Міністерство освіти і науки України

Луцький національний технічний університет
(повне найменування закладу вищої освіти)

Факультет комп'ютерних та інформаційних технологій
(повне найменування факультету)

Кафедра комп'ютерної інженерії та кібербезпеки
(повне найменування кафедри)

КВАЛІФІКАЦІЙНА РОБОТА ЗА СТУПЕНЕМ ВИЩОЇ ОСВІТИ «БАКАЛАВР»

СИСТЕМА ЗАХИСТУ НА ОСНОВІ МОДЕЛІ CAPTCHA

PROTECTION SYSTEM BASED ON THE CAPTCHA MODEL

спеціальність 123 Комп'ютерна інженерія
(шифр і назва спеціальності)

освітня програма Комп'ютерна інженерія
(назва освітньої програми)

Виконав: здобувач вищої освіти
групи КІс-21
Чекан Максим Костянтинович

(підпис)

Керівник:
д.пед.н., професор
Чернящук Наталія Леонідівна

(підпис)

Кваліфікаційну роботу
допущено до захисту
« 17 » червня 2024 р.
Гарант освітньої програми:
к.т.н., доцент
Лавренчук Світлана Василівна

(підпис)

Луцьк – 2024 року

ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет *комп'ютерних та інформаційних технологій*
Кафедра *комп'ютерної інженерії та кібербезпеки*
Ступінь вищої освіти: *бакалавр*
Галузь знань: *12 Інформаційні технології*
Спеціальність: *123 Комп'ютерна інженерія*
Освітня програма: *«Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ проф. Н.Чернящук
« 10 » 01 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ВИЩОЇ ОСВІТИ

Чекану Максиму Костянтиновичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи *Система захисту на основі моделі CAPTCHA*

Керівник роботи *д.пед.н., професор Чернящук Наталія Леонідівна*

затверджені наказом закладу вищої освіти від «30» грудня 2023 року № 459/01-02
2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 11.06.2024р.

3. Вихідні дані до роботи *Джерелом розробки є науково-технічна література та публікації в періодичних виданнях з даного питання, опубліковані зарубіжні та вітчизняні роботи в даній області та різні інтернет-ресурси технічного спрямування*

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити):
Вступ
Особливості тестування безпеки веб-ресурсів
Характеристика експертних систем для розв'язування задач інформаційної безпеки
Програмна реалізація експертної системи тестування безпеки веб-ресурсів
Висновки

5. Перелік графічного (ілюстративного) матеріалу:
Існуючі рішення
Аналіз вразливостей та загроз безпеки веб-ресурсів
Алгоритми функціонування експертної системи

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис	
		завдання видав	завдання прийняв
Аналіз проблеми за темою роботи та постановка завдань дослідження	*Чернящук Н.Л., професор*		
Теоретичне дослідження та практична реалізація	*Чернящук Н.Л., професор*		
Практична реалізація об'єкта проектування	*Чернящук Н.Л., професор*		
Нормоконтроль	*Багнюк Н.В., доцент*		
Гарант ОП	*Лавренчук С.В., доцент*		
Показник запозичень тексту	***___%***		
Академічна доброчесність	*Міскевич О.І.,асистент*		

7. Дата видачі завдання 10.01.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	*Розділ 1. Огляд літератури із досліджуваної проблеми. Аналіз теоретичних основ систем захисту на основі моделі Captcha*	до 15.02.2024 р.	Виконано
2.	*Розділ 2. Методи в обхід захисту captcha*	до 15.03.2024 р.	Виконано
3.	*Розділ 3. Дослідження системи на основі моделі Captcha*	до 04.05.2024 р.	Виконано
4.	*Висновки та пропозиції*	до 07.05.2025 р.	Виконано
5.	*Формування списку використаних джерел*	до 10.05.2024 р.	Виконано
6.	*Формування додатків*	до 15.05.2024 р.	Виконано
7.	*Оформлення ілюстративного матеріалу*	до 20.05.2024 р.	Виконано
8.	*Нормоконтроль*	до 01.06.2024 р.	Виконано
9.	*Інструментальна перевірка на академічний плагіат*	до 04.06.2024 р	Виконано
10.	*Представлення кваліфікаційної роботи бакалавра до захисту*	до 11.06.2024 р.	Виконано

Здобувач вищої освіти _____ Чекан М.К.
(підпис) (прізвище, ініціали)

Керівник кваліфікаційної роботи _____ Чернящук Н.Л.
(підпис) (прізвище, ініціали)

АНОТАЦІЯ

Чекан М.К. Система захисту на основі моделі CAPTCHA. Рукопис.

Кваліфікаційна робота бакалавра ОП «Комп'ютерна інженерія» спеціальності 123 Комп'ютерна інженерія. Луцький національний технічний університет. Луцьк, 2024.

Кваліфікаційна робота складається з вступу, трьох розділів, висновків, списку використаних джерел, трьох додатків.

Мета роботи – дослідити систему захисту на основі моделі Captcha .

Об'єктом дослідження є система захисту на основі моделі Captcha.

Предметом дослідження є вразливості використання системи захисту на основі моделі Captcha.

Практичне значення. Результати роботи можуть бути використані для покращення стану захист інформаційних ресурсів від атак, які в свою чергу переслідують мету викрадення інформації користувача, зараження веб – ресурсу, автомат підбір паролів тощо.

Ключові слова: вразливості, кібербезпека, захист, атака.

ANNOTATION

Chekan M.K. Protection system based on the CAPTCHA model. Manuscript.

Bachelor's qualifying thesis of the OP «Computer Engineering» specialty 123 Computer Engineering. Lutsk National Technical University. Lutsk, 2024.

The qualification work consists of an introduction, three sections, conclusions, a list of used sources, and three appendices.

The purpose of the work is to investigate the protection system based on the Captcha model.

The object of the study is a protection system based on the Captcha model.

The subject of the study is the vulnerability of the use of the protection system based on the Captcha model.

Practical meaning. The results of the work can be used to improve the protection of information resources from attacks, which in turn pursue the goal of stealing user information, infecting a web resource, automatically selecting passwords, etc.

Keywords: vulnerabilities, cyber security, protection, attack.

Зміст

ВСТУП

Актуальність теми у сучасному контексті є надзвичайно високою через ключових факторів. З розвитком інтернету та інформаційних технологій значно збільшилась кількість кібератак, зокрема бот-атак. Зловмисники використовують ботів для автоматичного виконання шкідливих дій, таких як спам, розповсюдження шкідливого програмного забезпечення, здійснення DDoS-атак, і автоматизованого викрадення даних. CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) виступає як ефективний механізм для відокремлення дій людини від автоматичних ботів. Захист особистих даних стає все більш важливим у зв'язку з зростанням кількості онлайн-сервісів, які вимагають введення конфіденційної інформації. Використання CAPTCHA допомагає захистити форми для введення даних від автоматизованого збору інформації, тим самим підвищуючи загальний рівень безпеки особистих даних користувачів. Онлайн-сервіси, які впроваджують ефективні заходи безпеки, включаючи CAPTCHA, отримують більшу довіру з боку користувачів. Це особливо важливо для платформ, що надають фінансові, медичні та інші критично важливі послуги. Технології CAPTCHA постійно розвиваються, адаптуючись до нових викликів. Зокрема, впроваджуються нові типи CAPTCHA, такі як reCAPTCHA від Google, які є більш зручними для користувачів та водночас забезпечують високий рівень захисту. Дослідження та розробка нових методів CAPTCHA є актуальною темою для інформаційної безпеки. У деяких країнах законодавство вимагає впровадження ефективних заходів безпеки для захисту персональних даних. Використання CAPTCHA може допомогти відповідати цим вимогам і уникнути юридичних наслідків.

Метою цієї роботи є аналіз і розробка ефективної системи захисту на основі моделі CAPTCHA для підвищення рівня безпеки онлайн-сервісів від автоматизованих бот-атак і зловмисного програмного забезпечення. Для виконання поставленої мети потрібно виконати поставлені завдання:

– проаналізувати різні типи CAPTCHA;

– здійснити оцінку ефективності, зручності використання та стійкості до зловмисних атак кожної моделі;

– визначити ключові параметри, за якими можна оцінювати ефективність CAPTCHA;

– розробити нові та вдосконалити існуючі методи CAPTCHA, що забезпечують вищий рівень захисту і зручність для користувачів;

– інтеграція запропонованих методів у реальні веб-додатки для оцінки їх практичної ефективності;

– проведення тестування розроблених моделей CAPTCHA з метою оцінки їх стійкості до сучасних методів обходу;

– формулювання рекомендацій для розробників і адміністраторів вебсайтів щодо вибору і впровадження найбільш ефективних моделей CAPTCHA;

– розробка стратегій щодо постійного моніторингу і оновлення систем CAPTCHA у відповідь на нові загрози.

Об’єктом дослідження є система захисту, яка використовує модель CAPTCHA.

Предметом дослідження є характеристики системи захисту на основі моделі CAPTCHA.

Практичне значення системи захисту на основі моделі CAPTCHA полягає в їх здатності забезпечувати ефективний захист від різноманітних кібератак та забезпечувати безпеку та конфіденційність користувачів у віртуальному середовищі.

