УДК 004.432.2 : 004.738.5 DOI https://doi.org/10.35546/kntu2078-4481.2025.3.2.50

О. А. ПОНОМАРЬОВА
кандидат технічних наук, доцент,
доцент кафедри комп'ютерних наук, інформаційних технологій
та прикладної математики
ННІ «Придніпровська державна академія будівництва та архітектури»
Українського державного університету науки і технологій
ORCID: 0000-0003-1254-4403

Г. М. ГУЗЬ
асистент кафедри спеціалізованих комп'ютерних систем
ННІ «Український державний хіміко-технологічний університет»
Українського державного університету науки і технологій
ORCID: 0009-0002-2908-8985

Д. В. ГУЗЬ
інженер-програміст
Товариство з обмеженою відповідальністю «АЛЛО»

РОЗРОБКА СИСТЕМИ РЕЄСТРАЦІЇ ТА АВТОРИЗАЦІЇ КОРИСТУВАЧІВ У КЛІЄНТ-СЕРВЕРНОМУ WEB-ДОДАТКУ

У сучасних умовах стрімкого розвитку інформаційних технологій та зростання кількості web-додатків питання безпечної та ефективної реєстрації й авторизації користувачів набуває особливої актуальності.

Дана стаття розглядає процес розробки системи реєстрації та авторизації користувачів у web-додатку з клієнт-серверною архітектурою, що забезпечує надійний контроль доступу до ресурсів та персоналізовану взаємодію з користувачем.

Під час розробки було розглянуто ключові вимоги до систем автентифікації, серед яких безпека, масштабованість, зручність у використанні та відповідність актуальним стандартам. Проаналізовано поширені підходи до реалізації клієнт-серверної архітектури, зокрема застосування REST API, JSON Web Token (JWT), протоколу HTTPS, а також фреймворків для фронтенду та бекенду, таких як React, Node.js і Express.

Розроблена система передбачає двоетапний процес: реєстрацію нового користувача, а також авторизацію з використанням токенів доступу.

Розроблена форма реєстрації у web-додатку включає вбудовану валідацію рядків, яка перевіряє коректність введених даних – зокрема формат електронної пошти, складність пароля, його підтвердження та унікальність Email-адреси. Після успішної реєстрації на вказану пошту надсилається лист із підтвердженням, що містить унікальний токен для активації облікового запису. Після підтвердження користувач автоматично перенаправляється до вікна авторизації, де може увійти до системи за допомогою своїх облікових даних, що забезпечує безпечний і контрольований доступ до ресурсу.

Запропоноване рішення може бути інтегроване в різноманітні web-платформи, можливе масштабування, розширення функціоналу та інтеграції з іншими сервісами, зберігаючи високий рівень зручності використання для кінцевих користувачів. Розроблена система реєстрація та авторизації може бути застосована у різних галузях, де необхідно забезпечити надійну ідентифікацію користувачів та захист інформаційних ресурсів.

Ключові слова: *реєстрація, авторизація, клієнт-серверна архітектура, валідація, web-додаток, форма.*

O. A. PONOMAROVA
Candidate of Technical Sciences, Associate Professor,
Associate Professor at the Department of Computer Science,
Information Technologies and Applied Mathematics
SEI "Prydniprovska State Academy of Civil Engineering and Architecture"
of Ukrainian State University of Science and Technology
ORCID: 0000-0003-1254-4403

H. M. HUZ
Assistant at the Department of Specialized Computer Systems
SEI "Ukrainian State University of Chemical Technology"
of Ukrainian State University of Science and Technology
ORCID: 0009-0002-2908-8985

D. V. HUZ
Software Engineer
Limited Liability Company "ALLO"

DEVELOPMENT OF A USER REGISTRATION AND AUTHORIZATION SYSTEM FOR A CLIENT-SERVER WEB APPLICATION

In the current context of rapid development in information technologies and the growing number of web applications, the issue of secure and efficient user registration and authorization has become increasingly relevant. This article explores the process of developing a user registration and authorization system within a web application based on a client-server architecture, which ensures reliable access control and personalized user interaction.

