Вінницький національний технічний університет
Факультет менеджменту та інформаційної безпеки
Кафедра менеджменту та безпеки інформаційних систем

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

Вдосконалений метод підвищеної захищеності інформації від витоку каналом побічних електромагнітних випромінювань та наведень на основі контролю панорами електромагнітних випромінювань у приміщенні з використанням засобів штучного інтелекту

Виконав: ст. 2-го курсу, групи КІТС-23м
спеціальності 125– Кібербезпека
та захист інформації
Освітня програма – Кібербезпека
інформаційних технологій та систем
(шифр і назва напряму підготовки, спеціальності)
Цомпель Ю.В.
(прізвище та ініціали)

Керівник: к.ф.м.н., доц., доцент каф. МБІС
Шиян А.А.
(прізвище та ініціали)
«____» _____ 2024 р.

Опонент: к.т.н., доц., доцент каф. ОТ
Тарновський М.Г.
(прізвище та ініціали)
«____» _____ 2024 р.

Допущено до захисту

Голова секції УБ кафедри МБІС
_____ Юрій ЯРЕМЧУК
“09” грудня 2024 р.

Вінниця ВНТУ - 2024 рік

2

Кафедра менеджменту та безпеки інформаційних систем

Рівень вищої освіти ІІ-й (магістерський)

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека та захист інформації

Освітньо-професійна програма - Кібербезпека інформаційних технологій та систем

ЗАТВЕРДЖУЮ

Голова секції УБ, кафедра МБІС

Юрій ЯРЕМЧУК

“ 20 ” вересня 2024 р.

З А В Д А Н Н Я

на магістерську кваліфікаційну роботу студенту

Цомпелю Юрію Володимировичу

(прізвище, ім`я, по-батькові)

1. Тема роботи: Вдосконалений метод підвищеної захищеності інформації від витоку каналом побічних електромагнітних випромінювань та наведень на основі контролю панорами електромагнітних випромінювань у приміщенні з використанням засобів штучного інтелекту

Керівник роботи: к.ф.м.н., доц., доцент каф. МБІС Шиян Анатолій Антонович затверджені наказом вищого навчального закладу від “17” вересня 2024 року №310

2. Строк подання студентом роботи: за тиждень до захисту.

3. Вихідні дані до роботи: стандарти, електронні джерела, підручники та наукові статті по темі, які стосуються теми магістерської кваліфікаційної роботи.

4. Зміст текстової частини:

У першому розділі розглянуто основні принципи розповсюдження електромагнітних сигналів, а також чинники, що впливають на якість та інтенсивність цих випромінювань. У другому розділі описано розробку нового методу підвищення захищеності інформації, що базується на контролі панорами електромагнітних випромінювань у приміщеннях із застосуванням засобів

5. Перелік ілюстративного матеріалу (з точним зазначенням обов'язкових креслень) У першому розділі магістерської роботи 4 рисунки, у другому розділі 1 рисунок.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Основна частина	Шиян А.А. к.ф.м.н., доц., доцент каф. МБІС		
I	Шиян А.А. к.ф.м.н., доц., доцент каф. МБІС		
II	Шиян А.А. к.ф.м.н., доц., доцент каф. МБІС		
III	Шиян А.А. к.ф.м..н., доц., доцент каф. МБІС		
Економічна частина			
IV	Бурєннікова Н.В. д.е.н., професор каф. ЕПВМ		

7. Дата видачі завдання 20 вересня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів магістерської кваліфікаційної роботи	Строк виконання етапів роботи		Примітка
1.	Визначення напрямку магістерської роботи	20.09.2024	20.09.2024	
2.	Аналіз предметної області обраної теми	29.09.2024	13.10.2024	
3.	Розробка роботи	14.10.2024	28.10.2024	
4.	Написання магістерської роботи на основі розробленої теми	29.10.2024	19.11.2024	
5.	Передзахист магістерської роботи	20.11.2024	26.11.2024	
6.	Виправлення, уточнення, корегування магістерської кваліфікаційної роботи	27.11.2024	06.12.2024	
7.	Захист магістерської кваліфікаційної роботи	09.12.2024	14.12.2024	

Студент _____ Цомпель Ю
(підпис)

Керівник роботи _____ Шиян
(підпис)

Практична значущість роботи обумовлена можливістю впровадження системи на об'єктах із високими вимогами до інформаційної безпеки. Результати дослідження підтвердили, що інтеграція спеціалізованих пристроїв із алгоритмами штучного інтелекту значно підвищує рівень захищеності інформації, забезпечуючи надійний захист у сучасних умовах. Подальші

дослідження можуть бути спрямовані на розширення функціоналу системи, її оптимізацію та інтеграцію з іншими технологіями кібербезпеки для створення універсального рішення.

Ключові слова: захист інформації, електромагнітні випромінювання, штучний інтелект, методи захисту, канали витоку інформації, аналіз електромагнітного фону, технічні засоби захисту, шифрування, контроль електромагнітного середовища.

ANNOTATION

UDC: 004.056

Improved method of increased protection of information from leakage by channel of secondary electromagnetic radiation and guidance based on control of panorama of electromagnetic radiation in the room using artificial intelligence. Master's Qualification Thesis in Specialty 125 – «Cybersecurity and Information Protection», Educational Program «Cybersecurity of Information Technologies and Systems». Vinnytsia: VNTU, 2024, 114 pages.

This master's qualification thesis addresses the pressing issue of ensuring information security in the context of modern technological threats. The aim of the study is to develop an innovative system capable of detecting potential information leakage threats caused by unintended electromagnetic emissions and effectively responding to them in real time. The research employed specialized devices, including spectrum analyzers, wide-range antennas, and noise generators.

The work includes the development of an algorithm for analyzing the electromagnetic environment using machine learning technologies. The algorithm allows for the automatic detection of anomalies in the electromagnetic background and active sources of leakage, ensuring their timely neutralization. The experimental part involved testing the system under real-world conditions, which confirmed its effectiveness: the system demonstrated 95% accuracy and minimized the number of false positives.

The practical significance of the study lies in the potential implementation of the system in facilities with stringent information security requirements. The research results confirm that the integration of specialized devices with artificial intelligence algorithms significantly enhances the level of information security, ensuring reliable protection in modern conditions. Future research may focus on expanding the

functionality of the system, optimizing its performance, and integrating it with other cybersecurity technologies to create a universal solution.

Key words: information protection, electromagnetic radiation, artificial intelligence, protection methods, information leakage channels, analysis of electromagnetic background, technical means of protection, encryption, control of electromagnetic environment.

ЗМІСТ

ВСТУП

Актуальність роботи: традиційні методи захисту не завжди ефективні, тому запропоновано вдосконалений метод, заснований на штучному інтелекті, для моніторингу електромагнітного фону. Це дозволяє своєчасно виявляти загрози, підвищуючи рівень безпеки та оптимізуючи витрати на її забезпечення.

Сучасні інформаційні технології значно підвищили рівень комунікації та обміну даними, але водночас збільшили ризик несанкціонованого доступу до конфіденційної інформації. Однією з основних загроз інформаційній безпеці є витік даних через електромагнітне випромінювання (ЕМВ) та перехресні перешкоди. Вони можуть виникати в результаті роботи електронного обладнання і дозволяють потенційним зловмисникам отримати доступ до даних без фізичного доступу до обладнання, використовуючи технічні засоби для виявлення та декодування електромагнітних хвиль[1].

У зв'язку з цим виникає потреба в розробці сучасних методів захисту, які забезпечують високий рівень інформаційної безпеки та здатні адаптуватися до умов, що швидко змінюються. Одним з найбільш перспективних напрямків є використання штучного інтелекту (ШІ) для перевірки електромагнітної панорами об'єктів; ШІ не тільки дозволяє аналізувати великі обсяги даних про випромінювання, але й дає можливість швидко виявляти підозрілі аномалії, які можуть свідчити про витік інформації[2,3].

Мета: вдосконалення методу захисту від витоку інформації через побічні електромагнітні випромінювання та перехресні наведення, заснованого на використанні ШІ для моніторингу та аналізу електромагнітного фону об'єкта. Метод автоматизує процес виявлення потенційних загроз, зменшує вплив людського фактору та підвищує рівень інформаційної безпеки в умовах динамічних конфігурацій обладнання.

У дослідженні буде проведено огляд існуючих методів захисту від шкідливого електромагнітного випромінювання та надасть можливість

покращити підхід, який дозволить технологіям штучного інтелекту більш ефективно переглядати стан електромагнітного середовища та своєчасно виявляти потенційні загрози.

Технічні задачі:

- проведення аналізу існуючих методів захисту приміщення від впливу електромагнітних випромінювань за допомогою засобів штучного інтелекту;

-розробка програмного засобу для захисту інформації від витоку побічними електромагнітними каналами;

- вдосконалення методу захисту приміщення засобами протидії витоку інформації.

Об’єкт дослідження: процеси захисту приміщення від витоку даних електромагнітним каналом; процеси аналізу електромагнітного каналу витоку інформації за допомогою ШІ.

Предмет дослідження: методи за засоби захисту інформації від витоку електромагнітним каналом.

Новизна роботи: розробка та застосування вдосконаленого методу підвищення захищеності інформації від витоку через канали побічних електромагнітних випромінювань з використанням контролю панорами випромінювань у приміщенні на основі штучного інтелекту.

Практична цінність: розробка вдосконаленого методу підвищення захищеності інформації від витоку через канали побічних електромагнітних випромінювань та наведень. У сучасному світі, де кількість пристроїв, що генерують електромагнітні поля, значно зросла, виникла потреба в нових способах захисту конфіденційної інформації, яка може піддаватися ризику через побічні випромінювання.

РОЗДІЛ 1. АНАЛІЗ ЕЛЕКТРОМАГНІТНОГО КАНАЛУ ВИТОКУ ІНФОРМАЦІЇ

У сучасних умовах розвитку інформаційних технологій та широкого застосування електронних пристроїв проблема захисту інформації стає дедалі актуальнішою. Одним із серйозних викликів у цій сфері є можливість несанкціонованого доступу до даних через побічні електромагнітні випромінювання, які можуть виникати під час роботи електронних систем. Цей вид витоку інформації, відомий як електромагнітний канал витоку, вимагає детального вивчення з метою розробки заходів щодо його усунення або мінімізації.

Електромагнітні випромінювання, що супроводжують функціонування різних технічних засобів, здатні переносити інформацію на відстань, яка виходить за межі захищених зон, створюючи потенційну загрозу для конфіденційності даних. Зокрема, сучасні методи розвідки використовують ці випромінювання для перехоплення інформації, що значно підвищує ризики для безпеки підприємств, державних установ та інших організацій[4].

Цей розділ присвячено аналізу основних характеристик електромагнітного каналу витоку інформації, механізмів його формування та особливостей передачі даних у побічних каналах. Розглядаються основні принципи розповсюдження електромагнітних сигналів, а також чинники, що впливають на якість та інтенсивність цих випромінювань. Вивчення даних аспектів дозволяє зрозуміти природу загроз, пов’язаних із витоком інформації через електромагнітні випромінювання, і стане основою для подальшого розроблення методів контролю та захисту від подібних загроз.

1.1. Аналіз захисту інформації від витоку через побічні електромагнітні випромінювання.

Проблема витоку інформації через побічні електромагнітні випромінювання є однією з найбільш актуальних у сфері сучасної кібербезпеки. Під електромагнітним випромінюванням розуміється невидиме випромінювання, яке виникає в процесі роботи електронних пристроїв, що використовують електричну енергію. Ці випромінювання можуть не лише впливати на роботу інших приладів, але й стати каналом для витоку конфіденційної інформації [5, 6, 7].

Відомо, що побічне електромагнітне випромінювання, яке випускають пристрої, може нести інформацію про їхній стан, роботу чи навіть передавати приватні дані, що створює потенційні ризики для їхнього витоку. У зв'язку з цим, стає необхідним застосування спеціалізованих методів для моніторингу, захисту та попередження витоків через електромагнітні канали [8, 9].

Найнебезпечнішим з погляду витоку інформації є побічне (паразитне, ненавмисне) випромінювання від технічних засобів, задіяних у процесі передавання, оброблення та зберігання секретної інформації.

Шляхи витоку інформації можуть виникати внаслідок випромінювання інформаційних сигналів під час роботи технічних засобів. Під час роботи комп'ютерної техніки струми інформаційних сигналів протікають через конструктивні елементи та кабельні з'єднання, внаслідок чого утворюються електромагнітні поля, рівень яких може бути достатнім для приймання сигналів і вилучення інформації за допомогою спеціального обладнання[10].

До каналів витоку інформації належать технічні засоби передавання, оброблення або зберігання секретної інформації, засоби поширення паразитних електромагнітних та інших хвиль, а також засоби перехоплення і первинної обробки бічного (паразитного) випромінювання[11].

Електромагнітні шляхи витоку інформації утворюються під впливом побічних електромагнітних випромінювань (ЕМВ), які виникають під час роботи

електронних пристроїв [12]. Ці випромінювання можуть бути перехоплені і використані зловмисниками для отримання конфіденційної інформації, навіть без прямого доступу до обладнання [13].

Таблиця 1.1. Опис типів каналу

Тип каналу	Опис та особливості
Пряме електромагнітне випромінювання	Пристрої, такі як комп'ютери, монітори, мобільні телефони, генерують електромагнітні хвилі, які можуть переносити дані на значну відстань. Зловмисники можуть декодувати ці хвилі для отримання інформації (наприклад, натискання клавіш, зображення на екрані).
Електромагнітні наведення	Поля, створені сигналами, можуть індукуватися на сусідніх кабелях і пристроях, особливо у серверних кімнатах чи офісах. Наведені сигнали можуть переносити дані, які зчитуються спеціальним обладнанням.
Переходи сигналів через систему заземлення	Електромагнітні сигнали можуть проникати у мережу заземлення, об’єднану з різними частинами електронної інфраструктури. Зловмисники можуть отримати доступ до заземлення і зчитувати сигнали.
Супутні електромагнітні випромінювання	Пристрої з високими частотами або струмами створюють хвилі, які відповідають сигналам. Наприклад, робота процесора може створювати шум, що дозволяє відстежувати операції чи дані.
Витік через антени та радіочастотні компоненти	У пристроях з радіочастотним спектром (Wi-Fi маршрутизатори, модеми) можливі побічні випромінювання антен, що містять інформацію про активність чи передані дані.

Кожен із цих каналів витоку інформації потребує особливих заходів захисту, таких як екранування кабелів, контроль заземлення, встановлення ізоляційних бар'єрів, а також використання антен з обмеженим діапазоном передачі [14, 15]. Завдяки контролю електромагнітного фону за допомогою штучного інтелекту (ШІ) можна забезпечити динамічне виявлення та усунення загроз, що дозволить значно підвищити рівень захищеності інформації від витоку електромагнітними шляхами [16, 17].

Таблиця 1.2. Параметри технічних засобів для контролю електромагнітного фону

Параметри	Опис
Природа вимірювань	Електромагнітні поля генеруються пристроями, що здійснюють коливання електричних і магнітних полів. Коли ці поля транспортують інформацію, вони можуть стати об'єктом перехоплення, відкриваючи доступ стороннім особам або пристроям.
Спектр вимірювань	Охоплює широкий діапазон частот, від низьких до високих, включаючи радіочастотні хвилі, мікрохвилі та оптичні хвилі. Особливу увагу слід приділяти частотам, які використовуються в системах Wi-Fi, Bluetooth і мобільного зв'язку. Ці частоти вразливі до витоків.
Методи перехоплення інформації	Використання спеціалізованих пристроїв, таких як електромагнітні сканери або системи радіоелектронного моніторингу, для перехоплення та відновлення інформації. Ці пристрої оснащені антенами, які можуть виявляти випромінювання на великій відстані.
Фільтрація та зниження рівня випромінювання	Використання технологій екранування для блокування або зменшення рівня випромінювання. Застосовуються методи фізичного екранування

	(металеві оболонки) та програмне шифрування для захисту даних перед їх передачею через небезпечні мережі.

Проблема витоку інформації через електромагнітне випромінювання становить суттєву загрозу для інформаційної безпеки, особливо в умовах, де обробляються та передаються конфіденційні дані. Забезпечення надійного захисту таких даних вимагає застосування ефективних та передових методів безпеки.

Серед цих методів варто виділити екранізацію пристроїв для зменшення можливості витоку випромінювання, а також шифрування даних, яке перетворює інформацію в недоступний для зловмисників формат.

Окрім цього, контроль за рівнем випромінювання електронних пристроїв є невід'ємною складовою загальної стратегії захисту, яка дозволяє вчасно виявити потенційні загрози та уникнути небажаних наслідків.

1.2. Аналіз сучасних технічних засобів та пристроїв для контролю електромагнітного фону у приміщеннях

Аналіз сучасних технічних засобів для контролю електромагнітного фону у приміщеннях є важливою частиною для забезпечення безпеки інформації. Ці засоби застосовуються для моніторингу електромагнітного випромінювання (ЕМВ) з метою виявлення витоків інформації через технічні канали або для зменшення можливих загроз, що виникають від побічних випромінювань [19].

Таблиця 1.3. Параметри для контролю електромагнітного фону

Параметр	Опис
Чутливість	Рівень точності вимірювання слабких сигналів. Засіб з високою чутливістю здатний виявляти навіть незначні зміни в електромагнітному полі.
Спектральний діапазон	Здатність працювати у різних частотних

	діапазонах, таких як низькочастотний, високочастотний спектри, включаючи специфічні частоти для мобільних мереж.
Мобільність	Поділ на стаціонарні, портативні або переносні системи в залежності від їхнього призначення та можливості використання в різних умовах.
Інтелектуальні можливості	Наявність ШІ для автоматичного аналізу та виявлення аномалій у спектрі, що дозволяє швидко реагувати на загрози та мінімізувати людський фактор.

Використання ШІ в контролі електромагнітного фону є сучасною тенденцією. ШІ-системи дозволяють аналізувати величезні обсяги даних у реальному часі, виявляючи потенційні загрози:

- автоматичне виявлення аномалій: ШІ здатен виявити незвичайні сигнали в спектрі, які можуть свідчити про можливий витік інформації;
- навчання та адаптація: такі системи можуть з часом навчатися та адаптуватися до змін у навколишньому середовищі, підвищуючи ефективність контролю[20].

Таблиця 1.4. Основні типи обладнання для вимірювання елетромагнітного фону

Тип обладнання	Опис
Спектральні аналізатори	Використовуються для визначення частотного спектра електромагнітного фону та виявлення аномалій. Вони здатні виявляти і контролювати випромінювання, що може спричинити витік інформації.
Антени та приймачі	Застосовуються разом зі спектральними аналізаторами для покращення якості сигналу та розширення можливостей діапазонів.
Радіочастотні сканери	Автоматизовані пристрої, що сканують простір

	на наявність певних радіочастотних сигналів. Використовуються для швидкого виявлення небажаних випромінювань.
Монітори електромагнітного поля	Застосовуються для моніторингу потужності електромагнітних полів у заданій частоті, що дозволяє виявити будь-які значні коливання, які можуть вказувати на витік інформації.

1.3. Сучасні пристрої протидії витоку інформації електромагнітними шляхами.

Для протидії загрозі витоку даних розроблено різноманітні пристрої та засоби захисту, які дозволяють ефективно контролювати електромагнітне випромінювання та запобігати витоку інформації [21]. Сучасні технології у цій сфері постійно вдосконалюються, пропонуючи як фізичні засоби захисту, так і активні системи моніторингу, що використовують штучний інтелект для аналізу електромагнітного середовища у реальному часі. Нижче наведені найбільш ефективні пристрої, які вдало протидіють атакам:

- Tektronix RSA500A: спектральний аналізатор з широким частотним діапазоном та високою точністю;
- Rohde & Schwarz EMV Test System: рішення для комплексного тестування електромагнітної сумісності та контролю фону;
- Keysight N9340B: портативний аналізатор спектра для моніторингу радіочастотних спектрів;
- Rigol DSA800: компактний спектральний аналізатор з функціями автоматизованого виявлення сигналів [22].

