№ 2(43) 2025
НАУКА і ТЕХНІКА СЬОГОДНІ
серії: право, економіка, педагогіка, техніка, фізико-математичні науки

УДК 004.5

https://doi.org/10.52058/2786-6025-2025-2(43)-1519-1527

Рутц Станіслав Вікторович аспірант УДУНТ, м. Дніпро, https://orcid.org/0009-0007-1000-3642

Чернецький Євгеній Вячеславович к.т.н., доцент кафедри КІТ та А УДУНТ, м. Дніпро, https://orcid.org/0000-0002-4197-7171

АЛГОРИТМИ ВЗАЄМОДІЇ КОРИСТУВАЧІВ ІЗ СУЧАСНИМИ CAPTCHA

Анотація. Стаття є дослідженням сучасних методів розпізнавання користувачів на основі технологій CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart). Зосереджено увагу як на класичних текстових завданнях, так і на інноваційних рішеннях, що використовують інтерактивні чи біометричні підходи до перевірки автентичності. Окреслено основні виклики, пов'язані з тим, що сучасні алгоритми машинного навчання та штучного інтелекту здатні успішно долати традиційні CAPTCHA, які раніше вважалися надійними. У статті проаналізовано ефективність різних типів CAPTCHA, зокрема текстових, графічних, аудіо та інтерактивних, а також визначено вплив рівня складності завдань на зручність для користувачів. Значну увагу приділено викликам у сфері доступності, враховуючи потреби людей із порушеннями зору та інших особливих категорій користувачів. Обґрунтовано перспективні напрями оптимізації CAPTCHA, спрямовані на підвищення безпеки та мінімізацію незручностей під час проходження перевірок. Окремо розглянуто важливість урахування поведінкових характеристик, які можуть підвищувати динамічність перевірок і складність їх автоматизованого обходу. Аналіз руху курсора, швидкості й послідовності кліків, а також унікальних патернів введення тексту дає змогу точніше ідентифікувати реальних користувачів і відрізнити їх від ботів, що імітують людські дії. Розглянуто також біометричні CAPTCHA, що ґрунтуються на розпізнаванні голосу, обличчя чи відбитків пальців. Ці методи створюють додаткові бар'єри для зловмисників, але одночасно викликають дискусії щодо приватності й безпеки персональних даних. Висвітлено приклади впровадження адаптивних CAPTCHA, які динамічно змінюють рівень складності залежно від поведінки користувача, а також ідеї використання технологій блокчейну для формування децентралізованих механізмів захисту. Показано, що поєднання різних форм CAPTCHA та інноваційних підходів до їх побудови може значно ускладнити роботу автоматизованих ботів і знизити

кількість хибних спрацьовувань. Зрештою, результати дослідження підкреслюють необхідність комплексного розгляду аспектів зручності, безпеки та конфіденційності під час розроблення CAPTCHA, адже лише збалансований підхід сприятиме підвищенню захищеності цифрового середовища й водночас враховуватиме потреби користувачів із різними можливостями та пристроями.

Ключові слова: CAPTCHA, розпізнавання користувачів, штучний інтелект, машинне навчання, верифікація користувачів, інформаційна безпека.

Stanislav Rutts Ukrainian State University of Science and Technologies, Dnipro, https://orcid.org/0009-0007-1000-3642

Chernetskyi Ievgenii Ukrainian State University of Science and Technologies, Dnipro, https://orcid.org/0000-0002-4197-7171

