Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

на тему
Метод оцінювання ефективності засобів захисту інформації розподілених інформаційних систем

Галузь знань 12 – Інформаційні технології

Спеціальність 125 –Кібербезпека

КРМКБ. 220182.22.01.09 ПЗ

Виконав: студент 2 курсу, група КБм-22-1 _____ Димбовський М.В.
Підпис

Керівник доц., к. т. н, доцент _____ Джулій В.М.
Підпис

Нормоконтролер старший викладач _____ Мостовий С.В.
Підпис

До захисту допускаю:
Зав. кафедри кібербезпеки, к.т.н., доц _____ Кльоц Ю.П.
Підпис

11 12 2023р.

Хмельницький, 2023

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра КІБЕРБЕЗПЕКИ

Освітній рівень МАГІСТР

Галузь знань 12 ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Спеціальність 125 КІБЕРБЕЗПЕКА

Освітня програма КІБЕРБЕЗПЕКА

ЗАТВЕРДЖУЮ

Зав. кафедри Ю.П. Кльоц

"30" 08 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Димбовському Максиму Вячеславовичу
(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) Метод оцінювання ефективності засобів захисту інформації розподілених інформаційних систем

Науковий керівник Джулій Володимир Миколайович, к.т.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджена наказом № 30 ректора університету, додаток №25 від 15.08.2023

2. Строк подання студентом проекту (роботи) на кафедру 05.12.2023.

3. Вихідні дані до проекту (роботи) Провести дослідження розподілених інформаційних систем, провести аналіз загроз та атак безпеці конфіденційної інформації, аналіз перспективних методів моделювання загроз інформаційній безпеці та оцінки ефективності систем безпеки інформації. Провести оцінку ефективності запропонованого методу.

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Дослідження сучасного стану моделей та методів побудови систем, загроз, атак безпеки даних. Модель визначення актуальних загроз безпеці конфіденційної інформації. Метод оцінки ефективності систем захисту конфіденційної інформації. Реалізація методу оцінки ефективності системи захисту конфіденційної інформації розподілених інформаційних систем

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

6. Консультанти розділів дипломного проекту (роботи)

Розділ	Прізвище, ініціали і посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Мостовий С.В. Старший викладач кафедри кібербезпеки		

7. Дата видачі завдання: «01»___лютого_____2023_р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	*Примітка*
1	Ґрунтовне ознайомлення та дослідження предметної галузі	21.02.2023	Виконано
2	Визначення змісту, структури магістерської роботи	11.03. 2023	Виконано
3	Опрацювання першого розділу магістерської роботи	4.04. 2023	Виконано
4	Опрацювання статті за результатами дослідження	3.05. 2023	Виконано
5	Опрацювання другого розділу магістерської роботи	2.06. 2023	Виконано
6	Опрацювання третього розділу магістерської роботи	2.09. 2023	Виконано
7	Опрацювання четвертого розділу магістерської роботи	4.10. 2023	Виконано
8	Підготовка та опрацювання ілюстративного матеріалу	7.11. 2023	Виконано
9	Оформлення магістерської роботи графічної та текстової частини	18.11. 2023	Виконано
10	Попередній захист магістерської роботи	17.11. 2023	Виконано
11	Захист магістерської роботи на засіданні ЕК	5.12. 2023	Виконано

Студент _____ М.В. Димбовський
Підпис Ініціали, прізвище

Керівник проекту (роботи) _____ В.М. Джулій
Підпис Ініціали, прізвище

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Метод оцінювання ефективності засобів захисту інформації розподілених інформаційних систем».

Автор роботи: Димбовський Максим Вячеславович

Керівник роботи: к.т.н. доц. Джулій Володимир Миколайович

Загальний обсяг роботи: 85 сторінок, 15 рисунків, 15 таблиць, 3 додатки, 59 посилань.

Ключові слова: моделі, алгоритми, розподілені інформаційні системи, конфіденційна інформація, ефективність системи.

Мета роботи полягає в підвищенні якості оцінки ефективності систем захисту розподілених інформаційних систем за рахунок визначення достатніх та необхідних показників.

Для досягнення поставленої мети в магістерській роботі необхідно вирішити наступні задачі: провести дослідження розподілених інформаційних систем; підвищити якість визначення атак та загроз інформаційній безпеці в розподілених інформаційних системах за рахунок визначення достатніх та необхідних показників для мінімізації помилки роботи методу; провести оцінку ефективності запропонованого методу.

Практична цінність роботи. Запропонований метод оцінки ефективності системи захисту, надає компаніям можливість оцінювати ефективність системи захисту інформації на всіх етапах життєвого циклу розподілених інформаційних систем в реальному часі, дозволяє вносити коригування до проектних рішень системи захисту для нейтралізації загроз безпеки даних та дотримання вимог щодо захисту інформації, враховуючи, при цьому, фінансову складову при створенні системи безпеки.

11.12.2023

ANNOTATION

Theme of qualification work: "Method of evaluating the effectiveness of information protection means of distributed information systems.".

Author of the work: Dymbovskyi Maxim Vyacheslavovich

Mentor: Ph.D. Dguliy Volodymyr Mykolayovych

Total volume of work: 85 pages, 15 figures, 15 tables, 3 appendices, 59 links.

Keywords: models, algorithms, distributed information systems, confidential information, system efficiency.

The purpose of the work is to improve the quality of the assessment of the effectiveness of distributed information system protection systems by determining sufficient and necessary indicators.

In order to achieve the set goal in the master's work, the following tasks must be solved: conduct research on distributed information systems; to improve the quality of identification of attacks and threats to information security in distributed information systems by determining sufficient and necessary indicators to minimize the error of the method; evaluate the effectiveness of the proposed method.

Practical value of work. The proposed method of evaluating the effectiveness of the protection system provides companies with the opportunity to evaluate the effectiveness of the information protection system at all stages of the life cycle of distributed information systems in real time, allows making adjustments to the design solutions of the protection system to neutralize data security threats and comply with information protection requirements, taking into account this, the financial component in the creation of a security system.

11.12.2023

ЗМІСТ

стор.

ВСТУП…….……..…….. 4
1 ДОСЛІДЖЕННЯ СУЧАСНОГО СТАНУ МОДЕЛЕЙ ТА МЕТОДІВ ПОБУДОВИ СИСТЕМ, ЗАГРОЗ, АТАК БЕЗПЕКИ ДАНИХ……...…… 10
1.1 Дослідження методів та моделей побудови інформаційних систем 10
1.2 Дослідження ІТ - архітектури та систем захисту конфіденційної інформації …… 15
1.3 Аналіз методик та методів оцінки ефективності систем захисту конфіденційної інформації ……..……. 19
1.4 Постановка задачі ……...…..……...……..……...……... 23
2 МОДЕЛЬ ВИЗНАЧЕННЯ АКТУАЛЬНИХ ЗАГРОЗ БЕЗПЕЦІ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ…..……...…….…..……. 25
2.1 Моделювання зловмисника та загроз безпеки конфіденційної інформації……... 25
2.2 Генерація набору даних для визначення актуальних загроз безпеці конфіденційної інформації…… 36
2.3 Модель визначення актуальних загроз безпеці конфіденційним даним ……..… 38
2.4 Висновки ……..……..……..…….. 44
3 МЕТОД ОЦІНКИ ЕФЕКТИВНОСТІ СИСТЕМ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ ……. 46
3.1 Показники оцінки ефективності та вимоги до систем захисту конфіденційної інформації ……...…… 46
3.2 Метод оцінки ефективності системи захисту конфіденційної інформації …….…..……..... 52
3.3 Оцінка ефективності методу захисту конфіденційної інформації… 56

3.4 Висновки ……..……...…… 61
4 РЕАЛІЗАЦІЯ МЕТОДУ ОЦІНКИ ЕФЕКТИВНОСТІ СИСТЕМИ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМ ……..……... 62
4.1 Оцінка відповідності систем захисту до вимог безпеки конфіденційної інформації …….…….. 62
4.2 Алгоритм оцінки ефективності систем захисту розподілених інформаційних систем …….…….. 64
4.3 Реалізація методу оцінки ефективності системи захисту інформації розподілених інформаційних систем ……... 69
4.4 Висновки ……..……..……..……..... 77
ВИСНОВКИ…….……...…….……..……. 78
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ….……..…….……..…… 80
ДОДАТОК А Фрагмент коду створення та навчання нейронної мережі, визначення помилки навчання мережі……. 86
ДОДАТОК Б Копії наукових публікацій ……...……...……..……... 88
ДОДАТОК В Презентація кваліфікаційної роботи ……..…….…… 106

ВСТУП

Інформаційна безпека стає все більш важливою та значущою сферою національної безпеки України, що відображено у Доктрині інформаційної безпеки України, затвердженої Указом Президента України від 25 лютого 2017 року № №47/2017 [21]. Відповідно до Доктрини, на теперішній час, інформаційні технології набули глобального характеру і стали невід'ємною частиною всіх сфер діяльності держави, суспільства та особистості. Розширення сфер застосування інформаційних технологій, на сучасному етапу, значно розширює перспективи розвитку нових інформаційних загроз та атак. Зарубіжні спеціальні служби розширюють інформаційно-психологічний вплив, спрямований на дестабілізацію соціальної та внутрішньополітичної ситуації в різних регіонах світу, що призводить, в свою чергу, до порушення територіальної цілісності та підриву суверенітету інших держав. Засоби масової інформації збільшують об’єми матеріалів та поширюють їх в мережі Інтернет, які містять упереджену оцінку державної політики. Значно зростають масштаби комп'ютерної злочинності, в першу чергу, у кредитно-фінансовій сфері суспільства. У сфері оборони держави, в економічній сфері, в області суспільної та державної безпеки, в галузі науки, освіти та технологій, в області рівноправного стратегічного партнерства та стратегічної стабільності спостерігаються визначені державою стратегічні цілі для забезпечення конфіденційної інформації ефективного стану безпеки [21, 23 -25].

Одночасно, з розвитком та зростанням інформаційних технологій зростає і кількість засобів та методів порушень стану безпеки конфіденційної інформації. Протягом останніх років спостерігається різке зростання кількості витоків конфіденційної інформації, зі звіту експертно-аналітичного центру групи компаній SafeNet [7,38]. Змінити ситуацію, до забезпечення інформаційної безпеки, можливо шляхом розробки нових методів, підходів які можуть надати від сучасних загроз безпеці інформації надійний захист [1,2,13].

Задача забезпечення безпеки конфіденційної інформації стає найактуальнішею, що обумовлено, зростанням комп'ютерних атак та витоків інформації, що відображаються у статистичних даних скоєння злочинів у сфері високих технологій [15,40,41,47], зростання кримінальної активності з використанням сучасних комунікаційних пристроїв та інтернету у 2021 році склало 39% [16,17]. Кожен двадцятий злочин, відповідно, від числа всіх зареєстрованих злочинів кваліфікується як кіберзлочин. Серед усіх скоєних у 2021 році комп'ютерних злочинів лідирують, які передбачають розповсюдження, використання, створення комп'ютерних «вірусів», а також відповідальність за неправомірний доступ до комп'ютерної конфіденційної інформації. Друге місце в незаконній електронній діяльності, займає шахрайство з використанням сервісів онлайн-платежів [9-11]. Кількість таких правопорушень у першому півріччі 2022 р. зросла у 8 разів. Іншим прикладом зростання витоків інформації є щорічні звіти міжнародної компанії Group-IB, в яких йдеться про активність проурядових організацій, які займаються проведенням атак (кіберзлочинами) на користь своїх держав. Відповідно до звіту "Hi-Tech Crime Trends 2021-2022", відзначається збільшення кібератак з використанням відповідного шпигунського програмного забезпечення, бекдорів, шифрувальників, зростання фінансового шахрайства з використанням соціальної інженерії та збільшення атак на банки, мотив кіберзлочинців - крадіжка інформації, за яку можна отримати винагороду чи грошей [3-7,47].

Для досягнення цілей забезпечення безпеки конфіденційної інформації необхідно: організувати ефективне створення системи захисту інформації (системи безпеки інформації), ефективне моделювання (визначення переліку) актуальних загроз інформаційної безпеки, визначення актуального порушника, а також надати можливість проводити якісну оцінку ефективності системи безпеки (захисту) інформації. Однією з найважливіших задач забезпечення безпеки конфіденційної інформації є оцінка ефективності системи захисту (безпеки). У зв'язку з цим метою магістерської роботи (дослідження) - підвищення якості

оцінки ефективності систем захисту (безпеки) розподілених інформаційних систем за рахунок визначення достатніх та необхідних показників оцінки з використанням сучасних (перспективних) інформаційних технологій, що дозволяють найбільш ефективно вирішувати наступні задачі: визначення параметрів роботи адаптивних продукційних нечітких нейронних систем, що найбільш підходять для вирішення поставлених задач, застосування технологій Data Science при обробці даних, алгоритмів нечіткого виведення [14-19].

Існуючі методи моделювання (визначення) актуальних загроз інформаційної безпеки та оцінки ефективності системи захисту інформації не можуть бути задіяні на всіх етапах життєвого циклу розподілених інформаційних систем - не враховують в комплексі наступні показники: IT-інфраструктура розподілених інформаційних систем, актуальні загрози інформаційної безпеки, вимог безпеки конфіденційної інформації, перелік засобів захисту конфіденційної інформації та їх вартість як важливих показників при вирішенні даних задач. Одночасно з цим, для розглянутих методів моделювання загроз інформаційної безпеки та проведення оцінки ефективності системи захисту розподілених інформаційних систем залишається мета — підвищення ефективності з огляду визначення кількості актуальних загроз інформаційної безпеки, виконання закладених вимог до безпеки інформації, зниження вартості витрат на проектування та створення системи захисту розподілених інформаційних систем, а також мінімізація (виключення) помилок експертів. Для існуючих методів залишається актуальною задача зменшення помилки середньоквадратичної роботи продукційних адаптивних нечітких нейронних систем [32-35].

На підставі проведеного аналізу можна зробити висновок про необхідність удосконалення методів оцінки ефективності системи захисту розподілених інформаційних систем.

Об'єкт дослідження - вимоги та загрози безпеці щодо захисту конфіденційної інформації.

Предмет дослідження - методи моделювання (визначення) актуальних загроз безпеці конфіденційної інформації, оцінки ефективності систем захисту конфіденційної інформації.

Метою магістерського дослідження - підвищення якості оцінки ефективності систем захисту розподілених інформаційних систем за рахунок визначення достатніх та необхідних показників.

Для досягнення поставленої мети в магістерській роботі необхідно вирішити наступні задачі:

1. Провести дослідження розподілених інформаційних систем, провести аналіз загроз та атак безпеці конфіденційної інформації, аналіз перспективних методів моделювання загроз інформаційній безпеці та оцінки ефективності систем безпеки інформації.

2. Підвищити якість визначення атак та загроз інформаційній безпеці в розподілених інформаційних системах за рахунок визначення достатніх та необхідних показників для мінімізації помилки роботи методу.

3. Провести оцінку ефективності запропонованого методу.

Наукова задача магістерського дослідження - підвищити якість оцінки ефективності системи захисту розподілених інформаційних систем, запропонувавши метод визначення актуальних загроз інформаційній безпеці та оцінки ефективності системи захисту, заснований на продукційних адаптивних нечітких нейронних мереж, за рахунок визначення достатніх та необхідних показників.

Наукова новизна результатів магістерського дослідження:

1. Запропоновано метод визначення атак та актуальних загроз безпеці конфіденційної інформації, на відміну від відомих, формує перелік актуальних загроз інформаційній безпеці, виключаючи помилки експертів.

2. Запропоновано метод оцінки ефективності систем інформаційного захисту, на відміну від відомих, заснований на нечітких адаптивних нейронних

продукційних мереж та алгоритмі нечіткого виведення із використанням IT Data Science.

Практична цінність магістерської роботи:

1. Проведений аналіз розподілених систем виявив основні аспекти технології обробки інформації, дозволив використати отримані результати дослідження при визначенні достатніх та необхідних показників моделювання (визначення) загроз інформаційній безпеці та провести оцінку ефективності системи захисту розподілених систем.

2. Запропоновий метод визначення загроз інформаційній безпеці дозволяє визначати актуальні загрози безпеці інформації мінімізує трудомісткість процесу, обчислювальні ресурси, виключаючи недоліки експертів.

3. Запропонований метод оцінки ефективності системи захисту, надає компаніям можливість оцінювати ефективність системи захисту інформації на всіх етапах життєвого циклу розподілених інформаційних систем в реальному часі, дозволяє вносити коригування до проектних рішень системи захисту для нейтралізації загроз безпеки даних та дотримання вимог щодо захисту інформації, враховуючи, при цьому, фінансову складову при створенні системи безпеки.

Методи дослідження. У магістерські роботі використано теорії ймовірності, методи неявного перебору, динамічного програмування, математичної статистики, теорії нечітких адаптивних нейронних систем, алгоритми нечіткого виводу.

Основні результати дослідження, що виносяться на захист:

1. Метод визначення актуальних загроз інформаційній безпеці.

2. Метод оцінки ефективності інформаційних систем захисту даних.

Обгрунтованість та достовірність результатів магістерського дослідження підтверджуються системним підходом до вирішення поставлених завдань, математичним обґрунтуванням результатів досліджень, обґрунтуванням обраних показників та методів визначення загроз безпеки конфіденційним даним, оцінки ефективності систем захисту, публікацією результатів роботи у провідних наукових виданнях, апробацією результатів роботи на міжнародних конференціях,

Особистий внесок. Дослідження, викладені в дипломній роботі, проведені автором при виконанні роботи в процесі наукової діяльності. Результати дипломної роботи, що виносяться на захист, отримані особисто автором, використаний в роботі запозичений матеріал позначений посиланнями.

Апробація роботи. За темою дипломної роботи ОКР «Магістр» опубліковано 1 фахова стаття, 1 теза доповідей.

Структура і обсяг роботи. Дипломна робота ОКР «Магістр» складається зі вступу, основної частини, що містить 4 розділи, висновків і списку використаних джерел посилань. Загальний обсяг роботи - 85 сторінок. Робота містить 15 рисунків та 15 таблиць. Список використаної літератури включає 59 бібліографічних джерела.

1 ДОСЛІДЖЕННЯ СУЧАСНОГО СТАНУ МОДЕЛЕЙ ТА МЕТОДІВ ПОБУДОВИ СИСТЕМ, ЗАГРОЗ, АТАК БЕЗПЕКИ ДАНИХ

1.1 Дослідження методів та моделей побудови інформаційних систем

Моделювання інформаційних систем є одним з основних методів дослідження в областях знань, науково обґрунтованим підходом оцінок характеристик інформаційних складних систем. Моделювання інформаційних систем - заміщення існуючої інформаційної системи іншою з метою отримання необхідної інформації реальної системи з використанням об'єкта-моделі інформаційної системи [14,16,19,35,58], аналогічно для проведення моделювання загроз та атак безпеки даних.

На теперішній час існує наступна класифікація типів моделювання інформаційних систем (рис. 1.1).

Рисунок 1.1 - Класифікація типів моделювання інформаційних систем

Відповідно класифікаційним ознакам моделі поділяються на: неповні, наближені повні. Залежно від характеристик у процесах, моделі поділяться на: стохастичні, детерміновані, динамічні, статичні, дискретні, дискретно-безперервні, безперервні. Статичне моделювання визначає, у будь-який момент, поведінку інформаційної системи. Детерміноване - відображає процеси, у яких відсутні випадкові дії. Динамічне моделювання відображає поведінку інформаційної системи у часі. Стохастичне - відображає імовірнісні події та процеси. Безперервне моделювання відображає безперервні процеси, дискретне - описує дискретні процеси в інформаційній системі. Моделювання дискретно - безперервне використовується при описі безперервних та дискретних процесів. Уявне використовується при моделюванні об'єктів, які існують поза умовами, їх створення або нереалізовані в визначеному інтервалі часу [31,32].

При наочному моделюванні формуються моделі інформаційної системи, що відображають процеси та явища, які протікають в системі. При гіпотетичному моделюванні викормстовується гіпотеза про закономірності процесів у реальній інформаційній системі, яка базується на причинно-наслідкових зв'язках між виходом і входом і відображає рівень знань експерта досліджуваної інформаційної системи. Гіпотетичне моделювання використовується, коли недостатні знання про інформаційну системи для побудови формальних моделей. Макетування застосовується в реальній інформаційній системі, коли процеси не піддаються фізичному моделюванню. В основі макетів лежать аналоги інформаційної системи, що базуються на причинно-наслідкових зв'язках між процесами та явищами системи. При математичному моделюванні має бути проведена формалізація цього процесу, побудовано математичну модель. Математичне моделювання – процес встановлення відповідності деякого математичного об'єкта реальної інформаційної системи– математичної моделі.

На сучасному етапі засобом моделювання інформаційних систем є засоби обчислювальної техніки. При побудові математичної моделі кожна система *S* характеризується відповідним набором властивостей, які враховують умови

взаємодії системи із зовнішнім середовищем E та відображають поведінку досліджуваної моделі системи. Модель системи S можна представити у вигляді множини величин, що описують процеси функціонування реальної інформаційної системи та утворюють наступні підмножини:

1. Сукупність внутрішніх параметрів системи: $h_k \in H, k = \overline{1, n_H}$.

2. Сукупність вихідних характеристик: $y_j \in Y, j = \overline{1, n_Y}$.

3. Сукупність вхідних впливів на систему: $x_i \in X, i = \overline{1, n_X}$.

4. Сукупність впливів зовнішнього середовища: $v_l \in V, l = \overline{1, n_V}$.

Змінні x_i, y_j, h_k, v_l - елементи підмножин, містять стохастичні і детерміновані складові, не перетинаються.

При моделюванні системи внутрішні параметри системи. впливи зовнішнього середовища, вхідні впливи є незалежними змінними, які у векторній формі мають наступний вид:

$$\vec{x}(t) = \left(x_1(t), x_2(t), ..., x_{n_X}(t) \right);$$
$$\vec{v}(t) = \left(v_1(t), v_2(t), ..., v_{n_V}(t) \right);$$
$$\vec{h}(t) = \left(h_1(t), h_2(t), ..., h_{n_H}(t) \right).$$

Вихідні характеристики інформаційної системи є залежними змінними, векторною формою мають наступний вид:

$$\vec{y}(t) = \left(y_1(t), y_2(t), ..., y_{n_Y}(t) \right).$$

Функціонування інформаційної системи S описується оператором F_S:

$$\vec{y}(t) = F_S\left(\vec{x}, \vec{v}, \vec{h}, t \right) \qquad (1.1)$$

Залежність (1.1) є законом функціонування інформаційної системи. Алгоритм функціонування системи A_S - метод отримання вихідних характеристик системи з урахуванням впливів внутрішніх параметрів системи $\vec{h}(t)$, зовнішнього середовища $\vec{v}(t)$, вхідних впливів $\vec{x}(t)$. Закон функціонування F_S інформаційної системи *S* може бути реалізований множиною різних алгоритмів функціонування A_S, різними способами.

Відношення (1.1) є математичним описом інформаційної системи моделювання *S* протягом часу *t*, математичні моделі такого типу є динамічними. Відношення (1.1) може бути реалізовано різними способами: таблично, аналітично, графічно.

Математична модель системи - кінцева підмножина змінних $\left\{\vec{x}(t),\vec{v}(t),\vec{h}(t)\right\}$ з математичними зв'язками між ними та характеристиками $\vec{y}(t)$ [24].

Дискретно детерміновані моделі системи *F*-схеми. В основі, яких лежить теорія автоматів, математична модель автомата. Автомат задається *F*- схемою:

$$F=\langle Z,X,Y,\varphi,\psi,z_0\rangle,$$

яка функціонує в дискретному автоматному часі, де *Z* - множина внутрішніх станів системи, *Y*-вихідні сигнали, *X*-вхідні сигнали, z_0 - початковий стан, $z_0 \in Z$, функція виходу $\psi(z,x)$, функція переходу $\varphi(z,x)$.

Мережеві моделі (*N* -схеми) - мережі Петрі. Для вирішення задач, пов'язаних з аналізом причинно-наслідкових зв'язків та з формалізованим описом у складних системах. Найпоширенішим формалізмом, що описує взаємодію та структуру процесів та паралельних систем використовуються мережі Петрі.

Мережа Петрі (*N*-схема) задається наступним чином:

$$N=\langle B,D,I,O\rangle,$$

де B – позиції, D – переходи, I – вхідна функція, O – вихідна функція.

Для кожного переходу $d_j \in D$ можна визначити для переходу множину вхідних позицій $I(d_j)$ і для переходу множину вихідних позицій $O(d_j)$.

Класифікація методів побудови моделей системи наведено рис. 1.2. Роглянуті методи та моделі мають свої недоліки та переваги.

Основні недоліки перерахованих моделей: будь-яка модель мінімізує пояснення можливих явищ; під час моделювання не завжди існує можливість виявлення якісних нових характеристик; як правило, необхідних даних не вистачає для налаштування моделей; статистичні моделі системи можуть бути об'єктивними в межах емпіричної множини побудови моделі.

Рисунок 1.2 - Класифікація методів побудови моделей атак

На основі проведеного дослідження, можна зробити висновок - існуючі підходи побудови моделей системи мають низку недоліків, що, своєю чергою, доводить необхідність удосконалення розглянутих моделей.

1.2 Дослідження IT - архітектури та систем захисту конфіденційної інформації

З розвитком та зростанням інформаційних технологій зростає і складність архітектури інформаційних систем. Сучасні інформаційні системи є клієнт-серверні територіально-розподілені та багаткористувацької архітектури. Програмне забезпечення на базі відкритого програмного інтерфейсу надає можливості функціональних модифікацій з використанням поширених мов програмування (TypeScript (середовище розробки dotnet.core, платформа розробки Angular)) [20,26,39].

Інформаційні системи забезпечують принцип централізованого накопичення, зберігання, багаторазового використання даних. Для забезпечення інформаційної безпеки, економії ресурсів на автоматизованих робочих місцях користувачів зберігання інформації не здійснюється. Обробка даних здійснюється на серверній частини [51,59]. Для реалізації даного підходу можуть використовуватись технології термінального доступу. Дана технологія може бути реалізована в ТТ-інфраструктурі шляхом розгортання термінальної ферми Remote Desktop Services (RDS), в даному випадку робочі профілі співробітників зберігаються на серверах термінальної ферми, що полегшує організацію доступу користувачів до ресурсів інформаційної системи, найбільш ефективно забезпечує процеси безпеки даних. Також технологія забезпечує процеси при віддаленій роботі користувачів [38,40,47]. Для розподілених інформаційних систем характерне розміщення мережевого обладнання, робочих місць користувачів,

серверних компонентів на всій території країни та за її межами. Такі системи мають складну архітектуру розташування компонентів і технологій обробки даних. Відповідно, при цьому, виникають складнощі із забезпеченням безпеки даних [27,28,39,42,49,57].

До складу розподіленої системи входять наступні компоненти:

1. Сервери, включають: спеціалізоване та прикладне програмне забезпечення, забезпечують представлення даних у виді, необхідному для автоматизованої обробки інформації; серверне обладнання.

2. Робоче місце користувачів: типові робочі місця користувача (стаціонарні персональні комп'ютери); мобільні робочі місця - мобільні телефони, планшети.

Для забезпечення захисту інформації, що передається по відкритих каналах зв'язку, використовується криптографічний захист між секціями інформаційними системами. Типова схема комплексу технічних засобів розподіленої інформаційної системи представлена на рис. 1.3.

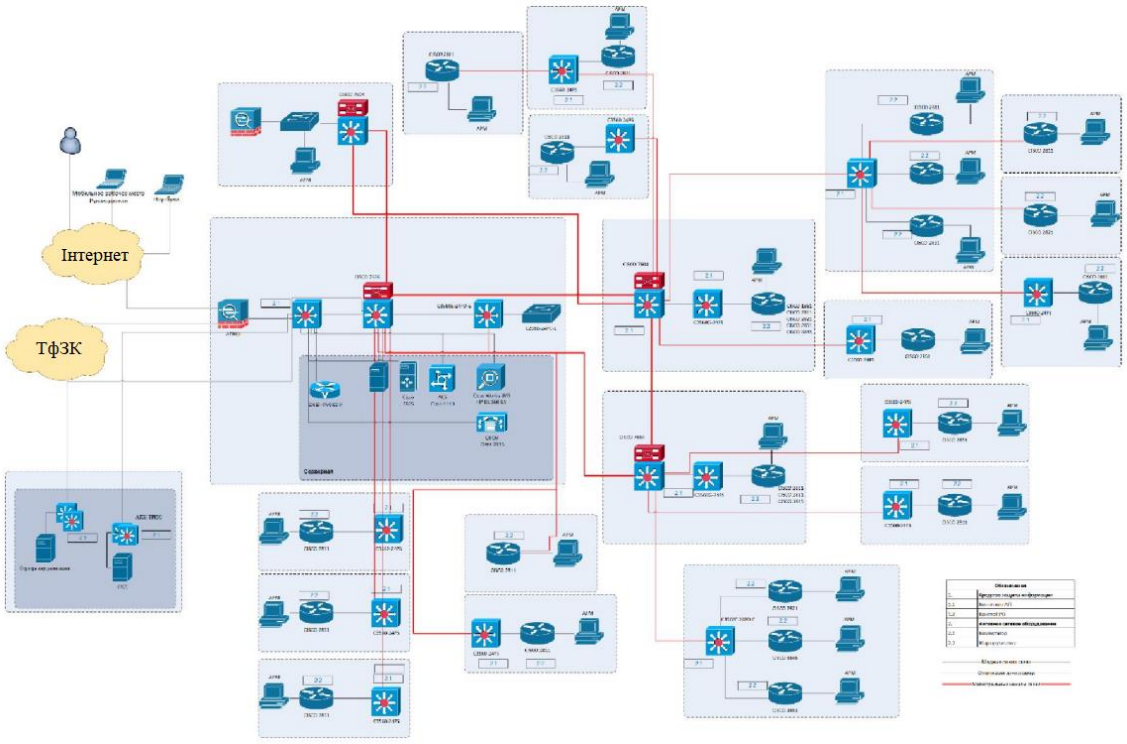


Рисунок 1.3 - Структурна схема комплексу технічних засобів розподіленої інформаційної системи

Розподілені інформаційні системи мають низку аспектів IT-інфраструктури, які необхідно враховувати при моделюванні загроз інформаційній безпеці, при формуванні показників оцінки ефективності системи інформаційної безпеки, ключовими є: канали зв'язку (незахищені мережі передачі даних), обробка інформації у центрах обробки даних, географічна розподіленість інформаційної системи, клієнт-серверні додатки, хмарні інфраструктури. Необхідно приділяти особливу увагу категоріям зловмисників у розподілених інформаційних системах, якими є внутрішні, зовнішні групи порушників [48,50,51].

Комп'ютерна атака - несанкціонований цілеспрямований вплив на ресурс, інформацію автоматизованої системи, отримання несанкціонованого доступу до даних із застосуванням програмно-апаратних, програмних засобів. Об'єкт атаки (мета атаки) елемент розподіленої інформаційної системи. На теперішній час існує множина моделей атак, засобів та методів моделювання атак. Порушник - особа, яка навмисно використовує вразливості нетехнічних та технічних заходів, засобів контролю, управління безпекою з метою компрометації чи захоплення мереж та систем, зниження доступності мережевих ресурсів, даних інформаційної системи для законних користувачів [19,30,34,53].

Основні моделі атак на розподілені системи представлені на рис. 1.4 [14,35,37]. Переваги та недоліки основних моделей атак представлені у табл. 1.1.

Таблиця 1.1 - Переваги та недоліки моделей атак

Модель	Переваги	Недоліки
1	2	3
Логічні	Обробка інцидентів та використання мов представлення знань про предметну область.	Потребує значних обчислювальних ресурсів
Графові на деревах атак	Наочність, масштабованість, адаптованість, універсальність	Складні при моделюванні циклічних атак.
Байєсівські графи	Масштабованість, адаптованість, універсальність, враховує невизначеності даних про атаки	Складні при моделюванні циклічних атак. Відсутність динамічного моделювання

Закінчення таблиці 1.1

1	2	3
Мережі Петрі	Зручність моделювання динамічних паралельних процесів, здатні відображати ймовірнісні процеси	Нездатність описувати поведінку порушника та цілі атаки
Імітаційні	Дозволяють моделювати поведінкові характеристики	Вимагають великих обчислювальних ресурсів

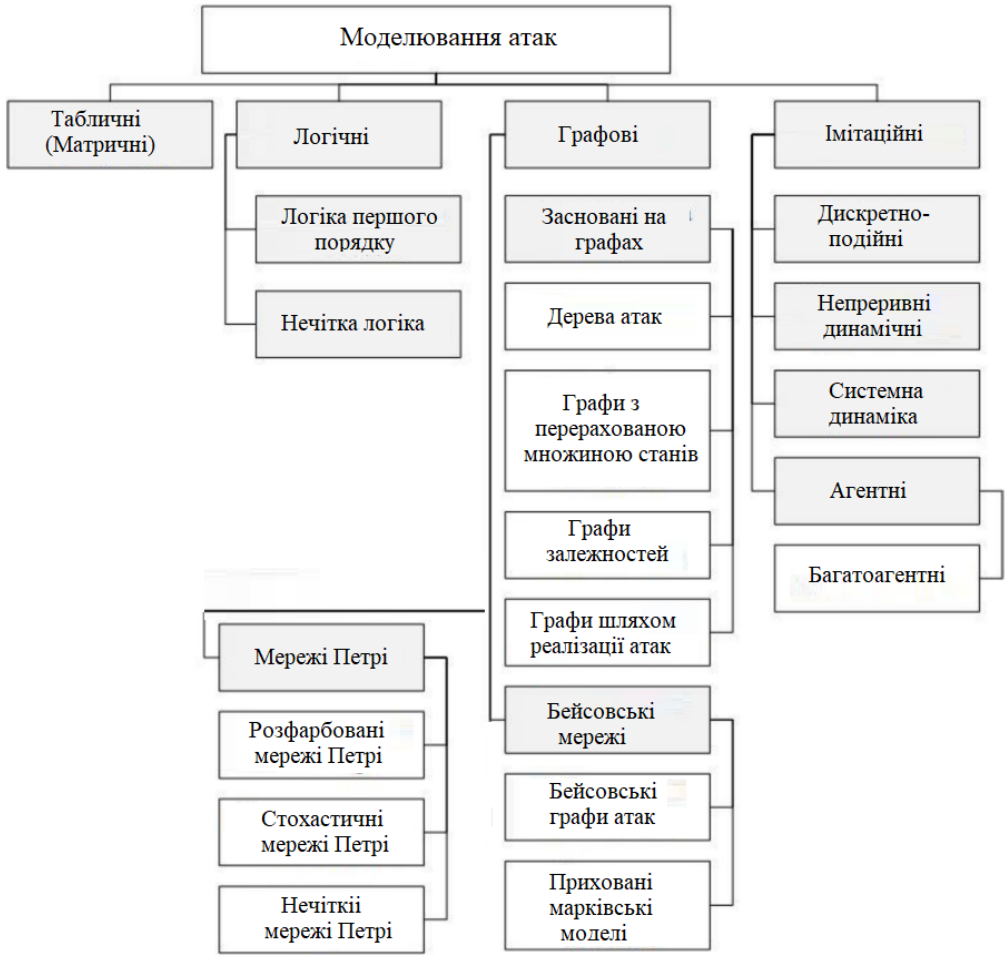


Рисунок 1.4 - Моделі атак на інформаційні системи

При розробці моделі зловмисника та моделі загроз інформаційної безпеки у розподіленої інформаційної системи необхідно враховувати вектори атак в інформаційній системі. З проведеного аналізу досліджень можна дійти висновку про необхідність враховувати недоліки методів моделювання, зокрема загрозам безпеки інформації.