During development, key requirements for authentication systems were considered, including security, scalability, usability, and compliance with modern standards. Common approaches to implementing client-server architecture were analyzed, particularly the use of REST API, JSON Web Token (JWT), HTTPS protocol, and frontend/backend frameworks such as React, Node.js, and Express.

The developed system features a two-stage process: registration of a new user and authorization using access tokens.

The registration form in the web application includes built-in string validation that checks the correctness of input data – the email format, password complexity, password confirmation, and uniqueness of the email address. Upon successful registration, a confirmation email is sent to the specified address containing a unique token for account activation. After confirmation, the user is automatically redirected to the login window, where they can access the system using their credentials, ensuring secure and controlled resource access.

The proposed solution can be integrated into various web platforms, with potential for scalability, functional expansion, and integration with other services, while maintaining a high level of usability for end users. The developed registration and authorization system can be applied across different industries where reliable user identification and protection of information resources are required.

Key words: *registration, authorization, client-server architecture, validation, web application, form.*

Постановка проблеми

У сучасному цифровому світі web-додатки є невід'ємною частиною повсякденного життя, бізнесу та комунікацій. Більшість з них вимагають взаємодії з користувачами, що передбачає наявність механізмів реєстрації та авторизації для забезпечення безпеки, персоналізації та контролю доступу.

Відсутність надійної системи автентифікації може призвести до витоків даних, несанкціонованого доступу та втрати довіри користувачів.

Проблема полягає в розробці ефективної, безпечної та масштабованої системи реєстрації та авторизації для web-додатку з клієнт-серверною архітектурою [1].

Клієнт-серверна модель передбачає поділ на клієнтську частину (frontend), яка взаємодіє з користувачем, та серверну частину (backend), яка обробляє запити, зберігає дані та забезпечує логіку автентифікації.

Отже, постає потреба у створенні комплексного рішення, яке поєднує надійний захист персональних даних, зручність для користувачів, масштабованість системи та відповідність сучасним веб-технологіям. Впровадження такого рішення сприятиме підвищенню безпеки web-додатків, покращенню користувацького досвіду та ефективному управлінню доступом у клієнт-серверній архітектурі.

Аналіз останніх досліджень і публікацій

Сучасні дослідження у сфері реєстрації та авторизації користувачів у клієнт-серверних web-додатках свідчать про поступовий перехід від традиційних методів, таких як паролі та SMS-коди, до безпечніших безпарольних рішень, зокрема passkeys.

Використання криптографії та апаратних засобів підвищує захист від фішингу та інших кіберзагроз. Стандарти WebAuthn Level 3 [2] і FIDO2 [3] визначають принципи безпечної автентифікації, а NIST SP 800-63B [4] пропонує рекомендації щодо різних рівнів автентифікації. Попри технічні переваги, широке впровадження обмежують питання відновлення доступу, сумісності з існуючими системами та регуляторні вимоги.

Формулювання мети дослідження

Метою розробки є проєктування та реалізація модуля реєстрації й авторизації користувачів у web-додатку з клієнт-серверною архітектурою, який забезпечує безпеку обробки даних, стійкість до атак та масштабованість для роботи з великою кількістю користувачів.

Викладення основного матеріалу дослідження

Форма реєстрації/авторизації – це інтерфейс, який дозволяє користувачам створювати обліковий запис на вебсайті або у додатку (реєстрація) та входити у вже існуючий (авторизація).

Форма реєстрації призначена для створення нового облікового запису. Як правило, містить наступні поля для введення:

– Ім'я користувача (логін);
– Електронна адреса;
– Пароль (його повторного введення для підтвердження);
– Іншої додаткової інформації (наприклад, номер телефону, дата народження).

Форма авторизації служить для входу в систему, якщо користувач вже має обліковий запис. Вона зазвичай містить поля для введення: Ім'я користувача (логін), Пароль.

