Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра обчислювальної техніки

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

Комп'ютерна система оцінювання захищеності об'єкту

ПОЯСНЮВАЛЬНА ЗАПИСКА

Виконав: студентка 2-го курсу, групи 1КІ-22мз
спеціальності 123 – Комп'ютерна інженерія
_____Артоуз А. О.

Керівник: к.т.н., доц. каф. ОТ
_____Колесник І. С.

«17» 06 2024 р.

Опонент: : Голова секції УБ, д.т.н., проф.
_____ Яремчук Ю.Є. . .

«18» 06 2024 р.

Допущено до захисту
Завідувач кафедри ОТ
_____д.т.н., проф. Азаров О. Д.

«19» 06 2024 р.

ВНТУ 2024

ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра обчислювальної техніки
Галузь знань — Інформаційні технології
Освітній рівень — магістр
Спеціальність — 123 Комп'ютерна інженерія
Освітньо-професійна програма — Комп'ютерна інженерія

ЗАТВЕРДЖУЮ
Завідувач кафедри
обчислювальної техніки
_____ проф., д.т.н. О. Д. Азаров
«06» 02 2024 р.

З А В Д А Н Н Я

НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ

студенту **Артоуз Анастасії Олександрівні**

1 Тема роботи: Комп'ютерна система оцінки захищеності об'єкту.

Керівник роботи: к.т.н., доц. каф. ОТ Колесник І. С.

Затверджені наказом вищого навчального закладу від 11.03.2024 №81.

2 Строк подання студентом роботи 12.06.2024.

3 Вихідні дані до роботи: методи розробки прикладних застосунків, навчальні матеріали на тему створення прикладних застосунків, пакет Mathcad, системи-аналоги.

4 Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):

— вступ;

— аналітичний огляд комп'ютерних систем та існуючих підходів до систем захищеності об'єкту;

— моделювання та проєктування системи захищеності об’єкту;

— практична реалізація системи захищеності об’єкту;

— економічна частина.

5 Структура системи створення захищеності об’єкту: система створення та коригування бази даних.

6 Консультантів розділів роботи наведено у табл. 1.

Таблиця 1 — Консультанти розділів МКР

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1-4	к.т.н., доц. каф. ОТ Колесник І. С.		
5	к.е.н., проф. каф. ЕПВМ Небава М. І.		

7 Дата видачі завдання 12.03.2024.

8 Календарний план розділів роботи наведено у таблиці 2.

Таблиця 2 — Календарний план МКР

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів роботи	Примітка
1	Постановка задачі роботи	1.03.2024	вик
2	Інформаційний пошук та огляд літературних джерел	21.03.2024	вик
3	Дослідження підходів та розробка системи	10.04.2024	вик
4	Підготовка матеріалів пояснювальної записки	20.04.2024	вик
5	Перевірка якості оформлення магістерської роботи	1.05.2024	вик
6	Оформлення пояснювальної записки і презентації	12.05.2024	вик
7	Перевірка «антиплагіат»	22.05.2024	вик
8	Попередній захист	24.05.2024	вик

Студент _____ Артоуз Анастасія Олександрівна

Керівник _____ к.т.н., доц. каф. ОТ Колесник Ірина Сергіївна

АНОТАЦІЯ

УДК 004.62

Артоуз А. О. Комп’ютерна система оцінки захищеності об’єкту. Магістерська кваліфікаційна робота зі спеціальності 123 — комп’ютерна інженерія, освітня програма — комп’ютерна інженерія. Вінниця: ВНТУ, 2024 112 с.

На укр. мові. Бібліогр.: 40 назв; рис.: 19; табл.: 11.

У цій магістерській дипломній роботі розглядаються існуючі підходи та програмні засоби для створення системи оцінки захищеності об’єкту. Проаналізовано особливості створення системи моніторингу захищеності об’єкту. Головною метою цієї роботи є досягнення максимальної ефективності захисту за допомогою використання всіх необхідних методів, ресурсів,а також засобів, які виключають неавторизований доступ до інформації.

Ключові слова: розробка, система, інформаційний простір, види мережевих атак, інтенсивність атак.

ABSTRACT

Artouz A. O. Computer system for assessing object security. Master's qualification thesis on specialty 123 — computer engineering, educational program — computer engineering. Vinnytsia: VNTU, 2024, 112 p.

In Ukrainian language. Bibliography: 40 titles; fig.: 19; tab.: 11.

This master's thesis examines the existing approaches and software tools for creating an object security assessment system. The peculiarities of creating a system for monitoring the object's security have been analyzed. The main goal of this work is to achieve the maximum effectiveness of protection by using all the necessary methods, resources, as well as means that exclude unauthorized access to information.

Keywords: development, system, information space, types of network attacks, intensity of attacks.

ЗМІСТ

ВСТУП

Інформаційна безпека стає все більш важливою та значущою сферою національної безпеки України, що відображено у Доктрині інформаційної безпеки України, затвердженій Указом Президента України від 25 лютого 2017 року №47/2017. Відповідно до Доктрини, інформаційні технології набули глобального характеру і стали невід'ємною частиною всіх сфер діяльності держави, суспільства та особистості. З розширенням сфер застосування інформаційних технологій значно зростають і ризики нових інформаційних загроз та атак. Зарубіжні спеціальні служби використовують інформаційно-психологічний вплив для дестабілізації соціальної та внутрішньополітичної ситуації в різних регіонах світу, що може призвести до порушення територіальної цілісності та підриву суверенітету інших держав.

У сфері оборони держави, економіки, суспільної та державної безпеки, науки, освіти та технологій спостерігаються визначені державою стратегічні цілі для забезпечення ефективного стану безпеки конфіденційної інформації. Одночасно з розвитком інформаційних технологій зростає і кількість засобів та методів порушення безпеки конфіденційної інформації. Останні роки характеризуються різким зростанням кількості витоків конфіденційної інформації, як це видно зі звітів експертно-аналітичного центру групи компаній SafeNet. Для зміни ситуації на краще необхідно розробляти нові методи та підходи, які можуть забезпечити надійний захист від сучасних загроз безпеці інформації.

Задача забезпечення безпеки конфіденційної інформації стає найактуальнішою у зв'язку з ростом комп'ютерних атак та витоків інформації, що відображаються у статистичних даних про злочини у сфері високих технологій. У 2021 році зростання кримінальної активності з використанням SafeNet. Для зміни ситуації на краще необхідно розробляти нові методи та

підходи, які можуть забезпечити надійний захист від сучасних загроз безпеці інформації.

Задача забезпечення безпеки конфіденційної інформації стає найактуальнішою у зв'язку з ростом комп'ютерних атак та витоків інформації, що відображаються у статистичних даних про злочини у сфері високих технологій. У 2021 році зростання кримінальної активності з використанням сучасних комунікаційних пристроїв та Інтернету склало 39%. Кожен двадцятий злочин кваліфікується як кіберзлочин. Лідирують злочини, пов'язані з розповсюдженням комп'ютерних вірусів та неправомірним доступом до конфіденційної інформації. Друге місце займає шахрайство з використанням онлайн-платежів, кількість таких правопорушень у першому півріччі 2022 року зросла у 8 разів. Щорічні звіти міжнародної компанії Group-IB також відзначають активність проурядових організацій, які проводять кібератаки для досягнення своїх цілей.

Для досягнення цілей забезпечення безпеки конфіденційної інформації необхідно організувати ефективне створення системи захисту інформації, моделювання актуальних загроз інформаційної безпеки, визначення актуальних порушників та проведення якісної оцінки ефективності системи захисту. Однією з найважливіших задач є оцінка ефективності системи захисту. Метою магістерської роботи є підвищення якості оцінки ефективності систем захисту розподілених інформаційних систем за допомогою визначення достатніх та необхідних показників, використовуючи сучасні інформаційні технології, що дозволяють ефективно вирішувати наступні задачі: визначення параметрів роботи адаптивних продукційних нечітких нейронних систем, застосування технологій Data Science для обробки даних, та алгоритмів нечіткого виведення.

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

Предмет дослідження – методи визначення актуальних загроз безпеці конфіденційної інформації та оцінки ефективності систем захисту конфіденційної інформації.

Метою магістерського дослідження є підвищення якості оцінки ефективності систем захисту розподілених інформаційних систем за допомогою визначення достатніх та необхідних показників. Для досягнення цієї мети необхідно вирішити наступні задачі:

1. Провести дослідження розподілених інформаційних систем, аналіз загроз та атак на безпеку конфіденційної інформації, аналіз перспективних методів моделювання загроз та оцінки ефективності систем захисту.

2. Підвищити якість визначення атак та загроз за рахунок визначення достатніх та необхідних показників для мінімізації помилок методу.

3. Провести оцінку ефективності запропонованого методу.

Наукова задача магістерського дослідження полягає у підвищенні якості оцінки ефективності системи захисту розподілених інформаційних систем через запропонування методу визначення актуальних загроз інформаційній безпеці та оцінки ефективності системи захисту, заснованого на продукційних адаптивних нечітких нейронних мережах.

Наукова новизна результатів дослідження включає:

1. Запропонування методу визначення атак та актуальних загроз безпеці конфіденційної інформації, який формує перелік актуальних загроз, виключаючи помилки експертів.

2. Запропонування методу оцінки ефективності систем захисту, заснованого на нечітких адаптивних нейронних продукційних мережах та алгоритмі нечіткого виведення з використанням технологій Data Science.

Практичне значення роботи полягає у:

1. Проведеному аналізі розподілених систем, що дозволив визначити основні аспекти технології обробки інформації та використати ці результати для

визначення показників моделювання загроз і оцінки ефективності системи захисту.

2. Запропонованому методу визначення загроз, який мінімізує трудомісткість процесу та обчислювальні ресурси, виключаючи недоліки експертів.

3. Запропонованому методу оцінки ефективності системи захисту, який дозволяє компаніям оцінювати ефективність системи захисту інформації на всіх етапах життєвого циклу розподілених систем у реальному часі, вносити коригування до проектних рішень, нейтралізувати загрози та дотримуватися вимог до захисту інформації, враховуючи фінансову складову.

Методи дослідження включають теорію ймовірностей, методи неявного перебору, динамічного програмування, математичну статистику, теорію нечітких адаптивних нейронних систем та алгоритми нечіткого виведення.

Основні результати дослідження, що виносяться на захист:

1. Метод визначення актуальних загроз інформаційній безпеці.

2. Метод оцінки ефективності систем захисту даних.

Обґрунтованість та достовірність результатів підтверджуються системним підходом, математичним обґрунтуванням, обґрунтуванням показників та методів визначення загроз і оцінки ефективності, публікацією результатів у наукових виданнях та апробацією на міжнародних конференціях.

Публікація за темою роботи – "Компютерна система оцінки захищеності обєкту"

Комп'ютеризована система оцінки захищеності об'єкта / О. Д. Азаров, А. О. Артоуз, І. С. Колесник // Матеріали конференції «Молодь в науці: дослідження, проблеми, перспективи» . Вінниця 2024 р. 2 с. [Електронний ресурс].

Режим доступу:https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2022/paper/view/15930/13376

1 ОГЛЯД ТА АНАЛІЗ СУЧАСНИХ МОДЕЛЕЙ ТА МЕТОДІВ ПОБУДОВИ СИСТЕМ ДЛЯ ОЦІНЮВАНЯ ЗАГРОЗ ТА БЕЗПЕКИ ДАНИХ

1.1 Огляд моделей та методів побудови інформаційних систем

Моделювання інформаційних систем є одним із основних методів дослідження в галузях знань, підходом до оцінки поведінки складних інформаційних систем на основі наукового методу. Моделювання інформаційних систем Замінити існуючу інформаційну систему на іншу з використанням об’єктної моделі інформаційної системи для отримання необхідної інформації про реальну систему [14, 16], а також для моделювання загроз безпеки даних та атак.

На даний момент існує наступна класифікація видів моделювання інформаційних систем. (рис. 1.1).

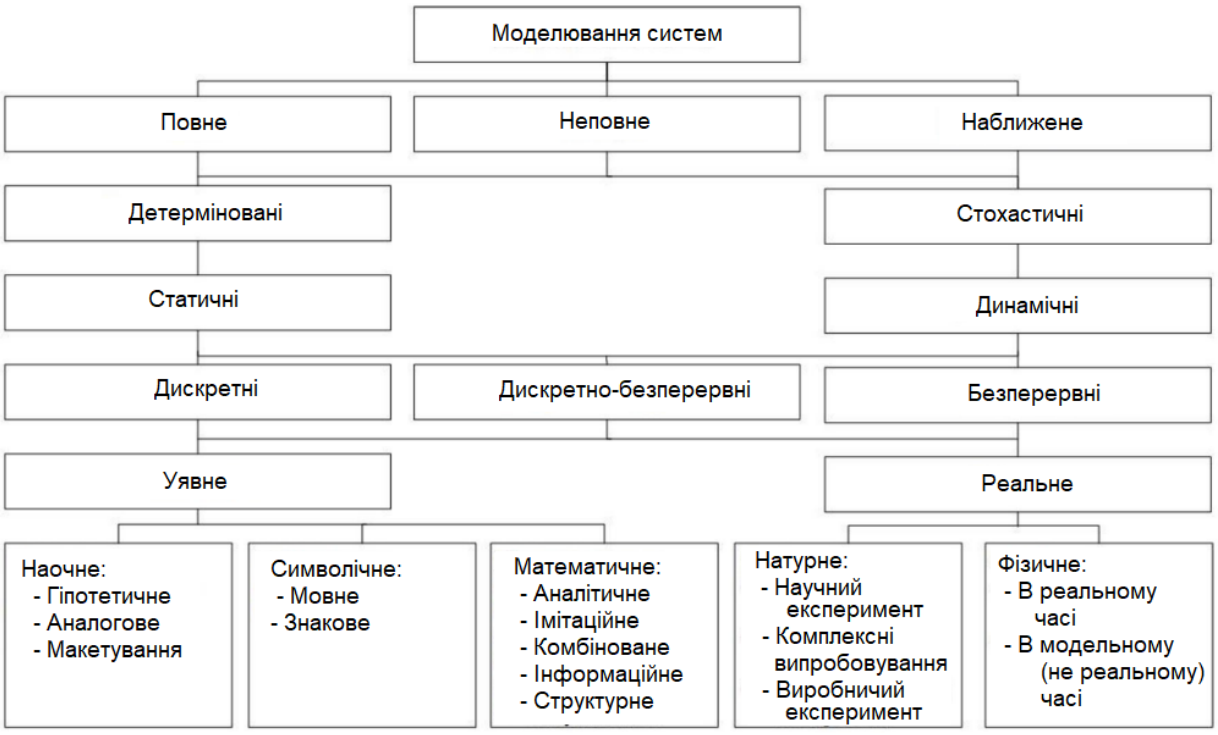


Рисунок 1.1 — Класифікація типів моделювання інформаційних систем

За класифікаційними ознаками моделі поділяються на: неповні, гіпотетично повні. Залежно від характеристик процесів моделі поділимо на: стохастичні, детерміновані, динамічні, статичні, дискретні, дискретно-неперервні, безперервні. Статичне моделювання визначає поведінку інформаційної системи в будь-який момент. Детермінований Відображає процеси без випадкових дій. Динамічне моделювання відображає поведінку інформаційної системи в часі. Стохастик відображає ймовірнісні події та процеси. Безперервне моделювання відображає безперервні процеси, дискретне – описує дискретні процеси в інформаційній системі. Дискретно-континуальне моделювання використовується для опису безперервних і дискретних процесів. Віртуальний використовується для моделювання об’єктів, які існують поза станом їх створення або є нематеріальними на певному інтервалі часу [12].

При візуальному моделюванні формулюються моделі інформаційної системи, які відображають процеси і явища, що відбуваються в системі. У гіпотетичному моделюванні розробляється гіпотеза про закономірності процесів у реальних інформаційних системах, заснована на причинно-наслідкових зв’язках між виходами та входами, що відображає рівень знань експерта про досліджувану інформаційну систему. Спекулятивне моделювання використовується, коли недостатньо знань про інформаційну систему для побудови формальних моделей. Макетування використовується в реальній інформаційній системі, коли процеси неможливо фізично змоделювати. Моделі базуються на аналогах інформаційної системи, заснованих на причинно-наслідкових зв'язках між процесами і явищами системи. У випадку з математичним моделюванням необхідно здійснити формалізацію цього процесу, побудувати математичну модель. Математичне моделювання – це процес встановлення відповідності деякого математичного об’єкта з реальною інформаційною системою – математичною моделлю.

Моделювання інформаційних систем на сучасному етапі здійснюється засобами комп'ютерної техніки. При побудові математичної моделі кожна система S характеризується відповідним набором властивостей, які

враховують стан взаємодії системи із зовнішнім середовищем E і відображають поведінку досліджуваної модельної системи. Модель системи S можна представити у вигляді набору значень, які визначають роботу процесу реальної інформаційної системи та утворюють наступні підмножини:

Сукупність внутрішніх параметрів системи: . h H k n k H

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. Вплив зовнішнього середовища, вхідні ефекти є незалежними змінними, у векторній формі наступного вигляду:

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

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

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

Функціонування інформаційної системи S описується оператором

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

Залежність (1.1) — правило роботи інформаційної системи. Алгоритм функціонування системи AS — це метод отримання початкових властивостей системи шляхом врахування впливу внутрішніх параметрів системи h(t), зовнішнього середовища v(t) та впливу вхідних даних x(t). Правило роботи Fs інформаційної системи S може бути реалізовано багатьма різними алгоритмами роботи AS 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 $\{\bar{x}(t),\bar{v}\}(t),\bar{h}\,(\mathrm{t})\}$ з математичними зв'язками між ними та характеристиками $\bar{y}(t)$ [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, z0 — початковий стан, $z0\in Z$, функція виходу ψ (z ,x) , функція переходу φ (z,x).

Мережеві моделі (N -схеми) — мережі Петрі Використовується для вирішення проблем, пов’язаних з аналізом причинно-наслідкових зв’язків і

формальним описом у складних системах. Мережі Петрі використовуються як найпоширеніший формалізм для опису взаємодії та структури процесів і паралельних систем.

Мережа Петрі (N-схема) задається наступним чином:

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

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 $O(d_j)$ і для переходу множину вихідних позицій $O(d_j)$.

Методи класифікації моделей побудови систем показано на рисунку 1.2.

Розглянуті методи та моделі мають свої переваги та недоліки.

Основними недоліками перерахованих моделей є те, що будь-яка модель скорочує опис можливих явищ; Під час моделювання не завжди можливо виявити нові якісні ознаки; Як правило, даних, необхідних для налаштування моделей, недостатньо; Статистичні моделі системи можуть бути об'єктивними в межах

емпіричного набору побудови моделей.

Рисунок 1.2 — Класифікація методів побудови моделей атак

За результатами проведених досліджень можна зробити висновок, що існуючі методи побудови системних моделей мають ряд недоліків, які в свою чергу свідчать про необхідність вдосконалення розглянутих моделей.

1.2 Аналіз архітектури систем захисту конфіденційної інформації

З розвитком і зростанням інформаційних технологій зростає і складність архітектури інформаційної системи. Сучасні інформаційні системи мають клієнт-серверну територіально розподілену та багатокористувацьку архітектуру. Програмне забезпечення, засноване на відкритому інтерфейсі програмування, надає можливість робити функціональні вдосконалення за допомогою поширених мов програмування (TypeScript (середовище розробки dotnet.core, платформа розробки Angular)) [20].

