

Анотація

Рассматриваются проблемы повышения интереса к изучению украинского языка путем использования фольклора и игровых приемов.

*П. В. Стефаненко,
Донецкий национальный технический университет*

**ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ БІОМЕТРИЧНОГО
МОНІТОРИНГУ ПРИ ДИСТАНЦІЙНОМУ НАВЧАННІ
У ВИЩІЙ ШКОЛІ**

Порівняльний аналіз дистанційної та традиційної форм навчання у вищій школі дозволяє крім істотних переваг визначити й деякі «вузькі місця» дистанційної форми. Одне з них — зниження якості навчання внаслідок ймовірної «підміни» особистості студента в процесі контролю отриманих їм знань. Таким чином, однією з найважливіших проблем дистанційного навчання (ДН) є проблема ідентифікації особистості студента в процесі дистанційного контролю й оцінки отриманих ним знань.

Однак ступінь розвитку науки та техніки на цей час дозволяє використовувати досить ефективні способи рішення цієї проблеми. Одним з них, на наш погляд, є застосування **технологій біометричного моніторингу** до ідентифікації особистості студента.

Інтенсивний розвиток цих технологій в останні роки зв'язують, насамперед, з виробництвом технічних систем, що забезпечують безпеку доступу до конфіденційної інформації. Через це основними сферами застосування подібних систем у цей час є системи безпеки фінансових, виробничих та інших бізнес-структур.

Однак крім захисту доступу людини до фізичних об'єктів, сферою застосування цих систем є *реєстрація користувача в комп'ютерній мережі й одержання доступу до інформації*. До таких сфер можна віднести й дистанційне навчання. У цьому випадку дистанційна реєстрація студента в комп'ютерній мережі освітньої установи визначає доступ до системи оцінки знань. Через це в процесі ДН оцінюються знання тільки «легальних користувачів»,

отже, технології біометричного моніторингу можна вважати елементом, що підсилює ступінь інтегративності дистанційного навчання.

Фундаментальну основу функціонування біометричних систем складає **біометрія** — наукова дисципліна, що вивчає способи виміру різних параметрів людини з метою встановлення подібності (розходження) між людьми та виділення однієї конкретної людини з безлічі інших людей [1]. Вимір параметрів здійснюється за допомогою методів статистики, тому біометрію часто ще називають статистичною наукою про біологічні явища [2].

Вимір параметрів людини здійснюється за допомогою методів *динамічними та статичними образами* (рис. 1).

Джерелом статичних образів є генна структура людини. До них відносять, наприклад, відбитки пальців та геометрію руки.

Джерелом динамічних образів є імпульси м'язів людини. До них відносять рукописні та голосові образи.

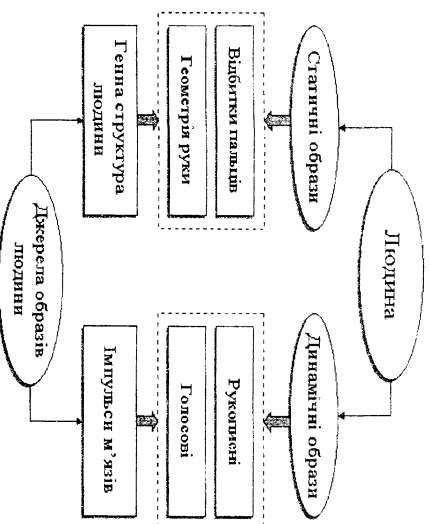


Рис. 1 Об'єкти біометричної ідентифікації

Таким чином, біометричні системи сканують такі унікальні параметри людини, як характеристики ока, голосу, відбитків пальців та рук [2].

Зокрема, при дистанційному навчанні під час контролю знань, на наш погляд, доцільно використовувати технологію ідентифікації **особистості за таким динамічним образом, як клавіатурний почерк**. Слід зазначити, що елементи цієї технології застосовува-

лися ще для ідентифікації особистості телеграфіста за його «почерком», що виявлявся в процесі передачі інформації кодом Морзе [1].

Загальний принцип функціонування скануючої біометричної системи полягає в тому, що вона фіксує наступні параметри: час натискання кожної клавіші й тривалість інтервалу часу між натисканням *чергової та відпусканням попередньої клавіш*.

Найпростіший графічний опис цього процесу на прикладі слова «навчання», що вводиться з клавіатури студентом, представлений на рис. 2.

