НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НН Інститут прикладного системного аналізу
Кафедра математичних методів системного аналізу

До захисту допущено:

Завідувач кафедри

_____ Оксана ТИМОЩУК

«___»_____2023р.

Дипломна робота

на здобуття ступеня бакалавра
за освітньо-професійною програмою «Системний аналіз і управління»
спеціальності 124 «Системний аналіз»
на тему: «Система підтримки прийняття рішень щодо захисту від хакерських атак»

Виконав:
студент IV курсу, групи КА-93
Болдарев Єгор Андрійович _____

Керівник:
к.т.н., старший викладач
Савченко Ілля Олександрович _____

Консультант з економічного розділу:
к.е.н., доцент
Рощина Надія Василівна _____

Рецензент:
PhD, старший викладач кафедри ШІ
Гуськова Віра Геннадіївна _____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент _____

Київ – 2023 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
НН Інститут прикладного системного аналізу
Кафедра математичних методів системного аналізу

Рівень вищої освіти – перший (бакалаврський)
Спеціальність – 124 «Системний аналіз»
Освітня програма «Системний аналіз і управління»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Оксана ТИМОЩУК
«__» травня 2023 р.

ЗАВДАННЯ
на дипломну роботу студенту
Болдареву Єгору Андрійовичу

1. Тема роботи «Система підтримки прийняття рішень щодо захисту від хакерських атак», керівник роботи Савченко Ілля Олександрович, кандидат технічних наук, старший викладач, затверджені наказом по університету від «__» травня 2023 р. № _____
2. Термін подання студентом роботи 12.06.2023.
3. Вихідні дані до роботи – коректні результати користування системою.
4. Зміст роботи – дослідження предметної області, теоретичний опис модифікованого методу морфологічного аналізу, реалізація системи підтримки прийняття рішень, функціонально-вартісний аналіз.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо) – актуальність, постановка задачі, метод морфологічного аналізу, перший етап МММА, другий етап МММА, Другий етап МММА з нерівномірним розподілом початкових оцінок, морфологічні таблиці, приклад.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Функціонально-вартісний аналіз	Рощина Н.В.		

7. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Вивчення літератури за темою	14.04.2023 – 18.04.2023	Виконано
2	Підготовка першого розділу	18.04.2023 – 22.04.2023	Виконано
3	Підготовка другого розділу	22.04.2023 – 07.05.2023	Виконано
4	Розробка програмного продукту	07.05.2023 – 16.05.2023	Виконано
5	Підготовка третього розділу	16.05.2023 – 21.05.2023	Виконано
6	Функціонально-вартісний аналіз	21.05.2023 – 24.05.2023	Виконано
7	Оформлення дипломної роботи	24.05.2023 – 30.05.2023	Виконано

Студент Єгор БОЛДАРЕВ

Керівник Ілля САВЧЕНКО

РЕФЕРАТ

Дипломна робота містить 114 сторінок, 12 рисунків, 27 таблиць, 10 джерел, 2 додатки.

СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ, СППР, МОРФОЛОГІЧНИЙ АНАЛІЗ, ЗАХИСТ ВІД ХАКЕРСЬКИХ АТАК, МММА.

Метою роботи є розробка системи підтримки прийняття рішень щодо захисту від хакерських атак на базі двоетапного модифікованого методу морфологічного аналізу.

Об’єктом дослідження в роботі є процес прийняття рішень щодо захисту цифрової системи від хакерських атак. Предметом дослідження є двоетапний модифікований метод морфологічного аналізу з нерівномірним розподілом початкових оцінок.

В роботі проведено аналіз характеристик хакерських атак. Розглянуто систему як об’єкт хакерської атаки та встановлено її основні характеристики. Проведено двоетапний модифікований метод морфологічного аналізу.

Результатом роботи є веб-застосунок, інтерфейс якого реалізовано за допомогою HTML та CSS, а функціональний алгоритм написаний за допомогою мови програмування JavaScript.

Подальший розвиток роботи полягає в долученні збору інформації та баз даних для автоматизації основного алгоритму.

ABSTRACT

Diploma Thesis (Bachelor's Thesis) contains 114 pages, 12 figures, 27 tables, 10 sources, 2 appendices.

DECISION SUPPORT SYSTEM, DSS, MORPHOLOGICAL ANALYSIS, PROTECTION AGAINST HACKER ATTACKS, MMMA.

The purpose of the work is to develop a decision support system for protection against hacker attacks based on a two-stage modified method of morphological analysis.

The object of research in the work is the decision-making process regarding the protection of the digital system from hacker attacks. The subject of the study is a two-stage modified method of morphological analysis with an uneven distribution of initial estimates.

The article analyzes the characteristics of hacker attacks. The system as an object of a hacker attack was considered and its main characteristics were established. A two-stage modified method of morphological analysis was carried out.

The result of the work is a web application, the interface of which is implemented using HTML and CSS, and the functional algorithm is written using the JavaScript programming language.

The further development of the work consists in the addition of information collection and databases for the automation of the main algorithm.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОПР – особа, що приймає рішення.

СППР – система підтримки прийняття рішень.

ММММА – модифікований метод морфологічного аналізу.

ММА – метод морфологічного аналізу.

МТ – морфологічна таблиця.

ПП – програмний продукт.

HTML – HyperText Markup Language

CSS – Cascading Style Sheets

ВСТУП

Не є новиною, що в сучасному світі інформаційні технології проникли у всі сфери нашого життя. Наслідком цієї цифрової інтеграції є величезний обсяг чутливих даних в цифровому вигляді та велика залежність від цифрових сервісів в організації роботи багатьох підприємств. В таких реаліях захист від хакерських атак стає надзвичайно актуальним питанням ніж будь-коли. Зловмисники постійно шукають нові способи проникнення в комп'ютерні системи, мережі та інші пристрої з метою викрадення конфіденційної інформації, спричинення збитків, або навіть паралізація діяльності системи. Тож дуже важливо робити ефективні кроки для захисту системи від хакерських атак, щоб уберегти себе від атаки цілком або мінімізувати втрати в результаті атаки.

Хакерські атаки як об'єкти характеризуються багатьма ключовими факторами. Розглядаючи захист системи від атак, треба враховувати й параметри системи. Через таку велику кількість факторів, здатних вплинути на рішення особи, що приймає рішення, якість прийнятого ним рішення багато в чому залежить від його можливостей врахувати всі обставини та зв'язок між ними. В сучасних умовах досвіду та інтуїції ОПР не завжди достатньо для прийняття ефективних та обґрунтованих рішень.

Ціллю даної роботи є розробка СППР щодо захисту від хакерських атак, яка надаватиме організаціям та фахівцям з безпеки можливість ефективно аналізувати загрози та вживати необхідні заходи для запобігання та протидії атакам.

В якості методів дослідження застосовується двоетапний модифікований метод морфологічного аналізу. МММА – це потужний метод якісного аналізу, який успішно застосовується в процесах передбачення [1].

РОЗДІЛ 1 ДОСЛІДЖЕННЯ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Хакерські атаки

Хакерська атака — це будь-яка дія, спрямована проти інформаційних систем, мереж, інфраструктури, персональних комп'ютерних пристроїв або смартфонів. Зловмисник — це особа або процес, які намагаються отримати доступ до даних, функцій або інших обмежених областей системи без використання авторизації, потенційно зі зловмисними намірами [2]. Наслідки хакерських атак можуть бути серйозними. Крадіжка особистих даних, банківських реквізитів або медичних записів може призвести до ідентифікаційної крадіжки або фінансових втрат. Також може бути порушена робота важливих систем, таких як банківські мережі або критична інфраструктура, що призводить до припинення послуг і негативно впливає на життя людей.

На теперішній час існує багато різноманітних інструментів та методів для хакерських атак, які один від одного відрізняються метою та цільовим об'єктом атаки. Якщо таким чином класифікувати хакерські атаки, то можна виділити такі найпопулярніші групи [3]:

- Фішингова атака (англ. Phishing). Кіберзловмисники намагаються отримати таку особисту інформацію або дані, як імена користувачів, паролі та номери кредитних карток, видаючи себе за надійну особу за таких обставин. Фішинг здебільшого здійснюється за допомогою технологічних засобів, таких як електронні листи та телефонні дзвінки.
- Зловмисне програмне забезпечення (англ. Malware). Зловмисне програмне забезпечення – це тип програмного забезпечення, яке

призначене для порушення нормальної роботи будь-якого пристрою, включаючи мобільні телефони, настільні комп’ютери та сервери. Користувач натискає на джерело зловмисного програмного забезпечення, яке зазвичай надається у вигляді виконуваного коду, і випадково встановлює його. Деякі варіації зловмисного програмного забезпечення спрямовані на отримання постійного доступу до мережі, тоді як інші призначені для шпигування за користувачем з метою отримання облікових даних або іншої корисної інформації.

- SQL-ін'єкція (англ. SQL Injection). SQL-ін’єкція – це різновид атаки, спрямованої лише на бази даних SQL. SQL-вирази використовуються для запиту даних у базах даних SQL, і ці вирази зазвичай виконуються через форму HTML на веб-сторінці. Якщо дозволи бази даних указано неправильно, зловмисник може використовувати форму HTML для виклику запитів, які створюють, читають, змінюють або видаляють дані з бази даних.
- Атаки на відмову в обслуговуванні (англ. Denial of Service Attacks, DoS). Використовуючи таку атаку, хакер намагається перешкодити користувачам отримати доступ до цифрових сервісів, порушуючи роботу служб хоста, підключеного до Інтернету. Атака включає в себе заповнення хост-сервера набагато більшою кількістю запитів, ніж він може обробити, що призводить до збою сервера.
- Міжсайтові сценарії (англ. Cross Site Scripting, XSS). Під час цієї атаки, хакер вставляє зловісний скрипт у веб-сторінку. Коли користувачі переглядають цю сторінку, виконується цей скрипт у їхньому браузері, що може призвести до викрадення конфіденційних даних, перехоплення сесій або виконання шкідливих дій в контексті потерпілого користувача.

– Бот-мережі (англ. Botnets). Бот-мережі — це мільйони систем, заражених шкідливим програмним забезпеченням під контролем хакерів для здійснення DDoS атаки.

Попри таке різноманіття типів атак, можна виділити основні характеристики хакерської атаки:

1) ***Вектор атаки*** – метод або шлях, використовуваний зловмисником для отримання неавторизованого доступу або виконання зловмисних дій.
   1.1) *E-mail.* В цьому випадку атаки здійснюються через електронну пошту. Як приклад, зловмисники використовують фішингові листи, надсилання шкідливих вкладень та посилань, атаки на поштові сервери або викрадення облікових даних.
   1.2) *Мережа*. Включає в себе атаки на мережеві протоколи, системи комутації даних та інфраструктуру мережі. Хакери використовують такі методи, як: використання слабких місць безпеки задля атаки, атаки на маршрутизатори, перехоплення мережевого трафіку, розповсюдження вірусів у мережі.
   1.3) *Інтернет*. Охоплює різні атаки, що використовують Інтернет як основний канал. Сюди входять атаки на веб-сайти, використання вразливостей в програмах, атаки на додатки з відкритим вихідним кодом, злам аккаунтів соціальних мереж та інші веб-орієнтовані атаки.
   1.4) *Фізично*. В цьому випадку злодії здійснюють атаки безпосередньо на фізичному рівні. Це можуть бути атаки на фізичний доступ до пристроїв або приміщень, викрадення пристроїв, інсталяція шкідливого обладнання або використання соціальної інженерії для отримання доступу до систем.
2) ***Витонченість атаки*** – рівень технічної або операційної складності або навичок, задіяних у атаці.

2.1) *Проста*. Проста атака відображає низький рівень витонченості. Вона може включати базові методи, які легко виконати навіть для непрофесійного зловмисника. Наприклад, використання відомих інструментів для атак, які не потребують глибоких знань або спеціальних навичок.

2.2) *Просунута*. Просунута атака позначає високий рівень витонченості. Вона вимагає великої експертизи та розуміння вразливостей системи або мережі. Такі атаки можуть використовувати нові, раніше невідомі вразливості, складні техніки обходу захисту.

2.3) *Автоматизована*. Такі атаки використовують спеціально розроблене програмне забезпечення, скрипти або інструменти для автоматичного виконання хакерських атак. Вони можуть бути здійснені без значного втручання хакера, оскільки вони можуть бути програмно налаштованими для виявлення та зламування систем. Прикладами автоматизованих атак можуть бути DDoS атаки та використання бот-мереж.

3) ***Мета атаки*** – характер або мета атаки.

3.1) *Крадіжка*. Отримання несанкціонованого доступу до конфіденційної інформації або ресурсів з метою викрадення цих даних.

3.2) *Знищення даних*. Знищення або пошкодження даних, інфраструктури. Це може призвести до великих втрат даних, або неправильної роботи систем.

3.3) *Шпигунство*. Передбачає отримання конфіденційної інформації або доступу до системи.

3.4) *Перенавантаження системи*. Перевантаження системи або мережі з метою призупинення їхньої нормальної роботи.

4) ***Складність атаки*** – складність виконання атаки з технічної точки зору.

4.1) *Одноетапна*. Передбачає просту послідовність кроків, де зловмисник виконує лише один етап для досягнення своєї цілі. Це може бути,

наприклад, виконання певної команди, використання вразливості або запуск певної програми, яка відразу ж призводить до небажаного наслідку.

4.2) *Багатоетапна*. Передбачає складну послідовність кроків, де злодій виконує багато етапів або дій для досягнення своєї цілі. Це може включати виконання кількох кроків: від розвідки та збору інформації про ціль, до використання різних методів атаки та обходу захисту.

4.3) *Поліморфна*. Має на увазі високий рівень змінності або варіативності в ході виконання атаки. Хакери використовують методи, щоб змінювати свій підхід, код або схему атаки з метою уникнення виявлення чи блокування захисними механізмами.

5) ***Засоби ухилення*** – заходи, які зловмисники вживають для ухилення від виявлення або слідів атаки.

5.1) *VPN* (Virtual Private Network). VPN використовується для забезпечення приватності та анонімності під час передачі даних через мережу. Злодії можуть використовувати VPN для приховування своєї справжньої IP-адреси та місцезнаходження, щоб уникнути виявлення та ідентифікації їхніх дій.

5.2) *TOR* (The Onion Router). TOR – це мережа, що надає анонімність під час перегляду веб-сторінок та передачі даних через Інтернет. Хакери можуть використовувати TOR для приховування своєї справжньої IP-адреси та маршрутизації свого трафіку через кілька вузлів, що робить їхні дії важкодоступними для виявлення та відстеження.

5.3) *Стеганографія*. Стеганографія – це метод приховування інформації у інших типах даних або носіях, таких як зображення, звукові файли або текстові документи. Зловмисники можуть використовувати стеганографію для приховування своїх зловісних дій або відправки конфіденційної

інформації через невинні носії, змінюючи бітову структуру файлів або використовуючи спеціальні алгоритми [4].

1.2 Система, як ціль хакерської атаки.

Система є важливою складовою нашого сучасного життя. Це може бути комп'ютерна мережа, сервер, веб-сайт або будь-яка інша інформаційна інфраструктура, яка забезпечує функціонування різних сфер діяльності.

Коли система стає ціллю хакерської атаки, то велике значення має розуміння структури та слабких місць цієї системи. Хакери можуть проводити дослідження, використовувати програми-сканери для виявлення вразливостей та способів проникнення в систему.

Для ефективного захисту від хакерських атак, дуже важливо врахувати параметри наявної системи, адже тип та мета атаки напряму залежить від її цілі. Тож під час розгляду даного питання варто врахувати наступні параметри системи:

1) ***Тип системи*** (персональний комп’ютер, мережа, веб-сайт і т.д.).
2) ***Наявність бази даних***.
3) ***Тип підключення системи до мережі***.
   3.1) *Локальна мережа* (англ. Local Area Network, LAN) – мережа, яка зазвичай охоплює обмежену географічну територію, таку як будинок або офіс.
   3.2) *Широкомасштабна мережа* (англ. Wide Area Network, WAN) – мережа, що охоплює велику географічну територію, таку як, наприклад, країна. Вона використовується для підключення віддалених локальних мереж та

комп'ютерних систем, щоб забезпечити обмін даними та комунікацію на великій відстані.

3.3) *Інтернет* – глобальна мережа мереж, яка об'єднує мільйони систем та пристроїв по всьому світу. Він надає доступ до широкого спектру ресурсів, таких як веб-сторінки, онлайн-сервіси та ін.

4) ***Наявність антивірусних програм***.

5) ***Наявність систем виявлення вторгнень***.

1.3 Огляд систем підтримки прийняття рішень.

На сьогоднішній день існує величезна кількість СППР, що застосовуються в найрізноманітніших сферах людської діяльності. СППР допомагають ОПР підвищити ефективність управління різними складовими організації за рахунок зменшення навантаження та відповідальності на ОПР та полегшення складності прийняття комплексних рішень на основі екстраполяції досвіду ОПР на наявну ситуацію.

Розглянемо деякі існуючі СППР, їх особливості та функціональність.

1.3.1 IBM QRadar

QRadar є системою управління подіями та інформацією про безпеку, розробленою компанією IBM. Система забезпечує комплексний аналіз, виявлення та реагування на потенційні загрози безпеки в реальному часі. QRadar

інтегрується з різними джерелами даних, наприклад, системи виявлення вторгнень, журнали подій, мережеві пристрої та додатки, з метою забезпечити цілісний огляд безпекового стану інформаційної системи [5].

До основних особливостей СППР QRadar можна віднести:

- Централізоване керування подіями безпеки: QRadar збирає дані з різних джерел і передає їх в одну централізовану систему. Це дозволяє аналізувати події та виявляти аномальну активність, яка може бути пов'язана з хакерськими атаками.
- Автоматизована відповідь на інциденти: QRadar дозволяє автоматизувати процеси реагування на безпекові інциденти. Вона може надавати автоматичні рекомендації щодо заходів, які можна вжити у відповідь на виявлені загрози, або виконувати певні дії автоматично.
- Інтеграція з іншими системами безпеки: QRadar підтримує інтеграцію з іншими системами безпеки та інструментами, що дозволяє розширити функціональність та використовувати вже існуючі рішення безпеки в організації.

До недоліків даної СППР можна віднести:

- Вартість: QRadar відноситься до пропрієтарного програмного забезпечення, тобто ПЗ, на яке зберігаються і немайнові, і майнові авторські права. Тож ціна за використання послугами цією СППР може бути завеликою, особливо для невеликих компаній або організацій з обмеженим бюджетом.
- Складність впровадження: Впровадження QRadar може бути непростим завданням через необхідність інтеграції з різними джерелами даних та налаштування системи відповідно до конкретних потреб організації.

– Масштабованість: QRadar може стикатись з обмеженнями масштабованості при великому обсязі даних, що може вплинути на швидкодію та продуктивність системи.

1.3.2 FireEye Threat Intelligence

FireEye Threat Intelligence є системою, яка допомагає організаціям виявляти, аналізувати та реагувати на загрози безпеки. В її основі лежить розширена база даних, яка містить інформацію про хакерські групи, вразливості програмного забезпечення, зловживання та інші дані [6].

До основних особливостей СППР FireEye Threat Intelligence можна віднести:

– Загрози безпеки в реальному часі: FireEye Threat Intelligence забезпечує постійне оновлення бази даних про загрози безпеки, що дозволяє організаціям отримувати актуальну інформацію про нові вразливості, атаки та хакерські групи.
– Аналіз інформації про загрози: Система забезпечує можливість аналізувати дані про потенційні загрози безпеки з метою виявлення спільних шаблонів, зв'язків та трендів, що допомагає розуміти характер та масштаб загроз і приймати обґрунтовані безпекові рішення.
– Інтеграція з іншими системами безпеки: FireEye Threat Intelligence може інтегруватись з іншими системами безпеки, такими як системи виявлення вторгнень або SIEM (Security information and event management) системи. Це дозволяє аналізувати інформацію про загрози з різних джерел і використовувати її для зміцнення оборонних заходів.і

До недоліків можна віднести:

- Складність в аналізі: Інформація, надана системою, може бути великою за обсягом, і її аналіз вимагатиме кваліфікованих фахівців та значних ресурсів. Організаціям може бути важко ефективно використовувати ці дані без необхідних знань та інструментів.
- Вартість: Використання FireEye Threat Intelligence може викликати високі витрати, особливо для невеликих компаній чи організацій з обмеженим бюджетом.
- Залежність від актуальності даних: Ефективність системи залежить від актуальності та достовірності інформації про загрози. Якщо база даних не оновлюється регулярно або містить помилкову інформацію, це може призвести до помилкових або неефективних рішень.

1.3.3 Palo Alto Networks Next-Generation Firewall

Palo Alto Networks Next-Generation Firewall (NGFW) є сучасною системою захисту мережі, яка комбінує в собі функції традиційних файрволів з додатковими можливостями виявлення загроз, контролю застосунків та забезпечення безпеки мережі. NGFW спроектований для ефективного виявлення та захисту від сучасних хакерських атак.

До основних особливостей СППР Networks Next-Generation Firewall можна віднести:

- Контроль застосунків: NGFW надає глибокий контроль над застосунками, що працюють в мережі. Він може розпізнавати та контролювати

використання різних протоколів, додатків та сервісів, забезпечуючи безпеку і дотримання політик безпеки в мережі.

- Виявлення загроз в реальному часі: NGFW використовує алгоритми машинного навчання для виявлення потенційних загроз безпеки в реальному часі. Він аналізує мережевий трафік, ідентифікує небажану активність та небезпечні з'єднання.
- Політика безпеки на основі користувачів та контексту: NGFW дозволяє налаштовувати політику безпеки на основі ідентифікації користувачів та контексту. Використовуючи інформацію про користувачів, їхні ролі та джерела з'єднання, він пропонує рішення про доступ та контроль мережі.

До недоліків можна віднести:

- Вартість: Використання Palo Alto NGFW може бути занадто витратним.
- Потреба у регулярному оновленні: Для ефективної роботи NGFW необхідне регулярне оновлення програмного забезпечення та баз даних.
- Масштабованість: NGFW може мати обмеження на масштабування у великих мережах або в середовищах з високим обсягом трафіку. При великому навантаженні система може стикатись з проблемами продуктивності.

Висновки до розділу 1

На сьогоднішній день, захист від хакерських атак та ефективна реакція на них є пріоритетними питаннями безпеки усіх інформаційних систем. Кожного дня дедалі більше інформації зберігається на цифрових носіях, і ці дані можуть стати ключовою ціллю хакерської атаки. Тож, при розгляданні проблеми безпеки проти хакерських атак, окрім безпосередньо можливих типів атак, варто розглядати і параметри інформаційної системи, щоб знати її вразливості та врахувати їх при прийнятті рішень.

Також було розглянуто і проаналізовано існуючі системи підтримки прийняття рішень, метою яких є захист від хакерських атак. Всі оглянуті СППР активно використовують сучасні досягнення в сфері штучного інтелекту для обробки даних та своєчасного реагування на хакерські атаки. Здебільшого всі їхні рекомендації та рішення ґрунтуються на величезному обсязі накопичених та оброблених даних. В функціоналі жодної з охоплених СППР не було помічено залучення методів аналізу таких, як метод морфологічного аналізу.

