Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Комп'ютерних наук
(повна назва)
Кафедра Інформаційно управляючих систем
(повна назва)

АТЕСТАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)
(рівень вищої освіти)

Дослідження методів забезпечення безпеки інформаційних систем від фішингових атак
(тема)

Виконав: студент 2 курсу, групи ІУСТм-18-1
Скакун Р.Г.
(прізвище, ініціали)

Спеціальність 122 – Комп'ютерні науки
(код і повна назва спеціальності)
Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма Інформаційні управляючі системи та технології
(повна назва освітньої програми)

Керівник проф. Левикін В.М.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри ІУС _____ _____
(підпис) (прізвище,ініціали)

2019 р.

Харківський національний університет радіоелектроніки

Факультет Комп'ютерних наук
(повна назва)
Кафедра Інформаційно управляючих систем
(повна назва)
Рівень вищої освіти другий (магістерський)
Спеціальність 122 – Комп'ютерні науки
(код і повна назва)
Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма Інформаційні управляючі системи та технології
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«____»_____ 2019 р.

ЗАВДАННЯ
НА АТЕСТАЦІЙНУ РОБОТУ

Студенту Скакуну Ростиславу Гориславовичу
(прізвище, ім'я, по батькові)

1. Тема роботи: Дослідження методів забезпечення безпеки інформаційних систем від фішингових атак
затверджена наказом університету від 31 жовтня 2019 р.
2. Термін подання студентом роботи до екзаменаційної комісії 17 грудня 2019
3. Вихідні дані до роботи Науково-технічні публікації та інтернет джерела з тематики атестаційної роботи
4. Перелік питань, що потрібно опрацювати в роботі Вступ; Аналіз існуючих методів забезпечення ІС від фішингових атак; Розробка вдосконаленого методу рейтингового оцінювання веб-сайту; Дослідження розробленого методу; Практичне використання вдосконаленого методу рейтингового оцінювання веб-сайту; Висновки
5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій
Блок схеми алгоритмів існуючих методів забезпечення безпеки ІС від фішингових атак; приклади інтерфейсів існуючих додатків; блок схеми алгоритму вдосконаленого методу; дані, обчислення та результати експерименту; екранні форми.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Аналіз літератури та Інтернет-джерел	4.11.19 – 10.11.19	
2	Постановка задачі	10.11.19-12.11.19	
3	Обробка матеріалу	12.11.19 – 15.11.19	
4	Аналіз існуючих методів розподілення робіт та постановка задачі дослідження	15.11.19 – 18.11.19	
5	Розробка вдосконаленого методу розподілення робіт	18.11.19 – 25.11.19	
6	Дослідження розробленого методу розподілення робіт	25.11.19 – 28.11.19	
7	Практичне використання вдосконаленого методу розподілення робіт	28.11.19 – 1.12.19	
8	Написання пояснювальної записки	1.12.19– 6.12.19	
9	Підготовка презентації	6.12.19 – 9.12.19	
10	Перевірка на плагіат	9.12.19	
11	Нормоконтроль	9.12.19 – 16.12.19	
12	Захист	17.12.19	

Дата видачі завдання 4 листопада 2019 р.

Студент _____
(підпис)

Керівник роботи _____ проф. Левикін В.М.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка до атестаційної роботи містить: 65 сторінок, 9 рисунків, 3 таблиці, 29 джерел.

Додаток А містить: 17 сторінок, 6 рисунків, 8 таблиць.

ФІШИНГ, ІНФОРМАЦІЙНІ СИСТЕМИ, ІДЕНТИФІКАЦІЯ ФІШИНГОВИХ АТАК, ФІШИНГОВА АТАКА, ШКІДЛИВИЙ ВЕБ-САЙТ, ДОДАТОК, GOOGLE SAFE BROWSING, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ

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 фішінгових атак.

Об’єктом дослідження в рамках даної магістерської атестаційної роботи є процес забезпечення безпеки ІС від фішінгових атак.

Предметом дослідження є методи ідентифікації та попередження фішингових атак.

Теоретичними результатами дослідження є описи етапів впровадження вдосконаленого методу рейтингового оцінювання веб-сайтів та блок схеми алгоритмів методу.

Практичними результатами є використання вдосконаленого методу рейтингового оцінювання веб-сайтів на практиці за допомогою демонстраційного додатку.

Новизна дослідження 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.

ABSTRACT

Explanatory note to the certification work contains 65 pages, 9 figures, 3 tables, 29 sources.

Attachment A contains: 17 pages, 6 figures, 8 tables

PHISHING, INFORMATION SYSTEMS, IDENTIFICATION OF PHISHING ATTACKS, PHISHING ATTACK, MALICIOUS WEBSITE, APP, GOOGLE SAFE BROWSING, PHISHING PREVENTION, SOFTWARE

The purpose of this work is to investigate methods for identifying and preventing phishing attacks, as well as developing an advanced method designed to complement and enhance the effectiveness of existing methods of ensuring the security of information systems against phishing attacks.

The object of research in the course of this master's certification work is the process of ensuring the security of information systems against phishing attacks.

The subject of the paper is methods of identification and prevention of phishing attacks.

The theoretical results of the study are descriptions of the stages of implementation of the advanced method of rating websites and a block diagram of the method algorithms.

The practical results are the use of an advanced method of rating websites in practice with a demo application.

The novelty of the research is the research and development of an improved method of rating websites, the development stages of its implementation, the algorithm of implementation, as well as the results of method automation.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

БД – база даних;

ІС – інформаційна система;

TDS – системи розподілення трафіку;

ОС – операційна система;

ПЗ – програмне забезпечення;

СУБД – Система Управління Базами Даних;

IDE – середовище розробки;

HTML – Hypertext Markup Language;

HTTP – Hyper Text Transfer Protocol

JSON – JavaScript Object Notation;

SSL - Secure Sockets Layer

ВСТУП

Фішинг – одна з найбільш поширених загроз в мережі Інтернет і однаково небезпечна для користувачів всіх рівнів. Швидкий розвиток даного напрямку кіберзлочинності обумовлений дуже багатьма факторами, серед яких: безкарність злочинців, що скоюють подібні злочини, велика цінність вилученої у жертв інформації, технічна недосконалість існуючих засобів та систем боротьби з фішингом та низька кваліфікація рядових користувачів Інтернету у питаннях комп'ютерної безпеки.

Крім того, навіть користувач із комплексом антифішингового програмного забезпечення все ще може стати жертвою фішингу. Це пов'язано з тим, що способи обходу систем захисту розвиваються швидше, ніж самі системи захисту і ніяке з існуючих програмних або технічних рішень не зможе повністю захистити користувача від втрати персональних даних. У підтвердження тому, приблизна оцінка збитків[4], завданих бізнесу в США у період с 2014 по 2017, дорівнює п'ятиста мільйонам доларів США щорічно, що засвідчує нездатність систем з забезпечення безпеки ефективно протистояти фішинговим атакам, а масштаб збитків доводить необхідність в розробці нових та вдосконаленні існуючих систем захисту від таких атак.

За визначенням, фішинг – злочин, направлений на отримання конфіденційної інформації, такої як імена користувачів і паролі, з використанням методів соціальної інженерії за допомогою підроблених сайтів та електронних листів від імені реальних компаній. Існує багато різновидів фішингу, основні з яких будуть розглянені у цій магістерській роботі, але об'єднує всі існуючі методи фішингу одне – людина, яка є жертвою цього злочину, завжди найбільш вразлива і ненадійна складова будь-якої антифішингової інформаційної системи. Це означає, що ні одна спроба фішингу не може бути успішною для зловмисника,

якщо особа, на яку направлена фішингова атака, має достатньо фактів и знань для ідентифікації атаки і відмовиться передавати конфіденційні дані.

Об’єктом дослідження в рамках даної магістерської атестаційної роботи є процес забезпечення безпеки інформаційних систем від фішінгових атак

Предметом дослідження є методи ідентифікації та попередження фішингових атак.

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 фішінгових атак.

Для досягнення визначеної мети в магістерській атестаційній роботі будуть вирішені такі задачі:

– дослідження існуючих методів з забезпечення безпеки інформаційних систем від фішингових атак;

– критичний аналіз існуючих методів з забезпечення безпеки;

– розробка вдосконаленого методу з забезпечення безпеки інформаційних систем;

– дослідження нового методу;

– практичне використання нового методу на контрольних прикладах.

Робота виконана і оформлена згідно з вимогами стандарту ДСТУ 3008 2016 [1]та методичними вказівками 2019 року[2] у виді пояснювальної записки. У даній магістерській науковій роботі є посилання на результати досліджень таких вітчизняних вчених, як В.М. Левикін, О.П. Костенко, О.В. Петриченко[10]

1 АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ ВІД ФІШІНГОВИХ АТАК ТА ПОСТАНОВКА ЗАДАЧІ ДОСЛІДЖЕННЯ

1.1 Аналіз актуальності дослідження методів забезпечення безпеки інформаційних систем від фішінгових атак

Сьогоденні методи фішингу швидко та успішно еволюціонують з метою запобігання їх ідентифікації антифішинговими інформаційними системами, максимізуючи життєвий цикл підробленого веб-сайту та кількість скомпрометованих даних користувачів і мінімізуючи витрати на організацію та підтримку фішингової атаки.

Згідно з даними досліджень за 2017 рік[5], середній розмір збитків від успішних фишингових атак, завдаваємий великим компаніям дорівнює 1.6 мільйонів доларів США, а підрахувати точні збитки, яких зазнають індивідуальні особи, не є можливим. Ні окремі користувачі, ні бізнес, не можуть бути цілком захищені від сучасних засобів викрадення конфіденційних даних, навіть користуючись всіма доступними на ринку інформаційними системами з виявлення та запобігання загроз. Найбільш часті жертви фішингу - банки, електронні платіжні системи, почтові сервіси, соціальні мережі . Інтерес злочинців розподілений між фінансовою вигодою та шпіонажем на 59 і 41 відсотків відповідно.[6]

За статистичними даними[3] більшість актів кіберзлочинності у Європі та всьому світі залишаються нерозкритими, а їх ініціатори залишаються непокараними. Через те, що більшість злочинців успішно переховується від слідчих дій і працюють майже в повній анонімності, розслідування таких злочинів не набуває достатньої ефективності у загальній картині боротьби з фішингом.

Ступінь успіху фишінгових атак сигналізує про те, що на ринку не представлені продукти, здатні забезпечити захист інформаційних систем у повному обсязі. Майже всі подібні атаки значною мірою покладаються на соціальну інженерію, з метою переконати користувачів негайно вжити заходів і, тим самим, блокуючи можливість та бажання детального аналізу ситуації. Через це, боротьба з фішингом потребує цілого комплексу заходів, направлених на забезпечення захисту інформаційних систем та їх користувачів.

У даній роботі проаналізовані два основних напрямки фішингових атак, незалежно від способу їх поширення. Це “масова фішинг-атака” та “направлена фішинг-атака”.

Масова фішинг-атака за характером розгортання, як правило, має ознаки "сліпої" спроби заволодіти даними, та передбачує тільки одну стадію атаки. Це може бути почтова розсилка або інший метод доставки підробленого веб-ресурсу, масово відправлений потенційним жертвам на основі отриманих раніше даних про їх інтереси, причетність до конкретних організацій, тощо. Згідно с цією моделлю атаки, зловмисник не зосереджений на конкретній жертві, а покладається про "велику кількість" потенційних жертв, щоб зібрати значну кількість викрадених даних у результаті нападу.

Демографія жертв у таких типах атак не враховується через масовий характер атаки. У процентному співвідношенні успіх таких атак є невеликим[7], проте за рахунок великого об’єму розсилок такі атаки часто залишаються фінансово ефективними для злочинця.

Методами розповсюдження для такої атаки є, зазвичай: електронна пошта, спам у соціальних мережах, або навіть пошукова і рекламна видача у відомих пошукових системах[8]

Направлена фішинг – атака, націлена спеціально на окремих людей, невеликої групи осіб або ж на співробітників цілої організації. З цієї причини для такого підходу характерний більш складний процес атаки, ніж звичайний фішинг, завдяки якому ітеративний збір інформації (розвідка) та соціальна

інженерія використовується для максимізації шансів на успішне досягнення мети атаки. Через ітеративну динаміку атаки і покроковий збір інформації про цільовий об’єкт, нападник є більш гнучким у виборі методів досягнення своєї мети. Багатоступеневий характер атаки дає можливість побудувати стратегію на основі попередньої взаємодії з потерпілим, що може стати основою для подальших нападів; наприклад, зловмисник може скористатися попереднім рішенням, які приймав потерпілий під час цієї взаємодії для посилення імовірності задоволення подальшого запиту.