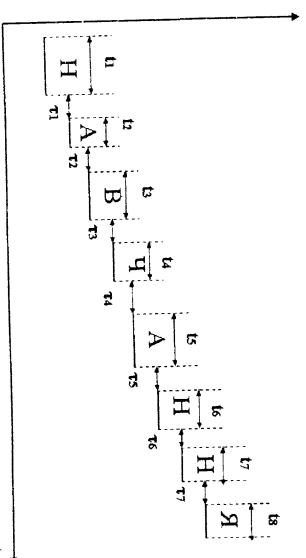


Рис. 2 Часова діаграма введення слова «Навчання»

На рис. 2 видно, що час натискання клавіш $t_1, t_2, t_3, \dots, t_8$, а також інтервали часу між натисканням сусідніх клавіш різні. Отже, ці контрольовані параметри можуть бути використані для виявлення «*індивідуального клавіатурного почерку*» студента.

Цей почерк залежить від характерних для користувача сполучень рухів різних пальців руки й від характерних рухів рук при наборі. Причому точність його сканування є максимальною у тому випадку, якщо студент набирає текст за «сліпим» методом з використанням усіх пальців обох рук.

Крім того, технологія біометричної ідентифікації припускає, що ідентифікацію зручно проводити на підставі деякої *парольної фрази*. Практика показує, що парольна фраза повинна легко запам'ятовуватись та містити **від 21 до 42** натискань на клавіші [1]. З урахуванням цього обмеження, можна експериментально під час пропуску ідентифікації клавіатурного почерку студента вибрати парольну фразу з числа деяких стандартних фраз, що використовуються при оформленні текстових документів (напри-

лад, на титульному листі), чи з числа специфічних термінів кон-
кретної навчальної дисципліни. Перевага пароліної фрази в біо-
метричній теорії ідентифікації в порівнянні з класичними паро-
лями полягає в тому, що помилка, яку студент може зробити в
деякому символі, не впливає на кінцевий результат ідентифікації
(з урахуванням обмеження на кількість помилок).

Дані приділимо увагу деяким математичним питанням іден-
тифікації. Розпізнавання біометричного образу здійснюється в
результаті порівняння показників, що його характеризують, з де-
яким *біометричним еталоном*.

Біометричний образ (БО) — це образ людини, що спостері-
гається безпосередньо системою без використання будь-яких опе-
рацій з його попередньої обробки та масштабування [1]. У нашо-
му випадку біометричним образом є індивідуальний клавіатур-
ний почерк студента.

Біометричний еталон (БЕ) — це дані про стабільну частину
контрольованих біометричних параметрів та їхніх присуттєвимих
відхилень, що зберігаються в біометричній системі для наступно-
го порівняння з ними біометричних образів [1]. Вид еталона виз-
начається *вирішальними правилами*, що прийнято в системі.

Наприклад, у найпростішому випадку стабільна частина кон-
трольованих біометричних параметрів та їхніх відхилень визнача-
ються двома показниками математичної статистики: *математич-
ним чеканням та дисперсією*. Саме ці параметри визначають вирі-
шальне правило, на підставі якого здійснюється ідентифікація
особистості студента.

Збереження еталонних даних усіх санкціонованих користу-
вачів здійснюється в **біометричній системі**, тобто такій технічній
системі, яка побудована на вимірі біометричних параметрів осо-
бистості та здатна після навчання її розпізнавати [1].

З пими еталонними даними порівнюються характеристики
знов запропонованих біометричних образів, тобто контрольова-
них параметрів клавіатурного почерку студентів, ідентифікація
особистості яких здійснюється в процесі контролю виконання
конкретного завдання.

Для формального виміру близькості еталонних даних та біо-
образів, що пропонуються системі, застосовують математичні
методи, засновані на розрахунку «відстаней» (наприклад, мір
близькості Евкліда, Хеммінга).

Відзначимо, що в процесі ДН можна користуватися існую-
чими комерційними програмними продуктами ринку біометрич-
них технологій. У разі потреби, за умови збереження рентабель-
ності ДН, можна розробити індивідуальну біометричну систему.
Для цього необхідне залучення дослідників у сфері проектування
(наукових працівників) та розроблювачів біометричних систем
(інженерів).

Крім того, фундаментальний підхід до розробки біометричної
системи передбачає виконання всіх пропелдур класичного процесу
формування біометричного еталона, представлених на рис. 3.