РОЗДІЛ 2 ТЕОРЕТИЧНИЙ ОПИС МОДИФІКОВАНОГО МЕТОДУ МОРФОЛОГІЧНОГО АНАЛІЗУ

В основу цільової СППР щодо захисту від хакерських атак покладено двоетапний модифікований метод морфологічного аналізу з нерівномірним розподілом початкових оцінок. Головна мета цього методу в рамках цільової проблеми – виведення стратегій, які найефективніше враховувати в умовах сукупності можливих реалізацій об'єкта, визначених під час виконання ММА.

Стартовим і основним елементом ММА є морфологічна таблиця. Таблиця складається з певної N кількості характеристичних параметрів $F_i, i \in \overline{1,N}$. Кожному параметру відповідає певна n_i множина альтернатив $a_j^{(i)}, j \in \overline{1,n_i}$ [1]. Маючи таку таблицю, для подальших розрахунків потрібно отримати початкові оцінки $p_j^{(i)}$ (експертні оцінки) для ймовірностей альтернатив характеристичних параметрів.

При виконанні роботи був задіяний метод безпосереднього експертного оцінювання, суть якого полягає в тому, що кожній альтернативі характеристичного параметра морфологічної таблиці кожен експерт надає свою суб'єктивну оцінку за оцінювальною шкалою від 0 до 1. Також зручно виразити оцінювальну шкалу не тільки в кількісному варіанті, а і в якісному. Приклад такого вираження оцінок в якісному вигляді представлено в таблиці 2.1.

Таблиця 2.1 – Оцінювальна шкала для альтернатив морфологічної таблиці.

Якісна характеристика	**Кількісна характеристика**
Неможливо	0
Практично неможливо	[0 – 0,1]
Дуже мала ймовірність	[0,1 – 0,25]
Мала ймовірність	[0,25 – 0,4]
Середня ймовірність	[0,4 – 0,6]
Велика ймовірність	[0,6 – 0,75]
Дуже велика ймовірність	[0,75 – 0,9]
Практично гарантовано	[0,9 - 1]
Гарантовано	1

Виставлені оцінки відіграють суттєву роль в якості результатів ММА.

2.1 Перший етап ММА

Головною метою першого етапу ММА є розрахунок ймовірностей всіх альтернатив параметрів морфологічної таблиці з врахуванням зв'язків між ними на основі експертного оцінювання. Загально кажучи, на першому етапі здійснюється аналіз зовнішніх факторів для, в нашому випадку, хакерської атаки.

Для встановлення взаємозв'язків між параметрами морфологічної таблиці використовується числова матриця взаємозв'язків. Кожній парі альтернатив $a_{j_1}^{(i_1)}, a_{j_2}^{(i_2)}$ різних характеристичних параметрів F_{i_1}, F_{i_2} дається оцінка $c_{i_1 j_1, i_2 j_2} \in [-1; 1]$ згідно таблиці 2.2.

Таблиця 2.2 – Оцінки матриці взаємозв’язків.

Оцінка	Тлумачення
-1	Альтернативи повністю неузгоджені. Конфігурація з цією парою альтернатив неможлива.
(-1;0)	Альтернативи неузгоджені. Вибір однієї з них певною мірою зменшує ймовірність вибору іншої.
0	Альтернативи незалежні. Вибір однієї з них не впливає на вибір іншої.
(0;1)	Альтернативи узгоджені. Вибір однієї з них певною мірою збільшує ймовірність вибору іншої.
1	Альтернативи повністю узгоджені. вибір однієї з них тягне за собою вибір іншої.

Для заповнення матриці взаємозв’язків залучаються експерти: їм задають питання стосовно зв’язку кожної пари альтернатив різних характеристичних параметрів.

Після складання матриці взаємозв’язків, між вибором альтернатив різних параметрів створюється певна залежність і виникає наступна задача – знаходження оновлених ймовірностей вибору кожної альтернативи характеристичних параметрів, враховуючи вплив інформації з матриці взаємозв’язків на попередні оцінки.

Розглядаючи задачу для МТ з двома характеристичними параметрами, рівняння для ймовірностей кожної з альтернатив можна записати в наступному вигляді:

$$p_1^{(1)} = \sum_{j=1}^{n_2} P\left(a_1^{(1)} \middle| a_j^{(2)}\right) p_j^{(2)} = \sum_{j=1}^{n_2} P\left(\left\{a_1^{(1)}, a_j^{(2)}\right\}\right)$$

Для знаходження оновлених ймовірностей, в даному випадку, розв’язують наступну систему рівнянь Байєса:

$$\begin{cases} p_1^{(1)} = \sum_{j=1}^{n_2} P(a_1^{(1)}|a_j^{(2)})p_j^{(2)}; \\ \dots \\ p_{n_1}^{(1)} = \sum_{j=1}^{n_2} P(a_{n_1}^{(1)}|a_j^{(2)})p_j^{(2)}; \\ p_1^{(2)} = \sum_{j=1}^{n_1} P(a_1^{(2)}|a_j^{(1)})p_j^{(1)}; \\ \dots \\ p_{n_2}^{(2)} = \sum_{j=1}^{n_1} P(a_{n_2}^{(2)}|a_j^{(1)})p_j^{(1)}; \\ \sum_{j=1}^{n_1} p_j^{(1)} = 1; \sum_{j=1}^{n_2} p_j^{(2)} = 1. \end{cases}$$

Сформулюємо умови, яким повинні відповідати значення $P\left(a_{j_1}^{(i_1)}\middle|a_{j_2}^{(i_2)}\right)$:

1) Якщо відповідне значення матриці взаємозв’язків $c_{i_1 j_1, i_2 j_2} = -1$, то $P(a_{j_1}^{(i_1)}|a_{j_2}^{(i_2)}) = P(a_{j_2}^{(i_2)}|a_{j_1}^{(i_1)}) = 0$.
2) $P\left(a_{j_1}^{(i_1)}\middle|a_{j_2}^{(i_2)}\right)$ монотонно зростає при збільшенні $c_{i_1 j_1, i_2 j_2}$.
3) $P\left(a_{j_1}^{(i_1)}\middle|a_{j_2}^{(i_2)}\right)$ монотонно зростає при збільшенні $p'^{(i_1)}_{j_1}$.
4) для будь-якої альтернативи $a_{j_2}^{(i_2)}$ і будь-якого параметру F_{i_1}, $i_1 \neq i_2$ виконується співвідношення $\sum_{j_1=1}^{n_{i_1}} P(a_{j_1}^{(i_1)}|a_{j_2}^{(i_2)}) = 1$.
5) для всіх альтернатив $a_j^{(i)}$ існує нетривіальний набір таких значень $p_j^{(i)}$, що для будь-якої пари альтернатив $a_{j_1}^{(i_1)}$, $a_{j_2}^{(i_2)}$, $i_1 \neq i_2$ виконується співвідношення $P(a_{j_2}^{(i_2)}|a_{j_1}^{(i_1)})p_{j_1}^{(i_1)} = P(a_{j_1}^{(i_1)}|a_{j_2}^{(i_2)})p_{j_2}^{(i_2)} = P(\{a_{j_1}^{(i_1)}, a_{j_2}^{(i_2)}\})$.

Одним із способів знаходження значення, яке б відповідало вказаним вимогам, вважатимемо такий: $P(a_{j_1}^{(i_1)}|a_{j_2}^{(i_2)}) = \frac{{p'}_{j_1}^{(i_1)}(c_{i_1 j_1, i_2 j_2}+1)}{\sum_{j=1}^{n_{i_1}} {p'}_{j}^{(i_1)}(c_{i_1 j, i_2 j_2}+1)}$.

При розв'язанні задачі для довільної кількості параметрів, рівняння для ймовірностей альтернативи мають вигляд:

$$p_1^{(1)} = \sum_{j_2=1}^{n_2}\sum_{j_3=1}^{n_3}\dots\sum_{j_N}^{n_N} P(a_1^{(1)}|\{a_{j_2}^{(2)},\ a_{j_3}^{(3)},\ \dots,\ a_{j_N}^{(N)}\})P(\{a_{j_2}^{(2)},\ a_{j_3}^{(3)},\ \dots,\ a_{j_N}^{(N)}\}) =$$

$$= \sum_{j_2=1}^{n_2}\sum_{j_3=1}^{n_3}\dots\sum_{j_N}^{n_N} P(\{a_1^{(1)}, a_{j_2}^{(2)},\ a_{j_3}^{(3)},\ \dots,\ a_{j_N}^{(N)}\}) =$$

$$= \sum_{j_2=1}^{n_2}\sum_{j_3=1}^{n_3}\dots\sum_{j_N}^{n_N} P(\{a_1^{(1)}, a_{j_2}^{(2)},\ a_{j_3}^{(3)},\ \dots,\ a_{j_N}^{(N)}\}|a_{j_2}^{(2)})p_{j_2}^{(2)}.$$

Умови для значень виразу $P(\{a_{j_1}^{(1)}, a_{j_2}^{(2)},\ a_{j_3}^{(3)},\ \dots,\ a_{j_N}^{(N)}\}|a_{j_m}^{(m)})$ повністю відповідають умовам, описаним вище, але з врахуванням довільної кількості параметрів.

Одним із способів знаходження значення, яке б відповідало вимогам, вважатимемо такий:

$$P\left(\left\{a_{j_1}^{(1)}, a_{j_2}^{(2)},\ a_{j_3}^{(3)},\ \dots,\ a_{j_N}^{(N)}\right\}\middle|a_{j_m}^{(m)}\right) =$$

$$= \frac{P'\left(\left\{a_{j_1}^{(1)}, a_{j_2}^{(2)},\ a_{j_3}^{(3)},\ \dots,\ a_{j_N}^{(N)}\right\}\middle|a_{j_m}^{(m)}\right)}{\sum_{k_2=1}^{n_2}\sum_{k_3=1}^{n_3}\dots\sum_{k_N=1}^{n_N} P'\left(\left\{a_{j_1}^{(1)}, a_{k_2}^{(2)},\ a_{k_3}^{(3)},\ \dots,\ a_{k_N}^{(N)}\right\}\middle|a_{j_m}^{(m)}\right)}$$

, де $P'(\{a_{j_1}^{(1)}, a_{j_2}^{(2)},\ a_{j_3}^{(3)},\ \dots,\ a_{j_N}^{(N)}\}|a_{j_m}^{(m)}) = \prod_{l=2}^{N} {p'}_{j_l}^{(l)} \cdot \prod_{l=1}^{N-1}\prod_{k=l+1}^{N}(c_{l j_l, k j_k}+1)$

Система рівнянь, розв'язком якої є оновлені ймовірності альтернатив має вигляд:

$$\begin{cases} p_1^{(1)} = \sum_{j_2=1}^{n_2}\sum_{j_3=1}^{n_3}\dots\sum_{j_N=1}^{n_N} P\left(\left\{a_1^{(1)}, a_{j_2}^{(2)},\ a_{j_3}^{(3)},\ \dots,\ a_{j_N}^{(N)}\right\}\middle| a_{j_2}^{(2)}\right) p_{j_2}^{(2)}; \\ \dots \\ p_{n_1}^{(1)} = \sum_{j_2=1}^{n_2}\sum_{j_3=1}^{n_3}\dots\sum_{j_N=1}^{n_N} P\left(\left\{a_{n_1}^{(1)}, a_{j_2}^{(2)},\ a_{j_3}^{(3)},\ \dots,\ a_{j_N}^{(N)}\right\}\middle| a_{j_2}^{(2)}\right) p_{j_2}^{(2)}; \\ p_1^{(2)} = \sum_{j_1=1}^{n_1}\sum_{j_3=1}^{n_3}\dots\sum_{j_N=1}^{n_N} P\left(\left\{a_{j_1}^{(1)}, a_1^{(2)},\ a_{j_3}^{(3)},\ \dots,\ a_{j_N}^{(N)}\right\}\middle| a_{j_3}^{(3)}\right) p_{j_3}^{(3)}; \\ \dots \\ p_{n_2}^{(2)} = \sum_{j_1=1}^{n_1}\sum_{j_3=1}^{n_3}\dots\sum_{j_N=1}^{n_N} P\left(\left\{a_{j_1}^{(1)}, a_{n_2}^{(2)},\ a_{j_3}^{(3)},\ \dots,\ a_{j_N}^{(N)}\right\}\middle| a_{j_3}^{(3)}\right) p_{j_3}^{(3)}; \\ \dots \\ p_1^{(N)} = \sum_{j_1=1}^{n_1}\sum_{j_2=1}^{n_2}\dots\sum_{j_{N-1}=1}^{n_{N-1}} P\left(\left\{a_{j_1}^{(1)}, a_{j_2}^{(2)},\ a_{j_3}^{(3)},\ \dots,\ a_1^{(N-1)}\right\}\middle| a_{j_1}^{(1)}\right) p_{j_1}^{(1)}; \\ \dots \\ p_{n_N}^{(N)} = \sum_{j_1=1}^{n_1}\sum_{j_2=1}^{n_2}\dots\sum_{j_{N-1}=1}^{n_{N-1}} P\left(\left\{a_{j_1}^{(1)}, a_{j_2}^{(2)},\ a_{j_3}^{(3)},\ \dots,\ a_{n_N}^{(N-1)}\right\}\middle| a_{j_1}^{(1)}\right) p_{j_1}^{(1)}; \\ \sum_{j=1}^{n_1} p_j^{(1)} = 1;\ \dots;\ \sum_{j=1}^{n_N} p_j^{(N)} = 1. \end{cases}$$

Розв’язавши систему рівнянь, отримується оновлена морфологічна таблиця, що містить оцінки альтернатив, які враховують взаємозв’язки характеристичних параметрів системи.

2.2 Другий етап ММА

Метою другого етапу ММА є розрахунок оцінок результативності кожної з альтернатив параметрів морфологічної таблиці стратегій в умовах ситуації, заданої морфологічною таблицею сценаріїв. Тут ми за МТ сценаріїв вважаємо

МТ, отриману в результаті першого етапу МММА. Морфологічну таблицю другого етапу назвемо морфологічною таблицею стратегій.

Специфіка другого етапу полягає в тому, що вибір альтернатив параметрів морфологічної таблиці стратегій залежить саме від особи, що приймає рішення, а не від випадкових зовнішніх чинників. Тому на цьому етапі використовується для оцінки альтернатив використовується величина очікуваної результативності.

Для врахування зв'язків між параметрами морфологічних таблиць першого та другого етапів пропонується використовувати числову матрицю зв'язків. Відповідно до стратегії, кожній парі альтернатив $a_{j_1}^{(i_1)}, a_{j_2}^{(i_2)}$ різних характеристичних параметрів F_{i_1}, F_{i_2} дається оцінка $c_{i_1 j_1, i_2 j_2} \in [-1; 1]$ згідно таблиці 2.3.

Таблиця 2.3 – Оцінки матриці зв'язків.

Оцінка	Тлумачення
-1	Альтернатива параметра МТ стратегій є абсолютно не ефективною при виборі відповідної альтернативи параметра МТ сценаріїв.
(-1;0)	Вибір відповідної альтернативи параметра МТ сценаріїв в певній мірі зменшує ефективність альтернативи параметра МТ стратегій.
0	Ефективність альтернативи параметра МТ стратегій ніяк не залежить від вибору відповідної альтернативи параметра МТ сценаріїв.
(0;1)	Вибір відповідної альтернативи параметра МТ сценаріїв в певній мірі збільшує ефективність альтернативи параметра МТ стратегій.
1	Альтернатива параметра МТ стратегій є повністю ефективною при виборі відповідної альтернативи параметра МТ сценаріїв.

До заповнення матриці залучають експертів. Аналогічно до матриці взаємозв'язків в першому етапі МММА.

Після, спираючись на матрицю зв'язків та МТ сценаріїв, розраховуються оцінки результативності $R_j^{(i)}$ кожної з альтернатив морфологічної таблиці стратегій $a_j^{(i)}$, породжених МТ стратегій в умовах ситуації заданої МТ сценаріїв.

Величина умовної результативності $R(a_j^{(i)}|\{a_{j_1}^{(1)}, a_{j_2}^{(2)}, a_{j_3}^{(3)}, \ldots, a_{j_N}^{(N)}\})$ альтернативи $a_j^{(i)}$, $i \in \overline{N+1, N+N'}$ при конфігурації МТ першого етапу $\{a_{j_1}^{(1)}, a_{j_2}^{(2)}, a_{j_3}^{(3)}, \ldots, a_{j_N}^{(N)}\}$:

$$R\left(a_j^{(i)}\middle|\left\{a_{j_1}^{(1)}, a_{j_2}^{(2)}, a_{j_3}^{(3)}, \ldots, a_{j_N}^{(N)}\right\}\right) = \frac{{p'}_j^{(i)} \cdot \prod_{m=1}^{N}\left(c_{mj_m,ij} + 1\right)}{\sum_{k=1}^{n_i}\left({p'}_k^{(i)} \cdot \prod_{m=1}^{N}\left(c_{mj_m,ik} + 1\right)\right)} \quad (2.1)$$

, де ${p'}_j^{(i)}$ – попередня оцінка результативності альтернативи $a_j^{(i)}$. В разі якщо така попередня інформація про результативність альтернатив відсутня, ці значення приймаються рівними для всіх альтернатив кожного з параметрів: ${p'}_j^{(i)} = {}^{1}/_{n_i}$.

Очікувана результативність альтернативи $a_j^{(i)}$ обчислюється за наступною формулою:

$$R_j^{(i)} = \sum_{j_1=1}^{n_1}\sum_{j_2=1}^{n_2}\ldots\sum_{j_N=1}^{n_N} R\left(a_j^{(i)}\middle|\left\{a_{j_1}^{(1)}, a_{j_2}^{(2)}, a_{j_3}^{(3)}, \ldots, a_{j_N}^{(N)}\right\}\right) P\left(\left\{a_{j_1}^{(1)}, a_{j_2}^{(2)}, a_{j_3}^{(3)}, \ldots, a_{j_N}^{(N)}\right\}\right)$$

Вже з отриманих очікуваних результативностей альтернатив ми можемо робити висновки про ефективність параметрів МТ стратегій.

2.3 Другий етап МММА з нерівномірним розподілом початкових оцінок

В умовах поставленої задачі, початкові оцінки, а точніше, оцінки характеристик хакерських атак, визначаються експертом без врахування параметрів системи-цілі хакерської атаки. Тож, перед тим, як проводити двоетапний модифікований метод морфологічного аналізу з метою дослідження ефективності стратегій щодо захисту від хакерської атаки, ми маємо отримати оновлені оцінки характеристик атак з врахуванням параметрів системи. Для цього проводиться другий етап двоетапного МММА, в якому за морфологічну таблицю сценаріїв приймається МТ параметрів системи, а за МТ стратегій – МТ характеристик хакерських атак. Цей другий етап двоетапного МММА відбувається аналогічно описаній вище процедурі, де під час пошуку величини умовної результативності (2.1), попередня оцінка результативності альтернативи $a_j^{(i)}$ ($p'^{(i)}_j$) береться з експертних оцінок відповідних характеристик хакерських атак.

Висновки до розділу 2

В розділі 2 було описано процедуру експертного оцінювання та двоетапного модифікованого методу морфологічного аналізу з особливістю. Особливість полягає в тому, що двоетапному МММА передує застосування другого етапу двоетапного МММА для побудови зв’язку між характеристичним параметрами двох стартових таблиць. В даній роботі вперше запропоновано подібну процедуру дій для оцінки ефективності стратегій щодо захисту від хакерських атак.

РОЗДІЛ 3 РЕАЛІЗАЦІЯ СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ

Реалізацію СППР щодо захисту від хакерських атак можна умовно поділити на три частини:

1) Створення морфологічних таблиць для двоетапного модифікованого методу морфологічного аналізу з нерівномірним розподілом початкових оцінок;
2) Проектування та реалізація програмного інтерфейсу;
3) Програмна реалізація основного алгоритму двоетапного МММА з нерівномірним розподілом початкових оцінок.

3.1 Створення морфологічних таблиць

Створимо морфологічні таблиці для характеристик хакерських атак та параметрів цільової системи. Таблиця, яка містить характеристики хакерських атак (таблиця 3.1) має наступні характеристичні параметри: вектор атаки, витонченість атаки, мета атаки, складність атаки, засоби ухилення.

Таблиця 3.1 – Морфологічна таблиця характеристик хакерських атак.

Вектор атаки	Витонченість атаки	Мета атаки	Складність атаки	Засоби ухилення
E-mail	Проста	Крадіжка	Одноетапна	VPN
Мережа	Просунута	Знищення даних	Багатоетапна	TOR
Інтернет	Автоматизована	Шпигунство	Поліморфна	Стеганографія
Фізично		Перенавантаження системи		

Таблиця, яка містить параметри цільової системи (таблиця 3.2) має наступні характеристичні параметри: тип системи, база даних, тип підключення системи до мережі, антивірусні програми, системи виявлення вторгнень.

Таблиця 3.2 – Морфологічна таблиця параметрів цільової системи.

Тип системи	База даних	Тип підключення системи до мережі	Антивірусні програми	Системи виявлення вторгнень
ПК	Є	LAN	Є	Є
Мережа	Немає	WAN	Немає	Немає
Веб-сайт		Інтернет		

Експертні оцінки для цих таблиць будуть виставлятись користувачем на початку роботи СППР.

Для приведення нерівномірних початкових оцінок характеристик хакерських атак до рівномірного вигляду, треба встановити зв’язки між ними та параметрами цільової системи. Складемо матрицю зв’язків між ним:

— Для параметру «Вектор атаки» (таблиця 3.3);

— Для параметру «Витонченість атаки» (таблиця 3.4);

— Для параметру «Тип атаки» (таблиця 3.5);

— Для параметру «Складність атаки» (таблиця 3.6);

— Для параметру «Засоби ухилення» (таблиця 3.7);

Таблиця 3.3 – Зв’язки альтернатив параметра «Вектор атаки» та цільової системи.

		Вектор атаки			
		E-mail	Мережа	Інтернет	Фізично
Тип системи	ПК	0.6	0.2	0.8	0.5
	Мережа	0.3	0.8	0.5	0.5
	Веб-сайт	-1	-0.2	1	-1
База даних	Є	0	0	0	0
	Немає	0	0	0	0
Тип підключення системи до мережі	LAN	0.3	0.5	0.1	0
	WAN	0.1	0.7	0.4	0
	Інтернет	0.5	-0.6	0.9	0
Антивірусні програми	Є	-0.2	-0.1	-0.2	-0.5
	Немає	0.3	0.1	0.3	0.5
Системи виявлення вторгнень	Є	-0.1	-0.8	-0.3	0
	Немає	0.2	0.5	0.4	0

Таблиця 3.4 – Зв’язки альтернатив параметра «Витонченість атаки» та цільової системи.

		Витонченість атаки		
		Проста	Просунута	Автоматизована
Тип системи	ПК	0.6	0.2	0.7
	Мережа	-0.4	0.6	0.1
	Веб-сайт	0.4	0.3	0.5
База даних	Є	-0.2	0.2	0.1
	Немає	0.2	-0.2	0.3
Тип підключення системи до мережі	LAN	0.5	0.2	0.4
	WAN	-0.2	0.6	-0.1
	Інтернет	0.3	0.4	0.6
Антивірусні програми	Є	-0.7	0.6	-0.5
	Немає	0.5	0	0.8
Системи виявлення вторгнень	Є	-0.9	1	-0.3
	Немає	0.5	0	0.7

Таблиця 3.5 – Зв’язки альтернатив параметра «Тип атаки» та цільової системи.