1.3 Аналіз методик та методів оцінки ефективності систем захисту конфіденційної інформації

Ефективність системи захисту інформації - ступінь відповідності результатів захисту інформації меті захисту інформації. Для проведення оцінки ефективності системи захисту даних необхідно визначити метод та показники оцінки.

Основні методи оцінки ефективності захисту дакних інформаційних систем наступні: імовірнісний; статистичний; експертний; частотний; інформаційно-ентропійний; нейромережний й (багатокритеріальни); формальний (матричний); метод мінімізації ризиків; оптимізаційний (комбінаторний); багаторівневий [33,34,43].

Статистичний метод - проводиться обробка потенційних атак, загроз та їх наслідків. Показник оцінки ефективності - загроза *i*-го типу виникає в середньому за період T_i.

Ймовірнісний метод - визначається можливість відмови інформаційної системи від обробки даних в результаті проведення успішної загрози. Сумарні втрати розраховуються за формулою (1.2):

$$R = \sum_{i=1}^{2^m} \sum_{j=1}^{2^m} P\left(\frac{\vec{\gamma}}{\vec{S}}\right) P\left(\vec{S}\right) \prod\left(\vec{\gamma}, \vec{S}\right) + m, \tag{1.2}$$

де $P\left(\frac{\vec{\gamma}}{\vec{S}}\right)$- ймовірність усунення, $P\left(\vec{S}\right)$ - ймовірність стану об'єкта контролю, $\prod\left(\vec{\gamma}, \vec{S}\right)$- втрати прийняття рішення при стані об'єкта *S*, *m*- кількість виявлених загроз безпеці даних.

Частотний метод - на підставі аналізу статичної інформації визначається значення *S*, величина *V* вибирається в діапазоні від 1 до максимальної можливої суми втрат, розраховується значення показника R_i, як функції параметрів *V* і *S*. Показник оцінки ефективності системи - очікувані втрати від *i*-ї загрози (1.3):

$$R_i = F(S,V), \tag{1.3}$$

де S показник частоти виникнення загрози безпеці даних, V - умовний показник шкоди.

Експертний метод - визначається кількість n параметрів, що характеризують систему захисту розподіленої інформаційної системи. Задаються суб'єктивні значення коефіцієнтів важливості W_i, кожної з характеристик G_i призначені експертним шляхом. Розраховується значення параметра SR. Показник оцінки ефективності системи - ступінь забезпечення безпеки даних SR системи S розраховується за формулою (1.4):

$$SR_{(s,r)} = \frac{1}{n_{i-1}^{n}} W_i G_i, \tag{1.4}$$

Інформаційно-ентропійний метод - проводиться аналітичне обчислення ентропії інформаційної системи, використовуючи, при цьому, поняття згортки функції. У випадку лінійної залежності ефективність інтеграції систем в плані інформаційному вважають задовільною, інакше неефективною. Показником оцінки ефективності є величина ентропії Шеннона (1.5):

$$\psi(t) = \left(\int_0^{\tau} S_n(t-\tau) \ldots \left(\int_0^{\tau} S_3 \left(\int_0^{\tau} S_1(\tau) S_2(t-\tau)\, dt \right) dt \ldots \right) dt \right), \tag{1.5}$$

де $S_1,\ldots,S_n$ - значення ентропій інформаційних різних підсистем.

Нейромережевий метод (багатокритеріальна оцінка). Приналежність до певного рівня безпеки даних визначається в діапазоні [0,1], показники надійності є функцією прилежності: $\mu^A(x_i)$, x_i, елемент множини X - вимог щодо безпеки даних, A - множина значень, що визначають виконання вимог щодо безпеки даних. Оцінка ефективності системи захисту розподіленої інформаційної системи проводиться за чітко визначених показників. Нечіткі показники системи захисту

розподіленої інформаційної системи - лінгвістичні змінні, такі як «середній ступінь захищеності», «низький ступінь захищеності» «високий ступінь захищеності».

Метод мінімізації ризиків. Реалізується за наступними кроками: фіксація ризиків безпеки даних; індекс ризику; проводиться класифікація ризиків; визначаються методи обробки ризиків безпеки даних; розраховуються показники, що характеризують ризики; розраховуються показники економічного ефекту управління ризиками безпеки даних. Показником оцінки ефективності - показник економічного ефекту захисту даних управління ризиками. Розраховується за формулою (1.6):

$$E = \left(\sum_{i=1}^{N} M_{oi} - \sum_{i=1}^{N} M_i\right) - \left(\left(\sum_{i=1}^{N} I_{фi} + \sum_{i=1}^{N} H_{фi}\right) + \left(\sum_{j=1}^{K} I_{фні} + \sum_{j=1}^{K} H_{фні}\right)\right), \quad (1.6)$$

де M_o - сумарні ймовірні втрати без обробки ідентифікованих ризиків, M - сумарні ймовірні втрати після обробки ризиків, $I_ф$ - сумарні фактичні втрати від прояву ризиків, $I_{фн}$ - сумарні фактичні втрати від прояву ризиків, $H_{фн}$ - сумарні фактичні витрати на обробку ризиків

Матричний метод (формальні моделі захисту) реалізується наступними кроками: визначаються параметри; складається матриця відношень; перетворення матриці на двовимірну матрицю; визначаються кількісні та якісні значення показників. Показником оцінки ефективності системи є стан системи захисту, описаний параметрами: (*S, O, M*) - множини *S* -суб'єктів, *O* - об'єктів, *M* - прав доступу або (*O, H, M*), де *O* - складові та основи частини системи (технічна, нормативно-правова, організаційна), *H* - напрями захисту, *M* - етапи створення системи захисту.

Багаторівневий метод використовує модель Д. Деннінга та модель кінцевих станів Белла Ла-Падули. Стан системи захисту описується наборов категорій

конфіденційності та сукупністю рівнів конфіденційності. Метод, також використовує алгоритми нечіткої логіки [31, 32].

Комбінаторний (оптимізаційний) - вирішується задача дискретного програмування типу: максимізувати $\sum_{j=1}^{n}\left(c_j x_j\right)$ за умов:

$$\sum_{j=1}^{n}\left(a_{ij} x_j\right) \le b_i;\ i=\overline{1,m},\ x_j \in \{0,1\}\ j=\overline{1,n}.$$

Недоліки та переваги методів [33] оцінки ефективності системи захисту наведені у табл. 1.2.

Таблиця 1.2 - Недоліки та переваги методів оцінки ефективності СЗ

Метод оцінки системи захисту	Переваги	Недоліки
Статистичний	Дозволяє отримувати результати, коли не відомі параметри СЗ, дозволяє оцінювати систему будь-якої складності	Результати достовірні з певною ймовірністю, великий обсяг обробки статистичних даних
Імовірнісний	Аналізується повний спектр загроз, використання реалістичного підходу, взаємозв'язків міжелементами системи враховуються у явному виді	Складність обчислень, неможливо виявити зміну імовірнісних характеристик спостережень
Експертний	Використання у відсутності статистичних даних. Швидкість отримання результатів.	Достовірність результатів залежить від компетенцій експертів.
Багатокритеріальний ий (нейромережний)	Дозволяє враховувати велику кількість критеріїв оцінки системи. Дозволяє враховувати кількісні, якісні показники	Складність вибору оптимальної структури Відсутність формалізованих процедур
Комбінаторний (оптимізаційний)	Найбільш ефективний метод оцінки ефективності.	Складність проведення обчислень
Матричний (формальний)	Універсальний для проведення оперативної оцінки системи захисту Вимагає мінімальних обчислювальних ресурсів	Не дозволяє проводити оцінку в умовах невизначеності, великої кількості показників оцінки

Проведений аналіз досліджень показав, що існуючі методи оцінки ефективності системи захисту мають низку недоліків, що зумовлює необхідність підвищення якостей існуючих на теперішній час методів.

1.4 Постановка задачі

Визначення переліку актуальних загроз безпеці інформації, оцінка ефективності системи захисту є невід'ємною частиною життєвого циклу розподіленої інформаційної системи. Специфіка IT-інфраструктури, складність визначення зловмисника, актуальних загроз для розподіленої інформаційної системи, вибору показників, недоліки методів оцінки ефективності систем захисту, як наслідок, недостатня ефективність захисту розподілених інформаційних систем призводить до ризиків заподіяння шкоди активам власників систем. Метою магістерської роботи є підвищення якості оцінки ефективності систем захисту інформаційних за рахунок визначення достатніх та необхідних показників.

У загальному вигляді задача дослідженні може бути сформульовані наступним чином: підвищити якість методів моделювання (визначення) актуальних загроз безпеки даних за рахунок визначення достатніх і необхідних показників, автоматизувати процес для виключення помилок експертів; підвищити якість методів оцінки ефективності системи захисту визначення найкращих параметрів роботи адаптивних нейронних нечітких продукційних систем, та застосування технологій Data Science при обробці великого обсягу даних; розробити рекомендації щодо оцінки ефективності системи захисту розподілених систем; провести оцінку ефективності запропонованих методів.

Математично задачу можна формалізувати наступним чином: вибрати кращі, для вирішення поставлених задач, математичні моделі, визначити кращий

алгоритм нечіткого виводу; визначити кращі параметри моделі, що дозволять мінімізувати середньоквадратичну помилку в порівнянні з існуючими методами.

Складність вирішення задач зумовлюється недостатнім опрацюванням на теперішній час наступних підзадач: недоліки існуючих підходів моделювання актуальних загроз безпеці інформації і, як наслідок, некоректне визначення атак, зазроз безпеки даних в розподілених системах; недоліки існуючих методів оцінки ефективності системи захисту, як наслідок, є результатом недостатньо ефективної системи захисту, що призводить до збільшення ризиків порушення цілісності, конфіденційності, доступності та інших властивостей.

Аналіз досліджень оцінки ефективності системи захисту показав, що на теперішній час існують недоліки оцінки ефективності систем захисту, пов'язані з вибором показників оцінки, складне обчислювальне навантаження, недостатня ефективність в частині достовірної оцінки системи захисту, необхідність залучення висококваліфікованих фахівців у галузі інформаційної безпеки, недоліки експертних оцінок.

Існуючі методи оцінки ефективності системи захисту недостатньо задовольняють показникам оцінки ефективності, не враховують достатні та необхідні показники оцінки ризиків реалізації загроз безпеці інформації, оцінки в частині виконання сукупності вимог безпеки даних, вартість фінансових витрат на створення системи захисту, IT-інфраструктури розподілених систем.

У розділі сформульовано мету магістерського дослідження. Визначено задачі, які необхідно вирішити для досягнення поставленої мети. Вирішення поставлених задач дозволить підвищити ефективність оцінки ефективності системи захисту розподілених систем.

2 МОДЕЛЬ ВИЗНАЧЕННЯ АКТУАЛЬНИХ ЗАГРОЗ БЕЗПЕЦІ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

2.1 Моделювання зловмисника та загроз безпеки конфіденційної інформації

Аналіз можливостей, які може мати зловмисник, проводиться у рамках розробки моделі зловмисника. Виходячи з актуальності порушників інформаційної безпеки, визначено внутрішні та ймовірні зовнішні порушники безпеки даних, що обробляються у розподілених системах. До можливих внутрішніх зловмисників інформаційної безпеки відносяться: особи, які мають санкціонований доступ до контрольованої зони розподілених систем, але не мають доступу до інформації, що обробляється в системі; зареєстровані користувачі розподіленої інформаційної системи - здійснюють обмежений доступ з робочого місця до ресурсів системи; зареєстровані користувачі розподіленої інформаційної системи - здійснюють віддалений доступ до інформації. До ймовірних зовнішніх зловмисників інформаційної безпеки даних відносяться: атакуючі інформаційну систему, колишні працівники розподіленої інформаційної системи.

Для виділених типів можливих зловмисників визначаються наступні методи реалізації загроз інформаційної безпеки [1,2,5,21,27,28]:

1. Загрози витоку даних з технічних каналів можуть бути реалізовані за допомогою: перегляду інформації за допомогою оптикоелектронних (оптичних) засобів з засобів відображення, екранів дисплеїв, інформаційно-обчислювальних комплексів, технічних засобів обробки буквенно-цифрової, графічної, відео-інформації; перехоплення випромінюваних чистот при обробці інформації у розподілених інформаційних системах, спеціальними технічними засобами радіотехнічної розвідки, розміщеними як на території контролюємої зони, так і за її межами.

2. Загрози несанкціонованого доступу до інформації можуть бути реалізовані за допомогою: впливу на технічні засоби в ході завантаження операційної системи; прямого доступу до технічних засобів чи програмного забезпечення після завантаження операційної системи; віддаленого доступу до технічних засобів чи програмного забезпечення; віддаленого або прямого впливу на об'єкти віртуального середовища системи і інформацію, яка зберігається у віртуальному просторі розподіленої системи.

3. Загрози спеціальних впливів на розподілену систему можуть бути реалізовані з використанням: хімічного впливу; механічного впливу; акустичного впливу; радіаційного впливу; біологічного впливу; електромагнітного впливу; термічного впливу; магнітного поля; електромагнітного випромінювання.

При визначенні способу реалізації загроз інформаційній безпеці передбачалося, що загрози можуть бути реалізовані за рахунок доступу до інформації, компонентів розподіленої інформаційнох системи, за рахунок створення засобів, умов які забезпечують необхідний доступ.

При визначенні можливих способів реалізації загроз інформаційній безпеці враховано наступні умови: існує можливість змови зловмисників (зовнішніх та внутрішніх); загроз інформаційній безпеці можуть бути реалізовані в будь-якій точці та в будь-який час інформаційної системи (на будь-якому хості, вузлі); для досягнення мети зловмисник обирає найслабшу ланку інформаційної системи.

Модель ймовірного зловмисника розподіленої інформаційної системи містить систему поглядів на потенційних зловмисників безпеки інформації, що обробляється в системі, мотивацію та причини їх дій, цілі, які вони переслідують, загальний характер дій у процесі підготовки до реалізації загроз інформаційній безпеці та здійснення впливу на дані, що обробляються в розподіленій системі.

Модель ймовірного порушника інформаційної системи відбиває теоретичні та практичні можливості ймовірного зловмисника, його апріорні знання, місце та час дії. За наявності права разового чи постійного доступу до контрольваної зони зловмисники поділяються на: особи, які не мають прав доступу до контрольваної

зони системи; особи, які мають право разового або постійного доступу до контрольваної зони системи. Факторами, які знижують ймовірність змови зловмисників, є: створення умов мінімальної фінансової зацікавленості юридичних та фізичних осіб, що входять до числа ймовірних зловмисників безпеки інформації розподілених систем, у реалізації загроз інформаційної безпеки, щодо розподілених систем; укладення угоди про конфіденційність даних між власником системи та фізичними, юридичними особами, що входять до числа ймовірних зловмисників безпеки інформації системи; підтримання та забезпечення високого рівня підготовки користувачів розподіленої інформаційної системи у сфері забезпечення безпеки інформації; створення умов настання негативних наслідків для потенційного зловмисника у разі реалізації загрози інформаційної безпеки: втрата прибутку та ділової репутації, розрив цивільно-правових відношень; визначення відповідальності, що покладається на користувача розподіленої інформаційної системи, при порушенні вимог безпеки даних у розподіленій інформаційній системі.

З урахуванням характеру, призначення оброблюваної інформації, характеристик, умов експлуатації та безпеки розподіленої інформаційної системи можуть бути зовнішніми одиночними порушниками наступні категорії [28, 34]:

- кримінальні структури;
- розвідувальні служби держав;
- конкуруючі організації (конкуренти);
- недобросовісні партнери;
- постачальники програмного забезпечення та технічних засобів (також засобів засобів інформації, систем комплексного ЗІ);
- фізичні особи (зовнішні суб'єкти): колишні працівники власника розподіленої інформаційної системи;
- розробники програмного забезпечення (в тому числі засобів захисту інформації).

До зовнішніх порушників групових пропонується віднести групу «осіб, які є одиночними зовнішніми порушниками, які здійснили змову з метою проведення на об'єкти атаки, які захищаються».

Зовнішній порушник може:

- здійснювати атаки на розподілену інформаційну систему шляхом використання штатних засобів інформаційної системири розташуванні технічних засобів розподіленої інформаційної системи за межами контрольованої зони;

- здійснювати атаки на розподілену інформаційну систему через канали зв'язку, що знаходяться за межами контрольованої зони інформаційної системи;

- здійснювати перехоплення інформації, що обробляється в розподіленій інформаційній системі, відповідними технічними каналами витоку;

- здійснювати безпосередній доступ до об'єктів розподіленої інформаційної системи, які в процесі свого життєвого циклу (супроводу, модернізації, ремонту, експлуатації, утилізації) виявляються за межами контрольованої зони системи;

- здійснювати атаки на розподілену інформаційну систему шляхом застосування вбудованих в технічні засоби інформаційної системи апаратних закладок;

- здійснювати атаки на розподілену інформаційну систему через відповідні системи забезпечення об'єкта інформатизації;

- здійснювати атаки на розподілену інформаційну систему у вигляді інфраструктурних сервісів та засобів комунікації, що знаходяться у межах контрольваної зони інформаційної системи.

Відповідно до документа «Базова модель загроз безпеці персональних даних в інформаційних системах при їх обробці персональних даних» [1,2] внутрішні потенційні порушники поділяються на вісім категорій залежно від повноважень доступу та способу доступу до інформації, що обробляється в розподіленій інформаційній системі. На підставі зазначених категорій порушників з урахуванням умов експлуатації, характеру оброблюваної інформації, суб'єктів доступу розподіленої інформаційної системи та об'єктів захисту, у рамках

магістерської роботи, пропонується використовувати класифікацію поодиноких внутрішніх порушників, представлену наступними дев'ятьма категоріями котистувачів:

- зареєстровані користувачі розподіленої інформаційної системи, які здійснюють обмежений доступ до ресурсів територіально розподіленої інформаційної системи з робочого місця;

- зареєстровані користувачі територіально розподіленої інформаційної системи, які здійснюють віддалений доступ до інформаційних ресурсів, що обробляється в розподіленій інформаційній системі;

- користувачі, які мають санкціонований доступ до територіально розподіленої інформаційної системи, але не мають доступу до інформаційних ресурсів, що обробляється в розподіленій інформаційній системі;

- зареєстровані особи з повноваженнями системного адміністратора розподіленої інформаційної системи;

- зареєстровані користувачі інформаційної системи із повноваженнями адміністратора інформаційної безпеки системи;

- постачальники (програмісти-розробники) прикладного програмного забезпечення та розробники, які забезпечують супровід програмного забезпечення на захищаємому об'єкті;

- особи та розробники, які забезпечують ремонт, постачання, супровід технічних засобів розподіленої інформаційної системи;

- зареєстровані користувачі розподіленої інформаційної системи з повноваженнями адміністратора інформаційної безпеки відповідного сегменту інформаційної системи.

До першої категорії належать користувачі, які мають санкціонований доступ до розподіленої інформаційної системи, але не мають доступу до інформації, що обробляється в інформаційній системі. До цього типу зловмисників належать працівники, які забезпечують функціонування розподіленої інформаційної системи.

До другої категорії відносяться зареєстровані працівники територіально розподіленої інформаційної системи, які мають обмежений доступ до ресурсів інформаційної системи з автоматизованих робочих місць відповідно до ролей які для них призначені.

До третьої категорії належать користувачі зареєстровані в розподіленій інформаційній системі, які здійснюють віддалений доступ до системи з мобільних автоматизованих робочих місць та ноутбуків.

До четвертої категорії належать користувачі зареєстровані в розподіленій інформаційній системі із повноваженнями адміністратора інформаційної безпеки інформаційної розподіленої системи.

До п'ятої категорії належать користувачі зареєстровані в розподіленій інформаційній системі з надами ролями «Прикладний адміністратор» та «Системний адміністратор».

До шостої категорії належать працівники зареєстровані в розподіленій інформаційній системі із повноваженнями адміністратора інформаційної безпеки. Користувачі цієї категорії відповідають за дотримання правил розмежування доступу в інформаційній системі, за зміну паролів, генерацію ключових елементів, здійснює аудит засобів розробки розподіленої інформаційної системи.

До сьомої категорії належать постачальники (програмісти-розробники) прикладного програмного забезпечення та користувачі, які забезпечують супровід програмного забезпечення на території контрольованої зони інформаційної системи.

До восьмої категорії належать особи та розробники, які забезпечують ремонт постачання, та супровід технічних засобів розподіленої інформаційної системи.

Внутрішній порушник може:

- здійснювати атаки на розподілену інформаційну систему через внутрішні канали зв'язку;

- здійснювати безпосередній доступ до об'єктів розподіленої інформаційної системи, які розташовані в рамках контрольованої зони;

- здійснювати атаки на розподілену інформаційну систему шляхом використання штатних засобів системи;

- здійснювати перехоплення інформації, що обробляється в розподіленій інформаційній системі, технічними каналами витоку;

- здійснювати атаки на розподілену інформаційну систему шляхом застосування вбудованих в технічні засоби ситстеми апаратних закладок;

- здійснювати атаки на розподілену інформаційну систему за допомогою інфраструктурних сервісів та засобів комунікації;

- здійснювати атаки на розподілену інформаційну систему через системи забезпечення.

Також до групових зловмисників інформаційної безпеки слід віднести групу користувачів, які є зовнішніми та внутрішніми одиночними зловмисниками, які здійснили змову з метою проведення атаки на об'єкти, що захищаються.

На підставі зазначених категорій порушників з урахуванням умов експлуатації, характеру оброблюваної інформації, суб'єктів доступу до інформаційної системи, об'єктів захисту пропонується використовувати класифікацію внутрішніх порушників, за наступними категоріями: особи, які не мають доступу до даних, що обробляється в інформаційній системі, але мають санкціонований доступ до системи; зареєстровані користувачі, які здійснюють обмежений доступ до ресурсів системи з робочого місця; зареєстровані користувачі інформаційної системи, які здійснюють віддалений доступ до даних, які обробляються в системі; зареєстровані користувачі з повноваженнями адміністратора інформаційної безпеки сегмента системи; зареєстровані користувачі інформаційної системи з повноваженнями системного адміністратора; зареєстровані користувачі системи з повноваженнями адміністратора безпеки даних інформаційної системи; постачальники (програмісти-розробники) програмного забезпечення та особи, які забезпечують супровід прикладних

програм на об'єкті, що захищається; особи та розробники, які забезпечують ремонт, постачання, супровід технічних засобів розподіленої інформаційної системи. Типи потенційних зловмисників інформаційної безпеки встановлюються на підставі відповідного потенціалу, що визначає наявні можливості реалізації загрози безпеки даних: порушники з низьким потенціалом - мають можливість використовувати дані, отриманих із загальнодоступних джерел для реалізації загрози інформаційній безпеці; порушники з середнім потенціалом - мають можливість здійснювати аналіз прикладного програмного забезпечення, знаходити в ньому вразливості та використовувати їх для реалізації загроз інформаційній безпеці; порушники з високим потенціалом - мають можливість вносити закладки в програмне забезпечення ІС, застосовувати спеціалізовані засоби проникнення, проводити спеціальні дослідження та добування інформації для реалізації зазгрози інформаційній безпеці. Для кожної категорії порушників визначення актуальності інформаційної безпеки інформації використовуються наступні критерії: рівень небезпеки; рівень мотивації. Перелік потенційних зловмисників ІБ, що обробляються в розподіленій ІС, та рівень мотивації наведені в табл. 2.1.

Таблиця 2.1 - Перелік потенційних порушників інформаційної безпеки

Порушник	Мотив	Рівень мотивації
Зовнішній порушник		
Розвідувальні служби держав	Відсутній	Мінімальний
Кримінальні структури	Корисні інтереси: досягнення безпосередньої матеріальної вигоди, чи підрив репутації організації	Високий
Конкуренти	Відсутній	Мінімальний
Недобросовісні партнери	Корисливі інтереси: досягнення безпосередньої матеріальної вигоди, чи підрив репутації організації	Високий
Зломщики інформаційних систем та мереж	Хуліганство (вандалізм); професійне самоствердження	Високий

Для визначення рівня небезпеки зловмисника інформаційній безпеці використовуються наступні характеристики: ступінь поінформованості про розподілену інформаційну систему; рівень знань в області безпеки даних. Рівень небезпеки зловмисника інформаційній безпеці представлено у табл. 2.2.

Таблиця 2.2 - Визначення рівня небезпеки одиночного зловмисника

Зловмисник	Рівень знань в області безпеки	Рівень інформованості про об'єкт	Рівень небезпеки
1	2	3	4
Зовнішній порушник			
Розвідувальні служби держав	Має глибокі експертні знання в області ІБ	Володіє інформацією про системне забезпечення ІС	Мінімальний
Кримінальні структури	Не володіє знаннями в області ІБ	Володіє інформацією про системне забезпечення ІС	Мінімальний
Конкуренти (конкуруючі організації)	Має фундаментальні знання в області ІБ	Володіє інформацією про системне забезпечення ІС	Мінімальний
Недобросовісні партнери	Має фундаментальні знання в області ІБ	Володіє інформацією про системне забезпечення ІС	Мінімальний
Зломщики інформаційних систем та мереж	Має глибокі експертні знання в області ІБ	Володіє інформацією про системне забезпечення ІС	Високий
Колишні працівники організації	Має фундаментальні знання в області ІБ	Володіє інформацією про використовувані ОС, ПЗ та системи захисту	Низький
Постачальники ПЗ, технічних засобів	Має фундаментальні знання в області ІБ	Володіє інформацією про використовувані ОС, ПЗ та системи захисту	Низький
Розробники ПЗ	Володіє професійними знання в області ІБ	Володіє інформацією про використовувані ОС, ПЗ та системи захисту	Середній
Внутрішній на рушник			
Особи, які мають доступ до системи, не мають доступу до інформації	Не володіє знаннями в галузі ІБ	Володіє інформацією про системне забезпечення ІС	Мінімальний

Закінчення таблиці 2.2

1	2	3	4
Зареєстровані користувачі з обмеженим доступом до ресурсів системи з робочого місця	Має фундаментальні знання в області ІБ	Володіє інформацією про використовувані ОС, ПЗ та системи захисту	Низький
Зареєстровані користувачі ІС, які здійснюють віддалений доступ до інформації	Має фундаментальні знання в області ІБ	Володіє інформацією про використовувані ОС, ПЗ та системи захисту	Низький
Зареєстровані користувачі з правами адміністратора безпеки сегменту системи	Має професійні знання в області ІБ	Володіє інформацією про конфігурацію та параметри налаштування ОС, ПЗ, ТЗ, системи захисту	Середній
Зареєстровані користувачі з правами системного адміністратора інформаційної системи	Має фундаментальні знання в області ІБ	Володіє інформацією про конфігурацію та параметри налаштування ОС, ПЗ, ТЗ, системи захисту	Середній
Зареєстровані користувачі з правами адміністратора безпеки системи	Має професійні знання в області ІБ	Володіє інформацією про конфігурацію та параметри налаштування ОС, ПЗ, ТЗ, СЗ	Середній
Програмісти-розробники ППЗ та особи, які забезпечують його супровід	Має фундаментальні знання в області ІБ	Володіє інформацію про найменування та версію ПЗ, відомостями про системи забезпечення	Середній
Розробники та особи, які забезпечують постачання, супровід та ремонт технічних засобів	Має фундаментальні знання в області ІБ	Володіє інформацію про найменування та версію ПЗ, відомостями про системи забезпечення	Середній

Відповідно аналізу проведеного дослідження актуальність актуальність інформаційної безпеки розподіленій інформаційній системі наведено в табл. 2.3.

Таблиця 2.3 - Визначення актуальності одиночного зловмисника ІБ

Зловмисник	Рівень мотивації	Рівень небезпеки	Актуальність
Зовнішній порушник			
Розвідувальні служби держав	Мінімальний	Мінімальний	Неактуальний
Кримінальні структури	Високий	Мінімальний	Неактуальний
Конкуренти (організації)	Мінімальний	Мінімальний	Неактуальний
Недобросовісні партнери	Високий	Мінімальний	Неактуальний
Зломщики ІС та мереж	Високий	Високий	Актуальний
Колишні працівники організації	Високий	Низький	Актуальний
Постачальники ПЗ, ТЗ	Мінімальний	Низький	Неактуальний
Розробники ПЗ	Мінімальний	Середній	Неактуальний
Внутрішній на рушник			
Особи мають доступ до системи, не мають доступу до інформації	Надзвичайно високий	Мінімальний	Актуальний
Зареєстровані користувачі з обмеженим доступом до ресурсів	Надзвичайно високий	Низький	Актуальний
Зареєстровані користувачі, мають віддалений доступ до інформації	Надзвичайно високий	Низький	Актуальний
Зареєстровані користувачі з правами адміністратора безпеки сегменту системи	Мінімальний	Середній	Неактуальний
Зареєстровані користувачі з правами системного адміністратора інформаційної системи	Мінімальний	Середній	Неактуальний
Зареєстровані користувачі з правами адміністратора безпеки інформаційної системи	Мінімальний	Середній	Неактуальний
Програмісти-розробники ППЗ та особи, які забезпечують супровід	Мінімальний	Середній	Неактуальний
Розробники та особи, які забезпечують постачання, супровід та ремонт технічних засобів	Мінімальний	Середній	Неактуальний

Виходячи з проведеного в рамках магістерської роботи аналізу досліджень можливих зловмисників інформаційній безпеці, визначено ймовірні порушники безпеки конфіденційним даним, які обробляються в розподіленій інформаційній системі. Залежно від наявних можливостей у виявлених ймовірних порушників

інформаційній безпеці, визначається відповідний рівень криптографічного захисту конфіденційних даних, який повинен забезпечити застосовувані для захисту засоби для нейтралізації загроз інформаційній безпеці.

2.2 Генерація набору даних для визначення актуальних загроз безпеці конфіденційної інформації

При формуванні переліку загроз безпеки інформації слід розглядати загрози наступних типів: загрози, що не є атакою; загрози, які є атаками. При обробці інформації в розподілених інформаційних системах можлива реалізація наступних загроз безпеки даних: загрози несанкціонованого доступу до даних; загрози спеціальних впливів на розподілену інформаційну систему, загрози витоку інформації по технічних каналах.

Загрози витоку можуть бути реалізовані зовнішніми, внутрішніми, зловмисниками, також шляхом розміщення закладних пристроїв у межах контрольованої зони, так і поза нею. Загрози несанкціонованого доступу пов'язані з діями зловмисників, які мають доступ до інформаційної системи, включаючи користувачів системи, які реалізують загрози безпосередньо в інформаційній системі, а також зловмисників, які не мають доступу до розподіленої системи, реалізують загрози із зовнішніх мереж міжнародного інформаційного обміну та загального користування.

Реалізація загроз несанкціонованого доступу до даних може призводити до наступних видів порушення безпеки: порушення цілісності; порушення конфіденційності; порушення достовірності; порушення доступності.

За результатами проведеного дослідження можна зробити висновок, що існуючі підходи мають здебільшого суттєві недоліки: відсутність документації, великий об’єм даних, необхідність високої кваліфікації фахівців з безпеки

інформації; відсутність автоматизованих засобів визначення актуальних загроз інформаційній безпеці.

У зв'язку з вищесказаним поставлено наступні задачі:

1. Підготовка набору даних для визначення актуальних загроз інформаційній безпеці на основі відомих баз даних вразливостей та загроз, розроблених статичних моделей загроз.

2. Аналіз сформованого набору даних.

3. Порівняння та вибір якості роботи декількох моделей, визначення найкращої.

4. Перевірка моделі.

Для генерації набору даних для розробки програмного забезпечення та автоматизованої обробки використовувалася технології Data Science, мова програмування Python. Складністю визначення актуальних загроз інформаційної безпеки досліджуваної розподіленої інформаційної системи - обробка великого об’єму даних, необхідних при визначенні актуальних загроз конфіденційній інформації: інформація з зарубіжних баз даних та знань, складність використання методичних документів регуляторів України у сфері забезпечення інформаційної безпеки.

