УДК 004.934
DOI: 10.31673/2409-7292.2025.023266

Корченко О.Г., Козловський В.В., Міщенко А.В., Терейковський О.І.

ВИЗНАЧЕННЯ ФУНКЦІОНАЛЬНИХ ВИМОГ ДО МУЛЬТИМОДАЛЬНОЇ СИСТЕМИ БІОМЕТРИЧНОЇ АУТЕНТИФІКАЦІЇ ПЕРСОНАЛУ ОБ'ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ З ВИКОРИСТАННЯМ UML-ДІАГРАМ ПРЕЦЕДЕНТІВ

Незважаючи на те, що впровадження мультимодальних систем біометричної аутентифікації на основі нейромережевого аналізу зображення обличчя та райдужної оболонки ока суттєво підвищило рівень безпеки об’єктів критичної інфраструктури, сучасні виклики зумовлюють потребу в їх адаптації до розпізнавання особи при наявності завад відеореєстрації та до функціонування в умовах спуфінг-атак. Показано, що для забезпечення актуальних потреб функціонування означених систем пріоритетним завданням є модернізація їх архітектури з опорою на сучасні теоретичні напрацювання в даній галузі. Базуючись на загальноприйнятих підходах до розробки архітектури інформаційних систем, запропоновано співвіднести перший етап модернізації з формалізацією функціональних вимог до мультимодальної системи біометричної аутентифікації персоналу об'єкта критичної інфраструктури за допомогою UML-діаграми прецедентів. Розроблена діаграма побудована на основі ітераційної методології та містить три рівні деталізації: базовий рівень описує ключові функції автентифікації та реєстрації біометричних параметрів; розширений рівень охоплює процеси, які реалізуються при навчанні нейронної мережі; фінальний рівень враховує передобробку відеоданих і розпізнавання спуфінг-атак за живучістю, за візуальними артефактами навколишнього середовища та за природністю емоцій, відображених на підконтрольному обличчі. Використання розробленої діаграми прецедентів забезпечує логічну цілісність системи, її адаптивність до експлуатаційних умов та створює підґрунтя для подальшого проєктування UML-діаграм, необхідних для завершення проєктування архітектури, а в подальшому і розробки апаратно-програмного забезпечення системи біометричної аутентифікації.

Ключові слова: захист інформації, об’єкт критичної інфраструктури, кібербезпека, нейронна мережа, біометрична аутентифікація

Вступ

В сучасних умовах ефективність систем біометричної аутентифікації є одним із ключових факторів забезпечення безпеки об’єктів критичної інфраструктури (ОКІ) [1, 2, 3], де вимоги до забезпечення оперативності та точності автентифікації персоналу є пріоритетними. При цьому завдяки доступності апробованих засобів відеореєстрації високої якості на ОКІ та розвитку нейромережевих технологій комп’ютерного зору все більш широко використовуються системи біометричної автентифікації (БА) на основі розпізнавання особи за зображенням обличчя (ЗО) та райдужної оболонки ока (РОО) [4, 5]. Разом з тим, відповідно до [6, 7], суттєвими викликами при розробці та впровадженні таких систем є складність інтеграції нейромережевих методів аналізу біометричних параметрів з технологіями відеореєстрації, що застосовуються на ОКІ. Цим пояснюється актуальність науково-прикладного завдання розробки інструментальних засобів нейромережевого аналізу ЗО та РОО людини при БА на ОКІ, що безпосередньо пов’язана з проблематикою забезпечення безпеки ОКІ.

Аналіз останніх досліджень і публікацій

На першому етапі проведено аналіз відомих систем БА за ЗО та РОО.

Сучасні системи БА активно застосовують штучний інтелект і тривимірне моделювання для забезпечення високої точності розпізнавання та протидії спуфінг-атакам. Наприклад, FaceTec формує 3D-карту обличчя за відеопотоком з однієї камери (≥3 МР), розпізнаючи моргання, міміку, посмішки. FAR становить ~8×10^{-9}. VisionLabs орієнтована на фінансовий сектор, визначає якість зображення, стать, емоції, вік, підтримує багатофакторну «живучість» і має точність до 99,9%.