		Тип атаки			
		Крадіжка	Знищення даних	Шпигунство	Перенавантаження системи
Тип системи	ПК	0.5	0.2	0.4	0
	Мережа	0.2	0	0.8	0.6
	Веб-сайт	0.2	0.5	0	0.7
База даних	Є	0.8	0.7	-0.9	-0.7
	Немає	-0.3	-0.6	0.4	0.1
Тип підключення системи до мережі	LAN	0	0	0	0
	WAN	0	0	0	0
	Інтернет	0	0	0	0
Антивірусні програми	Є	-0.3	-0.3	-0.4	0
	Немає	0	0	0	0
Системи виявлення вторгнень	Є	-0.2	-0.2	-0.4	-0.5
	Немає	0	0	0	0

Таблиця 3.6 – Зв’язки альтернатив параметра «Складність атаки» та цільової системи.

		Складність атаки		
		Одноетапна	Багатоетапна	Поліморфна
Тип системи	ПК	0.4	-0.4	0.3
	Мережа	-0.5	0.6	0.8
	Веб-сайт	0.3	0.4	0.6
База даних	Є	0	0	0
	Немає	0	0	0
Тип підключення системи до мережі	LAN	0	0	0
	WAN	0	0	0
	Інтернет	0	0	0
Антивірусні програми	Є	-0.5	0.8	0.5
	Немає	0	0	0
Системи виявлення вторгнень	Є	-0.9	0.7	0.8
	Немає	0	0	0

Таблиця 3.7 – Зв’язки альтернатив параметра «Засоби ухилення» та цільової системи.

		Засоби ухилення		
		VPN	TOR	Стеганографія
Тип системи	ПК	0.7	0.5	0.4
	Мережа	0.6	0.5	-0.2
	Веб-сайт	0.5	0.5	-0.3
База даних	Є	0	0	0
	Немає	0	0	0
Тип підключення системи до мережі	LAN	0	0	0
	WAN	0	0	0
	Інтернет	0	0	0
Антивірусні програми	Є	0	0	0.4
	Немає	0	0	0
Системи виявлення вторгнень	Є	0.7	0.5	0.6
	Немає	0	0	0

Наостанок, для першого етапу двоетапного ММА необхідно скласти таблицю взаємозв’язків параметрів характеристик хакерських атак:

— Для параметру «Вектор атаки» (таблиця 3.8);

— Для параметру «Витонченість атаки» (таблиця 3.9);

— Для параметру «Тип атаки» (таблиця 3.10);

— Для параметру «Складність атаки» (таблиця 3.11);

— Для параметру «Засоби ухилення» (таблиця 3.12);

Таблиця 3.8 – Взаємозв’язки альтернатив для параметра «Вектор атаки».

		Вектор атаки			
		Email	Мережа	Інтернет	Фізично
Вектор атаки	E-mail	0	0	0	0
	Мережа	0	0	0	0
	Інтернет	0	0	0	0
	Фізично	0	0	0	0
Витонченість атаки	Проста	0.2	-0.1	0	0.6
	Просунута	0	0.4	0	0
	Автоматизована	0.4	0.2	0.5	-1
Тип атаки	Крадіжка	0.5	0.4	0.7	0.6
	Знищення даних	-0.4	0.3	0.5	0.4
	Шпигунство	0.4	0.6	0.7	0.8
	Перенавантаження системи	-0.3	0.1	0.6	0.3
Складність атаки	Одноетапна	0.4	0.1	0.2	0.7
	Багатоетапна	0.1	0.4	0.5	0.1
	Поліморфна	-0.2	0.6	0.7	0.2
Ухилення	VPN	0.1	0.5	0.7	-0.7
	TOR	0.2	0.5	0.6	-0.7
	Стеганографія	0.5	-0.2	0.3	0.7

Таблиця 3.9 – Взаємозв’язки альтернатив для параметра «Витонченість атаки».

		Витонченість атаки		
		Проста	Просунута	Автоматизована
Вектор атаки	E-mail	0.2	0	0.4
	Мережа	-0.1	0.4	0.2
	Інтернет	0	0	0.5
	Фізично	0.6	0	-1
Витонченість атаки	Проста	0	0	0
	Просунута	0	0	0
	Автоматизована	0	0	0
Тип атаки	Крадіжка	0	0	0.4
	Знищення даних	0	0	0.1
	Шпигунство	0	0	0.3
	Перенавантаження системи	0	0	0.5
Складність атаки	Одноетапна	0.8	0.2	0.7
	Багатоетапна	0.1	0.6	0.3
	Поліморфна	-0.7	0.7	0.2
Ухилення	VPN	0	0	0.2
	TOR	0	0	0
	Стеганографія	-0.6	0	0

Таблиця 3.10 – Взаємозв’язки альтернатив для параметра «Тип атаки».

		Тип атаки			
		Крадіжка	Знищення даних	Шпигунство	Перенавантаження системи
Вектор атаки	E-mail	0.5	-0.4	0.4	-0.3
	Мережа	0.4	0.3	0.6	0.1
	Інтернет	0.7	0.5	0.7	0.6
	Фізично	0.6	0.4	0.8	0.3
Витонченість атаки	Проста	0	0	0	0
	Просунута	0	0	0	0
	Автоматизована	0.4	0.1	0.3	0.5
Тип атаки	Крадіжка	0	0	0	0
	Знищення даних	0	0	0	0
	Шпигунство	0	0	0	0
	Перенавантаження системи	0	0	0	0
Складність атаки	Одноетапна	0	0	0	0.2
	Багатоетапна	0	0	0	0
	Поліморфна	0	0	0.3	0
Ухилення	VPN	0	0	0	0
	TOR	0	0	0	0
	Стеганографія	0	0	0	0

Таблиця 3.11 – Взаємозв’язки альтернатив для параметра «Складність атаки».

		Складність атаки		
		Одноетапна	Багатоетапна	Поліморфна
Вектор атаки	E-mail	0.4	0.1	-0.2
	Мережа	0.1	0.4	0.6
	Інтернет	0.2	0.5	0.7
	Фізично	0.7	0.1	0.2
Витонченість атаки	Проста	0.8	0.1	-0.7
	Просунута	0.2	0.6	0.7
	Автоматизована	0.7	0.3	0.2
Тип атаки	Крадіжка	0	0	0
	Знищення даних	0	0	0
	Шпигунство	0	0	0.3
	Перенавантаження системи	0.2	0	0
Складність атаки	Одноетапна	0	0	0
	Багатоетапна	0	0	0
	Поліморфна	0	0	0
Ухилення	VPN	0.3	0.3	0.3
	TOR	0.2	0.4	0.5
	Стеганографія	0	0.3	0.4

Таблиця 3.12 – Взаємозв’язки альтернатив для параметра «Засоби ухилення».

		Засоби ухилення		
		VPN	TOR	Стеганографія
Вектор атаки	E-mail	0.1	0.2	0.5
	Мережа	0.5	0.5	-0.2
	Інтернет	0.7	0.6	0.3
	Фізично	-0.7	-0.7	0.7
Витонченість атаки	Проста	0	0	-0.6
	Просунута	0	0	0
	Автоматизована	0.2	0	0
Тип атаки	Крадіжка	0	0	0
	Знищення даних	0	0	0
	Шпигунство	0	0	0
	Перенавантаження системи	0	0	0
Складність атаки	Одноетапна	0.3	0.2	0
	Багатоетапна	0.3	0.4	0.3
	Поліморфна	0.3	0.5	0.4
Ухилення	VPN	0	0	0
	TOR	0	0	0
	Стеганографія	0	0	0

3.2 Обґрунтування вибору технологій

Для реалізації програмного інтерфейсу було обрано інструментарій HTML, CSS та JavaScript тобто в результаті отримано веб-сайт для взаємодії з СППР щодо захисту від хакерських атак. JavaScript (JS) – мова програмування, яка дозволяє реалізовувати скрипти будь-якої складності на веб-сторінках. Браузери всіх операційних систем мають вбудований інтерпретатор, який компілює та виконує JS скрипти. Ця мова програмування є дуже популярною, адже використовується чи не на кожній веб-сторінці. HTML використовується для розмітки веб-сторінки, а CSS – дизайну візуальної презентації сторінок.

В програмній реалізації СППР залучено JavaScript стандарту EcmaScript 6. Середовище розробки – редактор вихідного коду Visual Studio Code від компанії Microsoft.

3.3 Проектування та реалізація програмного інтерфейсу

Під час проектування програмного інтерфейсу була поставлена задача створення інтерфейсу, за допомогою якого користувач мав змогу вводити свої оцінки для параметрів цільової системи, характеристик хакерських атак та можливі альтернативи щодо захисту від хакерської атаки. Після чого, користувачеві відкривалась можливість заповнити матрицю зв’язків між характеристиками хакерських атак та раніше ним введеним альтернативам захисту, і, натискаючи кінцеву кнопку, користувач би отримував результат, а саме рекомендації стосовно найбільш ефективної альтернативи захисту. Також

потрібно врахувати й оброблювати помилки при неповному заповненню даних користувачем та забезпечити довідкову інформацію для нього.

Користувачеві буде запропоновано вводити оцінки для матриці зв’язків між характеристиками хакерських атак та альтернативами захисту у якісному вигляді. Відповідність якісної характеристики до кількісної наведено в таблиці 3.13.

Таблиця 3.13 – Оцінювальна шкала для матриці зв’язків.

Якісна характеристика	**Кількісна характеристика**
Абсолютно несумісні	-1
Дуже сильно несумісні	-0,75
Посередньо несумісні	-0,5
Мала несумісність	-0,25
Незалежні	0
Мало пов'язані	0,25
Посередньо пов'язані	0,5
Дуже сильно пов'язані	0,75
Абсолютно пов'язані	1

Інтерфейс програми наведено на рисунках 3.1 – 3.5.

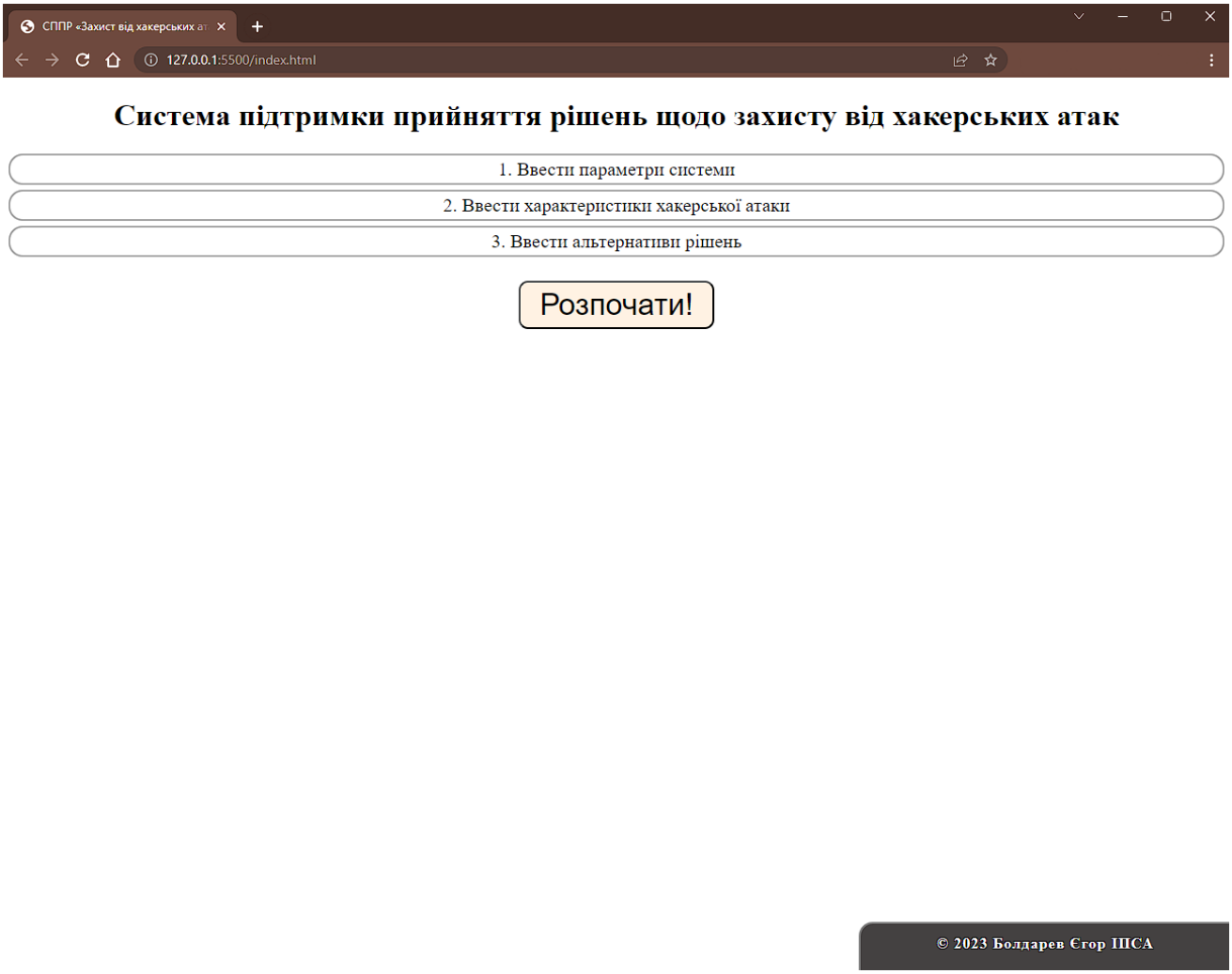


Рисунок 3.1 – Початок роботи програми

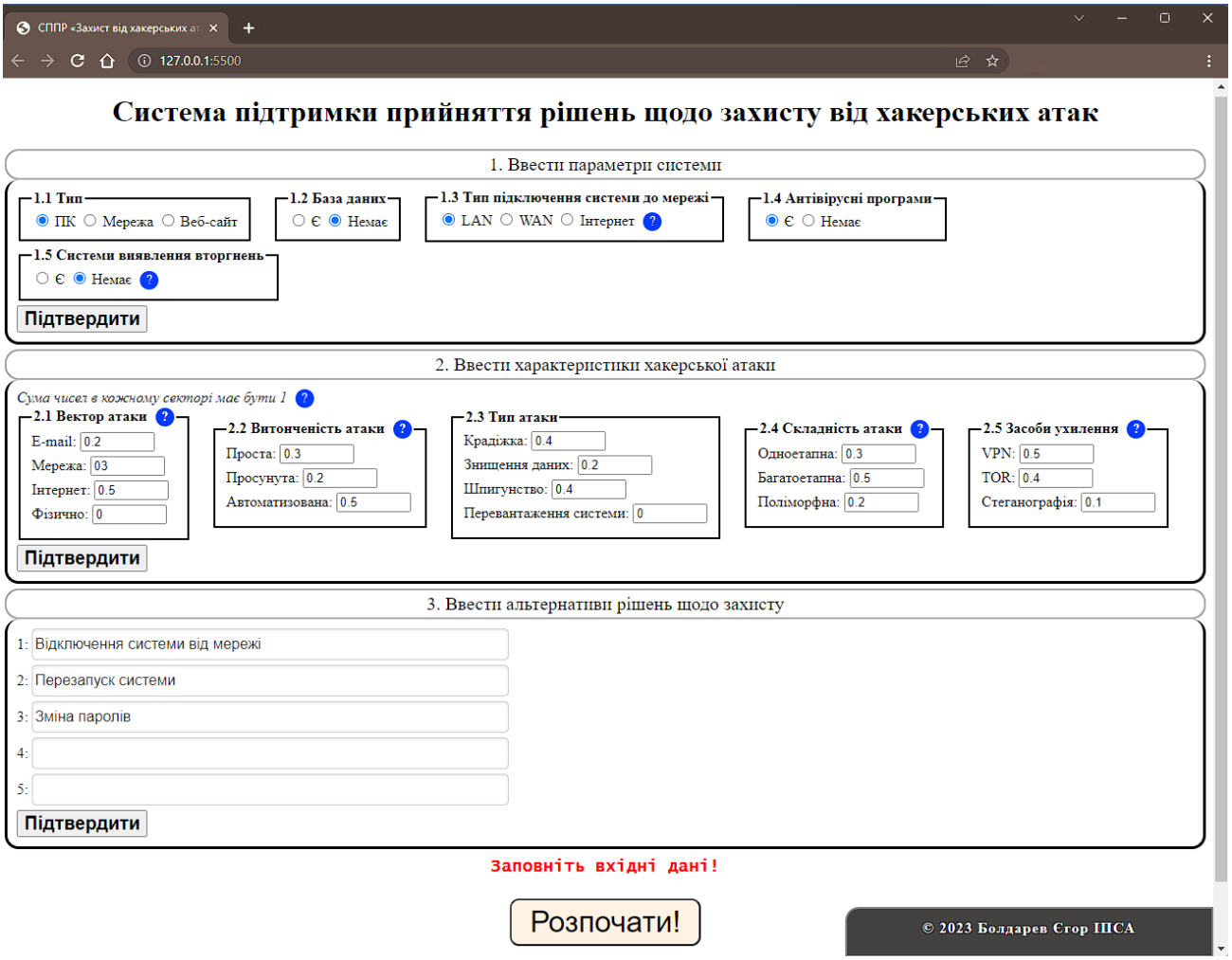


Рисунок 3.2 – Заповнені користувачем дані та помилка про незбережені дані.

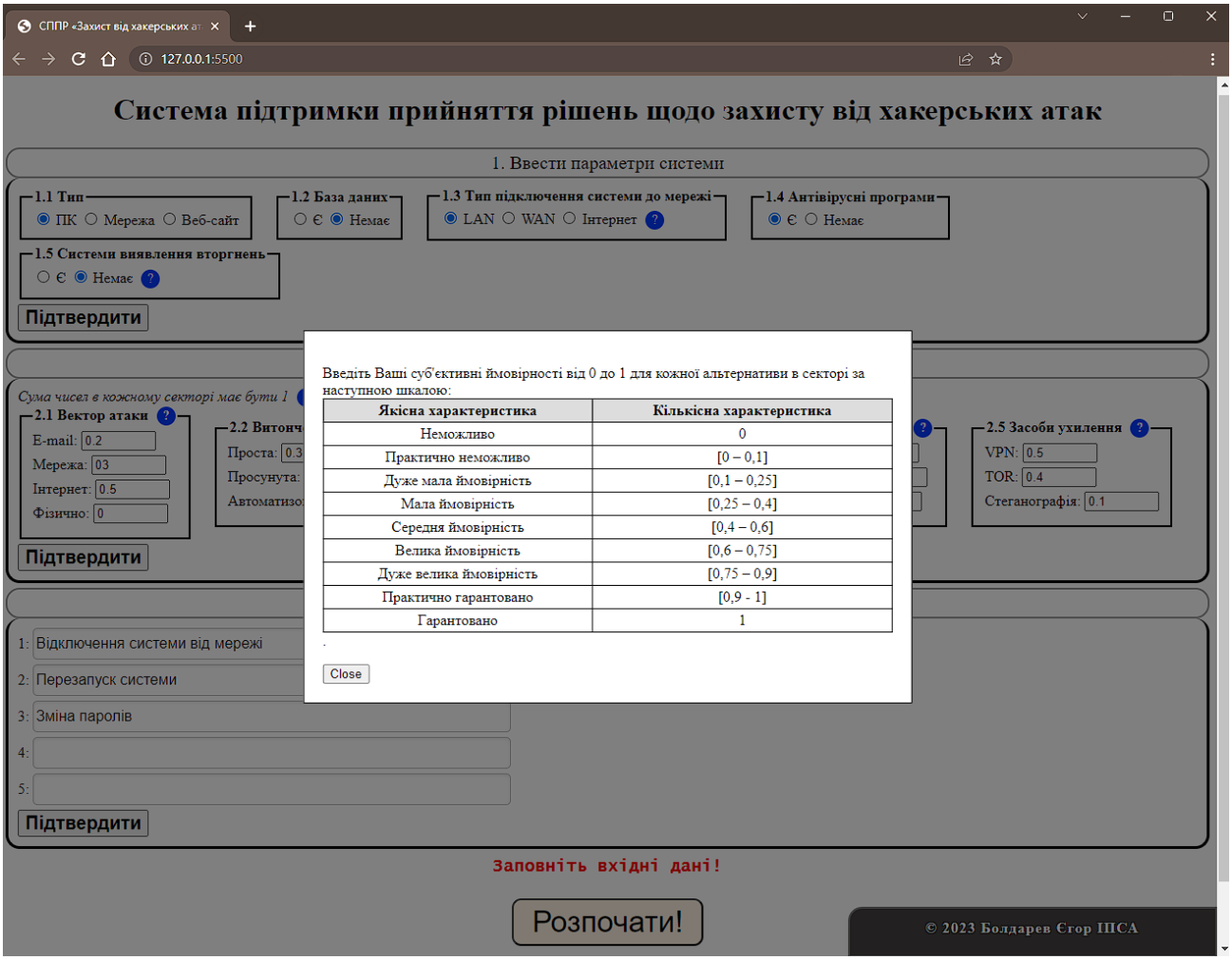


Рисунок 3.3 – Довідкова інформація для користувача.

