№ 9(50) 2025
НАУКА і ТЕХНІКА СЬОГОДНІ
серії: право, економіка, педагогіка, техніка, фізико-математичні науки

УДК 004.5

https://doi.org/10.52058/2786-6025-2025-9(50)-1500-1510

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

Чернецький Євгеній Вячеславович кандидат технічних наук, доцент кафедри КІТ та А УДУНТ, м. Дніпро, https://orcid.org/0000-0002-4197-7171

МЕТОДИ ОБХОДУ CAPTCHA ТА КОНТРЗАХОДИ В УМОВАХ РОЗВИТКУ МУЛЬТИМОДАЛЬНИХ МОДЕЛЕЙ

Анотація. У статті систематизовано сучасні підходи до обходу CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) для текстових, графічних, аудіо та інтерактивних схем і проведено комплексний огляд контрзаходів з урахуванням еволюції глибинного навчання, мультимодальних мовно-зорових моделей (VLM/LLM) і ринку «людина-в-циклі» (solver-сервіси). На основі аналізу наукових публікацій і промислових практик запропоновано таксономію атак: від класичних сегментаційно-OCR ланцюгів і end-to-end розв'язувачів для grid-завдань до емуляції поведінки (RL), ретрансляційних атак і соціальної інженерії. Для порівняльної оцінки загроз введено триєдину метрику SR-C-T (success rate - cost - time-to-solve) з додатковими ознаками detectability та scalability, що дозволяє узгоджувати політики захисту з економікою нападника та обмеженнями інфраструктури. Розглянуто адаптивні «невидимі» механізми на базі ризик-скорингу (reCAPTCHA v3, hCaptcha, Turnstile), докази виконаної роботи (PoW) і архітектурні прийоми - ескалація викликів, honeypot/канарки, короткий TTL і token binding для зниження ефективності relay-схем. Окремо проаналізовано альтернативи класичним пазлам - Privacy Pass / Private Access Tokens (IETF RFC 9576/9577/9578), що дають змогу підтверджувати «якість клієнта» без надмірного збору поведінкових/пристроєвих сигналів і з меншим тертям для доброчесних користувачів.Показано, що підвищення складності викликів без супровідних архітектурних змін має обмежений ефект через доступність solver-ринку та зростання можливостей VLM/LLM; натомість шарована стратегія (пасивний скоринг → керована ескалація → PoW/MFA → token-level контрзаходи) забезпечує кращий баланс «безпека - зручність - приватність». Узгоджено вимоги доступності за WCAG 2.2 та позицію W3C щодо недоступності окремих типів CAPTCHA, сформульовано рекомендації з надання еквівалентних альтернатив для користувачів з порушеннями

зору/слуху. Практичний внесок роботи - дорожня карта впровадження з контрольними метриками SR-C-T, принципами A/B-налаштування порогів, anti-relay гігієною й періодичною ротацією моделей/викликів, а також матриця відповідності «тип атаки → контрзахист» для типових сценаріїв зловживань.

Ключові слова: CAPTCHA, інформаційна безпека, обходи, глибинне навчання, мультимодальні моделі, ризик-скоринг, доступність, Privacy Pass, PoW.

