DOI 10.15276/imms.v15.no1.71
УДК 004.056.53

Informatics and Mathematical Methods in Simulation
Vol.15 (2025), No.1, pp. 71-82

ЗАХИЩЕНА СИСТЕМА ДЛЯ СТВОРЕННЯ ТА ПРОВЕДЕННЯ ОПИТУВАНЬ

В.Р. Капелюшний, Н.І. Кушніренко, О.В. Троянський

Національний університет «Одеська політехніка»
1, Шевченка пр., м.Одеса, 65044, Україна
Emails: kushnirenko@op.edu.ua, o.v.troyanskiy@op.edu.ua

У сучасних умовах цифрової трансформації особливої уваги набуває забезпечення безпеки для проведення онлайн-опитувань. Актуальність проблеми обумовлена активним використанням веб-сервісів для організації навчального процесу та підвищеними вимогами до захисту персональних даних, запобігання академічному шахрайству та забезпеченню прозорості результатів. Метою даної роботи є розробка безпечного веб-застосунку для створення, проведення та контролю опитувань, який забезпечує захист персональних даних користувачів, підтримку академічної доброчесності та відповідає сучасним вимогам кібербезпеки. У роботі здійснено аналіз сучасних систем для тестування знань (Google Forms, Quizlet, SurveyMonkey, Typeform), виявлено їх переваги та недоліки в контексті безпеки, зокрема обмежену підтримку двофакторної автентифікації та слабкий захист даних у стані спокою. Запропоновано та реалізовано безпечну систему опитувань з підтримкою сучасних криптографічних протоколів. Для захисту даних використано симетричний алгоритм шифрування AES-256, що дозволяє гарантувати конфіденційність і цілісність збережених результатів. Розроблена система також підтримує двофакторну автентифікацію, перевірку геолокації, email підтвердження, шифрування HTTPS/TLS, автоматичне завершення сесії та механізм цифрових водяних знаків, який дозволяє ідентифікувати джерело витоку тестового контенту. Проведено практичну реалізацію системи розмежування прав доступу, створення ролей студентів та викладачів, впроваджено систему моніторингу входів і змін. Результати дослідження підтверджують доцільність створення власної системи як безкоштовної альтернативи популярним сервісам із недостатнім рівнем безпеки. Запропоноване рішення може впроваджуватись у закладах освіти для підвищення якості процесу тестування знань та забезпечення високого рівня безпеки даних користувачів.

Ключові слова: система опитувань, шифрування, кібербезпека, водяні знаки, RBAC, двофакторна автентифікація, геолокація, академічна доброчесність

Вступ. Сучасна освіта активно переходить до цифрових форматів, що зумовлює потребу у створенні безпечних систем для дистанційного навчання, тестування знань та проведення різноманітних опитувань. Згідно з інформацією Segura, у 2024 році в середньому відбувалося понад 2200 атак на веб-сервіси щодня, більшість з яких були спрямовані на системи обміну інформацією, включаючи платформи для навчання та проведення опитувань [1]. Згідно з звітом ENISA [2] та рекомендаціями OWASP [3], ключовими ризиками для веб-платформ є несанкціонований доступ до облікових записів, ін'єкційні атаки (SQL, XSS), використання застарілого програмного забезпечення та слабка політика управління сеансами.

Як зазначено в дослідженні [4], онлайн-системи навчання мають низку системних вразливостей, серед яких несанкціонований доступ до облікових записів, вразливість до атак на сесію та недостатній контроль за збереженням результатів тестування. У даній роботі запропоновано рекомендації щодо покращення інформації небезпеки в освітньому середовищі, а також розроблена власна система для створення та проведення опитувань, яка забезпечує високий рівень захисту даних, гнучке керування курсами та тестами, а також підтримку ключових механізмів забезпечення академічної доброчесності.

Системи тестування знань відіграють критично важливу роль в освітньому процесі. Вони дозволяють ефективно проводити оцінювання, перевіряти знання,

організовувати курси та отримувати зворотний зв'язок. Такі програмні рішення як: Google Forms, Quizlet, SurveyMonkey, Typeform пропонують широкі можливості для створення та проведення опитувань. Однак, вони мають деякі недоліки в контексті безпеки: відсутність двофакторної автентифікації у безкоштовних версіях, обмежений захист персональних даних, неможливість контролювати академічну доброчесність. У зв'язку з цим, розробка власного безпечного застосунку для тестування знань є актуальним завданням.

Серед найпоширеніших інструментів для створення онлайн-опитувань вирізняється Google Forms [5], що надає користувачам широкі можливості для налаштування анкет відповідно до їхніх потреб. Простота використання та можливість здійснювати інтеграції з іншими сервісами Google робить платформу зручною як для навчальних, так і для робочих цілей.

Ще однією популярною платформою є Quizlet [6], яка дозволяє не лише створювати тести, а й використовувати картки для інтерактивного навчання. Її функціонал орієнтований як на студентів і викладачів, так і на молодшу аудиторію. Основна перевага полягає в застосуванні методів активного навчання – не лише для контролю знань, а й для кращого запам'ятовування матеріалу.

Платформа SurveyMonkey [7] заснована у 1999 році є потужним засобом для створення, проведення і аналізу опитувань. На відміну від деяких аналогів, вона дозволяє працювати з готовими шаблонами, що значно спрощує процес розробки тестів та анкет.

Порівняно новою, але сучасною платформою є Typeform [8], запущена у 2012 році. Вона вирізняється візуально привабливим дизайном, широким набором інтерактивних елементів і діалогових підходів до побудови опитувань. Завдяки цьому користувачі більше залучаються до процесу, що підвищує рівень проходження опитувань до кінця.

Критично важливим аспектом використання онлайн-форм для тестування є захист отриманих даних. Особиста інформація, результати тестів чи конфіденційні відомості повинні зберігатися у безпеці, адже їх витік може призвести до репутаційних і фінансових втрат. Тому оцінка надійності обраної платформи є важливою для запобігання зовнішнім загрозам та несанкціонованому доступу.

