

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

*Кваліфікаційна наукова праця
на правах рукопису*

ТЕРЕЙКОВСЬКИЙ ОЛЕГ ІГОРЕВИЧ

УДК 004.056.5

ДИСЕРТАЦІЯ
НЕЙРОМЕРЕЖЕВІ МЕТОДИ ТА МОДЕЛІ БІОМЕТРИЧНОЇ
АВТЕНТИФІКАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ОБ'ЄКТІВ
КРИТИЧНОЇ ІНФРАСТРУКТУРИ

125 – Кібербезпека

12 – Інформаційні технології

Подається на здобуття наукового ступеня доктора філософії.

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

 О.І. Терейковський

Наукові керівники:

Міщенко Андрій Віталійович,

доктор технічних наук, професор.

Корченко Олександр Григорович,

член-кореспондент НАН України,

лауреат Державної премії України

в галузі науки і техніки,

заслужений діяч науки і техніки України,

доктор технічних наук, професор

АНОТАЦІЯ

Терейковський О. І. Нейромережеві методи та моделі біометричної автентифікації в інформаційних системах об'єктів критичної інфраструктури. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека» (12 – Інформаційні технології). – Державний університет «Київський авіаційний інститут». Київ, 2026.

Дисертація присвячена вирішенню актуального наукового завдання, яке полягає у розробці та дослідженні нейромережевих моделей та методів розпізнавання особи за зображенням обличчя та райдужною оболонкою ока, що забезпечать підвищення ефективності засобів біометричної автентифікації в інформаційних системах об'єктів критичної інфраструктури.

Об'єктом дослідження є процеси біометричної аутентифікації персоналу об'єктів критичної інфраструктури за зображенням обличчя та райдужною оболонкою ока.

Предмет дослідження – нейромережеві моделі та методи біометричної автентифікації персоналу об'єктів критичної інфраструктури за зображенням обличчя та райдужною оболонкою ока.

Метою дисертаційної роботи є підвищення ефективності біометричної автентифікації за зображенням обличчя та райдужною оболонкою ока в інформаційних системах об'єктів критичної інфраструктури за рахунок зменшення похибки розпізнавання особи, адаптації до варіативних умов застосування, розширення переліку ознак розпізнавання спуфінг-атак, доповнення функціональних можливостей завдяки розпізнаванню емоцій та підвищення оперативності розробки відповідних нейромережевих засобів.

Основні науково-практичні результати дисертаційних досліджень.

Визначено, що перспективи підвищення ефективності нейромережевої системи біометричної автентифікації персоналу об'єктів критичної інфраструктури за зображенням обличчя та райдужною оболонкою ока пов'язані

з забезпеченням оперативності розробки нейромережових засобів, підвищенням точності виділення кордонів зображення обличчя, зареєстрованого в умовах завад, розширенням переліку ознак розпізнавання спуфінг-атак та доповненням функціональних можливостей системи автентифікації за рахунок розпізнавання емоцій.

Розроблено моделі біометричної автентифікації в інформаційних системах об'єктів критичної інфраструктури, що дозволило деталізувати шляхи підвищення ефективності засобів біометричної аутентифікації за зображенням обличчя та райдужною оболонкою ока та забезпечило теоретичний базис розробки методу побудови нейромережових засобів семантичної сегментації зображення обличчя при біометричній автентифікації та методу біометричної автентифікації за зображенням обличчя та райдужною оболонкою ока із застосуванням нейромережових засобів. Зокрема, розроблено модель процедури розпізнавання особи за зображенням обличчя та райдужною оболонкою ока, модульна нейромережева модель біометричної автентифікації персоналу об'єктів критичної інфраструктури за зображенням обличчя та райдужною оболонкою ока та модель семантичної сегментації зображення обличчя. При цьому модель процедури розпізнавання особи за зображенням обличчя та райдужною оболонкою ока, за рахунок реалізації формалізованого опису процедури розпізнавання, конкретизації параметрів умов відеореєстрації, конкретизації параметрів оцінювання ефективності і чинників впливу на ефективність процесу нейромережевого розпізнавання особи та за рахунок розроблених підходів до визначення параметрів завад для розпізнавання особи і емоцій, розпізнавання атак за допомогою муляжів та визначення доцільності побудови модульної нейромережевої моделі, дозволила деталізувати перспективні шляхи підвищення ефективності нейромережових засобів біометричної автентифікації.

Розроблено модель семантичної сегментації зображення обличчя, що, за рахунок застосування енкодер-декодерної архітектури нейронної мережі з варіативними конструктивними параметрами, які підлягають адаптації залежно

від умов застосування, забезпечила можливість розробки ефективного методу побудови нейромережових засобів семантичної сегментації зображення обличчя при біометричній автентифікації на об'єктах критичної інфраструктури.

Розроблено модульну нейромережеву модель біометричної автентифікації, що, за рахунок співвіднесення функціоналу модулів із виконанням завдань біометричної автентифікації, які доцільно виконувати за допомогою окремої нейронної мережі, з урахуванням можливості використання апробованих вільнодоступних нейромережових засобів, адаптованих до очікуваних умов застосування, забезпечила можливість побудови ефективного методу біометричної автентифікації представника персоналу об'єкту критичної інфраструктури за зображенням обличчя та райдужною оболонкою ока, з урахуванням необхідності розпізнавання спуфінг-атак та забезпечення оперативності розробки відповідних нейромережових засобів.

Розроблено метод побудови нейромережових засобів семантичної сегментації зображення обличчя при біометричній автентифікації, що, за рахунок поетапної адаптації типу та конструктивних параметрів нейромережевої моделі до умов застосування в напрямку зменшення архітектурної складності та за рахунок використання механізму динамічного коригування параметрів навчання, забезпечує можливість вже на першому етапі експериментів оцінити придатність базової архітектури до досягнення цільових показників, досягти стабільної збіжності навчання і уникнути перенавчання, що в результаті дозволяє в 1,2-1,25 рази підвищити точність виділення недеформованих завадами контурів зображення обличчя, та приблизно в 10 разів зменшити обсяг складних довготривалих експериментів, спрямованих на визначення архітектурних параметрів нейромережевої моделі.

Розроблено метод біометричної автентифікації персоналу об'єктів критичної інфраструктури за зображенням обличчя та райдужною оболонкою ока, що, за рахунок адаптації параметрів обробки відеопотоку до поточних значень показників відображення, обґрунтованого використання апробованих наперед навчених нейромережових моделей, фільтрації зображення обличчя та

райдужної оболонки від типових завад шляхом застосування процедури семантичної сегментації з наступним поелементним маскуванням піксельних значень та за рахунок аналізу ознак спуфінг-атак, з урахуванням артефактів зовнішнього оточення та динаміки емоційного стану, дозволяє в 1,1-1,2 рази зменшити похибку розпізнавання особи, забезпечує можливість здійснювати розпізнавання спуфінг-атак за розширеним переліком ознак, доповнює функціональні можливості системи біометричної автентифікації за рахунок розпізнавання емоцій, та забезпечує можливість оперативної розробки відповідних нейромережевих засобів. Розроблено та досліджено систему біометричної автентифікації на об'єкті критичної інфраструктури, ефективність якої приблизно в 1,1 разів перевищує ефективність найкращих відомих систем подібного призначення.

Ефективність дисертаційних рішень підтверджується впровадженням в Державному університеті «Київський авіаційний інститут» при виконанні держбюджетної науково-дослідної роботи «Система забезпечення кібербезпеки та стійкості об'єктів критичної інфраструктури» (№ДР 5-2024/18.02, 2024-2025 рр.) та їх використанням в навчальному процесі кафедри кібербезпеки факультету комп'ютерних наук та технологій. Також отримані результати впроваджені в діяльність ТОВ «АНТЕ МЕДІАМ», Львівської торгово-промислової палати, ТОВ «Науково-виробниче підприємство хімічних продуктів», ТОВ «Айті Курсор», ТОВ «ОПТОЕЛЕКТРОНІКА».

Ключові слова: автентифікація; глибоке навчання; детекція; захист даних; інформаційна безпека; інформаційна інфраструктура; інформаційний об'єкт; кібератака; кібербезпека; кіберзагрози; критична інфраструктура; машинне навчання; моделювання; нейронна мережа; штучний інтелект.

ABSTRACT

Tereikovskiy O.I. Neural network methods and models of biometric authentication in information systems of critical infrastructure facilities. – Qualification Scientific Work in the Form of a Manuscript.

Dissertation for the Degree of Doctor of Philosophy in the Specialty 125 "Cybersecurity" (12 – Information technologies). – State University "Kyiv Aviation Institute", Kyiv, 2026.

The dissertation is dedicated to solving an urgent scientific problem, which consists in the development and investigation of neural network models and methods for person recognition based on facial and iris images, which will ensure increased efficiency of biometric authentication tools in the information systems of critical infrastructure facilities.

The Object of the study is the processes of biometric authentication of personnel at critical infrastructure facilities using facial and iris images.

The Subject of the study is the neural network models and methods for biometric authentication of personnel at critical infrastructure facilities using facial and iris images.

The Aim of the dissertation is to increase the efficiency of biometric authentication based on facial and iris images in the information systems of critical infrastructure facilities by reducing person recognition error, adapting to variable application conditions, expanding the list of features for detecting spoofing attacks, supplementing functional capabilities through emotion recognition, and enhancing the operational efficiency of developing corresponding neural network tools.

Main scientific and practical results of the dissertation research. It is determined that the prospects for increasing the efficiency of the neural network biometric authentication system for critical infrastructure personnel based on facial and iris images are associated with ensuring the operational efficiency of neural network tool development, increasing the accuracy of extracting the boundaries of the registered

face image under interference conditions, expanding the list of features for spoofing attack recognition, and supplementing the functional capabilities of the authentication system through emotion recognition.

Biometric authentication models in the information systems of critical infrastructure facilities were developed. This allowed for the detailing of ways to increase the efficiency of biometric authentication tools based on facial and iris images and provided the theoretical basis for developing a method for constructing neural network tools for semantic segmentation of the face image during biometric authentication, and a method for biometric authentication using facial and iris images with the application of neural network tools. Specifically, the following were developed: a model of the person recognition procedure using facial and iris images, a modular neural network model for biometric authentication of critical infrastructure personnel using facial and iris images, and a model for semantic segmentation of the face image. Furthermore, the model of the person recognition procedure using facial and iris images, by means of implementing a formalized description of the recognition procedure, specifying parameters for video registration conditions, specifying parameters for evaluating effectiveness and factors influencing the effectiveness of the neural network person recognition process, and through the developed approaches to determining the parameters of interference for person and emotion recognition, recognizing attacks using dummies, and determining the feasibility of constructing a modular neural network model, allowed for the detailing of promising ways to increase the effectiveness of neural network biometric authentication tools.

The model of semantic segmentation of the face image, by employing an encoder-decoder neural network architecture with variable constructive parameters that are subject to adaptation depending on application conditions, provided the possibility of developing an effective method for constructing neural network tools for semantic segmentation of the face image during biometric authentication at critical infrastructure facilities.

The modular neural network model for biometric authentication, by correlating the functionality of modules with the execution of biometric authentication tasks that should be performed using a separate neural network, while considering the possibility of using tested publicly available neural network tools adapted to expected application conditions, ensured the possibility of constructing an effective method for biometric authentication of critical infrastructure personnel using facial and iris images, considering the necessity of recognizing spoofing attacks and ensuring the operational efficiency of developing corresponding neural network tools.

A method for constructing neural network tools for semantic segmentation of the face image during biometric authentication was developed, which, by means of step-by-step adaptation of the neural network model type and constructive parameters to application conditions towards reducing architectural complexity and by using a mechanism for dynamic correction of training parameters, ensures the possibility of evaluating the suitability of the base architecture to achieve target indicators at the first stage of experiments, achieving stable training convergence, and avoiding overfitting. This ultimately allows for a 1.2–1.25 fold increase in the accuracy of extracting non-deformed contours of the face image and an approximately 10-fold reduction in the volume of complex long-term experiments aimed at determining the architectural parameters of the neural network model.

A method for biometric authentication of critical infrastructure personnel using facial and iris images was developed, which, by means of adapting video stream processing parameters to current display indicators, justified use of tested pre-trained neural network models, filtering the face and iris image from typical interference by applying a semantic segmentation procedure followed by element-wise pixel masking, and by analyzing features of spoofing attacks considering artifacts of the external environment and the dynamics of emotional state, allows for a 1.1–1.2 fold reduction in person recognition error, ensures the possibility of performing spoofing attack recognition based on an expanded list of features, supplements the functional capabilities of the biometric authentication system through emotion recognition, and ensures the possibility of operational development of corresponding neural network

tools. A biometric authentication system for a critical infrastructure facility was developed and investigated, the efficiency of which exceeds the efficiency of the best known systems of a similar purpose by approximately 1.1 times.

The effectiveness of the dissertation solutions is confirmed by the implementation at the State University "Kyiv Aviation Institute" in the implementation of the state budget research work "System for ensuring cybersecurity and resilience of critical infrastructure facilities" (No. DR 5-2024/18.02, 2024-2025) and their use in the educational process of the Department of Cybersecurity of the Faculty of Computer Sciences and Technologies.

The results obtained have also been implemented in the activities of ANTE MEDIA LLC, the Lviv Chamber of Commerce and Industry, Scientific and Production Enterprise of Chemical Products LLC, IT Cursor LLC, and OPTOELECTRONICS LLC.

Keywords: authentication; deep learning; detection; data protection; information security; information infrastructure; information object; cyberattack; cybersecurity; cyberthreats; critical infrastructure; machine learning; modeling; neural network; artificial intelligence.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Список публікацій, в яких опубліковано основні наукові результати дисертації

Статті у фахових наукових виданнях:

1. Терейковський, І. А., Чернишев, Д. О., Корченко, О. Г., Терейковська, Л. О., & Терейковський, О. І. (2022). Процедура застосування нейронних мереж для сегментації растрових зображень. *Кібербезпека: освіта, наука, техніка*, 2(18), 25–38. <https://doi.org/10.28925/2663-4023.2022.18.2438>.

2. Корченко, О. Г., & Терейковський, О. І. (2023). Аналіз та оцінювання засобів біометричної аутентифікації за зображенням обличчя та райдужної оболонки ока персоналу об'єктів критичної інфраструктури. *Кібербезпека: освіта, наука, техніка*, 1(21), 136–148. <https://doi.org/10.28925/2663-4023.2023.21.136148>.

3. Корченко, О., & Терейковський, О. (2024). Модель процедури розпізнавання особи за зображенням обличчя та райдужною оболонкою ока при біометричній автентифікації персоналу об'єктів критичної інфраструктури із застосуванням нейромережових засобів. *Захист інформації*, 26(1), 157–170. <https://doi.org/10.18372/2410-7840.26.18839>.

4. Корченко, О., & Терейковський, О. (2024). Модульна нейромережева модель біометричної автентифікації персоналу об'єктів критичної інфраструктури за зображенням обличчя та райдужною оболонкою ока. *Безпека інформації*, 30(2), 339–347. <https://doi.org/10.18372/2225-5036.30.19247>.

5. Корченко, О., & Терейковський, О. (2025). Семантична сегментація зображення обличчя в системах біометричної аутентифікації персоналу об'єктів критичної інфраструктури. *Кібербезпека: освіта, наука, техніка*, 4(28), 385–399. <https://doi.org/10.28925/2663-4023.2025.28.816>.

6. Корченко, О. Г., Козловський, В. В., Міщенко, А. В., & Терейковський, О. І. (2025). Визначення функціональних вимог до мультимодальної системи біометричної аутентифікації персоналу об'єкта критичної інфраструктури з

використанням UML-діаграм прецедентів. *Сучасний захист інформації*, 2(62), 68–75. <https://doi.org/10.31673/2409-7292.2025.023266>.

7. Корченко, О., & Терейковський, О. (2025). Метод біометричної автентифікації персоналу об'єктів критичної інфраструктури за зображенням обличчя та райдужною оболонкою ока із застосуванням нейромережевих засобів. *Кібербезпека: освіта, наука, техніка*, 1(29), 92–106. <https://doi.org/10.28925/2663-4023.2025.29.866>.

Статті у періодичних виданнях, які включено до міжнародних наукометричних баз:

1. Hu, Z., Tereikovskiy, I., Chernyshev, D., Tereikovska, L., Tereikovskiy, O., & Wang, D. (2021). Procedure for processing biometric parameters based on wavelet transformations. *International Journal of Modern Education and Computer Science (IJMECS)*, 13(2), 11–22. <https://doi.org/10.5815/ijmecs.2021.02.02>. [Scopus, Q3].

2. Tereikovskiy, I., Hu, Z., Chernyshev, D., Tereikovska, L., Korystin, O., & Tereikovskiy, O. (2022). The method of semantic image segmentation using neural networks. *International Journal of Image, Graphics and Signal Processing (IJIGSP)*, 14(6), 1–14. <https://doi.org/10.5815/ijigsp.2022.06.01>. [Scopus].

3. Tereikovskiy, I., Korchenko, O., Bushuyev, S., Tereikovskiy, O., Ziubina, R., & Veselska, O. (2023). A neural network model for object mask detection in medical images. *International Journal of Electronics and Telecommunications*, 69(1), 41–46. <https://doi.org/10.24425/ijet.2023.144329>. [Scopus - Q4, Web of Science].

4. Tereikovskiy, I., AlShboul, R., Mussiraliyeva, S., Tereikovska, L., Bagitova, K., Tereikovskiy, O., & Hu, Z. (2024). Method for constructing neural network means for recognizing scenes of political extremism in graphic materials of online social networks. *International Journal of Computer Network and Information Security (IJCNIS)*, 16(3), 52–69. <https://doi.org/10.5815/ijcnis.2024.03.05>. [Scopus - Q3]

5. Korchenko, O., Tereikovskiy, I., Ziubina, R., Tereikovska, L., Korystin, O., Tereikovskiy, O., & Karpinskiy, V. (2025). Modular neural network model for biometric authentication of personnel in critical infrastructure facilities based on facial

images. *Applied Sciences*, 15(5), 2553. <https://doi.org/10.3390/app15052553> [Scopus - Q1/Q2, Web of Science - Q1/Q2].

6. Bagitova, K., Tereikovskiy, I., Babayev, I., Tereikovska, L., & Tereikovskiy, O. (2023). Model for processing images of online social networks used to recognize political extremism. *Journal of Mathematics, Mechanics and Computer Science*, 119(3), 91–103. <https://doi.org/10.26577/JMMCS2023v119i3a8>. [Scopus – Q4, Web of Science].

Список публікацій, які засвідчують апробацію матеріалів дисертації:

1. Терейковський, О. І. (2022). Проблематика біометричної автентифікації в інформаційних системах об'єктів критичної інфраструктури. У *Матеріали IX Міжнародної науково-технічної Internet-конференції «Сучасні методи, інформаційне, програмне та технічне забезпечення систем керування організаційно-технічними та технологічними комплексами»* (с. 126–127). Київ: НУХТ.

<https://drive.google.com/file/d/13R3VkfJtmeRMu7UtPxI-oY79iq2kSKbg/view>

2. Терейковський, О. І. (2023). Характеристика засобів автентифікації персоналу в інформаційних системах об'єктів критичної інфраструктури. У *Матеріали X Міжнародної науково-технічної Internet-конференції «Сучасні методи, інформаційне, програмне та технічне забезпечення систем керування організаційно-технічними та технологічними комплексами»* (с. 140–141). Київ: НУХТ.

<https://drive.google.com/file/d/19dkao0HSOgMIVIGQg1iASv6R0m5zVkcU/view?pli=1>

3. Bushuyev, S., Tereikovskiy, I., Korchenko, O., Dychka, I., Tereikovska, L., & Tereikovskiy, O. (2024). *Conceptual model of the face recognition process based on the image of the face and iris of personnel of critical infrastructure facilities*. In *Proceedings of the 5th International Workshop IT Project Management (ITPM 2024)* (Vol. 3709, pp. 278–291). CEUR Workshop Proceedings. urn:nbn:de:0074-3709-5. <https://ceur-ws.org/Vol-3709/paper22.pdf>. [Scopus].

4. Tereikovskiy, O. (2024). Characteristics of personnel authentication means in information systems of critical infrastructure facilities. У *XII Міжнародна науково-практична конференція «Управління високошвидкісними рухомими об'єктами та професійна підготовка операторів складних систем»* (с. 181–182). Кропивницький.

https://usfa.edu.ua/images/docs/Zbirnyk_tez_XII_Mizhnarodnoi_naukovo_konferent_sii_2024.pdf.

5. Терейковський, О. І. (2025). Застосування нейронних мереж при вирішенні завдань біометричної автентифікації на об'єктах критичної інфраструктури. У *Теорія модернізації в контексті сучасної світової науки: збірник наукових праць з матеріалами IV Міжнародної наукової конференції, м. Мукачево, 24 січня, 2025 р.* (с. 320–323). Вінниця: ТОВ «УКРЛОГОС Груп». <https://doi.org/10.62731/mcnd-24.01.2025>.

6. Tereikovskiy, O. (2025). Model of semantic segmentation of face images. У *2-га Міжнародна науково-практична конференція «Інформаційні системи та технології: результати і перспективи» (IST 2025)* (с. 260–263). Київ: Факультет інформаційних технологій КНУ імені Тараса Шевченка. https://ist.fit.knu.ua/_files/ugd/016074_b7bb48a91362486782d8fa1c7c88236b.pdf.

7. Tereikovskiy, O. (2025). Development of the architecture of the neural network model of biometric authentication based on the face and iris image. У *POLIT. Challenges of Science Today: Abstracts of XXV International Conference of Higher Education Students and Young Scientists* (pp. 82–83). Kyiv. https://nau.edu.ua/site/variables/docs/docsmenu/studnauka/polit2025/Polit-2025_FKNT.pdf.

Список публікацій, які додатково відображають наукові результати дисертації:

1. Tereikovskiy, I., Subach, I., Tereikovskiy, O., Tereikovska, L., Toliupa, S., & Nakonechnyi, V. (2019). Parameter definition for multilayer perceptron intended for speaker identification. In *2019 IEEE International Conference on Advanced Trends in*

Information Theory (ATIT) (pp. 227–231). IEEE. <https://doi.org/10.1109/ATIT49449.2019.9030504>. [Scopus].

2. Yudin, O., Toliupa, S., Korchenko, O., Tereikovska, L., Tereikovskiy, I., & Tereikovskiy, O. (2020). *Determination of signs of information and psychological influence in the tone of sound sequences*. In *2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT)* (pp. 276–280). IEEE. <https://doi.org/10.1109/ATIT50783.2020.9349302>. [Scopus].

3. Toliupa, S., Kulakov, Y., Tereikovskiy, I., Tereikovskiy, O., Tereikovska, L., & Nakonechnyi, V. (2020). *Keyboard dynamic analysis by AlexNet type neural network*. In *2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)* (pp. 416–420). IEEE. <https://doi.org/10.1109/TCSET49122.2020.235466>. [Scopus].

4. Tereikovskiy, I., Tereikovska, L., Kryvoruchko, O., Tereikovskiy, O., Tyshchenko, D., & Franchuk, T. (2022). *Speaker's emotions recognition module based on the GoogleLeNet neural network*. In *2022 IEEE International Conference on Smart Information Systems and Technologies (SIST)* (pp. 45–50). IEEE. <https://doi.org/10.1109/SIST54437.2022.9945825>. [Scopus].

5. Корченко, О. Г., & Терейковський, О. І. (2024). *Neural network analysis of images* [Свідectwo про авторське право на твір (комп'ютерна програма) № 123672]. Бюлетень № 80. <https://sis.nipo.gov.ua/uk/search/detail/1792165/>

ЗМІСТ

АНОТАЦІЯ.....	2
ABSTRACT.....	6
СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА.....	10
ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ.....	17
ВСТУП.....	18
РОЗДІЛ 1. АНАЛІЗ МОЖЛИВОСТЕЙ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАСОБІВ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ.....	27
1.1. Проблематика використання засобів біометричної автентифікації в інформаційних системах об'єктів критичної інфраструктури.....	27
1.2. Аналіз науково-прикладних рішень в області біометричної автентифікації за зображенням обличчя та райдужною оболонкою ока.....	30
1.3. Критичний огляд науково-прикладних рішень в області в області підвищення ефективності засобів аналізу зображень.....	46
1.4. Висновки до першого розділу.....	53
РОЗДІЛ 2. МОДЕЛІ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ.....	55
2.1. Модель процедури розпізнавання особи за зображенням обличчя та райдужною оболонкою ока при біометричній автентифікації персоналу об'єктів критичної інфраструктури з застосуванням нейромережових засобів.....	55
2.2. Модульна нейромережева модель біометричної автентифікації персоналу об'єктів критичної інфраструктури за зображенням обличчя та райдужною оболонкою ока.....	64
2.3. Модель семантичної сегментації зображення обличчя.....	77
2.4. Висновки до другого розділу.....	86

РОЗДІЛ 3. МЕТОДИ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ.....	88
3.1. Правила визначення архітектурних параметрів нейромережевої моделі семантичної сегментації.....	88
3.2. Метод побудови нейромережевих засобів семантичної сегментації зображення обличчя при біометричній автентифікації.....	97
3.3. Нейромережевий метод біометричної автентифікації за зображенням обличчя та райдужною оболонкою ока в інформаційних системах об'єктів критичної інфраструктури.....	105
3.4. Висновки до третього розділу.....	118
РОЗДІЛ 4. СИСТЕМА БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ТА ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ.....	120
4.1. Архітектура системи біометричної автентифікації.....	120
4.2. Експериментальна оцінка ефективності методу побудови нейромережевих засобів семантичної сегментації зображення обличчя.....	127
4.3. Експериментальна оцінка ефективності нейромережевого методу біометричної автентифікації за зображенням обличчя та райдужною оболонкою ока в інформаційних системах об'єктів критичної інфраструктури	137
4.4. Висновки до четвертого розділу.....	150
ВИСНОВКИ.....	151
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	154
ДОДАТОК А. Акти впровадження результатів дисертаційного дослідження.....	174
ДОДАТОК Б. Лістинг (код) програмного застосунку для сегментації зображення	181

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

БА – біометрична автентифікація

ЗНМ – згорткова нейронна мережа

ЗО – зображення обличчя

НМЗ – нейромережевий засіб

НММ – нейромережева модель

НМС – нейромережева система

ОКІ – об'єкт критичної інфраструктури

РОО – райдужна оболонка ока

DET (Detection Error Trade-off) – компроміс помилок виявлення

EER (Equal Error Rate) – коефіцієнт рівної ймовірності помилок

FAR (False Acceptance Rate) – ймовірність хибного допуску

FRR (False Rejection Rate) – ймовірність хибного відхилення

ROC (Receiver Operating Characteristic) – робоча характеристика приймача

PNN (Probabilistic Neural Network) – ймовірнісна нейронна мережа

ВСТУП

Актуальність теми. В умовах сучасного світу забезпечення ефективного захисту об'єктів критичної інфраструктури (ОКІ) є одним із ключових чинників, від якого безпосередньо залежить рівень національної безпеки держави. Важливість проблеми підвищення рівня захисту ОКІ визначено одним із пріоритетних завдань державної політики у сфері кібербезпеки, що відображено у положеннях Закону України “Про критичну інфраструктуру” та “Про основні засади забезпечення кібербезпеки України”, Постанові Кабінету Міністрів України “Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури” та Указі Президента України Про рішення Ради національної безпеки і оборони України “Про Стратегію кібербезпеки України” (2021 р.). Зважаючи на встановлені нормативні вимоги до захисту ОКІ, критично високу ціну порушення їх функціональних властивостей та недостатню ефективність наявних засобів біометричної автентифікації (БА) в умовах реальної експлуатації, важливим напрямком підвищення рівня захисту ОКІ є вдосконалення зазначених біометричних засобів, які відносяться до ключових елементів підсистеми розподілу прав доступу, що, у свою чергу, є однією із найбільш важливих складових комплексної системи захисту інформації ОКІ. При цьому в інформаційних системах ОКІ найбільш поширеними є нейромережеві засоби (НМЗ) БА, які ґрунтуються на нейромережевих технологіях аналізу зображення обличчя (ЗО) для розпізнавання особи представника персоналу ОКІ. Це в першу чергу пояснюється доступністю засобів відеореєстрації та апробованістю нейромережевих технологій аналізу цифрових зображень. Разом з тим, подальше широкі впровадження відеокамер із високою роздільною здатністю створює передумови для одночасного аналізу ЗО та райдужної оболонки ока (РОО), що в свою чергу, відкриває можливість підвищення точності БА за рахунок поєднання двох біометричних параметрів в межах єдиного відеопотоку. Слід зазначити, що дослідженнями в області розробки засобів БА та їх застосуванням на ОКІ займалися ряд вітчизняних та

закордонних науковців, зокрема Корченко О.Г., Міщенко А.В., Козловський В.В., Гнатюк С.О, Ільєнко А.В., Фесенко А.О., Давиденко А. М., Швець В.А., Темніков В.О., Висоцька О.В., Hamdani N., Pranav K.B., Kumar C. Отримані ними результати, а також результати дослідження відомих апаратно-програмних розробок відповідного призначення дозволяють стверджувати про доцільність вдосконалення БА персоналу ОКІ шляхом підвищення ефективності НМЗ розпізнавання особи за ЗО та РОО за рахунок зменшення похибки розпізнавання, розширення переліку ознак розпізнавання спуфінг-атак та адаптації до варіативних умов застосування, що реалізується, у тому числі, завдяки підвищенню оперативності розробки вказаних засобів. Ще одним напрямком вдосконалення засобів БА є впровадження в них сервісу розпізнавання емоцій, що забезпечить можливість встановити відповідність психоемоційного стану персоналу вимогам щодо належного виконання службових обов'язків. Цим пояснюється актуальність наукового завдання дисертаційного дослідження, яке полягає у розробці та дослідженні нейромережових моделей та методів розпізнавання особи за зображенням обличчя та райдужною оболонкою ока, що забезпечать підвищення ефективності засобів біометричної автентифікації в інформаційних системах об'єктів критичної інфраструктури.

Зв'язок роботи з науковими програмами, планами, темами, грантами.

Дисертаційна робота безпосередньо пов'язана з виконанням держбюджетної науково-дослідної роботи Державного університету «Київський авіаційний інститут» («Система забезпечення кібербезпеки та стійкості об'єктів критичної інфраструктури», №ДР 5-2024/18.02, 2024-2025 рр.).

Мета і завдання дослідження.

Метою дисертаційної роботи є підвищення ефективності біометричної автентифікації за зображенням обличчя та райдужною оболонкою ока в інформаційних системах об'єктів критичної інфраструктури за рахунок зменшення похибки розпізнавання особи, адаптації до варіативних умов застосування, розширення переліку ознак розпізнавання спуфінг-атак,

доповнення функціональних можливостей завдяки розпізнаванню емоцій та підвищення оперативності розробки відповідних нейромережових засобів.

Відповідно до поставленої мети визначено такі основні завдання дослідження:

1. Провести аналіз можливостей підвищення ефективності засобів біометричної автентифікації за зображенням обличчя та райдужною оболонкою ока в інформаційних системах об'єктів критичної інфраструктури.

2. Розробити моделі біометричної автентифікації в інформаційних системах об'єктів критичної інфраструктури, що дозволить деталізувати шляхи підвищення ефективності засобів біометричної автентифікації за зображенням обличчя та райдужною оболонкою ока та забезпечить теоретичний базис розробки відповідних методів.

