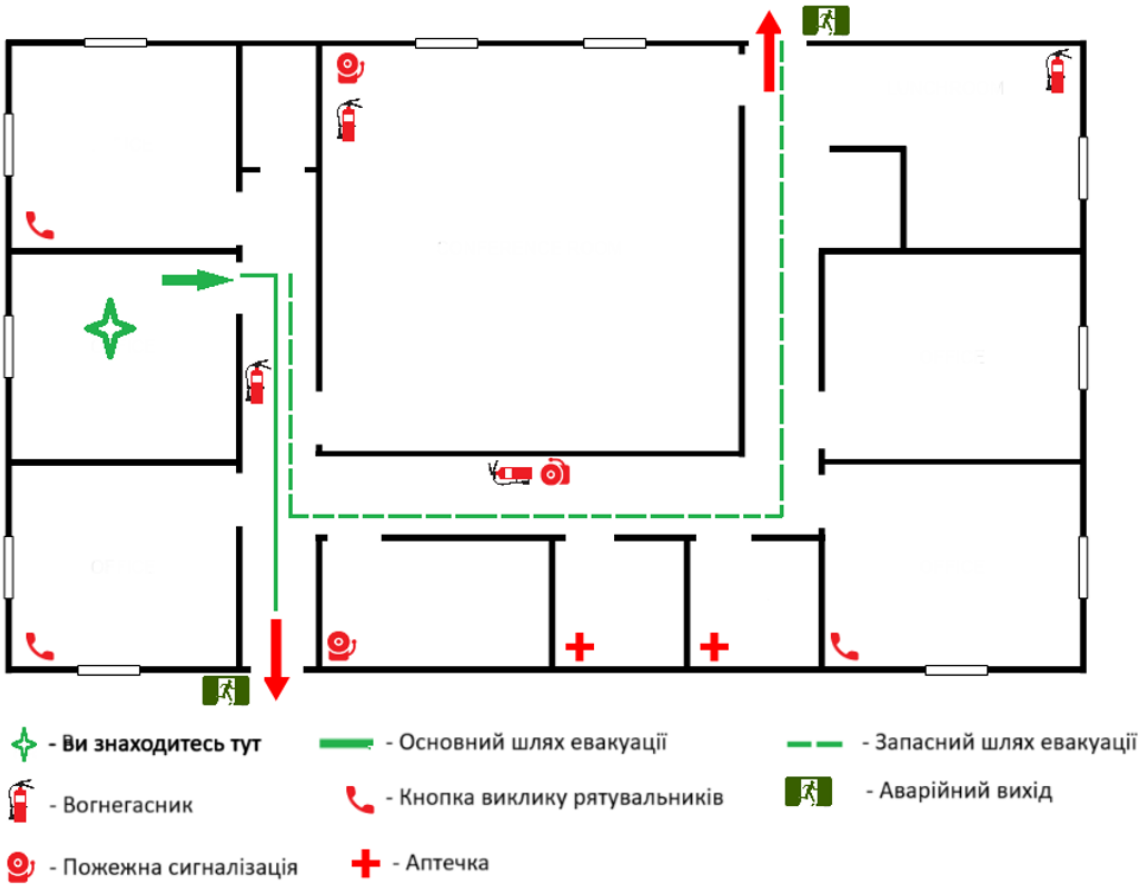


Рис. 4.2. План евакуації з робочого приміщення

Основним шляхом евакуації можна дістатися запасного виходу подолавши 7 метрів шляху прямим коридором. Виходячи з робочого кабінету треба повернути праворуч та пройти до кінця коридору до дверей з табличкою «Аварійни вихід». За умов необхідності використання запасного шляху евакуації який становить 18 метрів необхідно вийти з робочого кабінету, повернути праворуч, в кінці коридору повернути ліворуч та рухатись прямо до наступного повороту, там повернути ще раз ліворуч та рухатись прямо до дверей з табличкою «Аварійний вихід». Додатковим шляхом евакуації може стати вікно кабінету, адже приміщення знаходиться на 1 поверсі.

Висновки. В ході роботи над розділом було проведено аналіз дій щодо забезпечення необхідного рівня безпеки на робочому місці системного адміністратора. Розглянуто та розраховано систему забезпечення електробезпеки. Проаналізовано наявні на підприємстві варіанти забезпечення пожежної безпеки. Забезпечення високого рівня безпеки на підприємстві є важливою умовою для

ефективного та безперебійного функціонування. Систематичні навчання та інструктажі з безпеки, аналіз ризиків та вдосконалення робочого середовища сприяють зниженню можливості нещасних випадків та пожеж. Організація робочих процесів, ефективні процедури та використання засобів індивідуального захисту є ключовими аспектами у забезпеченні безпеки працівників. Крім того, важливо підтримувати психосоціальне благополуччя працівників та встановлювати ефективну співпрацю з відповідними органами та експертами з безпеки. Всі ці заходи сприяють створенню безпечного та здорового робочого середовища.

