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

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

Вдосконалення процесу оцінювання вразливості інформаційної безпеки засобами штучного інтелекту

Виконав: студент 2-го курсу, гр. 1КІТС-22м
спеціальності 125 – Кібербезпека
Освітня програма – Кібербезпека інформаційних технологій та систем
Смоляк І.А.

Керівник: к.т.н., проф., проф. каф. МБІС
Азарова А.О.
«04» грудня 2023 р.

Опонент: к.т.н., доцент, доцент каф. ОТ
Савицька Л. А.
«04» грудня 2023 р.

Допущено до захисту

Голова секції УБ кафедри МБІС
Юрій Яремчук
«04» грудня 2023 р.

Вінниця ВНТУ – 2023

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

Рівень вищої освіти ІІ-й (магістерський)
Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека
Освітньо-професійна програма - Кібербезпека інформаційних технологій та систем

ЗАТВЕРДЖУЮ
Голова секції УБ, кафедра МБІС
_____ Юрій ЯРЕМЧУК
«20» вересня 2023 р.

З А В Д А Н Н Я
на магістерську кваліфікаційну роботу студенту

Смоляку Ігорю Анатолійовичу

1. Тема роботи: **Вдосконалення процесу оцінювання вразливості інформаційної безпеки засобами штучного інтелекту**
Керівник роботи: **Азарова Анжеліка Олексіївна, к.т.н., проф., проф. каф. МБІС**
затверджені наказом вищого навчального закладу від “18” вересня 2023 року № 247
2. Строк подання студентом роботи: за тиждень до захисту магістерської роботи.
3. Вихідні дані до роботи: нормативно-правова база, монографії, підручники, наукові статті, публікації, інтернет-ресурси, стандарти, актуальне програмне забезпечення.
4. Зміст текстової частини: в першому розділі дослідити актуальність предметної області, розглянути особливості вразливостей інформаційної безпеки та оцінювання вразливості інформаційної безпеки; в другому розділі запропонувати модель процесу оцінювання вразливості рівня інформаційної безпеки за допомогою нейронної мережі Хеммінга як засобу штучного інтелекту; в третьому розділі виконати розробку програмну засобу та провести аналіз результатів; в четвертому розділі проаналізувати економічну ефективність розробленого програмного засобу.

5. Перелік ілюстративного матеріалу (з точним зазначенням обов`язкових креслень):
В першому розділі наведено рис. 1, табл. 1;

В другому розділі наведено рис.1, табл. 6;
В третьому розділі наведено рис. 6;
В четвертому розділі наведено табл. 8;

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Основна частина	к.т.н., проф. каф. МБІС Азарова А.О.		
Економічна частина	к.е.н., доц. каф. ЕПВМ Причепа І.В.		

7.Дата видачі завдання 20 вересня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів магістерської кваліфікаційної роботи	Строк виконання етапів роботи		Примітка
1	Визначення напрямку МКР, формулювання теми	20.09.2023	30.10.2023	
2	Аналіз предметної області обраної теми	01.10.2023	11.10.2023	
3	Розробка алгоритму роботи	12.10.2023	23.10.2023	
4	Написання МКР на основі розробленої теми	24.10.2023	12.11.2023	
5	Розробка економічної частини	13.11.2023	20.11.2023	
6	Попередній захист МКР	24.11.2023	25.11.2023	
7	Виправлення, уточнення, коригування роботи	28.11.2023	04.12.2023	
8	Захист МКР	14.12.2023	14.12.2023	

Студент _____ **Смоляк І.**

Керівник роботи _____ **Азарова А.**

АНОТАЦІЯ

УДК: 004.056

Смоляк І.А. Вдосконалення процесу оцінювання вразливості інформаційної безпеки засобами штучного інтелекту. Магістерська кваліфікаційна робота зі спеціальності 125 – «Кібербезпека», освітня програма «Кібербезпека інформаційних технологій та систем». Вінниця: ВНТУ, 2023. 75 с.

Укр. мовою. Бібліогр.: 35 назв; рис.: 8 ; табл. 15.

У магістерській кваліфікаційній роботі представлено математичну модель та метод оцінювання вразливості інформаційної безпеки (далі – ІБ) засобами нейронної мережі Хеммінга як інструменту штучного інтелекту.

У першому розділі роботи здійснено аналіз теоретичного матеріалу обраної галузі знань: досліджено розуміння інформаційної безпеки та існуючих вразливостей, а також проаналізовано різні методи їх оцінювання.

У другому розділі роботи розроблено математичну модель та метод оцінювання вразливості інформаційної безпеки із використанням нейронної мережі Хеммінга.

У третьому розділі роботи здійснено комп’ютерну реалізацію математичної моделі оцінювання вразливості інформаційної безпеки та проведено тестування програмного застосунку і наведено ілюстрацію його роботи.

У четвертому розділі роботи доведено економічну доцільність розробленого програмного засобу, що свідчить про її комерційний потенціал та потребу подальшого впровадження.

Ключові слова: вразливості інформаційної безпеки, штучний інтелект, нейронна мережа Хеммінга.

ABSTRACT

Igor Smolyak. Improvement of the information security vulnerability assessment process by means of artificial intelligence. Master's thesis in specialty 125 – «Cyber Security», Education Program « Cybersecurity of information technology and systems». Vinnitsa: VNTU, 2023. – 75 p.

In Ukrainian language. Bibliographer: 35 titles; fig.: 8; tabl. 15.

The master's thesis presents a mathematical model and a method of for assessing the vulnerability of the level of information security by means of artificial intelligence.

In the first section of the work, an analysis of the theoretical material of the chosen field of knowledge was carried out: the understanding of information security and existing vulnerabilities was investigated, as well as various methods of their assessment were analyzed.

In the second part of the work, a mathematical model and a method of assessing information security vulnerabilities by means of Hamming neural network has been developed.

In the third section of the work, computer implementation of a mathematical model for assessing information security vulnerability has been completed and its testing has been carried out accompanied by an illustration of its operation.

The fourth chapter of the work proves the economic feasibility of the developed software, which indicates its commercial potential and the need for further implementation.

Key words: information security’s vulnerabilities, artificial intelligence, neural network of Hemming.

ЗМІСТ

ВСТУП

Актуальність. Інформаційна безпека є важливою частиною сучасного світу, де захист даних та інформації має критичне значення. Вона містить заходи для забезпечення конфіденційності, доступності та цілісності інформації. Інформаційна безпека визначає багато видів загроз та має в арсеналі численні методи захисту, які залежать від сфери застосування, властивостей інформації, принципів забезпечення безпеки, законодавчих вимог та інших чинників.

Стан інформаційної безпеки визначається захищеністю системи оброблення й зберігання даних, за якого забезпечено конфіденційність, доступність і цілісність інформації або комплексом заходів, спрямованих на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення [1].

Однією з ключових характеристик інформаційної безпеки є наявність вразливостей такої безпеки. Вразливість інформаційної безпеки є слабким місцем в інформаційній системі, яке може бути використане різними особами (зловмисниками) для атаки, крадіжки або компрометації даних. Вразливості можуть бути пов’язані з апаратним забезпеченням, програмним забезпеченням, мережею, персоналом, сайтом або організацією. Для усунення вразливостей необхідно проводити регулярні перевірки, виявляти та мінімізувати ризики, застосовуючи моніторинг стану системи та відповідні заходи безпеки.

Підхід, заснований на аналізі інформаційних ризиків, є найбільш значним для практики створення інформаційної безпеки. Для того, щоб зберегти конкурентоспроможність різних суб’єктів, необхідно впроваджувати економічно обґрунтовані заходи захисту цінних інформаційних активів. На стан інформаційної безпеки впливають такі чинники, як постійне збільшення кількості електронних злочинів, жорсткі й часто змінювані вимоги з боку держави та регуляторів, посилення залежності бізнесу від безперебійної роботи інформаційної системи [2].

Для належного реагування на вразливості інформаційної безпеки потрібно правильно оцінювати вказані ризики, тобто виявляти слабкі місця в інформаційних системах, які можуть бути використані зловмисниками для атаки, крадіжки або компрометації даних. Цей процес допомагає оцінити рівень ризику та вживати заходів для підвищення рівня безпеки.

Сьогодні існує великий теоретичний доробок, який уможливлює реалізацію процесів захисту інформації. Серед таких дослідників пошуку вразливостей інформаційної безпеки та захисту інформації треба відзначити таких закордонних Альгарті А., Джешке С., Каббас А., Мунші А., а також вітчизняних Архіпов О. Є., Вознюк Є. В., Карпінець В. В., Ромака В. А., Яремчук Ю. Є. дослідників та ін. [1-6].

Незважаючи на те, що є значний теоретичний та практичний доробок в досліджуваній галузі знань, слід відзначити що не всі питання ретельно висвітлено в науковій літературі, зокрема недостатньо обґрунтовано множину тих вразливостей, яка б відповідала критеріям повноти, мінімальності і дієвості щоб дозволило якісно оцінювати потужну множину можливих вразливостей, а отже розробляти ефективні засоби боротьби з ними. Що і зумовлює актуальність подальших досліджень.

Одним із інструментів для здійснення діяльності в сфері інформаційної безпеки є використання штучного інтелекту (далі – ШІ). Використання штучного інтелекту в інформаційній безпеці приводить до значного підвищення ефективності захисту від кіберзагроз завдяки автоматизації процесів виявлення, аналізу та реагування на потенційні загрози. ШІ дозволяє оперативно виявляти аномалії у мережевому трафіку та активації, розпізнавати нові види кібератак, ідентифікувати зразки шкідливого коду та здійснювати аналіз лог-файлів. Усі ці процеси відбуваються в режимі реального часу, допомагаючи зменшити час реакції на загрози, а також скорочує необхідність постійного нагляду від людей. Такий підхід сприяє покращенню загального рівня безпеки інформаційних систем та даних, запобігає атакам та мінімізує можливі збитки внаслідок

кіберінцидентів [4].

Отже, актуальним є застосування апарату ШІ для оцінювання рівня вразливості інформаційної безпеки.

Мета і задачі дослідження. Метою роботи є вдосконалення процесу оцінювання вразливості інформаційної безпеки із застосуванням інструментів штучного інтелекту.

Для досягнення такої мети було поставлено та вирішено такі задачі:

– проаналізовано існуючі інструменти оцінювання вразливості інформаційної безпеки;

– запропоновано структурну та математичну модель процесу оцінювання вразливості ІБ;

– удосконалено математичний метод оцінювання вразливості інформаційної безпеки за допомогою нейронної мережі Хеммінга;

– на базі складеного підходу запропоновано алгоритм роботи відповідного програмного засобу;

– протестовано роботу ПЗ та проаналізовано отримані результати;

– обґрунтовано економічну доцільність впровадження запропонованої розробки.

Об’єкт дослідження – процес оцінювання вразливості інформаційної безпеки засобами штучного інтелекту.

Предмет дослідження – удосконалення процесу оцінювання вразливості інформаційної безпеки засобами нейронної мережі Хеммінга.

Наукова новизна: удосконалено метод оцінювання вразливості інформаційної безпеки, що, на відміну від існуючих підходів, дозволяє засобами нейронної мережі Хеммінга підвищити ефективність такого процесу.

Практична цінність: розроблено програмний засіб для оцінювання вразливості інформаційної безпеки засобами нейронної мережі Хеммінга.

Публікації. По темі дослідження було опубліковано тези доповідей [7].

Апробація. Результати дослідження було апробовано на Міжнародній

науково-практичній конференції «Молодь в науці: дослідження, проблеми, перспективи» (м. Вінниця, 2023).

1 ЗАГАЛЬНИЙ АНАЛІЗ ВРАЗЛИВОСТЕЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Роль та значення оцінювання вразливостей інформаційної безпеки

Оцінювання вразливостей інформаційної безпеки є надзвичайно важливим у сучасному цифровому світі, де інформаційні технології впроваджуються в різних сферах життя, і кіберзагрози стають необхідністю для багатьох організацій та індивідів. Зростання кіберзагроз та їхньої складності вимагає постійного аналізу вразливостей для виявлення нових загроз та забезпечення відповідного захисту. Розвиток інформаційних технологій в різних галузях суспільства створює нові можливості для атак і збільшує потенційний обсяг вразливостей, які потрібно вивчати та зменшувати. Захист даних та інформаційних ресурсів стає ключовим завданням в умовах зростання важливості цих активів та зменшення терпимості до втрати конфіденційності та цілісності інформації. У цьому контексті аналіз вразливостей є незамінним інструментом для підвищення рівня безпеки інформаційних систем і даних.

Збільшення важливості даних та інформації створює необхідність для їх ефективного захисту від загроз, що можуть включати в себе втрату даних, крадіжку особистої інформації, фінансові шахрайства та інші форми кіберзлочинності [8].

Вимоги відповідності та регулювання стають більш жорсткими і вимагають від організацій дотримуватися стандартів та нормативів щодо інформаційної безпеки. Аналіз вразливостей є ключовою складовою процесу дотримання цих вимог.

Зменшення ризику є важливою частиною аналізу вразливостей, оскільки цей процес допомагає ідентифікувати потенційні загрози та вжити відповідних заходів безпеки для їх запобігання [9].

Вразливість інформаційної безпеки є комплексною категорією, яка потребує певного виміру та обліку, саме таким чином потрібно здійснювати оцінювання вразливості інформаційної безпеки. Тому оцінювання вразливості інформаційної безпеки можна вважати систематичний та структурований процес, який включає в себе ідентифікацію, аналіз та оцінювання потенційних слабких місць та ризиків в інформаційних системах та мережах. В рамках цього процесу проводяться докладні перевірки програмного забезпечення, мережевої архітектури, налаштувань систем та політик безпеки з метою виявлення потенційних загроз та визначення їх наслідків для безпеки та конфіденційності даних. Ця діяльність включає в себе аналіз ризиків та ймовірності їх виникнення, призначення пріоритетів щодо виправлення або захисту вразливості, а також розробку стратегій та планів для запобігання можливим кіберзагрозам. Важливою частиною процесу є постійний моніторинг та оновлення інформації про вразливості, щоб забезпечити актуальний та надійний захист інформаційних активів та зменшити ризик виникнення кіберінцидентів.

1.2 Аналіз вразливостей інформаційної безпеки

Інформаційна безпека (ІБ) – це комплекс заходів, політик, процедур та технічних рішень, які спрямовані на забезпечення захисту інформації та інформаційних ресурсів від різних загроз і ризиків. Ця область займається збереженням конфіденційності, цілісності та доступності інформації. Різноманітні види інформації, такі як корпоративні дані, особиста інформація, фінансові дані, медичні записи і багато інших, потребують захисту від несанкціонованого доступу, втрати або порушення.

Інформаційну безпеку також розглядають як стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, використання й розвиток в інтересах

громадян або комплекс заходів, спрямованих на забезпечення захищеності інформації особи, суспільства і держави від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки запису чи знищення [10].

Загальний аналіз вразливостей інформаційної безпеки є критичним компонентом процесу забезпечення захисту від кіберзагроз і визначається шляхом ідентифікації, оцінювання та управління потенційними слабкими місцями в інформаційних системах та процесах. Виявлення вразливостей становить перший крок, де проводиться детальний аналіз програмного забезпечення, мереж, апаратних засобів, процесів та політик безпеки. Цей процес може включати в себе виявлення відомих сценаріїв атак або найновіших слабких місць, що виникають унаслідок змін у системі [11].

Після виявлення вразливостей проводиться їх оцінювання, включаючи серйозність та потенційні наслідки. Цей етап допомагає визначити, наскільки вразливості можуть бути використані зловмисниками та як вони можуть впливати на конфіденційність, цілісність та доступність даних та ресурсів.

На основі результатів аналізу вразливостей, власник інформаційної системи приймає рішення щодо того, які кроки потрібно вжити для зменшення ризику. Вказане може включати встановлення заходів безпеки, розробку плану відновлення в разі інциденту, або перегляд політик і процедур безпеки.

Управління ризиками є ключовою частиною аналізу вразливостей, і воно передбачає розробку та впровадження стратегій управління ризиками, моніторинг та оновлення заходів безпеки для забезпечення ефективного захисту інформаційних систем та даних. Загальний аналіз вразливостей допомагає організаціям підвищити безпеку та зменшити ризики, пов'язані з кіберзагрозами, тим самим забезпечуючи захист важливих ресурсів і інформації. Технології штучного інтелекту відкривають нові перспективи для розвитку сучасних засобів захисту інформації. Внаслідок останніх тенденцій в галузі діджиталізації аналітики інформаційної безпеки відзначають неухильне зростання як обсягу,

так і складності даних, які генеруються в інформаційному просторі [12].

Відповіддю на сучасні виклики, які стосуються ускладненню інформаційної безпеки, стало ухвалення міжнародних стандартів, які регулюють відносини в сфері інформаційної безпеки. Нижче наведені деякі з найбільш важливих міжнародних стандартів інформаційної безпеки:

1. ISO 27001: ISO/IEC 27001 – це міжнародний стандарт для систем управління інформаційною безпекою. Він надає рамки для встановлення, впровадження, управління та покращення системи управління інформаційною безпекою в організаціях. Відповідність цьому стандарту допомагає забезпечити належний рівень інформаційної безпеки.

2. ISO 27002: ISO/IEC 27002 – це документ, який надає рекомендації з реалізації конкретних заходів безпеки відповідно до ISO 27001. Він містить конкретні керівництва та вказівки щодо захисту інформації та систем.

3. ISO 22301: ISO 22301 визначає вимоги для систем управління неперервністю бізнесу. Цей стандарт допомагає організаціям готуватися до відновлення бізнес-процесів в разі кризи або надзвичайної ситуації.

4. NIST SP 800 серія: Специфікації, рекомендації та керівництва, розроблені Національним інститутом стандартів і технологій (NIST) США, що включають NIST SP 800-53 (стандарт контролю та управління інформаційною безпекою) та інші документи, які надають рамки та вказівки щодо безпеки інформації та кібербезпеки.

5. GDPR: Загальний регламент з захисту даних (General Data Protection Regulation) ЄС – це нормативний акт, що визначає правила для збору, обробки та збереження особистих даних громадян ЄС. Він має значний вплив на захист особистих даних та вимагає від організацій відповідати високим стандартам інформаційної безпеки.

6. HIPAA: Закон про портативність та відповідальність в галузі охорони здоров'я (Health Insurance Portability and Accountability Act) США – встановлює вимоги до збереження та передачі медичної інформації.

7. PCI DSS: Стандарт безпеки даних сектору платіжних карт (Payment Card Industry Data Security Standard) – це набір вимог для організацій, що обробляють платіжну інформацію, з метою забезпечення її безпеки.

8. COBIT: Контрольна область для інформаційних технологій (Control Objectives for Information and Related Technologies) – це фреймворк для управління та контролю IT-систем та послуг.

ITIL: Бібліотека інфраструктурних послуг (Information Technology Infrastructure Library) - набір практик для управління та обслуговування IT-систем [13].

Важливі аспекти інформаційної безпеки включають наступні елементи:

1. Конфіденційність: Ця характеристика інформаційної безпеки означає, що лише вповноважені особи мають доступ до конфіденційної інформації. Заходи, такі як шифрування та контроль доступу, допомагають забезпечити конфіденційність інформації.

2. Цілісність: Ця характеристика гарантує, що інформація не була змінена або пошкоджена без належних дозволів. Цілісність досягається через контроль змін в інформації та виявлення будь-яких незаконних змін.

3. Доступність: Інформація повинна бути доступною для користувачів, які мають до неї легальний доступ, в будь-який час, коли вони її потребують. Заходи для забезпечення доступності включають в себе резервне копіювання даних та плани відновлення після аварій.

4. Аутентифікація і авторизація: Ці поняття відповідають за перевірку ідентичності користувачів і надання їм відповідних дозволів. Аутентифікація визначає, хто користувач, а авторизація визначає, що користувач має право робити.

5. Моніторинг і виявлення загроз: Цей аспект включає постійний контроль і аналіз інформаційної системи для виявлення незвичайних або підозрілих активностей, що можуть свідчити про потенційні загрози [14].

Також під загрозами інформаційної безпеки розуміється можливість

порушення таких властивостей інформації як конфіденційність, цілісність та доступність. Інформаційні системи складаються з трьох основних частин: апаратного забезпечення, програмного забезпечення та засобів зв'язку з метою ідентифікації та застосування стандартів індустрії інформаційної безпеки як механізмів захисту та запобігання на трьох рівнях або шарах: фізичному, особистісному та організаційному. Основна ідея полягає в тому, що процедури або політики впроваджуються для того, щоб повідомляти адміністраторам, користувачам та операторам, як використовувати продукти для забезпечення інформаційної безпеки в організаціях [15]. Баланс атрибутів показаний у рис. 1.1.

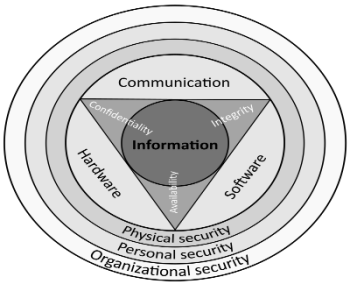


Рисунок 1.1 – Атрибути інформаційної безпеки [15]

Вразливість інформаційної безпеки – це властивість інформаційної системи або програмного забезпечення, яка створює потенційну можливість для атаки або порушення її безпеки. Вразливості можуть виникати внаслідок помилок у програмному коді, недоліків в проектуванні системи, слабкостей в реалізації криптографічних алгоритмів, підозрілих конфігурацій, незадовільних мережевих налаштувань та інших технічних причин [16].