Rutts Stanislav 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

METHODS FOR BYPASSING CAPTCHAs AND DEFENSIVE COUNTERMEASURES IN THE ERA OF MULTIMODAL MODELS

Abstract. The paper systematizes contemporary approaches to CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) circumvention across text-, image-, audio-, and interaction-based schemes and provides a comprehensive review of defensive measures in the context of advances in deep learning, multimodal vision-language/large language models (VLM/LLM), and the human-in-the-loop solver market. Based on academic literature and industrial practice, a taxonomy of attacks is proposed: classical segmentation-OCR pipelines and end-to-end solvers for grid tasks; behavior emulation (reinforcement learning); relay attacks; and social engineering. For comparative threat assessment, the SR-C-T triad (success rate - cost - time-to-solve) is introduced with auxiliary dimensions of detectability and scalability, enabling alignment of protection policies with attacker economics and infrastructure constraints. We examine adaptive “invisible” risk-scoring mechanisms (reCAPTCHA v3, hCaptcha, Turnstile), proof-of-work (PoW), and architectural techniques - challenge escalation, honeypots/canaries, short TTLs, and token binding - that reduce the effectiveness of relay schemes. As alternatives to traditional puzzles, Privacy Pass / Private Access Tokens (IETF RFC 9576/9577/9578) allow validating “good client” status without excessive collection of behavioral/device signals and with lower friction for legitimate users.

It is shown that merely increasing challenge complexity has limited effect due to solver market availability and growing VLM/LLM capabilities; instead, a layered strategy (passive scoring → controlled escalation → PoW/MFA → token-level countermeasures) provides a better security-usability-privacy trade-off. Accessibility requirements under WCAG 2.2 and the W3C position on the inaccessibility of certain

CAPTCHA types are reconciled, with recommendations for equivalent alternatives for users with visual/hearing impairments. The practical contribution is an implementation roadmap with SR-C-T control metrics, A/B threshold tuning principles, anti-relay hygiene, periodic model/challenge rotation, and a mapping from "attack type → countermeasure" for common abuse scenarios.

Keywords: CAPTCHA, information security, circumvention, deep learning, multimodal models, risk scoring, accessibility, Privacy Pass, PoW.

Постановка проблеми. CAPTCHA традиційно застосовується як бар'єр проти автоматизованих зловживань у веб- та мобільних сервісах: масових реєстрацій, скрейпінгу, спаму, атак на облікові записи тощо. Однак життєздатність класичних текстових, графічних та аудіо-схем суттєво підважено технічним прогресом у комп'ютерному баченні (CV) та розпізнаванні мовлення (ASR), появою мультимодальних моделей (VLM/LLM), а також індустрією «людина-в-циклі» (solver-сервіси), що забезпечує масштабований та дешевий обхід. Додатковим чинником є професіоналізація інструментарію атак: емуляція поведінки користувача (RL), підміна відбитків браузера/пристрою, relay-схеми та соціальна інженерія. У відповідь індустрія зміщується до «невидимих» механізмів ризик-скорингу та альтернатив на зразок Privacy Pass / Private Access Tokens, що зменшують тертя для доброчесних користувачів, але вимагають переосмислення метрик ефективності та відповідності вимогам доступності й приватності. Проблема ускладнюється відсутністю уніфікованих показників, здатних порівнювати різні схеми в координатах «успіх атаки - вартість - час» і водночас враховувати виявлюваність та масштабованість. Наявні огляди зосереджуються переважно на складності окремих викликів, тоді як економіка нападника, архітектурні контрзаходи та експлуатаційні компроміси (UX, продуктивність, доступність) аналізуються фрагментарно. Отже, постає завдання системно переоцінити роль CAPTCHA у багатошаровій архітектурі захисту, узгодивши безпеку, зручність та приватність на основі відтворюваних метрик і практичних рекомендацій для впровадження.

Аналіз останніх досліджень і публікацій. Огляд останніх двох десятиліть свідчить, що CAPTCHA еволюціонувала від спотворених текстових завдань до різнорідного набору схем (зображення, аудіо, інтерактивні пазли), однак темпи розвитку засобів обходу випереджають ускладнення викликів.

Узагальнювальний огляд Guerar та ін. систематизує класифікацію як CAPTCHA-схем, так і атакувальних підходів, підкреслюючи сталий компроміс між безпекою, зручністю користувача та сумісністю з асистивними технологіями [1]. Класичні методи обходу ґрунтуються на ланцюгу «попередня обробка → сегментація → OCR», де сучасні CNN/LSTM/CTC і трансформерні

архітектури забезпечують високу точність розпізнавання за наявності достатніх датасетів [1]. Для grid-капч поширилися end-to-end детектори та енкодер-декодерні моделі, які розв'язують завдання «оберіть усі світлофори/автобуси» за рахунок донавчання на «польових» даних; емпіричні оцінки свідчать, що стійкість таких викликів сильно залежить від дизайну набору міток та частоти ротації зображень [9].