РОЗДІЛ 5
ОХОРОНА НАВКОЛИШНЬОГО СЕРЕДОВИЩА

Охорона навколишнього середовища включає в себе заходи з використання, відтворення та раціонального використання природних ресурсів, а також попередження та ліквідацію негативного впливу господарської та іншої діяльності на природне середовище. Це включає охорону природних ресурсів, забезпечення безпеки, та взаємодію в галузі генетичних фондів. Природні об'єкти, як-от ландшафти та історико-культурна спадщина, також враховуються в цьому контексті.

Зараз сучасний фахівець важко уявляє свою роботу без використання комп'ютерних технологій, які, разом з тим, стали новим стандартом життя для людей. Враховуючи, що моя дипломна робота присвячена інформаційним технологіям, розділ, в якому обговорюються вплив персональних комп'ютерів, мобільних пристроїв та технологій WiFi на навколишнє середовище, є актуальним та важливим.

Наявні різні види відходів, такі як гази, рідини та тверді залишки, які викидаються в атмосферу внаслідок людської діяльності. Ці відходи можуть бути шкідливими для всіх живих істот, включаючи людей, оскільки природа не завжди може ефективно їх нейтралізувати. Наприклад, хімічне забруднення біосфери є серйозною проблемою. До того ж, фізичні фактори, такі як електромагнітне, теплове, шумове та радіоактивне забруднення, можуть також впливати на навколишнє середовище внаслідок техногенної діяльності.

Зрозуміло, що люди усвідомлюють загрози для навколишнього середовища, проте часто розглядають їх як неприємний, але необхідний наслідок розвитку цивілізації. Нещодавні події свідчать про те, що необхідно негайно діяти та використовувати економічно ефективні технології та методи для захисту та відновлення навколишнього середовища.

Законодавство України визначає основні принципи охорони навколишнього середовища та встановлює відповідальність підприємств за раціональне використання та відновлення природних ресурсів. Урахування екологічних стандартів та практик є обов'язковим. Також визначено пріоритетність екологічної

безпеки та обов'язкове дотримання стандартів для забезпечення екологічно безпечного середовища для життя та здоров'я людей.

Людський вплив на природу може мати довгострокові наслідки, такі як зміна клімату, зниження продуктивності та негативний вплив на фотосинтез. Цивільна авіація, крім того, призводить до забруднення навколишнього середовища, включаючи атмосферне забруднення та шум. Такі діяльності можуть викликати загрозу повітрю, воді та грунту.

Законодавчі акти та стандарти, такі як ДСТУ 17.00.01 та Закони про охорону навколишнього середовища, визначають основні принципи та завдання для забезпечення екологічної безпеки та охорони природи. Україна також визнає необхідність екологічної безпеки для збереження генофонду та гарантування здоров'я та безпеки своїх громадян [23].

5.1. Забруднення навколишнього середовища

Забруднення навколишнього середовища означає вплив на властивості середовища (хімічні, фізичні, біологічні та інші), який призводить до погіршення його функцій відносно будь-якого об'єкта, що перебуває в цьому середовищі.

Для виготовлення персонального комп'ютера, який використовується в сучасній роботі, витрачається приблизно п'ятнадцять тонн різних матеріалів. Це значення менше, ніж кількість матеріалів, яка використовується для виготовлення звичайного автомобіля, але слід зазначити, що частина цих матеріалів може залишитися невикористаною через швидкість технологічних змін. Зважаючи на те, що електронні пристрої, зокрема ПК, містять токсичні речовини, такі як ртуть, кадмій та свинець, їх вплив на навколишнє середовище та здоров'я людей є важливим питанням.

Спричинені суспільними турботами та владою, виробники активно працюють над створенням систем для збору та утилізації використаних електронічних пристроїв, які вийшли з обігу. Крім того, вони розвивають конструкції пристроїв, спрямовані на максимальне використання матеріалів, які можуть бути перероблені.

Оргтехніка включає в себе як органічні складові (пластик, полівінілхлорид, фенолформальдегід), так і різноманітні метали. У таблиці 6.1 представлені усереднені дані про вміст різних металів і матеріалів у персональному комп'ютері, включаючи пластик, алюміній, сталь, мідь, свинець тощо.

Такі дані вказують на важливість розробки екологічно штучних технологій та впровадження засобів вторинної переробки для зменшення впливу електронної техніки на довкілля [30].