РОЗДІЛ 1 АНАЛІЗ ТЕОРЕТИЧНИХ ОСНОВ СИСТЕМИ ЗАХИСТУ НА ОСНОВІ МОДЕЛІ CAPTCHA

1.1 Характеристика моделі Captcha

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) – це спеціальна форма тестування, призначена для визначення, чи є користувач людиною чи комп'ютерною програмою. Зазвичай CAPTCHA використовується на веб – сайтах для захисту від автоматизованих атак, таких як спам – реєстрація облікових записів або надсилання небажаної пошти. Основна ідея CAPTCHA полягає в тому, щоб створити завдання, яке легко розпізнає людина, але важко розв'язується комп'ютерною програмою. Найпоширенішим прикладом є графічні CAPTCHA, де користувачу пропонується визначити символи на зображенні або ввести текст зображення, що перекривається зашумленим фоном.т Інші типи CAPTCHA можуть включати аудіо-перевірку, де користувачу пропонується визначити слова або фрази в аудіозаписі, або математичні завдання, такі як розв'язання простих рівнянь. CAPTCHA не є 100% надійним методом захисту, іноді вони можуть бути розв'язані штучним інтелектом або людьми, які працюють на фабриках «кліків». Однак вони все ще залишаються популярним і ефективним інструментом для захисту веб – ресурсів від ботів і автоматизованих атак. CAPTCHA, або «запити з повністю автоматизованої громадської випробування людини та комп'ютера», є інструментом, який використовується для відрізнення між людськими користувачами Інтернету та комп'ютерними програмами або «ботами». Це система перевірки, яка зазвичай використовується на веб – сайтах для запобігання автоматизованому спаму, атакам зламу або іншим видам зловживання. Основна ідея CAPTCHA полягає в тому, щоб представити користувачам завдання або випробування, які легко розв'язують люди, але важко для програм. Це може бути зображення тексту, який потрібно переписати, вибір зображень з певними об'єктами або ситуаціями, аудіофрагмент, який потрібно перекласти, або інші завдання.

Існують різні типи CAPTCHA, включаючи традиційні текстові, графічні, аудіо та навіть математичні варіанти. Недавні тенденції включають використання CAPTCHA, що базується на машинному навчанні, де система навчається розрізняти між людьми та ботами на основі їхньої поведінки та інших параметрів. Хоча CAPTCHA допомагає вберегти веб – сайти від зловживань, вона також може бути дещо незручною для користувачів, особливо якщо завдання складне або якщо зображення нечітке. Також виникає проблема доступності для людей з обмеженими можливостями, тому деякі розробники стараються створювати більш доступні альтернативи.

1.2 Приклади моделі Captcha

Існує кілька різновидів моделей захисту CAPTCHA, які використовуються для розрізнення між людьми та комп'ютерними програмами. Текстові CAPTCHA. Це один з найпоширеніших типів CAPTCHA, де користувачу пропонується переписати текст, зображений на зображенні. Зазвичай цей текст перевернутий, спотворений або зашифрований, щоб ускладнити розпізнавання для комп'ютерних програм. Графічні CAPTCHA. Замість тексту користувачеві пропонується вибрати певні об'єкти або картинки на зображенні. Наприклад, користувач може бути попросив виділити всі машини на картинці. Аудіо CAPTCHA. У цьому типі CAPTCHA користувачу пропонується послухати аудіофрагмент та перекласти його в текст. Часто аудіофрагменти спотворені, щоб ускладнити розпізнавання програмами. Математичні CAPTCHA. У цьому варіанті користувачу ставиться математичне завдання, яке потрібно розв'язати, наприклад, підрахувати суму або вирішити просте рівняння. Машинне навчання CAPTCHA. Останнім часом з'явилися CAPTCHA, що базуються на машинному навчанні. Вони аналізують поведінку користувачів і використовують алгоритми машинного навчання для визначення, чи є користувач реальною людиною чи програмою. Кожен з цих типів CAPTCHA має свої переваги та недоліки, і вибір

конкретної моделі може залежати від потреб конкретного веб – сайту або додатку, приклад CAPTCHA зображено на рисунку 1.1.

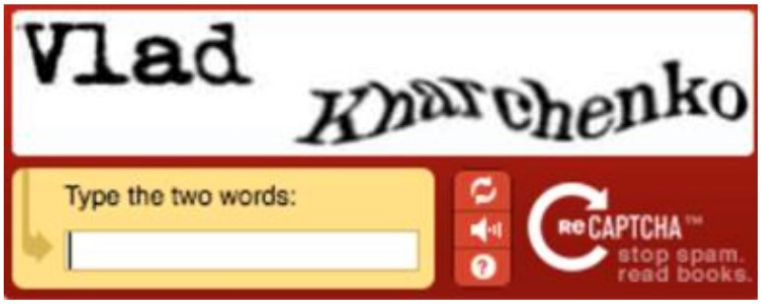


Рисунок 1.1 – Зображення Captcha [1]

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) – це інструмент захисту від автоматизованих програм, який вимагає від користувачів виконати завдання, яке легко для людини, але складне для комп'ютера. Існує кілька різновидів CAPTCHA, які використовуються для різних цілей та мають різні переваги і недоліки. Текстові CAPTCHA. Користувачеві пропонується ввести текст, зображений на зображенні, яке може бути перевернуте, спотворене або забарвлене. Такі CAPTCHA базуються на візуальному розрізненні між текстом і зображенням, що ускладнює автоматичний аналіз. Аудіо CAPTCHA. Користувачеві пропонується прослухати аудіозапис і ввести те, що він чує. Це особливо корисно для користувачів з обмеженими можливостями зору. Математичні CAPTCHA. Користувачеві пропонується вирішити просту математичну задачу, таку як додавання чисел або розв'язання простої математичної загадки. ReCAPTCHA. Розроблений компанією Google, ReCAPTCHA поєднує різні види CAPTCHA, такі як розпізнавання тексту та визначення образів, з метою перевірки користувача. Тривимірні CAPTCHA. Засновані на тривимірних об'єктах або візуальних ефектах, такі CAPTCHA створюють складніші завдання для розпізнавання автоматичними системами. Інтерактивні CAPTCHA.

Користувачеві пропонується взаємодіяти з об'єктом на екрані, наприклад, перетягуючи об'єкти або виконуючи інші дії, які важко автоматизувати. Ці

різновиди CAPTCHA можуть використовуватися окремо або в комбінаціях для забезпечення надійного рівня захисту від спаму та автоматизованих атак використання методів CAPTCHA зображено на рисунках 1.2, 1.5.

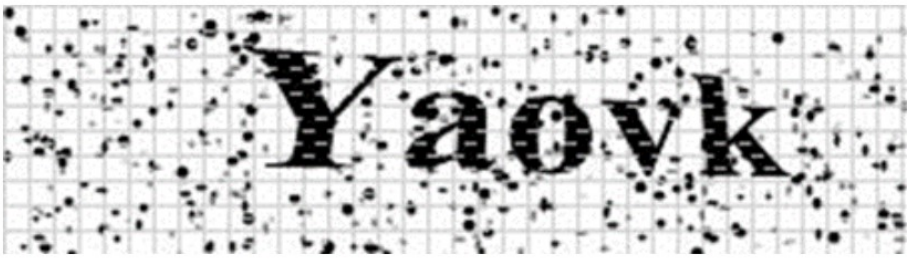


Рисунок 1.2 – Використання методів Captcha [2]

Рисунок 1.3 – Інші засоби [3]

Рисунок 1.4 – Зображення по горизонталі [4]

Рисунок 1.5 – Кольорова гама [5]

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) – це метод перевірки, розроблений для розрізнення між комп'ютерами і людьми. Існують різноманітні типи CAPTCHA, кожен з яких базується на різних принципах відокремлення людей від комп'ютерів. Ось деякі з найпоширеніших різновидів. Текстові CAPTCHA. Користувачам пропонується переписати текст з зображення, який має перекручений, розмитий або перевернутий шрифт. Зображення з вибором. Користувачам показуються зображення або частинки зображень, і їм потрібно вибрати всі зображення, що містять певний об'єкт або об'єкти (наприклад, всі зображення з автомобілями). Аудіо CAPTCHA. Користувачам пропонується прослухати аудіофайл і ввести слова або фрази, які вони чують. Математичні завдання. Користувачам пропонуються прості математичні завдання (наприклад, додавання або віднімання чисел), які вони повинні вирішити.т ReCAPTCHA. Розроблений Google, він використовується для вирішення складних завдань, таких як розпізнавання тексту на зображеннях або визначення об'єктів на зображеннях. Інтерактивні CAPTCHA. Користувачі повинні взаємодіяти з елементами на сторінці, наприклад, перетягуючи об'єкти або виконуючи дії, які доводять, що вони люди, а не комп'ютерні програми. Інші форми CAPTCHA. Іноді використовуються інші методи, такі як розпізнавання геометричних об'єктів, кольорів або знаків. Ці різновиди CAPTCHA призначені для ускладнення автоматизованого обходу систем безпеки та забезпечення того, що тільки люди можуть доступатися до веб – ресурсів.

1.3 Конфігурація безпеки

Основні типи вразливостей, які можуть використовуватися для атак на інформаційні системи, включають. SQL ін’єкція. Це атака, коли зловмисники використовують некоректно оброблені SQL запити для взяття контролю над базою даних або витягання конфіденційної інформації. Cross – Site Scripting (XSS). Зловмисники вбудовують скрипти у веб – сторінки, які потім виконуються в браузері користувача, що дозволяє їм виконувати різні дії на сторінці або крадіжку даних.

Cross – Site Request Forgery (CSRF). Зловмисники використовують авторизацію вже авторизованого користувача для виконання небажаних дій на стороні сервера веб – додатка. Несанкціонований доступ. Це включає в себе використання незаконно отриманих облікових даних для входу до системи або виконання дій, на які зловмисник не має права. Неправильна конфігурація безпеки. Недостатньо налаштовані параметри безпеки, такі як слабкі паролі, неправильна конфігурація файрволів або недостатнє оновлення програмного забезпечення, можуть призвести до вразливостей в системі. Небезпечні функції або API. Використання небезпечних функцій або API може відкрити двері для зловмисників, дозволяючи їм виконувати небажані дії або отримувати доступ до конфіденційної інформації. Фішинг. Це атака, коли зловмисники намагаються вивести користувачів з легітимних веб – сайтів, щоб вони відправляли конфіденційну інформацію, таку як паролі або номери кредитних карт, на фішингові сайти. Ці вразливості можуть бути використані зловмисниками для отримання несанкціонованого доступу до системи, крадіжки даних, розповсюдження шкідливого програмного забезпечення та інших шкідливих дій. Основні типи вразливостей, з якими можуть стикатися веб – додатки, включають.

