МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ БІЗНЕС-КОЛЕДЖ

кафедра комп’ютерної інженерії та інформаційних технологій

КВАЛІФІКАЦІЙНА РОБОТА

на тему

АНАЛІЗ ТА ПРОГНОЗУВАННЯ НАВАНТАЖЕННЯ НА МЕРЕЖІ З ВЕЛИКОЮ КІЛЬКІСТЮ КОРИСТУВАЧІВ

Виконав: студент групи 1К-20

спеціальності

123 Комп’ютерна інженерія

Антон СМУГЛІЙ

Керівник Маргарита МЕДОЛИЗ

Черкаси 2024

АНОТАЦІЯ

Кваліфікаційна робота присвячена аналізу та прогнозуванню навантаження на мережі з великою кількістю користувачів. У роботі обґрунтовано актуальність проєктування автоматизованої системи для цієї мети, а також проведено огляд та аналіз існуючих методів і засобів вирішення завдань аналізу та прогнозування мережевого навантаження. Детально розглянуто постановку задачі розробки автоматизованої системи, що забезпечує ефективне управління мережевими ресурсами. Основна увага приділяється методологіям, які дозволяють оптимізувати продуктивність мережі та запобігати перевантаженням у системах з високим трафіком користувачів.

ABSTRACT

This qualification paper focuses on the analysis and forecasting of network load in environments with a large number of users. The work substantiates the relevance of designing an automated system for this purpose and provides an overview and analysis of existing methods and tools for network load analysis and prediction. The problem statement for developing an automated system that ensures efficient network resource management is thoroughly examined. The main emphasis is placed on methodologies that enable network performance optimization and prevent overloads in high-user traffic systems.

ЗМІСТ

ВСТУП

Актуальність теми. У наш час надійність інформаційної сфери стає все більш важливою для ключових аспектів національної безпеки. Оскільки розвиток комп'ютерів продовжує зростати, важливість захисту інформації зростає. Ця тенденція підтримується значним сплеском кібератак і пов'язаних із ними ризиків, в тому числі зростання навантаження на вузли мереж і виведення їх з ладу. Тому існує нагальна потреба в розробці ефективних методів і систем для виявлення, моніторингу, прогнозування навантажень задля пом'якшення цих загроз.

Тому актуальним є дослідження можливостей аналізу та прогнозування навантаження на вузли мережі задля запобігання збоям та виявлення кібератак в мережевому трафіку.

Метою даної роботи є аналіз алгоритмів та прогнозування навантаження на вузли багатокористувацької мережі як засобу запобігання збоям та кіберзагрозам.

Виходячи з мети, перед нами постають наступні завдання:

- провести огляд і аналіз існуючих методів і засобів вирішення завдань діагностики та прогнозування мережевого трафіку;

- здійснити огляд структури та функцій алгоритму по виявленню змін навантаження та кібератак в мережевому трафіку;

- виконати аналіз алгоритмів по виявленню змін навантаження в мережевому трафіку;

- обрати найбільш ефективну модель.

Предметом дослідження є системи виявлення змін у навантаженні на вузли багатокористувацьких мереж з метою запобігання збоям.

Об'єктом дослідження є мережеві ресурси та додатки.

Практичне значення одержаних результатів – вибір алгоритму аналізу та прогнозування стану багатокористувацької мережі з врахуванням навантаження, яка дозволить спростити та значно покращити процес прогнозування кібератак та протидії кіберзагрозам.

Методи дослідження. В основі виконання даної роботи лежить використання таких загальнонаукових методів дослідження: логічного, діалектичного, історичного та порівняльного методів для обґрунтування наукових засад та вдосконалення понятійного апарату дослідження; методів спостереження, узагальнення, абстрагування, формалізації, аналізу та синтезу для характеристики методичних аспектів створення інформаційно-аналітичної системи; програмно-цільовий метод з метою обґрунтування механізмів розробки та реалізації програм інформатизації аналітичних процесів.

Інформаційну базу дослідження становлять розробки та публікації науковців, інтернет ресурси, офіційні матеріали, нормативно-правові акти в сфері інформатизації та кібербезпеки. Також широко використані наукові розробки з загальної теорії управління, моделювання складних систем, автоматизованих систем управління, інформаційної аналітики, теорії прийняття рішень, менеджменту тощо.

РОЗДІЛ 1.
ОГЛЯД АЛГОРИТМІВ ДЛЯ ВИЗНАЧЕННЯ НАВАНТАЖЕНОСТІ МЕРЕЖ

1.1 Обґрунтування актуальності проєктування автоматизованої системи аналізу та прогнозування навантаження в мережах з великою кількістю користувачів

Стабільність роботи комп'ютерної мережі підприємства є запорукою ефективності його діяльності. Тому будь-які збої, викликані зовнішніми чи внутрішніми причинами, порушують стабільність роботи підприємства і вимагають швидкої діагностики причин та усунення наслідків. Тому прогнозування навантаження в робочому стані, швидке реагування на його аномальне зростання та аналіз значень критичного навантаження, яке може призвести до збою є основними завданнями для проєктованої системи.

Зараз використовуються два типи систем виявлення: системи виявлення аномалій і системи виявлення особливостей. Однак системи виявлення функцій мають серйозний недолік, оскільки вони розроблені для виявлення конкретних типів атак, і коли з'являються нові атаки або змінюються параметри атак, систему потрібно оновлювати. З іншого боку, системи виявлення аномалій спираються на припущення щодо нормального функціонування системи, наприклад статистичну однорідність інтернет-трафіку. Однак недостатньо дискусій щодо того, до яких комп'ютерних систем застосовуються ці припущення, або умов, необхідних для їх реалізації. Це означає, що навіть незначні зміни в моделях трафіку або послугах можуть вимагати повторного навчання алгоритму виявлення. Одним із можливих рішень цієї проблеми є застосування комплексного підходу до боротьби з атаками, який передбачає моніторинг системи, збереження історії транзакцій, створення сховища для інтелектуального аналізу зловмисників та їхніх дій, а також визначення стратегії протидії. Пропонується побудувати систему контролю навантаження на основі наступних елементів:

– агенти відстеження;

– заходи попередньої обробки та зберігання;

– сховище для зберігання інформації про операції, що описує роботу системи;

– сховище з аналітичними компонентами для виявлення загроз та ознак зловмисної діяльності;

– заходи проти нападів [2; с. 572].

Важливим елементом побудови такої системи є визначення відповідного математичного забезпечення для кожного етапу роботи:

1. Процес моніторингу трафіку передбачає перехоплення пакетів з метою аналізу обсягу даних, типів трафіку та поведінки користувачів. Для успішного виконання цього завдання вкрай важливо розробити алгоритми, які можуть ефективно визначати оптимальну швидкість і частоту перехоплення пакетів на основі таких факторів, як перевантаження каналу та інших відповідних параметрів. Часте перехоплення пакетів може призвести до зниження ефективності трафіку, тоді як захоплення пакетів через фіксовані проміжки часу може призвести до формування зон, у яких дані не повідомляються [2; с. 572].

2. Перед подальшим аналізом перехоплені пакети проходять попередню обробку, оцінюється виявлення найбільш критичних загроз, а зібрана інформація зберігається у призначених сховищах. Через необхідність швидкої оцінки з використанням мінімальних ресурсів доцільно використовувати прості та гнучкі порогові значення або, якщо це виправдано, послідовні методи CUSUM.

3. Може проводитися перевірка даних під час їх перенесення в пам'ять, виявлення ворожої діяльності та оцінка потенційних загроз. Коли інформація буде збережена в сховищі, можна провести ретельну оцінку для визначення можливих ризиків. Щоб досягти цього, рекомендується використовувати багатоканальний CUSUM і алгоритми ковзного середнього, розглянуті раніше.

4. Перевірка історичних даних для виявлення спроб сканування, атак деградації та імпульсних атак виконується періодично або відповідно до заздалегідь визначеного розкладу. Враховуючи низький рівень загрози, яку

становлять ці атаки, необхідний більш глибокий аналіз. Для цього використовуються різні методи, такі як аналіз даних, інтелектуальні системи правил і нейронні мережі.

5. Вибір виявлення атаки передбачає визначення того, чи були перевищені попередньо визначені порогові значення на будь-якому з попередніх етапів, що вказує на потенційну атаку. У таких випадках виникає необхідність створити експертну систему, яка може оцінити серйозність загрози та згодом визначити, чи мала місце атака.

6. Оцінка ризику, вибір моделі, перевірка та пошук стратегії є ключовими компонентами у визначенні відповідних заходів протидії при виявленні атаки. Ефективність цих контрзаходів може змінюватися залежно від типу та характеристик атаки, що призводить до розробки конкретних стратегій. На якість цих стратегій, наприклад рівень обслуговування, що надається зареєстрованим користувачам, можна вплинути за допомогою аналітичного моделювання взаємодії між зловмисником і агентами захисту. Вивчаючи ці моделі, можна оцінити ефективність контрзаходів і потенційні наслідки. Процес прийняття стратегічних рішень керується конфліктною взаємодією між зловмисником і системою захисту, причому основна увага приділяється мінімізації навантаження на систему, будь то загальне навантаження чи певні критичні вузли, такі як ЦП, ОЗП, і мережевих каналів [2; с. 573].

Для розробки стратегії протидії необхідно спочатку оцінити параметри конфронтаційної динамічної моделі. Ця операція включає наступні кроки: визначення природи динаміки, оцінка кількості та потужності нападників, вимірювання рівня загрози та визначення потенційних контрзаходів із прогнозуванням їхніх наслідків.

Впровадження контрзаходів і оцінка наступників у порівнянні з прогнозами. Після впровадження захисного заходу система повинна оцінити його ефективність шляхом кількісного визначення рівня пом’якшення загрози.

1.2 Огляд і аналіз існуючих методів і засобів вирішення завдань аналізу та прогнозування навантаження в мережі

Методи нечітких множин виявляються особливо корисними в ситуаціях, коли бракує точної математичної моделі, що описує функціонування системи. Теорія нечітких множин дозволяє включати неточні та суб'єктивні експертні знання, що стосуються конкретного предмета, у процес прийняття рішень без необхідності формалізації за допомогою традиційних математичних моделей.

Використовуючи теорію нечітких множин, можна знайти рішення для збалансування суперечливих критеріїв прийняття рішень і розробки логічних засобів керування системою. Нечіткі набори дозволяють використовувати описи на основі мови для складних процесів, встановлення нечітких зв'язків між ідеями, прогнозування продуктивності системи, генерування діапазону потенційних дій та формальне формулювання нечітких принципів прийняття рішень.

Методи теорії нечітких множин служать практичним інструментом для розробки інтерфейсів у системах людина-машина. Різноманітні програми, такі як системи управління, представлення знань, підтримка прийняття рішень, наближення, структурна та параметрична ідентифікація, розпізнавання образів та оптимізація, базуються на принципах нечіткої логіки. Нечітка логіка застосовується в побутовій електроніці, діагностиці та різноманітних експертних системах. Нечіткі експертні системи підтримки прийняття рішень знаходять широке застосування у військовому, медичному та економічному секторах для таких завдань, як бізнес-прогнозування, оцінка ризиків і оцінка прибутковості інвестиційних проектів. Крім того, нечітка логіка використовується для моделювання глобальних політичних рішень і кризових сценаріїв [2, с. 115].

Концепція нечітких множин [4] була спочатку введена Лотфі Заде, американським математиком, у 1965 році. Її мета полягала в тому, щоб вирішити проблеми, пов'язані з представленням нечітких ідей, і створити основу для аналізу та моделювання систем із залученням людини.

Підхід, заснований на теорії нечітких множин, служить альтернативою загальноприйнятим кількісним методам системного аналізу. Цей підхід має три

основні характеристики: по-перше, він використовує невизначені значення, відомі як «лінгвістичні» змінні, або замість числових змінних, або в поєднанні з ними; по-друге, зв'язки між змінними описуються за допомогою неточних тверджень; і, нарешті, складні зв'язки з'ясовуються за допомогою використання нечітких алгоритмів.

Ця методологія пропонує приблизні, але ефективні методи для характеристики динаміки складних систем, які за своєю суттю не піддаються точному математичному аналізу через притаманні невизначеності.

