УДК 004.9

А.О. Азарова
В.В. Поліщук

ПРОГРАМНО-АПАРАТНИЙ КОМПЛЕКС ОНЛАЙН РЕКРУТИНГУ ІЗ ЗАСТОСУВАННЯМ ЗАСОБІВ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ

Вінницький національний технічний університет

Анотація

У роботі описано підхід до розроблення програмно-апаратного комплексу онлайн-пошуку роботи та підбору персоналу з використанням двофакторної біометричної ідентифікації. Підвищення достовірності користувачів досягається шляхом впровадження механізмів автентифікації, що унеможливлюють несанкціонований доступ до облікових записів. У межах роботи запропоновано використання біометричних підходів: розпізнавання обличчя та аналізу клавіатурного почерку як складових архітектури системи. Додатково передбачено удосконалення функціоналу сервісу, зокрема структурованість вакансій і резюме, можливість інтеграції портфоліо та впровадження контролю своєчасності зворотного зв'язку з боку роботодавців. Очікується, що запропоновані рішення сприятимуть підвищенню достовірності користувачів і ефективності процесу онлайн-рекрутингу.

Ключові слова: *програмно-апаратний комплекс, онлайн-рекрутинг, біометрична ідентифікація, FaceID, клавіатурний почерк.*

Abstract

The paper considers an approach to the development of a hardware-software complex for online job search and recruitment using two-factor biometric identification. Improving the reliability of users is achieved through the implementation of authentication mechanisms that prevent unauthorized access to user accounts. Within the framework of the study, the use of biometric approaches – facial recognition and keystroke dynamics analysis – is proposed as components of the system architecture. Additionally, improvements to the system functionality are proposed, including structured job postings and resumes, the ability to integrate portfolios, and the implementation of response time control for employers. It is expected that the proposed solutions will enhance user reliability and improve the efficiency of the online recruitment process.

Keywords: *hardware-software complex, online recruitment, biometric identification, FaceID, keystroke dynamics.*

Вступ

Онлайн-сервіси пошуку роботи сьогодні користуються значним попитом, оскільки ринок праці є динамічним: компанії постійно розвиваються, а фахівці прагнуть професійного зростання [1]. З урахуванням поширення різних форматів зайнятості (офлайн, дистанційної та гібридної) такі сервіси слугують основною точкою взаємодії між кандидатами та роботодавцями. Це зумовлює необхідність створення зручних, ефективних і надійних рішень для організації процесу рекрутингу [2].

Аналіз існуючих програмних рішень [3], відгуків користувачів та практичного досвіду їх використання свідчить, що попри загальну функціональність і доступність, вони мають низку недоліків, пов'язаних із достовірністю інформації, неповнотою профілів та недостатнім контролем взаємодії між користувачами. Необхідність розроблення підходу, спрямованого на підвищення достовірності користувачів у системі, зумовлена такими чинниками: наявність фіктивних або недостовірних облікових записів; відсутність ефективних механізмів перевірки особи користувача; недостатній рівень довіри між учасниками процесу рекрутингу.

Отже, побудова програмно-апаратного комплексу з використанням біометричних методів ідентифікації є **актуальною** задачею, оскільки уможливлює підвищення рівня захищеності облікових записів та забезпечує участь у системі реальних користувачів. Додаткове удосконалення функціоналу спрямоване на підвищення якості інформаційного наповнення та ефективності взаємодії між сторонами. **Метою** даного дослідження є підвищення достовірності користувачів у системі онлайн-рекрутингу шляхом розроблення програмно-апаратного комплексу з використанням двофакторної біометричної ідентифікації та удосконалення функціоналу сервісу.

Основна частина

Основною задачею розроблюваного програмно-апаратного комплексу онлайн-рекрутингу є підвищення достовірності користувачів. Запропонований підхід передбачає впровадження механізмів, що забезпечують участь у системі лише реальних осіб – як з боку шукачів роботи, так і з боку роботодавців (представників компаній або їх керівників). Основою організації доступу є рольова модель, яка передбачає розподіл користувачів за ролями з відповідними правами та функціональними можливостями.