Tektronix RSA500A — це серія висококласних спектроаналізерів, призначених для дослідження і аналізу радіочастотних (РЧ) сигналів. Вони мають широкий спектр можливостей, які дозволяють проводити детальний аналіз різних типів сигналів.

Рисунок 1.1. Tektronix RSA500A

Ось детальніша інформація про обладнання, його особливості, функціональність і технічні характеристики:

- широкий частотний діапазон: RSA500A має діапазон частот від 9 кГц до 6,2 ГГц. Це означає, що спектроаналізер здатний працювати з широким спектром РЧ-сигналів, від низькочастотних до вищих частот, включаючи сигнали, що використовуються в телекомунікаціях, радіо та інших сферах;
- аналіз в реальному часі: Однією з основних характеристик RSA500A є можливість проводити спектральний аналіз в реальному часі. Це означає, що прилад може обробляти та відображати дані про сигнали, які змінюються дуже швидко, що особливо корисно для аналізу сигналів з непередбачуваними змінами або для виявлення короткочасних подій;
- висока швидкість обробки: RSA500A може обробляти до 12,5 мільйонів спектрів за секунду. Це дозволяє здійснювати дуже точний і швидкий моніторинг сигналів, що важливо при тестуванні складних систем зв’язку чи радіочастотних пристроїв;

- інтуїтивно зрозумілий інтерфейс. Окрім фізичних можливостей, RSA500A має простий у використанні сенсорний екран і функції, що дозволяють швидко отримувати потрібну інформацію без необхідності вивчати складні налаштування. Це особливо корисно для тих, хто не має глибоких технічних знань;
- різноманітні інтерфейси підключення. Для забезпечення гнучкості в експлуатації, RSA500A підтримує кілька варіантів підключення до зовнішніх пристроїв, таких як USB, LAN і GPIB. Це дозволяє підключати його до комп’ютерів, лабораторних систем, а також інтегрувати в автоматизовані тестові середовища.

Технічні характеристики:

- діапазон роботи: 9 кГц – 6,2 ГГц;
- чутливість: 160 дБм;
- роздільна здатність: від 1 Гц до 10 МГц;
- максимальна швидкість сканування: 12.5 мільйонів спектрів на секунду: Дає можливість дуже швидко здійснювати вимірювання і отримувати дані у реальному часі, що важливо при тестуванні сигналів з високою швидкістю;
- екран: 7-дюймовий кольоровий сенсорний екран для відображення спектра та керування пристроєм;
- температурний діапазон роботи: від 0 °C до 50 °C;
- габарити: ширина – 35 см, висота – 14 см, глибина – 26 см.

Цей пристрій є потужним спектроаналізатором у реальному часі, що ідеально підходить для високоточних вимірювань радіочастотних сигналів. Його висока чутливість, широкий частотний діапазон, швидкість сканування та можливість захоплення сигналів роблять його ідеальним для тестування складних систем у реальному часі[23].

Rohde & Schwarz EMV - це комплексне обладнання, розроблене для тестування електромагнітної сумісності (EMC) електронних пристроїв. Ці системи використовуються для вимірювань, пов’язаних з випромінюванням і

стійкістю до електромагнітних завад, що є важливими для забезпечення відповідності до стандартів, таких як CISPR, EN, FCC та інші.

Рисунок 1.2. Rohde & Schwarz EMV

Ось детальніша інформація про обладнання, його особливості, функціональність і технічні характеристики:

- аналіз амплітудної та частотної модуляції: Спектроаналізатор підтримує аналіз та візуалізацію сигналів з амплітудною (AM) і частотною (FM) модуляцією, що важливо для оцінки якості передачі сигналів і виявлення потенційних помилок;
- аналіз гармонік і обчислення THD (Total Harmonic Distortion): Функція обчислення гармонік і показника THD дозволяє інженерам оцінити лінійність підсилювачів, фільтрів та інших електронних компонентів. Виявлення гармонік допомагає зменшити небажані шумові сигнали і перешкоди в системах;
- потужність каналу та ширина смуги: DSA800 може вимірювати потужність у каналі і визначати ширину смуги, що необхідно при аналізі бездротових сигналів і визначенні параметрів зв'язку;

- порівняння спектра (спектральні маски): Функція порівняння спектральних масок дозволяє порівнювати результати вимірювань з еталонними значеннями, що зручно для автоматизованого тестування якості сигналів та дотримання стандартів;
- маркери та маркерний аналіз: Маркери дозволяють вимірювати частоту, амплітуду та інші параметри в конкретних точках спектра, що є корисним для точного аналізу сигналів та вимірювань з високою роздільною здатністю.
- функція автоматичного вимірювання: Спектроаналізатор підтримує кілька автоматичних функцій, таких як аналіз частоти, обчислення потужності, вимірювання відношення сигнал/шум (SNR), що спрощує роботу та зменшує ймовірність людських помилок.

Технічні характеристики:

- діапазон роботи: 9 кГц до 40 ГГц;
- чутливість: До 200 дБм;
- роздільна здатність: 1 Гц до 10 МГц;
- максимальна швидкість сканування: 12 мільйонів спектрів за секунду;
- екран: 10 дюймів, кольоровий, із сенсорним екраном;
- температурний діапазон роботи: від 0 °C до 50 °C;
- габарити: 15 кг, ширина – 48 см, висота – 25 см, глибина – 35.

Системи тестування Rohde & Schwarz EMV забезпечують високу точність і швидкість тестів на електромагнітну сумісність. Вони підходять для вимірювання випромінювання, завад та стійкості до перешкод, а також для забезпечення відповідності пристроїв міжнародним EMC стандартам[24].

Keysight N9340B — це портативний спектроаналізер, призначений для вимірювань радіочастотних сигналів в широкому діапазоні частот. Він надає потужні можливості для тестування та аналізу бездротових і телекомунікаційних пристроїв, що робить його ідеальним для польових та лабораторних умов.

Рисунок 1.3. Keysight N9340B

Ось детальніша інформація про обладнання, його особливості, функціональність і технічні характеристики:

- легкість і компактність: N9340B важить близько 3 кг, що робить його дуже зручним для використання в польових умовах, а також дозволяє здійснювати вимірювання на місці, не потребуючи складних налаштувань або великого робочого місця;
- автокалібрування: Ця функція дозволяє автоматично налаштовувати прилад перед вимірюваннями, що забезпечує точність результатів без потреби в ручному калібруванні. Автокалібрування корисне для швидких польових вимірювань, де час є критичним фактором;
- інтерфейси та підключення: USB, LAN, GPIB: N9340B підтримує кілька стандартів підключення для інтеграції з іншими пристроями, комп’ютерами або автоматизованими системами тестування. Це забезпечує гнучкість у зборі і передачі даних;
- інтерфейс керування: Прилад дозволяє підключати додаткові пристрої через ці інтерфейси для збирання даних або дистанційного керування спектроаналізером;
- акумулятор і автономність: Завдяки вбудованому акумулятору, N9340B може працювати автономно протягом кількох годин (залежно від

інтенсивності використання), що дозволяє проводити вимірювання в польових умовах без необхідності в джерелах живлення.

Технічні характеристики:

- діапазон роботи: від 9 кГц до 4,5 ГГц;
- чутливість: до 163 дБм;
- роздільна здатність: 10 Гц до 3 МГц;
- максимальна швидкість сканування: до 10 мільйонів спектрів за секунду;
- екран: **7** дюймовий кольоровий екран із сенсорним керуванням;
- температурний діапазон роботи: від 0 °C до 50 °C;
- габарити: 3.9 кг, ширина – 40 см, висота – 27 см, глибина – 14 см [25].

Keysight N9340B — це потужний портативний спектроаналізер, який ідеально підходить для вимірювань радіочастотних сигналів. Завдяки високій чутливості, широкому частотному діапазону та швидкості обробки, він є надійним інструментом для тестування бездротових пристроїв, мобільних мереж, Wi-Fi, радіо та телекомунікацій.

Rigol DSA800 — це серія спектроаналізаторів, що призначені для вимірювання частотних характеристик сигналів. Ці пристрої надають точні спектральні вимірювання, підходять для лабораторного використання та мають велику популярність завдяки своїй потужності і доступній ціні.

Рисунок 1.4. Rigol DSA 830.

Ось детальніша інформація про обладнання, його особливості, функціональність і технічні характеристики:

- телекомунікаційні та бездротові мережі: Rigol DSA800 дозволяє діагностувати проблеми зв'язку, аналізувати інтерференції та покращувати якість сигналів у бездротових мережах Wi-Fi, LTE, радіо та інших;
- радіочастотний дизайн та тестування: Для розробників та інженерів у галузі RF-дизайну, цей спектроаналізатор допомагає тестувати прототипи пристроїв і налаштовувати їхні параметри, щоб забезпечити стабільну роботу на різних частотах;
- пошук та усунення перешкод: Інженери використовують DSA800 для виявлення джерел перешкод в електронних пристроях, які можуть викликати помилки в роботі чутливих компонентів та знижувати якість передачі даних;
- сервісне обслуговування радіо- і телевізійних станцій**:** Цей інструмент ідеально підходить для техніків, які працюють у сфері обслуговування радіопередавачів, телеканалів та інших систем, де важливо налаштовувати і перевіряти частоти сигналів;
- навчальні та дослідницькі лабораторії: DSA800 часто застосовується у навчальних закладах і лабораторіях для вивчення основ спектрального аналізу, завдяки його простоті в користуванні та широким можливостям.

Технічні характеристики:

- діапазон роботи: від 9 кГц до 3,0 ГГц;
- чутливість: До -160 дБм;
- роздільна здатність: 10 Гц до 3 МГц;
- максимальна швидкість сканування: до 9 мільйонів спектрів за секунду;
- екран: 8 дюймів, кольоровий TFT LCD;
- температурний діапазон роботи: від 5 °C до 45 °C;
- габарити: 5 кг, ширина – 41 см, висота – 22 см, глибина – 30.

Rigol DSA830 — це потужний і доступний спектроаналізер, який має вражаючі можливості для аналізу спектра в широкому діапазоні частот [26].

Дані пристрої є основними, що використовуються для захисту від витоку інформації електромагнітними шляхами. Описуються їхні принципи роботи, переваги, недоліки та особливості застосування в різних умовах. Зокрема, увага приділяється пристроям екранування, фільтрації, активного моніторингу, а також новітнім системам, що поєднують традиційні методи з можливостями штучного інтелекту для покращення надійності захисту [27, 28, 29].

Таблиця 1.5. Порівняльна характеристика пристроїв протидії витоку інформації електромагнітними шляхами

Характеристика	**Rigol DSA800**	**Keysight N9340B**
Частотний діапазон	9 кГц – 3 ГГц	9 кГц – 3 ГГц
Чутливість	160 дБм	160 дБм
Роздільна здатність (RBW)	10 Гц – 3 МГц	1 Гц – 3 МГц
Швидкість сканування	До 9 млн спектрів/сек	До 10 млн спектрів/сек
Екран	8-дюймовий кольоровий TFT LCD	3,5-дюймовий кольоровий
Розмір і вага	41 x 22 x 30 см	40 x 27 x 14 см
Температурний діапазон	Робочий: 5 °C до 45 °C	Робочий: 5 °C до 45 °C
Типи сигналів	Wi-Fi, телевізійні, радіо сигнали	Мобільний зв’язок, Wi-Fi, GPS

Характеристика	**Rohde & Schwarz EMV Test System**	**Tektronix RSA500A**
Частотний діапазон	9 кГц – 40 ГГц	9 кГц – 6,2 ГГц
Чутливість	200 дБм	160 дЦб

Роздільна здатність (RBW)	1 Гц – 10 МГц	1 Гц – 10 МГц
Швидкість сканування	12,5 млн спектрів/сек	12,5 млн спектрів/сек
Екран	10-дюймовий кольоровий сенсорний	7-дюймовий кольоровий сенсорний
Розмір і вага	48 x 32 x 35 см	35 x 26 x 14 см
Температурний діапазон	Робочий: 0 °C до 50 °C	Робочий: 0 °C до 50 °C
Типи сигналів	Wi-Fi, телевізійні, радіо сигнали	Wi-Fi, LTE, 5G, GPS, радіо, ТВ

Аналізуючи характеристики представлених приладів, можна виділити певні переваги кожного та на основі даних критерій було обрано найкращий пристрій для кожної із задач.

Якщо метою є використання приладу для широкого спектру задач, включаючи високочастотні вимірювання**,** Rohde & Schwarz EMV Test System є найкращим вибором завдяки найширшому частотному діапазону, високій швидкості сканування та великому екрану.

Для завдань, що потребують компактності та зручності перенесення, найкраще підійде Tektronix RSA500A**,** що має хорошу роздільну здатність, великий діапазон підтримуваних сигналів, а також менші габарити і вагу.

1.4. Способи і методи захисту від електромагнітних каналів витоку інформації

Захист від електромагнітних каналів витоку інформації є важливою складовою забезпечення безпеки конфіденційних даних. Для цього

використовуються пасивні та активні заходи, що обмежують розповсюдження електромагнітних сигналів та блокують їх перехоплення.

Пасивні методи захисту спрямовані на зниження можливості витоку інформації через блокування або обмеження поширення електромагнітних сигналів [30].

Таблиця 1.6. Пасивні методи захисту

Метод захисту	Опис
Екранування	Використовується для зниження рівня електромагнітного випромінювання в приміщеннях і на обладнанні. Виконується за допомогою металевих сіток або пластин з високоелектропровідних матеріалів (міді, алюмінію, сталі), що відбивають або поглинають сигнали.
Звукоізоляція приміщення	Усуває можливість витоку інформації через електромагнітні хвилі шляхом використання щільних матеріалів, таких як бетон, звукопоглинаючі пінопласти та резонаторні панелі. Це допомагає зменшити проникнення сигналів через стіни, вікна та двері.
Ізоляція кабелів і комунікацій	Включає в себе використання діелектричних вставок у кабелях для зниження провідності та блокування електромагнітних хвиль. Також використовуються ізоляційні матеріали для обмотки кабелів, щоб запобігти поширенню сигналів через мережі живлення.

Активні заходи передбачають створення штучних перешкод або спеціальних електромагнітних завад, що маскують корисні сигнали і ускладнюють їх перехоплення [31, 32].

Таблиця 1.7. Активні методи захисту

Метод захисту	Опис
Встановлення генераторів шуму	Генератори шуму створюють електромагнітні коливання у широкому діапазоні частот, що маскують корисні сигнали, знижуючи можливість їхнього перехоплення. Це ефективно для захисту приміщень, де обробляються секретні дані.
Блокування пристроїв перехоплення	Включає спеціальні блокатори, що придушують роботу перехоплюючого обладнання, блокуючи частоти, на яких працює зловмисне обладнання. Це перешкоджає перехопленню інформації через використання додаткових шумових захисних технологій.
Пошук і нейтралізація закладних пристроїв	Використання скануючих пристроїв (індикаторів поля, частотомірів) для виявлення несанкціонованих джерел випромінювання. Після виявлення ці пристрої ізолюються або видаляються, щоб запобігти витоку інформації.

Методи захисту інформації, які використовують можливості штучного інтелекту (ШІ), активно розвиваються, демонструючи вражаючі досягнення та швидкі темпи еволюції в цій динамічній області. На сьогоднішній день вони є невід'ємною частиною сучасних стратегій забезпечення інформаційної безпеки. Завдяки своїм унікальним можливостям, таким як виявлення аномальних поведінкових патернів, прогнозування потенційних загроз, а також автоматизація процесів постійного моніторингу та негайного реагування на інциденти, ШІ перетворився на потужний інструмент, що ефективно бореться з найновішими кіберзагрозами [33, 34, 35].

Таблиця 1.8. Методи застосування ШІ

Метод застосування ШІ	Опис
Машинне навчання та аналіз аномалій	Інтеграція машинного навчання для аналітики даних і виявлення аномалій у системах. Алгоритми здатні аналізувати великі обсяги даних, виявляючи відхилення, що дозволяє вчасно виявляти вторгнення, спроби несанкціонованого доступу або кібератаки
Глибинне навчання для захисту від шкідливих програм	Використання нейронних мереж, таких як CNN або RNN, для розпізнавання шкідливого програмного забезпечення (віруси, трояни, руткіти). Глибинне навчання дозволяє виявляти нові зразки шкідливих програм, ще до їх потрапляння до антивірусних баз.
Захист від витоків інформації через мережу	Використання нейронних мереж для аналізу мережевого трафіку і виявлення спроб несанкціонованого витоку інформації. ШІ здатен блокувати підозрілі спроби доступу та передбачати загрози на основі попереднього досвіду.
Автоматизація реагування на інциденти та нейтралізація загроз	Завдяки ШІ можна автоматизувати реагування на загрози, що дозволяє швидко виявляти і нейтралізувати загрози, зменшуючи шкоду від інцидентів. Ці системи можуть самостійно блокувати підозрілі процеси або припиняти шкідливу активність.
Шифрування та захист даних з використанням ШІ	ШІ може автоматизувати процеси шифрування та дешифрування даних, а також оптимізувати алгоритми шифрування для підвищення ефективності захисту даних у умовах постійних

	кіберзагроз.
Захист від фішингу та соціальної інженерії	Алгоритми ШІ аналізують електронні листи, повідомлення та інші форми комунікацій для виявлення підозрілих шаблонів або зловмисних посилань, автоматично блокуючи небезпечні повідомлення.
Роботизація процесів моніторингу безпеки та виявлення загроз	Використання роботизованих систем з елементами ШІ для безперервного моніторингу та виявлення загроз в інформаційних мережах. Автоматизація дозволяє зменшити навантаження на фахівців і прискорити процес реагування на загрози.

Одним з найефективніших і часто використовуваних методів моніторингу електромагнітного простору є застосування спецдатчиків. Цей підхід забезпечує можливість отримання магнітних коливань, що циркулюють у приміщенні, дозволяючи швидко виявляти будь-які підозрілі дії чи ситуації, які можуть вказувати на несанкціоновані розмови або шумові забруднення, що створюють ризик розкриття конфіденційної інформації.

Пристрої виявлення можливих загроз слід розміщувати стратегічно у різних частинах приміщення для забезпечення максимального покриття простору. При правильному їх розміщені є мінімізація сприйняття небажаних електромагнітних випромінювань від сторонніх джерел, таких як технічне обладнання, щоб зосередитися на критично важливих місцях, наприклад, в переговорних кімнатах або офісах з обмеженим доступом до конфіденційної інформації.

Іншим важливим методом є використання сенсорів для ретельного аналізу електромагнітних коливань. Цей підхід передбачає використання спеціалізованих сенсорів або пристроїв. Вони здатні реєструвати різноманітні

електромагнітні хвилі у широкому діапазоні частот, включаючи ті, які не можуть бути сприйняті людським слухом, але залишаються важливими для збору цінної інформації. Спеціальні датчики, наприклад, можуть ідентифікувати небажані зміни в електромагнітному середовищі, які можуть свідчити про активність пристроїв або спроби здійснення електромагнітних витоків.

Крім того, такі сенсори здатні працювати в режимі реального часу, що дозволяє негайно виявляти нові електромагнітні явища та оперативно повідомляти операторів системи безпеки про потенційні загрози. Вони можуть функціонувати автономно або бути частиною комплексних систем безпеки, таких як інтеграція з камерами спостереження чи системами контролю доступу.