Теорія нечітких множин — це математичний інструмент, який дозволяє представляти абстрактні поняття в числовій формі. Це дозволяє виражати нечіткі описи або властивості об’єктів за допомогою таких термінів, як високий, середній або малий. Включаючи неточну інформацію, теорія нечітких множин має на меті імітувати людські міркування та сприйняття. Нечітка логіка, ключовий компонент цієї теорії, вводить поняття часткової істинності, де значення істинності коливаються від 0,0 (повністю хибно) до 1,0 (повністю істинно). Нечітка множина A визначається як множина з функцією належності μA, яка приймає значення в діапазоні [0,0, 1,0]. Значення μA (x), що дорівнює 0,0 і 1,0, представляють нульову та повну приналежність x до A, відповідно, тоді як значення в діапазоні від 0,0 до 1,0 вказують на часткову приналежність. Математично, нечітка множина A характеризується функцією приналежності, визначеною в певній області X, відомої як область дискурсу (формула 1.1):

$$\mu A : X \rightarrow [\,0,1\,] \qquad (1.1)$$

де A — це нечітка мітка або лінгвістична змінна, яка характеризує змінну x. На відміну від булевої логіки, μA (x) кількісно визначає ступінь, до якої x є членом нечіткої множини A. Нечіткі множини застосовуються для визначення значень нечітких змінних.

Правила нечіткої логіки дають можливість включати встановлений досвід управління об’єктами та використовувати адаптовані правила в ситуаціях, коли традиційні методи моделювання можуть виявитися недостатніми.

Підвищення стандарту менеджменту досягається шляхом реалізації саморегуляції в системі менеджменту, а також використання випереджаючих модифікацій у відповідь на непередбачені події, які неможливо вирішити за допомогою звичайних методів менеджменту.

Використання методів управління в різних промислових застосуваннях, включаючи безперервні процеси, пакетну обробку та автоматизовані системи, постійно зростає. Нечітка логіка була визнана та розроблена як підхід до програмування завдяки своїй ефективності в цій області. Це дозволяє організувати емпіричні знання для управління процесами, коли традиційні методи виявляються складними [20]. Принципи нечіткої логіки пропонують структуру для реалізації стратегій керування, застосовних до систем реального світу та включають досвід операторів і технологів для динамічного керування процесом. Це полегшує опис і реалізацію конкретних аспектів виробничих процесів, таких як ініціалізація, налаштування параметрів і використання нечіткої логіки.

Ось деякі важливі характеристики нечіткої логіки:

– гнучка та проста у впровадженні технологія машинного навчання;

– допомагає слідкувати за логікою людського мислення;

– логіка може мати два значення, які представляють два можливі рішення;

– дієвий метод нечіткого чи приблизного міркування;

– нечітка логіка розглядає висновки як процес поширення обмежень;

– нечітка логіка дозволяє будувати нелінійні функції довільної складності;

– нечітка логіка повинна створюватися під повним керівництвом експертів.

Операційна структура нечіткої системи ґрунтується на певному механізмі логічного висновку, у якому діючі змінні характеризуються за допомогою використання нечітких наборів.

Використовуючи нечіткі набори, нечітка система може охопити невід'ємну невизначеність, присутню в сценаріях реального світу, шляхом формулювання ЯКЩО … ТО … правил, сформульованих повсякденною мовою. Ці правила, які разом називаються базою знань, служать для визначення приблизного співвідношення між вхідними та вихідними даними, керуючи процесом прийняття рішень. Таким чином, нечітка система функціонує як заснована на правилах структура, яка інтерпретує незнайомі вхідні/вихідні відносини в зрозумілий формат, використовуючи набір нечітких правил, заснованих на зрозумілих людині операторах.

Як правило, механізм нечіткого висновку Мамдані використовується в інженерних програмах і може бути реалізований у середовищі Matlab. Розроблений Ібрагімом Мамдані в 1975 році, цей метод був одним з перших, у яких використовувалася теорія нечітких множин, і класифікується як система нечіткого висновку (НСВ). Система НСВ, з іншого боку, використовує теорію нечітких множин для встановлення відображення вхідних даних (таких як функції в нечіткій класифікації) на виходи (таких як класи в нечіткій класифікації) [52].

Методологія включає послідовне виконання наступних кроків: створення бази правил, поетапність, агрегація попередніх умов, активація підвисновків, накопичення висновків і дефазифікація.

Етапи процесу виконуються послідовно, при цьому кожна наступна стадія використовує результати, отримані з попередньої стадії. Метод Мамдані використовує певний набір правил для визначення вхідних значень для системи.

Фундаментальна структура нечіткої системи, описана Мамдані та Асіліаном [52], проілюстрована на рисунку 1.1. Система працює, приймаючи точні вхідні дані та генеруючи точні вихідні дані за допомогою використання нечіткої бази правил, яка служить сховищем знань системи. Початкова стадія системи передбачає перетворення чітких даних у нечіткі змінні за допомогою фазифікатора, тоді як дефазифікатор використовується на виході системи для перекладу нечітких наборів у точні значення.

Рисунок. 1.1 - Загальна схема системи нечіткого виведення

Механізм нечіткого висновку використовує правила з бази правил відповідно до теорії наближеного міркування для встановлення відповідності між нечіткими наборами у вхідній області та нечіткими наборами у вихідній області. Отже, нечітка система пропонує обчислювальну структуру, яка описує процес, за допомогою якого правила оцінюються та інтегруються для отримання точного вихідного значення (вектора) для будь-якого заданого точного вхідного значення. Таким чином, нечітку систему можна концептуалізувати як параметричну функцію, яка перетворює умовні вектори в реальні вектори.

Для визначення системи, заснованої на нечітких правилах, можна використовувати різні моделі, як показано структурою нечітких правил. У нечіткій системі типу Мамдані результатом кожного правила є нечітка множина, визначена для лінгвістичної змінної. Виведення правил у цій системі слідує за розширенням моделі modus ponens на нечіткі множини. Це передбачає коригування нечіткого набору наслідків на основі вхідного значення та рівня активації правила, визначеного ступенем приналежності вхідного значення до попередніх умов. Оператор …ТО, також відомий як оператор імплікації, визначає вихідний нечіткий набір для кожного правила.

В результаті використання нечітких наборів у передумові правил стає можливим виконувати декілька нечітких правил одночасно.

Розглянемо основні інструменти нечіткої логіки, які застосовуються в сучасних умовах.

1) Нечіткі нейронні мережі. Нечіткі мережі роблять висновки на основі механізму нечіткої логіки, але параметри функції належності налаштовуються за

допомогою алгоритмів навчання нейронної мережі. Тому для вибору параметрів таких мереж використовується метод зворотного поширення помилок, спочатку запропонований для навчання багатошарового персептрона. Для цього модуль нечіткого управління представлений у вигляді багатошарової мережі. Нечітка нейронна мережа зазвичай складається з чотирьох рівнів: вхідного шару розмиття, рівня агрегації значень активації умови, рівня агрегації нечітких правил і вихідного рівня. В даний час найбільш поширеною є архітектура нечіткої нейронної мережі типу AFIS і TSK. Універсальність таких мереж була продемонстрована емпіричними доказами. Поєднання ефективних алгоритмів навчання та здатності інтерпретувати набуті знання зробило нечіткі нейронні мережі дуже перспективним і ефективним інструментом у сфері програмних обчислень.

2) Адаптивні нечіткі системи пропонують вирішення обмежень класичних нечітких систем, які покладаються на експертні знання, які не завжди можуть бути передані. Ці адаптивні системи вирішують цю проблему шляхом вибору параметрів нечіткої системи на основі експериментальних даних під час процесу навчання. Однак алгоритми навчання для адаптивних нечітких систем є більш трудомісткими та складними порівняно з алгоритмами навчання нейронної мережі. Як правило, ці алгоритми включають два етапи: створення мовного правила та налаштування функції належності. Перший має справу з вичерпними проблемами, тоді як другий зосереджується на оптимізації в безперервних просторах. Тим не менш, виникає парадокс у тому сенсі, що функції приналежності потрібні для генерації нечітких правил, а правила потрібні для нечіткого висновку. Крім того, при автоматичному створенні нечітких правил важливо забезпечити їх повноту та послідовність. Генетичні алгоритми зазвичай використовуються для вивчення нечітких систем, також відомих як Genetic Fuzzy Systems в англомовній літературі. Слід зазначити, що Ф. Еррера та команда іспанських дослідників зробили значний внесок у теорію та практику нечітких систем з еволюційною адаптацією.

3) Нечіткі запити. Перспективним напрямком сучасних систем обробки інформації є нечіткі запити до баз даних. Цей інструмент дозволяє формулювати запити природною мовою, наприклад: «Список недорогої оренди квартир поблизу центру міста», що неможливо за допомогою стандартного механізму запиту. Для цього розроблено нечітку реляційну алгебру та спеціальні розширення SQL для нечітких запитів.

4) Нечіткі асоціативні правила (Fuzzy Association Rules). Це інструмент для отримання та обробки шаблонів із баз даних, які сформульовані як лінгвістичні вирази. Тут представлено спеціальні поняття нечіткої транзакції, обробки та дійсності правила нечіткої асоціації.

5) Нечіткі когнітивні карти використовуються для зображення причинно-наслідкових зв’язків між поняттями в певній області. На відміну від традиційних когнітивних карт, нечіткі когнітивні карти складаються з нечітких наборів як вузлів у орієнтованому графі. Ребра на графіку не лише представляють причинно-наслідкові зв’язки між поняттями, але й вказують на силу впливу між ними. Популярність нечітких когнітивних карт у системах моделювання пояснюється їх здатністю візуально представляти складні системи та легко інтерпретувати причинно-наслідкові зв’язки між поняттями. Проблеми при створенні когнітивних карт включають відсутність формалізації в процесі та необхідність перевірити точність карти порівняно з реальною системою. Щоб вирішити ці проблеми, були розглянуті алгоритми автоматичної побудови когнітивних карт на основі вибірки даних [23].

6) Нечітке групування передбачає використання методів нечіткої кластеризації, які відрізняються від явних методів, таких як нейронні мережі Кохонена, тим, що вони дозволяють призначати об’єкти до кількох кластерів одночасно, але з різним ступенем членства. Нечіткій кластеризації часто надають перевагу в ситуаціях, коли об’єкти розташовані на межах кластера, оскільки це вважається більш природним підходом. Загальні приклади методів нечіткої кластеризації включають алгоритм самоорганізації нечітких с-середніх і алгоритм Густафсона-Кесселя. Крім того, існує ряд інших методів нечіткої

кластеризації, таких як нечіткі дерева рішень, нечіткі мережі Петрі, нечітка асоціативна пам’ять, нечіткі карти самоорганізації та гібридні методи.

Переваги систем нечіткої логіки включають їх просту та нескладну структуру, їх широке використання в комерційних і практичних застосуваннях, їх здатність керувати процесами зі змінними стохастичними параметрами через використання правил нечіткої логіки, їх здатність справлятися з невизначеністю в точних розрахунках і їх надійність у відсутності необхідності введення точних даних. Крім того, ці системи можуть бути запрограмовані на реагування у разі несправності датчика зворотного зв’язку, можуть бути легко модифіковані для підвищення або зміни продуктивності системи, можуть використовувати недорогі датчики введення, щоб зберегти загальну вартість і складність системи на мінімумі, і запропонувати високоефективні рішення до заплутаних проблем.

Недоліки нечітких систем включають недостатню точність нечіткої логіки, що призводить до результатів, заснованих на припущеннях, які можуть бути не загальновизнаними. Для пом’якшення цієї проблеми часто використовуються діапазони прийнятності. Крім того, нечітким системам не вистачає можливостей машинного навчання для визначення шаблонів нейронних мереж. Верифікація нечіткої системи з використанням онтологічних знань вимагає широкого тестування обладнання. Досягнення точних результатів на основі нечітких правил і функцій може бути складним завданням, і існує тенденція до неправильного тлумачення нечіткої логіки як теорії ймовірностей.

Отже, методика використання нечіткої логіки для отримання наближеної оцінки непараметризованих вхідних даних є досить універсальною, тому доцільно розглянути окремі моделі, що використовуються в системах визначення причин збою мережі.

1.3 Постановка задачі по розробці автоматизованої системи аналізу та прогнозування навантаження в мережах з великою кількістю користувачів

Аналіз та прогнозування навантаження проводяться з метою уникнення збоїв в мережі та забезпечення доступності вузлів мережі у будь-який час.

