ДОДАТОК А

Графічний матеріал до магістерської роботи на тему

«Дослідження методів забезпечення безпеки ІС від фішингових атак»

А.1 ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Таблиця А.1 – Загальна характеристика роботи

Тема МАР	Дослідження методів забезпечення безпеки ІС від фішингових атак
Актуальність	Сучасні види фішингових загроз не можуть бути цілком попереджені доступними на ринку інформаційними системами з запобігання фішингових атак. Очевидно, існуючі методи забезпечення безпеки потребують суттєвого вдосконалення.
Мета досліджень	Метою даної роботи є дослідження методів ідентифікації та попередження фішингових атак, а також розробка вдосконаленого методу, призначеного для доповнення та підвищення ефективності існуючих методів забезпечення безпеки інформаційних систем від фішингових атак.
Задачі досліджень	Аналіз існуючих методів забезпечення безпеки ІС від фішингових атак ; Розробка вдосконаленого методу рейтингового оцінювання веб-сайту; Дослідження розробленого методу рейтингового оцінювання веб-сайту; Практичне використання вдосконаленого методу.
Об’єкт та предмет дослідження	Об’єктом дослідження в рамках даної магістерської атестаційної роботи є процес забезпечення безпеки інформаційних систем від фішингових атак.Предметом дослідження є методи ідентифікації та попередження фішингових атак.
Наукова новизна роботи	Новизна роботи полягає в дослідженні та розробці вдосконаленого методу рейтингового оцінювання веб-сайту, розробці етапів та алгоритму його реалізації, а також в результатах дослідження ефективності та автоматизації методу.

А.2 ІСНУЮЧІ МЕТОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІС ВІД ФІШИНГОВИХ АТАК

Таблиця А.2.1 – Загальна характеристика існуючих методів з забезпечення безпеки ІС від фішингових атак.

Метод ідентифікації шкідливих веб-сайтів на основі спеціалізованих списків	Аналіз всіх доступних в інтернеті веб-сайтів. За допомогою алгоритмів на основі штучного інтелекту ідентифікуються шкідливі веб – сайти та додаються в спеціалізовані списки. Коли клієнт (як правило, браузер) намагається отримати шкідливу веб-сторінку, метод відображає проміжну сторінку попередження про небезпечність веб-сайту
Методу ідентифікації фішингових електронних листів	Блокування користувачу можливості отримати ідентифікований методом фішинговий електронний лист та блокування можливості перейти по небезпечній URL-адресі. Попередження користувача про підозрілість електронного листа. Серед параметрів, що аналізуються: надійність відправника, характерні ознаки фішингових листів, додатки та URL-адреси.
Метод рейтингового оцінювання веб-сайту	Аналіз веб-сайту здійснюється за багатьма параметрами, серед яких: наявність та рівень SSL-сертифікату; аналіз рейтингу хостинг-провайдера веб-сайту; аналіз рейтингу доменного регістратора веб-сайту та ін. За результатами аналізу обчислюється рейтингова оцінка веб-сайту та за необхідністю відбувається попередження користувача про небезпечність веб-сайту.

Таблиця А.2.2 – Основні проблеми існуючих методів з забезпечення безпеки ІС від фішингових атак.

Метод ідентифікації шкідливих веб-сайтів на основі спеціалізованих списків	Вразливість до систем розподілення трафіку(TDS) та клоакінгу. Вразливість до обфускації коду веб-сайтів.
Метод ідентифікації фішингових електронних листів	Вразливість до обфускації html-коду листів та URL-адрес веб-сайтів.
Метод рейтингового оцінювання веб-сайту	Запобігання об’єктивному рейтинговому оцінюванню веб-сайту за рахунок вразливих до підлаштування параметрів оцінювання. Ігнорування особливо явних параметрів, що характерні для фішингових веб-сайтів.

А.3 ВДОСКОНАЛЕНИЙ МЕТОД РЕЙТИНГОВОГО ОЦІНЮВАННЯ ВЕБ-САЙТУ

Таблиця А.3.1 – Етапи вдосконаленого методу рейтингового оцінювання веб-сайту

Етап 1	Отримання параметрів веб-сайту для аналізу. Вдосконалений метод має отримувати і оцінювати веб-сайти за такими параметрами: -дата реєстрації доменного імені веб-сайту; -кількість рівнів доменного імені; -відстеження ознак систем розподілення трафіку; -належність веб-сайту до 10000 найбільш відвідуваних веб-сайтів; -наявність форм вводу та відправки даних на веб-сайті.
Етап 2	Ідентифікація ознак систем розподілення трафіку на веб-сайті.
Етап 3	Обчислення рейтингу та ступеню загрози веб-сайту.