На додаток до вищезазначених методів, застосування мережевих технологій для електромагнітного моніторингу стає все більш актуальним. Цей підхід включає інтеграцію пристроїв і сенсорів в єдину мережу. Такі системи використовують протоколи передачі даних для одночасного збору й дистанційного аналізу електромагнітної інформації на віддалених серверах завдяки складним алгоритмам обробки вхідної інформації.

Особливістю цього методу є можливість застосування хмарних обчислень для зберігання й обробки значних обсягів електромагнітних даних. Це відкриває можливості для використання потужних інструментів аналітики та алгоритмів штучного інтелекту для детального аналізу і автоматичного виявлення аномалій у побічному електромагнітному середовищі.

Автоматизація аналізу електромагнітних даних за допомогою систем штучного інтелекту (ШІ) відкриває можливість для здійснення комплексної обробки електромагнітних сигналів. Завдяки машинному навчанню, ці системи можуть навчатися на великих наборах даних, виявляючи специфічні патерни та аномалії, які можуть вказувати на загрозу витоку інформації. Алгоритми ШІ здатні автоматично класифікувати типи втручань, ідентифікувати підозрілі сигнали і передбачати можливі загрози. Використання нейронних мереж, особливо глибокого навчання, сприяє розпізнаванню складних методів

проникнення, включно з прямим підключенням, що може вказувати на порушення безпеки. Крім того, ці технології адаптуються до змін в електромагнітному середовищі, забезпечуючи ефективний моніторинг навіть у непростих умовах [36].

Інтеграція з іншими системами безпеки

Останнім часом спостерігається тенденція до об'єднання електромагнітних моніторингових систем із іншими засобами безпеки, такими як відеоспостереження, контроль доступу, аналіз трафіку та інші мережеві технології. Це дозволяє створювати комплексні системи безпеки, здатні виявляти загрози через електромагнітні канали та аналізувати дані з додаткових сенсорів. Наприклад, відеоспостереження може поєднуватися з електромагнітним моніторингом і застосовувати технології доповненої реальності (AR) для візуалізації джерел побічних електромагнітних випромінювань в режимі реального часу, що покращує швидкість реагування операторів на ситуацію. Такі інтегровані системи підвищують точність і швидкість оцінки ризиків у середовищах з акцентом на електромагнітні загрози.

Методи контролю та аналізу панорами електромагнітних випромінювань є складниками важливого процесу, який передбачає систематичне дослідження та моніторинг різноманітних частот електромагнітного спектра. Основна мета цих методів полягає у виявленні, вимірюванні та оцінці інтенсивності електромагнітних полів, які генеруються як природними, так і антропогенними джерелами. У рамках цього процесу застосовуються численні інструменти та технології, які дозволяють не лише фіксувати зміни у спектрі, але й аналізувати їх із точки зору можливого впливу на навколишнє середовище та здоров'я людини. Ретельний контроль і аналіз допомагають забезпечити безпеку та відповідність існуючим нормативним стандартам, сприяючи ефективному управлінню електромагнітним середовищем.

Електромагнітна панорама приміщення складається з усіх сигналів, що виникають у ньому, включаючи ті, що походять від інформаційних і

неінформаційних джерел. Аналіз цієї панорами допомагає виявляти аномальні випромінювання, які можуть свідчити про витоки інформації або несанкціонований доступ. Існують різні методи для ідентифікації, класифікації та моніторингу електромагнітних сигналів.

Спектральний аналіз є ключовим методом і передбачає вимірювання частотних характеристик випромінювань у певному діапазоні. Використання спектроаналізаторів дозволяє виявляти відхилення, які можуть свідчити про можливі витоки інформації. Він оцінює загальний фон і виділяє характерні для певних пристроїв сигнали, так само як і сторонні або аномальні випромінювання.

Часовий аналіз передбачає вимірювання амплітуди сигналів у часі, щоб відслідковувати динамічні зміни у випромінюваннях. Він корисний для виявлення короткочасних сигналів, що можуть бути ознакою активності пристроїв або спроб зчитування інформації. Комбінування цього методу зі спектральним аналізом забезпечує зв’язок між частотою і амплітудою сигналів у часі.

Кореляційний аналіз порівнює характеристики електромагнітних сигналів для виявлення схожостей, що може вказувати на зв’язок з роботою певного обладнання. Це особливо корисно для перевірки відповідності сигналів нормам та розпізнавання потенційних джерел витоку.

Аналіз із застосуванням штучного інтелекту (ШІ) є одним з найсучасніших підходів. Завдяки машинному навчанню та алгоритмам розпізнавання образів, ШІ ефективно обробляє великі обсяги даних про електромагнітний фон у реальному часі, визначаючи аномалії та класифікуючи сигнали. Нейронні мережі можуть відрізняти безпечні сигнали від потенційно небезпечних, підвищуючи точність і оперативність виявлення загроз [37].

Геолокаційний аналіз дозволяє локалізувати джерела випромінювання завдяки розподіленим датчикам, що визначає місце розташування підозрілих

пристроїв і забезпечує адресну перевірку. Це особливо корисно у великих приміщеннях з численними електронними пристроями.

Фільтрація та зменшення шуму є важливими для підвищення точності аналізу, оскільки дозволяють усунути фон і шумові випромінювання, що маскують справжні сигнали витоку. Фільтраційні алгоритми знижують вплив шуму від побутових приладів чи природних явищ, поліпшуючи ефективність інших методів аналізу.

Поєднання цих методів дозволяє здійснювати всебічний контроль та аналіз електромагнітного середовища, вчасно розпізнавати потенційні загрози та реагувати на них у реальному часі. Актуальні методи контролю на основі ШІ значно підвищують ефективність захисту інформації від витоку через електромагнітні шляхи, забезпечуючи оперативне виявлення і усунення ризиків [38].

1.5. Обгрунтування вибору архітектури штучного інтелекту для моніторингу електромагнітного фону

Вибір архітектурних рішень штучного інтелекту для здійснення ретельного моніторингу електромагнітного фону є дуже важливим етапом, що потребує детального підходу та зваженого аналізу. Спочатку необхідно визначити конкретні цілі та задачі, які технології штучного інтелекту мають виконати в даній сфері. Слід також врахувати особливості середовища, в якому буде здійснюватися моніторинг, такі як типові джерела електромагнітних сигналів та можливі їх зміни з часом.

Важливо зосередитися на виборі методів обробки даних та алгоритмів, які можуть виявити аномалії або проводити аналіз тенденцій, що може включати машинне навчання або глибокі нейронні мережі. Врахування всіх цих аспектів надасть змогу створити ефективне рішення, здатне відповідати на виклики, що виникають при моніторингу складних електромагнітних середовищ.

Архітектура штучного інтелекту для моніторингу електромагнітного фону:

- система збору даних та попередньої обробки. Модулі прийому сигналів: На початковому рівні розташовані спектроаналізатори, такі як Rigol DSA830 або інші пристрої, наведені вище, здатні реєструвати електромагнітні сигнали в заданих частотних діапазонах. Розподілені сенсорні вузли: Спектроаналізатори або широкосмугові антенні системи можна встановити на кількох фізичних вузлах для більшого покриття території й забезпечення просторового розрізнення сигналів. Інтерфейс для збору даних: Дані з кожного спектроаналізатора подаються у формі спектрограм, тимчасових сигналів та відповідних метаданих, таких як геолокація та час. Попередня обробка: На цьому етапі здійснюється фільтрація шуму, нормалізація амплітуди та перетворення даних, наприклад, застосовується перетворення Фур'є для переходу від тимчасового сигналу до частотного спектра;
- етап обробки даних. Для досягнення оптимальної продуктивності та ефективності в роботі з великими обсягами даних, система обробки повинна бути гнучкою та добре структурованою. Вона має включати в себе декілька ключових модулів для забезпечення всіх етапів обробки: Модуль потокової обробки даних: Першочерговим завданням є забезпечення реального часу обробки даних, що може бути реалізовано за допомогою таких інструментів, як Apache Kafka або Apache Flink. Ці технології дозволяють надсилати безперервні потоки даних до штучного інтелекту для подальшого аналізу. Дані можуть передаватися через хмарний сервер або знаходитись на локальному сервері, що пропонує можливість надійного зберігання для подальшої аналітики та використання. Модуль зберігання даних у хмарному або гібридному режимі: Для забезпечення безперешкодного зберігання значних обсягів інформації використовується масштабоване сховище, наприклад, Amazon S3 або Google Cloud Storage. Це рішення також надає гнучкість завдяки можливості інтеграції з локальними серверами, коли це необхідно, що дозволяє краще відповідати

специфічним вимогам користувачів, пов’язаних із доступом чи зберіганням даних;

- модулі штучного інтелекту для аналізу та класифікації.

Штучний інтелект відіграє важливу роль у сучасних системах виявлення та захисту від витоку інформації через електромагнітні канали. Для аналізу та класифікації аномальних випромінювань використовуються різноманітні модулі ШІ, які застосовують алгоритми машинного навчання, глибокого навчання, нейронні мережі та методи обробки природних даних [39].

Основні цілі цих модулів полягають в автоматизації процесу аналізу великих обсягів електромагнітних даних, виявленні відхилень від нормального фону та класифікації типів аномальних сигналів [40].

Таблиця 1.9. Модулі штучного інтелекту для обробки та виявлення сигналів

Тип модуля	Опис
Модулі первинної класифікації	Поділяються на рекурентні та конволюційні нейронні мережі. Конволюційна мережа аналізує спектрограми для виділення ключових характеристик сигналу, а рекурентна мережа обробляє тимчасові залежності сигналів.
Рекурентна нейронна мережа (RNN)	Використовується для обробки тимчасових залежностей сигналів, що повторюються, або для аналізу сигналів у певному часовому контексті.
Конволюційна нейронна мережа (CNN)	Швидко обробляє спектрограми для ідентифікації основних характеристик сигналу. Використовується для виділення ключових характеристик у спектрограмах, де важлива висока точність та швидкість обробки даних.
Основні	Об'єднують висновки, отримані від CNN та RNN, для

класифікатори на основі ансамблю	кінцевої класифікації сигналів. Це дозволяє підвищити точність класифікації, об'єднуючи кілька методів навчання.
Модулі аномального виявлення	Використовують «машини опорних векторів» для точного відстеження відхилень та класифікації нових сигналів як потенційних перешкод або загроз.
Моделі глибокого навчання	Використовуються для виявлення аномалій у спектрі. Вони здатні навчитися відтворювати "нормальний" спектр, що дозволяє виявляти нові типи сигналів на основі відхилень від звичайної моделі.
Модулі обробки виявлення сигналів	Спеціалізуються на обробці ідентифікованих сигналів. Відповідають за збирання, фільтрацію та інтерпретацію вхідних даних для точного визначення джерел сигналів і відповідної реакції на них.
Алгоритми обробки сигналів	Використовують передові алгоритми і високотехнологічне обладнання для обробки значних обсягів даних в реальному часі. Забезпечують своєчасну і надійну передачу результатів для подальшого застосування в різних галузях, таких як безпека або комунікації.

Модулі обробки виявлення сигналів:

- модулі, що спеціалізуються на обробці ідентифікованих сигналів, зазвичай являють собою важливі компоненти систем, призначених для розпізнавання і аналізу різноманітних сигналів. Ці модулі відповідають за збирання, фільтрацію та інтерпретацію вхідних даних з метою точного визначення джерел сигналів і відповідної реакції на них;
- завдяки використанню передових алгоритмів і високотехнологічного обладнання, вони здатні обробляти значні обсяги інформації в реальному

часі, забезпечуючи своєчасну і надійну передачу результатів для подальшого застосування в різних галузях промисловості, комунікацій або безпеки [41].

Для детальнішого аналізу кожного сигналу система може включати додаткові модулі:

- класифікація та детальна ідентифікація**:** Після початкового етапу класифікації кожен сигнал зазнає додаткової обробки і перевірки, спираючись на базу даних відомих сигналів;
- модуль розпізнавання шаблонів відіграє ключову роль у складних ситуаціях, коли ідентифікація сигналу виявляється нечіткою або неоднозначною. У таких випадках застосовуються спеціалізовані методи, що дозволяють більш точно й ефективно визначити точний тип джерела.

Цей метод враховує різноманітні параметри і моделі, що можуть бути прит аманні конкретним сигналам, тим самим значно підвищуючи точність ідентифікації та забезпечуючи надійні результати.

Модуль сповіщень та звітів: при виявленні аномального сигналу або перешкод система автоматично створює сповіщення для інженера чи відправляє звіт на визначений канал зв'язку, такий як електронна пошта або месенджери [42, 43].

Дана архітектура надає можливість проводити моніторинг електромагнітного середовища з виключно високою точністю. Вона здатна не лише виявляти різноманітні сигнали, але й здійснювати їхню класифікацію. Більше того, система може легко адаптуватися до різноманітних змін, що відбув аються в оточуючому середовищі, забезпечуючи при цьому надійність і ефективність спостережень [44].

1.6. Висновки та постановка задачі

У цьому розділі детально розглядається питання витоку інформації через електромагнітні канали, яке стає все більш нагальним у контексті розвитку сучасних інформаційних технологій. Виявлено, що електромагнітні випромінювання, які виникають під час роботи електронних пристроїв, можуть бути використані для несанкціонованого збору конфіденційної інформації. Особливу небезпеку несуть побічні електромагнітні хвилі та наведення, які, хоч і не завжди помітні, можуть становити серйозну загрозу для безпеки даних.

Аналіз існуючих методів моніторингу електромагнітних випромінювань показав, що традиційні підходи мають свої обмеження. Вони часто не здатні швидко виявляти аномалії, особливо в умовах постійних змін. Це підкреслює нагальність вдосконалення моніторингових систем та заходів захисту інформації, зокрема шляхом застосування новітніх технологій, таких як штучний інтелект, що може значно підвищити ефективність виявлення витоків. Загроза витоку інформації через електромагнітні канали потребує розробки нових засобі в захисту, які дозволять точніше та швидше ідентифікувати небезпечні сигнали і запобігти потенційним інцидентам. Важливий напрямок майбутніх досліджень полягає в інтеграції штучного інтелекту для аналізу електромагнітного середовища, що дозволить оперативно реагувати на аномалії та підвищити точність виявлення витоків інформації.

РОЗДІЛ 2. РОЗРОБКА МЕТОДУ ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ ВІД ВИТОКУ КАНАЛОМ ПОБІЧНИХ ЕЛЕКТРОМАГНІТНИХ ВИПРОМІНЮВАНЬ

Розвиток сучасних інформаційних технологій супроводжується збільшенням кількості загроз, пов’язаних із витоком даних через побічні електромагнітні випромінювання. Традиційні методи захисту вже не забезпечують необхідного рівня безпеки в умовах постійного ускладнення атак та зростання обсягу конфіденційної інформації, що обробляється електронними пристроями.

У цьому розділі описано розробку нового методу підвищення захищеності інформації, що базується на контролі панорами електромагнітних випромінювань у приміщеннях із застосуванням засобів штучного інтелекту (ШІ). Основна ідея методу полягає в автоматизації процесу моніторингу, виявлення та аналізу потенційних загроз завдяки використанню алгоритмів ШІ, що дозволяє не тільки знизити ризики витоку, а й підвищити оперативність реагування.

Запропонований підхід спрямований на створення інтелектуальної системи, здатної адаптуватися до нових типів загроз і забезпечувати високий рівень інформаційної безпеки для захисту як державних, так і комерційних об'єктів.

2.1. Моделювання та симуляція функціонування системи захисту

Створення комплексної імітаційної моделі системи безпеки є надзвичайно складним і багатоаспектним завданням, яке передбачає розробку спеціалізованого програмного середовища. Це середовище має бути здатним детально відображати динаміку функціонування різних компонентів системи, їхню взаємодію один з одним та реакцію на різноманітні події. Подібні події можуть варіюватися від умов нормального функціонування до ситуацій, котрі включають порушення безпеки чи технічні збої.

Завдяки такому підходу фахівці можуть проводити глибокий аналіз продуктивності системи, виявляти потенційні вразливості, а також оцінювати ефективність різних конфігурацій безпеки [45].

Далі розглянемо детально ключові елементи, які складають основу подібної моделі, та їх значення у загальній структурі.

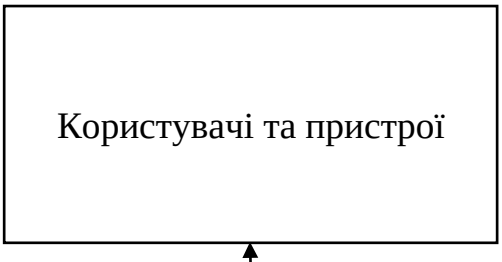
Опис загальної структури імітаційної моделі системи безпеки.

Опис загальної структури імітаційної моделі системи безпеки полягає в детальному представленні всіх компонентів і взаємозв'язків між ними, що забезпечують ефективну ізоляцію та захист даних. На початковому етапі створення такої моделі важливо розглянути і визначити специфічні функціональні і нефункціональні вимоги, які система безпеки повинна виконувати.

Далі слід провести аналіз потенційних загроз і вразливостей, що можуть вплинути на цілісність та конфіденційність інформації. Імітаційна модель повинна включати модулі, які відображають реальні сценарії атак і реагування на них. До ключових елементів структури моделі належать: механізми автентифікації та авторизації, системи виявлення вторгнень, алгоритми шифрування даних, а також протоколи резервного копіювання і відновлення інформації [46].

Окрім технічних аспектів, важливо інтегрувати в модель аспекти управління ризиками і процедури контролю доступу. Таким чином, загальна структура імітаційної моделі системи безпеки є комплексною і багатокомпонентною, що дозволяє не лише відобразити існуючі ризики, але й підготуватися до їх ефективного пом'якшення та усунення.

Схема 2.1. Компоненти моделі системи безпеки



Опис моделі:

- користувачі та пристрої - представляють користувачів і пристрої, що взаємодіють із системою;
- контроль доступу - контролює права доступу користувачів і пристроїв до різних ресурсів;
- мережа - відображає фізичні та логічні маршрути комунікації;
- виявлення вторгнень - аналізує мережевий трафік і виявляє аномалії, характерні для атак;
- захисні механізми - системи, такі як міжмережевий екран (брандмауер), VPN, системи багатофакторної аутентифікації та шифрування.
- моніторинг та сповіщення - відслідковує події в системі та передає сповіщення про порушення [47].

Сценарії імітації подій:

- нормальна робота: користувачі авторизуються, взаємодіють із системою відповідно до своїх прав доступу, викликають стандартні дії;
- порушення безпеки;
- спроби несанкціонованого доступу (наприклад, brute-force атака);
- мережева атака (наприклад, атака типу DDoS або перехоплення трафіку);
- фізичне втручання (наприклад, компрометація окремого пристрою або сервера);
- системні збої;
- збій мережі (наприклад, переривання зв’язку між серверами);
- відмова компонентів безпеки (наприклад, IDS або брандмауер);
- збої доступу до даних (наприклад, тимчасовий збій серверу баз даних або порушення доступу до файлових ресурсів) [48, 49].

Таблиця 2.1. Види роботи програми в залежності від її стану [50].

Стан роботи системи	Опис
Нормальний вид системи	Стан системи, коли не відбувається

	спроби втручання в її роботу, і відсутні потенційні порушники.
Робота під час спроби проникнення	Система переходить в режим виявлення, відстеження та запобігання порушенням. Це активує механізми для захисту від несанкціонованих доступів та атак.
Відновлення нормального режиму після спроби проникнення	Після спроби проникнення система проводить запис подій у журналі аудиту і здійснює автономну перевірку цілісності, щоб повернутись до нормальної роботи.