Вразливості можна класифікувати за різними технічними ознаками:

1. Вразливості в програмному забезпеченні. Вразливість в програмному забезпеченні – це слабкість або помилка в програмному коді, яка може бути використана зловмисниками для виконання несанкціонованих дій або доступу до системи, даних або ресурсів. Вразливості можуть виникати з різних причин, включаючи недоліки в проектуванні, помилки програмування, недостатню перевірку вхідних даних або неправильну конфігурацію. Нижче знаходяться

типи вразливостей в програмному забезпеченні:

- SQL-ін'єкція (SQL Injection);
- буферний переповнення (Buffer Overflow);
- уразливості Cross-Site Scripting (XSS);
- уразливості Cross-Site Request Forgery (CSRF);
- уразливості у обробці вхідних даних;
- вразливості у валідації та автентифікації.

2. Вразливості мережі. Вразливість мережі - це слабкість або помилка в компонентах мережі, яка може бути використана зловмисниками для отримання несанкціонованого доступу до мережі, даних або ресурсів, а також для виконання атак або завдання шкоди мережевому середовищу. Вразливості мережі можуть виникати з різних причин, включаючи недоліки в конфігурації, помилки проектування, відсутність необхідних заходів безпеки та патчів:

- отруєння ARP-кешу (ARP Cache Poisoning);
- атаки «людина посередині» (Man-in-the-Middle Attacks);
- атаки (отруєння) DNS (DNS Poisoning).
- вразливості в мережевому протоколі (наприклад, ICMP, SNMP)

3. Фізичні вразливості. Фізичні вразливості в інформаційній безпеці відносяться до тих аспектів, які стосуються фізичного доступу до обладнання, інфраструктури та ресурсів. Зловмисники можуть використовувати фізичний доступ для здійснення несанкціонованих дій або завдання шкоди. Ось деякі загальні типи фізичних вразливостей:

- викрадення пристроїв;
- фізичний доступ до серверних приміщень;
- вразливості у біометричних системах.

4. Соціальні вразливості. Соціальні вразливості в інформаційній безпеці виникають через вплив людей та соціокультурних аспектів, які можуть бути використані зловмисниками для отримання доступу до інформації, систем або ресурсів. Ці вразливості часто стосуються маніпуляції або обману людей, а

не технічних аспектів. Ось деякі загальні типи соціальних вразливостей:

- фішинг (Phishing);
- соціальний інженеринг (Social Engineering);
- втрата чутливої інформації через недбалість користувачів.

5. Вразливості управління доступом. Вразливості управління доступом в інформаційній безпеці виникають, коли не забезпечується належний контроль та обмеження доступу до ресурсів, систем або інформації в організації. Неправильне управління доступом може призвести до надмірного доступу, несанкціонованого доступу, а також інших загроз для безпеки даних та інформації. Ось деякі загальні види вразливостей управління доступом:

- недоліки в системах управління ідентифікацією та авторизацією;
- несанкціонований доступ до приміщень та обладнання.

6. Вразливості в додатках. Вразливості в додатках включають в себе слабкості та помилки в програмному коді, які можуть бути використані зловмисниками для атак або отримання несанкціонованого доступу до додатків або системи цілісності інформації. Ось деякі типові вразливості в додатках:

- вразливості в веб-додатках (наприклад, управління сесіями, внесення даних);
- вразливості в мобільних додатках.

7. Вразливості в системах шифрування. Вразливості в системах шифрування пов'язані з слабкостями або помилками в процесі шифрування та дешифрування даних, які можуть призвести до витоку конфіденційної інформації або невдачі у збереженні безпеки даних. Ось деякі загальні вразливості, що можуть виникати в системах шифрування:

- слабкість алгоритмів шифрування;
- недоліки в реалізації шифрування.

8. Вразливості в бізнес-процесах. Вразливості в бізнес-процесах включають в себе потенційні слабкі місця, де можуть виникнути помилки, недоліки або атаки, що можуть негативно вплинути на ефективність та безпеку

операцій організації. Вони можуть виникати як через технічні проблеми, так і через людські фактори. Ось деякі типові вразливості в бізнес-процесах:

- несправжня політика безпеки;
- недоліки в управлінні ризиками;
- внутрішні загрози та витік даних [17].

Завдяки аналізу різноманітних типів вразливостей інформаційної безпеки, важливо реалізувати високий рівень генерації і вибору варіантів стратегій безпеки та проактивної захисту. Технічні вразливості, такі як недоліки в програмному забезпеченні, архітектурні слабкості та ризики в мережевих протоколах, вимагають безперервного оцінювання та виправлення. Визначення та оцінювання критичності вразливостей за допомогою останніх методів сканування та аналізу дозволяє підвищити ефективність стратегій управління ризиками. Крім того, використання стандартів та протоколів інформаційної безпеки, таких як ISO 27001 і NIST SP 800-53, допомагає створити консолідовані та консистентні підходи до захисту інформації в середовищі, що надзвичайно вразливе до загроз.

1.3 Аналіз методів оцінювання вразливості інформаційної безпеки

Аналіз алгоритмів оцінювання вразливості інформаційної безпеки є ключовим етапом у забезпеченні надійного та ефективного захисту цифрових ресурсів. В умовах постійного розвитку кіберзагроз та змін у технологічному середовищі, виявлення та аналіз потенційних вразливостей стає необхідністю для організацій будь-якої розмірності та сфери діяльності. Алгоритми оцінювання вразливості можуть варіювати від сканування вразливості мережі та програмного забезпечення до тестування на проникнення та аналізу програмного коду. Вони допомагають ідентифікувати слабкі місця, які можуть бути використані зловмисниками для атак, та забезпечують основу для розробки

стратегій управління ризиками та захисту. В цьому контексті важливо розглянути різні алгоритми та їхню ефективність для різних сценаріїв оцінювання вразливості інформаційної безпеки.

Сьогодні в світі кібербезпеки існує декілька міжнародних методологій оцінювання вразливості інформаційної безпеки. Нижче знаходяться найбільш авторитетні та значимі із них:

Управління ризиками в системі інформаційних технологій –методологія оцінювання ризиків SP800-30 (Special Publications) Національного Інституту Стандартів і Технологій (National Institute of Standards and Technology –NIST) - NIST SP800-30. Методологія NIST SP800-30 детально описує всі можливі ризики для інформаційних активів і може використовуватися для підприємств різної величини. 101No 2(10), 2020ISSN 2663-4023Недоліком цієї методології є довготривалий процес аналізу і відсутність автоматизації деяких функцій.

Аналіз і управління ризиками – метод, розроблений Центральним комп'ютерним і телекомунікаційним агентством (Велика Британія) та реалізований у вигляді програмного забезпечення CRAMM (CCTA Risk Analysis and Managment Method). Він передбачає комплексний підхід до оцінювання ризиків, поєднуючи кількісні та якісні оцінювання. Є універсальним і підходить як для великих, так і для малих ІТС й АС, як для державного, так і для комерційного сектора. CRAMM орієнтований на різні типи організацій (установ), що різняться між собою базами знань. Для комерційних організацій застосовують комерційний профіль (Commercial Profile), а для державних – державний профіль (Government profile).

Оцінювання активів та вразливостей інформаційної безпеки – метод OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) розроблено у Сполучених Штатах Америки в Інституті програмної інженерії при Університеті Карнегі–Меллона (Software Engineering Institute і Carnegie Mellon University). Методологія OCTAVE дає змогу розробити практичні методи й рекомендації для оцінювання ризиків. Визначає стратегію оцінювання й

планування дій щодо забезпечення безпеки інформації на основі оцінювання ризиків [18]. Сам процес оцінювання вразливості інформаційної безпеки передбачає наявність відповідних послідовних дій, які дозволяють провести повну характеристику того чи іншого виду вразливості [19]. У табл. 1.1 наведено загальну схему етапів оцінювання вразливості [20].

Таблиця 1.1 – Етапи оцінювання вразливості інформаційної безпеки

Тип оцінювання	**Опис етапу**
1. Визначення цілей та об'єктів оцінювання	Визначення об'єктів, які підлягають оцінюванню, і цілей, що мають бути досягнуто.
2. Збір інформації	Збір інформації про об'єкти оцінювання, включаючи дані про архітектуру, конфігурації, програмне забезпечення і політики безпеки.
3. Ідентифікація вразливості	Виявлення потенційної вразливості в інформаційних системах та мережах.
4. Оцінювання ризику	Оцінювання ризику, пов'язаного з виявленими вразливостями, включаючи визначення ймовірності та наслідків.
5. Планування заходів з безпеки	Розробка плану заходів з безпеки для вирішення виявлених вразливостей.
6. Виконання заходів та тестування	Виконання запланованих заходів з безпеки та тестування їх на практиці.
7. Моніторинг та аналіз	Постійний моніторинг системи на наявність нових вразливостей та аналіз результатів.
8. Повторне оцінювання ризику	Повторна оцінка ризику для переконання в тому, що вразливості було виправлено та ризики зменшено.
9. Документування та звітність	Детальна документація кожного етапу оцінювання та розроблених заходів з безпеки.

Оцінювання вразливості інформаційної безпеки — це складний і багатоетапний процес, спрямований на виявлення потенційних вразливостей та ризиків у інформаційних системах. Представлена таблиця містить основні етапи цього процесу, починаючи від збору інформації про систему і класифікації

активів, і закінчуючи моніторингом та аудитом для виявлення та контролю нових вразливостей. Кожен етап спрямований на систематичне виявлення, аналіз та усунення потенційних загроз, що можуть впливати на безпеку інформаційних систем. Ця структура надає організаціям чіткий план дій для забезпечення найвищого рівня захисту інформації.

Оцінювання ризику полягає у визначенні його рівня (якісної або кількісної величини) і порівнянні цього рівня з максимально допустимим (прийнятним) рівнем, а також з рівнем інших ризиків, при цьому показник рівня ризику визначається шляхом комбінування наступних величин: ймовірності події, а також розмірів його наслідків. Подія полягає в реалізації загрози, що використовує уразливість активу для впливу на цей актив і порушення його безпеки.

Відомі методи оцінювання ризиків можна поділити на:

- методи, що використовують оцінювання ризику на якісному рівні (один із варіантів, за шкалою «високий», «середній», «низький»), прикладом такої методики, зокрема, є FRAP (Facilitated Risk Analysis Process);
- кількісні методи (ризик оцінюється через числове значення, наприклад, розмір очікуваних річних втрат).

Метод FRAP (Facilitated Risk Assessment Process) – це метод оцінювання ризиків в інформаційній безпеці, яка спеціалізується на визначенні вразливостей та потенційних наслідків для організації. Цей метод містить такі ключові кроки:

1. Ідентифікація вразливостей. Визначення можливих слабких місць і вразливостей в інформаційних системах та процесах організації.

2. Оцінювання вразливостей. Визначення серйозності та критичності кожної вразливості на основі факторів, таких як ймовірність використання вразливості та можливий вплив на організацію.

3. Визначення потенційних наслідків. Оцінювання можливих наслідків використання вразливостей, включаючи втрати даних, порушення конфіденційності, доступність та цілісність інформації.

4. Оцінювання ризику. Визначення ризику шляхом поєднання інформації про вразливості та потенційні наслідки. Оцінювання ризику може використовувати числові значення або категорії для класифікації ризику на високому, середньому або низькому рівнях.

5. Розроблення стратегій мінімізації ризиків. Визначення заходів для зменшення ризику, включаючи усунення вразливостей, впровадження технічних заходів безпеки та розробку політик і процедур.

6. Моніторинг та оновлення. Оцінювання ризиків та вразливостей є постійним процесом, який вимагає постійного моніторингу та оновлення оцінок на основі нових загроз та змін в інформаційному середовищі.

FRAP допомагає організаціям систематично оцінювати ризики та вразливості в їхній інформаційній безпеці та приймати обґрунтовані рішення щодо заходів безпеки та ресурсного розподілу для забезпечення найважливіших аспектів безпеки [21].

Кількісні методи оцінювання вразливості інформаційної безпеки базуються на використанні числових значень або метрик для визначення серйозності вразливостей та ризику, зокрема:

1. CVSS (Common Vulnerability Scoring System). CVSS надає числовий бал для визначення серйозності вразливостей. Ця система враховує такі фактори, як доступність експлойту, рівень привілеїв та інші параметри.

2. Дохідно-витратна аналітика (ROI). Цей метод включає в себе розрахунок та порівняння доходів, які можуть бути втрачені внаслідок використання вразливостей, та витрат на їх усунення.

3. Числові метрики вразливостей. Визначення конкретних числових значень, які оцінюють вартість або збитки, пов'язані з вразливістю, такі як втрата прибутку, шкода для репутації тощо.

4. Термін відновлення (Recovery Time Objective – RTO). Розрахунок часу, необхідного для відновлення системи після використання вразливості. Чим вищий RTO, тим більший може бути втрати.

5. Термін служби (Mean Time Between Failures – MTBF). Розрахунок середнього часу між виявленням вразливостей чи відмов системи, що дозволяє оцінити частоту виникнення проблем.

6. Метод Quantitative Information Risk Management (QIRM). Використовується для чисельного оцінювання ризику на основі фінансових даних та статистики.

7. Метод FMEA (Failure Modes and Effects Analysis). Використовується для визначення можливих вразливостей та їхніх можливих наслідків, при цьому кожному з них надається числовий бал.

Ці кількісні методики дозволяють оцінити ризик та серйозність вразливостей з точки зору числових значень, що спрощує процес прийняття рішень щодо заходів забезпечення інформаційної безпеки. Вони можуть бути корисними для планування бюджету безпеки та прийняття обґрунтованих рішень про вкладення ресурсів [22].

Проаналізуємо недоліки і переваги якісних та кількісних методів оцінювання вразливості інформаційної безпеки.

FRAP (Facilitated Risk Analysis Process). Використання якісної оцінювання ризику на основі шкали "високий", "середній", "низький".

Переваги: простота впровадження та розуміння; інтуїтивний підхід, особливо для менеджерів, не зайнятих безпосередньо безпекою.

Недоліки: суб'єктивність оцінок, що може призвести до неоднозначних результатів.

CVSS (Common Vulnerability Scoring System). Надає числові бали для кількісного оцінювання серйозності вразливостей.

Переваги: об'єктивність та точність оцінок; можливість порівняння різних аспектів безпеки.

Недоліки: вимога до точних даних та експертних знань; може не враховувати всі аспекти контексту ризику.

Враховуючи переваги та обмеження обох підходів, організації часто

використовують комбінацію кількісних та якісних методик для отримання комплексного оцінювання ризиків інформаційної безпеки.

Обраний метод управління вразливостями інформаційної безпеки має враховувати бізнесові потреби компанії, її масштаби, а також відповідати кращим світовим практикам і докладно описувати процеси і необхідні дії [23].

1.4 Можливості ШІ в оцінюванні вразливості інформаційної безпеки

Використання штучного інтелекту (ШІ) для підвищення оцінювання вразливості інформаційної безпеки є важливим кроком у захисті цифрових систем та даних в умовах постійно зростаючих кіберзагроз. ШІ відкриває перед нами низку унікальних можливостей, які роблять процес виявлення та оцінювання вразливості більш точним та продуктивним [24].

У першу чергу, ШІ здатний аналізувати великі обсяги даних та системну активність, виявляючи навіть мінімальні аномалії, які можуть свідчити про наявність вразливостей. Він використовує методи навчання з підкріпленням та нейронні мережі для виявлення патернів та аномалій, що залишаються непоміченими для традиційних методів аналізу.

Додатково, ШІ дозволяє автоматизувати оцінювання ризиків, шляхом розробки інтелектуальних алгоритмів, які визначають потенційні наслідки вразливості та визначають їхній пріоритет для подальшого усунення. Це полегшує процес прийняття рішень та допомагає організаціям фокусуватися на найбільш критичних пунктах безпеки.

Окрім цього, використання штучного інтелекту в інформаційній безпеці обумовлено насамперед двома чинниками: необхідністю оперативного реагування під час настання кіберінциденту; нестачею кваліфікованих спеціалістів з кіберзахисту [25].

У цілому, використання ШІ для оцінювання вразливості інформаційної

безпеки робить кібербезпеку більш передбачуваною та надійною, допомагаючи організаціям інтегрувати інтелектуальні інструменти у свої стратегії захисту інформаційних активів.

Використання інструментів штучного інтелекту для оцінювання вразливості інформаційної безпеки є сучасним та надзвичайно важливим аспектом в галузі кібербезпеки. Одним із ключових інструментів штучного інтелекту є нейронні мережі. Нейронні мережі, як ключова складова штучного інтелекту, надають здатність автоматизованого та точного оцінювання вразливості в різних інформаційних системах та мережах. Вони працюють на стику даних, статистики та шаблонів, що дозволяє їм ефективно виявляти потенційні загрози та ризики для безпеки.

Нейронні мережі можуть аналізувати різноманітні аспекти інформаційної безпеки, включаючи програмне забезпечення, мережевий трафік, журнали подій та багато інших. Вони працюють з великими обсягами даних, виявляючи навіть найдрібніші аномалії та вразливості. Основною перевагою їх використання є здатність до автоматизації та аналізу даних в реальному часі, що допомагає реагувати на загрози миттєво та забезпечувати постійний моніторинг інформаційної безпеки.

Використання штучного інтелекту для оцінювання вразливості інформаційної безпеки відкриває нові можливості для більш ефективного та автоматизованого аналізу та виявлення потенційних загроз.

Штучний інтелект може бути використаний для оцінювання вразливості інформаційної безпеки під час:

- Аналізу великих обсягів даних. Штучний інтелектуальний аналіз може автоматизувати оброблення та аналіз великих обсягів інформації, що допомагає виявити вразливості та аномалії в реальному часі. Нейронні мережі та алгоритми машинного навчання можуть аналізувати дані з різних джерел, виявляти аномалії та передбачати можливі загрози.
- Виявлення атак і аномалій: Моделі машинного навчання можуть бути

навчені розпізнавати патерни атак та незвичайну активність в мережі або системі. Це дозволяє автоматично виявляти кіберзагрози та інциденти, включаючи атаки на врозливість.

- Автоматизоване оцінювання коду та додатків: Штучний інтелект може аналізувати програмний код та додатки для виявлення потенційних вразливостей, таких як вразливості у безпеці вводу-виводу, переповнення буфера та інші. Це допомагає розробникам виправляти вразливості перед випуском продукту.

- Управління безпекою в реальному часі: Штучний інтелект може автоматично реагувати на загрози та вразливості в режимі реального часу, виконуючи відповідні заходи безпеки, такі як заборона доступу, блокування атак або автоматичне виправлення вразливостей. Прогнозування ризиків: Аналітика на основі штучного інтелекту допомагає передбачити можливі ризики та атаки, а також оцінювати вплив їх реалізації на інформаційну безпеку [26].

Застосування штучного інтелекту в оцінюванні вразливості інформаційної безпеки сприяє підвищенню ефективності та точності процесу виявлення, аналізу та запобігання кіберзагрозам, дозволяючи реагувати на них швидше та ефективніше [27].

Одним з інструментів штучного інтелекту для оцінювання вразливості інформаційної безпеки є використання нейронних мереж.

Використання нейронних мереж для оцінювання вразливості інформаційної безпеки є дуже потужним інструментом, який може значно полегшити процес виявлення та аналізу можливих загроз та слабких місць в інформаційних системах. Ось кілька способів, які дозволяють використовувати нейронні мережі в цьому контексті:

1. Нейронні мережі можуть бути навчені аналізувати нормальну активність системи і виявляти аномалії, які можуть свідчити про потенційні загрози. Вони розпізнають незвичайні патерни в трафіку, активності користувачів або програмному коді і сигналізують про можливі вразливості або атаки.

2. Нейронні мережі можуть бути використані для аналізу програмного коду з метою виявлення потенційних вразливостей, таких як SQL-ін'єкції, переповнення буфера, або недоліки в безпеці вводу-виводу. Вони можуть автоматично перевіряти код на предмет вразливостей під час розробки та впровадження.

3. Нейронні мережі можуть бути використані для аналізу великих обсягів структурованих та неструктурованих даних для виявлення вразливостей та загроз. Вони можуть автоматично агрегувати, класифікувати та аналізувати дані для виявлення потенційних ризиків.

4. Нейронні мережі можуть бути навчені прогнозувати можливі ризики та наслідки вразливостей на основі історичних даних та актуальних показників безпеки. Це допомагає приймати обгрунтовані рішення щодо заходів безпеки та призначення пріоритетів.

5. Нейронні мережі можуть бути долучені до системи автоматизованого відгуку на кіберінциденти. Вони можуть визначати тип атаки, її походження та наслідки, що допомагає вчасно та ефективно реагувати на інциденти.

Застосування нейронних мереж в оцінці вразливості інформаційної безпеки дозволяє підвищити точність та швидкість виявлення потенційних загроз, що є важливим для забезпечення надійного захисту інформаційних систем та даних [28].

Однією із нейронних мереж, є мережа Хеммінга, яка може бути використана для побудови моделі оцінювання типів вразливостей інформаційної безпеки. Застосування мережі Хеммінга для аналізу вразливості, потребує створення відповідної моделі, яка використовує цю мережу для аналізу даних про вразливості. Така модель може включати в себе обробку та порівняння патернів вразливостей, а також визначення типів вразливостей.

Для оцінювання вразливості інформаційної безпеки існують різні види нейронних мереж, які можуть бути використані. Нижче знаходяться деякі з них:

1. Згорткові нейронні мережі (CNN): Вони ідеально підходять для

оброблення зображень та відео, що може бути корисним при аналізі вразливостей на веб-сайтах або в мережевих камерах.