SQL Injection (SQLI). Це атака, в результаті якої зловмисник використовує некоректно оброблені SQL запити, щоб отримати доступ до бази даних або виконати небажані операції.

Cross – Site Scripting (XSS). Зловмисники вбудовують скрипти в веб – сторінки, які потім виконуються на браузерах користувачів, що відкривають ці сторінки. Це може призвести до викрадення сесійних кукі або виконання інших шкідливих дій в контексті веб-сайту.

Cross – Site Request Forgery (CSRF). Це атака, при якій атакуючий змушує автентифікованого користувача виконати небажані дії на веб – сайті, який вони відвідують, шляхом відправки підробленого запиту. Атаки на сесії. Зловмисники можуть використовувати різні методи для перехоплення або підроблення сесійних ідентифікаторів користувачів, щоб набути несанкціонований доступ до їх облікових записів. Недостатність автентифікації та авторизації. Слабка аутентифікація (наприклад, використання простих паролів) або недостатній контроль доступу можуть призвести до несанкціонованого доступу до важливих ресурсів. Недостатнє валідація введення. Відсутність або неправильна валідація введення даних може дозволити атакуючим вводити шкідливі дані, що може призвести до виконання небажаних дій або витоку конфіденційної інформації.

Недостатнє керування конфіденційністю. Несанкціонований доступ до конфіденційної інформації через недостатні заходи безпеки або витік інформації може спричинити серйозні проблеми з безпекою. Ці вразливості можуть бути використані зловмисниками для здійснення різних видів атак, включаючи крадіжку даних, розповсюдження шкідливого програмного забезпечення або заволодіння контролем над веб – додатком. Для захисту від таких загроз важливо вживати відповідні заходи безпеки, такі як регулярне оновлення програмного забезпечення, використання сильних методів аутентифікації та авторизації, а також налагодження механізмів валідації введення та контролю доступу.

1.4 Методи Captcha

Метод поділу CAPTCHA на основі сегментації полягає в тому, що CAPTCHA зображення розбивається на декілька сегментів, кожен з яких містить окремий елемент або частину тексту, і користувачеві потрібно вказати, що зображено в кожному сегменті. Цей метод спрощує процес створення CAPTCHA та розпізнавання для користувачів, а також ускладнює спроби автоматизованого розпізнавання тексту за допомогою програм. Основні кроки використання методу поділу CAPTCHA на основі сегментації можуть включати таке. Розділення зображення. Початкове CAPTCHA зображення розбивається на декілька частин або сегментів. Це може бути зроблено шляхом використання методів обрізання, розділення або виділення областей інтересу на зображенні. Генерація підписів. Для кожного сегмента генерується відповідний підпис або мітка, що описує його вміст або елемент. Відображення користувачам. Зображення з сегментами і відповідними підписами відображається перед користувачем, який повинен вказати, що відображено в кожному сегменті, зазвичай за допомогою введення текстових відповідей.

Перевірка введення. Після того, як користувач введе свої відповіді, вони перевіряються на відповідність з правильними підписами кожного сегмента. Якщо відповіді коректні, CAPTCHA вважається успішною. Метод поділу CAPTCHA на основі сегментації дозволяє створювати складніші CAPTCHA, які важче розпізнати програмам, оскільки вони повинні виявити та відповісти на кілька окремих запитань або елементів. Він також може бути менш завадливим для користувачів, оскільки вони можуть бути більш простими у виконанні.

Метод поділу CAPTCHA на основі несегментації передбачає створення CAPTCHA, де текст або об’єкти розташовані безпосередньо на зображенні, але вони перетинаються або перекриваються один одним, ускладнюючи визначення тексту або об’єктів для автоматизованих програм. Основні кроки використання методу поділу CAPTCHA на основі несегментації можуть включати таке.

Створення несегментованого зображення. Спочатку створюється зображення, на якому розташований текст або об’єкти. Це може бути зображення з фоном, на якому випадковим чином розміщені символи або об’єкти, або зображення, де об’єкти перекривають один одного. Перетворення тексту або об’єктів. Текст або об’єкти можуть бути перетворені за допомогою різних ефектів, таких як розмиття, розмивання, згортання або розтягування, щоб ускладнити їх розпізнавання. Відображення перед користувачем. Зображення з несегментованим текстом або об’єктами відображається перед користувачем, який повинен виконати певну дію, щоб довести, що він людина, а не програма.

Перевірка відповіді користувача. Після того, як користувач виконає відповідну дію (наприклад, введе текст або виконає операцію з об’єктами), його відповідь перевіряється на правильність. Метод поділу CAPTCHA на основі несегментації може бути ефективним, оскільки ускладнює розпізнавання тексту або об’єктів для автоматизованих програм, які спробують розпізнати CAPTCHA. Він також може бути менш завадливим для користувачів, оскільки не потребує введення кількох окремих відповідей або взаємодії з різними елементами, ефективність злому CAPTCHA зображено на рисунку 1.6.

Scheme	Success rate		Running Time per Captcha (ms)
	Base Solver	Fine-tuned Solver	
Sohu	83%	92%	43.78
eBay	52%	86.6%	4.22
JD	60%	86%	43.18
Wikipedia	7%	78%	4.71
Microsoft	36.6%	69.6%	46.06
Alipay	23%	61%	3.75
Qihu360	48.6%	56%	3.10
Sina	40.6%	52.6%	42.81
Weibo	4.7%	44%	3.41
Baidu	6%	34%	41.57
Google	0%	3%	4.02

Рисунок 1.6 – Аналіз Captcha [5]

1.5 Використанням текстового типу Captcha

Генерація текстових CAPTCHA зазвичай включає наступні кроки. Вибір тексту. Спочатку потрібно вибрати текст, який буде використовуватися в CAPTCHA. Це може бути випадково згенерований рядок символів або слово, яке важко читати комп'ютеру, але може бути легко розпізнано людиною. Форматування тексту. Текст може бути перетворений за допомогою різних ефектів, таких як нахил, згортання, розмиття, перевертання або розтягування. Це допомагає ускладнити розпізнавання тексту для комп'ютерних програм. Додавання шуму. Для покращення стійкості CAPTCHA до розпізнавання програмних ботів може бути доданий шум або випадкові риси на зображенні. Це може включати випадкові лінії, точки або різні малюнки, які розміщуються на фоні тексту. Генерація зображення. Текстовий рядок, сформатований та змінений відповідно до потреб, вставляється на випадковому фоновому зображенні. Це зображення стає основою для CAPTCHA. Додавання логіки безпеки. В деяких випадках до CAPTCHA можуть бути додані додаткові заходи безпеки, такі як обмеження часу на введення відповіді або додаткові перевірки користувача, які допомагають запобігти атакам.

Виведення CAPTCHA. Згенерована CAPTCHA виводиться на веб – сторінці або в іншому контексті, де вона буде використовуватися, так щоб користувач міг її побачити і відповісти на неї. Ці кроки допомагають створити текстові CAPTCHA, які є ефективними ускладненнями для автоматизованого розпізнавання програмами, але в той же час достатньо читабельними для людей, які хочуть пройти перевірку. Обсяг інформації за останні роки зріс до неймовірних розмірів і від зростає щохвилини з шаленою швидкістю. З цього випливає, що перед людством гостро стоїть питання захисту Інтернет – ресурсів від шкідливих дій кіберзлочинці. У цьому розділі порушується питання захисту інформаційних ресурсів від атаки, що здійснюються спеціальним програмним

кодом, ім’я якого – бот. Атаки цілеспрямовані до збою сервера, зараження сайту рекламою, роздування голосів онлайн – голосування, створення облікових записів для неіснуючих користувачів тощо.

Захист від цих атак відіграє дуже важливу роль у кібербезпеці в загальному.

Інструмент, який допомагає запобігти успішній атаці, називається captcha. Це тест, який користувача просять пройти під час використання ресурс для перевірки того, хто виконує дії, людина чи комп’ютер. На сьогодні існує безліч реалізацій проходження тесту. У цій роботі буде уразливості використання цього тесту були розглянуті та певні експериментувати з використанням текстового типу captcha.

РОЗДІЛ 2 МЕТОДИ В ОБХІД ЗАХИСТУ CAPTCHA

2.1 Методи оптичного розпізнавання символів

Атаки на різні моделі CAPTCHA можуть включати різні методи, спрямовані на обхід захисту CAPTCHA і отримання доступу до системи або автоматизоване створення або відправлення небажаних повідомлень. Атака на текстову CAPTCHA може бути здійснена різними способами, включаючи. Методи оптичного розпізнавання символів (OCR). Зловмисники можуть використовувати програми OCR для автоматичного розпізнавання тексту на зображеннях CAPTCHA. Хоча деякі методи форматування тексту можуть бути ефективними ускладненнями для OCR програм, але деякі атакуючі можуть розробити вдосконалені алгоритми, щоб обійти ці заходи захисту. Машинне навчання. Зловмисники можуть використовувати методи машинного навчання для створення моделей, які можуть автоматично розпізнавати текст на зображеннях CAPTCHA. Вони можуть використовувати навчальні дані з раніше розпізнаними CAPTCHA, щоб покращити ефективність їх моделей. Соціальна інженерія. Замість технічних методів обхід захисту, атакуючі можуть спробувати переконати людей (наприклад, найманців) в ручному розв’язанні CAPTCHA за невелику плату або іншу вигоду. Це може бути ефективним методом, оскільки деякі CAPTCHA можуть бути складними для розпізнавання навіть для програм, але можуть бути вирішені швидко людьми. Атаки на алгоритми генерації. Зловмисники можуть аналізувати алгоритми генерації текстових CAPTCHA для виявлення слабких місць, які можуть бути використані для прогнозування або обхіду генерації CAPTCHA. Для захисту від атак на текстові CAPTCHA можна використовувати такі заходи, як. Використання складних ефектів форматування тексту, які ускладнюють розпізнавання символів програмами OCR.