Демографічні показники жертв для атакуючого у цьому підході до фішингу мають дуже важливу роль, а процеси у кампанії, як правило, дуже добре аналізуються зловмисником перед початком нападу. Етап збору інформації дозволяє зловмиснику отримати розвідку стосовно профілю, звичок та соціального оточення жертви. Важливо, що за допомогою цієї оцінки зловмисник також може

зробити висновок про коло довіри навколо жертви та визначити можливі слабкі місця, щоб увійти в нього.

Для цього типу атаки також характерна не просто техніка викрадення інформації у окремої жертви, а й її використання як засіб отримати тривалий доступ до пристроїв, систем та / або баз даних для проведення складних розвідок та шпіонажу.

Отже, згідно с даними досліджень[3-7], спостерігається дужне невтішна тенденція, згідно з якою у найближчому майбутньому не очікується рішень для остаточного вирішення проблеми успішності фішинг-атак. Очевидно, що існуючі методи забезпечення безпеки інформаційних систем від фішингових атак потребують суттєвого вдосконалення, а отже, ретельного дослідження. Саме тому у цій магістерській роботі були досліджені та проаналізовані методи забезпечення безпеки інформаційних систем від фішингових атак.

1.2 Аналіз існуючих методів з забезпечення безпеки інформаційних систем від фішінгових атак

Надшвидкий розвиток фішингу як кримінального явища спонукав великі корпорації на відповідні заходи. Виробники захисних рішень розробили спеціальні фільтри з метою виявлення фішингових атак в електронних листах, розробили способи ідентифікації шкідливих ресурсів на основі спеціалізованих списків. Існують незалежні ресурси, що займаються моніторингом та ідентифікацією фішингових ресурсів силами волонтерів.

Втім, в більшості атак шахраї використовують комплексні заходи з обходу усіх існуючих інформаційних систем з забезпечення захисту. Наприклад, замість звичайного текстового формату у електронних листах, використовуються зображення. Крім того, фішингові веб-сайти часто покладаються на методи заплутування(обфускації) коду, щоб запобігти детектуванню зловмисної активності з боку систем захисту на основі штучного інтелекту. Зазвичай фішингові атаки застосовують шифрування на базі алгоритмів AES-256 або Base64 у JavaScript[11], або ж інші методики, що ускладнюють аналіз базового вихідного коду.

Як результат дослідження існуючих методів забезпечення безпеки, методи були розподілені на основних групи:

– метод ідентифікації шкідливих веб-сайтів на основі спеціалізованих списків;

– метод ідентифікації фішингових електронних листів;

– метод рейтингової оцінки веб-сайтів;

1.2.1 Аналіз методу ідентифікації шкідливих веб-сайтів на основі спеціалізованих списків

Серед великої кількості представлених на ринку систем з забезпечення безпеки інформаційних систем від фішінгових атак неможливо виділити найбільш дієвий і надійний з них. У цій роботі були проаналізовані найбільш масові інформаційні системи з забезпечення безпеки, серед яких:

– ІС з забезпечення безпеки як сервіс – Google safe browsing, Yandex Safe browsing, OpenDns, Phishtank[12];

– ІС з забезпечення безпеки як встановлений додаток – Антивірусні ПО, додатки до веб-браузерів, тощо.

Одним з найбільш розвинутих комплексів методів з забезпечення безпеки є Google Safe Browsing, сервіс, за замовчуванням інтегрований у такі веб-браузери, як Google Chrome, Chromium, Safari, Mozilla Firefox, Micrsoft Edge та ін. За даними Google, ІС Google Safe Browsing налічує більш ніж два мільярди користувачів[8].

Основна мета Google Safe Browsing - попередити та відвернути кінцевого користувача від відвідування шкідливих URL-адрес. Сервіс реалізований на рівні додатків (рівень HTTP) стандартного стеку Інтернету.

Отже, кожного разу, коли клієнт (як правило, браузер) намагається відвідати шкідливу URL-адресу, клієнт може відображати проміжну сторінку попередження перед тим, як підозріла веб-сторінка насправді буде завантажена на пристрій користувача.

Спрощена архітектура ІС Google Safe Browsing виглядає так[9]: спеціалізовані боти Google аналізують дані по всім веб-ресурсам в інтернеті, як новостворених, так і існуючим довільний час. За допомогою алгоритмів на основі штучного інтелекту ідентифікуються шкідливі веб – ресурси та додаються в єдину базу Google Safe Browsing database. Клієнтські звернення для перевірки

веб-ресурсу отримують дані з останньої версії Gogle Safe Browsing database. На Рис. 1.1 зображена блок-схема алгоритму обробки запитів клієнта IC Google Safe Browsing:

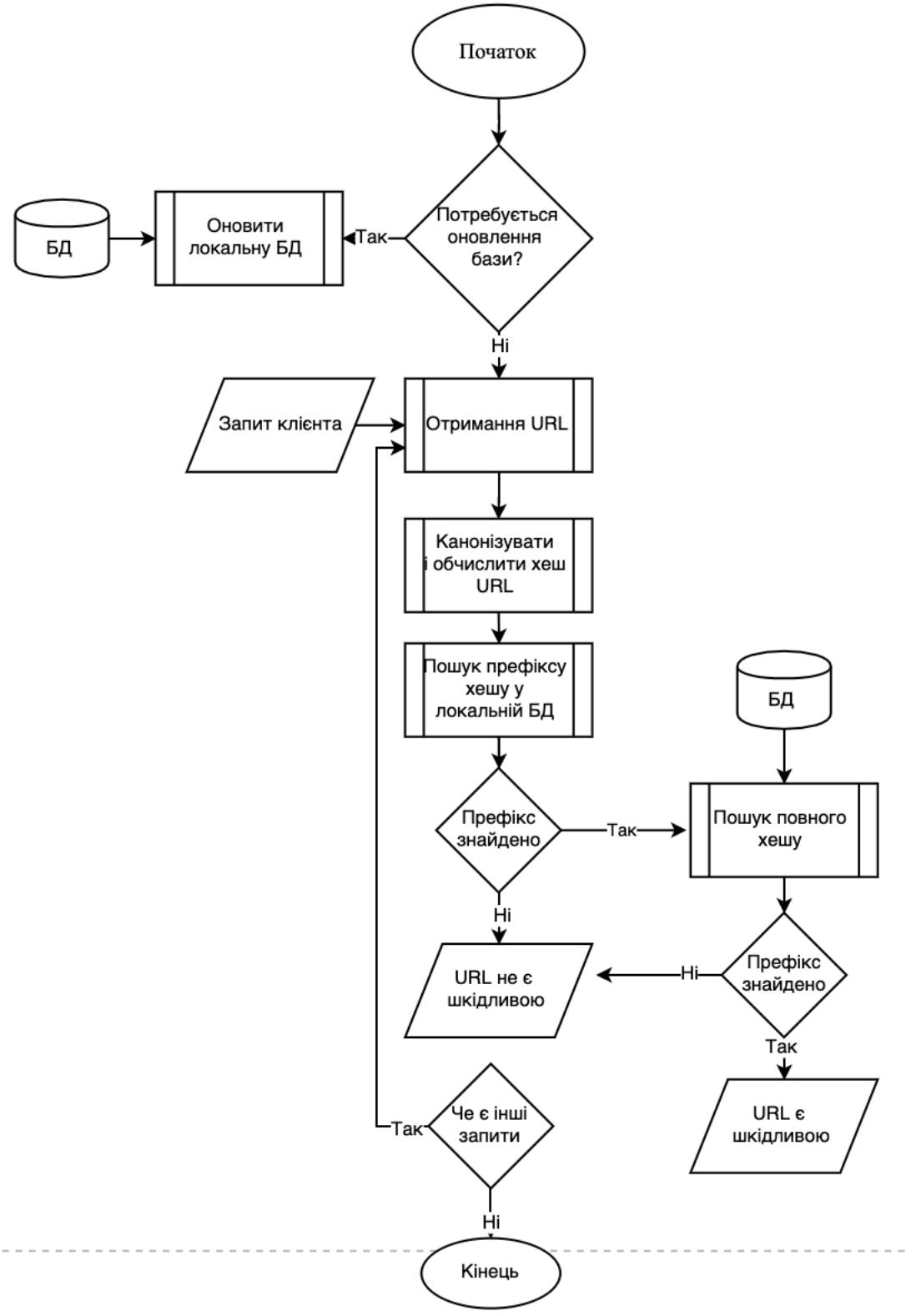

Рисунок 1.1 - блок-схема алгоритму обробки запитів клієнта IC Google Safe Browsing

Google спочатку обчислює в своїй базі даних хеш SHA256 кожної потенційно небезпечної URL-адреси та обрізає кожен хеш до 32-бітного префікса, щоб заощадити час та обчислювальну потужність на обробку запиту. Google надсилає базу даних усічених хешей до вашого браузера. Кожен раз, коли ви відвідуєте URL-адресу, ваш браузер хешує його і перевіряє, чи міститься його 32-бітний префікс у вашій локальній базі даних. Якщо префікс знайдений у локальній копії веб-переглядача, ваш веб-переглядач тепер надсилає префікс серверам Google, які доставляють назад список усіх повних 256-бітових хешів відповідних URL-адрес, щоб ваш браузер міг перевірити точність відповідності.

Як приклад, розглянемо випадок, коли при ідентифікації може знадобитися протестувати кілька під-адрес цільової URL-адреси. Це необхідно оскільки повна URL-адреса, можливо, не була включена до чорних списків. Розглянемо найбільш загальну URL-адресу HTTP форми http://a.b.c/1/2?param=1, a.b.c – це доменне ім’я, 1/2 - шлях до URL-адреси, ?param=1 - це запит. Потім, щоб перевірити, чи є зловмисна URL-адреса, клієнт спочатку здійснює канонізацію URL, а потім здійснює пошук наступних 8 декомпозицій у заданому порядку:

1. a.b.c /1/2?param=1
2. a.b.c /1/2
3. a.b.c /
4. a.b.c /1/
5. b.c/1/2ext?param = 1
6. b.c/1/2
7. b.c/
8. b.c/1/

Якщо будь-яка з перерахованих вище URL-адрес є в списках локальної бази даних, тоді попередньо URL-адреса вважається як підозріла, і повний хеш можна переслати на сервер Google для підтвердження.

З точки зору конфіденційності цей підхід є досить надійним, бо Google повинен вивчати лише 32-бітні хеші деяких запитів перегляду. Більше того,

усічені 32-бітні хеші не будуть точно розкривати ідентичність URL-адреси, до якої клієнт отримує доступ, оскільки коротка частина 256-бітного хешу не може буде ідентифікувати повний хеш URL-адреси, а значить і саму адресу. Проте у кожному з цих запитів сервери Google бачать IP-адресу клієнта, а також іншу ідентифікаційну інформацію, таку як стан бази даних. Також Google може випустити файл cookie у клієнтський веб-браузер під час деяких із цих запитів,[9] що є важливим аргументом проти твердження про абсолютну конфіденційність при користуванні ІС Google Safe Browsing.

Як сервіс Google safe browsing представлений у вигляді API[https://developers.google.com/safe-browsing/v4] та призначений лише для некомерційного використання. Якщо потрібно використовувати API для виявлення шкідливих URL-адрес для комерційних цілей - тобто “для продажу або для отримання прибутку" – Google пропонує Web Risk API.

Yandex Safe Browsing (YSB), що також надається у формі API [https://yandex.ru/dev/safebrowsing/], а також як захистна функція у браузері під назвою Yandex.Browser. YSB сумісний із C #, Python і PHP - це дослівна копія API Google Safe Browsing з тією лише різницею, що окрім списків шкідливих веб-сторінок, наданих Google, API YSB також включає 17 інших чорних списків. Кожен із цих списків містить шкідливі чи небезпечні веб-адреси певної категорії.

У таблиці 1.1 наведено назву та опис чорних списків із кількістю присутніх записів(префіксів)

Таблиця 1.1 – Приклад таблиці загроз Yandex Safe Browsing.