Показники надійності визначаються шляхом використання розрахунків, випробувань та аналізу статистичних даних, отриманих в результаті експлуатації виробу та комп'ютерного моделювання. Крім того, показники надійності встановлюються шляхом вивчення фізичних і хімічних процесів, які сприяють виробництву надійної продукції. Ці розрахунки базуються на розумінні того, що існують певні кореляції між надійністю окремих компонентів і загальною надійністю виробу, враховуючи структуру виробу та розподіл його терміну служби. Для встановлення цих кореляцій використовуються різні методи, такі як розв’язування рівнянь на основі структурної схеми продукту або логічних зв’язків між його станами, розв’язування диференціальних рівнянь, які описують перехід продукту між станами, і розробка функцій, які описують стани складного продукту.

Розрахунки надійності відіграють вирішальну роль на етапі проектування продукту, щоб передбачити очікувану надійність конкретного варіанту продукту. Це дозволяє підібрати найбільш підходящий варіант конструкції і способи забезпечення надійності, виявити потенційно слабкі місця, раціонально розподілити режими роботи і сформувати відповідний план технічного обслуговування виробу. Випробування на надійність проводяться на стадіях розробки прототипу та серійного виробництва продукту. Ці випробування включають первинні випробування на надійність для визначення показників пропускної здатності мережі, контрольні випробування, спрямовані на контроль якості технологічного процесу для забезпечення надійності не нижче заданого рівня, прискорені випробування з використанням факторів прискорення виникнення відмов, неруйнівні випробування на основі з методів дефектоскопії та інтроскопії, а також вивчення непрямих ознак, таких як шум і теплове випромінювання, пов'язаних з виникненням відмов. Комп’ютерне моделювання з використанням електронно-обчислювальних машин є найефективнішим підходом до аналізу надійності складних систем. Два широко використовуваних алгоритму моделювання включають один, який моделює фізичні процеси, що відбуваються в досліджуваному об’єкті, для оцінки надійності на основі

кількості параметрів, що перевищують допустимі межі, а інший розв’язує системи рівнянь, що описують стани об’єкта [12].

Дослідження фізико-хімічних процесів дозволяє дослідникам оцінити надійність досліджуваного стану. Це передбачає дослідження зв’язку між надійністю та станом і характером фізико-хімічних процесів, таких як співвідношення показників міцності та навантаження, зносостійкості, наявності домішок у матеріалах, зміни електричних і магнітних властивостей, впливу шуму. Аналіз фізико-хімічних процесів переважно використовується при оцінці компонентів радіоелектронного обладнання.

Значна кількість людей регулярно користується комп’ютером, не замислюючись про можливість зіткнутися з ситуацією, коли їхній комп’ютер раптово вимикається та не перезавантажується. Ця проблема зазвичай виникає, коли нещодавно сконструйований або оновлений комп’ютер не вмикається або коли робочий комп’ютер несподівано припиняє працювати. У таких випадках вкрай важливо точно діагностувати основну проблему, оскільки ремонт не завжди може знадобитися. Тому вкрай важливо визначити можливі причини, які можуть призвести до конкретних несправностей [13]. Як відомо, компоненти персонального комп’ютера можуть псуватися через пил і несприятливі атмосферні умови. Отже, поломка апаратного забезпечення може бути пов'язана з окисленням контактів, проникненням пилу (включаючи статичну електрику), а також температурними несправностями мікросхем і роз'ємів.

Крім того, всі несправності можуть виникнути через стрибки напруги, неправильну роботу блоку живлення або недостатнє заземлення. У таких випадках рекомендується спочатку застосувати мережеві фільтри та забезпечити належне заземлення комп’ютера. Щоб розпочати діагностику несправного персонального комп’ютера, рекомендується візуально перевірити компоненти, знявши захисну кришку та уважно оглянувши їх на наявність відхилень. Крім того, слід звернути увагу на наявність запаху диму, оскільки це часто вказує на проблеми, пов’язані зі стрибками напруги. Якщо на компонентах комп'ютера немає явних ознак несправності, то необхідно перевірити надійність

підключення живлення. Якщо ця перевірка не принесла результатів, наступним кроком буде увімкнути комп’ютер і перевірити, чи правильно працюють вентилятори блоку живлення (БЖ) і кулера процесора, а також перевірити кріплення кулера. Якщо вентилятор не працює і жорсткий диск не видає звичного звуку обертання, можна зробити висновок, що несправність пов’язана з джерелом живлення [14].

Одним із методів перевірки наявності напруги на виході джерела живлення є використання тестера для вимірювання напруги на контактах системної плати, де вони з’єднані з джерелом живлення. Для додаткового підтвердження можна підключити альтернативний блок живлення для оцінки функціональності інших компонентів комп’ютера. Хоча рідко, але важливо перевірити, чи монітор отримує сигнали від відеоадаптера. Цього можна досягти шляхом перевірки наявності активних сигналів за допомогою осцилографа.

Система автоматичної діагностики комп'ютера складається з програмних, мікропрограмних і апаратних компонентів. У цій системі існують як тестові, так і системи функціональної діагностики. Перший передбачає отримання діагностичних результатів за допомогою діагностичних інструментів, тоді як другий зазвичай використовує спеціалізовані методи діагностики в середніх і великих електронних обчислювальних машинах [15]. Використання вбудованих механізмів для передачі результатів тестування зовнішнім системам для запису та аналізу результатів переважно використовується в мікроелектронних обчислювальних пристроях. Процедура діагностики включає кілька етапів, кожен з яких відрізняється напругою, що подається на відповідний пристрій або виводиться з нього. Зважаючи на безліч потенційних проблем, які можуть виникнути, не існує універсального методу комп’ютерної діагностики. Апаратний компонент комп’ютерів часто стикається з низкою повторюваних проблем, які включають: неможливість увімкнення комп’ютера; комп’ютер вмикається, але не відображає інформації на екрані; видання комп’ютером чітких звуків («писків») при включенні; помилки, що виникають в процесі запуску BIOS; несправні компоненти; перегрів комп'ютера; апаратна

несумісність різного обладнання; і значне зниження загальної швидкості системи.

Очевидно, що діагностичні процедури для комп’ютерних систем можна проводити за допомогою фізичного втручання людини, однак програмні інструменти, які все більше поширені серед користувачів комп’ютерів, функціонують як порівнянна альтернатива [16]. Ці програмні засоби являють собою набір команд, які взаємодіють з кожним компонентом комп’ютера та дають певні результати, які потім відображаються в діалоговому вікні. Система діагностичного програмного забезпечення спирається на вже існуючі дані, що стосуються нормального функціонування комп’ютерних компонентів, порівнюючи та аналізуючи ці дані, щоб остаточно продемонструвати отримані результати. Стандартні інструменти Windows пропонують засоби визначення основних атрибутів персонального комп’ютера, наприклад, використання диспетчера завдань для цієї мети (рисунок 1.2).

Існує безліч методів, комп’ютерних програм, фізичних пристроїв і веб-платформ, призначених для діагностики комп’ютерних систем. Однак фундаментальні підходи до аналізу та діагностики узгоджені для всіх цих засобів. Ці підходи передбачають необхідну перевірку компонентів системного блоку з метою виявлення будь-яких фізичних недоліків, а також використання програмних засобів для виявлення помилок і проблем, які можуть стосуватися програмного коду системних програм або характеристик апаратного забезпечення [17].

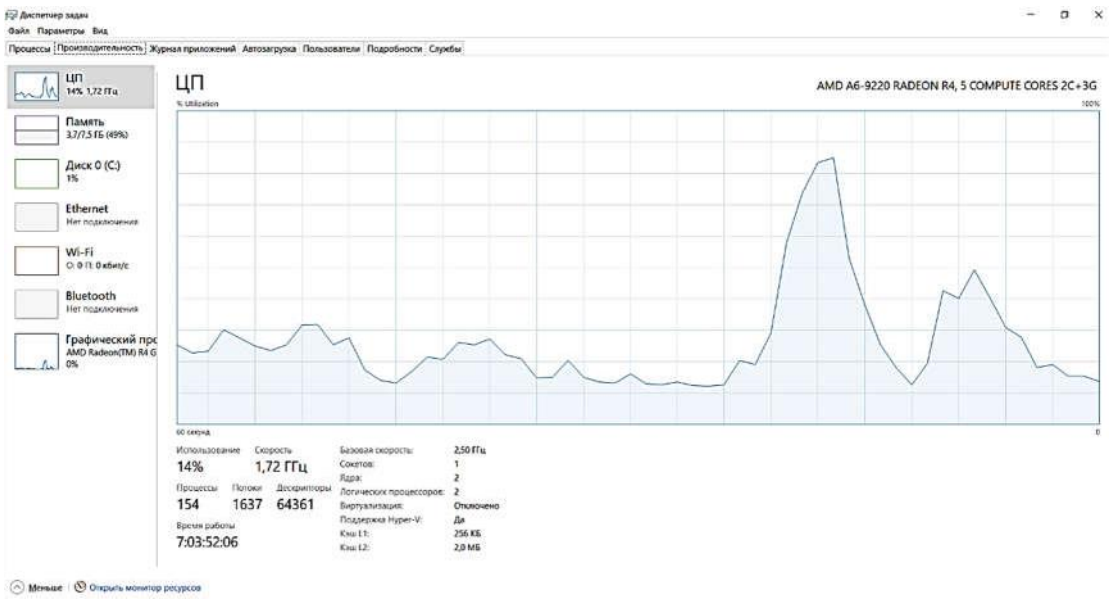

Рисунок 1.2 – Поточні характеристики комп’ютера

Аналіз комп’ютерних систем є широко вивченою та добре сприйнятою темою серед користувачів комп’ютерів. Оперативне виявлення проблем дозволяє запобігти значним проблемам і, як наслідок, уникнути дорогого ремонту. Отже, під час діагностичного процесу вкрай важливо враховувати кожен компонент, незалежно від його передбачуваної важливості. Це особливо важливо під час перевірки системних програм на потенційну присутність вірусів, оскільки вони можуть ховатися в незначних файлах і згодом завдати непоправної шкоди програмному та апаратному забезпеченню. Часто таке пошкодження системи виявляється надзвичайно складним, якщо не неможливим, для усунення.

Для вирішення даної проблеми необхідно використати модель інтелектуального класифікатора, за допомогою якого буде проведена діагностика стану мережі та визначення причини збою з подальшими рекомендаціями.

В якості простору ознак для проєктування нейромережевого забезпечення бізнес-процесів потрібно обрати показники, необхідні для оперативного визначення стану мережі.

Обов'язковою є розробка математичної основи завдання, яка стане основою для реалізації підтримки нейронних мереж.

Математична постановка завдання виглядає наступним чином:

$$| y^k | = F | x^m | \qquad (1.2)$$

Для вирішення поставленої задачі необхідно знайти відображення:

$$X_1 \subset \Re^L,\ Xn \subset \Re G,\ Y \subset \Re k, \qquad (1.3)$$

де $(X_1 \rightarrow \ldots . X^n)$ – 1, 2, … ^{n} – простір ознак,

F– способи перетворення ознак та визначення класів,

L, G – розмірність ознак в просторах 1, 2, …, *n*,

k – число досліджуваних класів (розмірність класів).

Для оцінки рівня інформативності кожного простору ознак X необхідно дослідити вплив відсутності чи наявності конкретних просторів ознак на продуктивність моделі інтелектуального класифікатора під час її розробки для діагностики стану підприємства. Усуваючи простори функцій з низькою інформативністю, мета полягає в тому, щоб досягти високоточних результатів у діагностиці стану мережі.

Проблема оцінки інформативності просторів ознак та побудова моделі на основі всіх технологій діагностики стану мережі досить складна та може зайняти багато часу. Тому в межах даної дипломної роботи необхідно визначити модель інтелектуального класифікатору нейромережевого забезпечення, адаптовану під аналіз базових показників, які дозволяють спрогнозувати можливість збою та визначити його причину. І вже на прикладі даної моделі можна буде будувати моделі з використанням значно ширших просторів ознак, які будуть базуватися на більшій кількості показників діяльності мережі з врахуванням її топології, кількості входів, рівня небезпеки тощо і надавати результати з однаково високою продуктивністю.

Розроблюваний проєкт має включати в себе створення нейромережевого аналізатора інформаційної системи підприємства для аналізу причин збою в мережі. Інформаційна система – сукупність взаємопов'язаних між собою

елементів, порушення у функціонуванні яких, або їх відсутність ведуть до порушення системи.