На тлі зростання мультимодальних VLM/LLM загрози переходять від «чисто візуальних» до гібридних сценаріїв: моделі використовуються для інтерпретації інструкцій та контексту, тоді як остаточне розв'язання делегується людині через соціальну інженерію або relay-сервіси; відповідний кейс задокументовано у технічному звіті GPT-4 [6]. Аудіо-CAPTCHA, попри наміри підвищити доступність, демонструють вразливість до сучасних ASR-систем; запропоновано adversarial-підходи (зокрема aaeCAPTCHA) для ускладнення автоматичного розпізнавання, але вони породжують питання сприйнятності та відповідності стандартам доступності [8]. У сфері «анти-ML»-захисту досліджуються дифузійні генеративні схеми, що зливають корисний сигнал із фоном та змінюють статистику ознак під моделі зору, однак узагальнених висновків щодо їх довгострокової стійкості наразі бракує [7].

Промислова практика поступово переходить від «видимих» тестів до пасивного ризик-скорингу (reCAPTCHA v3, hCaptcha, Cloudflare Turnstile), який мінімізує тертя для більшості користувачів і дозволяє політику ескалації лише для підозрілих сесій [2-4; 10-11]. У відповідь на relay-атаки й скриптову автоматизацію пропонуються архітектурні контрзаходи: короткий TTL і token binding, канарки/honeypot-поля, сегментація політик за платформами (веб, мобільні SDK, партнерські API) [2-4]. Паралельно формується напрямок безпекових альтернатив із нижчим ризиком для приватності — Privacy Pass / Private Access Tokens (IETF RFC 9576/9577/9578), що дозволяють підтверджувати «якість клієнта» без інтерактивних пазлів і з мінімізацією збору поведінкових/пристроєвих сигналів [14-16]. Ключовим, утім, залишається економічний вимір загроз: зрілі ринки solver-послуг знижують бар'єр вартості до обходів, тому просте підвищення складності викликів без перегляду архітектури захисту та метрик ефективності дає обмежений ефект [12-13].

Сукупно література підкреслює потребу у шарованій стратегії (пасивний скоринг → ескалація → PoW/MFA → анти-relay) та узгоджених метриках оцінювання ризику. Наявні огляди рідко інтегрують показники успішності, вартості та часу вирішення разом із виявлюваністю й масштабованістю; заповнення цієї прогалини є передумовою відтворюваних порівнянь і практичного тюнінгу політик у динамічному середовищі [1; 9-11; 14-16].

Мета статті – систематизувати сучасні методи обходу CAPTCHA, узагальнити архітектурні контрзаходи та альтернативи (ризик-скоринг, PoW,

Privacy Pass/PAT), запропонувати відтворювані метрики оцінювання ризику SR-C-T з ознаками *detectability* і *scalability*, а також сформувати практичну дорожню карту впровадження з урахуванням вимог доступності, приватності й економіки нападника для типових сценаріїв зловживань (масові реєстрації, скрейпінг, спам, АТО) і визначити принципи ескалації політик.

Виклад основного матеріалу. Розгляд стійкості CAPTCHA ведеться у рамках моделі загроз, що охоплює: (i) повністю автоматизовані боти (headless-браузери, скрипти з CV/ASR-модулями), (ii) гібридні ланцюги «модель → людина» (relay/solver-ринок), (iii) сценарії з мультимодальними VLM/LLM, де модель інтерпретує інструкцію/контекст і делегує остаточне рішення людині, та (iv) поведінкові атаки з емулюванням траєкторій і таймінгів користувача.

Вхідні дані для атак включають знімки екрану, DOM-структури, мережеві артефакти, а також телеметрію клієнта, за умови доступу зловмисника до інструментів підміни відбитків (fingerprint spoofing).