Проведений аналіз даних показує - інформація має великий об’єм, що викликає трудомісткість обчислень у процесі визначення актуальних загроз інфоформаційній безпеці. Використання експертного підходу для визначення актуальних загроз інфоформаційній безпеці спричиняє помилки, пов'язані з людським фактором, такі як: трудомісткість, неузгодженість та розрізненість думок, особиста думка експерта. Методичні документи Кваліфікаційного центру інформаційних технологій та кібербезпеки України визначають етапи та підхід визначення актуальних загроз конфіденційним даним, при цьому трудомісткість та помилки експертів не враховуються.

Відповідно до методичні документі Кваліфікаційного центру інформаційних технологій та кібербезпеки України актуальність загроз конфіденційним даним

визначається залежно від актуальності порушника в розподіленій інформаційній системі, переліком потенційних вразливостей та загроз в IT-інфраструктурі інформаційної системи, а також можливими наслідками від реалізації загроз інформаційної безпеки. Таким набір даних був сформований із відомостей бази даних загроз Кваліфікаційного центру інформаційних технологій та кібербезпеки України, моделей загроз інформаційної безпеки розподіленої інформаційної системи, технічних рішень досліджуваної системи.

За результатами генерації та перетворення набору даних необхідно визначити модель для реалізації методу, підвищити ефективність методу по відношенню до відомих підходів за рахунок адаптації та визначення найкращих параметрів системи.

2.3 Модель визначення актуальних загроз безпеці конфіденційним даним

Проведено дослідження адаптивних нейронних нечітких систем ANFIS із використанням алгоритмів нечіткого виведення Такагі-Сугено-Канга, Сугено-Такагі, Мамдані, Ванга-Менделя. Залежність похибки на тестовій вибірці від кількості правил під час перевірки менша у мережі ANFIS з алгоритмом Такагі-Сугено-Канга. Для визначення актуальних загроз інформаційній безпеці обрана нейронна система ANFIS, заснована системі Такагі-Сугено-Канга. Алгоритм роботи полягає в реалізації нечіткої моделі, заснованої на правилах типу (2.1):

$$R_i : IFx_i ISA_{i1} AND ... AND_{x_j} ISA_{ij} AND ... AND_{x_{im}} ISA_{im}, THEN$$
$$y = c_{i0} + \sum_{j=1}^{m} c_{ij} x_j,\ j = 1,...,n \qquad (2.1)$$

Сформовано базу правил визначення актуальних загроз інформаційній безпеці. Приклад заповнення бази знань правила виходячи з сформованого набору даних наведено у табл. 2.4.

Таблиця 2.4 - Фрагмент бази знань правил визначення актуальних загроз ІБ

№ п/п	IF (ЯКЩО)			THEN (ТО)
	Тип порушника (джерело впливу)	ІТ-інфраструктура (об'єкт впливу)	Версія ПЗ	
1	Зовнішній порушник із низьким потенціалом, Внутрішній порушник з низьким потенціалом	Віртуальна машина VMWare	6.5 (VMWare Workstation), від 7.0.0 до 7.1.4 включно (VMWare Workstation)	Загроза несанкціонованого доступу до захищених віртуальних машин з боку інших віртуальних машин
2	Зовнішній порушник з високим потенціалом	Мобільний пристрій на базі iOS	(Android), до 10.3.3 включно (iOS)	Загроза контролю шкідливою програмою списку додатків, запущених на мобільному пристрої
…				
N	Зовнішній порушник із середнім потенціалом, Внутрішній порушник з середнім потенціалом	Засіб захисту інформації	12.4 (Cisco IOS), 12.4 (Cisco IOS), 15.0 (Cisco IOS), 15.0 (Cisco IOS), 15.2 (Cisco IOS), 15.1 (Cisco IOS)	Загроза несанкціонованого впливу на засіб захисту інформації

Правила представлені в табл. 2.4 як єдине, фактично представляє множину правил, що складаються окремо за типом системи захисту інформації, типом зловмисника, (Dallas Lock, SecretNet) та впливом.

Нейронна продукційна адаптивна система ANFIS базується на наступних положеннях: вхідні змінні є чіткими; функції приналежності визначені функцією Гауса: $\mu_{A_{ij}}\left(x_j\right)=\exp\left(-\frac{1}{2}\left(\frac{x_j-a_{ij}}{b_{ij}}\right)^2\right)$, де x - вхідні дані мережі a_{ij}, b_{ij} - параметри функції приналежності, що налаштовуються; нечітка імплікація Ларсена нечіткий

добуток; *T*-норма – нечіткий добуток; композиція не здійснюється; метод дефазифікації – метод центроїду.

Функціональна залежність після дефазифікації має вид (2.2):

$$y' = \frac{\sum_i^n \left(\left(c_{i0} + \sum_{j=1}^m c_{ij} x_j \right) \prod_j^m \mu_{A_{ij}} \left(x_j^{'} \right) \right)}{\sum_{i=1}^n \prod_j^m \mu_{A_{ij}} \left(x_j^{'} \right)} = \frac{\sum_i^n \left(\left(c_{i0} + \sum_{j=1}^m c_{ij} x_j \right) \prod_j^m \exp \left[- \left(\frac{x_j^{'} - a_{ij}}{b_{ij}} \right)^2 \right] \right)}{\sum_{i=1}^n \prod_j^m \exp \left[- \left(\frac{x_j^{'} - a_{ij}}{b_{ij}} \right)^2 \right]} \quad (2.2)$$

Вираз 2.2 лежить в основі нейронної мережі ANFIS, включає п'ять шарів:

1. Виконує фазифікацію чітких вхідних змінних: $x_j^{'} \left(j = 1,...,n \right)$.

2. Обчислює значення ступенів функції приналежності $\mu_{A_{ij}} \left[x_j^{'} \right]$, заданих функціями Гаусса з параметрами a_{ij}, b_{ij}.

3. Генерує значення функцій $\left(c_{j0} + \sum_{j=1}^m c_{ij} x_j^{'} \right)$, які перемножуються на результати обчислень елементами другого шару.

4. Перший елемент четвертого шару необхідний для активізації виводів правил. Другий елемент четвертого шару проводить додаткові обчислення.

5. Даний шар складається з одного елемента нормалізуючого та робить дефаззифікацію результатів роботи нейронної мережі.

Нейронна мережа ANFIS містить параметричні шари (1 і 3). Параметрами, які налаштовуються в процесі навчання нейронної мережі є: в першому шарі - нелінійні параметри a_{ij}, b_{ij} функції приналежності фазифікатора; в третьому шарі - параметри c_{i0} і c_{ij} лінійних функцій $\left(c_{j0} + \sum_{j=1}^m c_{ij} x_j^{'} \right)$ з висновків бази правил.

На наступному кроці розраховуються параметри c_{i0} і c_{ij} лінійних функцій за умови фіксованих значень параметрів a_{ij}, b_{ij}. Параметри c_{i0} і c_{ij} знаходяться

шляхом розв'язання системи лінійних рівнянь. Вихідну змінну з виразу (2.2) подаємо в наступному виді (2.3):

$$y' = \sum_{i=1}^{n} w_i' \left(c_{i0} + \sum_{j=1}^{m} c_{ij} x_j \right), \tag{2.3}$$

де $w_i' = \dfrac{\prod_j^m \mu_{A_{ij}}\left(x_j'\right)}{\sum_{i=1}^n \prod_j^m \mu_{A_{ij}}\left(x_j'\right)} = \dfrac{\prod_j^m \exp\left[-\left(\dfrac{x_j' - a_{ij}}{b_{ij}}\right)^2\right]}{\sum_{i=1}^n \prod_j^m \exp\left[-\left(\dfrac{x_j' - a_{ij}}{b_{ij}}\right)^2\right]} = const$

Алгоритм навчання нейроної продукційної адаптивної система ANFIS із застосуванням алгоритму TSK. При k навчальних прикладах $x_1^{(k)}, x_2^{(k)}, \ldots, x_m^{(k)}, y^{(k)}$, де $k = 1,\ldots,K$ і заміна значень вихідних змінних $y'^{(k)}$ значеннями еталонних змінних $y^{(k)}$,отримаємо систему з k лінійних рівнянь (2.4):

$$\begin{bmatrix} w_1^{(1)} & w_1^{(1)}x_1^{(1)} & \ldots & w_1^{(1)}x_m^{(1)} & \ldots & w_n^{(1)} & w_n^{(1)}x_1^{(1)} & \ldots & w_n^{(1)}x_m^{(1)} \\ w_1^{(2)} & w_1^{(2)}x_1^{(2)} & \ldots & w_1^{(2)}x_m^{(2)} & \ldots & w_n^{(2)} & w_n^{(2)}x_1^{(2)} & \ldots & w_n^{(2)}x_m^{(2)} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ w_1^{(k)} & w_1^{(k)}x_1^{(k)} & \ldots & w_1^{(k)}x_m^{(k)} & \ldots & w_n^{(k)} & w_n^{(k)}x_1^{(k)} & \ldots & w_n^{(k)}x_m^{(k)} \end{bmatrix} \times \begin{bmatrix} c_{10} \\ \ldots \\ c_{1m} \\ \ldots \\ c_{n0} \\ \ldots \\ c_{nm} \end{bmatrix} = \begin{bmatrix} y^{(1)} \\ y^{(2)} \\ \ldots \\ y^{(k)} \end{bmatrix}, \tag{2.4}$$

де $w_1^{(k)}$- агрегований ступінь істинності передумов за і-им правилом при пред'явленні k-го вхідного вектора $\left(x_1^{(k)}, x_2^{(k)}, \ldots, x_m^{(k)}\right)$. Вираз (2.4) у скороченому виді: $W \cdot c = y$. Вирішення даної системи рівнянь можна провести за один крок за

допомогою псевдоінверсії матриці W: $c = W^{+} y = \left(W^{T} W\right)^{-1} W^{T} y$. Після визначення лінійних параметрів ij розраховуємо та фіксуємо фактичні вихідні сигнали системи, для чого використовуємо лінійну залежність:

$$y` = \begin{bmatrix} y^{(1)} \\ y^{(2)} \\ \dots \\ y^{(k)} \end{bmatrix} = W \cdot c$$

Визначаємо вектор помилок: $e = y` - y$.

Виконуємо уточнення параметрів (2.5):

$$\begin{aligned} a_{ij}^{(k)}(t+1) &= a_{ij}^{(k)}(t) - C \frac{\partial E^{(k)}(t)}{\partial a_{ij}^{(k)}} \\ b_{ij}^{(k)}(t+1) &= b_{ij}^{(k)}(t) - C \frac{\partial E^{(k)}(t)}{\partial b_{ij}^{(k)}} \end{aligned} \qquad (2.5)$$

Для визначення актуальних загроз інформаційній безпеці із переліку потенційних можливих загроз необхідно визначити ймовірність реалізації. Визначаємо коефіцієнти Y_2 експертним шляхом для кожної загрози інформаційній безпеці: 0 - малоймовірна загроза; 2 – низька ймовірність загрози; 5 – середня ймовірність загрози; 10 –висока ймовірність загрози.

З урахуванням визначених коефіцієнтів ймовірність реалізації загроз інформаційній безпеці Y визначається співвідношенням: $Y = \left(Y_1 + Y_2\right)$, де Y_1 - ступінь початкової захищеності розподіленої інформаційної системи, що визначається відповідно до методичних даних Кваліфікаційного центру інформаційних технологій та кібербезпеки України.

Структура нечіткої нейронної мережі ANFIS представлена рис. 2.1.

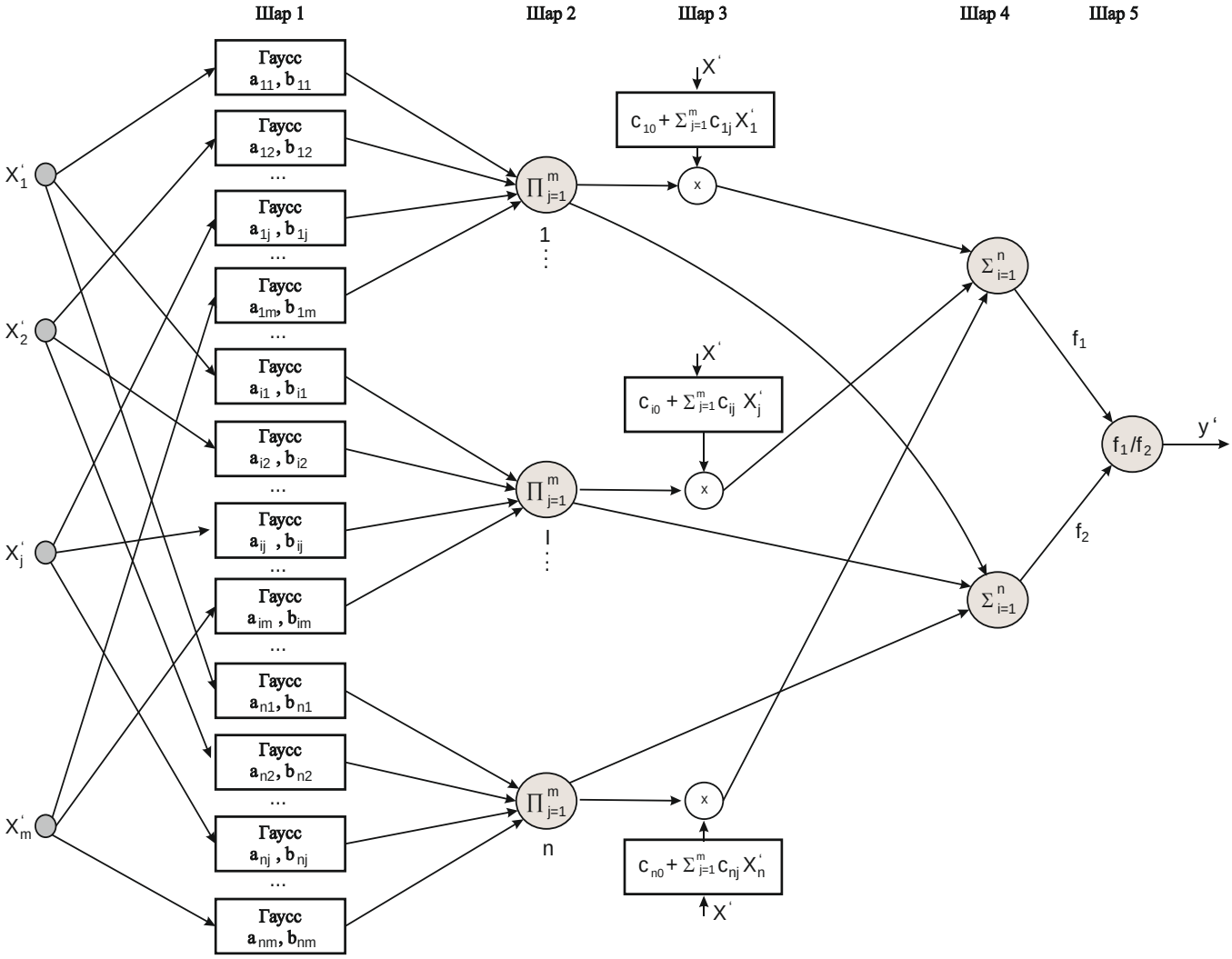


Рисунок 2.1 – Нейронна мережа ANFIS із застосуванням алгоритму TSK

Аналіз оцінки ефективності запропонованого підходу визначення актуальних загроз інформаційній безпеці наведені у табл. 2.5.

Таблиця 2.5 – Аналіз оцінки ефективності запропонованого підходу

Показник	Існуючі підходи	Запропонований підхід
RMSE	0,018-0,069	0,011-0,022
Визначення кількості актуальних загроз	понад 30%	більше 35%
Вартість системи захисту	зниження до 15%	зниження до 30%

Середньоквадратична помилка запропонованого підходу (2.6):

$$RMSE = \sqrt{\frac{1}{N}\sum_{i=1}^{N}\left(y_i - y_i\right)^2}, \tag{2.6}$$

де y_i, y_i - набори даних (перевірки, навчання).

Графіки порівняння *RMSE* запропонованого та існуючих підходів на заданому інтервалі представлені на рис. 2.2.

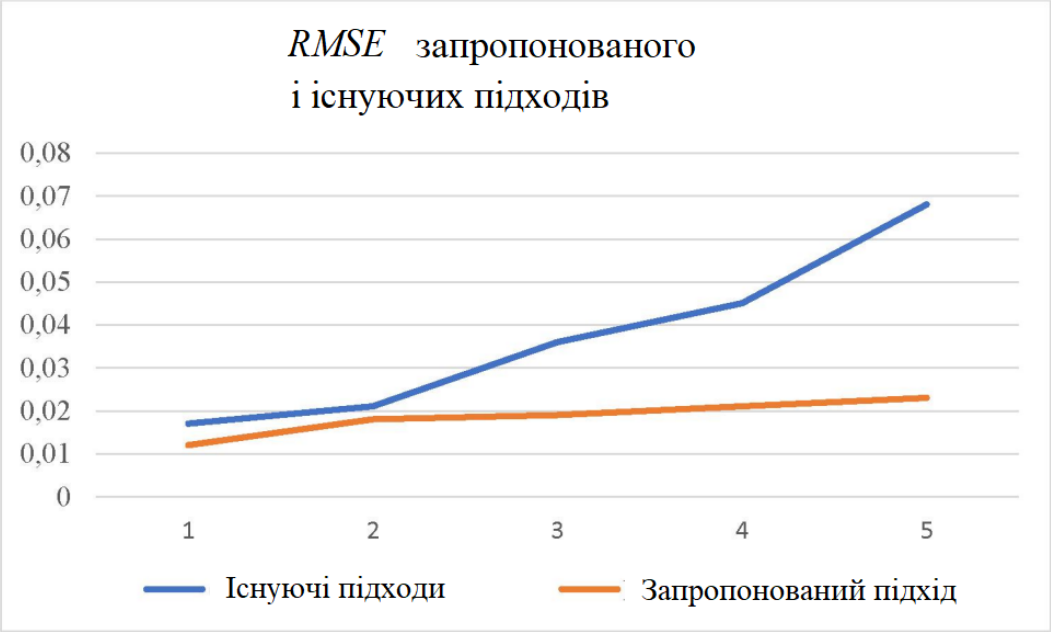


Рисунок 2.2 - Графік порівняння RMSE на заданому інтервалі

2.4 Висновки

Запропоновано модель визначення актуальних загроз інформаційній безпеці, заснована на алгоритмах нечіткого виводу та теорії нечітких нейронних систем, на відміну від відомих, використовує певні достатні та необхідні показники, виключає помилки експертів. Збільшує виявлення кількість актуальних загроз

інформаційній безпеці на 5%, знижує витрати на закупівлю засобів захисту інформації від 15 до 30%. Враховує наступні фактори: IT-інфраструктуру розподіленої інформаційної системи, можливості зловмисників та рівень мотивації у розподіленій інформаційній системи, перелік існуючих. Запропонований підхід відрізняється від існуючих: відсутність залучення висококваліфікованих фахівців у області безпеки інформації; процес автоматизований, має низьку обчислювальну складність; відсутність недоліків експертних оцінок; дозволяє визначати перелік актуальних загроз безпеки інформації в інформаційних системах різних класів та типів.

3 МЕТОД ОЦІНКИ ЕФЕКТИВНОСТІ СИСТЕМ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

3.1 Показники оцінки ефективності та вимоги до систем захисту конфіденційної інформації

На підставі моделей загроз інформаційній безпеці типових розподілених інформаційних систем та на підставі методичних документів Кваліфікаційного центру інформаційних технологій та кібербезпеки України сформовано перелік загроз безпеці конфіденційним даним. Вирішена задача перетворення та очищення великого об’єму даних, сформовано набір даних для визначення актуальних загроз інформаційній безпеці конфіденційних даних з використанням технологій Data Science. На основі використання нечітких адаптивних продукційних нейронних мереж запропоновано модель визначення актуальних загроз інформаційній безпеці даних.

При формуванні необхідних вимог захисту інформації в інформаційних системах на підставі даних Кваліфікаційного центру інформаційних технологій та кібербезпеки України сформовані вимоги для різних класів і типів інформаційних систем щодо захисту конфіденційної інформації. Під час розробки системи захисту для розподілених інформаційних систем враховувалися такі фактори, як використання, за вимогами безпеки інформації, сертифікованих засобів захисту

Для проведення адекватної оцінки ефективності системи захисту необхідно визначити достатні та необхідні показники. Оцінка ефективності системи захисту даних досягається шляхом створення відповідної системи, здатної максимально нейтралізувати актуальні загрози інформаційній безпеці, виконати вимоги захисту конфіденційних даних, що пред'являються до розподіленої інформаційної системи на підставі вимог в області безпеки інформаційної безпеки, а також дозволяє при розробці системи захисту максимально скоротити фінансові витрати. Таким

чином, показники оцінки пропонуються наступні: перелік актуальних загроз інформаційній безпеці; IT-інфраструктура розподіленої інформаційної системи з урахуванням їх специфіки; перелік вимог до безпеки інформації з урахуванням класифікації конкретної інформаційної системи; вартість засобів захисту інформації; перелік засобів захисту інформації, за результатами розробки системи захисту розподіленої інформаційної системи.

Виходячи з результатів проведеного аналізу досліджень розподілених інформаційних систем, визначень ефективності системи захисту в області інформаційної безпеки даних можна зробити наступний висновок: перераховані показники є достатніми та необхідними для достовірної та повноцінної оцінки ефективності системи захисту інформації.

На підставі результатів інформаційного обстеження розподілених систем, вхідних даних, у сфері забезпечення інформаційної безпеки у проведеному дослідженні пропонується визначити вимоги до безпеки інформації у сукупності. Вимоги, що пред'являються до досліджуваної розподіленої системи до безпеки конфіденційних даних, наведені в табл. 3.1.

Таблиця 3.1- Вимоги до інформаційної безпеки досліджуваної системи

Умовне позначення	Найменування функції підситеми	Відповідність функції системі	
		4 РЗ	3 -клас
1	2	3	4
Аутентифікація та ідентифікація суб'єктів до об'єктів доступу			
АІ.1	Аутентифікація та ідентифікація користувачів та процесів	+	+
АІ.2	Захист автентифікаційної інформації при передачі	+	+
АІ.3	Керування ідентифікаторами, створення, знищення.	+	+
АІ.4	Ідентифікація та аутентифікація користувачів	+	+
…			
Керування доступом суб'єктів до об'єктів доступу			
КД.1	Керування обліковими записами користувачів	+	+

Закінчення таблиці 3.1

1	2	3	4
КД.2	Дозвіл (заборона) дій користувачів, дозволених до ідентифікації та автентифікації	-	+
КД.3	Поділ повноважень (ролей) користувачів, адміністраторів, які забезпечують функціонування системи	+	+
…			
Обмеження програмного середовища			
ПС.1	Установка (інсталяція) дозволеного до використання програмного забезпечення та його компонентів	-	+
Захист машинних носіїв інформації			
МН.1	Облік машинних носіїв інформації	-	+
МН.2	Управління доступом до машинних носіїв інформації	-	+
…			
Реєстрація подій безпеки			
ПБ.1	Визначення змісту та складу інформації про події безпеки, що підлягають реєстрації	+	+
ПБ.2	Моніторинг (аналіз, перегляд) результатів реєстрації подій безпеки та реагування на них	-	+
…			
Захист інформаційної системи, її засобів, систем зв'язку та передачі даних			
ЗС.1	Захист бездротових з'єднань в системі	-	+
	Заборона несанкціонованої активації відеокамер, мікрофонів, периферійних пристроїв, які можуть активуватися віддалено, оповіщення користувачів	-	+
…			
Аналіз (контроль) захищеності інформації			
АК.1	Виявлення вразливостей системи та оперативне усунення вразливостей	-	+
АК.2	Контроль складу технічних засобів, ПЗ	-	+
АК.3	Контроль встановлення оновлень ПЗ	+	+

Наведений у табл. 3.1 перелік вимог щодо захисту інформації та сформований для четвертого рівня захищеності персональних даних та третього класу захищеності держвної інформаційної системи. Для кожного класу та типу, категорії значущості розподіленої інформаційної системи, рівня захищеності, формуються переліки вимог щодо захисту конфіденційних даних.

На підставі сформованого переліку вимог інформаційної безпеки, переліку засобів захисту інформації, переліку актуальних загроз безпеки даних, підготовлено набір даних для оцінки ефективності системи. Використання технологій Data Science виконано наступні кроки: перетворення та очищення підготовленого набору даних; порівняння якості роботи моделей; вибір найбільш актуальних ознак, створення нових більш репрезентативних; перевірка моделі на тестовій вибірці; визначення параметрів у найкращій моделі; підсумкове представлення результатів виконання задачі; інтерпретація результатів.

Враховуючи те, що в наборі даних присутня надлишкова інформація, що збільшує задіяні обчислювальні ресурси та ускладнює процес обробки отрманих даних, а отже в кінцевому варіанті може вплинути на результати методу оцінки ефективності системи захисту інформації, першим кроком було здійснено поведення фільтрації даних.

Фрагмент для перетворення набору даних представлений в лістингу 3.1:

Лістинг 3.1 - Фрагмент коду перетворення набору даних

```
rvul = pd.readexel('vullist.xlsx')
rvul pit. style.use('fivethityeighf)
df.resetindex().pivot('name','typeof_hacker').plt.hist(df, binss=10, edecolor = 'k'), plt.xlabelTnn зловмисника'), plt.label('Кількість загроз'), pit.title('Рівень безпеки')
# Перетворення рядкових даних інформації
for col in list(df.colums):
#Вибір колонок для перетворення даних
```

```
if (ft2 in col або kBtu in color Metric_Tons CO2e in col or kh in
col або therm col або gal in col або Score in col):
# Конвертація
df[col] = df[col].astype(float)
```

В процесі виконання магістерської роботи визначено ключові складові:

1. Список актуальних загроз інформаційної безпеки з ознаками не нейтралізації/нейтралізації.

2. Перелік вимог до інформаційної безпеки даних з ознаками відповідності: загалом відповідає, відповідає, не відповідає, частково відповідає.

3. Найменування засобів захисту інформації, їх версія, патчів (версії оновлень).

4. Вартість засобів від виробника (специфікації вендорів).

На підставі проведеного визначення ключових складових системи проведена фільтрація зайвої інформації з набору даних.

Ознаки інформації, що є напочатку числовими, інтерпретовані як тип object. Таким чином відповідні ознаки були конвертовані в дійсний тип - float. Наступним кроком є проводення заміни значення "Not Available" в dataframe на "not a number" ("не число"). Це дозволить змінити числовий тип ознак на float, в dataframe нейтралізуємо викиди та пропуски.

Наступним кроком є проводення попереднього аналізу отриманих даних (EDA - Exploratory Data Analysis), на підставі попереднього аналізу визначаємо аномалії, закономірності, зв'язки між ознаками. Таким чином, необхідно визначити значення ознак та ознаки, що мають суттєвий вплив на цільову ознаку отриманих даних, оцінюємо вплив значень категоріальних ознак на цільовий – density plot.

Для чисельного оцінювання ознак ступеня їхнього впливу, у магістерській роботі використовується коефіцієнт кореляції Пірсона - міра позитивності та ступеня лінійних зв'язків між двома змінними. Значення коефіцієнта +1 означає

ідеальну пропорційність між відповідними значеннями ознак і, -1 аналогічно, але з відємним коефіцієнтом.

Величина кореляції розраховується наступним чином: correlationsdata = data.corr()['score'].sort_values().

Вибір ознак інформації –вибір найбільш релевантних ознак. З dataframe видаляються ознаки даних, щоб модель відповідала більше признакам та ресурсів першорядним ознакам. Таким чином, проводиться фільтрація набору даних відповідної інформації, якій залишаються лише найважливіші для даної задачі.

Створення нових ознак - процес, у якому на основі наявних отриманих даних конструюються нові ознаки. Потім визначаються колінеарні ознаки.

Після виконання попереднього аналізу, фільтрації даних, залишаться лише найбільш важливі ознаки. Наступним кроком перед початком проведення навчання моделі ANFIS є отримання показника, на якому можна визначити, чи є позитивний результат від використання задіяного алгоритму.

До проведення розрахунку вищеописаного критерію, необхідно розділити вибірку на тестову та навчальну:

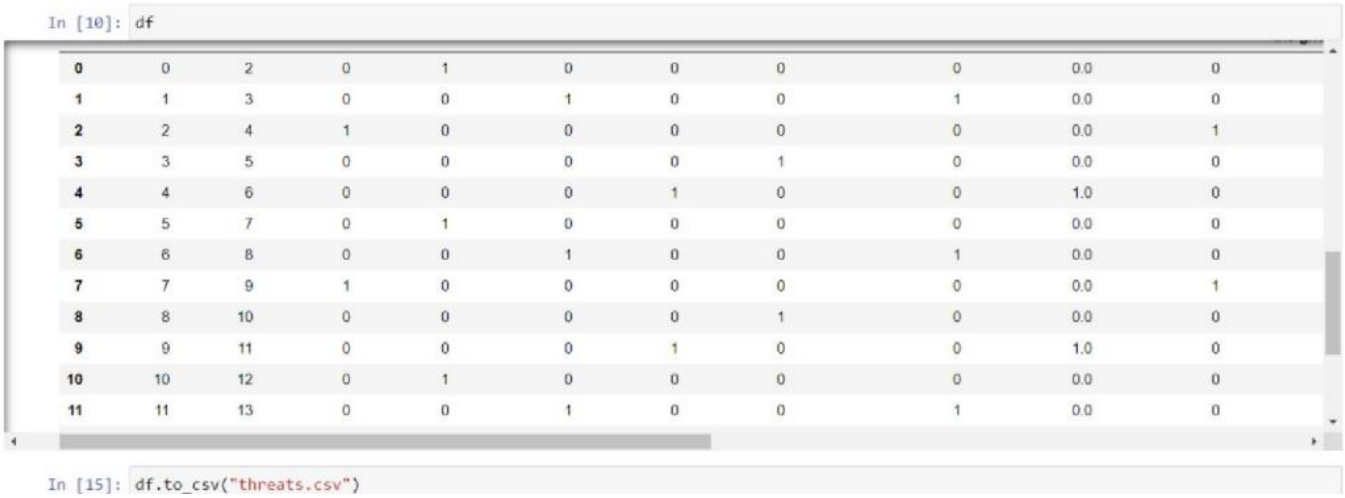
1. Тестова вибірка використовується для перевірки отриманої моделі ANFIS. Модель ANFIS не використовує цільової ознаки при обробці даних і, має передбачити його величину, використовуючи, при цьому, значення інших ознак. Отримані прогнози порівнюються з реальними відповідями.

2. Навчальна вибірка - набір сформованих даних, який подається разом з відповідями на вхід моделі ANFIS в процесі навчання, з метою навчити модель виявляти зв'язок між сформованими ознаками і правильною відповіддю.

Фрагменти dataframe після перетворення представлені на рис. 3.1.

Сформований набір даних включає в себе перелік вимог до інформаційної безпеки, перелік засобів захисту, актуальних загроз інформаційної безпеки в розподіленій системі, зроблено його форматування та перетворення, що дозволило зібрати лише достатні та необхідні дані для оцінки ефективності системи захисту,

що, зменшує кількість помилок експертних оцінок, складність обчислювального процесу, підвищуючи ефективність запропонованого підходу.



In [10]: df

0	0	2	0	1	0	0	0	0	0.0	0
1	1	3	0	0	1	0	0	1	0.0	0
2	2	4	1	0	0	0	0	0	0.0	1
3	3	5	0	0	0	0	1	0	0.0	0
4	4	6	0	0	0	1	0	0	1.0	0
5	5	7	0	1	0	0	0	0	0.0	0
6	6	8	0	0	1	0	0	1	0.0	0
7	7	9	1	0	0	0	0	0	0.0	1
8	8	10	0	0	0	0	1	0	0.0	0
9	9	11	0	0	0	1	0	0	1.0	0
10	10	12	0	1	0	0	0	0	0.0	0
11	11	13	0	0	1	0	0	1	0.0	0

In [15]: df.to_csv("threats.csv")

Рисунок 3.1 - Фрагмент dataframe після перетворення

3.2 Метод оцінки ефективності системи захисту конфіденційної інформації

На теперішній час існує велика кількість нейро-нечітких гібридних моделей, що відрізняються можливостями та архітектурою. У магістерському дослідженні проведено аналіз моделей і на основі отриманих результатів визначено основні властивості: застосування різних підходів навчання моделі; можливість автоматизованого формування набору правил; зберігання даних в процесі навчання новим правилам чи параметричної оптимізації; зміна структури моделі гібридних нейро-нечітких моделей наведені в табл. 3.2.

На основі аналізу проведеного дослідження моделей зроблені висновки щодо використання типів моделей для спектра розв'язуваних задач. Результати проведеного аналізу наведені у табл. 3.3.

З результатів проведеного аналізу, представлених у табл. 3.3, можна зробити висновок, що для вирішення задачі оцінки ефективності системи захисту доцільно використовувати ANFIS.

Таблиця 3,2 - Область застосування гібридних нейро-нечітких моделей

№ п/п	Модель	Область застосування
1	ANFIS	- структура бази правил має бути відома заздалегідь; - параметри налаштовуються в першому і останньому прихованому шарі; - навчання в два етапи: параметри першого шару фіксовані, використовується оцінка параметрів другого шару; параметри другого шару фіксовані, параметри першого шару оцінюються алгоритмом RMSE (зворотного розповсюдження помилки).
2	NEFCON	- можливість індукування та оптимізації бази правил; - лінгвістичні нечіткі моделі.
3	NEFCLASS	- можливість оптимізації бази правил; - структура бази правил може змінюватися.
4	FALCON	- навчання у два етапи: навчання без вчителя; параметрична оптимізація (метод градієнтного спуску).
5	FUN	- алгоритм зміни параметрів та перебудови зв'язків, функція приналежності має випадковий характер

Таблиця 3.3 - Спектр розв'язуваних задач в залежності від типу моделі

№ п/п	Модель	Спектр задач
1	NEFPROX, NEFCLASS	Інтелектуальна обробка та аналіз даних
2	NEFCLASS	Задачі класифікації, прийняття рішень
3	ANFIS, NEFPROX, FBF	Апроксимація нелінійних залежностей
4	NEFCON, FUN, GARIC, ANFIS	Інтелектуальне управління
5	NNDFR, ANFIS	Моделювання
6	FAM, NEFPROX	Прогнозування

Для розробки методу оцінки ефективності системи захисту конфіденційних даних проаналізовано модель мережі ANFIS з алгоритмами нечіткого виведення Мамдані, Такагі-Сугено-Канга, Ванга-Менделя, Такагі-Канга. Мережі ANFIS призначені, зокрема, для вирішення задач оцінювання. Вивід системи відповідє набору нечітких правил if-then (якщо-то), які мають здатність до навчання апроксимування нелінійних функцій.