Google Forms використовує протокол HTTPS та алгоритм AES-256 для шифрування переданих і збережених даних, а також інфраструктуру Google Key Management для керування ключами. Додатковий захист забезпечується двофакторною автентифікацією та можливістю контролю доступу до платформ. Платформа відповідає стандартам GDPR, CCPA та ISO 27001 [9].

Quzlet забезпечує базовий захист даних шляхом SSL та HTTPS, проте не надає детальну інформацію про шифрування даних при їх збереженні. Компанія співпрацює з рекламними партнерами, що може створювати ризики для конфіденційності. Двофакторна автентифікація передбачена лише у платній версії [10].

Сервіс SurveyMonkey підтримує HTTPS-з'єднання та шифрування за допомогою AES-256. Дата-центри платформи розташовані в США, Канаді та Ірландії. Двофакторна автентифікація доступна лише у платних тарифах. Деякі дані користувача можуть бути видалені повністю протягом 90 днів неактивності [11].

Typeform розгорнута в хмарному сервісі Amazon Web Services і також використовує шифрування AES-256 та захист HTTPS, а метадані форм підлягають шифруванню. Двофакторна автентифікація не є вбудованою функцією, але може бути активованою через Google або Microsoft. Сервіс відповідає вимогам GDPR, CCPA та SOC Type II [12].

Серед проаналізованих платформ Google Forms та SurveyMonkey забезпечують найвищий рівень безпеки завдяки сучасному шифруванню та підтримці двофакторної автентифікації. Quizlet та Typeform надають базовий, захист, проте не надають повної прозорості щодо збережених даних в стані спокою. При виборі платформи варто

враховувати не лише їх функціональність, а й рівень захисту персональної інформації, що особливо актуально у сфері освіти.

Усе це підкреслює актуальність розробки власного веб-застосунку для проведення опитувань, який би поєднував гнучкий функціонал з високим рівнем захисту, шифруванням даних, підтвердженням дії користувача, геолокаційним моніторингом і системою цифрових водяних знаків. Такий підхід дозволить підвищити довіру до результатів тестування, забезпечити прозорість навчального процесу та відповідність міжнародним стандартам.

Мета роботи. Метою роботи є підвищення безпеки процесу проведення опитувань в освітньому середовищі шляхом розробки захищеної веб-системи, яка реалізує сучасні механізми інформаційної безпеки та враховує потреби користувачів з різними ролями. Для досягнення поставленої мети було визначено такі основні задачі:

– розробити функціонал та інтерфейс безпечної веб-системи з урахуванням потреб різних ролей користувачів;

– реалізувати авторизацію через Google, двофакторну автентифікацію та підтвердження змін персональних даних через email-коди;

– реалізувати захист чутливої інформації на основі шифрування AES-256, підтвердження локації, завершення опитувань в разі покидання сторінки, автоматичне завершення сесії, захист від XSS-атак;

– реалізувати механізм формування водяного знака для виявлення джерела витоку завдань.

Основна частина. Для захисту конфіденційних даних, отриманих під час використання систем опитувань важливо використовувати надійні криптографічні алгоритми. Вибір відповідного методу шифрування залежить від обсягу даних, бажаної швидкості системи та вимог до безпеки. У сучасній практиці застосовується як симетричні, так і асиметричні підходи до шифрування, кожен із яких має свої переваги та обмеження.

Для шифрування даних в системі опитувань було обрано AES-256, який є одним з найпоширеніших симетричних криптографічних алгоритмів. AES відзначається високою криптостійкістю та офіційно затверджений як стандарт в США. Він працює з блоками по 128 біт та підтримує ключі довжиною 128, 192 або 256 біт. Найвищий рівень захисту забезпечує AES-256, який має 14 раундів перетворень та використовує унікальні раундові ключі, що генеруються з основного ключа [13].

AES-256 поєднує у собі кілька етапів обробки даних: підстановка байтів (SubBytes), перестановка рядків (ShiftRows), змішування стовпців (MixColumns) і накладання ключа (AddRoundKey). Кожен з них виконує важливу функцію для досягнення криптостійкості [14]. Серед переваг AES-256 можна виділити високу швидкість обробки даних, можливість оптимізації під апаратне забезпечення та підтримку різних режимів шифрування. Алгоритм стійкий до відомих атак, а повний перебір ключів (2^{256} варіантів) є абсолютно недосяжним навіть для суперкомп'ютерів. Саме тому AES-256 було обрано для шифрування даних у стані спокою – як надійний, продуктивний та загальновизнаний стандарт.

Від безпеки програмного забезпечення залежить захист зібраних даних, забезпечення їхньої цілісності та стійкість до зовнішніх атак. Система повинна відповідати сучасним стандартам кібербезпеки, включаючи можливі адаптації до нових загроз та постійного моніторингу подій. В запропонованій системі опитувань передбачено низку пов’язаних між собою заходів, які мінімізують потенційні ризики та гарантують стабільність роботи.

Важливим етапом забезпечення безпеки в системі опитувань є автентифікація – процедура перевірки особи користувача при вході в систему. Під час входу до системи користувач повинен ввести унікальний облікові дані: логін та пароль, які системи перевіряє на відповідність. У разі потреби може також виконуватися перевірка IP-адреси, сертифікату або додаткові верифікаційні дії. Якщо автентифікація завершилася успіхом,

наступним етапом є авторизація, тобто надання користувачу прав доступу до ресурсів. На рис. 1 показаний процес входу користувача в систему.