Розробку починали зі створення візуального інтерфейсу вікна реєстрації. Для побудови форми у вікні реєстрації з полями для заповнення використовували Ant Design. Для реєстрації у web-додатку користувач повинен заповнити наступні поля: E-mail, Ваше ім'я, Пароль та Повторити пароль (рис. 1) та натиснути кнопку Зареєструватися [5].

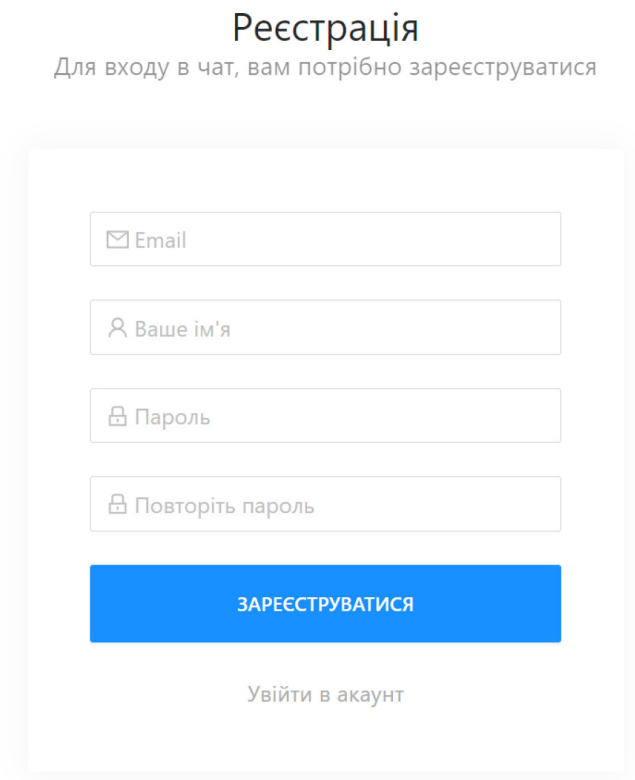


Рис. 1. Форма реєстрації

Як бачимо, форма розташована в центральній частині екрана. Це забезпечує фокус уваги користувача на основній дії – введенні даних. Вона складається з кількох логічних елементів.

Заголовок «Реєстрація» – чіткий, великий шрифт, розташований по центру. Він дає зрозуміти, у якій частині процесу перебуває користувач.

Пояснювальний підзаголовок – менший текст «Для входу в чат, вам потрібно зареєструватися». Виконує роль додаткової інструкції та мотивації.

Чотири поля вводу:

– Email – поле з іконкою конверта (символ пошти).
– Ваше ім'я – поле з іконкою користувача.
– Пароль – поле з іконкою замка, приховане введення.
– Повтор пароля – аналогічне до попереднього, але для підтвердження правильності введення.

Кнопка «Зареєструватися» – велика, синього кольору, з білим текстом, що чітко виділяється серед інших елементів. Такий колір часто обирають для основних дій, адже він привертає увагу.

Посилання «Увійти в акаунт» – розташоване під кнопкою, сірого кольору, меншого розміру, щоб не конкурувати з основною дією, але при цьому бути доступним.

Якщо під час реєстрації користувач залишить обов'язкові поля незаповненими, інтерфейс форми повідомить про некоректно введені дані (рис. 2). Перевірка коректності здійснюється за допомогою пакета Formik.

У разі коректного заповнення всіх полів форма реєстрації відображатиметься у вигляді, показаному на рис. 3.

Після натискання кнопки «Зареєструватися» виконується AJAX-запит, у якому введені користувачем дані передаються на сервер за вказаним маршрутом методом POST (створення маршрутів на сервері реалізовано за допомогою Express).