Алгоритм роботи мережі ANFIS з алгоритмом TSK (нечіткого виведення Такаги-Сугено-Канга) у запропонованому методі оцінки ефективності системи захисту даних полягає у реалізації нечіткої моделі, заснованої на правилах (3.1):

$$R_i : IFx_i ISA_{i1} AND ... AND_{x_j} ISA_{ij} AND ... AND_{x_{im}} ISA_{im}, THEN$$
$$y = c_{i0} + \sum_{j=1}^{m} c_{ij} x_j,\ j = 1,...,n \qquad (3.1)$$

На підставі вимог та показників щодо захисту даних, також на підставі актуальних загроз інформаційної безпеки та IT-інфраструктури розподілених систем було сформовано базу правил, фрагмент бази наведено в табл. 3.4.

Таблиця 3.4 - Фрагмент бази правил оцінки ефективності системи захисту

IF (ЯКЩО)			THEN (ТО)
Вимоги до захисту інформації	Загроза інформаційній безпеці	Вартість системи захисту	
АІ.3 С	ЗІБ. 01 Н	min	Ефективність СЗІ досягається
АІ.4 НС	ЗІБ. 02 НН	max	Ефективність СЗІ не досягається
...			
КД.2 ЦС	ЗІБ. 0N НН	min	Ефективність СЗІ не досягається

В табл. 3.4 наведено: терм-множинами змінних лінгвістичних є наступні: С - відповідає, ЧС - частково відповідає, ЦС – в цілому відповідає, Н - загроза нейтралізована, НН - загроза не нейтралізована, min - ціна системи захисту мінімальна, max - ціна системи захисту максимальна. Оцінка ефективності Д – досягається, НД – не досягається.

База правил для реалізації методу оцінки ефективності системи захисту конфіденційних даних має наступний вигляд (3.2):

$$
\begin{aligned}
&R_1 : AI.1(C)\,AND ЗІБ.01(H)\,ANDCOST(MIN)\,THENEVALSZI(Д)\\
&R_2 : AI.1(C)\,AND ЗІБ.01(H)\,ANDCOST(MAX)\,THENEVALSZI(Д)\\
&R_3 : AI.1(C)\,AND ЗІБ.01(HH)\,ANDCOST(MIN)\,THENEVALSZI(НД)\\
&R_4 : AI.1(C)\,AND ЗІБ.01(HH)\,ANDCOST(MAX)\,THENEVALSZI(НД)\\
&R_5 : AI.1(ЦС)\,AND ЗІБ.01(H)\,ANDCOST(MIN)\,THENEVALSZI(Д)\\
&R_6 : AI.1(ЦС)\,AND ЗІБ.01(H)\,ANDCOST(MAX)\,THENEVALSZI(Д)\\
&R_7 : AI.1(ЦС)\,AND ЗІБ.01(HH)\,ANDCOST(MIN)\,THENEVALSZI(НД)\\
&R_8 : AI.1(ЦС)\,AND ЗІБ.01(HH)\,ANDCOST(MAX)\,THENEVALSZI(НД)\\
&R_9 : AI.1(ЧС)\,AND ЗІБ.01(H)\,ANDCOST(MIN)\,THENEVALSZI(Д)\\
&\qquad\qquad\qquad\qquad\qquad\qquad ...\\
&R_n : КД.2(ЦС)\,AND ЗІБ.03(HH)\,ANDCOST(MIN)\,THENEVALSZI(НД)
\end{aligned}
\tag{3.2}
$$

Мережа ANFIS у запропонованому методі оцінки ефективності системи захисту конфіденційних даних базується на положеннях розглянутих в другому розділі. За результатами отриманих нелінійних параметрів та їх уточнення процес адаптації нейрона запускається до тих пір, поки не досягне повторення результатів, алгоритм, таким чином, є гібридним. Особливість роботи алгоритму полягає у розподілі етапів навчання. Такий алгоритм нечіткого виведення є найефективнішим, що дозволило, в магістерській роботі, досягти кращого результату у магістерському дослідженні. Структура нечіткої нейронної продукційної мережі ANFIS із застосуванням алгоритму нечіткого виведення Такагі-Сугено-Канга, представлено на рис. 3.2. За рахунок адаптації параметрів

нейронної мережі в магістерському дослідження вдалося досягти найменшої середньоквадратичної помилка (RMSE) на відміну від відомих методів оцінки ефективності систем захисту інформації.

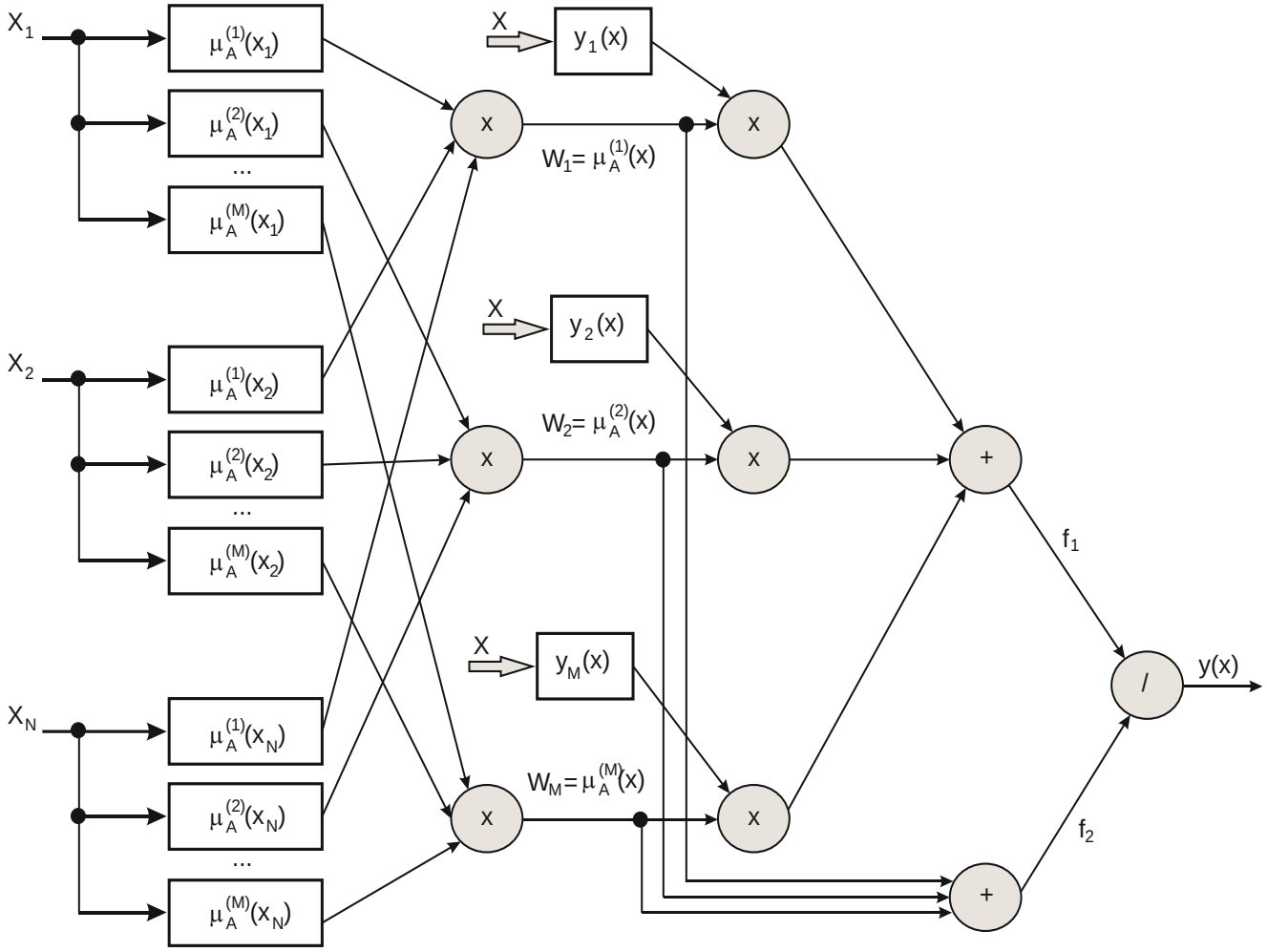


Рисунок 3.2 - Структура нечіткої нейронної продукційної мережі ANFIS із TSK

3.3 Оцінка ефективності методу захисту конфіденційної інформації

Для визначення ефективності запропонованого методу оцінки ефективності систем захисту даних, необхідно розглянути наступні аспекти продукційної нечіткої системи логічного висновку. Нечітка подукційна система логічного висновку представляє собою систему, яка певним чином відображає вхідні дані у

вихідні за допомогою використання трьох основних етапів: фазифікація; логічний вивід; дефаззифікація.

Розглянуто функції приналежності тільки фіксовані, які обрані, відповідним чином, довільно для моделювання оцінки ефективності системи захисту даних, структура правил яких визначена предвизначена експертом інтерпретацією характеристик використовуваних змінних у моделі. У певних ситуаціях моделювання систем захисту неможливо розрізнити, як мають виглядати, маючи набір даних, функції приналежності. Адаптуючи та аналізуючи набір даних для проведення оцінки ефективності системи, неможливо визначити відповідні функції приналежності. Нейро-адаптивні продукційні методи навчання надають методи нечіткого адаптивного моделювання, що дозволяють провести аналіз інформації про набори даних. Метод обчислює відповідні параметри функції приналежності, що дозволяють системі продукційного нечіткого виводу відстежувати дані введення-виведення. Структура адаптивної мережі подібної до нейронної продукційної мережі може використовуватися для інтерпретації входів-виходів, що дозволяє, в свою чергу відображати вхідні дані з набору даних за допомогою використовуваних функцій приналежності та пов'язаних, з цим, параметрів, і потім на основі пов'язаних параметрів та вихідних функцій приналежності для виведення. Параметри, що пов'язані з функціями приналежності, адаптуються у процесі проведення навчання системи. Адаптація та обчислення параметрів спрощується застосуванням вектора градієнта. Вектор градієнта забезпечує міру, наскільки добре система продукційного нечіткого виводу моделює вихідні та вхідні дані з набору даних параметрів. Після отримання вектора градієнта, надалі застосовується процедура оптимізації для налаштування параметрів функції приналежності. Зазначена процедура призначена зменшити значення середньоквадратичної помилки. RMSE визначається сумою квадратів різниці між бажаним та фактичним виходом.

Таким чином, необхідність використання мережі ANFIS, а також її ефективність для проведення оцінки системи захисту інформації стає очевидною.

Наступним кроком при обчисленні ефективності методу оцінки системи захисту інформації, є визначення алгоритму нечіткого виводу. На підставі проведених експериментів, аналізу досліджень, результати яких представлені в третьому розділі, можна зробити висновок, що мережа ANFIS з алгоритмом нечіткого продукційного висновку TSK (Такагі-Сугено-Канга), для вирішення задач проведення оцінки ефективності системи захисту інформації є найкращою.

Якість запропонованого методу оцінки ефективності системи, порівняно з існуючими методами, досягається наступними показниками: фінансові витрати можуть досягти зменшення вартості створюваної системи захисту, до 25%, ефективність системи захисту досягає 97%.

Поставлену задачу, в магістерському дослідженні щодо підвищення якості оцінки ефективності системи захисту розподіленої інформаційної системи можна вирішувати з використанням методів класифікації, які використовують різні підходи реалізації та математичні апарати, проте, ефективність використовуваних методів залежить від конкретної вирішуємої задачі. У магістерській роботі проведено порівняльний аналіз методів розв'язання поставленої задачі, порівняльний аналіз наведено в табл. 3.5.

Таблиця 3.5 - Порівняльний аналіз методів для вирішення поставленої задачі

Метод	Переваги	Недоліки
Метод Байєса (Naive Bayes, NB)	Швидкодія методу. Підтримка інкрементного навчання.	Відносно низька якість класифікації;
Метод *k*-найближчих сусідів (*KNN*)	Простота реалізації. Опрацьована теоретична база. Адаптація під необхідну задачу.	Недостатня продуктивність у реальних задачах. Труднощі в наборі ваг.
Метод опорних векторів	Еквівалентна двошарова нейронна мережа- простота реалізації	Неможливість калібрування попадання у клас
Метод дерев рішень	Висока продуктивність навчання та прогнозування. Дозволяє працювати з великим об’єом інформації	Проблема отримання оптимального дерева рішень

В магістерській роботі проведені експерименти порівняльного аналізу досліджень роботи методів та запропонованого методу, наведених у табл. 3.6. Як порівняльна характеристика, при проведенні експериментів, використовувалася точність визначення досяжності/не досяжності ефективності системи захисту розподіленої інформаційної системи (точність класифікації). Результати роботи досліджуваних методів оцінювалися експертним шляхом кожного із експериментів. Результати порівняльного аналізу наведено у табл. 3.6.

Таблиця 3.6 – Результати порівняльного аналізу

	Наївний Байєс	Метод *k*- найближчих сусідів	Дерева рішень	Логістична регресія	Запропонований метод на основі ANFIS
Точність ефективності %	86,7	70,4	92,1	93,6	97,2

На рис. 3.3 наведено графік порівняльного аналізу методів для вирішення поставленої задачі у магістерському дослідженні.

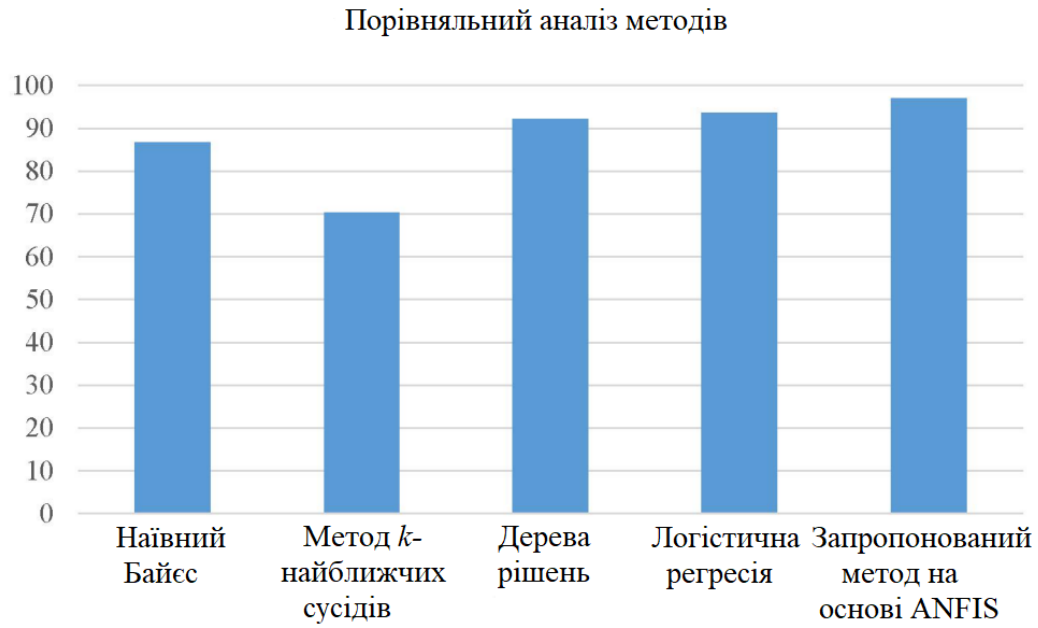


Рисунок 3.3 – Графік порівняльного аналізу методів

Таким чином, для заданих умов задачі (сформованого набору даних після перетворення, очищення, створених нових більш репрезентативних ознак та вибору найбільш корисних) та визначених у магістерській роботі показників оцінки ефективності системи захисту, запропонований метод є кращим у порівнянні з відомими методами. Аналіз дослідження наведено в табл. 3.7.

Таблиця 3.7 – Аналіз оцінки ефективності запропонованого методу

Показник	Існуючі методи	Запропонований метод
RMSE	0,022-0,214	0,012-0,017
Ефективність системи захисту	85,6%	97,2%
Вартість системи	зниження до 15%	зниження до 30%

Середньоквадратична помилка запропонованого методу, обчислюється за формулою: $RMSE = \sqrt{\frac{1}{N}\sum_{i=1}^{N}\left(y_i - y_i\right)^2}$, де y_i, y_i - набори даних (перевірки, навчання). Графіки порівняння RMSE відомих та запропонованого методу на заданому інтервалі представлені на рис. 3.4.

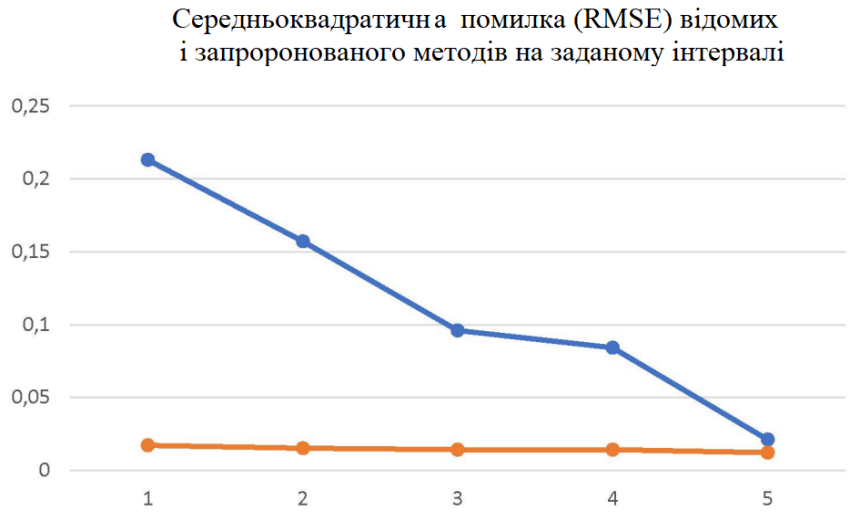


Рисунок 3.4 - Графік порівняння RMSE на заданому інтервалі

Середньоквадратична помилка RMSE досягає значення в діапазоні 0,012-0,017, є локальним мінімумом на заданому інтервалі та дозволяє довести виконання поставленої в магістерському дослідженні задачі.

3.4 Висновки

У розділі визначено достатні та необхідні показники, запропоновано метод оцінки ефективності систем захисту, заснований на продукційній, адаптивній нейронній нечіткій системі та алгоритмі нечіткого виведення *TSK* (Такагі-Сугено-Канга), на відміну від відомих, дозволяє досягати меншого значення RMSE - середньоквадратичної помилки роботи системи захисту, підвищує ефективність проведення оцінки системи до 97%, що на 15% вище порівняно з відомими, фінансові витрати на створення системи захисту даних дозволяють досягати зменшення вартості розробки системи до 30%. Запропонований метод оцінки ефективності дозволяють власникам систем автоматично оцінювати ефективність системи захисту у режимі реального часу на всіх етапах проведення життєвого циклу системи, що дозволяє, при цьому, своєчасно внести коригування до проектних рішень системи захисту для нейтралізації актуальних загроз інформаційній безпеці та виконання вимог щодо захисту інформації, також враховуючи фінансову складову. Слід зазначити, що для запропонованого методу, показники оцінки ефективності можуть бути змінені залежно від потреб та цілей власника системи у проведенні оцінки ефективності системи захисту.

Метод має наступні переваги та відмінні риси на відміну від існуючих: не вимагає залучення висококваліфікованих фахівців в області безпеки інформації; запропоновані показники оцінки ефективності системи захисту дозволяють найбільш точно проводити оцінку; дозволяє оцінити фінансові витрати на створення системи; використовує мінімальні обчислювальні ресурси; дозволяє своєчасно вносити коригування в проектні рішення щодо системи захисту.

4 РЕАЛІЗАЦІЯ МЕТОДУ ОЦІНКИ ЕФЕКТИВНОСТІ СИСТЕМИ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

4.1 Оцінка відповідності систем захисту до вимог безпеки конфіденційної інформації

Для проведення дослідження розподіленої інформаційноїсистеми обрано систему, що є одночасно системою третього класу захищеності державною інформаційною та системою обробки персональних даних четвертого рівня захищеності. Для проведення оцінки ефективності системи захисту необхідно виконати наступні кроки: обстеження ІТ-інфраструктури (технології обробки інформації) інформаційної системи; визначення актуальних загроз інформаційній безпеці; формування переліку вимог до захисту конфіденційних даних; підготовка набору даних для оцінки ефективності системи захисту ІС, що включає: перелік актуальних загроз інформаційній безпеці, ІТ-інфраструктуру інформаційної системи, перелік до використання засобів захисту інформації та їх вартість, перелік вимог щодо захисту інформації; експертні оцінки відповідності вимог інформаційної системи щодо захисту інформації; оцінка ефективності системи захисту на підставі запропонованого методу оцінки ефективності системи захисту; внесення коригувань до рішень проектування системи захисту.

Форми оцінки відповідності систем захисту вимогам безпеки інформації регламентуються законом України “Про технічні регламенти та оцінку відповідності” (від 15.01.2015 № 124-VIII). Закон регулює відношення, що виникають при: прийнятті, розробленні, застосуванні, виконанні обов'язкових вимог до процесів виробництва, продукції, зберігання, експлуатації, перевезення, утилізації та реалізації; прийнятті, розробленні, виконанні та застосуванні на добровільній основі вимог до процесів виробництва, продукції, експлуатації,

реалізації, утилізації, зберіганні, перевезенні, виконання робіт, надання послуг; оцінка відповідності вимогам; визначає обов'язки та права учасників у сфері технічного регулювання відношень.

Основні визначення закону: оцінка відповідності вимогам - опосередковане , пряме визначення дотримання вимог до об'єкта; підтвердження відповідності – документальне підтвердження відповідності об'єктів, продукції, процесів вимогам положенням стандартів, технічних регламентів, умов договорів.

Проведення оцінки ефективності та оцінки відповідності систем захисту інформації ІС є обов'язковим для державних інформаційних систем, систем обробки персональних даних, критичних інформаційних інфраструктур, автоматизованих систем управління технологічними процесами.

Атестація об'єктів інформатизації застосовується для оцінки відповідності вимогам захисту об'єктів інформатизації, підтвердження відповідності об’єктів, вимогам інформаційної безпеки. Об'єкт інформатизації (за вимогами безпеки інформації) - автоматизовані системи різного призначення та рівня, системи зв'язку, відображення та розміщення разом з приміщеннями, де встановлені, призначені для передачі та обробки інформації, що підлягає захисту, приміщення, призначені для ведення конфіденційних переговорів. Такими об'єктами є: виділені та захищаємі приміщення; засоби розмноження та виготовлення секретних документів; автоматизовані системи.

Обов'язковим проведення атестації для інформаційних систем, що обробляють інформацію, що становить державну таємницю та державних інформаційних систем, в інших випадках атестація інформаційної системи має добровільний характер.

Існують форми оцінки відповідності інформаційної системи у формах приймання системи захисту інформаційної системи, у формі декларації відповідності, встановлених законом України “Про технічні регламенти та оцінку відповідності”. Як правило, такі форми оцінки, недостатньо повно відображають реальну оцінку системи захисту інформаційної системи, через недоліки

експертного методу та суб'єктивні точки зору членів комісії. Пропонуються методичні рекомендації оцінки ефективності системи захисту розподілених інформаційних систем та не торкаються питань проведення атестації об'єктів інформатизації. Оцінка ефективності - ефективність системи захисту інформації досягається шляхом розробки системи захисту, здатної максимально нейтралізувати актуальні загрози інформаційній безпеці, виконати вимоги до захисту інформації, які пред'являються інформаційній системі на підставі визначених вимог регуляторами у сфері забезпечення інформаційної безпеки інформації, дозволяє, при цьому, максимально мінімізувати фінансові витрати на розробку системи захисту інформації.

4.2. Алгоритм оцінки ефективності систем захисту розподілених інформаційних систем

Алгоритм оцінки ефективності систем захисту розподілених інформаційних систем складається з наступних кроків:

1. Підготовка набору даних для оцінки ефективності систем захисту розподілених інформаційних систем, складається: відомості про IT-інфраструктуру розподіленої інформаційної системи; перелік актуальних загроз інформаційній безпеці у розподіленій інформаційній системі; перелік вимог щодо інформаційної безпеки; перелік засобів захисту інформації, що використовуються в розподіленій інформаційній системі; вартість створення системи захисту (вартість засобів захисту від виробників).

2. Аналіз, конвертація, форматування набору даних.

3. Формування бази правил для оцінки ефективності системи захисту розподілених інформаційних систем.

4. Проведення оцінки ефективності систем захисту розподілених інформаційних систем.

5. Оформлення результатів проведення оцінки ефективності систем захисту розподілених інформаційних систем. Внесення коригувань у проектні рішення, за потреби.

Алгоритм проведення оцінки ефективності та життєвого циклу розробки системи захисту та представлені на рис. 4.1 та рис. 4.2 відповідно.

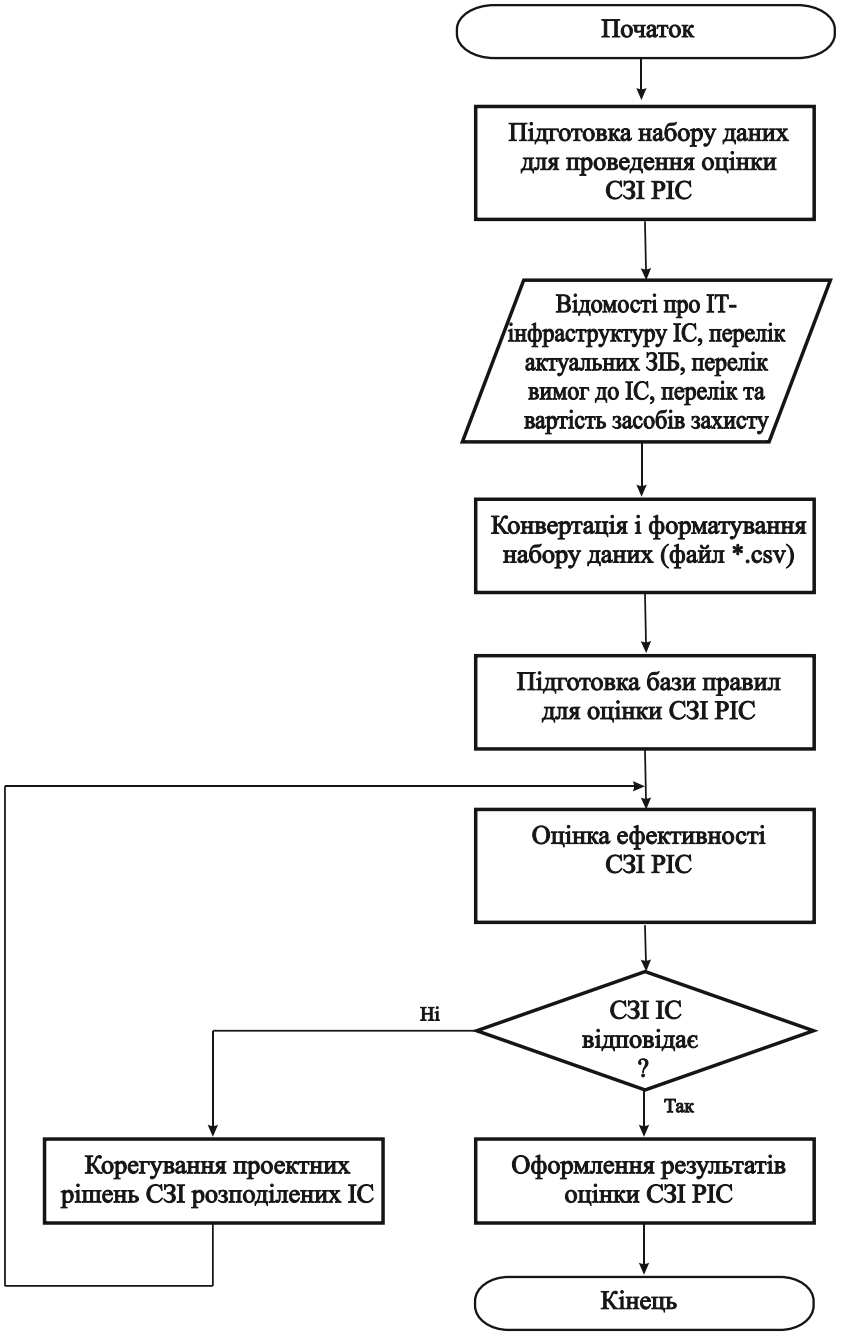


Рисунок 4.1 - Алгоритм оцінки ефективності системи захисту розподіленої інформаційної системи

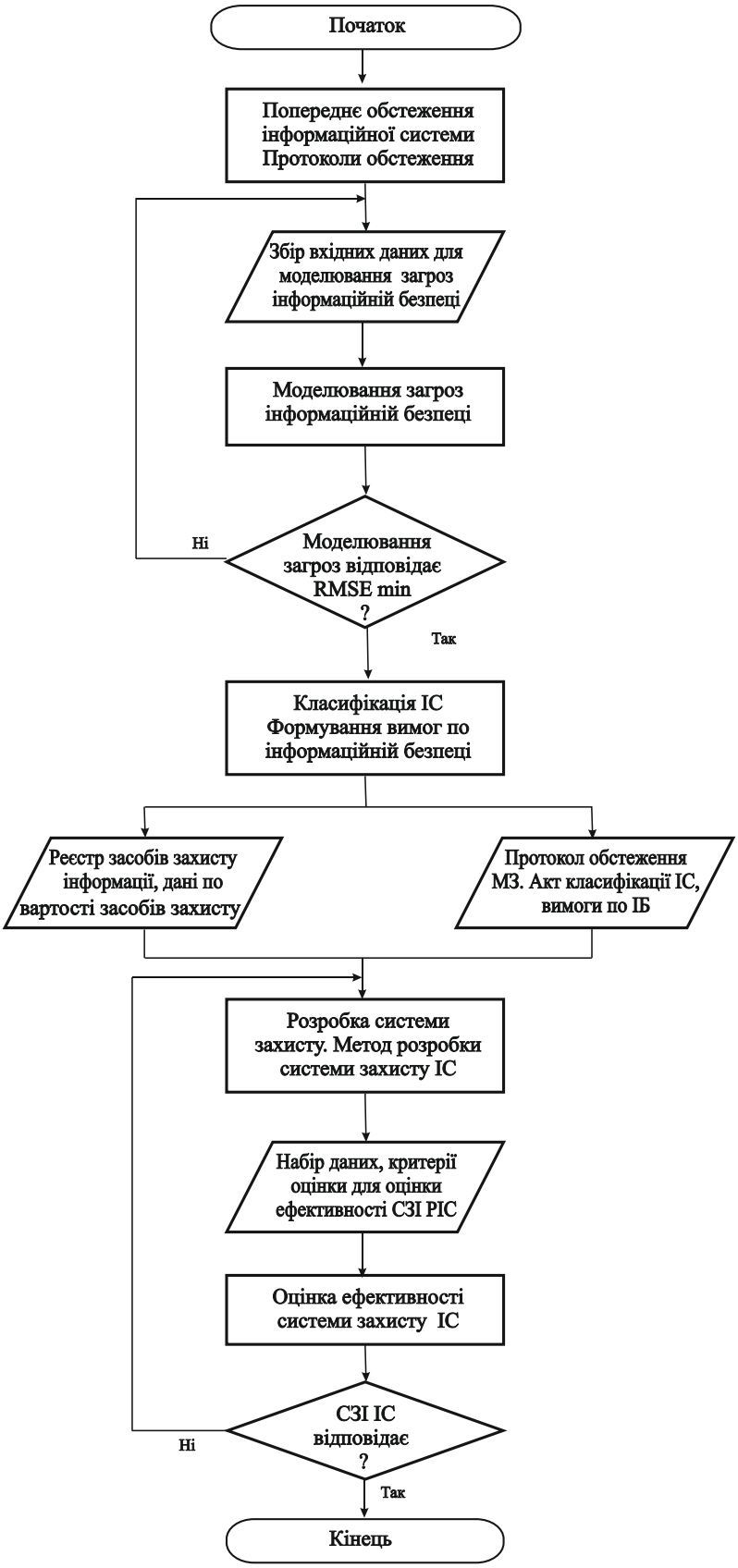


Рисунок 4.2 - Алгоритм життєвого циклу розробки системи захисту розподіленої інформаційної системи

Проведення оцінки ефективності системи захисту інформації необхідно виконнати, відповідно до методичних рекомендацій, наступні кроки:

1. Провести обстеження розподіленої інформаційної системи, за результатами обстеження формується протокол, який включає опис IT-інфраструктури системи, а також відомі системи захисту інформації.

2. Визначити актуальні загрози інформаційній безпеці відповідно до методичних документів регуляторів. Визначити категорію значущості розподіленої інформаційної системи, клас, тип, рівень захищеності. Актуальні загрози інформаційній безпеці.

3. Сформувати, на підставі переліку актуальних загроз інформаційній безпеці, класифікації, та вимог до захисту інформації, перелік вимог.

4. Сформувати набір даних, що включає: IT-інфраструктуру розподіленої інформаційної системи, перелік актуальних загроз інформаційній безпеці в інформаційній системі, перелік вимог до захисту інформації, перелік використання засобів захисту інформації в системі захисту та їх вартість.

5. Враховати та провести експертні оцінки відповідності розподіленої системи вимогам щодо захисту інформації.

6. На підставі розробленого методу оцінки ефективності системи захисту провести оцінку ефективності системи захисту розподіленої інформаційної системи.