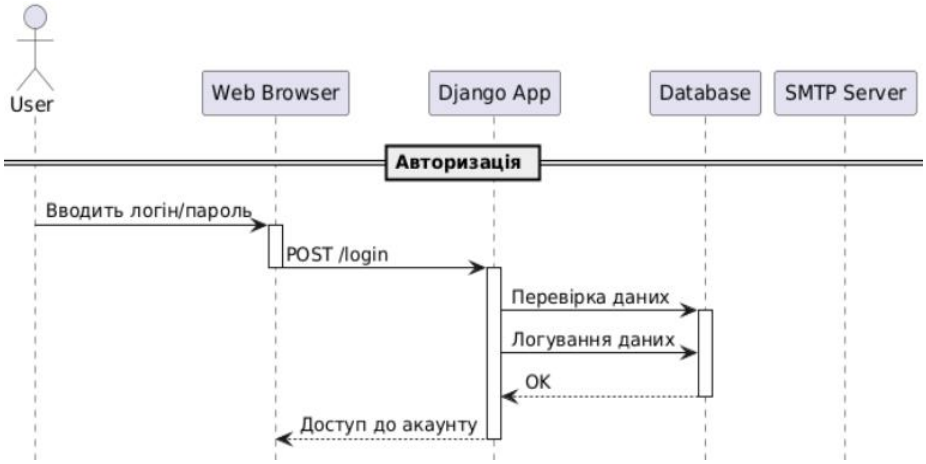

Рис. 1. Процес входу користувача в систему

Для підвищення рівня захисту впроваджено двофакторну автентифікацію (2FA), що надає додатковий рівень підтвердження особи – зазвичай це одноразові коди з SMS або email, телефонний дзвінок, резервний пароль чи спеціальний додаток [12]. Якщо не знайдено збігів щодо даного користувача, або він не зміг пройти до кінця процес автентифікації і підтвердити свою особу, йому буде відмовлено в доступі. Процес двофакторної автентифікації наведений на рис. 2.

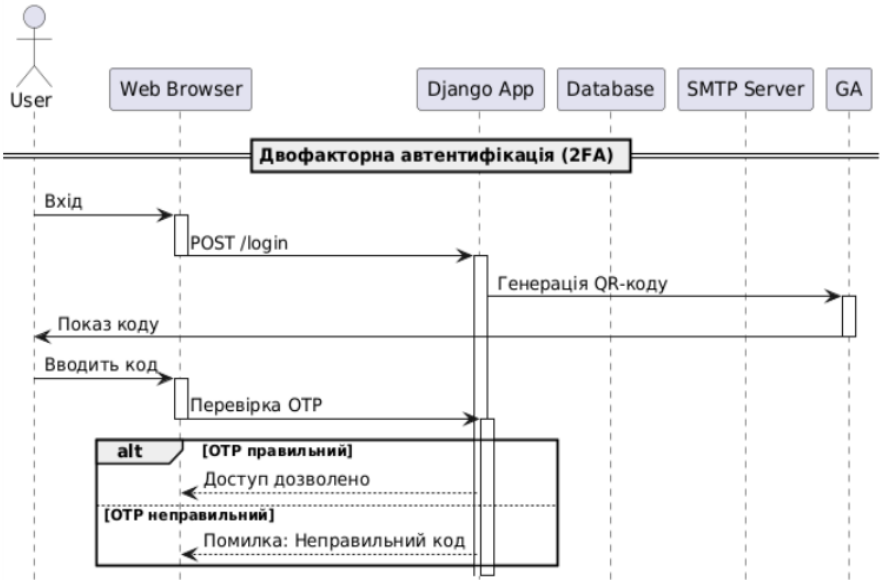

Рис 2. Процес двофакторної автентифікації користувача

Ще більш надійним методом автентифікації є використання біометричних даних – відбитків пальців або розпізнавання обличчя. Їх важко підробити, тому вони є потужним інструментом протидії шахрайству. Автентифікація слугує бар'єром для несанкціонованого доступу до системи та захищає персональні дані від сторонніх осіб.

Авторизація в запропонованій системі опитувань базується на моделі контролю доступу RBAC (Role Based Access Control) [15], яка дозволяє призначити доступ до функцій системи залежно від ролі користувача. Наприклад, студент може лише доєднатися до курсів та проходити опитування, викладач – створювати і редагувати тести та курси, керувати користувачами та системним налаштуванням.

Ще одним елементом безпеки є перевірка геолокації під час входу. Система фіксує поточну IP-адресу, визначає місто та країну, порівнює отримані значення з

попередніми збереженими даними. Якщо локація відрізняється, користувачеві надсилається одноразовий код на email. Доступ відкривається лише після успішного підтвердження. Процес перевірки локації користувача наведений на рис. 3.

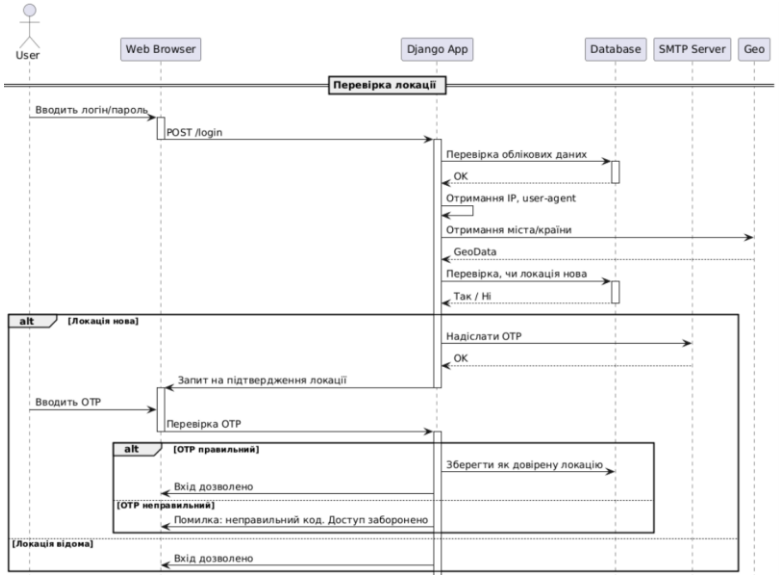

Рис 3. Процес перевірки локації користувача

Важливим аспектом забезпечення безпеки даних користувачів є політика створення надійних паролів. У системі встановлено мінімальну довжину пароля 12 символів, а також встановлені вимоги щодо використання великих та малих літер, цифр і спеціальних символів. Щоб уникнути зловживань або атак методом перебору, реалізовано блокування після декількох невдалих спроб входу. Після трьох помилок користувач мусить зачекати 60 секунд. Крім того, для безпеки сесій введено автоматичне завершення сесії після 12 годинної неактивності. При кожному запиті перевіряється час останньої активності, в разі перевищення ліміту, система автоматично завершує сесію користувача. З метою запобігання XSS-атакам, усі дані, які вводяться через форми, автоматично проходять санітизацію. Це гарантує, що шкідливі скрипти не потраплять у середовище виконання та не становитимуть загрозу для користувачів.

