

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПОЛІСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних
технологій, обліку та фінансів
Кафедра комп'ютерних технологій
і моделювання систем

Кваліфікаційна робота
на правах рукопису

Доронін Андрій Ілліч

УДК 004.738.5

КВАЛІФІКАЦІЙНА РОБОТА

Система виявлення деструктивних впливів в соціальних інтернет-сервісах

(тема роботи)

126 «Інформаційні системи та технології»

(шифр і назва спеціальності)

Подається на здобуття освітнього ступеня бакалавр

кваліфікаційна робота містить результати власних досліджень. Використання
ідей, результатів і текстів інших авторів мають посилання на відповідне
джерело

(підпис, ініціали та прізвище здобувача вищої освіти)

Керівник роботи:
Веретюк Сергій Миколайович
старший викладач кафедри комп'ютерних
технологій і моделювання систем, к.т.н.

Житомир – 2023

Висновок кафедри _____

за результатами попереднього захисту: _____

Протокол засідання кафедри

№ _____ від « _____ » _____ 20 _____ р.

Завідувач кафедри

доктор економічних наук,

професор

_____ **Николюк Ольга Миколаївна**

« _____ » _____ 2023 р.

Результати захисту кваліфікаційної роботи

Здобувач вищої освіти Доронін Андрій Ілліч захистив кваліфікаційну роботу з оцінкою:

сума балів за 100-бальною шкалою _____

за шкалою ECTS _____

за національною шкалою _____

Секретар ЕК

(науковий ступінь, вчене звання)

(прізвище, ім'я, по батькові)

(підпис)

АНОТАЦІЯ

Доронін А.І. Система виявлення деструктивних впливів в соціальних інтернет-сервісах. – Кваліфікаційна робота на правах рукопису.

Кваліфікаційна робота на здобуття освітнього ступеня бакалавра за спеціальністю 126 – Інформаційні системи та технології. – Поліський національний університет, Житомир, 2023.

Зміст анотації

В кваліфікаційній роботі визначено однією з основних ознак розвитку сучасного суспільства є стрімкий розвиток соціальних мереж, який дає можливість сучасній людині працювати, навчатися, обговорювати проблеми, які турбують, знайомитися та спілкуватися з друзями. Сьогодні Інтернет став невід’ємною частиною нашого життя. Проте слід зазначити, що мережа Інтернет дає не тільки можливість для розвитку здібностей, покращення знань та розширення кола інтересів, але й містить у собі реальні загрози як для дорослих, так і для дітей. Нарівні з позитивними сторонами, соціальні мережі мають і негативні наслідки – це інтернет-залежність, економія або відсутність часу на живе спілкування. Соціальні мережі, відсуваючи на другий план класичні інститути соціалізації – родину, школу, друзів, – займають усе більш домінуючу роль у процесі соціалізації особистості й здійснюють безпосередній вплив на її ціннісні орієнтації.

Ключові слова:

Соціальні мережі, перевірка домена, захист користувача, програмування.

SUMMARY

Doronin A.I. System for detecting destructive effects of other - Qualification work on the rights of the manuscript.

Qualification work for obtaining a master's degree in specialty 126 - Information systems and technologies - Polissya National University, Zhytomyr, 2023.

Content of the summary

In the qualification work, one of the main features of the development of modern society is the rapid development of social networks, which allows a modern person to work, study, discuss problems of concern, meet and communicate with friends. Today, the Internet has become an integral part of our lives. However, it should be noted that the Internet provides not only an opportunity to develop skills, improve knowledge and expand the range of interests, but also contains real threats to both adults and children. Along with positive aspects, social networks also have negative consequences, such as Internet addiction, saving or lack of time for face-to-face communication. Social networks, relegating to the background the classical institutions of socialization - family, school, friends - are playing an increasingly dominant role in the process of socialization of the individual and have a direct impact on his or her value orientations.

Keywords:

Social networks, domain verification, user protection, programming.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ	6
ВСТУП	7
Актуальність теми	7
Розділ 1 АНАЛІЗ ОСОБЛИВОСТЕЙ ПРЕДМЕТНОЇ ОБЛАСТІ ДОСЛІДЖЕННЯ ТА ЗАГАЛЬНІ ПОНЯТТЯ СИСТЕМИ	9
1.1 Визначення предметної області дослідження та аналіз інформаційних потреб системи	9
1.2 Функціональне моделювання та вимоги предметної області	12
Висновок до першого розділу	16
Розділ 2 РОЗРОБЛЕННЯ СИСТЕМИ ВИЯВЛЕННЯ ДЕСТРУКТИВНИХ ВПЛИВІВ В СОЦІАЛЬНИХ ІНТЕРНЕТ СЕРВІСАХ	17
2.1. Алгоритми функціонування системи виявлення деструктивних впливів в соціальних інтернет сервісах	17
2.2. Формалізація системи виявлення деструктивних впливів в соціальних інтернет сервісах	18
Висновок до другого розділу	26
Розділ 3. ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ВИЯВЛЕННЯ ДЕСТРУКТИВНИХ ВПЛИВІВ В СОЦІАЛЬНИХ ІНТЕРНЕТ СЕРВІСАХ	27
3.1. Інтерфейс системи виявлення деструктивних впливів в соціальних інтернет сервісах	27
Висновок до третього розділу	28
ВИСНОВКИ ТА ПРОПОЗИЦІЇ	29
Перелік літературних джерел	30
ДОДАТКИ:	32

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ПЗ	Програмне забезпечення.
JS	Динамічна, об'єктно-орієнтована прототипна мова програмування.
PHP	Скриптова мова програмування, була створена для генерації HTML-сторінок на стороні веб-сервера.
IDEF0	Методологія моделювання з використанням функціональних блоків.
IDEF3	Методологія моделювання з використанням процесних блоків та розгалужень.
ТЗ	Технічне завдання.
БД	База даних.

ВСТУП

Актуальність теми

Актуальність дослідження полягає у тому, що соціальні мережі на сьогоднішній день об'єднують мільйони людей, які спілкуються між собою. Тому є важливим дослідити вплив соціальних мереж на формування їх особистості.

Мета кваліфікаційної роботи

Метою дослідження є виявлення негативних та позитивних сторін спілкування в соціальних мережах та їх вплив на особистість.

Завдання кваліфікаційної роботи

Завданням на кваліфікаційну роботу є:

- 1) дослідження предметної області, виявлення необхідності в розробці рішення для існуючих екологічних проблем;
- 2) створення математичної моделі майбутньої установи;
- 3) розробка зручного інтерфейсу на базі математичної моделі.

Об'єкт дослідження

Об'єктом дослідження є процес вивчення соціалізації особистості в сучасному інформаційному суспільстві.

Предмет дослідження

Предметом дослідження є соціальні мережі як соціокультурний феномен та інститут соціалізації.

Методи дослідження

- Метод аналізу контенту: передбачає використання алгоритмів машинного навчання, щоб автоматично аналізувати контент, що публікується користувачами. Таким чином, система може виявляти деструктивні повідомлення, коментарі або фото, які містять небезпечні для здоров'я, пропагандистські, рекламні та інші негативні відгуки.

- Метод соціального аналізу: дозволяє виявляти певні зв'язки між користувачами, що можуть бути використані для поширення негативного впливу. Наприклад, система може виявляти користувачів, які взаємодіють з деструктивним контентом або певними користувачами, які розповсюджують небезпечну інформацію.
- Метод відстеження поведінки користувачів: дозволяє виявляти зміни в поведінці користувачів, які можуть свідчити про те, що їх впливають деструктивні фактори. Наприклад, система може відстежувати зміни в кількості публікацій, взаємодії з іншими користувачами та загальної активності на платформі.
- Метод аналізу сигналів: базується на виявленні сигналів, які можуть вказувати на наявність деструктивного впливу. Наприклад, система може виявляти певні ключові слова або теги, які пов'язані з деструктивним контентом

Перелік публікацій автора за темою дослідження:

1. Аналіз методів виявлення деструктивних впливів в соціальних інтернет сервісах - під номером 16 у переліку джерел літературних
2. Поточний стан от технологій - під номером 17 у переліку джерел літературних

Практичне значення отриманих результатів:

Така система може допомогти інтернет-платформам швидко виявляти та припиняти поширення деструктивного контенту, що може бути шкідливим для користувачів та загрожувати їхній безпеці. Це може допомогти зменшити кількість негативних впливів, що виникають на інтернет-платформах.