3. Розробити метод побудови нейромережових засобів семантичної сегментації зображення обличчя при біометричній автентифікації, які забезпечують підвищення точності виділення контурів обличчя.

4. Розробити метод біометричної автентифікації за зображенням обличчя та райдужною оболонкою ока із застосуванням нейромережових засобів, що забезпечує підвищення ефективності біометричної автентифікації у варіативних умовах застосування з урахуванням необхідності розпізнавання спуфінг-атак.

5. Розробити систему біометричної автентифікації об'єктів критичної інфраструктури та провести експериментальні дослідження.

Об'єктом дослідження є процеси біометричної автентифікації персоналу об'єктів критичної інфраструктури за зображенням обличчя та райдужною оболонкою ока.

Предмет дослідження – нейромережові моделі та методи біометричної автентифікації персоналу об'єктів критичної інфраструктури за зображенням обличчя та райдужною оболонкою ока.

Методи дослідження. Використовувались методи дослідження, що ґрунтуються на методологічному базисі теорії захисту інформації, нейронних мереж, складних систем, розпізнавання образів і системному аналізі – для

аналізу предметної області досліджень і окреслення перспектив підвищення ефективності нейромережових засобів розпізнавання особи при біометричній автентифікації персоналу об'єктів критичної інфраструктури; теорії нейронних мереж, кодування, прийняття рішень, моделювання, методи цифрової обробки сигналів та біометрії – для розроблення моделей та методів розпізнавання особи за зображенням обличчя та райдужною оболонкою ока при біометричній автентифікації персоналу об'єктів критичної інфраструктури; методів імітаційного моделювання, об'єктно-орієнтованого проєктування та елементів теорії алгоритмів, програмування та планування експерименту – для розроблення структурних рішень та інструментальних засобів розпізнавання особи. Достовірність наукових результатів, висновків та рекомендацій підтверджена їх узгодженістю із сучасними теоретичними положеннями, а також збіжністю отриманих аналітичних і експериментальних даних.

Наукова новизна отриманих результатів:

- *Вперше* розроблена модульна нейромережева модель біометричної автентифікації, що, за рахунок співвіднесення функціоналу модулів із виконанням завдань біометричної автентифікації, які доцільно виконувати за допомогою окремої нейронної мережі, з урахуванням можливості використання апробованих вільнодоступних нейромережових засобів, адаптованих до очікуваних умов застосування, забезпечує можливість побудови ефективного нейромережевого методу біометричної автентифікації за зображенням обличчя та райдужною оболонкою ока в інформаційних системах об'єктів критичної інфраструктури, з урахуванням необхідності розпізнавання спуфінг-атак та забезпечення оперативності розробки відповідних нейромережових засобів.

- *Вперше* розроблено метод побудови нейромережових засобів семантичної сегментації зображення обличчя при біометричній автентифікації, що, за рахунок поетапної адаптації типу та конструктивних параметрів нейромережевої моделі до умов застосування в напрямку зменшення архітектурної складності та за рахунок використання механізму динамічного коригування параметрів навчання, дозволяє підвищити точність виділення недеформованих завадами

контурів зображення обличчя та зменшити обсяг складних довготривалих експериментів, спрямованих на визначення архітектурних параметрів нейромережевої моделі.

- *Отримала подальший розвиток* модель процедури розпізнавання особи за зображенням обличчя та райдужною оболонкою ока при біометричній автентифікації персоналу об'єктів критичної інфраструктури з застосуванням нейромережевих засобів, що, за рахунок реалізації формалізованого опису процедури розпізнавання, конкретизації параметрів умов відеореєстрації, конкретизації параметрів оцінювання ефективності і чинників впливу на ефективність процесу нейромережевого розпізнавання особи та розроблених підходів до визначення параметрів завад для розпізнавання особи і емоцій, розпізнавання атак за допомогою муляжів та побудови модульної нейромережевої моделі, дозволила деталізувати перспективні шляхи підвищення ефективності нейромережевих засобів біометричної автентифікації.

- *Отримав подальший розвиток* нейромережевий метод біометричної автентифікації за зображенням обличчя та райдужною оболонкою ока в інформаційних системах об'єктів критичної інфраструктури, що, за рахунок адаптації параметрів обробки відеопотоку до поточних значень показників відображення, обґрунтованого використання апробованих наперед навчених нейромережевих моделей, фільтрації зображення обличчя та райдужної оболонки від типових завад шляхом застосування процедури семантичної сегментації з наступним поелементним маскуванням піксельних значень та за рахунок аналізу ознак спуфінг-атак, з урахуванням артефактів зовнішнього оточення та динаміки емоційного стану, забезпечує можливість зменшення похибки розпізнавання особи, дозволяє здійснювати розпізнавання спуфінг-атак за розширеним переліком ознак, доповнює функціональні можливості системи біометричної автентифікації за рахунок розпізнавання емоцій та забезпечує можливість оперативної розробки відповідних нейромережевих засобів.

Практичне значення одержаних результатів. Запропоновані нейромережеві моделі та методи біометричної автентифікації персоналу об'єктів

критичної інфраструктури за зображенням обличчя та райдужною оболонкою ока забезпечили можливість розробки системи біометричної автентифікації на об'єкті критичної інфраструктури, ефективність якої приблизно в 1,1 рази перевищує ефективність найкращих відомих систем подібного призначення.

Практична цінність полягає у наступному:

- В результаті аналізу науково-практичних робіт в області біометричної автентифікації персоналу об'єктів критичної інфраструктури за зображенням обличчя та райдужною оболонкою ока та в області нейромережових засобів обробки зображень обґрунтовано актуальність та можливість розробки доступних засобів, які, за рахунок застосування сучасних відомих нейромережових рішень, забезпечують достатню точність розпізнавання особи на основі нейромережевого аналізу зображення обличчя та райдужної оболонки ока, отриманих в різних умовах відеореєстрації, у тому числі за наявності завад, підвищують ефективність виявлення спуфінг-атак і створюють підґрунтя для визначення відповідності психоемоційного стану представника персоналу вимогам щодо належного виконання службових обов'язків.

- Розроблено архітектуру системи біометричної автентифікації за зображенням обличчя та райдужної оболонки ока персоналу об'єктів критичної інфраструктури, в якій, на відміну від відомих, з використанням UML-діаграми прецедентів сформовано формалізований опис функціональних вимог, пов'язаних із семантичною сегментацією зображень обличчя, а також із необхідністю виявлення та розпізнавання спуфінг-атак за природністю емоцій і артефактами зовнішнього оточення, що забезпечує підґрунтя для впровадження в систему біометричної автентифікації відповідних сервісів.

- Використання розробленого методу побудови нейромережових засобів семантичної сегментації зображення обличчя при біометричній автентифікації персоналу об'єктів критичної інфраструктури дозволяє в 1,2-1,25 рази підвищити точність виділення недеформованих завадами контурів зображення обличчя та приблизно в 10 разів зменшити обсяг складних довготривалих

експериментів, спрямованих на визначення архітектурних параметрів нейромережевої моделі.

- Використання розробленого нейромережевого методу біометричної автентифікації за зображенням обличчя та райдужною оболонкою ока в інформаційних системах об'єктів критичної інфраструктури дозволяє в 1,1-1,15 разів зменшити похибку розпізнавання особи.

- Розроблені програмні застосунки, що реалізують запропоновані моделі та методи, дозволяють здійснювати сегментацію обличчя та проводити розпізнавання особи і емоцій.

Практична цінність роботи підтверджується впровадженням дисертаційних рішень в діяльність Державного університету «Київський авіаційний інститут» при виконанні держбюджетної науково-дослідної роботи «Система забезпечення кібербезпеки та стійкості об'єктів критичної інфраструктури» (№ДР 5-2024/18.02, 2024-2025 рр.) (акт впровадження від 12.01.2026) та в навчальному процесі кафедри кібербезпеки факультету комп'ютерних наук та технологій (акт впровадження від 12.01.2026). Також отримані результати впроваджені в діяльність ТОВ «АНТЕ МЕДІАМ» (акт впровадження від 11.09.2025), Львівської торгово-промислової палати (акт впровадження від 12.03.2026), ТОВ «Науково-виробниче підприємство хімічних продуктів» (акт впровадження від 16.06.2025), ТОВ «Айті Курсор» (акт впровадження від 27.11.2025), ТОВ «ОПТОЕЛЕКТРОНІКА» (акт впровадження від 24.12.2025).

Особистий внесок здобувача. Усі наукові результати, що виносяться на захист, отримано здобувачем особисто. У працях за темою дисертації, опублікованих у співавторстві, здобувачу особисто належить: у [160] розроблено процедуру застосування нейронних мереж для сегментації растрових зображень; у [149] проведено аналіз та оцінювання ефективності засобів біометричної автентифікації за зображенням обличчя та райдужною оболонкою ока персоналу об'єктів критичної інфраструктури; у [144] розроблено модель процедури розпізнавання особи за зображенням обличчя та райдужною оболонкою ока при

біометричній автентифікації персоналу об'єктів критичної інфраструктури із застосуванням нейромережових засобів; у [147] розроблено модель та метод семантичної сегментації зображення обличчя в системах біометричної автентифікації персоналу об'єктів критичної інфраструктури; у [148] розроблено UML-діаграми прецедентів мультимодальної системи біометричної автентифікації персоналу об'єкта критичної інфраструктури; у [146] розроблено метод біометричної автентифікації персоналу об'єктів критичної інфраструктури за зображенням обличчя та райдужною оболонкою ока із застосуванням нейромережових засобів; у [43] розроблено підходи до формалізованого опису процедури розпізнавання біометричних параметрів; у [99] розроблено та досліджено метод семантичної сегментації растрових зображень із застосуванням нейромережових засобів; у [96] розроблено та досліджено нейромережову модель для сегментації растрових зображень; у [95] підходи до побудови нейромережових засобів аналізу растрових зображень та відеопотоку; у [145, 50] розроблено та досліджено модульну нейромережову модель біометричної автентифікації персоналу об'єктів критичної інфраструктури; у [13] розроблено процедуру оцінювання візуальних характеристик растрових зображень та підготовки цих зображень до подачі у нейромережові засоби розпізнавання; у [16] обґрунтовано концепцію розпізнавання особи персоналу об'єкта критичної інфраструктури за зображенням обличчя та райдужною оболонкою ока; у [97, 106] розроблено підходи до визначення конструктивних параметрів нейромережових засобів аналізу біометричних параметрів; у [121] розроблено підходи до обробки біометричних параметрів; у [98] розроблено підходи до розробки нейромережових засобів розпізнавання емоцій людини; у [143] розроблено комп'ютерну програму для аналізу растрових зображень.

З праць, що опубліковано в співавторстві, в дисертації використано лише ті результати, які отримано здобувачем особисто.

Апробація результатів дисертації. Основні результати дисертаційної роботи доповідались та отримали позитивні оцінки на таких міжнародних науково-технічних та науково-практичних конференціях:

IX Міжнародній науково-технічній Internet-конференції «Сучасні методи, інформаційне, програмне та технічне забезпечення систем керування організаційно-технічними та технологічними комплексами» (м. Київ, 2022); X Міжнародній науково-технічній Internet-конференції «Сучасні методи, інформаційне, програмне та технічне забезпечення систем керування організаційно-технічними та технологічними комплексами» (м. Київ, 2023); 5th International Workshop IT Project Management (ITPM 2024) м. (Братислава, 2024); XII Міжнародній науково-практичній конференції «Управління високошвидкісними рухомими об'єктами та професійна підготовка операторів складних систем» (м. Кропивницький, 2024); IV Міжнародній науковій конференції «Теорія модернізації в контексті сучасної світової науки» (м. Мукачеве, 2025); 2-й Міжнародній науково-практичній конференції «Інформаційні системи та технології: результати і перспективи» (IST 2025) (м. Київ, 2025); Polit. Challenges of Science Today: Abstracts of XXV International Conference of Higher Education Students and Young Scientists (Kyiv, 2025).

Публікації. Основні результати дисертаційного дослідження були опубліковані в 20 наукових працях, у тому числі: 7 наукових статей у фахових наукових журналах України, 6 наукових статей в міжнародних виданнях, що входять до баз даних Scopus та Web of Science, 1 з яких в журналі, що належить до квартилю Q1-Q2, та 7 тез доповідей наукових конференцій, 1 з яких проіндексована в базі даних Scopus.

Структура та обсяг роботи. Дисертація складається зі вступу, 4 розділів, загальних висновків, списку використаних джерел та 2 додатків.

Повний обсяг роботи становить 186 сторінок друкованого тексту, з них анотація – на 4 стор., зміст – на 2 стор., основний текст – на 173 стор., список із 168 використаних джерел – на 20 стор., додатки – на 12 стор. Дисертація містить 35 рисунків та 8 таблиць.

РОЗДІЛ 1. АНАЛІЗ МОЖЛИВОСТЕЙ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАСОБІВ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1. Проблематика використання засобів біометричної автентифікації в інформаційних системах об'єктів критичної інфраструктури

Практичний досвід та результати науково-технічних публікацій [6, 36, 108] однозначно свідчать про те, що за нинішніх обставин однією із найбільш важливих науково-практичних задач в області захисту ОКІ є задача підвищення ефективності систем автентифікації персоналу вказаних об'єктів. Навіть незначне порушення безпеки ОКІ може викликати суттєвий негативний вплив на соціальну та економічну сфери держави, рівень її обороноздатності та національної безпеки [138, 140, 164]. Так, в [137, 138, 141] відзначено, що захист критичної інфраструктури є складовою частиною забезпечення національної безпеки України. При цьому вказано, що безпека критичної інфраструктури – це такий стан захищеності, за якого забезпечуються функціональність, безперервність роботи, відновлюваність, цілісність і стійкість критичної інфраструктури. Під поняттям критичної інфраструктури розуміють сукупність об'єктів критичної інфраструктури, а під поняттям ОКІ – об'єкт інфраструктури, системи, їх частини та їх сукупність, який є важливим для економіки, національної безпеки та оборони, порушення функціонування якого може завдати шкоди життєво важливим національним інтересам [137, 153, 154]. Віднесення об'єктів до ОКІ здійснюються відповідно до Закону України "Про критичну інфраструктуру".

Безпека ОКІ забезпечується в тому числі і за рахунок здійснення заходів забезпечення кіберзахисту, що регулюється окремим законом України [138]. Зазначається, що заходи з кіберзахисту передбачаються та впроваджуються на всіх стадіях життєвого циклу ОКІ, що забезпечується шляхом впровадження комплексної системи захисту інформації або системи інформаційної безпеки з підтвердженою відповідністю [103, 161, 167]. Однією із основних вимог щодо

комплексної системи захисту інформації (або системи інформаційної безпеки) є забезпечення управління доступом користувачів та адміністраторів до об'єктів захисту об'єкта критичної інформаційної інфраструктури ОКІ, а також ідентифікацію та автентифікацію користувачів та адміністраторів об'єкта критичної інформаційної інфраструктури ОКІ [138, 150].

Для забезпечення ефективної ідентифікації та автентифікації персоналу використовується широкий спектр засобів, зокрема, на сьогодні найбільш поширеними є нейромережеві системи (НМС) БА за ЗО та РОО [100, 129, 139, 144]. Це передусім пояснюється широким розповсюдженням та доступністю відеокамер, які здатні з високою якістю реєструвати відповідні біометричні параметри, та апробованістю НМЗ аналізу відеопотоку, що забезпечує можливість достатньо точної ідентифікації персоналу.

Типова схема виконання процедури БА за ЗО та РОО показана на рис. 1.1.

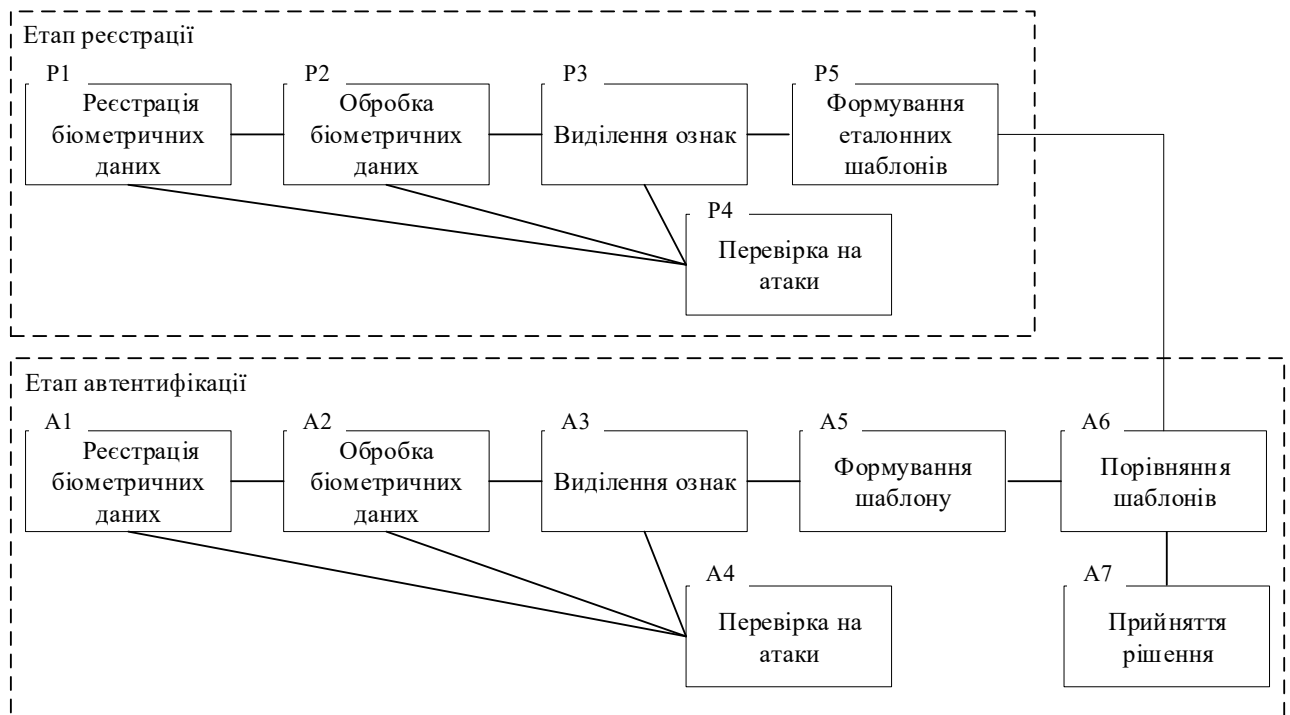


Рис. 1.1. Типова схема виконання процедури біометричної автентифікації за зображенням обличчя та райдужною оболонкою ока

Відповідно до діючих вимог процедура БА за ЗО та РОО персоналу ОКІ включає етап реєстрації біометричних параметрів легітимних представників

персоналу та етап автентифікації, на якому і приймається рішення про легітимність особи, чий біометричні параметри підлягають розпізнаванню [125, 144, 151, 165]. При цьому на рис. 1.1 кроки, що складають етап реєстрації, позначені P1-P5, а кроки, що складають етап автентифікації – A1-A7. Зазначимо, що в літературі [112, 115, 126] сукупність виконання кроків A1-A6 співвідносять з розпізнаванням особи в процесі БА.

Незважаючи на розповсюдженість НМЗ БА на основі аналізу ЗО та РОО, в багатьох науково-практичних роботах [15, 30, 37, 156] вказується на недосконалість таких засобів в процесі розпізнаванням особи, пов'язану з:

- Недостатньою ефективністю протидії атакам за допомогою муляжів (спуфінг-атакам).
- Недостатньою точністю та високою ресурсоемністю нейромережевих моделей (НММ).
- Недостатньою адаптованістю до умов застосування при впливі завад, пов'язаних з наявністю масок, окулярів, зміни зачіски, зміни кута нахилу голови людини відносно об'єктиву відеокамери, недостатнім, занадто високим та нерівномірним освітленням.

Відповідно до результатів [102, 103, 132, 142], в багатьох випадках це призводить до невідповідності систем БА нормативним вимогам, що стосуються точності та оперативності розпізнавання особи представника персоналу ОКІ ($FAR < 0,1\%$; $FRR < 1\%$; термін розпізнавання не більше 1 с), адаптації до реальних умов застосування та масштабованості [50, 133-136]. Крім того, аналіз нормативно-правових документів в області захисту інформації ОКІ дозволяє стверджувати про потенційну відмінність умов розпізнавання особи при вхідній автентифікації представника персоналу ОКІ від умов розпізнавання при автентифікації в процесі виконання службових обов'язків. Наприклад, можливо очікувати, що при вхідній автентифікації рівень освітленості, дистанція та ракурс відеореєстрації ЗО та РОО будуть знаходитись у наперед визначеному діапазоні. Тоді як при автентифікації в процесі виконання службових обов'язків цей діапазон буде значно розширений. При цьому незалежно від типу

автентифікації система БА повинна забезпечувати стійкість до різного роду спуфінг-атак. Крім того, в сучасних умовах для належного виконання службових обов'язків необхідно, щоб персонал ОКІ перебував у задовільному психоемоційному стані, порушення якого можливо фіксувати як при допуску персоналу до об'єкту, так і під час виконання службових обов'язків за рахунок аналізу ЗО та РОО. Цим пояснюється актуальність досліджень, спрямованих на підвищення ефективності НМЗ БА персоналу ОКІ за ЗО та РОО.

1.2. Аналіз науково-прикладних рішень в області біометричної автентифікації за зображенням обличчя та райдужною оболонкою ока

На першому етапі аналізу увагу зосереджено на відомих системах БА ОКІ за ЗО і РОО та на засобах аналогічного призначення, що можуть бути використані на таких об'єктах. Зазначимо, що, відповідно до [27, 63, 66, 149], в першу чергу розглянута можливість забезпечення достатньої точності розпізнавання легітимного представника персоналу при різноманітних умовах реєстрації відеоінформації за необхідності протидії атакам за допомогою муляжів.

Система БА від компанії FACETEC (www.facetec.com), вартість якої становить 600000\$, орієнтована на розпізнавання особи, для реєстрації обличчя якої використовується одна відеокамера. Зареєстрований відеопотік підлягає спеціалізованій обробці за допомогою засобів штучного інтелекту, що забезпечує створення 3D карти зображення обличчя. Декларується, що показник $FAR \approx 8 \times 10^{-9}$. При цьому система ефективно протидіє спуфінг-атакам, які реалізуються за допомогою двовимірних фотографій, цифрових зображень та відео, паперових масок з вирізами для очей та рота, "голівудських масок", створених з латексу, силікону, поліуретанової піни, гуми та спеціальних гримувальних матеріалів, воскових фігур, реалістичних ляльок, 3D-відеопроєкцій, емуляторів віртуальних відеокамер, а також сплячих (мертвих) користувачів із заплющеними очима. В технічному описі зазначено, що для створення 3D карти ЗО достатньо на протязі 2-3 секунд провести відеофіксацію

обличчя людини з використанням 2D відеокамери з роздільною здатністю більшою ніж 3 МР. Вказано, що результати обробки зібраних даних забезпечують визначення такої кількості унікальних параметрів, яка унеможливорює підробку обличчя в реальному масштабі часу. При цьому для перевірки "живучості", яка полягає у перевірці того, чи справді з системою БА взаємодіє саме людина, а не артефакт-підробка, використовується технологія виявлення слабкої активності на 3D карті 3О. Також в описі даної системи відзначено, що конкуруючі системи не дозволяють впевнено визначити такі прояви слабкої активності, як моргання, посмішку, поворот голови, миготіння світла, гримаси, вимовлення випадкових чисел, оскільки вони не містять достатній обсяг унікальних даних, необхідних для підтвердження відсутності підробки. Відзначено, що більшість відомих конкуруючих систем малоефективні у випадку, коли підроблене 3О присутнє у відеопотоці, що демонструється на 4К-моніторі без відблисків та перекосів, а в системі БА використовується 2D-камера з низькою роздільною здатністю.

Система Face Verification & Liveness for Remote Digital Onboarding від компанії Acuity (www.acuitymi.com) призначена для перевірки справжності як паперових, так і електронних документів, що засвідчують особу. Система носить закритий характер, але при цьому декларується можливість її застосування в аеропортах для автентифікації пасажирів.

Пакет прикладних програм IDLive від компанії ID R&D (www.idrnd.ai) призначений для перевірки справжності електронних документів, що засвідчують особу. Декларується, що означений пакет забезпечує захист від спуфінг-атак при пред'явленні документа. До переваг IDLive відносять можливість автономного функціонування на мобільних пристроях та можливість визначення спуфінг-атак, при реалізації яких використовується віртуальні та зовнішні відеокамери, що несанкціоновано підключені до системи БА.

Система БА від компанії VisionLabs (visionlabs.ai) в основному призначена для використання у фінансовій сфері та сфері роздрібної торгівлі. Система орієнтована на розпізнавання особи як за цифровим статичним 3О, так і за 3О у

відеопотоці. Відзначено, що в системі передбачена функція оцінки якості зареєстрованого зображення, що включає в себе визначення показників, до складу яких в тому числі входять розмитість та експозиція. Також, крім розпізнавання особи, функціонал системи забезпечує визначення віку, статі та емоцій. Вказано, що висока точність розпізнавання (99,9%) досягнена завдяки врахуванню широкого спектру геометричних параметрів ЗО. До переваг системи відносять багаточинниковий механізм визначення "живучості", що дозволяє визначити наявність динаміки зареєстрованого ЗО. Також до переваг системи відносять інструмент Track Engine, який забезпечує вибір кадрів, на основі яких відбувається розпізнавання особи. Крім ізольованої системи, компанія VisionLabs пропонує відповідний набір програмних бібліотек.

Система БА MegaMatcher Automated Biometric Identification System від компанії Neurotechnology (www.neurotechnology.com) призначена для використання в інформаційних системах, пов'язаних з наданням державних послуг, таких як реєстрація виборців, видача паспортів та інші адміністративні процеси. Система відповідає стандартам ANSI NIST, ISO, WSQ і реалізує автентифікацію на основі комплексу біометричних параметрів, включно з ЗО та РОО. Декларується, що висока точність системи підтверджена результатами тестування з використанням біометричних тестів NIST IREX (Iris Exchange) та FRVT (Face Recognition Vendor Test).

Система БА Iris Access від компанії Iridian Tech (www.iridiantech.com) носить універсальний характер і може бути використана на різноманітних підприємствах. Заявлено, що Iris Access забезпечує безконтактну автентифікацію людини за РОО з відстані біля 30 см. При цьому сервіс автоматичного налаштування кута нахилу зчитувача дає змогу прискорити процес розпізнавання під час використання пристрою як окремо, так і в комбінації з картками доступу або PIN-клавіатурою. Відзначається короткий термін реєстрації нового користувача.

Система БА від компанії Blink Identity (www.blinkidentity.com) адаптована до різноманітних умов експлуатації, що забезпечує можливість її застосування

на підприємствах, які працюють в умовах підвищеного ризику та громадських місцях. Система забезпечує можливість одночасної автентифікації до 60 осіб за хвилину навіть за умови швидкого пересування в натовпі. Особливістю системи є збереження 3D легітимного користувача у вигляді спеціального шаблону, що не підлягає зворотному перетворенню у зображення. Цим забезпечується посилення захисту збережених даних від можливого витоку інформації.

Система ідентифікації людини за 3D від компанії AxxonSoft (www.axxonsoft.com) адаптована до умов застосування в місцях масового скупчення людей та дозволяє проводити пошук обличчя людини за фотокарткою, фотороботом або відеокадром з урахуванням можливості зміни порогу схожості. До переваг системи відносять можливість пошуку з використанням баз даних державних установ та правоохоронних органів. Відзначається, що відповідні рішення компанії AxxonSoft використовуються на багатьох ОКІ.

Також проаналізовані можливості засобів ідентифікації особи за 3D та РОО, що використовуються в сучасних мобільних пристроях на платформі Apple та на платформі Android.

Визначено, що технологія Face ID (платформа Apple) передбачає проведення відеореєстрації як у видимому, так і у інфрачервоному діапазоні світла. При цьому на 3D проєктується набір ключових точок, що забезпечує можливість створення шаблону обличчя легітимного користувача, який надалі використовується в якості еталону для порівняння. Зазначається, що засоби розпізнавання особи, побудовані за технологією Face ID, адаптовані до завад, пов'язаних з нанесенням макіяжу, появою волосся, наявністю капелюха, шарфа, прозорих окулярів, контактних лінз або медичної маски. У останньому випадку необхідною умовою автентифікації являється відеореєстрація очей та увімкнення режиму "Face ID з маскою". Також вказані засоби можуть використовуватись в умовах різноманітного освітлення. Зазначається значне погіршення точності у випадку наявності темних сонцезахисних окулярів. Крім того, використання технології Face ID дозволяє розпізнати, чи розплющені очі

користувача, що використовується для зміни налаштувань екрану пристрою. Рекомендована відстань від обличчя до відеокамери 25-50 см. В процесі налаштування Face ID обличчя користувача сканується декілька разів в різних ракурсах, що забезпечує створення 3D-шаблону обличчя, який в тому числі використовується для підтвердження "живучості" при розпізнаванні спуфінг-атак.

На відміну від Face ID, засоби на платформі Android передбачають відеореєстрацію обличчя лише у видимому діапазоні світла. При цьому розпізнавання спуфінг-атак реалізується за рахунок виявлення відблисків, характерних для скляної або паперової поверхні, визначення кордонів пристрою, який використовується для демонстрації підробленого зображення, аналізу артефактів на зображенні (муар, розфокусування, дисторсія) та наявності мікроміміки обличчя. Зазначається зниження функціоналу засобів розпізнавання при зниженні рівня освітлення.

Таким чином, аналіз відомих прикладних систем БА за ЗО та РОО свідчить про те, що у загальному випадку перспективи їх вдосконалення пов'язані з забезпеченням достатньої точності розпізнавання особи з урахуванням можливості реалізації спуфінг-атак в умовах нерівномірного освітлення та впливу завад. Також, відповідно до положень, наведених в п. 1.1 даної дисертаційної роботи, проведено аналіз найбільш відомих прикладних систем, основним призначенням яких є розпізнавання емоційного стану людини.

Система FaceReader від компанії Noldus Information Technology [<https://www.noldus.com/facereader>] призначена для отримання точних та надійних даних про емоції людини по зображенню її обличчя. Для навчання нейронної мережі використано понад 20 000 зображень, які були розмічені вручну. Визначаються 7 базових емоцій і нейтральний стан. Процес розпізнавання емоцій розділено на три фази. Перша фаза – визначення положення обличчя на зображенні, використовуючи алгоритм пошуку обличчя з виділеними окремими ділянками на зображенні на основі глибокого навчання. Друга фаза полягає у побудові моделі обличчя з використанням глибоких

нейронних мереж, що описує розташування 468 ключових точок, та у стисненому векторному представленні моделі обличчя за допомогою методу головних компонентів. На третій фазі виконується класифікація обличчя за допомогою навченої глибокої нейронної мережі задля розпізнавання емоцій. FaceReader класифікує вирази обличчя з пікселів зображення. Крім того, FaceReader класифікує стать людини, її вік, наявність на обличчі бороди, вусів, напрямок погляду, орієнтацію голови, також система надає інформацію про стан очей (розплющені/заплющені), рот (відкритий/закритий), брови (підняті/нейтральні/опущені).