Одним з ефективних аспектів розвитку діяльності та вдосконалення управління є інтеграція та використання передових інформаційних технологій на підприємстві. Це передбачає виконання різних кроків, у тому числі визначення функцій, які необхідно виконати, щоб забезпечити підприємство надійною та високоякісною інформацією для прийняття рішень. Крім того, це передбачає визначення завдань, які необхідно виконати для забезпечення виконання цих функцій. Крім того, це вимагає визначення конкретних кількісних і якісних показників інформації, необхідних для належного функціонування інформаційної системи. Нарешті, це передбачає встановлення відповідних форм і методів, які використовують ці показники для успішного виконання необхідних завдань і виконання визначених функцій з метою полегшення процесу прийняття рішень.

Висновок до розділу

Стабільність роботи комп’ютерної мережі підприємства важлива для її ефективності. Несправності, спричинені зовнішніми або внутрішніми причинами, можуть порушити цю стабільність, тому важливо швидко діагностувати причину та усунути наслідки.

На даний момент використовуються дві системи виявлення атак: система виявлення аномалій та система виявлення особливостей. Але обидві системи мають свої недоліки.

Ефективним рішенням може стати комплексний підхід до боротьби з атаками, що включає системи моніторингу, зберігання історії транзакцій, створення сховищ для інтелектуального аналізу зловмисників і їх дій, а також для визначення стратегії реагування. Важливим фактором при створенні такої системи є визначення відповідної математичної підтримки для кожного етапу дослідження. Після застосування захисних заходів система повинна оцінити свою ефективність, вимірявши рівень зниження загрози.

РОЗДІЛ 2.
АНАЛІЗ ЗАСОБІВ РЕАЛІЗАЦІЇ ПОСТАВЛЕНОЇ ЗАДАЧІ

Розглядати модель аналізу навантаження до мережі доступу до інтернет-ресурсів також можна через відому математичну модель, яка має назву системи масового обслуговування.

Системи масового обслуговування відносяться до систем, які мають великий обсяг запитів на певні послуги, і спрямовані на задоволення цих запитів, щоб забезпечити задоволеність клієнтів.

Під обслуговуванням розуміється задоволення якихось потреб. Так, системою масового обслуговування (СМО) називається будь-яка система, призначена для обслуговування якогось потоку заявок (наприклад, ремонтна майстерня, телефонна станція, білетна каса тощо), зокрема і обчислювальна система [12, с. 65].

Систему масового обслуговування можна концептуалізувати як серію взаємопов’язаних вхідних потоків, черг і каналів обслуговування, які задовольняють різноманітні потреби в обслуговуванні, такі як ремонт, видача книг і запити на зліт. Крім того, система включає вихідні потоки для вимог після обслуговування.

Основні елементи СМО показано на рисунку 2.1.

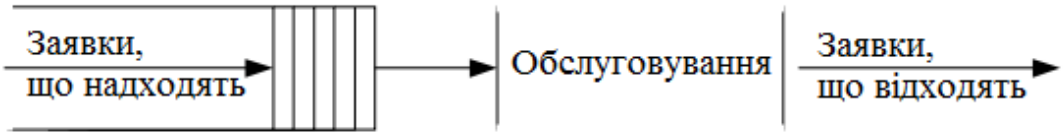

Рисунок 2.1 - Структура системи масового обслуговування

Сервісний блок в організації управління послугами (СМО) функціонує як приймач додатків, де вхідні додатки обробляються сервісним пристроєм. У випадках, коли сервісний пристрій не в змозі негайно вирішити отримані заявки, формується черга. Важливо зазначити, що не всі СМО працюють із системою

черги; деякі можуть відмовитися від вхідних запитів, якщо обслуговуючий пристрій зайнятий, тоді як інші дозволяють запитам стояти в черзі, доки обслуговуючий пристрій не стане доступним для обробки.

Процес вибору запиту на послугу в конкретний момент визначається набором вказівок, відомих як дисципліна обслуговування. Згодом запит виконується, і після надання послуги запит виходить із системи. Потік обслуговуваних запитів відіграє вирішальну роль, особливо коли він служить вхідною інформацією для іншої організації управління роботою (СМО).

Основні компоненти систем масового обслуговування включають приплив запитів, чергу обслуговування, канали обслуговування та відтік оброблених і необроблених запитів. Вхідний потік складається із запитів на послуги для задоволення конкретних потреб, тоді як черга послуг містить запити, що очікують на обробку. Канали обслуговування, що складаються з технічних ресурсів і персоналу, використовуються для розгляду та вирішення різноманітних запитів. Вихідний потік охоплює як обслуговані, так і необслужені запити, що виходять із системи обслуговування, потенційно потрапляючи в іншу систему для подальшої обробки [12, с. 73].

Існують різні класифікації систем масового обслуговування, кожна з яких характеризується окремими методами прийому запитів споживачів і управління роботою сервісного обладнання.

Щоб покращити процес моделювання, вкрай важливо використовувати категоризацію СМО на основі різних атрибутів, які узгоджуються з конкретними наборами методологій і моделей з теорії масового обслуговування. Ця категоризація спрощує ідентифікацію придатних математичних моделей для вирішення проблем, пов’язаних із послугами.

Системи масового обслуговування можна класифікувати на системи відновлення після відмови та резервні. Системи відновлення після відмови працюють за принципом безвідмовності, за яким будь-яка заявка, отримана під час періоду перевантаження каналу, відхиляється та виходить із системи. З іншого боку, системи з можливістю очікування не відхиляють такі запити;

натомість вони розміщують їх у черзі та чекають на доступність вільного каналу. Термін очікування та місткість черги можуть бути як необмеженими, так і обмеженими.

Системи масового обслуговування класифікуються на основі кількості каналів обслуговування, які вони пропонують: одноканальні системи мають лише один канал (n=1), а багатоканальні системи мають два або більше каналів (n≥2).

Одноканальний СМО — це простий метод, який можна використовувати для аналізу певних аспектів управління виробництвом. Тривалість часу обслуговування кожного замовлення непередбачувана, однак результуючий потік обслуговування характеризується інтенсивністю μ, яка визначається середнім часом обслуговування.

Вхідний потік замовлень, що характеризується параметром інтенсивності λ, спрямовується в систему, що складається з одного каналу. Замовлення, отримані під час періодів доступності системи, оперативно обробляються, тоді як будь-які замовлення, що надходять під час зайнятого каналу обслуговування, не можуть бути прийняті, і, отже, їм відмовляють в обслуговуванні.

СМО з одиночним каналом може існувати лише за однієї з двох умов: S0, що означає, що канал незайнятий, або S_1, що вказує, що канал зайнятий. Графічне зображення на рисунку 2.2 відображає можливі переходи між цими станами.

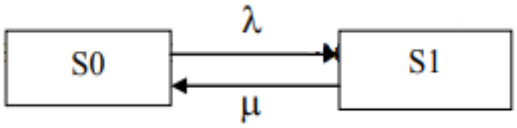

Рисунок 2.2 - Граф одноканальної СМО з відмовами

Багатоканальна СМО з відмовами формується аналогічним чином, але з більшою кількістю каналів пропуску інформації, тобто, наприклад, можна використовувати різні соціальні мережі для розповсюдження рекламних повідомлень, і якщо у певній країні стоїть заборона на дану мережу, повідомлення не пройде, бо отримає відмову, але воно може надійти через інші,

вільні канали. Багатоканальні СМО використовуються для підвищення пропускної спроможності мережі.

Так само можна інтерпретувати комунікаційний зв'язок між країнами через таку систему, де кожен канал – це певний Інтернет-ресурс, і при зверненні до нього користувачів окремої країни можна отримати відмову у доступі або ж отримати доступ.

Ефективність систем забезпечення кібербезпеки через регулювання навантаження на вузли мережі оцінюється за декількома параметрами, зокрема: кількості виявлених атак, кількості відбитих атак, масштабу наслідків атак, які не вдалось заблокувати тощо. Для перевірки ефективності існуючої системи слід провести її випробування, тобто створити штучні атаки і відслідкувати оперативність та якість реагування СЗІ на них.

Основна мета системи кібербезпеки полягає в тому, щоб сприяти досягненню цілей кібербезпеки. Отже, основну роль цієї системи можна охарактеризувати як забезпечення гармонійного співіснування інтересів особи, суспільства та держави шляхом виконання різноманітних заходів, таких як перевірки та оцінки, виявлення та розпізнавання, запобігання та припинення, а також зменшення та усунення як внутрішніх, так і зовнішніх загроз і небезпек у кіберсфері. Ці контрзаходи мають бути пропорційними характеру та масштабу, а також потенційному та бажаному рівню кібербезпеки.

Ефективність системи кібербезпеки значною мірою залежить від комплексної нормативно-правової бази, що регулює діяльність асоційованих державних і громадських установ, а також неурядових організацій [18, с. 112].

Оцінка ступеня кібербезпеки в результаті рівня захисту автоматизованих інформаційних систем проводиться за допомогою двох основних наборів показників:

1. В академічному контексті відносна кількісна оцінка стосується числового вимірювання або значення, яке потребує порівняння з іншими контрольними числами. Ці оцінки визначаються експертами. Основним завданням якісної оцінки є виявлення та вирішення помилок, які можуть

виникнути внаслідок незалежних суджень цих експертів. Метод Дельфі та його варіації широко використовуються для проведення таких оцінок. Ці оцінки можуть бути зосереджені на оцінці ефективності захисних систем, прийнятного рівня ризику, ступеня захисту, що забезпечується окремими підсистемами, і так далі.

2. Об'єктивне вимірювання інформаційної безпеки в інформаційних системах бухгалтерського обліку (AIC) може оцінити витрати з точки зору грошової вартості, виникнення негативних інцидентів або інших відповідних показників, які є вирішальними для підтримки інформаційної безпеки [9, с. 17].

Різні типи абсолютних кількісних показників можна поділити на наступні категорії:

1. Технічні:

– Кількість виявлених загроз визначає кількість загроз, які можна ідентифікувати та з якими можна впоратися. Загроза вважається ідентифікованою, якщо її характеристики відповідають опису в системі безпеки мережі;

– Якість захисту від загроз – Визначається здатністю системи безпеки мережі адекватно реагувати на виявлені загрози. Загрози виникають у вузлах зв'язку, і автоматизованим інформаційним системам важко впоратися з ними. У цьому випадку найкраще зазначити в протоколі ті дії, які здійснюються через погрози;

- Зниження загальної продуктивності інформаційної системи - відображає зниження продуктивності інформаційної системи через необхідність виконання дій, визначених політикою безпеки. Наприклад, карти шифрування зменшать швидкість передачі даних, оскільки шифрування потрібне під час передачі, розшифровка – під час отримання даних тощо [9, с 17].

2. Організаційні показники стосуються кількості персоналу, який займається підтримкою системи кібербезпеки. Реалізація заходів безпеки вимагає залучення різних ролей, таких як інженери, програмісти, системні адміністратори та менеджери безпеки ІС. Чітке розмежування обов'язків щодо

виконання функцій безпеки та нагляду за окремими аспектами системи кібербезпеки має бути визначено в посадових інструкціях для кожної групи персоналу.

3. Економічний аспект кібербезпеки включає різні показники, такі як витрати, пов’язані з розробкою, впровадженням, експлуатацією та навчанням користувачів і підтримкою системи кібербезпеки протягом її життєвого циклу. Сюди входять витрати, пов’язані з дослідженнями, придбанням технологій, спеціального обладнання, програмного забезпечення, а також оплата праці співробітників, які працюють над системою кібербезпеки. Крім того, існують витрати, пов’язані з певними матеріалами, такими як витратні матеріали, необхідні для роботи системи, як-от додаткові магнітні носії для резервного копіювання. Крім того, існують витрати, пов'язані з відновленням нормальної роботи системи після реалізації загрози, які включають витрати на інформацію, технічні ресурси, робочу силу та інші необхідні ресурси. Нарешті, коефіцієнт зменшення потенційних збитків вимірює співвідношення між зменшенням збитків і потенційною сумою збитків [9, с 17].