Використання аудіо CAPTCHA як альтернативи для тих, хто має проблеми з розпізнаванням тексту на зображеннях. Періодичне оновлення алгоритмів

генерації CAPTCHA для ускладнення прогнозування або обходу. Використання додаткових перевірок, таких як рішення складних математичних завдань або взаємодія з користувачем на сторінці, що допомагає визначити, чи є користувач реальною людиною. Атака на текстову CAPTCHA може бути виконана різними способами, включаючи. OCR (Optical Character Recognition) атака. Зловмисники можуть використовувати програми розпізнавання оптичного тексту для автоматизованого розпізнавання символів на зображеннях текстової CAPTCHA. Ця атака ефективна лише в тих випадках, коли символи на CAPTCHA легко читаються, і не ефективна проти CAPTCHA з захистом від OCR. Машинне навчання. Зловмисники можуть використовувати алгоритми машинного навчання для створення моделей, які можуть розпізнавати символи на текстовій CAPTCHA з високою точністю. Вони можуть навчати модель на великому обсязі текстових CAPTCHA, щоб зробити її більш ефективною в розпізнаванні.

Атаки з використанням людей. Зловмисники можуть використовувати людей, які працюють за малу плату (наприклад, в масових веб – сервісах або через платформи мікророботи), щоб розгадати текстові CAPTCHA вручну. Ця атака може бути ефективною, особливо якщо CAPTCHA легко читаються. Атаки з перебору. Якщо CAPTCHA не має обмеження на кількість спроб, зловмисники можуть використовувати методи перебору, намагаючись відгадати символи шляхом спроб і помилок. Атаки з деніалу обслуговування (DoS). Атаки DoS можуть бути спрямовані на сервер, що генерує CAPTCHA, з метою перевантаження його і призведення до того, що сторінка з CAPTCHA стає недоступною для легітимних користувачів. Для захисту від атак на текстову CAPTCHA рекомендується використовувати додаткові заходи безпеки, такі як використання захисту від OCR, додавання шуму або спотворення тексту, обмеження часу вирішення CAPTCHA, а також моніторинг активності для виявлення атак. Також важливо регулярно оновлювати методи генерації CAPTCHA, щоб уникнути простих методів розпізнавання, які зображено на рисунку 2.1.

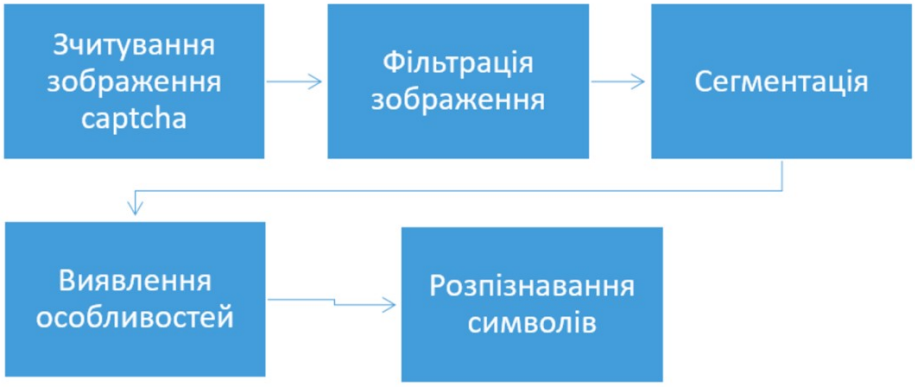


Рисунок 2.1 – Зчитування зображення Captcha

Атаки на різні моделі CAPTCHA можуть відрізнятися залежно від типу CAPTCHA. Одним з найпоширеніших типів CAPTCHA є текстова CAPTCHA, яка вимагає від користувача переписувати змішаний або перекручений текст. Ось деякі типи атак, які можуть бути спрямовані на текстову CAPTCHA. Методи оптичного розпізнавання символів (OCR). Зловмисники можуть використовувати програми для оптичного розпізнавання символів (OCR), щоб автоматично аналізувати та розпізнавати текст на CAPTCHA зображеннях. Хоча OCR може мати складнощі з розпізнанням викрученого або розмитого тексту, але з підходящою обробкою зображень вдалося отримати результат. Атаки з використанням масштабованих даних. Атакувачі можуть зібрати велику кількість CAPTCHA зображень, щоб тренувати свої моделі OCR на відповідних даних. З цим тренуванням, їхні моделі можуть стати досить ефективними в розпізнаванні текстової CAPTCHA.

Атакувачі можуть використовувати програми для перебору, які намагаються здійснити всі можливі комбінації символів, щоб знайти правильний варіант CAPTCHA. Це може бути виконано, якщо текст CAPTCHA складається з обмеженої кількості символів та обмеженого алфавіту.

Атаки з використанням людської праці. Зловмисники можуть використовувати платформи масової праці, такі як краудсорсингові майданчики, для найму людей, які будуть вирішувати CAPTCHA вручну. Це може бути ефективним, особливо для CAPTCHA, які важко розпізнати програмам, але легко

читаються людьми. Для захисту від атак на текстову CAPTCHA, важливо використовувати додаткові заходи безпеки, такі як розширення алфавіту символів, використання спеціальних ефектів (наприклад, шум, перекручення, розмиття), а також обмеження кількості спроб введення. Також можуть бути використані додаткові шари захисту, такі як аналіз поведінки користувача або використання CAPTCHA у поєднанні з іншими методами аутентифікації.

2.2 Розпізнавання тексту на зображенні

Атаки на CAPTCHA, засновані на зображеннях, можуть бути спрямовані на різні типи CAPTCHA, такі як вибір об’єктів на зображенні, перетягування об’єктів, розпізнавання тексту на зображенні тощо. Ось деякі типи атак, які можуть бути виконані на CAPTCHA заснованих на зображеннях. Методи оптичного розпізнавання символів (OCR). Атакувачі можуть використовувати програми OCR для автоматичного аналізу та розпізнавання символів на зображеннях CAPTCHA. Це може бути ефективним для CAPTCHA, які містять текст, який може бути легко розпізнаний. Атаки з використанням масштабованих даних. Зловмисники можуть зібрати велику кількість CAPTCHA зображень для тренування своїх моделей машинного навчання на відповідних даних. Це може зробити їхні моделі OCR більш ефективними в розпізнаванні об’єктів або тексту на зображеннях. Атаки з використанням обробки зображень. Атакувачі можуть використовувати різні методи обробки зображень, такі як фільтри, розмиття, згортання або інші техніки, щоб ускладнити розпізнавання CAPTCHA для OCR або інших програмних ботів.

Атаки з використанням глибокого навчання. Глибоке навчання може бути використане для розробки моделей, які можуть розпізнавати об’єкти або текст на зображеннях з високою точністю. Атакувачі можуть використовувати ці моделі для автоматичного розпізнавання CAPTCHA. Використання людської праці. Зловмисники можуть використовувати людей для вирішення CAPTCHA вручну через краудсорсингові платформи або інші методи. Це може бути ефективним для

CAPTCHA, які важко розпізнати програмам, але легко читаються людьми. Для захисту від атак на CAPTCHA заснованих на зображеннях, важливо використовувати додаткові заходи безпеки, такі як додавання шуму, розмиття або інших ефектів на зображення, вибір складного фону або контексту, а також використання анти – OCR методів. Також можуть бути використані додаткові шари захисту, такі як аналіз поведінки користувача або використання CAPTCHA у поєднанні з іншими методами аутентифікації.

Атаки на CAPTCHA, засновані на зображеннях, можуть бути спрямовані на різні типи CAPTCHA, такі як CAPTCHA з вибором об’єктів, CAPTCHA з перетягуванням об’єктів або CAPTCHA, які вимагають розпізнавання тексту або символів на зображеннях. Ось деякі типи атак, які можуть бути виконані на CAPTCHA заснованих на зображеннях. Методи оптичного розпізнавання символів (OCR). Зловмисники можуть використовувати програми для оптичного розпізнавання символів (OCR), щоб автоматично аналізувати та розпізнавати текст або об’єкти на зображеннях CAPTCHA. Хоча OCR може мати складнощі з розпізнанням змішаних або розмитих символів або об’єктів, але з вдосконаленням алгоритмів це може стати більш ефективним. Атаки з використанням масштабованих даних. Атакувачі можуть зібрати великий обсяг CAPTCHA зображень для тренування своїх моделей OCR на відповідних даних. З цим тренуванням, їхні моделі можуть стати досить ефективними в розпізнаванні об’єктів або символів на зображеннях. Атаки з використанням обробки зображень. Атакувачі можуть використовувати різні методи обробки зображень, такі як фільтри, розмиття, згортання або інші техніки, щоб ускладнити розпізнавання CAPTCHA для OCR або інших програмних ботів.

Атаки з використанням глибокого навчання. Глибоке навчання може бути використане для розробки моделей, які можуть розпізнавати об’єкти або символи на зображеннях з високою точністю. Атакувачі можуть використовувати ці моделі для автоматичного розпізнавання CAPTCHA. Використання людської праці. Зловмисники можуть використовувати людей для вирішення CAPTCHA вручну через краудсорсингові платформи або інші методи. Це може бути ефективним для

CAPTCHA, які важко розпізнати програмам, але легко читаються людьми. Для захисту від атак на CAPTCHA, заснованих на зображеннях, важливо використовувати додаткові заходи безпеки, такі як додавання шуму, розмиття або інших ефектів на зображення, вибір складного фону або контексту, а також використання анти – OCR методів. Також можуть бути використані додаткові шари захисту, такі як аналіз поведінки користувача або використання CAPTCHA у поєднанні з іншими методами аутентифікації.