Щоб запобігти несанкціонованій зміні персональних даних, при спробі редагувати дані профілю, email або пароль, надсилається підтвердження на електронну пошту. Лише після введення коду, зміни зберігаються, у протилежному випадку вони скасовуються. На рис. 4 наведено механізм редагування профілю. Даний механізм застосовується для відновлення забутого пароля.

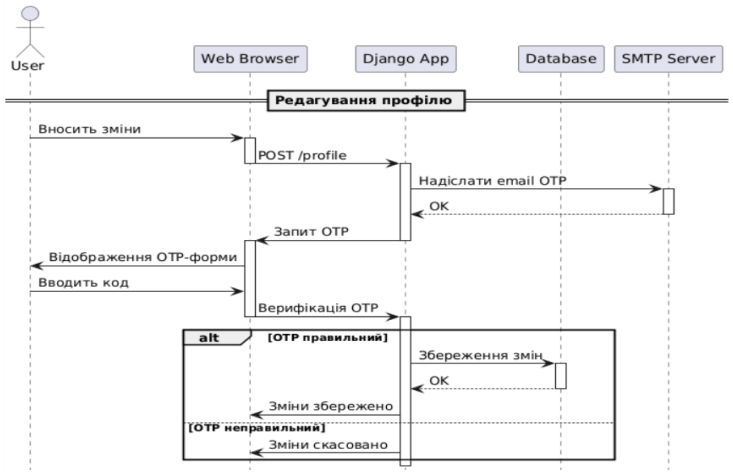

Рис. 4. Процес редагування профілю користувача

Для безпечної передачі інформації між клієнтом і сервером застосовується протокол HTTPS [16] у поєднанні з TLS. Під час встановлення з'єднання сторони узгоджують тимчасовий сесійний ключ, за допомогою якого шифрується трафік. Навіть у разі перехоплення потоку даних, без ключа інформація залишається недоступною для зловмисника. Враховуючи складність підбору ключа, злам такого з'єднання практично неможливий.

Забезпечення академічної доброчесності – ще один важливий аспект функціонування системи. Вона гарантує чесність, прозорість і довіру до результатів навчального процесу. Для запобігання несанкціонованого розповсюдження текстових матеріалів у системі реалізовано механізм додавання цифрових водяних знаків.

Водяний знак – унікальний ідентифікатор, який вбудовується у вміст тесту з метою захисту авторських прав і виявлення джерела витоку. У даній системі кожне запитання автоматично містить водяний знак, сформований на основі персональних даних користувача: його унікального ідентифікатора ID, прізвища, імені та дати народження.

Такий підхід дозволяє точно встановити, хто саме розповсюдив інформацію, якщо вона з'явилася у мережі, наприклад, на фото або знімку екрана. Генерований код вводиться у вигляді напівпрозорого сірого тексту над кожним запитанням, як це зображено на рис. 5.

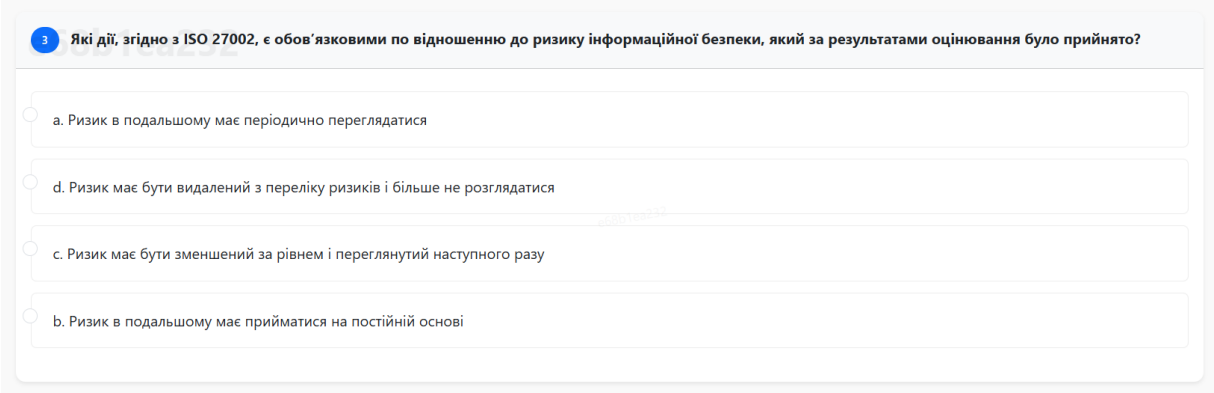

Рис. 5. Приклад розміщення водяного знаку на сайті

Для хешування використовується криптографічно стійка хеш-функція BLAKED2b [17], яка має властивість детермінованості, що дозволяє легко порівняти значення на зображенні з відповідним записом у базі даних, ідентифікувавши користувача, який порушив умови проходження опитування.

Інтерфейс системи розроблено відповідно до ролей користувачів – студентів та викладачів – з урахуванням типових сценаріїв взаємодії. Такий підхід забезпечує зручність, доступність та безпеку під час користування. Основу дизайну складають принципи мінімалізму й простоти, що дозволяє легко орієнтуватися навіть недосвідченим користувачам.