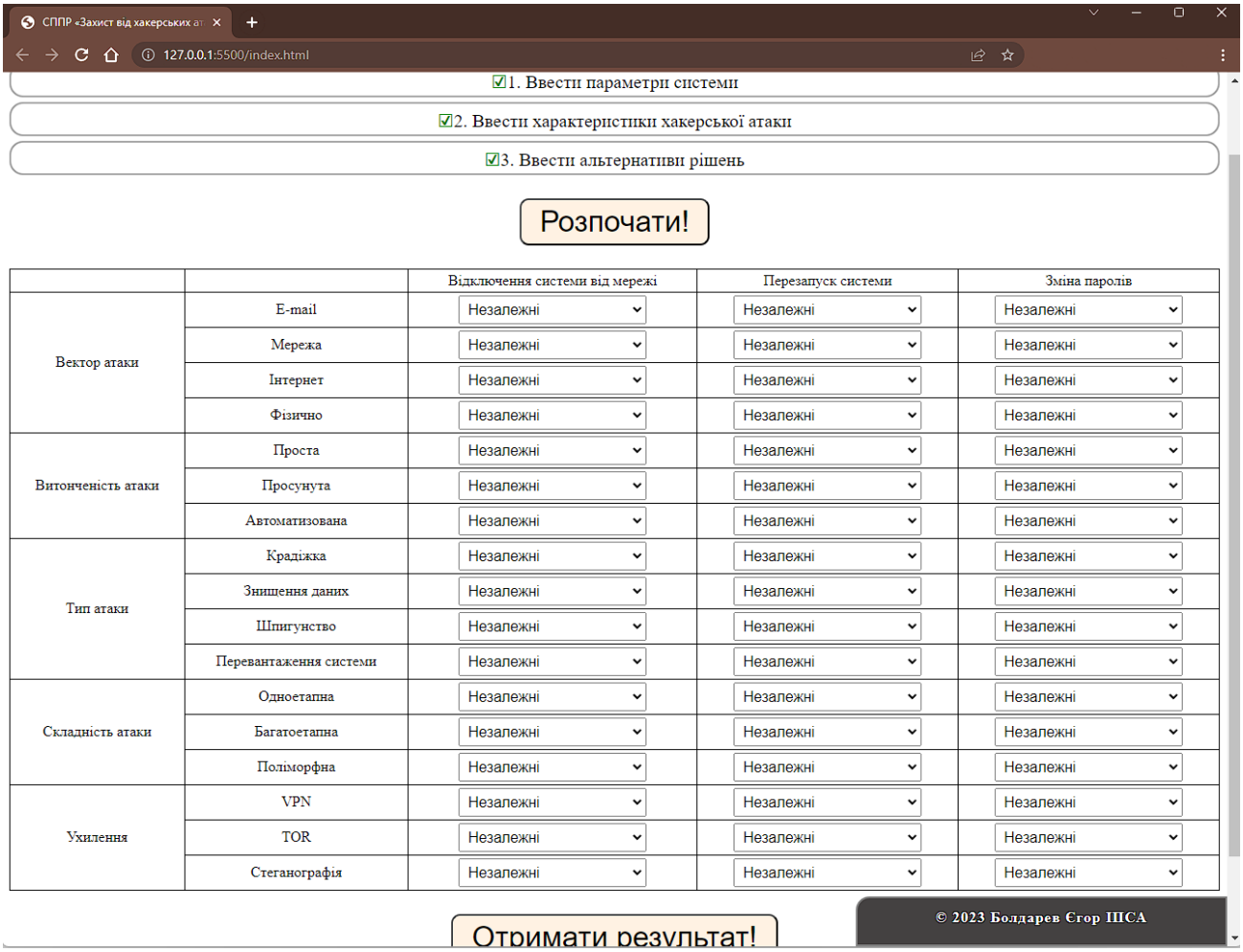


Рисунок 3.4 – Збережені вхідні дані та початкова матриця зв’язків характеристик хакерських атак та альтернатив захисту.

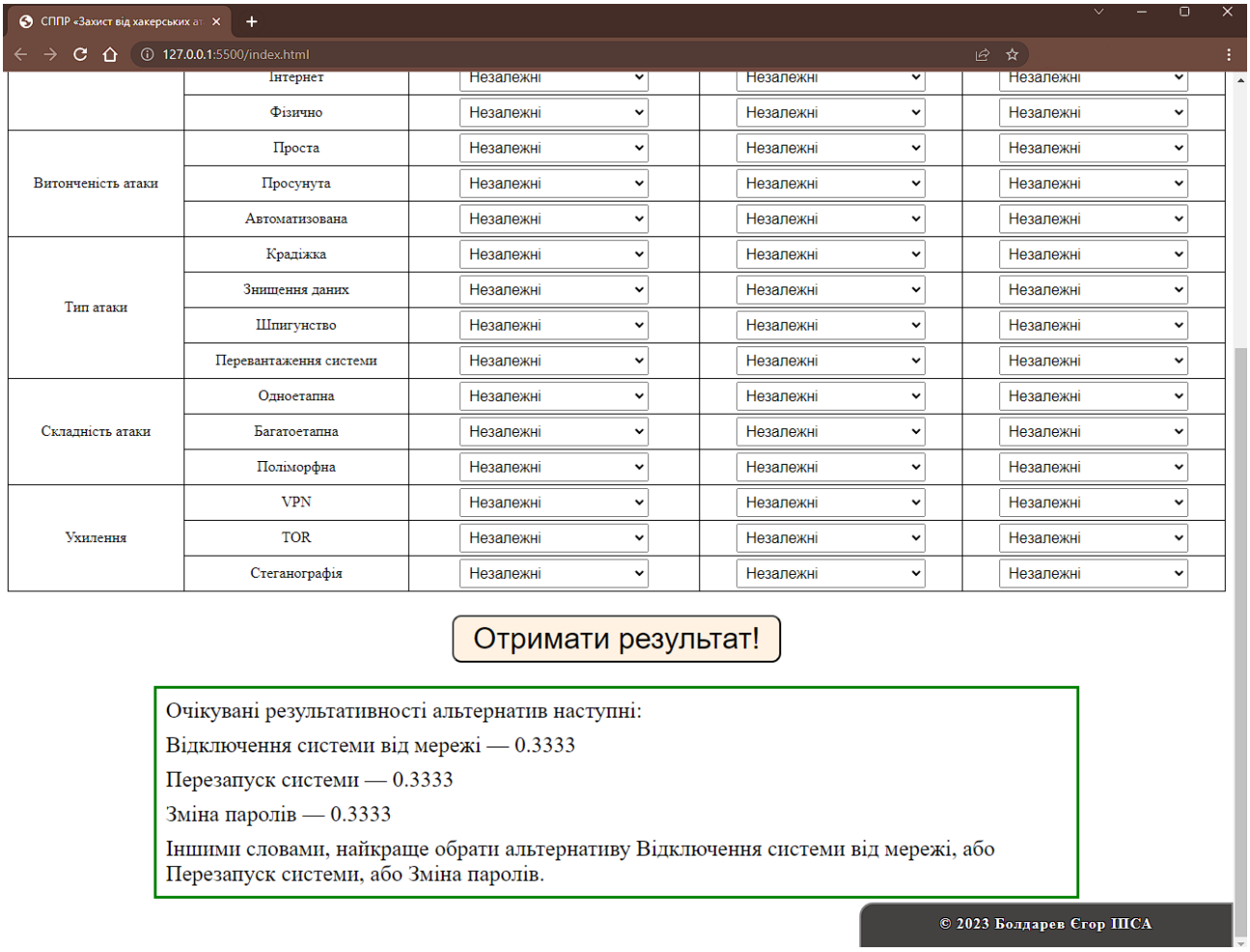


Рисунок 3.5 – Результат виконання СППР.

3.4 Програмна реалізація основного алгоритму

Для реалізації основного алгоритму двоетапного МММА застосовується мова програмування JavaScript стандарту EcmaScript 6 без використання сторонніх бібліотек.

Продемонструємо покрокове виконання алгоритму програми на таких початкових даних (рис. 3.6 - 3.7):

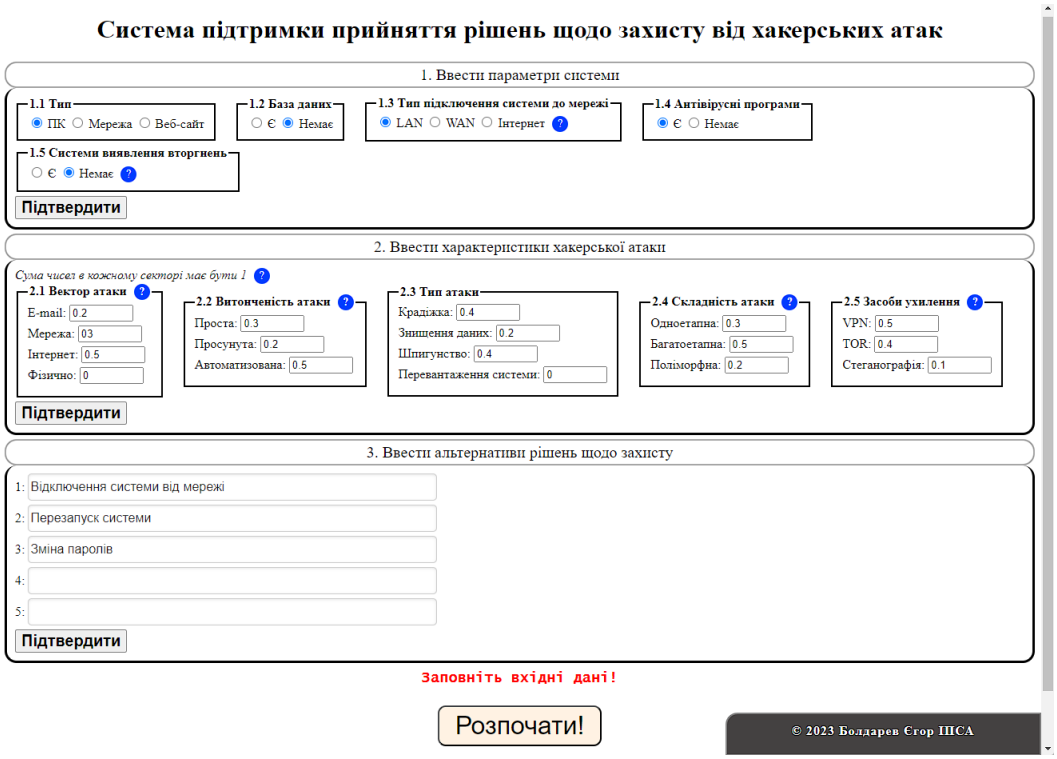


Рисунок 3.6 – Початкові експертні оцінки та альтернативи захисту.

		Відключення системи від мережі	Перезапуск системи	Зміна паролів
Вектор атаки	E-mail	Дуже сильно несумісні	Дуже сильно несумісні	Посередньо пов'язані
	Мережа	Дуже сильно пов'язані	Мало пов'язані	Мало пов'язані
	Інтернет	Дуже сильно пов'язані	Мало пов'язані	Дуже сильно пов'язані
	Фізично	Дуже сильно несумісні	Посередньо несумісні	Дуже сильно пов'язані
Витонченість атаки	Проста	Незалежні	Мала несумісність	Мало пов'язані
	Просунута	Незалежні	Мало пов'язані	Мало пов'язані
	Автоматизована	Мало пов'язані	Мало пов'язані	Посередньо пов'язані
Тип атаки	Крадіжка	Мало пов'язані	Мало пов'язані	Дуже сильно пов'язані
	Знищення даних	Посередньо пов'язані	Мало пов'язані	Мала несумісність
	Шпигунство	Дуже сильно пов'язані	Посередньо пов'язані	Посередньо пов'язані
	Перевантаження системи	Посередньо пов'язані	Посередньо пов'язані	Посередньо несумісні
Складність атаки	Одноетапна	Незалежні	Незалежні	Незалежні
	Багатоетапна	Незалежні	Мало пов'язані	Незалежні
	Поліморфна	Незалежні	Незалежні	Незалежні
Ухилення	VPN	Незалежні	Незалежні	Незалежні
	TOR	Незалежні	Незалежні	Незалежні
	Стеганографія	Незалежні	Незалежні	Незалежні

Отримати результат!

Рисунок 3.7 – Заповнена матриця зв’язків між характеристиками хакерських атак та альтернативами захисту.

На першому кроці виконання алгоритму відбувається процедура другого етапу двоетапного ММА для знаходження оцінок характеристик хакерських атак, враховуючи параметри цільової системи. В результаті виконання отримуються наступні оновлені оцінки (таблиця 3.14):

Таблиця 3.14 – Результат першого етапу алгоритму.

Вектор атаки	E-mail	0.1785120
	Мережа	0.3258595
	Інтернет	0.4956283
	Фізично	0
Витонченість атаки	Проста	0.1876094
	Просунута	0.1778815
	Автоматизована	0.6345089
Тип атаки	Крадіжка	0.3535353
	Знищення даних	0.0808080
	Шпигунство	0.5656565
	Перенавантаження системи	0
Складність атаки	Одноетапна	0.1842105
	Багатоетапна	0.4736842
	Поліморфна	0.3421052
Ухилення	VPN	0.5164034
	TOR	0.3645200
	Стеганографія	0.1190765

Другим кроком алгоритму виконання СППР є розрахунок ймовірностей всіх альтернатив параметрів хакерських атак з врахуванням зв’язків між ними на основі експертного оцінювання. Після розв’язку системи рівнянь Байєса, отримується наступні оновлені оцінки характеристик хакерських атак (таблиця 3.15):

Таблиця 3.15 – Результат виконання другого етапу алгоритму.

Вектор атаки	E-mail	0.0916052
	Мережа	0.2717113
	Інтернет	0.6366836
	Фізично	0
Витонченість атаки	Проста	0.0693509
	Просунута	0.1459473
	Автоматизована	0.7847018
Тип атаки	Крадіжка	0.3479400
	Знищення даних	0.0557542
	Шпигунство	0.5963058
	Перенавантаження системи	0
Складність атаки	Одноетапна	0.1713741
	Багатоетапна	0.4480947
	Поліморфна	0.3805312
Ухилення	VPN	0.5617013
	TOR	0.3592179
	Стеганографія	0.0790808

На третьому кроці алгоритму відбувається розрахунок оцінок результативності кожної з альтернатив стратегій захисту в умовах ситуації, заданої морфологічною таблицею характеристик хакерських атак. Покажемо перші 10 розрахованих величин очікуваної результативності для кожної альтернативи захисту за допомогою таблиці конфігурацій (таблиця 3.16):

Таблиця 3.16 – Величини очікуваної результативності для альтернатив захисту.

F_1	F_2	F_3	F_4	F_5	Зміна паролів	Відключення системи від мережі	Перезапуск системи
1	1	1	1	1	0.0000578829	0.0000434122	0.0006077714
1	1	1	1	2	0.0000411443	0.0000308582	0.0004320152
1	1	1	1	3	0.0000056002	0.0000042001	0.0000588021
1	1	1	2	1	0.0000703904	0.0000659910	0.0007390989
1	1	1	2	2	0.0000583739	0.0000547255	0.0006129261
1	1	1	2	3	0.0000088534	0.0000083000	0.0000929605
1	1	1	3	1	0.0000102378	0.0000076784	0.0001074969
1	1	1	3	2	0.0000090965	0.0000068224	0.0000955136
1	1	1	3	3	0.0000013867	0.0000010400	0.0000145605
1	1	2	1	1	0.0000120612	0.0000075382	0.0000452295

З таблиці величин очікуваної результативності для конфігурацій в подальшому розраховуються загальні величини очікуваної результативності для альтернатив захисту. В нашому випадку (таблиця 3.17):

Таблиця 3.17 – Результат виконання алгоритму СППР.

Зміна паролів	0.4227806447725351
Відключення системи від мережі	0.3336654021081129
Перезапуск системи	0.24355395311935193

Тобто, найбільш ефективною стратегією в цьому випадку буде заміна паролів.

Висновки до розділу 3

В даному розділі було наведено створені морфологічні таблиці для двоетапного MMMA з нерівномірним розподілом оцінок та обґрунтовано вибір інструментів для програмної реалізації СППР. Також булло детально розглянуто процес взаємодії користувача з СППР та алгоритм її виконання. В якості прикладу було наведено ситуацію, де цільовою системою є ПК середньостатистичного користувача та стандартні альтернативи захисту для нього: зміна паролів, відключення системи від мережі, перезапуск системи. В результаті, найбільш ефективною стратегією виявилась заміна паролів.

РОЗДІЛ 4 ФУНКЦІОНАЛЬНО-ВАРТІСНИЙ АНАЛІЗ

В даному розділі проводиться оцінювання основних характеристик для програмного продукту, розробленого для підтримки прийняття рішень щодо захисту від хакерських атак.

У даному дослідженні продемонстровано різні варіанти реалізації з метою забезпечення найбільш оптимальної стратегії вибору, яка впливає на економічні фактори та сумісність з майбутнім програмним продуктом. Для досягнення цієї мети було використано апарат функціонально-вартісного аналізу.

Функціонально-вартісний аналіз (далі ФВА) є технологією , що дозволяє оцінити реальну вартість продукту або послуги незалежно від організаційної структури компанії. ФВА проводиться з метою виявлення резервів зниження витрат за рахунок ефективніших варіантів виробництва, кращого співвідношення між споживчою вартістю виробу та витратами на його виготовлення. Для проведення аналізу використовується економічна, технічна та конструкторська інформація.

Алгоритм функціонально-вартісного аналізу включає в себе визначення послідовності етапів розробки продукту, визначення повних витрат (річних) та кількості робочих часів, визначення джерел витрат та кінцевий розрахунок вартості програмного продукту.

4.1 Постановка задачі проектування

Метод ФВА під час роботи застосовується для технічного-економічного аналізу розробки системи прогнозу стійкості фінансових показників. Рішення стосовно проектування та реалізації компонентів, що розробляється, впливають на всю систему, тож кожна окрема підсистема має її задовольняти. Тому фактичний аналіз представляє собою аналіз функцій програмного продукту, призначеного для збору, обробки та проведення аналізу даних по компанії.

Можна виділити наступні технічні вимоги до програмного продукту:

— Зручність та зрозумілість для користувача;

— Можливість зручного масштабування та обслуговування;

— Функціонування на персональних комп’ютерах із стандартним набором компонентів;

— Швидкість обробки даних та доступ до інформації в реальному часі;

— Мінімальні витрати на впровадження програмного продукту.

4.2 Обґрунтування функцій програмного продукту.

Головна функція F_0 – розробка можливого програмного продукту, яка дозволяє аналізувати різні характеристики, що безпосередньо впливають на стійкість підприємства. Беручи за основу цю функцію, можна виділити наступні:

F_1 – вибір мови програмування back-end частини.

F_2 – фреймворк для розробки користувацького інтерфейсу.

F_3 – середовище розробки.

Кожна з цих функцій має декілька варіантів реалізації (таблиця 4.1):

Таблиця 4.1 – Варіанти реалізацій функцій програмного продукту.

F_1	F_2	F_3
Python	Native HTML and CSS	Visual Studio Code
JavaScript	React.js	WebStorm
	Angular	IntelliJ IDEA

Варіанти реалізації функцій продемонстровано на морфологічній карті системи (рисунок 4.1). Морфологічна карта відображає множину всіх можливих варіантів основних функцій.

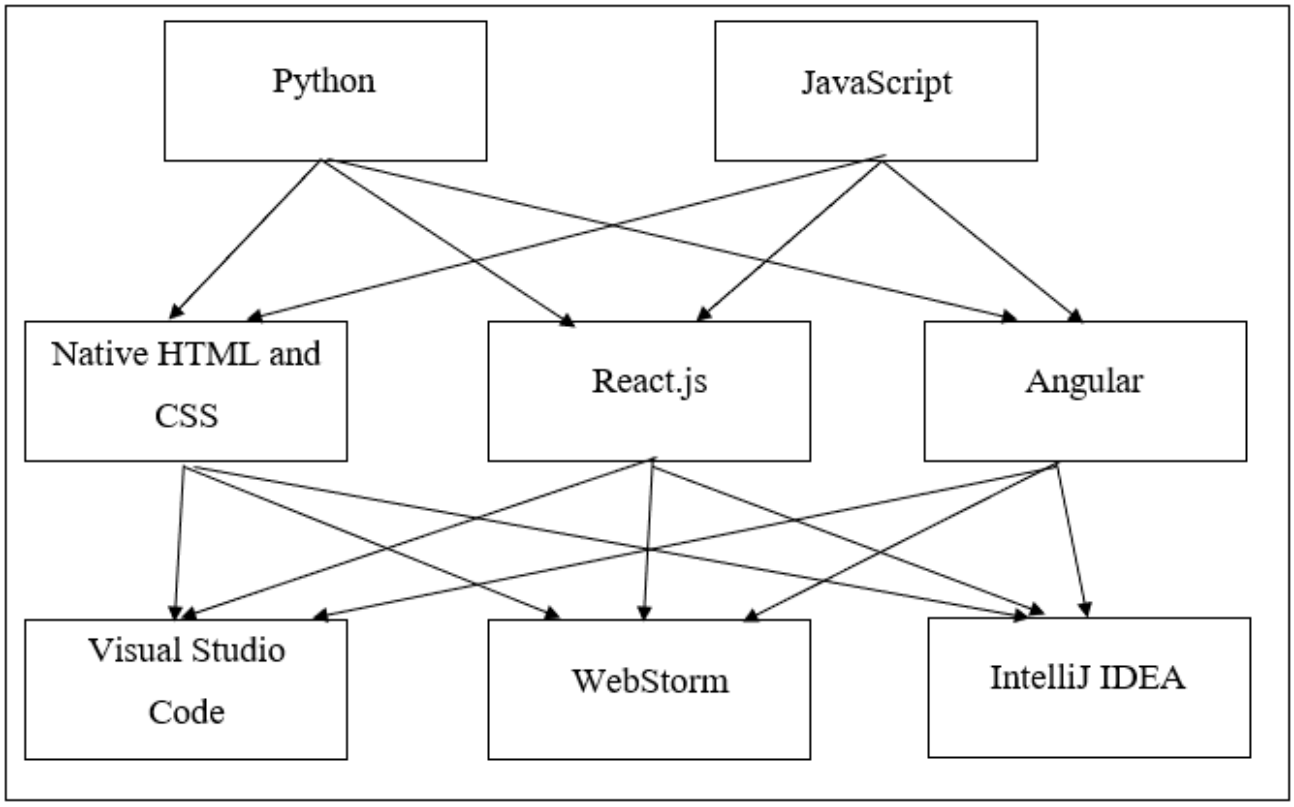


Рисунок 4.1 – Морфологічна карта.

Побудовану позитивно-негативну матрицю зображено в таблиці 4.2:

Таблиця 4.2 – Позитивно-негативна матриця.

Функції	Варіанти реалізації	Переваги	Недоліки
F_1	А	Простота вивчення, доступність бібліотек.	Низька швидкість роботи.
	Б	Клієнтська та серверна розробка, інтерактивність.	Безпека, відсутність типізації.
F_2	А	Швидкість завантаження, сумісність.	Обмежена гнучкість, великий об’єм коду.
	Б	Компонентний підхід, велика кількість сторонніх бібліотек та компонентів	Великий початковий поріг входу, необхідність використання інших інструментів
	В	Структурована архітектура, типізація.	Складність, обмежена гнучкість.
F_3	А	Легкість використання, швидкодія.	Обмежена функціональність для складних проектів.
	Б	Підтримка фреймворків, інтеграція з іншими інструментами.	Платна ліцензія, вимоги до системних ресурсів.
	В	Потужність та функціональність, підтримка фреймворків	Платна ліцензія.

З позитивно-негативної матриці робимо висновок, що, при розробці програмного продукту, деякі варіанти реалізації функції можна відкинути, тому що вони не відповідають поставленим перед програмним продуктом задачам.

Функція F_1*:*

Перевагу даємо інтерактивності. Для забезпечення швидкодії алгоритму варіант А має бути відкинутий.

Функція F_2*:*

Перевага надається сумісності та швидкодії. Тож відкидаються варіанти Б та В.

Функція F_3:

Хочемо забезпечити потужність та швидкодію. Залишаємо варіанти А та В. Таким чином, будемо розглядати такий варіанти реалізації ПП:

$$F_1\text{A} - F_2\text{A} - F_3\text{A}$$
$$F_1\text{A} - F_2\text{A} - F_3\text{B}$$

4.3 Обґрунтування системи параметрів програмного продукту

На основі даних, розглянутих вище, визначаються основні параметри вибору, які будуть використані для розрахунку коефіцієнта технічного рівня. Для того, щоб охарактеризувати програмний продукт, будемо використовувати наступні параметри:

- *X1* – швидкодія мови програмування;
- *X2* – об’єм пам’яті для обчислень та збереження даних;
- *X3* – час навчання даних;
- *X4* – потенційний об’єм програмного коду.

