DOI: https://doi.org/10.36910/6775-2524-0560-2025-61-12
УДК: 004.056.53:004.85+004.932
Кайдик Олег Леонтійович, кандидат технічних наук, доцент[1]
https://orcid.org/0000-0002-3620-270X
Терлецький Тарас Володимирович, кандидат технічних наук, доцент[1]
https://orcid.org/0000-0002-4114-0734
Пугач Сергій Олександрович, доктор географічних наук, професор[2]
https://orcid.org/0000-0002-3738-7961
Угрин Дмитро Ілліч, доктор технічних наук, професор[3]
https://orcid.org/0000-0003-4858-4511
Артеменко Ольга Іванівна, кандидат технічних наук, доцент[4]
https://orcid.org/0000-0002-4057-1217
[1] Луцький національний технічний університет, м. Луцьк, Україна
[2] Волинський національний університет імені Лесі Українки, м. Луцьк, Україна
[3] Чернівецький національний університет імені Юрія Федьковича, м. Чернівці, Україна
[4] Приватний вищий навчальний заклад «Буковинський університет» , м. Чернівці, Україна

МОДЕЛЮВАННЯ ТА ПІДВИЩЕННЯ НАДІЙНОСТІ ІДЕНТИФІКАЦІЇ СУБ'ЄКТІВ ДОСТУПУ В СКУД НА ОСНОВІ ГІБРИДНИХ PCA-АЛГОРИТМІВ

Кайдик О. Л., Терлецький Т. В., Пугач С. О., Угрин Д. І., Артеменко О І. Моделювання та підвищення надійності ідентифікації суб'єктів доступу в СКУД на основі гібридних PCA-алгоритмів. Аналіз сучасних викликів, які супроводжують ефективну роботу сучасних систем контролю та управління доступом (СКУД) дозволяє виокремити їх ключові проблеми: значне зростання об'ємів ідентифікаційних ознак, які перевантажують традиційні методи, та високу чутливість до нестандартних умов зчитування, що призводить до формування помилок. Метод головних компонент дозволяє ефективно вирішити проблему зниження розмірності даних та прискорити пошук. Проте цей метод залишається вразливим до неідеальних умов, що обмежує його застосування та надійність у динамічному середовищі СКУД. Для систематизації та детального розуміння процесу ідентифікування було застосовано структурний підхід із моделюванням за методологією IDEF0, який вказав на важливість етапу порівняння перетвореного образу з еталонними. Проаналізовано інтеграцію методу головних компонент із алгоритмами згорткових нейронних мереж, машинного та глибокого навчання на основі виявлення прихованих нелінійних закономірностей та стійких ознак. Для оцінки ефективності гібридних методів використано галузеві стандарти: FAR, FRR та EER. Результати дослідження підтверджують актуальність гібридних підходів для забезпечення максимальної безпеки та ефективності функціонування сучасних СКУД.
Ключові слова: управління доступом, суб'єкт доступу, інформаційна ознака, ідентифікування, моделювання, гібридні методи, надійність.

Kaidyk O., Terletskyi T., Pugach S., Uhryn D., Artemenko O. Modeling and Reliability Enhancement of Access Subject Identification in PACS Based on Hybrid PCA Algorithms. The analysis of current challenges accompanying the effective operation modern Physical Access Control Systems (PACS) reveals their key problems: a significant increase in the volume of identification features, which overloads traditional methods, and high sensitivity to non-standard reading conditions, leading to errors. The PCA method effectively addresses the problem of data dimensionality reduction and accelerates search. However, this method remains vulnerable to non-ideal conditions, limiting its application and reliability in dynamic PACS environments. To systematize and gain a detailed understanding of the identification process, a structured approach with modeling using the IDEF0 methodology was applied, which highlighted the critical importance of comparing the transformed image with reference templates. The integration of PCA method with Convolutional Neural Networks, Machine Learning, and Deep Learning algorithms was analyzed based on the detection of hidden nonlinear patterns and robust features. Industry standards such as FAR (False Acceptance Rate), FRR (False Rejection Rate) and EER (Equal Error Rate) were used to evaluate the effectiveness of hybrid methods. The research results confirm the relevance of hybrid approaches for ensuring maximum security and operational efficiency of modern PACS.
Keywords: access control, access subject, information feature, identification, modeling, hybrid methods, reliability.

Постановка проблеми. Сьогодні надійне та швидке ідентифікування суб'єктів доступу (СД) є важливою вимогою ефективного функціонування будь-якої системи контролю та управління доступом. Сучасні СКУД усе більше зіштовхуються із проблемою оброблення та порівняння великих об'ємів ідентифікаційних ознак зареєстрованих, у їх базах даних, суб'єктів доступу.