Структура кваліфікаційної роботи:

34 сторінки, 20 рисунків, 1 додаток, 15 джерел

Розділ 1 АНАЛІЗ ОСОБЛИВОСТЕЙ ПРЕДМЕТНОЇ ОБЛАСТІ ДОСЛІДЖЕННЯ ТА ЗАГАЛЬНІ ПОНЯТТЯ СИСТЕМИ

1.1 Визначення предметної області дослідження та аналіз інформаційних потреб системи

Ще декілька десятків років тому люди не могли і подумати що спілкування на відстані можливе, а тим паче бачити обличчя людини яка в іншій країні, або ж спілкуватися з неї. З розвитком Інтернету з'являлося багато різної інформації, а також і багато сервісів і програм, навіть документи і інші системи державних установ вже вносять в мережу Інтернет, також разом з цим з'явилися і соціальні мережі без яких вже ніхто не може обійтись і місяця, адже вони спрощують наше життя. Завдяки ним ми можемо спілкуватися з друзями, слідкувати за іншими людьми, які нам імпонують, читати новини, та слідкувати за загальною ситуацією в світі, що наразі дуже важливо. Але також важливою проблемою є і захист від негативного впливу на людину.

В 1954 англійській соціолог Барнс у збірці робіт «Людські стосунки» для позначення спільноти людей, що були об'єднані однаковими інтересами, вподобаннями та тих хто має спільні причини для спілкування між собою об'єднав в термін «соціальна мережа». В 1995 році історія соціальної мережі вийшла на нову ступінь еволюції, адже Ренді Конрад створив першу соціальну мережу – Classmates.com.

Саме з цього часу і почали з'являтися ті самі соціальні мережі, які ми знаємо сьогодні, навипередки вони змагалися за користувачів і їх увагу. Саме тому було розроблено багато соціальних інститутів, які вивчали соціальні мережі, їх вплив на людину, на групу людей, вплив на населення в цілому, в тому числі на окремі верстки населення, за віком і життєвими поглядами. На даний момент найпопулярнішими соціальними мережами є:

Twitter (www.twitter.com) – популярна соціальна мережа, що нагадує міні-блоги. Найчастіше саме в ній популярні люди висловлюють свої

думки , і всі кому цікаво можуть стежити за цим і давати свої коментар.

Instagram (www.instagram.com) – в останні роки ця соціальна мережа набрала великої популярності, саме в ній люди частіше всього виставляють свої фото/відео на показ і збирають реакцію.

Facebook (www.facebook.com) – міжнародна соціальна мережа, кількість користувачів вражає - 1,5 млрд., напевно кожен хто хоча б раз заходив в інтернет знає про цю соціальну мережу, або ж бачив рекламу, або сам є частиною фейсбук.

Telegram – це хмарний месенджер для мобільних пристроїв та комп'ютерів. Швидкий та безпечний. Telegram Messenger входить в топ-5 найбільш завантажуваних програм у світі. Влітку 2022 року його кількість перевищила 700 мільйонів активних користувачів щомісяця. Компанія базується в Дубаї. Telegram прагне захищати конфіденційність користувачів і права людини, такі як свобода слова та зібрань. Вона відіграла помітну роль у продемократичних рухах по всьому світу, зокрема в Ірані, Україні, М'янмі та Гонконгу.

З великою популярністю приходить і велика відповідальність. Соціальні мережі все частіше почали вводити регулюючі правила поведінки, поганих користувачів, що порушують політику безпеки, займаються булінгом, тощо все частіше почали блокувати в соціальній мережі, але і це не вирішує проблем. Також все частіше почали вводити цензуру в коментарях, в публікаціях, аби зменшити негативний вплив на людей.

Серед прикладів роботи з перевіркою сайтів є система – thehost.ua. Вона перевіряє доступність сайту з різних точок планети, за допомогою нього можна отримати загальну інформацію про IP-адресу, на якій розташований зазначений адрес. Перевіряє коректність налаштувань DNS і тому інше.

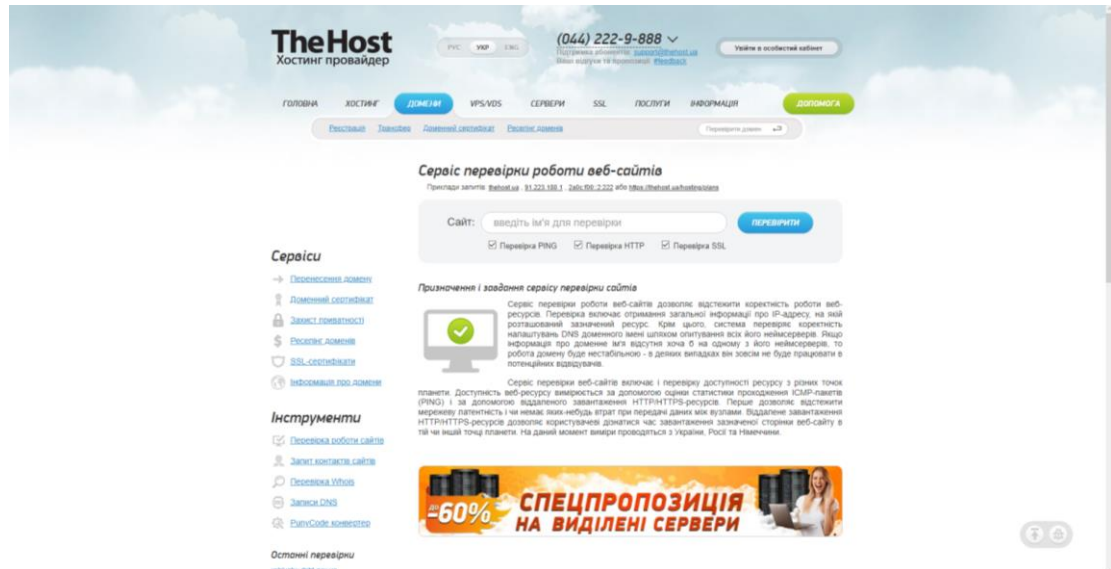


Рисунок 1.1 - сайт thehost.ua

Ще один приклад – сайт who.is. Що шукає інформацію про вебсайт, домен реєстру, тощо.