Гірші, середні і кращі значення параметрів вибираються на основі вимог замовника й умов, що характеризують експлуатацію програмного продукту, як показано у таблиці 4.3.

Таблиця 4.3 – Основні параметри програмного продукту.

Назва Параметра	Умовні позначення	Одиниці виміру	Значення параметра		
			гірші	середні	кращі
Швидкодія мови програмування	X1	оп/мс	9000	15000	28000
Об’єм пам’яті	X2	Мб	512	128	64
Час попередньої обробки даних	X3	мс	10	5	2
Потенційний об’єм програмного коду	X4	кількість рядків коду	1200	800	500

За даними таблиці 4.3, побудуємо графічні характеристики параметрів (рис. 4.2 – 4.5):

Рисунок 4.2 – X1, швидкодія мови програмування

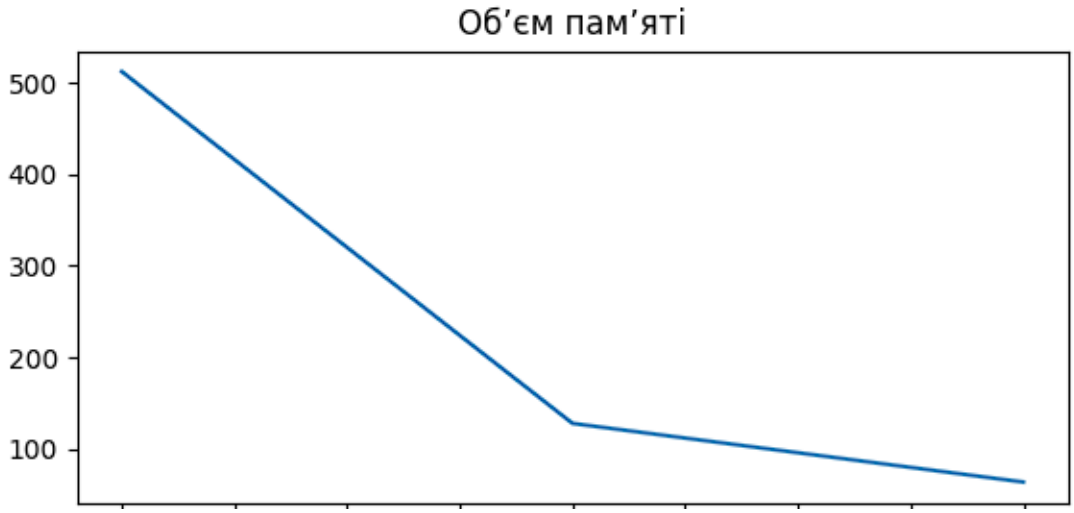


Рисунок 4.3 – X2, об’єм пам’яті

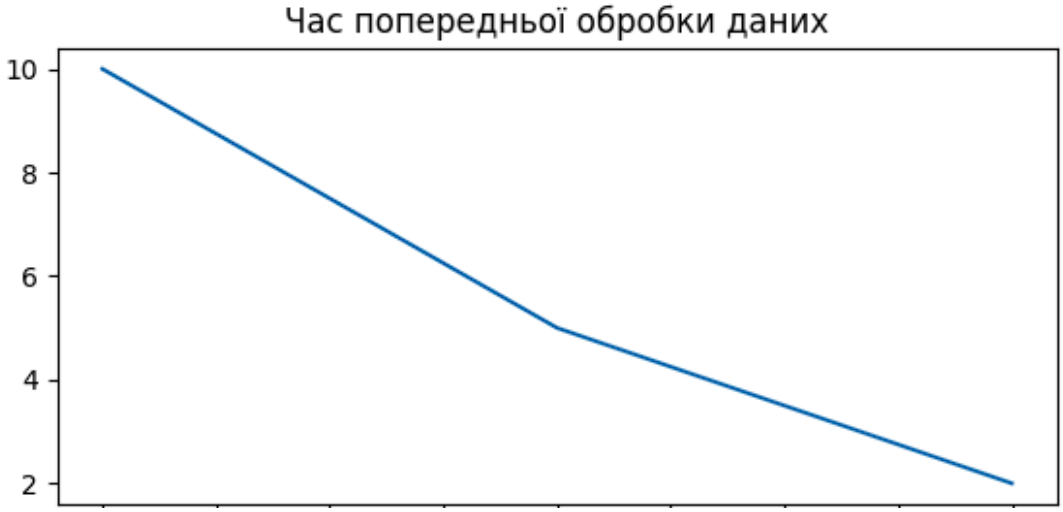


Рисунок 4.4 – X3, час попередньої обробки даних

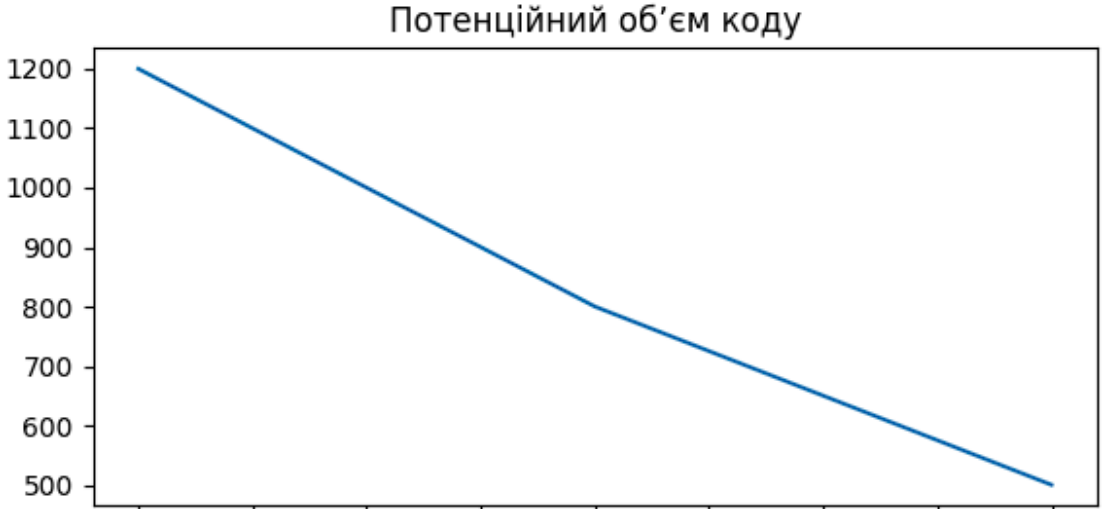


Рисунок 4.5 – X4, потенційний об’єм програмного коду

4.4 Аналіз експертного оцінювання параметрів

Після детального обговорення й аналізу кожний експерт оцінює стуЗпінь важливості кожного параметру для розробки конкретно поставленого програмного продукту.

Значимість кожного параметра визначається методом попарного порівняння. Оцінку проводить експертна комісія із 7 людей. Визначення коефіцієнтів значимості передбачає:

- визначення рівня значимості параметра шляхом присвоєння різних рангів;
- перевірку придатності експертних оцінок для подальшого використання;
- визначення оцінки попарного пріоритету параметрів;
- обробку результатів та визначення коефіцієнту значимості.

Результати експертного ранжування наведені у таблиці 4.4:

Таблиця 4.4 – Результати ранжування параметрів.

Позначення параметра	Назва параметра	Одиниці виміру	Ранг параметра за оцінкою експерта							Сума рангів R_i	Відхилення Δ_i	Δ_i^2
			1	2	3	4	5	6	7			
X1	Швидкодія мови програмування	оп/мс	2	1	1	2	1	1	2	10	-7.5	56.25
X2	Об’єм пам’яті	Мб	3	2	4	4	3	3	3	22	4.5	20.25
X3	Час попередньої обробки даних	мс	1	3	2	1	2	2	1	12	-5.5	30.25
X4	Потенційний об’єм коду	Кількість рядків коду	4	4	3	3	4	4	4	26	8.5	72.25
	Разом		10	10	10	10	10	10	10	70	0	179

Для перевірки степені достовірності експертних оцінок, визначимо наступні параметри:

а) сума рангів кожного з параметрів і загальна сума рангів:

$$R_i = \sum_{j=1}^{N} r_{ij} R_{ij} = \frac{Nn(n+1)}{2} = 70, \quad (4.1)$$

де N – число експертів, n – кількість параметрів;

б) середня сума рангів:

$$T = \frac{1}{n} R_i = 17{,}5 \quad (4.2)$$

в) відхилення суми рангів кожного параметра від середньої суми рангів:

$$\Delta_i = R_i - T. \tag{4.3}$$

Сума відхилень по всім параметрам повинна дорівнювати 0;

г)загальна сума квадратів відхилення:

$$S = \sum_{i=1}^{N} \Delta_i^2 = 179. \tag{4.4}$$

Порахуємо коефіцієнт узгодженості:

$$W = \frac{12S}{N^2(n^3 - n)} = \frac{12 \cdot 179}{7^2(4^3 - 4)} = 0.7306 > W_k = 0.67. \tag{4.5}$$

Ранжування можна вважати достовірним, тому що знайдений коефіцієнт узгодженості перевищує нормативний, котрий дорівнює 0,67.

Скориставшись результатами ранжирування, проведемо попарне порівняння всіх параметрів і результати занесемо у таблицю 4.5.

Таблиця 4.5 – Попарне порівняння параметрів.

Параметри	Експерти							Кінцева оцінка	Числове значення
	1	2	3	4	5	6	7		
X1 і X2	<	<	<	<	<	<	<	<	0,5
X1 і X3	>	<	<	>	<	<	>	<	0,5
X1 і X4	<	<	<	<	<	<	<	<	0,5
X2 і X3	>	<	>	>	>	>	>	>	1,5
X2 і X4	<	<	>	>	<	<	<	<	0,5
X3 і X4	<	<	<	<	<	<	<	<	0,5

Числове значення, що визначає ступінь переваги *i*–го параметра над *j*–тим, a_{ij} визначається по формулі:

$$a_{ij} = \begin{cases} 1.5 \text{ при } X_i > X_j \\ 1.0 \text{ при } X_i = X_j \\ 0.5 \text{ при } X_i < X_j \end{cases}. \quad (4.6)$$

З отриманих числових оцінок переваги складемо матрицю А=$\| a_{ij} \|$.

Для кожного параметра зробимо розрахунок вагомості $K_{\text{ві}}$ за наступними формулами:

$$K_{\text{ві}} = \frac{b_i}{\sum_{i=1}^{n} b_i} \quad (4.7)$$

$$b_i = \sum_{i=1}^{N} a_{ij} \quad (4.8)$$

Відносні оцінки розраховуються декілька разів доти, поки наступні значення не будуть незначно відрізнятися від попередніх (менше 2%). На другому і наступних кроках відносні оцінки розраховуються за наступними формулами:

$$K_{\text{ві}} = \frac{b_i'}{\sum_{i=1}^{n} b_i'}, \quad (4.9)$$

$$b_i' = \sum_{i=1}^{N} a_{ij} b_j \quad (4.10)$$

Розрахунки вагомості параметрів зображено в таблиці 4.6:

Таблиця 4.6 – Розрахунок вагомості параметрів.

Параметри x_i	Параметри x_j				Перша ітерація		Друга ітерація	
	X1	X2	X3	X4	b_i	$K_{\text{ві}}$	b_i^1	$K_{\text{ві}}^1$
X1	1	0,5	0,5	0,5	2,5	0.156	9,25	0.157
X2	1,5	1	1,5	0,5	4,5	0.281	16,25	0.275
X3	1,5	0,5	1	0,5	3,5	0.219	12,25	0.208
X4	1,5	1,5	1,5	1	5,5	0.344	21,25	0.360
Всього:					16	1	59	1

Як видно з таблиці 4.6, різниця значень коефіцієнтів вагомості не перевищує 2%, тому більшої кількості ітерацій не потрібно.

4.5 Аналіз рівня якості варіантів реалізації функцій

Визначимо рівень якості кожного варіанту виконання основних функцій окремо. Абсолютні значення параметрів *X2* (Об'єм пам'яті), *X3* (час попередньої обробки даних) та *X4* (потенційний об'єм програмного коду) відповідають технічним вимогам умов функціонування даного ПП. Абсолютне значення параметра *X1* (швидкість роботи мови програмування) обрано оптимальним.

Коефіцієнт технічного рівня для кожного варіанта реалізації ПП розраховується наступним чином:

$$K_K(j) = \sum_{i=1}^{n} K_{вij} B_{ij}\,, \qquad (4.11)$$

де n – кількість параметрів, $K_{вi}$ – коефіцієнт вагомості i–го параметра, B_i – оцінка i–го параметра в балах.

Розрахунок показників рівня якості варіантів реалізації основних функцій продемонстровано на таблиці 4.7:

Таблиця 4.7 – Розрахунок показників рівня якості варіантів реалізації основних функцій ПП.

Основні функції	Варіант реалізації функції	Параметри	Абсолютне значення параметра	Бальна оцінка параметра	Коефіцієнт вагомості параметра	Коефіцієнт рівня якості
F1	Б	X1	10000	8	0,157	1.256
F2	А	X2	64	9	0,275	2.475
F3	А	X4	800	6	0,360	2.16
	В	X4	900	5	0,360	1.8

За даними з таблиці 4.7 за формулою:

$$K_K = K_{\text{ТУ}}[F_{1k}] + K_{\text{ТУ}}[F_{2k}] + \ldots + K_{\text{ТУ}}[F_{zk}], \qquad (4.12)$$

визначаємо рівень якості кожного з варіантів:

$$K_{K1} = 1{,}256 + 2{,}475 + 2{,}16 = 5.891;$$
$$K_{K2} = 1{,}8 + 2{,}475 + 1{,}8 = 5.531.$$

Як видно з розрахунків, кращим є перший варіант, для якого коефіцієнт технічного рівня має найбільше значення.

4.6 Економічний аналіз варіантів розробки ПП

Для визначення вартості розробки ПП спочатку проведемо розрахунок трудомісткості. Всі варіанти включають в себе два окремих завдання:

1. Розробка проекту програмного продукту;
2. Розробка програмної оболонки;

Завдання 1, за ступенем новизни, відноситься до групи А, завдання 2 – до групи Б. За складністю алгоритми, які використовуються в завданні 1 належать до групи 1; а в завданні 2 – до групи 3.

Для реалізації завдання 1 використовується довідкова інформація, а завдання 2 використовує інформацію у вигляді даних.

Проведемо розрахунок часу на розробку та програмування для кожного з завдань.

Загальна трудомісткість обчислюється як:

$$T_O = T_P \cdot K_П \cdot K_{СК} \cdot K_M \cdot K_{СТ} \cdot K_{СТ.М}, \quad (4.13)$$

де T_P – трудомісткість розробки ПП, $K_П$ – поправочний коефіцієнт, $K_{СК}$ – коефіцієнт на складність вхідної інформації, K_M – коефіцієнт рівня мови програмування, $K_{СТ}$ – коефіцієнт використання стандартних модулів і прикладних програм $K_{СТ.М}$ – коефіцієнт стандартного математичного забезпечення.

Для першого завдання, виходячи із норм часу для завдань розрахункового характеру степеню новизни А та групи складності алгоритму 1, трудомісткість дорівнює: T_P =31 людино-днів. Поправочний коефіцієнт, який враховує вид нормативно-довідкової інформації для першого завдання: $K_П$ = 1.6. Поправочний

коефіцієнт, який враховує складність контролю вхідної та вихідної інформації для всіх завдань рівний 1: $К_{СК} = 1$. Оскільки при розробці першого завдання використовуються стандартні модулі, врахуємо це за допомогою коефіцієнта $К_{СТ} = 0.9$. Тоді загальна трудомісткість програмування першого завдання дорівнює:

$$Т_1 = 31 \cdot 1.6 \cdot 0.9 = 44.64 \text{ людино-днів.}$$

Проведемо аналогічні розрахунки для подальших завдань.

Для другого завдання (використовується алгоритм третьої групи складності, степінь новизни Б), тобто $Т_Р = 20$ людино-днів, $К_П = 0.95$, $К_{СК} = 1$, $К_{СТ} = 0.9$:

$$Т_2 = 29 \cdot 0.95 \cdot 0.9 = 17.1 \text{ людино-днів.}$$

Складаємо трудомісткість відповідних завдань для кожного з обраних варіантів реалізації програми, щоб отримати їх трудомісткість:

$$Т_I = (44.64 + 17.1 + 7.12 + 17.1) \cdot 8 = 687.68 \text{ людино-годин.}$$

$$Т_{II} = (44.64 + 17.1 + 5.68 + 17.1) \cdot 8 = 676.16 \text{ людино-годин.}$$

Найбільш високу трудомісткість має варіант I.

В розробці беруть участь два програмісти з окладом 21000 грн. та один Quality Assurance інженер з окладом 20000. Визначимо середню зарплату за годину за формулою:

$$С_Ч = \frac{М}{T_m \cdot t} \text{ грн.,} \qquad (4.14)$$

де М – місячний оклад працівників, T_m – кількість робочих днів тиждень, t – кількість робочих годин в день.

$$С_ч = \frac{21000 + 21000 + 20000}{3 \cdot 3 \cdot 7 \cdot 8} = 123.01 \text{ грн.} \quad (4.15)$$

Тоді, розрахуємо заробітну плату за формулою:

$$С_{ЗП} = С_ч \cdot Т_i \cdot К_Д, \quad (4.16)$$

де $С_ч$– величина погодинної оплати праці працівника, $Т_i$ – трудомісткість відповідного завдання, $К_Д$ – норматив, який враховує додаткову заробітну плату.

Зарплата розробників за варіантами становить:

I. $С_{ЗП} = 123.01 \cdot 687.68 \cdot 1.2 = 101509.82$ грн.

II. $С_{ЗП} = 123.01 \cdot 676.16 \cdot 1.2 = 99809.32$ грн.

Відрахування на єдиний соціальний внесок становить 22%, але максимальна сума ЄСВ становить 22110 грн.:

I. $С_{ВІД} = С_{ЗП} \cdot 0.22 = 101\ 509.82 \cdot 0.22 = 22332.16$ грн. => 22110 грн.

II. $С_{ВІД} = С_{ЗП} \cdot 0.22 = 99\ 809.32 \cdot 0.22 = 21958.05$ грн.

Тепер визначимо витрати на оплату однієї машино-години. ($С_М$)

Так як одна ЕОМ обслуговує одного програміста з окладом 21000 грн., з коефіцієнтом зайнятості 0,2 то для однієї машини отримаємо:

$$С_Г = 12 \cdot М \cdot К_З = 12 \cdot 21000 \cdot 0,2 = 50400 \text{ грн.}$$

З урахуванням додаткової заробітної плати:

$$С_{ЗП} = С_Г \cdot (1 + К_З) = 50400 \cdot (1 + 0.2) = 60480 \text{ грн.}$$

Відрахування на соціальний внесок:

$$С_{ВІД} = С_{ЗП} \cdot 0.22 = 60480 \cdot 0,22 = 13305,6 \text{ грн.}$$

Амортизаційні відрахування розраховуємо при амортизації 25% та вартості ЕОМ – 12000 грн.

$$С_А = К_{ТМ} \cdot К_А \cdot Ц_{ПР} = 1.4 \cdot 0.25 \cdot 12000 = 4200 \text{ грн.},$$

де $К_{ТМ}$– коефіцієнт, який враховує витрати на транспортування та монтаж приладу у користувача, $К_А$– річна норма амортизації, $Ц_{ПР}$– договірна ціна приладу.

Витрати на ремонт та профілактику розраховуємо як:

$$С_Р = К_{ТМ} \cdot Ц_{ПР} \cdot К_Р = 1.4 \cdot 12000 \cdot 0.08 = 1344 \text{ грн.},$$

де $К_Р$ – відсоток витрат на поточні ремонти.

Ефективний годинний фонд часу ПК за рік розраховуємо за формулою:

$$Т_{ЕФ} =(Д_К – Д_В – Д_С – Д_Р) \cdot t_З \cdot К_В = (365 – 100 – 12 – 16) \cdot 8 \cdot 0.35 = 663,6 \text{ години},$$

де $Д_К$ – календарна кількість днів у році, $Д_В$, $Д_С$ – відповідно кількість вихідних та святкових днів, $Д_Р$ – кількість днів планових ремонтів устаткування, t –кількість робочих годин в день, $К_В$– коефіцієнт використання приладу у часі протягом зміни.

Витрати на оплату електроенергії розраховуємо за формулою:

$$С_{ЕЛ} = Т_{ЕФ} \cdot N_С \cdot К_З \cdot Ц_{ЕН} = 663,6 \cdot 0,15 \cdot 0,25 \cdot 4,87 = 121,18 \text{ грн.},$$

де $N_С$ – середньо-споживча потужність приладу, $К_З$ – коефіцієнтом зайнятості приладу, $Ц_{ЕН}$ – тариф за 1 КВт-годин електроенергії.

Накладні витрати розраховуємо за формулою:

$$С_Н = Ц_{ПР} \cdot 0.67 = 12000 \cdot 0,67 = 8040 \text{ грн.}$$

Тоді, річні експлуатаційні витрати будуть:

$$С_{ЕКС} = С_{ЗП} + С_{ВІД} + С_А + С_Р + С_{ЕЛ} + С_Н, \qquad (4.17)$$

$$С_{ЕКС} = 60480 + 13305,6 + 4200 + 1344 + 121,18 + 8040 = 87490,78 \text{ грн.}$$

Собівартість однієї машино-години ЕОМ дорівнюватиме:

$$С_{М\text{-}Г} = С_{ЕКС} / Т_{ЕФ} = 87490,78 / 663,6 = 131,84 \text{ грн/год.}$$

Оскільки в даному випадку всі роботи, які пов‘язані з розробкою програмного продукту ведуться на ЕОМ, витрати на оплату машинного часу, в залежності від обраного варіанта реалізації, складає:

$$C_М = C_{М-Г} \cdot Т, \quad (4.18)$$

I. $C_М = 131,84 \cdot 687,68 = 90663,73$ грн.

II. $C_М = 131,84 \cdot 676,16 = 89144,93$ грн.

Накладні витрати складають 67% від заробітної плати:

$$C_Н = C_{ЗП} \cdot 0,67, \quad (4.19)$$

I. $C_Н = 101509,82 \cdot 0,67 = 68011,57$ грн.

II. $C_Н = 99809,32 \cdot 0,67 = 66872,24$ грн.

Отже, вартість розробки ПП за варіантами становить:

$$C_{ПП} = C_{ЗП} + C_{ВІД} + C_М + C_Н, \quad (4.20)$$

I. $C_{ПП} = 101509,82 + 22110 + 90663,73 + 68011,57 = 282295,12$ грн.

II. $C_{ПП} = 99809,32 + 21958,05 + 89144,93 + 66872,24 = 277784,54$ грн.

4.7 Вибір кращого варіанту ПП техніко-економічного рівня

Розрахуємо коефіцієнт техніко-економічного рівня за формулою:

$$К_{ТЕР j} = К_{Кj} / С_{ППj}, \quad (4.21)$$

$$К_{ТЕР1} = 5{,}891 / 282295{,}12 = 2{,}086 \cdot 10^{-5},$$
$$К_{ТЕР2} = 5{,}531 / 277784{,}54 = 1{,}991 \cdot 10^{-5}.$$

Як бачимо, найбільш ефективним є перший варіант реалізації програми з коефіцієнтом техніко-економічного рівня $К_{ТЕР1} = 2{,}086 \cdot 10^{-5}$.