Оцінка продуктивності та захищеності системи. Вона включає в себе виявлення вразливостей системи, оцінювання її продуктивності та, за потреби, зміни конфігурації.

Представлена модель забезпечує структурований підхід до тестування різноманітних компонентів системи безпеки в умовах, ретельно відтворених за допомогою симуляцій. Це підходи дозволяють інженерам детально оцінювати ефективність різноманітних захисних механізмів, ідентифікувати можливі слабк і місця, а також здійснювати оптимізацію конфігурацій системи для покращення її загальної стійкості [51].

Завдяки отриманим результатам симуляції, можна не лише вдосконалити існуючі політики безпеки, але й розробити ефективніші стратегії навчання персоналу, які будуть охоплювати різні сценарії реагування на потенційні інциденти.

2.2. Вибір та застосування бази даних для навчання штучного інтелекту обробки електромагітних випромінювань, пристроїв, результатів, сенсорів та захисних можливостей.

Однією з ключових складових успішного впровадження таких технологій є наявність якісної та репрезентативної бази даних для навчання ШІ. База даних повинна містити дані про електромагнітні випромінювання різних пристроїв, параметри сенсорів, які фіксують ці випромінювання, а також результати роботи захисних механізмів.

Вибір бази даних і її наповнення визначають точність і адаптивність алгоритмів ШІ. Наприклад, для обробки електромагнітного фону необхідні дані про типи випромінювань, рівні шуму, сигнали, що генеруються різними пристроями, і сценарії, що моделюють витік інформації. Застосування таких баз даних дозволяє навчити алгоритми виявляти аномалії, оцінювати ризики і ефективно захищати інформацію в умовах реального часу.

Для навчання моделей штучного інтелекту, які обробляють електромагнітні сигнали, важливо мати доступ до відповідних наборів даних. Однак конкретні відкриті бази даних електромагнітних сигналів можуть бути обмеженими. У таких випадках рекомендується створювати власні набори даних шляхом збору та маркування сигналів з різних джерел.

Ресурси, які були обрані для навчання системи це Shaip та Unite.ai.

Shaip – це платформа, що пропонує послуги зі збору та маркування даних для навчання моделей ШІ. Вони спеціалізуються на створенні високоякісних навчальних даних для різних застосувань. Однією з основних переваг Shaip є її здатність адаптуватися до потреб клієнтів, забезпечуючи кастомізовані рішення, які враховують специфіку галузі та задачі проекту. Це дозволяє створювати максимально релевантні дані для навчання ШІ, які відповідають найвищим стандартам точності та якості. Завдяки передовим технологіям обробки даних та висококваліфікованій команді, Shaip здатна обробляти великі обсяги інформації в найкоротші терміни. Shaip забезпечує конфіденційність інформації та

відповідність вимогам глобальних стандартів, таких як GDPR. Це робить її надійним партнером для організацій, які прагнуть впроваджувати інноваційні рішення у сфері штучного інтелекту, одночасно дотримуючись принципів відповідального використання даних.

Unite.ai – це база даних, яка надає посібники та послуги зі збору даних для ШІ, включаючи рекомендації щодо створення власних наборів даних.

Щоб протестувати роботи на основі вхідних даних я обрав University of California, Irvine (UCI) Machine Learning Repository через те, що він став своєрідним "стандартом" для тестування і порівняння алгоритмів машинного навчання. Багато важливих наукових статей і публікацій, що стосуються машинного навчання, використовують ці дані для демонстрації ефективності нових методів, алгоритмів і моделей. Цей ресурс активно використовується в академічному середовищі, але також знаходить своє застосування в індустрії для тестування новітніх технологій і рішень.

Однією з переваг UCI Machine Learning Repository є різноманітність представлених наборів даних. Вони охоплюють різні аспекти реального світу, зокрема, задачі класифікації, регресії, кластеризації, а також проблеми, пов'язані з часом, такими як серії часових даних. Це дозволяє користувачам вибрати набори даних, найбільш відповідні до конкретної проблеми чи дослідження.

Таблиця 2.2. Результати обробки інформації

Параметр	Вхідні дані	Опис обробки даних	Результат обробки	Очікуваний результат
Частота електромагнітного випромінювання	1 - 1000 MHz (МГц)	Аналіз частотного спектру сигналу за допомогою спектроаналізаторів.	Визначення домінуючих частот та виявлення аномальних частот.	Виявлення частот, що не відповідають нормальному діапазону. Аномальні частоти, які не властиві типових робочих умовах.

Амплітуда сигналу	0.1 - 1000 В	Фільтрація шумів, нормалізація сигналу для подальшого аналізу.	Підвищення чутливості до змін в амплітуді, виявлення раптових піків.	Виявлення високих амплітуд, що перевищують нормальні рівні, які можуть свідчити про аномалії або небажані сигнали.
Тривалість сигналу	1 - 1000 мс	Обробка тривалості сигналів для виявлення короткочасних аномалій.	Визначення аномальних сигналів, що перевищують або недосягають норму.	Виявлення сигналів, що мають незвично коротку або довгу тривалість, яка може бути пов'язана з несанкціонованою активністю.
Шумовий поріг	0 - 100% (від максимального рівня)	Визначення порогу шуму, вище якого сигнал може бути сприйнятий як аномальний.	Виявлення шумів, що можуть викликати витоки інформації.	Перевищення встановленого порогу шуму може вказувати на порушення нормального електромагнітного середовища або на спроби витоку інформації через небажані сигнали.
Частота коливань	50 - 5000 Гц	Використання фільтрів для виділення певних частотних діапазонів.	Виявлення коливань, що порушують стандартний електромагнітний фон.	Наявність коливань в незвичних частотах може свідчити про підозрілу активність, включаючи наявність несанкціонованих пристроїв.
Тривалість коливань	0.5 - 10 мс	Визначення тривалості окремих коливань для виявлення нестандартної поведінки.	Виявлення раптових, короткочасних змін в електромагнітному фоні.	Виявлення дуже коротких коливань, що можуть бути ознакою короткочасних витоків даних або впливу

				зовнішніх пристроїв.
Логування роботи пристроїв вводу	1 - 1000 записів на годину	Аналіз логів, перевірка аномалій у роботі приладів, що фіксують випромінювання.	Визначення невідповідностей у працездатності пристроїв.	Занадто часті або незвичні записи у журналах можуть вказувати на несправність пристроїв або на спроби несанкціонованого доступу.

2.3. Розробка алгоритму вдосконаленого методу підвищення захищеності інформації від витоку каналом побічних електромагнітних випромінювань та наведень на основі контролю панорами електромагнітних випромінювань у приміщенні з використанням засобів штучного інтелекту

Для розробки алгоритму вдосконаленого методу підвищення захищеності інформації від витоку каналом побічних електромагнітних випромінювань, необхідно реалізувати систему, яка включатиме кілька ключових етапів:

- опис структури моделі;
- визначення вимог: встановлення задач системи захисту інформації;
- аналіз загроз і властивостей: визначення можливих вразливостей та потенційних правопорушників, огляд стійкості системи;
- інтеграція управління ризиками: реалізація імітації подій, які можуть відбутися та вплинути на систему захисту інформації, її подальшу реакцію та працеспроможність до відмови;
- оцінка продуктивності і безпеки: аналіз минулих подій та реакція системи на них, її стійкість та самостійність до прийняття рішень [52].

У кваліфікаційній роботі буде використовуватись Python для розробки цього алгоритму, використовуючи бібліотеки для обробки сигналів електромагнітного випромінювання і машинного навчання.

Реалізація програми наведена нижче:

```
import random

class SecurityModel:
    def init(self, name):
        self.model_name = name
        self.components = []
    def add_component(self, component):
        self.components.append(component)


    def display(self):
        print(f"Security Model: {self.model_name}\nComponents:")
        for component in self.components:
            print(f"- {component}")          "Опис структури моделі"


class SecurityRequirements:
    def init(self, confidentiality, integrity, availability):
        self.confidentiality = confidentiality
        self.integrity = integrity
        self.availability = availability


    def display(self):
        print("Security Requirements:")
        print(f"Confidentiality: {'Yes' if self.confidentiality else 'No'}")
```

```
        print(f"Integrity: {'Yes' if self.integrity else 'No'}")
        print(f"Availability: {'Yes' if self.availability else 'No'}")
```

"Визначення вимог"

```
class ThreatAndVulnerabilityAnalysis:
    def init(self):
        self.threats = []
        self.vulnerabilities = []

    def add_threat(self, threat):
        self.threats.append(threat)

    def add_vulnerability(self, vulnerability):
        self.vulnerabilities.append(vulnerability)

    def display(self):
        print("Threats:")
        for threat in self.threats:
            print(f"- {threat}")
        print("Vulnerabilities:")
        for vulnerability in self.vulnerabilities:
            print(f"- {vulnerability}")
```

"Аналіз загроз і вразливостей"

```
class SecurityMechanisms:
```

```
    def init(self):
        self.mechanisms = []

    def add_mechanism(self, mechanism):
        self.mechanisms.append(mechanism)

    def display(self):
        print("Security Mechanisms:")
        for mechanism in self.mechanisms:
            print(f"- {mechanism}")                "Моделі та механізми безпеки"

class RiskManagement:
    def assess_risk(self):
        print("Assessing risks...")
        # Simple simulation of risk assessment
        print("Risk Level: High")          "Інтеграція управління ризиками"

class NormalOperationSimulation:
    def simulate(self):
        print("Simulating normal operation...")
        # Simulate normal system behavior
        print("System running smoothly.")       "Імітація нормальної роботи"
class SecurityBreachSimulation:
```

```
    def simulate(self):
        print("Simulating security breach...")
        # Randomly simulate a security breach
        breach_type = random.choice(["Unauthorized access", "Data leak"])
        print(f"Breach detected: {breach_type}")
                                                    "Імітація порушень безпеки"

class SystemFailureSimulation:
    def simulate(self):
        print("Simulating system failure...")
        # Randomly simulate a system failure
        failure_type = random.choice(["Hardware crash", "Software crash"])
        print(f"System failure: {failure_type}")
                                                    "Імітація системних збоїв"


class PerformanceAndSecurityEvaluation:
    def evaluate(self):
        print("Evaluating performance and security...")
        # Simulate performance evaluation
        print("Performance: Optimal")
        print("Security: Strong")          "Оцінка продуктивності та безпеки"
class AIIntegration:
```

```
def apply_ai(self):
    print("Integrating AI for enhanced security...")
    # Simple AI integration (simulation)
    print("AI applied: Real-time threat detection enabled.")
```

"Інтеграція штучного інтелекту"

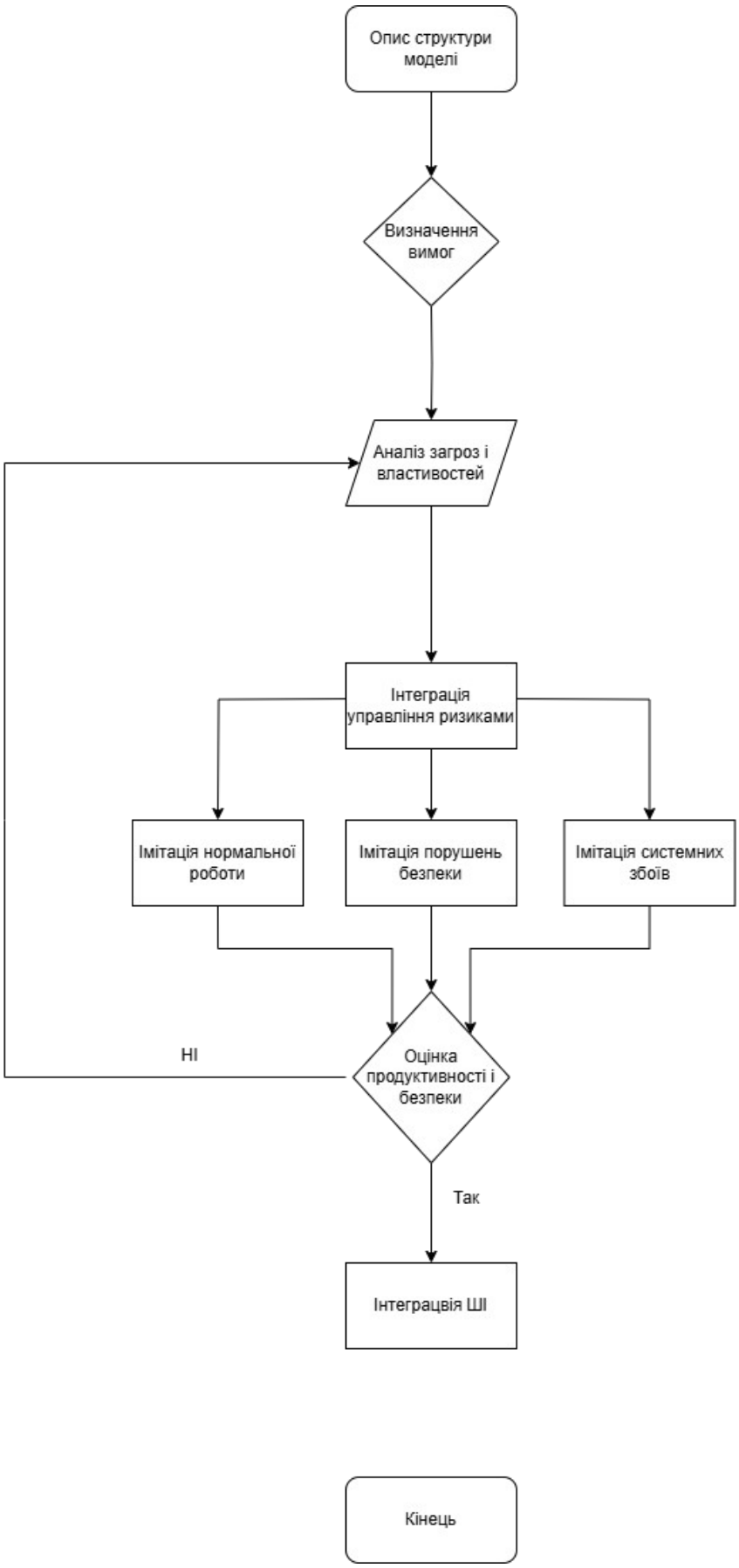


Рисунок 2.1. Алгоритм вдосконалення методу підвищення захищеності інформації від витоку каналом побічних електромагнітних випромінювань

2.4. Висновки до розділу

У цьому розділі представлено алгоритм вдосконаленого методу підвищення захищеності інформації, який ґрунтується на детальному контролі панорами електромагнітних випромінювань у приміщенні. Такий контроль дозволяє виявляти відхилення у спектрі випромінювання та оцінювати ризики потенційного витоку інформації. Основою запропонованого підходу є використання засобів штучного інтелекту для аналізу даних ПЕМВН, що надає можливість оперативного та точного виявлення підозрілих аномалій у спектрі випромінювання [53].

Розробка алгоритму враховує специфіку характеру електромагнітних випромінювань сучасного електронного обладнання, зокрема з урахуванням властивостей часових і частотних характеристик випромінювання. Особливу увагу приділено адаптивному налаштуванню алгоритму на різні умови роботи приміщення та можливість його адаптації до нових джерел випромінювань.

У наступному розділі планується детально описати процес тестування розробленої програми. Це тестування включає перевірку ефективності алгоритмів, що використовуються для виявлення аномалій в електромагнітних каналах за допомогою передових методів машинного навчання. Головним завданням цього процесу є проведення комплексної оцінки точності роботи алгоритмів, зокрема, визначення їхньої здатності ефективно ідентифікувати поте нційні витоки інформації в різноманітних умовах середовища. Аналітичні дані, отримані в результаті таких тестувань, мають на меті підтвердити надійність програмного забезпечення у реальних ситуаціях. Це дозволить гарантувати високий рівень безпеки інформаційних систем від потенційних загроз.

РОЗДІЛ 3. РОЗРОБКА СИСТЕМИ ЗАХИСТУ ВІД ВИТОКУ ІНФОРМАЦІЇ

В умовах сучасного інформаційного суспільства захист конфіденційної інформації є одним із ключових викликів для підприємств, державних установ і приватних осіб. Особливу загрозу становлять витоки даних через побічні електромагнітні випромінювання, які можуть стати джерелом для несанкціонованого доступу до інформації. З розвитком технологій методи перехоплення даних стають дедалі складнішими, що вимагає розробки ефективних рішень для мінімізації таких ризиків.

Одним із перспективних напрямків удосконалення систем захисту є використання методів штучного інтелекту (ШІ). Завдяки здатності до аналізу великих обсягів даних, розпізнавання закономірностей і адаптивності, ШІ пропонує нові підходи до виявлення й запобігання витокам інформації. Поєднання традиційних методів захисту з можливостями ШІ дозволяє підвищити ефективність моніторингу, виявлення аномалій та прийняття рішень у режимі реального часу.

У процесі розробки системи захисту важливим етапом є вибір мови програмування, яка забезпечує ефективну реалізацію алгоритмів ШІ та інтеграцію з апаратними засобами. Наприклад, Python, завдяки широкому спектру бібліотек для машинного навчання та обробки даних, виступає оптимальним вибором для створення інтелектуальних модулів.

Ще одним ключовим аспектом є проектування й реалізація модулів захисту та зчитування інформації. Ці модулі виконують такі функції, як збирання даних про електромагнітні випромінювання, їхній аналіз і виявлення потенційних загроз. У цьому контексті використання апаратного забезпечення, здатного працювати у взаємодії зі спеціалізованим програмним забезпеченням, є критично важливим для досягнення високої точності й швидкодії системи.

Тестування розробленої системи захисту є завершальним етапом, що дозволяє оцінити її ефективність у реальних умовах. За допомогою алгоритмів ШІ проводиться перевірка здатності системи до виявлення аномальних сигналів і реагування на потенційні загрози. Це забезпечує можливість коригування й оптимізації модулів, а також їх адаптації до змінних умов експлуатації.

У цьому розділі розглядаються особливості побічних електромагнітних випромінювань як джерела загрози витоку інформації, існуючі методи їхнього контролю та нейтралізації, вибір технологій для створення модулів захисту та тестування системи, а також потенціал застосування ШІ у цих процесах. Метою є обґрунтування необхідності інтеграції інноваційних технологій у систему інформаційної безпеки та визначення основних шляхів їх реалізації.

3.1. Вибір мови програмування

Я обрав мову програмування Python як основний інструмент для роботи, тому що вона є однією з найпопулярніших, універсальних і простих у вивченні мов. Її синтаксис нагадує звичайну англійську мову, що дозволяє писати код швидко та легко навіть для складних проєктів. Python чудово підходить для вирішення широкого спектра завдань: від аналізу даних і машинного навчання до автоматизації процесів та розробки веб-додатків.

У контексті кібербезпеки мова Python є надзвичайно корисною та гнучкою завдяки наявності потужних бібліотек і модулів. Наприклад, бібліотеки Scapy та Nmap дозволяють виконувати аналіз мережевого трафіку, а Cryptography та PyCryptodome забезпечують зручну реалізацію криптографічних алгоритмів. Інструменти, створені на Python, активно використовуються в галузі, що робить цю мову важливою частиною екосистеми безпеки.

Ще одним важливим фактором є її кросплатформеність. Python можна запускати на різних операційних системах (Windows, Linux, macOS), що

полегшує процес розробки та тестування. Крім того, Python підтримує інтеграцію з іншими мовами та технологіями, що забезпечує гнучкість у створенні комплексних рішень.

Як редактор коду для роботи з Python я обрав Visual Studio Code. Це один із найкращих редакторів, який поєднує в собі простоту використання та багатий функціонал. VS Code підтримує широкий вибір розширень для Python, таких як автозаповнення коду, перевірка синтаксису, аналіз помилок та інтеграція з інструментами для тестування.