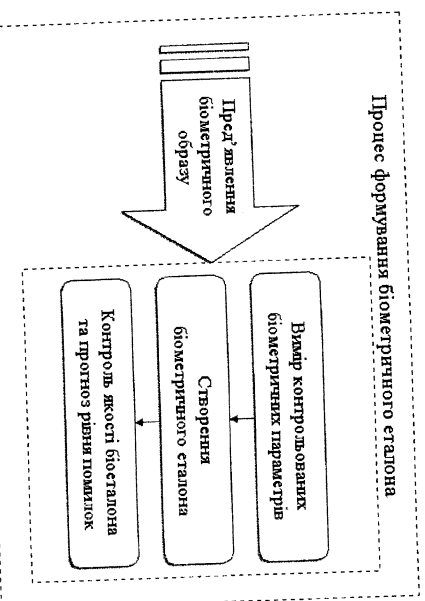


Рис. 3 Процедура формування біометричного еталона

Однак у цей час багато розроблювачів програм виконують
тільки перші 2 процедури, не звертаючи уваги на діапазони мож-
ливих помилок ідентифікації, які, в свою чергу, розділяють на 2
класи: помилки першого роду та помилки другого роду.

Помилки першого роду передбачають прийняття зареєстрова-
ного легального користувача за «зловмисника», а **помилки другого
роду** — прийняття зловмисника за легального користувача (зарее-
строваного студента).

Внаслідок стрімкої комерціалізації ринку біометричних тех-
нологій виробники подібних систем фактично диктують спожив-
вачам **випільні для себе умови та просядють системи, які орієнтовані
на середньостатистичного користувача** [1]. В першу чергу, таке їхнє
поводження обумовлено недостатнім рівнем конкуренції на рин-

ку біометричних систем, який знаходиться на стадії початкового розвитку. Крім того, низький рівень якості ідентифікації унікальних характеристик людини системою може бути результатом невдалого вибору пароля. При розробці індивідуальної біометричної системи варто враховувати усі вищевказані моменти.

Далі необхідно розглянути особливості *принципової схеми функціонування сучасних біометричних систем*. Перш ніж перейти до безпосереднього опису схеми, визначимо, що процес ідентифікації особистості студента в термінах біометрії зветься *аутентифікацією*.

Аутентифікація — це процес доказу та перевірки дійсності заявленого елементом інформаційної технології імені в рамках визначеного протоколу [1]. Іншими словами, аутентифікація — це процес перевірки дійсності «особистості», проведений в інтегресах інстанції, що розподіляє повноваження [2]. У даному випадку, установи освіти, що надає студентам послуги в сфері дистанційного навчання.

При цьому під «доступом до обчислювальних ресурсів» у даному випадку мається на увазі реєстрація студента в *дисципліній системі оцінки знань*.

На відміну від звичайної ідентифікації цей процес припускає **низький рівень довіри до особистості**, яку тестують. Це означає, що студент про проведення аутентифікації знати не повинен.

В основі схеми цього процесу полягає навчання на множині, що складається з декількох прикладів біометричних образів користувача (студента). Таким чином, у цьому випадку ми маємо справу з *роботою систем штучного інтелекту, що заснована на прикладах, тобто з функціонуванням нейронних мереж* [3, 4].

За цих умов процедура аутентифікації зводиться до взаємодії певних учасників навчального процесу (рис. 4).

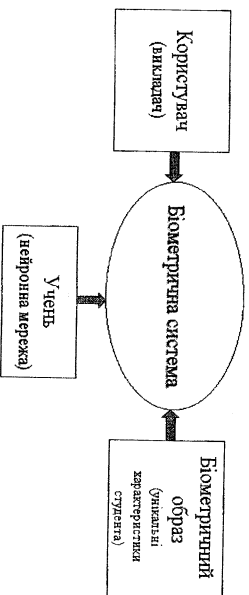


Рис. 4. «Учасники» процесу аутентифікації

У цьому процесі «*вчителем*» в загальному випадку є користувач біометричної системи. В процесі ДН ним є викладач. Його функція під час аутентифікації зводиться до того, що він пред'являє біометричній системі *приклади різних варіантів* біометричних образів (унікальних характеристик студентів), тобто *екзотери кон- трольованих параметрів*. Вони можуть бути представлені, наприклад, у вигляді багаторазового повторення попередньо встановленої паролльної фрази.

Приклади контрольованих параметрів подаються безпосередньо на вхід нейронної мережі, що у сукупності з певним алгоритмом навчання є «*учнем*» біометричної системи та може знаходитися в двох режимах: **режимі навчання та режимі тестування якості навчання**.

Застосування нейронних мереж як обчислювального базису біометричних систем обумовлене тим, що динамічні образи особистості мають властивість мінливості в часі. З урахуванням цієї властивості для більш точного формування визначеного еталона користувачу система необхідно задати кілька прикладів реалізації одного біометричного образу. Навчання на прикладах і є визначальною характеристикою *штучних нейронних мереж (ШНМ)*.

