

СИСТЕМИ АУТЕНТИФІКАЦІЇ НА ОСНОВІ БІОМЕТРИЧНИХ ДАНИХ

Системи аутентифікації на основі біометричних даних використовують унікальні фізіологічні та поведінкові характеристики, такі як відбитки пальців, риси обличчя або візерунки райдужної оболонки ока, для перевірки особи. Вони забезпечують вищий рівень безпеки порівняно з традиційними методами, як-от паролі, які легко втратити або викрасти. Аналізуючи унікальні маркери, такі системи дозволяють ефективно контролювати доступ у фінансовій, медичній та інших сферах, забезпечуючи надійність і зручність [1].

Сучасні системи аутентифікації – це комплекс технологій та методів, спрямованих на підтвердження особи користувача, який намагається отримати доступ до інформаційних ресурсів. Вони еволюціонували від простих паролів до складних біометричних систем, що враховують унікальні фізіологічні та поведінкові характеристики людини.

Основні типи сучасних систем аутентифікації:

- Парольна аутентифікація – найпоширеніший метод, але має ряд недоліків, таких як вразливість до зламу та необхідність запам'ятовувати складні паролі.
- Багатофакторна аутентифікація вимагає використання двох або більше факторів аутентифікації, що значно підвищує рівень безпеки.
- Біометрична аутентифікація використовує унікальні фізіологічні або поведінкові характеристики людини, такі як відбитки пальців, розпізнавання обличчя тощо.
- Аутентифікація на основі сертифікатів використовує цифрові сертифікати для підтвердження особи користувача.
- Аутентифікація на основі токенів використовує фізичні або програмні токени для генерації одноразових паролів.

Аналіз та порівняння існуючих біометричних систем є важливим етапом для розуміння їхніх можливостей, обмежень та сфери застосування.

Основні типи біометричних систем:

- Фізіологічні: відбитки пальців, розпізнавання обличчя, райдужна оболонка ока, геометрія руки.
- Поведінкові: розпізнавання голосу, динаміка підпису, натискання клавіш.

Критерії порівняння[2]:

- Точність – помилки хибного прийняття і хибного відхилення.
- Швидкість – час, необхідний для аутентифікації.
- Зручність – простота використання.
- Вартість – витрати на обладнання та впровадження.
- Безпека – стійкість до підробки.
- Прийнятність – сприйняття користувачами.

У таблиці 1 представлено порівняння існуючих типів біометричних систем за вище згаданими критеріями.

Таблиця 1

Порівняння існуючих типів біометричних систем

Характеристика	Відбитки пальців	Розпізнавання обличчя	Райдужна оболонка ока	Розпізнавання голосу
Точність	Висока	Середня	Висока	Середня
Швидкість	Висока	Висока	Висока	Середня
Зручність	Висока	Висока	Середня	Висока
Вартість	Низька	Середня	Висока	Низька
Безпека	Середня	Середня	Висока	Низька

Сучасні системи аутентифікації знаходяться на етапі трансформації, де традиційні методи поступово замінюються більш надійними та зручними рішеннями. Біометрична аутентифікація відіграє ключову роль у підвищенні рівня захисту, а багатофакторна біометрична аутентифікація є перспективним напрямком розвитку. Важливо враховувати етичні та юридичні аспекти використання біометричних даних, а також забезпечувати їхній захист від несанкціонованого доступу.

Список використаних джерел:

1. Tirfe D., Anand V.K. A Survey on Trends of Two-Factor Authentication. In: Sarma H.K.D., Balas V.E., Bhuyan B., Dutta N. (eds) Contemporary Issues in Communication, Cloud and Big Data Analytics. Lecture Notes in Networks and Systems, vol 281. Springer, Singapore, 2022.
2. Скорик Ю., Костромицький А., Копиця А. Порівняння видів біометричних пристроїв. Міжнародний науковий журнал інженерії та сільського господарства, 3 (5), 1–7, 2024.