RESEARCH ON USER RECOGNITION METHODS USING MODERN CAPTCHA TECHNOLOGIES

Abstract. The article investigates modern user recognition methods based on CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) technology. It focuses on both classic text-based tasks and innovative solutions that employ interactive or biometric approaches to authentication. The main challenges are outlined, particularly regarding the fact that contemporary machine learning and artificial intelligence algorithms can successfully overcome traditional CAPTCHAs once considered reliable. The article analyzes the effectiveness of various CAPTCHA types, including text, graphical, audio, and interactive versions, and also determines how task complexity affects user convenience. Special attention is paid to accessibility issues, taking into account the needs of visually impaired users and other special user categories. The paper substantiates promising directions for optimizing CAPTCHA to enhance security and reduce inconvenience during the verification process. The importance of considering behavioral characteristics, which can increase the dynamic nature of these checks and complicate automated bypass, is examined separately. Analyzing cursor movement, click speed and sequences, as well as unique text-entry patterns, enables more accurate identification of real users and differentiation from bots that mimic human actions. Biometric CAPTCHAs based on voice, facial, or fingerprint recognition are also considered. While these methods introduce additional barriers for attackers, they simultaneously raise concerns about privacy and the security of personal data. Examples of implementing adaptive CAPTCHAs are presented, which dynamically adjust complexity based on user behavior, along with ideas for using blockchain technology to establish decentralized protection mechanisms. It is shown that combining different forms of CAPTCHA and innovative approaches to

their design can significantly complicate automated bot operations and reduce false positives. Ultimately, the findings emphasize the need for a holistic consideration of convenience, security, and confidentiality when developing CAPTCHA, as only a balanced approach will foster greater protection of the digital environment while simultaneously meeting the needs of users with diverse abilities and devices.

Keywords: CAPTCHA, user recognition, artificial intelligence, machine learning, user verification, information security.

Постановка проблеми. Сучасний розвиток інформаційних технологій та активне поширення цифрових послуг зумовлюють необхідність забезпечення надійного розпізнавання користувачів у мережі Інтернет. Одним із ключових інструментів для боротьби зі зловмисниками та автоматизованими ботами є CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) – технологія, що дозволяє відрізнити дії реальної людини від автоматизованих програм. Однак у сучасних умовах ефективність традиційних CAPTCHA значно знижується через стрімкий розвиток штучного інтелекту та алгоритмів машинного навчання, які здатні швидко аналізувати й вирішувати завдання, призначені для перевірки користувачів.

Згідно зі статистичними даними, більшість вебсайтів, що працюють у сфері електронної комерції, соціальних медіа та онлайн-банкінгу, впроваджують CAPTCHA для захисту від автоматизованих атак та зловживань. Проте сучасні дослідження демонструють, що класичні текстові або графічні CAPTCHA вже не є ефективними на 100%, оскільки штучний інтелект здатен розпізнавати текстові коди зі швидкістю та точністю, що перевищують людські можливості.

Отже, проблема оптимізації CAPTCHA є актуальною з точки зору як інформаційної безпеки, так і зручності користувачів. Дослідження у цій сфері повинні зосереджуватися на розробці ефективних, але водночас доступних методів автентифікації, здатних протистояти новітнім технологіям автоматичного розпізнавання. У зв’язку з цим виникає необхідність системного аналізу сучасних методів CAPTCHA, їхніх переваг і недоліків, а також перспектив впровадження інноваційних рішень для підвищення ефективності розпізнавання користувачів.

Аналіз останніх досліджень і публікацій. Останні роки дослідження у сфері CAPTCHA спрямовані на розробку більш стійких методів розпізнавання користувачів, які здатні протистояти автоматизованим атакам ботів. Серед наукових робіт, присвячених цій тематиці, значну увагу приділено аналізу ефективності традиційних та інноваційних методів CAPTCHA, а також їхньому вдосконаленню з урахуванням сучасних загроз.

Традиційні текстові CAPTCHA є найпоширенішими завдяки простоті реалізації. У своїх дослідженнях Мітра та інші дослідники зазначають, що

текстові CAPTCHA вразливі до атак за допомогою алгоритмів оптичного розпізнавання символів (OCR), особливо у поєднанні з сучасними нейронними мережами. Автори наголошують, що навіть ускладнення текстових завдань шляхом додавання шуму чи спотворень не завжди дає бажаний результат, оскільки сучасні алгоритми навчання легко адаптуються до подібних перешкод [1 с. 218].

У роботах Ву та Чень було проведено дослідження графічних CAPTCHA, зокрема завдань на розпізнавання об'єктів на зображеннях. Автори дійшли висновку, що такі методи є ефективнішими у боротьбі з ботами порівняно з текстовими CAPTCHA. Проте з розвитком глибокого навчання та технологій комп'ютерного зору (наприклад, алгоритми YOLO та Faster R-CNN) точність автоматичного вирішення графічних завдань значно зросла, що знижує їхню ефективність у довгостроковій перспективі [2 с. 114].