Система Captemo [<https://www.captemo.com>] від компанії Logic Pursuits розпізнає емоції людини за її обличчям, використовуючи засоби штучного інтелекту та хмарних обчислень. Система використовується для оцінки рівня задоволення клієнтів наданням послуг у сфері обслуговування, зокрема у кафе. Captemo в режимі реального часу здатна фіксувати емоції за обличчям до десяти людей одночасно. Можливо розпізнавати такі емоції, як задоволення, роздратованість та подив. Також рішення фіксує інші внутрішні та зовнішні дані, такі як рівень продажів компанії, дані про співробітників, погоду, з метою надання якісної бізнес-статистики. Як результат, Captemo дозволяє оцінити залежність рівню задоволення клієнта від певних часових рамок, робочої зміни певного співробітника та інших параметрів, що надає змогу компанії побудувати ефективну бізнес-стратегію.

Система BioObserver [<https://hertasecurity.com/advanced-solution-facial-expression-analysis/>] від компанії Herta призначена для розпізнавання семи базових емоцій людини за обличчям, таких як здивування, сум, роздратування та інші. Також задекларовано розпізнавання вісімнадцяти мікро-експресій обличчя, таких як нахмуреність, моргання, підняття брів та інші. До того ж система відслідковує напрямок погляду та направлення голови, що дозволяє слідкувати за рівнем уваги людини. Система працює як в режимі реального часу при аналізі відеопотоку, так і дозволяє аналізувати попередньо записане відео.

Оскільки результати [3, 11, 69] вказують на те, що основою більшості

розглянутих систем являються НМЗ, то на наступному етапі було проаналізовано науково-прикладні роботи, присвячені таким засобам.

Стаття [129] присвячена вирішенню задачі виділення обличчя людини у відеопотоці для контролю за дотриманням співробітниками стану безпеки в процесі роботи та навчання. Задекларовано, що метою статті є дослідження доцільності використання технології MobileSSD для онлайн виділення у відеопотоці ЗО та виявлення обмежень і недоліків використання вказаної технології. Для цього авторами статті було розроблено відповідну систему виділення та проведені експериментальні дослідження, спрямовані на визначення залежності ефективності даної системи виділення від наступних чинників: відстань від обличчя до камери; наявність на обличчі окулярів; наявність на обличчі сторонніх предметів, які заважають фіксації характерних точок обличчя; рівень освітлення; наявність перед камерою не тільки самої людини, а й її фотографії; поворот або нахил обличчя людини; тип пристрою, що забезпечує функціонування системи виділення обличчя.

Наведені результати експериментів, в яких відображено залежність впевненості системи у результатах виділення при зміні означених чинників. Експериментально визначено, що поворот обличчя в більшості випадків унеможливорює його виділення. Також показано, що при застосуванні технології MobileSSD в системі виділення обличчя, яка призначена для експлуатації в контурі моніторингу присутності людини на робочому місці, є сенс періодичної перевірки зміни положення ЗО. Передбачається, що запропонований моніторинг дозволить перевірити, що відеокамера фіксує саме обличчя людини, а не її фотографію. Тобто для розпізнавання спуфінг-атак використано підхід «за живучістю». Слід зазначити, що в статті не достатньо детально описане поняття впевненості НММ в результатах виділення. Крім того, наведені результати не в повному обсязі дозволяють оцінити залежність точності (впевненості) виділення обличчя від величини впливу означених чинників, оскільки відхилень вихідного сигналу НММ від очікуваного значення не наведено. При цьому негативний

результат виділення повернутого обличчя можливо пояснити з позицій недостатньої кількості відповідних навчальних прикладів.

В роботі [77] розглянута задача розпізнавання обличчя, очей і РОО людини в реальному часі з використанням технологій комп'ютерного зору. Для ідентифікації областей обличчя, очей авторами запропоновано використовувати підхід Blob Analysis, що передбачає аналіз ЗО, а сегментація реалізується шляхом ізоляції пікселів у фоновому режимі з використанням порогової функції. Для виділення РОО використано підхід Circle Hough. Автори стверджують, що використання запропонованих ними рішень дозволило досягнути високих результатів, навіть у випадку аналізу ЗО низької якості. Дискусійним аспектом запропонованого в статті підходу являється процедура перетворення зображення із формату YCbCr у формат RGB. Результат аналізу даної статті вказує на важливість процедури сегментації піддослідних ЗО, очей та РОО.

Робота [132] присвячена визначенню шляхів для розробки універсального точного та надійного інструментарію для засобів БА з урахуванням необхідності виявлення Deepfake підробок ЗО. Декларується орієнтованість вказаного інструментарію на застосування в мобільних застосунках. Показано перспективність використання нейромережевих технологій. Запропонована архітектура НММ на базі моделі EfficientNetB0. Для навчання НММ використано датасет FaceForensics++, що містить оригінальні та підроблені ЗО з візуальними артефактами. Задекларована точність запропонованої НММ – 95% при встановленому порозі 0,21.

Робота [168] присвячена розробці системи розпізнавання осіб на основі згорткової нейронної мережі (ЗНМ) типу LeNet-5. Для навчання та тестування ЗНМ використано набір даних, що складався із 840 фотографій ЗО. В роботі увагу акцентовано на визначенні оптимального співвідношення величин помилок 1-го і 2-го роду з точки зору вимог системи БА.

В статті [126] запропоновано систему двохфакторної автентифікації користувача за допомогою розпізнавання обличчя. Як і в роботі [166], використано достатньо ранню модель ЗНМ типу LeNet-5, що поступається

ефективністю сучасним типам ЗНМ, однак є більш апробованою і менш ресурсоємною.

Стаття [127] присвячена розробці НМЗ для ідентифікації особи за ЗО. Пропонується використання НММ на базі LeNet-5. Запропоновано три варіанти мережі різної архітектури, для навчання яких використано набори даних п'ятидесяти ЗО десяти осіб. Визначено, що застосування модифікованої НММ типу LeNet-5 забезпечує точність класифікації 93,75%.

В статті [125] наведено опис двохфакторної системи автентифікації на базі сіамської НММ з триплетною функцією втрат. Використано датасет, що містить 5000 ЗО для 50 користувачів, зареєстрованих із різних ракурсів та з різними емоціями. Розмір кожного ЗО у відтинках сірого кольору – 128 на 128 пікселів, зареєстрованих на чорному фоні. Задекларована точність розпізнавання ЗО близько 93%. Зазначимо, що питання тестування моделі на прикладах ЗО, які не були представлені в навчальній вибірці, описані недостатньо повно. Це не дозволяє визначити можливість запропонованої системи щодо оперативного оновлення переліку легітимних користувачів.

Також проведений аналіз вказує на застосування різних підходів до побудови НММ, призначених для розпізнавання особи за ЗО та РОО. В роботах [5, 39] НММ використовується для здійснення порівняння вхідного зображення тільки з одним зображенням із набору даних, які відповідають еталонам ЗО та РОО легітимних користувачів. У цьому випадку процес автентифікації передбачає послідовне порівняння вхідного зображення із всіма зображеннями, асоційованими з кожним із користувачів.

В роботі [74] пропонується використовувати НММ, навчену на прикладах зображень, які відповідають всім легітимним користувачам. Тобто така НММ вирішує задачу віднесення вхідного зображення до одного із наперед визначених класів легітимних користувачів.

Хоча точність розпізнавання такої моделі вважається дещо вищою, однак її серйозним недоліком являється складність внесення даних нового користувача, що зумовлена необхідністю повного перенавчання моделі. При

цьому у першому випадку процедуру автентифікації можливо співвіднести з вирішенням задачі класифікації зображень, а в другому випадку – з вирішенням задачі порівняння зображень.

Ще один підхід, описаний у [41], передбачає використання додаткового нейромережевого модулю, призначеного для попередньої обробки зображень перед їх подачею у модуль розпізнавання. Також відомий підхід до нейромережевого розпізнавання особи на основі інтегрального аналізу 3О та РОО [120]. Ще один аспект розробки НМЗ розпізнавання досліджено в роботах [51, 58], де запропоновано реалізовувати нейромережевий аналіз зображень у відеопотоці з урахуванням інформації декількох кадрів. При цьому в роботі [51] пропонується проводити розпізнавання на основі покадрового порівняння вхідного відеопотоку з еталонним зображенням.

В роботах [33, 63] показана доцільність розпізнавання спуфінг-атак на основі аналізу аномалій вхідного відеопотоку та динаміки емоцій, що проявляються на обличчі людини. В результаті проведеного аналізу відомих засобів розпізнавання особи та емоцій на основі 3О та РОО, використовуючи результати [50, 106, 107, 121] та вимоги, визначені в нормативно-правових документах [133-136, 157, 158], виділено дві групи критеріїв ефективності зазначених засобів: основні (А) та додаткові (В).

До основної групи віднесено критерії, які безпосередньо характеризують ефективність процесу розпізнавання в умовах відеореєстрації, що зазвичай встановлені для контролю доступу при вході на ОКІ, коли умови відеореєстрації знаходяться у наперед визначених межах. До додаткової групи віднесено критерії, які дозволяють оцінити ефективність системи розпізнавання з позицій стійкості до зовнішніх чинників, ресурсоємності процесу розпізнавання, ресурсоємності розробки системи розпізнавання, та забезпечують підґрунтя для визначення належного психоемоційного стану представника персоналу ОКІ.

Перелік та опис вказаних критеріїв наведено в табл. 1.1 та табл. 1.2. При визначенні переліку критеріїв та їх поділу на групи враховано необхідність експертного оцінювання закритих комерційних систем на основі

опосередкованих даних із відкритих джерел, а також необхідність визначення напрямків вдосконалення систем розпізнавання на основі значень запропонованих критеріїв.

Таблиця 1.1

Опис критеріїв ефективності основної групи

№	Критерії ефективності основної групи
A ₁	Рівень точності розпізнавання особи
A ₂	Стійкість до спуфінг-атак
A ₃	Оперативність розпізнавання особи
A ₄	Оперативність розробки системи розпізнавання, адаптованої до умов експлуатації

Таблиця 1.2

Опис критеріїв ефективності додаткової групи

№	Критерії ефективності додаткової групи
B ₁	Стійкість до розпізнавання в умовах завад на ЗО
B ₂	Стійкість до зміни умов відеореєстрації
B ₃	Пристосованість до аналізу кадру, що містить декілька ЗО
B ₄	Ресурсоемність процедури розпізнавання
B ₅	Ресурсоемність розробки системи розпізнавання
B ₆	Можливість розпізнавання емоцій

Також результати [50, 149] свідчать про доцільність оцінювання інтегральної ефективності засобів розпізнавання особи за допомогою виразу:

$$E_{\Sigma} = E_{\Sigma_{n,A}} + E_{\Sigma_{n,B}} = \theta_A \sum_{i=1}^4 \alpha_{i,n} A_{i,n} + \theta_B \sum_{j=1}^6 \beta_{j,n} B_{j,n}, \quad (1.1)$$

де E_{Σ} – інтегральна оцінка ефективності рішення; $E_{\Sigma_{n,A}}, E_{\Sigma_{n,B}}$ – інтегральна оцінка ефективності n -го рішення по критеріям ефективності групи

A та групи B відповідно; $\alpha_{i,n}$ – ваговий коефіцієнт i -го критерію ефективності групи A для n -го рішення; $\beta_{j,n}$ – ваговий коефіцієнт j -го критерію ефективності групи B для n -го рішення; θ_A, θ_B – вагові коефіцієнти групи критеріїв групи A та групи B ; $A_{i,n}$ – значення i -го критерію ефективності групи A ; $B_{j,n}$ – значення j -го критерію ефективності групи B .

У формулі (1.1) враховуються значення критеріїв груп A та B , для кожної групи використовуються відповідні вагові коефіцієнти. Також окремо кожному із критеріїв присвоєно відповідно свій ваговий коефіцієнт. Зазначимо, що для комерційних закритих систем БА значення критерію A_4 можливо оцінити на основі вартості системи та терміну її розгортання. У випадку наявності опису технічної реалізації системи розпізнавання при визначенні значення критерію A_4 також доцільно врахувати пристосованість архітектури системи до модифікації та здатність використаних НММ враховувати нові чинники без повного перенавчання. Критерій B_1 означає здатність системи ефективно проводити БА за ЗО та РОО при наявності завад. Результати аналізу дозволили в першому наближенні визначити значення критеріїв ефективності, що наведені в табл. 1.3 та в табл. 1.4, по кожному проаналізованому рішенню.

Таблиця 1.3

Значення критеріїв ефективності основної групи

№	Рішення	Значення критеріїв			
		A_1	A_2	A_3	A_4
1	2	3	4	5	6
1	FACETEC (www.facetec.com)	0,9	0,8	0,7	0,8
2	Acuity (www.acuitymi.com)	0,9	0,7	0,8	0,8
3	ID R&D (www.idrnd.ai)	0,9	0,9	0,9	0,8
4	VisionLabs (visionlabs.ai)	0,9	0,8	0,8	0,7
5	Neurotechnology (www.neurotechnology.com)	0,9	0,6	0,9	0,6
6	Iridian Tech (www.iridiantech.com)	0,9	0,7	0,9	0,6

Таблиця 1.3 (продовження)

1	2	3	4	5	6
7	Blink Identity (www.blinkidentity.com)	0,8	0,1	0,9	0,6
8	AxxonSoft (www.axxonsoft.com)	0,8	0,3	0,7	0,7
9	Face ID (Apple)	0,9	0,8	0,9	0,7
10	Android	0,8	0,7	0,9	0,7
11	Noldus company, FaceReader [39]	0,8	0,1	0,9	0,7
12	Logic Pursuits company, Captemo [41]	0,8	0,1	0,9	0,5
13	Herta company, BioObserver [45]	0,8	0,1	0,9	0,5
14	Висоцька О.О., Давиденко А.М., Христевич В. [129]	0,8	0,5	0,9	0,2
15	Долганенко О.Д., Сєверінов О.В., В'юхін Д.О., Коцюба В.П., Крепко А.В. [132]	0,8	0,5	0,9	0,2
16	Яковенко О.О., Кушніренко Н.І., Дорофєєва І.С., Євтушенко А.Р. [168]	0,7	0,1	0,9	0,2
17	Бондарчук А.П., Онисько А.І., Отрох С.І., Шевчук Д.О [126]	0,7	0,1	0,9	0,2
18	Бубенщиков О.В., Лєпа Є.В. [127]	0,7	0,1	0,9	0,2
19	Батюк Т., Досин Д. [125]	0,8	0,1	0,9	0,3
20	Ranjith, G., Pallavi, K., Mahendra, V. [77]	0,8	0,1	0,5	0,2
21	Ahmad S., Setumin S. [5]	0,8	0,1	0,8	0,5
22	Hamdani N., Bousahba N., Braikia A. [39]	0,9	0,1	0,7	0,7
23	Pranav K., Manikandan J. [74]	0,8	0,1	0,9	0,5
24	Hangaragi S., Singh T., Neelima N. [41]	0,7	0,3	0,7	0,7
25	Yergesh A.K. [120]	0,8	0,3	0,7	0,7
26	Kumar C., Saranya N., Priyadharshini M. [51]	0,8	0,1	0,6	0,8
27	Li L., Correia P., Hadid, A. [58]	0,8	0,7	0,7	0,5
28	Edmunds T., Caplier, A. [33]	0,9	0,7	0,4	0,4
29	Lokhande M., Khedkar M., Desale N. [63]	0,9	0,7	0,5	0,6

Зауважимо, що більші величини критеріїв B_4 та B_5 відповідають меншому обсягу ресурсів, необхідному для реалізації процедури розпізнавання та розробки системи розпізнавання, відповідно.

Таблиця 1.4

Значення критеріїв ефективності додаткової групи

№	Рішення	Значення критеріїв					
		B_1	B_2	B_3	B_4	B_5	B_6
1	2	3	4	5	6	7	8
1	FACETEC (www.facetec.com)	0,5	0,8	0,8	0,3	0,2	0
2	Acuity (www.acuitymi.com)	0,1	0,2	0,1	0,7	0,3	0
3	ID R&D (www.idrnd.ai)	0,1	0,5	0,2	0,7	0,3	0
4	VisionLabs (visionlabs.ai)	0,1	0,8	0,2	0,3	0,2	0,9
5	Neurotechnology (www.neurotechnology.com)	0,1	0,7	0,1	0,3	0,2	0
6	Iridian Tech (www.iridiantech.com)	0,1	0,7	0,1	0,3	0,3	0
7	Blink Identity (www.blinkidentity.com)	0,6	0,9	0,9	0,3	0,3	0
8	AxxonSoft (www.axxonsoft.com)	0,6	0,7	0,9	0,3	0,2	0
9	Face ID (Apple)	0,8	0,9	0,1	0,9	0,3	0
10	Android	0,7	0,7	0,1	0,9	0,3	0
11	Noldus company, FaceReader [39]	0,6	0,5	0,9	0,3	0,3	0,9
12	Logic Pursuits company, Captemo [41]	0,4	0,5	0,5	0,4	0,3	0,9
13	Herta company, BioObserver [45]	0,4	0,7	0,2	0,3	0,3	0,9
14	Висоцька О.О., Давиденко А.М., Христович В. [129]	0,1	0,5	0,6	0,8	0,8	0,7
15	Долганенко О.Д., Сєверінов О.В., В'юхін Д.О., Коцюба В.П., Крепко А.В. [132]	0,1	0,3	0,2	0,5	0,5	0
16	Яковенко О.О., Кушніренко Н.І., Дорофєєва І.С., Євтушенко А.Р. [168]	0,1	0,2	0,1	0,9	0,8	0
17	Бондарчук А.П., Онисько А.І., Отрох С.І., Шевчук Д.О [126]	0,1	0,2	0,1	0,9	0,8	0

Таблиця 1.4 (продовження)

1	2	3	4	5	6	7	8
18	Бубенчиков О.В., Лєпа Є.В. [127]	0,1	0,2	0,1	0,9	0,8	0
19	Батюк Т., Досин Д. [125]	0,1	0,2	0,1	0,8	0,8	0
20	Ranjith, G., Pallavi, K., Mahendra, V. [77]	0,1	0,5	0,6	0,7	0,6	0
21	Ahmad S., Setumin S. [5]	0,1	0,5	0,1	0,8	0,9	0
22	Hamdani N., Bousahba N., Braikia A. [39]	0,3	0,4	0,1	0,7	0,8	0
23	Pranav K., Manikandan J. [74]	0,2	0,2	0,1	0,7	0,7	0
24	Hangaragi S., Singh T., Neelima N. [41]	0,2	0,2	0,1	0,7	0,7	0
25	Yergesh A.K. [120]	0,4	0,4	0,1	0,8	0,6	0
26	Kumar C., Saranya N., Priyadharshini M. [51]	0,1	0,5	0,1	0,6	0,7	0
27	Li L., Correia P., Hadid, A. [58]	0,1	0,5	0,1	0,6	0,7	0
28	Edmunds T., Caplier, A. [33]	0,6	0,6	0,1	0,7	0,7	0,1
29	Lokhande M., Khedkar M., Desale N. [63]	0,6	0,6	0,1	0,7	0,7	0,1

Зазначимо, що показані в табл. 1.3 та в табл. 1.4 оцінки ефективності n -го рішення по критеріям ефективності групи A та групи B визначаються десятковим числом в межах від 0 до 1. При цьому значення критерію дорівнює 1, якщо відповідна вимога повністю забезпечується, і дорівнює 0, якщо не забезпечується.

Як свідчать відображені в табл. 1.3 та табл. 1.4 результати аналізу відомих науково-практичних робіт, сучасні засоби БА за ЗО та РОО потребують комплексного вдосконалення в напрямках підвищення стійкості до спуфінг-атак, забезпечення оперативності розробки та адаптації системи розпізнавання до умов відеореєстрації, підвищення стійкості до розпізнавання в умовах завад на ЗО, зменшення ресурсоемності розробки системи розпізнавання, а також розширення функціоналу, зокрема можливості розпізнавання емоцій. Крім того, відповідно до даних [117, 123, 125], точність розпізнавання особи також потребує підвищення. При цьому, відповідно до результатів [95, 145, 146], підвищити оперативність розробки та адаптації системи розпізнавання до умов

експлуатації можливо за рахунок застосування апробованих вільнодоступних НМЗ, які забезпечують виконання операцій, що входять до складу процесу БА персоналу ОКІ (див. рис.1.1). Так, для захоплення ЗО у відеопотоці можливо використати інструментальні засоби на базі НММ типу: MTCNN (Multi-task Cascaded Convolutional Networks), RetinaFace, FaceBoxes, DSFD (Dual Shot Face Detector), SCRFD (Single-Shot Scale-Aware Face Detector), YOLO-Face, BlazeFace, MobileFace [2, 19, 40, 44, 64, 90, 91].

Для визначення координат ключових точок на ЗО можливо застосувати інструментальні засоби з використанням НММ типу: KeyPosS (KeyPoint Positioning System), NaimishNet, ArtFacePoints, Efficient Facial Key Point Detection, Face Mesh, OpenFace, Face Alignment Network (FAN) [4, 12, 14, 31, 50, 66, 87].

Для розпізнавання особи за ЗО та РОО можливо використати інструментарій на основі НММ типу: FaceNet, InsightFace, VGGFace2, MagFace, OSIRIS, ArcFace, MobileNet [18, 29, 44, 50, 66, 83]. Зазначимо, що НМЗ OSIRIS забезпечує розпізнавання особи лише за РОО. При цьому вказані інструментальні засоби використовують НММ, пристосовані для класифікації зображень. Через це введення або видалення особи із списку легітимних представників персоналу ОКІ призводить до необхідності як мінімум донавчання НММ, або навіть і до зміни архітектури НММ. Тому доцільно розглянути можливість використання в системі БА НМЗ, пристосованих до розпізнавання особи за рахунок порівняння ЗО.

Для розпізнавання емоцій можливо використати інструментальні НМЗ: OpenFace, EmoReact, DeepFace, FaceEmotion_ID, базові положення розробки яких наведено в [8, 12, 17, 78, 84, 98]. Для розпізнавання спуфінг-атак можливо використати інструментальні НМЗ: DeepFaceLab, DeepPixBiS [34, 113]. Також аналіз досліджень в області розпізнавання спуфінг-атак вказує на те, що поширені засоби розпізнавання базуються на аналізі якості підконтрольного зображення, аналізі його просторових характеристик, перевірці динаміки параметрів, характерній для ЗО і РОО живої людини, та виконанні

підконтрольною особою певних команд, що спричиняють зміну параметрів відеореєстрації [80, 110, 144-146].

Разом з тим, у цих же роботах відзначені труднощі ефективного аналізу якості ЗО і РОО при варіативних умовах відеореєстрації та труднощі визначення просторових характеристик при відеореєстрації однією камерою.

Труднощі визначення просторових характеристик виникають і при застосуванні декількох камер у випадку різних ракурсів відеореєстрації, що характерно для умов ОКІ. При цьому відомі підходи співставлення динаміки параметрів ЗО та РОО з приналежністю до живої людини недостатньо ефективні внаслідок можливого використання сучасних 3D-моделей та масок, що імітують ЗО та РОО, а негативні наслідки впровадження в систему БА контуру подачі команд та перевірки результатів полягають не тільки в ускладненні самої системи БА, але і у можливому перешкоджанні виконанню персоналом своїх функціональних обов'язків. Тому сучасні засоби БА потребують вдосконалення в напрямку підвищення стійкості розпізнавання представника персоналу ОКІ в умовах можливої реалізації спуфінг-атак за рахунок застосування нових підходів до розпізнавання спуфінг-атак.

Також в результаті проведеного аналізу показано, що підвищити ефективність НМЗ БА за ЗО та РОО можливо за рахунок впровадження в них сучасних технологій, орієнтованих на визначені напрями вдосконалення, що, у свою чергу, зумовило необхідність проведення критичного огляду науково-прикладних досліджень в області підвищення ефективності засобів аналізу зображень.

1.3. Критичний огляд науково-прикладних рішень в області підвищення ефективності засобів аналізу зображень

Враховуючи результати п. 1.2 даної дисертаційної роботи, при проведенні критичного огляду в першу чергу увагу було акцентовано на визначенні перспективних шляхів підвищення точності розпізнавання особи при вхідному контролі на ОКІ, коли можливо вважати, що умови відеореєстрації знаходяться

в заданих межах. Відповідно до результатів [146, 147], підвищити точність розпізнавання особи за ЗО та РОО можливо за рахунок підвищення точності виділення контурів обличчя на вхідному зображенні та за рахунок підвищення точності визначення координат ключових точок обличчя за передумови, що співставлення вхідного ЗО з еталонними ЗО реалізується з використанням методів аналізу ключових точок. Зазначимо, що в теперішній час для виділення контурів об'єктів широко застосовуються як нейромережеві технології семантичної сегментації, так і класичні технології комп'ютерної графіки, розробці яких присвячена велика кількість науково-практичних робіт, детальний аналіз яких наведено в статті [128]. Зокрема, було розглянуто процедуру оброблення послідовності зображень низької роздільної здатності з метою виділення об'єктів, визначених за кількома параметрами. Фільтрація напівтонових зображень здійснювалася за допомогою низькочастотного фільтра Гаусса, а для компенсації тіней використовувався пороговий розподіл гістограми інтенсивності. Виділення контурів об'єктів реалізовувалося за алгоритмом Кенні. Слід зазначити, що ефективність запропонованої методики, насамперед на етапах виділення меж і пошуку робочих об'єктів, викликає певні сумніви, оскільки експерименти проведено для порівняно простих растрових зображень, а використаний алгоритм виділення меж не забезпечує коректного розділення контурів об'єктів, що частково перекривають один одного.

Також результати [128] вказують на проведення досліджень, спрямованих на розроблення стратегій сегментації об'єктів у цифрових зображеннях із урахуванням їхніх структурних особливостей. Зокрема, було проаналізовано специфіку сегментації мікроструктурних зображень поверхні металів, отриманих за допомогою мікроскопа. Запропоновано підхід, що базується на припущенні про обмежену семантичну інформативність локальних сусідських відносин пікселів, притаманну іконічному рівню цифрової матриці зображення. Така особливість може спричиняти регулярні помилки сегментації. Для їх мінімізації передбачено перехід до більш складної семантичної моделі відносин сусідства, що враховує властивості об'єкта та дозволяє підвищити коректність виділення його меж.

У сфері обробки медичних зображень запропоновано метод сегментації, орієнтований на ідентифікацію однотипних об'єктів. Його принцип ґрунтується на аналізі індексу однорідності масиву вхідних зображень, який визначається за показниками яскравості. Заявлено, що застосування такого підходу дозволяє розділити тестові зображення на фон, окремі структурні елементи та контури цільових об'єктів, які подаються у вигляді масиву бінарних зображень. Метод передбачає поетапне уточнення меж об'єктів на основі аналізу локальної однорідності інтенсивності пікселів, що потенційно може підвищити точність виділення дрібних структур. Однак результати експериментів свідчать, що якість сегментації є недостатньою для довільних типів зображень, що зумовлено використанням виключно класичних алгоритмів обробки даних із фіксованими пороговими значеннями, визначеними за допомогою експертних правил.

У сфері обробки зображень для систем автоматичного супроводу було запропоновано багатоетапний алгоритм відбору, виявлення та оцінки параметрів аерооб'єктів. Даний алгоритм призначений для обробки зображень, отриманих з відеокамер у видимому та інфрачервоному діапазонах. Алгоритм заснований на тому принципі, що для вибору між гіпотезою Y_1 , яка вказує на наявність об'єкта, та гіпотезою Y_2 , яка вказує на його відсутність, розраховується значення коефіцієнта відношення правдоподібності, яке порівнюється із заздалегідь визначеним порогом.

У сфері комп'ютерного зору промислових роботів запропоновано підходи до відбору інваріантних ознак зображень, нечутливих до обертання, перенесення та масштабування. Запропоновані рішення ґрунтуються на поєднанні методів скелетизації, контурної побудови та сегментації зображення, що забезпечує поступове формування об'єктів: спочатку з незамкнених ліній, потім із замкнених контурів, а в кінцевому підсумку у вигляді силуетного представлення, яке може бути перетворене у площинні форми. Загалом такі підходи не мають принципових відмінностей від традиційних методів сегментації, що базуються на класичних алгоритмах обробки зображень та використанні фіксованих

коефіцієнтів обробки. Зокрема, застосований алгоритм скелетизації фактично є комбінацією відомих методів бінаризації зображення та видалення шумів.

Окремий напрям досліджень спрямовано на розробку алгоритмів автоматичної селекції рухомих об'єктів під час багатоспектрального спостереження. При цьому використовувалися математичні моделі зображень, які забезпечують можливість врахування геометричних перетворень, спричинених рухом датчика зображення. Крім того, заявлено про можливість нівелювання шуму, пов'язаного з геометричними спотвореннями, викликаними атмосферними явищами, що впливають на рухомий об'єкт. В аналітичній формі правило прийняття рішення щодо належності точки цільовому об'єкту записується у формі:

$$u^*(b_1, b_2) = \begin{cases} 1, \text{if } p\left(b_1, \frac{b_2}{h} = 0\right) < \delta \\ 0, \text{if } p\left(b_1, \frac{b_2}{h} = 0\right) \geq \delta \end{cases} \quad (1.2)$$

де (b_1, b_2) – результат прийняття рішення; δ – порогове значення; b_1, b_2 – яскравість пікселя в кожному з каналів спостереження; $p\left(b_1, \frac{b_2}{h} = 0\right)$ – умовна щільність розподілу яскравості цільового зображення.

Як і у більшості відомих підходів, на основі класичних технологій комп'ютерної графіки, для розрахунку порогового значення δ пропонується використовувати експертні правила, що обмежує можливість їх адаптації до нових типів зображень.

Зазначимо, що бібліотека OpenCV, яка використовується для реалізації засобів комп'ютерного зору, також містить сервіси, які можна віднести до виділення об'єктів на растровому зображенні. Ці сервіси забезпечують вибір меж об'єкту, кластеризацію об'єктів за допомогою каскадного алгоритму і порогової сегментації. У разі кластеризації простір ознак об'єктів зображення розбивається на кластери, якщо заданий критерій цього об'єкта перевищує заздалегідь визначене значення. Всі об'єкти на зображенні спочатку розподіляються по кластерах, а потім по сегментах, які об'єднують елементи одного кластера. Об'єднання в сегмент здійснюється шляхом визначення критерію однорідності.

Ефективність функціонування цих сервісів в основному залежить від емпірично визначених порогових коефіцієнтів.

Крім того, в роботах [13, 16, 62, 116] відзначено, що проблематика семантичної сегментації зображень ускладнюється через можливе часткове або повне перекриття цільових об'єктів, нечіткість їх кордонів, різноваріантність розмірів та розміщення. Варіативність умов розпізнавання посилюється внаслідок можливої зміни джерела отримання зображення, в якості якого в більшості комп'ютерних систем використовується відеокамера, що зумовлює можливу зміну основних параметрів піддослідного растрового зображення – розміру, роздільної здатності та кількості кольорових каналів. Також негативний вплив на результат розпізнавання може бути викликаний завадами та ракурсом відеореєстрації. Внаслідок описаних труднощів засоби семантичної сегментації зображень, що базуються на класичних методах типу «нарощування областей», «аналіз кордонів», «подрібнення областей», являються вузькоспеціалізованими і потребують значної модифікації навіть при незначних змінах умов застосування. Висновок щодо обмеженості класичних методів виділення підтверджується результатами аналізу статті [49], в якій наведено опис моделей відслідковування зображень об'єктів за допомогою інтегрованих фільтрів різного типу.