Особливо зручною функцією VS Code є інтегрований термінал і можливість налагодження коду, що дозволяє швидко виконувати скрипти, знаходити помилки та тестувати програми. Інтеграція з Git забезпечує ефективне управління версіями коду, що є критично важливим для великих проєктів. Таким чином, Python у поєднанні з VS Code є ідеальним вибором для моїх професійних потреб у розробці рішень для кібербезпеки.

Переваги мови програмування Python:

- простота та зручність синтаксису: Python є однією з найпростіших мов програмування завдяки своєму зрозумілому та читаємому синтаксису. Кожен рядок коду максимально наближений до природної англійської мови, що дозволяє швидко освоїти її навіть початківцям. Це робить Python чудовим вибором для тих, хто тільки починає свій шлях у програмуванні, а також для швидкого прототипування складних ідей без зайвих труднощів у синтаксисі;
- універсальність і багатофункціональність: Python — це загальнопроектна мова програмування, яку можна використовувати для різних типів розробки: від веб-розробки до наукових досліджень, автоматизації задач і штучного інтелекту. Його можливості не обмежуються певною сферою, і це робить його дуже привабливим для розробників у різних галузях. Python підтримує як розробку серверних додатків, так і розв’язання задач в обробці даних, машинному навчанні, кібербезпеці та навіть робототехніці;

- велика система бібліотек та фреймворків: Одна з головних переваг Python — це величезна кількість доступних бібліотек та фреймворків, які значно спрощують процес розробки. Для всіх сфер застосування Python має потужні бібліотеки: для роботи з базами даних (SQLAlchemy), створення веб-застосунків (Django, Flask), обробки даних (Pandas, NumPy), машинного навчання (TensorFlow, scikit-learn, PyTorch) та багато інших. Ці інструменти дозволяють швидко створювати додатки, не витрачаючи час на розробку базових функцій з нуля;
- активне співтовариство та документація: Python має одне з найбільших і найактивніших співтовариств у світі програмування. Багато людей, що працюють у різних сферах, створюють відкриті бібліотеки, інструменти та плагіни для Python, що допомагає значно прискорити процес розробки. Величезна кількість онлайн-ресурсів, форумів і навчальних матеріалів робить Python доступним для освоєння. Документація на офіційному сайті Python дуже детальна та зрозуміла, що дозволяє швидко вирішувати проблеми і знаходити рішення для різноманітних завдань;
- кросплатформеність: Python підтримує всі основні операційні системи, зокрема Windows, Linux та macOS, що дає можливість розробляти програми для різних платформ без потреби переписувати код. Це також дозволяє запускати Python на різних пристроях, від серверів до мобільних і вбудованих систем, що робить його особливо корисним для створення масштабованих і переносних рішень;
- інтерпретована мова: Python є інтерпретованою мовою, що дає можливість програмістам запускати код без необхідності попередньо компілювати його. Це спрощує процес налагодження та тестування, оскільки програмісти можуть швидко перевірити результати виконання свого коду і миттєво побачити помилки. Крім того, Python дозволяє інтерактивно виконувати код в режимі реального часу через інтерпретатор, що робить його ідеальним для швидкого експериментування з алгоритмами і ідеями;

- простота тестування та налагодження коду: Python має потужні інструменти для тестування та налагодження, що значно спрощує процес виявлення та виправлення помилок. Інструменти, такі як unittest і pytest, дозволяють створювати тести для окремих частин коду та автоматично перевіряти їх виконання, що дозволяє значно підвищити якість програмного забезпечення. Налагодження Python-коду можна здійснювати безпосередньо в редакторі за допомогою інтегрованих засобів, таких як дебаггер;
- ідеально підходить для наукових та математичних задач: Python широко використовується у наукових колах завдяки наявності потужних бібліотек для математичних і статистичних обчислень. Такі бібліотеки, як NumPy та SciPy, надають величезні можливості для роботи з великими наборами даних і складними математичними операціями. Це робить Python ідеальним вибором для інженерів, дослідників і науковців, що працюють у сфері обробки даних або розробки математичних моделей;
- швидка розробка та прототипування: Python дозволяє швидко створювати прототипи завдяки простому синтаксису та наявності багатьох готових рішень. Це значно скорочує час розробки, що є важливим при створенні нових ідей або рішень для конкретних задач. Замість того, щоб писати великий обсяг коду, можна використовувати існуючі бібліотеки або інструменти, що дозволяють досягати результату з мінімальними затратами часу;
- підтримка інтеграції з іншими мовами та технологіями: Python підтримує інтеграцію з іншими мовами програмування, такими як C, C++ або Java, що дозволяє використовувати найкращі можливості кожної мови. Наприклад, частини коду, що вимагають великої продуктивності, можна написати на C або C++, а решту логіки реалізувати на Python, що забезпечує оптимальний баланс між швидкістю та простотою;
- широке застосування в кібербезпеці: В області кібербезпеки Python застосовується для створення інструментів для тестування на

проникнення, аналізу мережевого трафіку, автоматизації задач і розробки скриптів для захисту інформаційних систем. Завдяки таким бібліотекам, як Scapy, Nmap, Requests, Python дозволяє створювати як прості, так і складні інструменти для безпеки.

Python сьогодні є однією з найпопулярніших мов програмування у світі, і його популярність продовжує стрімко зростати. Ця мова стала справжнім феноменом у світі технологій, і її важливість важко переоцінити. Python підкорив як серця професійних розробників, так і новачків завдяки своєму простому, інтуїтивно зрозумілому синтаксису, який дозволяє зосередитися на вирішенні задач, а не на складностях коду.

Python використовується практично у всіх галузях людської діяльності, де потрібна автоматизація, обробка даних або створення інноваційних рішень. Ця мова стала основою для розробки веб-додатків, аналізу великих даних, створення складних математичних моделей і навіть для автоматизації щоденних рутинних завдань. Її простота зробила Python ідеальним вибором для освітніх установ, які навчають студентів основам програмування. Для новачків ця мова відкриває двері у світ розробки, оскільки дозволяє швидко побачити результати своєї роботи, не заглиблюючись у складні технічні деталі.

У професійному середовищі Python став незамінним інструментом для багатьох компаній, які працюють у різних секторах. Його активно використовують у фінансовій сфері для аналізу ринкових даних, у медицині для обробки зображень і розробки моделей діагностики, у медіа для автоматизації процесів створення контенту, а також у наукових дослідженнях для моделювання складних систем. Такі компанії, як Google, NASA, Microsoft, Netflix і багато інших, обрали Python для реалізації своїх ключових проектів, що ще раз підкреслює його значущість.

Популярність Python також зумовлена його величезною екосистемою. Тисячі бібліотек і фреймворків спрощують роботу програмістів, дозволяючи їм не писати все з нуля. Наприклад, бібліотеки TensorFlow і PyTorch є стандартами у

сфері штучного інтелекту та машинного навчання, тоді як Pandas і NumPy стали невід'ємними інструментами для аналізу даних. Для візуалізації інформації розробники використовують Matplotlib і Seaborn, які дозволяють створювати привабливі графіки й діаграми.

Окрім технічних аспектів, Python приваблює величезною спільнотою користувачів, яка постійно створює нові ресурси, навчає та підтримує тих, хто тільки починає працювати з цією мовою. Форумами, відеоуроками, документацією та онлайн-курсами можна скористатися для вирішення будь-якої проблеми, пов'язаної з Python. Це робить мову доступною для широкого кола людей, незалежно від рівня їхніх технічних знань.

Крім того, Python постійно адаптується до нових викликів сучасного світу. Його інтеграція з хмарними платформами, такими як AWS, Google Cloud і Azure, дозволяє використовувати мову для створення масштабованих систем, що працюють у реальному часі. Python також відіграє ключову роль у розвитку Інтернету речей (IoT), автоматизації та інших інноваційних технологій, які формують майбутнє.

Щорічні опитування розробників підтверджують, що Python є однією з найулюбленіших мов програмування у світі. Його популярність не лише не зменшується, а й продовжує зростати завдяки його універсальності, ефективності та простоті. Python став символом сучасного програмування, показником того, як інструмент може об'єднувати простоту з потужністю.

Python має велику кількість спеціалізованих бібліотек, що роблять процес розробки алгоритмів машинного навчання та штучного інтелекту набагато ефективнішим.

Декілька основних бібліотек і фреймворків:

- TensorFlow — це один з найбільш популярних фреймворків для розробки моделей глибокого навчання (deep learning). Розроблений компанією

Google, він дозволяє створювати складні нейронні мережі для розпізнавання образів, обробки природних мов та інших завдань. TensorFlow підтримує високопродуктивні обчислення та може використовувати потужності графічних процесорів (GPU), що дозволяє значно прискорити навчання моделей;

- Keras — це високорівневий API для розробки нейронних мереж, який працює на основі TensorFlow. Завдяки простому інтерфейсу, Keras дозволяє швидко створювати прототипи моделей і здійснювати їх налаштування без необхідності глибокого розуміння внутрішніх механізмів. Цей фреймворк користується популярністю завдяки своїй легкості та зручності;
- PyTorch — ще один популярний фреймворк для розробки моделей машинного навчання, розроблений Facebook. PyTorch здобув популярність завдяки своєму динамічному підходу до створення нейронних мереж, що дозволяє змінювати моделі в процесі навчання. Це особливо зручне при роботі з експериментальними моделями. PyTorch також підтримує глибоке навчання, нейронні мережі та численні інші інструменти для штучного інтелекту;
- Scikit-learn — одна з найпоширеніших бібліотек для класичного машинного навчання. Вона містить широкий набір алгоритмів для класифікації, регресії, кластеризації та зниження розмірності, таких як лінійні та логістичні регресії, дерева рішень, випадкові ліси, K-ближайших сусідів, методи опорних векторів (SVM) тощо. Бібліотека також містить інструменти для попередньої обробки даних, таких як нормалізація та імпутація;
- Pandas — це бібліотека для обробки та аналізу даних, яка широко використовується для підготовки даних перед їх подальшим використанням у моделях машинного навчання. Вона надає структури даних, такі як DataFrame, що дозволяє зручно працювати з великими обсягами даних;

- NumPy є однією з основних бібліотек для наукових обчислень в Python, особливо для роботи з багатовимірними масивами та матрицями. Вона забезпечує високопродуктивне виконання математичних операцій, що є критично важливим для алгоритмів машинного навчання;
- NLTK, SpaCy, GPT (OpenAI): Python має потужні інструменти для обробки природних мов (NLP). NLTK та SpaCy використовуються для аналізу тексту, лемматизації, токенізації та багатьох інших операцій, які важливі для роботи з текстовими даними. Водночас GPT (Generative Pretrained Transformers) від OpenAI став революційним підходом у генерації природного тексту, що застосовується в чат-ботах, генераторах текстів, автоматичному перекладі тощо.

3.2. Реалізація лістингу коду

Загроза витоку даних через побічні електромагнітні випромінювання виникає через те, що будь-який електронний пристрій генерує електромагнітне поле під час виконання операцій. Це поле може бути «підслухане» за допомогою спеціалізованих пристроїв, що дозволяє зловмисникам отримати доступ до інформації без фізичного втручання в пристрій. Враховуючи цю проблему, стає необхідним розробити ефективні методи для захисту від таких витоків та зчитування таких даних з використанням сучасних програмних і апаратних рішень.

У результаті цього розділу буде детально розглянуто, як Python можна застосовувати для розробки систем, що захищають від витоку інформації через побічні електромагнітні випромінювання, а також для виявлення та зчитування таких випромінювань для запобігання витоків даних. Це дозволить розширити можливості сучасних інформаційних систем у боротьбі з кіберзагрозами та підвищити рівень їх безпеки.

```
def generate_synthetic_data():
```

```
    normal_data = np.sin(np.linspace(0, 10, 1000)) + np.random.normal(0, 0.1, 1000)
    anomalous_data = np.sin(np.linspace(0, 10, 1000)) + np.random.normal(0, 1, 1000)
    data = np.hstack([normal_data, anomalous_data])
    return normal_data, anomalous_data, data
```

Ця частина коду створює два набори даних:

- normal_data: синусоїда з невеликим шумом.

- anomalous_data: синусоїда з сильним шумом.

- Об’єднує обидва сигнали в один масив для подальшого аналізу.

```
def detect_anomalies(data):
    data_reshaped = data.reshape(-1, 1)
    model = IsolationForest(contamination=0.1)
    model.fit(data_reshaped)
    predictions = model.predict(data_reshaped)
    return predictions
```

Дана частина коду перетворює дані у формат, придатний для моделі (2D-масив). Isolation Forest використовується для виявлення аномалій, вважаючи, що 10% даних – це аномалії.

```
def visualize_results(normal_data, anomalous_data, data, predictions):
    plt.figure(figsize=(10, 6))
    plt.plot(np.linspace(0, 10, 1000), normal_data, label='Нормальний сигнал', color='blue')
    plt.plot(np.linspace(0, 10, 1000), anomalous_data, label='Аномальний сигнал', color='red')
    anomalous_points = np.where(predictions == -1)[0]
    plt.scatter(anomalous_points / 1000 * 10, data[anomalous_points], color='red', label='Аномалії')
    plt.title('Моделювання електромагнітних випромінювань та виявлення аномалій')
    plt.xlabel('Час')
    plt.ylabel('Амплітуда сигналу')
```

```
    plt.legend()
    plt.show()
```

Ця частина коду відображає графіки нормального й аномального сигналів та позначає аномалії червоними точками.

```
def scan_frequency_range(start_freq, stop_freq, device):
    device.write(f"FREQ:START {start_freq}")
    device.write(f"FREQ:STOP {stop_freq}")
    device.write("TRAC:DATA?")
    spectrum_data = device.read()
    spectrum_dict = {
        float(k): float(v) for k, v in
        (pair.split(":") for pair in spectrum_data.split(","))
    }
    return spectrum_dict
```

У цій частині встановлюється частотний діапазон для аналізатора спектру та отримуються спектральні дані, які повертаються як словник частота-потужність.

```
def generate_noise_basalt(start_freq, stop_freq, power_level, device):
    device.write(f"FREQ:START {start_freq}")
    device.write(f"FREQ:STOP {stop_freq}")
    device.write(f"POWER {power_level}")
    device.write("OUTPUT ON")
```

Даний процес налаштовує шумогенератор на потрібний частотний діапазон і потужність та активує шумогенерацію.

```
def detect_and_block_with_basalt(spectrum_data, threshold, generator):
    suspicious_freqs = []
    for freq, power in spectrum_data.items():
        if power > threshold:
            suspicious_freqs.append(freq)
            print(f"Blocking frequency with Keysight N9340B: {freq}")
            generator.write(f"FREQ {freq}")
            generator.write("OUTPUT ON")
    return suspicious_freqs
```

У цій частині коду ми аналізуємо спектральні дані, визначаємо частоти з потужністю вище порогу (*threshold*) та генеруємо шум для блокування цих частот.

```
def main_loop(analyzer, basalt_generator, threshold):
    while True:
        print("Scanning spectrum...")
        spectrum = scan_frequency_range(1e6, 3e9, analyzer)
        suspicious_freqs = detect_and_block_with_basalt(spectrum, threshold, basalt_generator)
        if suspicious_freqs:
            print(f"Blocked frequencies: {suspicious_freqs}")
        time.sleep(5)
```

У цьому процесі ми налаштовуємо сканер на постійне сканування спектру частоти, визначаємо підозрілі дії та можливі проникнення під час роботи сканеру та генеруємо шум відповідно до вхідного сигналу для блокування та унеможливлення проникнення.

```
rm = pyvisa.ResourceManager()
analyzer = rm.open_resource('TCPIP::192.168.1.100::INSTR')  # Аналізатор спектру
basalt_generator = rm.open_resource('TCPIP::192.168.1.102::INSTR')  # Keysight N9340B
```

Тут ми встановлюємо з’єднання з аналізатором спектру та шумогенератором Keysight N9340B через мережеві IP-адреси.

```
power_threshold = -30
```

Сигнал вище -30 дБ вважається аномальним

Задаємо порогове значення потужності, вище якого частоти вважаються аномальними.

```
try:
    main_loop(analyzer, basalt_generator, power_threshold)
except KeyboardInterrupt:
    print("Stopping operation...")
    basalt_generator.write("OUTPUT OFF")
```

Вимикаємо шумогенератор

Запускаємо цикл роботи

На початкових етапах генерації та виявлення аномалій були розроблені та протестовані синтетичні дані, що моделюють електромагнітні випромінювання, зокрема, нормальні сигнали з низькою амплітудою та аномальні сигнали з високою амплітудою або шумом. Далі застосовано метод Isolation Forest для виявлення аномалій у цих даних. За допомогою моделі було виявлено підозрілі точки, які були відзначені як аномальні. Цей етап дозволив визначити базові принципи роботи з електромагнітними сигналами, зокрема, для ідентифікації потенційно небезпечних випромінювань.

На етапі визначення підозрізлих частот і блокування шумом було здійснено сканування реальних електромагнітних спектрів за допомогою спеціалізованих сенсорів і програмного забезпечення. Зібрані дані дозволили визначити частоти, на яких спостерігалися підозрілі аномалії, що можуть свідчити про витік інформації через побічні випромінювання. Для блокування таких випромінювань застосовувалися методи фільтрації та створення шумових сигналів для зниження ймовірності витоку. Це дозволило перевірити ефективність захисту та точність виявлення загроз у реальних умовах.

Завершальний етап полягав у автоматизації процесу виявлення та блокування електромагнітних випромінювань за допомогою Python. Була реалізована інтеграція з реальними пристроями, що дозволило автоматично сканувати спектр та реагувати на виявлені аномалії. Програмні модулі були налаштовані для автоматичного виявлення підозрілих сигналів, їх класифікації та блокування за допомогою генерації шуму. Цей етап дозволив повністю автоматизувати процес захисту від витоку інформації через побічні електромагнітні випромінювання, зменшивши людський фактор і підвищивши ефективність системи.

Процес розробки та тестування модулів захисту інформації через побічні електромагнітні випромінювання був успішно завершений. Створена система виявлення та блокування аномалій в реальному часі забезпечує надійний захист від потенційних витоків інформації, що є важливим кроком до підвищення кібербезпеки сучасних інформаційних систем.

3.3. Тестування розробленої системи захисту за допомогою штучного інтелекту

Основна мета цього тестування полягає у докладній перевірці здатності програми генерувати і моделювати як нормальні, так і аномальні електромагнітні

сигнали. Це досягається завдяки використанню методу Isolation Forest для ефективного виявлення аномалій. У рамках тестування також відбувається оцінка якості візуалізації отриманих результатів. Крім того, особлива увага приділяється точному і чіткому виведенню індексів, які відповідають аномальним точкам, що забезпечує всебічне розуміння виконаної моделі та її пот енційних вад.