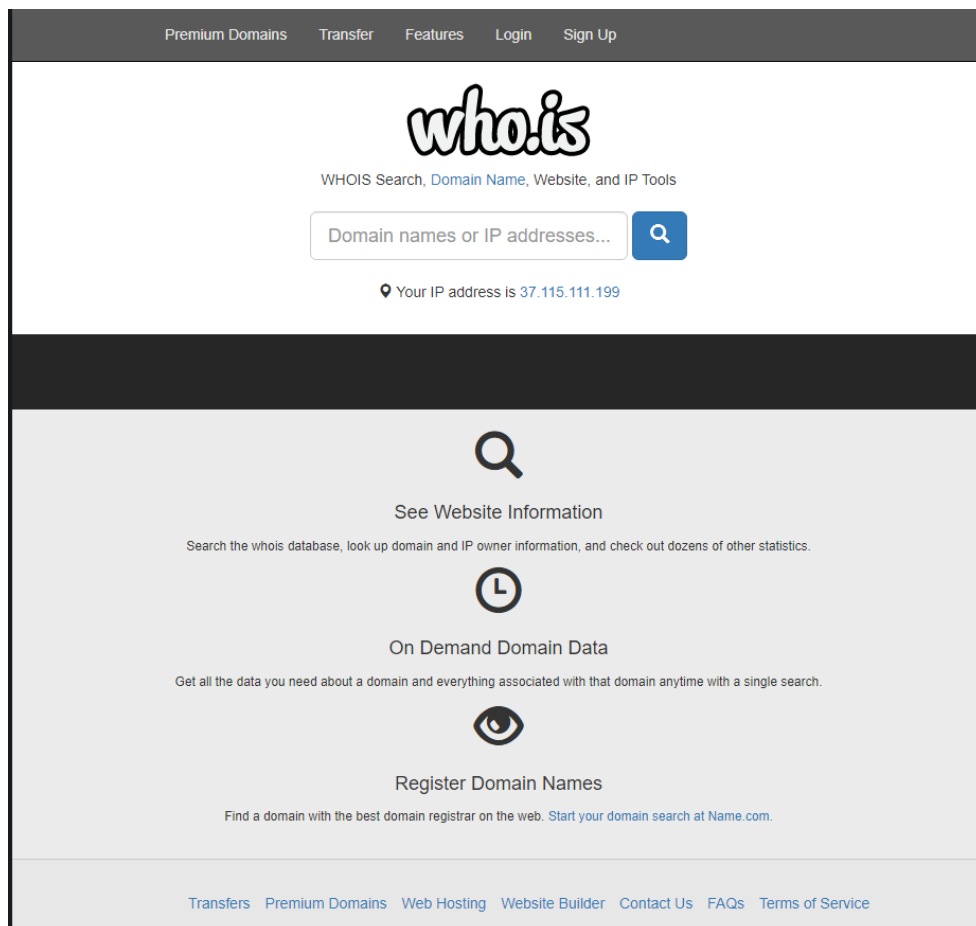


Рисунок 1.2 - сайт who.is

1.2 Функціональне моделювання та вимоги предметної області

Контекстна діаграма для моделі системи виявлення деструктивних впливів в соціальних інтернет-сервісах зображена на рисунку 1.3

Запит є вхідними даними системи, користувач інтернет-сервісу є механізмом, потрібним для створення система. Політика конфіденційності – інформація, яка управляє

Показник безпеності інтернет-сервісу – результат роботи системи, або ж вихідні дані

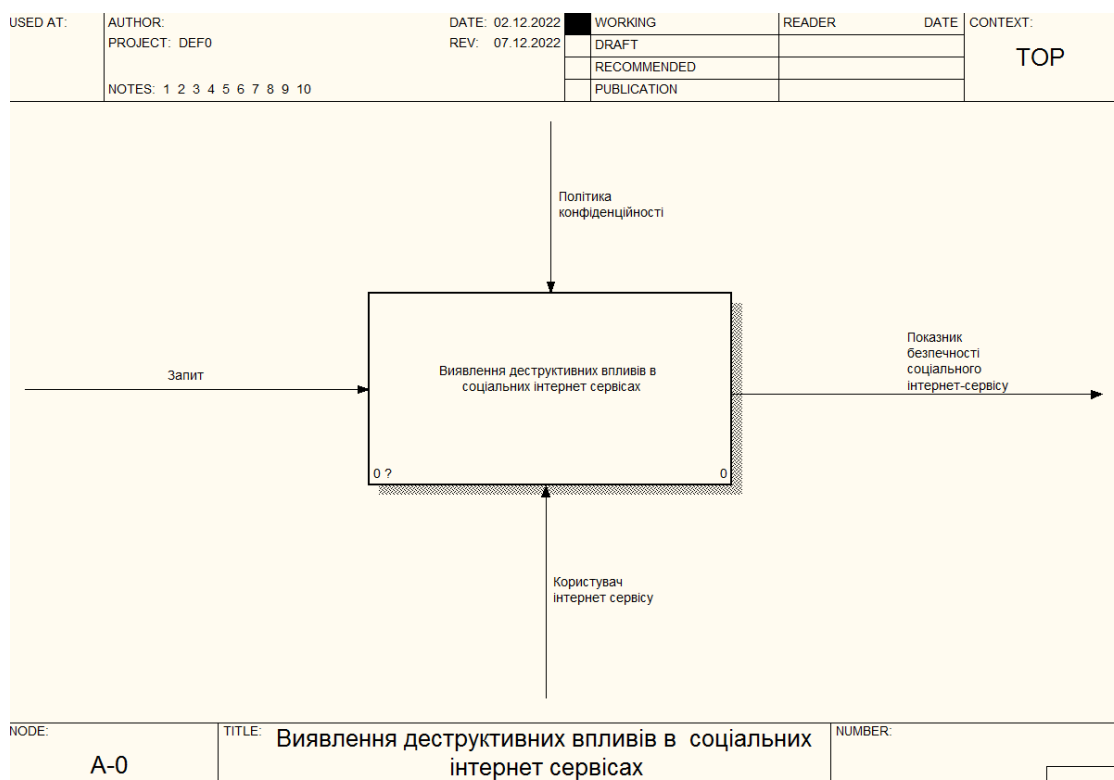


Рисунок 1.3 – Контекстна діаграма системи (IDEF0)

Діаграмою декомпозиції першого рівня приведена на рисунку 1.4

Вона виконує вирішення таких під задач:

1. Запит адреси інтернет сервісу – входить запит, на виході отримуємо адресу інтернету сервісу;
2. Отримання інформації про інтернет сервіс – в цей блок входить адреса інтернет сервісу, в кінці обчислення виходять дані про інтернет сервіс;

3. Аналіз отриманих даних про інтернет сервіс – в результаті роботи цього блоку дані про інтернет сервіс аналізуються та на виході отримуються проаналізовані дані;

4. Визначення показника безпечності – з проаналізованих даних формується показник безпечності соціального інтернет сервісу

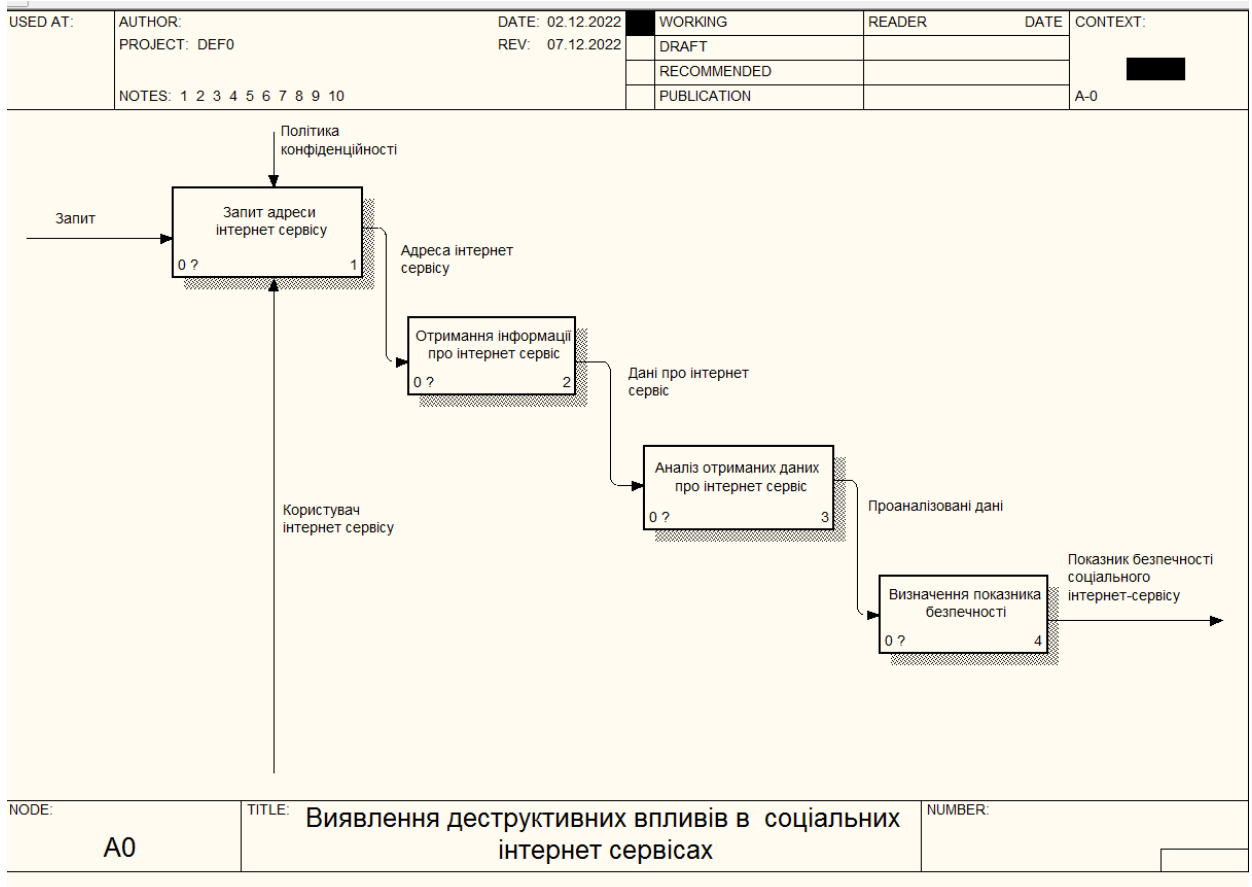


Рисунок 1.4 – Діаграма декомпозиції першого рівня (IDEF0)