Таким чином, аналіз сучасних літературних джерел, присвячених класичним технологіям комп'ютерної графіки, дозволяє обґрунтовано стверджувати, що особливості цих технологій, які полягають у використанні емпірично визначених коефіцієнтів, суттєво ускладнюють їх застосування при розв'язанні багатоваріантного завдання детектування кордонів обличчя людини в системах БА персоналу ОКІ. Перспективним шляхом виправлення цих недоліків є використання нейромережових технологій семантичної сегментації растрових зображень [35, 86].

Використання НММ для виділення об'єктів на зображеннях описане в науково-практичних роботах [10, 24, 96, 105, 119]. Проведений аналіз дозволив побудувати показану на рис. 1.2 типову структурну схему функціонування НМС семантичної сегментації растрових зображень. Також визначено, що до

апробованих НММ в області семантичної сегментації растрових зображень відносяться: Fully Convolutional Networks (FCN), DeepLabV3+, SegNet, U-Net, PSPNet (Pyramid Scene Parsing Network), HRNet (High-Resolution Network), Transformer-based Networks (SETR, MaskFormer).

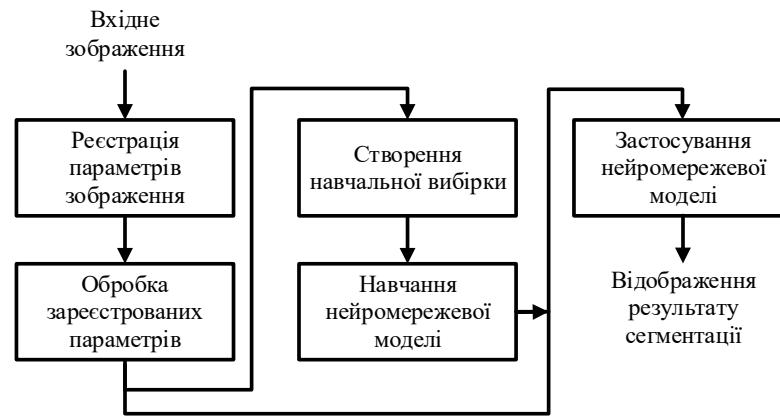


Рис. 1.2. Типова структурна схема функціонування нейромережевої системи семантичної сегментації растрових зображень

Результати науково-практичних робіт [10, 35, 79, 92] дозволяють стверджувати про те, що однією із найбільш ефективних нейромережових архітектур, пристосованих до семантичної сегментації растрових зображень, являється НММ, котра складається із двох блоків – енкодера та декодера. Завданням енкодера являється визначення багатовимірного масиву ознак початкового зображення, а завданням декодера являється отримання обробленого зображення, у якого кожен із пікселів отримує маркер відношення до одного із виділених цільових об'єктів або фону. Тобто в такій НММ зображення спочатку подається по так званому звужуючому шляху, на якому власне і реалізується виділення значимих ознак зображення, а потім по шляху розширення, що забезпечує маркування пікселів зображення.

На вхід моделі подається зображення в форматі RGB, а виходом являється сегментоване зображення. При цьому енкодер та декодер представляють собою дещо модифіковані ЗНМ. Модифікація полягає у тому, що використовуються не повнорозмірні ЗНМ, а тільки блоки ЗНМ, які призначені для визначення значимих ознак. Тобто до складу таких ЗНМ входять тільки шари згортки та

масштабування, а повнозв'язні шари вилучені. Відповідно до результатів [79, 92], однією із найбільш ефективних нейромережових енкодер-декодерних архітектур, пристосованих до семантичної сегментації растрових зображень, являється НММ типу U-Net. Принципова схема НММ типу U-Net, що призначена для виділення об'єктів на ЗО, показана на рис. 1.3.

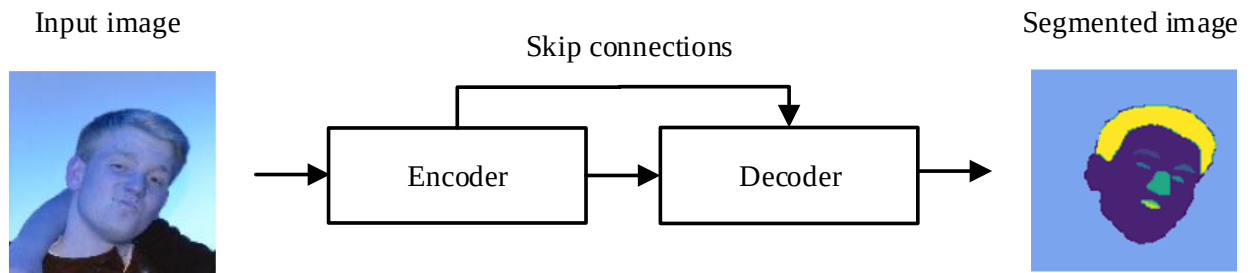


Рис. 1.3. Принципова схема нейромережової моделі типу U-Net, що призначена для сегментації зображення обличчя

Ще однією особливістю схеми НММ, показаної на рис. 1.3, являється симетричність шарів згортки та масштабування енкадера та декодера. В загальному випадку така симетрія може бути відсутня. Також на сьогодні не вирішеними залишаються ряд окремих задач, розв'язання яких дозволить підвищити ефективність НМЗ семантичної сегментації ЗО. Відповідно до висновків [27, 97, 106] та результатів аналізу [1, 57, 124], однією із таких задач являється адаптація типу та параметрів ЗНМ до умов виділення об'єкта на зображенні. В свою чергу, вирішенню цієї задачі має передувати визначення та формалізація означених умов виділення, розробка апарату для оцінки точності та обчислювальної ресурсоемності моделі. Крім того, потребують уточнення критерії визначення ефективності ЗНМ. При цьому, відповідно до оціночних результатів [50], до перспективних типів ЗНМ, що можуть бути використані в якості енкадера та декодера НММ для виділення контурів ЗО, належать: EfficientNet, MobileNet, ShuffleNet, GhostNet, MnasNet, FBNet. Це пояснюється доведеною високою точністю, низькою ресурсоемністю, апробованістю та

відкритим характером вказаних НММ, опис яких наведено в [19, 29, 40, 44, 66, 90, 91, 123].

Також, відповідно до результатів п. 1.2, проаналізовані можливості НММ, які пристосовані до порівняння зображень з метою розпізнавання особи представника персоналу ОКІ за ЗО. Визначено, що більшість таких НММ базуються на архітектурі типу Siamese Network або Two_channel Networks, опис яких наведено в роботах [39, 51, 130, 166]. При цьому, відповідно до [145-147], вдосконалення відповідних НММ, побудованих на базі цих архітектур, можливо реалізувати за аналогією із вдосконаленням мереж на базі архітектури U-Net за рахунок використання в них моделей типу EfficientNet, MobileNet, ShuffleNet, GhostNet, MnasNet, FBNet.

Також результати проведеного аналізу свідчать про відсутність формалізованого цілісного опису процесу БА персоналу ОКІ за ЗО та РОО, що враховує наявність типових завад, можливість атак на систему БА за допомогою муляжів (спуфінг-атак), необхідність визначення особи та визначення емоційного стану представника персоналу.

1.4. Висновки

В результаті аналізу науково-практичних робіт, присвячених захисту об'єктів критичної інфраструктури, показано, що одна із найбільш актуальних задач в даній області полягає у підвищенні ефективності засобів розпізнавання особи на основі нейромережевого аналізу зображення обличчя та райдужної оболонки ока. Також, проаналізувавши відомі промислові та дослідницькі рішення відповідного призначення, а також нормативні вимоги до системи біометричної автентифікації на об'єктах критичної інфраструктури, виділено дві групи критеріїв ефективності зазначених нейромережевого засобів. До основної групи віднесено критерії, які безпосередньо характеризують ефективність процесу розпізнавання в умовах відеореєстрації, що зазвичай встановлені для контролю доступу при вході на об'єкт критичної інфраструктури, коли умови відеореєстрації знаходяться у наперед визначених межах. До додаткової групи

віднесено критерії, які дозволяють оцінити ефективність системи розпізнавання з позицій стійкості до зовнішніх чинників, ресурсоемності процесу розпізнавання, ресурсоемності розробки системи розпізнавання, та забезпечують підґрунтя для визначення належного функціонального стану представника персоналу. З використанням методів експертного оцінювання проведено оцінювання ефективності означених нейромережевих рішень та визначено потребу їх комплексного вдосконалення в напрямках підвищення стійкості до спуфінг-атак, забезпечення оперативності розробки та адаптації до умов відеореєстрації, з урахуванням можливої наявності завад, зменшення ресурсоемності розробки, а також розширення функціоналу, зокрема в напрямку розпізнавання емоцій. Разом з тим, критичний огляд науково-прикладних робіт в області засобів аналізу зображень дозволяє стверджувати про можливість реалізації відповідних вдосконалень за рахунок застосування сучасних нейромережевих рішень, адаптованих до очікуваних умов застосування в інформаційних системах об'єктів критичної інфраструктури.

Таким чином, обґрунтовано актуальність та можливість розробки засобів, які, за рахунок застосування сучасних відомих нейромережевих рішень, забезпечують достатню точність розпізнавання особи на основі нейромережевого аналізу зображення обличчя та райдужної оболонки ока, отриманих в різних умовах відеореєстрації, у тому числі за наявності завад, підвищують ефективність виявлення спуфінг-атак і створюють підґрунтя для визначення відповідності психоемоційного стану представника персоналу вимогам щодо належного виконання службових обов'язків.

РОЗДІЛ 2. МОДЕЛІ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

2.1. Модель процедури розпізнавання особи за зображенням обличчя та райдужною оболонкою ока при біометричній автентифікації персоналу об'єктів критичної інфраструктури з застосуванням нейромережевих засобів

Як показують результати [42, 72, 88, 151, 155], в моделі процедури розпізнавання особи за ЗО та РОО при БА персоналу ОКІ з застосуванням НМЗ, що, відповідно до відомих підходів до розробки засобів БА [16, 144], являється відправним пунктом досліджень в напрямку побудови моделей та методів БА, слід відобразити термінологію, що враховує особливості прикладної області; аналітичний вираз, що описує перетворення інформації, реалізований даною процедурою; перелік основних завдань, що визначають окремі операції даної процедури; підходи до реалізації означених операцій; критерії оцінювання ефективності окремих операцій та процедури в цілому.

Використовуючи результати [28, 32, 43, 63, 102], при розробці моделі використано наступні терміни:

- НММ – модель, що описує архітектуру нейронної мережі та нейрони, які входять до її складу.
- РОО – це забарвлене кільце в передній частині ока, що оточує зіницю.
- ЗО – зображення передньої частини голови людини, що зверху обмежене чолом, внизу – нижнім краєм підборіддя, з боків – основою вушних раковин.
- БА – автентифікація, що базується на результатах аналізу біометричних даних людини.
- Атака за допомогою муляжів (спуфінг) – атака, що реалізується за рахунок подачі підроблених біометричних даних на сенсор.
- Емоція – це психічне відображення у формі безпосереднього, упередженого переживання життєвого сенсу явищ і ситуацій, обумовленого

відношенням їх об'єктивних властивостей до потреб суб'єкта.

- Базові емоції – гнів, відроза, сум, страх, здивування, презирство, радість.
- Контрольні точки – точки обличчя, які використовуються для розпізнавання особи та емоцій.

Враховуючи специфіку проблеми розробки НМЗ БА персоналу ОКІ, запропонована модель в першу чергу призначена для опису процесів нейромережевої обробки зареєстрованого відеопотоку для розпізнавання особи і емоцій представника персоналу ОКІ, а також для розпізнавання спуфінг-атак. Тому в базовому випадку модель розпізнавання можливо описати за допомогою виразу виду:

$$\langle \Theta, X \rangle \xrightarrow{NR} \langle Y_I, Y_E, Y_A \rangle, \quad (2.1)$$

де Θ – множина параметрів, що характеризують умови застосування НМЗ; X – множина параметрів, що характеризують зображення, асоційовані з окремими кадрами відеопотоку; Y_I, Y_E, Y_A – множини параметрів, що описують результат розпізнавання особи, розпізнавання емоцій та спуфінг-атак; NR – оператор нейромережевого розпізнавання.

Враховуючи [7, 13, 25, 56] та специфіку задачі нейромережевого аналізу ЗО та РОО для розпізнавання особи та емоцій, прийнято, що основні умови застосування НМЗ характеризуються розміром вхідного зображення ($W \times H$), кількістю кольорових каналів в зображенні (C), кількістю класів, що мають бути розпізнані (K), загальною кількістю навчальних прикладів у навчальній вибірці (N_Σ), кількістю навчальних прикладів для кожного із класів (N_{i_k}), максимально доступним обсягом пам'яті для зберігання параметрів НММ (V_{CR}^d), прийнятним обсягом пам'яті для зберігання параметрів НММ (V_{CR}^s), допустимим терміном процесу розпізнавання (Δ_T), видом та мінімально допустимим значенням показника точності розпізнавання (A, Δ_A), допустимою кількістю епох навчання (Δ_{TL}). Для деталізації базового варіанту моделі проведено декомпозицію процедури розпізнавання особи за ЗО та РОО при БА персоналу ОКІ з урахуванням необхідності розпізнавання емоцій та спуфінг-атак. Відповідно до [2, 33, 34, 37], увагу акцентовано на специфічних операціях, ефективність яких

в сучасних системах БА персоналу ОКІ можливо вважати недостатньою. До вказаних операцій слід віднести: виділення ЗО та РОО на зображенні; виявлення та нівелювання завад на ЗО і РОО; виявлення атак за допомогою муляжів (спуфінг-атак). Діаграма декомпозиції процедури розпізнавання особи за ЗО та РОО, побудована з урахуванням означених операцій, показана на рис. 2.1.

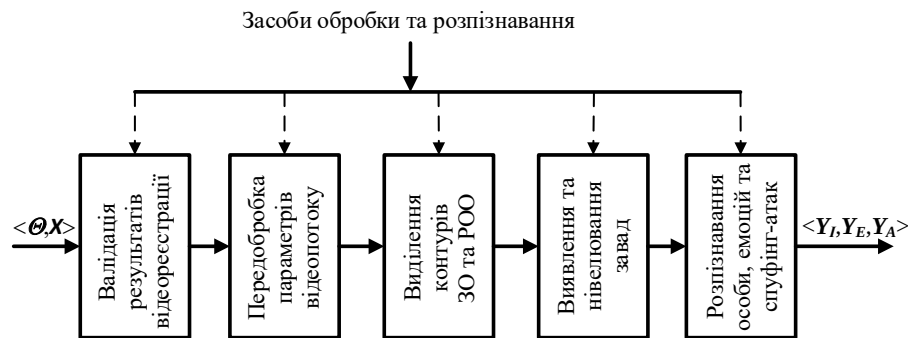


Рис. 2.1. Діаграма декомпозиції процедури розпізнавання особи за ЗО та РОО при БА персоналу ОКІ

При обґрунтуванні переліку операцій процедури розпізнавання з позицій обмеженості обчислювальних ресурсів, необхідності оперативної реалізації та можливостей сучасних НМЗ, визначено доцільність проведення однієї операції попередньої обробки вхідного відеопотоку, що реалізується без використання НМЗ. Зазначимо, що, відповідно до [20, 21, 99], процедури виділення контурів ЗО та РОО, виявлення та нівелювання завад і розпізнавання особи, емоцій та атак пропонується реалізовувати з використанням неймережевих підходів.

Також на основі [33, 37, 58, 63] визначено доцільність застосування багаточинникового підходу до розпізнавання спуфінг-атак, що передбачає неймережевий аналіз візуальних артефактів, артефактів зовнішнього оточення, показників живучості та показників, що характеризують природність емоцій. При цьому

$$Y_A = \{Y_v, Y_o, Y_l, Y_e\}, \quad (2.2)$$

де Y_v, Y_o, Y_l, Y_e – результат розпізнавання спуфінг-атаки за візуальними артефактами, артефактами зовнішнього оточення, за живучістю та за природністю емоцій.

Враховуючи розроблену діаграму та базуючись на результатах проведеного літературного аналізу [8, 9, 48, 52], з урахуванням можливості попередньої обробки відеопотоку за допомогою класичних технологій та багаточинникового підходу до розпізнавання спуфінг-атак, визначено, що до основних завдань нейромережових засобів БА персоналу ОКІ відносяться:

1. Виділення кордонів ЗО у піддослідному кадрі вхідного відеопотоку.
2. Детектування спуфінг-атак на основі візуальних артефактів, що відображаються за рахунок зміни текстури, кольору зображення, виникнення на ньому відблисків, розривів контурів зображення.
3. Детектування спуфінг-атак на основі артефактів зовнішнього оточення, наприклад, відображення обличчя на екрані мобільного пристрою або відсутність у відеокадрі предметів, які очікувано знаходяться у зоні відеореєстрації.
4. Виявлення областей завад, характерних для очікуваних умов відеореєстрації.
5. Виділення кордонів РОО.
6. Визначення множин координат контрольних і ключових точок, що використовуються для розпізнавання особи та емоцій.
7. Детектування спуфінг-атак за динамікою параметрів живучості (liveness detection parameters), що використовуються для розпізнавання відповідності зображення реальному обличчю живої людини.
8. Розпізнавання базових емоцій, відображених на обличчі.
9. Детектування спуфінг-атак на основі розпізнаних емоцій.
10. Розпізнавання особи представника персоналу ОКІ.

Визначення вказаних завдань проведено з урахуванням апробованих рішень в області нейромережового аналізу ЗО, РОО та в області БА. При цьому, з позицій реалізації НМЗ аналізу однорідних процесів, завдання детектування спуфінг-атак на основі спуфінг-артефактів розділено на два окремих завдання: детектування спуфінг-атак за візуальними артефактами (завдання 2) та детектування спуфінг-атак за артефактами зовнішнього оточення (завдання 3).

На наступному етапі побудови моделі процедури розпізнавання реалізовано визначення множин критеріїв, що використовуються для оцінки ефективності системи БА ОКІ, а також при побудові засобів розпізнавання для оцінювання ефективності окремих операцій та процедури розпізнавання в цілому. Базуючись на аналізі результатів [131, 155, 159], визначено, що для оцінювання ефективності систем БА на ОКІ доцільно використовувати критерії, які ґрунтуються на таких апробованих показниках: ймовірність хибного допуску (FAR), ймовірність хибного відхилення (FRR), коефіцієнт рівної ймовірності помилок (EER), площа під ROC-кривою (AUC), робоча характеристика приймача (ROC-крива) та DET-крива (компроміс похибок виявлення). Відповідно до результатів [13, 16, 46, 53, 71], ефективність операцій процедури розпізнавання, окрім операції передобробки параметрів відеопотоку, пропонується оцінювати за допомогою показників точності та ресурсоємності. Щодо операції передобробки, то для оцінювання її ефективності замість показників точності слід використовувати показники якості зображення. В теорії нейронних мереж при вирішенні задач класифікації базовим критерієм оцінки точності є *Accuracy*. Однак використання цього критерію має обмеження, пов'язані з необхідністю пропорційного представлення об'єктів різних класів у вибірці та неможливістю оцінки точності класифікації об'єктів певного класу, що можна вважати суттєвим недоліком в системах БА при розпізнаванні легітимного/нелегітимного користувача, коли неправильна класифікація нелегітимного може призвести до значних негативних наслідків. Тому для оцінки точності використовуються декілька критеріїв, комплексний аналіз яких дозволяє адекватно оцінити відповідність системи розпізнавання поставленим вимогам. Використовуючи результати [50, 94, 101], визначено, що, крім *Accuracy*, в якості критеріїв оцінювання точності доцільно використовувати *Recall*, *Precision*, *F1-score*. Операції виділення контурів 3О та РОО, можливо класифікувати як мультикласову семантичну сегментацію зображень [2, 144, 145], що дозволяє оцінити точність їх реалізації за допомогою коефіцієнта Дайтса (*Dice*) та коефіцієнта Жаккара (*IoU*):

$$Dice = \frac{2}{k_D} \sum_{k=1}^K (y_{t,n} \times y_{m,n}), \quad (2.3)$$

$$k_D = \sum_{k=1}^K y_{t,n} + \sum_{k=1}^K y_{m,n}, \quad (2.4)$$

$$IoU = \frac{1}{k_J} \sum_{k=1}^K (y_{t,n} \times y_{m,n}), \quad (2.5)$$

$$k_J = \sum_{k=1}^K y_{t,n} + \sum_{k=1}^K y_{m,n} - \sum_{k=1}^K (y_{m,n} \times y_{t,n}), \quad (2.6)$$

де K – кількість точок, що описують очікуваний вихідний сигнал для об'єкта, який має бути виділений; $y_{m,n}$ – значення, характерне для n -го пікселя виділеного об'єкта; $y_{t,n}$ – значення, характерне для i -го пікселя очікуваного вихідного сигналу.

При обґрунтуванні критерію оцінки якості попередньо обробленого зображення передбачається, що засоби розпізнавання будуть використовуватись для розпізнавання персоналу ОКІ не тільки при автентифікації при вході в систему, але й при виконанні ними функціональних обов'язків. В цьому випадку можливо очікувати широкий спектр умов відеореєстрації, що зумовлює потенційну необхідність оцінювання розмірів, яскравості та контрастності. Також при виборі критерію оцінювання якості попередньої обробки слід очікувати недоступність еталону зареєстрованого зображення. Ще одним важливим чинником, що впливає на вибір критерію, є необхідність його оперативного розрахунку не тільки на основі показників RGB-зображення, але і на основі каналу яскравості (Y) в кольоровій моделі $YCbCr$. При цьому конвертація RGB-зображення в $YCbCr$ -зображення реалізується відповідно до стандарту ITU-R BT.601 за допомогою виразів виду (2.7-2.9), а зворотня конвертація – за допомогою виразів (2.10-2.12).

$$Y(n) = 0.299R(n) + 0.587G(n) + 0.114B(n), \quad (2.7)$$

$$C_b(n) = -0.168736R(n) - 0.331264G(n) + 0.5B(n) + 128, \quad (2.8)$$

$$C_r(n) = -0.5R(n) - 0.418688G(n) - 0.081312B(n) + 128, \quad (2.9)$$

де n – номер пікселя зображення; $Y \in [0,255]$ – компонента яскравості; $C_b \in [0,255]$, $C_r \in [0,255]$ – компоненти, що відповідають за синьо-жовтий та червоно-зелений відтінок, відповідно.

$$R(n) = Y(n) + 1.402 \cdot (C_r(n) - 128), \quad (2.10)$$

$$G(n) = Y(n) - 0.344136 \cdot (C_b(n) - 128) - 0.714136 \cdot (C_r(n) - 128), \quad (2.11)$$

$$B(n) = Y(n) + 1.772 \cdot (C_b(n) - 128). \quad (2.12)$$

Враховуючи вказані передумови та результати досліджень в області оцінки якості обробки статичних зображень та відеопотоку, визначено необхідність розрахунку середньої (Y_{avg}), максимальної (Y_{max}), мінімальної (Y_{min}) яскравості, значень елементів вектору ($\mathbf{I} = |i|_{256}$), що забезпечує побудову гістограми яскравості. Також, відповідно до виразів (2.13-2.23), проводиться розрахунок контрасту Міхельсона (λ_M), стандартного відхилення яскравості (σ_Y), індексу засвітлення (R_{br}), індексу затемнення (R_{dr}), Лапласіан зображення ($\mathbf{L}$), дисперсію Лапласіана (σ_L^2), середню яскравість по кожному із каналів RGB-зображення (μ_R, μ_G, μ_B), середню яскравість каналів RGB-зображення (μ_{avgRGB}), максимальне відхилення яскравості каналу RGB-зображення (Δ_{avgRGB}).

$$\lambda_M = \frac{Y_{max} - Y_{min}}{Y_{max} + Y_{min}}, \quad (2.13)$$

$$\sigma_Y = \sqrt{N^{-1} \sum_{n=1}^N (Y_n - Y_{avg})^2}, \quad (2.14)$$

$$R_{br} = \frac{N_{Y>220}}{N}, \quad (2.15)$$

$$R_{dr} = \frac{N_{Y<30}}{N}, \quad (2.16)$$

$$L(i, j) = \sum_{k=-1}^1 \sum_{l=-1}^1 (K(k, l) \times Y(i + k, j + l)), \quad (2.17)$$

$$K = \begin{bmatrix} 0 & 1 & 0 \\ 1 & -4 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \quad (2.18)$$

$$L_{avg} = N^{-1} \sum_{n=1}^N L_n, \quad (2.19)$$

$$\sigma_L^2 = N^{-1} \sum_{n=1}^N (L_n - L_{avg})^2, \quad (2.20)$$

$$\mu_R = N^{-1} \sum_{n=1}^N R(n), \mu_G = N^{-1} \sum_{n=1}^N G(n), \mu_B = N^{-1} \sum_{n=1}^N B(n), \quad (2.21)$$

$$\mu_{avgRGB} = \frac{1}{3} (\mu_R + \mu_G + \mu_B), \quad (2.22)$$

$$\Delta_{avgRGB} = \max(|\mu_R - \mu_{avgRGB}|, |\mu_G - \mu_{avgRGB}|, |\mu_B - \mu_{avgRGB}|), \quad (2.23)$$

де Y_{max}, Y_{min} – максимальне та мінімальне значення яскравості пікселів; N – кількість пікселів у зображенні; $N_{Y>220}$ – кількість пікселів у зображенні з яскравістю більшою ніж 220; $N_{Y<30}$ – кількість пікселів у зображенні з яскравістю меншою ніж 30; L_{avg} – середнє значення.

У загальному випадку для оцінювання обчислювальної ресурсоемності кожної із операцій, що реалізуються для виконання означених завдань нейромережових засобів БА персоналу ОКІ, використовують обчислювальну складність та обсяг пам'яті, необхідний для їх виконання. На практиці провести попередній розрахунок вказаних показників достатньо складно через необхідність враховувати великий обсяг різноманітних чинників. Разом з тим, специфіка НМЗ БА вказує на те, що в першому наближенні в якості критерію оцінювання обчислювальної ресурсоемності кожної з цих операцій можливо використовувати кількість вагових коефіцієнтів відповідної НММ (N_W). При цьому для попереднього оцінювання обчислювальної складності та необхідного обсягу пам'яті НМЗ доцільно використовувати результати [16, 19, 29, 82], які дозволяють виконувати відповідні розрахунки з урахуванням типу НММ та особливостей використаного апаратно-програмного забезпечення. Загальну обчислювальну ресурсоемність процедури розпізнавання особи можливо оцінити на основі суми обчислювальної ресурсоемності всіх операцій, що входять до її складу, з урахуванням додаткових витрат, пов'язаних з їх

поєднанням. Очевидно, що діапазони допустимих та прийнятних значень критеріїв точності та обчислювальної ресурсоемності процедури розпізнавання особи та спуфінг-атак можуть бути визначені на основі нормативних вимог. Разом з тим, діапазони допустимих значень критеріїв, що асоціюються з реалізацією проміжних операцій процедури розпізнавання, в першому наближенні можливо визначити з урахуванням загальноприйнятих вимог, базуючись на відповідних показниках процедури розпізнавання в цілому. Також зазначимо, що, з позицій зручності інтерпретації отриманих результатів, вихідний сигнал НМЗ можливо представити у ймовірнісному вигляді, а у вимогах до НМЗ слід передбачити порогові значення вихідних сигналів, що забезпечать можливість остаточного визначення величин елементів Y_I, Y_E, Y_A .

Таким чином, в результаті проведених досліджень розроблено модель процедури розпізнавання особи за ЗО та РОО при БА персоналу ОКІ із застосуванням НМЗ, що, відповідно до результатів [16, 96, 144], забезпечує базис розробки НММ та нейромережових методів, призначених для розпізнавання особи та спуфінг-атак на основі відеопотоку, зареєстрованого в умовах ОКІ. Варто відзначити, що, використовуючи запропоновану модель розпізнавання особи за ЗО та РОО при БА персоналу ОКІ, при розробці відповідних НМЗ необхідно враховувати рівень розвитку технологій нейромережевого аналізу відеопотоку, критерії оцінки ефективності засобів БА [149], а також матеріальні ресурси, що виділяються на розробку та впровадження таких засобів.

Також аналіз розробленої моделі та результати [85, 147, 155] вказують на можливість підвищення точності розпізнавання особи представника персоналу ОКІ за рахунок застосування сучасних НМЗ семантичної сегментації зображень при виділенні контурів ЗО, РОО та контурів завад, що зумовлює необхідність розробки відповідної моделі семантичної сегментації. Крім того, реалізація окремих операцій процедури розпізнавання накладає такі обмеження, які складно забезпечити в монолітній НММ, що можливо компенсувати за рахунок підходу, який передбачає побудову модульної НММ, в котрій функціонал модулів співвідноситься із специфікою відповідних операцій.

2.2. Модульна нейромережева модель біометричної автентифікації персоналу об'єктів критичної інфраструктури за зображенням обличчя та райдужною оболонкою ока

Відправною точкою розробки модульної НММ послужив постулат про те, що функціонал кожного з модулів необхідно співвіднести з виконанням окремих завдань, визначених в п. 2.1, при побудові моделі процедури розпізнавання особи за ЗО та РОО. Використовуючи результати [102, 114, 155], встановлено, що традиційні підходи до вирішення 1-9 вказаних завдань передбачають застосування класифікаційних ЗНМ. Для вирішення 10 завдання, крім класифікаційних, використовуються ЗНМ, адаптовані до задачі порівняння вхідних зображень. Класифікаційні ЗНМ використовуються у випадку, коли не є критичним термін навчання, пов'язаний із внесенням в НММ даних нового представника персоналу, або із видаленням таких даних. ЗНМ, що призначені для порівняння зображень, використовуються, якщо цей термін є критично важливим. Тому завдання 10 розділене на два завдання. Завдання 10.1 полягає у розпізнаванні особи на основі нейромережевого порівняння підконтрольного ЗО із ЗО легітимних представників персоналу ОКІ, а завдання 10.2 – у розпізнаванні особи на основі нейромережевої класифікації підконтрольного ЗО. Послідовність виконання вказаних завдань, з урахуванням особливостей вирішення 10 завдання, проілюстровано за допомогою рис. 2.2. Передбачається виконання кожного завдання за допомогою окремого нейромережевого модулю. Базуючись на відомих методах побудови НМЗ захисту інформації [100, 114, 163], у кожному із модулів передбачено використання такої архітектури НММ, яка є найбільш ефективною при вирішенні відповідного завдання. При цьому ефективність архітектури розраховується так:

$$E_i = \sum_{v=1}^V \alpha_v e_{d,v}, \quad (2.24)$$

де E_i – ефективність i -ої архітектури; V – кількість критеріїв ефективності; α_v – ваговий коефіцієнт v -го критерію ефективності; $e_{d,v}$ – значення v -го критерію ефективності для i -ої архітектури.