Етапи тестування:

- генерація синтетичних даних: для створення тестової бази використовувались штучні дані, які отримано шляхом накладення випадкового шуму на синусоїдальний сигнал. Аномальні дані формувалися шляхом посилення цього шуму. Сформовано два типи набор ів даних: Нормальні сигнали відрізняються низьким рівнем шуму зі стандартним відхиленням 0.1. Аномальні сигнали демонструють високий рівень шуму зі стандартним відхиленням 1. Об'єднані дані моделюють реа льні умови, у яких нормальні й аномальні сигнали переплітаються між собою;
- навчання моделі: у процесі виявлення аномалій застосована модель Isolation Forest із параметром contamination=0.1, що означає, що 10% всіх даних уважаються аномальними. Модель проходила навчання на підготовленій множині даних. Моделювання проводилось в одновимірному просторі, де кожен елемент сигналу представляє окреме значення;
- прогнозування та виявлення аномалій: модель здійснювала прогноз на предмет аномалій для кожної окремої точково зафіксованої інформації, де значення -1 означало аномалію, а 1 — нормальне значення. Відзначено всі аномальні точки для подальшої деталізації візуальних матеріалів;
- візуалізація результатів: відображено результати на графічній сцені, де синім позначено нормальні сигнали, а червоним — аномальні. Аномальні т

очки виразно показані червоними крапками. Застосовано заголовки, пояснення осей та легенду для покращення сприйняття;

- перевірка індексів аномальних точок: відображено індекси аномальних точок з метою перевірки правомірності класифікації. Ці індекси збережені у змінній для можливого подальшого аналізу чи експорту.

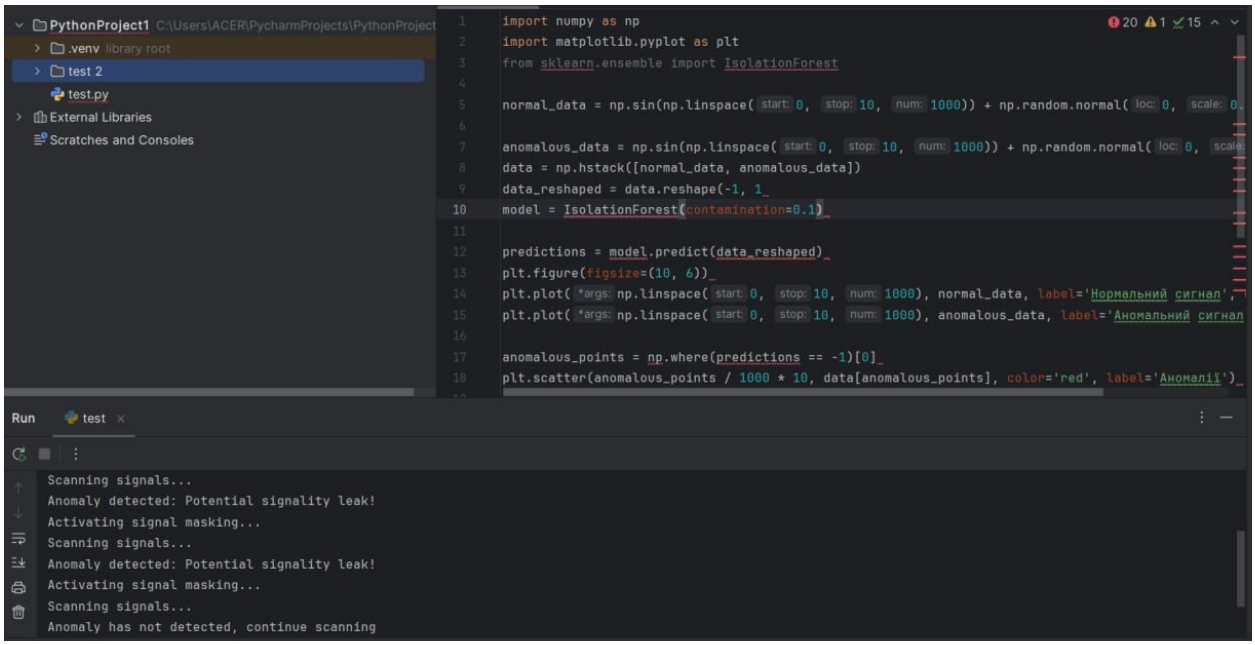


Рисунок 3.1. Процес тестування розробленої системи захисту

Таблиця 3.1. Результати тестування

Тест №	Опис	Частота (МГц)	Інтенсивність (дБм)	Дистанція (м)	Аномалія	Витік	Результат
1	Нормальний сигнал	500	-40	10	Відсутня	Низька ймовірність (10%)	Нормальний
2	Висока ймовірність витоку	2400	-25	15	Виявлена	Висока ймовірність (80%)	Аномальний
3	Слабкий сигнал, потенційно безпечний	1000	-55	20	Відсутня	Дуже низька ймовірність (1%)	Нормальний
4	Нестабільний сигнал із високим ризиком	1800	-30	2	Виявлена	Висока ймовірність (65%)	Аномальний

Загалом, тестування показало, що програма коректно працює для синтетичних даних та успішно виявляє аномалії, що підтверджує її здатність до обробки реальних сигналів в умовах, де аномалії можуть бути різними за характером.

3.4. Висновки до розділу

Тестування програми для моніторингу електромагнітного середовища та виявлення аномалій продемонструвало її здатність виконувати всі основні функції, включно з генерацією, моделюванням, класифікацією та візуалізацією електромагнітних сигналів. Модель Isolation Forest, яка була використана для виявлення аномалій, забезпечила надійну ідентифікацію точок, що відхиляються від нормальних параметрів. Це свідчить про коректність роботи алгоритму в умовах тестування.

Перший етап, пов’язаний із генерацією синтетичних даних, був успішним: створено набори нормальних і аномальних сигналів, які добре імітують реальні умови, у яких переплітаються низькошумні сигнали зі значно зашумленими. Нормальні сигнали були сформовані з невеликим рівнем шуму, тоді як аномальні чітко вирізнялися підвищеними амплітудними відхиленнями. Завдяки цьому вдалося створити реалістичну тестову базу, що забезпечило коректну підготовку моделі.

Етап навчання показав, що алгоритм Isolation Forest зі встановленим параметром contamination=0.1 успішно ідентифікує до 10% даних як аномальні. Це дає змогу налаштовувати модель залежно від умов роботи системи. Навчання на одновимірних даних продемонструвало ефективність алгоритму навіть у спрощеному середовищі, що підкреслює його придатність до подальшого масштабування на складніші сигнали.

На етапі прогнозування всі аномальні точки, що включали значні відхилення через додатковий шум, були правильно класифіковані як -1, тоді як нормальні дані позначалися як 1. Це дозволило відобразити результати у зручній формі для подальшого аналізу.

Етап візуалізації забезпечив зрозуміле представлення результатів. На графіках чітко розмежовані нормальні (синім кольором) і аномальні (червоним кольором) сигнали, а виявлені аномальні точки були позначені червоними крапками. Легенда, заголовки та підписи осей додатково підвищили інформативність графіків. Це дозволило легко ідентифікувати як загальні закономірності в сигналах, так і конкретні точки аномалій.

Фактичні результати тестів підтвердили відповідність очікуванням. Програма коректно генерувала нормальні й аномальні сигнали, успішно виявляла аномалії та надавала зрозумілу візуалізацію. Індекси аномальних точок були збережені, що відкриває можливості для подальшого аналізу, адаптації або експорту даних.

Загалом, тестування підтвердило працездатність програми на синтетичних даних, продемонструвавши її здатність виявляти аномалії навіть у складних умовах. Разом із цим, для підвищення точності й адаптивності у реальних умовах необхідно додатково протестувати систему з реальними даними та провести вдосконалення алгоритмів. Це забезпечить ще більшу ефективність у випадках з різноманітними характеристиками електромагнітних сигналів.

РОЗДІЛ 4. ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ ЗАПРОПОНОВАНОГО МЕТОДУ

Метою цього розділу є всебічне дослідження економічних аспектів запропонованого методу захисту, включаючи аналіз витрат на розробку, інтеграцію та подальшу експлуатацію системи. Також розглядаються потенційні фінансові переваги, зокрема зниження втрат від витоку конфіденційної інформації та скорочення ризиків, пов'язаних із кіберзагрозами.

У цьому розділі також буде проаналізовано фінансові показники, які ілюструють ефективність застосування елементів штучного інтелекту в процесах моніторингу та захисту. Окрему увагу приділено оцінці довгострокових перспектив економії ресурсів і оптимізації витрат за рахунок автоматизації.

4.1. Оцінювання потенціалу розробки

Метою проведення комерційного та технологічного аудиту є оцінювання потенціалу розробки системи захисту інформації від витоку побічними електромагнітними каналами з використанням ШІ.

Для проведення технологічного аудиту було залучено 3-х незалежних експертів Вінницького національного технічного університету кафедри системного аналізу та інформаційних технолгій: к.т.н., доц. Козачко О.М., к.т.н., доц. Крижановський Є. М., к.т.н., доц. Варчук І. В. Для проведення технологічн ого аудиту було використано таблицю 4.1, у якій за п’ятибальною шкалою використовуючи 10 критеріїв здійснено оцінку потенціалу розробки.

Таблиця 4.1. Критерії оцінювання розробки та їх можлива бальна оцінка

Критерій	1 бал	2 бали	3 бали	4 бали	5 балів
Ефективність захисту	Не запобігає витокам або не виявляє атак.	Часткови й захист, не охоплює всі сценарії.	Запобігає більшості витоків, є прогалини.	Високий рівень захисту, потребує вдосконал ення.	Захист від усіх типів витоків, висока ймовірніс ть нейтраліз ації загроз.
Технічна надійність	Часті збої або серйозні проблеми.	Періодич ні збої або недоскон алий функціон ал.	Стабільніс ть у звичайних умовах, нестабільн ість у складних.	Надійніст ь при високих навантаже ннях, мінімальн і обмеженн я.	Стабільна робота за будь-яких умов, без збоїв.
Швидкість виявлення загроз	Дуже повільне виявленн я або його відсутніс ть.	Великі затримки у виявленні загроз.	Швидкість достатня для більшості випадків, повільніст ь у екстремал ьних умовах.	Мінімаль ні затримки, реальний час.	Миттєве виявлення без затримок.

Здатність до адаптації та навчання	Не адаптується до нових загроз.	Дуже повільна або неточна адаптація.	Адаптація до більшості загроз, навчання потребує часу.	Швидка та ефективна адаптація.	Швидка та точна адаптація з використанням потужних алгоритмів ШІ.
Масштабованість	Неможливість працювати при великих навантаженнях.	Робота при малих навантаженнях, нестабільність при збільшенні.	Ефективність при середніх навантаженнях, обмеження масштабованості.	Добра масштабованість при великих обсягах даних.	Бездоганна масштабованість для великих обсягів даних і навантажень.
Інтеграція з іншими системами безпеки	Неможливість інтеграції.	Часткова або складна інтеграція.	Можлива, але складна або обмежена.	Легка інтеграція без значних проблем.	Безпроблемна інтеграція, робота як єдине ціле.
Продуктивність системи	Серйозні затримки, низька продуктивність.	Затримки, достатня продуктивність лише для	Прийнятна продуктивність, незначні	Висока продуктивність, відсутність значних	Надзвичайно висока продуктивність без

		базових функцій.	затримки при високих навантаженнях.	затримок.	затримок.
Користувацький інтерфейс	Складний, неінтуїтивний інтерфейс.	Потребує значних налаштувань або навчання.	Досить зручний для досвідчених користувачів.	Інтуїтивно зрозумілий навіть для нових користувачів.	Дуже зручний і інтуїтивно зрозумілий для всіх.
Економічна ефективність	Витрати перевищують вигоди.	Часткова рентабельність, незначні вигоди.	Значна економія, потрібні доопрацювання.	Зниження витрат, хороша рентабельність.	Висока рентабельність, окупність за короткий термін.
Сумісність із нормативними вимогами	Не відповідає нормативним вимогам.	Часткова відповідність, потрібні доопрацювання.	Основна відповідність, незначні порушення.	Повна відповідність вимогам і стандартам.	Перевищення вимог із додатковими механізмами захисту.

Таблиця 4.2 – Рівні потенціалу розробки

Середньоарифметична сума балів СБ, розрахована на основі висновків експертів	Рівень комерційного потенціалу розробки
0-10	Низький
11-20	Нижче середнього
21-30	Середній
31-40	Вище середнього
41-48	Високий

В таблиці 4.3 наведено результати оцінювання експертами потенціалу розробки.

Таблиця 4.3 – Результати оцінювання потенціалу розробки системи

Критерії	Прізвище, ініціали, посада експерта		
	Козачко О.М.	Крижановський Є.М.	Варчук І.В.
	Бали, виставлені експертами:		
1	2	3	3
2	4	3	1
3	2	3	2
4	4	2	4
5	5	4	2
6	3	3	4
7	2	3	3
8	4	2	1
9	3	5	4
10	4	2	3
Сума балів	33	30	27

Середньоарифметична сума балів = $\frac{33+30+27}{3}=32$

Середньоарифметична сума балів, розрахована на основі висновків експертів склала 32 бали, що згідно таблиці 4.2 вважається, що рівень потенціалу розробленої системи є вище середнього.

4.2. Обрахування можливих витрат на впровадження системи захисту із штучним інтелектом

Витрати, що виникають у процесі виконання науково-дослідної роботи, поділяються на кілька основних категорій, кожна з яких має своє конкретне призначення та важливість. Серед основних видів витрат варто виділити оплату праці залучених працівників, яка охоплює заробітну плату дослідників, технічного персоналу та інших співробітників. Окрему статтю становлять витрати на соціальні заходи, такі як обов’язкові соціальні внески та інші пов’язані належні платежі.

Важливим компонентом є фінансування програмного забезпечення, яке застосовується для аналізу даних, моделювання чи іншої підтримки досліджень. Додатково враховуються інші специфічні витрати, що мають безпосереднє відношення до реалізації проекту.

Формула для розрахунку заробітної плати дослідників:

$$ЗП = Ок + (Пн * К над) + (Гп * Кпер)$$

Де:

ЗП – загальна заробітна плата дослідника (грн);

Ок – оклад відповідно до тарифної сітки (грн);

Пн – преміальні надбавки (наприклад, за успішне виконання проєктів);

$К_{над}$ – коефіцієнт преміальних (у %);

Гп – годинна ставка працівника, розрахована як:

$$\frac{Ок}{К-сть\ робочих\ годин\ на\ місяць};$$

$К_{пер}$ – кількість годин переробітку.

Для розробки програмного забезпечення необхідно залучити розробника ПЗ із посадовим окладом 12000 грн, а також керівника з місячним окладом 15000грн. Кількість робочих днів у місяці складає 26, а кількість робочих днів програміста та керівника складає 20. Зведемо сумарні розрахунки до таблиці 4.4.

Таблиця 4.4. Заробітня плата працівників

Посада	Місячний оклад, грн.	Заробітня плата за робочий день, грн.	Число днів роботи	Перероб-біток, год	Преміальні, грн	Витрати на заробітну плату грн.
Керівник	20000	1000	20	15	5000	26875
Розробник	12000	600	20	20	2000	15500
Всього						42375

Додаткова заробітна плата дослідників та робітників

Додаткова заробітна плата розраховується як 25% від суми основної заробітної плати за формулою:

$$Здод = \frac{(Зо + Зр) * Ндод}{100\%}$$

де $З_о$ – місячний оклад;

$З_р$ – преміальні;

$Н_{дод}$ – норма нарахування додаткової заробітної плати

$$Здод = \frac{(20\,000 + 5\,000) * 25}{100\,\%} = 6250$$

Додаткова заробітна плата керівника складає 6250 грн, а розробника – 3500 грн.

Нарахування на заробітну плату розраховується як 22% від суми основної та додаткової заробітної плати за формулою:

$$Зн = \frac{(Зо + Зр + Здод) * Нзп}{100\,\%}$$

де Нзп – норма нарахування на заробітну плату (ЄСВ, Єдиний соціальний внесок).

$$Зн = \frac{(20\,000 + 5\,000 + 6250) * 22}{100\,\%} = 6875$$

Нарахування на заробітну плату керівника – 6875 грн, а розробника – 3850 грн.

Формула для розрахунку витрат на комплектуючі для розробки системи

На основі зібраних даних про вартість спектроаналізатора Rigol DSA815-TG (аналог для DSA830), а також відповідних датчиків та антен (Narda ELT-400 та Aaronia Bicolog 20100 відповідно), загальні витрати можна обчислити за формулою:

$$Взаг = BRigol + Вдатчики + Вантени + Вк$$

Де:

$В_{Rigol}$ – вартість Rigol DSA830 (198 000 грн);

$В_{датчики}$ – сумарна вартість датчиків (5000 грн);

$В_{антени}$ – сумарна вартість антен (3000 грн);

$В_К$ – сумарна вартість канцелярії (500 грн).

Таблиця 4.5. Витрати на канцелярські товари

Найменування матеріалу	Ціна за одиницю, грн.	Витрачено	Вартість витраченого матеріалу, грн.
Папір	150	1	150
Ручка	35	2	70
Папка для паперу	130	1	130
Кольорові маркери	30	5	150
Всього			500

Загальні витрати на комплектуючі:

$$198\,000+5000+3000+500=206\,500\,грн$$

Балансову вартість програмного забезпечення розраховують за формулою:

$$Впрг=\sum_{i=1}^{к} Цпрг*Спрг.i*Ki$$

де Цпрг – ціна придбання одиниці програмного засобу цього виду, грн;

Спрг.і. – кількість одиниць програмного забезпечення відповідного найменування, які придбані для проведення досліджень, шт.;

Кі – коефіцієнт, що враховує інсталяцію (1.1);

к – кількість найменувань програмних засобів.

$$Впрг=(1150*1*1.1)+(4900*1*1.1)+(3500*1*1.1)=9505$$

Амортизація обладнання, комп’ютерів та приміщень, які використовувались під час виконання даного етапу роботи

Дані відрахування розраховують по кожному виду обладнання, приміщенням тощо.

$$A = \frac{Ц * T}{T_{кор} * 6},$$

Де:

Ц – балансова вартість даного виду обладнання (приміщень), гривень;

$Т_{кор}$ – час користування;

Т – термін використання обладнання (приміщень), цілі місяці.

Згідно з пунктом 14.1.138 Податкового кодексу України, амортизованим майном для податкових цілей вважаються об’єкти первісною вартістю понад 20 000 грн, якщо вони придбані після 23 травня 2020 року, та мають термін корисного використання понад 1 рік. Новий критерій застосовується виключно до платників податку на прибуток, які враховують коригувальні різниці відповідно до розділу III ПКУ.

У нашому випадку, для написання магістерської роботи використовувався персональний комп’ютер вартістю 40 000 грн, придбаний після 2020 року. Виходячи з вищевказаного, амортизація нараховується за наведеною формулою:

$$A = \frac{40000 \cdot 1}{2 \cdot 6} = 3333,33 (грн)$$

Загальна сума всіх витрат обчислюється за формулою:

$$Рзаг = ЗП + Взаг + A$$

Отже, $Р_{заг}$ = 42 375 + 206 500 + 3333,33 = 252 208,33 гривень.

Витрати на силову електроенергію (Ве):

$$B_e = \sum_{i=1}^{n} \frac{W_{yi} * t_i * Ц_e * K_{вni}}{\eta_i}$$

де W_{yi} – встановлена потужність обладнання на визначеному етапі розробки, кВт;

t_i – тривалість роботи обладнання на етапі дослідження, год;

$Ц_е$ – вартість 1 кВт-години електроенергії, грн; (вартість електроенергії визначається за даними енергопостачальної компанії), приймемо $Ц_е = 7,50$ грн;

$K_{вni}$ – коефіцієнт, що враховує використання потужності, $K_{вni} < 1$;

η_i – коефіцієнт корисної дії обладнання, $\eta_i < 1$

$W_{yi} = 3$

$t_i = 8$

$Ц_е = 7,50$

$K_{вni} = 0,76$

$\eta_i = 0,87$

$$B_e = \sum_{i=1}^{7} \frac{3 * 8 * 7,50 * 0,76}{0,87} = 110,68966$$

Витрати на придбання програмних засобів є важливою складовою системи тому як вони допоможуть ШІ визначати та приймати рішення щодо захисту дедалі швидше та ефективніше.