Декомпована діаграма другого рівня для процесу отримання інформації про інтернет сервіс знаходиться на рисунку 1.5

Вирішення даного процесу:

1. Отримання інформації про домен – розглядаючи адресу отримуємо інформацію про домен;
2. Отримання даних про SSL сертифікат – розглядаючи адресу отримуємо дані про SSL сертифікат;
3. Перевірка домена через Virus Total – розглядаючи адресу отримуємо звіт Virus Total;

4. Виходячи з цього всього отримуємо дані про інтернет сервіс



Рисунок 1.5 – Діаграма декомпозиції другого рівня для процесу отримання інформації про інтернет сервіс

Діаграма декомпозиції другого рівня для процесу аналіза отриманих даних про інтернет сервіс на рисунку 1.6

Виконання процесу:

1. Аналіз даних про домен – аналізуються дані про домен інтернет сервісу;
2. Аналіз даних про SSL сертифікат – аналізуються дані про SSL сертифікат;
3. Аналіз домена через Virus Total – аналізується звіт Virus Total;
4. Виходячи з цього всього отримуємо проаналізовані дані про інтернет сервіс

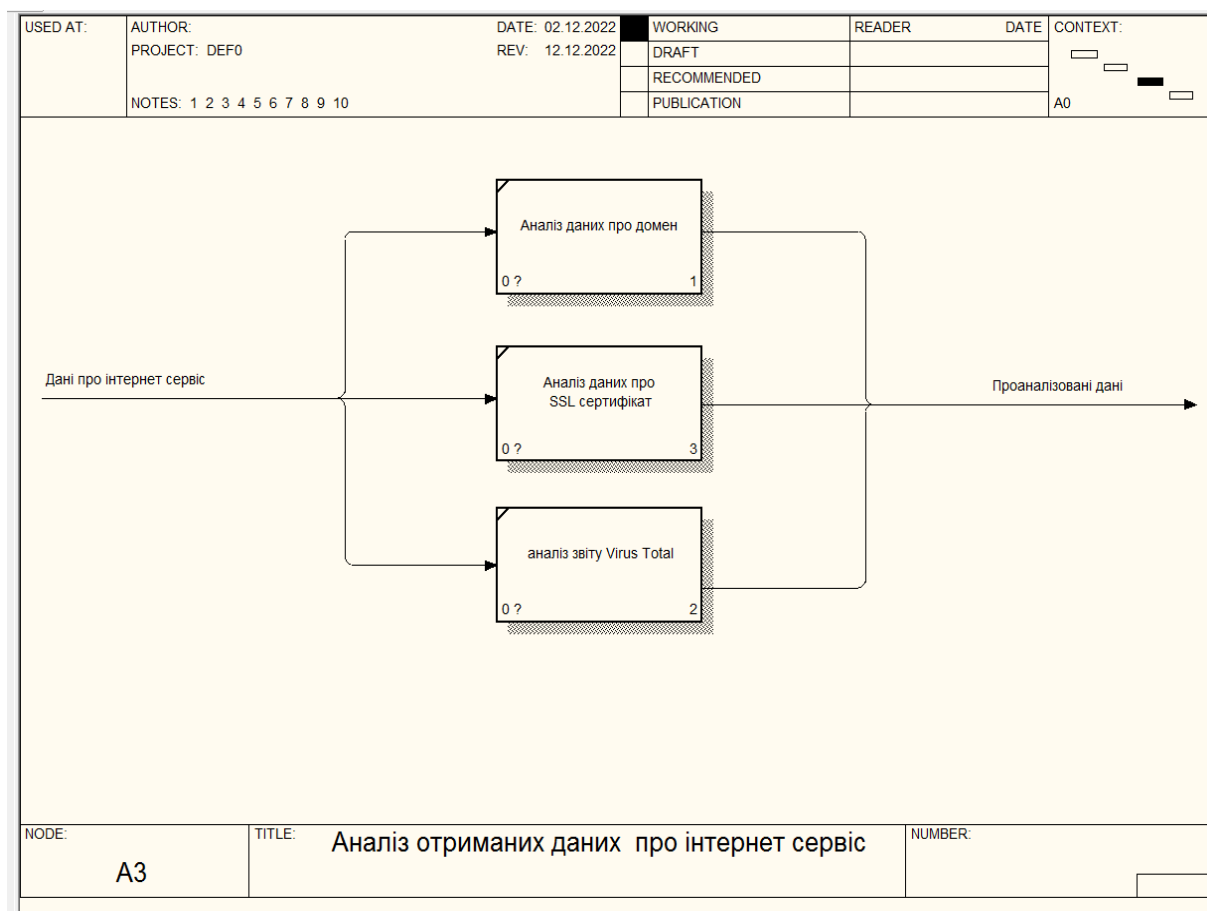


Рисунок 1.6 – Діаграма декомпозиції другого рівня для процесу аналізу отриманих даних про інтернет сервіс

Діаграма декомпозиції другого рівня для процесу визначення показника безпеки на рисунку 1.7

Вирішення процесу:

1. Визначення показника безпеки домену – визначається показник безпеки домену інтернет сервісу;
2. Визначення показника безпеки SSL сертифікат – визначається показник безпеки SSL сертифікат;
3. Визначення показника безпеки за звітом Virus Total – визначається показник безпеки за звітом Virus Total;
4. Визначення сукупного показника безпеки – на основі показників безпеки визначається єдиний показник безпеки соціального інтернет сервісу.



Рисунок 1.7 – Діаграма декомпозиції другого рівня для процесу визначення показника безпеки

Висновок до першого розділу

В цьому розділі було проаналізовано систему виявлення деструктивних впливів в соціальних інтернет сервісах. Було розглянуто соціальні мережі та інтернет сервіси, історію їх виникнення і їх вплив на людей в цілому, було проаналізовано декілька схожих систем.

Також було розроблено діаграму IDEF0, на основі якої буде реалізовано систему виявлення деструктивних впливів в соціальних інтернет сервісах

Розділ 2 РОЗРОБЛЕННЯ СИСТЕМИ ВИЯВЛЕННЯ ДЕСТРУКТИВНИХ ВПЛИВІВ В СОЦІАЛЬНИХ ІНТЕРНЕТ СЕРВІСАХ

2.1. Алгоритми функціонування системи виявлення деструктивних впливів в соціальних інтернет сервісах

Для того щоб краще розуміти які процеси виконуються в моделі системи виявлення деструктивних впливів в соціальних інтернет сервісах було розроблено карту процесів системи за допомогою діаграми IDEF3.

В якості вхідних даних розглядається адреса сайту.

Результатом виконання роботи буде відображення показника безпеки користувачу, або ж у випадку невдачі – відображення помилки користувачу.