Інформаційні системи забезпечують принцип централізованого накопичення, зберігання та багаторазового використання даних. З метою забезпечення інформаційної безпеки та економії ресурсів інформація не зберігається на автоматизованих робочих місцях користувачів. Обробка даних відбувається в серверній кімнаті [15]. Для реалізації цього підходу можна використовувати технології термінального доступу. Цю технологію можна реалізувати шляхом розгортання інфраструктури ферми терміналів TT Remote Desktop Services (RDS). У цьому випадку профілі співробітників зберігаються на сервері ферми терміналів, що полегшує доступ організаційних користувачів до ресурсів інформаційної системи, а найефективніші процеси безпеки забезпечують безпеку даних. Технологія також забезпечує віддалений робочий процес користувача [18]. Розподілені інформаційні системи характеризуються розташуванням мережевих пристроїв і робочих станцій користувачів, серверних компонентів на материку та за його межами. Такі системи мають складну

архітектуру організаційних компонентів і технологій обробки даних. Відповідно, одночасно виникають проблеми із забезпеченням безпеки даних [20].

Розподілена система включає наступні компоненти:

1. Сервери, наприклад спеціалізоване та прикладне програмне забезпечення, забезпечують представлення даних у формах, необхідних для автоматизованої обробки інформації; серверні пристрої.

2. Робочий простір користувача: типові робочі простори користувача (непортативні персональні комп'ютери); Мобільні робочі місця — мобільні телефони, планшети.

Він використовує криптографічний захист між компонентами інформаційних систем для забезпечення захисту інформації, що передається через відкриті комунікації. Типова схема комплексу технічних механізмів розподіленої інформаційної системи представлена на рисунку. 1.3.

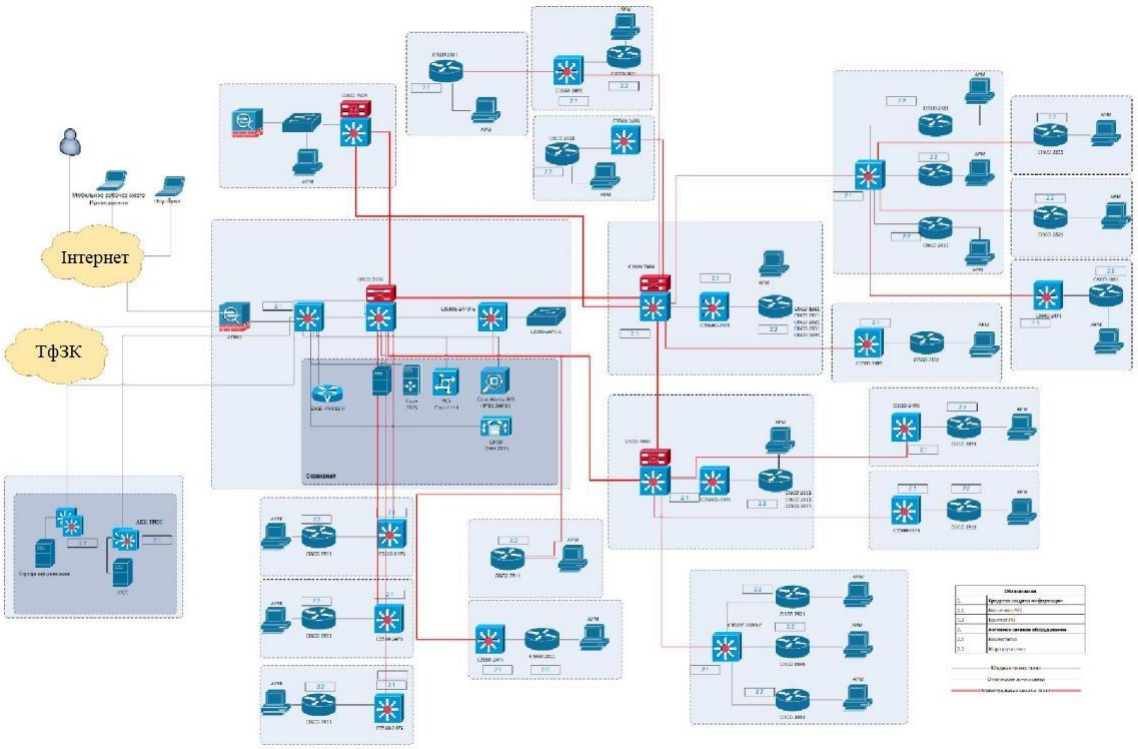


Рисунок 1.3 — Структурна схема комплексу технічних засобів розподіленої інформаційної системи

Розподілені інформаційні системи мають низку аспектів IT-інфраструктури, які необхідно враховувати при моделюванні ризиків інформаційної безпеки, створенні індикаторів для оцінки ефективності системи інформаційної безпеки, основними з яких є: канали зв'язку (незахищені мережі передачі даних), обробки інформації в центрах обробки даних, територіально розподілених інформаційних системах, клієнт-серверних додатках, хмарній інфраструктурі. Особливої уваги заслуговують категорії зловмисників у розподілених інформаційних системах, якими є внутрішні та зовнішні групи порушень [18].

Комп'ютерна атака — несанкціонований цілеспрямований вплив на ресурс з використанням інформації автоматизованої системи, апаратних і програмних засобів для отримання несанкціонованого доступу до даних. Об'єкт атаки (мішень атаки) – це елемент розподіленої інформаційної системи. В даний час існує багато моделей атак, підходів і методів моделювання атак. Порушник — особа, яка навмисно використовує нетехнічні та технічні заходи, механізми контролю, управління безпекою, щоб навмисно скомпрометувати мережі та системи, скомпрометувати мережі та системи, зменшити мережеві ресурси, дані інформаційної системи, дані інформаційної системи д ля законних користувачів [19].

Основні моделі атак на розподілені системи представлені на рисунку 1.4. Переваги та недоліки основних моделей атак наведено в таблиці 1.1.

Таблиця 1.1 — Переваги та недоліки моделей атак

Модель	Переваги	Недоліки
1	2	3
Логічні	Обробка подій і використання мов презентації. 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, універсальність, адаптованість, враховує невизначеності даних про атаки	Складні при моделюванні циклічних атак. відсутність динамічного моделювання
Мережі Петрі	Зручність моделювання динамічних паралельних процесів, які можуть показати ймовірнісні процеси	Відсутність опису характеру злочинця та цілей атаки
Імітаційні	Дозволяють моделювати пове-дінкові характеристики	Вимагають великих обчислювальних ресурсів

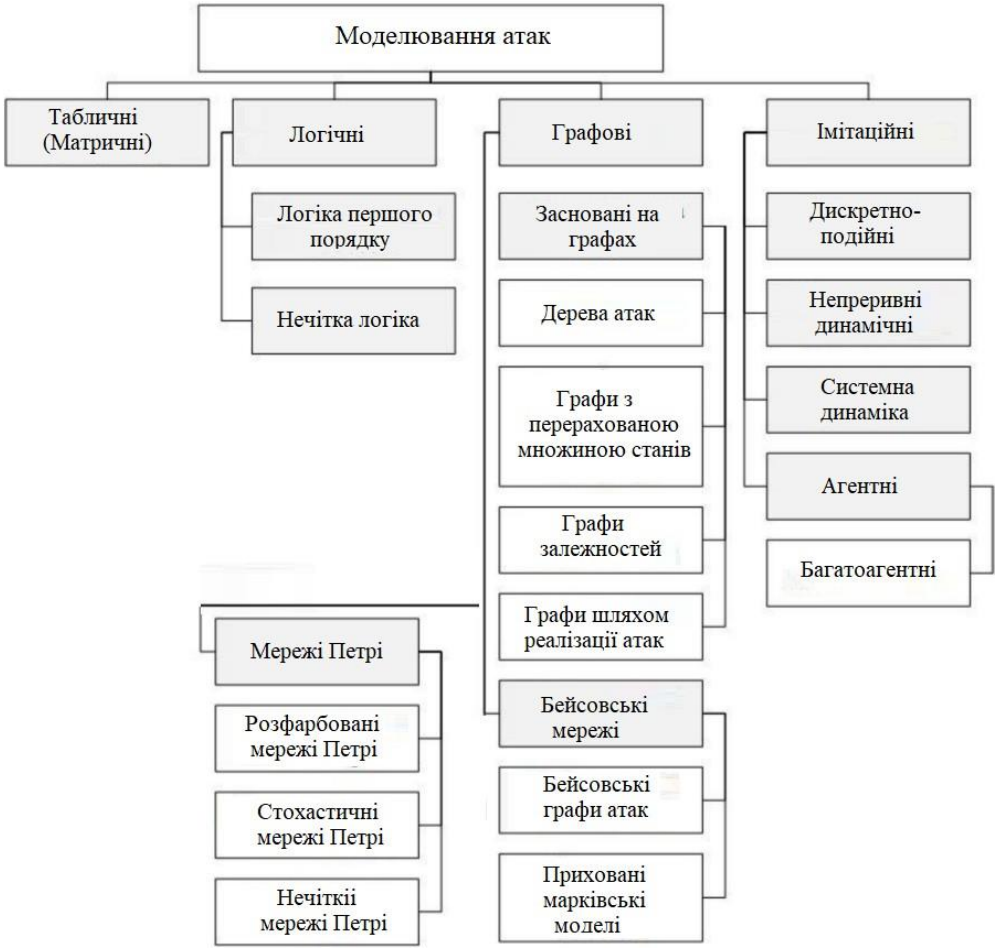


Рисунок 1.4 — Моделі атак на інформаційні системи

При розробці моделі зловмисника та моделі загроз інформаційній безпеці в розподіленій інформаційній системі необхідно враховувати вектори атак в інформаційній системі. З аналізу проведеного дослідження можна зробити висновок про необхідність розгляду недоліків методів моделювання, особливо загроз інформаційній безпеці.

1.3 Аналіз методів та методик оцінювання ефективності систем захисту інформації

Ефективність системи захисту інформації Ступінь, до якої результат захисту інформації відповідає меті захисту інформації. Для оцінки ефективності системи захисту даних необхідно визначити методи та показники оцінки.

Основними методами оцінки ефективності захисту приватних інформаційних систем є: імовірнісний; статистичні; експерт; частота; інформаційно-ентропійний; нейронні мережі та (кілька критеріїв); формальний (матричний); підхід до зниження ризику; вдосконалення (інтегративний); багаторівневий [23,].

Статистичний підхід — обробляються потенційні атаки, загрози та наслідки. Показник оцінки ефективності — загроза і-го типу, усереднена протягом Ті.

Імовірнісний підхід — визначається ймовірність того, що інформаційна система відмовиться обробляти дані через успішну загрозу. Загальні збитки розраховуються за формулою

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

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

Частотний метод - На основі аналізу статичної інформації визначається значення S, значення V вибирається в діапазоні від 1 до максимально. Показник оцінки ефективності системи - очікувані втрати від і-ї загрози (1.3):

$$R_i = F(S,V), \qquad (1.3)$$

де S — показник частоти виникнення загрози безпеці даних,

V — умовний показник шкоди.

Експертний метод — визначається кількість n параметрів для ідентифікації системи захисту розподіленої інформаційної системи. Наведено суб'єктивні значення коефіцієнтів важливості. Wi , кожної з характеристик Gi призначені експертним шляхом. Розраховується значення параметра SR. Показник оцінки ефективності системи — рівень безпеки даних системи розраховується за формулою (1.4):

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

Інформаційно-ентропійний метод — Аналітичний розрахунок ентропії інформаційної системи здійснюється, в той же час, з використанням концепції згортки функції. У випадку лінійної залежності ефективність системної інтеграції вважається задовільною в інформаційному плані, в іншому випадку вона неефективна. Значення ентропії Шеннона є показником оцінки ефективності (1.5):

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

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

Метод нейронної мережі (багатокритеріальна оцінка): належність до певного рівня безпеки даних визначається в діапазоні [0,1], показники надійності є функцією відповідності: x_i , елемент множини X — вимоги безпеки даних, A — набір значень, що визначають виконання вимог безпеки даних. Оцінка ефективності системи захисту розподіленої інформаційної системи здійснюється на основі чітко визначених показників. Нечіткими індикаторами розширеної системи захисту є такі

лінгвістичні змінні, як «середній рівень захисту», «низький рівень захисту» і «високий рівень захисту».

Метод мінімізації ризиків: реалізовано відповідно до таких заходів: усунення ризиків безпеки даних; індекс ризику; Виконується класифікація ризиків; визначено механізми обробки ризиків безпеки даних; Розраховуються показники ризику; Розраховано показники економічного ефекту управління ризиками безпеки даних. Показником оцінки ефективності є показник економічного впливу управління ризиками захисту даних. 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.

Реалізація матричного методу (моделі формальних бар’єрів) складається з наступних етапів: визначаються параметри; Створюється матриця взаємозв'язків; перетворювати матрицю в двовимірну матрицю; Визначено 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 [11].

Комбінаторний (оптимізаційний) — вирішується задача дискретного програмування типу: максимізувати $\sum_{j=1}^{n} c_j x_j$,

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

Недоліки та переваги методів [13] 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 між елементами 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 задач дослідження

Визначення переліку поточних ризиків інформаційної безпеки, оцінка ефективності системи захисту є невід'ємною частиною життєвого циклу розподіленої інформаційної системи. Специфіка IT-інфраструктури, складність ідентифікації зловмисників, поточні ризики в розподілених інформаційних системах, вибір показників, недоліки методів оцінки ефективності систем захисту, що призводить до недостатньої ефективності захисту розподілених інформаційних систем. Метою магістерської роботи є підвищення якості оцінювання ефективності систем захисту інформації шляхом визначення достатніх і необхідних показників.

Загалом завдання дослідження можна сформулювати так: підвищити якість методів моделювання (визначити) поточні ризики безпеки даних шляхом визначення достатніх і необхідних показників, автоматизувати процеси для уникнення експертних помилок; підвищити якість методик оцінки ефективності системи захисту, визначити найкращі параметри роботи адаптивних нейронних нечітких продукційних систем і застосувати технології data science при обробці великих обсягів даних; розробка рекомендацій щодо оцінки ефективності

розподіленої загороджувальної системи; Оцінити ефективність запропонованих методів.

Математично проблему можна формалізувати так: вибрати найкращі математичні моделі для розв’язування задач, визначити найкращий алгоритм нечіткого виводу; Визначити найкращі параметри моделі, які мінімізують середньоквадратичну похибку порівняно з існуючими методами.

Проблема вирішення проблем полягає в тому, що наразі недостатньо опрацьовуються наступні підзадачі: недоліки існуючих методів моделювання поточних ризиків інформаційної безпеки та, як наслідок, помилкова ідентифікація атак, ризики безпеки даних. У розподілених системах; Недоліки існуючих методів оцінки ефективності системи хеджування є, як наслідок, результатом недостатньо ефективної системи хеджування, що призводить до підвищення ризиків порушення цілісності, конфіденційності, доступності та інших активів.

Аналіз досліджень оцінки ефективності системи захисту Наразі з вибором оціночних показників, складним обчислювальним навантаженням, недостатньою ефективністю з точки зору надійної оцінки...

Існуючі методики оцінки ефективності системи захисту не задовольняють належним чином критерії оцінки ефективності, не враховують адекватних і необхідних показників оцінки ризиків ризиків інформаційної безпеки, оцінок з точки зору ефективності загальної безпеки даних. вимоги, значення фінансових витрат на створення системи захисту, IT-інфраструктури розподілених систем.

Мета дослідження магістрів сформульована в главі. Визначено завдання, які необхідно вирішити для досягнення поставленої мети. Filtering Tasks Effectiveness Assessment підвищить ефективність системи захисту розподілених систем.

2 МЕТОДИКИ ВИЗНАЧЕННЯ АКТУАЛЬНИХ ЗАГРОЗ БЕЗПЕЦІ ІНФОРМАЦІЇ

2.1 Моделювання зловмисника та загроз безпеки конфіденційної інформації

Аналіз потенційних можливостей зловмисника виконується в рамках розробки моделі зловмисника. Виходячи з актуальності порушення інформаційної безпеки, ідентифікуються внутрішні та потенційно зовнішні порушення безпеки даних, що діють у розподілених системах. потенційні зловмисники внутрішньої інформаційної безпеки: люди, які мають дозвіл на доступ до контрольованої зони розподілених систем, але не мають доступу до інформації, що обробляється в системі; Зареєстровані користувачі розподіленої інформаційної системи - мають обмежений доступ до ресурсів системи з робочого місця; зареєстровані користувачі розподіленої інформаційної системи - забезпечення віддаленого доступу до інформації. До потенційних зовнішніх зловмисників на інформаційну безпеку даних відносяться зловмисники інформаційної системи, колишні співробітники розподіленої інформаційної системи.

Для окремих типів потенційних зловмисників описано наступні методи застосування загроз інформаційній безпеці [21]:

1. Загрози витоку даних з технічних каналів можуть реалізовуватися за допомогою: оптико-електронних (оптичних) методів пристроїв відображення, екранів відображення, інформаційно-обчислювальних комплексів, технічних методів відображення інформації з перехоплення випромінюваних чистот при обробці інформації в розподілених інформаційних системах під час обробки інформації спеціальними технічними засобами радіотехнічної розвідки, розташованих на території контрольованого регіону та за його межами.

2. Ризики несанкціонованого доступу до інформації можуть бути реалізовані за допомогою: впливу на технічні процедури під час завантаження

операційної системи; прямий доступ до обладнання або програмного забезпечення після встановлення операційної системи; віддалений доступ до технічних процедур або програмного забезпечення; Віддалений або прямий вплив на об'єкти віртуального середовища системи та інформацію, що зберігається у віртуальному просторі розподіленої системи.

3. Небезпеки зі специфічним впливом на розподілену систему можуть бути реалізовані за допомогою: хімічного впливу; механічний вплив; шумовий вплив; вплив радіації; біологічний вплив; електромагнітний ефект; вплив температури; магнітне поле; електромагнітне випромінювання.

Процедури реалізації При визначенні загроз інформаційній безпеці передбачалося, що загрози можуть бути реалізовані за рахунок доступу до інформації, компонентів розподіленої інформаційної системи, шляхом створення необхідних процедур та умов доступу.

При визначенні можливих способів реалізації загроз інформаційній безпеці враховуються такі умови: ймовірність змови між зловмисниками (як зовнішніми, так і внутрішніми); Загрози інформаційній безпеці можуть бути реалізовані в будь-якій точці і в будь-який час інформаційної системи (на будь-якому хості, вузлі); Для досягнення мети зловмисник вибирає найслабшу ланку інформаційної системи.

Модель потенційного зловмисника розподіленої інформаційної системи, про потенційних зловмисників про безпеку інформації, що обробляється в системі, мотивації та причини їх дій, переслідувані цілі, загальний характер дій у процесі Впливу на дані, що обробляються.