IDLive (ID R&D) функціонує автономно на мобільних пристроях і виявляє атаки через віртуальні камери. Acuity перевіряє документи в аеропортах. MegaMatcher (Neurotechnology) підтримує комплексну аутентифікацію відповідно до міжнародних стандартів. Iris Access

забезпечує безконтактну ідентифікацію за райдужкою з 30 см, а Blink Identity — до 60 осіб/хв у русі. Рішення AxxonSoft дозволяє ідентифікацію за фото або відео з інтеграцією у держреєстри. При цьому в офіційній документації розглянутих інструментальних засобів опис їхньої архітектури практично відсутній.

На другому етапі аналізу проведено огляд науково-прикладних робіт, присвячених засобам БА.

Аналіз наукових джерел [8, 9, 10] підтверджує розвиток нейромережевих рішень для БА за ЗО та РОО. У [11, 12] застосовано зіставлення вхідного зображення з еталонами, що забезпечує гнучке додавання нових користувачів. У [13] класифікаційна модель демонструє високу точність, але потребує перенавчання при оновленні бази. Основні вимоги до систем БА для об’єктів критичної інфраструктури — точність за умов змін (освітлення, міміка, оклюзії), робота в реальному часі, стійкість до атак і адаптивність. Частково ці вимоги реалізовано через попередню обробку зображень [14], мультимодальні системи (ЗО+РОО) [15] і аналіз відеопотоку [16, 17, 18]. Для забезпечення прозорості й масштабованості рекомендовано використовувати формалізовані моделі, зокрема UML-діаграми прецедентів. Запропоноване архітектурне рішення орієнтоване саме на такі умови.

При цьому в доступній літературі вирішення завдання розробки архітектури мультимодальної системи біометричної автентифікації персоналу ОКІ за ЗО та РОО з урахуванням необхідності нівелювання впливу завад при відеореєстрації та протидії спуфінг-атакам освітлено недостатньо повно, що суттєво ускладнює створення відповідного програмного забезпечення. Відповідно до загальноприйнятої методології розробки архітектури інформаційних систем, першим етапом розробки являється визначення функціональних вимог до такої мультимодальної системи БА, для формалізованого опису яких доцільно використати UML-діаграми прецедентів.

Мета та завдання дослідження

Розробка UML-діаграми прецедентів, що відображає формалізований опис функціональних вимог до мультимодальної системи біометричної аутентифікації персоналу об'єкта критичної інфраструктури за зображенням обличчя та райдужною оболонкою ока.

Основна частина

UML-діаграми прецедентів системи базуються на авторській модульній нейромережевій моделі БА персоналу ОКІ за ЗО, що передбачає формалізацію архітектурних компонентів, потоків обробки біометричних даних, специфічних вимог до захисту від спуфінг-атак, деталізований опис якої наведено в [19, 20, 21]. Також були враховані вимоги стандартів [1, 2, 3] до систем БА.

Відповідно до рекомендацій [22], при побудові діаграми прецедентів було застосовано ітераційний підхід, при якому кожна ітерація відображає певний рівень деталізації функцій системи, що дозволяє поетапно розширювати обсяг врахованого функціоналу та логічно структурувати завдання, які вирішує система.

На першому рівні деталізації відображено базовий функціонал нейромережевої системи, який охоплює ключові прецеденти, пов’язані з БА, реєстрацією біометричних параметрів та налаштуванням параметрів відеозапису. Цей рівень формує основу для розуміння мінімального набору вимог до системи.

Другий рівень деталізації доповнює базовий функціонал, зосереджуючись на вимогах до реалізації механізмів навчання нейронної мережі (НМ), зокрема ініціалізації процесу навчання, налаштування його параметрів, збору необхідних даних та оцінювання результатів. Таким чином, на цьому етапі модель відображає здатність системи адаптуватись до умов експлуатації.

Третій рівень деталізації є фінальною ітерацією побудови діаграми прецедентів. На цьому рівні враховано необхідність розпізнавання спуфінг-атак на основі різних ознак, а також необхідність передобробки відеоданих з метою покращення якості вхідної інформації.

Послідовне введення нових прецедентів на кожному рівні деталізації забезпечує логічну цілісність діаграми, дає змогу повніше охопити функціональні вимоги до системи та створює основу для подальшої розробки архітектури та алгоритмів її реалізації.

На першому рівні деталізації нейромережевої системи БА враховано чотири основні актори, які взаємодіють із системою:

– «Підконтрольний об’єкт» – ініціює процедуру аутентифікації та є джерелом біометричних даних;

– «Сканер» – здійснює відеореєстрацію потоку даних, у тому числі зображень обличчя та райдужної оболонки ока;

– «Контролер доступу» – відповідає за прийняття рішення щодо надання або відмови у доступі;

– «Адміністратор» – виконує налаштування параметрів функціонування системи.