Процес ідентифікування СД, який передбачає порівняння перетвореного образу із зареєстрованими еталонами, зазвичай формалізується через встановлення міри близькості або функцій порівняння. При цьому, ключовим моментом залишається необхідність досягнення високої точності та швидкості ідентифікування суб'єкта доступу, за умови надмірного накопичення, у базі даних системи, його еталонних ідентифікаційних ознак. Традиційні методи порівняння у багатовимірному просторі ідентифікаційних ознак зачасту, з точки зору обчислювальних порівнянь,

є надто затратними та чутливими до варіацій умов зчитування, що призводить до формування помилок під час процедури ідентифікування СД. Метод головних компонент (PCA – Principal Component Analysis) залишається ефективним шляхом для зниження розмірності даних про ідентифікаційні ознаки, а відповідно й прискорення процесу пошуку «найближчого сусіда». Не варто забувати й про те, що цей метод залишається чутливим до неідеалізованих умов, а це призводить до зниження надійності ідентифікування у реальних умовах експлуатації СКУД, де такі варіації є неминучими.

Як бачимо моделювання адаптованих методів ідентифікування суб'єктів доступу, які базуються на принципах PCA є актуальними та спрямовані на підвищення стійкості цієї процедури до неідеальних умов зчитування, зберігаючи при цьому високу швидкість порівняння, яка досягається шляхом ефективного зниження розмірності даних.

Аналіз останніх досліджень та публікацій. Надійність ідентифікування суб'єктів доступу залишається актуальним механізмом у забезпеченні безпеки СКУД, а структурний підхід, який використовує моделювання за методологією IDEF0, підкреслює важливість етапу порівняння перетвореного образу з еталонними.

Аналіз інформаційних джерел підтверджує, що сучасні дослідження зосереджені на підвищенні надійності та швидкості цього процесу. Так M. Ghilom та S. Latifi [1] і Y. Wang та інші [2] стверджують, що машинне та глибоке навчання (ML – Machine Learning і DL – Deep Learning відповідно) є основною рушійною силою сучасної біометрії, акцентуючи увагу, при цьому, на необхідності подолання викликів, які пов'язані із варіаціями умов ідентифікування.

Для формалізації процесів ідентифікації активно використовують методологію IDEF0 [3, 4 і 5], яка здатна паралельно працювати над визначенням обчислювальної ефективності методу головних компонентів, у розрізі інструментів зниження розмірності інформаційних ознак та прискорення пошуку «найближчого сусіда». Основним недоліком, який обумовлює обидва напрямки досліджень, є низька чутливість до неідеальних умов експлуатації СКУД, що вимагає його вдосконалення.

Гібридні рішення, які акцентують свою увагу на поєднанні методу головних компонент з локальними бінарними шаблонами (LBP – Local Binary Patterns) розглянуті в роботах під керівництвом T. Dharmawan [6] та S. L. Masyitoh [7], а дослідженням нелінійних методів головних компонент (Kernel PCA) займались науковці під керівництвом M. Ahsan [8] і K. Attouri [9] із своїми командами. Аналогічні модифікації є предметом досліджень й українських вчених під керівництвом С. Долгополова [10], Н. Омецинської [11], К. Мельник [12] та інших.

Аналіз інформаційних джерел [13-15] показує, що сучасним трендом є інтеграція методу головних компонент із технологіями глибокого навчання. О. Яковенко та інші [16] використали згорткову нейронну мережу (CNN – Convolutional Neural Network) для вилучення стійких ознак, після чого метод головних компонент застосували для оптимального зниження їх розмірності та збереження обчислювальної переваги. Окрім цього С. Пуріш та М. Лобачов [17] й інші активно працюють над мультимодальними біометричними системами, об'єднання яких є кінцевою метою забезпечення надійної ідентифікації.

З проведеного аналізу очевидно, що сам по собі метод головних компонент застарів як самостійний метод, але він зберігає свою актуальність як ефективний інструмент зниження розмірності в сучасних гібридних системах, що підтверджує актуальність дослідження, спрямованого на моделювання адаптованого методу, який дозволить компенсувати його чутливість, зберігаючи, при цьому, його обчислювальну перевагу для забезпечення надійності СКУД.

Метою роботи є моделювання та пошук оптимального методу ідентифікування суб'єктів доступу для СКУД, який дасть змогу підвищити стійкість цієї системи до варіацій умов зчитування та великих об'ємів даних через гібридизацію методу головних компонент із сучасними алгоритмами обробки.

Виклад основного матеріалу дослідження. Як уже зазначалось, безпека СКУД, насамперед, пов'язана із надійністю ідентифікування суб'єктів доступу, а її якість вимагає обґрунтованого вибору шляхів, технологій та алгоритмів його вирішення. З метою систематизації та детального аналізу процесу ідентифікування доцільно застосувати структурний підхід та моделювання на основі методології IDEF0.

Моделювання процесу ідентифікування в СКУД (контекстний рівень А-0) передбачає чітке визначення його складових (рис. 1). Тут вхідними даними виступають: сам суб'єкт доступу та база даних, яка містить множину P зареєстрованих еталонних ідентифікаційних ознак. Основними

механізмами, які здатні забезпечити цей процес залишаються СКУД та уповноважена особа, яка відповідає за організацію контрольно-перепускного режиму. Її результат – це чіткий (однозначний) висновок про ідентифікацію СД.