Назва списку	Тип загрози	Кількість записів
goog-malware-shavar	malware	283211
goog-mobile-only-malware-shavar	mobile malware	2107
goog-phish-shavar	phishing	31593
ydx-adult-shavar	adult website	434
ydx-adult-testing-shavar	test file	535
ydx-imgs-shavar	malicious image	0
ydx-malware-shavar	malware	283211
ydx-mitb-masks-shavar	man-in-the-browser	87
ydx-mobile-only-malware-shavar	malware	2107
ydx-phish-shavar	phishing	31593
ydx-porno-hosts-top-shavar	pornography	99990
ydx-sms-fraud-shavar sms	fraud	10609
ydx-test-shavar	test file	0
ydx-yellow-shavar	shocking content	209
ydx-yellow-testing-shavar	test file	370
ydx-badcrxids-digestvar	crx file ids	-
ydx-badbin-digestvar	malicious binary	-

Під час дослідження вмісту таблиці загроз Yandex Safe Browsing було визначено, що списки шкідливих веб-ресурсів у рішенні від Google safe browsing “goog-malware-shavar” та від Yandex Safe Browsing “ydx-malware-shavar” ідентичні. Те саме стосується і списків префіксів шкідливих веб-ресурсів, призначених для мобільних пристроїв. Це підтверджує факт того, що методи забезпечення безпеки інформаційних систем від фишігових атак від Yandex, а конкретно Yandex Safe Browsing не є суттєво відмінною від Google Safe Browsing розробкою, тож у даній роботі не буде приведений детальний алгоритм роботи методів, що були використані у Yandex Safe Browsing.

Google Safe Browsing може бути використаний в будь-яких ІС та має найбільшу клієнтську базу з забезпечення безпеки інформаційних систем від фішінгових атак. Можна припустити, що рішення Google Safe Browsing як ідентифікатора шкідливих веб-сайтів є найбільш ефективними, а завдяки безкоштовній моделі поширення цього сервісу та його інтеграції з веб-браузерами кількість користувачів Google Safe Browsing буде зростати. Також той факт, що автоматизовані методи пошуку та ідентифікації шкідливих веб-ресурсів не мають поширених аналогів, Google Safe Browsing. Це підтверджує, що для більшості рядових користувачів Інтернету Google Safe Browsing стане єдиним джерелом захисту від шкідливих веб-сайтів, що є частиною фішингових атак. Саме тому Google Safe Browsing стикається з дуже високими вимогами до точності і своєчасності у ідентифікації шкідливих ресурсів. В реальності, ці вимоги не могуть бути цілком виконані, що підтверджують деякі свідоцтв[18-19].

Також, системи, подібні Google Safe Browsing, що методично сканують усі доступні URL-адреси на предмет фішингових загроз чи інших ознак шкідливого програмного забезпечення, стикаються з багатьма новими проблемами, серед яких: системи розподілення трафику[20] та системи клоакінгу[21]. Маючи різні алгоритми фунціонування, системи розподілення трафіку та клоакінгу однаково

призначені для запобігання сканування шкідливих веб ресурсів системами забезпечення захисту, серед яких:

– ІС з забезпечення безпеки від фішінгових атак та шкідливого ПО;

– ІС з моніторингу прозорості рекламних кампаній(Facebook, Google Ads, тощо)

Ще одним сервісом, що реалізує метод ідентифікації шкідливих веб-ресурсів на основі спеціалізованих списків є веб-сайт спільноти PhishTank.com, що об’єднана проти фішингу, на якому кожен може подати підозрювані веб-сайти на перевірку до волонтерів, відстежувати стан підозрюваних веб-сайтів та допомагати перевірити інформацію від інших користувачів. PhishTank абсолютно безкоштовний у використанні та має відкрите API для доступу. Система ідентифікації веб сайтів як шкідливих відбувається за рахунок добровольців, що надсилають URL-адреси підозрюваних у фішингу сайтів і голосують, чи дійсно підозрюваний веб-ресурс є шкідливим. Ідея PhishTank полягає в тому, щоб об'єднати досвід та ентузіазм людей у мережі Інтернет для боротьби з фішинг-атаками. PhishTank є проектом компанії Cisco OpenDNS[12], яка є одним з найбільних постачальників антифішингових ІС.

На рисунку 1.2 можна побачити інтерфейс веб-сайту PhishTank.com, де користувачі мають можливість віддавати свій голос в захист підозрюваного веб-сайту або підтвердити його причетність до фішингової групи.

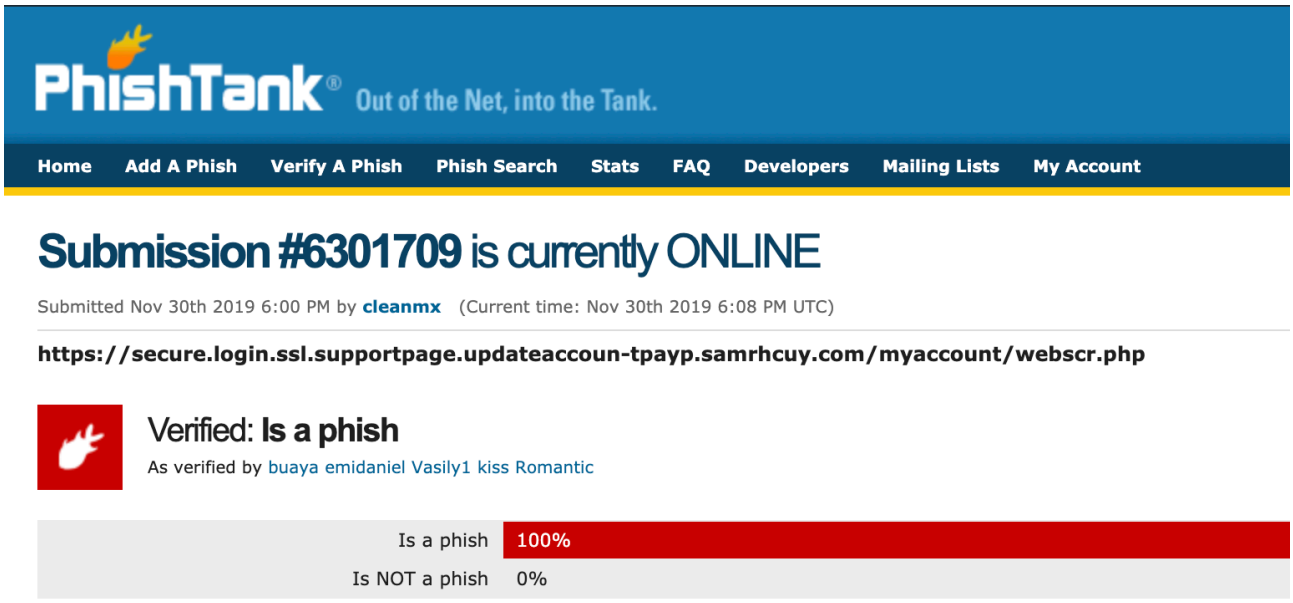

Рис. 1.2 – частково зображений інтерфейс веб-сайту PhishTank.com

Дійсно, спеціаліст з кібербезпеки зможе ідентифікувати фішинговий ресурс точніше ніж будь-який із існуючих автоматизованих методів з забезпечення безпеки інформаційних систем від фішінгових атак. Проте, за результатами аналізу записів[13] про подання та голосування користувачів PhishTank, виявляється що результати голосування не можуть бути однозначною мірою ідентифікації шкідливих веб-ресурсів. Хоча PhishTank має кілька тисяч зареєстрованих користувачів, невелике ядро з близько 25 модераторів виконувало основну частину роботи, віддаючи 74% голосів, які піддавались спостереженню. Це залишає PhishTank вразливим до маніпуляцій: якщо декілька найактивніших користувачів зупинять свою участь у голосуванні, може бути зібрана велика кількість неперевірених фішинг-сайтів. Це також означає, що зловмисник може приєднатися до системи та масово проголосувати. Оскільки 97% заявок на PhishTank перевіряються як фішинг-URL-адреси, зловмиснику буде легко створити репутацію, голосуючи випадковим чином багато разів, а потім розпорошити зловмисні голоси, захищаючи, наприклад, власні фішинг-сайти. Оскільки більше половини фішинг-сайтів у PhishTank - це дублікати популярних доменних імен, зловмисник може створити репутацію, голосуючи за

ці сайти, вносячи руйнуючий внесок у достовірність результатів діяльності PhishTank.

1.2.2 Аналіз методу ідентифікації фішингових електронних листів

За даними досліджень[14], більш як 80% фішингових атак поширюються через масову розсилку електронних листів. За цими ж результатами, аналіз яких був проведених у цій роботі, можна зробити висновок, що електронний лист, як спосіб доставки фішингових веб-ресурсів до жертви атаки, не втрачає актуальності й до сьогодні. Очевидно, успішно попереджена атака шляхом блокування фішигового листа ще на стадії його відправки або на стадії фільтрації отриманої електронної пошти може суттєво знизити шанси на успіх такої атаки. Саме тому на ринку представлені рішення від багатьох компаній, мета яких – не допустити користувача до шкідливого веб-ресурсу, блокуючи можливість відкрити фішинговий електронний лист та перейти по небезпечній URL-адресі або попереджуючи користувача про підозрілість електронного листа.

До існучих ІС, що використовують методи ідентифікації фішингових електронних листів належать: Cisco Advanced Phishing Protection[15], Office 365 Advanced Threat Protection[16] та інші.

Виділимо основні існуючі методи ідентифікації фішингових електронних листів на основі аналізу існуючих антифішингових інформаційних систем: евристичний метод, DMARC-автентифікація, метод оцінки надійності відправника та метод перевірки URL-адрес.

Евристичний метод[15] на основі машинного навчання. Цей метод побудований на аналізі проведених фішингових атак серед користувачів антифішингових ІС. Використання цього методу допомагає аналізувати електронні листи за багатьма параметрами, виділяючи характерні ознаки фішингових листів і перевіряючи всю отриману пошту за основі цих ознак.

Наявність методу зумовлено його ефективністю а також великою кількістю даних, що можуть буті використані як матеріал для навчання.

DMARC-автентифікація[17] (Domain-based Message Authentication Reporting and Conformance) - один з механізмів захисту компанії від фішингу з використанням імені її домену. Така проблема актуальна для будь-якого бренду, який працює з особистими даними користувачів і платіжними аккаунтами, найбільш часто вона стосується банків, платіжних систем, стільникових операторів, соціальних мереж, великих інтернет-магазинів. Листи маскуються під легальні розсилки, і важливу роль тут відіграє використання реального домену кампанії, від імені якої проводиться фішингова атака.

DMARC-автентифікація працює на основі протоколів автентифікації SPF(Sender Policy Framework) і DKIM(DomainKeys Identified Mail)[17] і перевіряє правильність проходження листом перевірок на SPF і DKIM, а також факт, що дані листи дійсно були відправлені з доменів під контролем організації. Ключові функції DMARC - перевірка автентифікації і відправка звітів. Що перевіряється:

– IP-адреса відправника електронного листа вказана в дозволених в запису SPF;

– перевірка DKIM має статус “pass” - тобто пройдена вдало.

За результатами перевірки оновлюється інформація в звітах: додаються дані про факт і результаті перевірки в агрегований звіт, який за замовчуванням відправляється раз на добу; у разі негативного спрацьовування (перевірка DMARC провалена) відправляється лист з повідомленням про провалену перевірку. Таке повідомлення отримується за будь-якої проваленої перевірки - тобто 1000 листів, які не пройшли перевірку, генерують тисячу відправок звіту на пошту користувача DMARC.

Метод оцінки надійності відправника. Такий метод забезпечення безпеки зазвичай встановлений на рівні поштового сервісу, але ІС з забезпечення системи поширюють його додатковими фільтрами. Перевірка надійності

відправника відбувається за десятками параметрів, але неможливо отримати точні дані з кожного із існуючих параметрів через політику недоступності такої інформації. Серед відомих складових методу оцінки надійності відправника є:

– наявність IP-адреси або домену в чорних списках, наприклад SpamHaus[spamhaus.org];

– скарги на спам від отримувачів;

– число неіснуючих адрес, на які було відправлено листи і наявність спам-пасток в базі;

– частка листів, які видалили без прочитання;

– регулярність розсилок;

– програмне забезпечення, за допомогою яких відправлена розсилка;

– складова листів і посилання в тексті;

– відсоток відкриття і переходів за посиланнями;

– число відповідей на листи і пересилань повідомлень.

Метод перевірки URL-адрес в момент вибору посилання (наприклад, в електронних повідомленнях і файлах). Посилання перевіряються під час кожної спроби переходу. Безпечні посилання залишаються доступними, а шкідливі динамічно блокуються. Дані про URL-адреси в цьому методі отримуються від ІС з забезпечення безпеки, наприклад, Google Safe Browsing та PhishTank API.