При цьому вважається, що актори «Адміністратор» та «Підконтрольний об’єкт» є діючими особами, а актори «Контролер доступу» та «Сканер» являються технічними засобами.

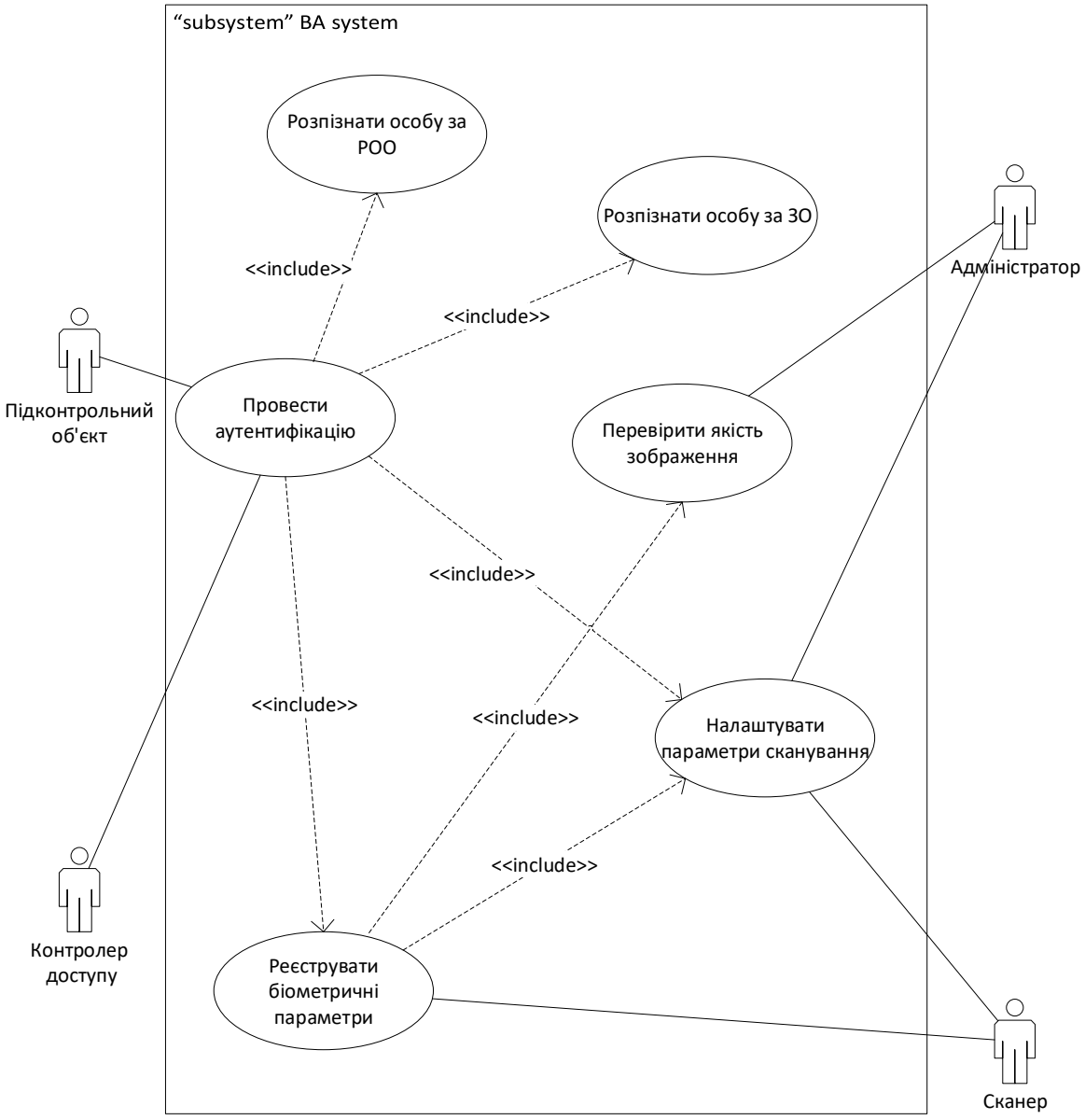

Рис. 1. Базовий варіант діаграми прецедентів

Базовий варіант діаграми включає такі прецеденти:

– «Провести аутентифікацію» – базовий прецедент, який об’єднує логіку перевірки біометричних параметрів особи з метою підтвердження її ідентичності;