2. Рекурентні нейронні мережі (RNN): Вони корисні для аналізу послідовних даних, таких як журнали подій, що допомагають виявити аномалії та потенційні атаки.

3. Мережі довгої короткочасної пам'яті (LSTM): Вони використовуються для аналізу послідовних даних та виявлення аномалій у великих наборах логів.

4. Варіаційні автокодери (VAE): Вони допомагають у моделюванні різних аспектів даних та виявленні аномалій в складних системах.

5. Глибокі нейронні мережі (DNN): Вони використовуються для загального аналізу та виявлення вразливостей в різних типах даних.

6. Автокодери: Вони допомагають у зменшенні розмірності даних та виділенні важливих ознак, що можуть вказувати на вразливості.

7. Генеративні зворотні мережі (GAN): Вони використовуються для створення синтетичних даних, які можуть бути використані для аналізу та виявлення вразливостей.

Окремим видом нейронних мереж є Нейронні мережі Хопфілда та Хеммінга. Це дві спеціалізовані моделі нейронних мереж, які можуть бути використані для оцінювання вразливості в інформаційній безпеці.

Мережі Хопфілда є рекурентними нейронними мережами, які використовуються для асоціативного запам'ятовування та відновлення вхідних шаблонів. Вони зазвичай використовуються для розв'язання задачі відновлення даних на основі фрагментів або ключових ознак.

У контексті оцінювання вразливості інформаційної безпеки, нейронні мережі Хопфілда можуть бути використані для виявлення аномалій або патернів у поведінці системи. Вони можуть визначати аномальні ситуації, які можуть бути індикаторами потенційних загроз.

Нейронні мережі Хеммінга базуються на бінарних обчисленнях та зазвичай використовуються для вирішення задач кодування та корекції помилок

в інформаційних системах. Вони можуть допомагати виявити та виправити помилки в передачі даних.

У контексті оцінювання вразливості інформаційної безпеки, нейронні мережі Хеммінга можуть бути використані для перевірки цілісності даних та виявлення можливих атак на системи передачі інформації.

Вибір конкретного типу нейронної мережі залежить від типу даних, які аналізуються, та завдання, яке потрібно вирішити в галузі кібербезпеки. Зазвичай комбінування різних типів нейронних мереж та ансамблів може допомогти досягти більшої ефективності в оцінюванні вразливості [29].

1.5 Висновки та постановка задач

У даному розділі було проведено проаналізовано потенційні вразливості інформаційної безпеки, зокрема, інтенсивність та розмаїтість загроз, які виникають у сучасному інформаційному ландшафті. Незалежно від галузі або розміру, організації постійно стикаються з великою кількістю загроз, які проникають через різні порти, намагаючись використовувати різні вразливості для проникнення та завдання шкоди конфіденційності, доступності та цілісності інформації.

Завдяки впровадженню різних методів оцінювання та класифікації вразливостей, організації можуть здійснити систематичний аналіз ризиків та вразливостей, із метою визначення та вирішення критичних проблем подальшого захисту.

Такі методи, як CVSS, FRAP та кількісні методи оцінювання надають важливі інструменти для обґрунтованого аналізу ризиків та вразливостей, що вдосконалює рішення з питань безпеки.

Важливо визначати та управляти кожним типом вразливості, не залежно від того, чи є це технічна, фізична, соціальна або інша вразливість, оцінювати її

вагомість і розробляти заходи щодо її мінімізації.

Шляхом аналізу можливостей ШІ було доведено його спроможність у оцінюванні вразливості інформаційної безпеки, що є подальшим напрямком досліджень магістерської роботи.

Загальний аналіз вразливості інформаційної безпеки вказує на те, що інформаційна безпека є необхідною складовою будь-якої сучасної організації і вимагає постійного оновлення та удосконалення для відповіді на небезпеки, які постійно зростають. Досягнення високого рівня інформаційної безпеки вимагає спільних зусиль технічних, управлінських та організаційних заходів, а також глибокого розуміння потенційних ризиків та вразливостей у всіх аспектах інформаційних систем.

У результаті проведеного аналізу та, виходячи з мети магістерської роботи, було поставлено такі задачі:

– проаналізувати існуючі інструменти оцінювання вразливості інформаційної безпеки;

– запропонувати структурну та математичну моделі процесу оцінювання вразливості ІБ;

– удосконалити математичний метод оцінювання вразливості інформаційної безпеки за допомогою нейронної мережі Хеммінга;

– на базі складеного підходу запропонувати алгоритм роботи відповідного програмного засобу;

– протестувати роботу ПЗ та проаналізувати отримані результати;

– обґрунтувати економічну доцільність впровадження запропонованої розробки.

Виконання поставлених завдань дозволяє покращити процес вирішено оцінювання вразливості інформаційної безпеки засобами штучного інтелекту.

Подальше дослідження передбачає розроблення та тестування моделі Хеммінга, автоматизацію процесу виявлення вразливості, урахування контексту та сценаріїв атак, інтеграцію з іншими інструментами безпеки, аналіз впливу на

загальну ефективність систем безпеки та створення практичних рекомендацій для застосування отриманих результатів у реальних умовах.

2. ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ОЦІНЮВАННЯ ВРАЗЛИВОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1 Аналіз інструментів штучного інтелекту для оцінювання вразливості інформаційної безпеки

Нейронна мережа Хеммінга є потужним інструментом в арсеналі кібербезпеки для оцінювання та виявлення вразливості інформаційних систем і мереж. Мережа використовує принципи аналізу нормальної поведінки системи та автоматизованого виявлення будь-яких відхилень від цієї норми. Цей підхід виявляється особливо ефективним у вимірюванні безпеки в реальному часі, допомагаючи реагувати на потенційні загрози миттєво.

Нейронні мережи Хеммінга використовують підходи до машинного навчання та аналізу даних для розпізнавання аномалій та вразливостей. Вони навчаються на прикладах нормальної поведінки системи та спроможні виявляти навіть найменші відхилення, що можуть бути індикаторами можливих атак чи порушень безпеки. Це допомагає попереджати атаки та вчасно реагувати на нові загрози.

Окрім цього, нейронні мережи Хеммінга є потужним інструментом для аналізу вразливості інформаційної безпеки, які допомагають підвищити рівень захисту та реагувати на потенційні ризики, забезпечуючи безпеку своїх інформаційних ресурсів.

Вибір нейронної мережі Хеммінга в якості інструменту для автоматизації оцінювання вразливості інформаційної безпеки може бути обґрунтований кількома важливими аспектами:

1. Виявлення помилок та вразливостей. Нейронні мережі Хеммінга зазвичай використовуються для виявлення та виправлення помилок в передачі інформації. Оскільки безпека часто пов'язана з правильністю обробки даних, використання мережі Хеммінга дозволяє виявляти можливі вразливості,

пов'язані з помилковими даними або атаками на цілісність інформації.

2. Здатність до виявлення та виправлення пошкоджень. Нейронні мережі Хеммінга мають вбудовану здатність виявлення та виправлення деяких помилок. Це може бути важливим в контексті виявлення вразливостей, пов'язаних з випадковими чи зловмисними змінами даних.

3. Ефективність для кодування та розпізнавання патернів. Нейронні мережі Хеммінга виявляють ефективність в кодуванні та розпізнаванні патернів. Це дозволяє їм аналізувати дані та ідентифікувати характерні аномалії, що може бути корисним для виявлення вразливостей.

4. Автоматизація та швидкість роботи. Нейронні мережі Хеммінга можуть бути реалізовані у вигляді апаратних або програмних рішень, що дозволяє їх використання для автоматизації процесів оцінювання вразливості. Це може значно збільшити швидкість виявлення та реагування на можливі ризики.

5. Застосування в комбінації з іншими методами. Нейронні мережі Хеммінга можуть бути ефективно використані в комбінації з іншими методами оцінювання вразливості. Вони можуть служити додатковим шаром захисту, сприяючи комплексному підходу до безпеки.

Усі ці чинники роблять нейронні мережі Хеммінга привабливим інструментом для автоматизації оцінювання вразливості інформаційної безпеки, зокрема в контексті виявлення та усунення помилок та аномалій у передачі даних.

Використання нейронної мережі Хеммінга дозволить отримати класифіковані та сегментовані дані як результат здійснення відповідного оцінювання вразливості інформаційної безпеки, що в свою чергу покаже рівень та тенденції вразливості інформаційної безпеки. Нейронна мережа Хеммінга також дозволить виконати співставлення образу вхідних векторів які описують вразливості інформаційної безпеки із найближчим еталонним вектором, що описує певну вразливість інформаційної безпеки [30].

2.2 Розроблення структурної моделі процесу оцінювання вразливості інформаційної безпеки із застосуванням нейронної мережі Хеммінгу

Структурна модель процесу оцінювання вразливості інформаційної безпеки з використанням нейронної мережі Хеммінгу уможливлює процес відображення множини вхідних оцінювальних параметрів впливу на множину вихідних рішень.

Для побудови множини оцінювальних параметрів та вихідного вектору автором магістерської дисертації було обґрунтовано множину оцінювальних параметрів вразливості інформаційної безпеки із застосуванням критеріїв повноти, мінімальності та дієвості.

Отже, розглянемо множину оцінювальних параметрів, які будемо досліджувати у роботі: вразливості автентифікації та авторизації; вразливості захищеності веб-додатків; вразливості керування доступом; вразливості шифрування даних; вразливості мережевої безпеки; вразливості фізичної безпеки; вразливості соціальної інженерії; вразливості системи виявлення та запобігання вторгнень; вразливості втрати даних [31].

Для побудови математичної моделі оцінювання вразливості інформаційної безпеки позначимо множину **A** вхідних оцінювальних параметрів $\mathbf{A} = \{a_i\}$, $i = 1,\ldots n$ та вихідних рішень $\mathbf{B}=\{b_j\}$, $j=1,..,m$. Така модель відображає множину параметрів вразливості інформаційної безпеки a_i на множину $\mathbf{B}=\{b_j\}$ вихідних рішень b_j.

Отже, для отримання показників рівня вразливості інформаційної безпеки необхідно проаналізувати множину $\mathbf{A} = \{a_i\}$, $i = 1,\ldots 9$ вхідних оцінювальних параметрів: вразливості автентифікації та авторизації – a_1; вразливості захищеності веб-додатків – a_2; вразливості керування доступом – a_3; вразливості шифрування даних – a_4; вразливості мережевої безпеки – a_5; вразливості фізичної безпеки – a_6; вразливості соціальної інженерії – a_7; вразливості системи виявлення та запобігання вторгнень – a_8; вразливості втрати даних – a_9.

При цьому, множина вихідних рішень **B** визначається такими рівнями вразливості інформаційної безпеки: b_1 – низький рівень; b_2 – середній рівень; b_3 – високий рівень.

Нижче на Рис.2 знаходиться структурна модель процесу оцінювання вразливості інформаційної безпеки із застосуванням системного підходу та нейронної мережі Хеммінга.

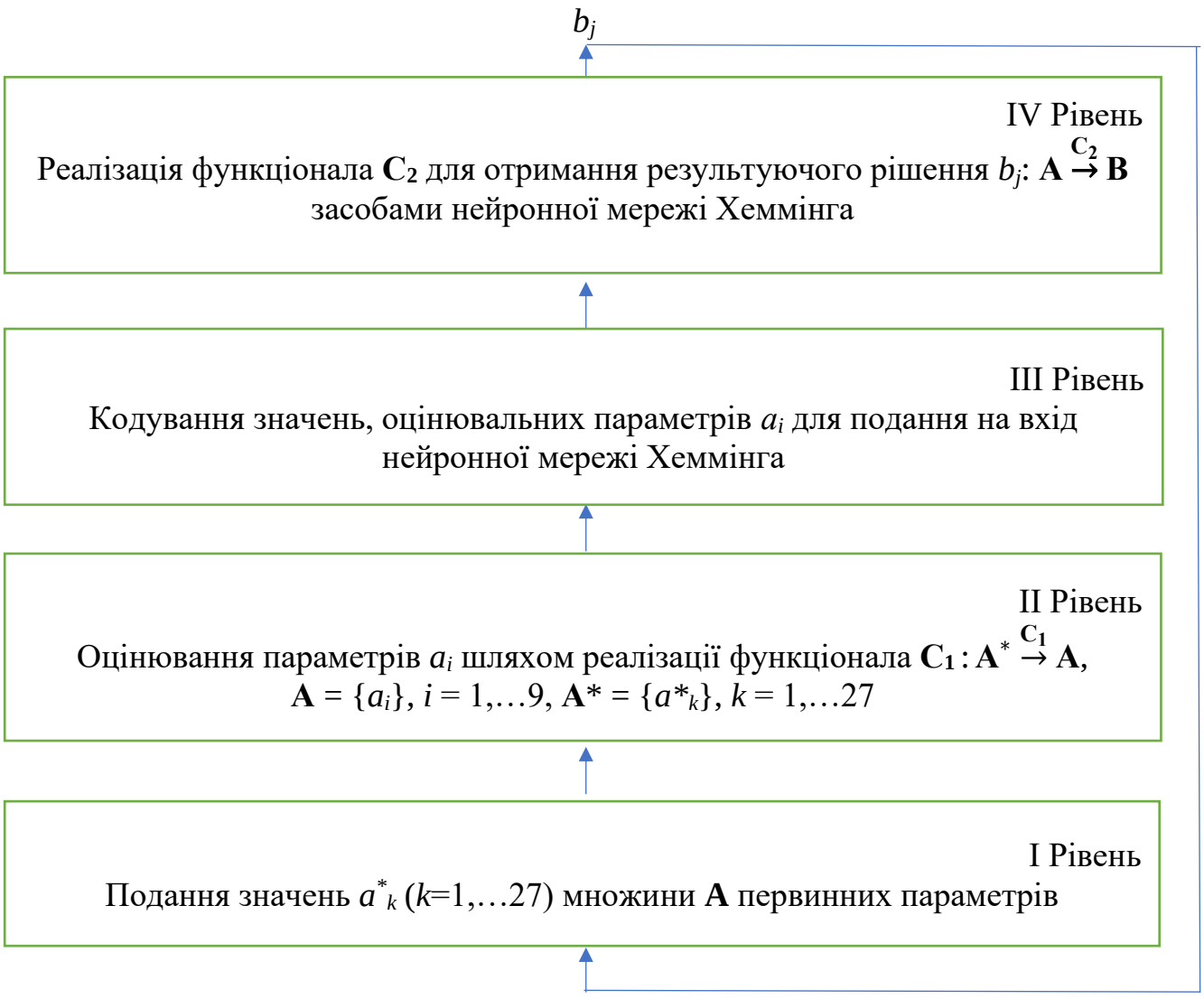


Рис. 1 Структурна модель процесу оцінювання вразливості інформаційної безпеки із застосуванням системного підходу та нейронної мережі Хеммінга

2.3 Розроблення математичної моделі нейронної мережі Хеммінгу для вивчення вразливості інформаційної безпеки

Математична модель для оцінювання вразливості інформаційної безпеки за допомогою нейронної мережі Хеммінга дозволяє оцінювати рівень вразливості із використанням вхідних бінарних кодів. Кожен показник вразливості представлений як бінарний вектор, до якого застосовується кодування Хеммінга для виявлення та виправлення можливих помилок. Модель оцінювання вразливості ґрунтується на порівнянні оригінального показника з відновленим, отриманим із кодового слова за допомогою процедури виявлення та виправлення помилок. Це дозволяє враховувати точність та ефективність мережі Хеммінга в контексті інформаційної безпеки, сприяючи надійній оцінці та управлінню вразливостями в інформаційних системах.

Нижче знаходиться математична модель процесу оцінювання вразливості інформаційної безпеки.

Математична модель дозволяє відобразити множину $\mathbf{A}^*$ первинних вхідних параметрів a^*_k на множину **B** вихідних рішень b_j за допомогою реалізації функціоналів $\mathbf{C_1}$ та $\mathbf{C_2}$:

$\mathbf{A}^* \xrightarrow{C_1} \mathbf{A} \xrightarrow{C_2} \mathbf{B}$, $\mathbf{A}^* = \{a^*_k\}$, $k = 1,\ldots 27$, $\mathbf{A} = \{a_i\}$, $i = 1,\ldots 9$, $\mathbf{B} = \{b_j\}$, $\mathbf{B}=\{b_j\}$, $j=1,..,m$

$\mathbf{A=C_1(A^*), B=C_2(A).}$

Функціонал $\mathbf{C_1}$ реалізує такі функції, що оцінюють відповідні залежності:

$a_1 = f(a^*_{1,}\ldots a^*_3)$,

$a_2 = f(a^*_{4,}\ldots a^*_6)$,

$a_3 = f(a^*_{7,}\ldots a^*_9)$,

$a_4 = f(a^*_{10,}\ldots a^*_{12})$,

$a_5 = f(a^*_{13,}\ldots a^*_{15})$,

$a_6 = f(a^*_{16,}\ldots a^*_{18})$,

$a_7 = f(a^*_{19,}\ldots a^*_{21})$,

$a_8 = f(a^*_{22,}\ldots a^*_{24})$,

$a_9 = f(a^*_{25,}\dots a^*_{27})$.

Нижче знаходяться перелік значень початкових показників a^*_k:

a^*_1 – використання слабких паролів обсягом до 7 символів;

a^*_2 – використання паролів із низькою ентропією, таких як "password123" обсягом до від 7 до 9 символів;

a^*_3 – використання паролів із високою ентропією, обсягом від 9 до 12 символів і більше;

a^*_4 – відсутність механізмів безпеки веб-додатків;

a^*_5 – використання стандартних механізмів безпеки веб-додатків: HTTPS, OWASP, CORS, CSP;

a^*_6 – використання передових технік безпеки веб-додатків: WAF, XSS;

a^*_7 – відсутність налаштувань рольового управління із обмеженням прав доступу (всі користувачі мають адміністративні привілеї);

a^*_8 – використання рольового управління для об'єднаної групи користувачів;

a^*_9 – використання деталізованого рольового управління (застосування принципу найменших привілеїв);

a^*_{10} – використання застарілих алгоритмів шифрування: DES, MD5, RSA, RC4;

a^*_{11} – використання стандартних алгоритмів шифрування, таких як AES або RSA, з ключами менше 128 біт для AES або менше 2048 біт для RSA;

a^*_{12} – використання сучасних алгоритмів шифрування з великою довжиною та унікальністю ключів, для AES з ключами довжиною 256 біт або RSA з ключами довжиною 3072 біт і більше;

a^*_{13} – відсутність брандмауерів;

a^*_{14} – використання брандмауерів для фільтрації та контролю трафіку типу WAF (Web Application Firewall);

a^*_{15} – комплексне використання брандмауерів типу NGFW;

a^*_{16} – відсутність контролю доступу;

a^*_{17} – застосування контрольованого доступу;

a^*_{18} – застосування системи доступу на підставі біометричних показників;

a^*_{19} – відсутність проведення навчання персоналу з питань безпеки;

a^*_{20} – ситуативне проведення навчання персоналу з питань безпеки після інцидентів порушення інформаційної безпеки;

a^*_{21} – постійне проведення навчання персоналу з питань безпеки;

a^*_{22} – відсутність систем виявлення вторгнень;

a^*_{23} – використання звичайних систем виявлення вторгнень: IDS, IPS;

a^*_{24} – використання інтелектуальних систем з автоматичним реагування на загрози: SIEM, Palo Alto Networks Panorama;

a^*_{25} – відсутність резервного копіювання даних;

a^*_{26} – резервне копіювання даних в ручному режимі;

a^*_{27} – автоматизоване резервне копіювання даних.

Реалізація функціоналу $\mathbf{C_2}$ полягає у відображенні множини вхідних функцій a_i, закодовані значення яких подаються на вхід нейронної мережі Хеммінга, на множину вихідних рішень $\mathbf{B}=\{b_j\}$, $j=1,..,m$. Мережа Хеммінга для сигналу поданого на її вхід – вектора оцінювальних параметрів a_i – знаходить відповідний еталонний зразок щодо рівня вразливості інформаційної системи.

Відповідно, нижче знаходиться таблиця еталонних показників оцінювання вразливості інформаційної безпеки, які будуть використовуватися для роботи нейронної мережі Хеммінга. Тому, шляхом використання експертних методів та проведення анкетного опитування серед фахівців з кібербезпеки стосовно питань захисту інформаційних систем, були визначені граничні значення оцінювальних показників. Ці значення розподілені відповідно до 9 оцінювальних параметрів на три діапазони: Н (низький), С (середній) та В (високий). Такий підхід дозволяє систематизувати інтервали значень для кожного оцінювального параметра a_i. В результаті було сформовано таблицю із значеннями оцінювальних параметрів.

Нижче знаходиться табл. 2.1 для оцінювання параметрів a_i на базі множини

початкових показників a^*_k [32].