Для ШНМ такі параметри, як число входів нейрона, число нейронів, вид *функції збудження* [4], число шарів мережі, вид зв'язків у мережі, варто розглядати як параметри *структури вивільного правила*, на підставі якого здійснюється ідентифікація особистості студента.

При цьому параметри біометричного еталона конкретного студента містять у собі значення ваг нейронної мережі та значення коефіцієнтів, що зміцнюють, для конкретної особистості.

Слід зазначити, що нейромережні вирішальні правила є найбільш точними при прийнятті рішення, чим звичайні алгоритми, засновані на обчисленні тільки *математичного чекання та дисперсії*.

Алгоритми роботи системи біометричної аутентифікації містять такі операції:

1. Перетворення неелектричних величин (при клавіатурному моніторингу — положення рук) в електричні сигнали;
2. Кодування сигналів та введення їх у процесор, що здійснює програмну обробку даних;

3. Масштабування амплітуд вхідних сигналів та пошук для них формального еталонного значення;
4. Приведення сигналів до єдиного масштабу часу;
5. Обчислення вектора функціоналів (вектора контрольованих параметрів), що можуть бути лінійними та нелінійними;
6. Назначання системи як сукупність операцій, що здійснюється з обміркованим вектором параметрів [1].

У загальному випадку при наявності в базі даних еталона конкретного студента оцінка його знань можлива тільки при «влученні» його біометричного образу в припустиму область «СВІЙ» (рис. 5).

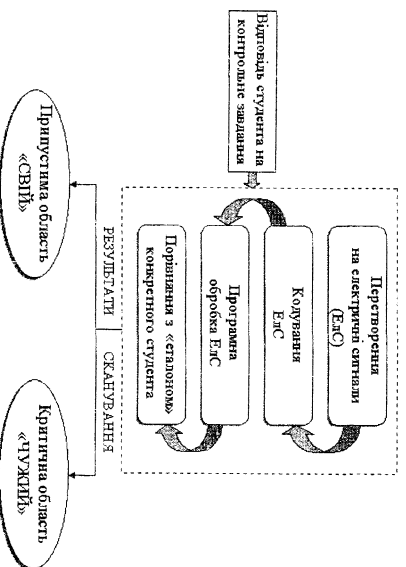


Рис. 5 Обробка відповіді студента біометричною системою

1, завершуючи розгляд загальних принципів біометричної ідентифікації, відзначимо, що в процесі олержання студентом дистанційної освіти необхідно враховувати технічні аспекти захисту системи сканування дійсності доступу, тому що в процесі функціонування ДН може виникнути потреба навмисної деформації біометричного еталона одним з користувачів біометричної системи.

Через це необхідно регулярно здійснювати аудит біометричної інформашії (АБІ).

АБІ — це процес, що припускає ресетрацію, збереження й обробку результатів біометричної аутентифікації за досить дов-

гий інтервал часу з метою виявлення спроб атак на біометричні фрагменти системи захисту [1].
Виходячи з цього, загальна схема процесу аутентифікації представлена на рис. 6.

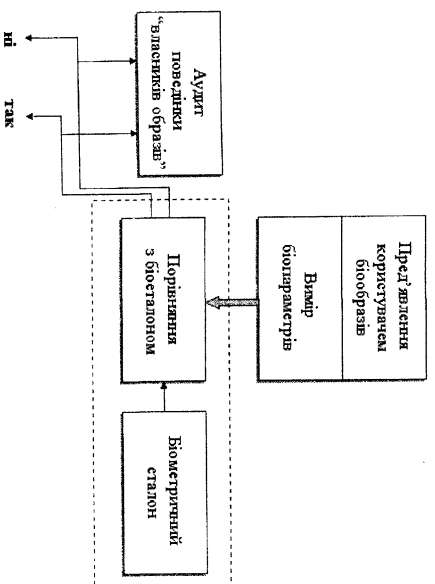


Рис. 6 Загальна схема біометричної аутентифікації

Таким чином, ми розглянули можливість застосування технологій біометричного моніторингу в процесі дистанційного навчання. Ці технології дозволяють підвищити ефективність ДН через поліпшення якості навчання за допомогою використання методів ідентифікації особистості студента, який навчається за дистанційною формою.

Література

1. Иванов А. И. Биометрическая идентификация личности по динамике подосознательных движений. — Монография, Пенза 2000*
2. Безопасная сеть: Балансируя между безопасностью и взаимодействием в распределенном мире. По материалам журнала «Огаде», 1996 г. *
3. С. А. Шумский Избранные лекции по нейрокомпьютерингу // нейро-учебник / theorg. files / shpmsku 1. htm
4. Уоссермен Ф. Нейрокомпьютерная техника: теория и практика*

* статті розміщені в мережі INTERNET