У цій роботі були проаналізовані лише основні методи ідентифікації фішингових електронних листів. За статистичними даними[7-11], щорічно методи з ідентифікації спам-листів забезпечують все більш ефективний захист для користувача, і об’єм отриманих небезпечних електонних листів знижується. Проте, за даними досліджень компанії Avanan [18], у 2019 році 25% фішингових листів були допущені стандартним захистом ІС Office 365 до отримання користувачем. Office 365 є одним із найбільш поширених почтових клієнтів у світі. Також будо досліджено, що успіх фішингових атак зумовлений використанням різних форма вразливості ІС з забезпечення безпеки, в особливості популярним серед організаторів фішинг-атак є метод обфускації

html-коду листів та веб-сайтів. Наприклад, Хакери приховують URL-адресу, роблячи її неможливою для ідентифікації системою безпеки Office 365

За допомогою цієї стратегії, хакери можуть використовувати навіть URL-адреси, які, згідно з даними Google Safe Browsing та ін., знаходяться в списках небезпечних веб-ресурсів, тому що системоа безпеки Office 365 не розпізнає форму цієї URL-адреси.

Приклад необфускованого HTML-коду:

```
<a href="https://malware.com">Link</a>
```

Приклад обфускованого HTML-коду:

```
<a href="https://malw&#8204are.&#8204com">Link</a>
```

1.2.3 Аналіз методу рейтингового оцінювання веб-сайту

Метод рейтингової оцінки безпечності веб-сайту для забезпечення забезпечення безпеки інформаційних систем від фішінгових атак широко використовується у рішеннях від таких постачальників ІС, як Netcraft[https://toolbar.netcraft.com], Sucuri, Scamadviser та ін. Аналіз веб-сайту здійснюється за багатьма показниками, серед яких:

– дата створення веб-сайту(реєстрації доменного імені);

– наявність та рівень SSL-сертифікату;

– аналіз рейтингу хостинг-провайдера веб-сайту;

– аналіз рейтингу доменного регістратора веб-сайту;

– пошук URL-адреси веб-сайту у відомих списках небезпечних ресурсів;

– аналіз подібності текстового вмісту та ключових слів аналізованого веб-сайту до довірених веб-ресурсів, що найчастіше підроблюються.

Проте, відкрита інформація про методи рейтингової оцінки безпечності веб-сайту дає організаторам фішинг-атак можливість підготувати шкідливі веб-ресурси таким чином, щоб відповідати вимогам, що аналізуються ІС з оцінки безпечності веб-ресурсів. При спеціальній підготовці веб-сайту, метод рейтингового оцінювання буде неефективно оцінювати реальну ступінь загрози.

1.3 Обґрунтування мети рішення поставленої проблеми та постановка задачі дослідження

У результаті аналізу існуючих методів з забезпечення безпеки інформаційних систем від фішінгових атак була виявлена необхідність у вдосконаленні існуючих методів, а саме методу рейтингової оцінки безпечності веб-сайту.

Необхідність вдосконалення методу рейтингової оцінки безпечності веб-сайту обгрунтована тим, що ефективність методів ідентифікації фішингових електронних листів та ідентифікації шкідливих веб-ресурсів на основі спеціалізованих списків, не є абсолютною. Дослідження Університету Іллінойса за 2018 рік[26] виявило, що тільки 8.4% активних фішингових веб-сайтів були ідентифіковані як шкідливі більш як 70 ІС з забезпечення безпеки від фішингових атак. У 91.5% випадків фішингові веб-сайти не були включені у жоднен із 70 списків фішингових ресурсів та могли бути використані у фішингових атаках. Необхідно допускати можливість незахищеного доступу користувача до фішингового веб-сайту та розробити вдосконалений метод рейтингового оцінювання веб-сайту, що зможе запобігти втраті конфіденційної інформації шляхом попередження користувача, заснованого на результаті обчислення рейтингової оцінки веб-сайту.

Для досягнення поставленої мети наукової роботи, необхідно виконати:

– дослідження існуючих методів забезпечення захисту ІС від фішингових атак;

– обґрунтувати мету вдосконалення методу рейтингової оцінки безпечності веб-сайту;

– сформувати вимоги до запропонованого вдосконаленого методу рейтингового оцінювання веб-сайту;

– проаналізувати ефективність нового вдосконаленого методу рейтингового оцінювання веб-сайту;

– визначити область використання вдосконаленого методу рейтингового оцінювання веб-сайту;

– оцінити вдосконалений метод на контрольних прикладах для демонстрації результатів його ефективності;

– збір даних на основі відкритої інформації про активні фішингові веб-сайти для виділення характерних ознак фішингового веб-сайту.

2 РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ У РАМКАХ НАУКОВОЇ РОБОТИ

У результаті досліджень існуючих методів забезпечення безпеки ІС від фішингових атак, на їх основі був вдосконалений метод рейтингового оцінювання веб-сайту.

Оскільки 100% ефективне попередження доступу до шкідливих ресурсів не може бути надано жодним з існуючих ІС з забезпечення безпеки[22], у рамках даної магістерської атестаційної роботи пропонується вдосконалений метод рейтингової оцінки безпечності веб-сайту.

2.1 Формування проблем та вимог до вдосконаленого методу рейтингового оцінювання веб-сайту

Застосування вдосконаленого методу має вирішити ряд проблем, яких зазнають існуючі методи з забезпечення безпеки ІС від фішингових атак. Серед проблем:

– спотворення результатів сканування вмісту потенційно небезпечних сторінок веб-сайтів, використовуючи технології розподілення трафіку(TDS);

– запобігання об’єктивному рейтинговому оцінюванню веб-сайту за рахунок вразливих до підлаштування параметрів оцінювання;

– ігнорування особливо явних параметрів, що характерні для фішингових веб-сайтів.

При розробці вдосконаленого методу рейтингового оцінювання веб-сайту до методу були сформовані таки вимоги:

– можливість паралельного функціонування з існуючими методами забезпечення безпеки ІС від фішингових атак;

– рейтингова оцінка має бути обчислена до завантаження веб-сторінки браузером користувача;

– попередження користувача про небезпечність веб-сайту має відбуватися без хибних спрацьовувань або прагнути до мінімальної їх кількості;

– точність оцінки під час аналізу потенційно фішингових веб-сайтів має прагнути до максимальної;

2.1 Розробка вдосконаленого методу рейтингового оцінювання веб-сайту.

Новий вдосконалений метод рейтингового оцінювання веб-сайту розроблений на основі існуючого однойменного методу та пропонується як доповнення до всіх існуючих методів з забезпечення безпеки ІС від фішингових атак. На основі дослідження відкритих матеріалів з сайту Phishtank.com, було отримано достатньо контрольних прикладів фішингових веб-сайтів для виділення найбільш точних параметрів, що притаманні типовому злоякісному веб-сайту.

Вдосконалений метод рейтингового оцінювання веб-сайту представлений такими етапами:

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.

Вибір таких параметрів для аналізу, як дата реєстрації доменного імені веб-сайту, врахування кількість рівнів доменного імені, наявність форм вводу та відправки даних, належність веб-сайту до 10000 найбільш відвідуваних веб-сайтів має вирішити дві виявлені раніше проблеми. Проблеми запобігання об’єктивному рейтинговому оцінюванню веб-сайту за рахунок вразливих до підлаштування параметрів оцінювання та ігнорування особливо явних параметрів, що характерні для фішингових веб-сайтів залишаються актуальними через застарілі методи рейтингового оцінювання або ж через їх віднустість. Наприклад Netcraft[21], що реалізує метод рейтингової оцінки веб-сайту, досить вагомо оцінює наявність SSL-сертифікату, який можна з легкістю отримати анонімно та безкоштовно[https://www.ssls.com/]. Через надлишкову кількість параметрів що оцінюються та недостатньо вагому оцінку найбільш характерних для фішингових веб-сайтів ознак, рейтингова оцінка може бути недостатньо точною та не попередити користувача від втрати конфіденційної інформації.

На даному етапі методу необхідно обчислити такі коефіцієнти, що засновані 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:

$$\text{Якщо } 0 \ \geq l \leq \ 2, \text{ то } z = 0 \ , (4)$$

$$\text{Якщо } 3 \ > l \leq \ 3, \text{ то } z = 1 \ , (5)$$

$$\text{Якщо } 3 > l \leq \ 127, \text{ то } z = 2 \ , (6)$$

Де l – кількість рівнів доменного імені веб-сайту. Може приймати значення у діапазоні $l \in [0; 127]$. Приклад веб-сайту з другим рівнем доменного імені виглядає так: “wikipedia.org”, де перший рівень – це доменна зона “.org”. Приклад веб-сайту з третім рівнем доменного імені виглядає так: “sign-in.securing-user-support.com”; якщо один з рівнів доменного ім’я має значення “www”, такий рівень не враховується у підрахунку кількість рівнів доменного імені l;

p- коефіцієнт наявності форм вводу та відправки даних,

$$p \in [0; 1] \text{ , (7)}$$

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 за даними Similarweb[https://www.similarweb.com/top-websites],

$$f \in [0; 1] \text{ , (8)}$$

За наявності веб-сайту у списку 10000 найбільш відвідуваних, f приймає значення 1, за відсутності – fприймає значення 0.

Етап 2 - ідентифікація ознак систем розподілення трафіку на веб-сайті

Також, для рішення проблеми спотворення результатів сканування вмісту потенційно небезпечних сторінок веб-сайтів, використовуючи технології систем розподілення трафіку був запропонований метод ідентифікації ознак використання цих технологій. Сам факт використання подібних технологій веб-сайтом є достатнім приводом для підвищення уваги до веб-сайту, а також включення факту наявності цих технологій у підсумкову рейтингову оцінку веб-сайту. Це пов’язано з тим, що найбільш поширений і ефективний метод ідентифікації шкідливих веб-сайтів на основі спеціалізованих списків не зможе

своєчасно або взагалі ідентифікувати потенційно фішинговий веб-сайт та за необхідністю внести його до списку небезпечних веб-сайтів, а внаслідок, не зможе попередити користувача від відвідування такого сайту.

На етапі ідентифікації ознак клоакінгу та систем розподілення трафіку виконуються паралельні HTTP-запити на URL-адресу веб-сайту, що аналізується.

Запит зі сторони клієнта означає, що HTTP-запити виконується на стороні користувача, наприклад, через інтерфейс його веб-браузеру, з його IP-адреси. Під час запиту зі сторони користувача ми майже повністю гарантуємо ідентифікацію клієнтського підключення як не бота, та отримуємо і фіксуємо цільову та потенційно небезпечну версію веб-сторінки.

Запит зі сторони сервера означає HTTP-запити на стороні сервера, що має ідентифікувати себе як автоматизований робот(бот) для аналізу вмісту сторінок на наявність ознак шкідливого веб сайту. Це є частиною реалізації методу ідентифікації шкідливих веб-сайтів на основі спеціалізованих списків. Цього можна досягти, наприклад, якщо у складі заголовку HTTP-запиту на веб-сайт у параметр “UserAgent” підставити значення:

```
Mozilla/5.0(compatible;Googlebot/2.1;+http://www.google.com/bot.html),
```

що є найбільш характерним ідентифікатором HTTP-запитів ботів, що аналізують веб-сайти у складі ІС з забезпечення безпеки Google Safe Browsing.[24] Це необхідно для того, щоб спровокувати потенційно наявні системи клоакінгу та розподілення трафіку на ідентифікацію серверного підключення як бота, та зафіксувати поведінку веб-сайту і вміст отриманої веб-сторінки. Отже, зміст HTTP-запитів зі сторони клієнта та сторони сервера має бути ідентичним, за виключенням значення параметру “UserAgent” у складі

заголовку HTTP-запиту. Клієнт має надавати серверу копію HTTP-запиту, який відправляє на URL-адресу веб-сайту, що аналізується.

Етап ідентифікації ознак систем розподілення трафіку на веб-сайті реалізується у такому порядку:

А). 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[25]

Б). Аналіз поведінки веб-сайту під час HTTP-запиту та отримання вмісту цієї веб-сторінки на стороні сервера.

В). Порівняння результатів аналізу поведінки веб-сайту між зафіксованими результатами зі сторони клієнта та сервера. Якщо переадресовування під час отримання HTTP-відповіді від веб-сайту, що аналізується були ідентифіковані, перевірка кінцевих веб-адрес здійснюється після закінчення процесу переадресовування.

$A_{\text{клієнта}}$ - 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.

В рамках цього етапу, при порівнянні відповіді сайту HTTP Status Codes з боку клієнта та сервера, мають бути ідентичними. Наприклад, статус HTTP Status 200, що умовно означає “успіх” на стороні клієнта та статус HTTP Status 404, що умовно означає “не знайдено” не є ідентичними.

t - коефіцієнт ідентифікації ознак використання технологій клоакінгу та систем розподілення трафіку,

$$t \in [0; 1]$$

t 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 $t = 1$;

За наявності ознак використання систем розподілення трафіку, t приймає значення 1, за відсутності – t приймає значення 0.