7. На підставі отриманих результатів оцінки ефективності системи захисту розподіленої інформаційної системи за необхідності впровести коригування до проектних рішень системи захисту інформації.

Структурна схема проведення оцінки ефективності системи захисту інформації розподіленої інформаційної системи наведена на рис. 4.3.

Процес проведення оцінки ефективності системи захисту складається з п'яти підсистем:

1. Підсистема обстеження розподіленої інформаційної системи.

2. Підсистема моделювання загроз інформаційній безпеці.

3. Підсистема формування вимог до системи щодо захисту інформації.

4. Підсистема оцінки ефективності системи захисту розподіленої інформаційної системи.

5. Підсистема коригування проектних рішень розробки системи захисту розподіленої інформаційної системи.

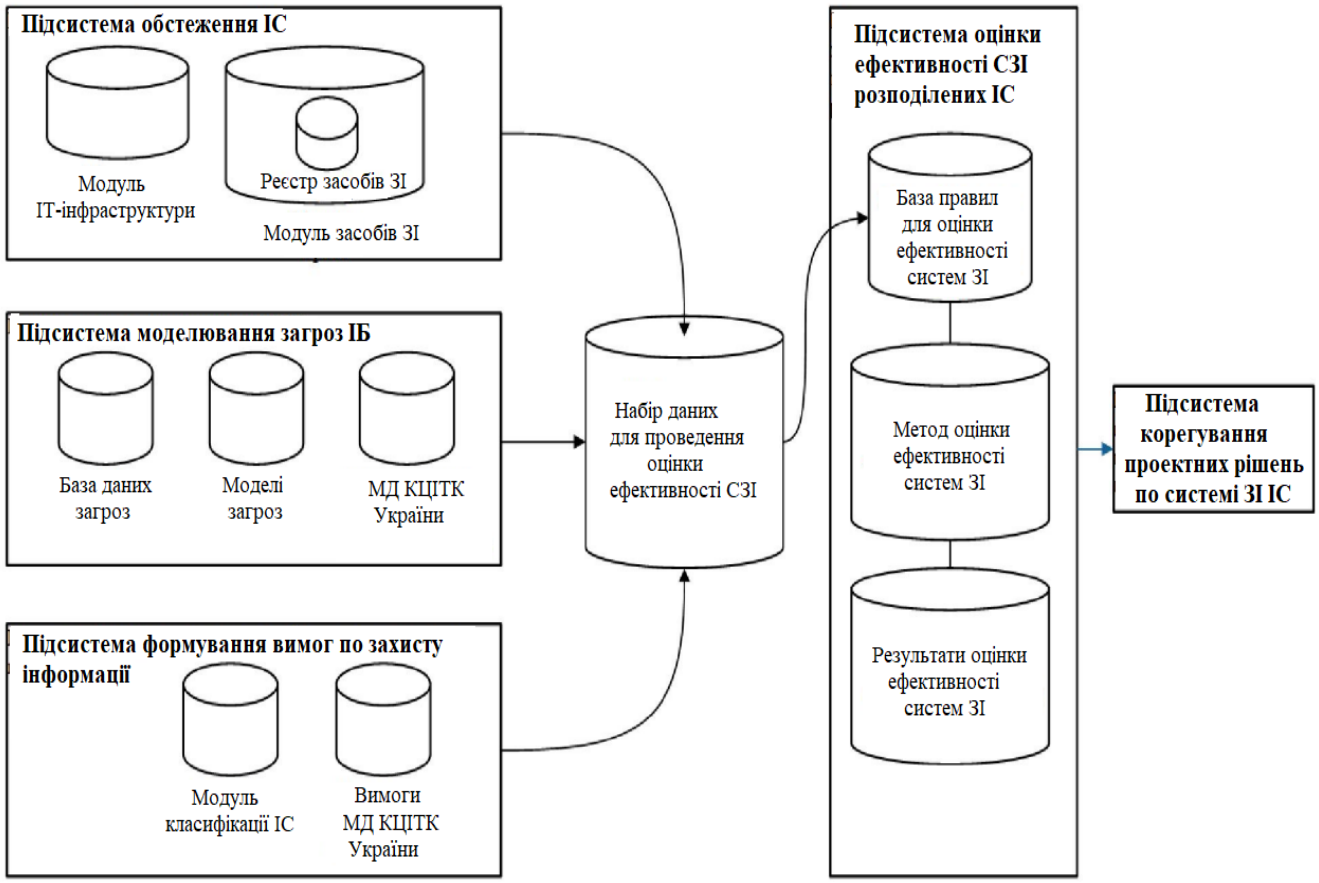


Рисунок 4.3 - Структурна схема оцінки ефективності системи захисту ІС

Запропоноване розбиття на підсистеми системи оцінки ефективності обумовлено незалежністю кожної з них, що, у свою чергу, дозволяє, у процесі проведення оцінки ефективності системи захисту інформації розподіленої інформаційної системи вносити коригування без внесення змін до суміжних підсистем.

4.3 Реалізація методу оцінки ефективності системи захисту інформації розподілених інформаційних систем

На підставі запропонованого методу оцінки ефективності системи захисту інформації розподілених інформаційних систем проведено оцінку ефективності системи. Система реалізована у форматі клієнт-серверної архітектури. Інформаційна система надає можливості модифікацій з урахуванням відкритого програмного інтерфейсу з використанням мов програмування (TypeScript, C# (середовище розробки dotnet.core, платформа розробки Angular)).

Система забезпечує принцип централізованого накопичення, зберігання, багаторазового використання даних. На робочих місцях користувачів зберігання даних не здійснюється, до складу інфраструктури інформаційної системи входять:

1. Сервери, включають: серверне обладнання; спеціалізоване та прикладне програмне забезпечення, забезпечують обробку інформації та представлення у вигляді, необхідному для подальшої автоматизованої обробки.

2. АРМ користувачів: типові робочі місця користувачів; АРМ керівника: використовується керівниками вищої ланки (мобільний пристрій).

Серверні компоненти інформаційної системи розміщені в середовищі віртуалізації. Апаратно-програмний комплекс віртуалізації системи складається з п’яти серверів віртуалізації на основі програмного забезпечення VMware, працює під управлінням сервера vCenter, мережі зберігання даних SAN.

У середовищі віртуалізації інформаційної системи розгорнуто віртуальні сервери: сервери програм; сервери OpenVPN для підключення віддалених користувачів із мережі Інтернет загального користування; сервери балансувальника навантаження Load Balancer; сервер СУБД; сервер для онлайн перегляду; термінальні сервери; сервери для веб-перегляду; менеджмент-сервер; сервери синхронізації для мобільного автоматизованого робочого місця.

Система зберігання даних, включає: повільне сховище – для Backup файлів віртуальних машин; швидкісні сховища - для зберігання файлів віртуальних машин.

Резервне копіювання даних інформаційної системи виконується з використанням можливостей Veeam Backup & Replication і MS SQL Server, не регламентовано час зберігання резервних копій.

Доступ до інформаційної системи для виконання функцій адміністрування IT-інфраструктури компонентів здійснюється з АРМ адміністратора, розташованих в межах контрольованої зони (периметра) системи. Контрольована зона інформаційної системи включає простори (приміщення, територія, будівлі), в яких розміщуються компоненти, виключено неконтрольоване перебування сторонніх транспортних засобів, відвідувачів.

Інформаційний обмін даними між клієнтськими робочими місцями та серверами забезпечується з використанням організацій користувачів та ресурсів обчислювальних мереж, є можливість віддаленої роботи за межами локальної обчислювальної мережі з об'єктом інформатизації з використанням робочих місць.

До об’єктів захисту інформаційної системи відносяться: персональні дані, що обробляються в розподіленій інформаційній системі; технічні засоби, для обробки інформації (системи та засоби зв'язку передачі даних, машинні носії); прикладне та системне програмне забезпечення; засоби захисту інформації; засоби криптографічного захисту інформації; середовище функціонування системи криптографічного захисту інформації; інформація, що відноситься до криптографічного захисту інформації (персональні дані, аутентифікуючу та парольну інформацію); документи, журнали, видання, картотеки, технічні документи, кіно-, відео-, фотоматеріали, робочі матеріали, в яких відображена інформація, що відноситься до інформаційної системи персональних даних, їх криптографічний захист; носії інформації, що використовуються в розподіленій інформаційній системі у процесі криптографічного захисту даних, носії автентифікуючої, ключової, парольної інформації та порядок доступу до них;

використовувані розподіленої інформаційної системи лінії (канали) зв'язку, включаючи кабельні системи; приміщення, в яких знаходяться ресурси розподіленої інформаційної системи, які мають відношення до криптографічного захисту інформації.

У розподіленій інформаційній системі обробляються наступні категорії інформації: службова інформація; персональні дані; технічні параметри розподіленої інформаційної системи, файли налаштувань та конфігураційні файли прикладного та системного програмного забезпечення, включаючи програмне забезпечення засобів системи.

Відповідно до алгоритму запропонованого методу проведено дослідження інформаційної системи, за отриманими результатами запропоновано модель загроз безпеки даних, з використанням запропонованого методу визначення актуальних загроз інформаційній безпеці.

За результатами дослідження інформаційної системи, визначення переліку актуальних загроз інформаційній безпеці та класифікації сформовано вимоги щодо захисту інформації.

В якості реалізації системи захисту інформаційної системи, наведено опис підсистеми реєстрації подій безпеки та захисту середовища віртуалізації. Підсистема захисту середовища віртуалізації забезпечує реалізацію наступних функцій: управління доступом суб'єктів доступу до об'єктів доступу у віртуальній інфраструктурі, також всередині віртуальних машин; аутентифікація та ідентифікація об'єктів доступу та суб'єктів доступу у віртуальній інфраструктурі, також адміністраторів управління засобами віртуалізації; реєстрація подій безпеки у віртуальній інфраструктурі; контроль цілісності віртуальної інфраструктури та її конфігурації; резервне копіювання даних, резервування каналів зв'язку всередині віртуальної інфраструктури, технічних засобів, програмного забезпечення віртуальної інфраструктури; керування переміщенням контейнерів (віртуальних машин) та даних, що на оброблюються; сегментування віртуальної інфраструктури (розбиття віртуальної інфраструктури системи на сегменти) для

подальшої обробки персональних даних групою користувачів або окремим користувачем; управління та реалізація антивірусним захистом у віртуальній інфраструктурі.

В якості підсистеми захисту середовища віртуалізації в інформаційній системі використовується сертифікований засіб захисту інформації - vGate. засіб захисту інформації vGate R2 забезпечує реалізацію функцій підсистеми захисту середовища віртуалізації, здійснює фільтрацію трафіку на рівні гіпервізора, дозволяє контролювати дії адміністраторів віртуальної інфраструктури та захист від специфічних загроз віртуалізації. До складу програмного забезпечення vGate входять консоль управління засобами захисту інформації, сервер авторизації, які встановлюються на автоматизованому робочому місці адміністратора по інформаційній безпеці. На рис. 4.4 представлена логічна схема підсистеми захисту середовища віртуалізації, реалізована із застосуванням засобу vGate R2.

Рисунок 4.4 – Логічна схема підсистеми захисту середовища віртуалізації ІС

Підсистема реєстрації подій безпеки забезпечує виконання наступних функцій: визначення подій безпеки та строків їх зберігання, що підлягають реєстрації; зберігання, збір, запис інформації про події безпеки протягом

встановленого політикою безпеки часу зберігання; визначення змісту, складу інформації про події безпеки, що підлягають реєстрації; захист інформації щодо подій безпеки; перегляд, аналіз (моніторинг) результатів реєстрації подій безпеки та реагування на події безпеки. Засобами забезпечення відповідних функцій підсистеми реєстрації подій безпеки є журнали безпеки засіб безпеки інформації Dallas Lock 8.0-К, комплект програмного забезпечення засіб захисту інформації EMM SafePhone, в якому міститься інформація про дії користувачів, починаючи з моменту входу користувача в операційну систему, про помилки, пов'язані з доступом до тих чи інших об'єктів, зокрема до тих додатків, доступ до яких заборонено. Засіб захисту інформації Dallas Lock 8.0-К містить наступні журнали: журнал управління обліковими записами; журнал входів; журнал ресурсів; журнал управління політиками; журнал друку; журнал пакетів міжмережевих екранів; журнал процесів; журнал з'єднань міжмережевих екранів; журнал контролю додатків; журнал трафіка; журнал подій операційної системи.

У кожному журналі фіксуються час, дата, операція, ім'я користувача, результат, інші параметри. Можливе, також, впорядкування (фільтрація) елементів списків журналу за необхідним значенням. На рис. 4.5 наведена логічна схема підсистеми реєстрації подій безпеки, реалізована із застосуванням засобу захисту інформації Dallas Lock 8.0-К. Перелік підсистем та функцій захисту інформації в досліджувальній магістерській роботі системи захисту наведено в табл. 4.1.

Таблиця 4.1 - Підсистеми та функції захисту конфіденційних даних

Підсистема	Функції
1	2
Підсистема автентифікації та ідентифікації суб'єктів доступу, об'єктів доступу	Аутентифікація ідентифікація користувачів, Управління ідентифікаторами. Управління засобами аутентифікації, видача, ініціалізація, зберігання, блокування Захист зворотного зв'язку. Аутентифікація та ідентифікація пристроїв, у тому числі стаціонарних, мобільних та портативних

Продовження таблиці 4.1

1	2
Підсистема управління доступом	Управління обліковими записами користувачів. Реалізація рольового або дискреційного методу доступу. Управління інформаційними потоками між пристроями, сегментами розподіленої інформаційної системи, а також між інформаційними підсистемами. Розподіл повноважень (ролей) користувачів, адміністраторів. Призначення мінімально необхідних прав та привілеїв користувачам, адміністраторам. Обмеження неуспішних спроб входу до ОС. Реалізація захищеного дистанційного доступу суб'єктів до об'єктів через зовнішні інформаційно-телекомунікаційні мережі. Дозвіл (заборона) дій користувачів, дозволених до аутентифікації та ідентифікації.
Підсистема обме-ження ПС	Забезпечення можливості встановлення лише дозволеного до використання програмного забезпечення
Підсистема захисту МН	Облік МН. Управління доступом до МН. Контроль переміщення МН за межі контрольованої зони системи. Контроль підключення МН.
Підсистема реєстрації подій безпеки	Визначення подій безпеки, що підлягають реєстрації та термінів їх зберігання. Визначення складу та змісту інформації про події безпеки, що підлягають реєстрації. Збір, запис та зберігання інформації про події безпеки протягом встановленого часу зберігання. Моніторинг (перегляд, аналіз) результатів реєстрації подій безпеки
Підсистема антивірусного захисту	Антивірусний захист АРМ та серверів розподіленої інформаційної системи. Оновлення бази даних ознак шкідливих комп'ютерних програм (вірусів)
Підсистема аналізу захищенності	Виявлення, аналіз уразливостей інформаційної системи Контроль установки оновлень програмного забезпечення, Контроль працездатності, параметрів налаштування та правильності функціонування програмного забезпечення. Контроль складу технічних засобів, програмного забезпечення. Контроль правил генерації та зміни паролів користувачів, реалізації правил розмежування доступу, повноважень користувачів.

Закінчення таблиці 4.1

Підсистема виявлення вторгнень	Виявлення вторгнень. Оновлення бази вирішальних правил
Підсистема забезпечення мережевої безпеки	Реалізація функції міжмережевого екранування в точках взаємодії розподіленої інформаційної системи. Захист мережевої інфраструктури розподіленої інформаційної системи.
Підсистема централізованого управління засобами захисту інформації	Управління засобами захисту інформації. Адміністрування засобів захисту інформації. Управління оновленнями програмного забезпечення. Розповсюдження виправлень ПЗ. Отримання виправлень та інших оновлень безпеки ПЗ для централізованої установки на сервери та АРМ

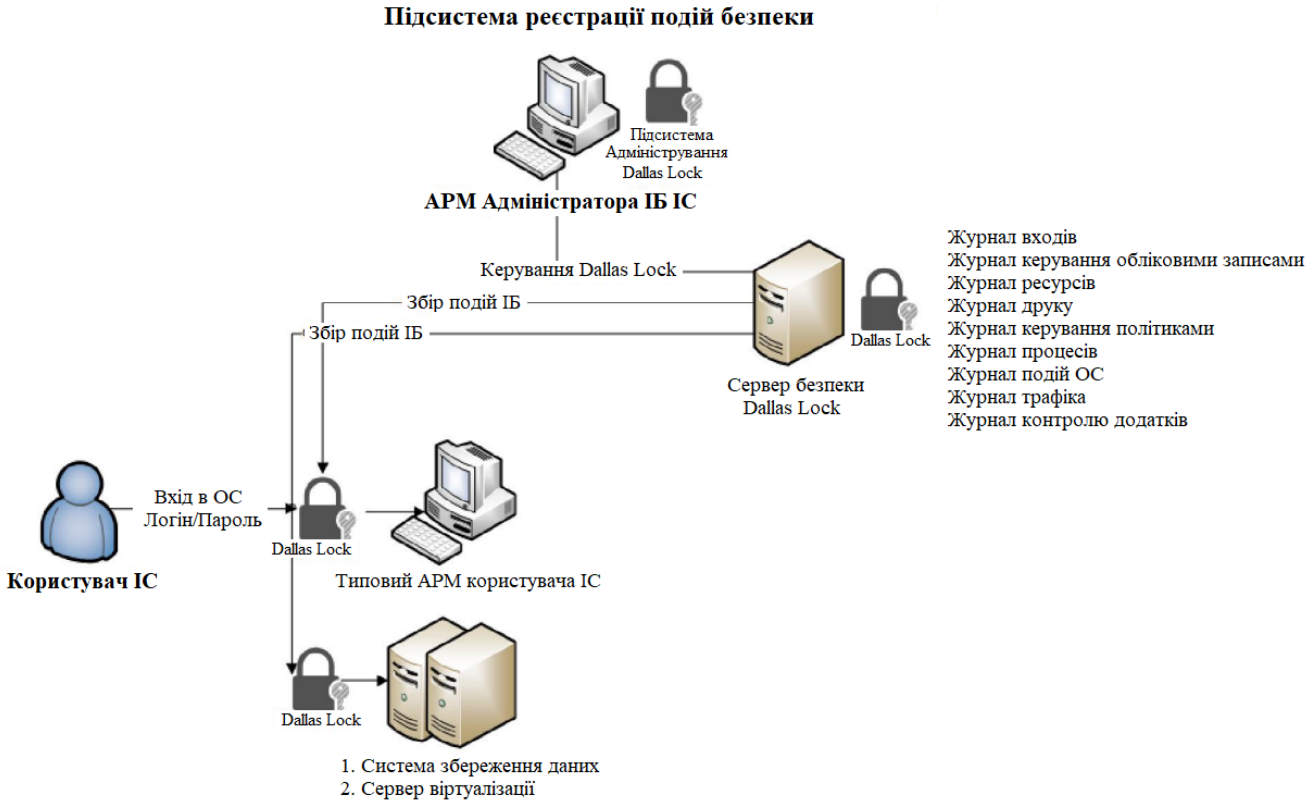


Рисунок 4.5 – Логічна схема підсистеми реєстрації подій

Отримані результати проведеної оцінки показали не ефективність запропонованих рішень щодо захисту конфіденційної інформації: проектні

рішення не враховують нейтралізацію всіх актуальних загроз інформаційній безпеці; ефективність системи захисту інформації можна підвищити за рахунок зменшення вартості запланованих засобів захисту інформації.

Проведена оцінка ефективності системи захисту інформації дозволить внести коригування в проектні рішення системи захисту інформації на ранньому етапі, що дозволяє заощадити фінансові витрати на створення системи захисту, запобігти ризикам витоку даних.

Для оцінки ефективності запропонованих підходів необхідно враховувати порядок проведення оцінки виходячи з визначення вимог власників розподілених інформаційних систем. Ефективність системи захисту інформації досягається шляхом створення системи захисту, здатної максимально нейтралізувати актуальні загрози інформаційній безпеці у розподіленій інформаційній системі, виконати вимоги щодо захисту конфіденційних даних, які пред'являються до розподілених систем на підставі вимог власників в області забезпечення інформаційній безпеці, дозволяє знизити фінансові витрати на створення системи захисту.

Однією з форм оцінки відповідності системи є атестація. За умовами задачі, поставленими в магістерській роботі, метод оцінка ефективності системи захисту розподіленої інформаційної системи має бути використаний на всіх етапах життєвого циклу інформаційної системи для своєчасного внесення змін до проектних рішень щодо захисту конфіденційних даних. Методичні рекомендації, запропоновані показники, а також метод визначення актуальних загроз інформаційній безпепці, методу оцінки ефективності системи захисту дозволяють проводити оцінку ефективності системи захисту конфіденційних даних на всіх етапах життєвого циклу розподіленої інформаційної системи. Таким чином, поставлена задача, в магістерському дослідженні підвищення якості оцінки ефективності системи захисту розподіленої інформаційної системи досягнута.

4.4 Висновки

Розроблені заходи щодо оцінки ефективності систем захисту інформації у розподілених інформаційних системах, на відміну від відомих, дозволяють власникам розподілених інформаційних системах в режимі реального часу оцінювати ефективність системи захисту, знизити фінансові витрати на розробку системи захисту, використання запропонованих заходів не потребує великих обчислювальних ресурсів, залучення висококваліфікованих фахівців з інформаційної безпеки, ефективність систем захисту в розподілених інформаційних системах сягає 97%.

Запропоновані в магістерському дослідженні заходи дозволяють:

- мінімізувати проведення непотрібних та зайвих кроків проведення оцінки;
- враховувати всі аспекти процесу проведення оцінки ефективності системи захисту розподіленої інформаційної системи;
- враховувати під час проведення оцінки ефективності системи захисту вимоги у сфері забезпечення інформаційної безпеки;
- автоматизувати процес оцінки, не потребує залучення висококваліфікованих спеціалістів у області інформаційної безпеки, виключити недоліки експертних методів;
- може бути адаптована під умови власників розподілених інформаційних систем.

ВИСНОВКИ

Поставлена в магістерському дослідженні задача щодо підвищення якості оцінки ефективності систем захисту конфіденційних даних розподілених інформаційних систем за рахунок визначення достатніх та необхідних показників досягнута. Для досягнення мети виконана та поставлена задача, що містить наступні результати дослідження:

1. Проведено аналіз розподілених інформаційних систем, визначено ключові аспекти IT-інфраструктури розподілених систем та систем захисту інформації, проведено аналіз методів та моделей інформаційних систем, моделей загроз інформаційній безпеці та атак, методів оцінки ефективності систем захисту інформації.

2. Запропоновано метод визначення актуальних загроз інформаційній безпеці, на відміну від відомих, в автоматизованому режимі формує перелік актуальних загроз інформаційній безпеці, мінімізує обчислювальні ресурси та трудомісткість процесу.

3. Запропонований метод оцінки ефективності систем захисту даних, заснований на теорії адаптивних продукційних нечітких нейронних систем та алгоритмі нечіткого виведення TSK. Дозволяє проводити оцінку ефективності систем захисту даних на основі достатніх та необхідних показників.

4. Запропоновані заходи щодо оцінки ефективності систем захисту інформації у розподілених інформаційних системах, на відміну від відомих, дозволяють власникам розподілених інформаційних систем у режимі реального часу оцінювати ефективність системи захисту, знизити фінансові витрати на розробку системи захисту даних, не потребує залучення висококваліфікованих фахівців з безпеки інформації, великих обчислювальних ресурсів.

Запропоновані заходи дозволяють: враховувати всі аспекти проведення оцінки ефективності системи захисту розподіленої інформаційної системи; може бути адаптована під умови власників розподілених інформаційних систем;

виключає недоліки експертних методів, процес автоматизований, не вимагає залучення висококваліфікованих спеціалістів у області інформаційної безпеки.

Ефективність запропонованого методу підтверджується: достовірними результатами визначення переліку актуальних загроз інформаційній безпеці та досягнення ефективності системи захисту конфіденційних даних; відсутністю необхідності залучення висококваліфікованих фахівців в області безпеки інформації; використанням мінімальних обчислювальних ресурсів; можливістю адаптації під конкретні цілі власників розподілених інформаційних систем при проведенні оцінки ефективності системи захисту.

Результати магістерського дослідження з оцінки ефективності системи захисту розподілених інформаційних систем можуть бути використані для управління життєвим циклом інформаційних систем, проведення оцінки стану IT-інфраструктури, парку автоматизованих робочих місць; з метою оцінки відповідності підприємств підходам до управління інформаційними технологіями.

За темою роботи опубліковано 1 теза та 1 наукова стаття.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Біленчук, П.Д. Правові засади інформаційної безпеки України: монографія /Л.В. Борисова, І.М. Неклонський.– Харків: 2018. – 289 с.

2. Богуш, В.М. Інформаційна безпека держави / В.М. Богуш, О.К. Юдін. – К.: МК-Прес, 2015. – 432 с.

3. Буров, Є.В. Комп'ютерні мережі. Том 1. / Є.В. Буров, М.М. Митник // Навчальний посібник – Львів, «Магнолія 2006», 2019р.- 256 с.

4. Буров, Є.В. Комп'ютерні мережі. Том 2. / Є.В. Буров, М.М. Митник // Навчальний посібник – Львів, «Магнолія 2006», 2019р. - 334 с.

5. Бурячок, В.Л. Інфомаційна та кібербезпека / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко – К.: ДУТ, 2015р. – 288 с.

6. Бурячок, В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : посібник / В. Л. Бурячок, С. В. Толюпа, В. В. Семко – К. : ДУТ-КНУ, 2016. – 178 с.

7. Василюк, В. Об'єкти захисту інформації. Методи та засоби захисту інформації / В. Василюк // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, 2016р. - 88 с.

8. Вербіцький, О.В. Вступ до криптології / О.В. Вербіцький. – Львів : ВНТЛ, 2017р. – 248 с.

9. Гончар С. Ф. Оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури : монографія./ С.Ф. Гончар. – Київ,2019.–175с.

10.Гошубєв, О.В. Програмно-технічні засоби захисту даних від комп'ютерних злочинів / О. В. Гошубєв– Запоріжжя : «Павел», 2018. – 145

11. Гошубєв, О.В. Розслідування комп'ютерних злочинів / О.В. Гошубєв – «Запоріз. ін-т муніцип. упр. і держ.», 2017. – 297 с.

12. Горбулін, П.В. Проблеми захисту інформаційного простору України / М.М. Бачeнок, П.В. Горбулін – К.: Інтертехнологія, 2019. – 138 с.

13. Державний стандарт України Захист інформації. Технічний захист інформації. Основні положення. ДСТУ 3396.0-96 [Електронний ресурс]. – Режим доступу:
http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?at_id=38883&cat_id =38836

14. Джулій, В.М. Інформаційно-ознакова модель шкідливої інформації в соціальних мережах/ І.В. Муляр, В.М. Джулій, В. М. Пічура, О.О Зацепіна – Вимірювальна та обчислювальна техніка в технологічних процесах № 3 (2022)-73–78с.

15. Джулій, В.М. Метод класифікації додатків інтернет - трафіка комп'ютерних мереж в умовах невизначеності / В.М. Джулій, Л.В. Солодєєва, О.В. Мірошніченко, // Збірник наукових праць ВІКНУ ім. Т. Шевченка. – К.: ВІКНУ, 2022. –№74. – С. 73-82.

16. Джулій, В.М. Модель оцінки ймовірнісно-часових характеристик інтернет речей інформаційної взаємодії в мережі / В.М. Джулій, Б.М. Кізюн, О.В. Сєлюков, І.В. Муляр // Збірник наукових праць ВІКНУ ім. Т. Шевченка. – К.: ВІКНУ, 2019. –№ 63. – С.96-106

17. Джулій, В.М., Муляр І.В., Кльоц Ю.П., Джулій А.В., Жилевич М.Л. Контроль додатків трафіка комп’ютерних мереж методами машинного навчання. Вісник ХНУ. Технічні науки. 2021. № 5. С. 22-26.

18.Димбовський, М.В. Дослідження актуальних загроз безпеки конфіденційної інформації/М.В. Димбовський, В.М. Джулій - Військова освіта і наука: сьогодення та майбутнє: зб. тез доповідей XIX Міжнародної науково-практичної конференції, м. Київ, 10 листопада 2023 р. Київ: Військовий інститут Київського національного університету імені Тараса Шевченка, 2023. – С. 33.

19. Димбовський, М.В. Модель визначення актуальних загроз безпеки конфіденційних даних в розподіленій інформаційній системі / В.М. Джулій, М.В. Димбовський, І.В. Муляр // Збірник наукових праць ВІКНУ ім. Т. Шевченка. – К.: ВІКНУ, 2023. –№ 80. – С.

20. Довгий, С.О. Сучасні телекомунікації: управління, технології, мережі, регулювання, економіка / С.О. Довгий, П.П. Воробієнко, О.Я. Савченко – К.: УВЦ, 2014. – 521 с.

21. Доктрина інформаційної безпеки України, затвердженої Указом Президента України від 25 лютого 2017 року № №47/2017р. - 15с.

22. Дроб'язко, В. С. Охорона баз даних : регіональні, національні аспекти, міжнародні / В. С. Дроб'язко – К. : Л.-Поліграф, 2018. – 132 с.

23.Закон України «Про внесення змін до законів України щодо інформаційної безпеки» веб-сайт. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/JH77G00A.html

24. Закон України Про криптографічний та технічний захист інформації [Електронний ресурс]. – Режим доступу : https://ips.ligazakon.net/document/NT1819

25. Закон України «Про основні засади забезпечення кібербезпеки України» веб-сайт. URL: https://zakon.rada.gov.ua/laws/show/2163-19

26. Качинський, А.Б. Безпека складних систем / Качинський А.Б. - К.: ТОВ «Видавництво «Юстон», 2017р. - 498 с.

27. Клінцв, Л.М. Безпека програм і даних / Л.М. Клінцв – Чернігов: ВСП Чернігівський інститут інформації, бізнесу і права, 2017р. – 81 с.

28. Кормич, Б.А. Інформаційна безпека: організаційно-правові основи: Навч. посібник. / Б.А. Кормич - К.: Кондор, 2014р. - 384 с.

29. Криворучко, О.В. Аналіз стану захищеності інформаційно-телекомунікаційних систем / О. В. Криворучко, О. М. Сунічук, Д. В. Швець. // Управління розвитком складних систем. 2020. № 42. С. 56–62; dx.doi.org\10.32347/2412-9933.2020.42.56-62.

30. Кудінов, В.А. Основи протидії кіберзлочинності. / В. М. Смаглюк, В. Г. Хахановський, В.А. Кудінов. – К. : НАВС, 2016. – 104 с.

31. Лавров, Є. А. Математичні методи дослідження операцій : підручник / Є. А. Лавров, Л. П. Перхун, В. В. Шендрик – Суми : Сумський державний університет, 2017. – 212 с.

32. Лєнков, С.В. Аналіз існуючих методів та алгоритмів виявлення атак в бездротових мережах передачі даних / С.В. Лєнков, В.М. Джулій, Н.М. Берназ, С.О. Божук // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2017. – Вип. № 56. – С.124-132

33. Ленков, С.В. Метод прогнозування вразливостей інформаційної безпеки на основі аналізу даних тематичних інтернет-ресурсів / С.В. Лєнков, В.М. Джулій, А.М. Берназ, І.В. Муляр, І.В. Пампуха // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2023. – Вип. №78. – С. 123-134.

34. Ленков, С.В. Метод протидії поширенню та виявлення шкідливої інформації в соціальних мережах/ С.В. Ленков, В.М. Джулій, Л.В. Солодєєва // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2022. – Вип. №77. – С. 103-117.

35. Ленков, С.В. Модель безпеки поширення забороненої інформації в інформаційно-телекомунікаційних мережах / С.В. Ленков, В.М. Джулій, В.С. Орленко, О.В. Сєлюков, А.В. Атаманюк // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2020. – Вип. №68. – С. 53-64.

36. Логінова, Н.І. Правовий захист інформації: навчальний посібник/ Н.І. Логінова, Р.Р. Дробожур. – Одеса : Фенікс, 2015р. – 264 с.

37. Лук’янов, Б. В. Комп’ютерний аналіз даних / Б. В. Лук’янов – К. : Академія, 2017. – 345 с.

38. Ляшенко, І.О. Європейські критерії безпеки інформаційних технологій / І.О. Ляшенко // Сучасні інформаційні технології у сфері безпеки та оборони, 2017р. - 84 с.

39. Митник, М.М. Комплексна безпека інформаційних мережевих систем / М.М. Митник, А.Г. Микитишин, П.Д. Стухляк // Навчальний посібник - – Львів, «Магнолія 2006», 2016р. - 261с.

40. Остапов, С.Е. Технологія захисту інформації: навчальний посібник / С.Е. Остапов, С.П. Євсеєв, О. Г. Король. – Х.:Вид. ХНЕУ, 2017р. – 476 с.

41. Пількевич, І.А. Захист інформації в автоматизованих системах управління: навчальний посібник/ І.А. Пількевич, Н.М. Лобанчикова, К.В. Молодецька. – Житомир: Вид-во ЖДУ ім. І. Франка, 2018. – 226 с.

42. Рибальченко, Л.В. Проблеми безпеки персональних даних в Україні / Регіональна економіка / Л.В. Рибальченко, О.О.Косиченко -Запоріжжя. 2019. – с.57-62

43. Ромака, В.А. Аудит інформаційної безпеки: підручник / В. А. Ромака, А.Е. Лагун, Ю.Р. Гарасим - Львів: Сполом, 2017р. - 363 с.

44. Сигнатура атаки. Wikipedia [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Сигнатура_атаки.

45. Сідак, В.С. Забезпечення інформаційної безпеки в країнах НАТО та ЄС: Навчальний посібник. / В.С. Сідак , В.Ю. Артемов - К.: КНТ, 2017р. - 568 с.

46. Соціальні мережі – реальні загрози віртуального світу. [Електронний ресурс]. – Режим доступу : http://ogo.ua/ articles/view/011–02–23/26490.htm.