На головній сторінці розміщено назву системи, стислий опис її призначення та кнопку входу у верхній правій частині (рис. 6). Це забезпечує швидкий старт роботи з системою для обох категорій користувачів. Кнопка входу веде до стандартної форми авторизації. Дизайн головної сторінки побудований таким чином, щоб користувач відразу розумів основну мету ресурсу та легко орієнтувався.

Після авторизації з логіном і паролем, користувача перенаправляє на сторінку перевірки локації. Якщо виявлено нову IP-адресу, система запитує підтвердження через OTP-код, який надсилається на електронну пошту.

Це дозволяє запобігти спробам входу з невідомих пристроїв. Механізм реалізовано таким чином, щоб мінімізувати ризик несанкціонованого доступу. У разі відмови підтвердити нову локацію, доступ до акаунту блокується.

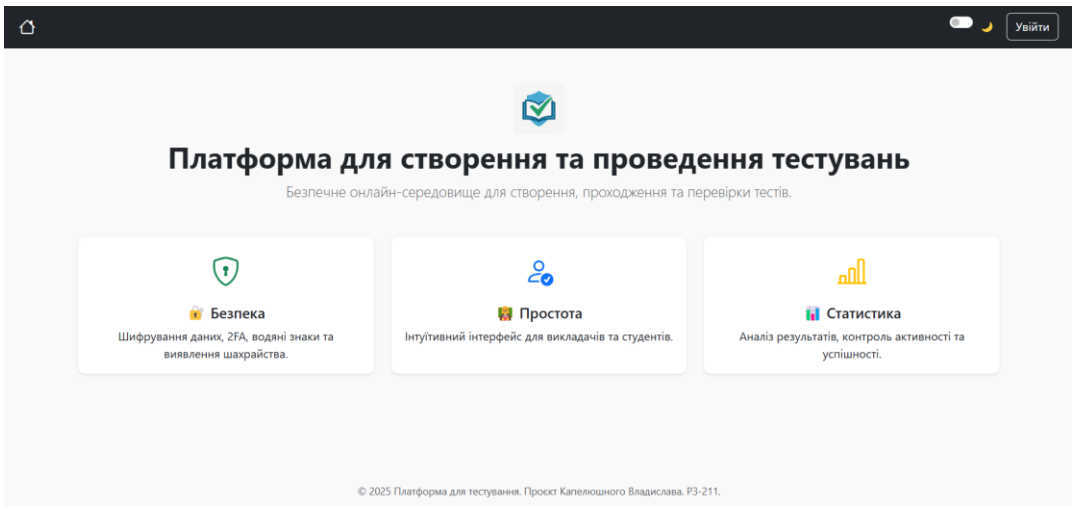

Рис. 6. Головна сторінка

При втраті пароля користувач може скористатися функцією «Забули пароль?». Після введення email-адреси, на пошту називається посилання для зміни пароля. Процес є простим та надійним, що забезпечує як зручність, так і захист акаунтів користувачів. Важливо що новий пароль повинен відповідати вимогам безпеки системи.

Кожен зареєстрований користувач має доступ до особистого профілю, де можна редагувати ім'я, прізвище, електронну пошту, номер телефону та аватар (рис. 7). Дана функціональність дозволяє підтримувати актуальність контактних даних. Усі зміни підтверджують кодом, який надходить на електронну пошту, що виключає можливість несанкціонованого редагування. Профіль має інтуїтивно зрозумілий інтерфейс редагування, що дозволяє легко оновлювати особисту інформацію.

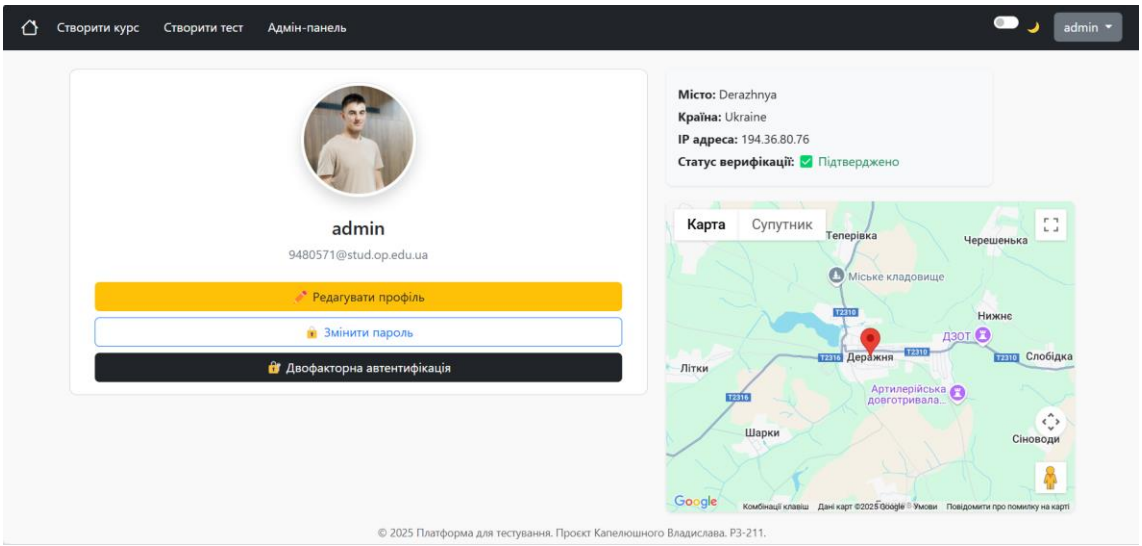

Рис. 7. Профіль користувача

Зміна пароля передбачає введення чинного пароля та нового – двічі, з додатковим підтвердженням через код з пошти, унеможливлюючи випадкову зміну пароля.