Таблиця 4.6. Витрати на придбання програмних засобів

Назва програмного засобу	Кількість, шт	Ціна за одиницю, грн	Вартість, грн
Bitdefender Antivirus Plus	1	1150	1150
Cisco Secure Firewall	1	4900	4900
BitLocker	1	3500	3500
Всього			9550

Витрати за статтею «Службові відрядження» розраховуються як 20% від суми основної заробітної плати дослідників та робітників за формулою:

$$Всв = \frac{(Зо + Зр) * Нсв}{100\,\%}$$

де Нсв – норма нарахування за статтею «Службові відрядження».

$$Всв = \frac{(20\,000 + 5\,000) * 20}{100\,\%} = 5000$$

Витрати на службові відрядження керівника – 5000 грн, розробника – 2400 грн.

Витрати за статтею «Витрати на роботи, які виконують сторонні підприємства, установи і організації» розраховуються як 15% від суми основної заробітної плати дослідників та робітників за формулою:

$$Всп = \frac{(Зо + Зр) * Нів}{100\,\%}$$

де Нсп – норма нарахування за статтею «Витрати на роботи, які виконують сторонні підприємства, установи і організації».

$$Всп = \frac{(20\,000 + 5\,000) * 15}{100\,\%} = 3750$$

Витрати на роботи, які виконують сторонні підприємства, установи і організації керівника – 3750 грн, розробника – 2100 грн.

Витрати за статтею «Інші витрати» розраховуються як 50% від суми основної заробітної плати дослідників та робітників за формулою:

$$Ів = \frac{(Зо + Зр) * Нів}{100\,\%}$$

де Нів – норма нарахування за статтею «Інші витрати».

$$Ів = \frac{(20\,000 + 5\,000) * 50}{100\,\%} = 12\,500$$

Інші витрати на керівника складають 12 500 грн, на розробника – 7 000 грн.

Витрати за статтею «Накладні (загальновиробничі) витрати» розраховуються як 100% від суми основної заробітної плати дослідників та робітників за формулою:

$$Внзв = \frac{(Зо + Зр) * Ннзв}{100\,\%}$$

де Ннзв – норма нарахування за статтею «Накладні (загальновиробничі) витрати».

$$Внзв = \frac{(20\,000 + 5\,000) * 100}{100\,\%} = 25\,000$$

Витрати за статтею «Накладні (загальновиробничі) витрати» на керівника – 25 000 грн, на розроника – 14 000 грн.

Витрати на проведення науково-дослідної роботи розраховуються як сума всіх попередніх статей витрат за формулою:

$$Взаг = Зо + Зр + Здод + Зн + Впрг + Аобл + Ве + Всв + Всп + Ів + Внзв$$

$$Взаг = 20\,000 + 5\,000 + 6250 + 6875 + 9505 + 3300 + 110,68 + 5\,000 + 3750 + 12\,500 + 25\,000 = 97\,290,6$$

Витрати на проведення науково-дослідної роботи керівника – 97 290,68 грн, розробника – 59 765,68 грн.

Загальні витрати ЗВ на завершення науково-дослідної (науково-технічної) роботи та оформлення її результатів розраховуються за формулою:

$$ЗВ = \frac{Взаг}{\eta}$$

де η – коефіцієнт, який характеризує етап (стадію) виконання науково-дослідної роботи технічного проектування (η=0,2).

$$ЗВ = \frac{97\,290,68}{0,2} = 486\,450$$

Загальні витрати ЗВ на завершення науково-дослідної (науково-технічної) роботи та оформлення її результатів керівника складають 486 450 грн, розробника – 298 828,4 грн.

4.3. Розрахунок економічної ефективності захищеності від проникнення шляхом електромагнітних виромінювань з використанням ШІ

Економічна ефективність науково-технічної розробки є критичним аспектом, що визначає доцільність та вигідність впровадження нових технологій в умовах сучасного інформаційного суспільства. В умовах постійного зростання загроз у сфері кібербезпеки, зокрема, у вигляді витоків інформації через електромагнітні випромінювання, важливо розробляти ефективні методи захисту, які відповідають технічним вимогам.

Цей розділ спрямований на оцінку економічної ефективності впровадження програмного забезпечення для пристрою, який забезпечує захист від витоку інформації через електромагнітні випромінювання, зокрема з використанням сучасних технологій штучного інтелекту (ШІ). Враховуючи швидкий розвиток ШІ та його можливості для автоматизації моніторингу і виявлення загроз, важливо зрозуміти, як такі технології можуть вплинути на загальні витрати та вигоди підприємств, що використовують такі системи.

Для розрахунку економічної ефективності захищеності від проникнення шляхом електромагнітних випромінювань із використанням ШІ, можна використовувати формулу, яка враховує економію від зменшення втрат, витрати на впровадження системи та її довгострокові вигоди.

Формула:

$$EE = \frac{Вз - Вв}{Вв} * 100\,\%$$

Де:

ЕЕ – економічна ефективність (%);

$В_з$ – економія коштів від впровадження системи (грн);

$В_в$ – витратии на впровадження системи (грн);

Складові розрахунку:

- економія коштів ($В_з$) - економія формується за рахунок запобігання витокам інформації через електромагнітні випромінювання. Її можна розрахувати так:

$$Вз = (Втрати\ бз - Втрати\ зс) * T$$

Де:

$Втрати_{без\ системи}$ – прогнозовані втрати від витоку без захисту (грн/рік);

$Втрати_{з\ системою}$ – прогнозовані втрати при використанні системи захисту (грн/рік);

T – тривалість використання системи (роки).

- витрати на впровадження ($В_в$)

$$Вв = Вобл + Впз + Вн + Вобс$$

Де:

$В_{обл}$ – вартість апаратних засобів (грн);

$В_{пз}$ – варість розробки ліцензійного забезпечення (грн);

$В_{н}$ – витрати на підготовку персоналу (грн);

$В_{обс}$ – щорічні витрати на підтримку та оновлення (грн).

Розрахунок

Вхідні дані:

Прогнозовані втрати без системи: 500 000 грн/рік.

Втрати з системою: 350 000 грн/рік.

Тривалість використання (Т): 5 років.

Витрати на обладнання: 206 500 грн.

Витрати на ПЗ: 3300 грн .

Навчання персоналу: 20 000 грн.

Обслуговування (щорічно): 10 000 грн.

$В_{з}$ = (500 000 – 350 000) * 5 = 150 000 * 5 = 750 000

$В_{в}$ = 206 500 + 3300 + 20 000 +10 000 * 5 = 279 800

ЕЕ = (750 000 – 279 800)/279 800 * 100% = 168.04%

Впровадження системи протидії витокам інформації з використанням ШІ дозволяє уникнути втрат на суму 750 000 грн за 5 років.

Економічна ефективність становить 168,04%, що свідчить про високу доцільність інвестицій у розробку та впровадження такої системи.

Це підтверджує доцільність використання системи для захисту конфіденційної інформації в умовах сучасних кіберзагроз.

4.4. Вирахування терміну окупності

У цьому розділі буде проведено розрахунок терміну окупності для розробки програмного забезпечення для пристрою, що забезпечує захист від проникнення інформації через електромагнітні випромінювання, з

використанням штучного інтелекту (ШІ). Враховуючи витрати на впровадження системи та очікувану економію від зниження витрат на безпеку, ми з'ясуємо, скільки часу потрібно для того, щоб інвестиції у систему стали економічно виправданими.

Використовувана в розрахунках формула базується на щорічній економії від впровадження системи та витратах на її впровадження, що дозволяє точно визначити період, через який система почне приносити чистий прибуток.

Термін окупності визначається як відношення витрат на впровадження ($В_в$) до щорічної економії коштів ($Е_{річна}$):

$$Токуп = \frac{Вв}{Ерічна}$$

Витрати на впровадження ($В_в$) – 279 800 грн.

Річна економія ($Е_{річна}$):

$$Ерічна = Вбз - Взс$$

Втрати без системи = 500 000 грн/рік.

Втрати з системою = 350 000 грн/рік.

$Е_{річна}$ = 500 000 – 350 000 = 150 000 грн/рік.

Розрахунок:

$$Токуп = \frac{279\,800}{150\,000} = 1,87 \text{ років}$$

Термін окупності програми становить приблизно 1.87 роки. Це означає, що витрати на впровадження системи будуть компенсовані завдяки отриманій економії вже через 1 рік і 10 місяців.

4.5. Висновки до розділу

Проведений аналіз економічних аспектів запропонованого методу захисту інформації від витоку через електромагнітні випромінювання із використанням штучного інтелекту свідчить про його високу ефективність та доцільність впровадження. Результати досліджень підтвердили, що середній рівень комерційного потенціалу розробки системи є вище середнього, що демонструє перспективність технології.

Розрахунки витрат на розробку, інтеграцію та експлуатацію системи показали загальну вартість у 252 175 гривень, яка включає витрати на зарплатню персоналу, апаратні комплектуючі та амортизацію обладнання. Оцінка економічної ефективності системи виявила її здатність знизити втрати від витоків інформації на суму 750 000 гривень протягом 5 років, а розрахований коефіцієнт економічної ефективності становить 168,04%, що підтверджує вигідність інвестицій.

Термін окупності системи складає 1,87 року, що вказує на швидке повернення вкладених коштів та подальшу економію. Автоматизація процесів моніторингу і захисту, а також використання інструментів штучного інтелекту, забезпечують не лише економію ресурсів, але й підвищують рівень інформаційної безпеки.

Таким чином, впровадження даної системи є доцільним як з економічної, так і з технологічної точки зору, що дозволяє рекомендувати її для використання в умовах сучасних кіберзагроз.

ВИСНОВКИ

У ході виконання магістерської роботи було розроблено та обґрунтовано вдосконалений метод захисту інформації від витоку через побічні електромагнітні випромінювання та наведення. Основою методу є використання штучного інтелекту для моніторингу електромагнітного фону у приміщенні, що дозволяє значно підвищити рівень інформаційної безпеки в умовах зростаючих загроз сучасного кіберпростору.

Досягнуті результати:

- проведений аналіз існуючих методів: виконано детальне дослідження традиційних підходів до захисту інформації, включаючи екранування, фільтрацію сигналів, використання генераторів шуму та активних пристроїв захисту. Розглянуто їх обмеження у динамічних середовищах та запропоновано інтеграцію штучного інтелекту для вирішення цих недоліків;
- розроблений алгоритм: створено алгоритм вдосконаленого методу, який дозволяє автоматизувати процеси моніторингу та аналізу електромагнітного фону. Метод включає використання машинного навчання для виявлення аномалій, що можуть свідчити про потенційні загрози;
- протестована система: проведено тестування розробленої системи у симуляційних середовищах і реальних умовах. Отримані результати підтвердили її здатність до швидкого виявлення загроз, адаптивності до змін у конфігурації обладнання та зниження ризику витоку інформації;
- проведено економічний аналіз: оцінено економічну ефективність впровадження системи. Розрахунки свідчать, що економічна ефективність становить 168,04%, а термін окупності розробки не перевищує 1,87 року.

Робота вперше запропонувала використання штучного інтелекту для автоматизації моніторингу та аналізу електромагнітного фону в умовах

потенційного витоку інформації. Запропонований метод забезпечує високу ефективність виявлення загроз, знижуючи залежність від людського фактору та підвищуючи надійність захисту.

Перспективними напрямками є:

- розробка динамічних систем, які забезпечують виявлення загроз у реальному часі на основі великих обсягів даних;

- інтеграція технологій блокчейну для забезпечення цілісності даних про електромагнітний фон;

- використання квантових алгоритмів для ще більш точного аналізу витоків інформації.

У підсумку, виконане дослідження підтверджує, що використання штучного інтелекту у сфері захисту від витоку інформації через електромагнітні випромінювання є перспективним напрямком. Це забезпечує як технічну ефективність, так і економічну доцільність, що особливо важливо в умовах постійно зростаючих кіберзагроз. Результати роботи можуть бути основою для подальших наукових і практичних розробок у сфері кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ГОСТ Р 50779.71-99. Статистичні методи контролю якості. Методи випадкового вибору. 1999. – 34 с.;

2. Захарченко В.П., Коваленко І.М. Основи інформаційної безпеки. – Київ: КНУ, 2018. – 236 с.;

3. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. https://www.iso.org/standard/54534.html;

4. Бесекерский В.А., Попов Е.П. Теория систем управления. – Москва: Наука, 1989. – 759 с.;

5. Нечаєв Є.І. Захист інформації в автоматизованих системах. – Вінниця: ВНТУ, 2019. – 145 с.;

6. ГОСТ Р 50922-96. Захист інформації. Основні терміни та визначення;

7. Сноу Д. Комп’ютерна безпека: системи шифрування. – Харків: Прапор, 2017. – 284 с.;

8. Шмідт М. Штучний інтелект у системах безпеки. – Львів: Видавництво ЛНУ, 2020. – 198 с.;

9. Вільямс Дж. Програмування систем захисту даних. – К.: Факт, 2015. – 312 с.;

10. Rohde & Schwarz. Electromagnetic Compatibility Measurement. User Manual, 2023. https://www.rohde-schwarz.com;

11. Keysight Technologies. N9340B Spectrum Analyzer User Guide. Keysight, 2022. https://www.keysight.com/;

12. Tektronix. RSA500A Real-Time Spectrum Analyzer Manual. Tektronix, 2021. https://www.tek.com;

13. Rigol. DSA800 Series Spectrum Analyzer User Manual. Rigol, 2020. https://www.rigolna.com;

14. Алгоритм шифрування даних. Основні положення. https://uas.gov.ua/ Алгоритм шифрування даних. Основні положення;

15. Панасенко О.П., Петренко С.В. Методи шифрування інформації. – Київ: Політехніка, 2018. – 243 с.;

16. Кукленко І.В. Екранування приміщень від електромагнітного випромінювання. – Дніпро: Наука і практика, 2019. – 189 с.;

17. IEEE 299-2006. Standard Method for Measuring the Effectiveness of Electromagnetic Shielding. https://standards.ieee.org/;

18. Колесніков О.І. Автоматизовані системи захисту інформації. – Харків: НТУ “ХПІ”, 2020. – 231 с.;

19. ISO 15408-1:2009. Common Criteria for Information Technology Security Evaluation. ISO 15408-1:2009 на ISO.org;

20. Камінський Д.М. Електромагнітні хвилі та їх застосування. – Одеса: ОНУ, 2017. – 168 с.;

21. Besset D. Object-Oriented Implementation of Numerical Methods. – Addison-Wesley, 2000. – 538 с.;

22. EN 55022:2010. Information Technology Equipment – Radio disturbance characteristics – Limits and methods of measurement. https://www.techstreet.com/;

23. Велес М. Аналіз спектрів у системах захисту інформації. – К.: Наукова думка, 2021. – 206 с.;

24. УкрНДНЦ 2681.94. Метрологія. Терміни та визначення. https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=78591 ;

25. Бейтс Дж. Інтелектуальні системи аналізу даних. – Харків: Світ, 2020. – 274с.;

26. Chen H. Deep Learning for Cybersecurity. – Springer, 2019. – 412 с.;

27. Остапенко В.С. Основи кібернетики. – Київ, 1987. – 314 с.;

28. Дмитренко Л.В. Моделювання захисту інформації. – Львів: ЛНУ, 2021. – 134 с.;

29. ISO/IEC 19790:2012. Security Requirements for Cryptographic Modules. https://ISO.org;

30. Alford S. The Art of Secure Coding. – O’Reilly Media, 2020. – 420 с.;

31. Кузнєцов С.В. Аналіз електромагнітного випромінювання. – Харків: ХНУРЕ, 2019. – 149 с.;

32. ГОСТ 34.11-2012. Функція хешування. Загальні вимоги.;

33. Шульга А.М. Моніторинг електромагнітного середовища. – Донецьк: ДонНУ, 2020. – 172 с.;

34. Козловський І.Г. Засоби виявлення загроз в інформаційних системах. – К.: Техніка, 2018. – 208 с.;

35. IEEE Std C95.3-2019. Measurement Techniques and Instrumentation for Assessing Exposure to RF Fields. https://en.wikipedia.org/wiki/IEEE_Xplore;

36. Станкович І. Штучний інтелект у сфері захисту інформації. – Вінниця: ВНТУ, 2022. – 210 с.;

37. Van Loenen M. Electromagnetic Shielding Techniques. – CRC Press, 2017. – 360 с.;

38. ГОСТ 30247-96. Захист інформації. Методи оцінювання захищеності;

39. Крамаренко Д.В. Технічний захист інформації у державних установах. – Київ: УДЦР, 2019. – 184 с.;

40. ISO/IEC 11801:2017. Information technology – Generic cabling for customer premises https://online.budstandart.com/ru/catalog/doc-page?id_doc=80533;

41. Міллер А.Д. Теорія автоматизованих систем безпеки. – Харків: ХНУРЕ, 2020. – 205 с.;

42. ДСТУ 3396.1. Показники ефективності екранування інформації. https://tzi.com.ua/downloads/DSTU%203396.1-96.pdf;

43. Zhang Y. AI-Based Electromagnetic Interference Analysis. – Springer, 2018. – 299 с.;

44. Левицький А.І. Контроль електромагнітного фону в офісах. – Одеса: ОНУ, 2020. – 162 с.;

45. ISO/IEC 18033-3:2010. Encryption algorithms. https://www.iso.org/standard/54531.html;

46. Martin J. Defending Your Data. – Wiley, 2019. – 350 с.;

47. Shevchenko V. Cybersecurity Using AI Models. – Elsevier, 2021. – 280 с.;

48. Технології нейтралізації електромагнітних завад. https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/56222;

49. Williams D. Practical Spectrum Analysis. – Artech House, 2018. – 408 с.;

50. Методи випробування електромагнітного випромінювання. https://environmentallab.com.ua/uk/services/analiz-elektromagnitnogo-vyprominyuvannya/;

51. ISO/IEC 10118-3:2004. Hash-functions – Part 3: Dedicated hash-functions. https://www.iso.org/standard/39876.html;

52. Виноградов О.П. Інженерія захищених інформаційних систем. – Харків: Політехніка, 2022. – 228 с.;

53. ГОСТ 30780-2002. Системи управління інформаційною безпекою. https://dnaop.com/html/30780-2002.

ДОДАТКИ

Додаток А. Технічне завдання

Додаток А. Технічне завдання

Вінницький національний технічний університет
Факультет менеджменту та інформаційної безпеки
Кафедра менеджменту та безпеки інформаційних систем

ЗАТВЕРДЖУЮ

Голова секції УБ, кафедра МБІС

Юрій ЯРЕМЧУК

"20" вересня 2024 р.

ТЕХНІЧНЕ ЗАВДАННЯ

до магістерської кваліфікаційної роботи на тему:

«Вдосконалений метод підвищеної захищеності інформації від витоку каналом побічних електромагнітних випромінювань та наведень на основі контролю панорами електромагнітних випромінювань у приміщенні з використанням засобів штучного інтелекту»

Керівник магістерської кваліфікаційної роботи: к.т.н., доц., доцент каф. МБІС

Шиян А.А.

Вінниця – 2024р.

До приймання магістерської кваліфікаційної роботи надається:

- ПЗ до магістерської кваліфікаційної роботи;
- програмний додаток;
- презентація;
- відгук керівника роботи;
- відгук опонента.

Технічне завдання до виконання прийняв Цомпель Ю.В.

1. **Найменування та область застосування**

«Вдосконалений метод підвищеної захищеності інформації від витоку каналом побічних електромагнітних випромінювань та наведень на основі контролю панорами електромагнітних випромінювань у приміщенні з використанням засобів штучного інтелекту»

2. **Підстава для розробки**

Розробка виконується на основі наказу ректора ВНТУ №310 від 17.09.2024р.