47. Тарнавський, Ю.А. Технології захисту інформації / Ю.А., Тарнавський. – Київ: КПІ ім. Ігоря Сікорського, 2018р. – 162 с.

48. Флах, П. Машинне навчання. Наука та мистецтво побудови алгоритмів, які вилучають знання з даних / П. Флах. — Litres, 2019р.-534с.

49. Харченко, В.С. Інформаційна безпека. Глосарій/ В.С. Харченко- К.: КНТ, 2015р. - 458 с.

50. Хорошко, В.О. Захист систем електронних комунікацій: навч. посіб. / В.О. Хорошко, О.В. Криворучко, М.М. Браіловський - Київ., 2019р. 164 с.

51. Ярцев, В.П. Розподілені бази даних: навчальний посібник. / В.П. Ярцев - К. ДУТ 2018. - 97с.

52. Developments in the field of information and telecommunications in the context of international security веб-сайт. URL: www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/64/25

53. Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network. веб-сайт. URL: http://redwave.net/books/hackg/index/html

54. Nadvarro, S.R. Cyberbullying Across the Globe: Mental Health, Gender, and Family / B.E. Larrañaga, S.R. Navarro, I.S. Yubero - Springer International Publishing Switzerland, 2016. 284 c.

55. On the Security of Today's Online Electronic Banking Systems веб-сайт. URL: http://docseurope.electrocomponents.com/b8156853c.pdf

56. Pokoradi L., Fuzzy logic-based risk assessment. [Електронний ресурс]. – Режим доступу: URL: http:// www.zmka.hu/docs/Volume1/Issue1/pdf/04poko.pdf.

57. Understanding difference between Cyber Security & Information Security – CISO Platform, 2016. веб-сайт. URL: http://www.cisoplatform.com/profiles/blogs/understanding-difference-between-cyber-security-information

58. OPWNAI: Cybercriminals Starting to Use ChatGPT, January 6, 2023 [Електронний ресурс] – Режим доступу до ресурсу: https://research.checkpoint.com/2023/opwnai-cybercriminals-starting-to-usechatgpt.

59. Trofymenko, O.H., Dubovoy, Ya.V. (2018) Concerning the legal capacity of cyberspace safe operation. Cybersecurity in Ukraine: legal and organizational issues: materials of the III AllUkrainian scientific-practical conference (November 30, 2018). Odessa. pp. 5–7.

ДОДАТОК А

(обовязковий)

Фрагмент коду створення та навчання нейронної мережі,
визначення помилки навчання мережі

```
class ANFIS:
def init (self, X, Y, memFunction):
self.X = np.array(copy.copy(X))
self. Y = np.array(copy.copy(Y))
self.XLen = len(self.X)
selfmemClass = copy. deepcopy(memF unction)
selfmemFuncs = selfmemClass.MFList
selfmemFuncsByVariable = [[x for x in range(len(self.memFuncs[z]))]] for z in range(len(self.memFuncs))]
selfrules = np.array(list(itertools.product(*self.memFuncsBy Variable)))
self.consequents = np.empty(self.Y.ndim * len(self.rules) * (self.X.shapefl] + 1))
self, consequents.fill(0)
self, errors = np.empty(O)
self.memFuncsHomo = all(len(i)==len(self.memFuncsByVariable[O]) for i in self. memF uncsBy Variable)
self trainingType = 'Not trained yef
def LSE(self, A, B, initial Gamma = 1000.):
coeffMat = A
rhsMat = B
S = np.eye(coeffMat.shape[l])*initialGamma
x = np.zeros((coeffMat. shape[1 ], 1)) # need to correct for multi-dim B
for i in range(len(coeffMat[:,0])):
a = coeffMatfi,:]
b = np.array(rhsMat[i])
S = S -
(np.array(np.dot(np.dot(np.dot(S,np.matrix(a).transpose()),np.matrix(a)),S)))//l+(np.dot
(np.dot(S,a),a))))
x = x + (np.dot(S,np.dot(np.matrix(a).transpose(),(np.matrix(b)-
np.dot(np.matrix(a),x))))) ) return x
```

```
def trainHybridJangOffLine(self, epochs=5, tolerance=le-5, initialGamma=1000, k=0.01):
self. trainingType = 'trainHybridJangOffLine'
convergence = False
epoch =1
while (epoch < epochs) and (convergence is not True):
#4 шар
[layerFour, wSum, w] = forwardHalfPass(self, self.X)
#5 шар
layerFive = np.array(self.LSE(layerFour,self. Y,initial Gamma))
self, consequents = layerFive
layerFive = np.dot(layerFour,layerFive)
#помилка
error = np.sum((self.Y-layerFive.T)**2)
printf current error: '+ str(error))
averageerror = np.average(np.absolute(self.Y-layerFive.T))
self.errors = np.append(self. errors,error)
if len(self.errors) !=0:
if self, errors [len(self. errors)-!] < tolerance:
convergence = True
# підтвердження поширення
if convergence is not True:
cols = range(len(self.X[O,:]))
dEdAlpha = list(backprop(self, colX, cols, wSum, w, layerFive) for colX in range(self. X. shapefl]))
if len(self. errors) >= 4:
if (self errors[-4] > self errors [-3] > self errors [-2] > self errors[-l]): до *1.1
if len(self. errors) >= 5:
if (self errors[-1] < self errors[-2]) and (self errors[-3] < self errors[-2]) and (self errors[-3] < self errors[-4]) and ( self errors [-5] > self errors[-4]):
k = k * 0.9
```

ДОДАТОК Б

(обовязковий)

Копії наукових публікацій

ВІЙСЬКОВИЙ ІНСТИТУТ
КИЇВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

ЗБІРНИК
ТЕЗ ДОПОВІДЕЙ

XIX Міжнародної науково-практичної конференції

«Військова освіта і наука: сьогодення та майбутнє»

10 листопада 2023 року

Київ – 2023

ЗМІСТ

Секція 1. Технічні проблеми озброєння і військової техніки та технології подвійного призначення 19

Бахвалов В.Б. Радіолокаційна фазово-доплірівська система. Супровід повітряної цілі 19

Бєльська О.А., Черних Ю.О. Обслуговування силових газотурбінних установок за станом 20

Бондар В.Ю. Створення боєприпасів для безпілотних літальних апаратів 22

Боровик Л.В., Боровик Д.О. Підвищення інформаційної ефективності виявлення недостовірної інформації в інтернеті 23

Шваб В.К., Браун В.О. Основні правила та рекомендації з кібернетичної безпеки під час ведення бойових дій 24

Гапоненко Г.М., Гапоненко Н.П. Безпілотні літальні апарати подвійного призначення 26

Гахович С.В., Жиров Г.Б. Керований комутатор цифрових і аналогових сигналів 26

Гахович С.В., Кеньо Г.В., Савченко Т.В. Архітектура технології захисту пристроїв IIOT у контексті industry 4.0 28

Глухов С.І., Семеха С.М. Обгрунтування розрахунку коефіцієнтів готовності об'єктів радіоелектронної техніки 30

Грох А.О., Чешун В.М. Оцінка ризиків кібербезпеки автоматизованих систем об'єктів критичної інфраструктури 31

Гунченко Ю.О., Пасенченко Т.О., Стукалов С.А., Зуй О.М. Візуальна одночасна локалізації та картографування для мобільних пристроїв 32

Гунявий Д.А., Чешун В.М. Аналіз протоколів консенсусу у блокчейн-технологіях: вплив доказу роботи (POW) та доказу частки (POS) на ефективність, безпеку та стійкість 33

Джулій В.М., Димбовський М.В. Дослідження актуальних загроз безпеки конфіденційної інформації 33

Джулій В.М., Кучерявий Є.І. Методи класифікації зашифрованих даних засобами запобігання та виявлення витоку інформації 34

Джулій В.М., Майор Є.В. Методи виявлення DDOS-атак на основі глибоких згорткових нейронних мереж 35

Жидков Д.В. Актуальні проблеми автоматизації БПЛА з використанням штучного інтелекту 36

Жирний В.А., Нікіфоров Г.С., Чередніков О.М. Технічні проблеми використання трофейної бронетехніки 37

Жиров Г.Б., Ольховиков Д.С. Комплекс заходів безпеки для мережевої системи віддаленого управління пристроями 38

Зайцев І.П. Сучасні реалії озброєння і військової техніки для підрозділів морської піхоти 39

Клепа В.В. Актуальні питання навантажувально-розвантажувальних робіт в системі логістики Збройних Сил України 40

Коваль М.О., Шамрай Н.М. Основні види та застосування сенсорних мереж в умовах ведення бойових дій 41

Кононенко А.А., Жиров Г.Б., Фелінський Г.С. Розподілений підсилювач оптичних сигналів в активних волокнах для телекомунікацій 42

Красильников С.Р., Овод О.А. Інструменти для видалення фону із зображень 43

к.т.н., доц. Джулій В.М. (ХмНУ)
Димбовський М.В. (ХмНУ)

ДОСЛІДЖЕННЯ АКТУАЛЬНИХ ЗАГРОЗ БЕЗПЕКИ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

Визначення переліку актуальних загроз безпеки інформації, оцінка ефективності системи захисту є невід'ємною частиною життєвого циклу

розподіленої інформаційної системи. Специфіка IT-інфраструктури, складність визначення зловмисника, актуальних загроз, вибору показників, недоліки методів оцінки ефективності систем захисту, як наслідок, недостатня ефективність захисту систем призводить до ризиків заподіяння шкоди активам власників систем.

У загальному вигляді задача дослідження може бути сформульовані наступним чином: підвищити якість методів моделювання актуальних загроз безпеки даних за рахунок визначення достатніх і необхідних показників, автоматизувати процес для виключення помилок експертів; підвищити якість методів оцінки ефективності системи захисту визначенням найкращих параметрів роботи адаптивних нейронних нечітких продукційних систем, та застосування технологій Data Science при обробці великого обсягу даних; розробити рекомендації щодо оцінки ефективності системи захисту мереж.

Математично задачу можна формалізувати наступним чином: вибрати відповідні математичні моделі, визначити кращий алгоритм нечіткого виводу; визначити кращі параметри моделі, що дозволять мінімізувати середньоквадратичну помилку в порівнянні з існуючими методами.

Складність вирішення задач зумовлюється недостатнім опрацюванням наступних підзадач: недоліки існуючих підходів моделювання актуальних загроз безпеки інформації і, як наслідок, некоректне визначення атак, зазроз безпеки даних в системах; недоліки існуючих методів оцінки ефективності системи захисту, що призводить до збільшення ризиків порушення цілісності, конфіденційності, доступності та інших властивостей.

Аналіз досліджень оцінки ефективності системи захисту показав, що на теперішній час існують недоліки оцінки ефективності систем захисту, пов'язані з вибором показників оцінки, складне обчислювальне навантаження, недостатня ефективність в частині достовірної оцінки системи захисту, необхідність залучення висококваліфікованих фахівців у галузі інформаційної безпеки, недоліки експертних оцінок.

УДК 004.891

к.т.н., доц., Джулій В.М. (ХмНУ)
ORCID http://orcid.org/0000-0003-1878-4301
e-mail: dzhuliivm@khmnu.edu.ua
к.т.н., доц., Муляр І. В. (ХмНУ)
ORCID http://orcid.org/0000-0003-1878-4301
e-mail: dzhuliivm@khmnu.edu.ua
Димбовський М.В. (ХмНУ)
e-mail: dzhuliivm@khmnu.edu.ua

МОДЕЛЬ ВИЗНАЧЕННЯ АКТУАЛЬНИХ ЗАГРОЗ БЕЗПЕКИ КОНФІДЕНЦІЙНИХ ДАНИХ В РОЗПОДІЛЕНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ

В роботі запропоновано модель визначення актуальних загроз інформаційній безпеці розподілених інформаційних систем, заснована на алгоритмах нечіткого виводу та теорії нечітких нейронних систем, на відміну від відомих, використовує достатні та необхідні показники, виключає помилки експертів, збільшує виявлення кількості актуальних загроз інформаційній безпеці розподілених систем на 5%, знижує витрати на закупівлю засобів захисту інформації від 15 до 30%. Враховує наступні фактори: IT-інфраструктуру розподіленої інформаційної системи, можливості зловмисників та їх рівень мотивації у розподіленій інформаційній системи, перелік існуючих засобів захисту в розподіленій інформаційній системі.

Запропонований підхід відрізняється від існуючих, в наступному: відсутність залучення висококваліфікованих фахівців в області безпеки інформації; процес автоматизований, має низьку обчислювальну складність; відсутність недоліків експертних оцінок; дозволяє визначати перелік актуальних загроз безпеки інформації в інформаційних системах різних класів та типів.

Задача забезпечення безпеки конфіденційної інформації стає найактуальнішею, що обумовлено, зростанням комп'ютерних атак та витоків інформації, що відображаються у статистичних даних скоєння злочинів у сфері високих технологій, зростання кримінальної активності з використанням сучасних комунікаційних пристроїв та інтернет.

Існуючі методи моделювання актуальних загроз інформаційної безпеки та оцінки ефективності системи захисту інформації не можуть бути задіяні на всіх етапах життєвого циклу розподілених інформаційних систем - не враховують в комплексі наступні показники: IT-інфраструктуру розподілених інформаційних систем, актуальні загрози інформаційної безпеки, вимоги безпеки конфіденційної інформації, перелік засобів захисту конфіденційної інформації та їх вартість як важливих показників при вирішенні даних задач

Для досягнення цілей забезпечення безпеки конфіденційної інформації необхідно: організувати ефективне створення системи захисту інформації (системи безпеки інформації), ефективне моделювання (визначення переліку) актуальних загроз інформаційної безпеки, визначення актуального порушника, а також надати можливість проводити якісну оцінку ефективності системи безпеки (захисту) інформації.

Однією з найважливіших задач забезпечення безпеки конфіденційної інформації є оцінка ефективності системи захисту (безпеки). У зв'язку з цим мета роботи (дослідження) - підвищення якості оцінки ефективності систем захисту (безпеки) розподілених інформаційних систем за рахунок визначення достатніх та необхідних показників оцінки з використанням сучасних (перспективних) інформаційних технологій, що дозволяють найбільш ефективно вирішувати наступні задачі: визначення параметрів

роботи адаптивних продукційних нечітких нейронних систем, що найбільш підходять для вирішення поставлених задач, застосування технологій Data Science при обробці даних, алгоритмів нечіткого виведення.

Ключові слова: модель, інформаційна безпека, розподілені інформаційні системи, вразливості, атаки, конфіденційні дані.

Вступ. Інформаційна безпека стає все більш важливою та значущою сферою національної безпеки України, що відображено у Доктрині інформаційної безпеки України, затвердженої Указом Президента України від 25 лютого 2017 року № №47/2017 [1]. Відповідно до Доктрини, на теперішній час, інформаційні технології набули глобального характеру і стали невід'ємною частиною всіх сфер діяльності держави, суспільства та особистості. Розширення сфер застосування інформаційних технологій, на сучасному етапі, значно розширює перспективи розвитку нових інформаційних загроз та атак. Зарубіжні спеціальні служби розширюють інформаційно-психологічний вплив, спрямований на дестабілізацію соціальної та внутрішньо-політичної ситуації в різних регіонах світу, що призводить, в свою чергу, до порушення територіальної цілісності та підриву суверенітету інших держав. Засоби масової інформації збільшують об’єми матеріалів та поширюють їх в мережі Інтернет, які містять упереджену оцінку державної політики [2]. Значно зростають масштаби комп'ютерної злочинності, в першу чергу, у кредитно-фінансовій сфері суспільства. У сфері оборони держави, в економічній сфері, в області суспільної та державної безпеки, в галузі науки, освіти та технологій, в області рівноправного стратегічного партнерства та стратегічної стабільності спостерігаються визначені державою стратегічні цілі для забезпечення конфіденційній інформації ефективного стану безпеки [2].

Одночасно, з розвитком та зростанням інформаційних технологій зростає і кількість засобів та методів порушень стану безпеки конфіденційної інформації. Протягом останніх років спостерігається різке зростання кількості витоків конфіденційної інформації, зі звіту експертно-аналітичного центру групи компаній SafeNet. Змінити ситуацію, до забезпечення інформаційної безпеки, можливо шляхом розробки нових методів, підходів які можуть надати від сучасних загроз безпеки інформації надійний захист [3-5].

Задача забезпечення безпеки конфіденційної інформації стає найактуальнішею, що обумовлено, зростанням комп'ютерних атак та витоків інформації, що відображаються у статистичних даних скоєння злочинів у сфері високих технологій [7,8], зростання кримінальної активності з використанням сучасних комунікаційних пристроїв та інтернет у 2021 році склало 39%. Кожен двадцятий злочин, відповідно до числа всіх зареєстрованих злочинів класифікується як кіберзлочин [10,11]. Серед усіх скоєних у 2021 році комп'ютерних злочинів лідирують злочини, які передбачають розповсюдження, використання, створення комп'ютерних «вірусів», а також відповідальність за неправомірний доступ до комп'ютерної конфіденційної інформації. Друге місце в незаконній електронній діяльності, займає шахрайство з використанням сервісів онлайн-платежів [8]. Кількість таких правопорушень у першому півріччі 2022 р. зросла у 8 разів. Іншим прикладом зростання витоків інформації є щорічні звіти міжнародної компанії Group-IB, в яких йдеться про активність проурядових організацій, які займаються проведенням атак (кіберзлочинами) на користь своїх держав. Відповідно до звіту "Hi-Tech Crime Trends 2021-2022", відзначається збільшення кібератак з використанням відповідного шпигунського програмного забезпечення, бекдорів, шифрувальників, зростання фінансового шахрайства з використанням соціальної інженерії та збільшення атак на банки, мотив кіберзлочинців - крадіжка інформації, за яку можна отримати винагороду чи грошей.

Існуючі методи моделювання (визначення) актуальних загроз інформаційної безпеки та оцінки ефективності системи захисту інформації не можуть бути задіяні на всіх етапах життєвого циклу розподілених інформаційних систем - не враховують в комплексі наступні показники: IT-інфраструктуру розподілених інформаційних систем, актуальні загрози

інформаційної безпеки, вимог безпеки конфіденційної інформації, перелік засобів захисту конфіденційної інформації та їх вартість як важливих показників при вирішенні даних задач [9, 10]. Одночасно з цим, для розглянутих методів моделювання загроз інформаційної безпеки та проведення оцінки ефективності системи захисту розподілених інформаційних систем залишається мета - підвищення ефективності, з огляду визначення кількості актуальних загроз інформаційної безпеки, виконання закладених вимог до безпеки інформації, зниження вартості витрат на проектування та створення системи захисту розподілених інформаційних систем, а також мінімізація (виключення) помилок експертів. Для існуючих методів залишається актуальною задача зменшення помилки середньоквадратичної роботи продукційних адаптивних нечітких нейронних систем.

На підставі проведеного аналізу можна зробити висновок про необхідність удосконалення методів оцінки ефективності системи захисту розподілених інформаційних систем.

Аналіз останніх досліджень та постановка задачі. Моделювання інформаційних систем є одним з основних методів дослідження в областях знань, науково обґрунтованим підходом оцінок характеристик інформаційних складних систем. Моделювання інформаційних систем - заміщення існуючої інформаційної системи іншою з метою отримання необхідної інформації реальної системи з використанням об'єкта-моделі інформаційної системи, аналогічно для проведення моделювання загроз та атак безпеки даних [5,9].

На теперішній час існує класифікація типів моделювання інформаційних систем, яка наведена на рис. 1.

Рисунок 1 - Класифікація типів моделювання інформаційних систем

Відповідно класифікаційним ознакам, моделі поділяються на: неповні, наближені повні. Залежно від характеристик у процесах, моделі поділяться на: стохастичні, детерміновані, динамічні, статичні, дискретні, дискретно-безперервні, безперервні. Статичне моделювання визначає, у будь-який момент, поведінку інформаційної системи. Детерміноване - відображає процеси, у яких відсутні випадкові дії. Динамічне моделювання відображає поведінку інформаційної системи у часі. Стохастичне - відображає імовірнісні події та процеси.

Безперервне моделювання відображає безперервні процеси, дискретне - описує дискретні процеси в інформаційній системі. Моделювання дискретно -безперервне використовується при описі безперервних та дискретних процесів. Уявне використовується при моделюванні об'єктів, які існують поза умовами, їх створення або нереалізовані в визначеному інтервалі часу [13 - 15].

При наочному моделюванні формуються моделі інформаційної системи, що відображають процеси та явища, які протікають в системі. При гіпотетичному моделюванні використовується гіпотеза про закономірності процесів у реальній інформаційній системі, яка базується на причинно-наслідкових зв'язках між виходом і входом і відображає рівень знань експерта досліджуваної інформаційної системи. Гіпотетичне моделювання використовується, коли недостатні знання про інформаційну систему для побудови формальних моделей. Макетування застосовується в реальній інформаційній системі, коли процеси не піддаються фізичному моделюванню. В основі макетів лежать аналоги інформаційної системи, що базуються на причинно-наслідкових зв'язках між процесами та явищами системи. При математичному моделюванні має бути проведена формалізація цього процесу, побудовано математичну модель. Математичне моделювання – процес встановлення відповідності деякого математичного об'єкта реальної інформаційної системи– математичної моделі [13,14].

На сучасному етапі засобом моделювання інформаційних систем є засоби обчислювальної техніки. При побудові математичної моделі кожна система *S* характеризується відповідним набором властивостей, які враховують умови взаємодії системи із зовнішнім середовищем *E* та відображають поведінку досліджуваної моделі системи. Модель системи *S* можна представити у вигляді множини величин, що описують процеси функціонування реальної інформаційної системи та утворюють наступні підмножини:

1. Сукупність внутрішніх параметрів системи: $h_k \in H, k = \overline{1, n_H}$.

2. Сукупність вихідних характеристик: $y_j \in Y,\ j = \overline{1, n_Y}$.

3. Сукупність вхідних впливів на систему: $x_i \in X, i = \overline{1, n_X}$.

4. Сукупність впливів зовнішнього середовища: $v_l \in V, l = \overline{1, n_V}$.

Змінні x_i, y_j, h_k, v_l - елементи підмножин, містять стохастичні і детерміновані складові, не перетинаються.

При моделюванні системи внутрішні параметри системи, впливи зовнішнього середовища, вхідні впливи є незалежними змінними, які у векторній формі мають наступний вид:

$$\vec{x}(t) = \left(x_1(t), x_2(t), ..., x_{n_X}(t)\right);$$

$$\vec{v}(t) = \left(v_1(t), v_2(t), ..., v_{n_V}(t)\right);$$

$$\vec{h}(t) = \left(h_1(t), h_2(t), ..., h_{n_H}(t)\right).$$

Вихідні характеристики інформаційної системи є залежними змінними, векторною формою мають наступний вид:

$$\vec{y}(t) = \left(y_1(t), y_2(t), ..., y_{n_Y}(t)\right).$$

Функціонування інформаційної системи *S* описується оператором F_S:

$$\vec{y}(t) = F_S\left(\vec{x}, \vec{v}, \vec{h}, t\right) \qquad (1)$$

Залежність (1) є законом функціонування інформаційної системи. Алгоритм функціонування системи A_S - метод отримання вихідних характеристик системи з урахуванням впливів внутрішніх параметрів системи $\vec{h}(t)$, зовнішнього середовища $\vec{v}(t)$, вхідних впливів

$\vec{x}(t)$. Закон функціонування F_S інформаційної системи *S* може бути реалізований множиною різних алгоритмів функціонування A_S, різними способами.

Відношення (1) є математичним описом інформаційної системи моделювання *S* протягом часу *t*, математичні моделі такого типу є динамічними.
Відношення (1) може бути реалізовано різними способами: таблично, аналітично, графічно.

Математична модель системи - кінцева підмножина змінних $\left\{\vec{x}(t),\vec{v}(t),\vec{h}(t)\right\}$ з математичними зв'язками між ними та характеристиками $\vec{y}(t)$ [9].

Дискретно детерміновані моделі системи *F*-схеми. В основі, яких лежить теорія автоматів, математична модель автомата. Автомат задається *F*- схемою

$$F=\langle Z,X,Y,\varphi,\psi,z_0\rangle,$$

яка функціонує в дискретному автоматному часі, де *Z* - множина внутрішніх станів системи, *Y*-вихідні сигнали, *X*-вхідні сигнали, z_0 - початковий стан, $z_0\in Z$, функція виходу $\psi(z,x)$, функція переходу $\varphi(z,x)$.

Мережеві моделі (*N* -схеми) - мережі Петрі. Для вирішення задач, пов'язаних з аналізом причинно-наслідкових зв'язків та з формалізованим описом у складних системах.

Найпоширенішим формалізмом, що описує взаємодію та структуру процесів та паралельних систем використовуються мережі Петрі.

Мережа Петрі (*N*-схема) задається наступним чином:

$$N=\langle B,D,I,O\rangle,$$

де, *B* – позиції, *D* – переходи, *I* – вхідна функція, *O* – вихідна функція.
Для кожного переходу $d_j\in D$ можна визначити для переходу множину вхідних позицій $I(d_j)$ і для переходу множину вихідних позицій $O(d_j)$.

Класифікація методів побудови моделей системи наведено на рис. 2.

Роглянуті методи та моделі мають свої недоліки та переваги.

Основні недоліки перерахованих моделей: будь-яка модель мінімізує пояснення можливих явищ; під час моделювання не завжди існує можливість виявлення якісних нових характеристик; як правило, необхідних даних не вистачає для налаштування моделей; статистичні моделі системи можуть бути об'єктивними в межах емпіричної множини побудови моделі.

Рисунок 2 - Класифікація методів побудови моделей атак

На основі проведеного дослідження, можна зробити висновок - існуючі підходи побудови моделей системи мають низку недоліків, що, своєю чергою, доводить необхідність удосконалення розглянутих моделей.

Для досягнення цілей забезпечення безпеки конфіденційної інформації необхідно: організувати ефективне створення системи захисту інформації (системи безпеки інформації), ефективне моделювання (визначення переліку) актуальних загроз інформаційної безпеки, визначення актуального порушника, а також надати можливість проводити якісну оцінку ефективності системи безпеки (захисту) інформації. Однією з найважливіших задач забезпечення безпеки конфіденційної інформації є оцінка ефективності системи захисту (безпеки). У зв'язку з цим мета роботи (дослідження) - підвищення якості оцінки ефективності систем захисту (безпеки) розподілених інформаційних систем за рахунок визначення достатніх та необхідних показників оцінки з використанням сучасних (перспективних) інформаційних технологій, що дозволяють найбільш ефективно вирішувати наступні задачі: визначення параметрів роботи адаптивних продукційних нечітких нейронних систем, що найбільш підходять для вирішення поставлених задач, застосування технологій Data Science при обробці даних, алгоритмів нечіткого виведення.

Моделювання зловмисника та загроз безпеки конфіденційної інформації. Аналіз можливостей, які може мати зловмисник, проводиться у рамках розробки моделі зловмисника. Виходячи з актуальності порушників інформаційної безпеки, визначено внутрішні та ймовірні зовнішні порушники безпеки даних, що обробляються у розподілених системах. До можливих внутрішніх зловмисників інформаційної безпеки відносяться: особи, які мають санкціонований доступ до контрольованої зони розподілених систем, але не мають доступу до інформації, що обробляється в системі; зареєстровані користувачі розподіленої інформаційної системи - здійснюють обмежений доступ з робочого місця до ресурсів системи; зареєстровані користувачі розподіленої інформаційної системи - здійснюють віддалений доступ до інформації. До ймовірних зовнішніх зловмисників інформаційної безпеки даних відносяться: атакуючі інформаційну систему, колишні працівники розподіленої інформаційної системи.

Для виділених типів можливих зловмисників визначаються наступні методи реалізації загроз інформаційної безпеки [16,17]:

1. Загрози витоку даних з технічних каналів можуть бути реалізовані за допомогою: перегляду інформації, з використанням оптикоелектронних (оптичних) засобів відображення, екранів дисплеїв, інформаційно-обчислювальних комплексів, технічних засобів обробки буквенно-цифрової, графічної, відео- інформації; перехоплення випромінюваних чистот при обробці інформації у розподілених інформаційних системах, спеціальними технічними засобами радіотехнічної розвідки, розміщеними як на території контролюємої зони, так і за її межами.

2. Загрози несанкціонованого доступу до інформації можуть бути реалізовані за допомогою: впливу на технічні засоби в ході завантаження операційної системи; прямого доступу до технічних засобів чи програмного забезпечення після завантаження операційної системи; віддаленого доступу до технічних засобів чи програмного забезпечення; віддаленого або прямого впливу на об'єкти віртуального середовища системи і інформацію, яка зберігається у віртуальному просторі розподіленої системи.

3. Загрози спеціальних впливів на розподілену систему можуть бути реалізовані з використанням: хімічного впливу; механічного впливу; акустичного впливу; радіаційного впливу; біологічного впливу; електромагнітного впливу; термічного впливу; магнітного поля; електромагнітного випромінювання.

При визначенні способу реалізації загроз інформаційній безпеці передбачалося, що загрози можуть бути реалізовані за рахунок доступу до інформації, компонентів розподіленої інформаційнох системи, за рахунок створення засобів, умов які забезпечують необхідний доступ.

При визначенні можливих способів реалізації загроз інформаційній безпеці враховано наступні умови: існує можливість змови зловмисників (зовнішніх та внутрішніх); загроз інформаційній безпеці можуть бути реалізовані в будь-якій точці та в будь-який час інформаційної системи (на будь-якому хості, вузлі); для досягнення мети зловмисник обирає найслабшу ланку інформаційної системи.

Модель ймовірного зловмисника розподіленої інформаційної системи містить систему поглядів на потенційних зловмисників безпеки інформації, що обробляється в системі, мотивацію та причини їх дій, цілі, які вони переслідують, загальний характер дій у процесі підготовки до реалізації загроз інформаційній безпеці та здійснення впливу на дані, що обробляються в розподіленій системі.

Модель ймовірного порушника інформаційної системи відбиває теоретичні та практичні можливості ймовірного зловмисника, його апріорні знання, місце та час дії. За наявності права разового чи постійного доступу до контрольваної зони зловмисники поділяються на: особи, які не мають прав доступу до контрольваної зони системи; особи, які мають право разового або постійного доступу до контрольваної зони системи. Факторами, які знижують ймовірність змови зловмисників, є: створення умов мінімальної фінансової зацікавленості юридичних та фізичних осіб, що входять до числа ймовірних зловмисників безпеки інформації розподілених систем, у реалізації загроз інформаційної безпеки, щодо розподілених систем; укладення угоди про конфіденційність даних між власником ситсеми та фізичними, юридичними особами, що входять до числа ймовірних зловмисників безпеки інформації системи; підтримання та забезпечення високого рівня підготовки користувачів розподіленої інформаційної системи у сфері забезпечення безпеки інформації; створення умов настання негативних наслідків для потенційного зловмисника у разі реалізації загрози інформаційної безпеки: втрата прибутку та ділової репутації, розрив цивільно-правових відношень; визначення відповідальності, що покладається на користувача розподіленої інформаційної системи, при порушенні вимог безпеки даних у розподіленій інформаційній системі.

На підставі зазначених категорій порушників з урахуванням умов експлуатації, характеру оброблюваної інформації, суб'єктів доступу до інформаційної системи, об'єктів захисту пропонується використовувати класифікацію внутрішніх порушників, за наступними категоріями: особи, які не мають доступу до даних, що обробляється в інформаційній системі,

але мають санкціонований доступ до системи; зареєстровані користувачі, які здійснюють обмежений доступ до ресурсів системи з робочого місця; зареєстровані користувачі інформаційної системи, які здійснюють віддалений доступ до даних, які обробляються в системі; зареєстровані користувачі з повноваженнями адміністратора інформаційної безпеки сегмента системи; зареєстровані користувачі інформаційної системи з повноваженнями системного адміністратора; зареєстровані користувачі системи з повноваженнями адміністратора безпеки даних інформаційної системи; постачальники (програмісти-розробники) програмного забезпечення та особи, які забезпечують супровід прикладних програм на об'єкті, що захищається; особи та розробники, які забезпечують ремонт, постачання, супровід технічних засобів розподіленої інформаційної системи. Типи потенційних зловмисників інформаційної безпеки встановлюються на підставі відповідного потенціалу, що визначає наявні можливості реалізації загрози безпеки даних: порушники з низьким потенціалом - мають можливість використовувати дані, отриманих із загальнодоступних джерел для реалізації загрози інформаційній безпеці; порушники з середнім потенціалом - мають можливість здійснювати аналіз прикладного програмного забезпечення, знаходити в ньому вразливості та використовувати їх для реалізації загроз інформаційній безпеці; порушники з високим потенціалом - мають можливість вносити закладки в програмне забезпечення інформаційної системи, застосовувати спеціалізовані засоби проникнення, проводити спеціальні дослідження та добування інформації для реалізації зазгрози інформаційній безпеці.

Для кожної категорії порушників визначення актуальності інформаційної безпеки інформації використовуються наступні критерії: рівень небезпеки; рівень мотивації. Перелік потенційних зловмисників інформаційної безпеки, що обробляються в розподіленій інформаційній системі, та рівень мотивації наведені в таблиці 1.

Для визначення рівня небезпеки зловмисника інформаційній безпеці використовуються наступні характеристики: ступінь поінформованості про розподілену інформаційну систему; рівень знань в області безпеки даних.