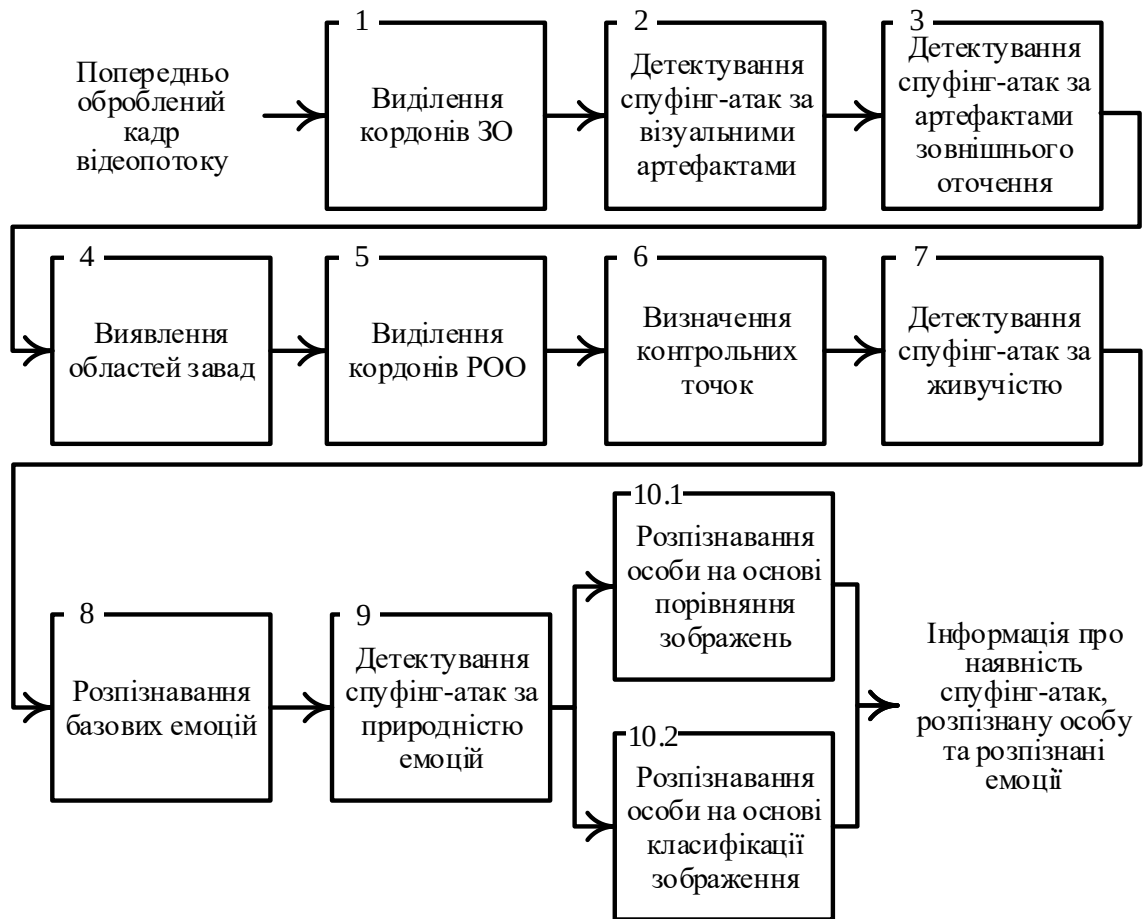


Рис. 2.2. Послідовність виконання завдань модульною нейромережевою моделлю

Використовуючи результати [50, 95, 145], в базовому варіанті до критеріїв ефективності віднесено точність розпізнавання (e_1), обчислювальну складність розпізнавання (e_2), пристосованість до розпізнавання в реальному масштабі часу (e_3), апробованість при вирішенні завдань, аналогічних до завдання модулю (e_4), доступність інструментального забезпечення (e_5). Крім того, до переліку критеріїв ефективності включено критерії, що співвідносяться із наявністю доступної попередньо навченої НММ (e_6) та із можливістю пройти донавчання задля досягнення заданих показників в умовах поставленого завдання (e_7). Використання критеріїв e_6 та e_7 пояснюється складністю формування репрезентативних навчальних вибірок, високою обчислювальною ресурсоемністю процесу навчання, можливою необхідністю адаптації НММ до особливостей поставленого завдання та наявністю доступних апробованих

переднавчених НММ, що забезпечують ефективне вирішення широкого спектру задач в області комп'ютерного зору. Враховуючи складність експертного оцінювання значень вказаних критеріїв, для їх оцінювання використана бінарна шкала. Значення критерію дорівнює 1, якщо відповідна вимога забезпечена, та дорівнює 0 у протилежному випадку. При цьому e_1 встановлювалось рівним 1 у випадку, якщо заявлена точність розпізнавання НММ була більшою ніж 0,95. При розрахунках виразу (2.24) прийняті наступні значення вагових коефіцієнтів: $\alpha_1 = 0,2$; $\alpha_2 = 0,1$; $\alpha_3 = 0,14$; $\alpha_4 = 0,14$; $\alpha_5 = 0,14$; $\alpha_6 = 0,14$; $\alpha_7 = 0,14$. Збільшення вагомості критерію α_1 пояснюється підвищеними вимогами до точності розпізнавання особи на ОКІ, а зменшення вагомості критерію α_2 – доступністю потужного апаратного забезпечення, що може частково компенсувати високу обчислювальну складність розпізнавання загальновідомих НММ. Використавши наведений підхід для кожного із модулів моделі БА, із застосуванням виразу (2.24), визначено множину ефективних архітектур НММ, що дозволило сформулювати табл. 2.1, в якій наведено відповідність нейромережових архітектур до завдань окремих модулів модульної НММ БА персоналу ОКІ. Перелік розглянутих архітектур НММ, відповідних кожному із модулів модульної НММ, визначено на основі даних науково-практичних робіт [50, 59, 68, 76, 81, 82, 145]. Зазначимо, що для наведених в табл. 2.1 архітектур значення функції ефективності знаходиться в межах від 0,95 до 1. Наявність в табл. 2.1 на перетині рядка з назвою архітектури та колонки з номером завдання позначки «+» означає, що у вільному доступі є відповідне апробоване, доступне для модифікації програмне забезпечення, задекларовані можливості якого забезпечують вирішення вказаного завдання. Позначка «+/-» стосується мережі DeerPiXBiS та свідчить про обмежені можливості даної мережі при детектуванні спуфінг-атак за артефактами зовнішнього оточення, які стосуються об'єктів, що мають бути зафіксовані при відеореєстрації обличчя. Також ця позначка стосується мережі Face Mesh та свідчить про те, що хоча дана мережа, строго кажучи, не виділяє контури ЗО та РОО, однак визначає контрольні точки та створює сітку, яка приблизно визначає вказані контури.

Таблиця 2.1

Відповідність нейромережових архітектур до завдань модулів
модульної нейромережевої моделі

Архітектура	Номер завдання										
	1	2	3	4	5	6	7	8	9	10.1	10.2
MTCNN	+					5					
RetinaFace	+					5					
BlazeFace	+					5					
YOLOv8n	+										
U-Net	!			!	!						
IrisParseNet					+						
DeepPixBiS		+	+/-								
ModifiedConvNeXtLarge							+				
FaceNet										+	
Face MeshV2	+/-				+/-	478					
FaceEmotion_ID						68		+			
Face Alignment Network						68					
MobileFaceNet										+	
MobileNet											+
PNN									!		
Siamese Network			!							!	
Two_channel Networks			!							!	

Позначка «!» означає, що відповідне програмне забезпечення у вільному доступі відсутнє, але наявність відкритого програмного коду, доведена ефективність в дотичних областях та доступність репрезентативних наборів даних забезпечують можливість реалізації відповідної розробки. Цифри в колонці з номером завдання 6 вказують кількість контрольних точок, що визначаються на обличчі при використанні відповідної НММ. В процесі розрахунків визначено, що при вирішенні завдань 1, 3, 5, 6, 10.1, 10.2 можливо

застосовувати декілька альтернативних варіантів НММ. Наприклад, для вирішення завдання 1 (виділення кордонів ЗО) можливо застосовувати MTCNN, RetinaFace, BlazeFace або YOLOv8n, інструментальне забезпечення яких є у вільному доступі. Разом з тим, для вирішення цього завдання можливо застосовувати U-Net, що забезпечує можливість підвищення точності виділення кордонів ЗО за рахунок виділення природніх контурів ЗО, а не визначення прямокутної області (bounding box), яка містить ЗО, що характерно для MTCNN, RetinaFace, BlazeFace та YOLOv8n. Це ж стосується і завдання 10.1 (розпізнавання особи на основі порівняння зображень), що є особливо актуальним у випадку необхідності оперативного оновлення переліку легітимних представників персоналу ОКІ.

В процесі дослідження визначено, що при вирішенні завдання 10.1, у випадку розпізнавання особи на основі порівняння ЗО, застосування мережі FaceNet забезпечує досягнення показника точності Accuracy на рівні 0,9963, а застосування мережі MobileFaceNet (із функцією втрат ArcFace) – досягнення показника точності Accuracy на рівні 0,9955. Зазначимо, що в базовому випадку величина Accuracy відповідає оцінці подібності (r_{FC}) ЗО особи, що підлягає розпізнаванню, та ЗО легітимних представників. Тобто при застосуванні FaceNet $r_{FC} = 0,9963$, а при застосуванні MobileFaceNet $r_{FC} = 0,9955$. При цьому кількість вагових коефіцієнтів FaceNet дорівнює приблизно 10^7 , а кількість вагових коефіцієнтів MobileFaceNet – приблизно 10^6 . Також слід зазначити, що вихідні сигнали НММ FaceNet та MobileFaceNet представляють собою вектори ознак (ембединги) ЗО, які використовуються для подальшого порівняння з відповідними еталонними векторами ознак легітимних представників персоналу ОКІ. Хоча використання FaceNet та MobileFaceNet забезпечується доступним інструментальним забезпеченням, однак внесення в таку НММ даних щодо розпізнавання особи на основі порівняння РОО зумовлює необхідність реалізації достатньо складної та нестабільної процедури налаштувань. Тому при вирішенні завдання 10.1 у випадку розпізнавання особи на основі порівняння РОО доцільно використовувати НМЗ на основі Siamese Network та Two_channel Network, які

мають приблизно однакові значення функції ефективності [51, 123]. Виходячи з тих же позицій, визначено доцільність застосування НММ Siamese Network та Two_channel Network для вирішення завдання 3, що стосується детектування спуфінг-атак за артефактами зовнішнього оточення. При цьому, на відміну від більшості відомих ЗНМ, в Siamese Network відмінність між двома вхідними зображеннями розраховується на основі манхетенської відстані між вихідними сигналами кожної із двох ЗНМ, що входять до її складу:

$$L_1 = \sum_{i=1}^{N_Y} |y_{1,i} - y_{2,i}|, \quad (2.25)$$

де $y_{1,i}$, $y_{2,i}$ – i -ий вихідний сигнал першої та другої ЗНМ; N_Y – кількість вихідних нейронів в ЗНМ.

Особливістю математичного забезпечення Two_channel Network, що стосується визначення відмінностей між двома вхідними зображеннями, є використання в якості функції втрат Hinge Loss, що розраховується за допомогою виразу виду:

$$H_Loss = \max(0; 1 - y_e \times y_r), \quad (2.26)$$

де y_e – очікуваний вихідний сигнал; y_r – реальний вихідний сигнал.

У випадку, коли в процесі навчання на вхід мережі Two_channel Network подаються зображення, що класифікуються як однакові, $y_e = 1$, а у протилежному випадку $y_e = -1$. Також зазначимо, що, в залежності від розмірів вхідного зображення, в базову структуру мережі Two_channel Network слід вносити зміни, що забезпечують зведення розмірів вхідного зображення до 1 пікселя.

Використовуючи дані табл. 2.1, проведено дослідження, спрямовані на уточнення перспектив застосування представлених в ній НММ для вирішення завдань, що реалізуються відповідними модулями в різних умовах експлуатації на ОКІ. Для цього проведено дві серії експериментів. В першій серії проведено уточнення заявлених можливостей НММ, позначених символом «+» в табл. 2.1. Увагу акцентовано на дослідженні впливу оклюзій на вирішення 1, 5, 6 завдань, тобто виділення кордонів ЗО та РОО та визначення координат контрольних

точок. Хід проведення першої серії експериментів проілюстровано за допомогою рис. 2.3-2.6, на яких показано результати застосування мережі Face Mesh для нанесення ключових точок на 3О, виділеного на фотокартці за допомогою мережі RetinaFace. Так, на рис. 2.3 показано результати нанесення ключових точок на обличчя жінки, зареєстроване без впливу завад та у випадку наявності на її обличчі прозорих окулярів. На рис. 2.4 показано результати нанесення ключових точок на анімоване обличчя, зареєстроване без впливу завад та у випадках наявності на обличчі медичної маски, темних окулярів та комбінації цих завад.



Рис. 2.3. Нанесення ключових точок на обличчя жінки

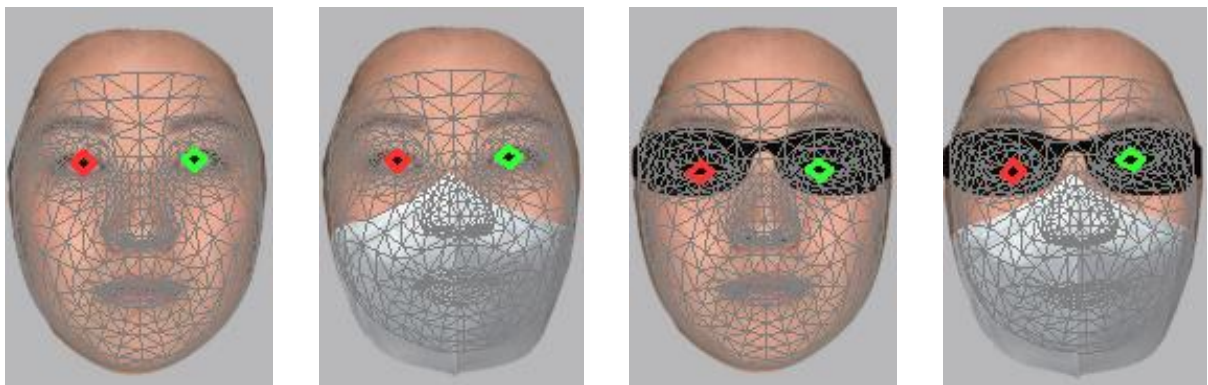


Рис. 2.4. Нанесення ключових точок на анімоване обличчя

На рис. 2.5 показано результати нанесення ключових точок на обличчя чоловіка європеоїдної раси, зареєстроване без впливу завад та у випадку наявності на обличчі медичної маски. На рис. 2.6 показано результати нанесення ключових точок на обличчя чоловіка монголоїдної раси, зареєстроване без

впливу завад, у випадку наявності на обличчі медичної маски та у випадку наявності темних окулярів.

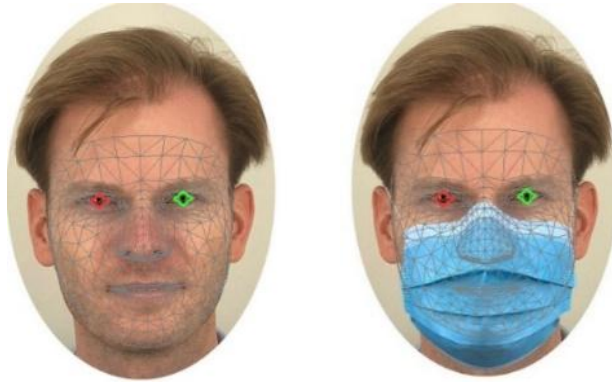


Рис. 2.5. Нанесення ключових точок на обличчя чоловіка європеїдної раси

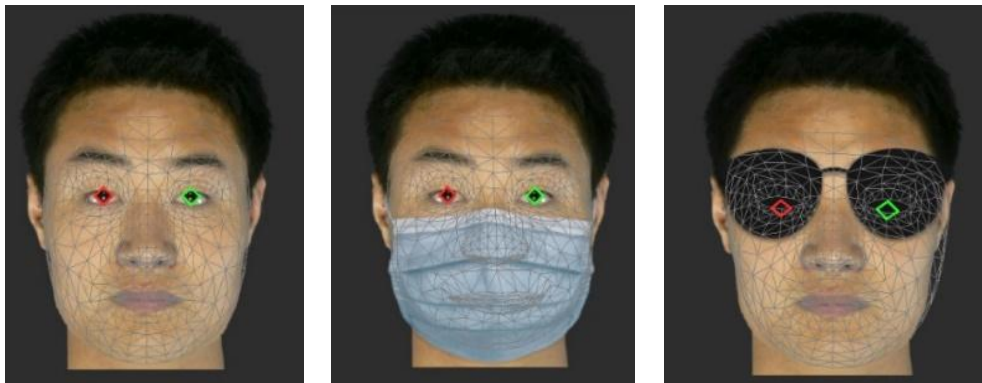


Рис. 2.6. Нанесення ключових точок на обличчя чоловіка монголоїдної раси

Результати першої серії експериментів показали можливість ефективного застосування мереж MTCNN, RetinaFace, BlazeFace та YOLOv8n для виділення у кадрах відеопотоку прямокутної області, що відповідає обличчю, незалежно від її статі та раси, як у випадку відсутності завад при відеореєстрації, так і у випадках наявності типових завад, що перекривають біля 60% площі обличчя. При цьому мережі MTCNN, RetinaFace, BlazeFace та YOLOv8n забезпечують приблизно однаковий рівень точності виділення ЗО, дозволяють детектувати декілька ЗО в одному кадрі, а їх швидкодія та ресурсоемність дозволяє розгортання відповідного НМЗ на поширеному апаратно-програмному

забезпеченні. Разом з тим, при виборі мережі, крім наявності доступного інструментального забезпечення, слід враховувати розмір вхідного поля, що в базовому випадку для MTCNN становить 320x240 або 640x480 пікселів, для RetinaFace – 640x640 або 800x800 пікселів, для BlazeFace – 128x128 або 256x256 пікселів, а для YOLOv8n – 640x640 пікселів. Крім того, слід враховувати необхідність нанесення п'яти контрольних точок на ЗО. Також визначено, що використання мереж Face Mesh, Face Alignment Network та FaceEmotion_ID для виділення ключових точок можливо лише при відсутності завад на обличчі.

В протилежному випадку на обличчя наносяться точки, які перекриваються завадами, а тому не можуть бути використані для розпізнавання особи та емоцій. Мережа IrisParseNet дозволяє виділити природні контури РОО, однак для її застосування необхідно подати на вхід мережі не все ЗО, а лише невелику частину, яка містить зображення ока, що зумовлює необхідність попередньої обробки ЗО.

Мережі DeepPixBiS та ModifiedConvNeXtLarge забезпечують задовільне розпізнавання спуфінг-атак за візуальними артефактами типу зміна текстури та кольору зображення, неприродні відблиски та тіні, неприродні варіації відстаней між різними частинами обличчя, за артефактами зовнішнього оточення, які пов'язані з кордонами маски та відблисками екрану, на якому демонструється обличчя, та за живучістю, що оцінюється за наявністю рухів обличчя та мімікою. Разом з тим, мережі DeepPixBiS та ModifiedConvNeXtLarge не забезпечують можливості розпізнавання спуфінг-атак на основі зображень об'єктів, що мають бути зареєстровані одночасно з ЗО в процесі БА. Це пов'язано зі складністю оперативного донавчання мережі. Також в результаті першої серії експериментів визначено, що характеристики мереж MobileFaceNet, FaceNet та MobileNet відповідають заявленим можливостям, однак їх функціональність значно погіршується у випадку наявності завад та зміни очікуваних умов відеореєстрації. В цілому результати першої серії експериментів свідчать про те, що для вирішення кожного із основних завдань НМЗ БА персоналу ОКІ можливо

використовувати декілька із наведених в табл. 2.1 типів НММ, ефективність яких залежить від конкретних умов застосування.

В другій серії експериментів перевірено доцільність застосування семантичної сегментації ЗО за допомогою НМЗ на базі архітектури U-Net (в табл. 2.1 позначена символом «!»). Доцільність застосування мережі U-Net при вирішенні завдання 1 (виділення кордонів ЗО) пояснюється можливістю точного виділення природніх контурів ЗО, а не обрамлення ЗО за допомогою прямокутної рамки, характерної для мереж MTCNN, RetinaFace, BlazeFace або YOLOv8n. Крім того, застосування засобів семантичної сегментації ЗО дозволяє одночасно з вирішенням завдання 1 вирішувати завдання 4 та 5, тобто реалізувати виявлення областей завад та виділення кордонів РОО. Для перевірки вказаного твердження використана мережа U-Net, що була навчена на наборі даних Human Face Segmentation, який є у вільному доступі за посиланням <https://www.kaggle.com/datasets/dnayan/human-face-segmentation/data>.

Вказаний набір даних містить 70846 сегментованих та несегментованих ЗО чоловіків та жінок різного віку азіатської, африканської та європеїдної етнічних груп. Зображення мають розміри не менші ніж 128 на 128 пікселів та представлені у файлах формату jpg та png. Особливістю представлених ЗО є те, що відстань між зіницями очей становить не менше ніж 60 пікселів. В наборі даних містяться ЗО, що відображають різноманітні емоції, зафіксовані під різними кутами нахилу, з відкритими та заплющеними очима, відкритим та закритим ротом.

Процес навчання U-Net проілюстровано за допомогою рис. 2.7, де представлено графік залежності показника Ассигасу від кількості епох навчання, розрахований на валідаційних даних. Відзначимо, що, враховуючи особливості поставленого завдання виділення контурів ЗО, показник Ассигасу співвіднесено з Jaccard Index (IoU). Як показано на графіку, вже після 23 епохи навчання на валідаційних даних значення показнику Ассигасу стабілізується на рівні 0,96, що свідчить про відповідність U-Net поставленому завданню.

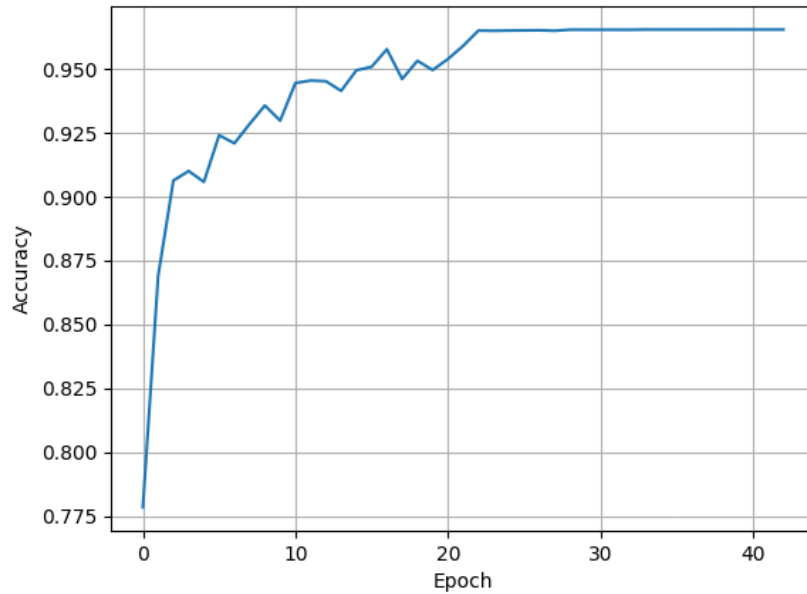


Рис. 2.7. Зміна показника Ассурасу в залежності від кількості епох навчання для U-Net

Результати застосування мережі U-Net для виділення природніх контурів ЗО чоловіка та жінки показано на рис. 2.8.

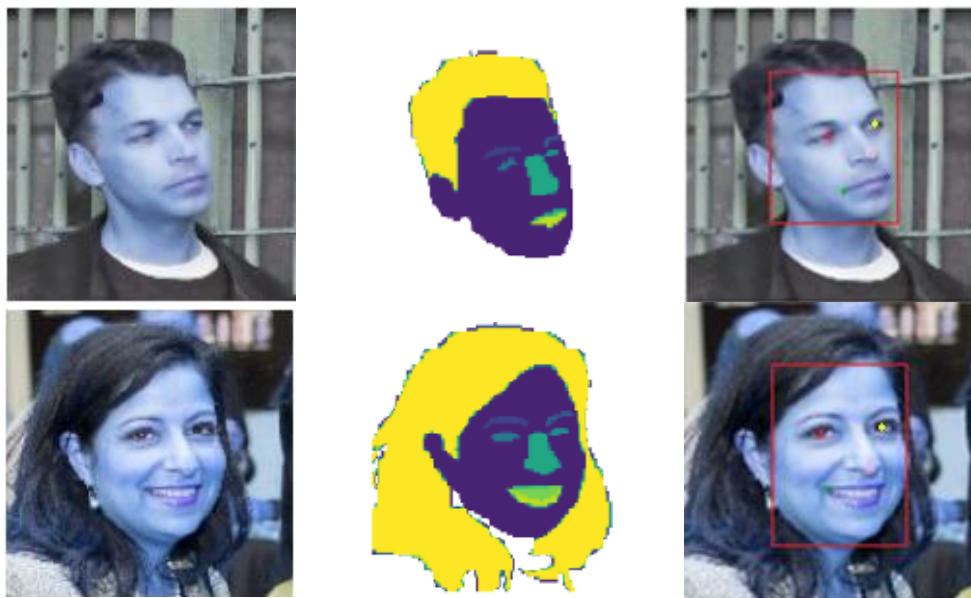


Рис. 2.8. Виділення кордонів зображення обличчя у вигляді контуру та у вигляді прямокутної рамки.

Для порівняння на рис. 2.8 показано ЗО чоловіка та жінки, виділені прямокутною рамкою, що характерно при застосуванні мереж MTCNN,

RetinaFace та BlazeFace, які традиційно використовуються в системах БА. Такий тип виділення кордонів ЗО призводить до того, що на зображенні, що подається для подальшого аналізу, можуть бути присутні сторонні об'єкти, які негативно впливають на точність розпізнавання особи представника персоналу ОКІ. При цьому деякі частини ЗО можуть бути обрізані, що також може призвести до зниження точності розпізнавання. Тому використання U-Net, що забезпечує виділення природніх контурів ЗО, дозволяє запобігти виникненню вказаного недоліку.

Крім того, мережа U-Net дозволяє виділити окремі частини ЗО, що може бути використано як для підвищення точності розпізнавання особи представника персоналу ОКІ, так і для підвищення точності розпізнавання спуфінг-атак. За попередніми розрахунками використання U-Net дозволить за показником Jaccard Index підвищити точність виділення обличчя на 10-12%, що зрештою підвищує точність розпізнавання особи представника персоналу ОКІ. Разом з тим, розробка НМЗ на базі U-Net, здатних вирішувати завдання детекції ЗО у відеопотоці в режимі реального часу, потребують проведення подальших досліджень. Тому можливо вважати доцільним поділ показаного на рис. 2.2 завдання 1 (виділення кордонів ЗО) на два завдання, для вирішення яких передбачено використання НМЗ, побудованих на базі різних типів НММ.

Перше завдання полягає у детекції ЗО в відеокадрі та виконується за допомогою НММ типу MTCNN, RetinaFace, BlazeFace, YOLOv8n, а друге завдання полягає у семантичній сегментації ЗО та виконується за допомогою НММ з енкодер-декодерною архітектурою типу U-Net.

Основний науковий результат проведених в п. 2.2 досліджень полягає у побудові базису розробки НМЗ БА персоналу ОКІ, що здатні адаптуватись до різних умов застосування. Розроблена модульна НММ передбачає використання спеціалізованих модулів, кожен із яких призначений до виконання завдання, яке доцільно виконувати з допомогою окремої монолітної НММ. Також передбачено можливість адаптації типу такої монолітної НММ до особливостей виконуваного завдання. При цьому показано, що одним з основних критеріїв вибору типу

монолітної НММ є наявність відповідного апробованого та доступного інструментального забезпечення, що насамперед передбачає наявність вже навченої мережі, здатної функціонувати в очікуваних умовах експлуатації. Обґрунтовано таблицю відповідності апробованих нейромережових архітектур завданням окремих модулів у модульній НММ.

Показано, що ефективне вирішення ключових завдань, пов'язаних з виділенням ЗО в кадрах відеопотоку, виділенням контрольних точок на ЗО в умовах перешкод, а також з розпізнаванням особи користувача з урахуванням необхідності оперативного оновлення списку легітимних представників персоналу ОКІ, складно забезпечити шляхом використання доступного інструментального забезпечення, що обґрунтовує необхідність розроблення відповідних НММ. Також обґрунтовано, що для вирішення завдання розпізнавання особи користувача, крім апробованих НММ FaceNet та MobileFaceNet, доцільно використовувати Siamese Network та Two_channel Network, які дозволяють реалізувати розпізнавання на основі нейромережового порівняння ЗО та РОО особи, яка підлягає автентифікації з ЗО та РОО легітимних співробітників.

Шляхи подальших досліджень пропонується співвіднести з підвищенням ефективності Siamese Network за рахунок використання в блоці ЗНМ архітектури типу MobileNet замість традиційно використаної архітектури типу LeNet. Крім цього, обґрунтовано доцільність застосування в модулі виділення ЗО НММ типу U-Net, що дозволяє виділити природні контури ЗО, а не виділяти ЗО за допомогою прямокутної рамки, характерної для відомих рішень на основі MTCNN, RetinaFace та BlazeFace.

Таким чином, остаточний склад запропонованої модульної НММ має бути сформований з урахуванням особливостей поставленої задачі БА персоналу ОКІ, що визначає необхідність проведення подальших досліджень в напрямку створення відповідних процедур адаптації параметрів модульної НММ до очікуваних умов застосування для БА персоналу ОКІ.

В цілому розробка модульної НММ забезпечила теоретичний базис для

побудови неймережевого методу БА за ЗО та РОО в інформаційних системах ОКІ. Також слід зазначити, що передбачена для використання в модульній моделі НММ типу U-Net відноситься до НММ з архітектурою типу енкодер-декодер, які в основному застосовуються для семантичної сегментації зображень. Відповідно до результатів [121, 150, 152], ефективність такої НММ значною мірою залежить від пристосованості її архітектури до умов поставленої задачі семантичної сегментації ЗО, що зумовлює необхідність створення відповідної моделі семантичної сегментації ЗО, а на її основі розробки методу побудови НМЗ семантичної сегментації ЗО при БА.

2.3. Модель семантичної сегментації зображення обличчя

Відповідно до результатів [2, 26, 43, 47, 67], у системах БА семантичну сегментацію ЗО доцільно виконувати з урахуванням інформативності окремих його зон. У найпростішому випадку виокремлюються лише дві області – фон та обличчя в межах своїх природних контурів, без деталізації внутрішніх компонентів. У більш складних випадках сегментації також підлягають очі, брови, ніс, рот і волосся, оскільки їх виділення сприяє підвищенню точності позиціонування обличчя та РОО під час подальшої обробки. Волосся, що асоціюється із зачіскою, також може бути виділене у випадках, коли його контури використовуються для нормалізації положення голови. Елементи, які перекривають або спотворюють обличчя (окуляри, маски, прикраси тощо), доцільно відносити до фону та не включати до маски сегментації.

Таким чином, залежно від застосованих правил виділення зон, кількість класів сегментації в моделі може змінюватися – від двох (обличчя/фон) до кількох, що деталізують структуру обличчя.