Припускається, що атакувальник має доступ до дешевої обчислювальної інфраструктури/хмар та до solver-послуг із погодинною/поштучною оплатою, що різко знижує поріг вартості обходів.

У такій моделі класичне «ускладнювати пазл» недостатньо: потрібні шари захисту, що піднімають ***загальну*** вартість атаки та зменшують її масштабованість. [1–3; 6; 12–13]

Таксономія методів обходу:

1.Сегментація → OCR. Ранні й досі ефективні для текстових схем підходи: попередня обробка (бінаризація, видалення шумів/ліній), сегментація символів, розпізнавання (CNN/LSTM/CTC; трансформери). За наявності датасетів та узагальнюваних перетворень досягається висока точність при низькій граничній вартості на спробу. [1]

2. End-to-end для grid-завдань. Сучасні детектори/енкодер-декодери навчаються вибирати комірки («усі світлофори/автобуси/переходи») без явної сегментації; практична стійкість залежить від якості зображень, ротації класів/сцен та контрольованого «витоку» датасетів у публічні моделі. [1; 9]

3. VLM/LLM-асистовані атаки. Мультимодальні моделі з інструкційним донавчанням розв’язують візуально-семантичні задачі, а також можуть «придумувати» стратегії relay (соціальна інженерія, делегування на людину) та комбінувати CV з текстовим міркуванням. [6]

4. Емуляція поведінки (RL). Синтез траєкторій курсора, таймінгів кліків/скролу, людоподібних пауз; модифікація/підміна відбитків середовища (canvas/webGL, шрифти, апаратні ідентифікатори), що знижує якість пасивного скорингу. [9–11]

5. Relay-схеми (людина-в-циклі). Ретрансляція завдання на solver-ринок через API/проксі; ціна за 1000 вирішень для «простих» задач є низькою, для

складніших — помірною, що робить атаки економічно привабливими при великому трафіку. [12–13]

6. Аудіо-CAPTCHA. Вразливі до сучасних ASR; у відповідь пропонуються adversarial-модифікації (наприклад, aaeCAPTCHA), однак це спірно з точки зору доступності та UX. [8]

7. «Анти-ML» генерація. Дифузійні схеми, що змішують сигнал із фоном, зсувають статистику ознак під CV-моделі; довгострокова стійкість потребує емпіричної валідації на adversarial-суперниках. [7]

Спектр обхідних технік охоплює і «класичний» CV/ASR, і нові мультимодальні/поведінкові/економічні вектори, тому захист має бути багатошаровим і адаптивним. [1; 6–9; 12–13]

Оскільки реальна ефективність захисту визначається не лише математичною складністю виклику, а й економікою атаки, пропонується рамка оцінювання **SR-C-T + D + S**: частка успішних обходів (*success rate*), очікувана вартість на корисну дію нападника (*cost*), час розв'язання (*time-to-solve*), виявлюваність (*detectability*) та масштабованість (*scalability*).

З практичної точки зору корисно відстежувати ефективну вартість C_{eff}, що наближено дорівнює відношенню сумарних витрат на інфраструктуру, solver-послуги й обхід політик до кількості успішних обходів; збільшення латентності та зниження пропускної здатності прямо підвищують C_{eff}. Для захисника ціллю є одночасне зменшення *SR* і *S* за контрольного впливу на користувацький досвід. Валідність рішень перевіряється A/B-експериментами: порівнюються розподіли часу проходження, кореляції між балами ризику та пост-фактум ідентифікованими зловживаннями, оцінюється вплив на конверсію й відмови «доброчесним» сегментам [1-5; 9-11; 14-16].