З проведеного аналізу можна зробити висновок, що з альтернатив, які залишились після першого відбору двох варіантів виконання програмного продукту, оптимальним є перший варіант реалізації. Цей варіант реалізації програмного продукту має такі параметри:

- Мова програмування Back-End частини – JavaScript.
- Фреймворк для розробки користувацького інтерфейсу – Native HTML and CSS.
- Середовище розробки – Visual Studio Code.

Висновки до розділу 4

В даному розділі було проведено функціонально-вартісний аналіз програмного продукту та розраховано оцінку основних функцій продукту.

В результаті проведеного аналізу програмного комплексу, що розробляється, окрім визначення оцінок основних функцій ПП, було знайдено параметри, що характеризують продукт.

Проведений аналіз допоміг зробити висновки щодо найбільш оптимального варіанту реалізації програмного продукту.

ВИСНОВКИ

В наш час цифрова безпека є одним з найактуальніших проблем. Все більше сервісів інтегрується в цифровий простір, і все більше чутливих даних потрапляє в мережу. Вся цифрова інформація є ціллю хакерських атак, тож дуже важливо вживати ефективні запобіжні заходи та швидко реагувати на потенційну безпеку.

Під час виконання роботи було проаналізовано літературу щодо хакерських атак. Внаслідок чого було побудовано морфологічні таблиці для характеристик хакерських атак та параметрів системи-цілі атаки. Проведено двоетапний модифікований морфологічний аналіз з нерівномірним розподілом початкових оцінок. Цей метод дозволяє врахувати вплив оцінок параметрів системи-цілі хакерської атаки на оцінки характеристик атаки.

В результаті було розроблено програмний продукт з веб-інтерфейсом, що слугує системою підтримки прийняття рішень щодо захисту від хакерських атак. Програма пропонує простий та доступний інтерфейс. Під час виконання роботи було проведено функціонально-вартісний аналіз програмного продукту.

В якості подальшого розвитку програмного продукту пропонується залучення баз даних та збору даних користувачів. При реалізації такого сценарію розвитку можна досягти часткової, або навіть повної автоматизації роботи СППР.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Савченко І.О. Методологічне і математичне забезпечення розв’язання задач передбачення на основі модифікованого методу морфологічного аналізу. *Системні дослідження та інформаційні технології*. 2011. № 3. С. 18–28.
2. Cyberattack. *Wikipedia*. URL: https://en.wikipedia.org/wiki/Cyberattack
3. Dr. Yusuf P., Syed Q.A., Jai P.D., Dr. Nikhat A., Anurag K.J. A Systematic Literature Review on the Cyber Security. *International Journal of Scientific Research and Management*. 2021. No. 9. P. 669-710.
4. What is Steganography? *PureVPN*. URL: https://www.purevpn.com/blog/what-is-steganography/
5. IBM QRadar. *IBM*. URL: https://www.ibm.com/qradar
6. FireEye Threat Intelligence. *Intelligence FireEye*. URL: https://intelligence.fireeye.com/
7. FireEye Threat Intelligence product demo. FireEye. URL: https://content.fireeye.com/product-demo/website-fireeye-intelligence-portal
8. Palo Alto Networks Next-Generation Firewall. *Palo Alto Networks*. URL: https://www.paloaltonetworks.com/network-security/next-generation-firewall
9. Яловий Г.К., Пашін В.П., Сичов В.С. Економіка та організація виробництва. Навчальне видання. Київ: "Політехніка", 2004, 80 с.
10. Богданюк В.Є., Березовський К.В., Пашін В.П. Методичні вказівки до виконання організаційно-економічного розділу дипломних проектів. Уклад. Київ: НТУУ "КПІ", 1999, 66 с.

ДОДАТОК А ЛІСТИНГ ПРОГРАМИ

– index.html

```
<!DOCTYPE html>
<html>
<head>
	<meta charset="UTF-8">
	<title>СППР «Захист від хакерських атак»</title>
    <link rel="stylesheet" type="text/css" href="style.css">
</head>
<body>
	<header>
		<h1>Система підтримки прийняття рішень щодо захисту від хакерських атак</h1>
	</header>

   <div id="overlay"></div>

   <div id="system-parameters-open" class="open-form-button">1. Ввести параметри системи</div>

	<form id="system-parameters" class="input-form">
		<fieldset>
			<legend>1.1 Тип</legend>
			 <label><input type="radio" name="sysType" value="PC"> ПК</label>
			 <label><input type="radio" name="sysType" value="Network"> Мережа</label>
			 <label><input type="radio" name="sysType" value="Website"> Веб-сайт</label>
		</fieldset>

		<fieldset>
			<legend>1.2 База даних</legend>
			 <label><input type="radio" name="isSysDB" value="sysDbTrue"> Є</label>
			 <label><input type="radio" name="isSysDB" value="sysDbFalse"> Немає</label>
		</fieldset>

		<fieldset>
			<legend>1.3 Тип підключення системи до мережі</legend>
		    <label><input    type="radio"    name="sysNetworkConnectionType"    value="LAN">
LAN</label>
			 <label><input   type="radio"   name="sysNetworkConnectionType"   value="WAN">
WAN</label>
			 <label><input   type="radio"   name="sysNetworkConnectionType"   value="Net">
Інтернет</label>
	      <a id="system-connection-hint" class="hint">?</a>
		</fieldset>
```

```
              <fieldset>
                     <legend>1.4 Антівірусні програми</legend>
                      <label><input type="radio" name="isAntivirus" value="antivirusTrue"> Є</label>
                      <label><input    type="radio"    name="isAntivirus"    value="antivirusFalse">
Немає</label>
              </fieldset>

              <fieldset>
                     <legend>1.5 Системи виявлення вторгнень</legend>
            <label><input type="radio" name="isDetection" value="detectionTrue"> Є</label>
            <label><input type="radio" name="isDetection" value="detectionFalse"> Немає</label>
            <a id="detection-hint" class="hint">?</a>
              </fieldset>

      <span class="warning-message"><b>Відповідь не було збережено!</b> Введіть всі параметри.</span>
              <button       id="system-parameters-confirm"       type="button"       class="submit-
button">Підтвердити</button>
       </form>

   <div  id="attack-parameters-open"  class="open-form-button">2.  Ввести  характеристики  хакерської
атаки</div>

   <form id="attack-parameters" class="input-form">
      <label style="display: block;"><i>Сума чисел в кожному секторі має бути 1</i> <a id="general-
attack-hint" class="hint">?</a> </label>
              <fieldset>
                     <legend>2.1 Вектор атаки <a id="vector-hint" class="hint">?</a> </legend>
                      <div>
               E-mail:
               <input type="number" min="0" max="1" step="0.05" value="0" name="Email"/>
            </div>
                      <div>
               Мережа:
               <input type="number" min="0" max="1" step="0.05" value="0" name="Network"/>
            </div>
                      <div>
               Інтернет:
               <input type="number" min="0" max="1" step="0.05" value="0" name="Internet"/>
            </div>
            <div>
               Фізично:
               <input type="number" min="0" max="1" step="0.05" value="0" name="Physically"/>
            </div>
              </fieldset>

              <fieldset>
                     <legend>2.2  Витонченість  атаки  <a  id="elegance-hint"  class="hint">?</a>
</legend>
```

```
            <div>
               Проста:
               <input type="number" min="0" max="1" step="0.05" value="0" name="Simple"/>
            </div>
            <div>
               Просунута:
               <input type="number" min="0" max="1" step="0.05" value="0" name="Complex"/>
            </div>
            <div>
               Автоматизована:
               <input type="number" min="0" max="1" step="0.05" value="0" name="Automatic"/>
            </div>
              </fieldset>

              <fieldset>
                     <legend>2.3 Тип атаки</legend>
            <div>
               Крадіжка:
               <input type="number" min="0" max="1" step="0.05" value="0" name="Steal"/>
            </div>
            <div>
               Знищення даних:
               <input type="number" min="0" max="1" step="0.05" value="0" name="Destruction"/>
            </div>
            <div>
               Шпигунство:
               <input type="number" min="0" max="1" step="0.05" value="0" name="Espionage"/>
            </div>
            <div>
               Перевантаження системи:
               <input type="number" min="0" max="1" step="0.05" value="0" name="Overload"/>
            </div>
              </fieldset>

              <fieldset>
                     <legend>2.4 Складність атаки <a id="complexity-hint" class="hint">?</a>
</legend>
            <div>
               Одноетапна:
               <input type="number" min="0" max="1" step="0.05" value="0" name="OneStep"/>
            </div>
            <div>
               Багатоетапна:
               <input type="number" min="0" max="1" step="0.05" value="0" name="MultiStep"/>
            </div>
            <div>
               Поліморфна:
               <input type="number" min="0" max="1" step="0.05" value="0" name="Polymorph"/>
            </div>
```

```
            </fieldset>

            <fieldset>
                    <legend>2.5 Засоби ухилення <a id="evasion-hint" class="hint">?</a> </legend>
          <div>
             VPN:
             <input type="number" min="0" max="1" step="0.05" value="0" name="VPN"/>
          </div>
          <div>
             TOR:
             <input type="number" min="0" max="1" step="0.05" value="0" name="TOR"/>
          </div>
          <div>
             Стеганографія:
             <input type="number" min="0" max="1" step="0.05" value="0" name="Steganography"/>
          </div>
            </fieldset>

      <span class="warning-message"><b>Відповідь не було збережено!</b> Перевірте, що сума оцінок в кожному секторі дорівнює 1.</span>
            <button id="attack-parameters-confirm" type="button" class="submit-button">Підтвердити</button>
        </form>

   <div id="resolve-alternatives-open" class="open-form-button">3. Ввести альтернативи рішень щодо захисту</div>

   <form id="resolve-alternatives" class="input-form">
          <div>
            <label for="alt1st">1:</label>
            <input type="text" id="alt1st" value="Відключення системи від мережі" />
          </div>
          <div>
            <label for="alt2nd">2:</label>
            <input type="text" id="alt2nd" value="Перезапуск системи" />
          </div>
          <div>
            <label for="alt3rd">3:</label>
            <input type="text" id="alt3rd" value="Зміна паролів" />
          </div>
          <div>
            <label for="alt4th">4:</label>
            <input type="text" id="alt4th" />
          </div>
          <div>
            <label for="alt5th">5:</label>
            <input type="text" id="alt5th" />
          </div>
```

```
        <span class="warning-message"><b>Відповідь не було збережено!</b> Введіть принаймні дві альтернативи.</span>
        <button id="resolve-alternatives-confirm" type="button" class="submit-button">Підтвердити</button>
   </form>

   <span id="begin-warning" class="warning-message"><b>Заповніть вхідні дані!</b></span>
   <button id="start-algorithm-button">Розпочати!</button>

   <div id="table-block">
      <span id="table-warning" class="warning-message"><b>Дані не збережено! Будь ласка, введіть оцінки.</b></span>
   </div>

   <span id="missing-data-warning" class="warning-message">Схоже, що дані не було повністю збережено. Перевірте, будь ласка, введені дані.</span>
   <button id="get-result-button">Отримати результат!</button>

   <span id="result"></span>


        <footer>
                <p>&copy; 2023 Болдарев Єгор ІПСА</p>
        </footer>

   <script type="module" src="script.js"></script>
</body>
</html>
```

– style.css

```
.input-form{
    display: none;
}

h1{
    text-align: center;
}

.check-mark{
    color: green;
}

.open-form-button{
    background-color: #FFFFFF;
    color: #000000;
    border: 2px solid #A6A6A6;
```

```
    padding: 3px;
    text-align: center;
    position: relative;
    cursor: pointer;
    border-radius: 15px;
    font-size: 20px;
}

div {
    margin-bottom: 5px;
  }

fieldset {
    display: inline-block;
    vertical-align: middle;
    margin-right: 20px;
    border: 2px solid black;
    margin-bottom: 5px;
}

legend {
    font-weight: bold;
}

form{
    padding: 10px;
    border-left: 3px solid black;
    border-right: 3px solid black;
    border-bottom: 3px solid black;
    border-radius: 15px;
    margin-bottom: 5px;
    margin-top: -5px;
}

.submit-button{
    display:block;
    font-size: 20px;
    font-weight: bold;
}

.warning-message{
    display: none;
    color: red;
    margin: 5px;
    font-size: 18px;
    font-family: "Lucida Console", sans-serif;
}

#begin-warning{
```

```
    margin: 10px 10px 0px 10px;
    text-align: center;
}

#table-warning{
    margin: 10px 10px 0px 10px;
    text-align: center;
}

#start-algorithm-button{
    display: block;
    border-radius: 10px;
    font-size: 200%;
    width: fit-content;
    margin: 25px auto;
    padding: 5px 20px;
    background-color:rgba(255, 228, 196, 0.466);
    cursor: pointer;
}

#get-result-button{
    display: none;
    border-radius: 10px;
    font-size: 200%;
    width: fit-content;
    margin: 25px auto;
    padding: 5px 20px;
    background-color:rgba(255, 228, 196, 0.466);
    cursor: pointer;
}

input[type="text"] {
    width: 40%;
    height: 30px;
    border: 1px solid #ccc;
    border-radius: 5px;
    font-size: 16px;
    color: #333;
    background-color: #fff;
    box-shadow: inset 0 1px 3px rgba(0, 0, 0, 0.1);
    outline: none;
}

input[type="text"]:focus {
    border-color: #6d9ed9;
    box-shadow: 0 0 5px rgba(109, 158, 217, 0.5);
}

table {
```

```
    border-collapse: collapse;
    width: 100%;
}

th, td {
    border: 1px solid black;
    padding: 3px;
    text-align: center;
}

th {
    background-color: #ddd;
}

select {
    width: max-content;
    padding: 5px;
    font-size: 16px;
    cursor: pointer;
}

.attack-parameters-select{
    font-size: 14px;
    padding: 2px;
}

#table-block {
    margin-top: 20px;
}

body{
    padding-bottom: 50px;
}

footer {
    position: fixed;
    bottom: 0;
    right: 0;
    left: auto;
    width: 30%;
    height: 50px;
    color: #fff;
    text-align: center;
    background: #444141;
    border-top-left-radius: 15px;
    border: 2px solid grey;
}

footer p{
```

```
    font-weight: bold;
    margin: 0;
    padding: 3% 0px;
    text-shadow:
        -1px -1px 0 #000,
        1px -1px 0 #000,
        -1px  1px 0 #000,
        1px  1px 0 #000;
    letter-spacing: 1px;
}

#result{
    display: none;
    border: 3px solid green;
    font-size: 24px;
    padding: 10px;
    margin: 0 12%;
}

pre{
    margin: 10px;
}

#missing-data-warning{
    margin-top: 20px;
    text-align: center;
    font-size: 22px;
    font-weight: bolder;
}

#overlay {
    display: none;
    position: fixed;
    top: 0;
    left: 0;
    width: 100%;
    height: 100%;
    background-color: rgba(0, 0, 0, 0.5);
    z-index: 9998;
}

#popup {
    display: none;
    position: fixed;
    top: 50%;
    left: 50%;
    transform: translate(-50%, -50%);
    background-color: white;
    padding: 20px;
```

```
    border: 1px solid black;
    z-index: 9999;
}

.hint {
    background-color: rgb(0, 60, 255);
    color: white;
    border: none;
    border-radius: 50%;
    font-size: 14px;
    cursor: pointer;
    display: inline-block;
    margin-left: 5px;
    min-width: 16px;
    text-align: center;
    padding: 2px;
}
```