Висновок до розділу

Існує кілька способів оцінити ефективність системи кібербезпеки, і вони можуть оцінити рівень захисту від окремих загроз і ступінь загального захисту. Існують наступні способи та способи оцінки ефективності медичного страхування:

1) Метод багатовимірного порівняльного аналізу. Цей метод створений для визначення ступеня взаємовпливу загроз і причин їх виникнення (і як результат – оцінки ефективності системи захисту інформації);

2) Методи аналізу ризиків інформаційних систем (ІС). У наш час особливого значення при побудові СЗІ для АС набуває завдання побудови моделей інформаційних загроз. Існує багато алгоритмів аналізу ризиків інформаційних систем. Найпопулярнішими алгоритмами є CRAMM і RiskWatch. Ці алгоритми мають ряд переваг і набули широкого поширення.

Крім того, окрім визначених підходів до оцінки ефективності системи кібербезпеки, можливо використовувати методи системної багатокритеріальної оцінки, які враховують величину ризиків та оперативність протидії системі, ефективність пом’якшення ризиків та економічна доцільність роботи системи безпеки.

Найбільш новими способами аналізу та прогнозування є нейромережі, які дозволяють моделювати стан мережі з врахуванням попередніх даних про навантаження на той чи інший вузол. Такі засоби дозволяють виявити аномальне навантаження, спрогнозувати навантаження на окремий вузол мережі на основі даних про навантаження за попередні періоди тощо. Тому доцільно розглянути їх як інструмент аналізу та прогнозування.

РОЗДІЛ 3.
ДЕМОНСТРАЦІЯ ТА ВЕРИФІКАЦІЯ ОТРИМАНИХ РЕЗУЛЬТАТІВ

Для діагностики навантаження у мережах з великою кількістю користувачів та відповідно можливості збоїв з-за невідповідності пропускної здатності вузлів існує потреба у визначенні архітектури мережі та основних її вузлів, у яких може відбуватись збій. З метою забезпечення спостережливості інформації в системах обміну інформацією використовуються спеціальні програми моніторингу. Програмне забезпечення моніторингу – це програмні продукти (модулі), призначені для забезпечення спостережливості систем зв’язку, а також такі, що дозволяють реєструвати діяльність користувачів і процесів, використання пасивних об'єктів, а також однозначно ідентифікувати ідентифікатори користувачів і процесів, що беруть участь у конкретній події, з метою запобігання порушенням безпеки та/або відповідальності за певну діяльність [**Ошибка! Источник ссылки не найден.**, с. 101].

Використання програмного забезпечення моніторингу дозволяє власнику (адміністратору безпеки) автоматизованої системи зв’язку:

– виявляти (розшукувати) усі випадки несанкціонованого доступу до конфіденційної інформації з точним визначенням часу та станції мережі, з якої була здійснена спроба;

– локалізувати всі випадки спотворення (знищення) інформації;

– встановити факти несанкціонованого встановлення програмного забезпечення;

– контролювати можливість використання персональних комп’ютерів у неробочий час та визначати мету такого використання;

– виявляти всі випадки несанкціонованого використання модемів у локальній мережі шляхом аналізу фактів запуску несанкціонованих спеціалізованих програм;

– виявити випадки введення спеціальних слів і фраз на клавіатурі чи іншому кодонабірному пристрої, інші випадки спроби несанкціонованої авторизації в системі для доступу до вузлу зв’язку;

– виявити факти неправомірного використання пристроїв зв’язку;

– отримати достовірну інформацію, на основі якої буде розроблена політика інформаційної безпеки компанії;

– контроль доступу до серверів, персональних комп’ютерів, інших пристроїв комунікацій;

– провести інформаційний аудит;

– проводити дослідження виявлених інцидентів;

– проводити дослідження, пов’язані з визначенням точності, ефективності та адекватності реакцій працівників на зовнішні дії;

– визначити завантаженість комунікаційних станцій;

– розробити механізми відновлення критичної інформації після збоїв системи;

– забезпечити спостережливість системи. Саме ця властивість, залежно від якості її виконання, дозволяє певною мірою контролювати дотримання працівниками компанії встановлених правил безпечної роботи на комп’ютерах та політики безпеки. [**Ошибка! Источник ссылки не найден.**, с. 102].

Існують три основні рішення захисту від атак: програмні, апаратні, хмарні.

Програмні рішення – найпопулярніші на ринку, вони представляють собою набір засобів фільтрації трафіку, які складені розробником з використанням особистого досвіду. Дане рішення є досить простим у використанні, але допоможе тільки від малопомітних атак виду вандалізм.

Апаратні рішення – представляють собою створення розподіленої мережевої структури з великим запасом пропускного трафіку. Використовуються в масштабних мережевих структурах, таких як: точки обміну трафіком, дата-центри, великі регіональні провайдери [**Ошибка! Источник ссылки не найден.**, с. 230].

Хмарні рішення представлені у вигляді мережевих структур з великою пропускною здатністю, до складу якої вводяться сервери для фільтрації шкідливого трафіку. Таким чином, така мережа поступово буде фільтрувати шкідливий трафік і знижувати кількість шкідливих пакетів [**Ошибка! Источник ссылки не найден.**, с. 231].

Зараз використовуються два типи систем виявлення: системи виявлення аномалій і системи виявлення особливостей. Однак основним недоліком систем виявлення функцій є те, що вони спеціально розроблені для виявлення конкретних типів атак, як правило, тих, які вважалися найнебезпечнішими на момент розробки системи. Це може стати проблемою, коли виникають нові атаки або коли відбуваються зміни в параметрах руху, оскільки процес виявлення потребує переадресації та вирішення ще раз. Системи виявлення аномалій (через складність моделювання нормального інтернет-трафіку) використовують різні припущення щодо функціонування системи, наприклад, статистичну однорідність трафіку. Проте обсяг комп'ютерних систем, до яких застосовні ці припущення, і конкретні умови, необхідні для їх реалізації, не були ретельно вивчені або окреслені. Отже, навіть незначні зміни в моделях трафіку або пропонованих послугах можуть вимагати перенавчання алгоритму виявлення. Щоб вирішити цю проблему, одним із потенційних рішень є застосування комплексного підходу до побудови надійної системи захисту від атак. Цей підхід включатиме різні компоненти, такі як системний моніторинг, запис і зберігання історії транзакцій, підтримку спеціального сховища для інтелектуального аналізу зловмисників та їхньої поведінки, а також формулювання ефективної стратегії протидії.

Крім того, буде створено окреме сховище для зберігання детальної інформації про роботу системи. Цей репозиторій слугуватиме цінним ресурсом для розуміння та аналізу функціонування системи, дозволяючи краще ідентифікувати потенційні вразливості та області, які потрібно покращити. Крім того, буде створено ще одне сховище для розміщення аналітичних компонентів, спеціально розроблених для виявлення загроз і виявлення ознак шкідливої

діяльності. Ці компоненти використовуватимуть складні алгоритми та методи для аналізу зібраних даних і надання сповіщень і попереджень у реальному часі, коли виявлено потенційні загрози. Нарешті, буде застосовано низку надійних заходів для протидії та пом’якшення будь-яких атак, які можуть виникнути. Ці заходи включатимуть різні протоколи безпеки, методи шифрування, системи виявлення вторгнень і брандмауери, серед іншого. Використовуючи ці заходи, система захисту забезпечить цілісність і безпеку системи, захищаючи від будь-яких потенційних порушень безпеки або несанкціонованого доступу. Висунуто пропозицію створити комплексну систему захисту, що складається з кількох ключових елементів. По-перше, агенти стеження будуть розгорнуті для моніторингу та відстеження різноманітних дій у системі. Ці агенти збиратимуть цінні дані, які далі оброблятимуться та зберігатимуться за допомогою передових засобів попередньої обробки та зберігання. Підсумовуючи, запропонована система захисту використовуватиме комплексний підхід, що включає агенти відстеження, заходи попередньої обробки та зберігання, сховища для інформації про роботу системи та виявлення загроз, а також потужні заходи проти атак. Завдяки впровадженню цих елементів система буде обладнана для ефективного захисту від зловмисних дій і забезпечення загальної безпеки та стабільності системи [2; с. 572].

Перший етап — це відстеження трафіку, що передбачає захоплення пакетів для оцінки обсягу потоку даних, складу трафіку та активності користувача. Щоб виконати це завдання, необхідно розробити алгоритми, які можуть визначати оптимальну кількість і частоту захоплення пакетів на основі таких факторів, як завантаження каналу та інших відповідних параметрів. Важливо знайти баланс, тому що якщо пакети перехоплюються занадто часто, це може перешкоджати безперебійному потоку трафіку. І навпаки, якщо пакети перехоплюються через постійні проміжки часу, це може призвести до «сліпих зон», де певні дані не повідомляються або не враховуються. [2; с. 572].

Початковий крок у процесі передбачає попередню обробку перехоплених пакетів з подальшою оцінкою найбільш критичних загроз і збереженням зібраної

інформації. Оскільки цей етап потребує швидкої оцінки з використанням мінімальних ресурсів, доцільно використовувати прості та адаптовані порогові значення або, якщо необхідно, послідовний CUSUM.

Важливим є процес аналізу даних під час їх завантаження в пам'ять, виявлення потенційних атак і оцінка рівня загрози. Коли інформацію буде збережено в сховищі, дуже важливо провести ретельну оцінку, щоб визначити можливі ризики. Щоб досягти цього, рекомендується використовувати багатоканальний CUSUM і алгоритми ковзного середнього, які були описані раніше. Ці алгоритми забезпечують надійний і ефективний засіб аналізу даних і виявлення будь-яких потенційних загроз або вразливостей. Використовуючи ці методи, організації можуть забезпечити безпеку та цілісність своїх даних і приймати обґрунтовані рішення для пом’якшення будь-яких ризиків, які можуть виникнути.

Аналіз фонових даних виконується на регулярній основі або за заздалегідь визначеним розкладом, щоб ідентифікувати різні типи атак, як-от спроби сканування, атаки деградації та імпульсні атаки. Оскільки ці атаки вважаються менш шкідливими, тепер необхідно провести більш детальний аналіз. Це передбачає використання методів аналізу даних, інтелектуальних систем правил, нейронних мереж та інших передових методів.

Щоб створити випадки використання, важливо ідентифікувати залучених осіб або організації. У разі розробки програмного забезпечення для виявлення вторгнень основним користувачем системи є адміністратор. Це програмне забезпечення спеціально розроблено, щоб допомогти адміністратору відстежувати та виявляти будь-які випадки збоїв у мережі. Таким чином, адміністратор є єдиним учасником цієї системи, як показано на рисунку 3.1 [10, 18].

Детальний опис варіантів використання наведено в табл. 3.1 – 3.4.

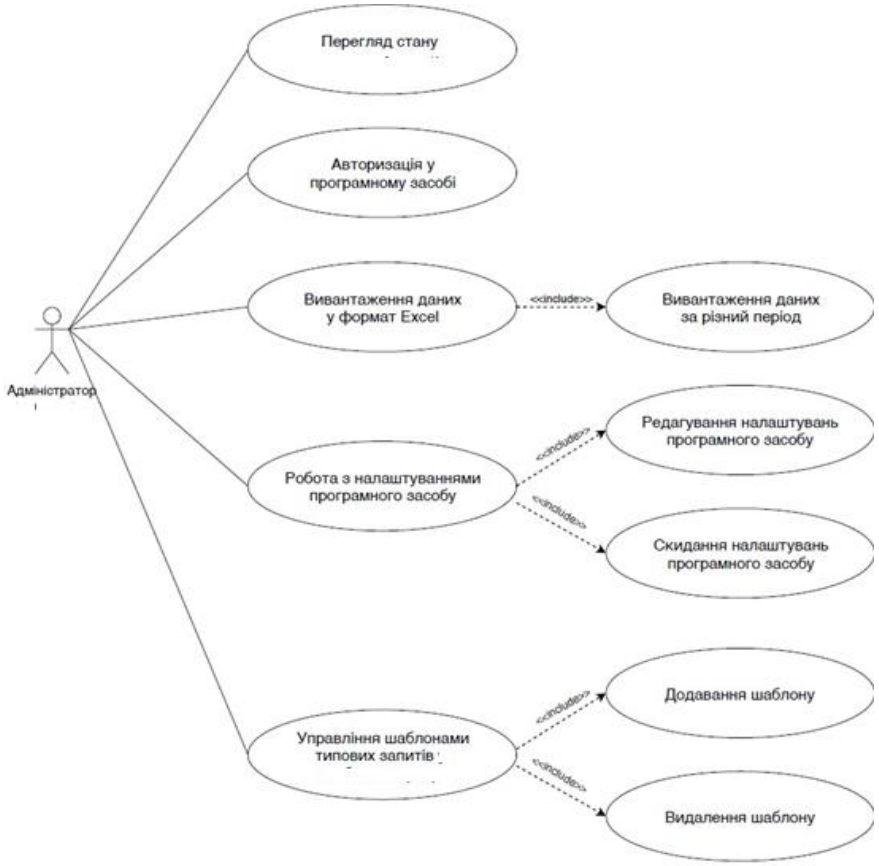

Рисунок 3.1 - Структурна схема варіантів використання програмного забезпечення для виявлення можливих збоїв

Логічна структура складається з різних функціональних і логічних модулів, які складаються з процедур і об'єктів, які служать стандартизованими моделями для додатків баз даних. Ці модулі містять форми, вікна для перегляду таблиць бази даних, звіти, запити та інші компоненти. Крім того, логічна структура включає в себе унікальні програмні блоки, які призначені для автоматизації конкретних функцій або завдань у предметній області, що вивчається [19].

Таблиця 3.1 -Варіант використання «Авторизація на сторінці перегляду стану мережі»

Найменування	Авторизація на сторінці перегляду стану мережі
Первинний актор	Адміністратор
Інші актори	Немає
Опис	Можливість авторизуватись на сторінці перегляду

Продовження таблиці 3.1

	стану системи
Попередні умови	Відкрита сторінка перегляду стану мережі
Вихідні умови	Відкрита сторінка перегляду стану мережі

Таблиця 3.2 - Варіант використання «Створення налаштувань програмного засобу діагностики причин збоїв»

Найменування	Створення налаштувань програмного засобу
Первинний актор	Адміністратор
Інші актори	Немає
Опис	Можливість налаштувати програмне забезпечення
Попередні умови	Відкрита сторінка налаштувань програмного засобу та адміністраторавторизований
Вихідні умови	Прийняті налаштування програмного засобу

Таблиця 3.3 - Варіант використання «Вивантаження даних про збої у форматі Excel»

Найменування	Вивантаження даних про причини збоїв у форматі Excel
Первинний актор	Адміністратор
Інші актори	Немає
Опис	Можливість вивантаження даних про виявлені вразливості у форматі Excel
Попередні умови	Відкрита сторінка перегляду виявлених причин
Вихідні умови	Сформований файл у форматі Excel

Таблиця 3.4 - Варіант використання «Перегляд стану мережі»

Найменування	Перегляд стану мережі
Первинний актор	Адміністратор
Інші актори	Немає
Опис	Можливість перегляду стану мережі

Продовження таблиці 3.4.

Попередні умови	Відкрита сторінка перегляду стану мережі та адміністратор авторизований
Вихідні умови	Перегляд стану мережі

Логічна структура складається з різних функціональних і логічних модулів, які складаються з процедур і об'єктів, які служать стандартизованими моделями для додатків баз даних. Ці модулі містять форми, вікна для перегляду таблиць бази даних, звіти, запити та інші компоненти. Крім того, логічна структура включає в себе унікальні програмні блоки, які призначені для автоматизації конкретних функцій або завдань у предметній області, що вивчається [19].

На рисунку 3.2 зображено структурну схему класів програмного засобу, яка представлена за допомогою відповідної UML-діаграми [10, 20].

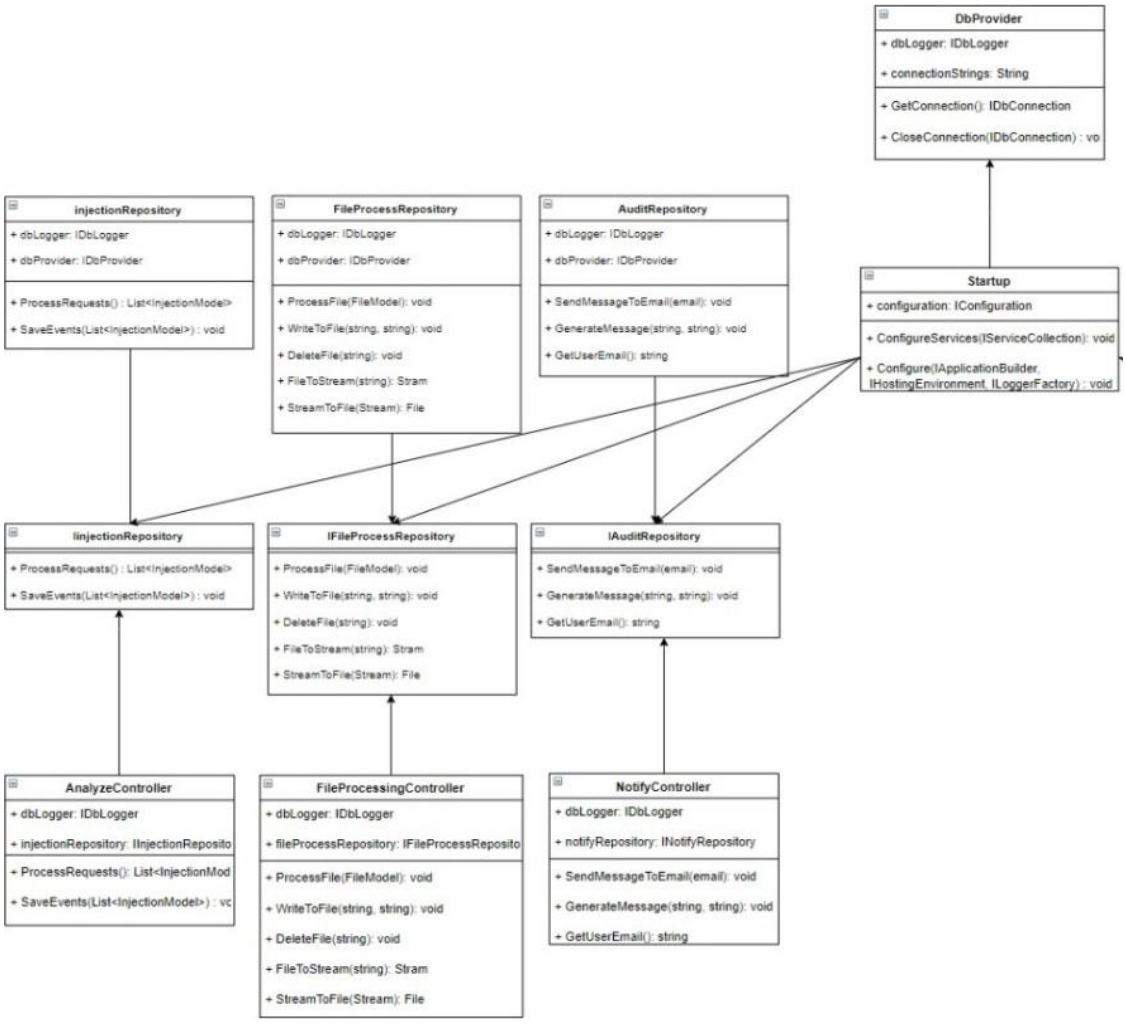

Рисунок 3.2- Структурна схема класів програмного засобу

Запропонована модель була оцінена за допомогою метрики оцінки точності, яка вимірює частку правильно класифікованих прогнозів. Цей показник вважає істинні позитивні та істинні негативні результати правильно класифікованими, а хибнопозитивні та хибнонегативні результати класифікованими неправильно. Модель рекурентної нейронної мережі оцінювалася за допомогою традиційних класифікаторів машинного навчання, зокрема SVM і Random Forest, у контексті використання кібербезпеки, що включає алгоритми, створені доменом (DGA). Три моделі було навчено та випробувано на наборі даних, пов'язаних із доменами шкідливих програм. У таблиці 3.5 представлено докладні результати моделей RNN та інших моделей машинного навчання для цього конкретного сценарію.

Таблиця 3.5 - Результати тесту різних видів алгоритмів виявлення

Алгоритми	Задача	Точність, %	Фактично	Відгук	F-score
SVM	Оцінка навантаження на вузол мережі	0,985	0,699	0,489	0,389
Random forest	Оцінка навантаження на вузол мережі	0,994	0,761	0,992	0,95
RNN з LSTM	Оцінка навантаження на вузол мережі	0,997	1,00	1,00	1,00
RNN (шарова нормалізація)	Оцінка навантаження на вузол мережі	0,994	0,98	0,88	0,99
RNN (пакетна нормалізація)	Оцінка навантаження на вузол мережі	0,946	0,95	0,94	0,94

Тому було проведено дослідження щодо застосування повторюваних нейронних мереж (RNN) у безпеці мережі, зокрема в області виявлення шкідливих програм. Ефективність RNN порівнювали з традиційними класифікаторами машинного навчання, такими як Support Vector Machines (SVM) і Random Forest, для класифікації шкідливих програм у сфері кібербезпеки. Результати цього дослідження демонструють, що RNN перевершує класичні класифікатори машинного навчання з точки зору точності. Це можна пояснити властивою RNN здатністю пам’яті, що дозволяє зберігати та згадувати кілька попередніх станів і витягувати важливі характеристики, а також складні послідовні зв’язки в даних. Отже, RNN з LTSM має переважне значення для розробки програм реального часу, спрямованих на аналіз шкідливих дій у мережах.

Для побудови нечіткої системи на основі розробленого алгоритму потрібно для початку задати вхідні дані, а також кінцевий результат. На вході було задано наступні значення:

- температура;
- швидкодія;
- навантаженість.

На виході отримано загальний стан системи, який напряму залежить від значень вхідних даних. База правил системи нечіткого виводу призначена для формального подання емпіричних знань або знань експертів в тій чи іншій проблемній області. У системах нечіткого виведення використовуються правила нечітких продукцій, в яких умови і укладення сформульовані в термінах нечітких лінгвістичних висловлювань. База правил нечітких продукцій – це кінцева множина правил нечітких продукцій, узгоджених щодовикористовуваних в них лінгвістичних змінних. Найчастіше база правил представляється в формі певного структурованого тексту. На рисунку 3.3 показано загальний вигляд розробленої нечіткої системи.

Далі для кожного з входів, а також для виходу необхідно створити функції належності. Для входів було обрану функції типу “gbellmf”, адже вонидозволяють

краще візуально показати зміну значень. Для виходу застосовуються функції типу “trimf”. Для подальшої роботи потрібновизначитись в яких межах значень будуть коливатись вхідні та вихідні дані.

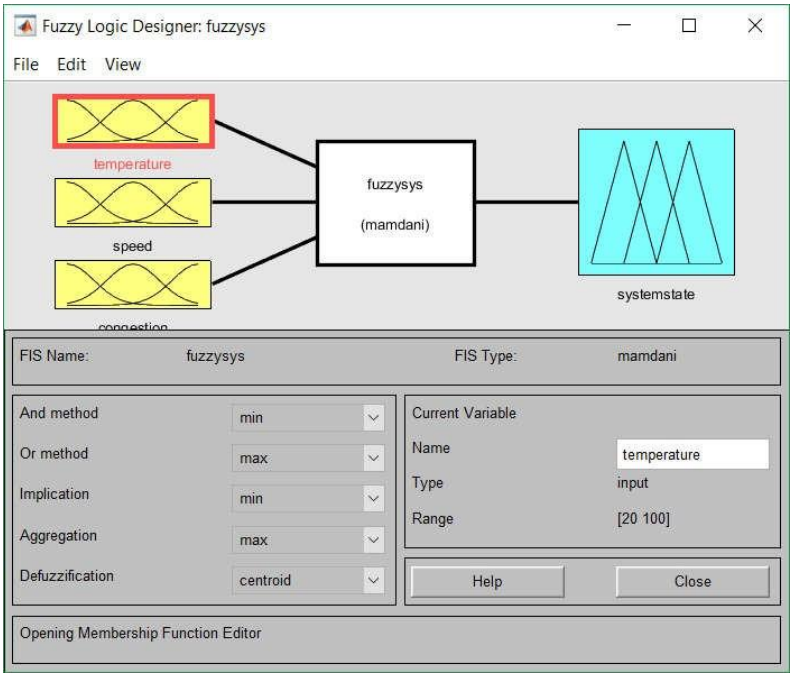

Рисунок 3.3 – Входи розробленої системи діагностики стану системи

Проаналізувавши роботу комп’ютерних систем для входів було призначено межі, а саме для температури від 20˚С до 100˚С:

– до 35˚С – температура в нормі;
– до 70˚С – температура підвищена;
– більше 70˚С – висока температура.