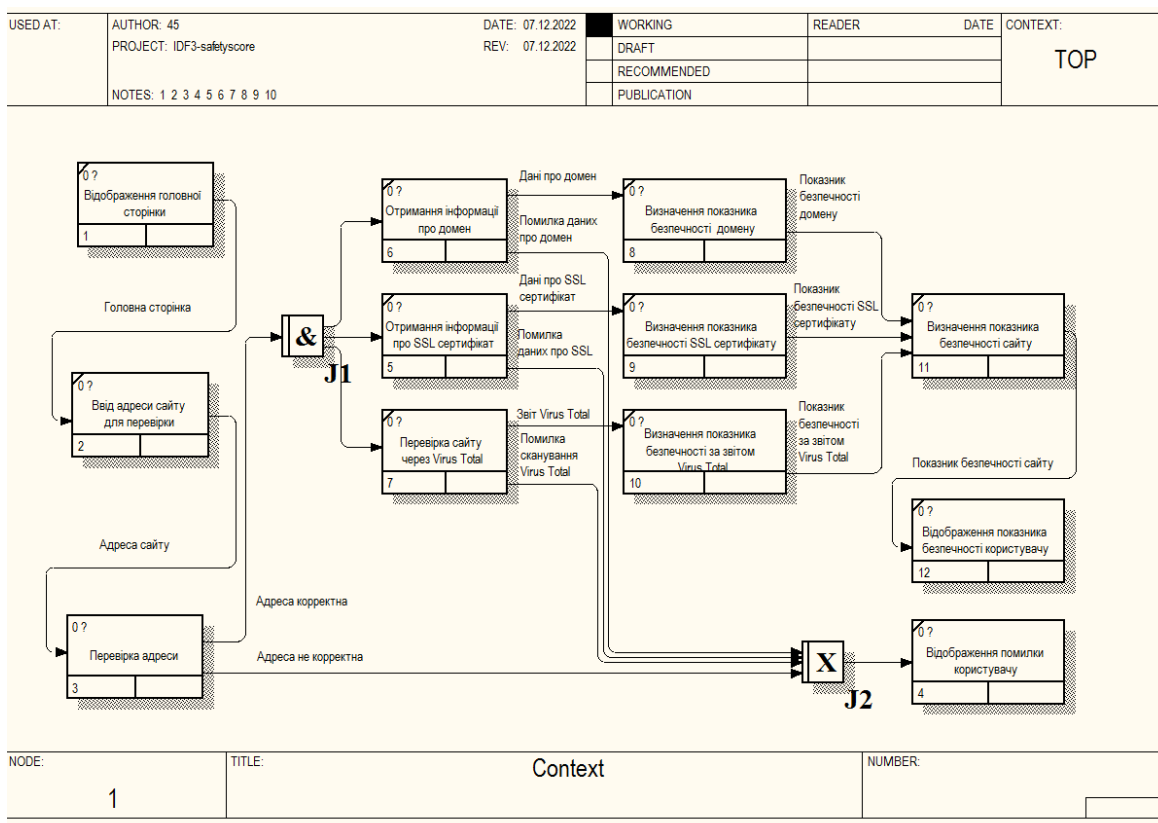


Рисунок 2.1 – Карта процесів системи (IDEF3)

Діаграма що виконує під задачу для перевірки адреси на рисунку 2.2:

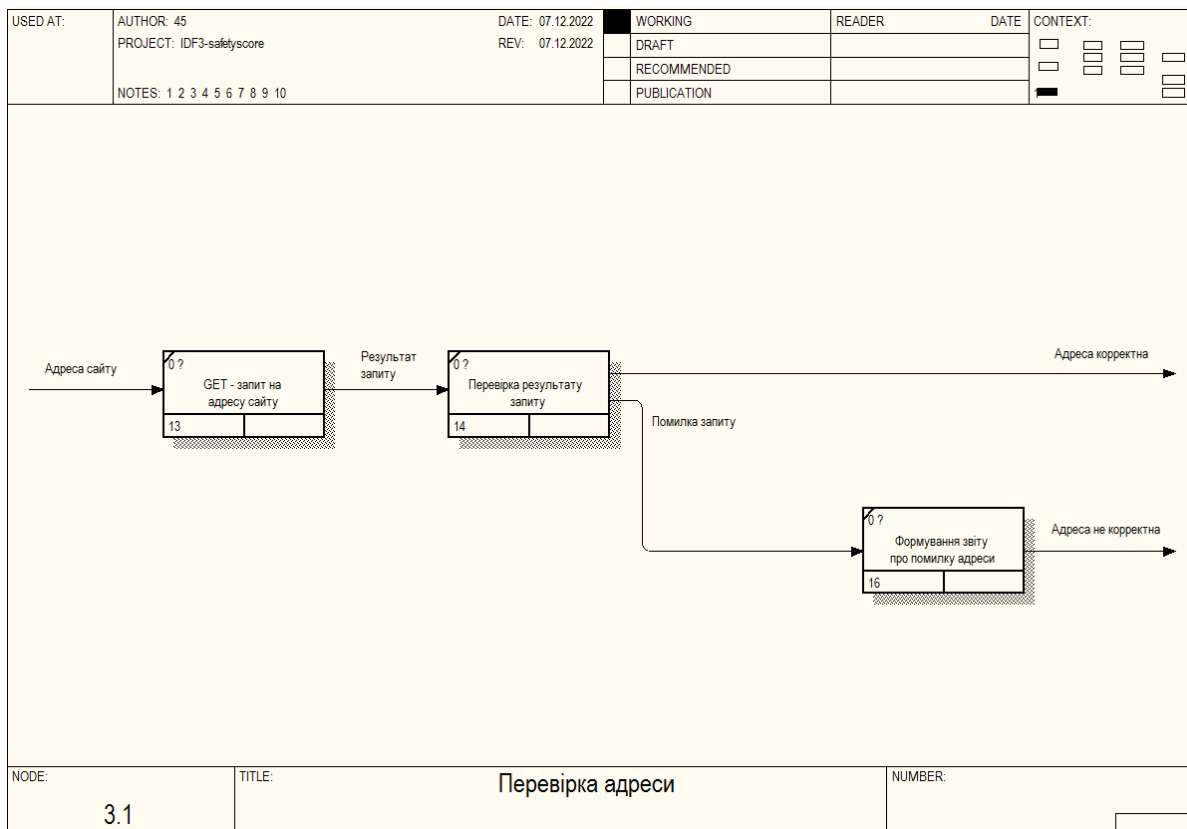


Рисунок 2.2 – Діаграма під задачі перевірки адреси (IDEF3)

2.2. Формалізація системи виявлення деструктивних впливів в соціальних інтернет сервісах

Для визначення показника безпечності сайту буде використано наступні ресурси:

- who.is – отримання інформації про доменне ім'я: власник домену, ір-адреса дата реєстрації домену тощо.
- DNS Checker – перевірка доступності сайту з різних точок світу.
- Wayback machine – це сервіс що здійснює архівування web-сайтів на різних етапах їх існування та формує статистику цих змін та активності сайту в цілому.
- Virus Total – це сервіс для перевірки файлів та web-сайтів на наявність вірусів, хробаків, троянів і інших шкідливих програм.

У процесі визначення загального показника безпечності сайту буде використано наступні показники:

- **Технічна репутація** – формується на основі строку існування домену, терміну сплати за нього та наявності SSL сертифікату
- **Активність** – історія сканувань сервісом Wayback Machine
- **Доступність** – можливість отримання доступу з різних країн.
- **Безпековий аспект** – результат сканування Virus Total

Технічна репутація

Для оцінки технічної репутації використовуються наступні показники: строк існування домену, терміну сплати за його аренду та наявності SSL сертифікату. Кожен з цих показників має певну свою частину у кінцевій оцінці технічної репутації:

- Наявність SSL – 1 бал
- Строк існування домену – 2 бали
- Строк сплати домену – 2 бали

Оцінка за параметром «строк існування домену» вираховується за наступною формулою: $R1 = MIN(2 \div T \times V; 2)$, де $MIN()$ – функція що вибирає мінімальне з декількох значень, і в даному випадку використовується для недопускання виходу оцінки за межі $[0; 2]$ балів, 2 – максимальна кількість балів за параметр, T – рекомендований термін існування домену в роках, V – термін існування домену в роках.

Оцінка строку сплати домену відбувається за формулою $R2 = MIN(2 \div U \times N; 2)$, де « $MIN()$ » та «2» виконують ту саму функцію що в попередній формулі, U – рекомендованих термін сплати за домен в роках, N – термін сплати за домен в роках.