- script.js

```
import {SystemParametersHints, AttackParametersHints, ConnectionMatrixSystemToAttack, ConnectionMatrixAttackToAttack, MatrixFillingHint} from "./data.js"




//global containers
const SystemParameters = [];
const AttackParameters = [];
const Alternatives = [];
const ConnectionMatrixAttackToAlternative = [];
var Ps = []
const AlternativesResult = [];




//predefined data
const TotalAttackComb = 3*3*4*3*4;
var tableCreated = false;

const SystemParametersFormId = "system-parameters"
const SystemParametersOpenId = "system-parameters-open"

const AttackParametersFormId = "attack-parameters"
```

```
const AttackParametersOpenId = "attack-parameters-open"

const AlternativesFormId = "resolve-alternatives"
const AlternativesOpenId = "resolve-alternatives-open"

const TableBlockId = "table-block"

const SystemMap = new Map([
    ['PC', 0], ['Network', 1], ['Website', 2],
    ['sysDbTrue', 3], ['sysDbFalse', 4],
    ['LAN', 5], ['WAN', 6], ['Net', 7],
    ['antivirusTrue', 8], ['antivirusFalse', 9],
    ['detectionTrue', 10], ['detectionFalse', 11]
]);

const AttackMap = new Map([
    ['Email', 0], ['Network', 1], ['Internet', 2], ['Physically', 3],
    ['Simple', 4], ['Complex', 5], ['Automatic', 6],
    ['Steal', 7], ['Destruction', 8], ['Espionage', 9], ['Overload', 10],
    ['OneStep', 11], ['MultiStep', 12], ['Polymorph', 13],
    ['VPN', 14], ['TOR', 15], ['Steganography', 16]
]);

const AlternativesConnectionRating = new Map([
    ['Абсолютно несумісні', -1], ['Дуже сильно несумісні', -0.75],
    ['Посередньо несумісні', -0.5], ['Мала несумісність', -0.25],
    ['Мало пов\'язані', 0.25], ['Посередньо пов\'язані', 0.5],
    ['Дуже сильно пов\'язані', 0.75], ['Абсолютно пов\'язані', 1]
]);

const AttackNames = [
    {name: 'Вектор атаки', content: ['E-mail', 'Мережа', 'Інтернет', 'Фізично']},
    {name: 'Витонченість атаки', content: ['Проста', 'Просунута', 'Автоматизована']},
    {name: 'Тип атаки', content: ['Крадіжка', 'Знищення даних', 'Шпигунство', 'Перевантаження
системи']},
    {name: 'Складність атаки', content: ['Одноетапна', 'Багатоетапна', 'Поліморфна']},
    {name: 'Ухилення', content: ['VPN', 'TOR', 'Стеганографія']}
]




//UI Elements modifying
function toggleForm(formId) {
    var form = document.getElementById(formId);
    var computedStyle = window.getComputedStyle(form);

    if (computedStyle.display === "none") {
```

```
        form.style.display = "block";
    } else {
        form.style.display = "none";
    }
}

function toggleWarning(formId, isVisible){
    var form = document.getElementById(formId);
    var warningMessage = form.querySelector('.warning-message');

    if (isVisible) {
        warningMessage.style.display = "block";
    } else {
        warningMessage.style.display = "none";
    }
}

function isBlockContainsCheck(divId){
    var div = document.getElementById(divId);
    var span = div.querySelector("span." + "check-mark");
    return (span !== null);
}

function addCheckToText(divId) {
    var div = document.getElementById(divId);
    var span = document.createElement("span");
    span.innerHTML = '&#9745;';
    span.classList.add("check-mark");
    div.insertBefore(span, div.firstChild);
}

function createTable() {
    const tableContainer = document.getElementById(TableBlockId);

    //Explanatory text
    var matrixHint = document.createElement('p');
    matrixHint.innerHTML = MatrixFillingHint;

    // Append the <p> element to the table container before the table
    tableContainer.appendChild(matrixHint);

    // Create the table element
    const table = document.createElement('table');

    // Create the header row with
    var header = document.createElement("thead");
    const headerRow = document.createElement('tr');
    // add two empty cell in the top-left corner
    headerRow.appendChild(document.createElement('td'));
```

```
headerRow.appendChild(document.createElement('td'));
for (const alternative of Alternatives) {
    const headerCell = document.createElement('td');
    headerCell.textContent = alternative;
    headerRow.appendChild(headerCell);
}
header.appendChild(headerRow);
table.appendChild(header);

AttackNames.forEach((attackName) => {
    var tbody = document.createElement("tbody");
    var tbodyRow = document.createElement("tr");
    var tbodyName = document.createElement("td");

    tbodyName.textContent = attackName.name;
    var tbodyContent = document.createElement("td");

    tbodyName.setAttribute("rowspan", attackName.content.length)
    tbodyContent.textContent = attackName.content[0];
    tbodyRow.appendChild(tbodyName);
    tbodyRow.appendChild(tbodyContent);

    // create cells for each alternative
    Alternatives.forEach((alternative) => {
        const cell = document.createElement('td');
        const select = document.createElement('select');
        // Create the default option with an empty value
        const defaultOption = document.createElement('option');
        defaultOption.value = 0;
        defaultOption.textContent = 'Незалежні';
        select.appendChild(defaultOption);

        AlternativesConnectionRating.forEach((value, key) => {
            const option = document.createElement('option');
            option.value = value;
            option.textContent = key;
            select.appendChild(option);
        })

        cell.appendChild(select);
        tbodyRow.appendChild(cell);
    });

    tbody.appendChild(tbodyRow);

    for(let i = 1; i < attackName.content.length; i++){
        var tBodyRowNext = document.createElement("tr");
        var tBodyContentNext = document.createElement("td");
        tBodyContentNext.textContent = attackName.content[i];
```

```
            tBodyRowNext.appendChild(tBodyContentNext);

            // create cells for each alternative
            Alternatives.forEach((alternative) => {
                const cell = document.createElement('td');
                const select = document.createElement('select');
                // Create the default option with an empty value
                const defaultOption = document.createElement('option');
                defaultOption.value = 0;
                defaultOption.textContent = 'Незалежні';
                select.appendChild(defaultOption);

                AlternativesConnectionRating.forEach((value, key) => {
                    const option = document.createElement('option');
                    option.value = value;
                    option.textContent = key;
                    select.appendChild(option);
                })

                cell.appendChild(select);
                tBodyRowNext.appendChild(cell);
            });

            tbody.appendChild(tBodyRowNext);
        }

        // add the body row to the table
        table.appendChild(tbody);
    });

    // Set the tableCreated flag to true
    tableCreated = true;
    var warning = document.getElementById('table-warning');
    // Add the table to the container

    tableContainer.insertBefore(table, warning);
    tableContainer.insertBefore(matrixHint, table);
}

function generateResult(){

    for (let i = 0; i < AlternativesResult.length; i++){
        for (let j = 0; j < AlternativesResult.length - i - 1; j++) {
            if (AlternativesResult[j] < AlternativesResult[j + 1]) {
              // Swap the elements
              var tempValues = AlternativesResult[j];
              AlternativesResult[j] = AlternativesResult[j + 1];
              AlternativesResult[j + 1] = tempValues;
```

```
                var tempNames = Alternatives[j]
                Alternatives[j] = Alternatives[j + 1];
                Alternatives[j + 1] = tempNames;
            }
        }
    }

    var outputText = "Очікувані результативності альтернатив наступні: <br>"
    for (let i = 0; i < Alternatives.length; i++)
        outputText    +=    '<pre></pre>'    +    Alternatives[i]    +    '    &mdash;    '    +
parseFloat(AlternativesResult[i]).toFixed(4) + '<br>';

    var bestAlternatives = [Alternatives[0]]

    for (let i = 1; i < AlternativesResult.length; i++){
        if (AlternativesResult[0] - AlternativesResult[i] <= 0.05)
            bestAlternatives.push(Alternatives[i]);
    }

    outputText += '<pre></pre>'+ "Іншими словами, найкраще обрати альтернативу " + bestAlternatives[0];
    for (let i = 1; i < bestAlternatives.length; i++){
        outputText += ", або " + bestAlternatives[i]
    }
    outputText += '.';

    var resultSpan = document.getElementById('result');
    resultSpan.style.display = 'block';
    resultSpan.innerHTML = outputText;
}

function createPopupWindow() {
    // Create the pop-up window dynamically
    var popupWindow = document.createElement('div');
    popupWindow.id = 'popup';
    popupWindow.innerHTML = `
        <p></p>
        <button id="popup-close">Close</button>`;

    // Get reference to the overlay element
    var overlay = document.getElementById('overlay');

    // Show the pop-up window and overlay
    function showPopupWindow(hintText) {
      overlay.style.display = 'block';
      popupWindow.querySelector('p').innerHTML = hintText;
      popupWindow.style.display = 'block';
    }

    // Hide the pop-up window and overlay
```

```
    function hidePopupWindow() {
      overlay.style.display = 'none';
      popupWindow.style.display = 'none';
    }

    // Add event listener to the close button
    popupWindow.querySelector('#popup-close')
        .addEventListener('click', hidePopupWindow);

    // Append the pop-up window to the body
    document.body.appendChild(popupWindow);

    // Return the functions to show and hide the pop-up window
    return { show: showPopupWindow, hide: hidePopupWindow };
}



//Input data verifying
function verifyRadioButtons(inputs){
    let isRadioChecked = false;

    inputs.forEach(element => {
        if(element.checked)
            isRadioChecked = true;
    });

    return isRadioChecked;
}

function validateRadioButtons(formId) {
    var form = document.getElementById(formId);
    var fieldsets = form.querySelectorAll("fieldset");

    for (let i = 0; i<fieldsets.length; i++) {
        var inputs = fieldsets[i].querySelectorAll("input");
        if(inputs[0].type == "radio"){
            if(!verifyRadioButtons(inputs)){
                toggleWarning(formId, true);
                return false;
            }
        }
    }

    return true;
}

function verifyTextInputs(inputs){
```

```
    var filledInputs = Array.from(inputs).filter(elem => elem.value.trim() !== "").length;

    return filledInputs >= 2;
}

function validateAlternatives(formId){
    var form = document.getElementById(formId);
    var inputs = form.querySelectorAll("input");

    if(!verifyTextInputs(inputs)){
        toggleWarning(formId, true);
        return false;
    }

    return true;
}

function verifyNumberInputs(fieldsets){
    var isSumEqualsOne = true;

    fieldsets.forEach(fieldset => {
        var inputs = fieldset.querySelectorAll("input");
        var sum = 0;
        inputs.forEach(input => sum += Number(input.value));
        console.log(sum);

        if (Math.abs(sum - 1) > 0.000001)
            isSumEqualsOne = false;
    })

    return isSumEqualsOne;
}

function validateNumberInputs(formId){
    var form = document.getElementById(formId);
    var fieldsets = form.querySelectorAll("fieldset");
    if(!verifyNumberInputs(fieldsets)){
        toggleWarning(formId, true);
        return false;
    }

    return true;
}




//Input data saving
```

```
function systemParametersToArray(formId){
    var form = document.getElementById(formId);

    // Get the value of each input element in the form and store it in an object
    var systemType = form.querySelector('input[name="sysType"]:checked').value;
    var isSysDB = form.querySelector('input[name="isSysDB"]:checked').value;
    var                                  sysNetworkConnectionType                                    =
form.querySelector('input[name="sysNetworkConnectionType"]:checked').value;
    var isAntivirus = form.querySelector('input[name="isAntivirus"]:checked').value;
    var isDetection = form.querySelector('input[name="isDetection"]:checked').value;

    var systemParams = {
    systemType,
    isSysDB,
    sysNetworkConnectionType,
    isAntivirus,
    isDetection
    };

    //Clear an array
    SystemParameters.length = 0;

    // Push the system parameters object to the array
    SystemParameters.push(systemParams);

    // Log the array to the console for debugging purposes
    console.log(SystemParameters);
}

function saveSystemParameters(){
    if(!validateRadioButtons(SystemParametersFormId)){
        SystemParameters.length = 0;
        return false
    }
    toggleWarning(SystemParametersFormId, false)

    systemParametersToArray(SystemParametersFormId)

    toggleForm(SystemParametersFormId)

    if(!isBlockContainsCheck(SystemParametersOpenId)){
        addCheckToText(SystemParametersOpenId)
    }
}

function attackParametersToArray(formId){
    var form = document.getElementById(formId);

    // Get all input elements in the form
```

```
    var inputs = form.querySelectorAll('input');

    //Clear an array
    AttackParameters.length = 0;

    // Loop through all input elements and create an object with their values
    for (let i = 0; i < inputs.length; i++) {
    var input = inputs[i];
    var obj = {
    name: input.name,
    value: Number(input.value)
    };
    AttackParameters.push(obj);
    }

    // Print the data array to the console
    console.log(AttackParameters);
}

function saveAttackParameters(){
    if(!validateNumberInputs(AttackParametersFormId)){
        AttackParameters.length = 0;
        return false
    }
    toggleWarning(AttackParametersFormId, false)

    attackParametersToArray(AttackParametersFormId)

    toggleForm(AttackParametersFormId)

    if(!isBlockContainsCheck(AttackParametersOpenId)){
        addCheckToText(AttackParametersOpenId)
    }
}

function alternativesToList(formId){
    var form = document.getElementById(formId);

    // Get all input elements in the form
    var inputs = form.querySelectorAll('input');

    //Clear an array
    Alternatives.length = 0;

    inputs.forEach(input => {
        if(input.value.trim() !== "")
            Alternatives.push(input.value);
    });
```

```
    console.log(Alternatives);
}

function saveAlternatives(){
    if(!validateAlternatives(AlternativesFormId)){
        Alternatives.length = 0;
        return false
    }
    toggleWarning(AlternativesFormId, false)

    alternativesToList(AlternativesFormId)

    toggleForm(AlternativesFormId)

    if(!isBlockContainsCheck(AlternativesOpenId)){
        addCheckToText(AlternativesOpenId)
    }
}

function saveConnectionMatrixForAlternatives(){
    var table = document.getElementById(TableBlockId);
    var bodies = table.querySelectorAll('tbody');

    ConnectionMatrixAttackToAlternative.length = 0;

    bodies.forEach(body => {
        var rows = body.querySelectorAll("tr");
        rows.forEach(row => {
            var selects = row.querySelectorAll("select");
            let tempArray = []
            selects.forEach(select =>
                tempArray.push(Number(select.value)));
            ConnectionMatrixAttackToAlternative.push(tempArray);
        })
    })

    console.log(ConnectionMatrixAttackToAlternative);
}




//Calculation helpers
function getAttackR(attackParameter){
    var attackParameterIndex = AttackMap.get(attackParameter.name)
```

```
    return                                                                                    (1+
ConnectionMatrixSystemToAttack[SystemMap.get(SystemParameters[0].systemType)][attackParameterIndex])
*
    (1+
ConnectionMatrixSystemToAttack[SystemMap.get(SystemParameters[0].isSysDB)][attackParameterIndex]) *
    (1+
ConnectionMatrixSystemToAttack[SystemMap.get(SystemParameters[0].sysNetworkConnectionType)][attackPa
rameterIndex]) *
    (1+
ConnectionMatrixSystemToAttack[SystemMap.get(SystemParameters[0].isAntivirus)][attackParameterIndex]
) *
    (1+
ConnectionMatrixSystemToAttack[SystemMap.get(SystemParameters[0].isDetection)][attackParameterIndex]
) *
    attackParameter.value;
}

function normalizeArray(arr) {
    var sum = arr.reduce((acc, val) => acc + val, 0);
    return arr.map((value) => value / sum);
}




//Parts of the main algorithm
function updateAttackAlternatives(){
    var newVector = [[],[],[],[]]
    var newSophistication = [[],[],[]]
    var newType = [[],[],[],[]]
    var newComplexity = [[],[],[]]
    var newEvasion = [[],[],[]]

    for (let i = 0; i < TotalAttackComb/4; i++){
        for (let j = 0; j < 4; j ++){
            newVector[j].push(Ps[i+(TotalAttackComb*j/4)])
        }
    }

    for (let i = 0; i < TotalAttackComb/(4*3); i++){
        for (let j = 0; j < 4*3; j++){
            newSophistication[j%3].push(Ps[i+(TotalAttackComb*j/(4*3))])
        }
    }

    for (let i = 0; i < TotalAttackComb/(4*3*4); i++){
        for (let j = 0; j < 4*3*4; j++){
            newType[j%4].push(Ps[i+(TotalAttackComb*j/(4*3*4))]);
```

```
        }
    }

    for (let i = 0; i < TotalAttackComb/(4*3*4*3); i++){
        for (let j = 0; j < 4*3*4*3; j++){
            newComplexity[j%3].push(Ps[i+(TotalAttackComb*j/(4*3*4*3))]);
        }
    }

    for (let i = 0; i < TotalAttackComb/(4*3*4*3*3); i++){
        for (let j = 0; j < 4*3*4*3*3; j++){
            newEvasion[j%3].push(Ps[i+(TotalAttackComb*j/(4*3*4*3*3))]);
        }
    }

    AttackParameters[AttackMap.get('Email')].value = newVector[0].reduce((accumulator, currentValue)
=> accumulator + currentValue);
    AttackParameters[AttackMap.get('Network')].value       =       newVector[1].reduce((accumulator,
currentValue) => accumulator + currentValue);
    AttackParameters[AttackMap.get('Internet')].value       =       newVector[2].reduce((accumulator,
currentValue) => accumulator + currentValue);
    AttackParameters[AttackMap.get('Physically')].value      =      newVector[3].reduce((accumulator,
currentValue) => accumulator + currentValue);

    AttackParameters[AttackMap.get('Simple')].value    =    newSophistication[0].reduce((accumulator,
currentValue) => accumulator + currentValue);
    AttackParameters[AttackMap.get('Complex')].value   =    newSophistication[1].reduce((accumulator,
currentValue) => accumulator + currentValue);
    AttackParameters[AttackMap.get('Automatic')].value  =  newSophistication[2].reduce((accumulator,
currentValue) => accumulator + currentValue);

    AttackParameters[AttackMap.get('Steal')].value = newType[0].reduce((accumulator, currentValue) =>
accumulator + currentValue);
    AttackParameters[AttackMap.get('Destruction')].value      =      newType[1].reduce((accumulator,
currentValue) => accumulator + currentValue);
    AttackParameters[AttackMap.get('Espionage')].value       =       newType[2].reduce((accumulator,
currentValue) => accumulator + currentValue);
    AttackParameters[AttackMap.get('Overload')].value = newType[3].reduce((accumulator, currentValue)
=> accumulator + currentValue);

    AttackParameters[AttackMap.get('OneStep')].value     =     newComplexity[0].reduce((accumulator,
currentValue) => accumulator + currentValue);
    AttackParameters[AttackMap.get('MultiStep')].value    =    newComplexity[1].reduce((accumulator,
currentValue) => accumulator + currentValue);
    AttackParameters[AttackMap.get('Polymorph')].value    =    newComplexity[2].reduce((accumulator,
currentValue) => accumulator + currentValue);

    AttackParameters[AttackMap.get('VPN')].value = newEvasion[0].reduce((accumulator, currentValue)
=> accumulator + currentValue);
```

```
    AttackParameters[AttackMap.get('TOR')].value = newEvasion[1].reduce((accumulator, currentValue)
=> accumulator + currentValue);
    AttackParameters[AttackMap.get('Steganography')].value    =    newEvasion[2].reduce((accumulator,
currentValue) => accumulator + currentValue);

    console.log("Attack Parameters after first step of MMMA: ", AttackParameters);
}

function firstPartOfAlgorithm(){
    systemParametersToArray(SystemParametersFormId)
    attackParametersToArray(AttackParametersFormId)
    alternativesToList(AlternativesFormId)

    var R = []
    AttackParameters.forEach(parameter => R.push(getAttackR(parameter)))

    var attackVector = normalizeArray(R.slice(0,4))
    for (let i = 0; i < 4; i++)
        AttackParameters[i].value = attackVector[i];

    var attackSophistication = normalizeArray(R.slice(4,7))
    for (let i = 0; i < 3; i++)
        AttackParameters[i+4].value = attackSophistication[i];

    var attackType = normalizeArray(R.slice(7,11))
    for (let i = 0; i < 4; i++)
        AttackParameters[i+7].value = attackType[i]

    var attackComplexity = normalizeArray(R.slice(11,14))
    for (let i = 0; i < 3; i++)
        AttackParameters[i+11].value = attackComplexity[i]

    var attackEvasion = normalizeArray(R.slice(14,17))
    for (let i = 0; i < 3; i++)
        AttackParameters[i+14].value = attackEvasion[i]

    console.log("Attack parameters with system parameters: ", AttackParameters);
}

function secondPartOfAlgorithm(){
    var p = []
    var C = []

    for (let i = 0; i < 4; i++) {
        for (let j = 4; j < 7; j++) {
            for (let k = 7; k < 11; k++){
                for (let m = 11; m < 14; m++){
                    for (let n = 14; n < 17; n++){
                        p.push(AttackParameters[i].value * AttackParameters[j].value *
```

```
                            AttackParameters[k].value * AttackParameters[m].value *
                            AttackParameters[n].value);
                        C.push((1+ConnectionMatrixAttackToAttack[i][j]) *
                            (1+ConnectionMatrixAttackToAttack[i][k]) *
                            (1+ConnectionMatrixAttackToAttack[i][m]) *
                            (1+ConnectionMatrixAttackToAttack[i][n]) *
                            (1+ConnectionMatrixAttackToAttack[j][k]) *
                            (1+ConnectionMatrixAttackToAttack[j][m]) *
                            (1+ConnectionMatrixAttackToAttack[j][n]) *
                            (1+ConnectionMatrixAttackToAttack[k][m]) *
                            (1+ConnectionMatrixAttackToAttack[k][n]) *
                            (1+ConnectionMatrixAttackToAttack[m][n]));
                    }
                }
            }
        }
    }

    var PmultC = []

    for (let i = 0; i < p.length; i++){
        PmultC.push(p[i]*C[i])
    }

    Ps = normalizeArray(PmultC);

    console.log("Matrix R for new Attack Parameters: ", Ps);
}

function thirdPartOfAlgorithm(){
    var R = []

    for (let i = 0; i < 4; i++) {
        for (let j = 4; j < 7; j++) {
            for (let k = 7; k < 11; k++){
                for (let m = 11; m < 14; m++){
                    for (let n = 14; n < 17; n++){
                        let tempArray = [];
                        for (let alt = 0; alt < Alternatives.length; alt++)
                            tempArray.push((1+ConnectionMatrixAttackToAlternative[i][alt]) *
                            (1+ConnectionMatrixAttackToAlternative[j][alt]) *
                            (1+ConnectionMatrixAttackToAlternative[k][alt]) *
                            (1+ConnectionMatrixAttackToAlternative[m][alt]) *
                            (1+ConnectionMatrixAttackToAlternative[n][alt]));

                        R.push(normalizeArray(tempArray));
                    }
                }
            }
```

```
        }
    }

    console.log("Matrix R for Alternatives: ", R);

    for (let i = 0; i < R.length; i++) {
        for (let j = 0; j < R[i].length; j++) {
          R[i][j] *= Ps[i];
        }
    }

    console.log("Expected Matrix R for Alternatives: ", R);

    AlternativesResult.length = 0;
    for (let j = 0; j < Alternatives.length; j++){
        var sum = 0;
        for (let i = 0; i < R.length; i++){
            sum += R[i][j]
        }
        AlternativesResult.push(sum);
    }

    console.log("Result: ", AlternativesResult);
}




//Event listeners
document.getElementById('system-parameters-open')
    .addEventListener('click', (event) => toggleForm('system-parameters'));

document.getElementById('system-parameters-confirm')
    .addEventListener('click', (event) => saveSystemParameters());

document.getElementById('attack-parameters-open')
    .addEventListener('click', (event) => toggleForm('attack-parameters'));

document.getElementById('attack-parameters-confirm')
    .addEventListener('click', (event) => saveAttackParameters());

document.getElementById('resolve-alternatives-open')
    .addEventListener('click', (event) => toggleForm('resolve-alternatives'));

document.getElementById('resolve-alternatives-confirm')
    .addEventListener('click', (event) => saveAlternatives());

document.getElementById('start-algorithm-button')
```

```
    .addEventListener('click', function(event){
        var warning = document.getElementById('begin-warning');
        if(SystemParameters.length === 0 || AttackParameters.length === 0 || Alternatives.length ===
0){
            warning.style.display = "block";
            var table = document.querySelector("table");
            if (table){
                table.parentNode.removeChild(table);
                document.getElementById('get-result-button').style.display = 'none';
                tableCreated = false;
            }
            return;
        }
        warning.style.display = "none";
        if(tableCreated){
            var table = document.querySelector("table");
            table.parentNode.removeChild(table);
            createTable();
        }
        else
            createTable();
        document.getElementById('get-result-button').style.display = 'block';
})

document.getElementById("get-result-button")
    .addEventListener('click', (event) => {
        toggleWarning('table-block', false)

        var warning = document.getElementById('missing-data-warning');
        if(SystemParameters.length === 0 || AttackParameters.length === 0 || Alternatives.length ===
0){
            warning.style.display = "block";
            var resultSpan = document.getElementById('result');
            resultSpan.style.display = 'none';
            return;
        }
        warning.style.display = "none";

        saveConnectionMatrixForAlternatives();
        firstPartOfAlgorithm();
        secondPartOfAlgorithm();
        updateAttackAlternatives();
        thirdPartOfAlgorithm();
        generateResult()
})

const popup = createPopupWindow()

document.getElementById('system-connection-hint')
```

```
    .addEventListener('click', (event) => {
        popup.show(SystemParametersHints.SystemConnectionHint);
})

document.getElementById('detection-hint')
    .addEventListener('click', (event) => {
        popup.show(SystemParametersHints.DetectionHint);
})

document.getElementById('general-attack-hint')
    .addEventListener('click', (event) => {
        popup.show(AttackParametersHints.InputHint);
})

document.getElementById('vector-hint')
    .addEventListener('click', (event) => {
        popup.show(AttackParametersHints.VectorHint);
})

document.getElementById('elegance-hint')
    .addEventListener('click', (event) => {
        popup.show(AttackParametersHints.EleganceHint);
})

document.getElementById('complexity-hint')
    .addEventListener('click', (event) => {
        popup.show(AttackParametersHints.ComplexityHint);
})

document.getElementById('evasion-hint')
    .addEventListener('click', (event) => {
        popup.show(AttackParametersHints.EvasionHint);
})
```