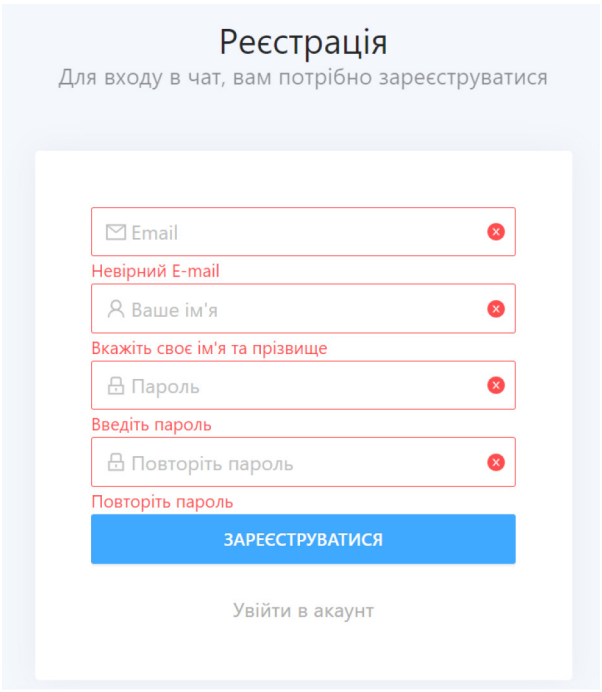


Рис. 2. Некоректне введення даних в форму реєстрації

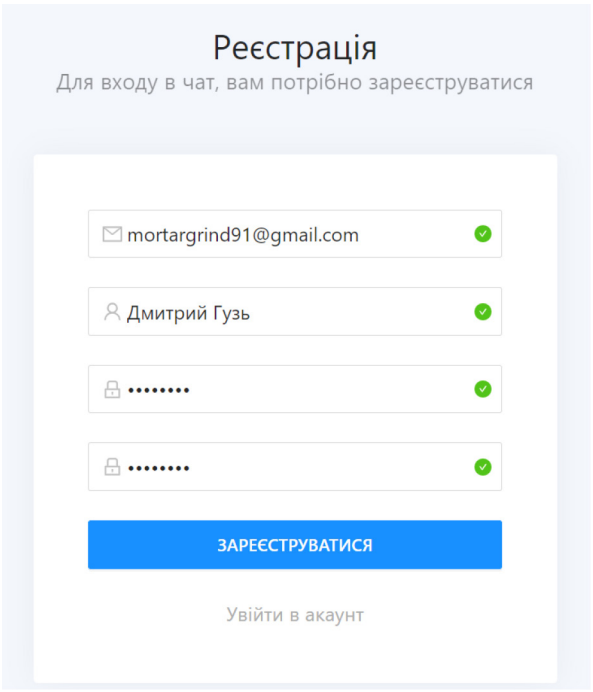


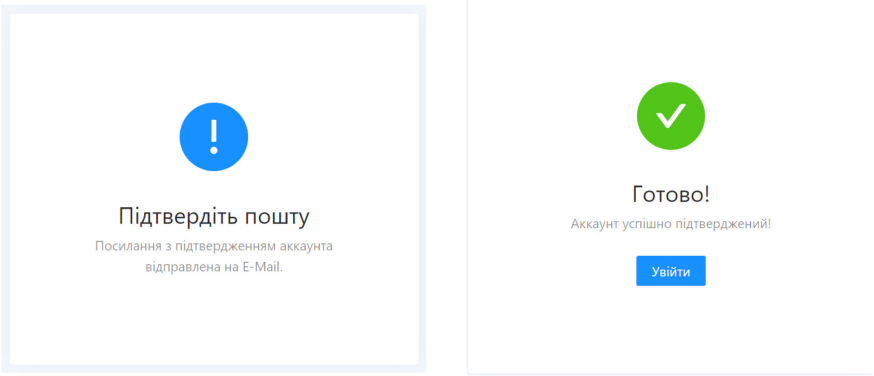
Рис. 3. Коректне введення даних в форму реєстрації

Отримана інформація зберігається у базі даних MongoDB, а також генерується хеш для подальшого підтвердження електронної пошти користувача. Після цього система переводить користувача на етап верифікації його E-mail (рис. 4, *а*).