Для підтвердження особи застосовуються біометричні методи автентифікації [4]. Крім стандартної пари логін–пароль, користувач додатково ідентифікується за геометрією обличчя та клавіатурним почерком. Реалізація цих підходів у вигляді окремих модулів забезпечує багатофакторну перевірку користувача як під час реєстрації, так і в процесі подальшої роботи із системою.

Відповідно до аналізу існуючих рішень у сфері онлайн-рекрутингу доцільним є усунення виявлених типових недоліків шляхом підвищення структурованості даних та якості взаємодії між користувачами. Зокрема, у розроблюваній системі передбачено контроль структури сторінок, заповнення обов'язкових полів. Такі дії надають можливість забезпечити наявність ключової інформації для прийняття рішень. Також передбачається часткове вирішення проблеми відсутності зворотного зв'язку шляхом впровадження рейтингової моделі взаємодії, що базується на факті наявності або відсутності відповіді у визначений проміжок часу. Додатково для підвищення зручності користування передбачено вбудоване портфоліо, яке дозволяє зберігати приклади робіт без використання зовнішніх сервісів. Реалізація цих удосконалень здійснюється в межах окремого функціонального модуля програмно-апаратного комплексу онлайн-рекрутингу.

На рис. 1 наведемо структурну схему архітектури програмно-апаратного комплексу онлайн-пошуку роботи та підбору персоналу з використанням біометричної ідентифікації.

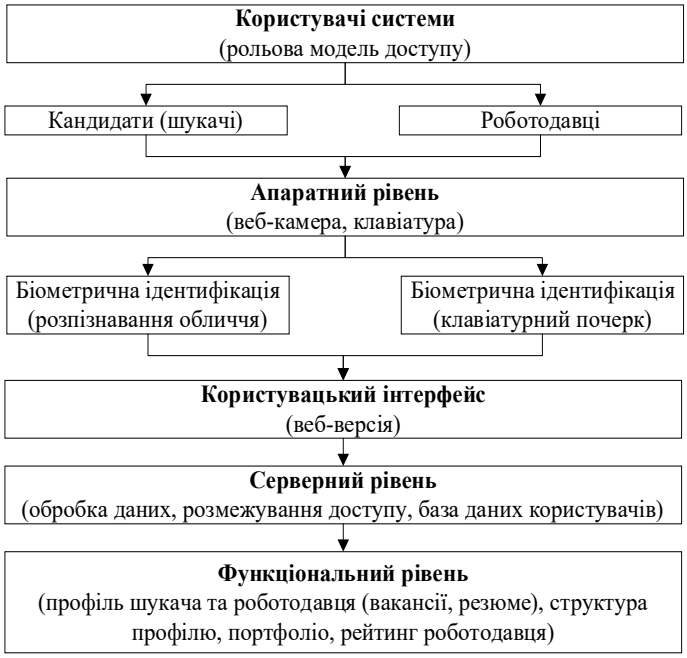

Рис. 1. Архітектура програмно-апаратного комплексу онлайн-рекрутингу

Відповідно до представленої на рис. 1 архітектури, у межах розроблюваного програмно-апаратного комплексу реалізовано двофакторну біометричну автентифікацію користувачів, що поєднує два незалежні підходи: розпізнавання обличчя та аналіз клавіатурного почерку. Така комбінація дозволяє підвищити надійність перевірки особи з використання доступних для користувачів апаратних засобів.

Для розробки модуля автентифікації на основі FaceID [5] використано загальний підхід до формування та порівняння біометричних ознак. У реалізації безпосередньо використовується етап формування ознакового представлення обличчя, тоді як процедура порівняння може бути реалізована на основі метрик відстані, зокрема евклідової.

Базові можливості обраного підходу включають: захоплення фото-, відеопотоку з камери; попереднє оброблення зображення (зміна розміру, перетворення у відтінки сірого); виділення ключових областей зображення (зокрема обличчя); порівняння отриманого зразка з еталонними даними.