Промислова практика демонструє відхід від «видимих» тестів до пасивного ризик-скорингу з керованою ескалацією. Такі рішення, як reCAPTCHA v3, hCaptcha та Cloudflare Turnstile, формують числовий або категоріальний ризик-сигнал, на основі якого політика доступу ухвалює рішення: пропустити без тертя, показати інтерактивний виклик або заблокувати сесію. Ключовими стають калібрування порогів на власній телеметрії, сегментація правил за типами трафіку та регулярний контроль дрейфу даних/моделей. Самі інтерактивні завдання повинні змінюватися за класами, сценами й параметрами відображення; слід уникати стабільних «сигнатур» у DOM і передбачати канаркові елементи, що дозволяють відрізняти автоматичні кліки від осмисленої взаємодії [2-4; 10-11].

Важливим інструментом підвищення вартості атаки є докази виконаної роботи (PoW), які додають часово-енергетичні витрати ботам і зменшують їхню пропускну здатність. Однак застосовувати PoW варто адресно — за ознак підвищеного ризику, з адаптацією складності до класу клієнта, аби не

дискримінувати малопотужні пристрої та не погіршувати доступність. Для боротьби з relay-ланцюгами ефективними виявляються короткі строки придатності токенів, прив'язування їх до параметрів сесії, походження або криптографічного контексту, що знижує цінність перепроданих рішень; доречні також правила на рівні географії та автономних систем, поділ політик за платформами (веб, мобільні SDK, партнерські API) і виявлення аномальних маршрутів трафіку [2-4].

З огляду на поширені headless-середовища потрібні багаторівневі перевірки відбитків (canvas, webGL, шрифти), часових профілів і мікрорухів курсора, а також активне зондування ознак автоматизації. Практика свідчить, що єдиний маркер ненадійний; слід агрегаційно оцінювати набір сигналів і працювати з «сірою зоною», в якій рішення ухвалюються на основі ризик-скорингу з ескалацією [9-11]. Щодо «анти-ML» підходів, доцільною є роль допоміжного шару - синтетична генерація, контрольовані шуми та трансформації справді зменшують успішність навченої на статичних розподілах моделі, проте в ізоляції не забезпечують стійкість проти адаптивного супротивника [7].

Зміна парадигми від когнітивних пазлів до криптографічних і протокольних гарантій відбивається у стандартах Privacy Pass / Private Access Tokens. Ідея полягає в тому, щоб підтвердити «якість клієнта» без передавання зайвих поведінкових або пристроєвих даних і без інтерактивних тестів, що зменшує тертя для доброчесних користувачів і покращує приватність. На практиці це радше позитивний сигнал у політиці доступу, ніж повноцінна заміна всім шарам захисту; найкращий ефект досягається у зв'язці з пасивним скорингом і ескалацією для підозрілих сесій [14-16]. Додатково для високоризикових дій мають сенс MFA/пас-ключі, квотування запитів і контекстні rate-limit-політики, а також механізми перевірки доброчесності клієнта, якщо це узгоджується з вимогами приватності та доступності [2-5].

Окремої уваги потребує відповідність WCAG 2.2 і позиції W3C щодо недоступності традиційних CAPTCHA для частини користувачів. Недопустимо покладатися на сенсорні або когнітивні тести як на єдиний бар'єр; мають існувати еквівалентні альтернативи для людей із порушеннями зору та слуху. Політики збору телеметрії мусять бути пропорційними та прозорими, з чітко визначеними строками зберігання й механізмами апеляції, інакше ризики для приватності нівелюють виграш у безпеці [4-5]. Для великих розгортань доцільною є оцінка впливу на приватність (DPIA), яка допомагає збалансувати вимоги безпеки й очікування користувачів.

Практична дорожня карта впровадження таких систем базується на циклі «загроза → сигнал → політика → вимірювання». Спочатку визначаються типові зловживання (масові реєстрації, скрейпінг, ATO, спам) і формулюються

гіпотези щодо каналів атак та очікуваних значень SR-C-T. Далі проєктується архітектура з пасивним скорингом як дефолтним маршрутом і ескалаційними гілками, що підвищують вартість атаки з мінімальним впливом на доброчесний трафік; у цій конфігурації короткий TTL і прив'язування токенів можуть суттєво зменшити рентабельність relay-ланцюгів. На етапі експлуатації безперервні експерименти з порогами й наборами сигналів дозволяють підтримувати потрібний компроміс між безпекою та конверсією, тоді як планова ротація викликів, ключів і моделей унеможливлює накопичення «зрілого» датасета в супротивника. Перспективним вектором пілотування є інтеграція PAT/Privacy Pass для «зелених» сегментів трафіку з паралельним моніторингом впливу на SR-C-T [2-5; 10-16].