Таблиця А.3.2 – Деталізація етапу отримання параметрів веб-сайту для аналізу.

1 Отримання параметрів веб-сайту	Параметри для аналізу можуть бути отримані з відкритих джерел з вільним доступом
2 Обчислення коефіцієнтів, заснованих на параметрах веб-сайту	m – коефіцієнт часу з моменту реєстрації доменного імені, $m \in [1; \infty)$, (3) Дорівнює повним місяцям з дати реєстрації доменного імені. Якщо з дати реєстрації доменного імені пройшло менше повного місяця, m приймає значення 1; z – коефіцієнт кількості рівнів доменного імені, $z \in [0; 2]$, (3) Обчислюється за таким правилами: Якщо $0 \geq l \leq 2$, то $z = 0$, (4) Якщо $3 > l \leq 3$, то $z = 1$, (5) Якщо $3 > l \leq 127$, то $z = 2$, (6) Де l – кількість рівнів доменного імені веб-сайту. Може приймати значення у діапазоні $l \in [0; 127]$. p- коефіцієнт наявності форм вводу та відправки даних, $p \in [0; 1]$, (7) За наявності на веб-сайті форм вводу та відправки даних, p приймає значення 1, за відсутності – p приймає значення 0. f- коефіцієнт наявності веб-сайту у списку 10000 найбільш відвідуваних сайтів , $f \in [0; 1]$, (8) За наявності веб-сайту у списку 10000 найбільш відвідуваних, f приймає значення 1, за відсутності – f приймає значення 0.

Таблиця А.3.3 – Деталізація етапу ідентифікації ознак систем розподілення трафіку на веб-сайті

1 Аналіз поведінки веб-сайту під час HTTP-запиту та отримання вмісту веб-сторінки на стороні клієнта.	Аналіз поведінки включає фіксацію переадресовувань, фіксацію відповідей сайту HTTP Status Codes
2 Аналіз поведінки веб-сайту під час HTTP-запиту та отримання вмісту цієї веб-сторінки на стороні сервера.	Запит зі сторони сервера означає ідентичній клієнтському HTTP-запит, що має ідентифікувати себе як автоматизований робот(бот). У складі заголовку HTTP-запиту на веб-сайт у параметр “UserAgent” підставити значення, характерне для HTTP-запитів ботів, які аналізують веб-сайти у складі ІС з забезпечення безпеки Google Safe Browsing.
3 Порівняння результатів аналізу поведінки веб-сайту	Порівняння відбувається між зафіксованими результатами зі сторони клієнта та сервера. $A_{\text{клієнта}}$ - кінцева веб-адреса зі сторони клієнта. $A_{\text{сервера}}$ - кінцева веб-адреса зі сторони сервера. $A_{\text{сервера}}$ та $A_{\text{клієнта}}$ будуть порівняні на першому та другому рівні доменного імені сайту. Наприклад URL-адреси “bank.org” та “login.bank.org” метод буде оцінювати як однакові, бо перший і другий рівень доменного імені ідентичний: “bank.org”. $R_{\text{клієнта}}$ - HTTP Status Code зі сторони клієнта незалежно від наявності переадресовувань. $R_{\text{сервера}}$ - HTTP Status Code зі сторони сервера незалежно від наявності переадресовувань. $R_{\text{сервера}}$ та $R_{\text{клієнта}}$ будуть порівняні. t - коефіцієнт ідентифікації ознак використання технологій клоакінгу та систем розподілення трафіку, $t \in [0; 1]$ та розраховується за такими правилами: якщо $R_{\text{сервера}} = R_{\text{клієнта}}$ AND $A_{\text{сервера}} = A_{\text{клієнта}}$ то $t = 0$; якщо $R_{\text{сервера}} \neq R_{\text{клієнта}}$ OR $A_{\text{сервера}} \neq A_{\text{клієнта}}$ то $t = 1$;

Таблиця А.3.4 – Деталізація етапу обчислення рейтингу та ступеню загрози веб-сайту