Модель потенційного порушника інформаційної системи відображає теоретичні та практичні можливості потенційного зловмисника, його апріорні знання, місце і час дії. При наявності одноразового або постійного права на контрольовану територію правопорушники поділяються на: осіб, які не мають права входу на контрольовану територію системи; Особи з одноразовими або

постійними правами доступу до контрольованої зони системи. Факторами, які зменшують ймовірність змови злочинців, є створення умов, у яких загрози інформаційній безпеці є відносно менш вигідними у фінансовому плані, ніж потенційні зловмисники на інформаційну безпеку розподілених систем. до розподілених систем; укладення угоди про конфіденційність даних між власником системи та фізичними та юридичними особами, які можуть перешкоджати інформаційній безпеці системи; Створити ситуацію, яка призводить до негативних наслідків для потенційної жертви у разі виникнення загрози інформаційній безпеці: втрата прибутку та ділової репутації, розрив цивільних відносин; Визначити відповідальність користувача розподіленої інформаційної системи у разі порушення вимог безпеки даних у розподіленій інформаційній системі.

Враховуючи характер, призначення обробленої інформації, характеристики, умови роботи та безпеку розподіленої інформаційної системи, наступні категорії можуть становити зовнішні одиничні порушення [18]:

— кримінальні структури;

— розвідувальні служби урядів;

— фірми-конкуренти (конкуренти);

— недобросовісні партнери;

— постачальники програмного забезпечення та технічних процедур (а також інформаційних засобів, складних IT-систем);

— фізичні особи (зовнішні особи): колишні співробітники власника PIC;

— розробники програмного забезпечення (включаючи засоби захисту інформації).

До групи зовнішніх порушників слід віднести «осіб, які є одноосібними сторонніми виконавцями, які змовилися з метою вчинення нападу на об’єкти, що охороняються».

зовнішній порушник може:

— здійснювати атаки на розподілену інформаційну систему з використанням рутинних процедур інформаційної системи та доступу до технічних процедур розподіленої інформаційної системи за межами контрольованої зони;

— здійснювати атаки на розподілені інформаційні системи по каналах зв'язку поза зоною контролю;

— припиняти обробку інформації в розподіленій інформаційній системі через відповідні технічні канали витоку;

— здійснювати прямий доступ до об'єктів розподіленої інформаційної системи, що знаходяться поза зоною управління системою в процесі їх життєвого циклу (підтримка, модернізація, технічне обслуговування, експлуатація, утилізація);

— здійснювати атаки на розподілену інформаційну систему з використанням апаратних закладок, вбудованих у технічний механізм інформаційної системи;

— здійснювати атаки на розподілену інформаційну систему через відповідну систему підтримки об'єкта-інформатора;

— здійснювати атаки на розподілену інформаційну систему у вигляді сервісної інфраструктури та механізмів зв'язку в межах контрольованої зони інформаційної системи.

Згідно з документом «Базова модель ризиків безпеки персональних даних в інформаційних системах під час обробки персональних даних» [1,2] внутрішні потенційні порушники поділяються на вісім категорій залежно від повноважень доступу та способу доступу до інформації. у розподіленій інформаційній системі. В рамках магістерської роботи пропонується використовувати класифікацію інсайдера, враховуючи визначені категорії порушників, умови роботи, характер інформації, з якою працює, тематику доступу до розподіленої інформаційної системи та заходи безпеки. порушників, представлених

наступними дев'ятьма категоріями:

— зареєстровані користувачі РІС з обмеженим доступом до ресурсів з робочого місця;

— зареєстровані користувачі державної розподіленої інформаційної системи, що забезпечують віддалений доступ до інформаційних ресурсів, що обробляються в розподіленій інформаційній системі;

— користувачі, які мають доступ до державної розподіленої інформаційної системи, але не мають інформаційних ресурсів, що обробляються в розподіленій інформаційній системі;

— зареєстровані особи з повноваженнями системного адміністратора розподілених інформаційних систем;

— постачальники (програмісти-розробники) прикладного програмного забезпечення та розробники, що забезпечують підтримку програмного забезпечення на об'єкті охорони;

— особи та розробники, що забезпечують обслуговування, постачання, супровід технічних процедур розподіленої інформаційної системи;

— зареєстровані користувачі розподіленої інформаційної системи за повноваженнями Адміністратора інформаційної безпеки відповідної частини інформаційної системи.

До першої категорії належать користувачі, які мають права доступу до розподіленої інформаційної системи, але не мають доступу до інформації, що обробляється в інформаційній системі. Виконавцями такого роду атак є співробітники, які перевіряють роботу розподіленої інформаційної системи.

До другої категорії належать зареєстровані працівники державної розподіленої інформаційної системи, які мають обмежений доступ до ресурсів інформаційної системи з автоматизованих робочих місць відповідно до закріплених за ними ролей.

До третьої категорії належать користувачі, зареєстровані в розподіленій

інформаційній системі, які отримують віддалений доступ до системи з мобільних автоматизованих робочих станцій і ноутбуків.

Четверта категорія включає користувачів, зареєстрованих у розподіленій інформаційній системі під керівництвом адміністратора інформаційної безпеки.

П'ята категорія — «адміністратор програми» і «Диспетчер системи».

До шостої категорії належать працівники, зареєстровані в розподіленій інформаційній системі під керівництвом адміністратора інформаційної безпеки. Користувачі цієї категорії відповідають за розробку правил доступу в інформаційних системах, зміну паролів, створення ключових елементів і перевірку способів розробки розподілених інформаційних систем.

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

Восьма категорія складається з супроводу постачальників і супроводу технічних процедур постачальників і розробників розподілених інформаційних систем.

Внутрішній порушник може:

— здійснювати атаки на розподілені інформаційні системи через внутрішні комунікації;

— забезпечувати прямий доступ до об'єктів розподіленої інформаційної системи в межах зони управління;

— здійснювати атак звичайними методами на розподілену інформаційну систему;

— здійснювати переривання обробки інформації в розподіленій інформаційній системі через канали технічного витоку;

— здійснювати атаки на розподілену інформаційну систему з використанням апаратних закладок, вбудованих у технічні засоби системи;

— здійснювати атаки з використанням сервісних і комунікаційних механізмів в інфраструктурі розподіленої інформаційної системи;

— здійснювати атаки на розподілені інформаційні системи через системи безпеки.

Також до групи зловмисників інформаційної безпеки слід віднести групу користувачів із зовнішніми та внутрішніми поодинокими зловмисниками, які планують атакувати об’єкти, що захищаються.

Враховуючи визначені категорії порушників, умови праці, характер інформації, що обробляється, надійність інформаційної системи, об’єкти захисту, пропонується використовувати класифікацію внутрішнього порушення відповідно до... Наступних категорій: Дані не обробляються в інформаційній системі, але та ліцензований доступ до системи; зареєстровані користувачі з обмеженим доступом до ресурсів системи з робочого місця;

Зареєстровані користувачі інформаційної системи, які надають віддалений доступ до даних, що обробляються в системі; Зареєстровані користувачі за повноваженнями адміністратора інформаційної безпеки системного підрозділу; зареєстровані користувачі інформаційної системи під керівництвом адміністратора системи; зареєстровані користувачі системи за повноваженнями адміністратора безпеки даних інформаційної системи; постачальники (програмісти-розробники) програмного забезпечення та особи, які забезпечують підтримку прикладних програм на об'єкті захисту люди та розробники, які забезпечують технічне обслуговування, постачання, підтримку розподіленої інформаційної системи.

Типи потенційних зловмисників інформаційної безпеки встановлюються відповідно до відносної спроможності, яка визначає можливості реалізації загрози безпеці даних: порушення низької потужності — мають можливість реалізувати загрозу за допомогою даних із загальнодоступних джерел. інформаційна безпека; Зловмисники середньої потужності — мають

можливість аналізувати прикладне програмне забезпечення, виявляти вразливості в ньому та застосовувати загрози інформаційній безпеці; Порушення великої ємності — мати можливість створювати закладки в програмному забезпеченні IS, використовувати спеціальні методи доступу, проводити спеціальні дослідження та отримувати інформацію та застосовувати загрози інформаційній безпеці. Для кожної категорії порушників для визначення актуальності інформаційної безпеки використовуються наступні критерії: рівень ризику; рівень мотивації. Перелік атак ІБ, які могли бути здійснені в розподіленій ІС, і рівні їх мотивації наведені в таблиці.. 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 забезпе чення ІС	Мінімальний
Конкурен ти (конкуру ючі організац ії)	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 фундамента-льні 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
Розробник ПЗ	Володіє професійними знання в області ІБ	Володіє інформацією про використовувані ОС, ПЗ та системи захисту	Середній
Внутрішній порушник			
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 ІС	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 РІС 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 порушник			
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

На основі аналізу потенційних атак на інформаційну безпеку, проведеного в рамках магістерської роботи, були виявлені потенційні порушення конфіденційних даних, що обробляються в розподілених інформаційних системах.

Залежно від наявних можливостей виявлених потенційних порушень інформаційної безпеки визначається відповідний рівень захисту конфіденційних даних шифруванням, який має забезпечити ефективність використання захисних механізмів для усунення загроз інформаційній безпеці.

2.2 Створення набору даних для визначення загроз безпеці інформації

При розробці списку загроз інформаційній безпеці слід враховувати такі типи загроз: загрози, не пов’язані з атаками; загрози нападу. При обробці інформації в розподілених інформаційних системах можуть застосовуватися такі загрози безпеці даних: загрози несанкціонованого доступу до даних; Загрози, які можуть мати специфічний вплив на розподілену інформаційну систему, загрози витоку інформації через технічні канали.

Загрози витоку можуть бути реалізовані зовнішніми, внутрішніми зловмисниками, а також шляхом розміщення пристроїв, вбудованих у контрольований простір або за його межами. Загроза несанкціонованого доступу стосується дій зловмисників з доступом до інформаційної системи, що реалізують загрози безпосередньо в інформаційній системі, і зловмисників без доступу до розподіленої системи, що реалізують загрози із зовнішніх мереж. міжнародного обміну інформацією та суспільного використання.

Реалізація загроз, що загрожують несанкціонованому доступу до даних, може призвести до таких типів порушень безпеки: порушення цілісності; порушення конфіденційності; зловживання довірою; Порушення доступності.

За результатами проведених досліджень можна зробити висновок, що існуючі методи часто мають суттєві недоліки: відсутність документації, великий обсяг даних, потреба у висококваліфікованих спеціалістах із безпеки інформації;

відсутність автоматизованих засобів визначення актуальних загроз інформаційній безпеці.

У зв'язку з вищесказаним вирішуються наступні задачі:

1. Підготувати набір даних для визначення поточних ризиків інформаційної безпеки на основі відомих баз даних уразливостей і ризиків, розробити статичні моделі загроз.

2. Проаналізувати згенерований набір даних.

3. Для якісної роботи порівняти та вибрати кілька моделей, визначивши найкращу.

4. Перевірити модель.

Мова програмування Data Science Technology Python була використана для створення наборів даних для розробки програмного забезпечення та автоматизованої обробки. Досліджувана розподілена інформаційна система захисту інформації Проблема визначення реальних ризиків полягає в обробці великої кількості даних, необхідних при визначенні реальних ризиків секретної інформації: відомостей із зарубіжних баз даних та знань.

Проведений аналіз даних показує, що інформація має великий обсяг, що призводить до нудних розрахунків у процесі визначення реальних ризиків інформаційної безпеки. Використання експертного підходу для визначення поточних ризиків інформаційної безпеки призводить до помилок, пов’язаних з людським фактором, таких як: зусилля, суперечливість та розбіжність думок, особиста думка експерта. Методичні документи Українського центру компетенцій з інформаційних технологій та кібербезпеки визначають стандарти та процедури виявлення конкретних загроз конфіденційним даним, не враховуючи зусиль та помилок експертів. Відповідно до методичних документів Кваліфікаційного центру інформаційних технологій та кібербезпеки України актуальність загроз для конфіденційних даних визначається на основі їх значущості для розподіленої інформаційної системи

зламу, потенційних уразливостей і ризиків в IT-інфраструктурі інформаційної системи та потенційних наслідків для реалізацій інформаційної безпеки. загроза. Такий набір даних створено з інформаційної бази даних загроз Центру компетенції інформаційних технологій та кібербезпеки України, моделей загроз інформаційній безпеці розподіленої інформаційної системи, технічних рішень досліджуваної системи.

За результатами генерації та перетворення набору даних необхідно визначити модель реалізації методу, за рахунок адаптації та визначення найкращих параметрів системи у поєднанні з відомими методами для підвищення ефективності методу.

2.2 Модель визначення загроз безпеці інформації

Для виявлення актуальних загроз інформаційній безпеці була обрана нейронна система ANFIS, заснована на системі Такагі-Сугено-Канга. Алгоритм роботи полягає в застосуванні нечіткої моделі на основі правил типу. (2.1):

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

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)	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

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

$$\mu_{A_{ij}}(x_j) = \exp\left(-\frac{1}{2}\left(\frac{x_j - a_{ij}}{b_{ij}}\right)^2\right),$$

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, він включає п'ять шарів:

Виконує оновлення різних вхідних змінних

2. Обчислює значення степенів заданої функції належності функціями Гауса з параметрами

3. Створює значення функції, які множаться на результати розрахунків за елементами другого шару.

4. Перший елемент четвертого шару необхідний для активації висновків правил. Другий елемент четвертого шару виконує додаткові обчислення.

5. Цей рівень складається з нормалізуючого елемента, який розсіює вихідні дані нейронної мережі.

Нейронна мережа ANFIS складається з параметричних рівнів (1 і 3). Параметри, які коригуються в процесі навчання нейронної мережі: на першому рівні — нелінійні параметри aij,bij функції належності вектора; У третьому шарі -

параметри ci0n siij лінійних функцій з висновків бази правил.

На наступному кроці обчислюються параметри ci0 і cij лінійної функції.

Умови фіксованих значень параметрів aij ,bij . Отримано параметри ci0 та изий

Шляхом розв'язування системи лінійних рівнянь. Вихідна змінна з виразу (2.2) подаємо в наступному виді (2.3):

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

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

Алгоритм навчання нейроної продукційної адаптивної система ANFIS із застосуванням алгоритму TSKпобудований так, що при k навчальних прикладах, де заміна значень вихідних змінних відбувається заміною значень еталонних змінних ,отримується система з k лінійних рівнянь (2.4):

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

Вирішення даної системи рівнянь можна провести за один крок за

допомогою псевдоінверсії матриці *W*:

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 та виконуємо уточнення параметрів (2.5):

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

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

(2.5)

Визначення реальних ризиків для інформаційної безпеки вимагає визначення доцільності впровадження з переліку потенційних ризиків.

Для кожної загрози інформаційній безпеці експертно визначаємо коефіцієнти Y2: 0 — несподівана загроза; 2 — низька ймовірність загрози; 5 — помірна ймовірність ризику; 10 — висока ймовірність загрози.

За допомогою певних коефіцієнтів кількісно визначається ймовірність реалізації загроз інформаційній безпеці Y; Y1 — рівень початкової безпеки розподіленої інформаційної системи, який визначається згідно з процедурними даними Центру компетенції інформаційних технологій та кібербезпеки України.Структура нечіткої нейронної мережі ANFIS представлена рис. 2.1.

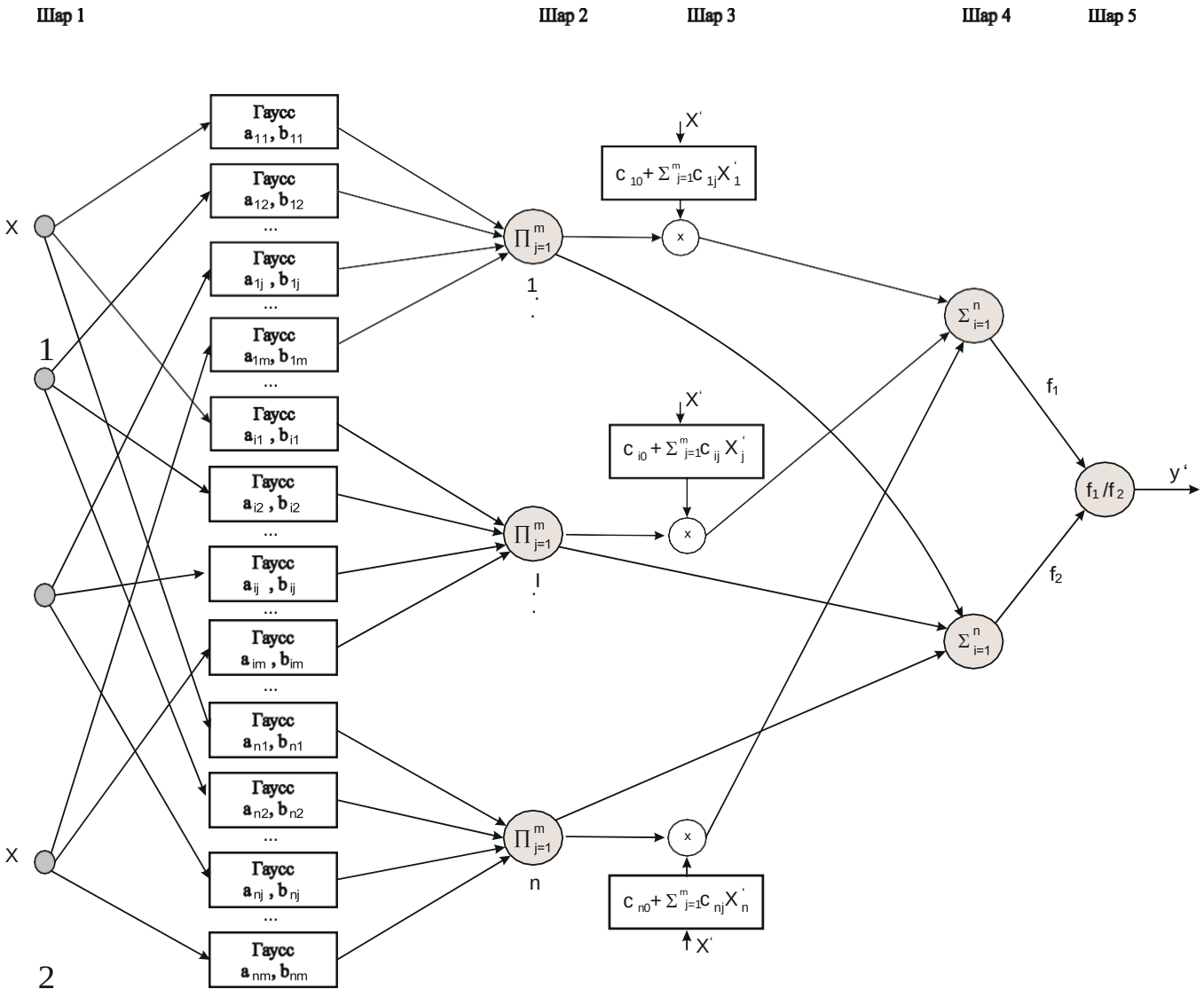


Рисунок 2.1 — Нейронна мережа ANFIS із застосуванням алгоритму TSK

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):

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

,

де 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

Запропоновано модель визначення поточних ризиків інформаційної безпеки, яка базується на алгоритмі нечіткого логічного висновку та теорії нечітких нейронних систем, на відміну від відомих, використовує певні достатні та дискримінаційні показники, що виключають експертні помилки. Виявлення реальних загроз інформаційній безпеці підвищується на 5%, знижуючи витрати на закупівлю засобів захисту інформації з 15 до 30%. Він розглядає наступні фактори: IT-інфраструктуру розподіленої інформаційної системи, можливості зловмисників і рівень мотивації в розподіленій інформаційній системі, список доступних. Запропонований підхід відрізняється від існуючих: незалученням висококваліфікованих фахівців у сфері інформаційної безпеки; Процес автоматичний, з низькою обчислювальною складністю; відсутність недоліків в експертних оцінках; Це дозволяє визначити перелік поточних ризиків інформаційної безпеки для різних класів і типів інформаційних систем.