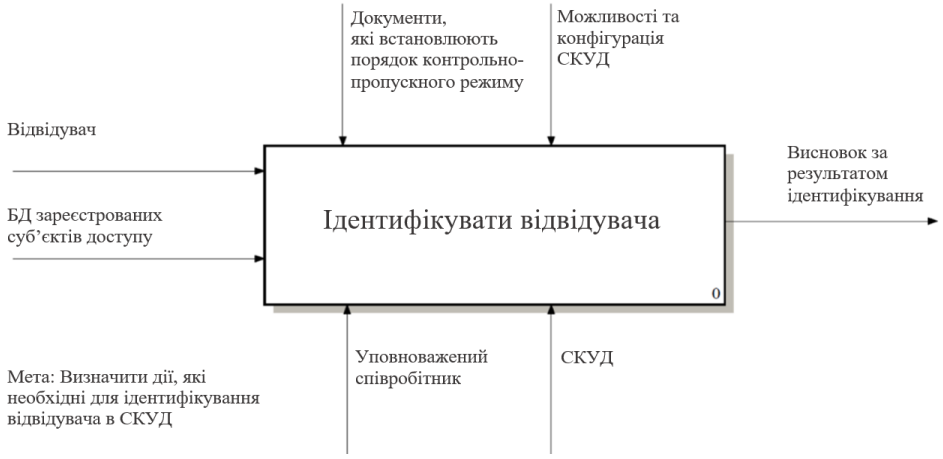

Рис.1 IDEF0-діаграма процесу ідентифікування суб'єкта доступу в системі [5]

Декомпозиція процесу ідентифікування суб'єкта доступу складається із деяких визначальних рівнів, перший з яких – перевірка необхідності реєстрування СД у системі (рис. 2).

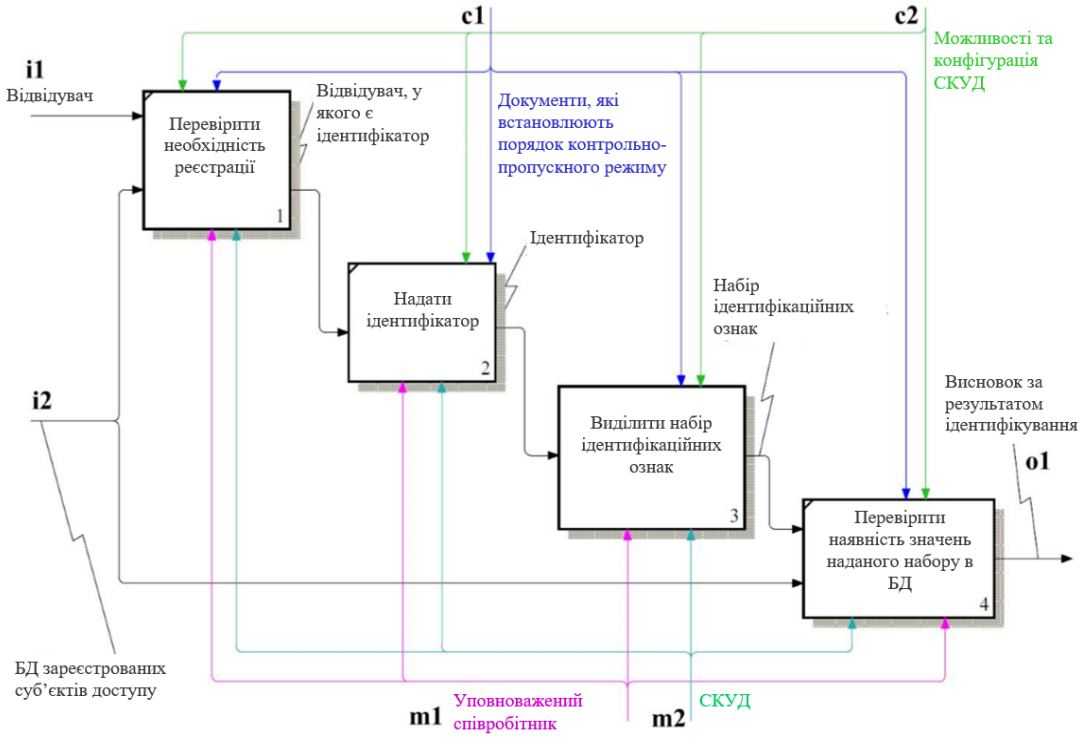

Рис.2 Декомпозиція першого рівня IDEF0-діаграми: «Перевірка необхідності реєстрування суб'єкта доступу в системі»

Перетворення фізичного ідентифікатора суб'єкта доступуу на цифровий образ є наступним визначальним рівнем цієї діаграми (рис. 3). Такий процес ідентифікування вимагає від СД надання ним для зчитування свого образу p*, який, зазвичай, є однією із ідентифікаційних ознак $z_j \in Z$. Зчитувальний пристрій після сприйняття цього образу використовує функцію перетворення F(p*) для його переведення у зручний для подальшого опрацювання контролером формат $p_k^{/}$. Цей етап можна формалізувати через наступний вираз:

$$p_k^{/} = F(p^*).$$

Після такого перетворення контролер здатний вирішити покладені на його завдання із ідентифікування СД шляхом порівняння його перетвореного образу $p_k^{/}$ із зареєстрованими у базі даних СКУД еталонними образами $p_i \in P$.