1 Обчислення рейтингової оцінки $W_{\text{сайту}}$	Формула розрахунку рейтингу: $W_{\text{сайту}} = \left(25 * \frac{1}{m}\right) + (2.5 * 2^z * z) + 15 * p + 15 * f + 25 * t$, (1) $W_{\text{сайту}}$ – підсумковий рейтинг веб-сайту. При отриманні нецілого результату застосовується математичне округлення до найближчого цілого ; $0 \geq W_{\text{сайту}} \leq 100$, (2)
2 Обчислення Ступінь загрози x веб-сайту	Ступінь загрози x визначається на основі значення $W_{\text{сайту}}$ за такими правилами: якщо $0 \geq W_{\text{сайту}} \leq 30$, то $x = 0$, (10) якщо $30 > W_{\text{сайту}} \leq 50$, то $x = 1$, (11) якщо $50 > W_{\text{сайту}} \leq 100$, то $x = 2$. (12) Значення $x = 1$ та то $x = 2$ означає середню та високу загрозу відповідно, та алгоритм передбачає сповіщення користувача. Значення $x = 0$ означає, що загроза не була знайдена і не передбачає сповіщення користувача.

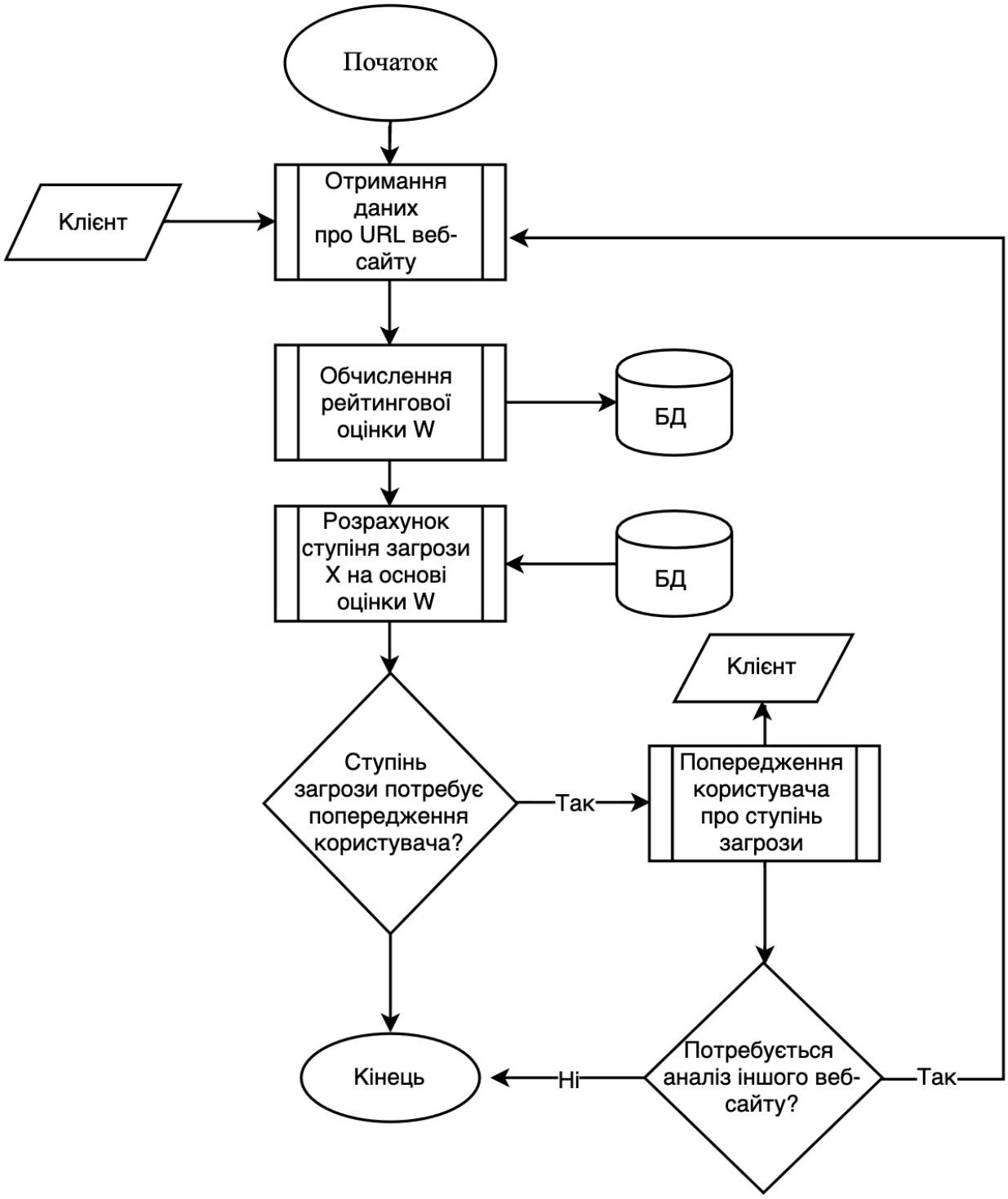

Рисунок А.3.1– Базовий алгоритм нового методу забезпечення безпеки користувачів веб-сайтів