3 МЕТОД ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

3.1 Показники оцінки ефективності та вимоги до систем захищеності інформації

Перелік ризиків безпеки конфіденційних даних створено на моделях ризиків інформаційної безпеки типових розподілених інформаційних систем та згідно з методичними документами Центру компетенцій інформаційних технологій та кібербезпеки України. Було вирішено завдання трансформації та очищення великих обсягів даних та створено набори даних за допомогою технологій data science для виявлення поточних ризиків інформаційної безпеки конфіденційних даних. На основі використання нечітких адаптивних виробничих нейронних мереж запропоновано модель ідентифікації актуальних загроз інформаційній безпеці даних.

За даними Центру компетенцій інформаційних технологій та кібербезпеки України, при встановленні вимог до захисту інформації в інформаційних системах сформульовано вимоги до захисту конфіденційної інформації для різних класів і типів інформаційних систем. Під час розробки системи захисту розподілені інформаційні системи враховували такі фактори, як використання сертифікованих пристроїв захисту відповідно до вимог безпеки інформації.

Для проведення адекватної оцінки ефективності системи захисту необхідно визначити адекватні та необхідні показники. Оцінка ефективності системи захисту даних досягається шляхом створення відповідної системи для максимального усунення поточних загроз інформаційній безпеці шляхом виконання вимог щодо захисту конфіденційних даних, що висуваються до розподіленої інформаційної системи на основі вимог у контексті. інформаційної безпеки, а також дозволяє максимально мінімізувати фінансові витрати на розробку системи захисту. Таким чином, наведено такі показники оцінки: перелік поточних ризиків інформаційної безпеки; IT-інфраструктура розподіленої інформаційної системи з урахуванням їх

специфіки; Специфікації вимог до інформаційної безпеки з урахуванням класифікації конкретної інформаційної системи; Значення засобів захисту інформації; Перелік механізмів захисту інформації за результатами розробки системи захисту розподіленої інформаційної системи.

На підставі даних результатів аналізу розподілених інформаційних систем, визначення ефективності системи захисту у сфері інформаційної безпеки можна зробити наступний висновок: Перелічені показники є достатніми та необхідними для достовірного та комплексного. Оцінка ефективності системи захисту інформації.

За результатами інформаційного обстеження розгорнутих систем, вхідних даних у сфері забезпечення інформаційної безпеки, проведене дослідження пропонує визначити вимоги інформаційної безпеки в цілому. Вимоги до захисту конфіденційних даних досліджуваної розподіленої системи наведені в таблі. 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	+	+

У табл. 3.1 наведено перелік вимог щодо захисту інформації, який становить четвертий рівень захисту персональних даних і третій рівень захисту державної інформаційної системи. Для кожного сегмента та типу вони формулюють визначення категорії розподіленої інформаційної системи, рівень безпеки та перелік вимог щодо захисту конфіденційних даних.

На основі сформульованого переліку вимог до інформаційної безпеки, переліку засобів захисту інформації та переліку поточних даних про ризики безпеки розроблено набір даних для оцінки ефективності системи. За допомогою технологій data science виконуються наступні кроки: перетворення та очищення підготовленого набору даних; порівняння моделей за якістю роботи; виділення найважливіших ознак, створення нових, більш репрезентативних; перевірка моделі на дослідному зразку; визначення параметрів у найкращій моделі; підбивати підсумки виконання завдання; інтерпретація результатів.

Враховуючи, що набір даних містить надлишкову інформацію, що збільшує задіяні обчислювальні ресурси та ускладнює процес обробки отриманих даних, тому в остаточному варіанті оцінити ефективність методу для... Система захисту інформації, перший крок Він проводив фільтрацію даних.

Лістинг 3.1 показує набір даних перетворення фрагментів;