Кінцева оцінка технічної репутації є сумою оцінок її складових, та вираховується за формулою $O1 = R1 + R2 + R3$, де $R1$ – оцінка параметру «Строк існування домену», $R2$ – оцінка параметру «Строк сплати домену», $R3$ – оцінка параметру «Наявність SSL». При цьому $R3$ буде дорівнювати одиниці у разі наявності SSL сертифікату, та нулю у разі його відсутності.

Оцінка технічної репутації			
Параметр	Значення	Макс. Оцінка	Оцінка
Наявність SSL	+	1	1
Строк існування домену (рік)	5	2	2
Строк сплати домену (рік)	1	2	0,66666667
Оцінка технічної репутації			3,66666667

Рисунок 2.3 – Оцінка технічної репутації на прикладі сайту
«windows10activation.ru»

Активність

Для оцінки активності необхідно отримати загальну кількість сканувань сайту за всі роки та помісячну кількість сканувань за даний рік. Всього для оцінки використовуються два параметри:

1. Кількість сканувань – оцінка кількості сканувань сайту за всі роки
2. Стабільність сканувань – відображає стабільність сканувань протягом року

Оцінка кількості сканувань відбувається за наступною формулою: $T1 = C \times 5 \div M \times K \times 50\%$, де C – кількість сканувань за рік, 5 – загальна максимальна оцінка, M – середня кількість сканувань кожного сайту за час його існування, 50% – ваговий коефіцієнт параметру.

В свою чергу оцінювання стабільності сканувань проходить за формулою $T2 = (1 - D / (MAX, MIN)) \times 50\% \times K$, де D – середнє квадратичне відхилення місячних сканувань протягом року, MAX – максимальна кількість сканувань за місяць протягом року, MIN – мінімальна кількість сканувань протягом року, 50% – ваговий коефіцієнт параметру, K – додатковий коефіцієнт. Додатковий коефіцієнт K вираховується за формулою

$K = C \div M$, де C – кількість сканувань за рік, M – середня кількість сканувань кожного сайту за час його існування.

Кінцева оцінка репутації є сумою оцінок її параметрів, тобто вираховується за формулою $O2 = T1 + T2$, процес отримання оцінок $T1$ та $T2$ описаний вище.

Оцінка активності													
	Місяць												
	Січень	Лютий	Березень	Квітень	Травень	Червень	Липень	Серпень	Вересень	Жовтень	Листопад	Грудень	
Кількість сканувань	1	0	27	20	3	1	3	1	0	8	1	1	
Мін. Сканувань	0												
Макс. Сканувань	27												
Сер. Відхилення	8,805989697												
Кількість сканувань	66												
Сканувань за всі роки	88												
			Параметр	Оцінка	Ваговий коефіцієнт	Додатковий ваг. Коef.	Зважена оцінка						
			Кількість сканувань	0,436507937	50,00%	100,00%	0,218253968						
			Стабільність сканувань	3,369261167	50,00%	8,73%	0,147070924						
										Оцінка активності		0,365324892	
												Середня кількість сканувань на сайт за час його існування	756

Рисунок 2.4 – Оцінка активності на прикладі сайту «windows10activation.ru»

Доступність

Доступність представляє собою оцінку доступності сайту у різних точках світу за даними ресурсу «DNS Checker», та вираховується за формулою $O3 = 5 - \frac{5}{A} \times V$, де 5 – загальна максимальна оцінка, A – кількість точок в яких сайт недоступних, V – загальна кількість точок в яких роботу сайту було перевірено.

Оцінка доступності	
Звіт DNS Checker	
Доступність	Кількість
Доступно у точках	33
Недоступно у точках	1
Загалом	34
Оцінка доступності:	4,852941176

Рисунок 2.5 – Оцінка доступності на прикладі сайту «windows10activation.ru»

Безпековий аспект

Оцінка безпекового аспекту відображає безпечність сайту з точки зору наявності вірусів та іншого шкідливого програмного забезпечення, та формується на основі звіту ресурсу Virus Total. Оцінка безпекового аспекту вираховується за наступною формулою: $O4 = \text{MAX}(5 - R * 1.5 - U * 1; 0)$, де $\text{MAX}()$ – функція що вибирає максимальне з декількох значень (в даному випадку використовується для недопускання виходу оцінки за межі [0; 5] балів), R – кількість спеціалізованих джерел Virus Total що позначили сканований сайт як шкідливий, 1.5 – штраф за кожен позначку «шкідливий», U – кількість спеціалізованих джерел Virus Total що позначили сканований сайт як підозрілий, 1 – штраф за кожен позначку «підозрілий».

Оцінка безпекового аспекту			
Звіт Virus Total		Оцінювання	
Рішення	Кількість	Рішення	Штраф
Безпечний	66	Безпечний	0
Шкідливий	10	Шкідливий	1,5
Підозрілий	1	Підозрілий	1
Кількість	77		
Оцінка безпекового аспекту			0

Рисунок 2.6 – Оцінка безпекового аспекту на прикладі сайту «windows10activation.ru»

Показник безпечності сайту

Показник безпечності сайту є оцінкою в межах від 0 до 5 балів, та формується на основі чотирьох вище розглянутих показників за наступною формулою: $O = O1 \times K1 + O2 \times K2 + O3 \times K3 + O4 \times K4$, де:

- $O1$ – Оцінка технічної репутації

- O2 – Оцінка активності
- O3 – Оцінка доступності
- O4 – Оцінка безпекового аспекту
- K1, K2, K3 та K4 – вагові коефіцієнти кожного з показників. Отримання цих коефіцієнтів буде описано нижче.

Вирахування вагових коефіцієнтів буде проходити за допомогою спеціальної матриці вагомості показників, що буде сформована в результаті наступних кроків: спочатку сформуємо саму матрицю та заповнимо її діагональ одиницями (Рисунок 2.2.4).

Назва параметру	Технічна репутація	Активність	Доступність	Безпековий аспект
Технічна репутація	1			
Активність		1		
Доступність			1	
Безпековий аспект				1

Рисунок 2.7 – Сформована матриця вагомості показників

Після формування матриці почнемо її заповнення за наступною методикою: порівнюємо за важливістю параметр ряду та параметр стовпцю та вписуємо у матриці відповідне значення: 0 – якщо параметр стовпцю важливіший за параметр ряду, 1 – якщо обидва параметри рівні, та 2 якщо параметр ряду важливіший.

Розглянемо на прикладі клітинки у першому ряду другого стовпця: тут параметром ряду буде «технічна репутація», а параметром стовпця буде «активність», і оскільки технічна репутація важливіша за активність, вписуємо у дану клітинку двійку. Відповідно у другому ряду першого стовпця вже буде порівнюватись «активність» в якості параметра ряду, і «технічна репутація» як параметр стовпцю, тому в цій клітині буде нуль, оскільки технічна репутація,

як ми раніше визначили, важливіша за активність. Результат заповнення перших клітинок зображено на рисунку 2.2.5.

Назва параметру	Технічна репутація	Активність	Доступність	Безпековий аспект
Технічна репутація	1	2		
Активність	0	1		
Доступність			1	
Безпековий аспект				1

Рисунок 2.8 – Заповнення перших клітинок матриці

Тепер за розглянутим прикладом заповнюємо матрицю вагомості показників. Отриману матрицю зображено на рисунку 2.2.6.

	Технічна репутація	Активність	Доступність	Безпековий аспект
Технічна репутація	1	2	2	0
Активність	0	1	0	0
Доступність	0	2	1	0
Безпековий аспект	2	2	2	1

Рисунок 2.9 – Отримана матриця вагомості показників

Тепер, після створення матриці вагомості показників, можемо перейти до обчислення самих показників. Кожен з показників вираховується за наступною формулою: $K = R \div S$, де R – сума відповідного ряду матриці, S – загальна кількість комірок матриці.

Розглянемо на прикладі обчислення коефіцієнту K_1 , показника «технічна репутація». Підставивши відповідні значення до формули отримаємо формулу наступного вигляду: $K_1 = (1 + 2 + 2 + 0) \div 16$, де (1, 2, 2, 0) – обчислення суми рядка матриці, а 16 – кількість комірок матриці.