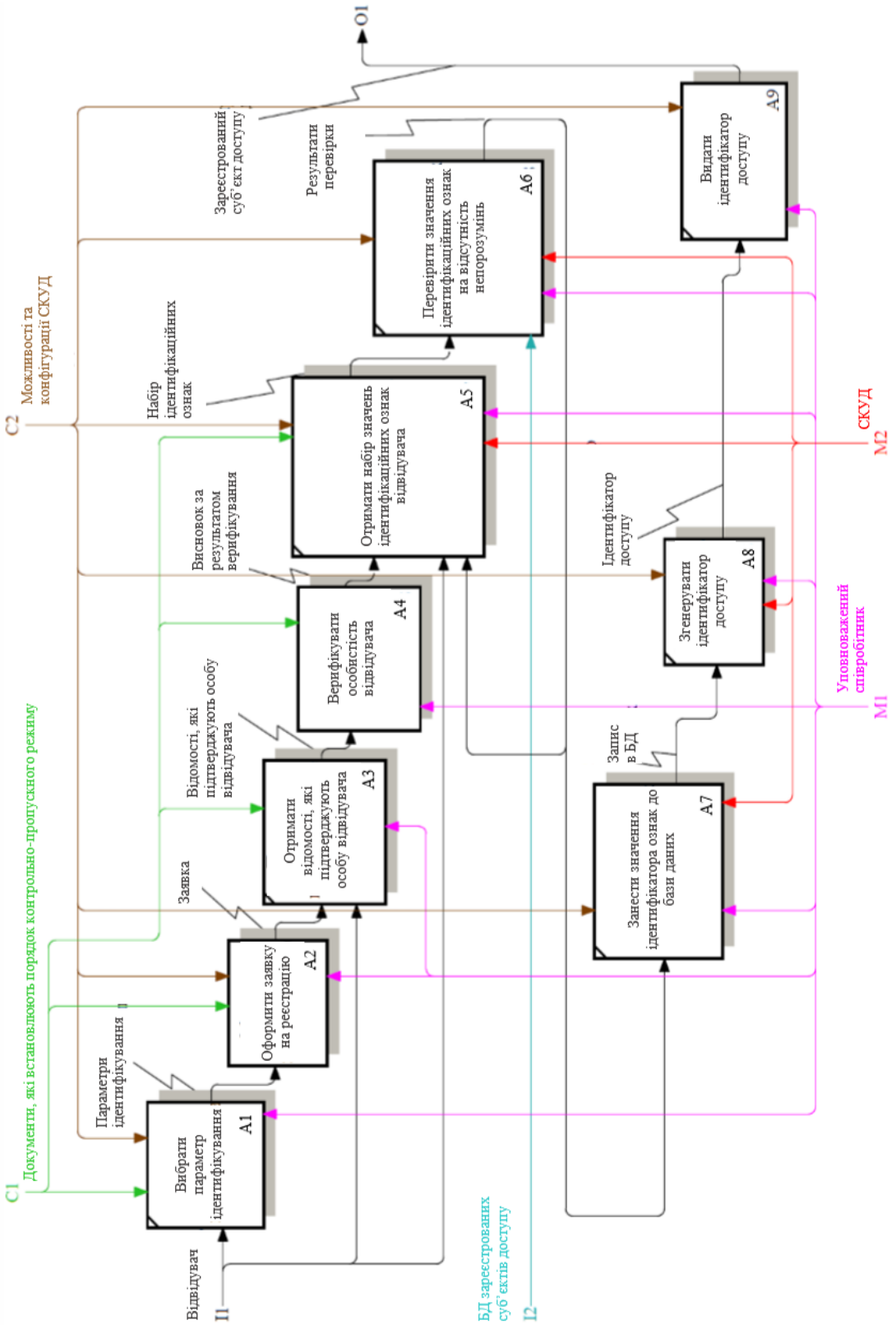

Рис.3 Декомпозиція другого рівня IDEF0-діаграми: «Перетворення фізичного ідентифікатора суб'єкта доступу на цифровий образ»

Математичний апарат ідентифікування суб'єкта доступу базується на встановленні міри наближення $Q(p_k^{/}, p_i)$, яка кількісно формується у вигляді функції порівняння $\Phi(z^{/}, D_i)$. Ця функція

встановлює числове значення критерія порівняння. Рішення про пройдене ідентифікування СД приймається лише за умови, якщо оцінка $\Phi(z^{/}, D_i)$ задовольняє встановлену граничну межу λ. Для метрики наближення ця умова приймає наступний вигляд:

$$\Phi(z^{/}, D_i) \leq \lambda.$$

У тому випадку коли умова виконується, а система підтверджує суб'єкта доступу на виконавчий пристрій надходить керуючий сигнал.

Слід пам'ятати, що перед тим, як отримати доступ, СД повинен пройти обов'язкову процедуру реєстрування. З метою генерування унікального ідентифікатора доступу, який буде занесено до бази даних СКУД, уповноважена особа визначає параметри його ідентифікування та верифікацію, забезпечує формування ним ідентифікаційних ознак та порівнює їх для уникнення, в подальшому, конфліктних ситуацій.