Таблиця 2.1 – Присвоєння характеристичного терму, який описує значення параметра a_i

Назва оцінювального параметра a_i	Назва первинного вхідного параметра a^*_k	Характеристичний терм, який описує значення параметра a_i
a_1 – вразливості автентифікації та авторизації	a^*_1 – використання слабких паролів обсягом до 7 символів	В – високий рівень вираженості параметра a_i
	a^*_2 – використання паролів із низькою ентропією, таких як «password123» обсягом до від 7 до 9 символів	С – Середній рівень вираженості параметра a_i
	a^*_3 – використання паролів із високою ентропією, обсягом від 9 до 12 символів і більше	Н – Низький рівень вираженості параметра a_i
a_2 – вразливості захищеності веб-додатків	a^*_4 – відсутність механізмів безпеки веб-додатків	В
	a^*_5 – використання стандартних механізмів безпеки веб-додатків: HTTPS, OWASP, CORS, CSP	С
	a^*_6 – використання передових технік безпеки веб-додатків: WAF, XSS	Н
a_3 – вразливості керування доступом	a^*_7 – відсутність налаштувань рольового управління із обмеженням прав доступу (всі користувачі мають адміністративні привілеї)	В
	a^*_8 – використання рольового управління для об'єднаної групи користувачів	С
	a^*_9 – використання деталізованого рольового управління (застосування принципу найменших привілеїв)	Н
a_4 – вразливості шифрування даних	a^*_{10} – використання застарілих алгоритмів шифрування: DES, MD5, RSA, RC4	В
	a^*_{11} – використання стандартних алгоритмів шифрування, таких як AES або RSA, з ключами менше	С

	128 біт для AES або менше 2048 біт для RSA	
	a^*_{12} – використання сучасних алгоритмів шифрування з великою довжиною та унікальністю ключів, для AES з ключами довжиною 256 біт або RSA з ключами довжиною 3072 біт і більше	H
a_5 – вразливості мережевої безпеки	a^*_{13} – відсутність брандмауерів	B
	a^*_{14} – використання брандмауерів для фільтрації та контролю трафіку типу WAF (Web Application Firewall)	C
	a^*_{15} – комплексне використання брандмауерів типу NGFW	H
a_6 – вразливості фізичної безпеки	a^*_{16} – відсутність контролю доступу	B
	a^*_{17} – застосування контрольованого доступу	C
	a^*_{18} – застосування системи доступу на підставі біометричних показників	H
a_7 – вразливості соціальної інженерії	a^*_{19} – відсутність проведення навчання персоналу з питань безпеки	B
	a^*_{20} – ситуативне проведення навчання персоналу з питань безпеки після інцидентів порушення інформаційної безпеки	C
	a^*_{21} – постійне проведення навчання персоналу з питань безпеки	H
a_8 – вразливості системи виявлення та запобігання вторгнень	a^*_{22} – відсутність систем виявлення вторгнень	B
	a^*_{23} – використання звичайних систем виявлення вторгнень: IDS, IPS	C
	a^*_{24} – використання інтелектуальних систем з автоматичним реагування на загрози: SIEM, Palo Alto Networks Panorama	H

a_9 – вразливості втрати даних	a^*_{25} – відсутність резервного копіювання даних	В
	a^*_{26} – резервне копіювання даних в ручному режимі	С
	a^*_{27} – автоматизоване резервне копіювання даних	Н

Розглянемо табл. 2.2, в якій експертами сформовано найбільш типові еталони для роботи мережі Хеммінга. Тут використовуються отримані на попередньому етапі характеристичні терми для опису значень оцінювальних параметрів a_i, що є функціями від a^*_k, як зазначено у табл. 2.1.

Таблиця 2.2 – Таблиця еталонних зразків нейронної мережі Хеммінга

№ еталону	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	b_j
1	Н	Н	Н	Н	Н	Н	Н	Н	Н	Н
2	Н	С	Н	Н	В	Н	Н	С	В	
3	С	С	С	С	С	С	С	С	С	С
4	Н	В	В	С	В	В	В	С	Н	В
5	В	В	В	В	В	В	В	В	В	

Нейронна мережа Хеммінга використовує тільки числові значення «1» та «-1», тому автор пропонує закодувати значення 3 характеристичних термів – Н, С, В, що описують значення вхідних функцій a_i відповідним двійковим кодом, представленим у табл. 2.3. При цьому формат коду складається з двох цифр, що дозволяє закодувати 4 (2^2=4).

Значення вихідних параметрів b_j (j=1,..3) оцінювання вразливості інформаційної безпеки описується також трьома рівнями – Н, С, В, як вказано у табл. 2.3.

Таблиця 2.3 – Кодування рівнів двійковим кодом

Характеристичний рівень	Код мережі Хеммінга	
Низький	-1	-1
Середній	-1	1
Високий	1	1

Використовуючи дві попередні таблиці, можемо зобразити еталонні показники вразливості інформаційної безпеки за допомогою мережі Хеммінга.

Таблиця 2.4 – Закодована таблиця еталонних зразків для роботи мережі Хеммінга

№ еталону	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	b_j
1	-1-1	-1-1	-1-1	-1-1	-1-1	-1-1	-1-1	-1-1	-1-1	-1-1
2	-1-1	-1 1	-1-1	-1-1	1 1	-1-1	-1-1	-1 1	1 1	
3	-1 1	-1 1	-1 1	-1 1	-1 1	-1 1	-1 1	-1 1	-1 1	-1 1
4	-1-1	1 1	1 1	-1 1	1 1	1 1	1 1	-1 1	-1-1	1 1
5	1 1	1 1	1 1	1 1	1 1	1 1	1 1	1 1	1 1	

Використання мережі Хеммінга полягає у подачі на її вхід вектору із 18 закодованих значень 9 оцінювальних параметрів a_i та порівняння цього вектору з найближчим до нього вектором із табл. 2.4 еталонів. Отже, нейронна мережа Хеммінга ідентифікує еталон, який найближчий до вектора, поданого на вхід. Номер даного еталону, який взятий із табл. 2.4 дозволяє здійснити класифікацію результуючого рішення з присвоєння відповідного рівня вразливості інформаційної безпеки $b_j(j=1,..3)$.

Розглянемо етапи реалізації функціоналів $\mathbf{C_1}$ та $\mathbf{C_2}$ запропонованої автором математичної моделі.

Етап 1. Подання значення a^*_k (k=1,…27) первинних вхідних параметрів, що використовуються для розрахунку функцій (оцінювальних параметрів) a_i (i =1,…9) досліджуваних інформаційних систем;

Етап 2. Значення оцінювальних параметрів $a_1...a_9$ описуються конкретним характеристичним рівнем (Н – низький, С – середній, В – високий) шляхом реалізації функціоналу $\mathbf{C_1}$;

Етап 3. Формування вхідного вектору (який складається з 18 цифр «1» та «-1») для роботи мережі Хеммінга шляхом кодування значень оцінювальних параметрів a_i.

Етап 4. Нейронна мережа Хеммінга визначає найближчий до даного вектору еталон, номер якого відповідає певному вихідному рішенню b_j.

Отже, розглянемо використання нейронної мережі Хеммінга для оцінювання рівня вразливості інформаційної безпеки 5 вітчизняних компаній [32], що працюють у медичній та банківській сферах, шляхом використання програмного застосунку, розроблення якого описано розділі 3.

Таблиця 2.5 – Результат використання нейронної мережі Хеммінга для оцінювання вразливостей п’яти ІС у сфері медичних та банківських послуг.

№ компанії	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	Рівень вразливості b_j
1	Н	В	В	С	В	В	В	Н	С	Високий
2	Н	С	В	С	С	С	С	С	С	Середній
3	В	Н	Н	С	Н	Н	Н	В	Н	Низький
4	Н	В	В	С	С	В	В	С	Н	Високий
5	Н	С	С	С	В	С	С	Н	С	Середній

Для перевірки адекватності складеної математичної моделі та методу її формалізації було порівняно отримані за допомогою розробленого програмного застосунку рівнів вразливості інформаційної безпеки в відповідних системах на досліджуваних суб’єктах господарювання та отримані за допомогою відомих на ринку ПЗ: Nessus, OpenVAS, Metasploit, Wireshark, Burp Suite [33], що розглянуто у табл. 2.6.

Таблиця 2.6 – Порівняння оцінок запропонованого програмного застосунку із оцінками, отриманими засобами ПЗ Nessus, OpenVAS, Metasploit, Wireshark, Burp Suite для ІС 5 компаній у сфері медичних та банківських послуг

ПЗ / № компанії	Рівень вразливості b_j за «Nessus»	Рівень вразливості b_j за «OpenVAS»	Рівень вразливості b_j за «Metasploit»	Рівень вразливості b_j за «Wireshark»	Рівень вразливості b_j за «Burp Suite»	**Рівень вразливості b_j за запропонованою ІТ**
1	В	В	В	В	В	В
2	С	С	С	С	С	С
3	Н	Н	Н	С	Н	Н
4	В	В	В	В	В	В
5	С	С	В	С	С	С

Порівняння оцінок рівнів вразливостей 5 сучасних ІС, визначених за розробленим програмним застосунком та існуючими на ринку ПЗ, дозоляє отримати фактично однакові результати, що свідчить про адекватність складених математичної моделі та методу її формалізації, що автоматизовані засобами відповідного програмного застосунку.

Отже, використання нейронної мережі Хеммінга з метою оцінювання рівня вразливості інформаційної безпеки показує наочний результат їх дієвості та ефективності.

Таким чином, використання математичної моделі, яку запропоновано автором магістерської дисертації дає такі переваги:

- забезпечення цілісності інформації;
- точність видачі результатів;
- захист від помилок;
- використання та врахування значної кількості оцінювальних параметрів;
- наявність елементів самостійного навчання;
- швидкість отримання результатів.

Інтеграція елементів самонавчання дозволяє системі адаптуватися до нових умов та ідентифікувати нові загрози, а швидкість видачі результатів забезпечує оперативність у реагуванні на потенційні ризики та впровадженні відповідних заходів безпеки.

2.4 Висновки до розділу

У другому розділі обґрунтовано вибір мережі Хеммінга для реалізації остаточного етапу визначення рівня вразливості досліджуваного суб’єкта господарювання.

Запропоновано структурну модель процесу оцінювання вразливості рівня інформаційної безпеки засобами системного підходу.

Розроблено математичну модель, яка включає множину вхідних

параметрів **A** та множину вихідних рішень **B** за допомогою реалізації функціоналів $\mathbf{C_1}$ та $\mathbf{C_2}$.

Запропоновано метод відображення множини вхідних рішень на множину вихідних рішень, що на відміну існуючого підходу дозволяє засобами нейронної мережі Хеммінга підвищити ефективність такого процесу.

Детальний аналіз мережі Хеммінга в контексті забезпечення інформаційної безпеки розкриває її можливості надійного виявлення помилок та відновлення цілісності даних. Це стає ключовим фактором для забезпечення надійності обміну інформацією в умовах постійних кібератак та технічних аномалій.

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ ПЗ ДЛЯ ОЦІНЮВАННЯ ВРАЗЛИВОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Виходячи із поставлених задач роботи та розробленої математичної моделі оцінювання вразливості інформаційної безпеки, в цьому розділі буде надано детальний опис практичної реалізації програмного застосунку, який реалізує процес оцінювання вразливості інформаційної безпеки за допомогою нейронної мережі Хеммінга.

В цьому розділі буде описано проектування користувацького інтерфейсу розробки, програмну реалізацію, інструкцію користувачу для роботи з програмним застосунком, та проведено його тестування.

Для реалізації програмного застосунку (веб-сервісуф) заплановано: використання платформи ASP.NET Core 3.1, мови програмування C# (backend), фреймворку Angular та мови програмування JavaScript (frontend).

4 Розробка програмного застосунку для оцінювання вразливості інформаційної безпеки

Програмний застосунок використовує за основу розроблену математичну модель для оцінювання вразливості інформаційної безпеки із застосуванням нейронної мережі Хеммінга.

Під час розробки програмного застосунку ключовим етапом є створення користувацького інтерфейсу. Плануючи веб-сервіс, слід приділити увагу таким вимогам до графічного інтерфейсу (GUI):

1. Сторінка сервісу повинна мати чітку візуальну ієрархію елементів.
2. Розташування текстових фрагментів на екрані має сприяти природньому руху погляду користувача у потрібному напрямку.
3. Вміст полів не повинен стискатися до меж екрану, але повинен розташовуватися вздовж горизонтальних або вертикальних осей.

З урахуванням цих завдань та вимог до інтерфейсу було розроблено зовнішній вигляд програмного застосунку (веб-сервісу).

Нижче знаходяться основні етапи роботи застосунку:

1. Обрання параметрів. Серед переліку оцінювальних параметрів, Користувач обирає первинні вхідні параметри які відповідають його інформаційній системі. Візуально це можна спостерігати на Рис. 3.1

Рисунок 3.1 – Приклад відображення первинних вхідних параметрів

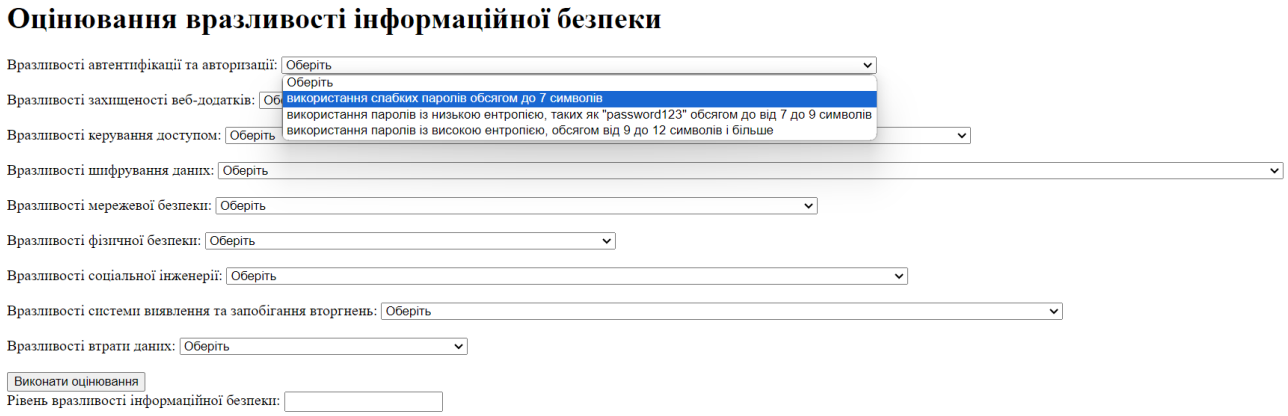
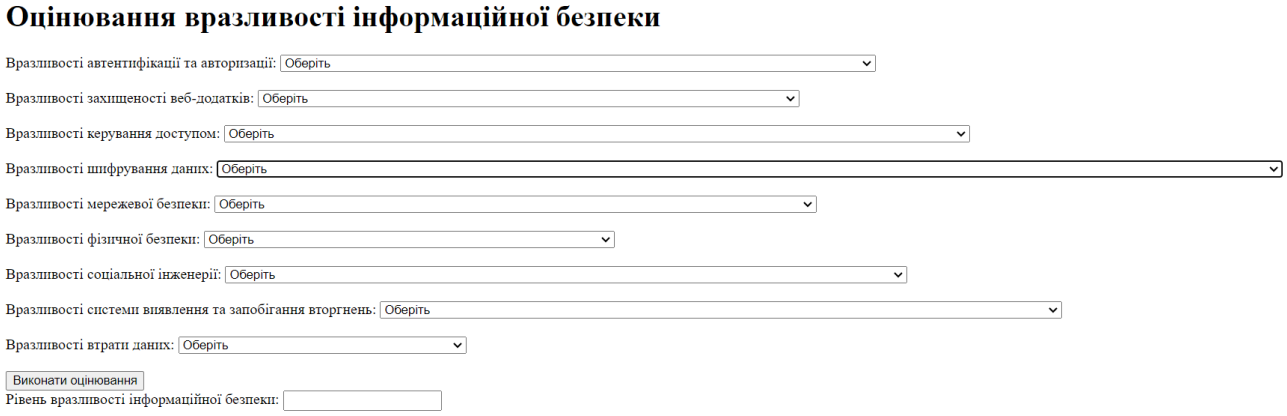


Рис. 3.2 Зображення загального вигляду оцінювальних показників вразливості



2. Виклик програми Хеммінга. Після обрання параметрів користувач натискає кнопку "Виконати оцінювання", що ініціює виклик функції runHammingProgram() у JavaScript.

3. Відправка даних на сервер. JavaScript-код використовує fetch для відправки введених користувачем даних на сервер для обчислення за алгоритмом

Хеммінга.

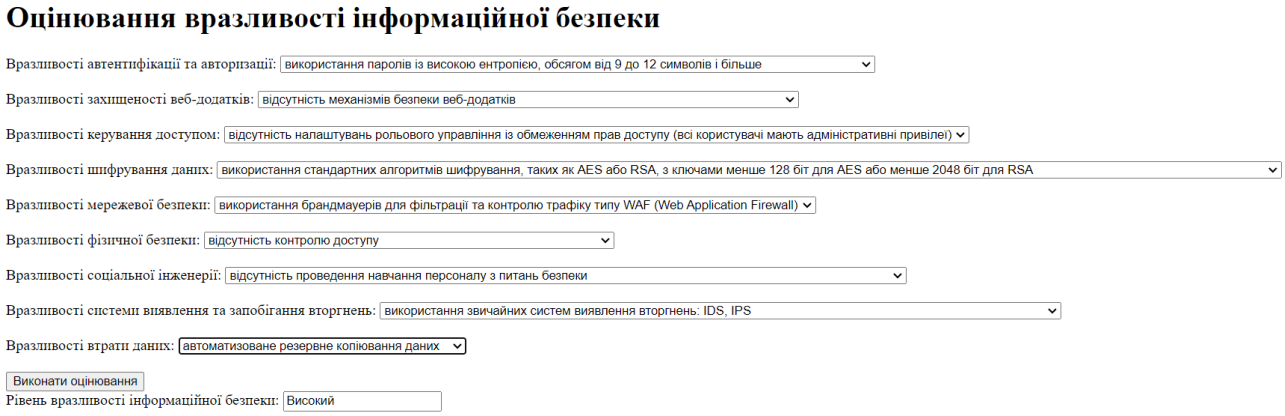
4. Обчислення на сервері. На сервері оброблюються отримані від користувача дані, і застосовується алгоритм Хеммінга для визначення рівня вразливості інформаційної безпеки.

5. Отримання результатів. Результати програми Хеммінга повертаються на клієнтську сторінку.

6. Відображення результатів. JavaScript-код відображає результати на сторінці, наприклад, в блоку з ідентифікатором "resultContainer".

7. Відображення рівня вразливості. Рівень вразливості інформаційної безпеки виводиться в полі "Рівень вразливості інформаційної безпеки", Рис. 3.3.

Рисунок 3.3. Відображення рівня вразливості інформаційної безпеки



Нижче показано інструкцію з користування програмного застосунку:

Крок 1: Запуск програми

- Відкрити посилання на веб-застосунок в веб-браузері.

Крок 2: Обрання параметрів вразливості

- Обрати рівні вразливості для кожного з 9 параметрів інформаційної безпеки, використовуючи випадаючі списки, які містять один із трьох рівнів.

Крок 3: Виконання оцінювання

- Після вибору рівнів вразливості, натиснути кнопку "Виконати оцінювання".

Крок 4: Очікування результатів

- Очікувати, поки програма обчислює результати за алгоритмом Хеммінга.

Крок 5: Перегляд результатів

- Після завершення обчислень результати відобразяться на сторінці в полі "Рівень вразливості інформаційної безпеки".

3.2. Аналіз результатів

Розроблена програма є інструментом для оцінювання вразливості інформаційної безпеки за допомогою нейронної мережі Хеммінга. Вона призначена для визначення рівня вразливості.

Розробка дозволяє вдосконалити та автоматизувати процес оцінювання вразливості інформаційної безпеки, зокрема врахувати широку множину різних первинних показників, врахувати різні рівні вразливості, пришвидшити процес оцінювання вразливості інформаційної безпеки.