2.3 Найпоширеніші системи Captcha

reCAPTCHA, розроблена компанією Google, є однією з найпоширеніших систем CAPTCHA. Вона використовує різні методи для перевірки людської активності, такі як введення тексту, вибір об’єктів або визначення об’єктів на зображеннях. Хоча reCAPTCHA вважається досить ефективною системою CAPTCHA, але вона також піддатна до деяких атак. Ось деякі з них. Атаки з використанням роботів. Зловмисники можуть використовувати роботів або програмне забезпечення для автоматизованого розв’язання reCAPTCHA. Це може бути виконано, наприклад, шляхом використання OCR для розпізнавання тексту або об’єктів на зображеннях, або шляхом вирішення завдань reCAPTCHA за допомогою автоматизованих скриптів. Атаки з використанням анти – CAPTCHA сервісів. Зловмисники можуть використовувати анти – CAPTCHA сервіси, де люди розв’язують CAPTCHA за плату. Це дозволяє їм ефективно обходити захист, оскільки розв’язання CAPTCHA виконується людьми, які працюють на сервісі. Атаки з використанням викрадення сесій. Інша можлива атака на reCAPTCHA полягає в зламі сесій користувача, щоб пройти перевірку CAPTCHA без фактичного розв’язання. Це може бути досягнуто, наприклад, шляхом перехоплення та використання сесійних куків або інших ідентифікаторів сесій. Атаки з використанням людської праці. Хоча reCAPTCHA спрямована на ускладнення автоматизованих атак, атакувачі все ж можуть використовувати

людську працю через анти – CAPTCHA сервіси або краудсорсингові платформи для розв'язання CAPTCHA.

Для захисту від таких атак, reCAPTCHA постійно оновлюється і вдосконалюється Google. Однак деякі методи, які можуть допомогти, включають удосконалення алгоритмів розпізнавання, використання додаткових завдань для перевірки людської активності, моніторинг поведінки користувачів та виявлення надмірної активності, імплементація механізмів захисту від викрадення сесій та обмеження доступу до анти – CAPTCHA сервісів. reCAPTCHA, розроблена Google, є однією з найпопулярніших систем CAPTCHA, і вона використовується для захисту від спаму та автоматизованих атак на веб – сайти. Однак, як і будь – яка інша система, вона також може стати об'єктом атак. Ось кілька можливих атак на reCAPTCHA. Атаки з використанням людської праці (CAPTCHA ферми). Атакувачі можуть використовувати людські праці для розв'язання reCAPTCHA великими масштабами. Вони можуть використовувати спеціалізовані сервіси або краудсорсингові платформи, де люди розв'язують CAPTCHA за невелику плату. Атаки з використанням маніпулювання поведінкою користувачів. Атакувачі можуть спробувати маніпулювати поведінкою користувачів, щоб змусити їх вирішувати reCAPTCHA. Наприклад, вони можуть створювати ситуації, де регулярні користувачі веб – сайту масово зіткнуться з CAPTCHA, що змусить їх вирішувати їх. Атаки з використанням перехоплення сесій (session hijacking). Атакувачі можуть намагатися перехопити сесійні куки користувачів, які вже проходили reCAPTCHA, і використовувати їх для вирішення інших CAPTCHA або виконання інших дій в контексті цих сесій.

Атаки з використанням інтеграції з ботами. Атакувачі можуть намагатися інтегрувати reCAPTCHA з програмними ботами, які намагатимуться автоматично розв'язувати CAPTCHA. Це може бути складним завданням через те, що reCAPTCHA постійно вдосконалюється для запобігання таким атакам.

Атаки з використанням інженерії зворотного введення (reverse engineering). Атакувачі можуть намагатися проаналізувати алгоритми reCAPTCHA та шукають уразливості в їх реалізації. Наприклад, вони можуть намагатися розпізнати

патерни, які використовуються для генерації CAPTCHA, і розробляти відповідні алгоритми для їх розв'язування. Щоб захистити себе від атак на reCAPTCHA, важливо використовувати всі можливі налаштування та оновлення, які надає Google. Також важливо використовувати додаткові заходи захисту, такі як обмеження кількості спроб введення CAPTCHA, аналіз поведінки користувачів і використання інших методів аутентифікації в додаток до reCAPTCHA.

reCAPTCHA – це одна з найпоширеніших систем CAPTCHA, яка використовується для визначення, чи є користувач людиною чи ботом. Ця система має декілька варіантів, включаючи текстові CAPTCHA, CAPTCHA з вибором об'єктів, а також інші форми взаємодії, наприклад, вибір квадратів з вмістом. Хоча reCAPTCHA має високий рівень захисту, вона не є неуразливою до атак. Ось деякі можливі атаки, які можуть бути спрямовані на модель reCAPTCHA. Атаки з використанням OCR. Атакувачі можуть спробувати використати програмні засоби для оптичного розпізнавання символів (OCR) для автоматичного розпізнавання текстових CAPTCHA. Вони можуть збирати велику кількість CAPTCHA, які потім будуть використані для тренування моделей OCR. Це може стати проблемою для рекапчи, яка використовує текстові варіанти. Атаки з використанням обробки зображень. Атакувачі можуть намагатися використати різні методи обробки зображень, такі як фільтри або ефекти, щоб ускладнити розпізнавання об'єктів на CAPTCHA. Це може включати додавання шуму або зміни контрасту, які можуть зробити розпізнавання важким для програмних алгоритмів.

Використання людської праці. Атакувачі можуть використовувати людей для вирішення CAPTCHA вручну через краудсорсингові платформи або інші методи. Це може бути ефективним, особливо для складних CAPTCHA, які важко розпізнати програмам, але легко читаються людьми. Атаки з використанням збиткових обчислювальних ресурсів. Атакувачі можуть використовувати ботнети або інші методи для розподілу завдань з розв'язання CAPTCHA між багатьма комп'ютерами. Це може дозволити їм збільшити шанси на успішне розв'язання CAPTCHA шляхом використання більшої кількості обчислювальних ресурсів.

Для захисту від таких атак, reCAPTCHA використовує різноманітні методи, такі як аналіз поведінки користувача, використання анти – OCR методів, додавання шуму або інших ефектів на зображення, а також використання різних типів CAPTCHA, які важко розпізнати програмам. Також важливо постійно вдосконалювати систему захисту, оскільки атакувачі можуть намагатися розвивати нові методи атак.

2.4 Динамічні Captcha

Динамічні CAPTCHA – це системи CAPTCHA, які змінюються в часі або в залежності від взаємодії з користувачем, з метою підвищення рівня захищеності від автоматизованих атак. Ось деякі методи підвищення стану захищеності, які можуть бути використані в динамічних CAPTCHA. Змінність формату CAPTCHA. Динамічні CAPTCHA можуть змінювати свій формат час від часу або залежно від кожного конкретного запиту. Наприклад, вони можуть варіювати кількість символів, типи об’єктів або взагалі змінювати свою структуру. Часові обмеження. Динамічні CAPTCHA можуть використовувати часові обмеження для вирішення. Наприклад, користувач може мати обмежений час для введення відповіді на CAPTCHA. Це може ускладнити атаки, які спробують вирішити CAPTCHA шляхом перебору. Адаптивність. Динамічні CAPTCHA можуть адаптуватися до рівня складності в залежності від спостережного поведінки користувача. Наприклад, якщо система спостерігає, що користувач має труднощі з вирішенням CAPTCHA, вона може зменшити його складність для подальших запитів.

Використання мультимедійних елементів. Динамічні CAPTCHA можуть включати мультимедійні елементи, такі як анімації або відео, які можуть бути важкі для автоматизованих програм розпізнати або імітувати. Взаємодія з користувачем. Динамічні CAPTCHA можуть вимагати від користувача виконання певних дій або вирішення завдань, які важко або неможливо автоматизувати. Наприклад, вони можуть вимагати перетягування об’єктів, виконання графічних

завдань або взаємодії з елементами на сторінці. Ці методи можуть бути використані для створення динамічних CAPTCHA, які є більш ефективними у захисті від автоматизованих атак порівняно з статичними CAPTCHA. Однак, важливо також зберігати баланс між безпекою та зручністю для користувачів, щоб не ускладнити процес аутентифікації до неприйнятного рівня, CAPTCHA гра на зіставлені фігури зі своїм силуетом зображено на рисунку 2.2.

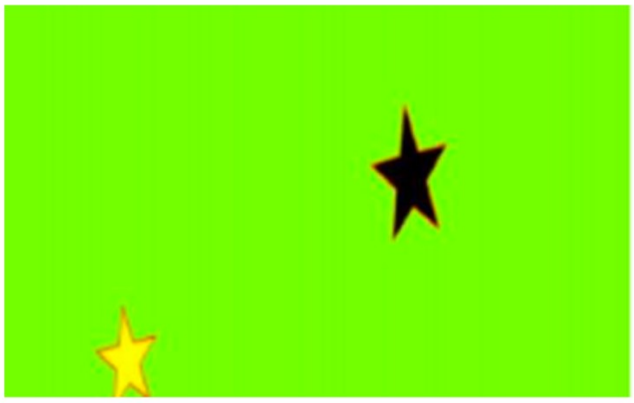


Рисунок 2.2 – Динамічна Captcha [6]

Використання довірених USB – ключів для підвищення рівня захисту в Інтернеті є одним із способів двофакторної аутентифікації та забезпечення безпеки вашого облікового запису. Ось як це працює та як це може підвищити стан безпеки. Двофакторна аутентифікація. Крім звичайного пароля, який ви вводите, вам потрібно мати фізичний USB – ключ, щоб підтвердити свою особу. Це називається двофакторною аутентифікацією, оскільки для входу в обліковий запис потрібно два фактори – щось, що ви знаєте (пароль) і щось, що ви маєте (USB – ключ). Фізичний доступ. Оскільки USB – ключ є фізичним пристроєм, зловмисникам важко здійснити віддалені атаки на ваш обліковий запис. Навіть якщо хтось зламає ваш пароль, вони все одно повинні мати фізичний доступ до вашого USB – ключа для доступу до облікового запису. Шифрування та безпека. Деякі USB – ключі мають вбудовані заходи безпеки, такі як апаратне шифрування або захист паролем. Це додатково захищає ваші дані, навіть якщо ключ втрачений або вкрадений.