Як йшлося раніше, одним із найбільш ефективних шляхів вирішення завдань пов'язаних із ідентифікуванням СД, через розпізнавання його обличчя, є використання методу головних компонент, більш відомого як метод «власних облич» (Eigenfaces). PCA базується на стисканні інформації шляхом лінійно-ортогонального перетворення зображення (вектора x високої розмірності N) до значно меншого набору «власних облич» (вектора y розмірністю M, де $N > M$), що дозволяє значно зменшити об'єм даних для зберігання та прискорити процес пошуку.

Математично, метод головних компонент передбачає обчислення коваріаційної матриці для набору навчальних зображень. Після цього визначають її власні значення λ_i та власні вектори v_i за наступним виразом:

$$Sv_i = \lambda_i v_i.$$

Шляхом вибору M найбільших власних чисел, які відповідають найбільшій дисперсії даних, формується підпростір головних компонент. Процес розпізнавання базується на проектуванні оброблюваного зображення (ідентифікаційної ознаки СД) у цей підпростір та пошуку, за допомогою метрик відстаней (DIFS або DFFS), його «найближчого сусіда» (еталонного образу) серед наявних навчальних зразків.

Хоча PCA вимагає ідеалізованих умов (нейтральний вираз обличчя, стабільне освітлення), його висока ефективність у зниженні розмірності даних і прискоренні порівняння робить його цінним і економічним засобом для реалізації швидких та надійних механізмів ідентифікації в сучасних СКУД. Слід зазначити, що сучасні СКУД часто використовують більш сучасні методи, які засновано на глибоких нейронних мережах (DL – Deep Learning), але PCA, як і лінійний дискримінантний аналіз (LDA – Linear Discriminant Analysis) залишаються важливими базовими алгоритмами та використовуються або для порівняння, або як етапи попередньої обробки даних.

З огляду на необхідність подолання чутливості методу головних компонент до неідеальних умов та виявлення прихованих нелінійних закономірностей в ідентифікаційних ознаках СД необхідно зосереджувати свою увагу на гібридизації. У таких системах PCA здатна виконувати функцію інтелектуальної обробки даних. При цьому, сформований ним набір головних компонент подається на вхід потужнішим алгоритмом розпізнавання.

Залежно від складності завдань, об'єму даних та вимог, які висуваються до точності ідентифікування СД достатньо порівняти ключові комбінації таких методів (табл. 1), описати їх підходи та зробити остаточні висновки.

Таблиця 1 – Матриця технічних рішень гібридних методів ідентифікування в СКУД

Характеристика	Гібридні методи ідентифікування в СКУД		
	PCA з ML	PCA з DL	PCA з CNN
1	2	3	4
Виокремлення ідентифікаційних ознак	Низька (модель базується на тому, що PCA достатньо якісно підготував ознаки)	Висока (DL автоматично вивчає складні нелінійні ознаки, які формуються в компонентах PCA)	Дуже висока (CNN спеціалізується на виявленні просторових або часових ієрархічних закономірностей у вхідних даних)
Потреба у даних	Помірна (ефективно працює як на невеликих, так і	Значна (потребує великих наборів даних для	Критична (потребує дуже великих наборів даних, які структуруються як

	середніх наборах даних)	ефективного навчання глибоких шарів)	зображення або часові ряди-матриці)

Кінець таблиці 1

1	2	3	4
Складність порівняння ідентифікаційної ознаки з еталоном	Низька (швидке навчання)	Середня (вимагає більше часу на навчання та кращого графічного процесора)	Висока (тривале навчання, вимагає потужного графічного процесора)
Точність / продуктивність	Середня (залежить від лінійності проблеми)	Вище середньої (за умови коли дані великі, задача нелінійна)	Висока (за умови коли дані вирізняються явною просторово-часовою структурою)
Перевага у застосуванні	Традиційна біометрія або ідентифікування за невеликою кількістю поведінкових ознак	Ідентифікування за голосом, складні поведінкові профілі, обробка часових рядів	Ідентифікування за зображенням обличчя, натисканням клавіш та обробкою фізіологічних та рухових параметрів

Проаналізовані методи не достатньо оцінювати лише за їх потребою у даних чи складністю порівнянь ідентифікаційної ознаки з еталонним образом. Тут необхідно звернути увагу на остаточну надійність та точність ідентифікування. Комплексна оцінка ефективності СКУД вимагає використання галузевих стандартів, які базуються на метриках хибного доступу (FAR), хибного відхилення (FRR) та рівня рівних помилок (EER).

Варто наголосити на тому, що поки FAR відображає рівень безпеки FRR характеризує зручність використання системи. Зведення цих показників до єдиної метрики EER (точка, де FAR = FRR) дозволить отримати об'єктивну оцінку загальної точності моделі (табл. 2), оскільки вона відображає найкращий компроміс між безпекою та зручністю за оптимального порогового значення.

Таблиця 2 – Матриця надійності гібридних алгоритмів ідентифікації за критеріями ефективності

Характеристика	Гібридні методи ідентифікування в СКУД		
	PCA з ML	PCA з DL	PCA з CNN
Виокремлення ідентифікаційних ознак	Низька (обмежується лінійними / простими нелінійними залежностями)	Висока (здатний виявляти складні нелінійні залежності)	Надто висока (спеціалізується на ієрархічному виявленні просторових / часових ознак)
Очікуваний FAR та FRR	Високі (виникнення труднощів із розділенням класів за складних варіацій – більша кількість помилок)	Середні (краще розрізняє суб'єкти доступу завдяки глибині прихованих шарів, але може пропускати просторові / часові патерни)	Низькі (краще за усіх розділяє класи, оскільки здатна вилучати найтонші, стійкі до змін ознаки)
Очікуваний EER	Найвищий (найменш точне ідентифікування)	Середній (оптимальний компроміс між складністю та точністю)	Найнижчий (найвища надійність ідентифікування)

Проведений аналіз підтвердив, що інтеграція методу головних компонент із згортковою нейронною мережею, завдяки їх здатності виявляти складні ієрархічні просторові закономірності, забезпечує найнижчий EER. Це прямо вказує на те, що вони є найбільш ефективним гібридним

підходом для досягнення максимальної надійності ідентифікування суб'єктів доступу в сучасних СКУД.

Для глибшого розуміння цих концептуальних відмінностей, а також підтвердження теоретичних положень, достатньо візуалізувати ці відмінності за допомогою очікуваного концептуального EER для кожного із методів. З рисунка 4 стає зрозуміло, що додавання більшої структурної обчислювальної складності (від машинного до глибокого навчання, а потім до згорткової нейронної мережі) призводить до підвищення здатності моделі розділяти класи, а отже, зниження рівня помилок EER.

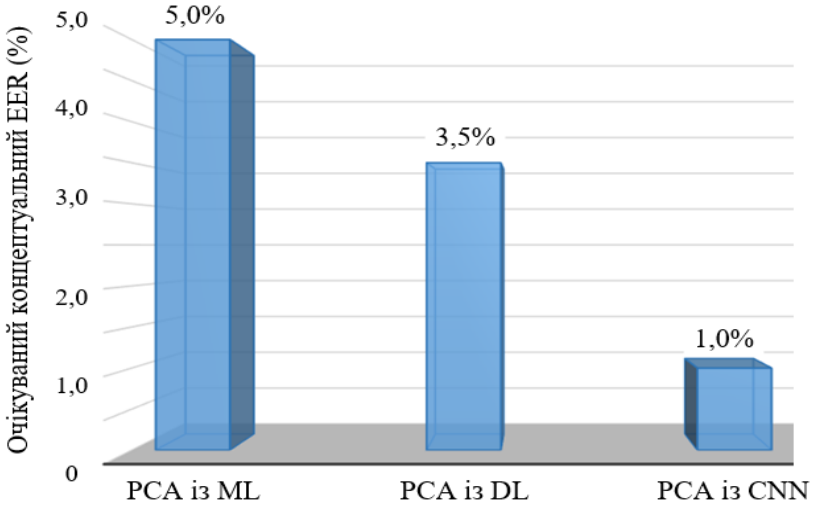

Рисунок 4 – Порівняння очікуваного концептуального EER для ідентифікації гібридних методів

Висновки та перспективи подальших досліджень. Проведений у роботі аналіз дозволяє стверджувати, що надійність ідентифікування суб'єктів доступу є критичною вимогою для забезпечення безпеки сучасних СКУД. Систематизація процесу ідентифікування досягається за допомогою методології IDEF0, яка дозволяє чітко формалізувати етапи перетворення фізичного ідентифікатора на цифровий образ ($p_к^{/} = F(p^*)$) та подальшим його порівнянням із еталонними даними. Встановлено, що класичний метод головних компонент ефективно знижує розмірність цих даних й прискорює їх пошук, проте він застарів, як самостійний алгоритм, через його високу чутливість до неідеальних умов експлуатування СКУД.

Аналіз ключових гібридних підходів та їх оцінка за метриками біометричної ефективності наштовхує на наступні висновки – надійність системи є прямопропорційною до її обчислювальної складності (підвищення складності класифікатора корелюється із зниженням рівня EER), а оптимальним рішенням залишається комбінація PCA з CNN (підтверджено максимальною ефективністю для досягнення найкращого компромісу між безпекою та зручністю умов експлуатації системи).

У подальшому доцільно здійснити моделювання та оптимізації гібридних CNN-моделей. Експериментальне тестування архітектур PCA-CNN, на реальних наборах біометричних даних, дозволить мінімізувати EER, зберігши при цьому високу швидкість ідентифікування. Розробка адаптивного порогового критерію надасть можливість інтегрувати динамічне порогове значення та підвищити, при цьому, стійкість процедури ідентифікування до неідеальних умов. У свою чергу, дослідження мультимодальної гібридизації (ефективне поєднання PCA-CNN з іншими гібридними підходами) посприяє встановленню умов забезпечення абсолютної надійності ідентифікування в біометричних СКУД.

Список бібліографічного опису

1. Ghilom, M. and Latifi, S. (2024). The Role of Machine Learning in Advanced Biometric Systems. *Electronics*, 13(13), 2667. https://doi.org/10.3390/electronics13132667
2. Wang, Y., He, Z., Wang, C., Wei, J. and Ren, M. (2025). Editorial: Biometric Recognition-Latest Advances and Prospects. *Electronics*, 14(15), 3108. https://doi.org/10.3390/electronics14153108

3. Manenti, G., Ebrahimiarjestan, M., Yang, L. and Yu, M. (2019). Functional Modelling and IDEF0 to Enhance and Support Process Tailoring in Systems Engineering. *International Symposium on Systems Engineering*. https://doi.org/10.1109/ISSE46696.2019.8984539
4. Amirreza Masoumzadeh, Hans van der Laan and Albert Dercksen. (2022). BlueSky: Physical Access Control: Characteristics, Challenges, and Research Opportunities. *Symposium on Access Control Models and Technologies*. https://doi.org/10.1145/3532105.3535019
5. Кайдик О. Л., Терлецький Т. В., Кондіус І. С., Меус О. С., Остапюк В. В. До питання організації процедури ідентифікування суб'єктів доступу в СКУД. *Прогресивні напрямки розвитку автоматичних технологічних комплексів* (ТК-2024) : збірник наук. праць VII Міжнар. наук.-техн. конф. (м. Луцьк, 28-30 травня 2024 р.). Луцьк, 2024. С. 82-84. / URL: http://surl.li/vwsjfy
6. Dharmawan, T., Nugroho, D. A. and Hidayat, M. A. (2024). Face Gender Classification using Combination of LPQ-Self PCA. *JUITA: Jurnal Informatika*, 12(1), 101-109. https://doi.org/10.30595/juita.v12i1.21137
7. Masyitoh, S. L., Ma'ruf, K. and Setiawan. R. J. (2024). Local Binary Pattern and Principal Component Analysis for Low-light Face Recognition. *Electrical Engineering, Computer Science and Informatics*. https://doi.org/10.1109/EECSI63442.2024.10776119
8. Ahsan, M., Mashuri, M., Khusna, H. and Wibawati, W. (2022). Kernel Principal Component Analysis (PCA) Control Chart for Monitoring Mixed Non-Linear Variable and Attribute Quality Characteristics. *Heliyon*. https://doi.org/10.1016/j.heliyon.2022.e09590
9. Attouri, K., Mansouri, M., Hajji, M., Kouadri, A., Bouzrara, K. and Nounou, H. (2023). Wind Power Converter Fault Diagnosis Using Reduced Kernel PCA-Based BiLSTM. *Sustainability*, 15(4), 3191. https://doi.org/10.3390/su15043191
10. Dolhopolov, S., Kruk, P., Zhuk, R. and Honcharenko, T. (2025). Methods of Image Pre-Processing for Automated Object Recognition Systems. *Management of Development of Complex Systems*. 62. 155-163. https://doi.org/10.32347/2412-9933.2025.62.155-163
11. Омецинська Н.В., Лісовець С.М., Вишемірська Я.С., Юсипів Т.В., Жовнерчук І.В. Система контролю доступу на основі розпізнавання облич методом Віоли-Джонса. *Вчені записки ТНУ імені В. І. Вернадського. Серія: Технічні науки*. Т. 32 (71). №6. 2021, с. 123-127. / URL: https://doi.org/10.32838/2663-5941/2021.6/20
12. Мельник К., Багнюк Н., Лавренчук С., Христинець Н., Боба Р., Омельчук Д. (2023). Застосування методів машинного навчання для розпізнавання обличчя. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво.* Т. 51. С. 73-78. / URL: https://doi.org/10.36910/6775-2524-0560-2023-51-09
13. Nur Nobi, M., Krishnan, R., Huang, Y., Shakarami, M. and Sandhu, R. (2022). Toward Deep Learning Based Access Control. *Conference on Data and Application Security and Privacy*. https://doi.org/10.1145/3508398.3511497
14. Geo Francis, E., Sheeja, S., Antony John, E. F. and Joseph, J. (2024). IoT Network Security with PCA and Deep Learning for Unmasking Anomalies. *Communication Systems and Network Technologies*. https://doi.org/10.1109/CSNT60213.2024.10545733
15. Păvăloaia, V.-D. and Husac, G. (2023). Tracking Unauthorized Access Using Machine Learning and PCA for Face Recognition Developments. *Information*, 14(1), 25. https://doi.org/10.3390/info14010025
16. Яковенко О.О., Кушніренко Н.І., Дорофєєва І.С., Євтушенко А.Р. Розробка системи розпізнавання осіб на основі згорткової нейронної мережі. *Інформатика та математичні методи в моделюванні*. Т. 9, №1-2. 2019. С. 77-87. / URL: http://immm.op.edu.ua/files/archive/n1-2_v9_2019/2019_1-2(8).pdf
17. Purish, S. and Lobachev, M. (2023). Gait Recognition Methods in the Task of Biometric Human Identification. *HAIT*, 6, 13-25. https://doi.org/10.15276/hait.06.2023.1