При значенні $t = 0$

При значенні $t = 1$

Етап 3 - обчислення рейтингу та ступеню загрози веб-сайту

Вдосконалений метод рейтингової оцінки передбачає обчислення рейтингової оцінки веб-сайту. Формула розрахунку рейтингу:

$$W_{\text{сайту}} = \left(25 * \frac{1}{m}\right) + (2.5 * 2^z * z) + 15 * p + 15 * f + 25 * t \ , \ (1)$$

Де:

$W_{\text{сайту}}$ – підсумковий рейтинг веб-сайту. При отриманні нецілого результату застосовується математичне округлення до найближчого цілого ;

$$0 \geq W_{\text{сайту}} \leq 100, (2)$$

m – коефіцієнт часу з моменту реєстрації доменного імені,

$$m \in [1; \infty) \ ,$$

z – коефіцієнт кількості рівнів доменного імені,

$$z \in [0; 2] \ ,$$

p- коефіцієнт наявності форм вводу та відправки даних,

$$p \in [0; 1] \ ,$$

f- коефіцієнт наявності веб-сайту у списку 10000 найбільш відвідуваних сайтів за даними Similarweb,

$$f \in [0; 1] \ ,$$

t - коефіцієнт ідентифікації ознак використання технологій клоакінгу та систем розподілення трафіку,

$$t \in [0; 1] \ , (9)$$

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.

2.2 Алгоритм нового вдосконаленого методу рейтингового оцінювання веб-сайтів

Алгоритм реалізації нового вдосконаленого методу рейтингового оцінювання веб-сайту зображений на Рисунках 2.1, 2.2, 2.3. Приведений алгоритм дозволяє реалізувати відповідні етапи розробленого методу рейтингового оцінювання веб-сайтів

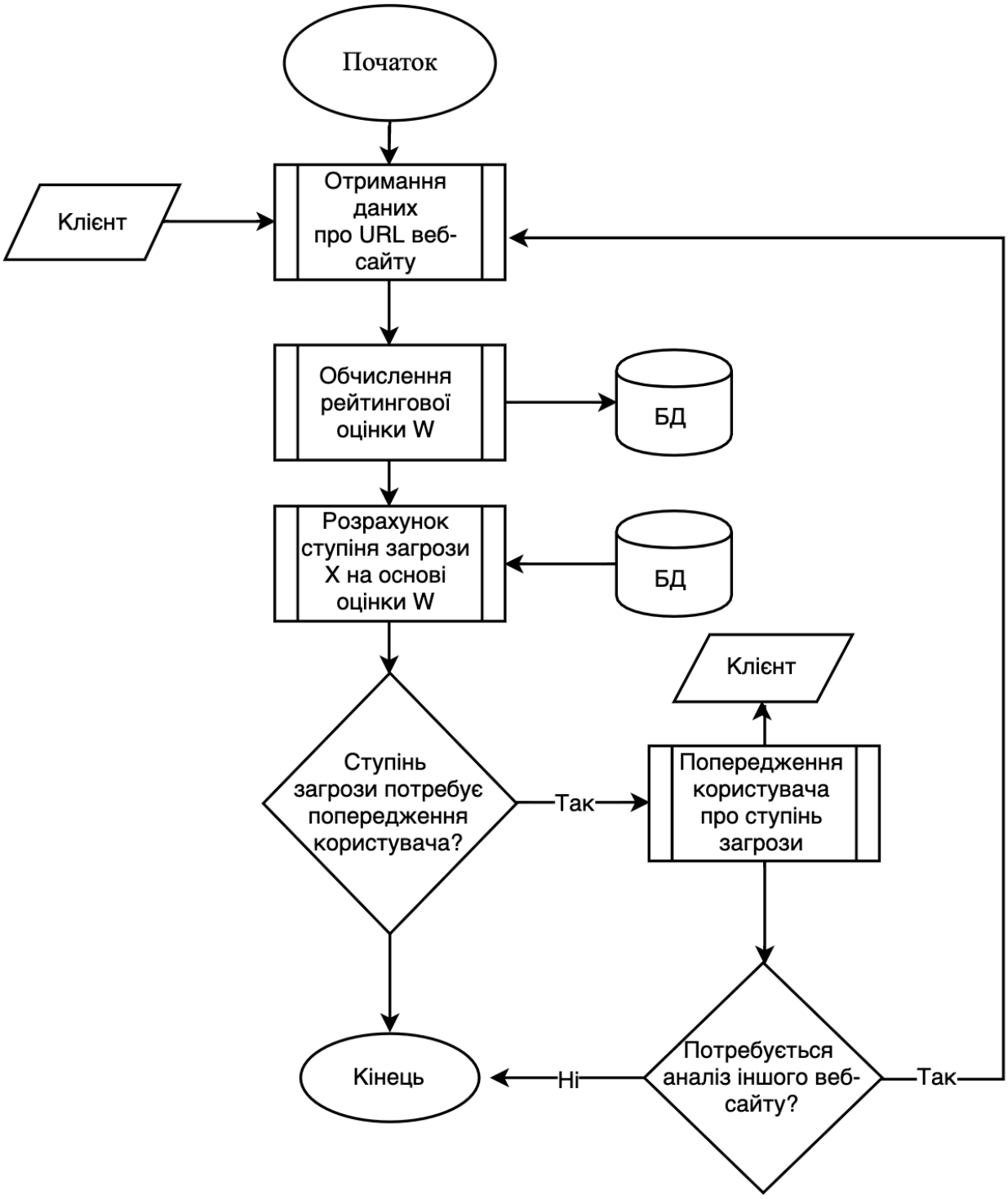

Рисунок 2.1 – Базовий алгоритм нового методу забезпечення безпеки користувачів веб-сайтів

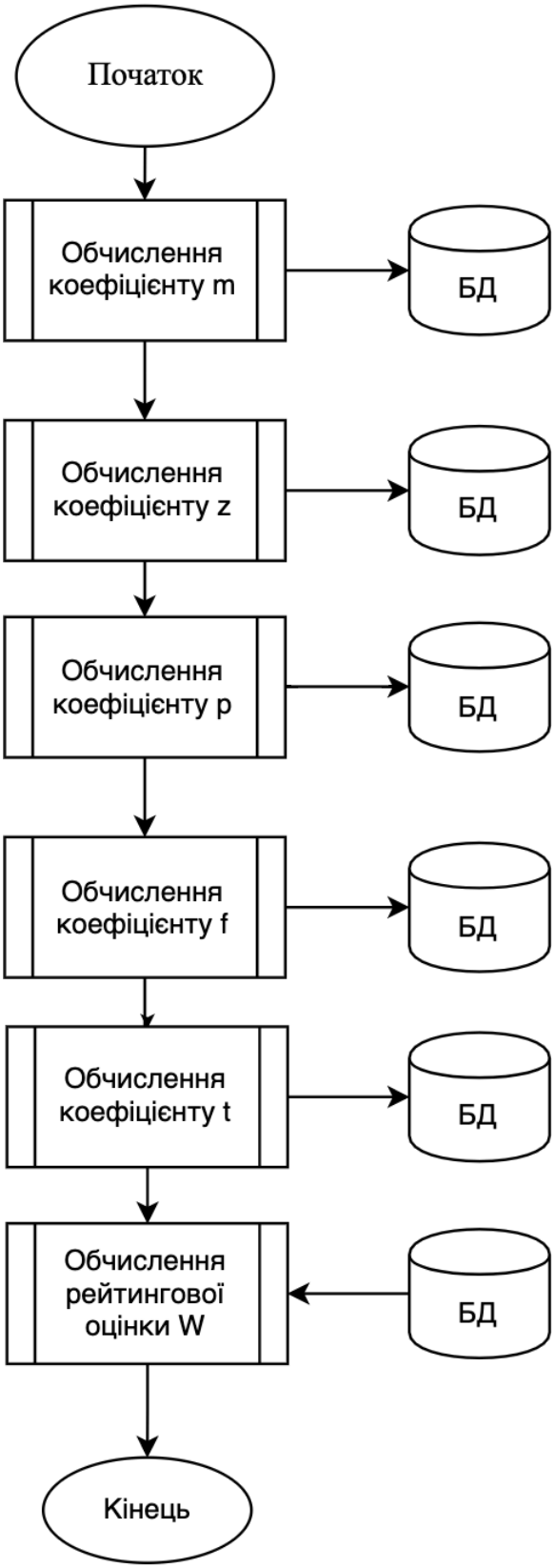

Рисунок 2.2 – Деталізація алгоритму обчислення рейтингової оцінки $W_{\text{сайту}}$

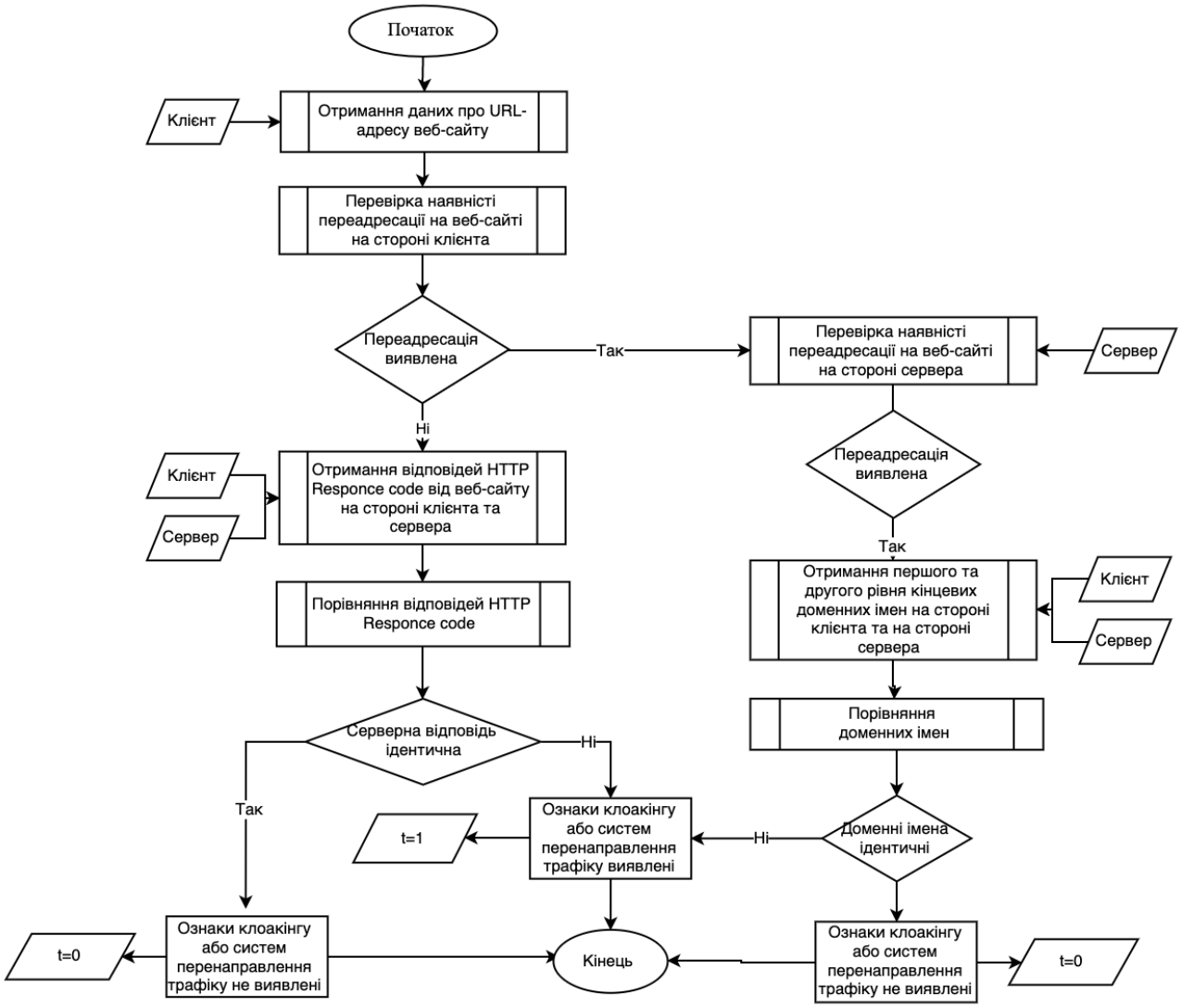

Рисунок 2.3 – Деталізація алгоритму обчислення коефіцієнту ідентифікації ознак використання систем розподілення трафіку t

3 ДОСЛІДЖЕННЯ ОТРИМАНИХ НАУКОВИХ РЕЗУЛЬТАТІВ

Новий вдосконалений метод рейтингового оцінювання веб-сайту, що був запропонований на основі результатів досліджень у рамках наукової роботи може бути досліджений на основі контрольних прикладів діючих фішингових сайтів. Результати дослідження будуть представлені та оцінені у цьому розділі.