– «Розпізнати особу за ЗО» – окремий прецедент, який відповідає за аутентифікацію особи на основі аналізу ЗО у відеоряді;

– «Розпізнати особу за РОО» – прецедент, що реалізує біометричне розпізнавання на основі аналізу РОО;

– «Реєструвати біометричні параметри» – прецедент, що фіксує ознаки, виявлені у відеопотоці, для подальшого аналізу;

– «Перевірити якість зображення» – забезпечує контроль якості отриманих відеокадрів для подальшої обробки;

– «Налаштувати параметри сканування» – реалізує можливість конфігурації параметрів відеореєстрації, таких як частота кадрів, роздільна здатність тощо.

Структура зв’язків між прецедентами реалізована через відношення типу <<include>>, яке вказує на обов’язкове включення відповідного підпроцесу до виконання основного прецеденту.

Прецедент «Провести аутентифікацію» включає в себе прецденденти:

– «Розпізнати особу за ЗО»;

– «Розпізнати особу за РОО»;

– «Реєструвати біометричні параметри»;

Функціонал означених прецедентів відповідає їх назвам.

Прецедент «Реєструвати біометричні параметри» включає прецденденти:

– «Перевірити якість зображення» – оскільки розпізнавання особи представника персоналу ОКІ здійснюється лише за умови відповідної якості вхідного зображення;

– «Налаштувати параметри сканування» також є частиною підпроцесу забезпечення коректної роботи сканера, ініційованого актором «Адміністратор»;

Розробка базового варіанту діаграми прецедентів дозволила визначити основні функції системи, відобразити їхню взаємозалежність та забезпечила можливість подальшої деталізації діаграми на наступних рівнях проектування.

На другому рівні деталізації нейромережевої системи БА розглядаються додаткові можливості, пов’язані з навчанням НМ, що власне і забезпечує розпізнавання особи представника персоналу ОКІ.

Показаний на рис. 2 розширений варіант діаграми включає всі прецеденти базового рівня, а також прецеденти, що розширюють функціональні можливості даної системи аутентифікації.

Додані прецеденти та їх призначення:

– «Провести навчання НМ» – реалізувати навчання нейромережевої моделі розпізнавання особи за ЗО та РОО на основі підготовлених біометричних даних;

– «Оцінити точність навчання нейронної мережі» – розрахунок основних метрик точності для перевірки якості роботи моделі;

– «Налаштувати параметри навчання НМ». Оскільки при експлуатації системи БА вважається, що архітектура та архітектурні параметри НМ є заданими, то, відповідно до [8, 13, 15], налаштування параметрів навчання зводиться до визначення: алгоритму градієнтного спуску (в теорії нейронних мереж зазвичай називають гіперпараметрами оптимізації процесу навчання), регуляризації, обробки даних, критеріїв зупинки навчання та ініціалізації вагових коефіцієнтів;

– «Провести збір даних для навчання НМ» – створення та перевірка датасету для тренування моделі, що включає біометричні зразки зображень осіб.

Зв’язки між прецедентами. Прецедент «Провести навчання НМ» має відношення << include>> з наступними підпроцесами:

– «Оцінити точність навченої НМ», оскільки оцінка результату є обов'язковим етапом процесу навчання;

– «Налаштувати параметри навчання НМ», адже модель має бути правильно сконфігурована перед запуском тренування;

– «Провести збір даних для навчання НМ», оскільки для якісного навчання необхідний верифікований набір зображень.