Для посилення безпеки реалізовано можливість активації двофакторної автентифікації через Google Authenticator. Процес налаштування 2FA передбачає сканування QR-коду або ведення секретного ключа вручну, після чого користувач

вводить шестизначний код із застосунка. Увімкнення цієї функції значно підвищує рівень захищеності облікового запису. Користувач також має змогу вимкнути двофакторну автентифікацію, підтвердивши цю дію через електронну пошту.

Для викладачів основним елементом взаємодії є панель адміністрування, яка надає доступ до керування курсами, тестами, користувачами та результатами. Панель має зручну навігацію та логічну структуру. Всі елементи згруповані за категоріями, що дозволяє швидко знаходити потрібні функції (рис. 8). Наприклад, викладач може перейти до списку наявних курсів, де зазначається назва, код доступу, кількість тестів і дата завершення. Кожен курс має набір кнопок для керування.

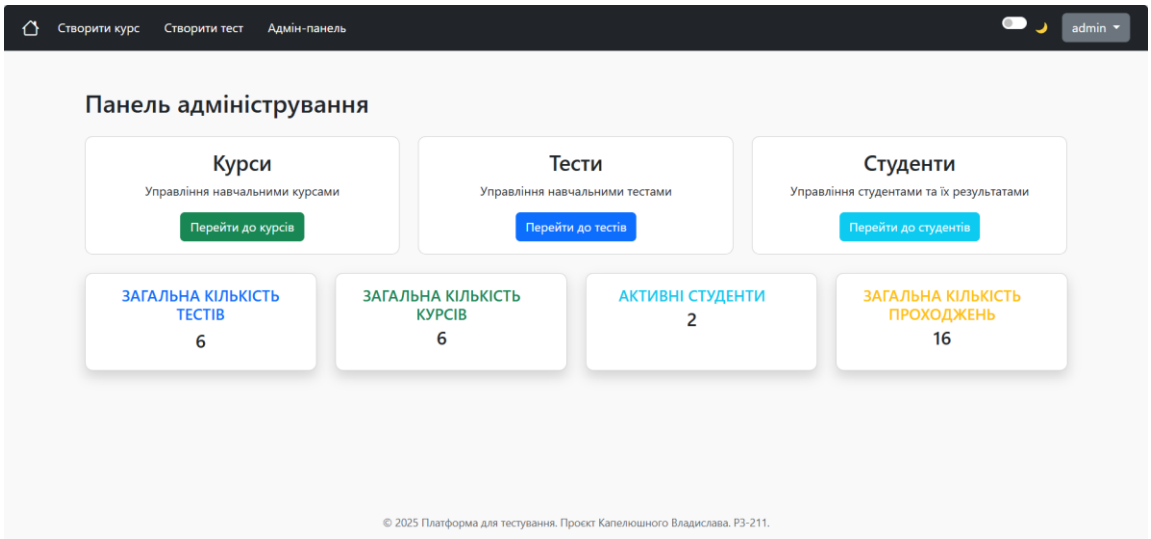

Рис. 8. Панель адміністрування

Кнопка «Створити курс» відкриває форму, в якій потрібно вказати назву, короткий опис і дату завершення. Код доступу до курсу генерується автоматично. Якщо дата завершення вказана – після неї тест буде недоступний. Курс може містити декілька тестів. Для перегляду результатів викладач може перейти до розділу статистики, де відображається ПІБ студента, отримані бали, дата проходження та кількість спроб. Інтерфейс також дозволяє виконувати пошук за курсом або студентом (рис. 9).

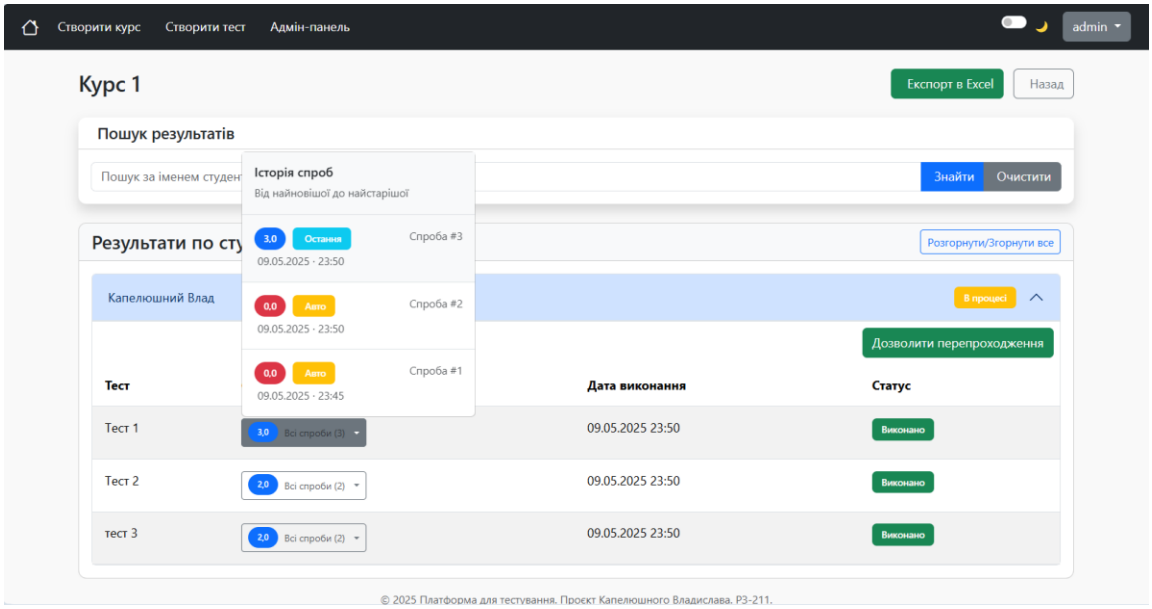

Рис. 9. Результати курсу

Відкривши вкладку «Перейти до тестів», викладач отримає доступ до списку всіх наявних в системі тестів, які можна редагувати та видаляти. При створенні нового тесту необхідно вказати назву, опис та пов'язаний курс. Після збереження, система автоматично перенаправляє користувача до інтерфейсу додавання запитань, що дозволяє безпосередньо після створення почати його наповнення контентом. Всі запитання можна редагувати, що забезпечує гнучкість при оновленні матеріалу (рис. 10).