Разом із тим лишаються обмеження й відкриті питання. Швидкість розвитку VLM/LLM і доступність solver-послуг підтримують низький поріг обходу, тому ставка на дедалі складніші пазли поза архітектурними змінами має короткий горизонт. По-справжньому відтворювані бенчмарки, які поєднують SR-C-T + D + S і моделюють сучасні relay-ланцюги, все ще перебувають у зародковому стані; публічної телеметрії щодо довгострокових ефектів ескалації також бракує. Дискусійним залишається застосування PoW на мобільних і енергообмежених пристроях, включно з екологічним виміром. Нарешті, на рівні протоколів перспективним видається поєднання Privacy Pass із легкими перевірками контексту присутності та крос-платформними сигналами, стійкими до підміни і приватними за замовчуванням [1; 4-5; 9-16].

Підсумовуючи, ефективність протидії автоматизованим зловживанням визначається сукупною економікою атаки, а не локальною складністю тесту. Найкращі результати демонструє шарована архітектура з ризик-скорингом, керованою ескалацією, anti-relay-прийомами та ротацією моделей і викликів; альтернативи на кшталт PAT допомагають знизити тертя та покращити приватність без втрати керованості. Керівною ідеєю має лишатися вимірюваність: тільки через системні метрики й постійний експериментальний цикл вдається стабільно зменшувати SR і S за прийнятного впливу на UX та повної відповідності вимогам доступності [2-5; 10-16].

Висновки. Проведений огляд показує, що життєздатність окремих видів CAPTCHA дедалі менше визначається їх «локальною» складністю і все більше - загальною економікою атаки та архітектурою захисту. Класичні підходи на основі сегментації та OCR, енд-ту-енд розв'язувачі для grid-завдань, мультимодальні стратегії із залученням VLM/LLM, relay-ланцюги з людиною в циклі та емуляція поведінки користувача формують різнорідний, взаємодоповнювальний набір векторів обходу. За таких умов ставка лише на ускладнення окремого виклику має короткостроковий ефект і не забезпечує стійкості в масштабі.

Ефективною відповіддю виявляється багатошарова архітектура, у центрі якої - пасивний ризик-скоринг з керованою ескалацією.

Для більшості доброчесних сесій взаємодія лишається «без тертя», тоді як підозрілі маршрутизуються крізь послідовність контрзаходів: інтерактивні виклики, докази виконаної роботи, додаткові фактори автентифікації, а також протокольні й архітектурні механізми (короткі TTL, прив'язування токенів, сегментація політик за платформами, honeypot/канарки). Така конфігурація підвищує вартість і латентність атаки, знижуючи її масштабованість без істотних втрат у зручності для користувача.

Ключовою передумовою керованості є відтворюване вимірювання. Запропонована рамка **SR-C-T + D + S** дозволяє порівнювати та налаштовувати політики на основі частки успішних обходів, очікуваної вартості для нападника, часу розв'язання, виявлюваності та пропускної здатності.

Практичне застосування рамки передбачає безперервні A/B-експерименти, контроль дрейфу даних і регулярну ротацію типів викликів, ключів та моделей, що перешкоджає накопиченню «зрілого» датасета у супротивника.

Перспективним доповненням до традиційних механізмів є **Privacy Pass / Private Access Tokens**, які забезпечують позитивні сигнали якості клієнта з меншим тертям і кращими гарантіями приватності. Водночас ці технології повинні інтегруватися у загальну стратегію ризик-скорингу, а не розглядатися як універсальна заміна.