Таблиця 1 - Перелік потенційних порушників інформаційної безпеки та рівень їх мотивації

Порушник	Мотив	Рівень мотивації
Зовнішній порушник		
Розвідувальні служби держав	Відсутній	Мінімальний
Кримінальні структури	Корисні інтереси: досягнення безпосередньої матеріальної вигоди, підрив репутації фірми	Високий
Конкуренти (конкуруючі організації)	Відсутній	Мінімальний
Недобросовісні партнери	Корисливі інтереси: досягнення безпосередньої матеріальної вигоди, підрив репутації організації	Високий
Зломщики інформаційних систем та мереж	Хуліганство (вандалізм); професійне самоствердження	Високий

Модель визначення актуальних загроз безпеки конфіденційним даним. Проведено дослідження адаптивних нейронних нечітких систем ANFIS із використанням алгоритмів нечіткого виведення Такагі-Сугено-Канга, Сугено-Такагі, Мамдані, Ванга-Менделя. Залежність похибки на тестовій вибірці від кількості правил під час перевірки менша у мережі ANFIS з алгоритмом Такагі-Сугено-Канга. Для визначення актуальних загроз інформаційної безпеки обрана нейронна продукційна адаптивна система ANFIS, заснована на нечіткій системі Такагі-

Сугено-Канга. Алгоритм роботи полягає в реалізації нечіткої моделі, заснованої на правилах типу (2):

$$R_i : IFx_i ISA_{i1} AND...AND_{x_j} ISA_{ij} AND...AND_{x_{im}} ISA_{im}, THEN$$
$$y = c_{i0} + \sum_{j=1}^{m} c_{ij} x_j,\ j = 1,...,n \qquad (2)$$

Сформовано базу правил визначення актуальних загроз інформаційної безпеки. Приклад заповнення бази знань правил, виходячи з сформованого набору даних наведено в таблиці 2.

Правила представлені в таблиці 2, фактично представляють множину правил, що складаються окремо за типом системи захисту інформації, типом зловмисника, (Dallas Lock, SecretNet) та впливом.

Нейронна продукційна адаптивна система ANFIS базується на наступних положеннях:

- вхідні змінні є чіткими;

- функції приналежності визначені функцією Гауса: $\mu_{A_{ij}}\left(x_j\right) = \exp\left(-\frac{1}{2}\left(\frac{x_j - a_{ij}}{b_{ij}}\right)^2\right)$, де x - вхідні дані мережі, a_{ij}, b_{ij} - параметри функції приналежності, що налаштовуються;

- нечітка імплікація Ларсена нечіткий добуток;
- *T*-норма – нечіткий добуток; композиція не здійснюється;
- метод дефазифікації
– метод центроїду.

Таблиця 2 - Фрагмент бази знань правил визначення актуальних загроз інформаційній безпеці

№ п/п	IF (ЯКЩО)			THEN (ТО)
	Тип порушника (джерело впливу)	IT-інфраструктура (об'єкт впливу)	Версія ПЗ	
1	Зовнішній порушник із низьким потенціалом. Внутрішній порушник з низьким потенціалом	Віртуальна машина VMWare	6.5 (VMWare Workstation), від 7.0.0 до 7.1.4 включно (VMWare Workstation)	Загроза несанкціонованого доступу до захищених віртуальних машин з боку інших віртуальних машин
2	Зовнішній порушник з високим потенціалом	Мобільний пристрій на базі iOS	(Android), до 10.3.3 включно (iOS)	Загроза контролю шкідливою програмою списку додатків, запущених на пристрої
…				
N	Зовнішній порушник із середнім потенціалом, Внутрішній порушник з середнім потенціалом	Засіб захисту інформації	12.4 (Cisco IOS), 12.4 (Cisco IOS), 15.0 (Cisco IOS), 15.0 (Cisco IOS), 15.2 (Cisco IOS), 15.1 (Cisco IOS)	Загроза несанкціонованого впливу на засіб захисту інформації

Функціональна залежність після дефазифікації для отримання вихідної змінної має вид (3):

$$y' = \frac{\sum_i^n \left(\left(c_{i0} + \sum_{j=1}^m c_{ij} x_j \right) \prod_j^m \mu_{A_{ij}} \left(x_j^{'} \right) \right)}{\sum_{i=1}^n \prod_j^m \mu_{A_{ij}} \left(x_j^{'} \right)} = \frac{\sum_i^n \left(\left(c_{i0} + \sum_{j=1}^m c_{ij} x_j \right) \prod_j^m \exp \left[- \left(\frac{x_j^{'} - a_{ij}}{b_{ij}} \right)^2 \right] \right)}{\sum_{i=1}^n \prod_j^m \exp \left[- \left(\frac{x_j^{'} - a_{ij}}{b_{ij}} \right)^2 \right]} \quad (3)$$

Вираз 3 лежить в основі нейронної мережі ANFIS із використанням алгоритму TSK, включає п'ять шарів:

1. Виконує фазифікацію чітких вхідних змінних: $x_j^{'} \left(j = 1, ..., n \right)$.

2. Обчислює значення ступенів функції приналежності $\mu_{A_{ij}} \left[x_j^{'} \right]$, заданих функціями Гаусса з параметрами a_{ij}, b_{ij}.

3. Генерує значення функцій $\left(c_{j0} + \sum_{j=1}^m c_{ij} x_j^{'} \right)$, які перемножуються на результати обчислень елементами другого шару.

4. Перший елемент четвертого шару необхідний для активізації виводів правил відповідно до значень, в третьому шарі, ступенів належності передумов правил. Другий елемент четвертого шару проводить додаткові обчислення для подальшої дефазифікації.

5. Даний шар складається з одного елемента нормалізуючого та робить дефаззифікацію результатів роботи нейронної мережі.

Нейронна мережа ANFIS містить два параметричні шари (1 і 3). Параметрами, які налаштовуються в процесі навчання нейронної мережі є: в першому шарі - нелінійні параметри a_{ij}, b_{ij} функції приналежності фазифікатора; в третьому шарі - параметри c_{i0} і c_{ij} лінійних функцій $\left(c_{j0} + \sum_{j=1}^m c_{ij} x_j^{'} \right)$ з висновків бази правил.

На наступному кроці розраховуються параметри c_{i0} і c_{ij} лінійних функцій за умови фіксованих значень параметрів a_{ij}, b_{ij}. Параметри c_{i0} і c_{ij} знаходяться шляхом розв'язання системи лінійних рівнянь. Вихідну змінну з виразу (3) представимо в наступному виді (4):

$$y' = \sum_{i=1}^n w_i^{'} \left(c_{i0} + \sum_{j=1}^m c_{ij} x_j \right), \quad (4)$$

де $w_i^{'} = \frac{\prod_j^m \mu_{A_{ij}} \left(x_j^{'} \right)}{\sum_{i=1}^n \prod_j^m \mu_{A_{ij}} \left(x_j^{'} \right)} = \frac{\prod_j^m \exp \left[- \left(\frac{x_j^{'} - a_{ij}}{b_{ij}} \right)^2 \right]}{\sum_{i=1}^n \prod_j^m \exp \left[- \left(\frac{x_j^{'} - a_{ij}}{b_{ij}} \right)^2 \right]} = const$

Алгоритм навчання нейроної продукційної адаптивної система ANFIS із застосуванням алгоритму TSK.

При k навчальних прикладах $x_1^{(k)}, x_2^{(k)}, \ldots, x_m^{(k)}, y^{(k)}$, де $k = 1, ..., K$ і заміна значень вихідних змінних $y^{'(k)}$ значеннями еталонних змінних $y^{(k)}$, отримаємо систему з k лінійних рівнянь (5):

$$\begin{bmatrix} \grave{w}_1^{(1)} & \grave{w}_1^{(1)}x_1^{(1)} & \dots & \grave{w}_1^{(1)}x_m^{(1)} & \dots & \grave{w}_n^{(1)} & \grave{w}_n^{(1)}x_1^{(1)} & \dots & \grave{w}_n^{(1)}x_m^{(1)} \\ \grave{w}_1^{(2)} & \grave{w}_1^{(2)}x_1^{(2)} & \dots & \grave{w}_1^{(2)}x_m^{(2)} & \dots & \grave{w}_n^{(2)} & \grave{w}_n^{(2)}x_1^{(2)} & \dots & \grave{w}_n^{(2)}x_m^{(2)} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \grave{w}_1^{(k)} & \grave{w}_1^{(k)}x_1^{(k)} & \dots & \grave{w}_1^{(k)}x_m^{(k)} & \dots & \grave{w}_n^{(k)} & \grave{w}_n^{(k)}x_1^{(k)} & \dots & \grave{w}_n^{(k)}x_m^{(k)} \end{bmatrix} \times \begin{bmatrix} c_{10} \\ \dots \\ c_{1m} \\ \dots \\ c_{n0} \\ \dots \\ c_{nm} \end{bmatrix} = \begin{bmatrix} y^{(1)} \\ y^{(2)} \\ \dots \\ y^{(k)} \end{bmatrix} \quad (5)$$

де $\grave{w}_1^{(k)}$ - агрегований ступінь істинності передумов за і-им правилом при пред'явленні *k*-го вхідного вектора $\left(x_1^{(k)}, x_2^{(k)}, \dots, x_m^{(k)}\right)$. Вираз (5) у скороченому виді: $W \cdot c = y$. Вирішення даної системи рівнянь можна провести за один крок за допомогою псевдоінверсії матриці *W*: $c = W^{+} y = \left(W^T W\right)^{-1} W^T y$. Після визначення лінійних параметрів *ij* розраховуємо та фіксуємо фактичні вихідні сигнали системи, для чого використовуємо лінійну залежність (6):

$$\grave{y} = \begin{bmatrix} y^{(1)} \\ y^{(2)} \\ \dots \\ y^{(k)} \end{bmatrix} = W \cdot c \quad (6)$$

Визначаємо вектор помилок: $e = \grave{y} - y$.

Виконуємо уточнення параметрів (7):

$$a_{ij}^{(k)}(t+1) = a_{ij}^{(k)}(t) - C\frac{\partial E^{(k)}(t)}{\partial a_{ij}^{(k)}}$$
$$b_{ij}^{(k)}(t+1) = b_{ij}^{(k)}(t) - C\frac{\partial E^{(k)}(t)}{\partial b_{ij}^{(k)}} \quad (7)$$

Для визначення актуальних загроз інформаційній безпеці із переліку потенційних можливих загроз необхідно визначити ймовірність реалізації. Визначаємо коефіцієнти Y_2 експертним шляхом для кожної загрози інформаційної безпеки: 0 - малоймовірна загроза; 2 – низька ймовірність загрози; 5 – середня ймовірність загрози; 10 –висока ймовірність загрози.

З урахуванням визначених коефіцієнтів ймовірність реалізації загроз інформаційній безпеці *Y* визначається співвідношенням: $Y = \left(Y_1 + Y_2\right)$, де Y_1 - ступінь початкової захищеності розподіленої інформаційної системи, що визначається відповідно до методичних даних Кваліфікаційного центру інформаційних технологій та кібербезпеки України.

Структура нечіткої нейронної продукційної мережі ANFIS із застосуванням алгоритму TSK представлена на рис. 3.

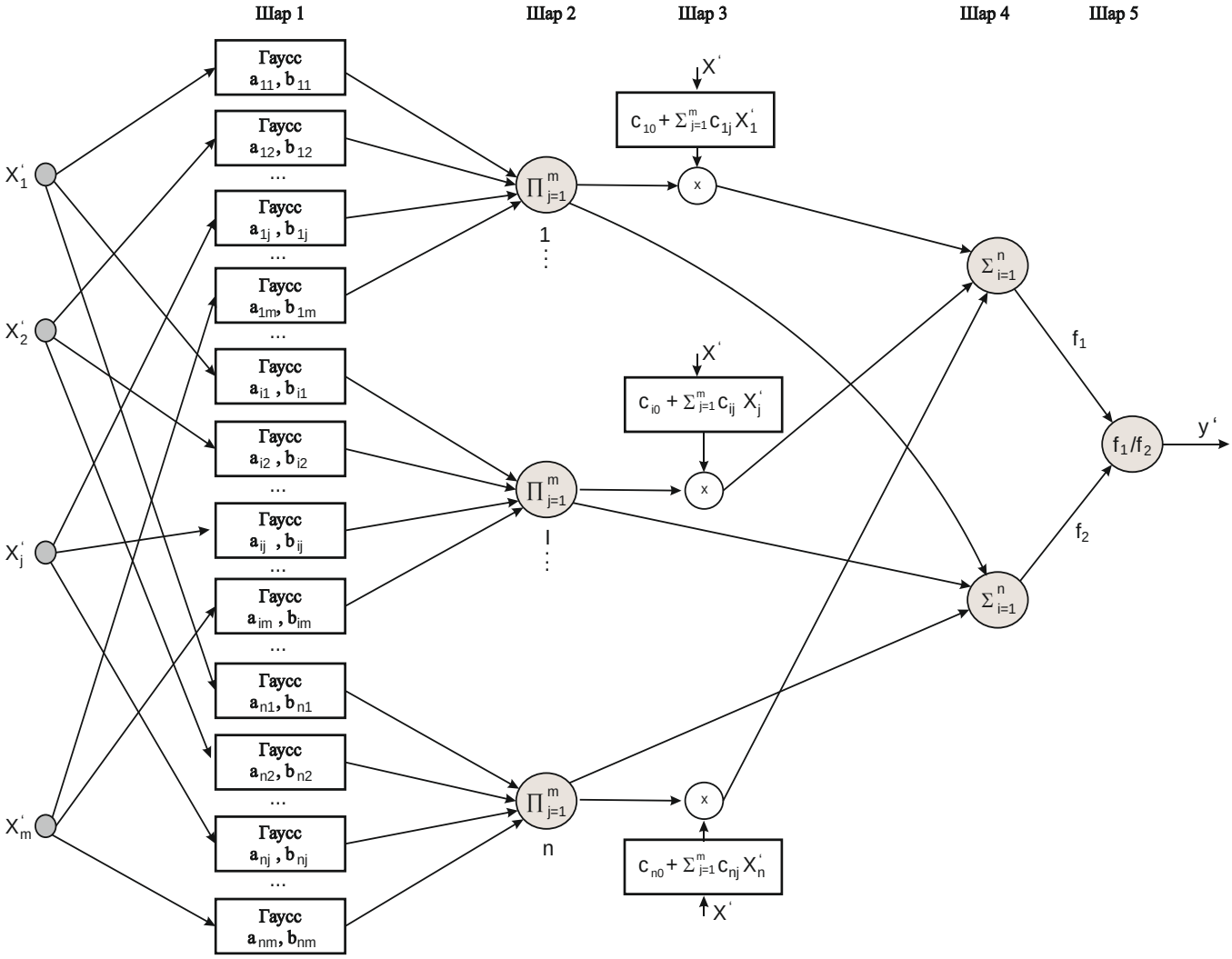


Рисунок 3 – Нейронна мережа ANFIS із застосуванням алгоритму TSK

Аналіз оцінки ефективності запропонованого підходу визначення актуальних загроз інформаційній безпеці наведені у табл. 3.

Таблиця 3 – Аналіз оцінки ефективності запропонованого підходу визначення актуальних актуальних загроз інформаційній безпеці

Показник	Існуючі підходи	Запропонований підхід
RMSE	0,018-0,069	0,011-0,022
Визначення кількості актуальних загроз	понад 30%	більше 35%
Вартість системи захисту	зниження до 15%	зниження до 30%

Середньоквадратична помилка запропонованого підходу, що обчислюється за формулі (8):

$$RMSE = \sqrt{\frac{1}{N}\sum_{i=1}^{N}\left(y_i - y_i\right)^2}, \qquad (8)$$

де y_i, y_i - набори даних (перевірки, навчання).

Графіки порівняння *RMSE* запропонованого та існуючих підходів на заданому інтервалі представлені на рис. 4.

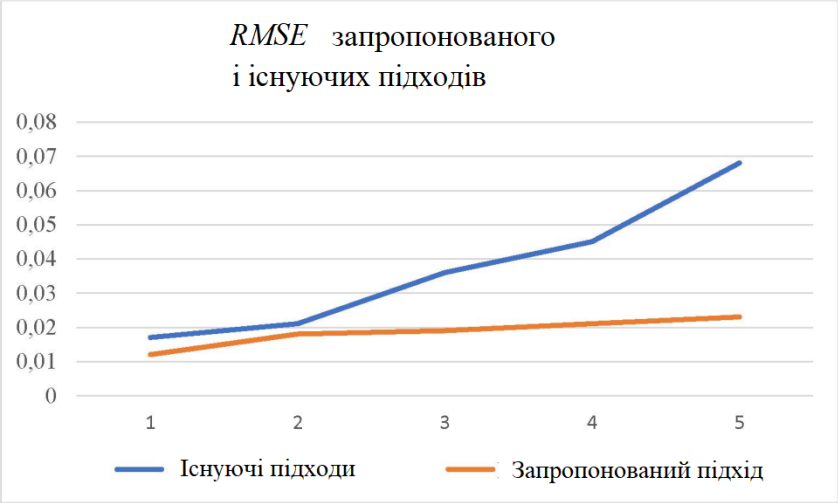


Рисунок 4 - Графік порівняння RMSE запропонованого та існуючих підходів на заданому інтервалі

Висновки. Запропоновано модель визначення актуальних загроз інформаційній безпеці, заснована на алгоритмах нечіткого виводу та теорії нечітких нейронних систем, на відміну від відомих, використовує певні достатні та необхідні показники, виключає помилки експертів. Збільшує виявлення кількість актуальних загроз інформаційній безпеці розподілених систем на 5%, знижує витрати на закупівлю засобів захисту інформації від 15 до 30%. Враховує наступні фактори: ІТ-інфраструктуру розподіленої інформаційної системи, можливості зловмисників та їх рівень мотивації у розподіленій інформаційній системи, перелік існуючих засобів захисту в розподіленій інформаційній системі. Запропонований підхід відрізняється від існуючих, в наступному: відсутність залучення висококваліфікованих фахівців у області безпеки інформації; процес автоматизований, має низьку обчислювальну складність; відсутність недоліків експертних оцінок; дозволяє визначати перелік актуальних загроз безпеки інформації в інформаційних системах різних класів та типів.

ЛІТЕРАТУРА:

1. Доктрина інформаційної безпеки України, затвердженої Указом Президента України від 25 лютого 2017 року № №47/2017, 15с.

2. Державний стандарт України Захист інформації. Технічний захист інформації. Основні положення. ДСТУ 3396.0-96 [Електронний ресурс]. – Режим доступу : http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=38883&cat_id =38836

3. Ленков, С.В. Метод прогнозування вразливостей інформаційної безпеки на основі аналізу даних тематичних інтернет-ресурсів / С.В. Лєнков, В.М. Джулій, А.М. Берназ, І.В. Муляр, І.В. Пампуха // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2023. – Вип. №78. – С. 123-134.

4. Ленков, С.В. Метод протидії поширенню та виявлення шкідливої інформації в соціальних мережах/ С.В. Ленков, В.М. Джулій, Л.В. Солодєєва // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2022. – Вип. №77. – С. 103-117.

5. Ленков, С.В. Модель безпеки поширення забороненої інформації в інформаційно-телекомунікаційних мережах / С.В. Ленков, В.М. Джулій, В.С. Орленко, О.В. Сєлюков, А.В. Атаманюк // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2020. – Вип. №68. – С. 53-64.

7. Соціальні мережі – реальні загрози віртуального світу. [Електронний ресурс]. – Режим доступу : http://ogo.ua/ articles/view/011–02–23/26490.htm.

8. Остапов С. Е. Технології захисту інформації: навчальний посібник / С.Е. Остапов, С.П. Євсеєв, О.Г. Король – Харків : Вид-во ХНЕУ, 2016. – 476 с.

9. Лєнков, С.В. Аналіз існуючих методів та алгоритмів виявлення атак в бездротових мережах передачі даних / С.В. Лєнков, В.М. Джулій, Н.М. Берназ, С.О. Божук // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2017. – Вип. № 56. – С.124-132

10. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : посібник / [В. Л. Бурячок, С. В. Толюпа, В. В. Семко та ін.]. – К. : ДУТ-КНУ, 2016. – 178 с.

11. Рибальченко Л.В., Косиченко О.О. Проблеми безпеки персональних даних в Україні / Регіональна економіка / Запоріжжя. 2019. – с.57-62

12. Джулій, В.М. Метод класифікації додатків трафіка комп'ютерних мереж на основі машинного навчання в умовах невизначеності / В.М. Джулій, О.В. Мірошніченко, Л.В. Солодєєва // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2022. – Вип. №74. – С. 73-82.

13. Лавров, Є. А. Математичні методи дослідження операцій : підручник / Є. А. Лавров, Л. П. Перхун, В. В. Шендрик – Суми : Сумський державний університет, 2017. – 212 с.

14. Гончар С. Ф. Оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури : монографія. / С. Ф. Гончар. – Київ, 2019. – 175 с.

16. Сигнатура атаки. Wikipedia [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Сигнатура_атаки.

17. OPWNAI: Cybercriminals Starting to Use ChatGPT, January 6, 2023 [Електронний ресурс] – Режим доступу до ресурсу: https://research.checkpoint.com/2023/opwnai-cybercriminals-starting-to-usechatgpt.

ДОДАТОК В

Презентація кваліфікаційної роботи

Тема Метод оцінювання ефективності засобів захисту інформації розподілених інформаційних систем

Мета магістерської роботи - підвищення якості оцінки ефективності систем захисту розподілених інформаційних систем за рахунок визначення достатніх та необхідних показників.

Наукова задача – підвищити якість оцінки ефективності системи захисту розподілених інформаційних систем, запропонувавши метод визначення актуальних загроз інформаційній безпеці та оцінки ефективності системи захисту, заснований на продукційних адаптивних нечітких нейронних мереж, за рахунок визначення достатніх та необхідних показників..

Об'єкт дослідження: Загрози безпеки та вимоги по захисту конфіденційної інформації.

Предмет дослідження: Методи моделювання (визначення) актуальних загроз безпеці конфіденційної інформації, оцінки ефективності систем захисту конфіденційної інформації.

Задачі досліджень у роботі формулюються наступним чином:

1. Провести дослідження розподілених інформаційних систем, провести аналіз загроз та атак безпеці конфіденційної інформації, аналіз перспективних методів моделювання загроз інформаційній безпеці та оцінки ефективності систем безпеки інформації.
2. Підвищити якість визначення атак та загроз інформаційній безпеці в розподілених інформаційних системах за рахунок визначення достатніх та необхідних показників для мінімізації помилки роботи методу.
3. Провести оцінку ефективності запропонованого методу.

Наукова новизна роботи визначає:

1. Запропоновано метод визначення атак та актуальних загроз безпеці конфіденційної інформації, на відміну від відомих, формує перелік актуальних загроз інформаційній безпеці, виключаючи помилки експертів.

2. Запропоновано метод оцінки ефективності систем інформаційного захисту, на відміну від відомих, заснований на нечітких адаптивних нейронних продукційних мереж та алгоритмі нечіткого виведення із використанням IT Data Science.

Методи дослідження. Для вирішення задач у магістерській роботі застосовувалися методи: теорії ймовірності, методи неявного перебору, динамічного програмування, математичної статистики, теорії нечітких адаптивних нейронних систем, алгоритми нечіткого виводу.

Практична цінність

1. Проведений аналіз розподілених систем виявив основні аспекти технології обробки інформації, дозволив використати отримані результати дослідження при визначенні достатніх та необхідних показників моделювання (визначення) загроз інформаційній безпеці та провести оцінку ефективності системи захисту розподілених систем.

2. Запропоновий метод визначення загроз інформаційній безпеці дозволяє визначати актуальні загрози безпеці інформації мінімізує трудомісткість процесу, обчислювальні ресурси, виключаючи недоліки експертів.

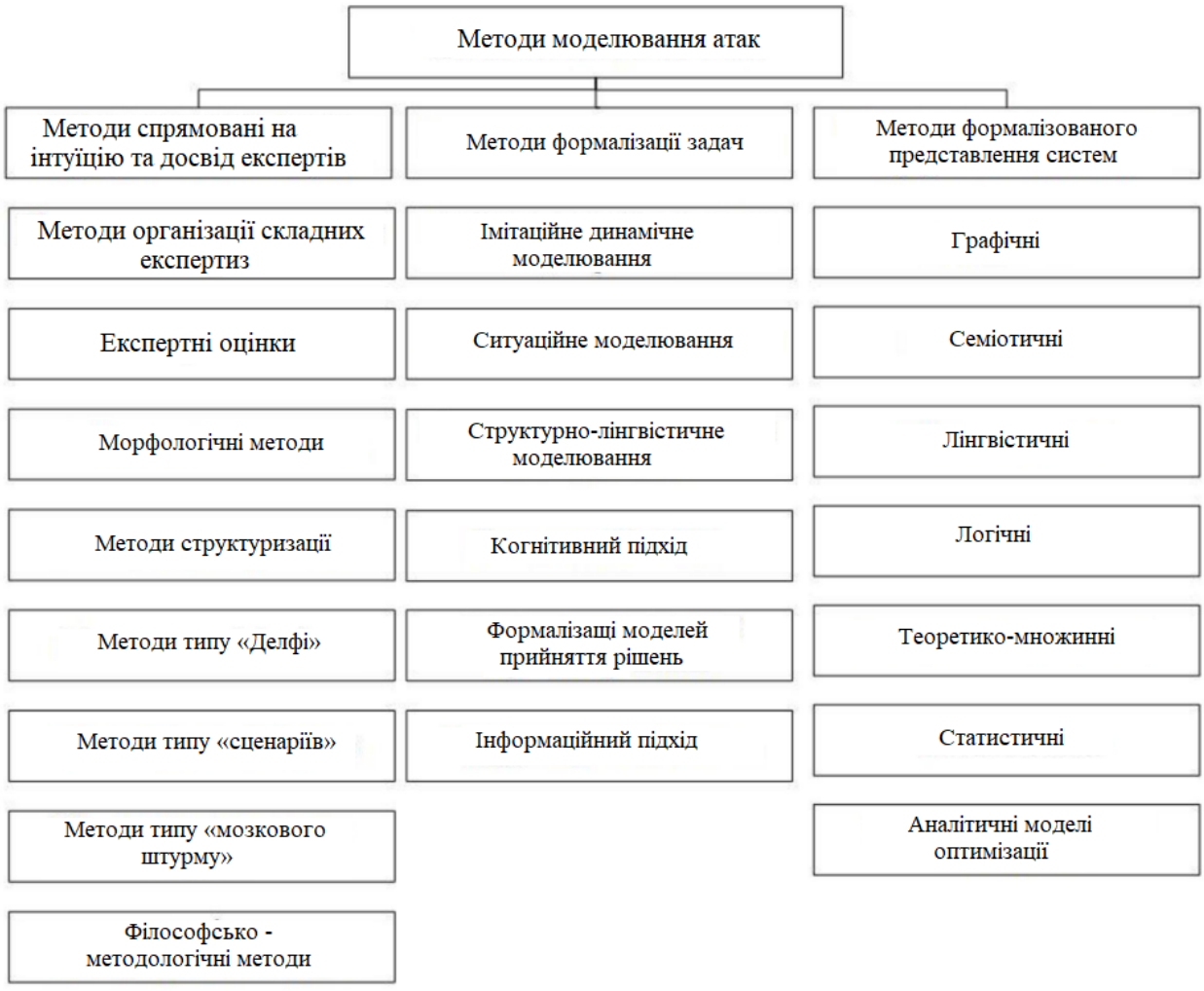
3. Запропонований метод оцінки ефективності системи захисту, надає компаніям можливість оцінювати ефективність системи захисту інформації на всіх етапах життєвого циклу розподілених інформаційних систем в реальному часі, дозволяє вносити коригування до проектних рішень системи захисту для нейтралізації загроз безпеки даних та дотримання вимог щодо захисту інформації, враховуючи, при цьому, фінансову складову при створенні системи безпеки.

Апробація роботи. Наукові результати і основні положення магістерської роботи доповідались і обговорювались на всеукраїнських та міжнародних науково-технічних конференціях,

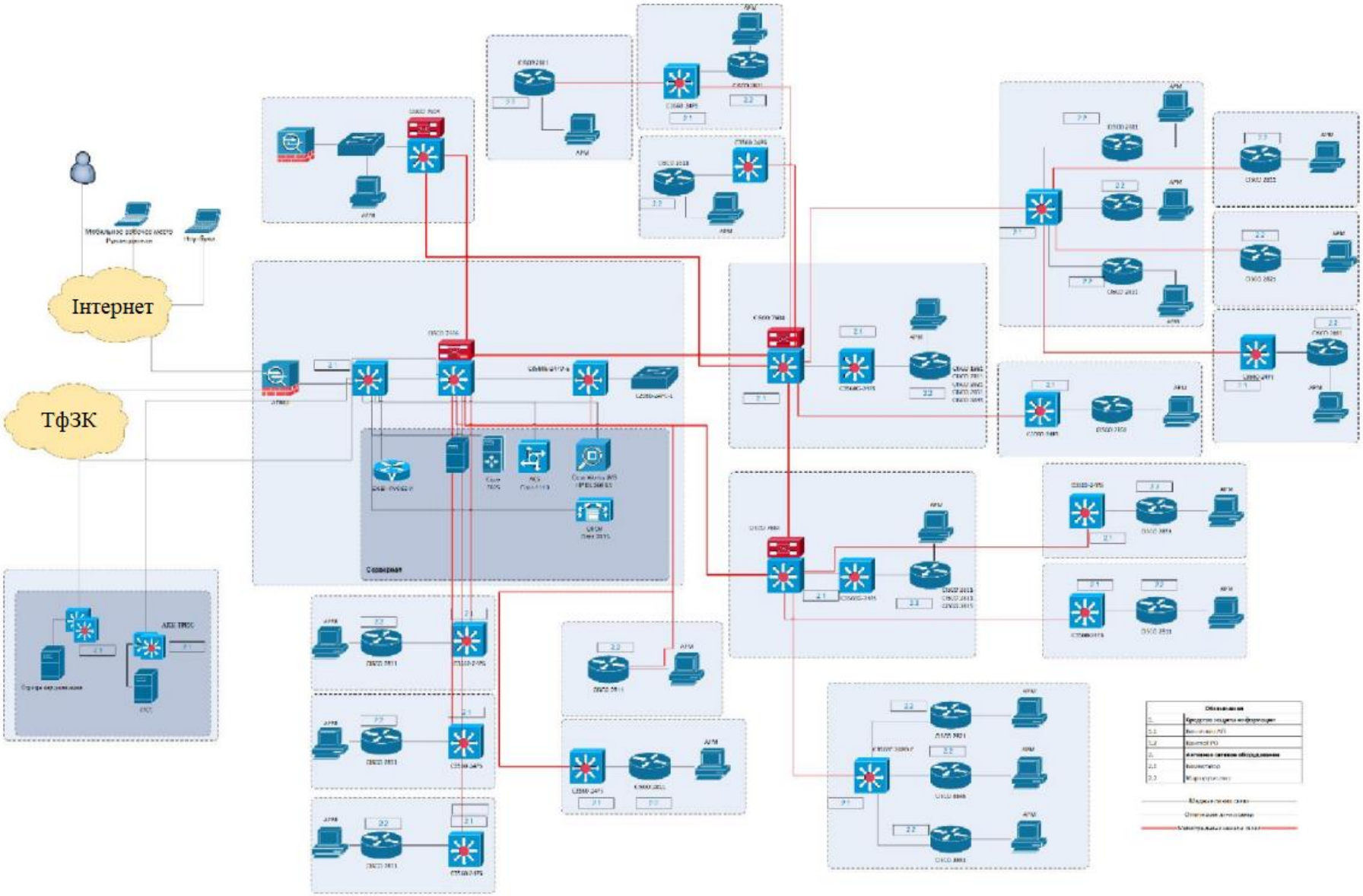
Публікації. За темою дипломної роботи ОКР «Магістр» опубліковано 1 теза доповідей, 1 фахова стаття.