На електронну пошту користувача надсилається лист, що містить згенероване посилання з URL-адресою та унікальним хешем, призначеним для підтвердження E-mail. Після натискання на отримане посилання користувач переходить на сторінку з підтвердженням успішного E-mail та кнопкою для входу в акаунт (рис. 4, *б*).

Щоб увійти у веб-додаток, потрібно натиснути кнопку «Увійти». Після цього відкривається сторінка авторизації.

У вікні авторизації (рис. 5) слід ввести E-mail та пароль, а потім натиснути кнопку «Увійти в акаунт».



а) **б)**

Рис. 4. Верифікація користувача:
а) Підтвердження E-mail; б) Успішне підтвердження E-mail

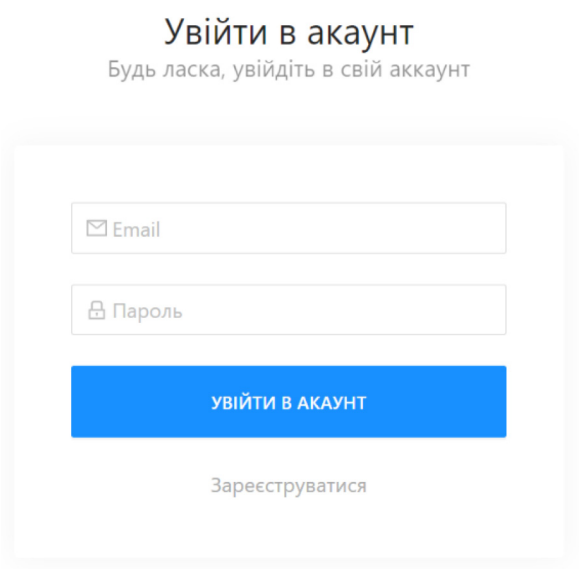


Рис. 5. Вікно авторизації

Якщо введені дані є некоректними або не збігаються з даними, зазначеними під час реєстрації, при натисканні кнопки «Увійти в акаунт» сервер повідомить про помилку введення (рис. 6).