Нарешті, відповідність **WCAG 2.2** та прозорі практики обробки даних мають розглядатися як невід'ємні вимоги до систем протидії зловживанням.

Подальші дослідження доцільно спрямувати на відкриті бенчмарки, що моделюють сучасні relay-ланцюги, на оцінювання енергетичних/екологічних наслідків PoW на мобільних пристроях та на протокольні схеми, стійкі до підміни сигналів, - із пріоритетом вимірюваності та практичної відтворюваності.

Література:

1. Guerar M., Verderame L., Migliardi M., Palmieri F., Merlo A. Спіймай усі CAPTCHA: огляд двадцяти років дилеми «людина чи комп'ютер». arXiv, 2021. arXiv:2103.01748. URL: https://arxiv.org/abs/2103.01748 (Дата звернення: 2025-09-12).

2. Google Developers. reCAPTCHA v3: документація [Електронний ресурс]. 2024. URL: https://developers.google.com/recaptcha/docs/v3 (Дата звернення: 2025-09-12).

3. Cloudflare Developers. Turnstile: огляд і документація [Електронний ресурс]. 2025. URL: https://developers.cloudflare.com/turnstile/ (Дата звернення: 2025-09-12).

4. W3C. Недоступність CAPTCHA [Електронний ресурс]. 2021. URL: https://www.w3.org/TR/turingtest/ (Дата звернення: 2025-09-12).

5. W3C. Настанови з доступності веб-вмісту (WCAG) 2.2 [Електронний ресурс]. 2024. URL: https://www.w3.org/TR/WCAG22/ (Дата звернення: 2025-09-12).

6. OpenAI. Технічний звіт GPT-4. 2023. URL: https://cdn.openai.com/papers/gpt-4.pdf (Дата звернення: 2025-09-12).

7. Jiang R., Zhang S., Liu L., Peng Y. Diff-CAPTCHA: схема з дифузійною генерацією. arXiv, 2023. arXiv:2308.08367. URL: https://arxiv.org/abs/2308.08367 (Дата звернення: 2025-09-12).

8. Hossen M. I., Rahman S., Purohit A., Chi H., Li W., Ren K. aaeCAPTCHA — аудіо-адверсарні CAPTCHA. arXiv, 2022. URL: https://arxiv.org/pdf/2203.02735 (Дата звернення: 2025-09-12).

9. Abdullah H. та ін. Атаки на аудіо-CAPTCHA (aaeCAPTCHA). arXiv, 2022. URL: https://arxiv.org/pdf/2203.05408 (Дата звернення: 2025-09-12).

10. Teoh X. та ін. Чи залишаються CAPTCHA складними для ботів? USENIX Security (переддрук), 2025. URL: https://www.usenix.org/system/files/usenixsecurity25-teoh.pdf (Дата звернення: 2025-09-12).

11.] hCaptcha. Огляд рішень для підприємств [Електронний ресурс]. 2024–2025. URL: https://docs.hcaptcha.com/ent_overview/ (Дата звернення: 2025-09-12).

12. hCaptcha. Документація API [Електронний ресурс]. 2024–2025. URL: https://docs.hcaptcha.com/api/ (Дата звернення: 2025-09-12).

13. Arkose Labs. Огляд продукту [Електронний ресурс]. 2025. URL: https://www.arkoselabs.com/ (Дата звернення: 2025-09-12).

14. 2Captcha. Прайсинг послуг розв’язування CAPTCHA [Електронний ресурс]. 2025. URL: https://2captcha.com/pricing (Дата звернення: 2025-09-12).

15. AIMultiple. Сервіси розв’язування CAPTCHA — огляд цін [Електронний ресурс]. 2025. URL: https://research.aimultiple.com/captcha-solving-services/ (Дата звернення: 2025-09-12).

16. IETF. RFC 9576 — Архітектура Privacy Pass. 2024. URL: https://www.rfc-editor.org/rfc/rfc9576.html (Дата звернення: 2025-09-12).