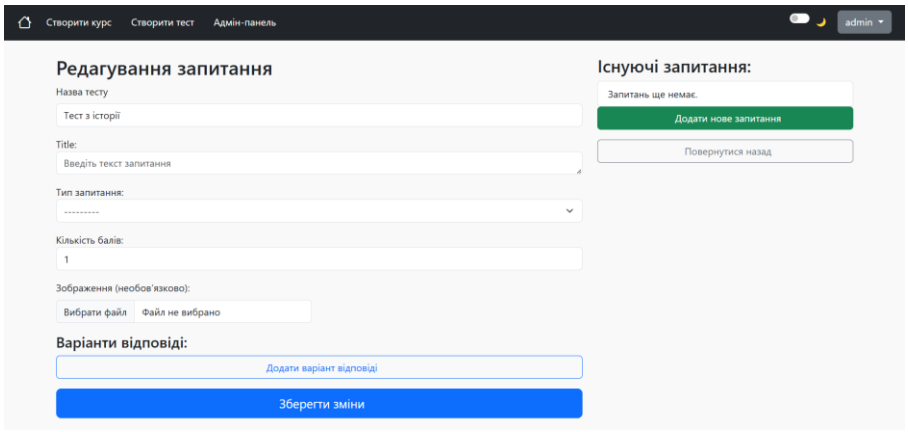

Рис. 10. Додавання запитань до тесту

Студенти після авторизації переходять до персональної панелі з вкладками: «Додати курс», «Додати тест», «Мої курси» та «Мої результати». Вони мають змогу додавати курс за кодом, який надає викладач. Якщо курс завершений або неактивний – система виведе відповідне повідомлення. Кожен студент може приєднатися до курсу лише один раз, після чого зберігає постійний доступ до всіх оновлень. У розділі мої курси студент бачить перелік приєднаних курсів та їх статус (рис. 11).

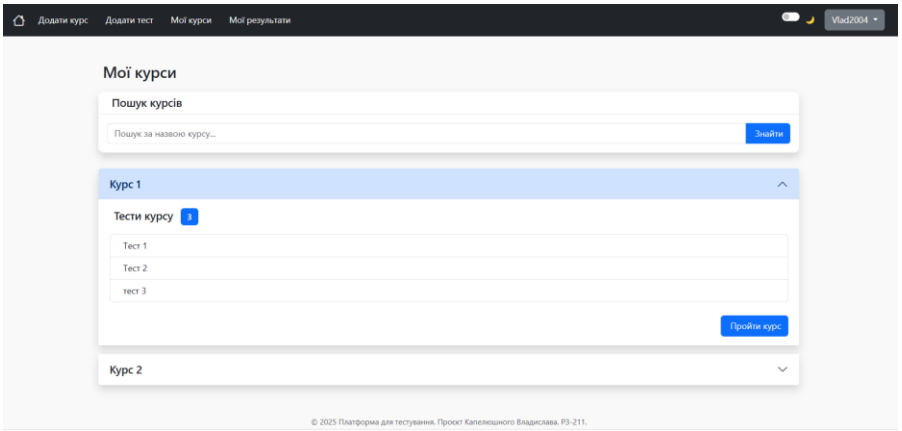

Рис. 11. Доступні для студента курси

Інтерфейс дозволяє швидко перейти до тестів, якщо вони активні. Під час проходження тесту студент бачить запитання з варіантів відповідей (рис. 12). Якщо запитання містить зображення – воно відображається праворуч. Студент може відповідати на питання у довільному порядку. Тест завершується вручну або автоматично – у випадку виходу користувача зі сторінки.

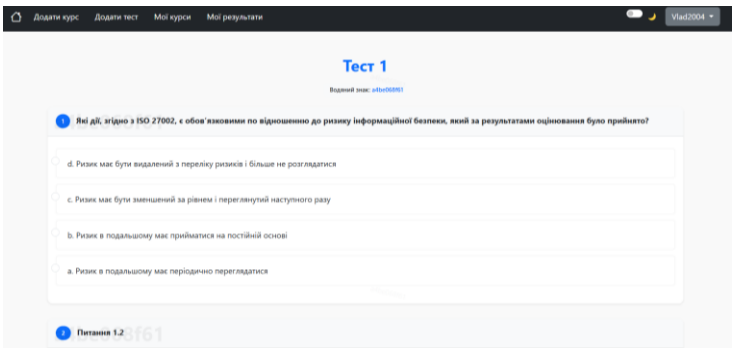

Рис. 12. Проходження тесту

Для реалізації системи було використано сучасні технології веб-програмування: Django, HTML, CSS, Bootstrap, PyCryptodome, що дозволило досягнути функціональної та візуальної відповідності потребам цільових користувачів. Інтерфейс системи адаптовано під ролі студентів та викладачів. Викладач може створювати курси, тести, редагувати запитання, контролювати кількість спроб проходження і переглядати результати. Студент може приєднуватися до курсів та тестів, проходити їх та переглядати свою статистику. Під час проходження тесту в кожному завдані відображаються водяні знаки, призначені для контролю академічної доброчесності та виявлення джерел витоку завдань. Реалізована система є комплексним безпечним рішенням для організації навчального процесу, враховуючи технічні вимоги та потреби користувачів залежно від їхніх ролей.