На рис. 5.1 показано таблицю шкідливих речовин які можуть міститися в персональному комп’ютері. Дані про ці речовини зібрані на основі лабораторних та хімічних аналізів були усереднені.

Найменування	Дорогоцінні метали		Кольорові і чорні метали			Полімери і скло	
	Au, г	Ag, г	Al, кг	Cu, кг	Fe, кг	Пластик, кг	Скло, кг
Персональний комп'ютер (монітор, системний блок, клавіатура, маніпулятор)	0,053-0,072	0,8-1,1	0,1-0,4	0,1-0,2	3-4	3-3,5	10-20

Рис. 5.1. Шкідливі речовини які містяться в ПК

На підприємстві весь процес утилізації або переробки техніки починається з виключення її з балансу. Після цього відбувається централізоване збирання техніки, яка потім передається до центрів переробки. Там проводиться розбір техніки, і матеріали, які можна переробити, відокремлюються від тих частин, які можна лише утилізувати.

Однією з нововведень у сфері утилізації друкованих плат є розробка спеціального розчину вченими з Національної фізичної лабораторії Великобританії. Цей розчин, який розчиняється у гарячій воді, сприяє відшаруванню електронних

компонентів. Це дозволяє повторно використовувати до 90% компонентів нових друкованих плат, порівняно зі звичайними методами, де цей показник становить лише 2%.

Більшість підприємств не здатні самостійно утилізувати свою техніку, тому цей процес зазвичай віддається на обробку фахівцям, які спеціалізуються на утилізації технічного обладнання.

ВИСНОВКИ

Розробка методики автоматизованого аналізу ризиків інформаційної безпеки за допомогою алгоритмів машинного навчання дозволила окреслити перспективний напрямок у розробці нових систем безпеки трафіку в корпоративних мережах. Тренд на використання штучного інтелекту в найрізноманітніших галузях все більше набирає обертів, тому безсумнівно така методика буде викликати інтерес з боку телекомунікаційних компаній та підприємств. Зібрані в ході дослідження дані показали, що система з використанням штучного інтелекту може швидко та ефективно виявляти спроби різноманітних зловмисницьких атак на інформаційні мережі. Розглянута в даній кваліфікаційній роботі система направлена на забезпечення безпеки в сегменті бездротових мереж Wi-Fi. Дуже часто в зоні ризику перебувають клієнти, які підключаються до таких мереж в публічних місцях, і саме за таких умов зловмисникам найлегше заволодіти конфіденційними даними.

Незважаючи на досягнуті успіхи на поточному етапі, система має значний потенціал для доопрацювання та інтеграції її в значно більші системи та використання її не тільки у бездротових мережах. Вибір платформи на мові програмування Python дозволить швидко масштабувати систему та інтегрувати її у всі популярні платформи завдяки безмежним можливостям мови програмування.

Під час виконання кваліфікаційної роботи було досягнуто наступні цілі:

- проаналізовано існуючі підходи до аналізу трафіку та їх реалізації;
- розроблено систему перехоплення мережевого трафіку;
- розробити структуру аналізатора та варіанти його реалізації;
- розроблено нейронну мережу для аналізу мережевої активності та виявлення аномалій трафіку
- проведено експериментальне дослідження ефективності розробленої системи
- доведено ефективність розробленої системи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. A dataset for evaluating intrusion detection systems in IEEE 802.11 wireless networks / D. W. F. L. Vilela et al. 2014 IEEE colombian conference on communications and computing (COLCOM), Bogota, Colombia, 4–6 June 2014. 2014.
2. Autom atic profiling and behavior prediction of computer system users / J. Monroy et al. 2006 IEEE international workshop on measurement systems for homeland security, contraband detection and personal safety, Radisson Hotel Old Town, Alexandria, VA, USA, 18–19 October 2006. 2006.
3. Cai M., Wu Z., Zhang J. Research and prevention of rogue AP based mitm in wireless network. 2014 ninth international conference on P2P, parallel, grid, cloud and internet computing (3PGCIC), Guangdong, China, 8–10 November 2014. 2014.
4. Intrusion detection in 802.11 networks: empirical evaluation of threats and a public dataset / C. Kolias et al. IEEE communications surveys & tutorials. 2016. Vol. 18, no. 1. P. 184–208.
5. Kohlios C., Hayajneh T. A comprehensive attack flow model and security analysis for wi-fi and WPA3. Electronics. 2018. Vol. 7, no. 11. P. 284.
6. Kolias C., Kambourakis G., Maragoudakis M. Swarm intelligence in intrusion detection: a survey. Computers & security. 2011. Vol. 30, no. 8. P. 625–642.
7. Tensor based framework for Distributed Denial of Service attack detection / J. P. A. Maranhão et al. Journal of network and computer applications. 2021. Vol. 174. P. 102894.
8. Абдулхаков А.Р., Катасёв А.С., Кирпичников А.П. Методы редукции нечетких правил в базах знаний интеллектуальных систем // Вестник Казан. технол. ун-та. -2014. – Т. 17. – № 23. – С. 389-392.
9. Глова В.И., Аникин И.В., Катасёв А.С., Кривилёв М.А., Насыров Р.И. Мягкие вычисления: учебное пособие. Казань: Изд-во Каз. гос. технич. университета им. А.Н. Туполева, 2010. – 206 с.