Варто зазначити, що в подальшому отримані маски синхронізуються з початковими зображеннями, на основі чого формується оброблене зображення, що надалі використовується для виявлення спуфінг-атак і розпізнавання особи. Використавши в якості прототипу напрацювання в області застосування нейронних мереж для сегментації зображень [96, 99, 147, 160], визначено, що в

базовому випадку модель семантичної сегментації 3О при БА на ОКІ (M_{SS}) можливо описати за допомогою виразів виду:

$$\hat{\mathbf{P}} = f(\mathbf{X}) \quad \hat{\mathbf{P}} \in \mathbb{R}^{H \times W \times K}, \mathbf{X} \in \mathbb{R}^{H \times W \times C}, \quad (2.27)$$

$$\mathbf{X}_{i,j} = [x_{i,j,1}, x_{i,j,2}, \dots, x_{i,j,C}], \quad (2.28)$$

$$\hat{\mathbf{P}}_{i,j} = [p_{i,j,1}, p_{i,j,2}, \dots, p_{i,j,K}], \quad (2.29)$$

де $\mathbf{X}$ – вхідне 3О, що підлягає сегментації; $\hat{\mathbf{P}}$ – карта ймовірностей піксель-класів; f – функція сегментації ($f: \mathbb{R}^{H \times W \times C} \rightarrow \mathbb{R}^{H \times W \times K}$); $\mathbb{R}$ – множина дійсних чисел; H, W – висота та ширина зображення; C – кількість кольорових каналів в зображенні; K – кількість класів сегментації; $x_{i,j,c}$ – яскравість c -го кольорового каналу пікселя з координатами (i, j) ; $p_{i,j,k}$ – ймовірність того, що піксель з координатами (i, j) належить до k -го класу.

Зазначимо, що в поширених форматах представлення зображень значення яскравості кожного із кольорових каналів зберігаються у вигляді цілих чисел. Наприклад, при використанні формату RGB достатньо часто для збереження яскравості кожного із пікселів передбачається використовувати 8-бітне число. Це означає, що $\mathbf{X} \in \mathbb{Z}^{H \times W \times C}$, де $\mathbb{Z}$ – множина цілих чисел, а яскравість кожного із кольорових каналів довільного пікселю є цілим числом від 0 до 255. Однак де-факто стандартна процедура підготовки зображення перед подачею на вхід НММ передбачає масштабування яскравості кожного із кольорових каналів до діапазону $[0,1]$, за рахунок ділення початкового значення яскравості кожного із пікселів на число, що відповідає максимально можливому значенню яскравості, наприклад, на 255 для 8-бітних зображень. Тому у виразі (2.27) $\mathbf{X} \in \mathbb{R}^{H \times W \times C}$.

Враховуючи, що, відповідно до результатів [20, 36, 139], при семантичній сегментації доцільно використовувати НММ, архітектура якої передбачає використання енкодера та декодера, вираз (2.27) можливо модифікувати так:

$$\hat{\mathbf{P}} = f_D(f_E(\mathbf{X})), \quad (2.30)$$

де $f_E(\cdot)$ та $f_D(\cdot)$ – функції, що описують результат застосування нейромережевого енкодера та нейромережевого декодера.

Використавши результати [79, 92], визначено, що в базовому випадку функціонал нейромережевого енкодера та нейромережевого декодера можливо описати за допомогою виразів виду (2.31) та (2.32). Зазначимо, що, відповідно до результатів [93, 147], в якості базису енкодера та декодера доцільно використовувати такі типи НММ, як VGG, ResNet, MobileNet, EfficientNet, HRNet. При цьому вважається, що найбільш апробовані типи енкодера та декодера базуються на VGG-моделях та використовуються в U-Net-подібних НММ семантичної сегментації з можливими пропусками шарів субдискретизації та варіативною кількістю шарів згортки.

$$\mathbf{Z} = f_E(\mathbf{X}), \mathbf{Z} \in \mathbb{R}^{H' \times W' \times D}, \quad (2.31)$$

$$\hat{\mathbf{P}} = f_D(\mathbf{Z}), \hat{\mathbf{P}} \in \mathbb{R}^{H \times W \times K}, \quad (2.32)$$

де $\mathbf{Z}$ – тензор ознак закодованого зображення; $H' \times W'$ – розмір карт згортки/субдискретизації на виході з енкодера; D – кількість карт згортки/субдискретизації на виході з енкодера (глибина ознакового простору).

Деталізований опис процедури функціонування енкодера (2.31) можливо здійснити, використовуючи вирази (2.33, 2.34), а для деталізації функціонування декодера (2.32) – вирази (2.35, 2.36).

$$\mathbf{X}_l^{c_l} = \sigma_l(W_l^{c_l} * \mathbf{X}_{l-1}^{c_{l-1}} + b_l), l = 0, 1, \dots, L_{LCE}, \quad (2.33)$$

$$\mathbf{X}_l^{s_l} = Pool(\mathbf{X}_l^{c_l}), \quad (2.34)$$

де $\mathbf{X}_l^{c_l}$ – двовимірна матриця ознак на виході із c -ої карти згортки в l -му згортковому шарі ($\mathbf{X}_0^{c_0} = \mathbf{X}$); L_{LCE} – кількість шарів згортки в енкодері; $\mathbf{X}_l^{s_l}$ – двовимірна матриця ознак на виході із s -ої карти субдискретизації; $W_l^{c_l}, b_l$ – вагові коефіцієнти, що відповідають c -ій карті згортки в l -му згортковому шарі; $Pool(\cdot)$ – операція субдискретизації; σ_l – функція активації в l -му згортковому шарі енкодера.

$$\mathbf{Z}_{n-1}^{c_{n-1}} = \sigma(W_n^{c_n} * Dec(\mathbf{Z}_n^{c_n}) + b_n), n = 0, 1, \dots, N_{LCD}, \quad (2.35)$$

$$\mathbf{Z}_{n-1}^{c_{n-1}} = \sigma(W_n^{c_n} * Dec(\mathbf{Z}_n^{c_n}) \parallel \mathbf{X}_{l-1}^{c_{l-1}} + b_n), \quad (2.36)$$

де $\mathbf{Z}_n^{c_n}$ – двовимірна матриця ознак, що відповідає c -ій карті згортки в n -му згортковому шарі декодера ($\mathbf{Z}_0^{c_0} = \mathbf{X}_{N_{LCD}}^{c_L}$); N_{LCD} – кількість шарів згортки в

декодері; $\parallel$ – конкатенація (skip-connection) вагових коефіцієнтів з відповідного рівня енкодера; $Dec(\cdot)$ – функція, що описує реалізацію процедури апсемплінгу в нейромережевому декодері.

При цьому, відповідно до [47, 79, 147], термін апсемплінг описує процедуру, що реалізується за рахунок збільшення просторової роздільності тензора ознак, яка виконується в декодері НМ з метою покрокового відновлення вихідного розміру зображення після даунсемплінгу, тобто стиснення внаслідок проходження вхідного зображення через енкодер.

Процедуру апсемплінгу можливо описати за допомогою виразу:

$$Z_{up}(h, w, d) = \sum_{i=0}^{k_h-1} \sum_{j=0}^{k_w-1} Z\left(\text{trunc}\left(\frac{h}{d}\right) - i, \text{trunc}\left(\frac{w}{d}\right) - j\right) \cdot Kr(i, j), \quad (2.37)$$

де Z_{up} – результат апсемплінгу; h, w – висота та ширина вхідного тензора ознак Z ; k_h, k_w – висота і ширина ядра апсемплінгу Kr ; d – масштабний коефіцієнт апсемплінгу; $\text{trunc}(\cdot)$ – функція визначення найближчого найменшого цілого; $Kr(i, j)$ – значення ядра апсемплінгу в позиції (i, j) .

Значення $Kr(i, j)$ залежать від використаного методу інтерполяції і визначаються за допомогою виразів виду:

$$Kr(i, j) = \delta(i) \cdot \delta(j), \quad (2.38)$$

$$Kr(i, j) = \max(0, 1 - |i|) \cdot \max(0, 1 - |j|), \quad (2.39)$$

$$Kr(i, j) = R(i) \cdot R(j), \quad (2.40)$$

$$R(x) = \begin{cases} (a + 2) |x|^3 - (a + 3) |x|^2 + 1, & 0 \leq |x| < 1 \\ a |x|^3 - 5a |x|^2 + 8a |x| - 4a, & 1 \leq |x| < 2 \\ 0, & |x| \geq 2 \end{cases} \quad (2.41)$$

$$Kr(i, j) = F_l(NM), \quad (2.42)$$

де δ – дельта-функція Кронекера; a – фіксований параметр ($a = -0,5$); $F_l(NM)$ – функція, що співвідноситься з визначенням $Kr(i, j)$ в результаті навчання НММ.

Вираз (2.38) використовується при застосуванні методу інтерполяції типу «найближчого сусіда», вираз (2.39) – при двовимірній лінійній інтерполяції,

вирази (2.40, 2.41) – при бікубічній інтерполяції, а вираз (2.42) – при визначенні ядра апсемплінгу в результаті навчання НММ.

Інтеграція виразів (2.31-2.42), з урахуванням особливостей функціонування декодера на основі ЗНМ, дозволяє записати результуючий вираз для розрахунку карти ймовірностей піксель-класів у наступному вигляді:

$$\hat{\mathbf{P}} = \sigma(W_{out} \cdot Dec(f_E(\mathbf{X})) + b_{out}), \quad (2.43)$$

де W_{out}, b_{out} – вагові коефіцієнти останнього згорткового шару нейромережевого декодера.

У найбільш поширеному випадку застосування у нейронах вихідного шару декодера функції активації типу Softmax, ймовірність того, що піксель з координатами (i, j) належить до k -го класу, можливо розрахувати так:

$$P_{i,j,k} = e^{a_{i,j,k}} / \sum_{m=1}^K e^{a_{i,j,m}}, \quad (2.44)$$

де $a_{i,j,k}$ – вихідний сигнал декодера (логіт), що представляє ненормалізовану оцінку належності пікселя з координатами (i, j) до k -го класу.

Також зазначимо, що специфіка задачі розпізнавання особи представника персоналу ОКІ вказує на необхідність отримання результату семантичної сегментації не лише у вигляді карти ймовірностей піксель-класів, а й у вигляді сегментованого ЗО, на якому відображені його природні кордони, кордони очей та кордони завад. Враховуючи [23, 118], визначення такого сегментованого зображення може бути реалізоване за рахунок віднесення кожного з пікселів цього зображення до класу з найбільшою ймовірністю. Тобто

$$y_{i,j} = \operatorname{argmax}_k(p_{i,j,k}), k \in [1, K, 1], p_{i,j,k} \in \hat{\mathbf{P}}, \quad (2.45)$$

$$\mathbf{Y} = |y_{i,j}|_{i=1,j=1}^{H,W}, \quad (2.46)$$

де $y_{i,j}$ – клас, до якого відноситься піксель з координатами (i, j) ; $p_{i,j,k}$ – ймовірність віднесення пікселя до k -го класу; $\mathbf{Y}$ – сегментоване зображення.

Враховуючи результати [61, 79], аналіз розробленого математичного забезпечення (2.27-2.46) НММ семантичної сегментації ЗО представника персоналу ОКІ, побудованої на базі U-Net-подібної архітектури, вказує на те, що

до переліку конструктивних параметрів цієї моделі, які забезпечують можливість її адаптації до очікуваних умов застосування, відносяться: кількість шарів згортки та кількість карт згортки, розмір та крок ядра згортки в кожному із шарів для енкодера та декодера; кількість та локалізація шарів субдискретизації енкодера; кількість та локалізація шарів апсемплінгу; розмір ядра, масштабний коефіцієнт та метод інтерполяції для кожного із шарів апсемплінгу; кількість skip-зв'язків, локалізація входу в енкодері та вставки в декодер кожного із skip-зв'язків; кількість рівнів агрегації ознак skip-зв'язків; варіант агрегації skip-зв'язків.

Зазначимо, що, у випадку використання в якості базису НММ семантичної сегментації альтернативних архітектур (ResNet, MobileNet, EfficientNet, HRNet), перелік конструктивних параметрів додатково розширюється за рахунок типу енкодера, параметрів модулів багатомасштабного контексту, attention-блоків, стратегій об'єднання багаторівневих ознак і методів семантичної постобробки. Так, для енкодера та декодера, в яких передбачено використання Residual-блоків, характерних для НММ ResNet, функціонування яких описується за допомогою виразів (2.47, 2.48), до переліку конструктивних параметрів доцільно віднести: кількість стадій, кількість блоків у кожній із стадій, параметри згорток для кожного блоку та параметри проєктуючої згортки.

$$R_{l,j}(X_l) = \sigma(X_l + \mathcal{F}(X_l; W_{l,j})), \quad l \in \{1, 2, \dots, L_{RS}\}, \quad (2.47)$$

$$X_{l+1} \rightarrow W_{proj} * X_l, \quad (2.48)$$

де $R_{l,j}(\cdot)$ – j-й Residual-блок на l-ій стадії; X_l – вхідний тензор l-ої стадії; L_{RS} – кількість стадій; $\mathcal{F}(X; W_{l,j})$ – послідовність згорток/апсемплінгу у Residual-блоці; $W_{l,j}$ – параметри шарів згортки/апсемплінгу; W_{proj} – параметри згортки/апсемплінгу для приведення розмірності X_l до розмірності X_{l+1} .

Крім того, базуючись на результатах [5, 7, 57, 122], визначено доцільність відображення в переліку конструктивних параметрів не лише структурних та функціональних характеристик НММ, але й характеристик процедури навчання. При цьому до конструктивних параметрів, що співвідносяться з процедурою

навчання віднесено: тип оптимізатора (наприклад, Adam, SGD), розмір міні-пакету (batch size), швидкість навчання (learning rate), стратегія зміни швидкості навчання (learning rate scheduling), умови зупинки навчання (early stopping, кількість епох), методи регуляризації (dropout, batch normalization тощо), а також вид функції втрат.

Використавши дані [55, 57, 122], визначено, що в НММ семантичної сегментації, як правило, використовуються наступні види функції втрат: Categorical Cross-Entropy, Binary Cross-Entropy, Dice Loss, Jaccard Loss, Focal Loss, Tversky Loss. Зазначимо, що функція втрат Categorical Cross-Entropy визначається виразом (2.49), Binary Cross-Entropy – (2.50), Dice Loss – (2.51, 2.52), Jaccard Loss – (2.53, 2.54), Focal Loss – (2.55), Tversky Loss – (2.56, 2.57).

$$\mathcal{L}_{CCE} = - \sum_{i=1}^M \sum_{k=1}^K g_{i,k} \log(p_{i,k}), \quad (2.49)$$

$$\mathcal{L}_{BCE} = - \frac{1}{M} \sum_{i=1}^M \sum_{k=1}^K (g_{i,k} \cdot \log(p_{i,k}) + (1 - g_{i,k}) \cdot \log(1 - p_{i,k})), \quad (2.50)$$

$$\mathcal{L}_{Dice} = 1 - \frac{2 \cdot |TP|}{|P| + |G|}, \quad (2.51)$$

$$\mathcal{L}_{Dice} = 1 - \frac{1}{K} \sum_{k=1}^K \frac{2 \sum_{i=1}^M p_{i,k} g_{i,k} + \varepsilon}{\sum_{i=1}^M p_{i,k} + \sum_{i=1}^M g_{i,k} + \varepsilon}, \quad (2.52)$$

$$\mathcal{L}_{IoU} = 1 - \frac{|TP|}{|TP| + |FP| + |FN|}, \quad (2.53)$$

$$\mathcal{L}_{IoU} = 1 - \frac{1}{K} \sum_{k=1}^K \frac{\sum_{i=1}^M p_{i,k} g_{i,k} + \varepsilon}{\sum_{i=1}^M p_{i,k} + \sum_{i=1}^M g_{i,k} - \sum_{i=1}^M p_{i,k} g_{i,k} + \varepsilon}, \quad (2.54)$$

$$\mathcal{L}_{Focal} = - \frac{1}{M} \sum_{i=1}^M \sum_{k=1}^K \alpha^k (1 - p_{i,k})^\gamma g_{i,k} \log(p_{i,k}), \quad (2.55)$$

$$\mathcal{L}_{Tv} = 1 - \frac{TP}{TP + \alpha \cdot FP + \beta \cdot FN}, \quad (2.56)$$

$$\mathcal{L}_{Tv} = 1 - \frac{1}{K} \sum_{k=1}^K \frac{\sum_{i=1}^M p_{i,k} g_{i,k} + \varepsilon}{\sum_{i=1}^M p_{i,k} g_{i,k} + \alpha \sum_{i=1}^M p_{i,k} (1 - g_{i,k}) + \beta \sum_{i=1}^M (1 - p_{i,k}) g_{i,k} + \varepsilon}, \quad (2.57)$$

де M – кількість пікселів в зображенні; K – кількість класів; P – отримана маска сегментації; G – істинна маска сегментації; TP, FP, FN – множини пікселів, що потрапили відповідно до категорій істинно-позитивні, хибно-позитивні та хибно-негативні; $p_{i,k}$ – передбачена ймовірність належності пікселя i до класу k ; $g_{i,k}$ – істинна мітка; ε – коефіцієнт, що використовується для уникнення ділення на 0; α^k – ваговий коефіцієнт для класу k ; γ – параметр фокусування; α, β – вагові коефіцієнти для пікселів що відносяться до множин FP та FN , відповідно.

Відповідно до [57, 60], прийнято $\gamma = 2$, $\alpha = 0,3$, $\beta = 0,7$, а величина α^k встановлюється обернено пропорційною до частки пікселів класу k у наборі навчальних даних.

Взявши до уваги той факт, що в процесі побудови НМЗ семантичної сегментації використовуються специфічні показники, що відображають особливості навчальної вибірки, процесу навчання та специфіку результатів семантичної сегментації, до складу математичного забезпечення моделі семантичної сегментації включено коефіцієнт дисбалансу навчальної вибірки (I_R), дисперсію градієнтів функції втрат (D_g), коефіцієнт відхилення положення кордонів виділеного об'єкту від істинних кордонів (Δ_{Br}), коефіцієнт відносного розміру маски об'єкта (Δ_{obj}), середнє значення стандартного відхилення яскравості $\bar{\sigma}_V$ та розмах середніх значень яскравості $R_{\langle V \rangle}$ зображень в навчальній вибірці, що розраховуються за допомогою виразів (2.58-2.66).

$$I_R = 1 - \frac{\min_{k \in \{1, \dots, K\}} DM_k}{\max_{k \in \{1, \dots, K\}} DM_k}, \quad (2.58)$$

де DM_k – кількість пікселів класу k у всій навчальній вибірці.

Зазначимо, що $I_R \in [0,1]$. Вибірка вважається збалансованою, якщо $I_R \approx 0$, а випадок $I_R \approx 1$ відповідає значному дисбалансу навчальної вибірки.

Дисперсія градієнтів функції втрат D_g розраховується як відносне середньоквадратичне відхилення норми градієнта функції втрат $\mathcal{L}(w)$, обчислене протягом декількох послідовних епох:

$$D_g = \frac{std_T(\|\nabla \mathcal{L}(w)\|)}{mean_T(\|\nabla \mathcal{L}(w)\|)}, \quad (2.59)$$

де $std_T(\|\nabla \mathcal{L}\|)$, $mean_T(\|\nabla \mathcal{L}\|)$ – середньоквадратичне відхилення та середнє значення $\|\nabla \mathcal{L}(w)\|$ протягом T ; $\nabla \mathcal{L}(w)$ – градієнт функції втрат.

Коефіцієнт відхилення положення кордонів виділеного об'єкту від істинних кордонів Δ_{Br} розраховується за допомогою виразів:

$$\Delta_{Br} = \frac{1}{\sum_{k=1}^K |C_p^{(k)}|} \sum_{k=1}^K \sum_{p \in C_p^{(k)}} d(p, C_p^{(k)}), \quad (2.60)$$

$$d(p, C_t^{(k)}) = \min_{q \in C_t^{(k)}} \sqrt{(x_p - x_q)^2 + (y_p - y_q)^2}, \quad (2.61)$$

де $C_p^{(k)}$ – множина пікселів контуру передбаченої маски для k -го об'єкта; $C_t^{(k)}$ – множина пікселів контуру істинної маски для k -го об'єкта; $\sum_{k=1}^K |C_p^{(k)}|$ – загальна кількість пікселів у передбачених контурах усіх об'єктів (нормуючий чинник); $d(p, C_p^{(k)})$ – мінімальна евклідова відстань від пікселя $p \in C_p^{(k)}$ до найближчого пікселя істинного контуру $C_t^{(k)}$.

Коефіцієнт відносного розміру маски об'єкта Δ_{obj} розраховується так:

$$\Delta_{obj} = \frac{1}{N_{obj}} \sum_{i=1}^{N_{obj}} \frac{\sum_{j=1}^{n_i} Ms_{i,j}}{M_i}, \quad (2.62)$$

де N_{obj} – кількість об'єктів у вибірці; $Ms_{i,j}$ – кількість пікселів у масці j -го об'єкта у i -му зображенні; $|I_i|$ – загальна кількість пікселів у i -му зображенні; n_i – кількість об'єктів на i -му зображенні.

Середнє значення стандартного відхилення яскравості $\bar{\sigma}_V$ та розмах середніх значень яскравості $R_{\langle V \rangle}$ зображень у форматі HSV у навчальній вибірці розраховуються відповідно до виразів (2.63-2.66). При цьому яскравість (канал V) виражається як ціле число в діапазоні від 0 до 255.

$$\bar{\sigma}_V = \frac{1}{N_\Sigma} \sum_{n=1}^{N_\Sigma} \sigma_{V_n}, \quad (2.63)$$

$$R_{\langle V \rangle} = \max_{1 \leq n \leq N} \langle V_n \rangle - \min_{1 \leq n \leq N} \langle V_n \rangle, \quad (2.64)$$

$$\langle V_n \rangle = \frac{1}{WH} \sum_{x=1}^W \sum_{y=1}^H V_n(x, y), \quad (2.65)$$

$$\sigma_{V_n} = \sqrt{\frac{1}{WH} \sum_{x=1}^W \sum_{y=1}^H (V_n(x, y) - \langle V_n \rangle)^2}, \quad (2.66)$$

де N_Σ – кількість прикладів (зображень) у навчальній вибірці; σ_{V_n} – стандартне відхилення значень яскравості в n -му зображенні; V_n – масив значень каналу яскравості в n -му зображенні; $\langle V_n \rangle$ – середнє значення яскравості n -го зображення; W, H – ширина та висота зображення.

В підсумку вирази (2.27-2.66) складають базис опису математичного апарату моделі семантичної сегментації, що за рахунок визначення переліку конструктивних параметрів сучасних НММ, модифікація яких дозволяє адаптувати НММ до конкретних умов застосування, забезпечує теоретичний базис методу побудови НМЗ семантичної сегментації 3О при БА персоналу ОКІ.

2.4. Висновки до другого розділу

Даний розділ присвячено вирішенню науково-практичної задачі розробки моделей біометричної аутентифікації в інформаційних системах об'єктів критичної інфраструктури. Основні результати розділу наступні:

- Отримала подальший розвиток модель процедури розпізнавання особи за зображенням обличчя та райдужною оболонкою ока при біометричній автентифікації персоналу об'єктів критичної інфраструктури з застосуванням нейромережових засобів, що, за рахунок реалізації формалізованого опису процедури розпізнавання, конкретизації параметрів умов відеореєстрації, конкретизації параметрів оцінювання ефективності і чинників впливу на ефективність процесу нейромережевого розпізнавання особи та розроблених підходів до визначення параметрів завад для розпізнавання особи і емоцій, розпізнавання атак за допомогою муляжів та визначення доцільності побудови

модульної нейромережевої моделі, дозволила деталізувати перспективні шляхи підвищення ефективності нейромережевих засобів біометричної автентифікації.

- Вперше розроблена модульна нейромережева модель, що, за рахунок співвіднесення функціоналу модулів із виконанням завдань біометричної автентифікації, які доцільно виконувати за допомогою окремої нейронної мережі, та за рахунок адаптації архітектурних параметрів нейронних мереж кожного із модулів до поставленого завдання з урахуванням наявності доступних апробованих інструментальних засобів, забезпечує можливість побудови ефективного нейромережевого методу біометричної автентифікації за зображенням обличчя та райдужною оболонкою ока в інформаційних системах об'єктів критичної інфраструктури, з урахуванням необхідності розпізнавання спуфінг-атак та забезпечення оперативності розробки відповідних нейромережевих засобів.

- Отримала подальший розвиток модель семантичної сегментації зображення обличчя при біометричній автентифікації на об'єктах критичної інфраструктури, що за рахунок застосування енкодер-декодерної архітектури нейронної мережі з варіативними конструктивними параметрами, які підлягають адаптації залежно від умов застосування, забезпечує можливість розробки ефективного методу побудови нейромережевих засобів семантичної сегментації зображення обличчя при біометричній автентифікації на об'єктах критичної інфраструктури.

РОЗДІЛ 3. МЕТОДИ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

3.1. Правила визначення архітектурних параметрів нейромережевої моделі семантичної сегментації

Оскільки, відповідно до [21, 55, 99, 118], визначення механізму формування множини допустимих архітектур і параметрів навчання доцільно реалізовувати поза межами моделі семантичної сегментації, то даний крок дослідження асоційовано з формуванням множини правил ($\{R\}$), що регламентують відповідні аспекти розробки НМЗ.

R1. Правило формування множини допустимих базових архітектур

Множина базових архітектур формується з урахуванням обчислювальних обмежень, допустимого терміну сегментації, характеристик зображень, дисбалансу класів, варіативності умов і вимог до точності. Формування множини базових архітектур здійснюється шляхом послідовного аналізу ключових умов задачі семантичної сегментації зображень:

- У випадку обмеженості терміну сегментації та обчислювальних ресурсів (допустимий термін сегментації – 100 мс, обсяг доступної пам'яті для зберігання параметрів моделі менший ніж 30 МБ) – MobileNet, EfficientNet (B0-B1).

- Для зображень в форматі RGB розміром до 256×256 – VGG (U-Net, U-Net++, або Attention U-Net++), MobileNet.

- Якщо кількість класів сегментації не перевищує 3 – MobileNet, VGG (U-Net), а в протилежному випадку – VGG (U-Net++ або Attention U-Net++), ResNet, HRNet.

- За необхідності сегментувати невеликі об'єкти (площа об'єкту займає менше ніж 0,1 площі вхідного зображення) та при високому дисбалансі прикладів об'єктів (коефіцієнт дисбалансу менший ніж 0,2), що підлягають сегментації у навчальній вибірці – VGG (U-Net++ або Attention U-Net++), HRNet.

- При високій варіативності освітлення та ракурсу відеореєстрації 30 після попередньої обробки (діапазони освітлення та ракурсу відеореєстрації перевищують порогові значення, що в першому наближенні дорівнює 0,5) - VGG (U-Net++ або Attention U-Net++), ResNet, EfficientNet, HRNet.

- За необхідності досягнення високої точності ($\text{IoU} > 0.85$) – VGG (U-Net++ або Attention U-Net++), ResNet, HRNet.

- Якщо загальна кількість навчальних прикладів $N_{\Sigma} \leq 10^4$, а допустима кількість епох навчання $\Delta_{TL} < 50$ – пріоритет надається моделям, що досягають швидкої збіжності на малих вибірках (MobileNet, EfficientNet, ResNet-18, VGG (U-Net)).

- Якщо $N_{\Sigma} > 10^4 \wedge \Delta_{TL} < 50$ – пріоритет надається моделям, яким притаманні висока початкова збіжність та стійкість динаміки втрат (ResNet-34, EfficientNet, VGG (U-Net++)).

- У випадках, коли жодна з базових архітектур не задовольняє всі вимоги, передбачено використання MobileNet як компромісної моделі, що забезпечує оптимальний баланс між швидкістю обробки та якістю сегментації.

Використовуючи результати [92, 123, 147], визначено доцільним, в залежності від кількості вагових коефіцієнтів (N_w), виділити три класи складності нейромережових архітектур: малої складності, для яких $N_w < 5 \times 10^6$, середньої складності – $5 \times 10^6 \leq N_w < 2 \times 10^7$, високої складності – $N_w \geq 2 \times 10^7$. До моделей малої складності відносяться MobileNet та EfficientNet-B0, до моделей середньої складності – ResNet-18, ResNet-34, U-Net (VGG) та Attention U-Net, а до моделей високої складності – ResNet-101, HRNet, U-Net++ та Attention U-Net++.

R2. Правило аугментації навчальних даних

Правило визначає механізм аугментації навчальних даних, що здійснюється задля підвищення здатності моделі до узагальнення. В базовому варіанті використовуються механізми аугментації типу:

- Random Crop, що полягає у випадковому обмеженні зображення до 90% від початкового розміру. Це дозволяє моделі краще фокусуватись на локальних

ділянках обличчя.

- Gaussian Noise зі стандартним відхиленням $\sigma < 0.01$, що моделює шум, типовий для сенсорів камер, і підвищує стійкість до перешкод у вхідному зображенні.

Крім того, у випадку виявлення у навчальній вибірці значної варіативності характеристик яскравості застосовується аугментація Random Brightness/Contrast: стохастичне змінення яскравості та контрастності з амплітудою в межах $\pm 15\%$. Рішення про наявність значної варіації приймається, якщо середнє значення стандартного відхилення $\bar{\sigma}_V > 20$ або розмах $R_{\langle V \rangle} > 40$, що розраховуються відповідно до виразів (2.63, 2.64).

R3. Правило вибору функції втрат

Вибір реалізується із переліку функцій втрат, визначених виразами (2.49-2.57), з урахуванням кількості класів сегментації K , коефіцієнту дисбалансу навчальної вибірки I_R , коефіцієнту відхилення положення кордонів виділеного об'єкту від істинних кордонів Δ_{Br} і коефіцієнту відносного розміру маски об'єкта Δ_{obj} , що розраховуються відповідно до виразів (2.58, 2.60-2.62).

- При $K = 2$. Якщо $I_R \geq 0.2$ використовується Binary Cross-Entropy, якщо $I_R < 0.2$ та $\Delta_{obj} \leq 0,1$ – Focal Loss, а в іншому випадку – Dice Loss.

- При $K = 3$. Якщо $I_R \geq 0.2$ та $\Delta_{Br} \leq 0,05$ – Jaccard Loss, а якщо $\Delta_{Br} > 0,05$ – Dice Loss. Якщо $I_R < 0.2$ – Tversky Loss.

- При $K > 3$. Якщо $I_R \geq 0.2$ використовується Categorical Cross-Entropy, якщо $I_R < 0.2$ або $\Delta_{obj} \leq 0,01$ – Tversky Loss, а в інших випадках Dice Loss.

- При недостатній інформації або суперечливих вимогах – Dice Loss.

R4. Правило вибору оптимізатора

Правило визначає алгоритм оптимізації значень вагових коефіцієнтів нейронної мережі, що використовується під час навчання задля забезпечення стабільної збіжності функції втрат, підтримання стійкої динаміки оновлення параметрів протягом усього процесу навчання та досягнення високої якості сегментації за умови обмежень обсягу навчальної вибірки й складності моделі. Також під час навчання аналізується динаміка функції втрат на валідаційній

вибірці для підтвердження ефективності обраного алгоритму або прийняття рішення про його корекцію. В зв'язку з цим правило R4 охоплює два рівні ухвалення рішень: початковий вибір алгоритму оптимізації (R4.1) та його адаптацію під час навчання (R4.2).

R4.1. Початковий вибір алгоритму оптимізації

- Для моделей середньої та високої складності, зокрема, ResNet, HRNet, U-Net++, Attention U-Net, що навчаються на обмежених за обсягом вибірках ($N_{\Sigma} \leq 10^4$) доцільно використовувати оптимізатор Adam, оскільки він забезпечує адаптивне масштабування градієнтів та сприяє стабільній збіжності навіть за шумного або нерівномірного градієнтного поля.