Виконавши обчислення отримаємо $K1 = 0.31$, тобто ваговий коефіцієнт $K1$ становить 31%.

Обчисливши інші коефіцієнти за розглянутим прикладом отримаємо результат зображений на рисунку 2.2.7.

	Технічна репутація	Активність	Доступність	Безпековий аспект	Сумма по рядках	Вагові коефіцієнти	Позначка коефіцієнта
Технічна репутація	1	2	2	0	5	31%	K1
Активність	0	1	0	0	1	6%	K2
Доступність	0	2	1	0	3	19%	K3
Безпековий аспект	2	2	2	1	7	44%	K4
					16	100%	

Рисунок 2.10 – Створена матриця вагомості показників та відповідні коефіцієнти

Тепер, після визначення оцінок всіх показників та обчислення всіх вагових коефіцієнтів, можемо перейти до фінального етапу – обчислення показника безпечності сайту за розглянутою вище формулою $O = O1 \times K1 + O2 \times K2 + O3 \times K3 + O4 \times K4$. Підставляємо до формули необхідні значення: $O = 3.66666667 \times 31\% + 0,365324892 \times 6\% + 4,852941176 \times 19\% + 0 \times 44\%$. І після виконання обчислень отримуємо кінцевий результат – показник безпечності сайту, що для розглянутого в якості прикладу сайту «windows10activation.ru» становить 2.07 балів з 5.

Оцінка безпечності сайту "windows10activation.ru"			
Показник	Ваговий коефіцієнт	Оцінка	Зважена оцінка
Технічна репутація	31%	3,66666667	1,14583333
Активність	6%	0,36532489	0,02283281
Доступність	19%	4,85294118	0,90992647
Безпековий аспект	44%	0	0
Загальний показник безпечності сайту:			2,07859261

Рисунок 2.11 – Фінальний етап обчислень і отриманий показник безпечності розглянутого в якості прикладу сайту «windows10activation.ru».

Висновок до другого розділу

В цьому розділі було розроблено формалізацію моделі системи виявлення деструктивних впливів в соціальних інтернет сервісах та розроблено структуру системи виявлення деструктивних впливів в соціальних інтернет сервісах

Розділ 3. ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ВИЯВЛЕННЯ ДЕСТРУКТИВНИХ ВПЛИВІВ В СОЦІАЛЬНИХ ІНТЕРНЕТ СЕРВІСАХ

3.1. Інтерфейс системи виявлення деструктивних впливів в соціальних інтернет сервісах

Проектування інтерфейсу вкрай важливе, адже це основа, на яку в першу чергу буде звертати користувач. Було обрано легкі кольори, аби було приємно дивитись на дизайн сайту.

На рисунку 3.1 приведено загальний інтерфейс системи виявлення деструктивних впливів в соціальних інтернет сервісах;

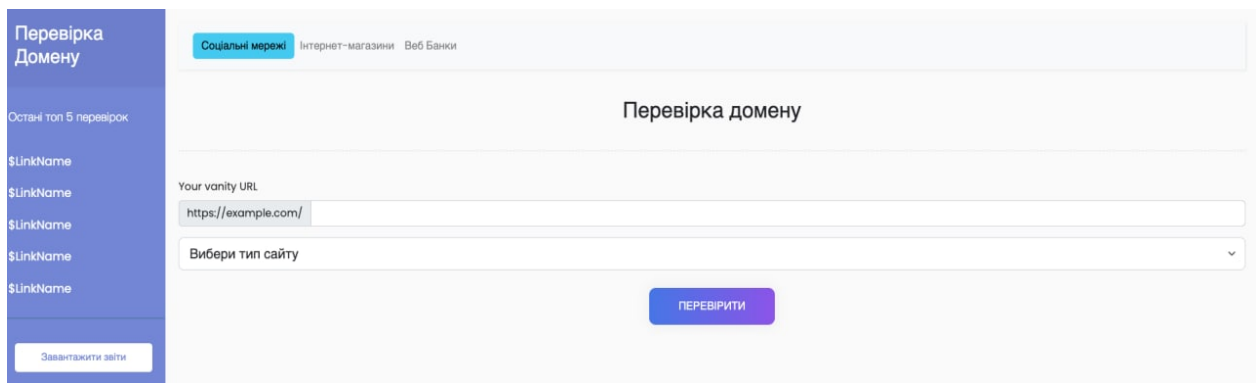


Рисунок 3.1 Загальний інтерфейс системи виявлення деструктивних впливів в соціальних інтернет-сервісах

Ви можете бачити що на сайті зображено топ 5 останніх перевірок, основний інтерфейс потребує від користувача посилання на інтернет сервіс в центрі сайту в полі – your vanity URL, також бажано обрати тип сайту і після цього натиснути перевірити. В процесі перевірки сайт буде провірено на коректність, аналізовано його SSL сертифікат, проаналізовано на віруси і тому подібне за допомогою звіту Virus Total, та в загальному аналіз домену, після перевірки буде виведено показник безпечності сайту.

На рисунку 3.2 було перевірено фейковий веб-сайт банку, наша система виявила небезпечність і надала користувачу цю інформацію. Також користувач може надіслати цю інформацію пошуковій системі GOOGLE, що допоможе іншим користувачам не стати жертвами фішингу.

Соціальні мережі
Інтернет-магазини
Веб Банки

Перевірка домену

Ваша URL-адреса

https://example.com/

Веб Банки
▼

ПЕРЕВІРИТИ

⚠ Обережно! Це посилання не має відношення до Приват Банку. Повідом про нього пошуковій платформі [GOOGLE](#). Так ти допоможеш іншим користувачам не стати жертвами фішингу.

Технічна Репутація	Активність	Доступність	Безпечний
1%	1%	1%	1%

Рисунок 3.2 – Перевірка фейкового веб-сайту

Висновок до третього розділу

В цьому розділі було реалізовано надано опис користувачу в користуванні системою деструктивних впливів в соціальних інтернет сервісах, логіку системи, де можна побачити функції які реалізуються в даній інформаційній системі .

ВИСНОВКИ ТА ПРОПОЗИЦІЇ

В процесі виконання кваліфікаційної роботи було створено та проаналізовано систему виявлення деструктивних впливів в соціальних інтернет-сервісах. Було проаналізовано інші приклади систем (наприклад avcheck.net, who.is), історію інформації домену , а також створено функціональні моделі IDEF0 та IDEF3, за допомогою яких можна зрозуміти в цілому систему, які виконуються під задачі, та як працює система і що з чого виходить. Також було спроектовано інтерфейс системи, а також розроблена математична модель системи, яка було реалізована завдяки програмному коду на мові PHP. Порівнюючи цю систему з іншими, що були наведені в 1 розділі, можна сміливо сказати що було чимало нововведень та кроків, що могли б зробити систему виявлення деструктивних впливів в соціальних інтернет-сервісах, краще та безпечніше.