3.1 Методика проведення досліджень нового методу рейтингового оцінювання веб-сайту

Найбільш коректні результати дослідження можна отримати, якщо застосувати новий вдосконалений метод рейтингового оцінювання на діючих фішигнових веб-сайтах, достовірний список яких можна отримати з веб-сайту phishtank.com[12]. Планується використовувати метод тільки на тих фішингових сайтах, що були визнані спільнотою як однозначно фішингові та мають статус “Is a Phish”. Для достовірності результатів дослідження до аналізу будуть взяті 10 фішингових веб-сайтів, що були додані до списку phishtank за останні 24 години. Ті фішингові веб-сайти, що не відправляють http-відповідь, тобто, не є онлайн, взяті до аналізу не будуть. Для демонстрації ступеню помилкових оцінювань ступню небезпечності веб-сайту до аналізу додатково будуть взяти 5 доменів, що гарантовано не є фішинговими.

Новий вдосконалений метод рейтингового оцінювання веб-сайту необхідно порівняти з існуючими методами забезпечення ІС від фішингових атак. Оскільки отримати доступ до великої кількості фішингових електронних листів у рамках даного дослідження не є можливим, результати нового методу будуть порівняні з існуючим методом ідентифікації шкідливих веб-ресурсів на основі спеціалізованих списків та існуючим методом рейтингової оцінки

шкідливих ресурсів. Фішингові веб-сайти будуть проаналізовані ІС що реалізували вищеназвані методи відповідно, а саме Google Safe Browsing[https://developers.google.com/safe-browsing/v4] та Netcraft Google Chrome extention[https://toolbar.netcraft.com].

Результати аналізу фішингового веб-сайту ІС Google Safe Browsing будуть представлені у формі наявності чи відсутності фішингового домену у списках небезпечних веб-ресурсів, що означає наявність чи відсутність попередження користувача про відвідування небезпечного веб-сайту.

Результати аналізу фішингового веб-сайту ІС Netcraft Google Chrome extention будуть представлені у формі обчисленої рейтингової оцінки (0-10) фішингового домену та факту наявності чи відсутності попередження користувача про відвідування небезпечного веб-сайту. Максимальне значення рейтингової оцінки дорівнює 10, що означає найбільшу загрозу від веб-сайту, що аналізується. Мінімальне значення рейтингової оцінки дорівнює 0, що означає відсутність загрози.

Результати аналізу фішингового веб-сайту новим вдосконаленим методом рейтингової оцінки будуть представлені у формі обчисленої рейтинової оцінки (0-100) фішингового домену та формі попередження користувача про про відвідування небезпечного веб-сайту чи відсутність цього попередження.

3.2 Опис експерименту із використанням нового методу рейтингового оцінювання веб-сайтів

Для дослідження результатів використання нового вдосконаленого методу рейтингового оцінювання на основі аналізу 15 контрольних прикладів веб-сайтів була представлена Таблиця 3.1, де було розраховано $W_{\text{сайту}}$ – підсумковий рейтинг веб-сайту та ступінь загрози x.

У Таблиці 3.2 представлені результати порівняння нового вдосконаленого методу з реалізованими існуючими методами забезпечення безпеки ІС від фішингових атак.

Таблиця 3.1 – 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 $W_{\text{сайту}}$
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 3.1 – 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 3.2 – 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 3.2 – 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)

$W_{\text{сайту}}$ було розраховано за формулою:

$$W_{\text{сайту}} = \left(25 * \frac{1}{m}\right) + (2.5 * 2^z * z) + 15 * p + 15 * f + 25 * t$$

m – коефіцієнт часу з моменту реєстрації доменного імені.

z – коефіцієнт кількості рівнів доменного імені,

p- коефіцієнт наявності форм вводу та відправки даних,

f- коефіцієнт наявності веб-сайту у списку 10000 найбільш відвідуваних сайтів за даними Similarweb.com,

t - коефіцієнт ідентифікації ознак використання систем розподілення трафіку.

Кожен із коефіцієнтів має множник, що відповідає вазі даного коефіцієнту. Множник виведений на основі дослідження результатів використання нового вдосконаленого методу рейтингового оцінювання на основі аналізу 15 контрольних прикладів веб-сайтів.

Ступінь загрози x визначається на основі значення $W_{\text{сайту}}$ за такими правилами:

якщо $0 \geq W_{\text{сайту}} < 30$, то $x = 0$,

якщо $30 \geq W_{\text{сайту}} < 50$, то $x = 1$,

якщо $50 \geq W_{\text{сайту}} \leq 100$, то $x = 2$.

Значення $x = 1$ та то $x = 2$ означає середню(підозрілий) та високу(небезпечний) загрозу відповідно, та метод передбачає сповіщення користувача. Значення $x = 0$ означає, що загроза не була знайдена(безпечний) і не передбачає сповіщення користувача.

Правила, що визначають ступінь загрози x були виведені на основі дослідження результатів використання нового вдосконаленого методу рейтингового оцінювання на основі аналізу 15 контрольних прикладів веб-сайтів.

Аналізуючи результати експерименту, потрібно виділити такі результати:

Метод ідентифікації шкідливих веб-ресурсів на основі спеціалізованих списків, реалізований IC Google Safe Browsing, виявився ефективним та міг попередити користувача від відвідування фішингових сайтів тільки у 50% випадків. Це демонструє низьку ефективність методу, що має найбільшу клієнтську базу у світі.

Існуючий метод рейтингової оцінки веб-сайтів, реалізований IC Netcraft Chrome extention, видавав рейтингову оцінку дійсно фішингових веб-сайтів досить точно, та лише в 10% випадків оцінив фішинговий веб-сайт як цілком безпечний, розрахувавши рейтингову оцінку як 1/10. Але, не дивлячись на високу точність в оцінюванні, попередження користувача не було здійснене у 30% випадків. На Рисунку 3.1 зображено приклад попередження користувача IC Netcraft Chrome extention.

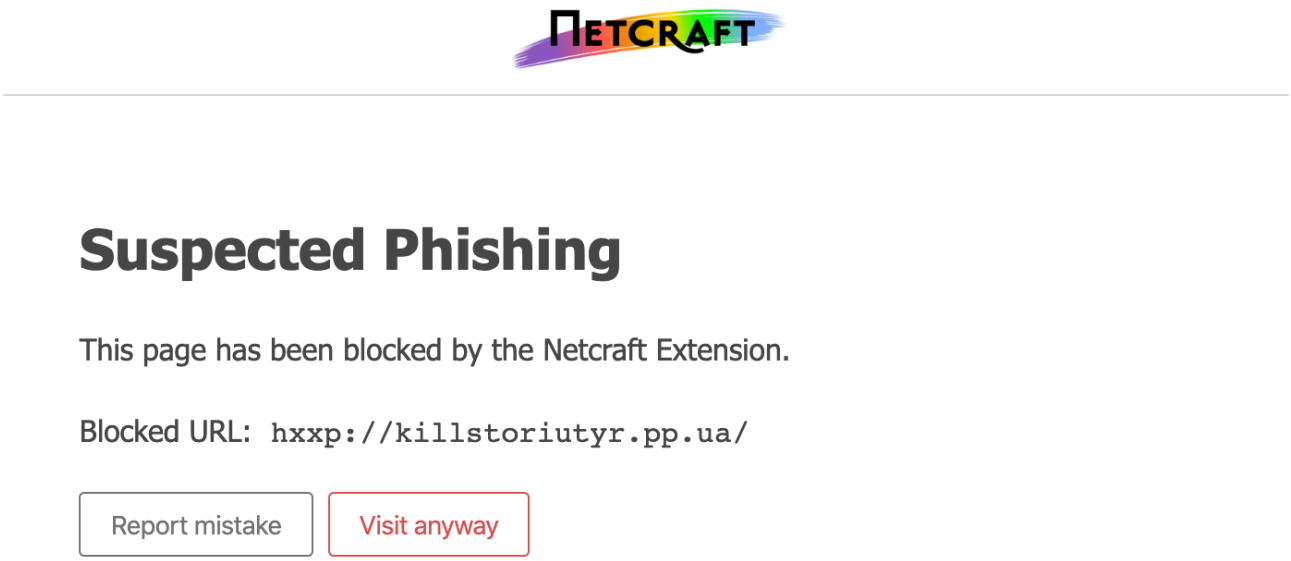

Рисунок 3.1 – приклад попередження користувача IC Netcraft Chrome extention.

Новий вдосконалений метод рейтингової оцінки веб-сайтів показав високу точність в виявлені фішингових веб-сайтів. Усі 10 контрольних прикладах фішингових веб-сайтів були оцінені коректно, потенційно попередивши користувача про відвідування цих небезпечних веб-сайтів.

Також, усі порівнювані методи не показали хибних попереджень на контрольній групі з 5 не фішингових веб-сайтів.

Рівень загрози був поділений на 3 рівні, щоб врегулювати ступінь попередження користувача, та зменшити вірогідність хибного присвоєння рівню безпеки 2(небезпечно) насправді безпечному веб-сайту.

Новий метод може бути покращений шляхом додавання більш точних та характерних для фішингових веб-сайтів ознак для аналізу, а також шляхом розробки нових етапів з ідентифікації типових ознак фішингових сайтів. Наприклад, впровадження етапу ідентифікації ознак клоакінгу на веб-сайті дозволить ще точніше формувати рейтингову оцінку, та знизити вірогідність допущення користувача до потенційно небезпечного веб-сайту без попередження.

3.3 Аналіз області використання отриманих результатів

На основі дослідження отриманих наукових результатів даної наукової магістерської роботи, а саме на підставі результатів експерименту з порівняння нового вдосконаленого методу рейтингового оцінювання веб-сайтів та існуючих методів з забезпечення безпеки ІС від фішингових атак, можна припустити, що новий вдосконалений метод може стати ефективним доповненням існуючих методів та знайде широку область застосування.

Серед можливих областей застосування нового методу рейтингового аналізу веб-сайтів:

- клієнт-орієнтовані ІС з ідентифікації фішингових веб-сайтів, які можуть бути представлені комплексними антивірусними ІС;

- клієнт-орієнтовані ІС з рейтингового оцінювання веб-сайтів, які можуть бути представлені як встановлювані додатки до веб-браузерів.

4 ПРАКТИЧНЕ ВИКОРИСТАННЯ РЕЗУЛЬТАТІВ ДОСЛІДЖЕНЬ

Для демонстрації впровадження нового вдосконаленого методу рейтингового оцінювання веб-сайту, було розроблене програмне забезпечення, що призначене для автоматизації усіх етапів використання методу.

Задля впровадження нового методу рейтингового аналізу веб-сайтів та можливості його практичного використання було розроблене програмне забезпечення, що дозволяє використовувати новий метод в автоматичному режимі. Розроблене програмне забезпечення є додатком до браузеру Google Chrome[26]. Вибір такої форми реалізації обумовлений метою впровадження нового вдосконаленого методу - доповнення та підвищення ефективності існуючих методів забезпечення безпеки інформаційних систем від фішінгових атак.

ІС Google Safe Browsing поширюється в останніх версіях Google Chrome безкоштовно та ввімкнена за замовчуванням, а існуючий додаток до Google Chrome, що реалізує існуючий метод рейтингового аналізу веб-сайтів – Netcraft Chrome extention може співіснувати з іншим додатком. Саме тому обрана форма реалізації нового методу у вигляді додатку до веб-браузера, що дозволить доповнювати існуючі методи забезпечення безпеки ІС від фішингових атак.

4.1 Опис програмного забезпечення для впровадження нового методу рейтингового аналізу веб-сайтів

Додаток реалізований на мові Javascript, що є основною мовою для розробки дотатків для Google Chrome[26]. Була обрана IDE JetBrains Webstorm як найбільш доречна при розробці на мові javascript.

Збереження та опрацювання даних – для додатку обраний файловий формат виді JSON, адже оптимізований для роботи з невеликими об’ємами даних він є більш ефективним ніж, наприклад XML або СУБД MySQL[27].

Платформи, на яких розроблений додаток до Google Chrome може функціонувати, обмежені такими найменуваннями: Microsoft Windows 7(або підзніше), macOS 10.10(або піздніше), ОС Linux. Проте, цього вибору більш ніж достатньо.