- Для тих же моделей середньої та високої складності, при $N_{\Sigma} > 10^4$ застосовується оптимізатор SGD з імпульсом (momentum=0,9). Такий підхід забезпечує стабільності збіжності функції втрат та, за умови достатньої кількості даних, дозволяє досягти вищої точності сегментації на валідаційних даних у порівнянні з адаптивними методами.

- Для моделей на базі MobileNet та EfficientNet-B0 і при $N_{\Sigma} > 10^4$ використовується AdamW як компромісне рішення між швидкістю збіжності та контролем над регуляризацією.

R4.2. Адаптація алгоритму оптимізації

- Якщо в процесі навчання спостерігається висока дисперсія градієнтів функції втрат або спостерігається нестабільність динаміки функції втрат, то здійснюється перехід до оптимізатора Adam. Дисперсія градієнтів вважається високою, якщо розрахована відповідно до виразу (2.59) величина $D_g > 0,3$ протягом щонайменше 5 послідовних епох навчання. Динаміка функції втрат вважається нестабільною, якщо за 5 послідовних епох її сумарне зменшення становить менше ніж 1% або амплітуда коливань перевищує 20% від середнього значення на цьому інтервалі.

R5. Правило визначення параметрів швидкості навчання

Правило визначає параметри швидкості навчання НММ, що включає вибір початкового значення швидкості та стратегії її зміни в процесі навчання. Це

забезпечує стабільну збіжність функції втрат, стійку динаміку оптимізації протягом усього періоду навчання. Оскільки початкове значення швидкості визначається з урахуванням складності архітектури, а вибір стратегії зміни швидкості реалізується з урахуванням обсягу навчальної вибірки, допустимої кількості епох навчання і особливостях збіжності функції втрат, то правило R5 охоплює три рівні ухвалення рішень: визначення початкового значення швидкості навчання (R5.1), вибір стратегії зміни швидкості навчання (R5.2) та адаптація параметрів стратегії до проміжних показників навчання (R5.3).

R5.1. Визначення початкового значення швидкості навчання

Вибір початкового значення швидкості навчання (learning rate) здійснюється з позицій забезпечення стабільності процесу навчання, що, відповідно до [2, 5, 36], в значній мірі залежить від складності НММ, що, в свою чергу, в основному залежить від кількості вагових коефіцієнтів (N_w). Моделі малої складності характеризуються обмеженою глибиною та невеликою кількістю вагових коефіцієнтів, тому обчислювані на кожній ітерації градієнти функції втрат мають, як правило, меншу норму, тобто відносно менший абсолютний розмір зміни ваг. Це знижує ризик дестабілізації під час оновлення параметрів навіть за підвищеного значення швидкості навчання. Іншими словами, малі моделі демонструють меншу чутливість до коливань градієнтів, а отже, можуть ефективно навчатися з більшим кроком оновлення, що забезпечує швидшу збіжність у початковій фазі навчання. Для таких моделей learning rate = 0,001. Моделі середньої складності характеризуються більшою кількістю шарів і вагових коефіцієнтів, що призводить до накопичення похибок градієнтів у глибших шарах. У таких мережах норма градієнтів, обчислена, наприклад, у вигляді L2-норми, може змінюватися від шару до шару – зменшуватись (ефект згасання градієнтів) або зростати (ефект вибуху градієнтів). У цих умовах підвищене значення learning rate може призвести до нестабільних коливань у процесі оптимізації, тому потребують деякого зменшення. Тому для моделей середньої складності learning rate = 0,0007. Моделі високої складності характеризуються великою глибиною і складною структурою зв'язків (включно

з резидуальними блоками, механізмами уваги тощо), що підвищує ймовірність нелінійного зростання норм градієнтів у різних частинах мережі. Це робить їх особливо чутливими до великого кроку оновлення, оскільки надмірне значення learning rate може спричинити нестійке оновлення ваг, дивергентну поведінку або вибух значень активацій. Відповідно, для моделі високої складності learning rate = 0,0005. Різниця між рекомендованими значеннями learning rate для моделей середньої та високої складності є емпірично обґрунтованою та орієнтована передусім на випадки використання адаптивних оптимізаторів (Adam або AdamW). Таким чином,

- Для нейромережових моделей на базі MobileNet або EfficientNet-B0, що відносяться до моделей малої складності, learning rate = 0,001.

- Для нейромережових моделей на базі ResNet-18, ResNet-34, U-Net (VGG) та Attention U-Net, що відносяться до моделей середньої складності, learning rate = 0,0007.

- Для нейромережових моделей на базі ResNet-101, HRNet та моделей типу, U-Net++, Attention U-Net++, що відносяться до моделей високої складності, learning rate = 0,0005.

R5.2. Вибір стратегії зміни швидкості навчання

Вибір стратегії зміни швидкості навчання реалізується з позиції забезпечення адаптивного керування темпом навчання, що дозволяє ефективно використовувати доступні обчислювальні ресурси при збереженні стабільності оптимізації функції втрат. Вибір стратегії здійснюється з урахуванням допустимої кількості епох навчання (Δ_{TL}) та загальної кількості навчальних прикладів (N_{Σ}).

- Якщо $\Delta_{TL} < 50$, то використовується стратегія Cosine Annealing, що передбачає поступове зменшення learning rate за косинусоподібною траєкторією, є найбільш прийнятною в умовах обмеженого часу на навчання, оскільки дозволяє швидко проходити фазу грубої оптимізації й поступово переходити до точної локальної мінімізації.

- Якщо $N_{\Sigma} \leq 10^4 \wedge \Delta_{TL} \geq 50$, то використовується стратегія Step Decay із

зменшенням learning rate у 10 разів кожні 10 епох, що дозволяє уникнути перенавчання на обмеженій навчальній вибірці.

- В інших випадках використовується стратегія ReduceLROnPlateau.

R5.3. Адаптація стратегії зміни швидкості навчання

- У випадку використання стратегії Cosine Annealing, якщо після навчання на протязі першої третини від визначеної кількості епох навчання (T_L) зменшення функції втрат становить менш ніж 0,5% за 5 епох, параметр T_{max}^{CA} стратегії (повна довжина косинусної фази) зменшується на 20%, що прискорює зниження learning rate.

- У випадку використання стратегії Step Decay, якщо після першого зменшення learning rate (тобто після 10 епох) значення функції втрат зростає або залишається практично незмінним (зменшення $<1\%$) протягом наступних 5 епох, то інтервал між зниженнями learning rate скорочується до 5 епох.

- У випадку використання стратегії ReduceLROnPlateau, якщо значення функції втрат на валідаційній вибірці не зменшується більше ніж на 0,001 протягом 5 послідовних епох, то поточне значення learning rate зменшується в 2 рази.

При цьому в R5.3 враховуються граничні межі зміни параметрів означених стратегій навчання [5, 36, 147].

Зазначимо, що в правилі R5 тип вхідних зображень та архітектура моделі безпосередньо не враховуються, оскільки ці характеристики вже були використані у правилі вибору базової архітектури.

R6. Правило вибору розміру батчу

Вибір розміру батчу реалізується з урахуванням доступних обчислювальних ресурсів (доступного обсягу відеопам'яті графічного процесора в байтах) (V_{CR}^d), архітектурної складності нейромережевої моделі, розміру вхідного зображення та дисперсії градієнтів, що дозволяє ефективно використовувати потужності апаратного забезпечення та забезпечити оптимальне співвідношення швидкості та стабільності збіжності функції втрат. Відповідно, правило R6 охоплює два рівні ухвалення рішень: вибір розміру батчу

на початку навчання (R6.1) та адаптацію розміру батчу до процесу навчання (R6.2).

R6.1. Вибір початкового розміру батчу

Для НММ на базі ResNet-18, ResNet-34, U-Net (VGG) та Attention U-Net, що відносяться до моделей середньої складності, при розмірі зображення 256×256 пікселів:

- Якщо $V_{CR}^d \leq 4 \times 10^9$, то batch size = 4.
- Якщо $4 \times 10^9 < V_{CR}^d \leq 8 \times 10^9$, то batch size = 8.
- Якщо $8 \times 10^9 < V_{CR}^d \leq 1.6 \times 10^{10}$, то batch size = 16.
- Якщо $1.6 \times 10^{10} < V_{CR}^d$, то batch size = 32.

Для НММ на базі MobileNet або EfficientNet-B0, що відносяться до моделей малої складності, batch size збільшується у два рази, а для НММ на базі ResNet-101, HRNet та моделей типу, U-Net++, Attention U-Net++, що відносяться до моделей високої складності, batch size зменшується у два рази. Також величина batch size коригується в залежності від розміру зображення. Для зображення розміром 512×512 batch size зменшується в 4 рази, при розмірі 384×384 – зменшується в 2 рази, а при розмірі 128×128 збільшується у 2 рази.

R6.2. Адаптація розміру батчу

Якщо в процесі навчання на протязі 5 послідовних епох навчання величина розрахованої за допомогою виразу (2.59) дисперсії градієнтів функції втрат (D_g) перевищує 0,2, але менша ніж 0,3, тобто коли $0,2 < D_g \leq 0,3$, за умови достатнього обсягу обчислювальних ресурсів розмір батчу збільшується у 2 рази.

R7. Правило вибору механізму регуляризації

Адаптація механізму регуляризації до умов задачі сегментації реалізується задля забезпечення балансу між темпом навчання, стабільністю збіжності функції втрат і ризиком перенавчання. Вибір виду та параметрів механізму регуляризації здійснюється з урахуванням кількості навчальних прикладів N_Σ та складності архітектури моделі, зокрема. кількості вагових коефіцієнтів:

- У випадку, коли обсяг навчальної вибірки $N_\Sigma \leq 10^4$, для запобігання перенавчанню застосовується механізм $Dropout = 0,1$, а також механізм L2-

регуляризації з $weight\ decay = 10^{-4}$.

- Для компактних моделей на базі архітектур MobileNet або EfficientNet-B0 Dropout може негативно впливати на збіжність і ефективність навчання. У цьому випадку Dropout не застосовується, а для забезпечення однорідної динаміки збіжності та темпу навчання використовується L2-регуляризація із $weight\ decay = 10^{-5}$.

- Для зменшення ризику перенавчання та стабілізації вагових коефіцієнтів при навчанні моделей з кількістю параметрів більшою ніж 5×10^6 , таких як ResNet (у конфігураціях від ResNet-34 і вище), HRNet, Attention U-Net, U-Net++, Attention U-Net, застосовується Dropout із ймовірністю 0,3, а також L2-регуляризація з $weight\ decay = 10^{-5}$.

Зазначимо, що використання лише механізмів Dropout та L2-регуляризації пояснюється їх доведеною ефективністю при застосуванні нейронних мереж для семантичної сегментації зображень в умовах обмежених обчислювальних ресурсів [5, 36].

R8. Правило визначення кількості навчальних епох

Визначення кількості епох навчання (T_L) здійснюється з позицій необхідності уникнення перенавчання, забезпечення можливості досягнення необхідної точності сегментації з урахуванням обмеженості тривалості навчання. При цьому враховується динаміка збіжності функції втрат, максимально допустима кількість епох навчання, обсяг та збалансованість навчальної вибірки.

R8.1. Визначення мінімальної кількості епох навчання

- Якщо $N_\Sigma \leq 10^3$ або середня кількість прикладів кожного класу менша ніж 500, або $I_R > 0,2$ (розраховується відповідно до (2.58)), то мінімальна кількість епох навчання 20. В інших випадках мінімальна кількість епох навчання 30.

- Якщо $\Delta_{TL} < T_L$, то $T_L = \Delta_{TL}$.

R8.2. Визначення умов зупинки та продовження навчання

Навчання припиняється, якщо після мінімальної кількості епох навчання

функція втрат на валідаційній вибірці не покращується більше ніж на 0,02 протягом останніх 5 послідовних епох, або досягнуто наперед задану точність сегментації. У протилежному випадку, за умови, що $T_L < \Delta_{TL}$, навчання продовжується.

Зазначимо, що порогові значення параметрів, використаних у наведених правилах, визначено на основі практичного досвіду та даних літературних джерел [5, 36, 146, 147] як початкові орієнтири, що можуть бути уточнені на подальших етапах дослідження. Також слід відзначити, що сформована система правил визначення архітектурних параметрів забезпечує можливість розробки формалізованих механізмів вибору типу НММ та параметрів її навчання з урахуванням обчислювальних обмежень, допустимого терміну сегментації, характеристик вхідних зображень, дисбалансу класів, варіативності умов навчання і вимог до точності. Це сприяє структурованості й прозорості процесу конфігурування моделі, дозволяє уникнути суперечностей між архітектурними рішеннями та стратегіями оптимізації, а також закладає основу для інтеграції означених механізмів вибору у загальний метод визначення архітектурних параметрів НММ семантичної сегментації 3О при БА на ОКІ.

3.2. Метод побудови нейромережових засобів семантичної сегментації зображення обличчя при біометричній автентифікації

Використавши як прототип описаний в [99] метод семантичної сегментації зображень, спираючись на запропоновану модель семантичної сегментації (2.27-2.66) та сформовану множину правил визначення архітектурних параметрів, виконання запропонованого методу визначення архітектурних параметрів НММ семантичної сегментації 3О при БА на ОКІ розділено на шість етапів. При цьому, враховуючи необхідність адаптації до варіативних умов застосування та результати [16, 147, 160], в основу методу покладено принцип поетапної адаптації архітектури, включно з параметрами навчання – спочатку шляхом ініціалізації максимально допустимих значень для визначеного виду НММ, а надалі через поступову модифікацію параметрів моделі з урахуванням

досягнутої точності, рівня ресурсоспоживання та стабільності процесу навчання.

Етап 1. Визначення умов розробки НММ. На вхід етапу подається кортеж параметрів $\langle L_{in} \rangle$, що описують умови поставленої задачі БА, нормативні вимоги до системи БА, характеристики доступного набору навчальних даних, опис розробленої моделі семантичної сегментації M_{SS} та сформовану множину правил $\{R\}$, що регламентують розробку НМЗ.

Крок 1.1. Формалізація умов застосування. На основі експертного оцінювання кортежу параметрів $\langle L_{in} \rangle$, M_{SS} та $\{R\}$, з урахуванням результатів п. 2.1, 2.3, визначається кортеж параметрів $\langle L_G \rangle$, що характеризують загальні умови застосування НМЗ: $W \times H$, C , N_Σ , V_{CR}^d , V_{CR}^s , Δ_{TL} . Також визначаються параметри, що характеризують специфіку процесу семантичної сегментації: кількість класів сегментації (K_{SS}), кількість навчальних прикладів для кожного із елементів сегментації ($N_{i_{SS}}$), допустимий термін процесу семантичної сегментації (Δ_{TSS}), вид та мінімально допустиме значення показника точності сегментації (A_{SS}, Δ_A), коефіцієнт дисбалансу навчальної вибірки (I_R), коефіцієнт відхилення положення кордонів виділеного об'єкту від істинних кордонів (Δ_{Br}), коефіцієнт відносного розміру маски об'єкта (Δ_{obj}), середнє значення стандартного відхилення яскравості $\bar{\sigma}_V$ та розмах середніх значень яскравості $R_{\langle V \rangle}$ зображень в навчальній вибірці, що розраховуються за допомогою виразів (2.58, 2.60, 2.62-2.64), відповідно.

Крок 1.2. Визначення доступних архітектур. На основі експертного оцінювання визначається множина доступних базових нейромережових архітектур ($\{AN\}$). За замовчуванням до вказаної множини віднесено архітектури на основі VGG (U-Net, U-Net++, Attention U-Net++) та архітектури типу ResNet, MobileNet, EfficientNet, HRNet. На основі експертного оцінювання, з урахуванням результатів, отриманих при розробці моделі семантичної сегментації, визначаються конструктивні параметри кожної архітектури, що входить до складу $\{AN\}$ та діапазон значень цих конструктивних параметрів, що визначається множиною мінімальних ($\{AN_{min}\}$) та максимальних значень ($\{AN_{max}\}$). Процедури експертного оцінювання передбачено реалізовувати з

використанням результатів [104, 107, 163].

Виходом етапу являється кортеж значень параметрів, що характеризують: обмеження, які стосуються засобів сегментації, множину доступних базових архітектур, множини конструктивних параметрів кожної із базових архітектур – $S_1 = \langle \langle L_G \rangle, \{AN\}, \langle R_{AN} \rangle \rangle$. Зазначимо, що отримані на вхід першого етапу опис розробленої моделі семантичної сегментації M_{SS} та сформована множина правил $\{R\}$ в подальшому використовуються при виконанні етапів 2-6.

Етап 2. Вибір архітектурного рішення. На вхід етапу подається кортеж S_1 , визначений в результаті реалізації етапу 1.

Крок 2.1. Вибір допустимих архітектур. Вибір реалізується на основі правила R1, з урахуванням множини доступних архітектур, обчислювальних обмежень, характеристик зображень, дисбалансу класів, варіативності умов і вимог до точності, що визначені на етапі 1.

Крок 2.2. Вибір базової архітектури. На даному кроці реалізується вибір архітектури, що буде використовуватись в якості базової. У випадку, коли реалізація попереднього кроку призводить до вибору декількох архітектур, то в якості базової (A_{NB}) обирається та архітектура, програмно-апаратна реалізація якої є менш складною. Також, відповідно до визначеного типу, з позицій досягнення максимальної точності сегментації, визначається множина архітектурних параметрів ($\langle R_{ANB} \rangle$).

Вихід етапу 2 визначається виразом $S_2 = \langle A_{NB}, \langle R_{ANB} \rangle \rangle$.

Етап 3. Визначення параметрів енкодера. На вхід етапу подаються $\langle L_G \rangle$, S_2 , Δ_A , A_{SS}^r – відповідність між величиною допустимого та величиною досягнутого показника точності, що визначається в результаті виконання етапу 6. При виконанні етапу 3 безпосередньо після етапу 2 вважається, що $A_{SS}^r = true$.

Крок 3.1. Ініціалізація параметрів енкодера. Крок виконується у випадку $A_{SS}^r = true$. Величини конструктивних параметрів енкодера (2.31, 2.33, 2.34, 2.47, 2.48) встановлюються рівними значенням відповідних елементів із множини $\{AN_{max}\}$ для $\langle R_{ANB} \rangle$, тобто $EN_{te}(i) = AN_{max}$, де i – номер конструктивного параметру.

Крок 3.2. Модифікація параметрів енкодера. Крок виконується у випадку $A_{ss}^r = false$. При цьому глибина енкодера (кількість згорткових шарів/кількість стеків) змінюється відповідно до виразів:

$$EN_{te}(i) = EN_{t-1}(i) - 1, i = z, \quad (3.1)$$

$$if\ EN_{te}(i) < EN_{min}(i) \Rightarrow EN_{te}(i) = AN_{min}(i), \quad (3.2)$$

де z – номер конструктивного параметру, що відповідає глибині енкодера.

Інші параметри енкодера модифікуються з позиції збереження сумісності вихідного сигналу енкодера з вхідним сигналом декодера. Виходом етапу 3 є множина значень конструктивних параметрів енкодера, $S_3 = \{EN_{te}\}$.

Етап 4. Визначення параметрів декодера. На вхід етапу подаються $\langle L_G \rangle$, S_3 , S_2 , Δ_A та A_{ss}^r . При виконанні етапу 4 безпосередньо після етапу 3 вважається, що $A_{ss}^r = true$.

Крок 4.1. Ініціалізація параметрів декодера. Крок виконується у випадку $A_{ss}^r = true$. Величини конструктивних параметрів декодера (2.32, 2.35-2.42, 2.47, 2.48) встановлюються рівними значенням відповідних конструктивних параметрів енкодера, тобто $DN_{td}(i) = EN_{te}(i)$, де i – номер конструктивного параметру. При цьому використовується максимальна кількість skip-зв'язків та attention-модулі, за їх наявності в базовій архітектурі.

Крок 4.2. Модифікація параметрів декодера. Крок виконується у випадку $A_{ss}^r = false$. Модифікація полягає в тому, що починаючи з найглибшого рівня декодера, який відповідає шару з найменшим розміром карти ознак, у відповідності до (3.3, 3.4) реалізується послідовне видалення attention-модулів, skip-зв'язків та шарів апсемплінгу.

$$DN_{td}(i) = DN_{td-1}(i) - 1, \quad (3.3)$$

$$if\ DN_{td}(i) < AN_{min}(i) \Rightarrow DN_{td}(i) = AN_{min}(i). \quad (3.4)$$

Інші параметри декодера модифікуються з позиції збереження сумісності вихідного сигналу енкодера з вхідним сигналом декодера. Виходом етапу 4 є множина значень конструктивних параметрів декодера, $S_4 = \{DN_{td}\}$.

Етап 5. Навчання нейромережевої моделі. На вхід етапу подаються $\langle L_G \rangle$, S_4 , S_3 , S_2 , Δ_A та A_{ss}^r . При виконанні етапу 5 безпосередньо після етапу 4

вважається, що $A_{ss}^r = true$.

Крок 5.1. Ініціалізація параметрів навчання, що регулюють процес визначення вагових коефіцієнтів синаптичних зв'язків при навчанні НММ.

Крок виконується у випадку $A_{ss}^r = true$ та здійснюється відповідно до правил R2, R3, R4.1, R5.1, R5.2, R6.1, R7, R8.1. При цьому вагові коефіцієнти нейронів згорткових і повнозв'язних шарів, в яких використовується функція активації типу ReLU, ініціалізуються за схемою He Normal (Kaiming Normal). Для нейронів вихідного шару з функцією активації Softmax або Sigmoid застосовується Xavier Uniform.

Крок 5.2. Проведення навчання. На кожній епосі навчання оцінюються значення функції втрат $\mathcal{L}(w)$ та дисперсії функції втрат D_g , що розраховуються відповідно до (2.49-2.57, 2.59) та використовуються в правилах R4.2, R5.3, R6.2 та R8.2 для прийняття рішення щодо модифікації параметрів навчання або щодо припинення навчання.

Якщо показники точності навчання відповідають допустимим значенням, то відбувається перехід до виконання першого кроку етапу 6, в протилежному випадку відбувається перехід до четвертого кроку етапу 6.

Виходом кроку 5.2 та етапу 5 в цілому являються: значення показників точності на кожній епосі навчання на тренувальній та валідаційній вибірках ($|A_{ss}|$) та значення вагових коефіцієнтів синаптичних зв'язків, отриманих в результаті навчання ($|W_l|$).

Етап 6. Налаштування архітектурних параметрів. На вхід етапу подаються: $|A_{ss}|$, $|W_l|$, $\langle L_G \rangle$, V_{CR}^S , S_4 , S_3 , S_2 , Δ_A та A_{ss}^r .

Крок 6.1. Оцінювання результатів навчання – досягнуті на останній епосі навчання значення показників точності $|A_{ss}(T_L)|$ порівнюються з допустимими.

Якщо досягнуті показники відповідають допустимим, тобто $A_{ss}^r = true$, то відбувається перехід на крок 6.2, в протилежному випадку, при $A_{ss}^r = false$, відбувається перехід на крок 6.4.

Крок 6.2. Оцінювання точності на тестових даних – зводиться до порівняння значень показників точності ($|A_{ss}^{TS}|$), отриманих при застосуванні

навченої НММ до сегментації зображень із тестової вибірки, що не використовувались при навчанні, з допустимими значеннями. Якщо точність сегментації не відповідає заданій, тобто $A_{ss}^r = false$, то відбувається перехід на крок 6.4. У протилежному випадку, $A_{ss}^r = true$, відбувається перехід на крок 6.3.

Крок 6.3. Квантування моделі – зводиться до нелінійного перетворення числового представлення вагових коефіцієнтів у формат з меншою бітовою глибиною, що забезпечує підвищення оперативності визначення вихідного сигналу НММ та зменшення обсягу пам'яті, необхідної для зберігання параметрів моделі. Передбачено, що процес квантування здійснюється з урахуванням результатів [56, 67]. Функціонал кроку реалізується лише у випадку $A_{ss}^r = true$ за умови, що ресурсоємність моделі вища за V_{CR}^S . В базовому варіанті квантування передбачено збереження вагових коефіцієнтів у форматі 8-бітних цілих чисел, що, за умови початкового збереження вагових коефіцієнтів у форматі 32-бітних чисел з плаваючою комою, дозволяє приблизно у 4 рази зменшити обсяг пам'яті, яка використовується для збереження вагових коефіцієнтів. В результаті квантування формується модифікована матриця вагових коефіцієнтів $|W_{l_k}|$, що використовується для повторного розрахунку та оцінювання точності моделі на тестовій вибірці.

Якщо точність моделі достатня, то в подальшому використовується модифікована матриця $|W_{l_k}|$, а в протилежному випадку – використовується $|W_l|$, отримана в результаті виконання кроку 5.2.

Крок 6.4. Адаптація архітектурних параметрів – полягає у модифікації архітектурних параметрів нейромережевої моделі в залежності від поточних значень архітектурних параметрів та результатів оцінювання, отриманих в залежності від здійснених переходів або в результаті виконання кроку 5.2, або в результаті виконання кроків 6.1-6.3. При цьому:

- Якщо $A_{ss}^r = false$, то реалізується перехід на крок 2.1, що забезпечує зміну типу базової НММ, при цьому розглянутий тип архітектури вилучається із множини допустимих. У випадку, коли всі архітектури з множини допустимих базових архітектур досліджено, а жодна з них не дозволила досягти заданих

значень показників ефективності, приймається рішення про неможливість побудови НММ, яка в заданих умовах застосування забезпечує ефективну семантичну сегментацію ЗО.

- Якщо $A_{ss}^r = true$ і ресурсоемність моделі вища за V_{CR}^s , то реалізується перехід на крок 4.2, виконання якого призводить до модифікації параметрів декодера, пов'язаної із зменшенням його ресурсоемності. У випадку, коли всі можливі комбінації значень архітектурних параметрів декодера досліджено, реалізується перехід на крок 3.2, пов'язаний з модифікацією параметрів енкодера щодо зменшення його ресурсоемності, за умови, що параметри енкодера знаходяться в допустимих межах.

Дослідження завершується після визначення архітектурних параметрів декодера та енкодера, що за прийнятного обсягу обчислювальних ресурсів забезпечують достатню точність сегментації ЗО представника персоналу ОКІ. Виходом кроку 6.4, етапу 6 та методу в цілому являється кортеж параметрів $\langle L_{out} \rangle$, що характеризують архітектуру (S_2, S_3, S_4, V_{CR}) , вагові коефіцієнти синаптичних зв'язків $(|W_l|)$ та результати навчання (A_{ss}, T_L, T_{ss}) НММ семантичної сегментації ЗО представника персоналу ОКІ.

Узагальнена схема запропонованого методу, що ілюструє порядок його виконання, показана на рис. 3.1. Напрямок виконання методу відповідає напрямку стрілок на схемі. При цьому послідовні переходи позначені суцільними лініями, а альтернативні переходи, що реалізуються за результатами перевірки виконання умов на кроках 6.1, 6.2, 6.4, позначені пунктиром.

На кроці 6.1 перевіряється умова достатньої точності НММ на навчальних даних, на кроці 6.2 перевіряється умова достатньої точності на тестових даних, а на кроці 6.4 перевіряються умови, пов'язані з модифікацією базової архітектури та модифікацією параметрів енкодера і декодера. Зазначимо, що перевірка доцільності квантування моделі на кроці 6.3 та перевірка виконання умов, пов'язаних з модифікацією параметрів навчання на кроці 5.2, не змінюють послідовність виконання методу.

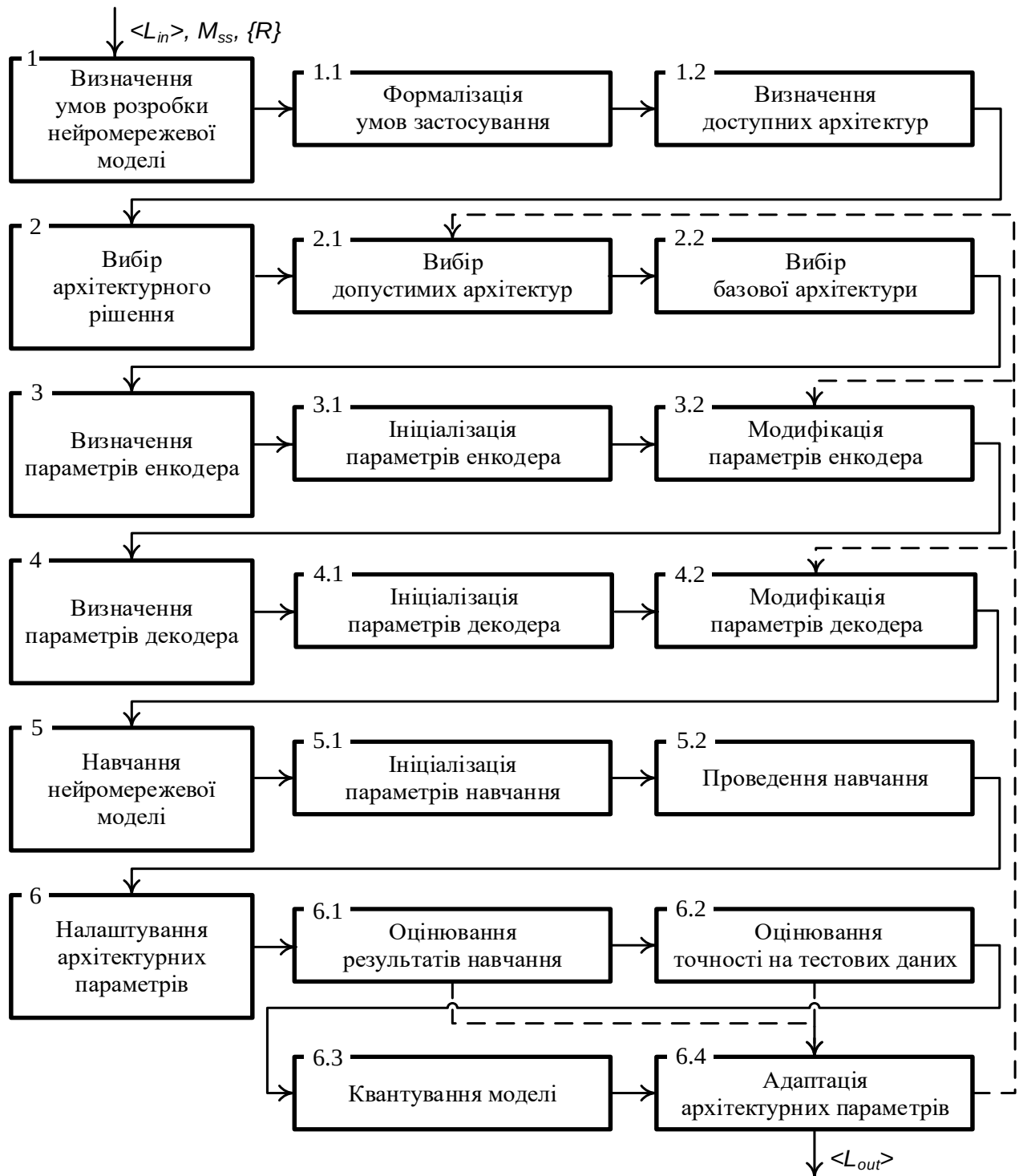


Рис. 3.1. Узагальнена схема методу побудови нейромережевих засобів семантичної сегментації зображення обличчя при біометричній автентифікації

Зазначимо, що запропонований метод передбачає поетапну адаптацію як типу НММ, так і конструктивних параметрів НММ у межах обраного типу, що реалізується в напрямку зменшення архітектурної складності – від максимально до мінімально допустимих конфігурацій. На відміну від більшості відомих

рішень [2, 4, 10, 20, 22, 25, 35, 38], такий підхід дозволяє вже на першому етапі оцінити придатність базової архітектури щодо досягнення цільових показників в очікуваних умовах застосування. Крім того, використаний в методі механізм динамічного коригування параметрів навчання, включно з тривалістю його проведення, забезпечує можливість досягти стабільної збіжності, уникнути перенавчання та ефективно використовувати обчислювальні ресурси.