Висновки. У даній роботі було розглянуто ключові аспекти забезпечення безпеки системи опитувань, які є необхідною умовою для її ефективного та надійного функціонування. Визначено основні загрози пов'язані з використанням онлайн-систем, а також здійснено аналіз популярних сервісів з точки зору захисту персональних даних та відповідності сучасним вимогам кібербезпеки. Реалізована власна веб-система для створення та проведення опитувань, яка забезпечує широкий функціонал для тестування знань та надійний захист даних за допомогою сучасних механізмів інформаційної безпеки, а також має зручний і зрозумілий інтерфейс, адаптований під потреби викладачів та студентів. Описано реалізовані в системі механізми безпеки: шифрування даних в стані спокою, двофакторну автентифікацію, авторизацію на основі ролей, перевірку геолокації, політику складних паролів, автоматичне завершення сесій, захист від XSS-атак, підтвердження змін через електронну пошту, шифрування трафіку через HTTPS/TLC. Окрему увагу приділено академічній доброчесності. Запропоновано використання цифрових водяних знаків, для персоналізації кожного завдання та виявлення джерел витоку інформації. Такий підхід сприяє прозорості та контролю за розповсюдженням тестових матеріалів.

У сукупності реалізовані підходи дозволяють забезпечити високий рівень захисту системи опитувань, зберігаючи конфіденційність, цілісність та доступність даних, а також сприяють підтримуванню академічної етики в освітньому процесі. Розроблене програмне забезпечення може використовуватися як основа для впровадження в освітній процес навчальних закладів з метою безпечного й ефективного оцінювання знань. У перспективі можливе масштабування для розширення аналітики, підтримки мультимовності, додавання різних категорій завдань.

Список літератури

1. 32 Cybersecurity Stats You Can’t Ignore in 2025. https://segura.security/post/cybersecurity-stats-you-cant-ignore (дата звернення: 15.04.2025).
2. European Union Agency for Cybersecurity. Threat Landscape for Education Sector.https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

3. OWASP Foundation. Top 10 Security Risks for Web Applications. https://owasp.org/www-project-top-ten/
4. Zhang et al., Security Issues in Online Learning Platforms, IEEE Access. https://www.researchgate.net/publication/287717556_Security_Risks_and_Protection_in_Online_Learning_A_Survey
5. Google Форми: онлайн-редактор форм. https://workspace.google.com/products/forms/ (дата звернення: 02.05.2024).
6. Навчальні інструменти, картки та рішення з підручників. https://quizlet.com/ (дата звернення: 02.02.2025).
7. SurveyMonkey: The World's Most Popular Survey Platform. https://www.surveymonkey.com/?msockid=35a01cc759c3678138bb09d358d166a0 (дата звернення: 02.02.2025).
8. Google Forms. Безпека. https://www.google.com/intl/uk_ua/forms/about/#security (дата звернення: 05.02.2025).
9. Політика конфіденційності Quizlet. https://quizlet.com/privacy (дата звернення: 05.02.2025).
10. Two-factor authentication (2FA). https://help.surveymonkey.com/en/surveymonkey/account/two-factor-authentication/?utm_source=chatgpt.com#how-to-set-up-authenticator-app.
11. What happens to my data? – Help Center. https://help.typeform.com/hc/en-us/articles/360029581691 (дата звернення: 05.02.2025).
12. Aumasson J.-P. Serious Cryptography: A Practical Introduction to Modern Encryption. ed. by L. Chun. San Francisco, 2017. P. 59–75, 181-199.
13. Stallings W. Cryptography and Network Security: Principles and Practice. 7th ed. Global Edition / ed. by J. Tracy. Harlow, 2016. P. 177–179.
14. Що таке двофакторна автентифікація, і як вона працює. URL: https://cip.gov.ua/ua/faqs/sho-take-dvofaktorna-avtentifikaciya-i-yak-vona-pracyuye (дата звернення: 20.02.2025).
15. Cruz J. P., Kaji Y., Yanai N. RBAC-SC: Role-based access control using smart contract. IEEE Access. 2018. P. 12240–12251.
16. Gourley D., Totty B., Sayer M., Aggarwal A., Reddy S. HTTP: The Definitive Guide. O'Reilly Media, Inc., 2002.
17. Aumasson J.-P., Meier W., Phan R. C.-W., Henzen L. The hash function BLAKE. Springer, 2014. URL: https://content.e-bookshelf.de/media/reading/L-3932227-bec7a2b730.pdf

В.Р. Капелюшний, Н.І. Кушніренко, О.В. Троянський

A SECURE SYSTEM FOR CREATING AND CONDUCTING SURVEYS

V.R. Kapelyushnyi, N.I. Kushnirenko, O.V. Troyanskiy

National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine
Email: kushnirenko@op.edu.ua, o.v.troyanskiy@op.edu.ua

In the current conditions of digital transformation, security for online surveys is gaining special attention The relevance of this issue is driven by the widespread use of web services in the educational process, along with increased demands for the protection of personal data, the prevention of academic dishonesty, and the need to ensure transparency of results. The purpose of the work is to develop a secure web platform for creating, conducting and monitoring surveys that protects users' personal data, maintains academic integrity and meets modern cybersecurity requirements. The paper analyzes modern testing platforms (Google Forms, Quizlet, SurveyMonkey, Typeform), identifies their advantages and disadvantages in the context of security, in particular, limited support for two-factor authentication and weak data protection. A secure survey system with support for modern cryptographic protocols is proposed and implemented. The symmetric AES-256 encryption algorithm is used to protect the data, which guarantees the confidentiality and integrity of the stored results. The developed system also supports two-factor authentication, geolocation verification, email confirmation, HTTPS/TLC encryption, automatic session termination, and a digital watermarking mechanism that allows identifying the source of test content leakage. A practical implementation of an access control system has been carried out, including the creation of student and teacher roles and the introduction of a monitoring system for logins and changes. The results of the study confirm the feasibility of developing a custom platform as a free alternative to popular services with insufficient security levels. The proposed solution can be used in educational institutions to enhance the quality of knowledge assessment processes and ensure a high level of user data security.
Keywords: survey system, AES-256 encryption, cybersecurity, watermarks, RBAC, two-factor authentication, geolocation, academic integrity