17. IETF. RFC 9577 — Схема автентифікації HTTP для Privacy Pass. 2024. URL: https://datatracker.ietf.org/doc/rfc9577/ (Дата звернення: 2025-09-12).

18. IETF. RFC 9578 — Протоколи випуску Privacy Pass. 2024. URL: https://www.rfc-editor.org/rfc/rfc9578.html (Дата звернення: 2025-09-12).

References:

1. 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, 2021. arXiv:2103.01748. URL: https://arxiv.org/abs/2103.01748 (Accessed on: 2025-09-12).

2. Google Developers. reCAPTCHA v3. Documentation [Electronic resource]. 2024. URL: https://developers.google.com/recaptcha/docs/v3 (Accessed on: 2025-09-12).

3. Cloudflare Developers. Turnstile: Overview [Electronic resource]. 2025. URL: https://developers.cloudflare.com/turnstile/ (Accessed on: 2025-09-12).

4. W3C. Inaccessibility of CAPTCHA [Electronic resource]. 2021. URL: https://www.w3.org/TR/turingtest/ (Accessed on: 2025-09-12).

5. W3C. Web Content Accessibility Guidelines (WCAG) 2.2 [Electronic resource]. 2024. URL: https://www.w3.org/TR/WCAG22/ (Accessed on: 2025-09-12).

6. OpenAI. GPT-4 Technical Report. 2023. URL: https://cdn.openai.com/papers/gpt-4.pdf (Accessed on: 2025-09-12).

7. Jiang R., Zhang S., Liu L., Peng Y. Diff-CAPTCHA. arXiv, 2023. arXiv:2308.08367. URL: https://arxiv.org/abs/2308.08367 (Accessed on: 2025-09-12).

8. Hossen M. I., Rahman S., Purohit A., Chi H., Li W., Ren K. aaeCAPTCHA — Audio Adversarial CAPTCHAs. arXiv, 2022. URL: https://arxiv.org/pdf/2203.02735 (Accessed on: 2025-09-12).

9. Abdullah H., et al. Adversarial Attacks on Audio CAPTCHA (aaeCAPTCHA). arXiv, 2022. URL: https://arxiv.org/pdf/2203.05408 (Accessed on: 2025-09-12).

10. Teoh X., et al. Are CAPTCHAs Still Bot-hard? USENIX Security (preprint), 2025. URL: https://www.usenix.org/system/files/usenixsecurity25-teoh.pdf (Accessed on: 2025-09-12).

11. hCaptcha. Enterprise overview [Electronic resource]. 2024–2025. URL: https://docs.hcaptcha.com/ent_overview/ (Accessed on: 2025-09-12).

12. hCaptcha. API documentation [Electronic resource]. 2024–2025. URL: https://docs.hcaptcha.com/api/ (Accessed on: 2025-09-12).

13. Arkose Labs. Product overview [Electronic resource]. 2025. URL: https://www.arkoselabs.com/ (Accessed on: 2025-09-12).

14. 2Captcha. Pricing [Electronic resource]. 2025. URL: https://2captcha.com/pricing (Accessed on: 2025-09-12).

15. AIMultiple. CAPTCHA Solving Services — pricing overview [Electronic resource]. 2025. URL: https://research.aimultiple.com/captcha-solving-services/ (Accessed on: 2025-09-12).

16. IETF. RFC 9576 — Privacy Pass Architecture. 2024. URL: https://www.rfc-editor.org/rfc/rfc9576.html (Accessed on: 2025-09-12).

17. IETF. RFC 9577 — Privacy Pass HTTP Authentication Scheme. 2024. URL: https://datatracker.ietf.org/doc/rfc9577/ (Accessed on: 2025-09-12).

18. IETF. RFC 9578 — Privacy Pass Issuance Protocols. 2024. URL: https://www.rfc-editor.org/rfc/rfc9578.html (Accessed on: 2025-09-12).