Для реалізації функції FaceID в роботі пропонується підхід на основі детекції ознак. В такому випадку зображення аналізується як сукупність характерних структурних елементів. Після виділення обличчя формується числове представлення (ознаковий вектор), яке надалі використовується для математичного порівняння з еталонним профілем користувача.

Опишемо базову математичну модель біометричної автентифікації, що складається з послідовності етапів. На першому етапі виконується перетворення кольорового зображення у відтінки сірого, що дозволяє зменшити обчислювальну складність та підвищити стабільність оброблення:

$$I_{gray} = 0.299R + 0.587G + 0.114B \tag{1.1}$$

де R, G, B – значення червоного, зеленого та синього каналів.

Далі зображення подається у вигляді матриці інтенсивностей пікселів I, яка нормалізується для зменшення впливу умов освітлення:

$$I_{norm} = \frac{I - I_{min}}{I_{max} - I_{min}} \tag{1.2}$$

де I_{max} та I_{min} – мінімальне та максимальне значення інтенсивності.

Після обробки формується ознаковий вектор обличчя F, який містить значення пікселів нормалізованого зображення розміром 32×32:

$$F = \{f1, f2, \dots, f_{1024}\} \tag{1.3}$$

де f_i – значення і-го елемента вектора.

Порівняння поточного зразка F з еталонним F' виконується через евклідову відстань:

$$D = \sqrt{\sum_{i-1}^{n} (f_i - f_i')^2} \tag{1.4}$$

де n – кількість ознак.

Рішення про автентифікацію приймається за умовою:

$$D < T \tag{1.5}$$

де T – порогове значення допустимого відхилення.

У модулі поведінкової біометричної ідентифікації використовується класичний часовий підхід аналізу клавіатурного почерку [6, 7]. Як ознака користувача застосовуються інтервали між послідовними натисканнями клавіш. Отримані часові характеристики формують вектор ознак, який використовується для подальшого порівняння з еталонним профілем користувача, представляються як:

$$D_i = t_{i+1} - t_i \tag{1.6}$$

де D_i – інтервал між послідовними натисканнями клавіш, t_{i+1}, t_i – моменти часу натискання відповідних клавіш.

На основі цих значень формується вектор ознак користувача:

$$K = \{D_1, D_2, \dots, D_n\} \tag{1.7}$$

де K – поведінковий профіль клавіатурного почерку, n – кількість інтервалів у контрольній фразі.

Порівняння поточного профілю з еталонним здійснюється через обчислення евклідової відстані (1.4). Рішення про відповідність користувача приймається за результатами перевірки умови (1.5).

Застосування біометричної ідентифікації за рахунок розпізнавання обличчя та аналізу клавіатурного почерку дозволяє реалізувати багатофакторну перевірку користувача [8, 9]. Оскільки дані параметри є статичними та поведінковими ознаками, така комбінація підвищує загальний рівень захисту системи.

Для вдосконалення функціональної частини програмно-апаратного комплексу передбачено реалізацію таких заходів: контроль структури профілю користувача; часовий контроль зворотного зв’язку від роботодавців; впровадження вбудованого резюме та профілю-«візитки» для організацій.

Таким чином, запропоновані в роботі удосконалення функціоналу спрямовані на підвищення якості взаємодії між користувачами системи. Формуються більш прозорі і відповідальні механізмів комунікації між кандидатами та роботодавцями, що дозволяє покращити ефективність процесу підбору працівників та вакансій.

Висновки

Запропонований в роботі підхід спрямований на підвищення достовірності користувачів у програмно-апаратному комплексі онлайн-рекрутингу. Таке рішення безпосередньо впливає на якість взаємодії між шукачами роботи та роботодавцями. Під час аналізу існуючих аналогів виявлено низку типових проблем. Зокрема, виявленими недоліками є поширення недостовірних або неповних даних у профілях користувачів, а також відсутність ефективних механізмів перевірки особи. Це ускладнює процес підбору персоналу та знижує ефективність використання подібних систем у практичних умовах.