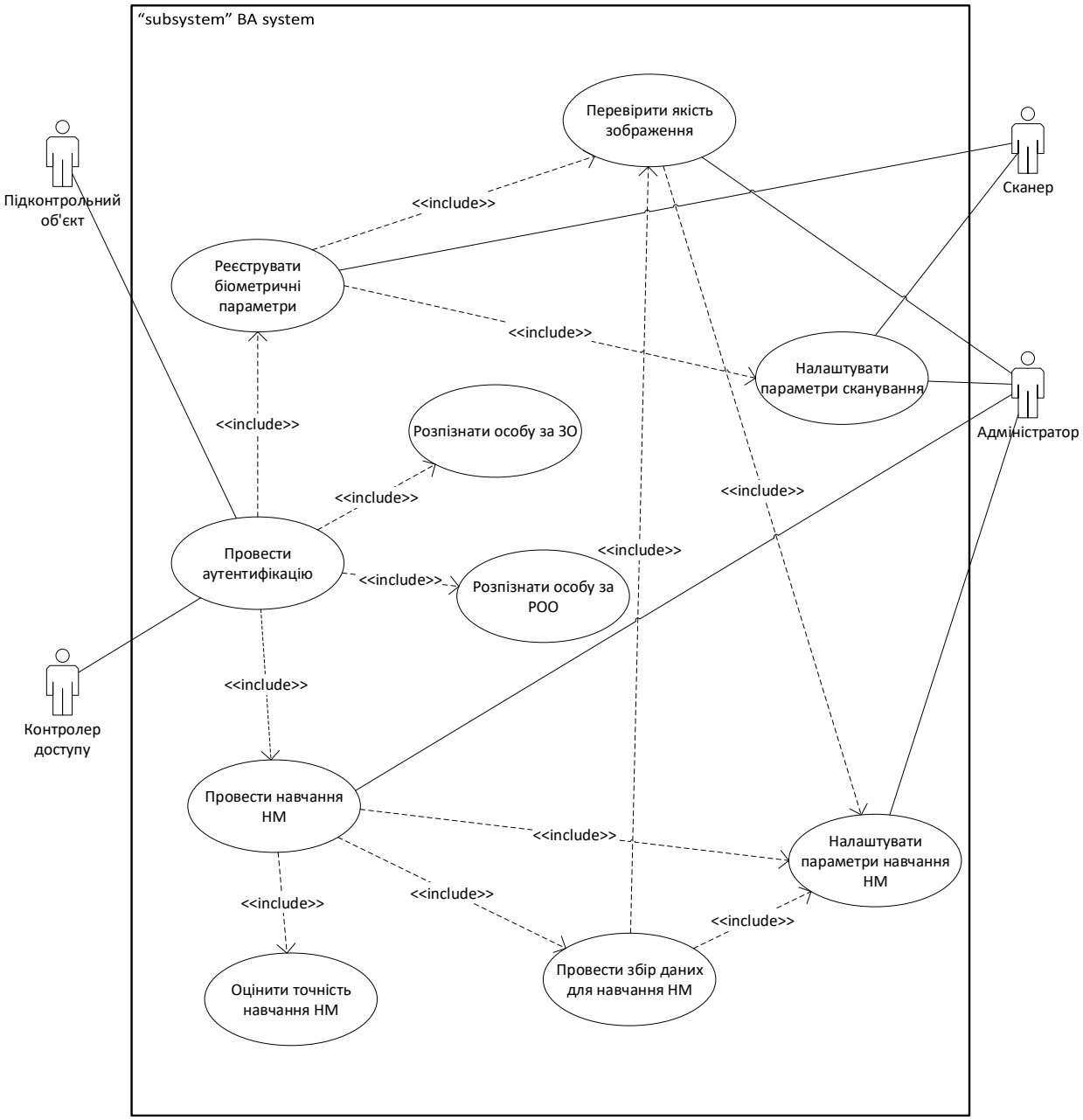

Рис. 2. Розширений варіант діаграми прецедентів

Адміністратор ініціює процес навчання НМ, налаштовує її параметри та контролює якість навчання. Сканер виконує функцію реєстрації біометричних даних, зокрема тих, що використовуються для збору навчального датасету. Контролер доступу залишається відповідальним за ухвалення рішень на основі результатів БА. Додавання навчання НМ на цьому етапі деталізації дає змогу адаптувати систему до змін у базі біометричних даних та підвищити її ефективність в реальних умовах експлуатації.

Остаточний варіант діаграми прецедентів, що представлено на рис. 3, розширює модель системи, подану на другому рівні деталізації (рис. 2), за рахунок включення додаткових прецедентів, пов’язаних із розпізнаванням в умовах завад та неякісної відеореєстрації та з розпізнаванням спуфінг-атак.

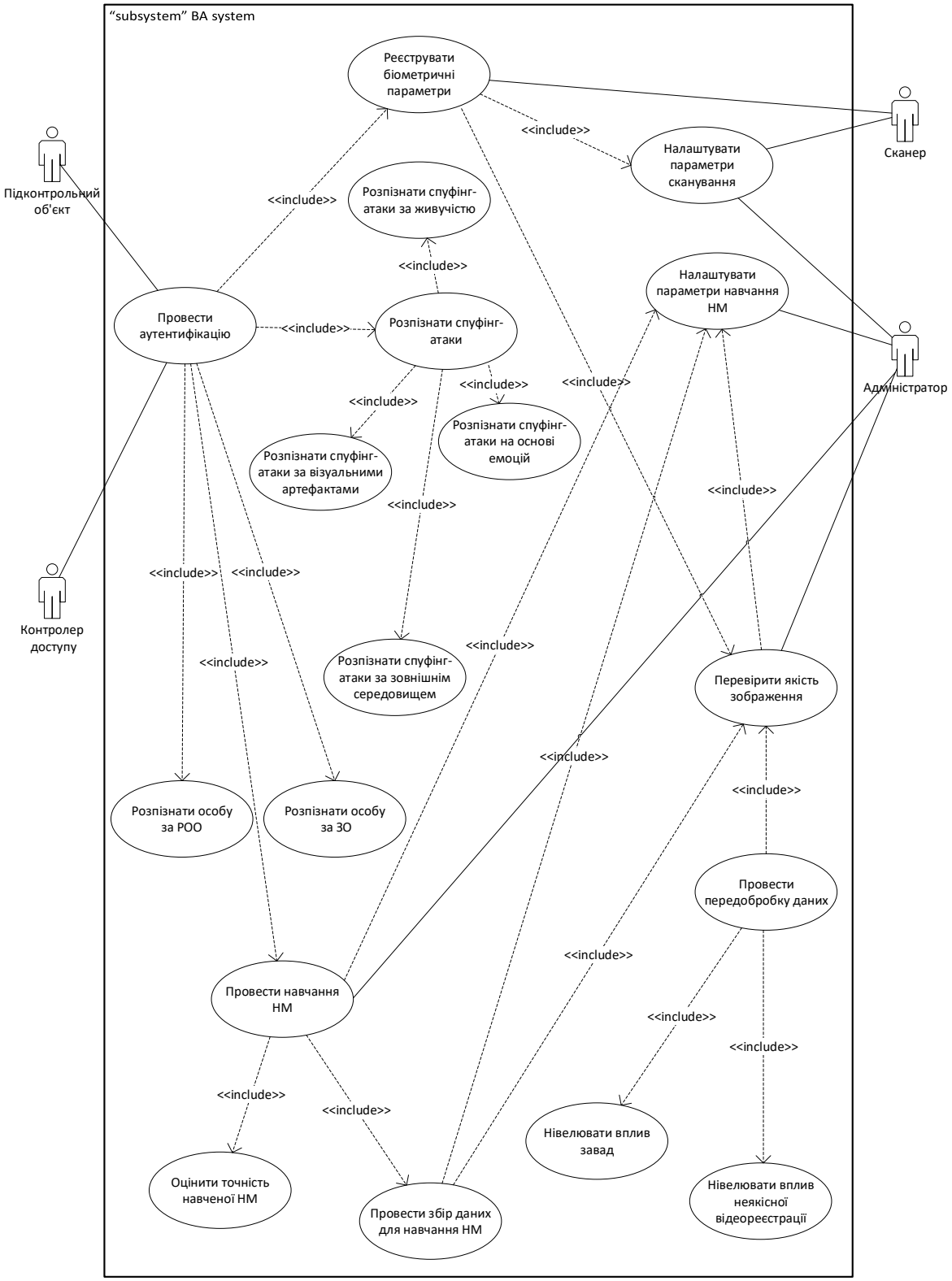

Рис. 3. Остаточний варіант діаграми прецедентів

Зокрема, додано нову групу прецедентів, що відповідають за виявлення спуфінг-атак, які можуть бути реалізовані під час БА представника персоналу ОКІ:

– «Розпізнати спуфінг-атаки за живучістю», що зводиться до визначення відповідності підконтрольного зображення зображенню обличчя живої людини на основі динаміки ключових точок;

– «Розпізнати спуфінг-атаки за візуальними артефактами», що полягає у визначенні аномальних змін текстури, кольору зображення, виникнення на ньому відблисків, розривів контурів зображення;

– «Розпізнати спуфінг-атаки на основі емоцій», що полягає у визначенні відповідності емоцій, які відображаються на зображенні підконтрольного обличчя до природніх емоцій;

– «Розпізнати спуфінг-атаки за зовнішнім середовищем», що полягає у виявленні артефактів зовнішнього оточення, наприклад, відображення обличчя на екрані мобільного пристрою або відсутність у відеокадрі предметів, які очікувано знаходяться у зоні відеореєстрації.

Усі ці прецеденти включаються до узагальнюючого прецеденту «Розпізнати спуфінг-атаки», який, у свою чергу, є включеним (<<include>>) до основного процесу БА. Крім того, в діаграмі передбачено запровадження механізмів передобробки відеоінформації, спрямованих на підвищення якості вхідних біометричних даних. Вказані механізми відповідають прецедентам «Нівелювати вплив завад» та «Нівелювати вплив неякісної відеореєстрації». Ці прецеденти входять до складу узагальнюючого прецеденту «Провести передобробку даних», який реалізується за результатами перевірки якості підконтрольного зображення (прецедент «Перевірка якості зображення»). Таким чином, остаточний варіант діаграми прецедентів забезпечує формалізований опис функціональних вимог не лише до процесів розпізнавання особи представника персоналу ОКІ та побудови НМ, як це було в розширеному варіанті, а й вимог до нівелювання впливу неякісної відеореєстрації, впливу завад та до необхідності розпізнавання спуфінг-атак, що забезпечує підґрунтя для подальшого проєктування компонентів архітектури системи БА представника персоналу ОКІ, визначення критичних шляхів обробки даних, та базу для тестування вказаної системи і документування архітектурних рішень.

Висновки

В результаті проведених досліджень розроблено UML-діаграму прецедентів, що відображає формалізований опис функціональних вимог до мультимодальної системи біометричної аутентифікації персоналу об'єкта критичної інфраструктури за зображенням обличчя та райдужною оболонкою ока. До основних переваг розробленої діаграми слід віднести наявність формалізованого опису функціональних вимог щодо необхідності нівелювання впливу завад на зображенні обличчя та необхідності розпізнавання спуфінг-атак за природністю емоцій, відображених на обличчі людини, та за артефактами зовнішнього оточення, що забезпечує підґрунтя для підвищення ефективності системи біометричної аутентифікації в ракурсі впровадження в неї нових відповідних сервісів. Перспективи подальших досліджень доцільно пов’язати з розробкою UML-діаграм, необхідних для повноцінного проектування архітектури мультимодальної системи біометричної аутентифікації персоналу об'єкта критичної інфраструктури за зображенням обличчя та райдужною оболонкою ока та розробкою відповідного апаратно-програмного забезпечення.

Перелік посилань

1. ДСТУ ISO/IEC 19989-1:2023. Інформаційна безпека. Критерії та методологія оцінювання безпеки біометричних систем. Частина 1. Структура (ISO/IEC 19989-1:2020, IDT). [Чинний від 2023-08-22]. Київ : ДП «УкрНДНЦ», 2023. 32 с.

2. ДСТУ ISO/IEC 19989-2:2023. Інформаційна безпека. Критерії та методологія оцінювання безпеки біометричних систем. Частина 2. Структура (ISO/IEC 19989-2:2020, IDT). [Чинний від 2023-08-22]. Київ : ДП «УкрНДНЦ», 2023. 36 с.

3. ДСТУ ISO/IEC 24745:2023. Інформаційні технології. Кібербезпека та захист конфіденційності. Захист біометричної інформації (ISO/IEC 24745:2022, IDT). [На заміну ДСТУ ISO/IEC 24745:2015; чинний від 2023-08-22]. – Київ: ДП «УкрНДНЦ», 2023. – 28 с.

4. Про затвердження Методичних рекомендацій щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами : Наказ Адміністрація Держспецзв'язку України від 29.05.2023. № 463. – Київ, 2023. – 38 с.

5. Про затвердження Положення про національну систему біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства: Постанова Кабінету Міністрів України від 27.12.2017 р. № 1073. – Київ, 2017.

6. Lakhno V., Kozlovskyi V., Klobukov V., Kryvoruchko O., Chubaievskyi V., Tyshchenko D. Software Package for Information Leakage Threats Relevance Assessment. In: Silhavy, R. (eds) Cybernetics Perspectives in Systems. CSOC 2022. Lecture Notes in Networks and Systems, vol 503. Springer, Cham. P. 290-301. DOI: 10.1007/978-3-031-09073-8_25.

7. Шульга В., Міщенко А., Моркляник Б., Лазаренко С., Ліщиновська Н. План управління безпекою інформаційних активів об'єктів авіатранспортного комплексу України. Захист інформації. Т. 25, № 4, 2023. С. 213-221. DOI: 10.18372/2410-7840.25.18227.

8. Muthukumaran B., Harshavarthanan L., Dhyaneshwar S., Sharief M.Z. Face and Iris based Human Authentication using Deep Learning. 2023. 4th International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2023, pp. 841-846. DOI: 10.1109/ICESC57686.2023.10193230.

9. Wang Y., Tan T., Jain A.K. Combining Face and Iris Biometrics for Identity Verification. In: Kittler J., Nixon M.S. (eds) Audio- and Video-Based Biometric Person Authentication. AVBPA 2003, Lecture Notes in Computer Science. Vol. 2688. Springer, Berlin, Heidelberg. DOI: 10.1007/3-540-44887-X_93.

10. Корченко О.Г., Терейковський О.І. Аналіз та оцінювання засобів біометричної аутентифікації за зображенням обличчя та райдужної оболонки ока персоналу об'єктів критичної інфраструктури. Кібербезпека: освіта, наука, техніка, №1(21), 2023. С. 136-148. DOI: 10.28925/2663-4023.2023.21.136148.

11. Ahmad Sabri N.I., Setumin S. One-Shot Learning for Facial Sketch Recognition using the Siamese Convolutional Neural Network. 2021 IEEE 11th IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE), Penang, Malaysia, 2021, pp. 307-312. DOI: 10.1109/ISCAIE51753.2021.9431773.

12. Hamdani N., Bousahba N., Bousbai A., Braikia A. Face Detection and Recognition Using Siamese Neural Network. International Journal of Computing and Digital System (Jāmiʻat al-Baḥrayn. Markaz al-Nashr al-ʻIlmī), 2023, Vol. 14, No. 1, pp. 889-897. DOI: 10.12785/ijcds/140169.

13. Pranav K.B., Manikandan J. Design and Evaluation of a Real-Time Face Recognition System using Convolutional Neural Networks. Procedia Computer Science. Vol. 171, 2020, pp. 1651-1659. DOI: 10.1016/j.procs.2020.04.177.

14. Hangaragi S., Singh T., Neelima N. Face Detection and Recognition Using Face Mesh and Deep Neural Network. Procedia Computer Science, Volume 218, 2023, pp. 741-749. DOI: 10.1016/j.procs.2023.01.054.

15. Yergesh A.K. Development of an advanced biometric authentication system using iris recognition based on a convolutional neural network. Herald of Science. Vol. 2, no. 5 (74), 2024, pp. 615-625. DOI: 10.24412/2712-8849-2024-574-615-625.

16. Edmunds T., Caplier A. Motion-based countermeasure against photo and video spoofing attacks in face recognition. Journal of Visual Communication and Image Representation, Volume 50, 2018, P. 314-332. DOI: 10.1016/j.jvcir.2017.12.004.

17. Kumar C.R., Saranya N., Priyadharshini M., Gilchrist E.D., Rahman M.K. Face recognition using CNN and siamese network. Measurement: Sensors, Vol. 27, 2023. DOI: 10.1016/j.measen.2023.100800.

18. Li L., Correia P.L., Hadid A. Face recognition under spoofing attacks: countermeasures and research directions. IET Biometrics, 2018, Vol. 7, pp. 3-14. DOI: 10.1049/iet-bmt.2017.0089.

19. Корченко О., Терейковський О. Модель процедури розпізнавання особи за зображенням обличчя та райдужною оболонкою ока при біометричній автентифікації персоналу об'єктів критичної інфраструктури із застосуванням нейромережевих засобів. Захист інформації. Т. 26, № 1, 2024. С. 157-170. DOI: 10.18372/2410-7840.26.18839.

20. Korchenko O., Tereikovskyi I., Ziubina R., Tereikovska L., Korystin O., Tereikovskyi O., Karpinskyi V. Modular Neural Network Model for Biometric Authentication of Personnel in Critical Infrastructure Facilities Based on Facial Images. Applied Sciences. 2025, 15, 2553. DOI: 10.3390/app15052553.

21. Корченко О., Терейковський О. Модульна нейромережева модель біометричної автентифікації персоналу об'єктів критичної інфраструктури за зображенням обличчя та райдужною оболонкою ока. Безпека інформації. 2024. Том 30, № 2. С. 339-347. DOI: 10.18372/2225-5036.30.19247.

22. Unified Modeling Language Specification Version 2.5.1. URL: https://www.omg.org/spec/UML/2.5.1/PDF (дата звернення: 14.04.2025).

Надійшла 01.05.2025