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)
```

У процесі виконання магістерської роботи визначаються ключові елементи;

1. Перелік поточних ризиків інформаційної безпеки з симптомами нейтральності/нейтралітету.

2. Перелік вимог безпеки даних з ознаками відповідності: в цілому відповідає, відповідає, не відповідає, частково відповідає.

3. Назви засобів захисту інформації, їх версії, патчі (версії оновлення).

4. Вартість обладнання від виробника (специфікація постачальника).

Фільтрація надлишкової інформації з набору даних здійснювалася згідно з визначенням ключових компонентів системи.

Інформаційні символи, які спочатку є числовими, інтерпретуються як тип об'єкта. Таким чином відповідні символи були перетворені в правильний тип - float. Наступним кроком є заміна значення «Недоступно» у кадрі даних на «не число». Це дозволяє нам змінити числовий тип символів на плаваючий, нейтралізуючи викиди та пропуски у кадрі даних.

Наступним кроком є проведення попереднього аналізу отриманих даних (EDA — Exploratory Data Analysis), на основі попереднього аналізу ми визначаємо відмінності, закономірності та кореляції між ознаками. Отже, необхідно визначити значення атрибутів і атрибутів, які мають істотний вплив на цільову поведінку отриманих даних, оцінюємо вплив значень категоріальних ознак на цільовий — density plot.

Для кількісної оцінки симптомів ступеня їх впливу в магістерській роботі використовується коефіцієнт кореляції Пірсона – міра позитивності та

ступеня лінійного зв’язку між двома змінними. Значення коефіцієнта +1 означає ідеальну пропорційність між відповідними значеннями коефіцієнтів і, -1 так само, але з негативним коефіцієнтом.

Значення кореляції обчислюється таким чином: correlationsdata = data.corr()['score'].sort_values().

Вибір атрибутів інформації – вибір найважливіших атрибутів. Атрибути даних видаляються з кадру даних, щоб модель зіставляла більше атрибутів і ресурсів з основними атрибутами. Таким чином, набір даних фільтрується для релевантної інформації, у якій залишаються лише ті, що найбільш релевантні для даного завдання.

Створення нових функцій — це процес створення нових функцій на основі наявних даних. Потім визначаються колінеарні властивості.

Після попереднього аналізу, фільтрації даних залишаться лише найважливіші функції. Наступним кроком перед початком навчання моделі ANFIS є пошук можливого показника, щоб визначити, чи є позитивний результат від використання задіяного алгоритму.

Перед обчисленням вищезазначеного критерію необхідно розділити вибірку на тестову та досліджувану:

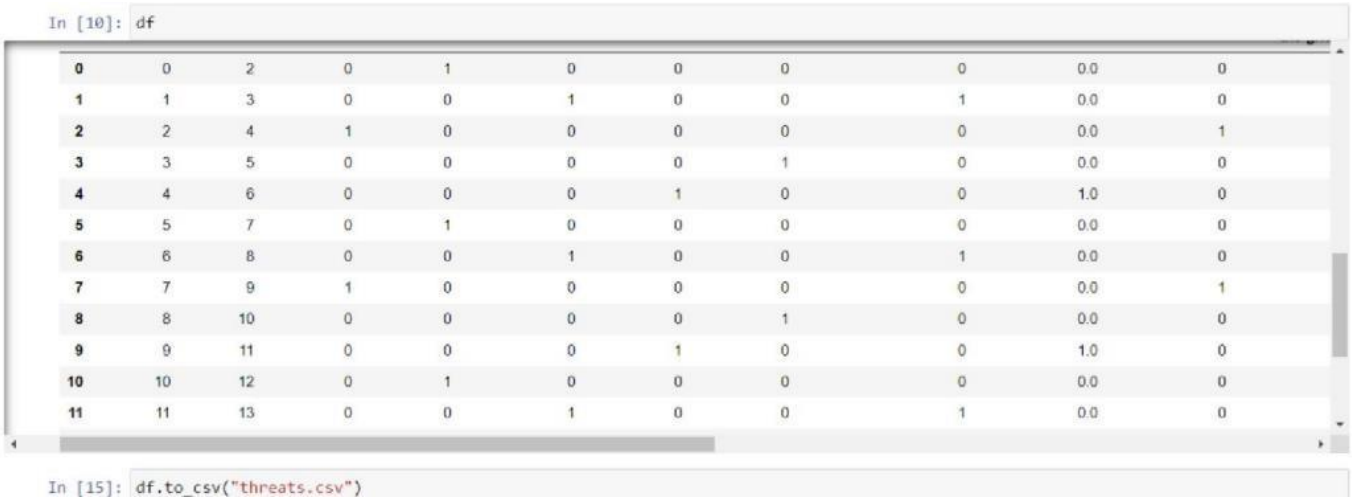
1. Тестовий зразок використовується для перевірки отриманої моделі ANFIS. Модель ANFIS не використовує цільовий атрибут в обробці даних і в той же час повинна використовувати значення інших атрибутів для оцінки його значення. Отримані прогнози порівнюються з фактичними відповідями.

2. Навчальна вибірка — набір отриманих даних, наданих разом із вхідними відповідями моделі ANFIS під час процесу навчання, щоб навчити модель виявляти кореляцію між згенерованими ознаками та правильною відповіддю.

Фрагменти кадру даних після перетворення представлені на рис. 3.1.

Встановлений набір даних, що містить перелік вимог до інформаційної

безпеки, перелік засобів захисту, поточні ризики інформаційної безпеки в розподіленій системі, було відформатовано та модифіковано, щоб дозволити збір лише достатніх і необхідних даних для оцінки ефективності система захисту, що зменшує кількість помилок експертних оцінок, 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 оцінювання ефективності системи захисту інформації

В даний час існує велика кількість нейро-нечітких гібридних моделей,

Вони відрізняються місткістю та архітектурою. У магістерському дослідженні моделі були проаналізовані, і з бази результатів визначено основні характеристики: використання різних методів для вивчення моделі; можливість автоматичного формування набору правил; зберігання даних у процесі вивчення нових правил або параметричної оптимізації; Зміни в структурі моделі змішаних нейро-нечітких моделей наведені в таблиці. 3.2.

На основі аналізу моделі дослідження зроблено висновки щодо використання моделей рівня розв’язаних типів задач. Результати аналізу наведені

в таблиці. 3.3.

З результатів аналізу в табл. 3.3, можна зробити висновок, що використання ANFIS рекомендовано для вирішення задачі оцінки ефективності системи захисту.

Таблиця 3.2 — Область застосування гібридних нейро-нечітких моделей

№ п/п	Модель	Область застосування
1	ANFIS	— структура правової бази повинна бути відома заздалегідь; — параметри налаштовуються на першому і останньому прихованому шарі; — навчання в два етапи: фіксуються параметри першого рівня, використовується оцінка параметрів другого рівня; — параметри другого шару фіксовані, параметри першого шару оцінюються за алгоритмом RMSE (зворотне поширення). — 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

Щоб розробити метод оцінки ефективності системи захисту даних шифрування, мережева модель ANFIS була проаналізована за допомогою алгоритмів нечіткого висновку Mamdani, Takagi-Sugeno-Kang, Wang-Mendel і Takagi-Kang. Зокрема, мережі ANFIS призначені для вирішення задач оцінювання. Вихідні дані системи відповідають набору нечітких правил «якщо-тоді», які мають здатність до навчання прогнозувати нелінійні функції.

Алгоритм мережі ANFIS з алгоритмом TSK (Takaga-Sugeno-Kang fuzzy derivation) полягає в запропонованому методі оцінки ефективності системи захисту даних при застосуванні нечіткої моделі на основі правил. (3.2):

$$
\begin{aligned}
&R_1 : AI.1(C)\,AND3IБ.01(H)\,ANDCOST(MIN)\,THENEVALSZI(Д)\\
&R_2 : AI.1(C)\,AND3IБ.01(H)\,ANDCOST(MAX)\,THENEVALSZI(Д)\\
&R_3 : AI.1(C)\,AND3IБ.01(HH)\,ANDCOST(MIN)\,THENEVALSZI(НД)\\
&R_4 : AI.1(C)\,AND3IБ.01(HH)\,ANDCOST(MAX)\,THENEVALSZI(НД)\\
&R_5 : AI.1(ЦС)\,AND3IБ.01(H)\,ANDCOST(MIN)\,THENEVALSZI(Д)\\
&R_6 : AI.1(ЦС)\,AND3IБ.01(H)\,ANDCOST(MAX)\,THENEVALSZI(Д)\\
&R_7 : AI.1(ЦС)\,AND3IБ.01(HH)\,ANDCOST(MIN)\,THENEVALSZI(НД)\\
&R_8 : AI.1(ЦС)\,AND3IБ.01(HH)\,ANDCOST(MAX)\,THENEVALSZI(НД)\\
&R_9 : AI.1(ЧС)\,AND3IБ.01(H)\,ANDCOST(MIN)\,THENEVALSZI(Д)\\
&\qquad\qquad\ldots\\
&R_n : КД.2(ЦС)\,AND3IБ.03(HH)\,ANDCOST(MIN)\,THENEVALSZI(НД)
\end{aligned}
\qquad (3.2)
$$

На основі вимог і показників захисту даних, актуальних загроз інформаційній безпеці та IT-інфраструктурі розподілених систем створено законодавчу базу, фрагменти якої наведено в таблиці. 3.4.

Таблиця 3.4 — Фрагмент бази правил оцінки ефективності системи захисту

IF (ЯКЩО)			THEN (ТО)
Вимоги до захи-сту інформації	Загроза інформа-ційній 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

У таблиці 3.4 наведено набори слів лінгвістичних змінних: S — реагує, CS — частково реагує, CS — повністю реагує, N — загроза нейтральна, NN - загроза не нейтралізована, min — значення системи захисту мінімальне, max — значення системи захисту максимальне. Рівень кваліфікації D — досягнуто, ND — не досягнуто.

Основні правила реалізації процедури оцінки ефективності системи захисту шифрованих даних побудовані таким чином. (3.2):

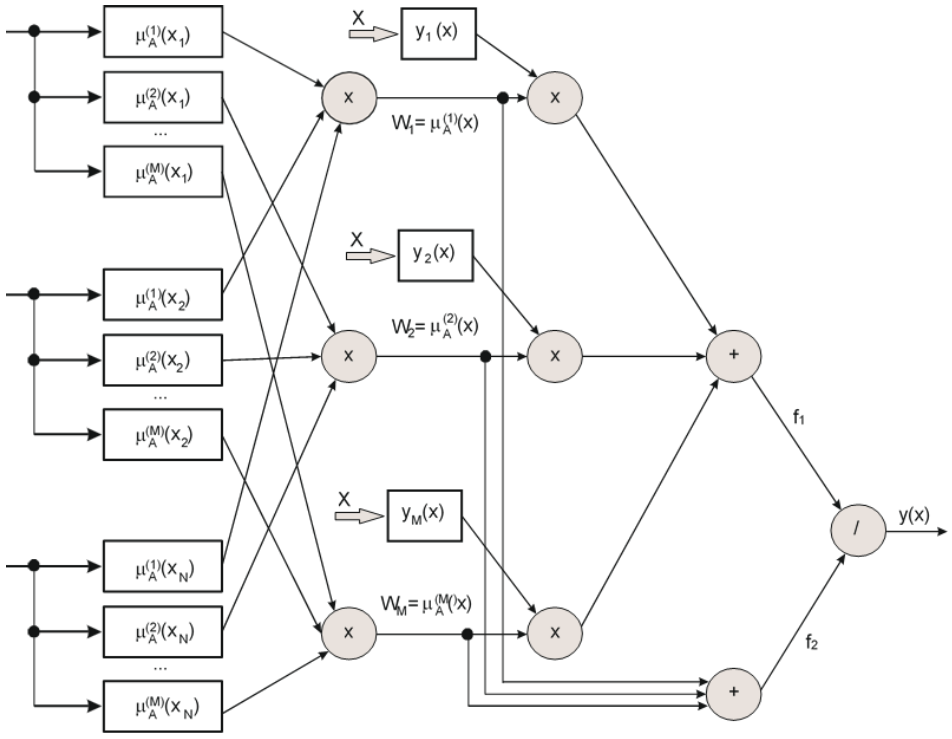


Рисунок 3.2 — Структура нечіткої нейронної продукційної мережі ANFIS із TSK

Мережа ANFIS базується на положеннях, розглянутих у другому розділі запропонованої методики оцінки ефективності системи захисту шифрування. За результатами отриманих нелінійних параметрів та їх уточнення запускається процес адаптації нейрона до ітерації результатів, таким чином алгоритм є гібридним. Унікальність алгоритму полягає в розподілі рівнів навчання. Такий алгоритм нечіткого висновку є найефективнішим, що в магістерській роботі призвело до кращих результатів магістерського дослідження. Структура нечіткої нейронної мережі ANFIS з використанням алгоритму нечіткого висновку Такагі-Сугено-Канга представлена на рисунку 3.2. Завдяки змінним параметрам нейронної мережі в майстер-дослідженні вдалося отримати найменшу середньоквадратичну помилку (RMSE), всупереч відомим методам оцінки ефективності систем захисту інформації.

3.3 Оцінювання ефективності методу захисту конфіденційної інформації

Для визначення ефективності запропонованого підходу до оцінки ефективності систем захисту даних необхідно розглянути наступні аспекти логічного висновку продуктивної нечіткої системи. Нечітка дедуктивна система — це система, в якій логічний висновок певним чином відображає вхідні та вихідні дані за допомогою трьох основних етапів: фазифікація; логічний висновок; дефазифікація

Розглядаються лише постійні функції належності, які, відповідно, довільно вибираються для оцінки ефективності системи захисту даних, структура правил якої визначається експертною інтерпретацією властивостей змінних, що використовуються в моделі. . У певних ситуаціях моделювання безпеки, враховуючи набір даних, неможливо розрізнити, як мають виглядати функції членства. Під час підгонки та аналізу набору даних неможливо визначити відповідні функції належності для оцінки продуктивності системи. Нейроадаптивні методи генеративного навчання надають методи нечіткого

адаптивного моделювання для інформативного аналізу наборів даних. Метод обчислює відповідні параметри функції належності, які дозволяють системі виробництва нечітких виводів відстежувати дані введення-виведення. Адаптивна мережева структура, подібна до нейронної вихідної мережі, може бути використана для інтерпретації введення-виведення, що, у свою чергу, дозволяє відображати вхідні дані з набору даних за допомогою функцій належності та пов'язаних параметрів, а потім робити висновок про належність на основі зв'язків. Функції Параметри, пов'язані з функціями належності, налаштовуються під час навчання системи. Підгонка та розрахунок параметрів спрощується завдяки використанню вектора градієнта. Вектор градієнта визначає, наскільки добре виробнича система нечіткого висновку моделює вихідні та вхідні дані з набору даних вимірювання. Після отримання вектора градієнта застосовується додаткова процедура оптимізації для коригування параметрів функції належності. Цей метод призначений для мінімізації значення середньоквадратичної помилки. RMSE визначається сумою квадратів різниці між бажаним і фактичним результатами.

Таким чином, стає очевидною необхідність використання мережі ANFIS та її ефективності для оцінки системи захисту інформації.

Наступним етапом розрахунку ефективності методу оцінки системи захисту інформації є визначення алгоритму нечіткого логічного висновку. На основі проведених експериментів і аналітичних досліджень, результати представлені в третьому розділі мережі ANFIS з TSK (Takagi-Sugeno-Kanga) алгоритмом нечіткого виробничого висновку для задач... Оцінити ефективність системи захисту інформації.

Про якість запропонованого методу оцінки ефективності системи порівняно з існуючими методами свідчать наступні показники: фінансові витрати дозволяють знизити вартість виготовленої системи захисту до 25%, ефективність системи захисту досягає 97%.

Завдання, поставлене в магістерській роботі щодо вдосконалення оцінки якості ефективності захисної інформаційної системи, може бути вирішено за допомогою методів класифікації з використанням різних методів реалізації та математичних засобів, однак від цього залежить ефективність використовуваних методик. Вирішується конкретна проблема. Проведено порівняльний аналіз методів вирішення задачі, наведених у магістерській роботі, порівняльний аналіз якого наведено в таблиці. 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*-найближ чих сусідів (*KNN*)	Простота реалізації. Опрацьована теоретична база. Адаптація під необхідну задачу.	Недостатня продуктивні-сть у реальних задачах. Труднощі в наборі ваг.
Метод опорних векторів	Еквівалентна двошарова нейронна мережа- простота реалізації	Неможливість калібрува-ння попадання у клас
Метод дерев рішень	Висока продуктивність навчання та прогнозування. Дозволяє працюва-ти з великим об’єом інформації	Проблема отримання оптимального дерева рішень

У магістерській роботі проведено експериментально-порівняльний аналіз роботи методів та запропонованого способу, наведених у таблиці. 3.6. Для визначення ефективності розподіленої захисної інформаційної системи (точність класифікації) доступність/недоступність при проведенні експериментів використовувалася як порівняльна ознака. Результати досліджуваних методів оцінювалися експертом у кожному з експериментів. Результати порівняльного аналізу наведені в таблиці. 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.

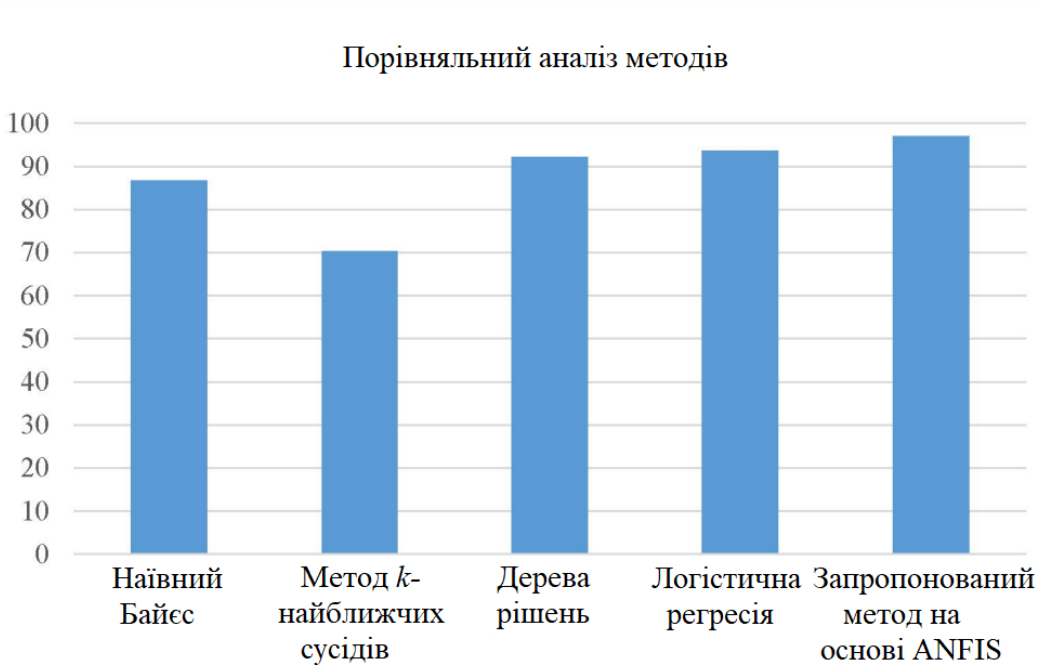


Рисунок 3.3 — Графік порівняльного аналізу методів

Таким чином, для заданого стану завдання (генерований пост-перетворення, якісно отриманий набір даних, нові, більш репрезентативні функції та вибір найбільш корисних) і визначені в магістерській роботі показники оцінки ефективності системи захисту, запропонований метод є кращим. порівняно з відомими методами. Аналіз дослідження наведено в таблиці. 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 — набори даних (перевірки, навчання)Графіки порівняння RMSE відомих та запропонованого методу на заданому інтервалі представлені на рис. 3.4.

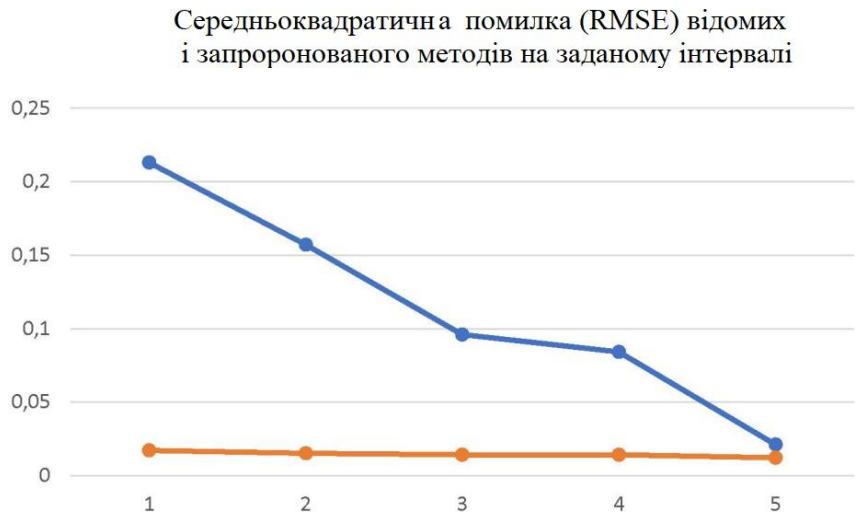


Рисунок 3.4 — Графік порівняння RMSE на заданому інтервалі

Середня квадратична похибка RMSE досягає значення в діапазоні 0,012-0,017, локального мінімуму в заданому інтервалі, що дозволяє перевірити виконання завдання, поставленого в майстер-дослідженні.

4 РЕАЛІЗАЦІЯ МЕТОДУ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ ІНФОРМАЦІЇ ІНФОРМАЦІЙНИХ СИСТЕМ

4.1 Оцінювання відповідності захисту до вимог безпеки

Для проведення дослідження розподіленої інформаційної системи, була обрана система, яка є урядовою системою третього рівня захищеності безпеки інформаційної системи та четвертого рівня захисту персональних даних. Для оцінки ефективності системи захисту необхідно виконати наступні кроки: перевірити IT-інфраструктуру (технологію обробки інформації) інформаційної системи; визначити поточні ризики інформаційної безпеки; встановлення переліку вимог щодо захисту конфіденційних даних; Підготувати набір даних для оцінки ефективності системи захисту ІБ, включаючи: перелік поточних ризиків інформаційної безпеки, IT-інфраструктуру інформаційної системи, перелік використання засобів захисту інформації та їх вартість, перелік вимог до захисту інформації; Експертні оцінки відповідності системи вимогам захисту інформації; оцінити ефективність системи захисту на основі запропонованої методики оцінки ефективності системи захисту; коригування проектних рішень системи захисту.

Форми оцінки відповідності систем захисту вимогам безпеки інформації регулюються Законом України «Про технічні регламенти та оцінку відповідності» (від 15.01.2015 № 124-VIII). Кодекс регулює відносини, що виникають під час: прийняття, розроблення, впровадження, виконання обов'язкових вимог до виробничих процесів, виготовлення, зберігання, експлуатації, транспортування, утилізації та реалізації; Для виробничих процесів, продуктів, операцій, реалізація, утилізація, зберігання, транспортування, виконання, надання послуг; перегляд вимог відповідності; Він визначає обов'язки та права учасників у сфері технічного регулювання відносин.