Нижче, на Рис. 3.4-3.6 знаходяться відображення результатів тестування роботи програмного застосунку:

Рисунок 3.4 – Візуальне зображення результату процесу оцінювання інформаційної безпеки для низького рівня вразливості

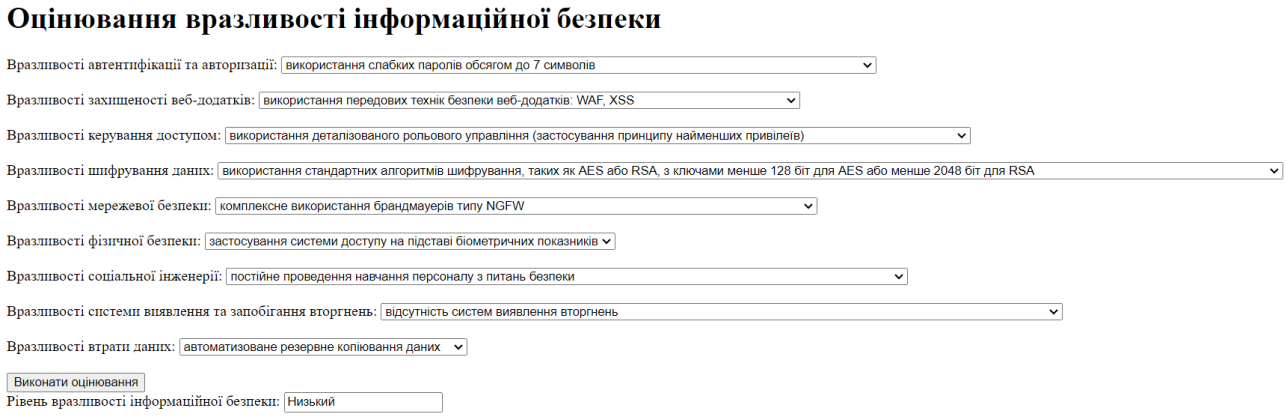


Рисунок 3.5 – Візуальне зображення результату процесу оцінювання інформаційної безпеки для середнього рівня вразливості

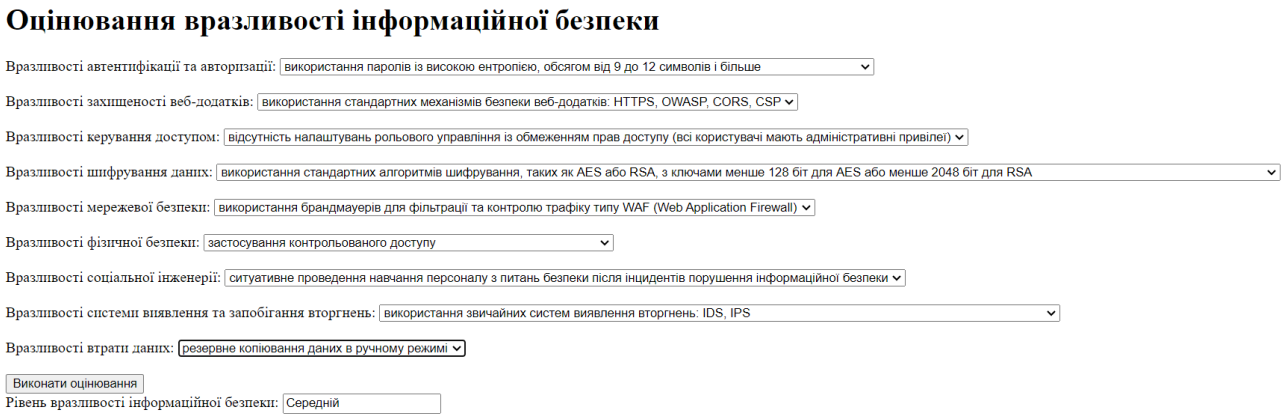
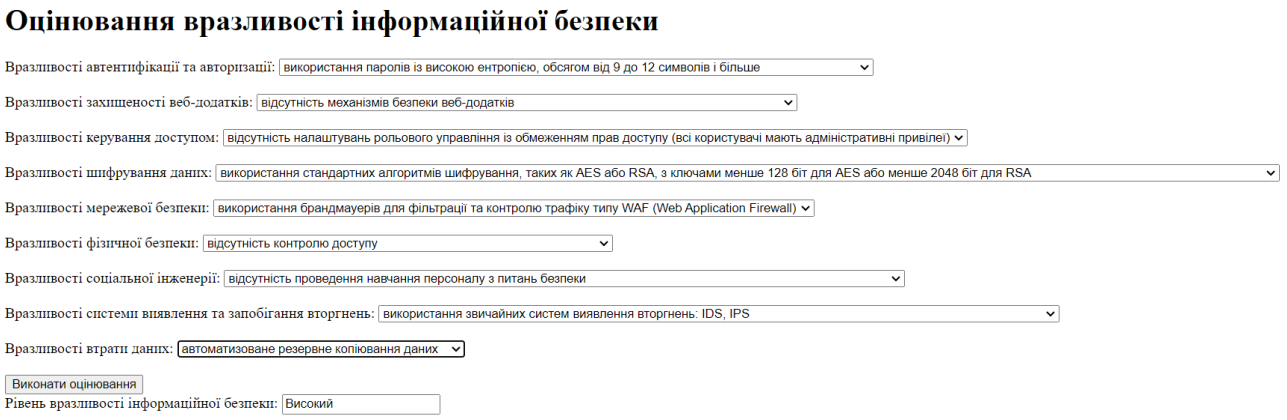


Рисунок 3.6 – Візуальне зображення результатів процесу оцінювання інформаційної безпеки для високого рівня вразливості



3.3. Висновки до розділу

Програмний застосунок, реалізований на основі розробленого методу оцінювання вразливості інформаційної безпеки з використанням нейронної мережі Хеммінга.

Відповідно до поставлених завдань, розробка була проведена з використанням платформи ASP.NET Core 3.1 та мови програмування C# для backend частини, а також фреймворку Angular та мови програмування JavaScript для frontend частини. Описано проектування інтерфейсу користувача,

особливості програмної реалізації та надано інструкцію користувача для роботи з додатком.

Такий підхід до оцінювання вразливості інформаційної безпеки не лише підкреслює сучасні тенденції в галузі кібербезпеки, але й демонструє важливість використання передових технологій штучного інтелекту для досягнення високого рівня безпеки в інформаційних системах.

4. ЕКОНОМІЧНА ЧАСТИНА

В даному розділі проведемо дослідження економічного потенціалу наступної розробки: оцінка потенціалу в комерційному плані; передбачення витрат на проведення наукового дослідження та впровадження його результатів; прогнозування комерційних вигод від впровадження розробок та розрахунок ефективності інвестицій та строків їх повернення.

В результаті цього дослідження буде зроблено висновок щодо економічної обґрунтованості створення програмного продукту для оцінки вразливості інформаційної безпеки із використанням нейронної мережі Хеммінга.

Оцінка економічного потенціалу розробки буде виконуватись відповідно до вимог Методичних вказівок до виконання економічної частини магістерських кваліфікаційних робіт [34].

4.1 Оцінювання комерційного потенціалу розробки програмного забезпечення

Метою технологічного аудиту є аналіз комерційної перспективи продукту, який виникає внаслідок науково-технічної діяльності.

Результатом магістерської кваліфікаційної роботи є розробка програмного засобу на основі алгоритму для вдосконалення оцінки вразливості інформаційної системи за допомогою нейронної мережі Хеммінга, який реалізований у вигляді веб-сервісу.

Для проведення технологічного аудиту залучено трьох незалежних експертів.

У межах даної роботи такими експертами є викладачі кафедри МБІС:

– Карпінець В. В. (к.т.н., доцент каф. МБІС ВНТУ),

– Салієва О.В. (доктор філософії з ІТ, доцент каф. МБІС ВНТУ)

– Грицак А. В. (доц., викл. каф. МБІС ВНТУ).

Оцінювання комерційного потенціалу здійснимо за критеріями, що наведені в таблиці 4.1

Таблиця 4.1 – Критерії оцінювання комерційного потенціалу розробки бальна оцінка

Критерії оцінювання та бали (за 5-ти бальною шкалою)					
Кри-терій	0	1	2	3	4
Технічна здійсненність концепції:					
1	Достовірність концепції не підтверджена	Концепція підтверджена експертними висновками	Концепція підтверджена розрахунками	Концепція перевірена на практиці	Перевірено роботоздатність продукту в реальних умовах
Ринкові переваги (недоліки):					
2	Багато аналогів на малому ринку	Мало аналогів на малому ринку	Кілька аналогів на великому ринку	Один аналог на великому ринку	Продукт не має аналогів на великому ринку
3	Ціна продукту значно вища за ціни аналогів	Ціна продукту дещо вища за ціни аналогів	Ціна продукту приблизно дорівнює цінам аналогів	Ціна продукту дещо нижче за ціни аналогів	Ціна продукту значно нижче за ціни аналогів
Критерії оцінювання та бали (за 5-ти бальною шкалою)					
Кри-тер.	0	1	2	3	4

4	Технічні та споживчі властивості продукту значно гірші, ніж в аналогів	Технічні та споживчі властивості продукту трохи гірші, ніж в аналогів	Технічні та споживчі властивості продукту на рівні аналогів	Технічні та споживчі властивості продукту трохи кращі, ніж в аналогів	Технічні та споживчі властивості продукту значно кращі, ніж в аналогів
5	Експлуатаційні витрати значно вищі, ніж в аналогів	Експлуатаційні витрати дещо вищі, ніж в аналогів	Експлуатаційні витрати на рівні експл. витрат аналогів	Експлуатаційні витрати трохи нижчі, ніж в аналогів	Експлуатаційні витрати значно нижчі, ніж в аналогів
Ринкові перспективи					
6	Ринок малий і не має позитивної динаміки	Ринок малий, але має позитивну динаміку	Середній ринок з позитивною динамікою	Великий стабільний ринок	Великий ринок з позитивною динамікою
7	Активна конкуренція великих компаній на ринку	Активна конкуренція	Помірна конкуренція	Незначна конкуренція	Конкурентів немає
Практична здійсненність					
8	Відсутні фахівці як з технічної, так і з комерційної реалізації ідеї	Необхідно наймати фахівців або витрачати значні кошти та час на навч. наявних фахівців	Необхідне незначне навчання фахівців та збільшення їх штату	Необхідне незначне навчання фахівців	Є фахівці з питань як з технічної, так із комерційної реалізації ідеї
9	Потрібні значні фінансові ресурси, які відсутні. Джерела фінансування ідеї відсутні	Потрібні незначні фінансові ресурси. Джерела фінансування відсутні	Потрібні значні фінансові ресурси. Джерела фінансування є	Потрібні незначні фінансові ресурси. Джерела фінансування є	Не потребує додаткового фінансування

10	Необхідна розробка нових матеріалів	Потрібні матеріали, що використовуються у військово-промисловому комплексі	Потрібні дорогі матеріали	Потрібні досяжні та дешеві матеріали	Всі матеріали для реалізації ідеї відомі та давно використовуються у виробництві
11	Термін реалізації ідеї більший за 10 років	Термін реалізації ідеї більший за 5 років. Термін окупності інвестицій більше 10-ти років	Термін реалізації ідеї від 3-х до 5-тироків. Термін окупності інвестицій більше 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій від3-х до 5-ти років	н реалізаціїідеї менше 3-х років. Термін окупності інвестицій менше 3-х років
12	Необхідна розробка регламентних документів та отримання великої кількості дозвільних документів на виробництво та реалізацію продукту	Необхідно отримання великої к-ті дозвільних документів навир-во та реалізацію продукту, що вимагає значних коштів та часу	Процедура отримання дозвільних документів для виробництва та реалізації продукту вимагає незначних коштів тачасу	Необхідно тільки пові-домлення відповідним органам про виробництво та реалізацію продукту	Відсутні будь-які регламентні обмеження на виробництво та реалізацію продукту

Результати оцінювання комерційного потенціалу експертами розробки зведено в таблицю 4.2.

Таблиця 4.2 – Результати оцінювання комерційного потенціалу розробки

Критерії	Прізвище, ініціали, посада експерта		
	1 – КарпінецьВ.В.	2 – Салієва О.В.	3 – Грицак А.В.
1	3	4	4
2	4	3	4
3	3	4	4
4	3	4	4
5	4	3	4
6	4	4	4
7	4	3	3

8	3	3	3
9	4	4	4
10	4	3	4
11	3	4	4
12	4	4	3
Сума балів	$СБ_1 = 44$	$СБ_1 = 44$	$СБ_1 = 49$
Середньоарифметична сума балів $\overline{СБ}$	$\overline{СБ} = 45,6$		

За даними таблиці 4.2 можна зробити висновок, щодо рівня комерційного потенціалу розробки. Зважимо на результат й порівняємо його з рівнями комерційного потенціалу розробки, що представлено в таблиці 4.3.

Таблиця 4.3 – Рівні комерційного потенціалу розробки

Середньоарифметична сума балів $\overline{СБ}$, розрахована на основі висновків експертів	Рівень комерційногопотенціалу розробки
0 – 10	Низький
11 – 20	Нижче середнього
21 – 30	Середній
31 – 40	Вище середнього
41 – 48	Високий

Рівень комерційного потенціалу розробки, становить 45,6 балів, що відповідає рівню «високий».

Далі зробимо аналіз технічної проблеми та розглянемо аналоги. Наукова новизна розробки полягає у вдосконаленні оцінки вразливості інформаційної безпеки за допомогою нейронної мережі Хеммінга.

Розробка програмного засобу має на меті практичну реалізацію вдосконалення методу оцінювання вразливості інформаційної безпеки.

Розроблюваний програмний продукт у вигляді програмного застосунку надаватиме можливість провести оцінювання рівня вразливості власної інформаційної системи.

Оцінюючи результати проведеного дослідження розробленого програмного продукту, заснованого на використанні нейронної мережі Хеммінга, можна стверджувати, що цей продукт відкриває можливість для

реалізації більш точного, систематизованого та автоматизованого процесу оцінки вразливості інформаційної системи. Крім того, його здатність до самонавчання додає ефективності та адаптивності у виявленні та усуненні потенційних проблем безпеки в інформаційних системах.

Враховуючи ці переваги розробленого програмного засобу, можна провести порівняльний аналіз з його аналогами. У табл. 4.4 представлені ключові технічні показники аналога та нового програмного продукту.

Таблиця 4.4 – Основні технічні показники аналога і нового програмного продукту

Показники, %	Аналог	Нова розробка	Відношення параметрів нової розробки до параметрів аналога
Функціональність	73	100	1,37
Надійність	75	100	1,33
Сумісність	95	100	1,05
Супровід	90	100	1,11
Економія ресурсів і часу	80	100	1,25
Простота використання	82	100	1,22

У висновку, розроблений програмний застосунок на базі нейронної мережі Хеммінга виявився ефективним інструментом для оцінювання вразливості інформаційних систем. Його точність та систематизація дозволяють детально досліджувати потенційні ризики, забезпечуючи високий рівень безпеки. Автоматизація та можливість самонавчання забезпечують швидку адаптацію до нових загроз та змінних умов. Порівняльний аналіз підтверджує переваги цього застосунку, встановлюючи його як передовий засіб для сучасного оцінювання безпеки інформаційних систем.

Застосунок вирізняється високою автоматизацією, що спрощує та прискорює процес оцінки вразливостей. З врахуванням цих переваг, можна визнати програмний застосунок на основі нейронної мережі Хеммінга високоефективним і передовим засобом для вирішення викликів забезпечення

інформаційної безпеки в сучасному інформаційному середовищі.

4.2 Прогнозування витрат на виконання наукової роботи та впровадження її результатів

Прогнозування витрат на виконання науково-дослідної, дослідно-конструкторської та конструкторсько-технологічної роботи складається з таких етапів:

1- й етап: розрахунок витрат, які безпосередньо стосуються виконавців даного розділу роботи;

2- й етап: розрахунок загальних витрат на виконання даної роботи;

3- й етап: прогнозування загальних витрат на виконання та впровадження результатів даної роботи.

Виконаємо розрахунок витрат, які безпосередньо стосуються виконавців даного розділу роботи, за такими статтями та формулами, приймаючи до уваги те, що для розробки інформаційної технології було залучено керівника проекту та одного розробника програмного забезпечення.

1. Основна заробітна $З_о$ розраховується за формулою (4.1):

$$З_о = \sum_{i=1}^{k} \frac{M_{ni} \cdot t_i}{T_p}$$

Де:
M_1 – місячний посадовий оклад керівника проекту – 42 000 грн.;
M_2 – місячний посадовий оклад розробника – 37 000 грн.;
T_p – число робочих днів в місяці; приблизно $Т_р$ = 23 дні;
t – число робочих днів – 50 днів.
Таким чином:

$З_1$ = 91 304,35 (грн.) – для керівника проекту

$З_2$ = 80 434,78 (грн.) – для розробника

$З_о = З_1 + З_2$ = 91 304,35 + 80 434,78 = 171 739,13

Таблиця 4.5 – Розрахунок заробітних плат

Найменування посади	Місячний посадовий оклад, грн	Оплата за робочий день, грн	Кількість днів роботи	Витрати на заробітну плату, грн
Керівник проекту	42 000	1 826	50	91 304,35
Розробник	37 000	1 608,7	50	80 434,78
Всього:				171 739,13

2. Додаткова заробітна плата $З_Д$ розраховується як 10% відосновної заробітної плати. Розрахунок здійснюється за наступною формулою (4.2):

$$З_{дод}=(З_о+З_р)\cdot\frac{Н_{дод}}{100\%}$$

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

$$З_{дод} = 0{,}1\cdot 171\ 739{,}13 = 17\ 173{,}9 \text{ (грн.)}$$

3. відрахування внеску на загальнообов’язкове державне соціальне страхування та для здійснення заходів щодо соціального захисту населення (ЄСВ – єдиний соціальний внесок) розробника становить 22% від суми основної та додаткової заробітної плати, і розраховується за наступною формулою (формула 4.3):

$$З_н = (З_о + З_д)\cdot\frac{Н_{зп}}{100\%}$$

де $Н_{зп}$ – норма нарахування на заробітну плату.

$$З_н = (171\ 739{,}13 + 17\ 173{,}9)\cdot 0{,}22 = 41\ 560{,}86 \text{ (грн.)}$$

4. Програмне забезпечення для наукових (експериментальних) робіт. До балансової вартості програмного забезпечення входять витрати на його

інсталяцію, тому ці витрати беруться додатково в розмірі 10% від вартості програмного забезпечення. Балансову вартість програмного забезпечення розраховують за формулою (формула 4.4):

$$B_{прг} = \sum_{i=1}^{k} Ц_{iпрг} \cdot C_{прг.i} \cdot K_i$$

де $Ц_{iпрг}$ – ціна придбання одиниці програмного засобу цього виду, грн;

$C_{прг.i}$ – кількість одиниць програмного забезпечення відповідного найменування, які придбані для проведення досліджень, шт.;

K_i – коефіцієнт, що враховує інсталяцію, налагодження програмного засобу тощо, (Кі = 1,10);

k – кількість найменувань програмних засобів.

Отримані результати занесені до таблиці.

Таблиця 4.6 – Витрати на придбання програмних засобів по кожному виду

Найменування програмного засобу	Кількість, шт	Ціна за одиницю, грн	Вартість, грн
Microsoft Windows 11 Pro	2	7 899	15 798
Microsoft 365 E3	2	2 664	5 328
Microsoft Visual C #	2	0	0
Microsoft Forms	2	0	0
.NET	2	0	0
Всього			21 126

5. Амортизація обладнання, комп’ютерів та приміщень, які використовувались під час виконання даного етапу роботи розраховуємо за формулою (формула 4.5):

$$A_{обл} = \frac{Ц_б}{T_в} \cdot \frac{t_{вик}}{12},$$

де $Ц_б$ – балансова вартість обладнання, програмних засобів, приміщень тощо, які використовувались для проведення досліджень, грн;

$t_{вик}$ – термін використання обладнання, програмних засобів, приміщень під час досліджень, місяців;

$T_в$ – строк корисного використання обладнання, програмних засобів, приміщень тощо, років.

Для офісного приміщення $A_1 = \frac{1\ 000\ 000}{20} \cdot \frac{2}{12} = 8\ 333{,}3$ грн.;

Для ноутбука $A_2 = \frac{30\ 000}{3} \cdot \frac{2}{12} = 1\ 666{,}6$ грн.;

Для роутера $A_3 = \frac{3\ 000}{3} \cdot \frac{2}{12} = 166{,}6$ грн.;

Для програмного забезпечення $A_4 = \frac{21\ 126}{2} \cdot \frac{2}{12} = 1\ 760{,}5$ грн.;

$A_{обл} = A_1 + A_2 + A_3 + A_4 = 8\ 333{,}3 + 1\ 666{,}6 + 166{,}6 + 1\ 760{,}5 = 11\ 927$ грн.

Таблиця 4.7 - Амортизаційні відрахування по кожному виду обладнання

Найменування	Балансова вартість (грн.)	Строк корисного використання, років	Фактична тривалість в-ня, (міс.)	Величина амортизаційних відрахувань, (грн.)
Приміщення	1 000 000	20	2	8 333,3
Ноутбук	30 000	3	2	1 666
Роутер	3 000	3	2	166,6
Програмне забезпечення	21 126	2	2	1 760,5
Всього				

Розробка програмного забезпечення ведеться орієнтовно 2 місяці.

6. Витрати на силову електроенергію $В_е$ розраховуються за формулою (формула 4.6):

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

Де W_{yi} – встановлена потужність обладнання на певному етапі розробки, кВт;

t_i – тривалість роботи обладнання на етапі дослідження, год;

$Ц_e$ – вартість 1 кВт-години електроенергії, грн; (вартість електроенергії визначається за даними енергопостачальної компанії).

$K_{вп i}$ – коефіцієнт, що враховує використання потужності, $K_{вп i} <1, = 0,1$;

η_i – коефіцієнт корисної дії обладнання, $\eta_i <1, = 0,9$.

$$Ц_е = (Ц_{опт} + Ц_{розп} + Ц_{пост}) \cdot \left(1 + \frac{ПДВ}{100\%}\right)$$

Де:

$Ц_{опт}$ - середня оптова ціна електроенергії, яка визначається оператором ринку (без ПДВ), 4,34837 грн за 1 кВт·год;

$Ц_{розп}$ - вартість розподілу електроенергії окремою енергорозподільною компанією (без ПДВ), 1,76978 грн за 1 кВт·год;

$Ц_{пост}$ - вартість постачання електроенергії від енергорозподільної компанії до конкретного споживача (без ПДВ), 0,13136 грн за 1 кВт·год.

ПДВ - величина податку на додану вартість, %, у 2023 році ПДВ=20%.

$$Ц_е = (4,34837 + 1,76978 + 0,13136) \cdot \left(1 + \frac{20\%}{100\%}\right) = 7,5 \text{ грн.}$$

Проведені розрахунки необхідно звести до таблиці.

Таблиця 4.8 - Витрати на електроенергію

Найменування обладнання	Встановлена потужність, кВт	Тривалість роботи, год	Сума, грн
Ноутбук	0,15	400	392,2

Роутер	0,04	400	104,6
Лампи освітлення	0,1	400	261,48
Всього			496,8

$$B_e = \sum_{i=1}^{n} \frac{0{,}29 \cdot 400 \cdot 7{,}5 \cdot 0{,}1}{0{,}9} = 96{,}6$$

7. Інші витрати.

