УДК 004.056.523:57.087.1]:621.39

АНАЛІЗ БІОМЕТРИЧНИХ МЕТОДІВ АВТЕНТИФІКАЦІЇ В ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Лавренчук А.А., Пастушенко М.С.
e-mail: andrii.lavrenchuk@nure.ua
Харківський національний університет радіоелектроніки, каф. ІКІ
м. Харків, Україна

Biometric authentication methods play a crucial role in ensuring security in modern infocommunication networks. Traditional authentication methods, such as passwords and tokens, present significant vulnerabilities, including theft, forgery, and management complexity. Biometric systems leverage unique physiological and behavioral characteristics for user identification, offering higher reliability and ease of use.

The paper highlights innovative biometric authentication methods, including neuroauthentication via EEG signals, dynamic biometrics based on eye micro-movements and gait analysis, and countermeasures against deepfake-based threats. It also explores blockchain-based biometric template protection and quantum-resistant cryptography as future-proofing measures.

Із розвитком інфокомунікаційних технологій питання безпечної ідентифікації користувачів набуває особливої актуальності. Традиційні способи автентифікації, зокрема паролі та токени, мають значні недоліки, серед яких можливість їх крадіжки, підробки та складність адміністрування. У зв’язку з цим біометричні методи автентифікації, що базуються на унікальних фізіологічних та поведінкових характеристиках людини, стають все більш популярними завдяки їхній надійності та зручності.

Методи автентифікації можна поділити на три основні категорії: використання паролів, токенів та біометричних характеристик. Біометричні системи спираються на унікальні риси кожного користувача, які поділяються на фізіологічні (наприклад, відбитки пальців, сканування райдужної оболонки ока, аналіз обличчя, ДНК) та поведінкові (зокрема голос, особливості почерку, стиль натискання клавіш). Ефективність таких систем оцінюється за параметрами рівня хибного прийняття (FAR), рівня хибного відхилення (FRR) та точки рівноваги помилок (EER). Крім того, впровадження біометричних технологій регулюється міжнародними стандартами, такими як ISO/IEC 19794, рекомендації NIST та вимоги GDPR щодо захисту персональних даних [1].

Сучасний розвиток біометричних методів включає такі інноваційні напрямки:

— Нейроавтентифікація (EEG) – застосування електроенцефалографічних сигналів для ідентифікації особи.

— Динамічна біометрія – аналіз мікрорухів очей та використання IMU-сенсорів для розпізнавання унікальної ходи користувача.

— Протидія Deepfake-загрозам – дослідження методів створення підроблених біометричних даних та способів їх виявлення.

— Захист біометричних шаблонів – застосування технологій блокчейну для надійного зберігання біометричних даних.

— Квантово-стійка криптографія – розробка методів захисту біометричних даних від потенційних загроз з боку квантових обчислень [2].

Біометрична автентифікація все ширше застосовується в сучасних концепціях безпеки, таких як Zero Trust Architecture та IoT. Проте існують певні ризики, зокрема можливі атаки на біометричні дані: Presentation Attack (спроби обману системи шляхом підробки біометричних характеристик), Deepfake-атаки та компрометація сховищ біометричних шаблонів. Надійність таких систем можна підвищити завдяки використанню мультимодальної автентифікації, застосуванню блокчейну для децентралізованого зберігання шаблонів та вдосконаленню криптографічного захисту даних [3].

У межах дослідження було розроблено експериментальну платформу для тестування біометричних технологій у реальних умовах. Отримані результати підтвердили високу точність методів автентифікації та дозволили виявити потенційні слабкі місця. Особливу увагу було приділено аналізу стійкості біометричних систем до атак, таких як Deepfake, Spoofing та Replay Attack. Також проведено моделювання захищеного середовища для біометричних технологій, що дозволяє оцінити перспективи їхнього подальшого розвитку у сфері інформаційної безпеки.

Результати дослідження підтвердили ефективність біометричних методів автентифікації та їхню перспективність у забезпеченні безпеки інформаційних систем. Практична значущість роботи полягає у можливості інтеграції розглянутих методів у реальні кіберзахисні системи. Подальші дослідження можуть зосереджуватися на розвитку технологій нейроавтентифікації, покращенні захисту біометричних шаблонів та впровадженні квантово-стійких методів шифрування.

Список використаних джерел:

1. Нечипоренко О.В., Корпань Я.В. Біометрична ідентифікація і автентифікація особи за геометрією обличчя. *Вісник Національного університету «Львівська політехніка»*. Львів, 2015 №824, С. 66–67.

2. Швець В., Фесенко А. *Основні біометричні характеристики, сучасні системи та технології біометричної аутентифікації*. Безпека інформації, 2013.№9, С. 99.