Варто відзначити дослідження Сатіш та інші дослідники, розглядаються інтерактивні CAPTCHA, які включають завдання на виконання певних дій: перетягування елементів, вибір правильних об'єктів або вирішення логічних задач. Ці методи демонструють кращу стійкість до атак, проте їхнє впровадження може викликати незручності для користувачів, особливо на мобільних пристроях чи при повільному інтернет-з'єднанні [4 с. 181].

Окрему увагу заслуговують дослідження біометричних CAPTCHA, які використовують унікальні особливості людини, такі як голос, відбитки пальців або поведінкові фактори (рух миші, динаміка натискання клавіш). За даними роботи Тана та Лі (2023), такі методи мають потенціал для підвищення рівня безпеки, але вони також викликають питання щодо конфіденційності даних користувачів і потребують значних обчислювальних ресурсів для реалізації [5 с. 49].

Таким чином, сучасні дослідження демонструють, що жоден із методів CAPTCHA не є універсальним. У той час як текстові CAPTCHA залишаються популярними завдяки простоті, інноваційні підходи, такі як інтерактивні завдання та біометричні методи, поступово стають необхідністю для протидії сучасним загрозам. Подальші дослідження повинні бути спрямовані на пошук балансу між рівнем безпеки, зручністю для користувачів і ресурсними витратами на впровадження новітніх технологій.

Мета статті – проаналізувати та оцінити сучасні методи розпізнавання користувачів за допомогою технологій CAPTCHA, а також визначення перспектив їхнього розвитку в умовах інтенсивного прогресу штучного інтелекту та машинного навчання.

Об'єкт дослідження – системи автентифікації користувачів у цифровому середовищі.

Предмет дослідження – методи та технології CAPTCHA, їхні алгоритми реалізації, ефективність і стійкість до автоматизованих атак.

Виклад основного матеріалу. Ідея відокремлення дій людини від автоматизованих програм бере свій початок на початку 2000-х років, коли стрімке зростання кількості ботів та автоматизованих атак створило реальну загрозу для безпеки вебресурсів. Одним із перших значних кроків у цьому напрямі стало впровадження тесту Turing-a, адаптованого для автоматичного середовища.

Термін CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) був запропонований дослідниками з Університету Карнегі-Меллона у 2003 році – Луїсом фон Аном, Мануелем Блюмом, Ніколасом Хоппером та Джоном Ленгфордом. Головною метою першого CAPTCHA було перевірити здатність користувача розпізнавати спотворений текст, що неможливо для алгоритмів тогочасного рівня. Прості текстові CAPTCHA стали масово використовуватися для:

- захисту від спаму при реєстрації електронної пошти;
- обмеження автоматичних публікацій на форумах та блогах;
- захисту від автоматизованих атак на системи онлайн-голосувань [7].

На початкових етапах впровадження класичні текстові CAPTCHA вважалися надійними, оскільки програми не мали ефективних інструментів для обробки спотворених зображень тексту. Проте вже у 2010-х роках, зі зростанням потужності алгоритмів оптичного розпізнавання символів (OCR) та розвитком нейронних мереж, ефективність таких CAPTCHA почала знижуватися.

У відповідь на ці виклики з'явилися нові типи CAPTCHA:

- графічна CAPTCHA – завдання на розпізнавання об’єктів на зображеннях. Наприклад, користувачам пропонувалося обрати всі зображення з пішохідними переходами або транспортними засобами. Вони були впроваджені компанією Google через reCAPTCHA.
- словесна задача – прості логічні завдання або математичні приклади (скільки буде 2+3?).
- аудіо CAPTCHA – розроблені для користувачів із порушеннями зору, але вони швидко стали вразливими для програм аудіорозпізнавання.
- інтерактивна CAPTCHA – завдання, що потребують виконання певної дії: перетягування об’єктів мишею, натискання на визначені області екрана чи вирішення невеликих логічних задач [10].