Основні визначення закону включають: оцінка відповідності вимогам - непряме, пряме визначення відповідності вимогам пункту; Перевірка

відповідності – документальне підтвердження відповідності товарів, продукції, процесів вимогам стандартів, технічних регламентів, умов договору.

Оцінка ефективності та оцінка відповідності ІБ систем захисту інформації є обов’язковою для державних інформаційних систем, систем обробки персональних даних, критичної інформаційної інфраструктури та автоматизованих систем управління технологічними процесами.

Атестація об'єктів інформаційного забезпечення використовується для оцінки відповідності вимогам щодо захисту інформаційних об'єктів, перевірки відповідності об'єктів та безпеки інформації. Об'єкт інформаційного забезпечення (відповідно до вимог інформаційної безпеки) - автоматизовані системи, системи зв'язку, відображення та розміщення різного призначення та стандарту разом із приміщеннями, де вони встановлені, що охороняються для передачі та обробки інформації. обладнання для розмноження та виготовлення конфіденційних документів; автоматизовані системи.

Атестація є обов'язковою для інформаційних систем, які обробляють відомості, що становлять державну таємницю, і державних інформаційних систем, а в інших випадках сертифікація інформаційної системи є добровільною. Форми оцінки відповідності інформаційної системи існують у формах приймання систем захисту інформаційної системи, у формі декларації про відповідність законодавству України «на основі технічних регламентів та оцінки відповідності». Як правило, такі форми оцінки не повністю відображають справжню оцінку системи захисту інформаційних систем через недоліки.

Експертний підхід та суб'єктивні погляди членів комісії пропонує процедурні рекомендації щодо оцінки ефективності системи захисту розподілених інформаційних систем надано та не торкаються пунктів інформаційного забезпечення у випадках сертифікації. Оцінка ефективності. Ефективність системи захисту інформації досягається виконанням вимог щодо захисту інформації, які пред’являються до інформаційної системи відповідно до

визначених критеріїв, і розробкою системи захисту, здатної максимально усунути існуючі ризики інформаційної безпеки. Забезпечення інформаційної безпеки регуляторами у сфері інформації, водночас, дозволяє максимально мінімізувати фінансові витрати на розробку систем захисту інформації.

4.2 Алгоритм оцінювання ефективності систем захисту

Алгоритм оцінки ефективності розподілених систем захисту ІКТ складається з наступних кроків;

1. Підготовка набору даних для оцінки ефективності системи захисту розподіленої інформаційної системи, який містить інформацію про IT-інфраструктуру розподіленої інформаційної системи; перелік актуальних загроз інформаційній безпеці в розподіленій інформаційній системі; детальні вимоги щодо безпеки інформації; перелік засобів захисту інформації, які використовуються в розподіленій інформаційній системі; Вартість створення загороджувальної системи (вартість загороджувального обладнання від виробників).

2. Проаналізуйте, трансформуйте та відформатуйте набір даних.

3. Встановити базові правила для оцінки ефективності системи захисту розподілених інформаційних систем.

4. Провести оцінку ефективності систем захисту розподілених інформаційних систем.

5. Завершіть результати оцінки ефективності систем захисту розподілених інформаційних систем. За потреби внесіть корективи в дизайнерські рішення.

Алгоритм оцінки ефективності та життєвого циклу розробки загороджувальної системи представлено на рисунку 1. 4.1 та РІС. 4.2 відповідно.

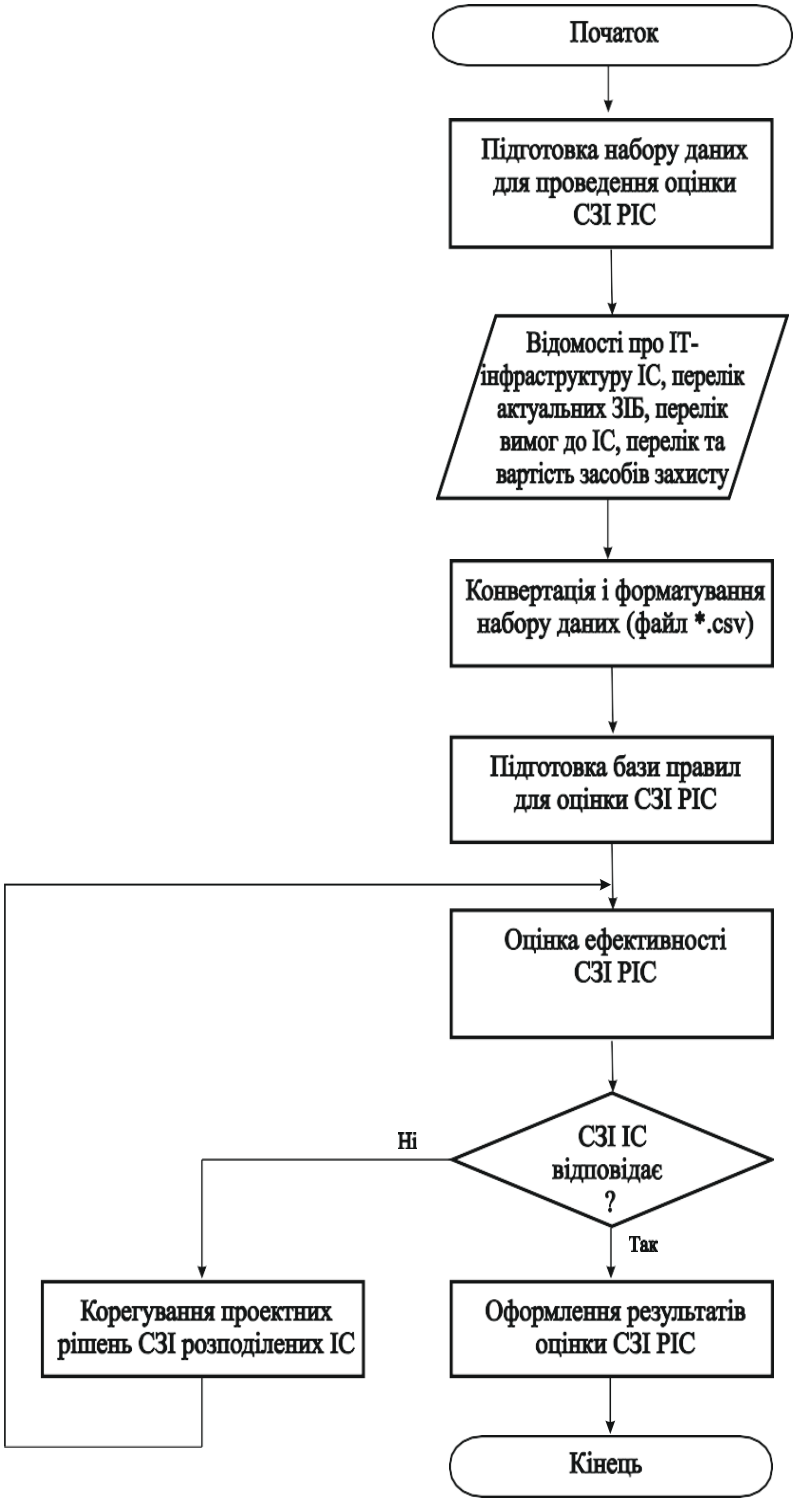


Рисунок 4.1 — Алгоритм оцінки ефективності системи захисту розподіленої інформаційної системи

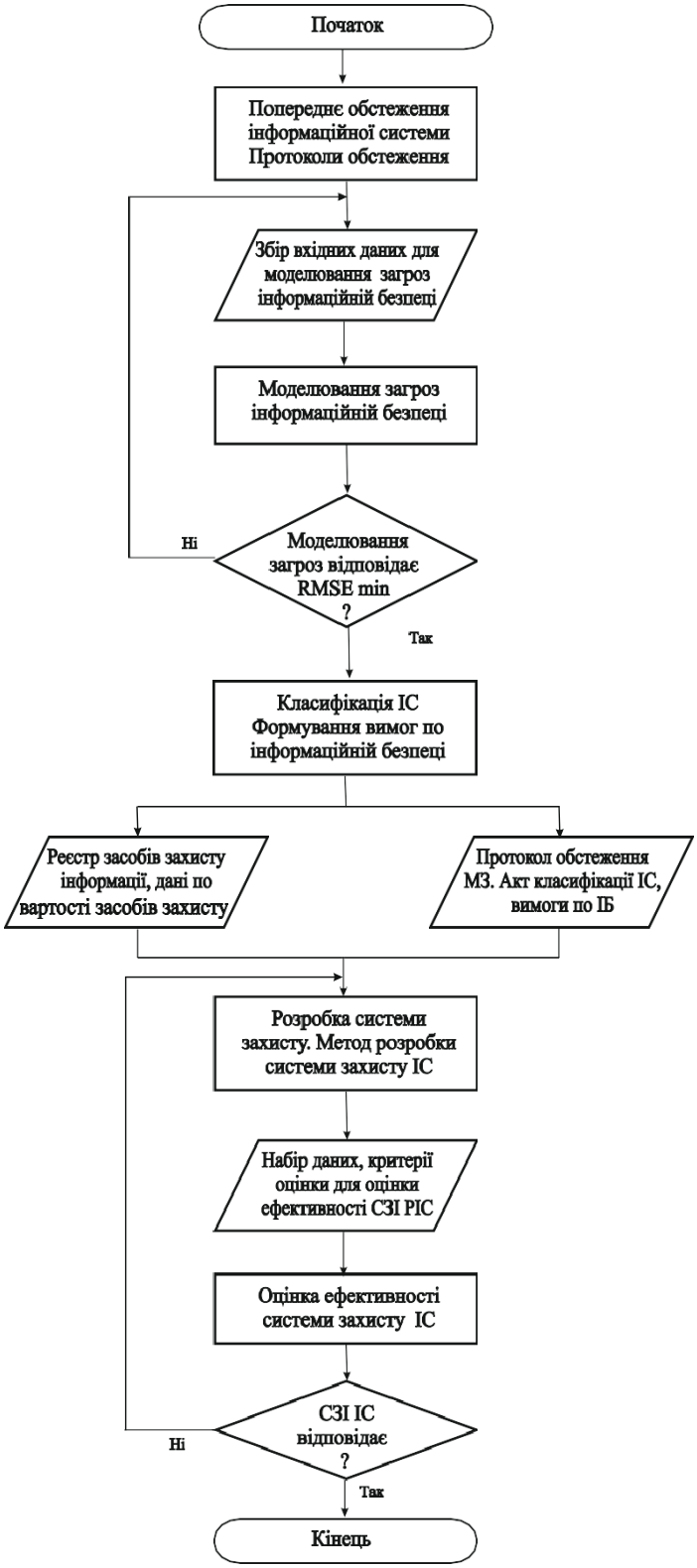


Рисунок 4.2 — Алгоритм життєвого циклу розробки системи захисту розподіленої інформаційної системи

Для оцінки ефективності системи захисту інформації необхідно виконати наступні дії відповідно до методичних рекомендацій:

1. 1. Проведіть дослідження розподіленої інформаційної системи, створіть протокол на основі результатів тесту, який включає опис IT-інфраструктури системи та відомих систем захисту інформації.

2. 2. Визначити поточні ризики інформаційної безпеки відповідно до нормативно-наглядових документів. Категорія Визначити визначення розподіленої інформаційної системи, клас, тип, рівень безпеки. Поточні ризики інформаційної безпеки.

3. 3. Створити список вимог на основі списку поточних ризиків інформаційної безпеки, класифікацій та захисту інформації.

4. 4. Створіть набір даних: IT-інфраструктура розподіленої інформаційної системи, перелік поточних ризиків інформаційної безпеки в інформаційній системі, перелік вимог до захисту інформації, перелік використання засобів захисту інформації в… системах захисту та їх вартість.

5. 5. Провести експертизу на відповідність розгорнутої системи вимогам захисту інформації.

6. Оцінити ефективність системи захисту розподіленої інформаційної системи на основі розробленої методики оцінки ефективності системи захисту.

7. У разі необхідності внести корективи в проект рішень системи захисту інформації за результатами оцінки ефективності системи захисту розподіленої інформаційної системи.

Структурна схема оцінки ефективності системи захисту інформації розподіленої інформаційної системи наведена на рисунку 1. 4.3.

Процес оцінки ефективності системи захисту складається з п'яти підсистем;

1. Підсистема опитування розподіленої інформаційної системи.

2. Підсистема моделювання загроз інформаційній безпеці.

3. Вимоги до створення підсистеми системи захисту інформації.

4. Підсистема оцінки ефективності системи захисту розподіленої інформаційної системи.

5. Проектні рішення налагодження підсистеми розвитку системи захисту розподіленої інформаційної системи.

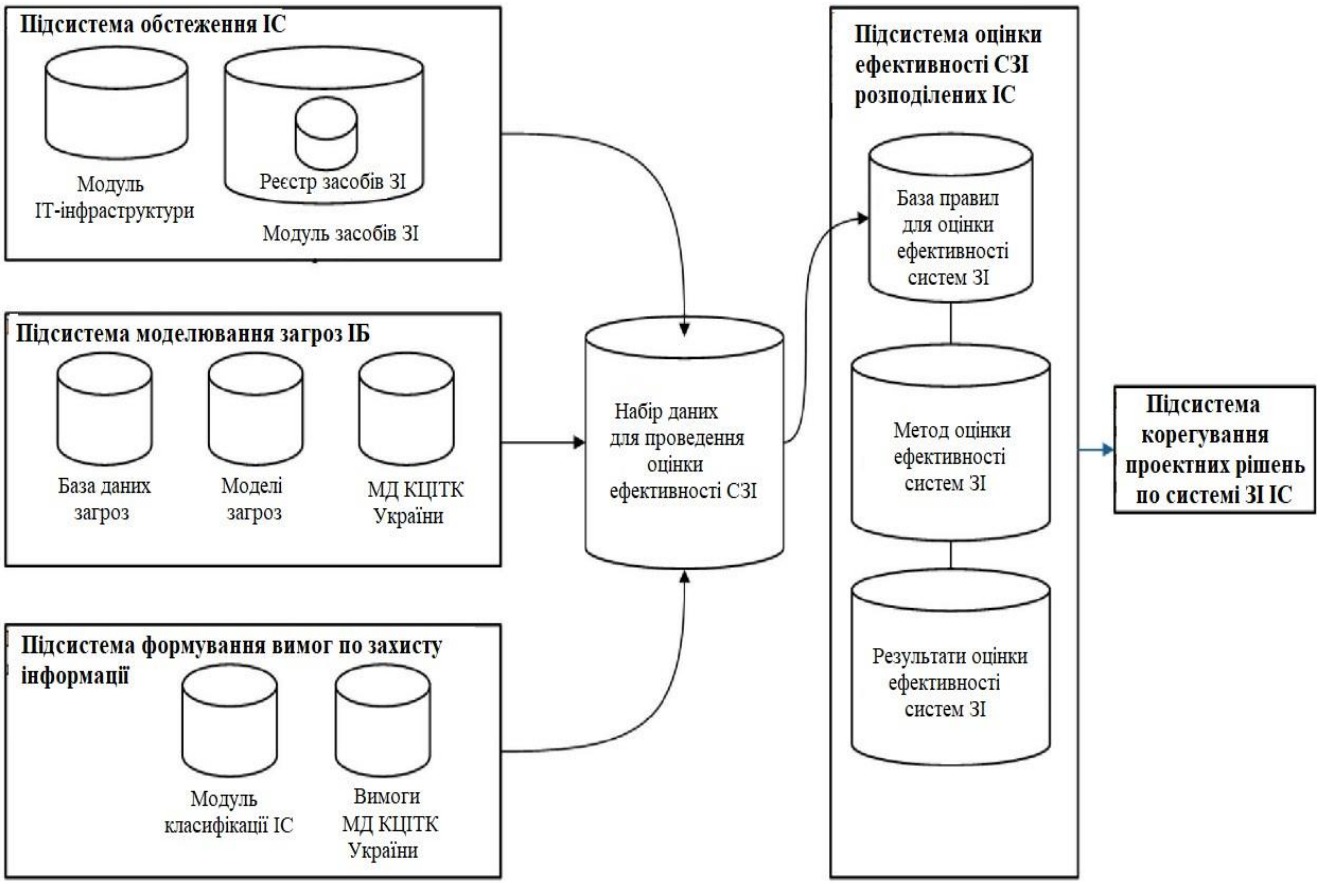


Рисунок 4.3 — Структурна схема оцінки ефективності системи захисту ІС

Запропонований поділ на підсистеми системи оцінки ефективності трансформується в суміжні підсистеми за рахунок незалежності кожної, що, у свою чергу, дозволяє вносити корективи в процес оцінювання ефективності системи захисту інформації розподіленої інформаційної системи.

4.3 Реалізація методу оцінювання ефективності захисту інформації інформаційних систем

Відповідно до запропонованої методики оцінки ефективності системи захисту інформації розподілених інформаційних систем проведено оцінку ефективності системи. Система реалізована у вигляді клієнт-серверної архітектури. В інформаційній системі використовуються мови програмування (TypeScript, C# (середовище розробки dotnet.core, платформа розробки Angular)), щоб забезпечити можливість модифікацій з урахуванням відкритого програмного інтерфейсу.

Системний принцип передбачає централізоване накопичення, зберігання та багаторазове використання даних. Дані не зберігаються в робочих просторах користувачів, інфраструктурі інформаційної системи;

1. Сервери, в тому числі: серверні пристрої; Спеціалізоване та прикладне програмне забезпечення, що надає технологічну інформацію та презентації у формі, необхідній для подальшої автоматизації процесів.

2. Робочі місця користувача: типові робочі простори користувача; Банкомат менеджера: використовується вищим керівництвом (мобільний пристрій).

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

Віртуальні сервери розгортаються в середовищі віртуалізації інформаційної системи: сервери додатків; Сервери OpenVPN для підключення віддалених користувачів з публічної мережі Інтернет; Сервери балансування навантаження; сервер СУБД; сервер онлайн-перегляду; термінальні сервери; сервери веб-перегляду; сервер управління; Сервери

підключення для робочого середовища мобільної автоматизації.

Відповідно до запропонованої методики оцінки ефективності системи захисту інформації розподілених інформаційних систем проведено оцінку ефективності системи. Система реалізована у вигляді клієнт-серверної архітектури. В інформаційній системі використовуються мови програмування (TypeScript, C# (середовище розробки dotnet.core, платформа розробки Angular)), щоб забезпечити можливість модифікацій з урахуванням відкритого програмного інтерфейсу.

Системний принцип передбачає централізоване накопичення, зберігання та багаторазове використання даних. Дані не зберігаються в робочих просторах користувачів, інфраструктурі інформаційної системи;

1. Сервери, в тому числі: серверні пристрої; Спеціалізоване та прикладне програмне забезпечення, що надає технологічну інформацію та презентації у формі, необхідній для подальшої автоматизації процесів.

2. Робочі місця користувача: типові робочі простори користувача; Банкомат менеджера: використовується вищим керівництвом (мобільний пристрій).

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 зв'язку, включаючи кабельні системи; приміщення, в яких знаходяться ресурси розподіленої ІС, які мають відношення до криптографічного захисту інформації.

У розподіленій інформаційній системі обробляються такі категорії інформації: службова інформація; особисті дані; Технічні параметри розподіленої інформаційної системи, файли налаштувань і файли конфігурації та прикладне та системне програмне забезпечення, включаючи програмне забезпечення системних засобів.

Відповідно до алгоритму запропонованого методу було проведено дослідження інформаційної системи та з бази результатів розраховано модель ризику безпеки даних з використанням реальних ризиків інформаційної безпеки відповідно до запропонованого методу.

За результатами дослідження інформаційних систем створено перелік актуальних ризиків інформаційної безпеки та класифікацію, вимоги до захисту інформації.

Як реалізацію системи захисту інформаційної системи представлено опис підсистеми реєстрації подій безпеки та захисту середовища віртуалізації. Підсистема Virtualization Environment Protection забезпечує реалізацію наступних функцій: керування доступом принципалів доступу до об’єктів віртуальної інфраструктури, у тому числі в межах віртуальних машин; Перевіряти та ідентифікувати об’єкти доступу та суб’єкти доступу в адміністраторах керування віртуальною інфраструктурою та пристроях віртуалізації; реєстрація подій безпеки у віртуальній інфраструктурі; контроль цілісності віртуальної інфраструктури та її конфігурації; резервне копіювання даних, резервування каналів зв'язку в рамках віртуальної інфраструктури, технічні процедури, програмне забезпечення віртуальної інфраструктури; керувати переміщенням контейнерів (віртуальних машин) і оброблених даних; Розбиття віртуальної інфраструктури (поділ віртуальної інфраструктури системи на сегменти) і.подальша обробка персональних даних групою користувачів або окремим користувачем; Управління антивірусним захистом і забезпечення у віртуальних інфраструктурах.

В якості підсистеми середовища захисту віртуалізації інформаційна система використовує сертифікований пристрій захисту інформації – vGate. Пристрій vGate R2 Information Protection реалізує функції підсистеми захисту середовища віртуалізації, виконує фільтрацію трафіку на рівні гіпервізора, дозволяє контролювати функції адміністратора віртуальної інфраструктури та захищати від конкретних загроз віртуалізації. Програмне забезпечення vGate включає консоль керування захистом інформації, сервер ліцензій, які інстальовано на автоматизованій робочій станції менеджера захисту інформації. На малюнку. 4.4 представлена логічна схема підсистеми середовища захисту віртуалізації, яка

реалізована за допомогою засобу vGate R2..

Рисунок 4.4 – Логічна схема підсистеми захисту середовища віртуалізації ІС

Підсистема реєстрації подій безпеки перевіряє наступне

Функції: визначення подій безпеки та часу їх зберігання, журналювання піддано; зберігати, збирати та записувати інформацію про інциденти безпеки протягом періоду зберігання, встановленого політикою безпеки; визначення змісту, структури інформації про події безпеки, що підлягають реєстрації; обробка інформації щодо інцидентів безпеки; Перегляд, аналіз (моніторинг) і реагування на результати журналу інцидентів безпеки. Основні функції підсистеми реєстрації подій безпеки включають: журнал безпеки, засіб захисту інформації Dallas Lock 8.0-K, пакет програмного забезпечення захисту інформації EMM SafePhone, який містить інформацію про дії користувача з моменту, коли користувач починає операцію. системи, про помилки тощо, пов’язані з доступом до певних речей, особливо програм, до яких заборонено доступ. Пристрій Dallas Lock 8.0-K Information Security містить такі журнали: журнал керування обліковим записом; вступна реєстрація; Реєстр ресурсів; Журнал політичного менеджменту; друк журналів; журнал пакетів брандмауера; процес реєстрації;

журнал підключень брандмауера; додаток для контролю записів; журнали руху; журнал подій операційної системи.

Час, дата, операція, ім’я користувача, результати та інші параметри записуються в журналі. Також є можливість сортувати (фільтрувати) елементи списків журналів за потрібним значенням. На малюнку. 4.5 показана логічна схема підсистеми реєстрації подій безпеки, реалізована за допомогою Dallas Lock 8.0-K для захисту інформації. Перелік підсистем та функцій захисту інформації при дослідженні системи захисту магістерської роботи 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
Підсистема управління доступом	Керування обліковими записами користувачів. Застосуйте рольовий або дискреційний підхід до доставки. Управління інформаційними потоками між пристроями, компонентами розподіленої інформаційної системи та між інформаційними підсистемами. Розподіл повноважень (ролей) користувачів, адміністраторів. Призначення мінімально необхідних прав і привілеїв користувачам і адміністраторам. Обмежте невдалі спроби входу в ОС. Реалізувати захищений віддалений доступ суб’єктів до об’єктів через зовнішні інформаційно-телекомунікаційні мережі. Авторизація (заборона) дій користувача, дозволених для аутентифікації та ідентифікації.
Підсистема обме-ження ПС	Забезпечення можливості встановлення лише дозволеного до використання програмного забезпечення

Продовження таблиці 4.1

1	2
Підсистем а захисту МН	Облік МН. Управління доступом до МН. Контроль переміщення МН за межі контрольованої зони системи. Контроль підключення МН.
Підсистема реєстрації подій безпеки	Визначте події безпеки, які потрібно реєструвати, і періоди їхнього зберігання. Визначення структури та змісту інформації про події безпеки, що реєструються. Збирайте, записуйте та зберігайте інформацію про інциденти безпеки протягом певного періоду зберігання. Результати моніторингу (перегляду, аналізу) журналів інцидентів безпеки
Підсистема антивірусного захисту	Антивірусний захист АРМ та серверів розподіленої інформаційної системи. Оновлення бази даних ознак шкідливих комп'ютерних програм (вірусів)