– data.js

```
export const SystemParametersHints = {
    SystemConnectionHint: "<i>Локальна мережа</i> (LAN) – мережа, яка зазвичай охоплює обмежену географічну територію, таку як будинок або офіс.<br><i>Широкомасштабна мережа</i> (WAN) – мережа, що охоплює велику географічну територію, таку як, наприклад, країна. Вона використовується для підключення віддалених локальних мереж та комп'ютерних систем, щоб забезпечити обмін даними та комунікацію на великій відстані.<br><i>Інтернет</i> – глобальна мережа мереж, яка об\'єднує мільйони систем та пристроїв по всьому світу. Він надає доступ до широкого спектру ресурсів, таких як веб-сторінки, онлайн-сервіси та ін.",
    DetectionHint: "Як приклад системи виявлення вторгень можна навести такі системи як: <i>Snort</i>, <i>Suricata</i>, <i>McAfee Intrusion Prevention System</i> та інші."
}
```

```
export const AttackParametersHints = {
    InputHint: "Введіть Ваші суб\'єктивні ймовірності від 0 до 1 для кожної альтернативи в секторі за наступною шкалою: <table><tr><th>Якісна характеристика</th><th>Кількісна характеристика</th></tr><tr><td>Неможливо</td><td>0</td></tr><tr><td>Практично неможливо</td><td>[0 - 0,1]</td></tr><tr><td>Дуже мала ймовірність</td><td>[0,1 - 0,25]</td></tr><tr><td>Мала ймовірність</td><td>[0,25 - 0,4]</td></tr><tr><td>Середня ймовірність</td><td>[0,4 - 0,6]</td></tr><tr><td>Велика ймовірність</td><td>[0,6 - 0,75]</td></tr><tr><td>Дуже велика ймовірність</td><td>[0,75 - 0,9]</td></tr><tr><td>Практично гарантовано</td><td>[0,9 - 1]</td></tr><tr><td>Гарантовано</td><td>1</td></tr></table>.",
    VectorHint: "<i>E-mail.</i> В цьому випадку атаки здійснюються через електронну пошту. Як приклад, зловмисники використовують фішингові листи, надсилання шкідливих вкладень та посилань, атаки на поштові сервери або викрадення облікових даних.<br><i>Мережа.</i> Включає в себе атаки на мережеві протоколи, системи комутації даних та інфраструктуру мережі. Хакери використовувють такі методи, як: використання слабких місць безпеки задля атаки, атаки на маршрутизатори, перехоплення мережевого трафіку, розповсюдження вірусів або «черв'яків» у мережі.<br><i>Інтернет.</i> Охоплює різні атаки, що використовують Інтернет як основний канал. Сюди входять атаки на веб-сайти, використання вразливостей в програмах, атаки на додатки з відкритим вихідним кодом, злам аккаунтів соціальних мереж та інші веб-орієнтовані атаки.<br><i>Фізично.</i> В цьому випадку злодії здійснюють атаки безпосередньо на фізичному рівні. Це можуть бути атаки на фізичний доступ до пристроїв або приміщень, викрадення пристроїв, інсталяція шкідливого обладнання або використання соціальної інженерії для отримання доступу до систем.",
    EleganceHint: "<i>Проста.</i> Проста атака відображає низький рівень витонченості. Вона може включати базові методи, які легко виконати навіть для непрофесійного зловмисника. Наприклад, використання відомих інструментів для атак, які не потребують глибоких знань або спеціальних навичок.<br><i>Просунута.</i> Просунута атака позначає високий рівень витонченості. Вона вимагає великої експертизи та розуміння вразливостей системи або мережі. Такі атаки можуть використовувати нові, раніше невідомі вразливості, складні техніки обходу захисту.<br><i>Автоматизована.</i> Такі атаки використовують спеціально розроблене програмне забезпечення, скрипти або інструменти для автоматичного виконання хакерських атак. Вони можуть бути здійснені без значного втручання хакера, оскільки вони можуть бути програмно налаштованими для виявлення та зламування систем.",
    ComplexityHint: "<i>Одноетапна.</i> Передбачає просту послідовність кроків, де зловмисник виконує лише один етап для досягнення своєї цілі. Це може бути, наприклад, виконання певної команди, використання вразливості або запуск певної програми, яка відразу ж призводить до небажаного наслідку.<br><i>Багатоетапна.</i> Передбачає складну послідовність кроків, де злодій виконує багато етапів або дій для досягнення своєї цілі. Це може включати виконання кількох кроків: від розвідки та збору інформації про ціль, до використання різних методів атаки та обходу захисту.<br><i>Поліморфна.</i> Має на увазі високий рівень змінності або варіативності в ході виконання атаки. Хакери використовують методи, щоб змінювати свій підхід, код або схему атаки з метою уникнення виявлення чи блокування захисними механізмами.",
    EvasionHint: "<i>VPN (Virtual Private Network).</i> VPN використовується для забезпечення приватності та анонімності під час передачі даних через мережу. Злодії можуть використовувати VPN для приховування своєї справжньої IP-адреси та місцезнаходження, щоб уникнути виявлення та ідентифікації їхніх дій.<br><i>TOR (The Onion Router).</i> TOR - це мережа, що надає анонімність під час перегляду веб-сторінок та передачі даних через Інтернет. Хакери можуть використовувати TOR для приховування своєї справжньої IP-адреси та маршрутизації свого трафіку через кілька вузлів, що робить їхні дії важкодоступними для виявлення та відстеження.<br><i>Стеганографія.</i> Стеганографія - це метод приховування інформації у інших типах даних або носіях, таких як зображення, звукові файли або текстові документи. Зловмисники можуть використовувати стеганографію для приховування своїх зловісних дій або
```

```
відправки конфіденційної інформації через невинні носії, змінюючи бітову структуру файлів або використовуючи спеціальні алгоритми."
}

export const MatrixFillingHint = "<b>Оцініть зв\'язки між певною альтернативою характеристики хакерської атаки та альтернативою захисту.</b>"

export const ConnectionMatrixSystemToAttack = [
    [0.6, 0.2, 0.8, 0.5, 0.6, 0.2, 0.7, 0.5, 0.2, 0.4, 0, 0.4, -0.4, 0.3, 0.7, 0.5, 0.4],
    [0.3, 0.8, 0.5, 0.5, -0.4, 0.6, 0.1, 0.2, 0, 0.8, 0.6, -0.5, 0.6, 0.8, 0.6, 0.5, -0.2],
    [-1, -0.2, 1, -1, 0.4, 0.3, 0.5, 0.2, 0.5, 0, 0.7, 0.3, 0.4, 0.6, 0.5, 0.5, -0.3],
    [0, 0, 0, 0, -0.2, 0.2, 0.1, 0.8, 0.7, -0.9, -0.7, 0, 0, 0, 0, 0, 0],
    [0, 0, 0, 0, 0.2, -0.2, 0.3, -0.3, -0.6, 0.4, 0.1, 0, 0, 0, 0, 0, 0],
    [0.3, 0.5, 0.1, 0, 0.5, 0.2, 0.4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0],
    [0.1, 0.7, 0.4, 0, -0.2, 0.6, -0.1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0],
    [0.5, -0.6, 1, 0, 0.3, 0.4, 0.6, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0],
    [-0.2, -0.1, -0.2, -0.5, -0.7, 0.6, -0.5, -0.3, -0.3, -0.4, 0, -0.5, 0.8, 0.5, 0, 0, 0.4],
    [0.3, 0.1, 0.3, 0.5, 0.5, 0, 0.8, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0],
    [-0.1, -0.8, -0.3, 0, -0.9, 1, -0.3, -0.2, -0.2, -0.4, -0.5, -0.9, 0.7, 0.8, 0.7, 0.5, 0.6],
    [0.2, 0.5, 0.4, 0, 0.5, 0, 0.7, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
];

export const ConnectionMatrixAttackToAttack = [
    [0, 0, 0, 0, 0.2, 0, 0.4, 0.5, -0.4, 0.4, -0.3, 0.4, 0.1, -0.2, 0.1, 0.2, 0.5],
    [0, 0, 0, 0, -0.1, 0.4, 0.2, 0.4, 0.3, 0.6, 0.1, 0.1, 0.4, 0.6, 0.5, 0.5, -0.2],
    [0, 0, 0, 0, 0, 0, 0.5, 0.7, 0.5, 0.7, 0.6, 0.2, 0.5, 0.7, 0.7, 0.6, 0.3],
    [0, 0, 0, 0, 0.6, 0, -1, 0.6, 0.4, 0.8, 0.3, 0.7, 0.1, 0.2, -0.7, -0.7, 0.7],
    [0.2, -0.1, 0, 0.6, 0, 0, 0, 0, 0, 0, 0, 0.8, 0.1, -0.7, 0, 0, -0.6],
    [0, 0.4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0.2, 0.6, 0.7, 0, 0, 0],
    [0.4, 0.2, 0.5, -1, 0, 0, 0, 0.4, 0.1, 0.3, 0.5, 0.7, 0.3, 0.2, 0.2, 0, 0],
    [0.5, 0.4, 0.7, 0.6, 0, 0, 0.4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0],
    [-0.4, 0.3, 0.5, 0.4, 0, 0, 0.1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0],
    [0.4, 0.6, 0.7, 0.8, 0, 0, 0.3, 0, 0, 0, 0, 0, 0, 0.3, 0, 0, 0],
    [-0.3, 0.1, 0.6, 0.3, 0, 0, 0.5, 0, 0, 0, 0, 0.2, 0, 0, 0, 0, 0],
    [0.4, 0.1, 0.2, 0.7, 0.8, 0.2, 0.7, 0, 0, 0, 0.2, 0, 0, 0, 0.3, 0.2, 0],
    [0.1, 0.4, 0.5, 0.1, 0.1, 0.6, 0.3, 0, 0, 0, 0, 0, 0, 0, 0.3, 0.4, 0.3],
    [-0.2, 0.6, 0.7, 0.2, -0.7, 0.7, 0.2, 0, 0, 0.3, 0, 0, 0, 0, 0.3, 0.5, 0.4],
    [0.1, 0.5, 0.7, -0.7, 0, 0, 0.2, 0, 0, 0, 0, 0.3, 0.3, 0.3, 0, 0, 0],
    [0.2, 0.5, 0.6, -0.7, 0, 0, 0, 0, 0, 0, 0, 0.2, 0.4, 0.5, 0, 0, 0],
    [0.5, -0.2, 0.3, 0.7, -0.6, 0, 0, 0, 0, 0, 0, 0, 0.3, 0.4, 0, 0, 0]
];
```

ДОДАТОК Б ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ЩОДО ЗАХИСТУ ВІД ХАКЕРСЬКИХ АТАК

Болдарев Є.А. КА-93

Науковий керівник: Савченко І.О.

- **Об'єкт дослідження:** процес прийняття рішень щодо захисту цифрової системи від хакерських атак.
- **Предмет дослідження:** двоетапний модифікований метод морфологічного аналізу з нерівномірним розподілом початкових оцінок.
- **Мета роботи:** Розробка системи підтримки прийняття рішень щодо хакерських атак на основі двоетапного методу морфологічного аналізу з нерівномірним розподілом початкових оцінок.

АКТУАЛЬНІСТЬ

В наш час цифрова безпека є одним з найактуальніших проблем. Все більше сервісів інтегрується в цифровий простір, і все більше чутливих даних потрапляє в мережу. Вся цифрова інформація є ціллю хакерських атак, тож дуже важливо вживати ефективні запобіжні заходи та швидко реагувати на потенційну безпеку.

ПОСТАНОВКА ЗАДАЧІ

Ціллю роботи є розробка системи підтримки прийняття рішень, яка допоможе кінцевому користувачеві обрати найефективніший засіб захисту від хакерської атаки. СППР базується на двоетапному модифікованому методу морфологічного аналізу з нерівномірним розподілом початкових оцінок. Цей метод дозволяє врахувати вплив оцінок параметрів системи-цілі хакерської атаки на оцінки характеристик атаки.

МЕТОД МОРФОЛОГІЧНОГО АНАЛІЗУ

В основу цільової СППР щодо захисту від хакерських атак покладено двоетапний модифікований метод морфологічного аналізу з нерівномірним розподілом початкових оцінок. Головна мета цього методу в рамках цільової проблеми – виведення стратегій, які найефективніше враховувати в умовах сукупності можливих реалізацій об'єкта, визначених під час виконання ММА.

Стартовим і основним елементом ММА є морфологічна таблиця. Таблиця складається з певної N кількості характеристичних параметрів $F_i, i \in \overline{1,N}$. Кожному параметру відповідає певна n_i множина альтернатив $a_j^{(i)}, j \in \overline{1,n_i}$.

МОРФОЛОГІЧНІ ТАБЛИЦІ

Під час виконання роботи було побудовано морфологічні таблиці для характеристик хакерських атак та параметрів системи-цілі

Вектор атаки	Витонченість атаки	Мета атаки	Складність атаки	Засоби ухилення
E-mail	Проста	Крадіжка	Одноетапна	VPN
Мережа	Просунута	Знищення даних	Багатоетапна	TOR
Інтернет	Автоматизована	Шпигунство	Поліморфна	Стеганографія
Фізично		Перенавантаження системи		

Морфологічна таблиця характеристик хакерських атак

Тип системи	База даних	Тип підключення системи до мережі	Антивірусні програми	Системи виявлення вторгнень
ПК	Є	LAN	Є	Є
Мережа	Немає	WAN	Немає	Немає
Веб-сайт		Інтернет		

Морфологічна таблиця параметрів цільової системи

ПЕРШИЙ ЕТАП МММА

Головною метою першого етапу МММА є розрахунок ймовірностей всіх альтернатив параметрів морфологічної таблиці з врахуванням зв'язків між ними на основі експертного оцінювання. Загально кажучи, на першому етапі здійснюється аналіз зовнішніх факторів для, в нашому випадку, хакерської атаки.

Для встановлення взаємозв'язків між параметрами морфологічної таблиці використовується числова матриця взаємозв'язків. Кожній парі альтернатив $a_{j_1}^{(i_1)}, a_{j_2}^{(i_2)}$ різних характеристичних параметрів F_{i_1}, F_{i_2} дається оцінка $c_{i_1 j_1, i_2 j_2} \in [-1; 1]$

Оцінка	Тлумачення
-1	Альтернативи повністю неузгоджені. Конфігурація з цією парою альтернатив неможлива.
(-1;0)	Альтернативи неузгоджені. Вибір однієї з них певною мірою зменшує ймовірність вибору іншої.
0	Альтернативи незалежні. Вибір однієї з них не впливає на вибір іншої.
(0;1)	Альтернативи узгоджені. Вибір однієї з них певною мірою збільшує ймовірність вибору іншої.
1	Альтернативи повністю узгоджені. вибір однієї з них тягне за собою вибір іншої.

ПЕРШИЙ ЕТАП МММА

Після складання матриці взаємозв'язків, між вибором альтернатив різних параметрів створюється певна залежність і виникає наступна задача – знаходження оновлених ймовірностей вибору кожної альтернативи характеристичних параметрів, враховуючи вплив інформації з матриці взаємозв'язків на попередні оцінки.

Розв'язавши систему рівнянь, отримується оновлена морфологічна таблиця, що містить оцінки альтернатив, які враховують взаємозв'язки характеристичних параметрів системи.

$$\begin{cases} p_1^{(1)} = \sum_{j_2=1}^{n_2} \sum_{j_3=1}^{n_3} \dots \sum_{j_N=1}^{n_N} P\left(\left\{a_1^{(1)}, a_{j_2}^{(2)}, a_{j_3}^{(3)}, \dots, a_{j_N}^{(N)}\right\} \middle| a_{j_2}^{(2)}\right) p_{j_2}^{(2)}; \\ \dots \\ p_{n_1}^{(1)} = \sum_{j_2=1}^{n_2} \sum_{j_3=1}^{n_3} \dots \sum_{j_N=1}^{n_N} P\left(\left\{a_{n_1}^{(1)}, a_{j_2}^{(2)}, a_{j_3}^{(3)}, \dots, a_{j_N}^{(N)}\right\} \middle| a_{j_2}^{(2)}\right) p_{j_2}^{(2)}; \\ p_1^{(2)} = \sum_{j_1=1}^{n_1} \sum_{j_3=1}^{n_3} \dots \sum_{j_N=1}^{n_N} P\left(\left\{a_{j_1}^{(1)}, a_1^{(2)}, a_{j_3}^{(3)}, \dots, a_{j_N}^{(N)}\right\} \middle| a_{j_3}^{(3)}\right) p_{j_3}^{(3)}; \\ \dots \\ p_{n_2}^{(2)} = \sum_{j_1=1}^{n_1} \sum_{j_3=1}^{n_3} \dots \sum_{j_N=1}^{n_N} P\left(\left\{a_{j_1}^{(1)}, a_{n_2}^{(2)}, a_{j_3}^{(3)}, \dots, a_{j_N}^{(N)}\right\} \middle| a_{j_3}^{(3)}\right) p_{j_3}^{(3)}; \\ \dots \\ p_1^{(N)} = \sum_{j_1=1}^{n_1} \sum_{j_2=1}^{n_2} \dots \sum_{j_{N-1}=1}^{n_{N-1}} P\left(\left\{a_{j_1}^{(1)}, a_{j_2}^{(2)}, a_{j_3}^{(3)}, \dots, a_1^{(N-1)}\right\} \middle| a_{j_1}^{(1)}\right) p_{j_1}^{(1)}; \\ \dots \\ p_{n_N}^{(N)} = \sum_{j_1=1}^{n_1} \sum_{j_2=1}^{n_2} \dots \sum_{j_{N-1}=1}^{n_{N-1}} P\left(\left\{a_{j_1}^{(1)}, a_{j_2}^{(2)}, a_{j_3}^{(3)}, \dots, a_{n_N}^{(N-1)}\right\} \middle| a_{j_1}^{(1)}\right) p_{j_1}^{(1)}; \\ \sum_{j=1}^{n_1} p_j^{(1)} = 1; \dots; \sum_{j=1}^{n_N} p_j^{(N)} = 1. \end{cases}$$

ДРУГИЙ ЕТАП МММА

Метою другого етапу МММА є розрахунок оцінок результативності кожної з альтернатив параметрів морфологічної таблиці стратегій в умовах ситуації, заданої морфологічною таблицею сценаріїв. Тут ми за МТ сценаріїв вважаємо МТ, отриману в результаті першого етапу МММА. Морфологічну таблицю другого етапу назвемо морфологічною таблицею стратегій.

Для врахування зв'язків між параметрами морфологічних таблиць першого та другого етапів пропонується використовувати числову матрицю зв'язків. Відповідно до стратегії, кожній парі альтернатив $a_{j_1}^{(i_1)}, a_{j_2}^{(i_2)}$ різних характеристичних параметрів F_{i_1}, F_{i_2} дається оцінка $c_{i_1 j_1, i_2 j_2} \in [-1; 1]$

Оцінка	Тлумачення
-1	Альтернатива параметра МТ стратегій є абсолютно не ефективною при виборі відповідної альтернативи параметра МТ сценаріїв.
(-1;0)	Вибір відповідної альтернативи параметра МТ сценаріїв в певній мірі зменшує ефективність альтернативи параметра МТ стратегій.
0	Ефективність альтернативи параметра МТ стратегій ніяк не залежить від вибору відповідної альтернативи параметра МТ сценаріїв.
(0;1)	Вибір відповідної альтернативи параметра МТ сценаріїв в певній мірі збільшує ефективність альтернативи параметра МТ стратегій.
1	Альтернатива параметра МТ стратегій є повністю ефективною при виборі відповідної альтернативи параметра МТ сценаріїв.

ДРУГИЙ ЕТАП МММА

Після, розраховуються оцінки результативності $R_j^{(i)}$ кожної з альтернатив морфологічної таблиці стратегій $a_j^{(i)}$. Величина умовної результативності $R(a_j^{(i)}|\{a_{j_1}^{(1)}, a_{j_2}^{(2)}, a_{j_3}^{(3)}, \ldots, a_{j_N}^{(N)}\})$ альтернативи $a_j^{(i)}$, $i \in \overline{N+1, N+N'}$ при конфігурації МТ першого етапу $\{a_{j_1}^{(1)}, a_{j_2}^{(2)}, a_{j_3}^{(3)}, \ldots, a_{j_N}^{(N)}\}$:

$$R\left(a_j^{(i)} \middle| \left\{a_{j_1}^{(1)}, a_{j_2}^{(2)}, a_{j_3}^{(3)}, \ldots, a_{j_N}^{(N)}\right\}\right) = \frac{p_j^{'(i)} \cdot \prod_{m=1}^{N}\left(c_{mj_m,ij} + 1\right)}{\sum_{k=1}^{n_i}\left(p_k^{'(i)} \cdot \prod_{m=1}^{N}\left(c_{mj_m,ik} + 1\right)\right)}$$

Очікувана результативність альтернативи $a_j^{(i)}$ обчислюється за наступною формулою:

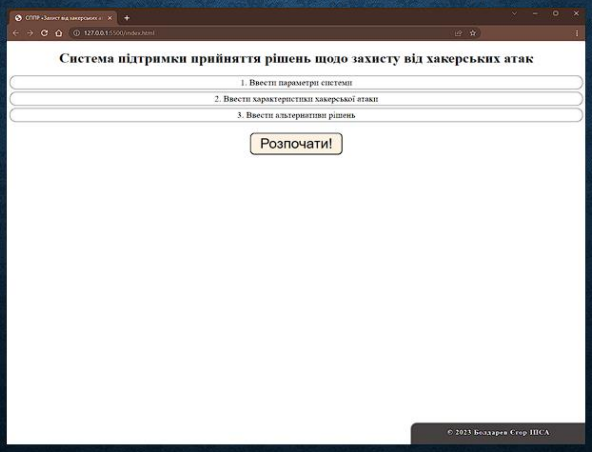
$$R_j^{(i)} = \sum_{j_1=1}^{n_1}\sum_{j_2=1}^{n_2}\ldots\sum_{j_N=1}^{n_N} R\left(a_j^{(i)} \middle| \left\{a_{j_1}^{(1)}, a_{j_2}^{(2)}, a_{j_3}^{(3)}, \ldots, a_{j_N}^{(N)}\right\}\right) P\left(\left\{a_{j_1}^{(1)}, a_{j_2}^{(2)}, a_{j_3}^{(3)}, \ldots, a_{j_N}^{(N)}\right\}\right)$$

ДРУГИЙ ЕТАП МММА З НЕРІВНОМІРНИМ РОЗПОДІЛОМ ПОЧАТКОВИХ ОЦІНОК

В умовах поставленої задачі, початкові оцінки, а точніше, оцінки характеристик хакерських атак, визначаються експертом без врахування параметрів системи-цілі хакерської атаки. Тож, перед тим, як проводити двоетапний модифікований метод морфологічного аналізу з метою дослідження ефективності стратегій щодо захисту від хакерської атаки, ми маємо отримати оновлені оцінки характеристик атак з врахуванням параметрів системи. Для цього проводиться другий етап двоетапного МММА, в якому за морфологічну таблицю сценаріїв приймається МТ параметрів системи, а за МТ стратегій – МТ характеристик хакерських атак.

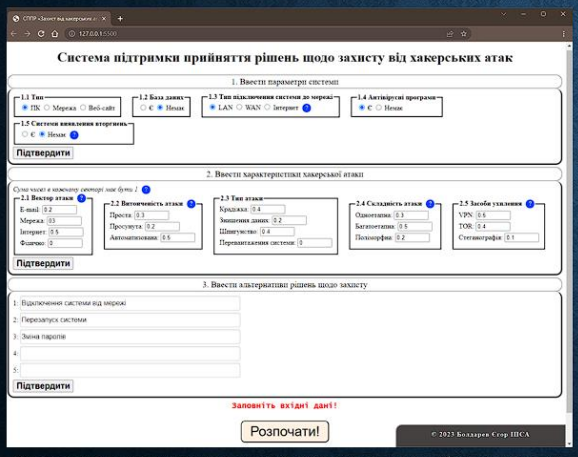
ПРИКЛАД

В якості прикладу наведено ситуацію, де цільовою системою є ПК середньостатистичного користувача та стандартні альтернативи захисту для нього

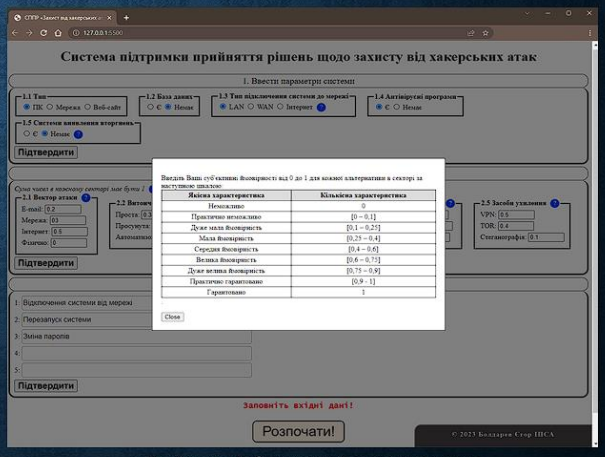


Початок роботи з СППР

ПРИКЛАД

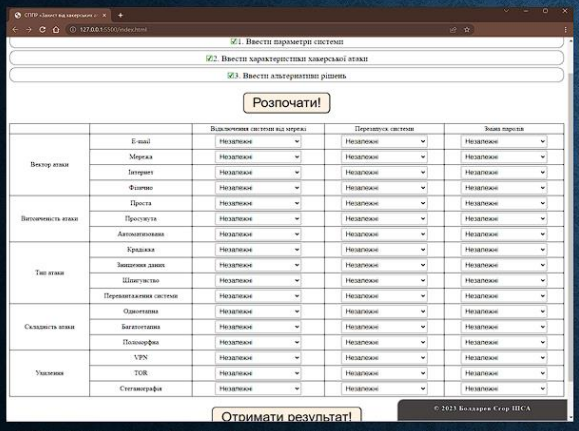


Заповнені користувачем дані та помилка про незбережені дані.



Довідкова інформація для користувача.

ПРИКЛАД



Збережені вхідні дані та початкова матриця зв'язків характеристик хакерських атак та альтернатив захисту.

Заповнена матриця зв'язків між характеристиками хакерських атак та альтернативами захисту.

ПРИКЛАД

При натисканні на кнопку «Отримати результат», отримується наступні висновки:

Зміна паролів	**0.4227806447725351**
Відключення системи від мережі	0.3336654021081129
Перезапуск системи	0.24355395311935193

Отже, найбільш ефективною альтернативою захисту в даній ситуації є зміна паролів.

ВИСНОВОК

Під час виконання роботи було досліджено та проаналізовано різновиди хакерських атак. Внаслідок чого було побудовано морфологічні таблиці для характеристик хакерських атак та параметрів системи-цілі атаки.

Проведено опис кожного з етапів двоетапного модифікованого методу морфологічного аналізу. Проаналізовано існуючі системи підтримки прийняття рішень, що пов'язані з кібербезпекою.

В результаті було спроектовано і реалізовано програмний продукт у вигляді системи підтримки прийняття рішень з веб-інтерфейсом на основі двоетапного модифікованого методу морфологічного аналізу з нерівномірним розподілом початкових оцінок. Приведено приклад використання розробленого програмного продукту.

ПОДАЛЬШИЙ РОЗВИТОК

В якості подальшого розвитку програмного продукту пропонується залучення баз даних та методи їх обробки. При реалізації такого сценарію розвитку можна досягти часткової, або навіть повної автоматизації роботи СППР.

ДЯКУЮ ЗА УВАГУ!