Згодом **Google reCAPTCHA v2** стало одним із найпопулярніших рішень, що використовує комбінацію графічних та поведінкових факторів. Його еволюція призвела до **reCAPTCHA v3,** що працює у фоновому режимі та аналізує поведінку користувача для визначення, чи є він людиною.

На сучасному етапі історія розвитку CAPTCHA демонструє, що кожен етап еволюції технології супроводжувався постійною гонкою між розробниками методів захисту та новітніми інструментами для їх обходу, зокрема на основі **глибокого навчання** та **штучного інтелекту.**

З розвитком цифрових технологій та штучного інтелекту (AI) традиційні методи CAPTCHA почали втрачати свою ефективність, адже автоматизовані системи навчилися розпізнавати спотворений текст, аналізувати зображення та навіть вирішувати логічні задачі. Глибокі нейронні мережі та алгоритми комп'ютерного зору, такі як OCR та CNN, дозволяють автоматизованим ботам з легкістю обходити текстові та графічні CAPTCHA, які раніше вважалися надійними. У той же час збільшення складності завдань CAPTCHA призводить до зниження зручності для користувачів, особливо на мобільних пристроях або в умовах повільного інтернет-з'єднання.

Сучасні CAPTCHA також стикаються з проблемою доступності для людей із особливими потребами. Аудіо CAPTCHA, які є альтернативою для людей із вадами зору, стають вразливими до розпізнавання голосу за допомогою спеціалізованих програм. Крім того, використання біометричних CAPTCHA, що базуються на голосі, відбитках пальців або поведінкових характеристиках, викликає занепокоєння щодо конфіденційності даних користувачів. Подібні системи вимагають значних обчислювальних ресурсів, що може ускладнити їхнє масове впровадження [3].

Для вирішення цих викликів сучасні розробники CAPTCHA зосереджуються на створенні динамічних і адаптивних систем, які аналізують поведінку користувача в реальному часі. Наприклад, Google reCAPTCHA v3 працює у фоновому режимі, оцінюючи ймовірність того, що дії виконуються людиною, і мінімізуючи необхідність активної взаємодії з CAPTCHA. Іншим перспективним напрямком є CAPTCHA на основі штучного інтелекту, які використовують семантичний аналіз тексту або зображень. Такі задачі складно автоматизувати, але вони є зрозумілими для людини.

Ще одним інноваційним підходом є інтерактивні та ігрові CAPTCHA, які пропонують користувачам виконати цікаві завдання, наприклад, зібрати пазл або провести об'єкт через лабіринт. Це не лише ускладнює автоматизацію злому, але й підвищує рівень залучення користувачів. Водночас технології блокчейну починають застосовуватися для створення унікальних ключів перевірки, що додає додатковий рівень захисту від атак. Таким чином, розвиток CAPTCHA орієнтується на пошук балансу між безпекою, доступністю та комфортом для користувачів, створюючи нові рішення, які враховують виклики сучасного цифрового світу [9].

Сучасні рішення для удосконалення CAPTCHA зосереджені на подоланні основних викликів, пов'язаних із зручністю для користувачів, стійкістю до автоматизованих атак і конфіденційністю даних. Одним із найперспективніших напрямків є впровадження динамічних і адаптивних CAPTCHA, які автоматично змінюють рівень складності залежно від поведінки користувача. Наприклад, Google reCAPTCHA v3 аналізує дії користувача у фоновому режимі, визначаючи ймовірність автоматизації без необхідності активної участі користувача, що значно підвищує зручність використання.

Ще одним ефективним підходом є використання завдань, створених на основі штучного інтелекту. Такі CAPTCHA орієнтовані на розпізнавання семантики, що залишається складним завданням для машинного навчання, але зрозумілим для людини. Наприклад, користувачам можуть пропонувати вибрати зображення, які відповідають певному контексту, або вирішувати логічні задачі з текстом. Це дозволяє забезпечити високий рівень безпеки, зберігаючи доступність для звичайних користувачів [6 с. 21].