Перелік літературних джерел

1. Електронний Підручник HTML. URL: <https://www.w3schools.com/html/default.asp>. Дата перегляду: (10.12.22)
2. Електронний Підручник CSS. Режим доступу: <https://www.w3schools.com/css/default.asp>. Дата перегляду: (10.12.22)
3. Електронний Підручник JS. URL: <https://www.w3schools.com/js/default.asp> - Дата перегляду: (10.12.22)
4. Електронний Підручник PHP. URL: <https://www.w3schools.com/php/default.asp> - Дата перегляду: (10.12.22)
5. Документація фреймворку CSS Bootstarap 5 URL: <https://getbootstrap.com/docs/5.0/getting-started/introduction/> - Дата перегляду: (10.12.22)
6. Методологія IDEF0 [Електронний ресурс]. URL: https://stud.com.ua/87184/ekonomika/metodologiya_idef0. - Дата перегляду: (10.12.22)
7. Методологія IDEF3 [Електронний ресурс]. URL: https://stud.com.ua/87186/ekonomika/metodologiya_idef3. - Дата перегляду: (10.12.22)
8. Превірка веб сайту на віруси. URL: <https://www.virustotal.com/gui/home/upload> . - Дата перегляду: (11.12.22)
9. Перевірка домену. URL: <https://who.is/> - Дата перегляду: (11.12.22)
10. Перевірка домену. URL: <https://thehost.ua/> - Дата перегляду: (11.12.22)
11. Методи запитів на сервер. URL: https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol - Дата перегляду: (12.12.22)
12. Перевірка DNS. URL: <https://dnschecker.org/> - Дата перегляду: (12.12.22)
13. Перевірка історії домену та наявності вірусів домену. URL: <https://archive.org/web/> - Дата перегляду: (12.12.22)

14. Глибовець М.М. Основи комп'ютерних алгоритмів / М.М. Глибовець – К.: Вид.дім «КМ Академія», 2003. – 452 с.
Караванова Т.П. Інформатика: методи побудови алгоритмів та їх аналіз: обчислювальні алгоритми / Т.П. Караванова – К.: Генеза, 2009. – 336 с.
15. Бродський Ю. Б., Молодецька К. В., Николук О. М. Системний аналіз в економіці : навч. посіб. Житомир : ЖНАЕУ, 2014. 175 с.
16. Аналіз методів виявлення деструктивних впливів в соціальних інтернет сервісах – [Електронний ресурс] - <https://drive.google.com/file/d/1qBxHc7bTla--u6FbuPtHKucXxggF18ro/view>
17. Поточний стан от технологій – [Електронний ресурс] - <https://sci-conf.com.ua/wp-content/uploads/2023/05/SCIENTIFIC-PROGRESS-INNOVATIONS-ACHIEVEMENTS-AND-PROSPECTS-1-3.05.2023.pdf>

ДОДАТКИ:


ДОДАТОК А:

```

<!doctype html> <html lang="en"> <head> <meta charset="utf-8"> <meta
name="viewport" content="width=device-width, initial-scale=1">
<title>1337-Scan</title> <link
href="https://cdn.jsdelivr.net/npm/bootstrap@5.2.3/dist/css/bootstrap.min.css
" rel="stylesheet" integrity="sha384-
rbsA2VBKQhggwzxH7pPCaAqO46MgnOM80zW1RWuH61DGLwZJEdK2
Kadq2F9CUG65" crossorigin="anonymous"> <link rel="icon"
type="image/x-icon" href="domain-trademark.png"> </head> <body> <div
class="wrapper"> <!-- Sidebar --> <nav id="sidebar"> <div class="sidebar-
header"> <h3>1337-Scan</h3> </div> <ul class="list-unstyled components">
<p>Остані топ 5 перевірок</p> <li> <a href="#">$LinkName</a> </li> <li>
<a href="#">$LinkName</a> </li> <li> <a href="#">$LinkName</a> </li>
<li> <a href="#">$LinkName</a> </li> <li> <a href="#">$LinkName</a>
</li> </ul> <ul class="list-unstyled CTAs"> <li> <a
href="https://bootstrapious.com/tutorial/files/sidebar.zip"
class="download">Завантажити звіти</a> </li> </ul> </nav> <!-- Page
Content --> <div id="content"> <nav class="navbar navbar-expand-lg
navbar-light bg-light"> <div class="container-fluid"> <button type="button"
id="sidebarCollapse" class="btn btn-info"> <i class="fas fa-align-left"></i>
<span>Соціальні мережі</span> </button> <button class="btn btn-dark d-
inline-block d-lg-none ml-auto" type="button" data-toggle="collapse" data-
target="#navbarSupportedContent" aria-
controls="navbarSupportedContent" aria-expanded="false" aria-
label="Toggle navigation"> <i class="fas fa-align-justify"></i> </button> <div
class="collapse navbar-collapse" id="navbarSupportedContent"> <ul
class="nav navbar-nav ml-auto"> <li class="nav-item active"> <a class="nav-
link" href="#">Інтернет-магазини</a> </li> <li class="nav-item"> <a
class="nav-link" href="#">Веб Банки</a> </li> </ul> </div> </div> </nav>
<h2 align="center">Перевірка домену </h2> <div class="line"></div> <label
for="basic-url" class="form-label">Ваша URL-адреса</label> <div
class="input-group mb-3"> <span class="input-group-text" id="basic-
addon3">https://example.com/</span> <input type="text" class="form-
control" id="basic-url" aria-describedby="basic-addon3"> </div> <select
class="form-select form-select-lg mb-3" aria-label=".form-select-lg example">
<option selected>Вибери тип сайту </option> <option value="1">Соціальні
мережі</option> <option value="2">Інтернет-магазини</option> <option
value="3">Веб Банки</option> <option value="3">Інше</option> </select>
<div class="btn_con" style="display: flex; justify-content:center;"> <button
class="btn-grad" type="submit">Перевірити</button> </div> <div
class="info_domen" align="center"> <p class="good"

```

```

style="color:#00bc8c;">Це посилання на 100% справжнє $website. </p> <!--
- Тут якщо гуд то гуд якщо не то не) --> <p class="no-good"
style="color:#dc3545;">  Обережно! Це посилання не має відношення до
$website. Повідом про нього пошуковій платформі <a
href="https://safebrowsing.google.com/safebrowsing/report_phish/?hl=ru%С
2%A0" style="text-decoration: underline;">GOOGLE</a>. Так ти
допоможеш іншим користувачам не стати жертвами фішингу.</p> </div>
<!-- Це вилазить после перевірки тіпа табл --> <section> <table class="table
table-dark"> <thead> <tr> <th>Технічна Репутація</th>
<th>Активність</th> <th>Доступність</th> <th>Безпековий</th> </tr>
</thead> <tbody> <tr> <td style="color:#00bc8c;">100%</td> <td
style="color:#00bc8c;">100%</td> <td style="color:#00bc8c;">100%</td>
<td style="color:#00bc8c;">100%</td> <!-- если все параша то тіпа 0% і
красний колір --> </tr> </tbody> </table> </section> </div> </div> <style> /*
DEMO STYLE */ @import
"https://fonts.googleapis.com/css?family=Poppins:300,400,500,600,700"; body
{ font-family: 'Poppins', sans-serif; background: #fafafa; } p { font-family:
'Poppins', sans-serif; font-size: 1.1em; font-weight: 300; line-height: 1.7em;
color: #999; } a, a:hover, a:focus { color: inherit; text-decoration: none;
transition: all 0.3s; } .navbar { padding: 15px 10px; background: #fff; border:
none; border-radius: 0; margin-bottom: 40px; box-shadow: 1px 1px 3px
rgba(0, 0, 0, 0.1); } .navbar-btn { box-shadow: none; outline: none !important;
border: none; } .line { width: 100%; height: 1px; border-bottom: 1px dashed
#ddd; margin: 40px 0; } /* ----- SIDEBAR
STYLE ----- */ .btn-grad { border: none;
cursor: pointer; background-image: linear-gradient(to right, #4776E6 0%,
#8E54E9 51%, #4776E6 100%); margin: 10px; padding: 15px 45px; text-align:
center; text-transform: uppercase; transition: 0.5s; background-size: 200%
auto; color: white; box-shadow: 0 0 20px #eee; border-radius: 10px; display:
block; } .btn-grad:hover { background-position: right center; /* change the
direction of the change here */ color: #fff; text-decoration: none; } .wrapper {
display: flex; width: 100%; align-items: stretch; } #sidebar { min-width: 250px;
max-width: 250px; background: #7386D5; color: #fff; transition: all 0.3s; }
#sidebar.active { margin-left: -250px; } #sidebar .sidebar-header { padding:
20px; background: #6d7fcc; } #sidebar ul.components { padding: 20px 0;
border-bottom: 1px solid #47748b; } #sidebar ul p { color: #fff; padding: 10px;
} #sidebar ul li a { padding: 10px; font-size: 1.1em; display: block; } #sidebar
ul li a:hover { color: #7386D5; background: #fff; } #sidebar ul li.active>a,
a[aria-expanded="true"] { color: #fff; background: #6d7fcc; } a[data-
toggle="collapse"] { position: relative; } .status { display: flex; justify-content:
center; align-items: center; width: 70px; height: 70px; background-color:

```