Для вирішення зазначених проблем у роботі запропоновано апаратний підхід до підвищення достовірності, що базується на використанні двофакторної біометричної ідентифікації. Зокрема, реалізовано автентифікацію за геометрією обличчя з використанням методів комп'ютерного зору, а також поведінкову ідентифікацію на основі клавіатурного почерку. Такий підхід дозволяє поєднати статичні та динамічні біометричні ознаки користувача. Додатково, для підвищення функціональної ефективності системи, запропоновано удосконалення структури профілів користувачів, впровадження рейтингової системи взаємодії та інтеграцію вбудованого портфоліо. Це забезпечує більш прозорий обмін інформацією та підвищує відповідальність сторін у процесі рекрутингу. Таким чином, реалізоване рішення на основі двофакторної біометричної ідентифікації та удосконаленого функціоналу системи дозволяє підвищити рівень достовірності користувачів, покращити якість даних у профілях та забезпечити більш ефективний і надійний процес онлайн-рекрутингу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Азарова А., Міронова Ю., Шиян А., Ярмола О. Аналіз недоліків та переваг сучасних HR-систем для оптимізації роботи підприємств. *Вісник Хмельницького національного університету. Економічні науки.* 2023. № 2. С. 89 – 96.

2. Ілляш І., Баб'як Г. Сучасні технології у сфері рекрутингу персоналу. *Регіональні аспекти розвитку продуктивних сил України.* 2023. № 28. С. 112–123. URL: https://doi.org/10.35774/rarrpsu2023.28.112 (дата звернення: 24.04.2026).

3. Платформи пошуку роботи | Університет Короля Данила. Університет Короля Данила. URL: https://ukd.edu.ua/platformy-poshuku-roboty (дата звернення: 24.04.2026).

4. Лісовський Б., Журавель І. Автентифікація користувача в інформаційних системах на основі біометричних сигналів мобільних пристроїв. Сучасний захист інформації. 2025. Т. 64, № 4. С. 116–122. URL: https://doi.org/10.31673/2409-7292.2025.041211 (дата звернення: 24.04.2026).

5. Гребенюк А. М., Прокопов С. О., Рибальченко Л. В. Використання технологій розпізнавання обличчя на відео- та фотозображеннях : метод. рекоменд. / А. М. Гребенюк, С. О. Прокопов, Л .В. Рибальченко. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2023. 48 с.

6. Бутенко Л. І., Шарадкін Д. М. Безперервна біометрична автентифікація користувачів на основі клавіатурного почерку. *Computer-integrated technologies: education, science, production.* 2025. № 61. С. 319–329. URL: https://doi.org/10.36910/6775-2524-0560-2025-61-41 (дата звернення: 24.04.2026).

7. Коваленко С., Красножон О. Методи первинної обробки даних у системах ідентифікації користувачів на основі клавіатурного почерка. *Технічні науки та технології.* 2025. № 2 (40). С. 294–302. URL: https://doi.org/10.25140/2411-5363-2025-2(40)-294-302 (дата звернення: 24.04.2026).

8. Азарова А. О., Богачук В. В., Безмощук О. В. Автентифікації користувачів засобами технології Face ID на основі вдосконаленого методу фільтрування зображення. *Тези Всеукраїнської науково-практичної інтернет конференції студентів, аспірантів та молодих науковців «молодь в науці: дослідження, проблеми, перспективи». 2022.* URL : https://conferences.vntu.edu.ua/index.php/mn/mn2022/paper/viewfile/14176/11988 (дата звернення: 24.04.2026).

Азарова Анжеліка Олексіївна **–** кандидат технічних наук, професор кафедри менеджменту та безпеки інформаційних систем Вінницького національного технічного університету, м. Вінниця

Поліщук Вадим Вікторович **–** студент групи КІ-24мз, Факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця

Anzhelika Azarova **–** PhD in technique, Professor of the Department of Management and Information Systems Security, Vinnytsia National Technical University, Vinnytsia

Vadym Polishchuk − Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia