

# ОСОБЛИВОСТІ ВИКОРИСТАННЯ МОДУЛІВ ІДЕНТИФІКАЦІЇ ТИПУ КОРИСТУВАЧА ПРИ АВТОРИЗАЦІЇ

Вінницький національний технічний університет

## **Анотація**

*Авторизація користувачів є важливою складовою процесу забезпечення безпеки в системах обробки та передачі даних. Програмний модуль ідентифікації типу користувача є ключовим елементом авторизації, який дозволяє системі перевірити рівень доступу користувача до вмісту або функцій, які він намагається отримати. Модуль працює на основі даних, що зберігаються в базі даних користувачів, і використовує різноманітні методи ідентифікації, такі як аутентифікація з використанням логіну та паролю, використання біометричних даних або ідентифікація на основі сертифікатів. Використання програмного модуля ідентифікації типу користувача забезпечує безпеку системи та зручний спосіб управління доступом користувачів, що дозволяє адміністраторам системи швидко відключати доступ користувачам, що вже не мають права доступу.*

**Ключові слова:** програмний модуль, ідентифікація користувача, передача даних, система.

## **Abstract**

*User authorization is an important component of the process of ensuring security in data processing and transmission systems. The user type identification software module is a key element of authorization that allows the system to verify a user's level of access to the content or features they are trying to access. This module works on the basis of data stored in the user database and uses a variety of identification methods, such as login and password authentication, biometrics or certificate-based identification. The use of the user type identification software module provides system security and a convenient way to manage user access, allowing system administrators to quickly disable access to users who no longer have access rights.*

**Keywords:** software module, user identification, data transfer, system.

## **Вступ**

Системи обробки та передачі даних в сучасному світі є необхідною складовою для багатьох галузей та сфер діяльності, починаючи від бізнесу та закінчуючи наукою та технікою. Одним із найважливіших аспектів у роботі таких систем є забезпечення надійного та безпечного доступу [1, 2]. Для цього використовуються різноманітні методи та технології авторизації, що дозволяють відокремити користувачів та забезпечити їм доступ до потрібної інформації [1].

Одним із таких методів є використання програмного модуля ідентифікації типу користувача [3]. Цей модуль дає можливість ідентифікувати користувачів та надавати їм доступ до певних ресурсів відповідно до їх ролі в системі. Це може бути особливо важливо для великих організацій зі значною кількістю користувачів, де потрібно забезпечити різні рівні доступу до інформації.

Програмний модуль ідентифікації типу користувача може використовувати різноманітні методи для ідентифікації користувача, включаючи малювання заданих об'єктів, введення пароля, біометричну ідентифікацію та інші. Кожен з цих методів має свої переваги та недоліки, тому вибір методу залежить від конкретних потреб та обставин [2, 4].

Метою роботи є розробка програмного модуля ідентифікації типу користувача для авторизації користувача за допомогою використання інтерактивних візуальних об'єктів, зокрема необхідність малювання заданого об'єкту.

## **Результати досліджень**

Програмний модуль ідентифікації типу користувача в системах обробки і передачі даних є ключовим елементом процесу авторизації, який дозволяє системі перевірити, що користувач має відповідний рівень доступу до вмісту або функцій, які він намагається отримати.

Цей модуль зазвичай працює на основі даних, що зберігаються в базі даних користувачів, де кожен користувач має свій унікальний ідентифікатор і список дозволених дій. При запиті на авторизацію, модуль перевіряє ідентифікатор та пароль користувача, після чого визначає його тип і рівень доступу до системи [3, 5].

Залежно від конфігурації системи, модуль може використовувати різноманітні методи ідентифікації, такі як аутентифікація з використанням логіну та паролю, використання біометричних даних або ідентифікація на основі сертифікатів [5]. Більш складні системи можуть включати багатофакторну аутентифікацію, де користувач повинен пройти кілька етапів перевірки, щоб отримати доступ.

Використання візуальних елементів (включаючи використання візуальних елементів) у програмних модулях авторизації може мати деякі переваги, такі як:

1. Захист від автоматизованих атак. Багато зловмисників використовують автоматизовані скрипти для намагання взлому систем авторизації. Використання візуальних елементів може допомогти унеможливити або ускладнити такі атаки, оскільки скрипти не зможуть розпізнати та малювати об'єкти на екрані [7].