Підсистема аналізу захищенності	Ідентифікація та аналіз уразливостей інформаційної системи Контроль встановлення оновлень програмного забезпечення Контроль продуктивності, налаштування параметрів та коректної роботи програмного забезпечення. Технічні засоби управління структурою, програмне забезпечення. Контроль правил для створення та зміни паролів користувачів, виконання правил для проектування доступу, дозволів користувачів.
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	Управління засобами захисту інформації. Адміністрування засобів захисту інформації. Управління оновленнями програмного забезпечення. Розповсюдження виправлень ПЗ. Отримання виправлень та інших оновлень безпеки ПЗ для

інформації	централізованої установки на сервери та АРМ

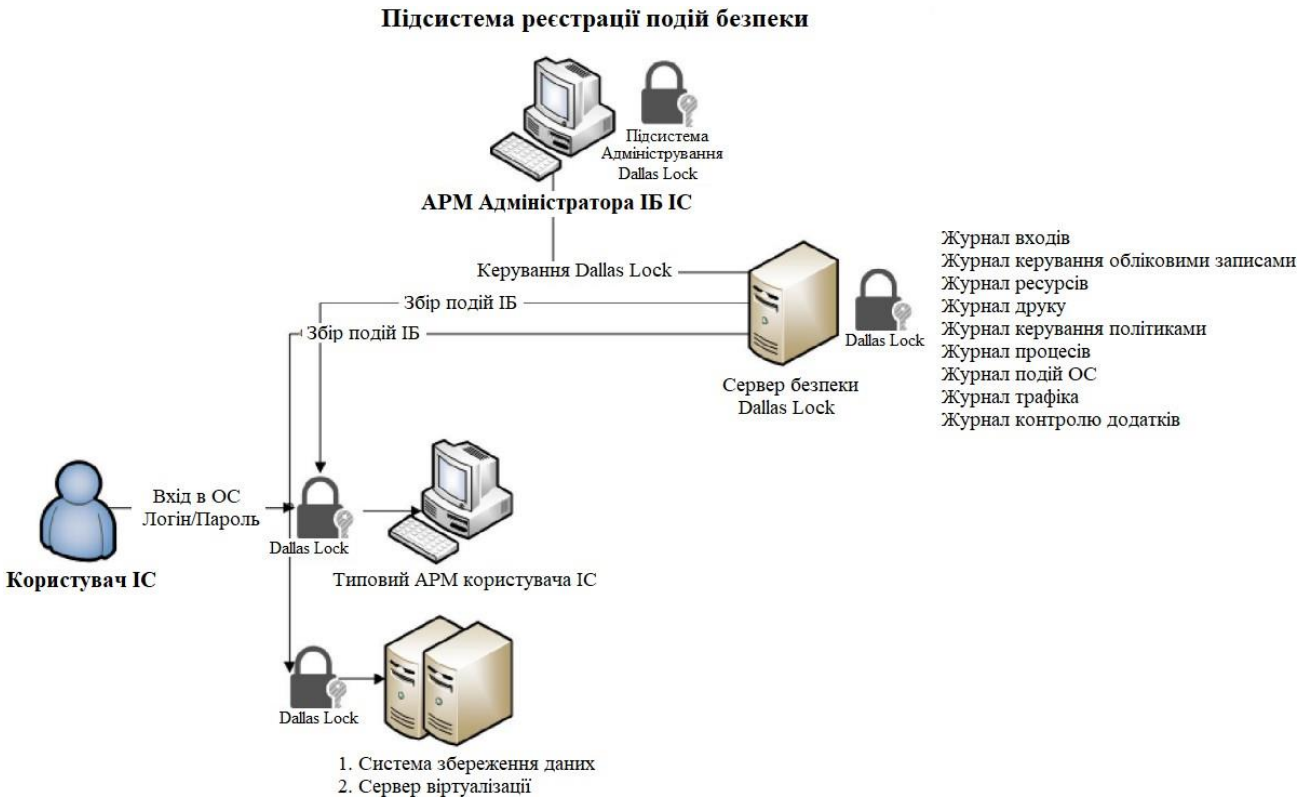


Рисунок 4.5 – Логічна схема підсистеми реєстрації подій

Результати оцінки показали, що прийняті рішення щодо захисту конфіденційної інформації були неефективними: проектні рішення не враховували всі актуальні загрози інформаційній безпеці; Підвищити ефективність системи захисту інформації можна за рахунок скорочення витрат на плановий захист інформації.

Оцінка ефективності системи захисту інформації дозволяє завчасно вносити корективи в проектні рішення системи захисту інформації, що економить фінансові витрати на створення системи захисту та запобігає ризикам. Витік даних.

Для оцінки ефективності запропонованих методів необхідно розглянути інформаційний метод оцінки при визначенні вимог власників розподілених систем. Ефективність системи захисту інформації досягається шляхом створення гарантій у розподіленій системі для максимального усунення існуючих ризиків інформаційної безпеки, адаптації вимог до захисту розподілених систем відповідно до вимог... Власники в області інформаційної безпеки Це дозволяє.

Однією з форм оцінки відповідності є сертифікація системи. Відповідно до статусу завдання, викладеного в магістерській роботі, метод оцінки ефективності розподіленої інформаційної системи на всіх етапах життєвого циклу інформаційної системи повинен використовуватися для своєчасного внесення змін у проектні рішення щодо запобігання. конфіденційних даних.

- Заходи, призначені для оцінки ефективності систем захисту інформації в розподілених інформаційних системах, на відміну від відомих, дозволяють власникам розподілених інформаційних систем оцінювати ефективність системи захисту в режимі реального часу, зменшують фінансові витрати на розробку системи захисту, використання запропонованих заходів. не вимагають великих обчислювальних ресурсів, ефективність систем захисту в розподілених інформаційних системах досягає 97 %;
- Пропоновані кроки в магістерському дослідженні;
- - Зменшити непотрібні та зайві етапи оцінювання;
- - Розглядати всі аспекти процесу оцінки ефективності системи захисту розподіленої інформаційної системи;
- - При оцінці ефективності системи захисту враховувати вимоги в області забезпечення інформаційної безпеки;
- - автоматизація процесу оцінки, усунення недоліків експертних методик, без необхідності залучення висококваліфікованих експертів у сфері інформаційної безпеки;
- - Можливість адаптації до статусу власників розподілених інформаційних

систем.

5 ЕКОНОМІЧНА ЧАСТИНА

5.1 Проведення комерційного та технологічного аудиту науково-технічної розробки

Метою даного розділу є проведення технологічного аудиту, в даному випадку нової комп'ютерної системи оцінювання захищеності об'єкта. Особливістю розробки є підвищення захищеності інформаційно комунікаційних систем шляхом адаптації методів управління ризиками інформаційної безпеки для визначення оптимального підходу до оцінки ризиків для підприємств в межах розробки комп'ютеризованої системи моніторингу безпеки об'єктів.

Аналогом може бути "DELTA-7" – засіб активного захисту автоматизованих систем вартість 22400 грн.

Для проведення комерційного та технологічного аудиту залучають не менше 3-х незалежних експертів. Оцінювання науково-технічного рівня розробки та її комерційного потенціалу рекомендується здійснювати із застосуванням п'ятибальної системи оцінювання за 12-ма критеріями, у відповідності із табл. 5.1.

Таблиця 5.1 – Рекомендовані критерії оцінювання комерційного потенціалу розробки та їх можлива бальна оцінка

Бали (за 5-ти бальною шкалою)					
Крите-рій	0	1	2	3	4
Технічна здійсненність концепції					
1	Достовірність концепції не підтверджена	Концепція підтверджена експертними висновками	Концепція підтверджена розрахунками	Концепція перевірена на практиці	Перевірено роботоздат-ність продук-ту в реаль-них умовах

Продовження табл. 5.1

Ринкові переваги					
2	Багато аналогів на малому ринку	Мало аналогів на малому ринку	Кілька аналогів на великому ринку	Один аналог на великому ринку	Продукт не має аналогів на великому ринку
3	Ціна продукту значно вища за ціни аналогів	Ціна продукту дещо вища за ціни аналогів	Ціна продукту приблизно дорівнює цінам аналогів	Ціна продукту дещо нижче за ціни аналогів	Ціна продукту значно нижче за
4	Технічні та споживчі властивості продукту значно гірші, ніж в аналогів	Технічні та споживчі властивості продукту трохи гірші, ніж в аналогів	Технічні та споживчі властивості продукту на рівні аналогів	Технічні та споживчі властивості продукту трохи кращі, ніж в аналогів	Технічні та споживчі властивості продукту значно кращі, ніж в
5	Експлуатаційні витрати значно вищі, ніж в аналогів	Експлуатаційні витрати дещо вищі, ніж в аналогів	Експлуатаційні витрати на рівні експлуатаційних витрат аналогів	Експлуатаційні витрати трохи нижчі, ніж в аналогів	Експлуатаційні витрати значно нижчі, ніж в аналогів
Ринкові перспективи					
6	Ринок малий і не має позитивної динаміки	Ринок малий, але має позитивну динаміку	Середній ринок з позитивною	Великий стабільний ринок	Великий ринок з позитивною динамікою
7	Активна конкуренція великих компаній на ринку	Активна конкуренція	Помірна конкуренція	Незначна конкуренція	Конкурентів немає
Практик на здійсненність					
8	Відсутні фахівці як з технічної, так і з комерційної реалізації ідеї	Необхідно наймати фахівців або витрачати значні кошти та час на навчання наявних фахівців	Необхідне незначне навчання фахівців та збільшення їх штату	Необхідне незначне навчання фахівців	Є фахівці з питань як з технічної, так із комерційної реалізації ідеї
9	Потрібні значні фінансові ресурси, які відсутні. Джерела фінансування	Потрібні незначні фінансові ресурси. Джерела фінансування відсутні	Потрібні значні фінансові ресурси. Джерела фінансування є	Потрібні незначні фінансові ресурси. Джерела фінансування є	Не потребує додаткового фінансування

10	Необхідна розробка нових матеріалів	Потрібні матеріали, що використовуються у військово-промисловому комплексі	Потрібні дорогі матеріали	Потрібні досяжні та дешеві матеріали	Всі матеріали для реалізації ідеї відомі та давно використовуються у

Продовження табл. 5.1

11	Термін реалізації ідеї більший за 10 років	Термін реалізації ідеї більший за 5 років. Термін окупності інвестицій більше 10-ти років	Термін реалізації ідеї від 3-х до 5-ти років. Термін окупності інвестицій більше 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій від 3-х до 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій менше 3-х років
12	Необхідна розробка регламентних документів та отримання великої кількості дозвільних документів на виробництво та реалізацію продукту	Необхідно отримання великої кількості дозвільних документів на виробництво та реалізацію продукту, що вимагає значних коштів та часу	Процедура отримання дозвільних документів для виробництва та реалізації продукту вимагає незначних коштів та часу	Необхідно тільки повідомлення відповідним органам про виробництво та реалізацію продукту	Відсутні будь-які регламентні обмеження на виробництво та реалізацію продукту

Усі дані по кожному параметру занесено в таблиці 5.2

Таблиця 5.2 – Результати оцінювання комерційного потенціалу розробки

Критерії оцінювання	ПІБ експертів		
	Експерт 1	Експерт 2	Експерт 3
	Бали		
Технічна здійсненність концепції	3	4	4
Наявність аналогів на ринку	3	3	4
Цінова політика	4	4	4
Технічні та споживчі властивості виробу	4	3	4
Експлуатаційні витрати	4	4	3
Ринок збуту	4	3	4
Конкурентоспроможність	3	4	3

Фахівці з технічної і комерційної реалізації	4	3	4
Фінансування	4	4	3
Матеріально-технічна база	3	3	3
Термін реалізації ідеї	4	4	4
Супровідна документація	4	3	4
Сума	44	42	44
Середньоарифметична сума балів	(44+42+44) / 3 = 43,33		

За даними таблиці 5.2 можна зробити висновок щодо рівня комерційного потенціалу даної розробки. Для цього доцільно скористатись рекомендаціями, наведеними в таблиці 5.3.

Таблиця 5.3 - Рівні комерційного потенціалу розробки

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

Як видно з таблиці, рівень комерційного потенціалу розроблюваного нового програмного продукту є високим, що досягається за рахунок підвищення захищеності інформаційно комунікаційних систем шляхом адаптації методів управління ризиками інформаційної безпеки для визначення оптимального підходу до оцінки ризиків для підприємств в межах розробки комп’ютеризованої системи моніторингу безпеки об’єктів.

5.2 Прогнозування витрат на виконання науково-дослідної (дослідно-конструктрорської) роботи

5.2.1 Основна заробітна плата розробників, яка розраховується за формулою:

$$З_о = \frac{M}{T_р} \cdot t, \quad (5.1)$$

де М – місячний посадовий оклад конкретного розробника (дослідника), грн.;

$T_р$ – число робочих днів за місяць, 21 днів;

t – число днів роботи розробника (дослідника).

Результати розрахунків зведемо до таблиці 5.4.

Таблиця 5.4 – Основна заробітна плата розробників

Найменування посади	Місячний посадовий оклад, грн.	Оплата за робочий день, грн.	Число днів роботи	Витрати на заробітну плату, грн.
Керівник проекту	34500	1642,86	28	46000,000
Програміст	31200	1485,71	28	41600,000
Всього				87600,00

Так як в даному випадку розробляється програмний продукт, то розробник виступає одночасно і основним робітником, і тестувальником розроблюваного програмного продукту.

5.2.2 Додаткова заробітна плата розробників, які брати участь в розробці обладнання/програмного продукту.

Додаткову заробітну плату прийнято розраховувати як 15 % від основної заробітної плати розробників та робітників:

$$З_д = З_о \cdot 15\ \% / 100\ \% \qquad (5.2)$$

$З_д = (87600{,}00 \cdot 15\ \% / 100\ \%) = 13140{,}00$ (грн.)

5.2.3 Нарахування на заробітну плату розробників.

Згідно діючого законодавства нарахування на заробітну плату складають 22 % від суми основної та додаткової заробітної плати.

$$Н_з = (З_о + З_д) \cdot 22\ \% / 100\% \qquad (5.3)$$

$Н_з = (87600{,}00 + 13140{,}00) \cdot 22\ \% / 100\ \% = 22162{,}80$ (грн.)

5.2.4. Оскільки для розроблювального пристрою не потрібно витрачати матеріали та комплектуючи, то витрати на матеріали і комплектуючі дорівнюють нулю.

5.2.5 Амортизація обладнання, яке використовувалось для проведення розробки.

Амортизація обладнання, що використовувалось для розробки в спрощеному вигляді розраховується за формулою:

$$A = \frac{Ц}{Тв} \cdot \frac{t_{вик}}{12} \text{ [грн.].} \qquad (5.4)$$

де Ц – балансова вартість обладнання, грн.;

Т – термін корисного використання обладнання згідно податкового

законодавства, років

$t_{вик}$ – термін використання під час розробки, місяців

Розрахуємо, для прикладу, амортизаційні витрати на комп'ютер балансова вартість якого становить 28000 грн., термін його корисного використання згідно податкового законодавства – 2 роки, а термін його фактичного використання – 1,33 міс.

$$A_{обл} = \frac{28000}{2} \times \frac{1{,}33}{12} = 1555{,}56 \; грн.$$

Аналогічно визначаємо амортизаційні витрати на інше обладнання та приміщення. Розрахунки заносимо до таблиці 4.5. Так як вартість ліцензійної ОС та спеціалізованих ліцензійних нематеріальних ресурсів менше 20000 грн, то даний нематеріальний актив не амортизується, а його вартість включається у вартість розробки повністю, $B_{нем.ак.}$ = 6300 грн.

Таблиця 5.5 – Амортизаційні відрахування на матеріальні та нематеріальні ресурси для розробників

Найменування обладнання	Балансова вартість, грн.	Строк корисного використання, років	Термін використання обладнання, місяців	Амортиза-ційні відрахуван-ня, грн.
Комп'ютер та комп'ютерна периферія	28000	2	1,33	1555,556
Офісне обладнання (меблі)	25000	4	1,33	694,444
Приміщення	900000	20	1,33	5000,000
Всього				7250,00

5.2.6 Тарифи на електроенергію для непобутових споживачів (промислових підприємств) відрізняються від тарифів на електроенергію для населення. При цьому тарифи на розподіл електроенергії у різних постачальників

(енергорозподільних компаній), будуть різними. Крім того, розмір тарифу залежить від класу напруги (1-й або 2-й клас). Тарифи на розподіл електроенергії для всіх енергорозподільних компаній встановлює Національна комісія з регулювання енергетики і комунальних послуг (НКРЕКП). Витрати на силову електроенергію розраховуються за формулою:

$$В_е = В \cdot П \cdot Ф \cdot К_п, \quad (5.5)$$

де В – вартість 1 кВт-години електроенергії для 1 класу підприємства з ПДВ в 2024 році для Вінницької області за даними Енера-Вінниця, В = (5635,47/1000)*1,2 = 6,76 грн./кВт;

П – встановлена потужність обладнання, кВт. П = 0,3 кВт;

Ф – фактична кількість годин роботи обладнання, годин.

$К_п$ – коефіцієнт використання потужності, $К_п$ = 0,9.

$В_е = 0,9 \cdot 0,3 \cdot 8 \cdot 28 \cdot 6,76 = 408,8448$ (грн.)

5.2.7 Інші витрати та загальновиробничі витрати.

До статті «Інші витрати» належать витрати, які не знайшли відображення у зазначених статтях витрат і можуть бути віднесені безпосередньо на собівартість досліджень за прямими ознаками. Витрати за статтею «Інші витрати» розраховуються як 50…100% від суми основної заробітної плати дослідників:

$$I_в = (З_о + З_р) \cdot \frac{Н_{ів}}{100\%}, \quad (5.6)$$

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

$I_в$ = 87600,00 * 60% / 100% = 52560 (грн.)

До статті «Накладні (загальновиробничі) витрати» належать: витрати, пов’язані з управлінням організацією; витрати на винахідництво та раціоналізацію; витрати на підготовку (перепідготовку) та навчання кадрів; витрати, пов’язані з набором робочої сили; витрати на оплату послуг банків; витрати, пов’язані з освоєнням виробництва продукції; витрати на науково-технічну інформацію та рекламу та ін. Витрати за статтею «Накладні (загальновиробничі) витрати» розраховуються як 100…150% від суми основної заробітної плати дослідників:

$$H_{нзв} = (З_о + З_р) \cdot \frac{H_{нзв}}{100\%}, \qquad (5.7)$$

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

$H_{нзв}$ = 87600,00 * 130 % / 100 % = 113880 (грн.)

5.2.9 Витрати на проведення науково-дослідної роботи.

Сума всіх попередніх статей витрат дає загальні витрати на проведення науково-дослідної роботи:

$B_{заг}$ = 87600,00+13140,00+22162,80+7250,00+6300+408,84+52560+
+113880 = 303301,64 грн.

5.2.11 Розрахунок загальних витрат на науково-дослідну (науково-технічну) роботу та оформлення її результатів.

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

$$ЗВ = \frac{В_{заг}}{\eta} \text{ (грн)}, \quad (5.8)$$

де η – коефіцієнт, який характеризує етап (стадію) виконання науково-дослідної роботи.