Для швидкодії від 0 до 1:

– від 0 до 0,5 – висока швидкодія;
– від 0,4 до 0,7 – нормальна швидкодія;
– від 0,6 до 1 – низька швидкодія.

Для навантаженості від 0 до 200:

– від 0 до 80 – низька навантаженість;
– від 70 до 140 – середня навантаженість;
– від 130 до 200 – висока навантаженість.

Для загального стану системи було умовно встановлено шкалу від 0 до 10:

– від 0 до 3 – відмінний стан;

– від 3 до 7 – нормальний стан;

– від 7 до 10 – поганий стан.

Нечіткий вивід моделі вибору стану комп’ютерної системи, побудованого на основі заданих правил з поточними значеннями змінних має вигляд, представлений на рисунку 3.4.

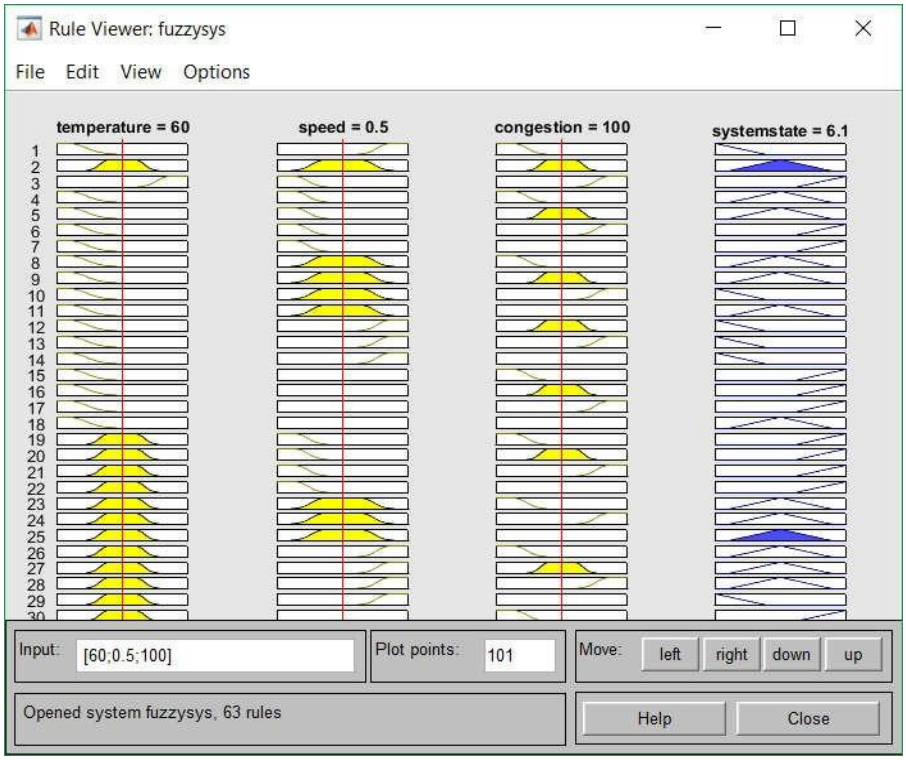

Рисунок 3.4 – Графічне зображення правил нечіткої системи

На рисунках 3.5, 3.6 та 3.7 графічно зображені значення вхідних змінних системи, а також вихідної змінної, яка і показуєрезультат роботи і дозволяє визначити загальний стан досліджуваної системи.

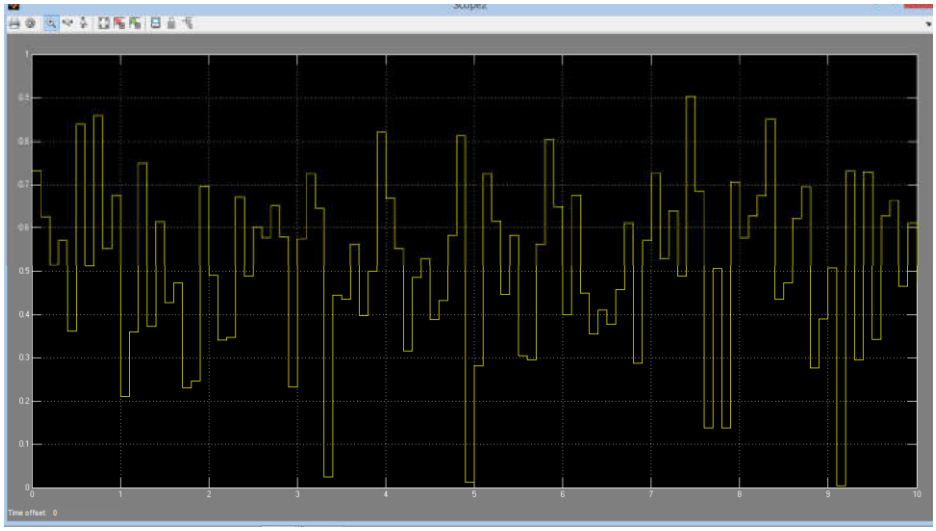

Рисунок 3.5 – Значення вхідної змінної швидкодії мережі

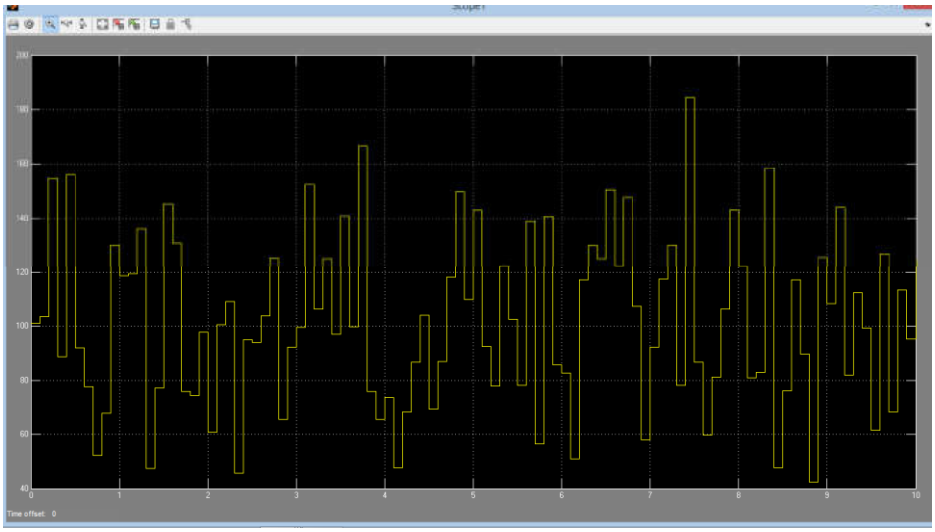

Рисунок 3.6 – Значення вхідної змінної завантаженості на вузлах зв’язку

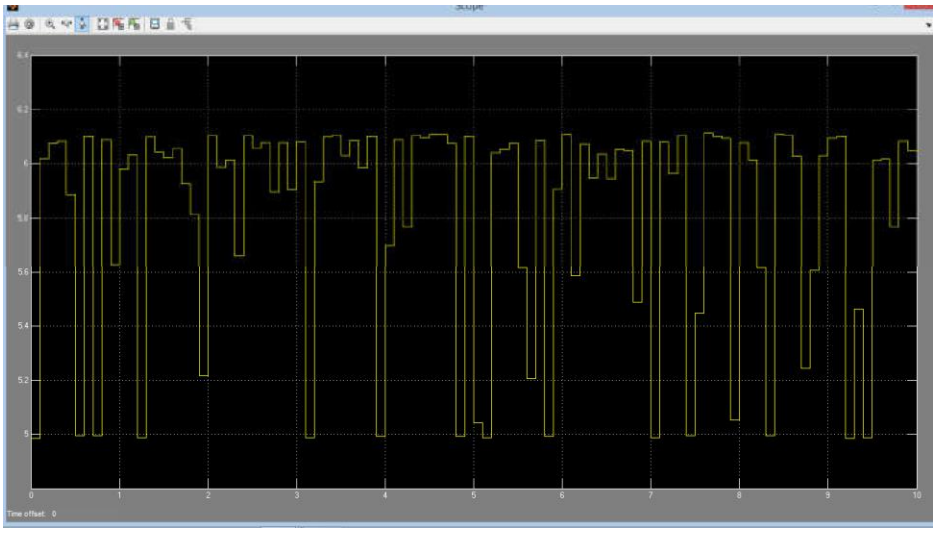

Рисунок 3.7 – Значення виходу нечіткого контролера (стан системи)

Висновки до розділу

Є три основні рішення для захисту від атак: програмне, апаратне та хмарне. Програмні рішення є найпопулярніші на ринку, але вони можуть допомогти лише проти малопомітних атак. Апаратні рішення дозволяють створювати розподілені мережеві структури з великою пропускною здатністю. Хмарні рішення представлені у вигляді мережевої структури з високою пропускною здатністю, яка включає сервери для фільтрації шкідливого трафіку.

Для побудови нечіткої системи на основі розглянутого алгоритму задаються вхідні дані та кінцевий результат. Входи регулюються температурою, швидкістю та навантаженням. На виході відображається загальний стан системи.

Отже, результати стану системи на певний момент доволі легко отримати та відстежити. Достатньо лише щоб контролер зчитав значення з входів, опрацював їх за допомогою бази правил, методів фазифікації та дефазифікації і тоді, як результат, на виході ми отримуємо чітко структуровані значення в певних межах, які і дозволяють визначити кінцевий стан систем.

ВИСНОВКИ

В 2 розділі роботи був викоканий аналіз до мережі доступу до інтернет-ресурсів за математичною моделлю, яка має назву системи масового обслуговування (СМО). Системи масового обслуговування є важливим інструментом для аналізу завантаженості мереж. Вони дозволяють моделювати велику кількість запитів на конкретну послугу і спрямовані на задоволення цих запитів для забезпечення задоволеності клієнтів. СМО можуть бути одноканальними(має лише одни канал, і запити, що надходять під час зайнятого каналу не приймаються) або багатоканальними(має 2 або більше каналів і може обробляти більше запитів одночасно).Ефективність системи кібербезпеки можна оцінити за допомогою різних методів, включаючи технічні, організаційні та економічні показники. Технічні показники включають кількість виявлених загроз та якість захисту від них; організаційні- кількість персоналу, який бере участь у підтримці системи; економічний- витрати пов’язані з розробкою, впорядженням, експлуатацією та навчанням користувачів, а також підтримку систем кібербезпеки. Таким чином, СМО є важливим інструментом для аналізу навантаження на мережі доступу до інтернет-ресурсу.

У 3 розділі розглядається важливість моніторингу та діагностики в мережі з великою кількістю користувачів. Через можливі збої, спричинені великою кількістю користувачів та невідповідністю пропускної здатності вузлів, необхідно визначити архітектуру мережі та основні вузли, які можуть вийти з ладу. З цією метою використовуються спеціальні програми моніторингу, які забезпечують спостереження за системами зв’язку, реєструють діяльність користувачів і процесів, а також допомагають однозначно ідентифікувати ідентифікатори користувачів і процесів, що беруть участь в певних подіях.

У цьому розділі також розглядаються 3 основні рішення для захисту від атак: програмне, апаратне та хмарне. Програмні рішення є найпопулярніші на ринку, але вони можуть допомогти лише проти малопомітних атак. Апаратні рішення дозволяють створювати розподілені мережеві структури з великою

пропускною здатністю. Хмарні рішення представлені у вигляді мережевої структури з високою пропускною здатністю, яка включає сервери для фільтрації шкідливого трафіку. Використовуються два типи систем виявлення: система виявлення аномалій та система виявлення особливостей. Однак обидва типи систем мають свої недоліки.

Для побудови нечіткої системи на основі розглянутого алгоритму задаються вхідні дані та кінцевий результат. Входи регулюються температурою, швидкістю та навантаженням. На виході відображається загальний стан системи.

База правил системи нечіткого виводу призначена для формального подання емпіричних знань або знань експертів.

Легко отримувати і відстежувати результати поточного стану системи. Контролер зчитує значення з вхідних даних і обробляє їх з використанням бази даних правил, методів фазифікації та дефазифікації і на виході отримуємо чітко структуровані значення в певних межах, що дозволить визначити кінцевий стан системи.

Таким чином, у цьому розділі пояснюється важливість моніторингу та діагностики мережі, а також різні способи захисту від атак та систем виявлення.