2. Захист від підбору паролів. Іноді зловмисники намагаються підібрати паролі шляхом перебору. Використання візуальних елементів може зменшити ризик успішної атаки, оскільки користувачі повинні малювати задані об'єкти, а не вводити прості числові або текстові паролі [4].

3. Створення привабливого інтерфейсу. Візуальні елементи можуть створити більш привабливий та легко зрозумілий інтерфейс для користувачів. Це може допомогти покращити користувацький досвід та знизити ризик помилкових авторизацій [4].

4. Надійність. Візуальні елементи можуть бути складнішими для розпізнання іншими людьми, що дозволяє забезпечити більш надійний рівень захисту. Крім того, візуальні елементи можуть бути досить складними для розпізнання для зловмисників, що допомагає зменшити ризик злому [6].

Незважаючи на переваги використання візуальних елементів у програмних модулях авторизації, вони можуть також викликати певні проблеми зі зручністю використання та прозорістю процесу авторизації для користувачів, тому що їх ефективність може бути обмеженою у випадку з користувачами, які мають обмежені здібності до малювання або візуального сприйняття [5].

### **Висновки**

Отже, в даній роботі було розглянуто використання програмного модуля ідентифікації типу користувача в системах обробки та передачі даних при авторизації. Було показано, що такий модуль дає можливість ідентифікувати користувачів та забезпечити їм доступ до потрібної інформації відповідно до їх ролі в системі.

Особлива увага була приділена використанню візуальних елементів, зокрема малюванню заданих об'єктів, як методу ідентифікації користувача. Було проаналізовано переваги цього методу, зокрема висока стійкість до атак злому та його простота для користувачів, а також недоліки, зокрема низьку швидкість та можливу непридатність для деяких користувачів з моторними порушеннями або низьким рівнем візуальних навичок.

У цілому, використання програмного модуля ідентифікації типу користувача є важливою складовою для забезпечення безпеки та надійності систем обробки та передачі даних. Кожен метод ідентифікації має свої переваги та недоліки, тому вибір конкретного методу залежить від потреб та особливостей користувачів системи.

### **СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ**

1. Authentication and Access Control in Web Applications. Lieven Desmet. [Електронний ресурс]. Режим доступу: <https://www.springer.com/gp/book/9780387724175>. Дата звернення: Березень 2023.

2. Identification of Users in Networked Environments: Challenges and Opportunities. Andrea Atzeni. [Електронний ресурс]. Режим доступу: <https://link.springer.com/book/10.1007/978-3-319-04651-8>. Дата звернення: Березень 2023.

3. "User Identification and Authentication in Web Services" (автор: Bhavani Thuraisingham). [Електронний ресурс]. Режим доступу: <https://www.springer.com/gp/book/9780387772824>. Дата звернення: Березень 2023.

4. Designing Secure and Usable Authentication Systems. Susan Wiedenbeck). [Електронний ресурс]. Режим доступу: <https://www.springer.com/gp/book/9781441920715>. Дата звернення: Березень 2023.

5. Authentication Technologies for Cloud Computing, IoT and Big Data. Banshidhar Majhi) [Електронний ресурс]. Режим доступу: <https://www.springer.com/gp/book/9789811068775>. Дата звернення: Березень 2023.

6. User Authentication Techniques for Computer Systems. Dario Catalano. [Електронний ресурс]. Режим доступу: <https://www.springer.com/gp/book/9781447123934>. Дата звернення: Березень 2023.

7. Secure and Resilient Software: Requirements, Test Cases, and Applications. Prof. Chris Hankin. [Електронний ресурс]. Режим доступу: <https://www.springer.com/gp/book/9783319764401>. Дата звернення: Березень 2023.

**Крикливий Кирило Юрійович** – студент групи ІКН-196, факультет інтелектуальних інформаційних технологій та автоматизації, Вінницький національний технічний університет, м. Вінниця, e-mail:sususik52@gmail.com.

**Іванчук Ярослав Володимирович** – д-р техн. наук, професор, професор кафедри комп'ютерних наук, Вінницький національний технічний університет, м. Вінниця.

**Kyrylo Kryklyvyi U.** – Faculty of Automation and Intelligent Information Technology, Vinnytsia National Technical University, Vinnytsia, e-mail: sususik52@gmail.com.

**Ivanchuk Yaroslav V.** — Dr. Sc. (Eng.), Professor of the Computer Science Department, Vinnytsia National Technical University, Vinnytsia.