Так, якщо науково-технічна розробка знаходиться на стадії: науково-дослідних робіт, то η=0,1; технічного проектування, то η=0,2; розробки конструкторської документації, то η=0,3; розробки технологій, то η=0,4; розробки дослідного зразка, то η=0,5; розробки промислового зразка, то η=0,7; впровадження, то η=0,9. Оберемо η = 0,5, так як розробка, на даний момент, знаходиться на стадії дослідного зразка:

ЗВ = 303301,64 / 0,5 = 606603 грн.

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

В ринкових умовах узагальнювальним позитивним результатом, що його може отримати потенційний інвестор від можливого впровадження результатів тієї чи іншої науково-технічної розробки, є збільшення у потенційного інвестора величини чистого прибутку. Саме зростання чистого прибутку забезпечить потенційному інвестору надходження додаткових коштів, дозволить покращити фінансові результати його діяльності, підвищить конкурентоспроможність та може позитивно вплинути на ухвалення рішення щодо комерціалізації цієї розробки.

Для того, щоб розрахувати можливе зростання чистого прибутку у потенційного інвестора від можливого впровадження науково-технічної розробки необхідно:

а) вказати, з якого часу можуть бути впроваджені результати науково-технічної розробки;

б) зазначити, протягом скількох років після впровадження цієї науково-технічної розробки очікуються основні позитивні результати для потенційного інвестора (наприклад, протягом 3-х років після її впровадження);

в) кількісно оцінити величину існуючого та майбутнього попиту на цю або аналогічні чи подібні науково-технічні розробки та назвати основних суб'єктів (зацікавлених осіб) цього попиту;

г) визначити ціну реалізації на ринку науково-технічних розробок з аналогічними чи подібними функціями.

При розрахунку економічної ефективності потрібно обов'язково враховувати зміну вартості грошей у часі, оскільки від вкладення інвестицій до отримання прибутку минає чимало часу. При оцінюванні ефективності інноваційних проектів передбачається розрахунок таких важливих показників:

- абсолютного економічного ефекту (чистого дисконтованого доходу);
- внутрішньої економічної дохідності (внутрішньої норми дохідності);
- терміну окупності (дисконтованого терміну окупності).

Аналізуючи напрямки проведення науково-технічних розробок, розрахунок економічної ефективності науково-технічної розробки за її можливої комерціалізації потенційним інвестором можна об'єднати, враховуючи визначені ситуації з відповідними умовами.

5.3.1 Розробка чи суттєве вдосконалення програмного засобу (програмного забезпечення, програмного продукту) для використання масовим споживачем.

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

$$\Delta П_i = (\pm \Delta Ц_0 \cdot N + Ц_0 \cdot \Delta N)_i \cdot \lambda \cdot \rho \cdot (1 - \frac{\vartheta}{100}), \quad (4.9)$$

де $\pm\Delta Ц_o$ – зміна вартості програмного продукту (зростання чи зниження) від впровадження результатів науково-технічної розробки в аналізовані періоди часу;

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

$Ц_o$ – основний оціночний показник, який визначає діяльність підприємства у даному році після впровадження результатів наукової розробки, $Ц_o = Ц_б \pm \Delta Ц_o$;

Цб – вартість програмного продукту у році до впровадження результатів розробки;

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

λ – коефіцієнт, який враховує сплату податку на додану вартість. Ставка податку на додану вартість дорівнює 20%, а коефіцієнт $\lambda = 0{,}8333$.

ρ – коефіцієнт, який враховує рентабельність продукту;

ϑ – ставка податку на прибуток, у 2024 році ϑ =18%.

Припустимо, що при прогнозованій ціні 9500 грн. за одиницю виробу, термін збільшення прибутку складе 3 роки. Після завершення розробки і її вдосконалення, можна буде підняти її ціну на *300* грн. Кількість одиниць реалізованої продукції також збільшиться: протягом першого року – на 1000 шт., протягом другого року – на 1500 шт., протягом третього року на 2000 шт. До моменту впровадження результатів наукової розробки реалізації продукту не було:

*$\Delta П_1$ = (0*300 + (9500 + 300)*1000)* 0,8333* 0,3) * (1 - 0,18) = 1947499,922 грн.*

*$\Delta П_2$ = (0*300 + (9500 + 300)*(1000+1500)* 0,8333* 0,3) * (1 - 0,18) = 5022499,799 грн.*

*$\Delta П_3$ = (0*300 + (9500 + 300)*(1000+1500+2000)* 0,8333* 0,3) * (1 - 0,18) = 9040499,638 грн.*

Отже, комерційний ефект від реалізації результатів розробки за три роки складе 16010499,36 грн.

5.3.2 Розрахунок ефективності вкладених інвестицій та періоду їх окупності.

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

$$ПП = \sum_{1}^{T} \frac{\Delta П_i}{(1+\tau)^t}, \qquad (5.10)$$

де $\Delta П_i$ – збільшення чистого прибутку у кожному із років, протягом яких виявляються результати виконаної та впровадженої науково-дослідної (науково-технічної) роботи, грн;

Т – період часу, протягом якою виявляються результати впровадженої науково-дослідної (науково-технічної) роботи, роки;

τ – ставка дисконтування, за яку можна взяти щорічний прогнозований рівень інфляції в країні, $\tau = 0,05...0,15$;

t – період часу (в роках).

Збільшення прибутку ми отримаємо, починаючи з першого року:

$$ПП = (1947499,922/(1+0,1)^1)+(5022499,799/(1+0,1)^2)+(9040499,638/$$
$$/(1+0,1)^3) = 1770454,47 + 4150826,28 + 6792261,186 = 12713541,94 \text{ грн.}$$

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

$$PV = k_{інв} * ЗВ, \quad (5.11)$$

де $k_{інв}$ – коефіцієнт, що враховує витрати інвестора на впровадження науково-технічної розробки та її комерціалізацію. Це можуть бути витрати на підготовку приміщень, розробку технологій, навчання персоналу, маркетингові заходи тощо; зазвичай $k_{інв}=2...5$, але може бути і більшим;

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

$PV = 2 * 606603 = 1213206{,}58$ *грн.*

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

$$E_{абс} = ПП - PV, \quad (5.12)$$

$E_{абс} = 12713541{,}94 - 1213206{,}58 = 11500335{,}36$ грн.

Оскільки $E_{абс} > 0$ то вкладання коштів на виконання та впровадження результатів даної науково-дослідної (науково-технічної) роботи може бути доцільним.

1. Для остаточного прийняття рішення з цього питання необхідно розрахувати внутрішню економічну дохідність або показник внутрішньої но-рми

дохідності *(IRR, Internal Rate of Return)* вкладених інвестицій та порівняти її з так званою бар'єрною ставкою дисконтування, яка визначає ту мінімальну внутрішню економічну дохідність, нижче якої інвестиції в будь-яку науково-технічну розробку вкладати буде економічно недоцільно.

2. Розрахуємо відносну (щорічну) ефективність вкладених в наукову розробку інвестицій $E_в$. Для цього використаємо формулу:

$$E_в = \sqrt[T_ж]{1 + \frac{E_{абс}}{PV}} - 1, \tag{5.13}$$

$T_ж$ – життєвий цикл наукової розробки, роки.

$$E_в = \sqrt[3]{(1 + 11500335{,}36/1213206{,}58} - 1 = 1{,}188$$

Визначимо мінімальну ставку дисконтування, яка у загальному вигляді визначається за формулою:

$$\tau = d + f, \tag{5.14}$$

де d – середньозважена ставка за депозитними операціями в комерційних банках; в 2024 році в Україні d = (0,09…0,14);

f – показник, що характеризує ризикованість вкладень; зазвичай, величина f = (0,05...0,5).

$$\tau_{\min} = 0{,}14 + 0{,}05 = 0{,}19.$$

Так як $E_в > \tau_{min}$, то інвестор може бути зацікавлений у фінансуванні даної наукової розробки.

Розрахуємо термін окупності вкладених у реалізацію наукового проекту інвестицій за формулою:

$$T_{ок} = \frac{1}{E_в}, \tag{5.15}$$

$T_{ок}$ = 1 / 1,188 = 0,84 р.

Оскільки $T_{ок}$ < 3-х років, а саме термін окупності рівний 0,84 роки, то фінансування даної наукової розробки є доцільним.

Висновки до розділу: економічна частина даної роботи містить розрахунок витрат на розробку нового програмного продукту, сума яких складає 606603 гривень. Було спрогнозовано орієнтовану величину витрат по кожній з статей витрат. Також розраховано чистий прибуток, який може отримати виробник від реалізації нового технічного рішення, розраховано період окупності витрат для інвестора та економічний ефект при використанні даної розробки. В результаті аналізу розрахунків можна зробити висновок, що розроблений програмний продукт за ціною дешевший за аналог і є висококонкурентоспроможним. Період окупності складе близько 0,84 роки.

ВИСНОВКИ

У магістерській роботі була досягнута мета підвищення якості оцінки безпеки об’єктів за допомогою комп’ютеризованої системи. Основними висновками дослідження були:

1. Проведено аналіз сучасних інформаційних систем, визначено ключові аспекти IT-інфраструктури та систем захисту інформації. Досліджено методи та моделі інформаційних систем, моделі загроз безпеки та атак, методи оцінки ефективності систем захисту інформації.

2. Запропоновано метод визначення поточних загроз безпеці, який автоматично формує список поточних ризиків, зменшуючи витрати на обчислення та складність обробки.

3. Розроблено метод оцінки ефективності систем захисту даних, заснований на теорії адаптивного виробництва нечітких нейронних систем та алгоритмі нечіткого виведення TSK. Такий підхід дозволяє проводити оцінку на основі достатніх і необхідних показників.

4. Запропоновані заходи щодо оцінки ефективності систем захисту інформації в комп’ютерних системах дозволяють власникам оцінювати ефективність системи захисту в режимі реального часу, зменшують фінансові витрати на розробку системи, а також зменшують потребу в спільному використанні висококваліфікованих експертів і великих обчислювальних ресурсів. .

Запропоновані заходи враховують усі аспекти оцінки ефективності системи захисту комп’ютерної системи, можуть бути адаптовані до потреб власників і завдяки автоматизації процесу усувають недоліки експертних процедур, які не потребують… висококваліфікованого експерта залучення.

Ефективність запропонованого способу підтверджується наступними аспектами;

- Визначити список поточних загроз безпеці Надійні результати.

- Досягти високої ефективності системи захисту даних.

- Відсутність необхідності відвідування висококваліфікованих фахівців з інформаційної безпеки.

- Використовуйте менше обчислювальних ресурсів.

- Можливість адаптації до конкретних цілей власників при оцінці ефективності системи захисту.

Результати магістерських досліджень можуть бути використані для управління життєвим циклом інформаційних систем, оцінки стану IT-інфраструктури, парку автоматизованих робочих просторів, а також оцінки відповідності організацій сучасним підходам до управління інформаційними технологіями.

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 – Вимі- рювальна 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: htt

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.

ДОДАТОК А

Міністерство освіти і науки України

Вінницький національний технічний університет

Факультет інформаційних технологій та комп’ютерної інженерії

Кафедра обчислювальної техніки

ЗАТВЕРДЖУЮ

Завідувач кафедри

обчислювальної техніки

_____проф., д.т.н. О. Д. Азаров

«29 » лютого 2024 року

ТЕХНІЧНЕ ЗАВДАННЯ

на виконання магістерської кваліфікаційної роботи

Комп’ютерна система оцінювання захищеності обєкту

08-54.МКР.001.00.000 ПЗ

Науковий керівник к.т.н., доц. каф. ОТ

_____ Колесник І. С.

Студента групи КІ-22мз

_____ Артоуз А. О.

ВНТУ 2024

1 Підставою для виконання магістерської кваліфікаційної роботи є наказ про затвердження теми дипломної роботи, а також актуальність процесу розробки системи оцінювання захищеності обєкту або успішного використання на виробництві, наказ про затвердження теми дипломної роботи.

2 Мета і призначення МКР:

— підвищення якості оцінки ефективності систем захисту розподілених інформаційних систем за допомогою визначення достатніх та необхідних показників;

— підвищити якість визначення атак та загроз за рахунок визначення достатніх та необхідних показників для мінімізації помилок методу

3 Вихідні дані для виконання МКР:

— розробити комп’ютерну систему оцінювання захищеності обєкту;

4 Технічні вимоги до виконання МКР:

— виведення математичної моделі створення словників.

— впровадження системи для створення словників.

5 Етапи МКР та очікувані результати (див. табл. А.1).

Таблиця А.1 — Етапи роботи

№ етапу	Назва етапу	Термін виконання		Очікувані результати
		початок	кінець	
1	Постановка задачі роботи	1.03.2024	20.03.2024	Розділ 1
2	Інформаційний пошук та огляд літературних джерел	21.03.2024	9.04.2024	Розділ 2

Продовження таблиці А.1

3	Дослідження підходів та розробка системи	10.04.2024	19.04.2024	Розділ 1, 3 частково
4	Підготовка матеріалів пояснювальної записки	20.04.2024	1.05.2024	Розділ 3 повністю
5	Перевірка якості оформлення магістерської роботи	2.05.2024	22.05.2024	Розділ 4
6	Оформлення пояснювальної записки і презентації	24.05.2023	24.05.2024	Пояснювальна записка, графічний матеріал, лістинг, презентація

6 Матеріали, що подаються до захисту МКР:

— пояснювальна записка МКР;

— графічні і ілюстративні матеріали;

— протокол попереднього захисту МКР на кафедрі;

— відгук наукового керівника;

— рецензія на виконану роботу;

— анотації до МКР українською та іноземною мовами;

— нормоконтроль про відповідність оформлення МКР діючим вимогам.

7 Порядок контролю виконання та захисту МКР:

— виконання етапів графічної та розрахункової документації МКР контролюється науковим керівником згідно зі встановленими термінами;

— захист МКР відбувається на засіданні Державної екзаменаційної комісії, затвердженою наказом ректора.

8 Вимоги до оформлення МКР викладені в методичних вказівках до виконання магістерських кваліфікаційних робіт зі спеціальності 123 — «Комп’ютерна інженерія, ДСТУ 3008 : 2015 «Звіти в сфері науки і техніки. Структура та правила оформлювання», ДСТУ 8302 : 2015 «Бібліографічні посилання. Загальні положення та правила складання».

ДОДАТОК Б

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

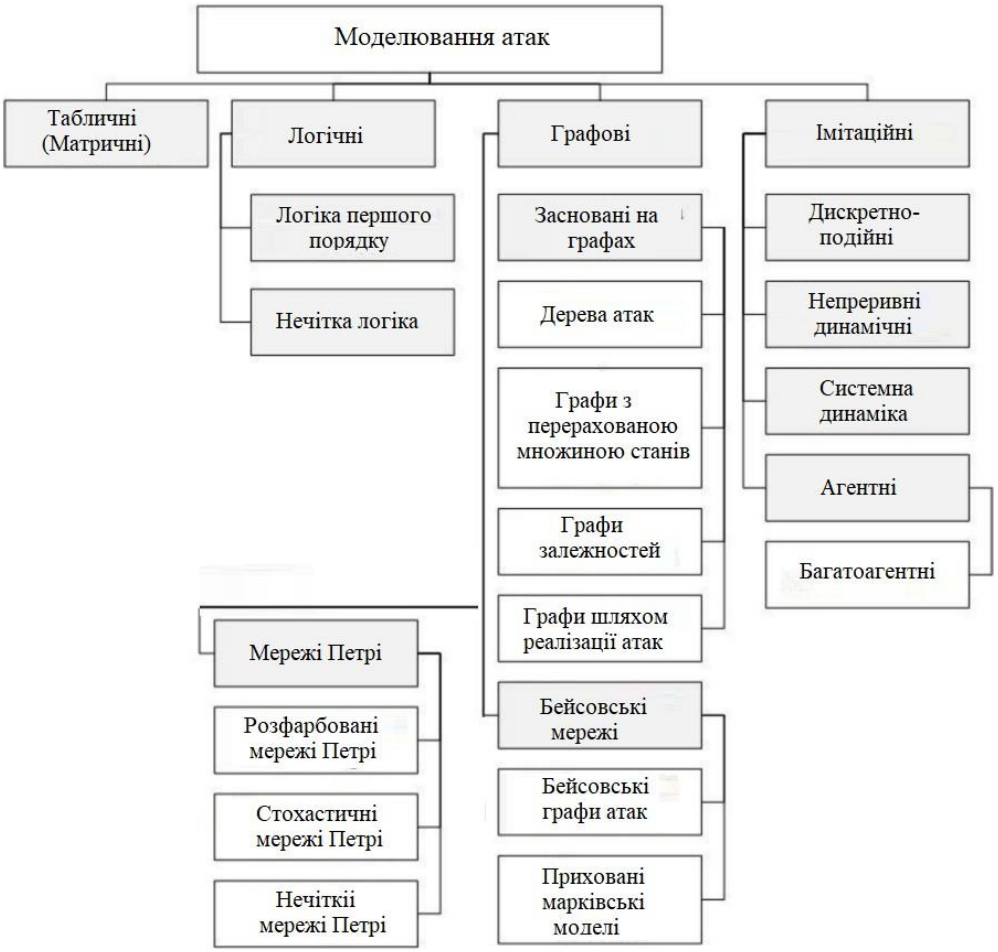
```
class ANFIS:
def init (self, X, Y, memFunction):
self.X =
np.array(copy.copy(X))
self. Y =
np.array(copy.copy(Y))
self.XLen = len(self.X)
selfmemClass = copy. deepcopy(memF
unction) selfmemFuncs =
selfmemClass.MFList
selfmemFuncsByVariable = [[x for x in range(len(self.memFuncs[z]))]] for z in range(len(self.memFuncs))]
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
```

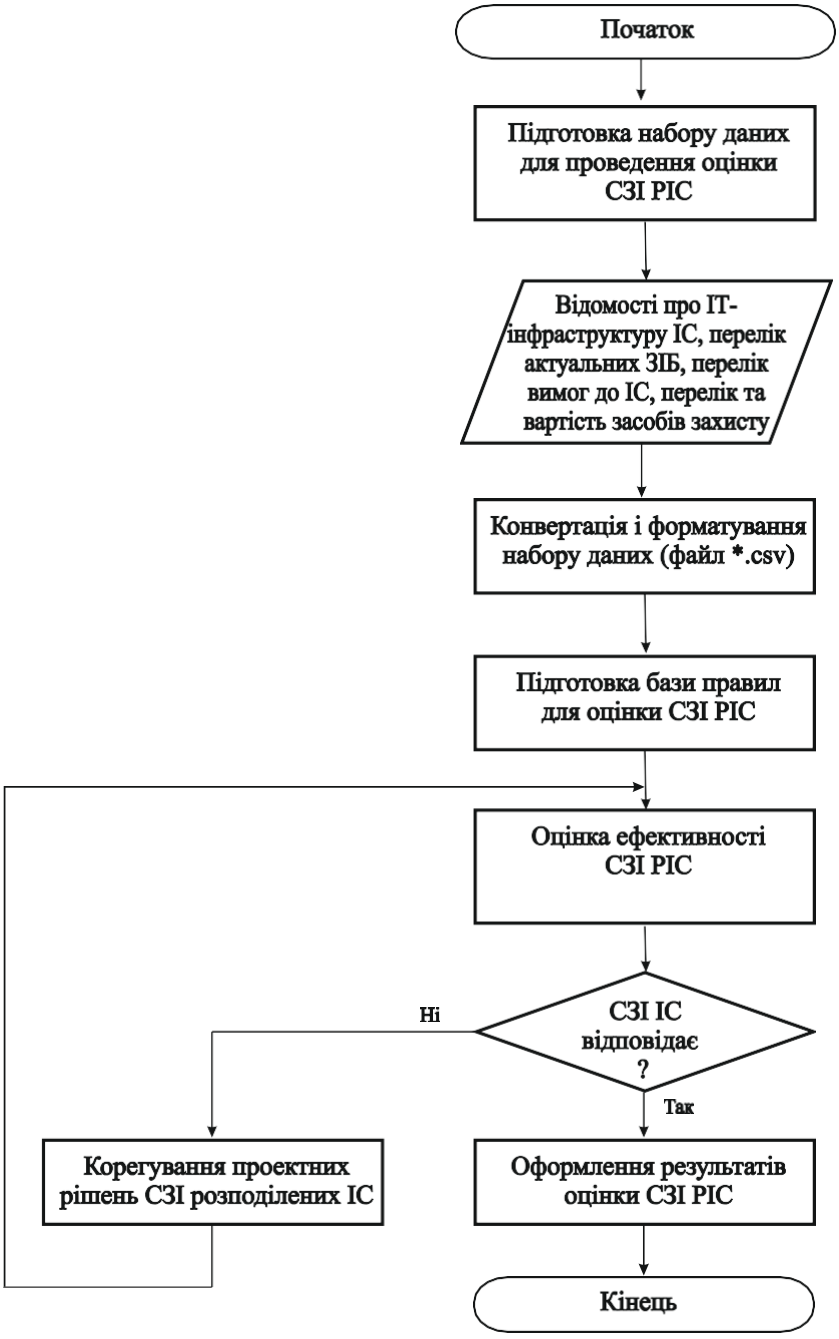
ДОДАТОК В

Моделі атак на інформаційні системи



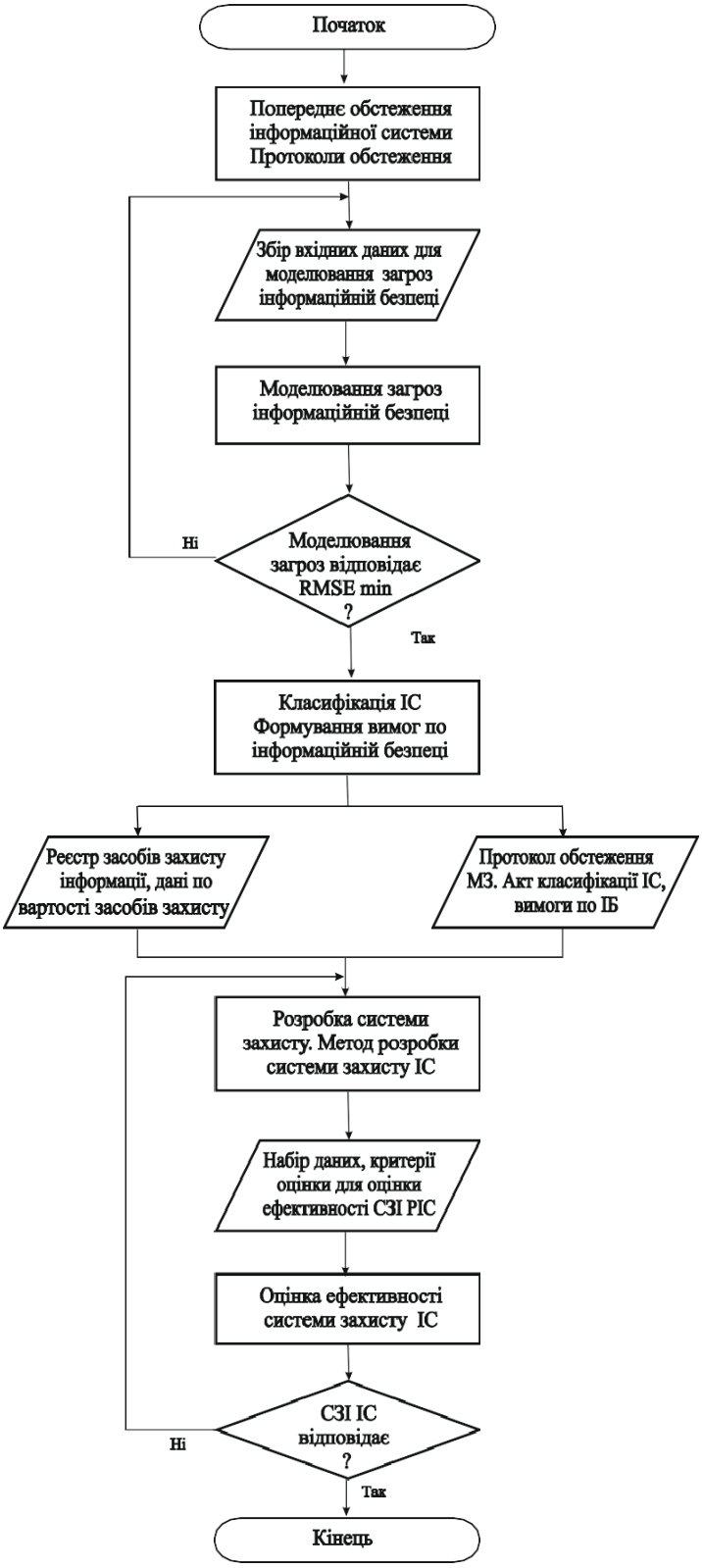
ДОДАТОК Г

Алгоритм оцінки ефективності системи захисту розподіленої інформаційної системи



ДОДАТОК Д

Алгоритм життєвого циклу розробки системи захисту розподіленої інформаційної системи



ДОДАТОК Е

ПРОТОКОЛ
ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ
НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: Комютеризована система оцінки захищеності обєкту

Тип роботи: магістерська кваліфікаційна робота
(БДР, МКР)

Підрозділ кафедра обчислювальної техніки
(кафедра, факультет)

Показники звіту подібності Unicheck

Оригінальність 89,5% Схожість 10,5%

Аналіз звіту подібності (відмітити потрібне):

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

Особа, відповідальна за перевірку _____ Захарченко С.М.
(підпис) (прізвище, ініціали)

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

Автор роботи _____ Артоуз А. О.
(підпис) (прізвище, ініціали)

Керівник роботи _____ Колесник І.С.
(підпис) (прізвище, ініціали)