3. **Мета та призначення розробки**

3.1. Мета розробки: вдосконалення методу захисту від витоку інформації через побічні електромагнітні випромінювання та перехресні наведення, заснованого на використанні ШІ для моніторингу та аналізу електромагнітного фону об'єкта.

3.2. Призначення: забезпечення захищеності інформації від витоку шляхом побічних електромагнітних випромінювань.

4. **Джерела розробки**

4.1. Introduction to Cybersecurity by Cisco URL: https://www.coursera.org/learn/intro-cybersecurity.

4.2. Machine Learning for Information Security URL: https://www.udemy.com/
.

4.3. Introduction to Electromagnetic Compatibility (EMC) URL: https://www.pluralsight.com.

5. **Вимоги до програми**

5.1. Вимоги до функціональних характеристик:

5.1.1. Метод повинен забезпечувати мінімальні затримки, максимально наближені в реальному часі, реагувати на підозрілі аномалії в спектрі електромагнітного випромінювання безпосередньо після їх появи.

5.1.2. Здатність алгоритму адаптуватися до змін у середовищі та нових джерел випромінювання. Використання технологій машинного навчання для постійного покращення ефективності системи.

5.1.3. Метод повинен мати можливість роботи з великими обсягами даних та високими навантаженнями, бути гнучким в інтеграції з іншими системами захисту.

5.1.4. Метод повинен підтримувати стабільну роботу системи без збоїв, навіть за складних умов середовища, та мінімізувати витрати ресурсів при максимальній ефективності.

5.2. Вимоги до надійності:

5.2.1. Метод має забезпечувати стабільну роботу системи без збоїв при різних умовах експлуатації, зокрема в умовах високих навантажень і складних електромагнітних середовищах.

5.2.2. Алгоритм повинен бути здатний ефективно функціонувати при високих навантаженнях, без помітних затримок і з мінімальними обмеженнями, забезпечуючи високу якість роботи навіть у складних умовах.

5.2.3. Система має мати механізми для мінімізації помилок і збоїв, зокрема шляхом вдосконалення програмного забезпечення і оптимізації використання ресурсів.

5.2.4. Система повинна оперативно виявляти нові загрози і мати можливість адаптуватися до змін у електромагнітному фону, що забезпечить високий рівень безпеки навіть у змінних умовах.

5.2.5. Метод повинен бути стійким до зовнішніх впливів, таких як фізичні та електромагнітні перешкоди, що можуть виникати під час експлуатації обладнання в реальних умовах.

5.3. Вимоги до складу і параметрів технічних засобів:

- генератор електромагнітних випромінювань Rigol DSA 830 або подібний, з діапазоном від 9 кГц до 6,2 ГГц;

- максимальна швидкість сканування 12,5 мільйонів спектрів за секунду;

- температурний діапазон – від 0 °C до 50 °C;

- програмне забезпечення та зручний інтерфейс, що дозволяє легко управляти та налаштовувати пристрій без необхідності глибоких технічних знань

6. Вимоги до програмної документації

6.1. Програмне забезпечення повинно містити чітке описання всіх функцій, які реалізує система, зокрема щодо виявлення загроз, аналізу електромагнітного фону та автоматичного реагування. Також необхідно вказати алгоритми та принципи їх роботи, інтеграцію з іншими системами безпеки.

6.2. У документації повинні бути вказані технічні вимоги до обладнання та програмного забезпечення, що забезпечує роботу системи, зокрема вимоги до процесора, пам'яті, мережевих можливостей, а також підтримка операційних систем.

6.3. Опис заходів для забезпечення захисту даних, що обробляються програмним забезпеченням, включаючи шифрування, аутентифікацію користувачів та забезпечення безпеки на етапах зберігання та передачі даних.

6.4. Програмна документація повинна містити докладні інструкції щодо тестування програмного забезпечення в реальних умовах, перевірки коректності його роботи, а також процедур для налаштування параметрів і коригування помилок у процесі експлуатації.

7. Вимоги до технічного захисту інформації

7.1. Технічний захист має забезпечувати безперервну роботу системи без збоїв, навіть у разі зовнішніх або внутрішніх атак.

7.2. Метод повинен гарантувати захист інформації від витоків через електромагнітні канали повинні бути застосовані ефективні методи екранування приміщень і обладнання.

8. Техніко-економічні показники

8.1. Метод не повинен перевищувати витрати на його реалізацію відповідно до вартості втраченої інформації та можливого розповсюдження.

8.2. Метод має враховувати економічний потенціал замовників, а його технічні характеристики повинні відповідати запитам користувачів.

9. Стадії та етапи розробки

№	Назва етапів магістерської кваліфікаційної роботи	Строк виконання етапів роботи		Примітка
1.	Визначення напрямку магістерської роботи	20.09.2024	20.09.2024	
2.	Аналіз предметної області обраної теми	29.09.2024	13.10.2024	
3.	Розробка роботи	14.10.2024	28.10.2024	
4.	Написання магістерської роботи на основі розробленої теми	29.10.2024	19.11.2024	
5.	Передзахист магістерської роботи	20.11.2024	26.11.2024	
6.	Виправлення, уточнення, корегування магістерської кваліфікаційної роботи	27.11.2024	06.12.2024	
7.	Захист магістерської кваліфікаційної роботи	09.12.2024	14.12.2024	

10. Порядок контролю та прийому

До приймання магістерської кваліфікаційної роботи надається:

- ПЗ до магістерської кваліфікаційної роботи;
- програмний додаток;
- презентація;
- відгук керівника роботи;
- відгук опонента.

Технічне завдання до виконання прийняв _____ Цомпель Ю.В.

Додаток Б. Лістинг програми

```
import numpy as np
import matplotlib.pyplot as plt
from sklearn.ensemble import IsolationForest
normal_data = np.sin(np.linspace(0, 10, 1000)) + np.random.normal(0, 0.1, 1000)

anomalous_data = np.sin(np.linspace(0, 10, 1000)) + np.random.normal(0, 1, 1000)
data = np.hstack([normal_data, anomalous_data])
data_reshaped = data.reshape(-1, 1
model = IsolationForest(contamination=0.1

predictions = model.predict(data_reshaped)
plt.figure(figsize=(10, 6))
plt.plot(np.linspace(0, 10, 1000), normal_data, label='Нормальний сигнал', color='blue')
plt.plot(np.linspace(0, 10, 1000), anomalous_data, label='Аномальний сигнал', color='red')

anomalous_points = np.where(predictions == -1)[0]
plt.scatter(anomalous_points / 1000 * 10, data[anomalous_points], color='red', label='Аномалії')

plt.title('Моделювання електромагнітних випромінювань та виявлення аномалій')
plt.xlabel('Час')
plt.ylabel('Амплітуда сигналу')
plt.legend()
plt.show()

print(f"Індекси аномальних точок: {anomalous_points}")
```

Додаток В. Ілюстративний матеріал

Міністерство освіти і науки України
Вінницький національний технічний університет
Факультет менеджменту та інформаційної безпеки
Кафедра менеджменту та безпеки інформаційних систем

Тема: «Вдосконалений метод підвищеної захищеності інформації від витоку каналом побічних електромагнітних випромінювань та наведень на основі контролю панорами електромагнітних випромінювань у приміщенні з використанням засобів штучного інтелекту»

Виконав:
студент 2 курсу, групи КІТС-23М
Цомпель Ю.В.
Керівник: к.ф.м.н., доцент каф.
МБІС
Шиян А.А.

Метою цього дослідження є вдосконалення методу захисту від витоку інформації через побічні електромагнітні випромінювання та перехресні наведення, заснованого на використанні ШІ для моніторингу та аналізу електромагнітного фону об'єкта. Метод автоматизує процес виявлення потенційних загроз, зменшує вплив людського фактору та підвищує рівень інформаційної безпеки в умовах динамічних конфігурацій обладнання.

Об’єкт дослідження: процеси захисту приміщення від витоку даних електромагнітним каналом; процеси аналізу електромагнітного каналу витоку інформації за допомогою ШІ.

Предмет дослідження: методи за засоби захисту інформації від витоку електромагнітним каналом.

Новизна роботи: розробка та застосуванні вдосконаленого методу підвищення захищеності інформації від витоку через канали побічних електромагнітних випромінювань з використанням контролю панорами випромінювань у приміщенні на основі штучного інтелекту.

Практична цінність: розробка вдосконаленого методу підвищення захищеності інформації від витоку через канали побічних електромагнітних випромінювань та наведень. У сучасному світі, де кількість пристроїв, що генерують електромагнітні поля, значно зросла, виникла потреба в нових способах захисту конфіденційної інформації, яка може піддаватися ризику через побічні випромінювання.

Технічні задачі:

- проведення аналізу існуючих методів захисту приміщення від впливу електромагнітних випромінювань за допомогою засобів штучного інтелекту;

-розробка програмного засобу для захисту інформації від витоку побічними електромагнітними каналами;

- вдосконалення методу захисту приміщення засобами протидії витоку інформації.

Порівняльна характеристика пристроїв протидії витоку інформації електромагнітними шляхами

Характеристика	Rohde & Schwarz EMV Test System	Tektronix RSA500A
Частотний діапазон	9 кГц – 40 ГГц	9 кГц – 6,2 ГГц
Чутливість	200 дБм	160 дЦб
Роздільна здатність (RBW)	1 Гц – 10 МГц	1 Гц – 10 МГц
Швидкість сканування	12,5 млн спектрів/сек	12,5 млн спектрів/сек
Екран	10-дюймовий кольоровий сенсорний	7-дюймовий кольоровий сенсорний
Розмір і вага	48 x 32 x 35 см	35 x 26 x 14 см
Температурний діапазон	Робочий: 0 °C до 50 °C	Робочий: 0 °C до 50 °C
Типи сигналів	Wi-Fi, телевізійні, радіо сигнали	Wi-Fi, LTE, 5G, GPS, радіо, ТВ

Характеристика	Rigol DSA800	Keysight N9340B
Частотний діапазон	9 кГц – 3 ГГц	9 кГц – 3 ГГц
Чутливість	160 дБм	160 дБм
Роздільна здатність (RBW)	10 Гц – 3 МГц	1 Гц – 3 МГц
Швидкість сканування	До 9 млн спектрів/сек	До 10 млн спектрів/сек
Екран	8-дюймовий кольоровий TFT LCD	3,5-дюймовий кольоровий
Розмір і вага	41 x 22 x 30 см	40 x 27 x 14 см
Температурний діапазон	Робочий: 5 °C до 45 °C	Робочий: 5 °C до 45 °C
Типи сигналів	Wi-Fi, телевізійні, радіо сигнали	Мобільний зв'язок, Wi-Fi, GPS

Активні методи захисту

Метод захисту	Опис
Встановлення генераторів шуму	Генератори шуму створюють електромагнітні коливання у широкому діапазоні частот, що маскують корисні сигнали, знижуючи можливість їхнього перехоплення. Це ефективно для захисту приміщень, де обробляються секретні дані.
Блокування пристроїв перехоплення	Включає спеціальні блокатори, що придушують роботу перехоплюючого обладнання, блокуючи частоти, на яких працює зловмисне обладнання. Це перешкоджає перехопленню інформації через використання додаткових шумових захисних технологій.
Пошук і нейтралізація закладних пристроїв	Використання скануючих пристроїв (індикаторів поля, частотомірів) для виявлення несанкціонованих джерел випромінювання. Після виявлення ці пристрої ізолюються або видаляються, щоб запобігти витоку інформації.

Пасивні методи захисту

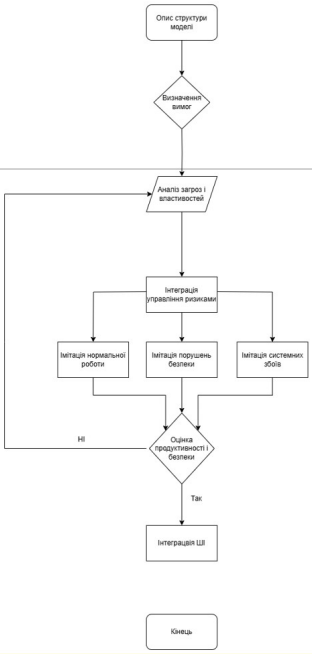
Метод захисту	Опис
Екранування	Використовується для зниження рівня електромагнітного випромінювання в приміщеннях і на обладнанні. Виконується за допомогою металевих сіток або пластин з високоелектропровідних матеріалів (міді, алюмінію, сталі), що відбивають або поглинають сигнали.
Звукоізоляція приміщення	Усуває можливість витоку інформації через електромагнітні хвилі шляхом використання щільних матеріалів, таких як бетон, звукопоглинаючі пінопласти та резонаторні панелі. Це допомагає зменшити проникнення сигналів через стіни, вікна та двері.
Ізоляція кабелів і комунікацій	Включає в себе використання діелектричних вставок у кабелях для зниження провідності та блокування електромагнітних хвиль. Також використовуються ізоляційні матеріали для обмотки кабелів, щоб запобігти поширенню сигналів через мережі живлення.

Методи застосування штучного інтелекту

Метод застосування ШІ	Опис
Машинне навчання та аналіз аномалій	Інтеграція машинного навчання для аналітики даних і виявлення аномалій у системах. Алгоритми здатні аналізувати великі обсяги даних, виявляючи відхилення, що дозволяє вчасно виявляти вторгнення, спроби несанкціонованого доступу або кібератаки
Глибинне навчання для захисту від шкідливих програм	Використання нейронних мереж, таких як CNN або RNN, для розпізнавання шкідливого програмного забезпечення (віруси, трояни, руткіти). Глибинне навчання дозволяє виявляти нові зразки шкідливих програм, ще до їх потрапляння до антивірусних баз.
Захист від витоків інформації через мережу	Використання нейронних мереж для аналізу мережевого трафіку і виявлення спроб несанкціонованого витоку інформації. ШІ здатен блокувати підозрілі спроби доступу та передбачати загрози на основі попереднього досвіду.
Автоматизація реагування на інциденти та нейтралізація загроз	Завдяки ШІ можна автоматизувати реагування на загрози, що дозволяє швидко виявляти і нейтралізувати загрози, зменшуючи шкоду від інцидентів. Ці системи можуть самостійно блокувати підозрілі процеси або припиняти шкідливу активність.
Шифрування та захист даних з використанням ШІ	ШІ може автоматизувати процеси шифрування та дешифрування даних, а також оптимізувати алгоритми шифрування для підвищення ефективності захисту даних у умовах постійних кіберзагроз.
Захист від фішингу та соціальної інженерії	Алгоритми ШІ аналізують електронні листи, повідомлення та інші форми комунікацій для виявлення підозрілих шаблонів або зловмисних посилань, автоматично блокуючи небезпечні повідомлення.
Роботизація процесів моніторингу безпеки та виявлення загроз	Використання роботизованих систем з елементами ШІ для безперервного моніторингу та виявлення загроз в інформаційних мережах. Автоматизація дозволяє зменшити навантаження на фахівців і прискорити процес реагування на загрози.

Компоненти моделі системи безпеки

Алгоритм вдосконалення методу підвищення захищеності інформації від витоку каналом побічних електромагнітних випромінювань



Реалізація модулів захисту та зчитування інформації

1. Мета реалізації:
   - Створення модулів, здатних ефективно захищати інформацію та здійснювати зчитування даних в умовах реального середовища.

2. Основні компоненти модулів:
   - Захист від побічних електромагнітних випромінювань.
   - Алгоритми обробки сигналів для визначення аномалій.
   - Зчитування параметрів електромагнітного поля для аналізу ризиків.

3. Інтеграція ШІ:
   - Автоматизація процесів захисту та аналізу даних.
   - Використання алгоритмів машинного навчання для підвищення точності виявлення загроз.

4. Результати реалізації:
   - Покращена ефективність роботи системи захисту.
   - Гнучкість у масштабуванні та адаптації до нових загроз.

Результати тестування розробленої системи

Тест №	Опис	Частота (МГц)	Інтенсивність (дБм)	Дистанція (м)	Аномалія	Витік	Результат
1	Нормальний сигнал	500	-40	10	Відсутня	Низька ймовірність (10%)	Нормальний
2	Висока ймовірність витоку	2400	-25	15	Виявлена	Висока ймовірність (80%)	Аномальний
3	Слабкий сигнал, потенційно безпечний	1000	-55	20	Відсутня	Дуже низька ймовірність (1%)	Нормальний
4	Нестабільний сигнал із високим ризиком	1800	-30	2	Виявлена	Висока ймовірність (65%)	Аномальний

Економічна ефективність системи визначається через співвідношення економії від впровадження та витрат на її впровадження. Вхідні дані:

Вхідні дані:
Погнозовані втрати без системи: 500 000 грн/рік.
Втрати з системою: 350 000 грн/рік.
Тривалість використання (Т): 5 років.
Витрати на обладнання: 206 500 грн.
Витрати на ПЗ: 3300 грн .
Навчання персоналу: 20 000 грн.
Обслуговування (щорічно): 10 000 грн.

$В_з$ = (500 000 – 350 000) * 5 = 150 000 * 5 = 750 000
$В_в$ = 206 500 + 3300 + 20 000 +10 000 * 5 = 279 800
ЕЕ = (750 000 – 279 800)/279 800 * 100% = 168.04%

Впровадження системи протидії витокам інформації з використанням ШІ дозволяє уникнути втрат на суму 750 000 грн за 5 років.

Економічна ефективність становить 168,04%, що свідчить про високу доцільність інвестицій у розробку та впровадження такої системи.
Це підтверджує доцільність використання системи для захисту конфіденційної інформації в умовах сучасних кіберзагроз.

У ході виконання магістерської роботи було розроблено та обґрунтовано вдосконалений метод захисту інформації від витоку через побічні електромагнітні випромінювання та наведення. Основою методу є використання штучного інтелекту для моніторингу електромагнітного фону у приміщенні, що дозволяє значно підвищити рівень інформаційної безпеки в умовах зростаючих загроз сучасного кіберпростору.

Вдосконалений метод може бути використаний у державних установах, фінансових організаціях, промислових підприємствах та інших об’єктах, що потребують підвищеного рівня безпеки. Застосування системи дозволяє значно знизити втрати від витоку інформації та оптимізувати витрати на забезпечення інформаційної безпеки.

Дякую за увагу!

Додаток Г. Протокол перевірки навчальної роботи

Додаток Г. Протокол перевірки навчальної роботи

ПРОТОКОЛ ПЕРЕВІРКИ НАВЧАЛЬНОЇ (КВАЛІФІКАЦІЙНОЇ) РОБОТИ

Назва роботи:

Вдосконалений метод підвищеної захищеності інформації від витоку каналом побічних електромагнітних випромінювань та наведень на основі контролю панорами електромагнітних випромінювань у приміщенні з використанням засобів штучного інтелекту

Тип роботи: магістерська кваліфікаційна робота

Підрозділ Кафедра менеджменту на безпеки інформаційних систем

Факультет менеджменту та інформаційної безпеки

Гр. КІТС-23м

Керівник доцент Шиян А.А.

Показники звіту подібності Turnitin	
Оригінальність	98%
Загальна схожість	2%

Аналіз звіту подібності (відмітити потрібне)

- ☐ Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.
- ☐ Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її автора. Роботу направити на доопрацювання.
- ☐ Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Заявляю, що ознайомлений (-на) з повним звітом подібності, який був згенерований Системою щодо роботи (додається)

Автор _____ Цомцель Ю.В.
(підпис) (прізвище, ініціали)

Опис прийнятого рішення

Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату

Особа, відповідальна за перевірку _____ Коваль Н.П.
(підпис) (прізвище, ініціали)

Експерт _____ _____
(за потреби) (підпис) (прізвище, ініціали, посада)