10. Джеймс Кеннеди. Нейросетевые технологии в диагностике аномальной сетевой активности // Fort Lauderdale, FL 33314.
11. Емалетдинова Л.Ю., Катасёв А.С., Кирпичников А.П. Нейронечеткая модель аппроксимации сложных объектов с дискретным выходом // Вестник Казан. технол. ун-та. – 2014. – Т. 17, № 1. – С. 295-299.
12. Исследование подходов интеграции мессенджеров с корпоративными информационными системами. М.М., Ковцур, Н.И., Казаков и В.В., Коновалова. Санкт-Петербург : б.н., 2020. МЕТОДЫ И ТЕХНИЧЕСКИЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ.
13. Катасёв А.С., Катасёва Д.В., Кирпичников А.П. Нейросетевая технология классификации электронных почтовых сообщений // Вестник технол. ун-та. – 2015. – Т. 18, № 5. – С. 180-183.
14. Кирпичников А.П., Осипова А.Л., Ризаев И.С. Повышение аналитических возможностей баз данных // Вестник Казан. технол. ун-та. – 2012. – № 3. – С. 157-160.
15. Красов А. В., Косов Н. А., Холоденко В. Ю. Исследование методов провижининга безопасной сети на мультивендорном оборудовании с использованием средств автоматизированной конфигурации. COLLOQUIUM-JOURNAL. 2019 г., Т. 13, 2, стр. 243-247.
16. Крыжановский А.В. Применение искусственных нейронных сетей в системах обнаружения атак // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2008. – Т. 2. – № 1. – С. 104-105.
17. Кудряшов И.С. Регистрация событий в системах обнаружения компьютерных атак // Информационное противодействие угрозам терроризма. – 2005. – № 5. – С. 106-109.
18. Марченко А.А., Матвиенко С.В., Нестерук Ф.Г. К обнаружению атак в компьютерных системах нейросетевыми средствами // Научно-технический вестник информационных технологий, механики и оптики. – 2007. – № 39. – С. 83 93.

19. Паклин Н.Б., Орешков В.И. Бизнес-аналитика: от данных к знаниям: учебное пособие. – 2-е изд., испр. – СПб.: Питер, 2013. – 704 с.
20. НПАОП 0.00-1.29-97 «Правила захисту від статичної електрики».
21. ДБН В.2.5-28-2006 «Інженерне обладнання будинків і споруд. Природне і штучне освітлення».
22. ДСТУ 12.1.005-88 «ССБП. Загальні санітарно-гігієнічні вимоги до повітря робочої зони».
23. ДСТУ 8604:2015 «Дизайн і ергономіка. Робоче місце для виконання робіт у положенні сидячи. Загальні ергономічні вимоги».
24. ДСТУ Б В.2.5-82:2016 «Електробезпека в будівлях і спорудах. Вимоги до захисних заходів від ураження електричним струмом».
25. Linux Driver for USB WiFi Adapters that are based on the RTL8812BU and RTL8822BU Chipsets. [Електронний ресурс] – Режим доступу до ресурсу: https://github.com/morrownr/88x2bu.
26. Poston H. 13 popular wireless hacking tools [updated 2021] [Електронний ресурс] / Howard Poston. – 2021. – Режим доступу до ресурсу: https://resources.infosecinstitute.com/topics/hacking/13-popular-wireless-hacking-tools/.
27. Radiotap [Електронний ресурс] – Режим доступу до ресурсу: https://www.radiotap.org/.
28. Seyma T. Faster Lookups In Python. towards data science. [Електронний ресурс] / Tas Seyma – Режим доступу до ресурсу: https://towardsdatascience.com/faster-lookups-in-python-1d7503e9cd38
29. Vanhoef M. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2 [Електронний ресурс] / M. Vanhoef, F. Piessens\'s – Режим доступу до ресурсу: https://www.researchgate.net/publication/320417220_Key_Reinstallation_Attacks_Forcing_Nonce_Reuse_in_WPA2.
30. Конституція України [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.