Інші витрати, які охоплюють витрати, які не знайшли відображення у зазначених статтях витрат і можуть бути віднесені безпосередньо на собівартість досліджень за прямими ознаками. Витрати за статтею «Інші витрати» розраховуються як 100% від суми основної заробітної плати розробника за формулою (формула 4.7):

$$I_в = (З_о + З_р) \cdot \frac{Н_{ів}}{100\%}$$

де $Н_{ів}$ – норма нарахування за статтею «*Інші витрати*».

$$I_в = 171\ 739{,}13 \cdot 1 = 171\ 739{,}13 \text{ грн.}$$

8. Накладні (загальновиробничі) витрати

До статті «Накладні (загальновиробничі) витрати» належать: витрати на винахідництво та раціоналізацію; послуг банків; витрати, пов’язані з освоєнням виробництва продукції; витрати на науково-технічну інформацію та рекламу та ін.

Витрати за статтею «Накладні (загальновиробничі) витрати» розраховуються як 100% від суми основної заробітної плати розробника за формулою (формула 4.8):

$$В_{нзв} = (З_о + З_р) \cdot \frac{Н_{нзв}}{100\%}$$

де $Н_{нзв}$ – норма нарахування за статтею «*Накладні (загальновиробничі) витрати*».

Тому, показник $В_{нзв}$ буде наступним:

$$B_{нзв}=171\ 739{,}13\cdot 1=171\ 739{,}13 \text{ грн.}$$

9. Витрати на проведення науково-дослідної роботи розраховуються як сума всіх попередніх статей витрат за формулою (формула 4.9):

$$B_{заг}=З_р+З_{дод}+З_н+A_{обл}+B_е+I_в+B_{нзв}$$

$В_{заг}$ = 171 739,13 + 17 173,9 + 41 560,86 + 11 927 + 96,6 + 171 739,13 + 171 739,13 = 585 975,75 грн.

Загальні витрати *ЗВ* на завершення науково-дослідної (науково-технічної) роботи та оформлення її результатів розраховуються за формулою (формула 4.10):

$$ЗВ = \frac{B_{заг}}{\eta}$$

де η – коефіцієнт, який характеризує етап (стадію) виконання науково-дослідної роботи. Так, науково-технічна розробка знаходиться на стадії розробки дослідного зразка, то η=0,5, тому:

$$ЗВ = \frac{585\ 975{,}75}{0{,}5} = 1\ 171\ 951{,}5 \text{ грн.}$$

4.3 Розрахунок економічної ефективності науково-технічної розробки за її можливої комерціалізації потенційним інвестором

Розглянемо розрахунок економічної ефективності розробки програмного засобу для використання масовим споживачем.

В цьому випадку майбутній економічний ефект буде формуватися на основі таких даних:

ΔN – збільшення кількості споживачів продукту, в аналізовані періоди часу, від покращення його певних характеристик,

тобто:

1 рік – 1 000;

2 рік – 1 500;

3 рік – 3 000.

N – кількість споживачів які використовували аналогічний продукт у році до впровадження результатів нової науково-технічної розробки, тобто 1 000;

$Ц_б$ – вартість програмного продукту у році до впровадження результатів розробки, тобто 5 000;

$\pm\Delta Ц_о$ – зміна вартості програмного продукту (зростання чи зниження) від впровадження результатів науково-технічної розробки в аналізовані періоди часу, тобто 999 грн;

λ – коефіцієнт, який враховує сплату потенційним інвестором податку на додану вартість. У 2023 році ставка податку на додану вартість становить 20%, а коефіцієнт λ=0,8333;

ρ – коефіцієнт, який враховує рентабельність інноваційного продукту (послуги), ρ=0,3;

ϑ – ставка податку на прибуток, який має сплачувати потенційний інвестор, у 2023 році ϑ=18%.

$$\Delta П_i=\left(\pm\Delta Ц_o \cdot N + Ц_б \cdot \Delta N\right)_i \cdot \lambda \cdot \rho \cdot \left(1 - \frac{\vartheta}{100}\right)$$

1 рік: $\Delta П_i=(999 \cdot 1\,000 + 5\,999 \cdot 1\,000)_i \cdot 0{,}8333 \cdot 0{,}3 \cdot \left(1 - \frac{18}{100}\right)=$ 1 399 600

2 рік: $\Delta П_i=(999 \cdot 1\,000 + 5\,999 \cdot (1000+1\,500)_i \cdot 0{,}8333 \cdot 0{,}3 \cdot \left(1 - \frac{18}{100}\right)=$ 3 199 300

3 рік: $\Delta П_i=(999 \cdot 1\,000 + 5\,999 \cdot (1000+1500+ 3\,000)_i \cdot 0{,}8333 \cdot 0{,}3 \cdot \left(1 - \frac{18}{100}\right)=$6 798 700

Далі розраховують приведену вартість збільшення всіх чистих прибутків ПП, що їх може отримати потенційний інвестор від можливого впровадження та комерціалізації науково-технічної розробки:

$$ПП = \sum_{i=1}^{T} \frac{\Delta П_i}{(1+\tau)^t}$$

де $\Delta П_i$ – збільшення чистого прибутку у кожному з років, протягом яких виявляються результати впровадження науково-технічної розробки, грн;

T – період часу, протягом якого очікується отримання позитивних результатів від впровадження та комерціалізації науково-технічної розробки, роки;

τ – ставка дисконтування, за яку можна взяти щорічний прогнозований рівень інфляції в країні, τ=0,10;

t – період часу (в роках) від моменту початку впровадження науково-технічної розробки до моменту отримання потенційним інвестором додаткових чистих прибутків у цьому році.

$$1 \text{ рік - } ПП = \sum_{i=1}^{T} \frac{1\,399\,600}{(1+0,1)^1} = 1\,272\,363,6$$

$$2\text{рік - } ПП = \sum_{i=1}^{T} \frac{3\,199\,300}{(1+0,1)^2} = 2\,644\,049,6$$

$$3\text{рік - } ПП = \sum_{i=1}^{T} \frac{6\,798\,700}{(1+0,1)^3} = 5\,107\,963,9$$

ПП за 3 роки = 9 024 377,1

Далі розраховують величину початкових інвестицій PV, які потенційний інвестор має вкласти для впровадження і комерціалізації науково-технічної розробки. Для цього можна використати формулу:

$$PV = k_{інв} \cdot ЗВ$$

Де $k_{інв}$ – коефіцієнт, що враховує витрати інвестора на впровадження науково-технічної розробки та її комерціалізацію. Це можуть бути витрати на підготовку приміщень, розробку технологій, навчання персоналу, маркетингові заходи тощо; зазвичай $k_{інв}$=3;

$ЗВ$ – загальні витрати на проведення науково-технічної розробки та оформлення її результатів, грн.

$$PV = 3 \cdot 1\,171\,951{,}5 = 3\,515\,854{,}5$$

Тоді абсолютний економічний ефект $E_{інв}$ або чистий приведений дохід (NPV, Net Present Value) для потенційного інвестора від можливого впровадження та комерціалізації науково-технічної розробки становитиме:

$$\text{Е}_{\text{абс}} = \text{ПП} - PV$$

де *ПП* – приведена вартість зростання всіх чистих прибутків від можливого впровадження та комерціалізації науково-технічної розробки, грн;

PV – теперішня вартість початкових інвестицій, грн.

$$\text{Е}_{\text{абс}} = 9\,024\,377{,}1 - 3\,515\,854{,}5 = 5\,508\,522{,}6$$

Для остаточного прийняття рішення з цього питання необхідно розрахувати внутрішню економічну дохідність $E_в$ або показник внутрішньої норми дохідності (IRR, Internal Rate of Return) вкладених інвестицій та порівняти її з так званою бар'єрною ставкою дисконтування, яка визначає ту мінімальну внутрішню економічну дохідність, нижче якої інвестиції в будь-яку науково-технічну розробку вкладати буде економічно недоцільно.

Внутрішня економічна дохідність інвестицій $E_в$, які можуть бути вкладені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки, розраховується за формулою:

$$\text{Е}_{\text{в}} = \sqrt[\text{Тж}]{1 + \frac{\text{Е}_{\text{абс}}}{PV}} - 1$$

де $\text{Е}_{\text{абс}}$ – абсолютний економічний ефект вкладених інвестицій, грн;

PV – теперішня вартість початкових інвестицій, грн;

$T_ж$ – життєвий цикл науково-технічної розробки, тобто час від початку її розробки до закінчення отримування позитивних результатів від її впровадження: 3 роки.

$$\text{Е}_{\text{в}} = \sqrt[3]{1 + \frac{5\,508\,522{,}6}{3\,515\,854{,}5}} - 1 = 0{,}6$$

Далі визначаємо бар'єрну ставку дисконтування $\tau_{мін}$, тобто мінімальну внутрішню економічну дохідність інвестицій, нижче якої кошти у впровадження науково-технічної розробки та її комерціалізацію вкладатися не будуть.

Мінімальна внутрішня економічна дохідність вкладених інвестицій $\tau_{мін}$ визначається за формулою:

$$\tau_{\text{мін}} = d + f$$

де d – середньозважена ставка за депозитними операціями в комерційних банках; в 2023 році в Україні d=0,16;

f – показник, що характеризує ризикованість вкладення інвестицій; зазвичай величина f=0,05.

$$\tau_{\text{мін}} = 0{,}16 + 0{,}05 = 0{,}21$$

Порівнюючи величини $E_в$ та $\tau_{\text{мін}}$, бачимо, що перший показник більший за другий, а отже потенційний інвестор може бути зацікавлений у фінансуванні впровадження науково-технічної розробки та виведенні її на ринок, тобто в її комерціалізації.

Далі розраховуємо період окупності інвестицій $T_{ок}$ (DPP, Discounted Payback Period), які можуть бути вкладені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки:

$$T_{ок} = \frac{I}{E_в} = \frac{1}{0{,}6} = 1{,}66$$

Як бачимо, показник є меншим 3-х років, то це свідчить про комерційну привабливість науково-технічної розробки і може спонукати потенційного інвестора профінансувати впровадження цієї розробки та виведення її на ринок.

4.4 Висновки до розділу

У цьому розділі було проведено аналіз потенціалу комерційного успіху програмного продукту, який базується на нейронній мережі Хеммінга та спрямований на покращення процесу оцінювання вразливості інформаційної

безпеки.

Здійснено технологічний аудит, в якому взяли участь три незалежні експерти. Результати вказують на вищий, ніж середній, рівень комерційного потенціалу розробки, що було підтверджено порівняльним аналізом з аналогічним продуктом на ринку.

Загальна консенсус експертів вказує на те, що нова розробка є високоякісною та конкурентоспроможною. Рівень комерційного потенціалу розробки, становить 45,6 бала, що відповідає рівню «високий».

Згідно із розрахунками всіх статей витрат на виконання науково-дослідної, дослідно-конструкторської та конструкторсько-технологічної роботи загальні витрати на розробку складають 1 171 951,5 грн.

Розрахована абсолютна ефективність вкладених інвестицій в сумі 5 508 522,6 грн. свідчить про отримання прибутку інвестором від комерціалізації програмного продукту.

Термін окупності вкладених у реалізацію проекту інвестицій становить менше 3 років, що також свідчить про доцільність фінансування нової розробки. Отже, проаналізувавши отримані економічні показники, можна вважати, що запропонована розробка програмного засобу має високий комерційний потенціал, а тому є доцільною для подальшого впровадження.

ВИСНОВКИ

В магістерській кваліфікаційній роботі здійснюється дослідження розробки та застосування моделі оцінювання вразливості інформаційної безпеки за допомогою нейронної мережі Хеммінга як інструменту штучного інтелекту.

Одним із інструментів для здійснення діяльності в сфері інформаційної безпеки є використання штучного інтелекту. Використання штучного інтелекту в інформаційній безпеці приводить до значного підвищення ефективності захисту від кіберзагроз завдяки автоматизації процесів виявлення, аналізу та реагування на потенційні загрози. ШІ дозволяє оперативно виявляти аномалії у мережевому трафіку та активації, розпізнавати нові види кібератак, ідентифікувати зразки шкідливого коду та здійснювати аналіз лог-файлів. Магістерська кваліфікаційна робота присвячена дослідженню застовування засобів штучного інтелекту для оцінювання вразливості інформаційної безпеки.

У першому розділі було проведено аналіз теоретичних аспектів у вибраній галузі. Досліджено актуальність предметної області, розглянуто особливості вразливостей інформаційної системи та оцінювання вразливості інформаційної безпеки. Також визначено подальші напрямки досліджень, які були розглянуті в даній роботі.

У другому розділі було запропоновано структурну та математичні моделі процесу оцінювання вразливості рівня інформаційної безпеки засобами системного підходу. Запропоновано метод відображення множини вхідних рішень на множину вихідних рішень, що на відміну існуючого підходу дозволяє засобами нейронної мережі Хеммінга підвищити ефективність такого процесу. Проведений детальний аналіз мережі Хеммінга в контексті забезпечення інформаційної безпеки розкриває її можливості надійного виявлення помилок та відновлення цілісності даних. Це стало ключовим фактором для забезпечення надійності обміну інформацією в умовах постійних кібератак та технічних аномалій.

Третій розділ описує використання розробленого програмного застосунку на основі розробленої моделі із застосуванням нейронної мережі Хеммінга, який проявив значний потенціал у покращенні ефективності та точності оцінювання вразливості інформаційної безпеки. Її адаптована структура дозволяє гнучко конфігурувати параметри оцінювання, забезпечуючи високу реактивність до змін у загрозах кібербезпеки. Програмний застосунок показав адекватність складених математичної моделі та методу її формалізації.

У четвертому розділі дослідження проведено аналіз економічної доцільності впровадження розробленого програмного засобу. Зазначені отримані економічні показники, які свідчать про високий комерційний потенціал запропонованої розробки. Отже, на підставі аналізу можна зробити висновок, що програмний засіб є ефективним та доцільним для подальшого впровадження.

Потенційні Сфери Використання:

Системи Фінансової Безпеки. Розроблені методи можуть бути успішно впроваджені в системи фінансової безпеки для захисту від кіберзагроз та маніпуляцій.

Медична Інформаційна Система. Застосування в області медичних інформаційних систем для забезпечення конфіденційності та цілісності пацієнтських даних.

Корпоративна Кібербезпека. Використання методів в корпоративних інформаційних системах для захисту важливої корпоративної інформації.

Магістерська робота виявляється важливим кроком у напрямку впровадження інтелектуальних методів в сфері управління інформаційною безпекою. Отримані результати свідчать про ефективність та перспективність використання нейронної мережі Хеммінга для вдосконалення оцінювання вразливості інформаційної безпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Вознюк Є. В. SWOT-аналіз стану інформаційної безпеки України. *Науковий часопис НПУ імені М. П. Драгоманова*, 2021. Т. 22. № 30. С. 116 – 124 URL: https://enpuir.npu.edu.ua/bitstream/handle/123456789/36755/Vozniuk_116-124.pdf?sequence=1&isAllowed=y (дата звернення: 15.11.2023).

2. Ромака В.А. та ін. Аудит інформаційної безпеки: підручник. Львів : СПОЛОМ, 2015. 363 с.

3. Kabbas A., Alharthi A, Munshi A. Artificial Intelligence Applications in Cybersecurity. *IJCSNS International Journal of Computer Science and Network Security*. VOL.20 No.2, Fabruary 2020. P. 120-124. URL: http://paper.ijcsns.org/07_book/202002/20200216.pdf (дата звернення: 23.11.2023).

4. Jeschke S. et al. Industrial Internet of Things and Cyber Manufacturing Systems. Cham. *Springer International Publishing Switzerland*. Vol. 3. 2017. P. 3–19. URL: https://link.springer.com/chapter/10.1007/978-3-319-42559-7_1 (дата звернення: 23.11.2023).

5. В. В. Карпінець, О. І. Костюченко, П. В. Павловський, А. В. Приймак, С. В. Юхименко. Забезпечення захищеності користувача від несанкціонованого доступу до інформації засобами гібридного гіпервізора : *Оптико-електронні інформаційно-енергетичні технології*, 2018. № 2. С. 34-43. URL: http://nbuv.gov.ua/UJRN/oeiet_2017_2_6 (дата звернення: 15.11.2023).

6. Яремчук Ю. Є., Карпінець В. В., Зоря І.С. Проблеми експлуатації та захисту інформаційно-комунікаційних систем. Тези науково-практичної конференції, м. Київ, 7 – 9 червня 2023 р., *Національний авіаційний університет. – К.: Вид-во НАУ*. 2023. С. 49-51. URL: https://iq.vntu.edu.ua/method/getfile.php?fname=132812.pdf&x=1 (дата звернення: 23.11.2023).

7. Азарова А.О., Смоляк І.А. Інформаційна технологія для оцінювання вразливостей інформаційної безпеки сучасних ІС / Азарова А.О., Смоляк І.А. // Матеріали Міжнародної науково-практичної конференції «Молодь в науці:

дослідження, проблеми, перспективи», м. Вінниця, 11 травня – 20 травня 2024 р., – 2023. URL: https://conferences.vntu.edu.ua/index.php/mn/mn2024/paper/viewFile/19660/16275 (дата звернення: 08.12.2023).

8. Artificial Intelligence (AI) In Cyber Security Market Will Reach to USD 30.9 Billion By 2025: *Zion Market Research*. веб-сайт. URL: https://www.globenewswire.com/news-release/2019/08/28/1907655/0/en/Artificial-Intelligence-AI-In- Cyber-Security-Market-Will-Reach-to-USD-30-9-Billion-By-2025-Zion-Market-Research.html (дата звернення: 15.11.2023).

9. Архипов О. Є. Вступ до теорії ризиків : інформаційні ризики : монографія. Київ : Нац. акад. СБУ, 2015. 248 с. URL: https://drive.google.com/file/d/1YyY2JE6SmFPpEEdWBB9MZZR4sPFqXNgn/view (дата звернення: 15.11.2023).

10. Єжова Л. Ф. Економічні аспекти ризиків інформаційної безпеки *Сучасна спеціальна техніка*. 2011. № 3(26). С. 80 – 91. URL: https://elar.naiau.kiev.ua/server/api/core/bitstreams/a4f433c3-1ddf-41b0-92aa-459b0b724af9/content (дата звернення: 15.11.2023).

11. Глосарій: навчальний енциклопедичний словник-довідник з питань інформаційної безпеки / за заг. редакцією д. політ. н., проф. А.М. Шуляк, 2019. 580 с.

12. Pretorius B., van Niekerk B. Cyber-Security for ICS/SCADA. Int. J. *Cyber Warf. Terror*. 2016. Vol. 6, P. 1–16. URL: https://www.researchgate.net/publication/305416756_Cyber-Security_for_ICSSCADA_A_South_African_Perspective/link/5ccaec3792851c8d22146ef4/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19 (дата звернення: 15.11.2023).

13. Герт Крюгер. Стандарти інформаційної безпеки – огляд. *Dqsglobal*. веб-сайт. URL: https://www.dqsglobal.com/uk-ua/navchajtesya/blog/standarti-informacijnoyi-bezpeki-oglyad (дата звернення: 15.11.2023).

14. Лужецький В.А., Кожухівський А.Д., Войтович О.П. Основи інформаційної безпеки : навчальний посібник. Вінниця. ВНТУ, 2013. – 221 с. URL: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/21843/osnovy-inf-bezp-2013.pdf?sequence=1&isAllowed=y (дата звернення: 15.11.2023).

15. Cherdantseva Y. and Hilton J.: Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals. In: Organizational, Legal, and Technological Dimensions of Information System Administrator. Almeida F., Portela, I. (eds.). *IGI Global Publishing*, 2013 P. 32. URL: https://www.igi-global.com/gateway/chapter/80717 (дата звернення: 15.11.2023).

16. Коваленко, Ю. О. Забезпечення інформаційної безпеки на підприємстві. *Економіка промисловості*, 2010. С. 123–129. URL: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/econpr_2010_3_20.pdf (дата звернення: 15.11.2023).

17. Корпань Я.В. Класифікація загроз інформаційній безпеці в комп'ютерних системах при віддаленій обробці даних. *Реєстрація, зберігання і обробка даних*. 2015. Т. 17, № 2. С. 39-46. URL: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/rzod_2015_17_2_6.pdf (дата звернення: 15.11.2023).

18. Будько М.М. Визначення залишкового ризику при оцінці захищеності інформації в інформаційно-обчислювальних системах. *Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні*. Вип. 8. 2004. С. 20-26. URL: http://old.pnzzi.kpi.ua/8/08_p20.pdf (дата звернення: 15.11.2023).

19. Лагун А., Кухарська Н. Ризики інформаційної безпеки IT-підприємства. Захист інформації і безпека інформаційних систем : *VII Міжнародна науково-технічна конференція*, 30–31 травня 2015 року. Львів, 2015. С. 1-2. URL: https://sci.ldubgd.edu.ua/bitstream/123456789/750/1/11.doc (дата

звернення: 15.11.2023).

20. NIST Special Publication 800-30. Risk Management Guide for Information Technology Systems. 2012. P. 95. URL: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf (дата звернення: 15.11.2023).

21. Messerschmitt, D. G. & C. Szyperski. Marketplace Issues in Software Planning and Design. *IEEE Software*. 21 (3): 62–70. CiteSeerX 10.1.1.57.9389. 2014. P. 62-70. URL: https://www.researchgate.net/publication/220092838_Marketplace_Issues_in_Software_Planning_and_Design (дата звернення: 15.11.2023).

22. Tay K. M.; Lim C.P. On the use of fuzzy inference techniques in assessment models: part II: industrial applications. *Fuzzy Optimization and Decision Making*. 2008. 7 (3). P. 283–302. URL: https://www.proquest.com/docview/223338400 (дата звернення: 15.11.2023).

23. . ДСТУ IEC/ ISO 31010:2013. Керування ризиком. Методи загального оцінювання ризику. [Чинний від 2014-07-01]. Мінекономрозвитку України Вид. офіц. Київ, 2015. 73 с. (Інформація та документація).