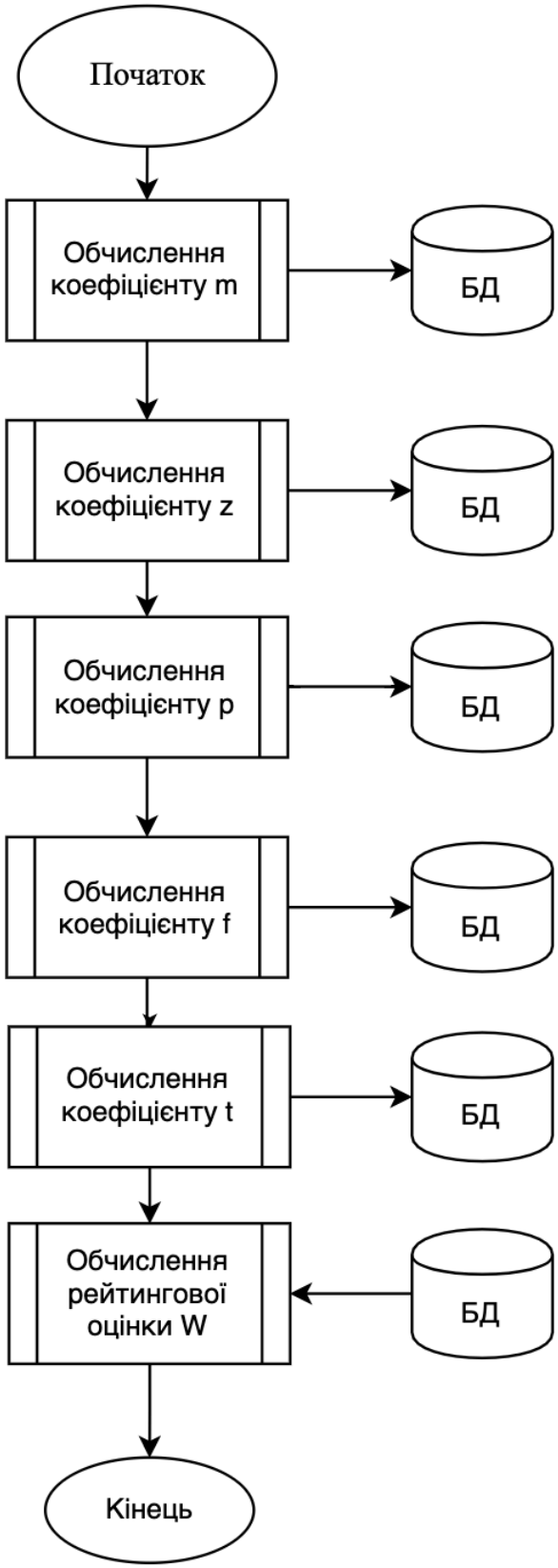

Рисунок А.3.2 – Деталізація алгоритму обчислення рейтингової оцінки $W_{\text{сайту}}$