4.2 Опис розробленого додатку

Розроблене програмне забезпечення являє собою додаток для автоматизованого рейтингового оцінювання відвіданих користувачем веб-сайтів, що є реалізацією нового вдосконаленого рейтингового оцінювання веб-сайту.

Робота з додатком потребує запуску браузера Google Chrome та наявності додатка у списку встановлених та функціонуючих додатків Chrome.

Рейтингове оцінювання веб-сайту виконується автоматично при відвідуванні користувачем будь-якого веб-сайту. Оскільки реалізація методу передбачає сповіщення користувача при рівнях небезпеки $x = 1$ та $x = 2$ що означає “підозрілий” та “небезпечний” відповідно, ці вимоги були взяті до уваги при розробці інтерфейсу користувача.

Ідентифікація систем розподілення трафіку реалізована прямо у додатку і не потребує окремого сервера для симуляції підключень від пошукових роботів. Це було досягнуто шляхом паралельного HTTP-запиту зі спеціальним параметром User Agent, що детально описано у розділі 2.1 даної магістерської наукової роботи.

Інформація про параметри що необхідні для аналізу веб-сайту новим методом автоматизовано отримуються із відкритих джерел. Наприклад інформація щодо віку доменного імені за дати реєстрації або поновлення отримується з API за веб-адресою [https://www.whoisxmlapi.com/whois-api-doc.php] у форматі JSON.

Інтерфейс додатку представлений на Рисунках 4.1, 4.2, 4.3:

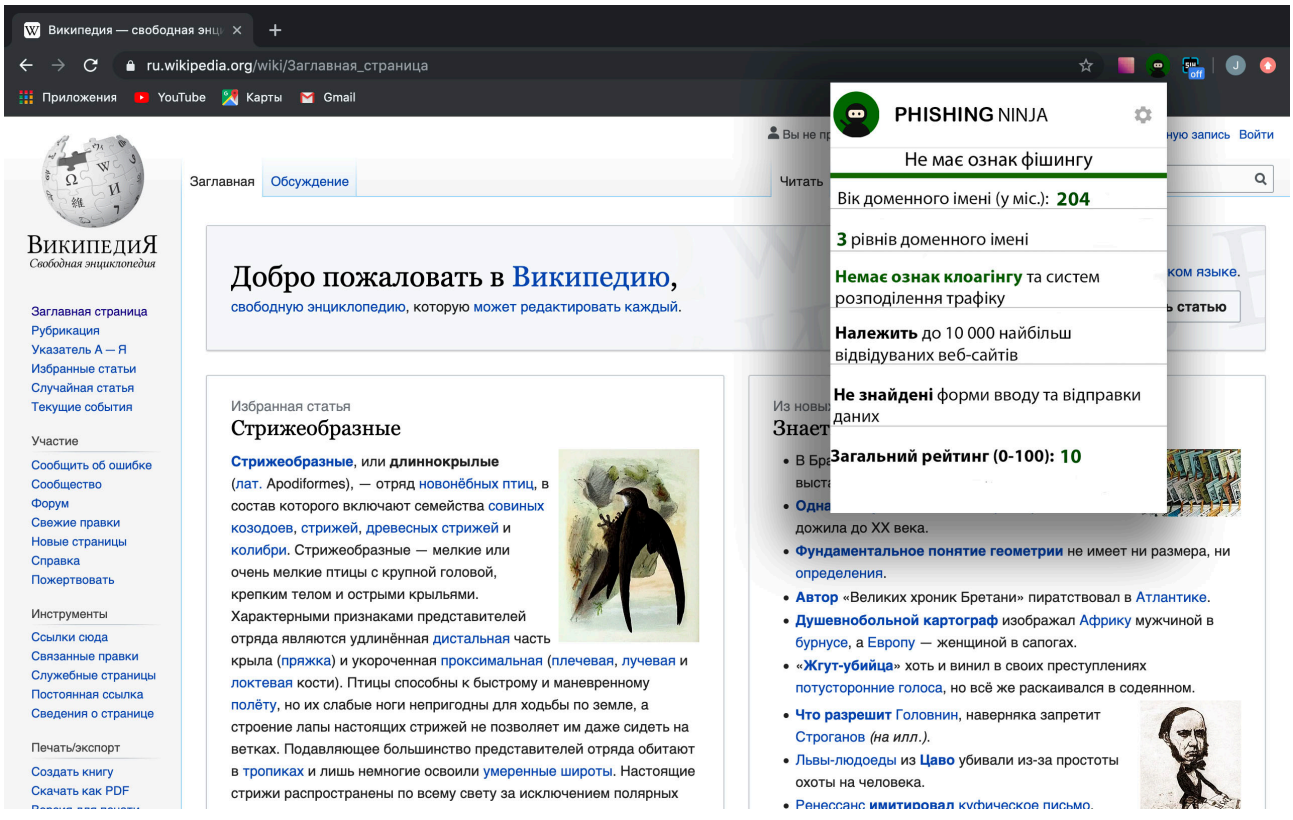

Рисунок 4.1 – Інтерфейс розробленого додатку при запиті користувачем рейтингової оцінки веб-сайту.

На рисунку 4.1 зображено приклад обчислення рейтингової оцінки для веб-сайту. Отримати результат обчислення рейтингу користувач може, якщо клікнути на іконку додатку у панелі додатків Google Chrome. Інформація щодо веб-сайту отримується у формі звіту щодо кожного із аналізуємих параметрів. На даному прикладі зображений запит рейтингової оцінки веб-сайту, що за результатами аналізу новим методом не виявився підозрілим або небезпечним та рівень загрози $x = 0$.

На рисунку 4.2 зображено приклад попередження користувача про небезпечний вміст сайту, що був проаналізований додатком. Користувачу дається вибір, чи продовжити користування веб-сайтом, чи блокувати його. При виборі “продовжити” вікно попередження буде закрите, а веб-сайт буде доступний у повному обсязі. Якшо користувач вибере “блокувати сайт”, сторінка з веб-сайтом буде закрита.

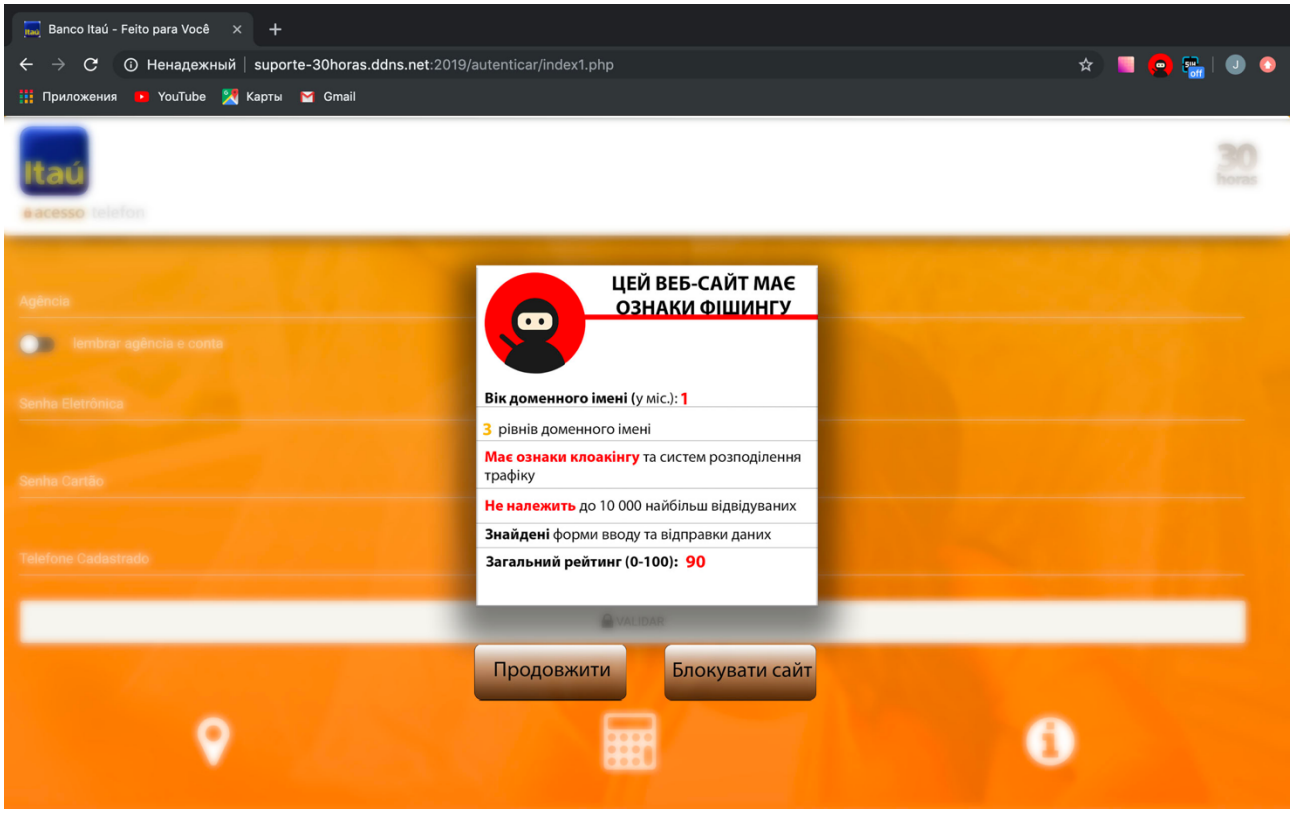

Рисунок 4.2 – Інтерфейс розробленого додатку при попередженні користувача при ступені загрози веб сайту $x = 2$ “небезпечно” .

На рисунку 4.3 зображений приклад попередження користувача при обчисленій ступені загрози $x = 1$, що означає “підозрілий”. Також, логотип додатку в панелі додатків Google Chrome змінює колір від зеленого до жовтого і червоного, що відповідає обчисленому рівню загрози веб сайту як “безпечний”, “підозрілий” і “небезпечний” відповідно.

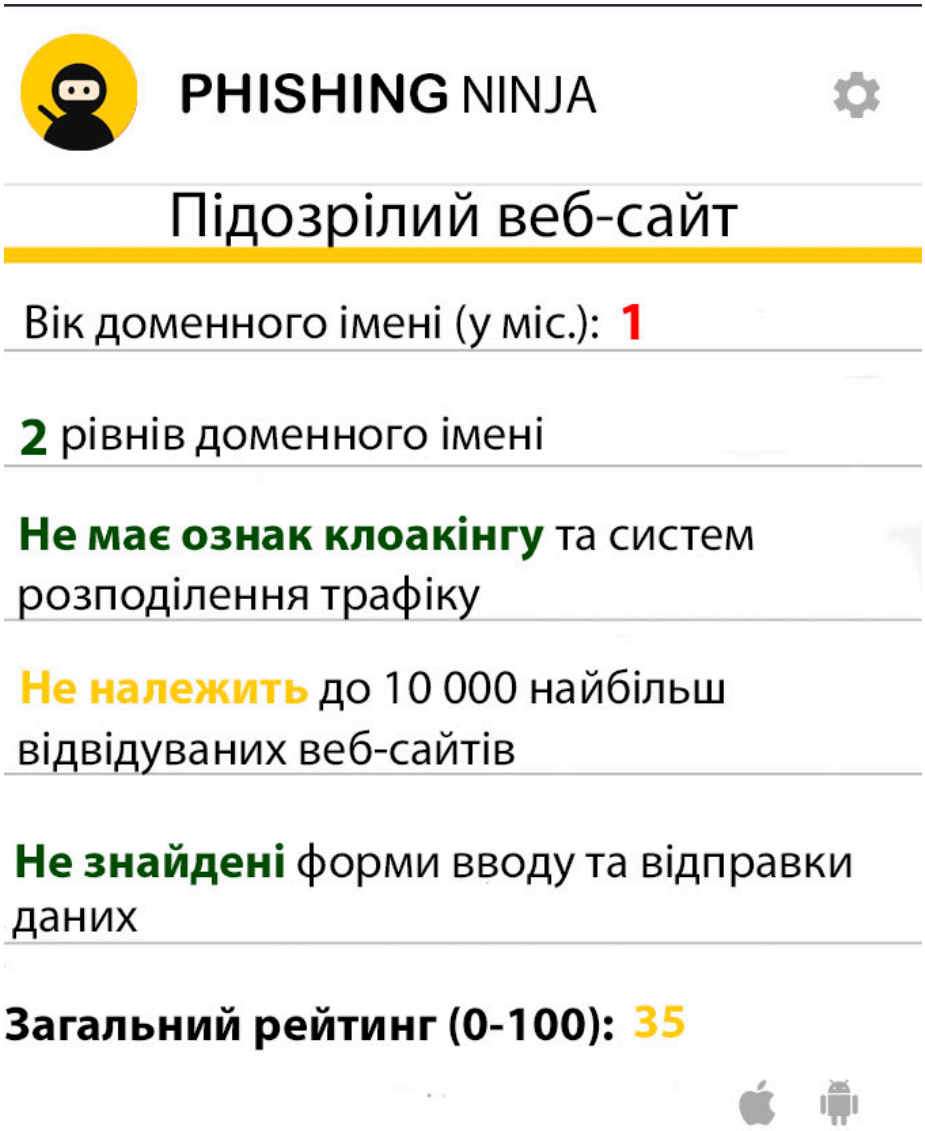

Рисунок 4.3 – Частково зображений інтерфейс розробленого додатку при попередженні користувача при ступені загрози веб сайту $x = 1$ “підозрілий” .