24. Доценко І.О. Якісні методи оцінки ризиків в системі управлінням підприємством. *Матеріали міжнародної науково-практичної конференції «Тенденції управління фінансовими та інноваційними процесами в умовах ринкових перетворень»*. Вінниця, 2012. С. 283-285. URL: https://elar.khmnu.edu.ua/server/api/core/bitstreams/2a2a1a73-c84c-4a2e-af8b-0a333c0e131a/content (дата звернення: 15.11.2023).

25. Концепція розвитку штучного інтелекту в Україні : затв. розпорядження Кабінету міністрів України від 02.12.2020 № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text (дата звернення: 15.11.2023).

26. Leveraging artificial intelligence to maximize critical infrastructure cybersecurity. : веб-сайт. URL:

https://www.thalesgroup.com/en/worldwide/security/magazine/leveraging-artificial-intelligence-maximize-critical-infrastructure (дата звернення: 15.11.2023).

27. Віннікова І. І., Марчук С. В. Кіберризики як один із видів сучасних ризиків у діяльності малого та середнього бізнесу та управління ними. *Східна Європа: Економіка, бізнес та управління*. Вип. 5 (16). 2018. С. 110 – 114. URL: http://easterneurope-ebm.in.ua/journal/16_2018/21.pdf (дата звернення: 15.11.2023).

28. Терейковський І. А. Нейромережева методологія розпізнавання інтернет-орієнтованого шкідливого програмного забезпечення. *Безпека інформації*. Т. 19, № 1. 2013, С. 24–28. URL: http://nbuv.gov.ua/j-pdf/bezin_2013_19_1_6.pdf (дата звернення: 15.11.2023).

29. Рогоза П., Єсін В. Використання нейронної мережі замість бази знань у експертній системі детектору зловмисного трафіку до веб-ресурсів. *Комп'ютерні науки та кібербезпека*. № 1. 2022 С. 6-15. URL: https://doi.org/10.26565/2519-2310-2022-1-01 (дата звернення: 15.11.2023).

30. Корченко, О. Г., Терейковський, І. А., Дзюбаненко, А. В. (2014). Сучасні нейромережеві методи та моделі оцінки параметрів безпеки ресурсів інформаційної системи. Вип. 16 №. 3. 2014. С. 223-232. URL: https://jrnl.nau.edu.ua/index.php/ZI/article/view/7539/8597 (дата звернення: 15.11.2023).

31. Global Risks Report 2022. *World Economic Forum* : веб-сайт. URL: https://www.weforum.org/publications/global-risks-report-2022/in-full/chapter-3-digital-dependencies-and-cyber-vulnerabilities/ (дата звернення: 23.11.2023).

32. Визначення доцільності інвестування з використанням апарату нейронної мережі Хеммінга [Текст] / А. О. Азарова, Д. І. Катєльніков, Д. М. Бершов, Д. А. Резчиков // Матеріали міжнародної науково-практичної конференції «Інвестиційні пріоритети епохи глобалізації: вплив на національну економіку та окремий бізнес», Дніпропетровськ, 14-15 лютого 2008 р. – Дніпропетровськ, 2008. – Т. 3. – С. 26–27. URL: http://ir.lib.vntu.edu.ua/handle/123456789/11842 (дата звернення: 23.11.2023).

33. Nivedita James Palatty. 160 Cybersecurity Statistics 2023. Astra. URL: https://www.getastra.com/blog/security-audit/cyber-security-statistics/.

34. Cybersecurity - Ukraine | Statista Market Forecast. Statista : веб-сайт. URL: https://www.statista.com/outlook/tmo/cybersecurity/ukraine (дата звернення: 23.11.2023).

35. Методичні вказівки до виконання економічної частини магістерських кваліфікаційних робіт / Уклад. : В. О. Козловський, О. Й. Лесько, В. В. Кавецький. – Вінниця : ВНТУ, 2021. – 42 с.

ДОДАТКИ

Додаток А

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

ЗАТВЕРДЖУЮ
Голова секції «Управління
інформаційною
Безпекою» кафедри МБІС
д.т.н., професор
Юрій ЯРЕМЧУК
“20” Вересня 2023 р.

ТЕХНІЧНЕ ЗАВДАННЯ

до магістерської кваліфікаційної роботи на тему:

Вдосконалення процесу оцінювання вразливості інформаційної безпеки засобами штучного інтелекту

08-72.МКР.011.00.075.ТЗ

Керівник магістерської кваліфікаційної роботи
к.т.н., професор
Азарова А.О.

Вінниця – 2023 р.

1. Найменування та область застосування

Вдосконалення процесу оцінювання вразливості інформаційної безпеки засобами штучного інтелекту. Область застосування: оцінювання вразливості інформаційної безпеки.

2. Підстава для розробки

Розробка виконується на основі наказу ректора ВНТУ №203 від 18.09.2022 р.

3. Мета та призначення розробки

3.1 Мета розробки: Вдосконалення процесу оцінювання вразливості інформаційної безпеки засобами штучного інтелекту та розроблення програмного засобу для його практичної реалізації.

3.2 Призначення: програмний засіб виконує оцінювання вразливості інформаційної безпеки.

4. Джерела розробки

4.1 Савченко В.А., Шаповаленко О.Д. Основні напрями застосування технологій штучного інтелекту у кібербезпеці. Сучасний захист інформації. 2020. № 4 (44). 6-11 с. URL: https://journals.dut.edu.ua/index.php/dataprotect/article/view/2456/2356 (дата звернення: 23.11.2023).

4.2 Kabbas A., Alharthi A, Munshi A. Artificial Intelligence Applications in Cybersecurity. IJCSNS International Journal of Computer Science and Network Security. VOL.20 No.2, Fabruary 2020. P. 120-124. URL: http://paper.ijcsns.org/07_book/202002/20200216.pdf (дата звернення: 23.11.2023).

4.3 Вознюк Є. В. SWOT-аналіз стану інформаційної безпеки України. Науковий часопис НПУ імені М. П. Драгоманова, 2021. Т. 22. № 30. С. 116 – 124 URL: https://enpuir.npu.edu.ua/bitstream/handle/123456789/36755/Vozniuk_116-124.pdf?sequence=1&isAllowed=y (дата звернення: 15.11.2023).

4.4 Єжова Л. Ф. Економічні аспекти ризиків інформаційної безпеки Сучасна спеціальна техніка. 2011. № 3(26). С. 80 – 91. URL:

https://elar.naiau.kiev.ua/server/api/core/bitstreams/a4f433c3-1ddf-41b0-92aa-459b0b724af9/content (дата звернення: 15.11.2023).

5. Вимоги до програми

5.1 Вимоги до функціональних характеристик:

5.1.1 Програмний засіб повинен мати зручний, легкий у використанні інтерфейс користувача;

5.1.2 Реалізація засобу не повинна вимагати спеціальних ліцензійних програмних додатків;

5.2 Вимоги до надійності:

5.2.1 Програмний засіб повинен працювати без помилок, у випадку виникнення критичних ситуацій необхідно передбачити виведення відповідних повідомлень;

5.2.2 Програмний засіб повинен виконувати свої функції.

5.3 Вимоги до складу і параметрів технічних засобів:

– процесор – Intel Core I 1500 МГц і подібні до них;

– оперативна пам’ять – не менше 2 Gb;

– середовище функціонування – операційна система сімейство Windows;

– вимоги до техніки безпеки при роботі з програмою повинні відповідати існуючим вимогам та стандартам з техніки безпеки при користуванні комп’ютерною технікою.

6. Вимоги до програмної документації

6.1 Обов’язкова поетапна інструкція для майбутніх користувачів, наведена у пункті 3.1

7. Вимоги до технічного захисту інформації

7.1 Необхідно забезпечити захист розроблюваного програмного засобу від несанкціонованого використання.

7.2 Неможливість отримання доступу незареєстрованих користувачів до інформаційних ресурсів.

8. Техніко-економічні показники

8.1 Цінність результатів використання даного проекту повинна перевищувати витрати на його реалізацію.

8.2 Має бути реалізований таким чином, щоб підходити для використання широкого загалу.

9. Стадії та етапи розробки

№ з/п	Назва етапів магістерської кваліфікаційної роботи	Початок	Закінчення
1	Визначення напрямку магістерської роботи, формулювання теми	20.09.2023	30.10.2023
2	Аналіз предметної області обраної теми	01.10.2023	11.10.2023
3	Апробація отриманих результатів	12.10.2023	16.10.2023
4	Розробка алгоритму роботи	17.10.2023	23.10.2023
5	Написання магістерської роботи на основі розробленої теми	24.10.2023	18.11.2023
6	Розробка економічної частини	19.11.2023	23.11.2023
7	Передзахист магістерської кваліфікаційної роботи	24.11.2023	25.11.2023
8	Виправлення, уточнення, корегування магістерської кваліфікаційної роботи	28.11.2023	04.12.2023
9	Захист магістерської кваліфікаційної роботи	14.12.2023	14.12.2023

10. Порядок контролю та прийому

10.1 До приймання магістерської кваліфікаційної роботи надається:

– ПЗ до магістерської кваліфікаційної роботи;

– програмний додаток;

– презентація;

– відзив керівника роботи;

– відзив опонента

Технічне завдання до виконання прийняв _____ Смоляк І.А.

Додаток Б

Лістинг фрагементів backend-частини програмного застосунку:

```
using System;
using System.IO;
class Program
{
    static void Main(string[] args)
    {
        try
        {
            if (args.Length < 1)
            {
                Console.WriteLine("Usage: HammingProgram.exe input.txt");
                return;
            }
            string inputFileName = args[0];
            if (!File.Exists(inputFileName))
            {
                Console.WriteLine($"File '{inputFileName}' not found!");
                return;
            }
            RunHammingProgram(inputFileName);
        }
        catch (Exception ex)
        {
            Console.WriteLine($"An error occurred: {ex.Message}");
        }
```

```
        finally
        {
            Console.WriteLine("Press any key to exit.");
            Console.ReadKey();
        }
    }
    static void RunHammingProgram(string inputFileName)
    {
        string[] lines = File.ReadAllLines(inputFileName);


        int N = 0;
        double[] input = null;
        double[,] vectors = null;
        int M = 0;
        double[,] weights = null;
        double[] first = null;
        double[] newSecond = null;
        double[] oldSecond = null;
        ParseInput(lines, ref N, ref input, ref vectors, ref M, ref weights, ref first, ref
newSecond, ref oldSecond);
        Console.WriteLine("Hamming Program results:");
        // Additional code if needed
    }


    static void ParseInput(string[] lines, ref int N, ref double[] input, ref double[,]
vectors,
                           ref int M, ref double[,] weights, ref double[] first,
                           ref double[] newSecond, ref double[] oldSecond)
```

```
    {
        foreach (string line in lines)
        {
            if (VerifyEmpty(line))
                continue;
            if (N == 0)
            {
                N = VerifyQuantity(line);
                input = new double[N];
                vectors = new double[100, 100];
                weights = new double[100, 100];
                first = new double[100];
                newSecond = new double[100];
                oldSecond = new double[100];
            }
            string[] tokens = line.Split(' ', StringSplitOptions.RemoveEmptyEntries);
            for (int i = 0; i < N; i++)
            {
                if (!double.TryParse(tokens[i], out input[i]))
                {
                    Console.WriteLine($"Error reading {i}th component of the input
vector!");
                    return;
                }
            }
            break;
        }
        M = -1;
```

```
    for (int lineIndex = 1; lineIndex < lines.Length; lineIndex++)
    {
        string line = lines[lineIndex];
        if (VerifyEmpty(line))
            continue;
        int k = VerifyQuantity(line);
        if (k != N)
        {
            Console.WriteLine("Input vector size and vectors vector sizes differ!");
            return;
        }
        M++;
        string[] tokens = line.Split(' ', StringSplitOptions.RemoveEmptyEntries);
        for (int i = 0; i < N; i++)
        {
            if (!double.TryParse(tokens[i], out vectors[M, i]))
            {
                Console.WriteLine($"Error reading {i}th component of the vectors
vector number {M}!");
                return;
            }
        }
    }
    Console.WriteLine($"Input vector size: {N}");
    for (int i = 0; i < N; i++)
    {
        Console.Write($"{input[i]:0.000} ");
    }
```

```
Console.WriteLine();
M++;
Console.WriteLine($"Number of vectors: {M}");
for (int j = 0; j < M; j++)
{
    for (int i = 0; i < N; i++)
    {
        Console.Write($"{vectors[j, i]:0.000} ");
    }
    Console.WriteLine();
}
Console.WriteLine();
for (int j = 0; j < M; j++)
{
    for (int i = 0; i < N; i++)
    {
        weights[j, i] = vectors[j, i] / 2.0;
    }
}
double theta = N / 2.0;
double epsilon = 1.0 / (2.0 * M);
double precision = 0.05;
for (int j = 0; j < M; j++)
{
    first[j] = 0.0;
    for (int i = 0; i < N; i++)
    {
        first[j] += weights[j, i] * input[i];
```

```
    }
    first[j] += theta;
}
int nstep = 0;
for (int j = 0; j < M; j++)
{
    oldSecond[j] = first[j];
}
do
{
    for (int j = 0; j < M; j++)
    {
        newSecond[j] = 0.0;
        for (int i = 0; i < N; i++)
        {
            if (j == i)
            {
                newSecond[j] += oldSecond[i];
            }
            else
            {
                newSecond[j] -= epsilon * oldSecond[i];
            }
        }
        newSecond[j] = FThreshold(newSecond[j]);
    }
    double maxDelta = 0;
    for (int j = 0; j < M; j++)
```

```
    {
        if (Math.Abs(newSecond[j] - oldSecond[j]) > maxDelta)
            maxDelta = Math.Abs(newSecond[j] - oldSecond[j]);
    }
    if (maxDelta < precision)
        break;
    for (int j = 0; j < M; j++)
    {
        oldSecond[j] = newSecond[j];
    }
    nstep++;
    if (nstep == MAXSTEPS)
    {
        Console.WriteLine($"Reached maximum number of steps: {nstep}");
        break;
    }

} while (true);
int maxj = -1;
double maxSecond = 0.0;
for (int j = 0; j < M; j++)
{
    if (newSecond[j] > maxSecond)
    {
        maxj = j;
        maxSecond = newSecond[j];
    }
}
```

```
if (maxj == -1)
{
   Console.WriteLine("None of the output values exceeds 0.0");
   return;
}
if (maxSecond > precision)
{
   Console.WriteLine($"Solution: class {maxj + 1} (out of {M})");
}
else
{
   Console.WriteLine("The network cannot choose between classes:");
   for (int j = 0; j < M; j++)
   {
      if (newSecond[j] > 0.0)
         Console.WriteLine($"Class {j + 1}");
   }
}
Console.WriteLine();
Console.WriteLine("Outputs of the second layer neurons:");
for (int j = 0; j < M; j++)
{
   Console.WriteLine($"y({j + 1}) = {newSecond[j]:0.000}");
}
Console.WriteLine();
Console.WriteLine($"theta={theta} epsilon={epsilon} precision={precision}");
// Calculate and display parameters and Hamming code
CalculateParameters(input);
```

```
}
static void CalculateParameters(double[] components)
{
    double a1 = FunctionA1(components);
    double a2 = FunctionA2(components);
    double a3 = FunctionA3(components);
    double a4 = FunctionA4(components);
    double a5 = FunctionA5(components);
    double a6 = FunctionA6(components);
    double a7 = FunctionA7(components);
    double a8 = FunctionA8(components);
    double a9 = FunctionA9(components);

    Console.WriteLine($"a1: {a1}");
    Console.WriteLine($"a2: {a2}");
    Console.WriteLine($"a3: {a3}");
    Console.WriteLine($"a4: {a4}");
    Console.WriteLine($"a5: {a5}");
    Console.WriteLine($"a6: {a6}");
    Console.WriteLine($"a7: {a7}");
    Console.WriteLine($"a8: {a8}");
    Console.WriteLine($"a9: {a9}");

    int hammingCode = ComputeHammingCode(a1, a2, a3, a4, a5, a6, a7, a8, a9);

    Console.WriteLine($"Hamming Code: {hammingCode}");
}
```

```
static int ComputeHammingCode(params double[] parameters)
{
    int low = -1;
    int medium = -1;
    int high = 1;

    int code = 0;

    for (int i = 0; i < parameters.Length; i++)
    {
        if (parameters[i] == 1)
            code |= high << i;
        else if (parameters[i] == 2)
            code |= medium << i;
        else if (parameters[i] == 3)
            code |= low << i;
    }

    return code;
}

// Replace these functions with your actual calculations
static double FunctionA1(double[] components)
{
    // Implement your logic for a1 calculation
    return 0.0;
}
```

```
static double FunctionA2(double[] components)
{
    // Implement your logic for a2 calculation
    return 0.0;
}
static double FunctionA3(double[] components)
{
    // Implement your logic for a3 calculation
    return 0.0;
}
static double FunctionA4(double[] components)
{
    // Implement your logic for a4 calculation
    return 0.0;
}
static double FunctionA5(double[] components)
{
    // Implement your logic for a5 calculation
    return 0.0;
}
static double FunctionA6(double[] components)
{
    // Implement your logic for a6 calculation
    return 0.0;
}
static double FunctionA7(double[] components)
{
    // Implement your logic for a7 calculation
```

```
    return 0.0;
}

static double FunctionA8(double[] components)
{
    // Implement your logic for a8 calculation
    return 0.0;
}

static double FunctionA9(double[] components)
{
    // Implement your logic for a9 calculation
    return 0.0;
}
static bool VerifyEmpty(string line)
{
    // Implement your logic for verifying empty lines
    return string.IsNullOrWhiteSpace(line);
}
static int VerifyQuantity(string line)
{
    // Implement your logic for verifying quantity
    return 0;
}
static double FThreshold(double value)
{
    // Implement your threshold function
    return value >= 0 ? 1.0 : -1.0;
```

```
    }
    const int MAXSTEPS = 1000;
    // ... existing code ...
}
```

Лістинг HTML коду:

```
<!DOCTYPE html>
<html lang="uk">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Оцінювання вразливості інформаційної безпеки</title>
    <style>
    </style>
</head>
<body>
    <h1>Оцінювання вразливості інформаційної безпеки</h1>
    <form id="hammingForm">
        <label for="a1">Вразливості автентифікації та авторизації:</label>
        <select id="a1" name="a1">
            <option value="">Оберіть</option>
            <option value="1">використання слабких паролів обсягом до 7 
символів</option>
            <option value="2">використання паролів із низькою ентропією, таких як 
"password123" обсягом до від 7 до 9 символів</option>
            <option value="3">використання паролів із високою ентропією, обсягом 
від 9 до 12 символів і більше</option>
        </select>
        <br><br>

        <label for="a2">Вразливості захищеності веб-додатків:</label>
        <select id="a2" name="a2">
            <option value="">Оберіть</option>
            <option value="4">відсутність механізмів безпеки веб-додатків</option>
            <option value="5">використання стандартних механізмів безпеки веб-
додатків: HTTPS, OWASP, CORS, CSP</option>
            <option value="6">використання передових технік безпеки веб-додатків: 
WAF, XSS</option>
        </select>
        <br><br>
```

```
    <label for="a3">Вразливості керування доступом:</label>
    <select id="a3" name="a3">
        <option value="">Оберіть</option>
        <option value="7">відсутність налаштувань рольового управління із обмеженням прав доступу (всі користувачі мають адміністративні привілеї)</option>
        <option value="8">використання рольового управління на підставі для об'єднаної групи користувачів</option>
        <option value="9">використання деталізованого рольового управління (застосування принципу найменших привілеїв)</option>
    </select>
    <br><br>

    <label for="a4">Вразливості шифрування даних:</label>
    <select id="a4" name="a4">
        <option value="">Оберіть</option>
        <option value="10">використання застарілих алгоритмів шифрування: DES, MD5, RSA, RC4</option>
        <option value="11">використання стандартних алгоритмів шифрування, таких як AES або RSA, з ключами менше 128 біт для AES або менше 2048 біт для RSA</option>
        <option value="12">використання сучасних алгоритмів шифрування з великою довжиною та унікальністю ключів, для AES з ключами довжиною 256 біт або RSA з ключами довжиною 3072 біт і більше</option>
    </select>
    <br><br>

    <label for="a5">Вразливості мережевої безпеки:</label>
    <select id="a5" name="a5">
        <option value="">Оберіть</option>
        <option value="13">відсутність брандмауерів</option>
        <option value="14">використання брандмауерів для фільтрації та контролю трафіку типу WAF (Web Application Firewall)</option>
        <option value="15">комплексне використання брандмауерів типу NGFW</option>
    </select>
    <br><br>

    <label for="a6">Вразливості фізичної безпеки:</label>
    <select id="a6" name="a6">
        <option value="">Оберіть</option>
        <option value="16">відсутність контролю доступу</option>
```

```
            <option value="17">застосування контрольованого доступу</option>
            <option value="18">застосування системи доступу на підставі
біометричних показників</option>
        </select>
        <br><br>

        <label for="a7">Вразливості соціальної інженерії:</label>
        <select id="a7" name="a7">
            <option value="">Оберіть</option>
            <option value="19">відсутність проведення навчання персоналу з питань
безпеки</option>
            <option value="20">ситуативне проведення навчання персоналу з питань
безпеки після інцидентів порушення інформаційної безпеки</option>
            <option value="21">постійне проведення навчання персоналу з питань
безпеки</option>
        </select>
        <br><br>

        <label for="a8">Вразливості системи виявлення та запобігання
вторгнень:</label>
        <select id="a8" name="a8">
            <option value="">Оберіть</option>
            <option value="22">відсутність систем виявлення вторгнень</option>
            <option value="23">використання звичайних систем виявлення
вторгнень: IDS, IPS</option>
            <option value="24">використання інтелектуальних систем з
автоматичним реагування на загрози: SIEM, Palo Alto Networks
Panorama</option>
        </select>
        <br><br>

        <label for="a9">Вразливості втрати даних:</label>
        <select id="a9" name="a9">
            <option value="">Оберіть</option>
            <option value="25">відсутність резервного копіювання даних</option>
            <option value="26">резервне копіювання даних в ручному
режимі</option>
            <option value="27">автоматизоване резервне копіювання даних</option>
        </select>
        <br><br>

        <button type="button" onclick="runHammingProgram()">Виконати
оцінювання</button>
```

```
    </form>

    <div id="resultContainer">
        <!-- Тут відображатимуться результати програми Хеммінга -->
    </div>

    <!-- Поле для відображення рівня вразливості інформаційної безпеки -->
    <div id="securityVulnerabilityLevel">
        <label for="securityVulnerability">Рівень вразливості інформаційної
безпеки:</label>
        <input type="text" id="securityVulnerability" readonly>
    </div>

     <script>
        function runHammingProgram() {
            var form = document.getElementById('hammingForm');
            var formData = new FormData(form);

            fetch('HammingProgramHandler.ashx', {
                method: 'POST',
                body: formData
            })
            .then(response => response.json())
            .then(data => {
                var resultContainer = document.getElementById('resultContainer');
                resultContainer.innerHTML = '<h2>Результати програми
Хеммінга:</h2>';

            })
            .catch(error => console.error('Помилка:', error));

            // Приклад встановлення значення рівня вразливості інформаційної
безпеки (для демонстрації)
            var securityVulnerabilityInput =
document.getElementById('securityVulnerability');
            securityVulnerabilityInput.value = ' ';
        }
    </script>
</body>
</html>
```

Додаток В
Ілюстративний матеріал

Магістерська кваліфікаційна робота

Вдосконалення процесу оцінювання вразливості інформаційної безпеки засобами штучного інтелекту

Виконав : ст. групи 1КІТС -22М Смоляк І.А.