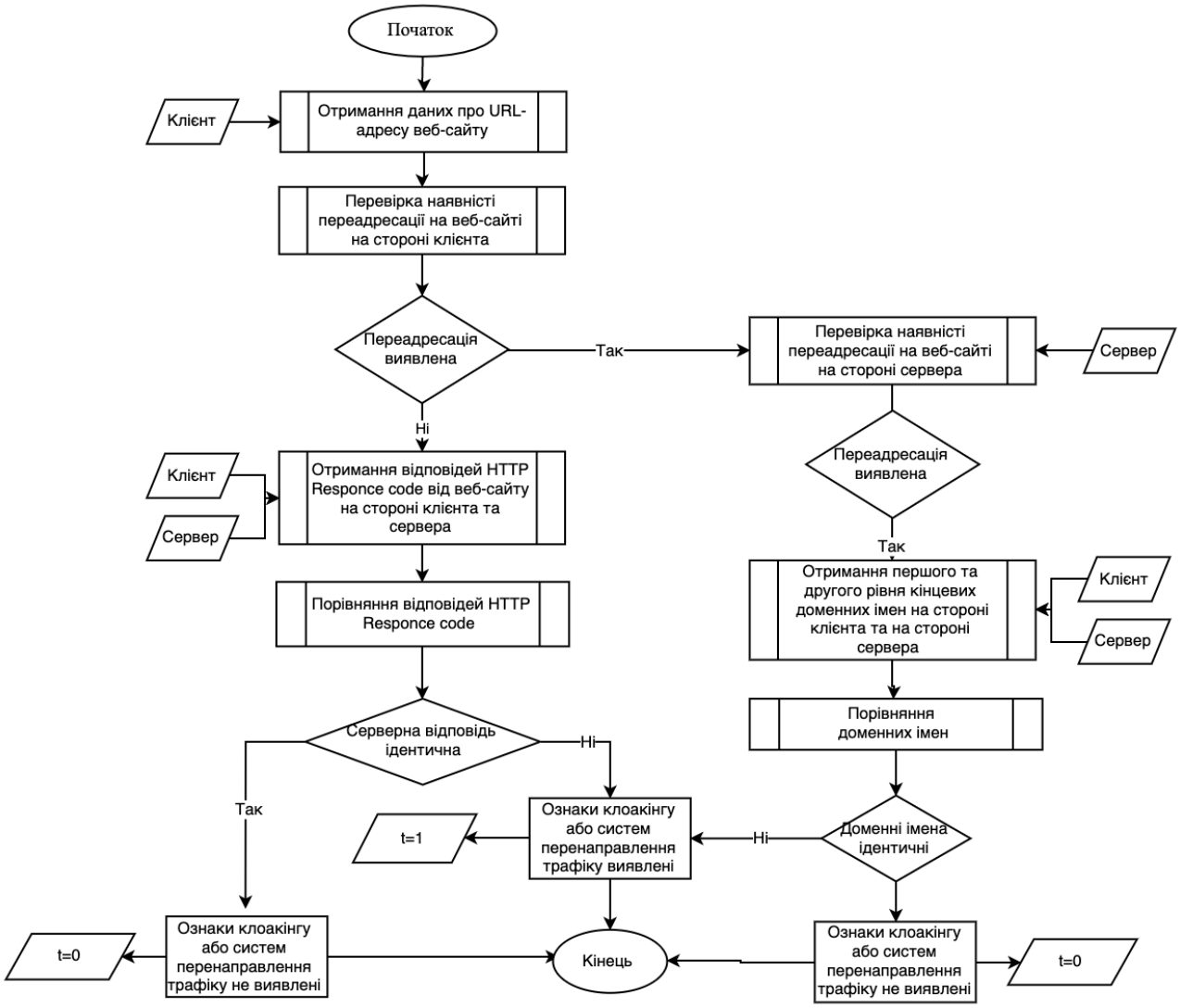

Рисунок А.3.3 – Деталізація алгоритму обчислення коефіцієнту ідентифікації ознак використання систем розподілення трафіку t

А.4 ОПИС ЕКСПЕРИМЕНТУ

Таблиця А.4.1 – результат розрахунку $W_{\text{сайту}}$ – підсумкового рейтингу веб-сайтів.

URL-адреса веб-сайту	Коеф. m	Коеф. z	Коеф. p	Коеф. f	Коеф. t	$W_{\text{сайту}}$	Ступін загрози x, розрахована н основі $W_{\text{сайту}}$
http://www.shibaurahacnet.chifanblack.top/	>50	1	1	1	0	35	1 (підозрілий)
https://www.protectiserv.com.br/fr/Office365.php	>50	1	1	1	1	60	2(небезпечний
http://liverpoolstreetphysio.com/cimi/citi	>50	0	1	1	1	50	2(небезпечний
http://www.tesla-3.online/ethers/	1	0	0	1	0	35	1 (підозрілий)
http://punnagaigroup.com/c/ali-old/	10	0	1	1	0	33	1 (підозрілий)
https://ikanosecure.com/cb/	1	0	1	1	0	50	2(небезпечний
https://appjbb.com/acompanhamento/	1	0	1	1	1	80	2(небезпечний
http://suporte-30horas.ddns.net:2019/autenticar/index1.php	1	1	1	1	1	90	2(небезпечний
https://xxxb0faxxx.webcindario.com	>50	1	1	1	0	40	1 (підозрілий)
https://ca.surveygizmo.com/s3/50062717/ATT-NET	2	1	1	1	0	53	2(небезпечний

Продовження таблиці А.4.1 – результат розрахунку $W_{\text{сайту}}$ – підсумкового рейтингу веб-сайтів.