Зручність. Використання USB – ключа може бути зручним, оскільки вам просто потрібно підключити його до комп’ютера або пристрою для підтвердження вашої особи. Це може бути особливо зручно в порівнянні з іншими методами двофакторної аутентифікації, такими як одноразові паролі або програми аутентифікації.

Щоб забезпечити максимальний рівень безпеки, важливо дотримуватися кращих практик безпеки, таких як використання сильних паролів, оновлення програмного забезпечення та встановлення антивірусного програмного забезпечення. Також слід мати на увазі, що якщо ви втратите свій USB – ключ або він буде скомпрометований, вам слід якнайшвидше змінити всі паролі та вжити заходів для відновлення безпеки вашого облікового запису, приклад USB – ключів зображено на рисунку 2.3.

Рисунок 2.3 – Криптографічній токен [6]

Під час аналізу вразливостей різних моделей капчі виявлено велику кількість кількість недоліків у кожному з представлених видів. При вивченні літератури було отримано знання про варіанти використання слабких місць captcha для проведення успішної атаки на систему. Розглянуто основну проблему використання капчі, а саме створення тесту Turing, який може бути стійким до вирішення ботом і простим у роботі людський прохід. Аналіз запропонував нові способи рішення представленої проблеми. Одним з них є використання динамічної капчі, боту важко вирішити через рухливі частини, але людині це буде цікаво тим, що тестування проходить в ігровій формі.

Інший варіант для підвищення стійкості до атак є використання спеціальних USB – ключів, за допомогою якого перевірка буде проведена за лічені секунди і з мінімальними зусилля.

РОЗДІЛ 3 ДОСЛІДЖЕННЯ СИСТЕМИ НА ОСНОВІ МОДЕЛІ CAPTCHA

3.1 Організація дослідної частини

Проведення практичного дослідження CAPTCHA може бути корисним з кількох причин. Оцінка ефективності. Дослідження може допомогти в оцінці того, наскільки ефективні різні види CAPTCHA в захисті від автоматизованих атак. Це може включати в себе оцінку того, які методи атаки (наприклад, застосування OCR або машинного навчання) найефективніше подолують різні типи CAPTCHA. Оцінка стійкості до атак. Дослідження може допомогти в оцінці того, наскільки стійкі різні типи CAPTCHA до різних видів атак. Це може включати в себе аналіз того, які CAPTCHA легше піддаються атакам через перебір, а також які CAPTCHA важко підробити з використанням машинного навчання або інших методів. Оцінка зручності для користувачів. Дослідження може допомогти в оцінці того, наскільки зручно користувачам використовувати різні типи CAPTCHA. Деякі типи CAPTCHA можуть бути важкими для вирішення людиною, що може призвести до погіршення користувацького досвіду. Пошук нових підходів. Дослідження може допомогти в пошуку нових підходів до створення CAPTCHA, які були б як ефективними в захисті від атак, так і зручними для користувачів. Наприклад, дослідження може включати розробку та оцінку нових методів CAPTCHA на основі різних типів викликів для користувачів.

Отже, проведення практичного дослідження CAPTCHA може допомогти в поліпшенні та вдосконаленні системи захисту в Інтернеті, забезпечуючи більшу безпеку для користувачів та веб-сайтів зображено на рисунку 3.1.

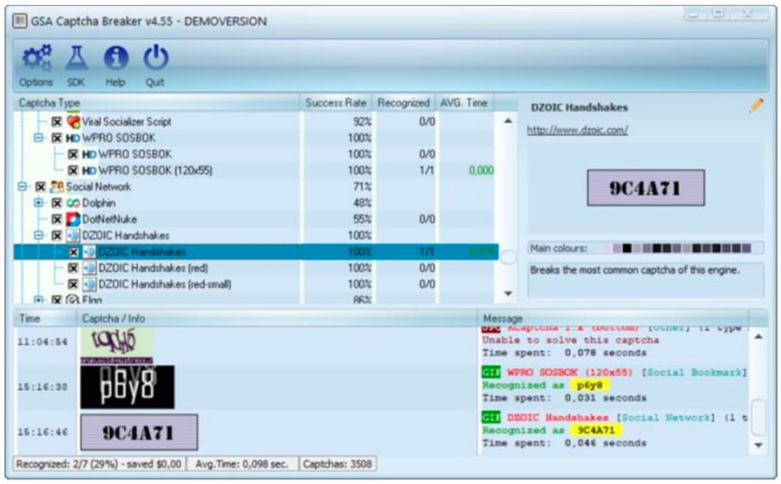


Рисунок 3.1 – Типи CAPTCHA

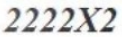
Проведення практичного дослідження CAPTCHA може бути корисним з кількох причин. Оцінка ефективності захисту. Дослідження може допомогти визначити, наскільки ефективно різні типи CAPTCHA захищають від автоматизованих атак. Це може включати аналіз того, як швидко та точно атаки можуть розпізнати CAPTCHA, а також які методи атак є найбільш успішними. Оцінка користувацького досвіду. Дослідження може допомогти визначити, як користувачі сприймають різні типи CAPTCHA. Перевірка нових технологій. Дослідження може допомогти в оцінці нових методів CAPTCHA або покращених версій існуючих методів. Результати дослідження можуть бути використані для розробки рекомендацій щодо вибору та використання CAPTCHA для захисту веб – ресурсів. Обгрунтування для проведення дослідження може включати потребу в покращенні безпеки веб – ресурсів, розумінні та вдосконаленні користувацького досвіду, а також потребу в оцінці нових технологій та методів аутентифікації.

3.2 Методи захисту Captcha

GSA Captcha Breaker – це програма, яка автоматично розпізнає і вирішує різні типи CAPTCHA, включаючи текстові, числові та інші складні CAPTCHA. Ця програма використовується для автоматизованого обхіду CAPTCHA на веб – сайтах, що дозволяє зловмисникам створювати програми, які автоматично пройдуть через захист CAPTCHA. Використання GSA Captcha Breaker або аналогічних програм для зламу CAPTCHA може бути незаконним та порушувати політику безпеки веб – сайтів. Така діяльність може призвести до небезпеки для веб – сайтів та їх користувачів, зокрема, зловмисники можуть отримати несанкціонований доступ до конфіденційної інформації, поширити шкідливі програми або здійснити інші злочинні дії. З метою захисту веб – сайтів від таких атак, важливо використовувати надійні та ефективні методи захисту CAPTCHA, а також здійснювати моніторинг активності на веб – сайті для виявлення потенційно шкідливої діяльності. Також важливо встановлювати програмне забезпечення для виявлення та запобігання атакам, такі як системи виявлення вторгнень (IDS) або використання сервісів захисту веб – застосунків (WAF).

Результати злому різних моделей текстової captcha подано в таблиці 3.1.

Таблиця 3.1 – Характеристики Captcha

№	Зображення	Відсоток успіху	Швидкість розв'язання
1		100%	0.02 с
2		100%	0.32 с
3		98%	0.31 с
4		18%	0.47 с
5		4%	0.39 с
6		1%	0.86 с

GSA Captcha Breaker – це програмне забезпечення, яке використовується для автоматичного розпізнавання і розв'язання CAPTCHA. Воно використовує різноманітні методи, включаючи оптичне розпізнавання символів (OCR), для автоматичного розв'язання CAPTCHA без участі людини. За допомогою GSA Captcha Breaker, зловмисники можуть намагатися атакувати системи, які використовують CAPTCHA для захисту від автоматизованих атак. Вони можуть програмувати це програмне забезпечення таким чином, щоб воно автоматично аналізувало та розв'язувало CAPTCHA, що дозволяє їм обхідати захист і отримувати доступ до захищених веб – ресурсів. Важливо зазначити, що використання програм для розпізнавання CAPTCHA для злому систем захисту є недозволеним та порушує правила використання веб – ресурсів. Такі дії можуть мати серйозні юридичні наслідки, включаючи штрафи та судові позови. Також, це може завдати шкоди репутації та довірість до особи або організації, яка здійснює такі дії.

Для захисту від атак, заснованих на використанні програм для розпізнавання CAPTCHA, важливо використовувати найновіші методи захисту, такі як розв’язання CAPTCHA, які важко розпізнати програмам, використання двофакторної аутентифікації та інші методи безпеки. Також, важливо постійно вдосконалювати захист вашого веб – сайту або системи, щоб запобігти злому та несанкціонованому доступу.

Соціальний експеримент із проходженням тесту Тьюрінга може бути цікавим та інформативним дослідженням взаємодії між людьми та штучним інтелектом. Ось кілька етапів, які можуть бути включені до такого експерименту. Підготовка тесту. Спочатку потрібно розробити тест Тьюрінга, який включає запитання та завдання, які допоможуть визначити, чи може штучний інтелект імітувати розмову з реальною людиною. Тест може включати запитання з різних областей знань, завдання для вирішення проблем та ситуацій, які вимагають розуміння та логічного мислення. Залучення учасників. Для проведення експерименту потрібно залучити як можна більше учасників. Це можуть бути як індивідуальні користувачі, так і групи людей. Проходження тесту. Учасники проходять тест Тьюрінга, відповідаючи на запитання та виконуючи завдання, які ставить штучний інтелект. Під час проходження тесту може бути важливо спостерігати за реакцією учасників, їхнім ставленням до інтеракції з системою та загальними враженнями. Це може включати оцінку того, наскільки ефективно штучний інтелект імітує розмову з реальною людиною, реакцію учасників на інтеракцію, а також будь – які інші відомості, які можуть бути корисними для розуміння взаємодії між людьми та штучним інтелектом. На основі аналізу результатів формулюються висновки та висновки щодо ефективності тесту Тьюрінга, взаємодії між учасниками та штучним інтелектом, а також можливих перспектив використання таких систем у майбутньому. Цей соціальний експеримент може бути корисним для розуміння впливу штучного інтелекту на суспільство, взаємодії між людьми та машинами та майбутнього розвитку технологій штучного інтелекту.