Досліджено підходи до аналізу та прогнозування навантаження на вузли мереж з великою кількістю користувачів. Такі мережі часто піддаються зовнішньому впливу (кібератаки, які підвищують навантаження на вузли зв’язку і виводять їх з ладу), а також можуть мати збої з-за невідповідності пропускної здатності вузлів запланованому чи фактичному навантаженню. Тому дослідження навантаження на вузли, прогнозування майбутнього навантаження на основі попередніх даних, запобігання кібератакам шляхом моніторингу аномальних навантажень тощо, є важливими задачами адміністрування комп’ютерної мережі.

В дипломній роботі було розглянуто різні алгоритми аналізу та прогнозування навантажень, зокрема, як суто математичні алгоритми (система масового обслуговування), так і елементи нечіткої логіки та використання нейромережевих аналізаторів стану мережі. У результаті було визначено, що

оптимальною є рекурентна нейромережа з аналізом часових рядів, яка дозволяє на основі попередніх даних про навантаження на вузли мережі спрогнозувати регламентоване навантаження і дати інформацію про можливі аномальні відхилення у разі виявлення, що можна використати як детектор кібератаки на вузол мережі або запобігання іншій небажаній активності (підвищення температури вузла, яке призведе до збою, тощо).

Отже, запропонована система аналізу та прогнозування навантаження на вузли багатокористувацької мережі є ефективним інструментом адміністрування комп’ютерних мереж і може бути застосована як на підприємствах з великою кількістю користувачів мережі, так і при розробці веб-застосунків.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Андон П.І., Ігнатенко О.П. Атаки на відмову в мережі Інтернет : опис проблеми та підходів до її вирішення. Київ. : Ін-т ПС, 2008. 52 с.

2. Андон П.І., Ігнатенко О.П. Протидія атакам на відмову в мережі інтернет: концепція підходу. Проблеми програмування. 2008. № 2-3. с. 564-574.

3. Антонюк П.Є. Класифікація ймовірних способів вчинення атак на інформацію як напрям протидії комп'ютерній злочинності. URL: http://www.nbuv.gov.ua/portal/Soc_Gum/bozk/19text/g1927.htm.

4. Бабенко Т.В. Дослідження ентропії мережевого трафіка як індикатора DDoS-атак. Науковий вісник НГУ. 2013. № 2. с. 86-89.

5. Багнюк Н.В., Мельник В.М., Клеха О.В. Види DDoS-атак та алгоритм виявлення DDoS-атак типу Flood-атак. Комп'ютерно-інтегровані технології: освіта, наука, виробництво. 2015. № 18. с. 6-12.

6. Бевз О.М., Папінов В.М., Скидан Ю.А. Проєктування програмних засобів систем управління. URL: http://posibnyky.vntu.edu.ua/bevz/

7. Воронов М.П. Інформаційне забезпечення діяльності місцевих органів держав ної влади та органів місцевого самоврядування. Державне управління та місцеве самоврядування. 2011. Вип. 2, ч. 2. С. 106–108.

8. Гаман Т.В. Вдосконалення організаційно-правового механізму інформаційної діяльності місцевих державних адміністрацій : дис. ... канд. наук з держ. упр.: 25.00.02. Л., 2006. 246 с.

9. Гарасимчук О.І., Костів Ю.М. Оцінка ефективності систем захисту інформації. Вісник КНУ імені Михайла Остроградського. 2016. № 1. с. 16–20.

10. Гвозденко М.В., Чобу Я.В. Технічні та програмні засоби виявлення джерела DDoS-атаки. GLOBAL SCIENTIFIC UNITY. 2014. с. 106-115.

11. Геєць В.П., Клебанова Т.С., Іванов В.В. Моделі й методи соціально-економічного прогнозування. Харків: Вид-во ХДЕУ, 2003. 422 с.

12. Гнатюк С. Є. Математичні моделі оцінки та прогнозування надійності програмно-керованих засобів захисту інформації в системі урядового зв'язку. Ukrainian Information Security Research Journal. 2016. № 2. с. 150-156.

13. Гордієнко І.В. Інформаційні системи і технології в менеджменті. 5-ге вид., перероб. і допов. Київ.: КНЕУ, 2013. 279 с.

14. Грайворонський М.В., Новиков О.М. Безпека інформаційно-комунікаційних систем / за заг. ред. Академіка НАН України М. З. Згуровського. Київ. : BHV, 2009. 608 с.

15. Гриценко О. Природа інформаційного суспільства та розвиток світового ринку мас-медіа. Вісник Львівського університету. 2009. № 32. С. 214-222.

16. Грищук Р. В. Атаки на інформацію в інформаційно-комунікаційних системах. Сучасна спеціальна техніка. 2011. № 1(24). С. 61-66.

17. Грищук Р. В. Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень : моногр.. Житомир : Рута, 2010. 280 с.

18. Діордіца І. Система забезпечення кібербезпеки: сутність та призначення. Інформаційне право. 2017. № 7. С. 109-116.

19. Дубовой В.М., Москвіна С.М., Никитенко О.Д. Моделювання процесів і систем керування. Вінниця, ВНТУ, 2009.103 с.

20. Єрмошин В.В., Хорошко В.О., Капустян М.В. Методика оцінки інформаційних ризиків системи управління інформаційною безпекою. Сучасний захист інформації. 2010. №3. С. 95-104.

21. Журавель Н. О. Організаційна регламентація бізнес-процесів як умова забезпечення їх ринкової безпеки. Управління розвитком. 2014. № 2. с. 121-124.

22. Ілляшенко С. М. Економічний ризик: навч. посіб. К.: Центр навчальної літератури, 2014. 220 с.

23. Квєтний Р. Н., Коцюбинський В. Ю., Кислиця Л. М., Казимірова Н. В., і Кириленко Г. О., Адаптивна система підтримки прийняття рішень з використанням методів нечіткого логічного висновку. НаукПраці ВНТУ, вип. 3, Лис 2011. С. 1-10.

24. Козенков Д.Е. Проєктування бізнес-процесів як основа створення архітектури підприємства. Вісник СумДУ. Серія Економіка. 2011. № 3. с. 126-136.

25. Кравець П., Киркало Р. Системи прийняття рішень з нечіткою логікою. Вісник НУ «Львівська політехніка». 2009. № 650. с. 115-123.

26. Лаврінський Г.В. Моделювання системних характеристик в економіці /Г.В. Лаврінський, О.С. Пшенишнюк, С.В. Устинко, О.Д. Шарапов. Київ.: ЕКМО, 2004. 169с.

27. Лазарєв Ю. Ф. MATLAB і моделювання динамічних систем. Навчальний посібник. Глава 3. Пакет програм Simulink. Київ: НТУУ «КПІ», 2009. 79 с.

28. Моделювання бізнес-процесів/ уклад. О. І. Подоляка, К.М. Жулінська. Суми : ДВНЗ “УАБС НБУ”, 2013. 20 с.

29. Нейромережева методологія розпізнавання інтернет-орієнтованого шкідливого програмного забезпечення. URL: http://jrnl.nau.edu.ua/index.php/Infosecurity/article/view/4688

30. Нейронні мережі. STATISTICA Neural Networks: Методологія і технології сучасного аналізу даних / за редакцією В. П. Боровикова. 2-е вид. , перероб. і дод. К.: Телеком, 2008. 392 с.

31. Нечітка логіка на прикладах. iSearch. URL: http://www.isearch.kiev.ua/index.php/uk/internetsecurity/837–fuzzy–message

32. Писаревський І. М., Нохріна Л.А., Познякова О.В. Менеджмент організацій: Навчальний посібник. Харків: ХНАМГ, 2018. 133с.

33. Плескач В.Л., Рогушина Ю.В., Кустова Н.П. Інформаційні технології та системи: підруч. для студ. екон. спец. К.: Книга, 2018. 520 с.

34. Пономаренко В. С., Мінухін С. В., Знахур С. В. Теорія та практика моделювання бізнес-процесів: монографія. Харків: Вид. ХНЕУ, 2013. 244 с.

35. Ромашко С.М. Опорний конспект лекцій з дисципліни «Інформаційні системи в менеджменті». Львів: ЛІМ, 2017. 49с.

36. Системи підтримки прийняття рішень : навчальний посіб- ник для самостійного вивчення дисципліни / уклад.: С. М. Братушка, С. М. Новак, С. О. Хайлук. Суми : ДВНЗ «УАБС НБУ», 2010. 265 с.

37. Субботін С. О. Подання й обробка знань у системах штучного інтелекту і підтримки прийняття рішень: Навчальний посібник. Запоріжжя: ЗНТУ, 2008. 341 с.

38. Субботін С.О., Корнієнко О.В. Нейромережеве моделювання залежностей результатів випробувань газотурбінних авіадвигунів. Автоматизація технологічних і бізнес-процесів. 2018. № 10. с. 9-16.

39. Твердохліб М.Г. Інформаційне забезпечення менеджменту : Навч. посібник. Київ.: КНЕУ, 2012. 224 с.

40. Хмельов О.Г. Моделювання процесів бізнес-прогнозування за допомогою нейромережевих структур. URL: http://www.economy.nayka.com.ua/?op=1&z=38

41. Цмоць О.І., Маршук А.А. Прогнозування фінансового стану підприємства за допомогою штучних нейронних мереж. Науковий вісник НЛТУ України, 2011. Вип. 21.9. с.347-352.

42. Яремко С., Кузьміна О., Новицький Р. Використання технологій штучного інтелекту для прогнозування бізнес-процесів. Комп'ютерно-інтегровані технології: освіта, наука, виробництво. 2021. № 43. с. 230-235.

43. Ясинська Н.А., Івченкова О.Ю. Використання нейронних мереж в моделюванні фінансових результатів бізнес-процесів. Світ фінансів. 2019. № 3(60). с. 108-120.

44. A fuzzy expert system for automatic seismic signal classification. URL: https://www.sciencedirect.com/science/article/pii/S09574114053

45. A novel fuzzy decision–making system for CPU scheduling algorithm. URL: https://link.springer.com/article/10.1007/s00521–015– 1987–8

46. Abadeh M., Habibi L., Kortos N. Intrusion Detection Using a Fuzzy Genetics–Based Learning. Deli, 2007. P. 314–318.

47. Classification of Network Traffic Using Fuzzy Clustering for Network Security. URL: https://link.springer.com/chapter/10.1007/978– 3–319–62701–4_22

48. Computer Aided Development of Fuzzy, Neural and Neuro–Fuzzy Systems. URL: https://www.researchgate.net/publication/312590719_Computer_Aided_Development_of_Fuzzy_Neural_and_Neuro–Fuzzy_Systems

49. Diagnosing computer hardware failures using expert system (rule–based technique). URL: https://www.researchgate.net/publication/79205502_DIAGNOSING_COMPUTER_HARDWARE_FAILURES_USING_EXPERT_SYSTEM_RULEBASED_TECHNIQUE

50. Expert diagnosis of computer systems, neuro–fuzzy knowledge base. IEEE: web–site. URL: https://ieeexplore.ieee.org/document/metrics#metrics

51. Expert evaluation model of the computer system diagnostic features. URL: https://ieeexplore.ieee.org/document/7027101/metrics

52. Mamdani, E.H., Assillan, S.: An experiment in linguistic synthesis with a fuzzy logic controller.Int. J. Man-Mach. Stud. 7(1), 1–13, 1975.

53. Network–based output tracking control for T–S fuzzy systems using an event–triggered communication scheme. URL: https://www.sciencedirect.com/science/article/pii/S0165011032

54. Simulation and Model–Based Design. Mathworks: web–site. URL: https://www.mathworks.com/simulink.html(дата звернення: 16.10.2023).

55. Stuart Russell and Peter Norvig Artificial Intelligence: A Modern Approach: Fourth edition (2020). Hoboken: Pearson. https://lccn.loc.gov/2019047498.

56. The neuro–fuzzy diagnostic model synthesis with hashed transformation in the sequence and parallel mode. URL: https://ric.zntu.edu.ua/article/view/101022/96247(дата звернення: 02.10.2023).

57. Usability Determination Using Multistage Fuzzy System. Sciencedirect: web–site. URL: https://www.sciencedirect.com/science/article/pii/S1842 (дата звернення: 08.10.2023).

58. Yu.Yu. Gromov, O.G. Ivanova, V.V. Alekseev and ets. Intelligent information systems and technologies: textbook. Tambov: FGBOU VPO «TSTU», 2013. 244 p.