URL-адреса веб-сайту	Коеф. m	Коеф. z	Коеф. p	Коеф. f	Коеф. t	$W_{\text{сайту}}$	Ступінь загрози x, розрахована на основі $W_{\text{сайту}}$
https://Nure.ua	>50	0	0	1	0	15	0(безпечний)
https://Ru.Wikipedia.org	>50	1	0	0	0	10	0(безпечний)
https://Facebook.com	>50	0	1	0	0	15	0(безпечний)
https://Privat24.ua	>50	0	1	0	0	15	0(безпечний)
https://Google.com	>50	0	0	0	0	1	0(безпечний)

Таблиця А.4.2 – результат розрахунку $W_{\text{сайту}}$ – підсумкового рейтингу веб-сайтів.

URL-адреса веб-сайту	Google Safe Browsing: наявність у списках небезпечних ресурсів	Netcraft Chrome extention: оцінка(0-10), попередження користувача	Ступінь загрози x, отримана удосконаленим методом
http://www.shibaurahacnet.chifanblack.top/	Не виявлено	10, не попереджено	1 (підозрілий)
https://www.protectiserv.com.br/fr/Office365.php	Виявлено	10, попереджено	2(небезпечний)
http://liverpoolstreetphysio.com/cimi/citi	Виявлено	10, попереджено	2(небезпечний)
http://www.tesla-3.online/ethers/	Не виявлено	10, не попереджено	1 (підозрілий)
http://punnagaigroup.com/c/ali-old/	Виявлено	7, попереджено	1 (підозрілий)
https://ikanosecure.com/cb/	Не виявлено	7, не попереджено	2(небезпечний)
https://appjbb.com/acompanhamento/	Не виявлено	10, попереджено	2(небезпечний)
http://suporte-30horas.ddns.net:2019/autenticar/index1.php	Виявлено	10, попереджено	2(небезпечний)

Продовження таблиці А.4.2 – результат розрахунку $W_{\text{сайту}}$ – підсумкового рейтингу веб-сайтів.

URL-адреса веб-сайту	Google Safe Browsing: Наявність в списках небезпечних ресурсів	Netcraft Chrome extention: оцінка(0-10), попередження користувача	Ступінь загрози x, отримана удосконаленим методом (0-2)
https://xxxb0faxxx.webcindario.com/	Виявлено	10, попереджено	1 (підозрілий)
https://ca.surveygizmo.com/s3/50062717/ATT-NET	Не виявлено	1, не попереджено	2(небезпечний)
https://Nure.ua	Не виявлено	1, не попереджено	0(безпечний)
https://Ru.Wikipedia.org	Не виявлено	0, не попереджено	0(безпечний)
https://Facebook.com	Не виявлено	0, не попереджено	0(безпечний)
https://Privat24.ua	Не виявлено	0, не попереджено	0(безпечний)
https://Google.com	Не виявлено	0, не попереджено	0(безпечний)

А.4 ЗАСТОСУВАННЯ ТА АВТОМАТИЗАЦІЯ ВДОСКОНАЛЕНОГО МЕТОДУ НА ПРАКТИЦІ

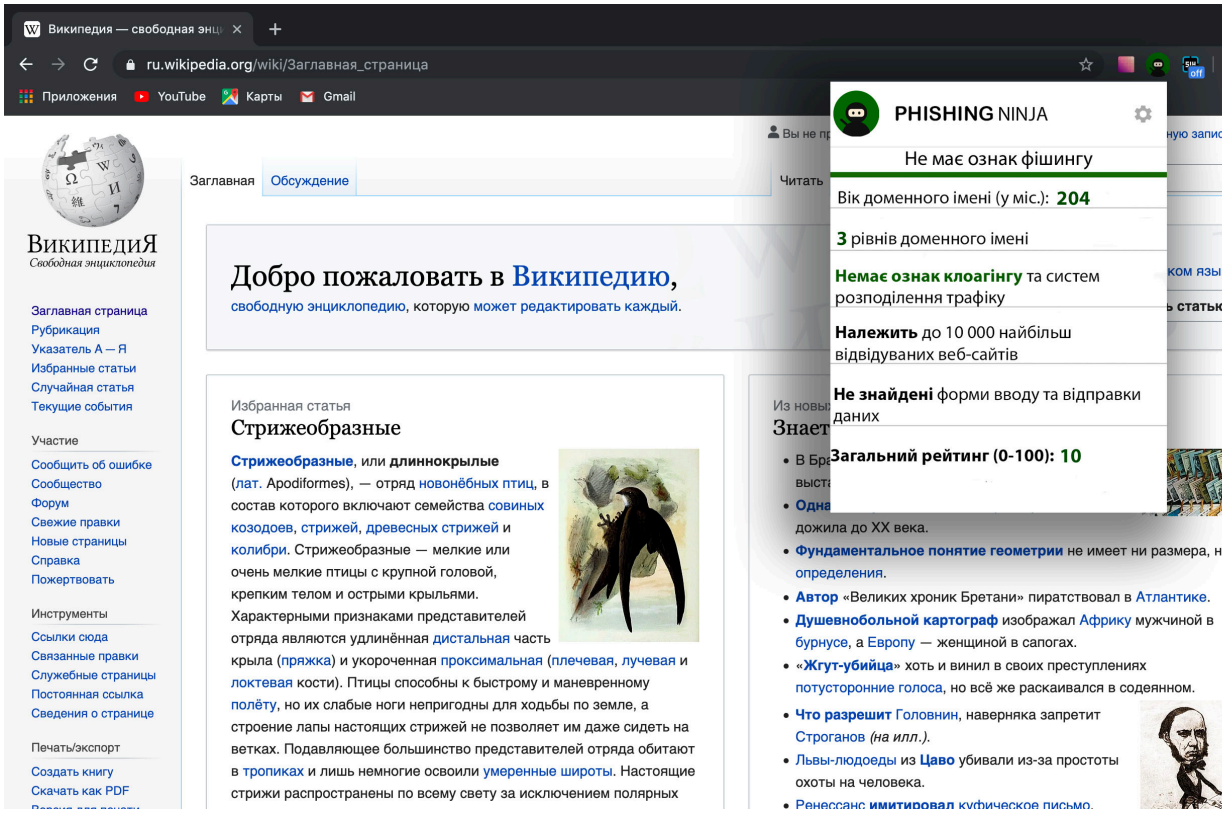

Рисунок А.4.1 – Інтерфейс розробленого додатку при запиті користувачем рейтингової оцінки веб-сайту.

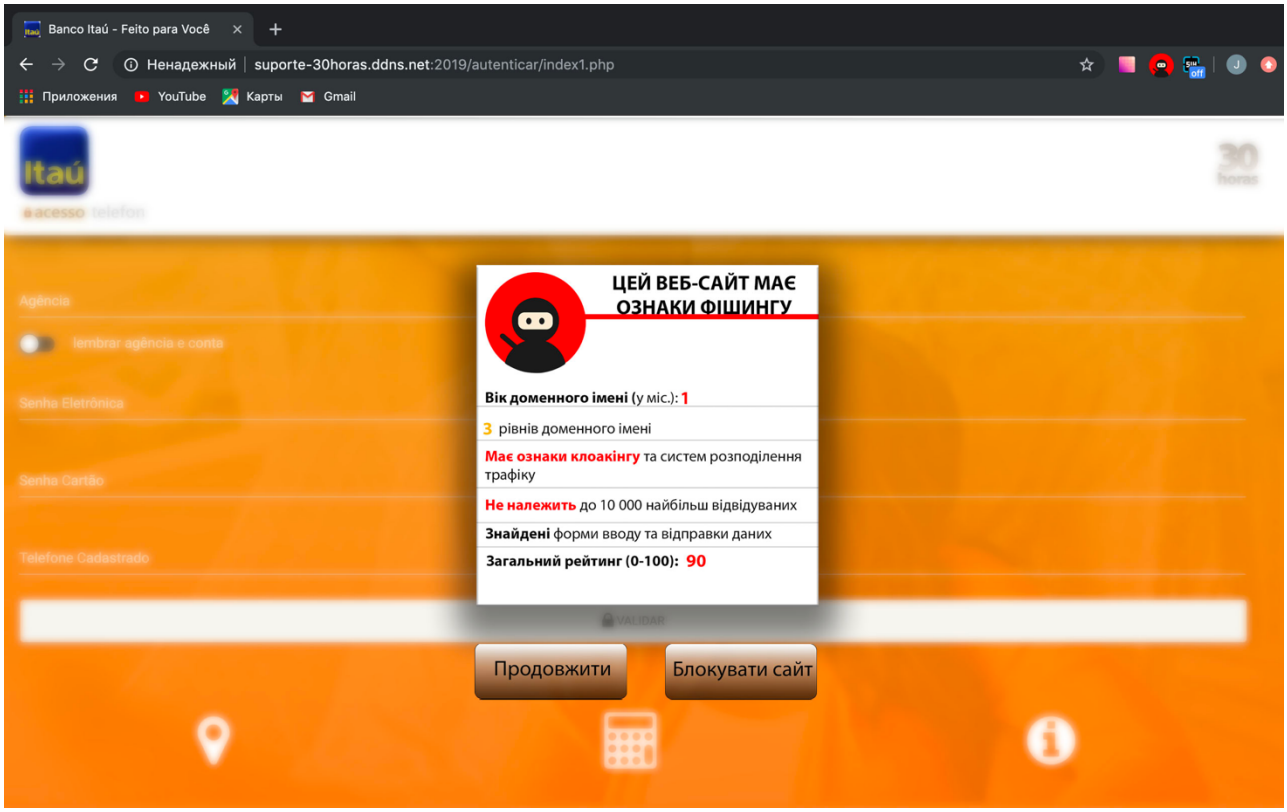

Рисунок А.4.2 – Інтерфейс розробленого додатку при попередженні користувача при ступені загрози веб сайту $x = 2$ “небезпечно” .

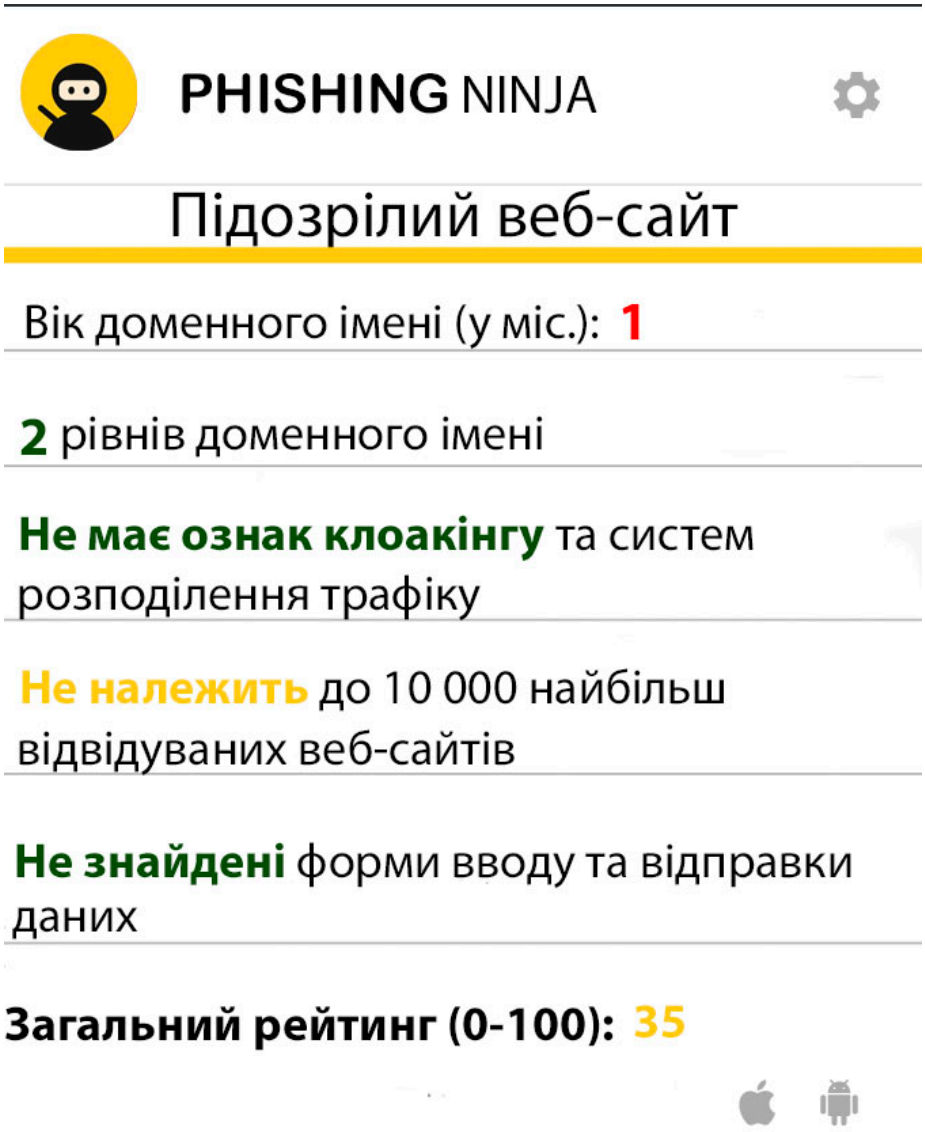

Рисунок А.4.3 – Частково зображений інтерфейс розробленого додатку при попередженні користувача при ступені загрози веб сайту $x = 1$ “підозрілий” .