References

1. Ghilom, M. and Latifi, S. (2024). The Role of Machine Learning in Advanced Biometric Systems. *Electronics*, 13(13), 2667. https://doi.org/10.3390/electronics13132667
2. Wang, Y., He, Z., Wang, C., Wei, J. and Ren, M. (2025). Editorial: Biometric Recognition-Latest Advances and Prospects. *Electronics*, 14(15), 3108. https://doi.org/10.3390/electronics14153108
3. Manenti, G., Ebrahimiarjestan, M., Yang, L. and Yu, M. (2019). Functional Modelling and IDEF0 to Enhance and Support Process Tailoring in Systems Engineering. *International Symposium on Systems Engineering*. https://doi.org/10.1109/ISSE46696.2019.8984539
4. Amirreza Masoumzadeh, Hans van der Laan and Albert Dercksen. (2022). BlueSky: Physical Access Control: Characteristics, Challenges, and Research Opportunities. *Symposium on Access Control Models and Technologies*. https://doi.org/10.1145/3532105.3535019
5. Kaidyk, O., Terletskyi, T., Kondius I., Meus O., Ostapiuk V. (2024). On the Issue of Organizing the Procedure for Identifying Access Subjects in PACS. *Progressive Directions in the Development of Automatic Technological Complexes (TK-2024): Proceedings of the VII International Scientific and Technical Conference* (Lutsk, May 28-30, 2024). Lutsk, 2024. P. 82-84. http://surl.li/vwsjfy
6. Dharmawan, T., Nugroho, D. A. and Hidayat, M. A. (2024). Face Gender Classification using Combination of LPQ-Self PCA. *JUITA: Jurnal Informatika*, 12(1), 101-109. https://doi.org/10.30595/juita.v12i1.21137
7. Masyitoh, S. L., Ma'ruf, K. and Setiawan. R. J. (2024). Local Binary Pattern and Principal Component Analysis for Low-light Face Recognition. *Electrical Engineering, Computer Science and Informatics*. https://doi.org/10.1109/EECSI63442.2024.10776119
8. Ahsan, M., Mashuri, M., Khusna, H. and Wibawati, W. (2022). Kernel Principal Component Analysis (PCA) Control Chart for Monitoring Mixed Non-Linear Variable and Attribute Quality Characteristics. *Heliyon*. https://doi.org/10.1016/j.heliyon.2022.e09590

9. Attouri, K., Mansouri, M., Hajji, M., Kouadri, A., Bouzrara, K. and Nounou, H. (2023). Wind Power Converter Fault Diagnosis Using Reduced Kernel PCA-Based BiLSTM. *Sustainabilit*y, 15(4), 3191. https://doi.org/10.3390/su15043191
10. Dolhopolov, S., Kruk, P., Zhuk, R. and Honcharenko, T. (2025). Methods of Image Pre-Processing for Automated Object Recognition Systems. *Management of Development of Complex Systems*. 62. 155-163. https://doi.org/10.32347/2412-9933.2025.62.155-163
11. Ometsynska, N., Lisovets, S., Vyshemirska, Ya., Yusypiv, T. and Zhovnerchuk, I. (2021). Access Control System Based on Face Recognition Using the Viola-Jones Method. *Scientific Notes of Taurida V. I. Vernadsky National University. Series: Technical Sciences*, 32(71, No. 6), 123-127. https://doi.org/10.32838/2663-5941/2021.6/20
12. Melnyk, K., Bahniuk, N., Lavrenchuk, S., Khrystynets, N., Boba, R. and Omelchuk, D. (2023). Application of Machine Learning Methods for Face Recognition. *Computer-Integrated Technologies: Education, Science, Production*, (51), 73-78. https://doi.org/10.36910/6775-2524-0560-2023-51-09
13. Nur Nobi, M., Krishnan, R., Huang, Y., Shakarami, M. and Sandhu, R. (2022). Toward Deep Learning Based Access Control. *Conference on Data and Application Security and Privacy*. https://doi.org/10.1145/3508398.3511497
14. Geo Francis, E., Sheeja, S., Antony John, E. F. and Joseph, J. (2024). IoT Network Security with PCA and Deep Learning for Unmasking Anomalies. *Communication Systems and Network Technologies*. https://doi.org/10.1109/CSNT60213.2024.10545733
15. Păvăloaia, V.-D. and Husac, G. (2023). Tracking Unauthorized Access Using Machine Learning and PCA for Face Recognition Developments. *Information*, 14(1), 25. https://doi.org/10.3390/info14010025
16. Yakovenko, O., Kushnirenko, N., Dorofieieva, I. and Yevtushenko, A. (2019). Development of a facial Recognition System Based on a convolutional Neural Network. *Informatics and Mathematical Methods in Modeling*, 9(1-2), 77-87. http://immm.op.edu.ua/files/archive/n1-2_v9_2019/2019_1-2(8).pdf
17. Purish, S. and Lobachev, M. (2023). Gait Recognition Methods in the Task of Biometric Human Identification. *HAIT*, 6, 13-25. https://doi.org/10.15276/hait.06.2023.1