Класифікація типів моделювання інформаційних систем

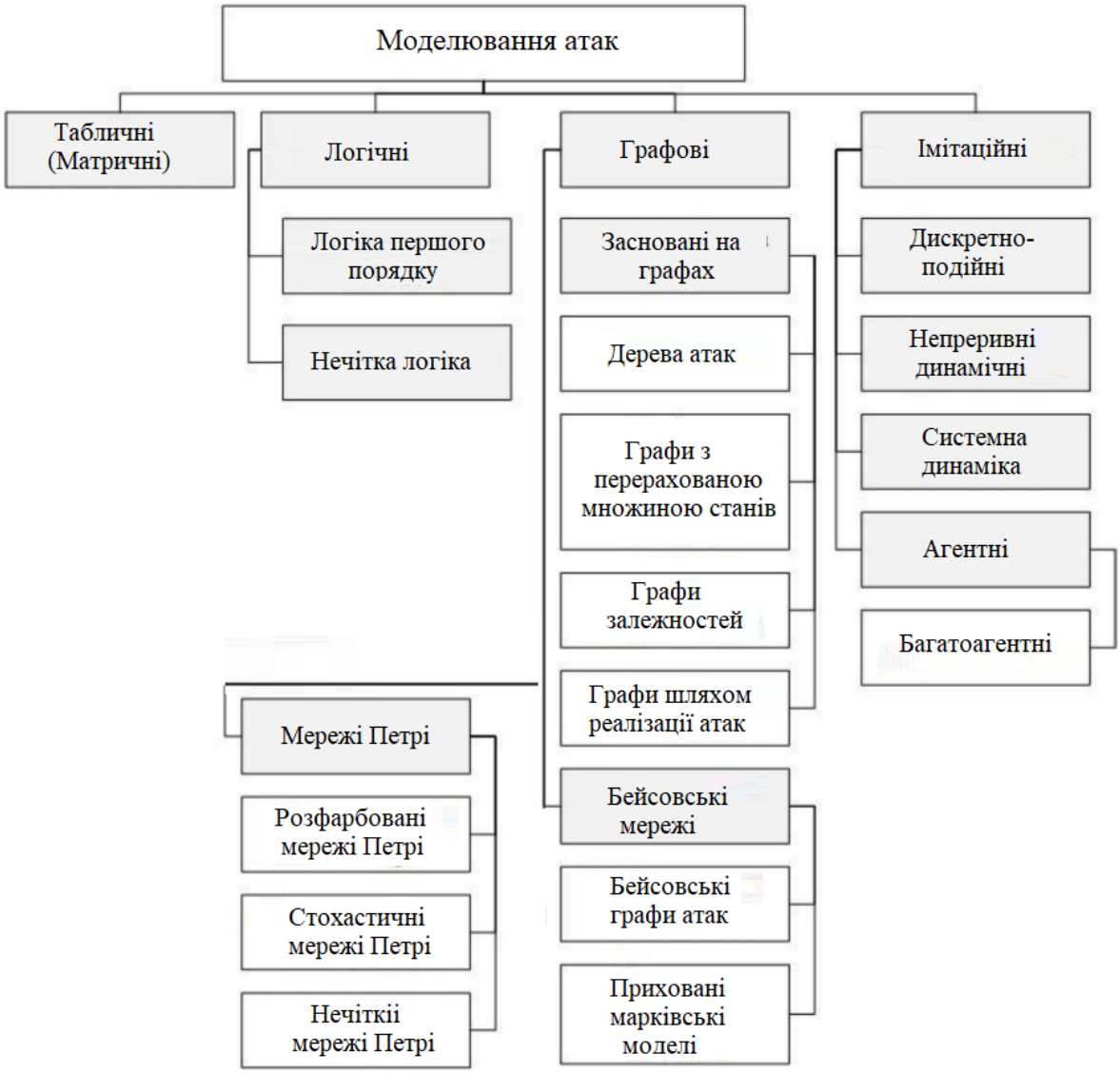
Класифікація методів побудови моделей атак



Структурна схема комплексу технічних засобів розподіленої інформаційної системи



Моделі атак на інформаційні системи



Переваги та недоліки моделей атак

Модель	Переваги	Недоліки
Логічні	Обробка інцидентів та використання мов представлення знань про предметну область.	Потребує значних обчислювальних ресурсів
Графові на деревах атак	Наочність, масштабованість, адаптованість, універсальність	Складні при моделюванні циклічних атак. Відсутність динамічної моделювання
Байєсівські графи	Масштабованість, адаптованість, універсальність, враховує невизначеності даних про атаки	Складні при моделюванні циклічних атак. Відсутність динамічного моделювання
Мережі Петрі	Зручність моделювання динамічних паралельних процесів, здатні відображати ймовірнісні процеси	Нездатність описувати поведінку порушника та цілі атаки
Імітаційні	Дозволяють моделювати поведінкові характеристики порушника та цілі атаки	Вимагають великих обчислювальних ресурсів

Модель визначення актуальних загроз безпеки конфіденційним даним

Перелік потенційних порушників інформаційної безпеки та рівень їх мотивації

Порушник	Мотив	Рівень мотивації
Зовнішній порушник		
Розвідувальні служби держав	Відсутній	Мінімальний
Кримінальні структури	Корисні інтереси: досягнення безпосередньої матеріальної вигоди, чи підрив репутації організації	Високий
Конкуренти (конкуруючі організації)	Відсутній	Мінімальний
Недобросовісні партнери	Корисливі інтереси: досягнення безпосередньої матеріальної вигоди, чи підрив репутації організації	Високий
Зломщики інформаційних систем та мереж	Хуліганство (вандалізм); професійне самоствердження	Високий

Нечітка модель, заснована на правилах типу:

$$R_i : IFx_i ISA_{i1} AND ... AND_{x_j} ISA_{ij} AND ... AND_{x_{im}} ISA_{im}, THEN$$

$$y = c_{i0} + \sum_{j=1}^{m} c_{ij} x_j,\ j = 1,...,n$$

Фрагмент бази знань правил визначення актуальних загроз інформаційній безпеці

№ п/п	IF (ЯКЩО)			THEN (ТО)
	Тип порушника (джерело впливу)	IT-інфраструктура (об'єкт впливу)	Версія ПЗ	
1	Зовнішній порушник із низьким потенціалом, Внутрішній порушник з низьким потенціалом	Віртуальна машина VMWare	6.5 (VMWare Workstation), від 7.0.0 до 7.1.4 включно (VMWare Workstation)	Загроза несанкціонованого доступу до захищених віртуальних машин з боку інших віртуальних машин
2	Зовнішній порушник з високим потенціалом	Мобільний пристрій на базі iOS	(Android), до 10.3.3 включно (iOS)	Загроза контролю шкідливою програмою списку додатків, запущених на мобільному пристрої
…				
N	Зовнішній порушник із середнім потенціалом, Внутрішній порушник з середнім потенціалом	Засіб захисту інформації	12.4 (Cisco IOS), 12.4 (Cisco IOS), 15.0 (Cisco IOS), 15.0 (Cisco IOS), 15.2 (Cisco IOS), 15.1 (Cisco IOS)	Загроза несанкціонованого впливу на засіб захисту інформації

Метод оцінки ефективності системи захисту конфіденційної інформації

Фрагмент бази правил оцінки ефективності системи захисту

IF (ЯКЩО)			THEN (ТО)
Вимоги до захисту інформації	Загроза інформаційній безпеці	Вартість системи захисту	
AI.3 C	ЗІБ. 01 Н	min	Ефективність СЗІ досягається
AI.4 НС	ЗІБ. 02 НН	max	Ефективність СЗІ не досягається
...			
КД.2 ЦС	ЗІБ. 0N НН	min	Ефективність СЗІ не досягається

База правил для реалізації методу оцінки ефективності системи захисту

$R_1 : AI.1(C)\ AND ЗІБ.01(H)\ AND COST(MIN)\ THEN EVALSZI(Д)$

$R_2 : AI.1(C)\ AND ЗІБ.01(H)\ AND COST(MAX)\ THEN EVALSZI(Д)$

$R_3 : AI.1(C)\ AND ЗІБ.01(НН)\ AND COST(MIN)\ THEN EVALSZI(НД)$

$R_4 : AI.1(C)\ AND ЗІБ.01(НН)\ AND COST(MAX)\ THEN EVALSZI(НД)$

$R_5 : AI.1(ЦС)\ AND ЗІБ.01(H)\ AND COST(MIN)\ THEN EVALSZI(Д)$

$R_6 : AI.1(ЦС)\ AND ЗІБ.01(H)\ AND COST(MAX)\ THEN EVALSZI(Д)$

$R_7 : AI.1(ЦС)\ AND ЗІБ.01(НН)\ AND COST(MIN)\ THEN EVALSZI(НД)$

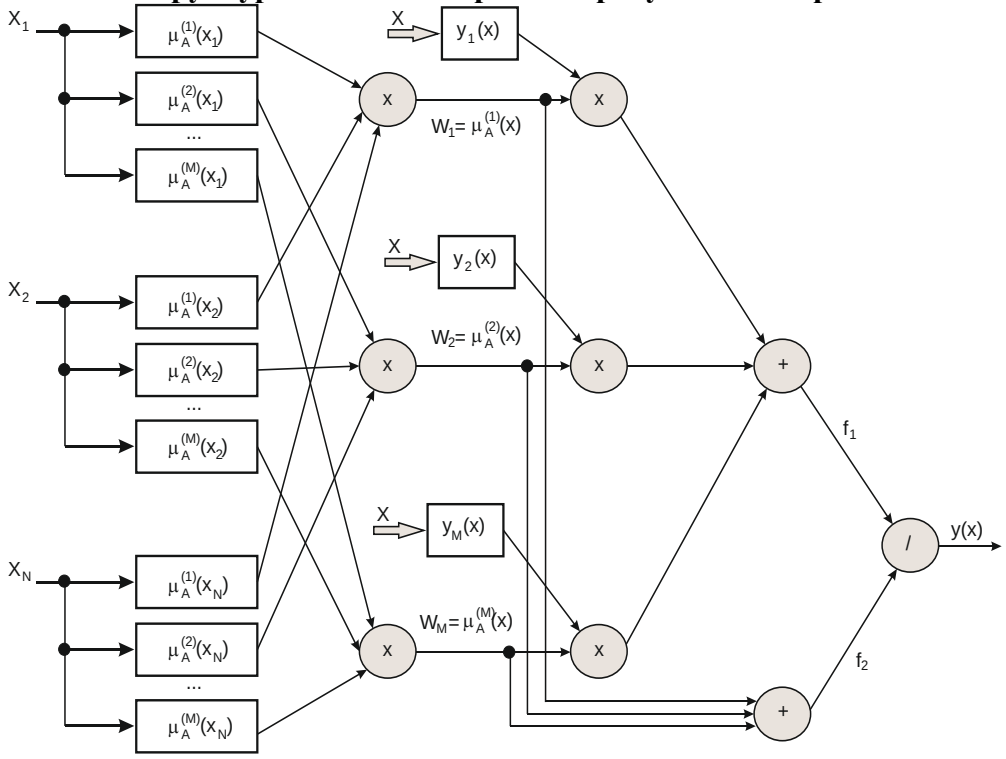
$R_8 : AI.1(ЦС)\ AND ЗІБ.01(НН)\ AND COST(MAX)\ THEN EVALSZI(НД)$

$R_9 : AI.1(ЧС)\ AND ЗІБ.01(H)\ AND COST(MIN)\ THEN EVALSZI(Д)$

...

$R_n : КД.2(ЦС)\ AND ЗІБ.03(НН)\ AND COST(MIN)\ THEN EVALSZI(НД)$

Структура нечіткої нейронної продукційної мережі



Аналіз дослідження оцінки ефективності запропонованого методу

Показник	Існуючі методи	Запропонований метод
RMSE	0,022-0,214	0,012-0,017
Ефективність системи захисту	85,6%	97,2%
Вартість системи захисту	зниження до 15%	зниження до 30%

Середньоквадратична помилка запропонованого методу, обчислюється за формулою: $RMSE = \sqrt{\frac{1}{N}\sum_{i=1}^{N}\left(y_i - \hat{y}_i\right)^2}$, де $y_i, \hat{y}_i$ - набори даних (перевірки, навчання). Графіки порівняння RMSE відомих та запропонованого методу на заданому інтервалі представлені на рис. 1

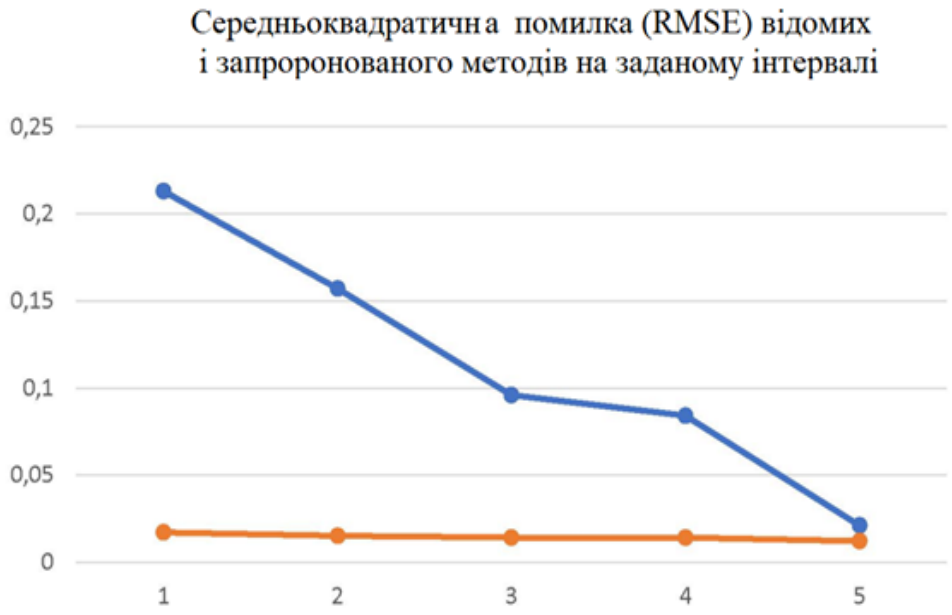
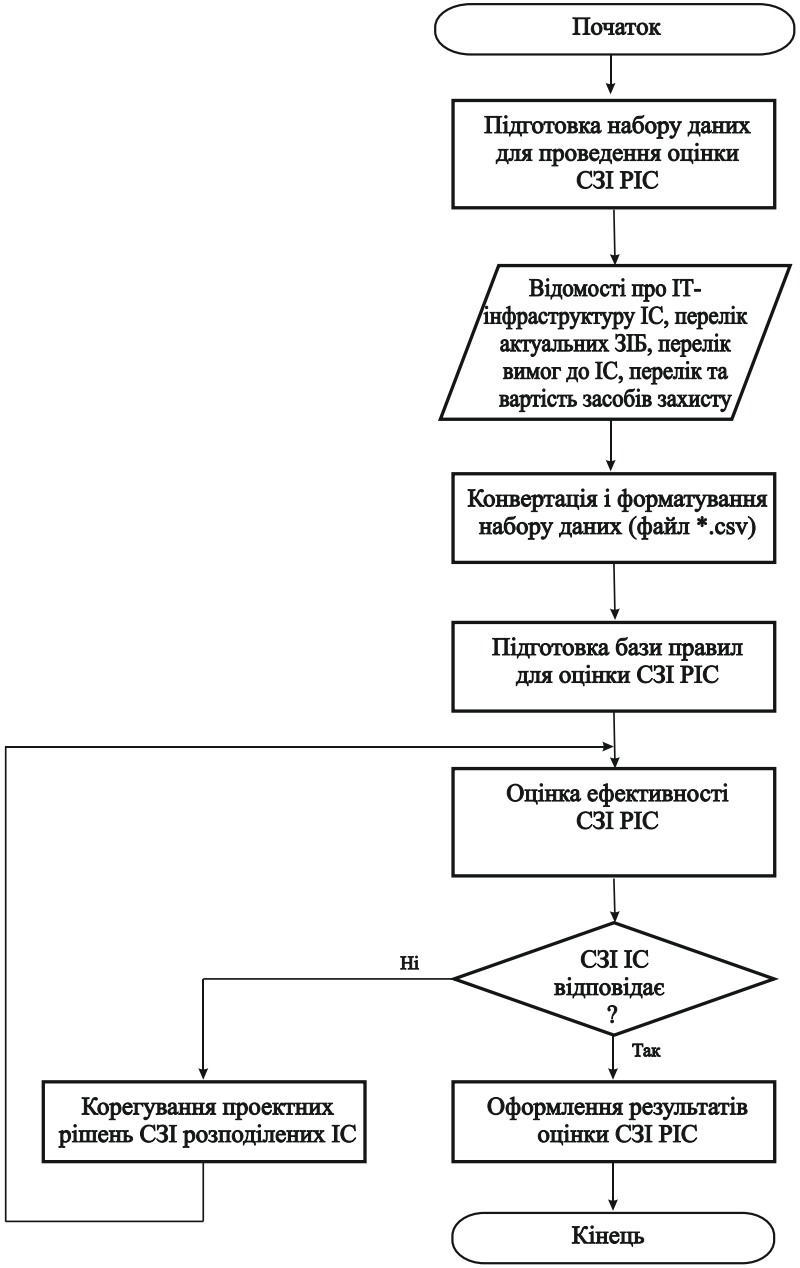
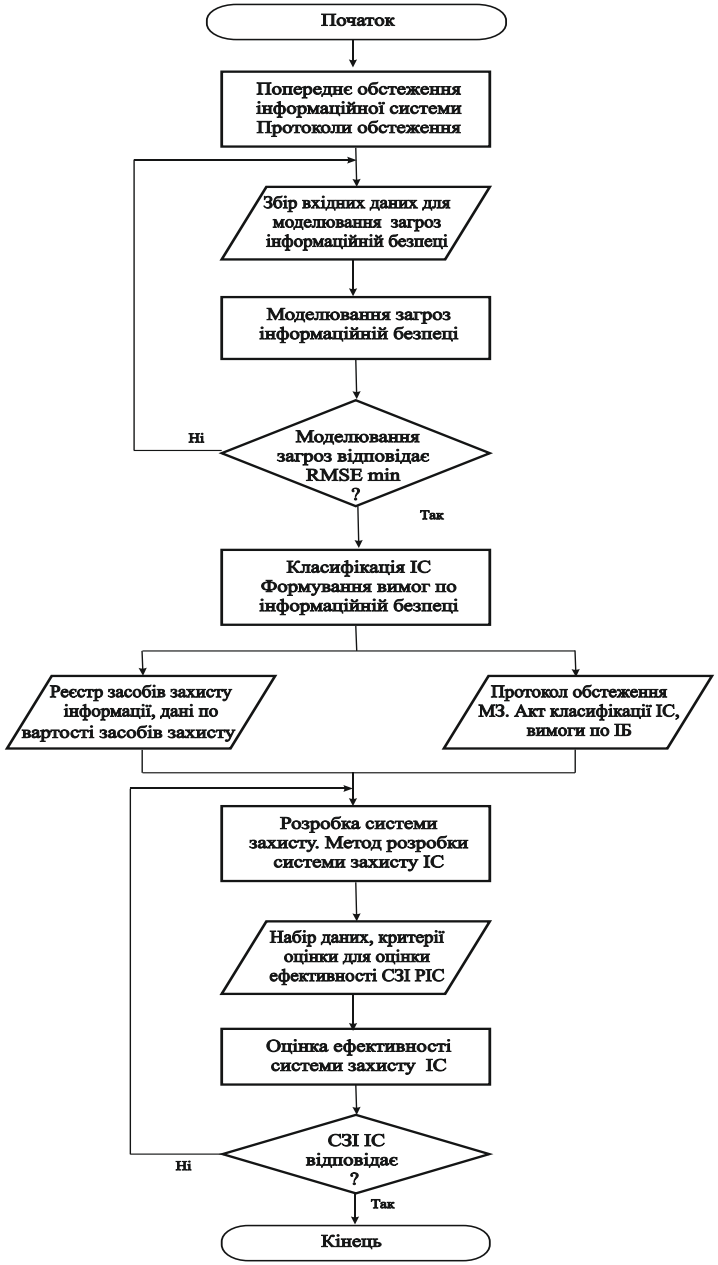


Рисунок 1 - Графік порівняння RMSE відомих та запропонованого методу на заданому інтервалі

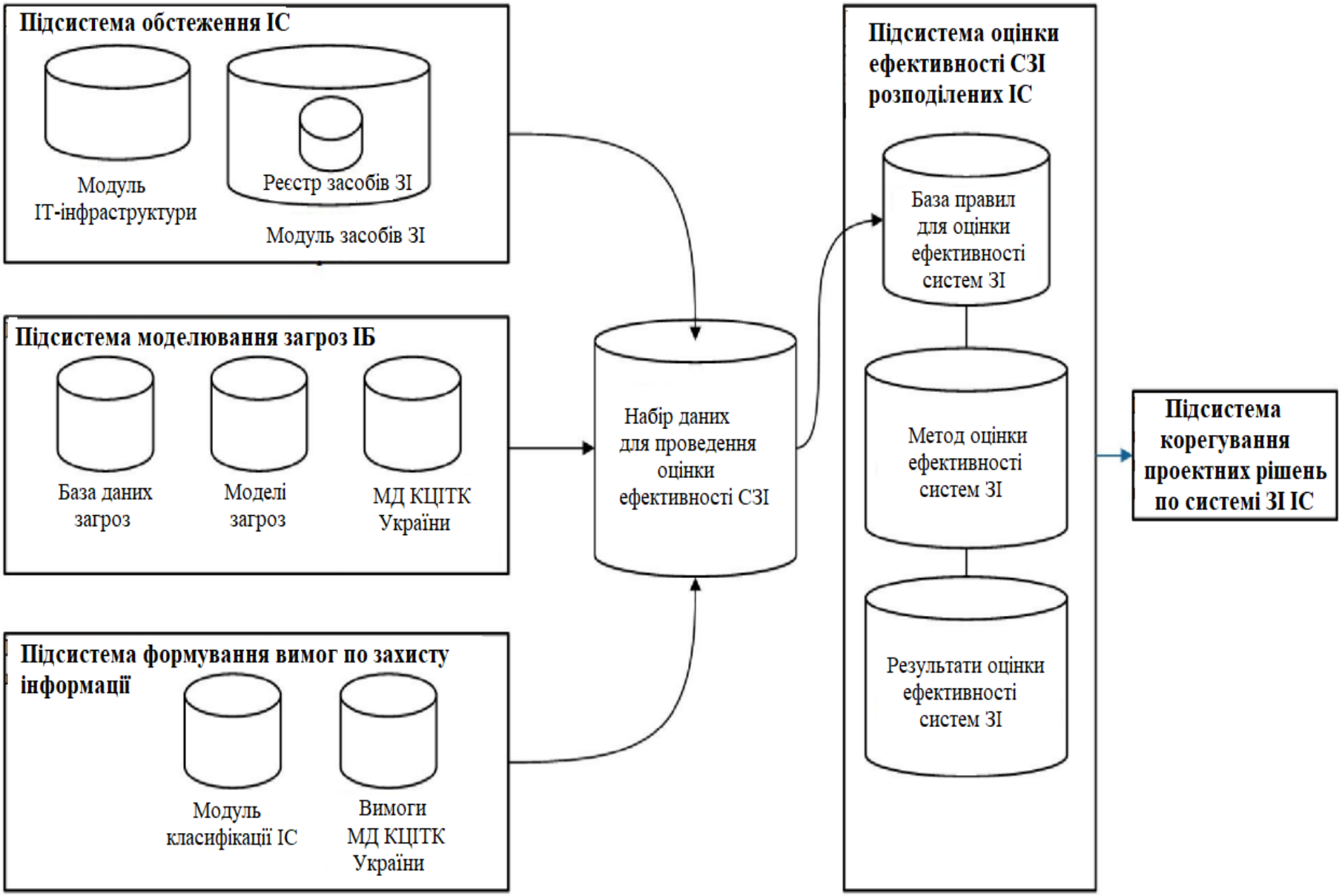
Алгоритм проведення оцінки ефективності системи захисту розподіленої інформаційної



Алгоритм життєвого циклу розробки системи захисту системи розподіленої інформаційної системи

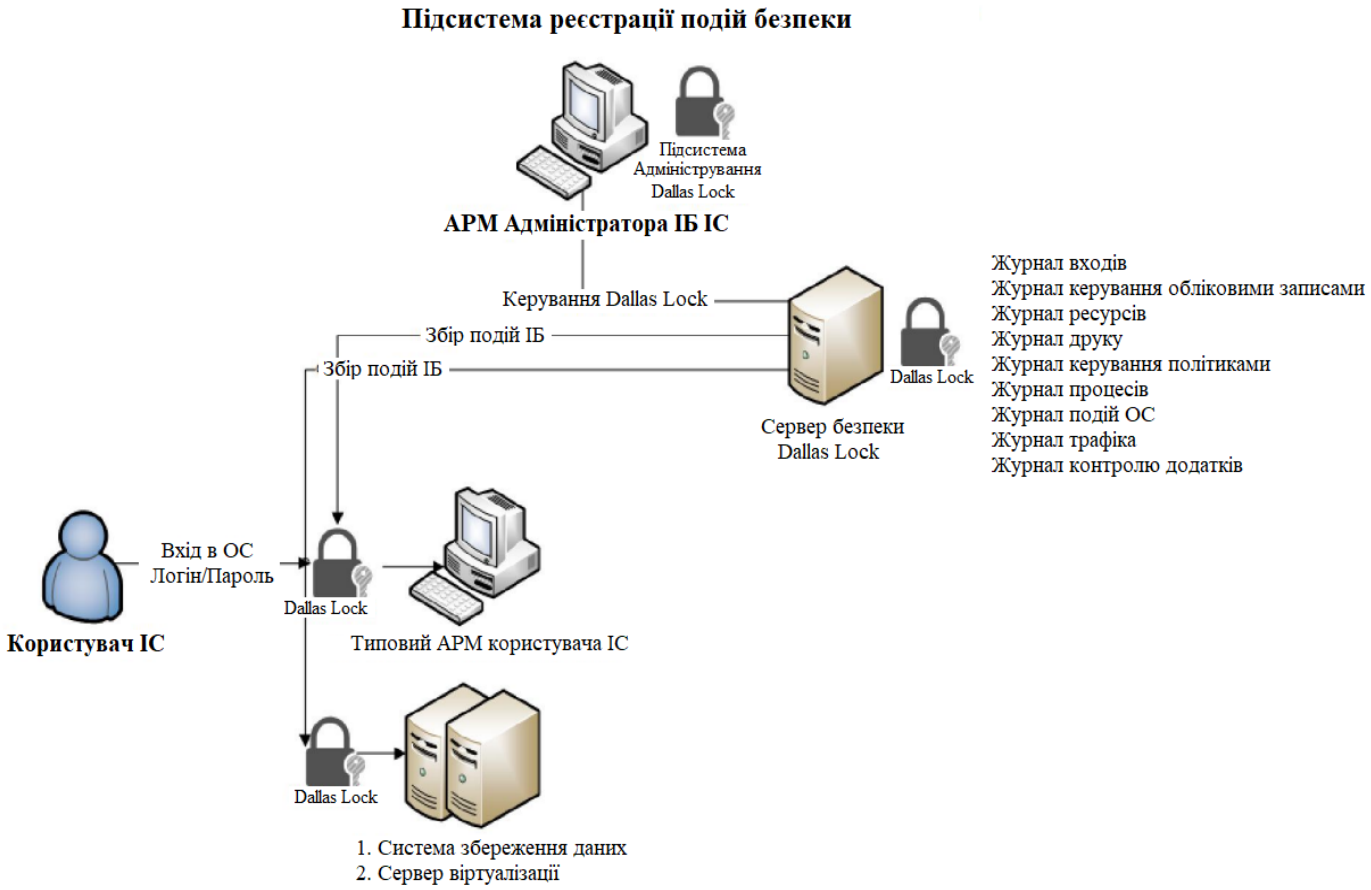


Структурна схема проведення оцінки ефективності системи захисту інформації розподіленої інформаційної системи



Логічна схема підсистеми захисту середовища віртуалізації інформаційної системи

Логічна схема підсистеми реєстрації подій безпеки інформаційної системи



ВИСНОВКИ

Для досягнення мети виконана та поставлена задача, що містить наступні результати дослідження:

1. Проведено аналіз розподілених інформаційних систем, визначено ключові аспекти IT-інфраструктури розподілених систем та систем захисту інформації, проведено аналіз методів та моделей інформаційних систем, моделей загроз інформаційній безпеці та атак, методів оцінки ефективності систем захисту інформації.

2. Запропоновано метод визначення актуальних загроз інформаційній безпеці, на відміну від відомих, в автоматизованому режимі формує перелік актуальних загроз інформаційній безпеці, мінімізує обчислювальні ресурси та трудомісткість процесу.

3. Запропонований метод оцінки ефективності систем захисту даних, заснований на теорії адаптивних продукційних нечітких нейронних систем та алгоритмі нечіткого виведення TSK. Дозволяє проводити оцінку ефективності систем захисту даних на основі достатніх та необхідних показників.

4. Запропоновані заходи щодо оцінки ефективності систем захисту інформації у розподілених інформаційних системах, на відміну від відомих, дозволяють власникам розподілених інформаційних систем у режимі реального часу оцінювати ефективність системи захисту, знизити фінансові витрати на розробку системи захисту даних, не потребує залучення висококваліфікованих фахівців з безпеки інформації, великих обчислювальних ресурсів.

Запропоновані заходи дозволяють: враховувати всі аспекти проведення оцінки ефективності системи захисту розподіленої інформаційної системи; може бути адаптована під умови власників розподілених інформаційних систем; виключає недоліки експертних методів, процес автоматизований, не вимагає залучення висококваліфікованих спеціалістів у області інформаційної безпеки.

Ефективність запропонованого методу підтверджується: достовірними результатами визначення переліку актуальних загроз інформаційній безпеці та досягнення ефективності системи захисту конфіденційних даних; відсутністю необхідності залучення висококваліфікованих фахівців в області безпеки інформації; використанням мінімальних обчислювальних ресурсів; можливістю адаптації під конкретні цілі власників розподілених інформаційних систем при проведенні оцінки ефективності системи захисту.

Результати магістерського дослідження з оцінки ефективності системи захисту розподілених інформаційних систем можуть бути використані для управління життєвим циклом інформаційних систем, проведення оцінки стану IT-інфраструктури, парку автоматизованих робочих місць; з метою оцінки відповідності підприємств підходам до управління інформаційними технологіями.

За темою роботи опубліковано 1 теза та 1 наукова стаття.

Завідувачу кафедри КБ
канд.техн.наук, доц. Кльоцу Ю. П.

Димбовського Максима Вячеславовича
ПІБ здобувача вищої освіти

ФІТ, 2 курсу, групи КБ-22-1

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 01.07.2022, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений(а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

11 грудня 2023 року

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 0.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 8%**

	Документ		Сумарний збіг по Базі Даних	
ID: 121896 Назва: Метод оцінювання ефективності засобів захисту інформації розподілених інформаційних систем Додано в БД: 2023-12-06 Автора: Димбовський М.В. Керівники: Джулій В.М. Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	106407	726	934 (1%)	17 (2%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

UNICHECK
by Turnitin

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1015975258

Дата перевірки:
06.12.2023 10:25:43 EET

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
06.12.2023 10:44:04 EET

ID користувача:
100008300

Назва документа: **Димбовський_Магістерська_Плагіат**

Кількість сторінок: **80** Кількість слів: **14361** Кількість символів: **119685** Розмір файлу: **11.70 MB** ID файлу: **1015654797**

3.76%
Схожість

Найбільша схожість: **0.79%** з джерелом з Бібліотеки (ID файлу: **1015654799**)

3.4% Джерела з Інтернету	688	Сторінка 82
1.57% Джерела з Бібліотеки	142	Сторінка 86

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи	76

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Метод оцінювання ефективності засобів захисту інформації розподілених інформаційних систем

Автор: Максим ДИМБОВСЬКИЙ
Спеціальність: 125 – Кібербезпека
Освітня програма: Кібербезпека
Науковий керівник: Володимир ДЖУЛІЙ., к.т.н, доц.
Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи.	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
5	Інше:	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) запозичення розміщені в розділах аналізу існуючих аналогів та прототипів, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
2) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
3) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає 3.76% і адресується до 142 першоджерела, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ Володимир ДЖУЛІЙ

Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ

Дата: 11.12.2023

Тарань О.Г

Тітова В.М

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітньо-кваліфікаційного рівня «магістр»

Студент Димбовський Максим Вячеславович

Тема: «Метод оцінювання ефективності засобів захисту інформації розподілених інформаційних систем»

Галузь знань 12 «*Інформаційні технології*» Спеціальність 125 «*Кібербезпека*» Освітня програма «Кібербезпека»

Обсяг дипломної роботи освітньо-кваліфікаційного рівня «магістр»: кількість сторінок записки 85;

1. Короткий зміст КР та прийнятих рішень Кваліфікаційна робота присвячена дослідженню питань, пов'язаних з розробкою та впровадженням системи оцінювання ефективності засобів захисту інформації розподілених інформаційних систем, з метою підвищення якості оцінки ефективності систем захисту за рахунок визначення достатніх та необхідних показників. Для досягнення мети проведено дослідження розподілених систем; визначені достатні та необхідних показників для мінімізації помилки роботи методу; оцінку ефективності запропонованого методу. Надає компаніям можливість оцінювати ефективність системи захисту на всіх етапах життєвого циклу в реальному часі, дозволяє вносити коригування до проектних рішень, для нейтралізації загроз безпеки даних та дотримання вимог щодо захисту інформації, враховуючи, при цьому, фінансову складову при створенні системи безпеки

2. Висновок про відповідність КР завданню Кваліфікаційна робота у повній мірі відповідає поставленому завданню як в теоретичній так і у практичній частині роботи.

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі обґрунтовується актуальність теми роботи, її зв'язок з галуззю знань «Інформаційні технології» та спеціальністю «Кібербезпека», формулюється мета та основні завдання кваліфікаційної роботи. У першому розділі було проведено аналіз існуючих систем захисту та управління доступом, що дозволило виявити проблеми та завдання, що потребують вирішення; застосування принципів побудови систем оцінювання ефективності безпеки стало основою для постановки задачі і проєктування архітектури системи. У другому розділі було проаналізовано вимоги та потреби підприємства з урахуванням специфіки, визначено необхідні компоненти та функціонал системи оцінювання ефективності безпеки, побудована модель визначення актуальних загроз безпеці конфіденційним даним. У третьому розділі наведено опис процесу реалізації системи оцінювання ефективності безпеки на підприємстві.

4. Позитивні сторони кваліфікаційної роботи Запропоновано метод визначення актуальних загроз інформаційній безпеці, на відміну від відомих, в автоматизованому режимі формує перелік актуальних загроз інформаційній безпеці, мінімізує обчислювальні ресурси та трудомісткість процесу. Запропонований метод оцінки ефективності систем захисту даних, заснований на теорії адаптивних продукційних нечітких нейронних систем та алгоритмі нечіткого виведення TSK. Дозволяє проводити оцінку ефективності систем захисту даних на основі достатніх та необхідних показників.Запропоновані заходи дозволяють: враховувати всі аспекти проведення оцінки ефективності системи захисту розподіленої інформаційної системи; може бути адаптована під умови власників розподілених інформаційних систем; виключає недоліки експертних методів, процес автоматизований, не вимагає залучення висококваліфікованих спеціалістів у області інформаційної безпеки.

5. Негативні сторони проекту: З роботи не зрозуміло яким чином в автоматизованому режимі формується перелік актуальних загроз інформаційній безпеці ситеми, і як при цьому мінімізуються обчислювальні ресурси, трудомісткість процесу виявлення загроз

6. Оцінка графічного оформлення та пояснювальної записки роботи._____

7. Відгук про роботу в цілому В загальному кваліфікаційна робота заслуговує позитивної оцінки. Весь матеріал кваліфікаційної роботи структурований, чіткий та послідовний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи. У пояснювальній записці багато наглядних пояснень. Графічний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої задачі проектування.

8. Інші зауваження -

9. Оцінка дипломної роботи Розглянувши позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що робота заслуговує оцінки «добре/ С (4,0)».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) _____

Лисенко Сергій Миколайович, д.т.н., професор, кафедра комп'ютерної інженерії та інформаційних систем, Хмельницького національного університету

« __11___ » ____грудня_____ 2023 . _____ (підпис)