Розроблений додаток дає користувачу можливість приймати рішення щодо відвідування веб-сайту самостійно та отримувати найважливішу інформацію для ідентифікації фішингових веб-сайтів.

Додатково розроблений функціонал попередження користувача зменшує шанси не помітити високий рівень загрози веб-сайту на знижує вірогідність введення конфіденційної інформації на фішинговому веб-сайті.

Для найбільш точної демонстрації роботи розробленого додатку, рейтингова оцінка обчислювалася на тих самих контрольних прикладах веб-сайтів, як і в експерименті у розділі 3.2 даної магістерської наукової роботи.

Серед вагомих переваг даної реалізації нового методу рейтингового оцінювання веб-сайтів:

– додаток не потребує специфічного ПО та підтримує найбільш поширені платформи;

– повна автоматизація нового методу рейтингового оцінювання веб-сайтів;

– зручний та зрозумілий інтерфейс додатку;

– додаток аналізує веб-сайт у середі користувача, що не дозволяє системам розподілення трафіку бути непоміченими при аналізі веб-сайту;

– ідентифікація систем розподілення трафіку реалізована прямо у додатку і не потребує окремого сервера для симуляції підключень від пошукових роботів;

Серед недоліків треба відмітити те, що обчислення рейтингової оцінки займає час та частково залежить від зовнішніх ресурсів, що надають дані для аналізу. При подальшій модифікації додатку рекомендується зменшити час на обчислення рейтингової оцінки та зменшити кількість зовнішніх джерел для отримання даних.

4.3 Опис технічного забезпечення для впровадження нового вдосконаленого методу

Для підтримки роботи програмної реалізації вдосконаленого методу розподілення робіт був розроблений базовий підхід для використання необхідного технічного забезпечення. Він включає себе в опис необхідних технічних засобів для функціонування програмного забезпечення, деякі їх специфікації, а також обґрунтування їх використання.

При формуванні комплексу технічних засобів в якості програмного середовища для програмної реалізації нового методу був обраний веб-браузер користувача, оскільки архітектура додатків до Google Chrome дозволяє обчислення, роботу з інформацією та формування запитів до зовнішніх джерел у середовищі веб-браузера.

Технічне забезпечення задачі включає персональний клієнтський комп’ютер та джерело безперебійного живлення. Кількість персональних комп'ютерів залежить від кількості користувачів.

Для функціонування розробленого додатку необхідна наявність каналу зв'язку, що дозволяє підключитись до мережі Internet. Комп'ютерна мережа може складатися з комутаторів або ж маршрутизаторів мережі і мати доступ до інтернет за стандартом Ethernet 100Base-T [28] або вище.

ВИСНОВКИ

У результаті виконання магістерської атестаційної роботи було проведено дослідження методів забезпечення безпеки ІС від фішингових атак. Доведена актуальність дослідження, проаналізовані існуючі методи, обґрунтована мета розробки вдосконаленого методу, поставлена задача дослідження.

На основі результатів досліджень був розроблений вдосконалений метод рейтингового оцінювання веб-сайтів, описані етапи роботи нового методу, та розроблений алгоритм його реалізації.

Проведений експеримент, де новий вдосконалений метод був застосований на практиці а також порівняний з результатами існуючих методів з забезпечення безпеки ІС від фішингових атак. Результати аналізу отриманих наукових результатів демонструють ефективність нового методу рейтингового оцінювання веб-сайтів.

Для практичного застосування нового методу було розроблене програмне забезпечення, яке автоматизує вдосконалений метод рейтингового оцінювання веб-сайту.

Новий вдосконалений метод може бути покращений та розширений новими етапами з рейтингового оцінювання веб-сайтів для отримання ще більш достовірних результатів при оцінюванні ступеню загрози веб-сайту.

За результатами магістерської наукової роботи можна зробити висновок що поставлена мета - 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 фішінгових атак була успішно виконана.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. ДСТУ 3008-2016. Документація. Звіти у сфері науки і техніки. Структура і правила оформлення. - К., 2016. - 37 с.

2. Методичні вказівки щодо розробки та оформлення магістерської атестаційної роботи за спеціальністю 122 – „Комп'ютерні науки” програма «Інформаційні управляючі Методичні вказівки щодо розробки та оформлення магістерської атестаційної роботи за спеціальністю 122 Комп’ютерні науки (освітня програма «Інформаційні управляючі системи та технології» освітньо-кваліфікаційного рівня «магістр» / Упоряд.: Петров К.Е., Левикін В.М., Чалий С.Ф., Євланов М.В., Саєнко В.І., Міхнов Д.К., Міхнова А.В., Чала О.В. – Харків: ХНУРЕ, 2019. – 24 с.

3. Why 95% of cybercrimes committed in Spain are going unpunished, Jesus Duva [Електронний ресурс] // 2019 URL: https://tproger.ru/translations/ sqlite-mysql-postgresql-comparison/ (дата звернення 25.11.2019)

4. Enterprise phishing resiliency and defense report [Електронний ресурс] // 2019 URL: https://cofense.com/wp-content/uploads/2017/11/Enterprise-Phishing-Resiliency-and-Defense-Report-2017.pdf (дата звернення 25.11.2019)

5. Phishing Scams Cost American Businesses Half A Billion Dollars A Year, Lee Mathews [Електронний ресурс] // 2017 URL: www.forbes.com/sites/leemathews/2017/05/05/phishing-scams-cost-american-businesses-half-a-billion-dollars-a-year/#190fc0c33fa1 (дата звернення 25.11.2019)

6. Symantec Internet Security Threat Report 2018 [Електронний ресурс] // 2018 URL: https://www.phishingbox.com/news/phishing-news/symantec-internet-security-threat-report-2018 (дата звернення 25.11.2019)

7. On the Need for New Antiphishing Measures Against Spear Phishing Attacks, Luca Allodi [Електронний ресурс] // 10.1109/MSEC.2019.2940952URL:

https://www.researchgate.net/publication/336156333_On_the_Need_for_New_Anti-phishing_Measures_Against_Spear_Phishing_Attacks (дата звернення 25.11.2019)

8. Group Makes $50 Million by Phishing Bitcoin Users Using Google AdWords, Catalin Cimpanu [Електронний ресурс] // 2017 URL: www.forbes.com/sites/leemathews/2017/05/05/phishing-scams-cost-american-businesses-half-a-billion-dollars-a-year/#190fc0c33fa1 (дата звернення 25.11.2019)

9. A Privacy Analysis of Google and Yandex Safe Browsing Thomas Gerbet, Amrit Kumar, Cédric Lauradoux [Електронний ресурс] // 2015 URL: https://hal.inria.fr/hal-01120186v4/document (дата звернення 25.11.2019)

10. Розробка методу оцінки системних вимог до рішення маркетингових задач для проектування інформаційних систем / В.М. Левикін, О.П. Костенко, О.В. Петриченко // Радіоелектроніка, інформатика, управління. Науковий журнал. – Запоріжжя: Запорізький національний технічний університет, 2012. - № 1(26). - С. 123-129.

11. Баричев С. Г., Гончаров В. В., Серов Р. Е. 2.4.2. Стандарт AES. Алгоритм Rijdael // Основы современной криптографии — 3-е изд. — М.: Диалог-МИФИ, 2011. — С. 30–35. — 176 с. — ISBN 978-5-9912-0182-7

12. PhishTank [Електронний ресурс] // 2011 URL: https://umbrella.cisco.com/blog/2006/10/02/friends-of-opendns-meet-phishtank/ (дата звернення 25.11.2019)

13. How effective is the wisdom of crowds as a security mechanism, Tyler Moore [Електронний ресурс] // 2018 URL:

https://www.lightbluetouchpaper.org/2007/12/21/how-effective-is-the-wisdom-of-crowds-as-a-security-mechanism/ (дата звернення 25.11.2019)

14. Akinyelu, A; Adewumi, AO. ‘Classification of Phishing Email Using Random Forest Machine Learning Technique’. Journal of Applied Mathematics, vol.2014, pp.1–7, Apr 2014.

15. Cisco Advanced Phishing Protection [Електронний ресурс] // 2018 URL: https://www.cisco.com/c/dam/en/us/products/collateral/security/cloud-email-security/at-a-glance-c45-740894.pdf (дата звернення 25.11.2019)

16. Office 365 Advanced Threat Protection [Електронний ресурс] // 2019 URL: https://docs.microsoft.com/ru-ru/microsoft-365/security/office-365-security/office-365-atp (дата звернення 25.11.2019)

17. DomainKeys Identified Mail (DKIM) Signatures, E. Allman, J. Callas, M. Delany, M. Libbey [Електронний ресурс] // 2011 URL: https://tools.ietf.org/html/rfc4871 (дата звернення 25.11.2019)

18. Global-Phish-Report [Електронний ресурс] // 2011 URL: https://www.avanan.com/hubfs/2019-Global-Phish-Report.pdf (дата звернення 25.11.2019)

19. Protecting users from repeatedly dangerous sites, Brooke Heinichen [Електронний ресурс] // November 8, 2016 URL: https://security.googleblog.com/2016/11/protecting-users-from-repeatedly_8.html (дата звернення 25.11.2019)

20. BlackTDS Traffic Distribution System for Malware Offered as a Service in the Dark Web [Електронний ресурс] // 2018 URL: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-

threats/blacktds-traffic-distribution-system-for-malware-offered-as-a-service-in-the-dark-web (дата звернення 25.11.2019)

21. Cloaker Catcher: A Client-based Cloaking Detection System, Ruian Duan , Weiren Wang, Wenke Lee [Електронний ресурс] // 2017 URL: https://arxiv.org/pdf/1710.01387.pdf (дата звернення 25.11.2019)

22. Needle in a Haystack: Tracking Down Elite Phishing Domains in the Wild, Ke Tian, Steve T.K. Jan, Hang Hu, Danfeng Yao, Gang Wang [Електронний ресурс] // 2018 URL: https://gangw.cs.illinois.edu/imc18.pdf (дата звернення 25.11.2019)

23. Detecting phishing attacks using natural language processing and machine learning Peng, T., Harris, I., & Sawa, Y. // 2018 / ieee 12th international conference on semantic computing (icsc) (pp. 300–301)

24. Googlebot Crawl Issue Identification Through Server Logs, David Sottimano [Електронний ресурс] // 2018 URL: https://moz.com/blog/server-log-essentials-for-seo (дата звернення 25.11.2019)

25. Hypertext Transfer Protocol (HTTP) Status Code Registry [Електронний ресурс] // 2018 URL: https://www.iana.org/assignments/http-status-codes/http-status-codes.xhtml (дата звернення 25.11.2019)

26. Advanced Chrome Extension Exploitation Leveraging API powers for Better Evil, Krzysztof Kotowicz, Kyle Osborn [Електронний ресурс] // 2016 URL: https://media.blackhat.com/bh-us-12/Briefings/Osborn/BH_US_12_Osborn_Kotowicz_Advanced_Chrome_Extension_WP.pdf (дата звернення 25.11.2019)

27. Comparison of JSON and XML Data Formats, Alen Cimec [Електронний ресурс] // 2014 URL:

https://www.researchgate.net/publication/329707959_Comparison_of_JSON_and_XML_Data_Formats (дата звернення 25.11.2019)

28. Компьтерные сети, Анна Варашус [Електронний ресурс] // 2014 URL: https://sites.google.com/site/varashus/ (дата звернення 25.11.2019)

29. Основи охорони праці та безпека життєдіяльності, Заікіна Д. П. [Електронний ресурс] // 2019 URL: https://www.academia.edu/40052159 (дата звернення 25.11.2019)