Інтерактивні та ігрові CAPTCHA стають все більш популярними завдяки їхній здатності залучати користувачів і підвищувати рівень стійкості до автоматизованих атак. Завдання, що вимагають виконання дій, таких як збирання пазлів або перетягування об'єктів, не лише забезпечують захист, але й покращують загальний досвід взаємодії користувача із системою. Такі рішення є особливо ефективними для платформ із високими вимогами до зручності.

Нарешті, новітні розробки використовують біометричні CAPTCHA та технології блокчейну для забезпечення ще більшого рівня захисту. Біометричні CAPTCHA аналізують унікальні характеристики користувача, такі як поведінкові патерни або голос, що робить їх практично недоступними для автоматизованих систем. Технології блокчейну, у свою чергу, дозволяють створювати децентралізовані системи перевірки, які є стійкими до багатьох типів атак. Таким чином, сучасні рішення для CAPTCHA спрямовані на створення збалансованих технологій, які одночасно гарантують безпеку, зручність і захист персональних даних [8].

Висновки. У сучасних умовах швидкого розвитку цифрових технологій та штучного інтелекту CAPTCHA залишається важливим інструментом для забезпечення безпеки у вебсередовищі. Технологія пройшла значний шлях еволюції, починаючи від перших текстових CAPTCHA до сучасних динамічних систем, адаптуючись до нових загроз і викликів. Проте, ефективність традиційних методів значно знизилася через стрімкий розвиток нейронних мереж, OCR-систем та алгоритмів машинного навчання. Це поставило під сумнів надійність текстових та графічних CAPTCHA, які раніше вважалися ефективними.

Окрім технічних вразливостей, CAPTCHA стикається із сучасними викликами, такими як незручність для користувачів, особливо на мобільних пристроях, зниження продуктивності та складнощі з доступністю для людей із особливими потребами. Біометричні рішення, які використовують унікальні особливості користувачів, викликають питання щодо конфіденційності даних, що також обмежує їхнє широке застосування. У таких умовах стає очевидним, що для забезпечення стійкості CAPTCHA необхідне впровадження нових підходів, які враховують сучасні виклики.

Штучний інтелект відіграє подвійну роль у контексті CAPTCHA. З одного боку, AI дозволяє створювати більш ефективні системи, що включають аналіз поведінкових характеристик користувачів, семантичний аналіз тексту чи зображень, а також логічні завдання, які важко автоматизувати. З іншого боку, AI є ключовим інструментом для зламу CAPTCHA, оскільки глибокі нейронні мережі та алгоритми комп'ютерного зору значно підвищили точність автоматизованих атак.

Перспективи розвитку CAPTCHA зосереджуються на впровадженні динамічних та адаптивних систем, які змінюють складність завдань залежно від поведінки користувача. Інтерактивні та ігрові CAPTCHA забезпечують високу стійкість до зломів, поєднуючи захист із зручністю для користувачів. Біометричні рішення, які аналізують поведінкові патерни, можуть стати надійною альтернативою класичним CAPTCHA, особливо в умовах зростання потреби в захисті від автоматизованих атак.

Загалом, подальший розвиток CAPTCHA має бути орієнтований на пошук балансу між безпекою та зручністю для користувачів. Інноваційні підходи, що базуються на штучному інтелекті, блокчейні та біометрії, здатні створити ефективні рішення, які відповідають викликам сучасного цифрового середовища, забезпечуючи стійкість до автоматизованих атак та комфорт для користувачів.

Література:

1. Аналіз вразливості текстових CAPTCHA. Мітра С., та ін. *Журнал інформаційної безпеки*. 2020. №4, т. 8. С. 215–228.

2. Ву Л., Чень Ю. Ефективність CAPTCHA на основі зображень у сучасній веб-безпеці. *Журнал кібербезпеки*. 2021. №3, т. 14. С. 102–119.

3. Емпіричне дослідження та оцінка сучасних CAPTCHA. *Qudata*. URL: https://qudata.com/uk/news/an-empirical-study-and-evaluation-of-modern-captchas/.

4. Інтерактивні CAPTCHA: баланс між зручністю та безпекою. Сатіш П., та ін. *Матеріали Міжнародної конференції з систем безпеки*. 2022. С. 178–185.