На рисунку 3.2 представлено білет 1 Captcha, який було запропоновано розв’язати користувачу.

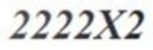


Рисунок 3.2 – Білет 1 Captcha

На рисунку 3.3 можна побачити варіанти відповідей білет 1.

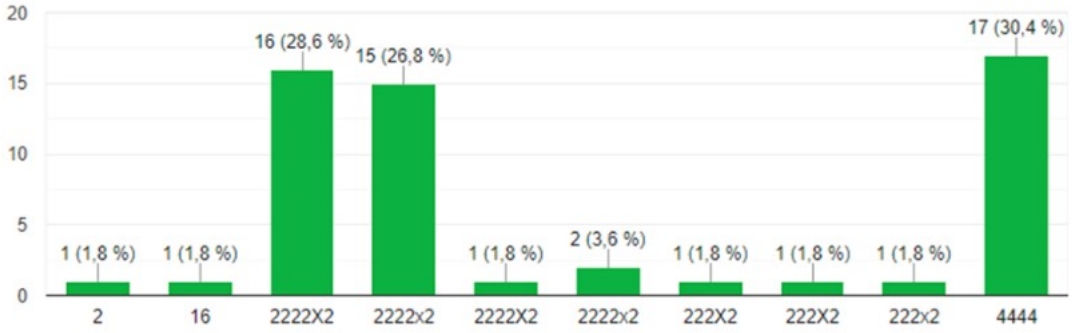


Рисунок 3.3 – Схема відповідей білету 1

Кількість витрачених секунд секунд під час проходження білету 1 (рис. 3.4).

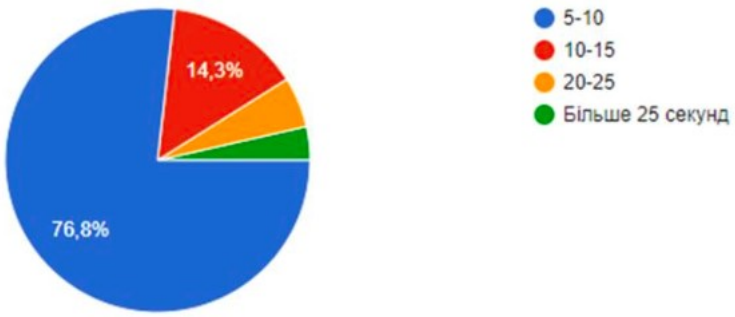


Рисунок 3.4 – Час затрачений на білет 1

Всі учасники експерименту розуміють свої права і добровільно згоджуються взяти участь. Важливо, щоб не було ніяких примусових дій або

порушень приватності. Доцільність. Переконайтеся, що ваш експеримент має конкретну мету або дослідницьке питання, яке ви хочете вивчити. Наприклад, ви можете бажати дослідити, наскільки ефективно люди можуть взаємодіяти з штучним інтелектом або як вони реагують на те, що їхні співрозмовники є машинами. Безпека даних. Зберігайте дані про учасників експерименту конфіденційно та захищено. Пам’ятайте, що це особисті дані, і ви маєте відповідальність за їхню безпеку. Аналіз результатів. Після завершення експерименту аналізуйте отримані дані та робіть висновки. Це дозволить вам зрозуміти реакції учасників і здійснити висновки щодо вашого дослідницького питання. Дозвіл і регуляторні вимоги. Впевніться, що ваш експеримент відповідає всім законодавчим і регуляторним вимогам, що можуть стосуватися дослідження з людьми або збору особистої інформації. Загалом, соціальні експерименти з проходженням тесту Тьюрінга можуть бути важливими для розуміння взаємодії між людьми та машинами, але вони повинні бути проведені з увагою до етичних та безпечних аспектів.

На рисунку 3.5 представлено білет 2 captcha, який було запропоновано розв’язати користувачу.

Рисунок 3.5 – Білет 1 captcha

На рисунку 3.6 можна побачити варіанти відповідей білет 2.

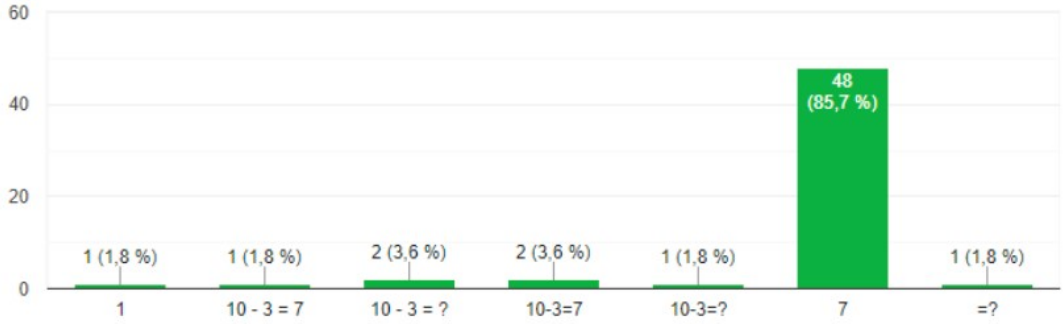


Рисунок 3.6 – Дані білет 2

Час проходження білет 2 (рис. 3.7).

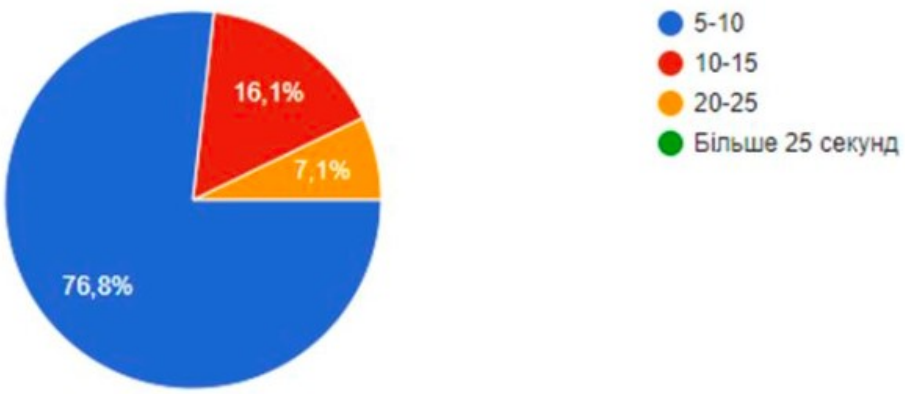


Рисунок 3.7 – Час затрачений білет 2

На рисунку 3.8 представлено білет 3 captcha.

Рисунок 3.8 – Білет 3 captcha

На рисунку 3.9 можна побачити варіанти відповідей білету 3.

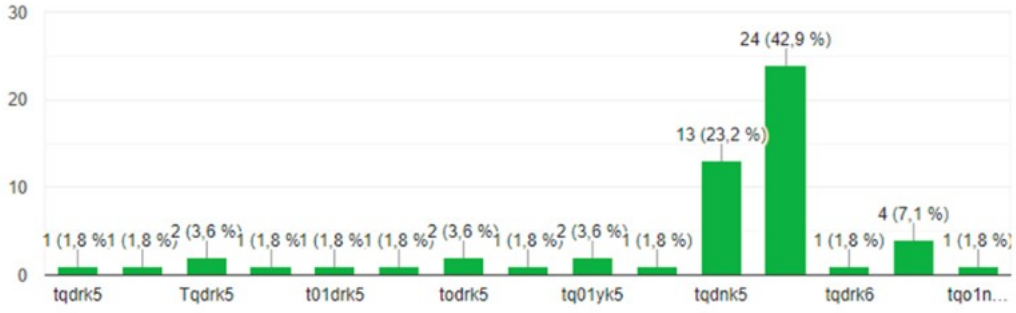


Рисунок 3.9 – Дані білету 3

Час під час проходження білету 3 (рис. 3.10).

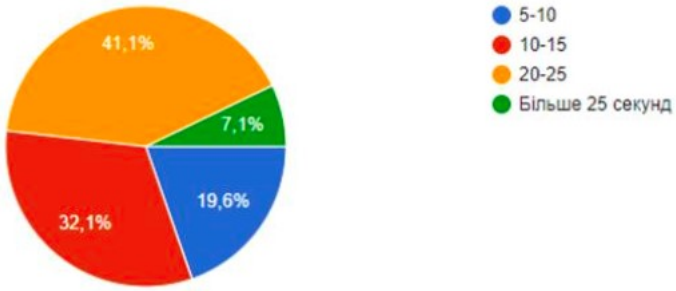


Рисунок 3.10 – Час затрачений згідно білету 3

Дана модель captcha отримала найбільший резонанс серед людей, які проходили тест.

На рисунку 3.11 представлено білет 4 Captcha.

Рисунок 3.11 – Білет 4 Captcha

На рисунку 3.12 можна побачити варіанти відповідей білету 4.