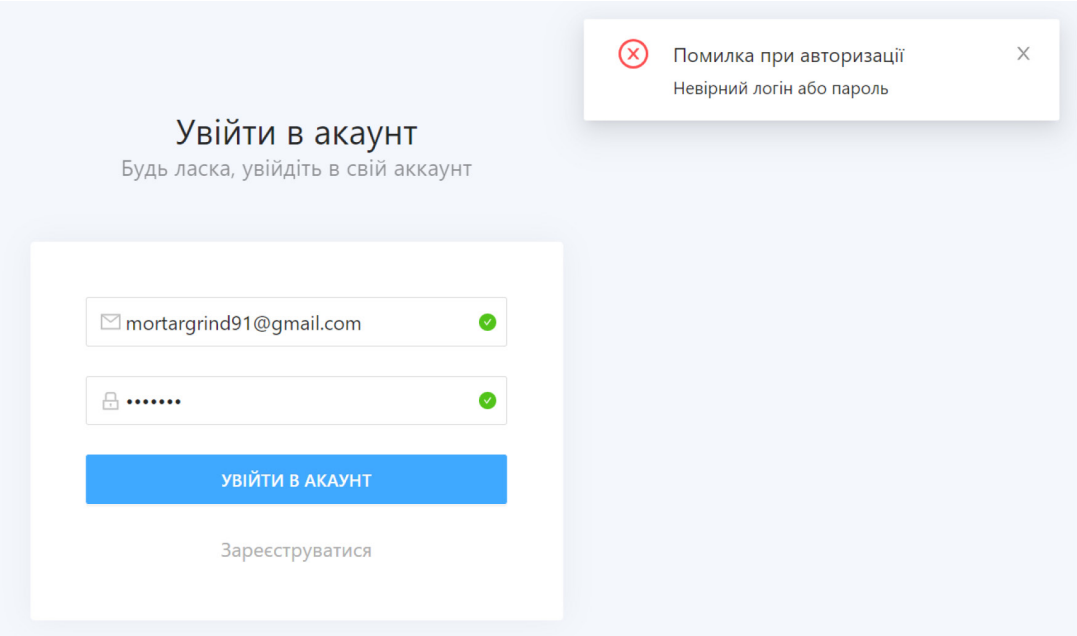


Рис. 6. Некоректні дані у вікні авторизації

Висновки

Розробка системи реєстрації та авторизації користувачів для web-додатку з клієнт-серверною архітектурою забезпечила створення надійного та ефективного механізму управління доступом, який гарантує безпеку зберігання конфіденційних даних, контроль прав користувачів та зручну взаємодію з інтерфейсом.

В процесі реалізації було створено інтуїтивно зрозумілий інтерфейс для введення даних, впроваджено комплексну валідацію на стороні клієнта та сервера, налаштовано обробку запитів і відображення повідомлень про успіх або помилки, а також застосовано сучасні заходи безпеки, включно з хешуванням паролів та захистом від несанкціонованого доступу.

Система продемонструвала високу практичну цінність, підвищуючи ефективність роботи web-додатку та рівень довіри користувачів, і має великий потенціал для подальшого розвитку, зокрема через впровадження функцій відновлення пароля, авторизації через соціальні мережі, розширене управління ролями користувачів та інтеграцію з іншими сервісами для забезпечення комплексної взаємодії.

Список використаної літератури

1. Мельник Р. А. Програмування веб-застосувань (фронт-енд та бек-енд). Львів : Львівська політехніка. 2018. 248 с.
2. Web Authentication: An API for accessing Public Key Credentials: веб-сайт. URL: https://www.w3.org/TR/webauthn-3/ (дата звернення 15.08.2025).
3. Passkeys: веб-сайт. URL: https://fidoalliance.org/passkeys/ (дата звернення 15.08.2025).
4. Digital Identity Guidelines Authentication and Lifecycle Management: веб-сайт. URL: https://pages.nist.gov/800-63-3/sp800-63b.html (дата звернення 15.08.2025).
5. Гузь Д. В., Пономарьова О. А. Розробка веб-додатку для спілкування між користувачами з використанням клієнт-серверних технологій. *Науковий процес та наукові підходи: методика та реалізація досліджень*: матеріали міжнародної конференції, 23 жовтня 2020 р. Одеса: МЦНД, 2020. С. 52–53.

References

1. Melnyk, R.A. (2018). Prohramuvannia veb-zastosuvan (front-end ta bek-end) [Web application programming (front-end and back-end)]. Lviv : Lvivska politekhnika. [in Ukrainian].
2. Web Authentication: An API for accessing Public Key Credentials. (2019). W3C. https://www.w3.org/TR/webauthn-3/
3. FIDO Alliance. (n.d.). Passkeys. https://fidoalliance.org/passkeys/
4. National Institute of Standards and Technology. (n.d.). *Digital identity guidelines: Authentication and lifecycle management* (SP 800-63B). NIST. Retrieved August 15, 2025, from https://pages.nist.gov/800-63-3/sp800-63b.html
5. Huz D. V., Ponomarova O. A. (2020) Rozrobka veb-dodatku dlia spilkuvannia mizh korystuvachamy z vykorystanniam kliient-servernykh tekhnolohii. [Development of a web application for communication between users using client-server technologies]. Naukovyi protses ta naukovi pidkhody: metodyka ta realizatsiia doslidzhen: materialy mizhnarodnoi konferentsii. pp. 52–53.

Дата першого надходження рукопису до видання: 20.09.2025
Дата прийнятого до друку рукопису після рецензування: 16.10.2025
Дата публікації: 28.11.2025