5. Тан М., Лі Дж. CAPTCHA на основі біометрії: можливості та виклики. *Міжнародний журнал інновацій у кібербезпеці*. 2023. №2, т. 9. С. 45–56.

6. Штучний інтелект. Машинне навчання / О. В. Григоров та ін. *Автомобіль і електроніка.* 2019. № 15. С. 17-27.

7. Guerar, M., Verderame, L., Migliardi, M., Palmieri, F., & Merlo, A. Gotta CAPTCHA 'Em All: A Survey of Twenty years of the Human-or-Computer Dilemma. *arXiv:2103.01748* DOI: 10.1145/3477142.

8. Jiang R., Zhang S., Liu L., Peng Y. Diff-CAPTCHA: An Image-based CAPTCHA with Security Enhanced by Denoising Diffusion Model. *arXiv*. 2023. DOI: 10.48550/arXiv.2308.08367.

9. Noury Z., Rezaei M. Deep-CAPTCHA: a deep learning based CAPTCHA solver for vulnerability assessment. *arXiv*. 2020. DOI: 10.48550/arXiv.2006.08296.

10. Tariq, N., Khan, F. A., Moqurrab, S. A., & Srivastava, G. CAPTCHA Types and Breaking Techniques: Design Issues, Challenges, and Future Research Directions *arXiv:2008.05112*. DOI: 10.48550/arXiv.2008.05112.

References:

1. Mitra S., ta in. (2020). Analiz vrazlyvosti tekstovykh CAPTCHA (Analysis of the vulnerability of text-based CAPTCHAs). Zhurnal informatsiinoi bezpeky (Journal of Information Security), 4(8), 215–228.

2. Vu L., Chen Yu. (2021). Efektyvnist CAPTCHA na osnovi zobrazhen u suchasnii veb-bezpetsi (The effectiveness of image-based CAPTCHA in modern web security). Zhurnal kiberbezpeky (Journal of Cybersecurity), 3(14), 102–119.

3. Empirychne doslidzhennia ta otsinka suchasnykh CAPTCHA (An empirical study and evaluation of modern CAPTCHAs). Qudata. URL: https://qudata.com/uk/news/an-empirical-study-and-evaluation-of-modern-captchas/.

4. Satish P., ta in. (2022). Interaktyvni CAPTCHA: balans mizh zruchnistiu ta bezpekoiu (Interactive CAPTCHA: balancing convenience and security). In Materialy Mizhnarodnoi konferentsii z system bezpeky (Proceedings of the International Conference on Security Systems), 178–185.

5. Tan M., Li Dzh. (2023). CAPTCHA na osnovi biometrii: mozhlyvosti ta vyklyky (Biometric-based CAPTCHA: opportunities and challenges). Mizhnarodnyi zhurnal innovatsii u kiberbezpetsi (International Journal of Innovations in Cybersecurity), 2(9), 45–56.

6. Hryhorov O. V., ta in. (2019). Shtuchnyi intelekt. Mashynne navchannia (Artificial intelligence. Machine learning). Avtomobil i elektronika (Automobile and Electronics), 15, 17–27.

7. Guerar, M., Verderame, L., Migliardi, M., Palmieri, F., & Merlo, A. Gotta CAPTCHA 'Em All: A Survey of Twenty years of the Human-or-Computer Dilemma. *arXiv:2103.01748* DOI: 10.1145/3477142.

8. Jiang R., Zhang S., Liu L., Peng Y. Diff-CAPTCHA: An Image-based CAPTCHA with Security Enhanced by Denoising Diffusion Model. *arXiv*. 2023. DOI: 10.48550/arXiv.2308.08367.

9. Noury Z., Rezaei M. Deep-CAPTCHA: a deep learning based CAPTCHA solver for vulnerability assessment. *arXiv*. 2020. DOI: 10.48550/arXiv.2006.08296.

10. Tariq, N., Khan, F. A., Moqurrab, S. A., & Srivastava, G. CAPTCHA Types and Breaking Techniques: Design Issues, Challenges, and Future Research Directions *arXiv:2008.05112*. DOI: 10.48550/arXiv.2008.05112.