Керівник : к.т.н ., професор каф. МБІС Азарова А.О.

Вступ

Актуальність: Одним із інструментів для здійснення діяльності в сфері інформаційної безпеки є використання штучного інтелекту (далі – ШІ). Використання штучного інтелекту в інформаційній безпеці приводить до значного підвищення ефективності захисту від кіберзагроз завдяки автоматизації процесів виявлення, аналізу та реагування на потенційні загрози. ШІ дозволяє оперативно виявляти аномалії у мережевому трафіку та активації, розпізнавати нові види кібератак, ідентифікувати зразки шкідливого коду та здійснювати аналіз лог-файлів. Усі ці процеси відбуваються в режимі реального часу, допомагаючи зменшити час реакції на загрози, а також скорочує необхідність постійного нагляду від людей. Такий підхід сприяє покращенню загального рівня безпеки інформаційних систем та даних, запобігає атакам та мінімізує можливі збитки внаслідок кіберінцидентів.

Метою роботи є вдосконалення процесу оцінювання вразливості інформаційної безпеки із застосуванням інструментів штучного інтелекту.

Практична цінність роботи: розроблено програмний засіб для оцінювання вразливості інформаційної безпеки засобами нейронної мережі Хеммінга.

Нейронна мережа Хеммінга як інструмент штучного інтелектудля оцінювання вразливості інформаційної безпеки

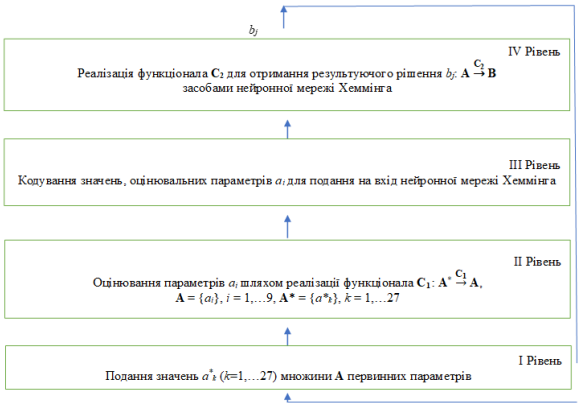
- Нейронна мережа Хеммінга є потужним інструментом в арсеналі кібербезпеки для оцінювання та виявлення вразливості інформаційних систем і мереж. Мережа використовує принципи аналізу нормальної поведінки системи та автоматизованого виявлення будь-яких відхилень від цієї норми. Цей підхід виявляється особливо ефективним у вимірюванні безпеки в реальному часі, допомагаючи реагувати на потенційні загрози миттєво.

- Використання нейронної мережі Хеммінга дозволить отримати класифіковані та сегментовані дані як результат здійснення відповідного оцінювання вразливості інформаційної безпеки, що в свою чергу покаже рівень та тенденції вразливості інформаційної безпеки. Нейронна мережа Хеммінга також дозволить виконати співставлення образу вхідних векторів які описують вразливості інформаційної безпеки із найближчим еталонним вектором, що описує певну вразливість інформаційної безпеки

Розроблення структурної моделі процесу оцінювання вразливості інформаційної безпеки із застосуванням нейронноїмережі Хеммінгу

Структурна модель процесу оцінювання вразливості інформаційної безпеки з використанням нейронної мережі Хеммінгу уможливлює процес відображення множини вхідних оцінювальних параметрів впливу на множину вихідних рішень.

Досліджувана множина оцінювальних параметрів	
1. Вразливості автентифікації та авторизації	6. Вразливості фізичної безпеки
2. Вразливості захищеності веб-додатків	7. Вразливості соціальної інженерії
3. Вразливості керування доступом	8. Вразливості системи виявлення та запобігання вторгнень
4. Вразливості шифрування даних	9. Вразливості втрати даних
5. Вразливості мережевої безпеки	



Структурна модель процесу оцінювання вразливості інформаційноїбезпеки із застосуванням нейронної мережі Хеммінгу

Математична модель для оцінювання вразливості інформаційної безпеки за допомогою нейронної мережі Хеммінга

Математична модель дозволяє відобразити множину $\mathbf{A}^*$ первинних вхідних параметрів a^*_k на множину **B** вихідних рішень b_j за допомогою реалізації функціоналів $\mathbf{C}_1$ та $\mathbf{C}_2$:

$$\mathbf{A}^* \xrightarrow{\mathbf{C}_1} \mathbf{A} \xrightarrow{\mathbf{C}_2} \mathbf{B},\ \mathbf{A}^* = \{a^*_k\},\ \mathbf{A} = \{a_i\},\ i=1,..,n,\ \mathbf{B}=\{b_j\},\ j=1,..,m,\ \mathbf{A} = \mathbf{C}_1(\mathbf{A}^*),\ \mathbf{B} = \mathbf{C}_2(\mathbf{A}).$$

$a_1 = f(a^*_1,\ldots a^*_3)$; $a_2 = f(a^*_4,\ldots,a^*_6)$; $a_3 = f(a^*_7,\ldots,a^*_9)$; $a_4 = f(a^*_{10},\ldots,a^*_{12})$; $a_5 = f(a^*_{13},\ldots,a^*_{15})$;
$a_6 = f(a^*_{16},\ldots,a^*_{18})$; $a_7 = f(a^*_{19},\ldots,a^*_{21})$; $a_8 = f(a^*_{22},\ldots a^*_{24})$; $a_9 = f(a^*_{25},\ldots,a^*_{27})$.

Назва оцінювального параметра a_i	Назва первинного вхідного параметра a^*_k	Характеристичний терм, який описує значення параметра a_i
a_1 – вразливості автентифікації та авторизації	a^*_1 – використання слабких паролів обсягом до 7 символів	В – високий рівень вираженості параметра a_i
	a^*_2 – використання паролів із низькою ентропією, таких як «password123» обсягом до від 7 до 9 символів	С – Середній рівень вираженості параметра a_i
	a^*_3 – використання паролів із високою ентропією, обсягом від 9 до 12 символів і більше	Н – Низький рівень вираженості параметра a_i
a_2 – вразливості захищеності веб - додатків	a^*_4 – відсутність механізмів безпеки веб -додатків	В
	a^*_5 – використання стандартних механізмів безпеки веб -додатків: HTTPS, OWASP, CORS, CSP	С
	a^*_6 – використання передових технік безпеки веб -додатків: WAF, XSS	Н
a_3 – вразливості керування доступом	a^*_7 – відсутність налаштувань рольового управління із обмеженням прав доступу (всі користувачі мають адміністративні привілеї)	В
	a^*_8 – використання рольового управління для об'єднаної групи користувачів	С
	a^*_9 – використання деталізованого рольового управління (застосування принципу найменших привілеїв)	Н
a_4 – вразливості шифрування даних	a^*_{10} – використання застарілих алгоритмів шифрування: DES, MD5, RSA, RC4	В
	a^*_{11} – використання стандартних алгоритмів шифрування, таких як AES або RSA, з ключами менше 128 біт для AES або менше 2048 біт для RSA	С
	a^*_{12} – використання сучасних алгоритмів шифрування з великою довжиною та унікальністю ключів, для AES з ключами довжиною 256 біт або RSA з ключами довжиною 3072 біт і більше	Н
a_5 – вразливості мережевої безпеки	a^*_{13} – відсутність брандмауерів	В
	a^*_{14} – використання брандмауерів для фільтрації та контролю трафіку типу WAF (Web Application Firewall)	С
	a^*_{15} – комплексне використання брандмауерів типу NGFW	Н
a_6 – вразливості фізичної безпеки	a^*_{16} – відсутність контролю доступу	В
	a^*_{17} – застосування контрольованого доступу	С
	a^*_{18} – застосування системи доступу на підставі біометричних показників	Н
a_7 – вразливості соціальної інженерії	a^*_{19} – відсутність проведення навчання персоналу з питань безпеки	В
	a^*_{20} – ситуативне проведення навчання персоналу з питань безпеки після інцидентів порушення інформаційної безпеки	С
	a^*_{21} – постійне проведення навчання персоналу з питань безпеки	Н
a_8 – вразливості системи виявлення та запобігання вторгнень	a^*_{22} – відсутність систем виявлення вторгнень	В
	a^*_{23} – використання звичайних систем виявлення вторгнень: IDS, IPS	С
	a^*_{24} – використання інтелектуальних систем з автоматичним реагуванням на загрози: SIEM, Palo Alto Networks Panorama	Н
a_9 – вразливості втрати даних	a^*_{25} – відсутність резервного копіювання даних	В
	a^*_{26} – резервне копіювання даних в ручному режимі	С
	a^*_{27} – автоматизоване резервне копіювання даних	Н

Оцінювання значень параметрів a_i

Шляхом використання експертних методів та проведення анкетного опитування серед фахівців з кібербезпеки щодо питань захисту інформаційних систем, було визначено граничні значення оцінювальних показників за трьома діапазонами: Н (низький), С (середній) та В (високий). Такий підхід дозволяє систематизувати інтервали значень для кожного оцінювального параметра a_i.

Атрибути інформаційної безпеки

Типові еталони для роботи мережі Хеммінга

Вхідними параметрами мережі є отримані на рівні 2 структурної моделі значення оцінювальних параметрів a_i, що описуються характеристичними термами (Н, С, В)

№ еталону	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	b_j
1	Н	Н	Н	Н	Н	Н	Н	Н	Н	Н
2	Н	С	Н	Н	В	Н	Н	С	В	
3	С	С	С	С	С	С	С	С	С	С
4	Н	В	В	С	В	В	В	С	Н	В
5	В	В	В	В	В	В	В	В	В	

№ еталона	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	b_j
1	-1-1	-1-1	-1-1	-1-1	-1-1	-1-1	-1-1	-1-1	-1-1	-1-1
2	-1-1	-1 1	-1-1	-1-1	1 1	-1-1	-1-1	-1 1	1 1	
3	-1 1	-1 1	-1 1	-1 1	-1 1	-1 1	-1 1	-1 1	-1 1	-1 1
4	-1-1	1 1	1 1	-1 1	1 1	1 1	1 1	-1 1	-1-1	1 1
5	1 1	1 1	1 1	1 1	1 1	1 1	1 1	1 1	1 1	

Нейронна мережа Хеммінга використовуєтільки числові значення «1» та «-1», то пропонується закодувати значення 3 характеристичнихтермів – Н, С, В, що описують значення вхідних функцій a_i, відповідним двійковим кодом

Використання мережі Хеммінга полягає у подаванні на її вхід вектору із 18 закодованих значень 9 оцінювальних параметрів a_i та порівняння цього вектору з найближчим до нього вектором із таблиці еталонів.

Отже, нейронна мережа Хеммінга ідентифікує еталон, який є найближчим до вектора поданого на її вхід. номер даного еталону, що попередньо подано, дозволяє визначити результуюче рішення щодо рівня вразливості інформаційної безпеки b_j (j = 1,…,3) ІС.

Етапи реалізації функціоналів C_1 та C_2 структурної моделі

- Етап 1. Подання значення a^*_k (k=1,…27) первинних вхідних параметрів, що використовуються для розрахунку функцій (оцінювальних параметрів) a_i (i =1,…9) досліджуваних інформаційних систем;

- Етап 2. Значення оцінювальних параметрів $a_1 ... a_9$ описуються конкретним характеристичним рівнем (Н – низький, С – середній, В – високий) шляхом реалізації функціоналу $\mathbf{C_1}$;

- Етап 3. Формування вхідного вектору (який складається з 18 цифр «1» та «-1») для роботи мережі Хеммінга шляхом кодування значень оцінювальних параметрів a_i.

- Етап 4. Нейронна мережаХеммінга визначає найближчий до даного вектору еталон, номер якого відповідає певному вихідному рішенню b_j.

№ компанії	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	Рівень вразливості b_j
1	Н	В	В	С	В	В	В	Н	С	Високий
2	Н	С	В	С	С	С	С	С	С	Середній
3	В	Н	Н	С	Н	Н	Н	В	Н	Низький
4	Н	В	В	С	С	В	В	С	Н	Високий
5	Н	С	С	С	В	С	С	Н	С	Середній

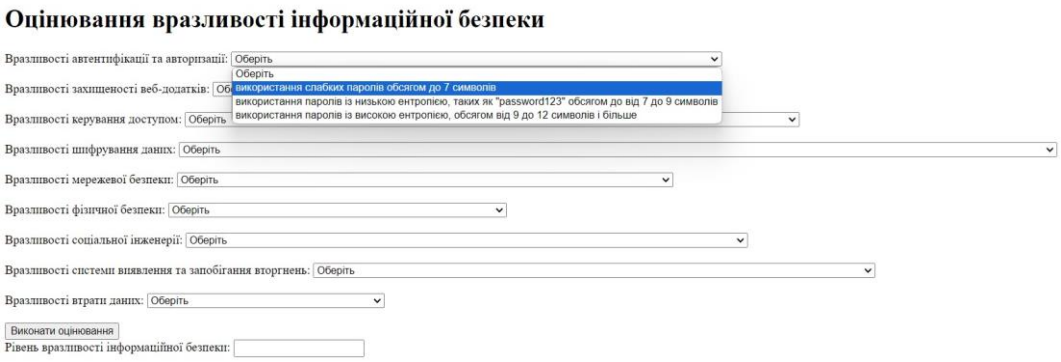
Використаннямережі Хеммінга для оцінювання рівнів вразливості інформаційноїбезпеки, які застосовуютьсяна 5 вітчизняних компаніях, що працюють у медичній та банківській сферах

ПЗ № компанії	Рівень вразливості b_j за «Nessus»	Рівень вразливості b_j за «OpenVAS»	Рівень вразливості b_j за «Metasploit»	Рівень вразливості b_j за «Wireshark»	Рівень вразливості b_j за «Burp Suite»	Рівень вразливості b_j за запропонованою IT
1	В	В	В	В	В	В
2	С	С	С	С	С	С
3	Н	Н	Н	С	Н	Н
4	В	В	В	В	В	В
5	С	С	В	С	С	С

Перевірка адекватності використаної моделі на 5 суб'єктах господарювання (у сфері медичних та банківських послуг) із отриманими для цих компаній результатами за допомогою відомих на ринку ПЗ: Nessus, OpenVAS, Metasploit, Wireshark, BurpSuite

Зображення користувацького інтерфейсу програмного застосунку для оцінювання вразливості інформаційної безпеки

Відображення первинних вхідних параметрів

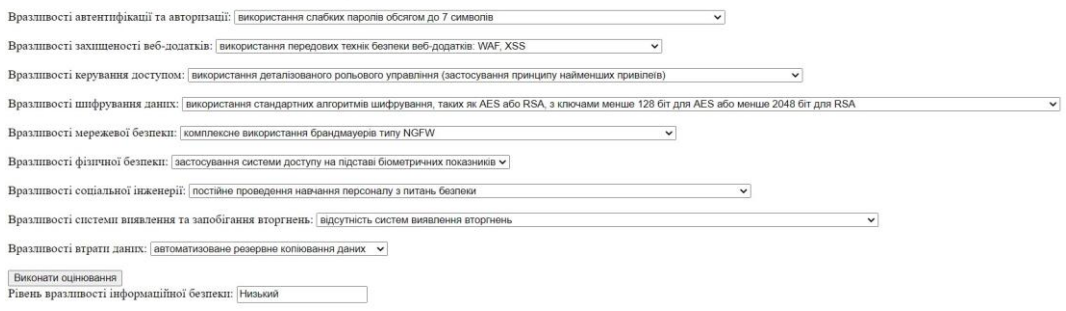


Зображення користувацького інтерфейсу програмного застосунку для оцінювання вразливості інформаційної безпеки

Зображення загального вигляду оцінювальних показників вразливості

Зображення користувацького інтерфейсу програмного застосунку для оцінювання вразливості інформаційної безпеки

Зображення результату процесу оцінюванняінформаційної безпеки



Апробація магістерської кваліфікаційної роботи

- Результати дослідження було апробовано на Міжнародній науково-практичній конференції «Молодь в науці: дослідження, проблеми, перспективи» (м. Вінниця, 2023).
- По темі дослідження було опубліковано тези доповідей: Азарова А.О., Смоляк І.А. Інформаційна технологія для оцінювання вразливостей інформаційної безпеки сучасних ІС / Азарова А.О., Смоляк І.А. // Матеріали Міжнародної науково-практичної конференції «Молодь в науці: дослідження, проблеми, перспективи», м. Вінниця, 11 травня – 20 травня 2024 р.,– 2023. URL: https://conferences.vntu.edu.ua/index.php/mn/mn2024/paper/viewFile/19660/16273 (дата звернення: 08.12.2023).

Висновки

В магістерській кваліфікаційній роботі здійснюється дослідження розробки та застосування моделі оцінювання вразливості інформаційної безпеки за допомогою нейронної мережі Хеммінга як інструменту штучного інтелекту.

Було проведено аналіз теоретичних аспектів у вибраній галузі. Досліджено актуальність предметної області, розглянуто особливості вразливостей інформаційної системи та оцінювання вразливості інформаційної безпеки. Також визначено подальші напрямки досліджень, які були розглянуті в даній роботі.

Запропоновано структурну та математичні моделі процесу оцінювання вразливості рівня інформаційної безпеки засобами системного підходу. Запропоновано метод відображення множини вхідних рішень на множину вихідних рішень, що на відміну існуючого підходу дозволяє засобами нейронної мережі Хеммінга підвищити ефективність такого процесу. Проведений детальний аналіз мережі Хеммінга в контексті забезпечення інформаційної безпеки розкриває її можливості надійного виявлення помилок та відновлення цілісності даних. Це стало ключовим фактором для забезпечення надійності обміну інформацією в умовах постійних кібератак та технічних аномалій.

Описано використання розробленого програмного застосунку на основі розробленої моделі із застосуванням нейронної мережі Хеммінга, який проявив значний потенціал у покращенні ефективності та точності оцінювання вразливості інформаційної безпеки. Її адаптована структура дозволяє гнучко конфігурувати параметри оцінювання, забезпечуючи високу реактивність до змін у загрозах кібербезпеки. Програмний застосунок показав адекватність складених математичної моделі та методу її формалізації.

Проведено аналіз економічної доцільності впровадження розробленого програмного засобу. Зазначені отримані економічні показники, які свідчать про високий комерційний потенціал запропонованої розробки. Отже, на підставі аналізу можна зробити висновок, що програмний засіб є ефективним та доцільним для подальшого впровадження.

Магістерська робота виявляється важливим кроком у напрямку впровадження інтелектуальних методів в сфері управління інформаційною безпекою. Отримані результати свідчать про ефективність та перспективність використання нейронної мережі Хеммінга для вдосконалення оцінювання вразливості інформаційної безпеки.

Додаток Г
ПРОТОКОЛ
ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ
НА НАЯВНІСТЬ ТЕКСТОВИХ
ЗАПОЗИЧЕНЬ

Назва роботи: Вдосконалення процесу оцінювання вразливості інформаційної безпеки засобами штучного інтелекту

Тип роботи: магістерська кваліфікаційна робота
(БДР, МКР)

Підрозділ: Кафедра менеджменту та безпеки інформаційних систем
Факультет менеджменту та інформаційної безпеки
(кафедра, факультет)

Показники звіту подібності Unicheck

Оригінальність 91 % Схожість 9 %

Аналіз звіту подібності (відмітити потрібне):

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

2. Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.

3. 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.

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

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи _____ Смоляк І.А.
(підпис) (прізвище, ініціали)

Керівник роботи _____ Азарова А.О.
(підпис) (прізвище, ініціали)