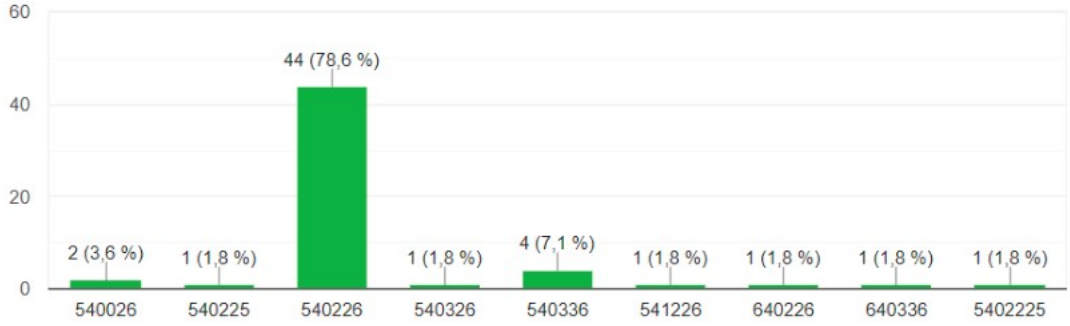


Рисунок 3.12 – Дані білету 4

Кількість витрачених секунд під час проходження білету 4 зображено на рисунку 3.13.

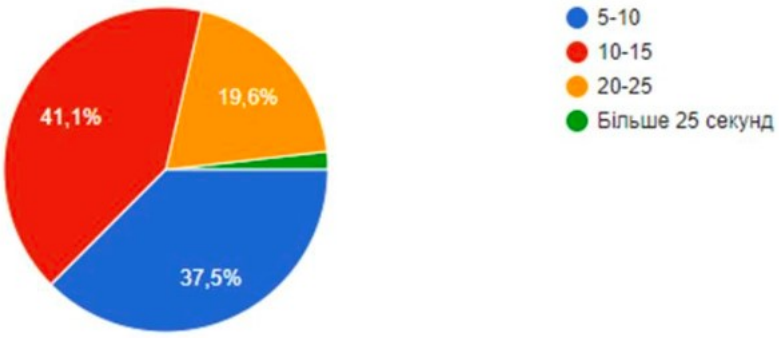


Рисунок 3.13 – Час затрачений білет 4

Схожа ситуацію можна поміти і дивлячись на останній тест. Користувачі так само надали велику кількість подібних варіантів, проте відсоток правильної відповіді більший ніж у попередньому тесту (таблиця 3.5).

В якості останнього питання респондентам потрібно було вирішити який саме тест виявився для них найскладнішим зображено на рисунку 3.14.

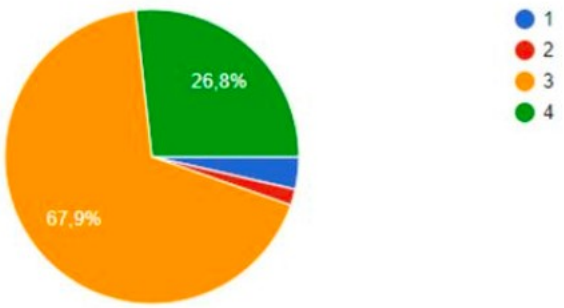


Рисунок 3.14 – Рівні складності

Як видно на рисунку 3.14, це найскладніше для користувачів тест виявився третім, за нього проголосували 67,9% користувачів. На другому місці респонденти обрали останній тест, 26,8% вважають саме цей тест Модель captcha є найскладнішою. У цій роботі продемонструвати, як використання різних моделей captcha досліджувалися в два етапи. Перший був проведення експериментів зі злому обраних зображень captcha за допомогоюспеціальне програмне забезпечення та проведення соціологічного опитування. При виконанні практичної частини виявлено закономірність щодо використання допоміжних елементів захисту від кібератак, таких як оверлейт персонажі один на один, використання шумного фону та інші недолікит призводить до зниження шансів успішного вирішення тесту програмним методом. А аналіз проводився з іншого боку, зі сторони користувача. За результатами, яка дійшла висновку, що використання складної капчі для бота є прямим пропорційно складності розв’язання тесту людиною.

ВИСНОВКИ

В даній кваліфікаційній роботі проаналізовані різні типи CAPTCHA, система захисту на основі моделі CAPTCHA є ефективним інструментом для відрізнення людей від комп'ютерних програм, таких як боти, на веб-сайтах і онлайн-платформах. Вона допомагає запобігти спаму, злому акаунтів, видаленню даних та іншим видам атак, що можуть виникнути в інтернетсередовищі.

Здійснено оцінку ефективності, зручності використання та стійкості до зловмисних атак кожної моделі інтеграція CAPTCHA забезпечує додатковий шар захисту, вимагаючи від користувачів виконати завдання, яке складно або неможливо автоматизувати. Завдяки поєднанню технологій, таких як штучний інтелект та машинне навчання, CAPTCHA стає все більш складною для обхіду та надійною в захисті від різних видів атак.

Визначені ключові параметри, за якими можна оцінювати ефективність CAPTCHA, розроблені нові та вдосконалені існуючі методи CAPTCHA, що забезпечують вищий рівень захисту і зручність для користувачів.

Проведено тестування розроблених моделей CAPTCHA з метою оцінки їх стійкості до сучасних методів обходу, незважаючи на свою ефективність, важливо забезпечити, щоб CAPTCHA не ускладнювала взаємодію з реальними користувачами. Це означає розробку завдань, які можуть бути легко вирішені людиною, але складні для програмного забезпечення, а також мінімізацію кількості CAPTCHA, які потрібно вирішити користувачам під час їх взаємодії з веб-сайтами.

Розроблена стратегія щодо постійного моніторингу і оновлення систем CAPTCHA у відповідь на нові загрози система захисту на основі моделі CAPTCHA є важливим елементом для забезпечення безпеки в Інтернеті, допомагаючи уникнути автоматизованих атак та зберегти інтернет-ресурси від небажаних втручань.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Named Entity Recognition PhD Study Report, University of West Bohemia in Pilsen. URL: https://hantek.com.ua/at7328 (дата звернення: 10.02.2024).

2. A survey of named entity recognition and classification. URL: https://hantek.com.ua/sds1022 (дата звернення: 10.02.2024).

3. NLP (Natural Language Processing) Tutorial. URL: https://bitkit.com.ua/shho-take-arduino (дата звернення: 10.02.2024).

4. NLP CORE. URL: https://sxema.com.ua/ua/p799237784-arduino-nanov30.html (дата звернення: 10.02.2024).

5. Text Summarization using NLTK: TF-IDF Algorithm. URL: https://itmaster.biz.ua/electronics/arduino/arduino-ide.html (дата звернення: 10.02.2024).

6. Brief Introduction to Neural Networks. URL: https://www.hamlab.net/mcu/training/proteus.html (дата звернення: 10.02.2024).

7. A Complete Guide To Artificial Neural Network In Machine Learning: https://radio-detaly.com/oscilografi-vidi-ta-tipi (дата звернення: 10.02.2024).

8. How neural networks work. URL: https://geekmatic.in.ua/ua/arduino_osnovyi_programmirovaniya (дата звернення: 10.02.2024).

9. Understanding Activation Functions in Neural Networks. URL: https://arduinka.biz.ua/blok-zhivlennya-9v-1a-p297c75.html (дата звернення: 10.02.2024).

10. Neural networks versus Logistic regression for 30 days all-cause readmission prediction. URL: https://en.wikipedia.org/wiki/ATmega328 (дата звернення: 10.02.2024).

11. Deep Learning for NLP. URL: https://vencon.ua/ua/articles/kak-vybratbatarejku-ili-akkumulyator-vybiraem-batarejki-akkumulyatornye-i-obychnye (дата звернення: 10.02.2024).

12. Word2vec Made Easy. URL : https://www.hwlibre.com/uk/tft/ (дата звернення: 10.02.2024).

13. How is GloVe different from word2vec? URL: https://electronica.in.ua/ua/p1630184399-ostsilograf-dso-shell.html (дата звернення: 10.02.2024).

14. What are the advantages and disadvantages of Word2vec and GloVe? URL : https://uk.fmuser.net/content/?11010.html (дата звернення: 10.02.2024).

15. How is GloVe different from word2vec?. URL : https://www.guru99.com/uk/analog-vs-digital.html (дата звернення: 10.02.2024).

16. Distributed Representations of Words and Phrases and their Compositionality. Головна | Elib LNTU. URL : https://elib.lntu.edu.ua/sites/default/files/elib_upload/ipv/page10.html (дата звернення: 10.02.2024).

17. Word2Vec Tutorial Part I: The Skip-Gram Model. URL : https://radioshop.com.ua/uk/osnovni-parametry-ostsylohrafiv (дата звернення: 10.02.2024).

18. Electronics for Beginners: A Practical Introduction to Schematics, Circuits, and Microcontrollers. O'Reilly Online Learning. URL: https://www.oreilly.com/library/view/electronics-for-beginners/9781484259795/ (date of access: 10.02.2024).

19. ABCs of Electronics: An Easy Guide to Electronics Engineering. O'Reilly Online Learning. URL: https://www.oreilly.com/library/view/abcs-ofelectronics/9798868801341/ (date of access: 10.02.2024).

20. Circuit Design and Simulation Quick Start Guide: Create Schematics and Layout Electronic Components. URL: https://www.oreilly.com/library/view/circuitdesign-and/9781484295823/ (date of access: 10.02.2024).

21. PCB Design for Absolute Beginners: Layout Printed Circuit Boards in a Web Browser. URL: https://www.oreilly.com/library/view/pcb-designfor/9781484280409/ (date of access: 10.02.2024).

Applications, 2019. International Conference on,Sivakasi, Tamil Nadu. 2019, vol. 4, no. pp. 54-58.

22. Practical Electronic Design for Experimenters. URL: https://www.oreilly.com/library/view/practical-electronic-design/9781260456165/ (date of access: 10.02.2024).

23. DIY Microcontroller Projects for Hobbyists. URL: https://www.oreilly.com/library/view/diy-microcontroller-projects/9781800564138/ (date of access: 10.02.2024).