3.3. Нейромережевий метод біометричної автентифікації за зображенням обличчя та райдужною оболонкою ока в інформаційних системах об'єктів критичної інфраструктури

Базуючись на результатах попередніх розділів даної дисертаційної роботи, визначено, що в нейромережевому методі БА за ЗО та РОО в інформаційних системах ОКІ доцільно врахувати необхідність реалізації означених в [1, 2, 146] процедур попередньої обробки кадрів. Базуючись на запропонованому підході, реалізація методу БА передбачає виконання етапів, що співвідносяться з реалізацією процедур: перевірки відповідності параметрів зареєстрованого відеопотоку допустимим значенням; попередньої обробки відеопотоку; виділення кордонів ЗО у піддослідному кадрі вхідного відеопотоку; детектування спуфінг-атак на основі візуальних артефактів; детектування спуфінг-атак на основі артефактів зовнішнього оточення; виявлення областей завад, характерних для очікуваних умов відеореєстрації; виділення кордонів РОО; визначенням множин координат контрольних точок на ЗО; детектування спуфінг-атак за динамікою параметрів живучості; розпізнавання базових емоцій; детектування спуфінг-атак на основі розпізнаних емоцій; розпізнавання особи представника персоналу ОКІ. Узагальнена схема реалізації даного методу показана на рис. 3.2.

Зазначимо, що реалізація процедур виділення кордонів ЗО у піддослідному кадрі вхідного відеопотоку, виявлення областей завад, характерних для очікуваних умов відеореєстрації, та виділення кордонів РОО асоціюється з виконанням етапу 3, а реалізація процедур детектування спуфінг-атак на основі

візуальних артефактів, детектування спуфінг-атак на основі артефактів зовнішнього оточення, детектування спуфінг-атак за динамікою параметрів живучості та детектування спуфінг-атак на основі розпізнаних емоцій – з виконанням етапу 4.

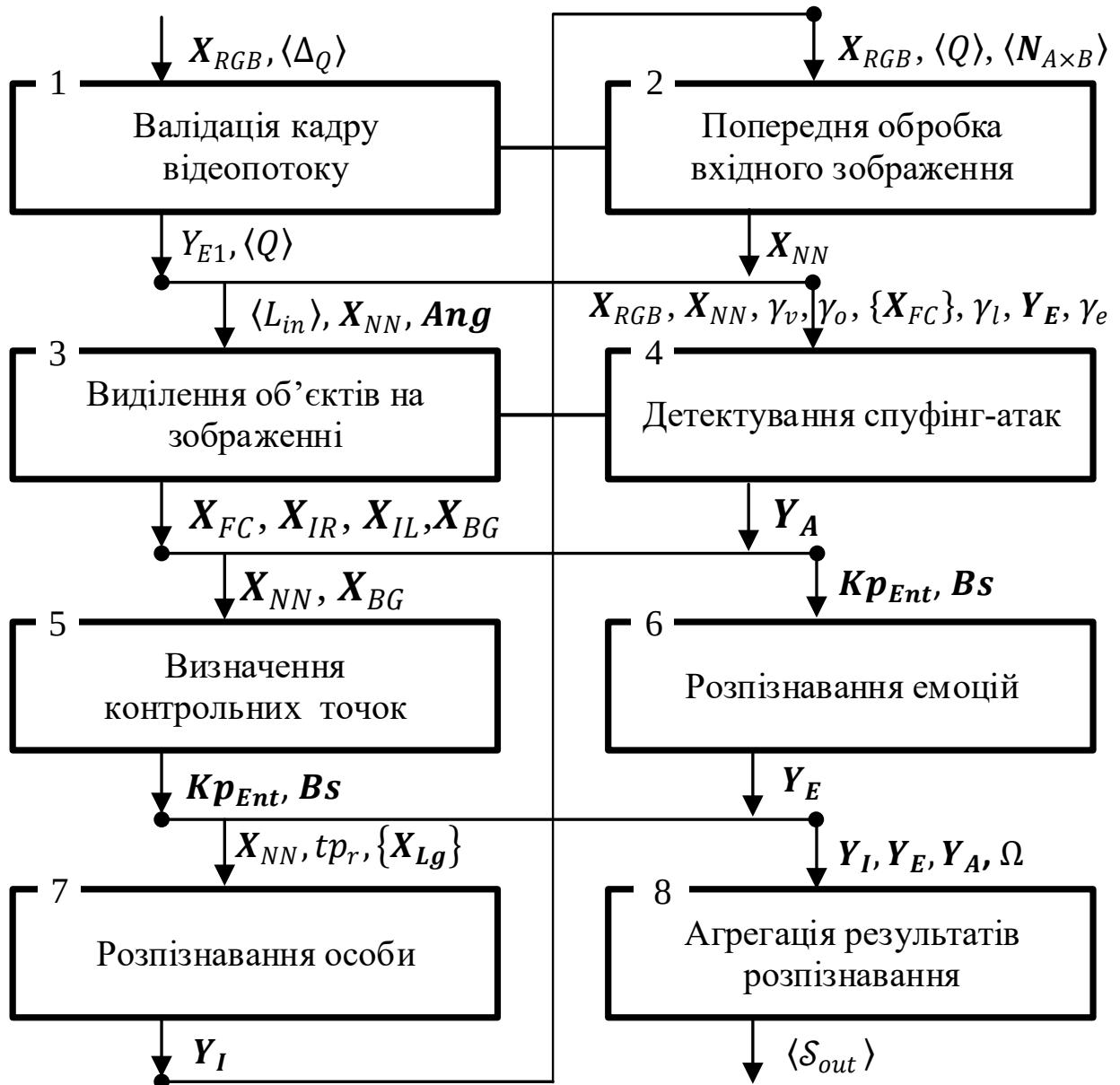


Рис. 3.2. Узагальнена схема реалізації нейромережевого методу біометричної автентифікації за зображенням обличчя та райдужною оболонкою ока в інформаційних системах об'єктів критичної інфраструктури

Етап 1. Валідація кадру відеопотоку. На вхід етапу подається матриця параметрів (X_{RGB}), що описують кадр (RGB-зображення), отриманий із відеопотоку камери відеоспостереження, а також кортеж допустимих значень параметрів ($\langle \Delta_Q \rangle$), що характеризують якість зображення. При цьому $X_{RGB} = |x_{RGB}|_{W \times H}$ – матриця, що описує колір кожного із пікселів вхідного RGB-зображення розміром $W \times H$. Кожен елемент цієї матриці представляє собою вектор, що містить значення яскравості червоного (R), зеленого (G), синього (B). Елементами $\langle \Delta_Q \rangle$ є: Δ_W – допустима ширина діапазону яскравості; $Y_{avg,min}, Y_{avg,max}$ – мінімальне та максимальне значення середньої яскравості зображення (в першому наближенні 70 та 180); $\lambda_{M,min}$ – мінімальне значення контрасту Міхельсона; $\Delta_{\sigma_Y,min}, \Delta_{\sigma_Y,max}$ – мінімальне та максимальне значення стандартного відхилення яскравості; $\Delta_{R_{br}}, \Delta_{R_{dr}}$ – допустимі значення індексів засвітлення та затемнення; $\Delta_{\sigma_L^2}$ – поріг розмитості.

В першому наближенні $\Delta_W = 40$, $Y_{avg,min} = 70$, $Y_{avg,max} = 180$, $\lambda_{M,min} = 0,35$, $\Delta_{\sigma_Y,min} = 0,1$, $\Delta_{\sigma_Y,max} = 0,05$, $\Delta_{R_{br}} = 0,1$, $\Delta_{R_{dr}} = 0,05$, $\Delta_{\sigma_L^2} = 100$.

Відповідно до [146, 155, 156], етап базується на підході до безеталонної оцінки якості зображення, а його виконання розділено на два кроки.

Крок 1.1. Розрахунок показників відображення. Розрахунок здійснюється на основі показників зображення в форматі RGB та на основі яскравості каналу Y в кольоровій моделі YCbCr. Конвертація зареєстрованого зображення в формат YCbCr здійснюється за допомогою (2.7-2.9). Відповідно до результатів п. 2.1, за допомогою виразів (2.13-2.23) розраховуються Y_{avg} , Y_{max} , Y_{min} , I , λ_M , σ_Y , R_{br} , R_{dr} , L , σ_L^2 , μ_R , μ_G , μ_B , μ_{avgRGB} , Δ_{avgRGB} .

Крок 1.2. Перевірка придатності кадру. Зображення, що асоціюється з кадром відеопотоку, вважається непридатним для подальшого аналізу, якщо:

- Більш ніж 50% пікселів мають яскравість нижчу за 50 або вищу ніж 200.
- Середня яскравість виходить за встановлені межі:

$$Y_{avg} \notin [Y_{avg,min}, Y_{avg,max}]$$
- Контраст Міхельсона менший ніж допустимий: $\lambda_M < \lambda_{M,min}$.

- Стандартне відхилення яскравості виходить за встановлені межі $\sigma_Y \notin [\Delta_{\sigma_Y, min}, \Delta_{\sigma_Y, max}]$.
- Індекс засвітлення перевищує допустимий: $R_{br} > \Delta_{R_{br}}$.
- Індекс затемнення перевищує допустимий: $R_{dr} > \Delta_{R_{dr}}$.
- Дисперсія Лапласіана менша від порогового значення: $\sigma_L^2 < \Delta_{\sigma_L^2}$.
- Ширина основного діапазону яскравості, є недостатньою, тобто:

$$W_Y = P_{95} - P_5, \quad (3.5)$$

$$W_Y < \Delta_W, \quad (3.6)$$

де P_{95}, P_5 – відповідно 95-й та 5-й перцентилі розподілу яскравості.

Виходом кроку та етапу в цілому є сигнал про можливість подальшого розпізнавання (Y_{E1}) та, у випадку можливості подальшого розпізнавання ($Y_{E1} = 1$), кортеж, що містить розраховані показники яскравості, різкості та контрастності ($\langle Q \rangle$).

Етап 2. Попередня обробка вхідного зображення. На вхід етапу подається X_{RGB} , $\langle Q \rangle$, а також розміри вхідних полів НММ ($\langle N_{A \times B} \rangle$), що використовуються для подальшого аналізу зображень. Основним завданням виконання етапу являється нормалізація кольорових характеристик зображення, узгодження розмірів зображення з розмірами вхідних полів НММ, що використовуються в системі БА, та фільтрація шуму. Виконання етапу розділено на чотири кроки.

Крок 2.1. Корекція кольорових характеристик.

- Корекція балансу білого кольору, що здійснюється відповідно до виразу (3.7), за правдивості умови (3.8):

$$R(i) = R(i) \frac{\mu_{avgRGB}}{\mu_R}, \quad G(i) = G(i) \frac{\mu_{avgRGB}}{\mu_G}, \quad B(i) = B(i) \frac{\mu_{avgRGB}}{\mu_B}, \quad (3.7)$$

$$\Delta_{avgRGB} > \Delta_{avgRGB}^{ent}, \quad (3.8)$$

де Δ_{avgRGB}^{ent} – допустима величина Δ_{avgRGB} , що, в першому наближенні дорівнює 15 [13, 146].

- Конвертація RGB-зображення в YCbCr-зображення, що здійснюється за допомогою виразів (2.7-2.9).

- Якщо в конвертованому YCbCr-зображенні $Y_{avg} < 70$ або $Y_{avg} > 180$, то застосовується гамма-корекція:

$$Y(n) = 255 \times \left(\frac{Y(n)}{255}\right)^\gamma \quad \gamma = \begin{cases} 1.2, Y_{avg} < 70 \\ 0.8, Y_{avg} > 180 \end{cases} \quad (3.9)$$

- Якщо після гама-корекції $\sigma_Y < 20$ або $\lambda_M < 0.35$, то здійснюється процедура адаптивного вирівнювання гістограми яскравості (Contrast Limited Adaptive Histogram Equalization, CLAHE) з параметром обмеження контрасту (clip limit), рівним 2 [13, 48, 66, 72].

Крок 2.2. Фільтрація шуму. Виконання кроку полягає у почерговому застосуванні медіанного, білатерального фільтрів та фільтру підвищення чіткості.

- Медіанна фільтрація застосовується у разі виявлення імпульсного шуму типу «сіль-перець», ознаками якого є надмірна частка пікселів з екстремальними значеннями яскравості на зображеннях із низьким контрастом та обмеженою варіативністю компонент яскравості. Тобто медіанна фільтрація застосовується за виконання умови (3.10) та реалізується відповідно до виразу (3.11).

$$\frac{N_{Y>240} + N_{Y<15}}{N} > 0.03 \wedge \lambda_M < 0.5 \wedge \sigma_Y < 50, \quad (3.10)$$

$$Y(i, j) = \text{median}\{Y(i + k, j + l)\} \quad k, l \in [-r; r], \quad (3.11)$$

де *median* – оператор вибору медіани (центрального значення впорядкованого списку); r – радіус фільтра (для ядра 3×3 $r = 1$).

- Білатеральна фільтрація застосовується для зменшення локального шуму в каналі яскравості із збереженням контурів при виявленні гаусівського шуму у разі виконання умов (3.12) та реалізується відповідно до виразів (3.13-3.17).

$$\sigma_Y \in [25, 50] \wedge \sigma_L^2 \in [500, 1500] \wedge \lambda_M < 0.6, \quad (3.12)$$

$$Y(i, j) = \frac{1}{W(i, j)} \sum_{k=-r}^r \sum_{l=-r}^r Y(i + k, j + l) \times G_s(k, l) \times G_r(Y(i, j) - Y(i + k, j + l)), \quad (3.13)$$

$$W(i, j) = \sum_{k=-r}^r \sum_{l=-r}^r G_s(k, l) \times G_r(Y(i, j) - Y(i + k, j + l)), \quad (3.14)$$

$$G_s(k, l) = \exp\left(-\frac{k^2 + l^2}{2\sigma_s^2}\right), \quad (3.15)$$

$$G_r(\delta) = \exp\left(-\frac{\delta^2}{2\sigma_r^2}\right), \quad (3.16)$$

$$\delta = |Y(i, j) - Y(i + k, j + l)|, \quad (3.17)$$

де G_s – просторове ядро Гауса; G_r – радіальне (яскравісне) ядро Гауса; $W(i, j)$ – нормалізуючий коефіцієнт; r – радіус вікна фільтрації ($r = 2$, вікно 5×5); σ_s – параметр просторової згладжувальної компоненти ($\sigma_s = 5$); σ_r – параметр радіальної (яскравісної) згладжувальної компоненти ($\sigma_r = 10$).

Зазначимо, що σ_Y відображає загальну варіативність яскравості у зображенні. Умова $\sigma_Y > 50$ вказує на наявність можливого текстурного шуму, характеристики якого відрізняються від шуму з гаусівським розподілом. У такому випадку застосування білатеральної фільтрації може призводити до погіршення якості зображення.

За умови $\sigma_Y < 25$ застосування фільтрації є недоцільним, оскільки варіативність яскравості зображення є незначною. Умова $\sigma_L^2 \in [500, 1500]$ вказує на те, що фільтр буде застосовано до не надто розмитих та чітких зображень. В протилежному випадку білатеральна фільтрація або не дасть результату, або загладить важливі дрібні деталі. Умова $\lambda_M < 0.6$ свідчить про те, що фільтр буде застосовано до висококонтрастних зображень. В протилежному випадку застосування фільтра може призвести до втрати деталізації.

- Якщо після застосування медіанного та білатерального фільтрів чіткість зображення є помірною ($\sigma_L^2 \in [100, 200]$), то застосовується фільтр підвищення чіткості (unsharp masking):

$$G(x, y) = \sum_{i=-k}^k \sum_{j=-k}^k Y(x + i, y + j) \times w(i, j), \quad (3.18)$$

$$w(i, j) = \frac{1}{2\pi\sigma^2} \exp\left(-\frac{i^2 + j^2}{2\sigma^2}\right), \quad (3.19)$$

$$Y(x, y) = Y(x, y) + \alpha(Y(x, y) - G(x, y)), \quad (3.20)$$

де $G(x, y)$ – зображення розмите за допомогою фільтра Гауса; w – ядро фільтра Гауса; α – коефіцієнт підсилення чіткості (в базовому випадку 0.5); k – радіус фільтра (за замовчуванням $k=2$, що відповідає ядру 5×5); σ – стандартне відхилення розподілу (за замовчуванням $\sigma = 1$).

Після цього, відповідно до (2.10-2.12), YCbCr-зображення конвертується в RGB-зображення.

Крок 2.3. Узгодження розмірів. Виконується за умов можливості ефективного масштабування, що визначаються на основі даних [13, 48, 54, 66, 72]. Реалізується методом бікубічної інтерполяції з урахуванням масштабного коефіцієнту між розмірами вхідного зображення вхідного поля кожної із НММ.

Крок 2.4. Нормалізація кольору. Виконується відповідно до апробованих підходів [13, 54, 95, 115, 120] та полягає у приведенні значень відображення кольору кожного пікселя в заданий діапазон.

Виходом кроку 2.4 та етапу 2 в цілому є X_{NN} – матриця, що описує колір кожного із пікселів вхідного RGB-зображення розміром $H_{NN} \times W_{NN}$, який відповідає вхідному полю НММ. Зазначимо, що порогові значення параметрів, що використовуються в умовах визначення доцільності застосування процедур обробки зображення, можуть бути в подальшому модифіковані з урахуванням практичного досвіду та результатів теоретичних досліджень. Крім того, в подальшому перспективним є впровадження додаткових механізмів обробки на основі вейвлет-перетворень.

Етап 3. Виділення об'єктів на зображенні. Виконання етапу передбачає захоплення ЗО на вхідному зображенні та виділення на ньому природніх контурів ЗО та РОО за допомогою НМЗ семантичної сегментації побудованого в результаті використання наведеного в п. 3.2 методу. Відповідно до наведеного в п. 3.2 опису, на вхід етапу подаються кортеж параметрів $\langle L_{in} \rangle$, отриманий на етапі 2 матриця X_{NN} та **Ang** – множина значень вертикальних та горизонтальних кутів, які визначають положення ЗО, що вважаються найбільш прийнятними для розпізнавання. Виконання даного етапу розділено на 5 кроків.

Крок 3.1. Детектування ЗО. Виконання кроку передбачає застосування

НМЗ, побудованих на основі однієї із НММ, призначених для вирішення завдання 1 (див. рис. 2.2 та табл. 2.1). В результаті виконання кроку, крім bounding box, що обмежує зовнішні межі виявленого в кадрі ЗО, визначаються координати п'яти показаних на рис. 2.8 контрольних точок ЗО. В базовому випадку для детектування ЗО передбачено використання НМЗ на основі НММ RetinaFace, оскільки серед наведених табл. 2.1 ця модель дозволяє визначити координати п'яти базових контрольних точок та забезпечує більший bounding box, що гарантує достатній контекст для подальшої сегментації.

Крок 3.2. Позиціонування ЗО. Виконуються геометричні перетворення, спрямовані на забезпечення відповідності положення ЗО положенню, яке вважається найбільш прийнятним для розпізнавання. Для цього використовуються множини X_{NN} та **Ang**. В базовому випадку позиціонування полягає у реалізації афінних перетворень ЗО на основі 5 контрольних точок.

Крок 3.3. Побудова НМЗ семантичної сегментації ЗО. Виконання кроку передбачає реалізацію всіх етапів запропонованого в п. 3.2 методу побудови НМЗ семантичної сегментації ЗО при БА.

Крок 3.4. Семантична сегментація ЗО. Виконання кроку передбачає застосування побудованого в результаті виконання кроку 3.3. НМЗ для семантичної сегментації вхідного зображення для виділення природніх контурів ЗО та РОО, а також виділення фонових об'єктів.

Крок 3.5. Інтеграційна обробка ЗО. Даний крок передбачає інтеграцію вхідного зображення з масками ЗО та РОО, отриманими в результаті виконання кроку 3.4. Результатом виконання кроку є екстрактоване ЗО та екстрактовані зображення правої і лівої РОО, що містять лише пікселі, які належать об'єкту сегментації, з відсіченням фону та сторонніх елементів.

Виходом кроку 3.5 та етапу в цілому є масиви: X_{FC} – містить значення яскравості пікселів для екстрактованого ЗО; X_{IR} , X_{IL} – містять значення яскравості пікселів для екстрактованого зображення правої і лівої РОО; X_{BG} – містить значення яскравості пікселів, що відповідають фону та стороннім елементам.

Етап 4. Детектування спуфінг-атак. Відповідно до результатів [19, 25, 34, 36, 37, 73, 89] виконання етапу розділено на чотири кроки:

Крок 4.1. Детектування спуфінг-атак на основі візуальних артефактів.

Виконання кроку полягає у застосуванні НММ DeerPixBiS, на вхід якої подається масив X_{RGB} , а також заздалегідь визначене порогове значення класифікації γ_v . Виходом кроку 4.1 є бінарний сигнал Y_v щодо наявності спуфінг-атаки, сформований на основі порівняння вихідного сигналу DeerPixBiS з γ_v .

Крок 4.2. Детектування спуфінг-атак на основі артефактів зовнішнього оточення. Відповідно до [50, 145, 146], детектування здійснюється за рахунок нейромережевого аналізу X_{RGB} та X_{NN} , що разом з пороговим значенням класифікації γ_o подається на вхід даного кроку. В якості нейромережевого класифікатора використовується НММ типу Siamese Network або Two_channel Networks, побудова яких виконується відповідно до [39, 50, 145]. Виходом кроку 4.2 бінарний сигнал Y_o щодо наявності спуфінг-атаки, сформований на основі результату вихідного сигналу нейромережевого класифікатора з порогом γ_o .

Крок 4.3. Детектування спуфінг-атак за динамікою параметрів живучості.

Виконання кроку полягає у нейромережевому аналізі 10 кадрів, що містять відфільтроване ЗО (включно з РОО). В базовому випадку, з урахуванням результатів [27, 63], для аналізу прийнято застосувати доступну за посиланням <https://www.kaggle.com/code/leduchoank17hl/liveness-convnext>, НММ ModifiedConvNeXtLarge, яка пройшла донавчання на наборі даних Liveness Detection - Zalo AI Challenge 2022, що знаходиться за посиланням <https://www.kaggle.com/datasets/hlly34/liveness-detection-zalo-2022/>. На вхід кроку подається порогове значення γ_l та матриця X_{FC} , отримана в результаті виконання етапу 3 при обробці 10 кадрів відеопотоку. Виходом кроку 4.3 є та бінарний сигнал Y_l про наявність спуфінг-атаки, сформований на основі порівняння вихідного сигналу НММ з порогом γ_l .

Крок 4.4. Детектування спуфінг-атак на основі розпізнаних емоцій.

Виконання кроку полягає у нейромережевому аналізі динаміки емоцій на предмет їх природності. На вхід кроку подається множина Y_E , що містить

числові значення інтенсивностей 7 базових емоцій визначених на протязі 10 послідовних відеокадрів. У відповідності до результатів п. 2.2, детектування реалізується за рахунок нейромережевого оцінювання динаміки емоцій. Для цього використовується НМЗ на базі мережі PNN, на вхід якої подаються числові значення інтенсивності 7 базових емоцій для 10 послідовних кадрів, а виходом являється ймовірність відсутності спуфінг-атаки та ймовірність реалізації спуфінг-атаки/неадекватного стану особи, що підлягає автентифікації. Виходом кроку 4.4 є бінарний сигнал Y_e про наявність спуфінг-атаки, сформований на основі порівняння вихідного сигналу PNN з γ_e .

Виходом етапу 4 при виконанні кроку 4.1 є Y_v , при виконанні кроку 4.2 - Y_o , при виконанні кроку 4.3 - Y_l , а при виконанні кроку 4.4 - Y_e . В сукупності вказані вихідні сигнали формують множину Y_A , описану в виразі (2.2).

Етап 5. Визначення контрольних точок. Виконання етапу передбачає визначення множини контрольних точок обличчя, очищеної від елементів, що потрапили в зони завад. На вхід етапу подається X_{NN} , X_{BG} . Реалізація етапу розділена на два кроки.

Крок 5.1. Визначення контрольних точок. Виконання кроку передбачає застосування НММ FaceMeshV2, яка навіть при розгортанні на малопотужних мобільних пристроях забезпечує обробку із затримкою 20–100 мс, що дозволяє в реальному часі на основі X_{NN} , сформувати масив Kp_{Ent} , елементи якого співвідносяться з тривимірними координатами 478 контрольних точок обличчя (468 точок відповідають власне ЗО, а 10 точок відповідають зіницям очей) особи, що проходить авторизацію. Зазначимо, що використання FaceMeshV2 дозволяє визначити масив BS , елементи якого співвідносяться з 52 Blendshape Scores, які є числовим представленням інтенсивності різних мімічних виразів. Відповідно до [27, 31, 33, 111], такі показники забезпечують достатньо оперативне та топологічно точне представлення ЗО для подальшого нейромережевого розпізнавання емоцій та особи представника персоналу ОКІ.

Крок 5.2. Фільтрація контрольних точок у зоні завад. На даному кроці обнуляються елементи масиву Kp_{Ent} та BS , що відповідають контрольним

точкам, які не знаходяться в зонах, що відповідають X_{BG} . Виходом кроку та етапу в цілому є масив Kp_{Ent} та Bs , модифікований відповідним чином.

Етап 6. Розпізнавання емоцій. Виконання етапу полягає у визначенні базових емоцій, що відображаються на ЗО особи, яка проходить автентифікацію. На вхід етапу подається Kp_{Ent} та Bs , а виходом являється множина Y_E , елементи якої відповідають інтенсивності відображення на ЗО семи базових емоцій. Виконання етапу розділяється на два кроки.

Крок 6.1. Побудова НМЗ розпізнавання емоцій. Враховуючи особливості задачі та рекомендації [50, 63, 144, 145], у випадку визначення на п'ятому етапі 68 контрольних точок реалізується побудова НМЗ на основі НММ FaceEmotion_ID. У випадку визначення на п'ятому етапі 52 Blendshape Scores передбачено використання MLP зі структурою 52 (вхідний шар) – 128 (перший схований шар) – 64 (другий схований шар) – 7 (вихідний шар), для навчання якого в дослідницьких цілях можливо використати попередньо оброблений за допомогою FaceMeshV2 набір даних CK+ (Extended Cohn-Kanade Dataset) з розрахованими значеннями Blendshape Scores.

Крок 6.2. Визначення базових емоцій. Реалізується за рахунок застосування побудованого на кроці 6.1 НМЗ, на вхід якого подаються Kp_{Ent} та/або Bs .

Етап 7. Розпізнавання особи. На вхід етапу подаються X_{NN} , параметр tp_r , значення якого вказує на тип розпізнавання особи, та порогове значення γ_{rr} , з яким порівнюється інтегрована оцінка схожості, отримана за рахунок об'єднання результатів аналізу ЗО і РОО. У випадку $tp_r = 0$ на вхід етапу також подається множина $\{X_{Lg}\}$, що містить ЗО та РОО легітимних представників персоналу ОКІ, а розпізнавання здійснюється за допомогою нейромережевого порівняння ЗО та РОО особи, що проходить перевірку, з ЗО та РОО легітимних представників персоналу ОКІ. У випадку $tp_r = 1$ розпізнавання асоціюється з класифікацією особи за допомогою НММ, попередньо навченої на ЗО та РОО легітимних представників персоналу. Виконання етапу розділено на три кроки.

Крок 7.1. Розпізнавання особи за ЗО. Виконується нейромережевий аналіз

X_{NN} обличчя з метою формування оцінки подібності r_{FC} між ЗО особи, яка підлягає розпізнаванню та ЗО легітимних представників.

Крок 7.2. Розпізнавання особи за РОО. Полягає у нейромережевому аналізі відфільтрованої від завад області РОО з метою формування оцінки подібності r_{IR} між РОО особи, що підлягає розпізнаванню та РОО легітимних представників.

Крок 7.3. Інтеграція результатів. На цьому кроці обидві оцінки r_{FC} і r_{IR} за допомогою виразу (3.21) об'єднуються в інтегровану оцінку r_{RR} та приймається остаточне рішення на основі порівняння r_{RR} з пороговим значенням γ_{RR} , що реалізується за допомогою виразу (3.22).

$$r_{RR} = \alpha \times r_{FC} + (1 - \alpha) \times r_{IR}, \quad (3.21)$$

$$\text{if } r_{RR} > \gamma_{RR} \Rightarrow RR = 1 \text{ else } RR = 0. \quad (3.22)$$

Якщо $RR = 1$, вважається, що особа розпізнана як легітимний представник персоналу ОКІ, після чого визначається відповідний ідентифікатор (ID). Якщо $RR = 0$, вважається, що особа не розпізнана, а $ID = 0$. У базовому випадку $\alpha = 0.7$, а $\gamma_{RR} = 0.82$, що, зважаючи на результати [30, 88, 146], відповідає співвідношенню True Acceptance Rate (TAR) $\approx 97\text{--}98\%$ при False Acceptance Rate (FAR) $\leq 1\%$, і є прийнятним у системах доступу до ОКІ. Зазначимо, що у випадку $tp_r = 0$ при реалізації кроків 7.1 та 7.2, відповідно до [144-146], пропонується використання НММ на основі Siamese Network або Two_channel Networks, а при $tp_r = 1$ НММ типу MobileNet. Виходом етапу 7 являється $Y_I = \{RR, ID\}$.

Етап 8. Агрегація результатів розпізнавання. Етап призначено для формування вихідного сигналу $\langle S_{out} \rangle$ даного методу відповідно до специфікації формату (Ω), що подається на вхід етапу. Специфікація передбачає використання шаблону, що забезпечує уніфікацію вихідної інформації для її подальшого використання. Виконання етапу розділено на два кроки.

Крок 8.1. Формування результатів відповідно до специфікації. Значення вихідних параметрів приводяться до структури, визначеної специфікацією формату Ω , яка включає: формат представлення (наприклад, JSON), перелік необхідних полів, їх порядок, типи даних, правила ідентифікації та кодування. У разі потреби здійснюється перетворення типів даних і додаткове маркування.

При достроковому завершенні виконання методу (наприклад, через виявлення спуфінг-атаки) поля, що не можуть бути визначені, залишаються порожніми (null або "-" згідно зі специфікацією формату).

Крок 8.2. Формування вихідного сигналу. На основі підготовлених даних формується вихідний сигнал $\langle \mathcal{S}_{out} \rangle$ для подальшого використання або збереження. У базовому випадку вихід кроку 8.2, етапу 8 та методу в цілому являється $\langle \mathcal{S}_{out} \rangle = \langle Y_I, Y_E, Y_A \rangle$.

Враховуючи результати п.2.1-2.3 та п.3.2, реалізація запропонованого методу передбачає послідовне виконання наступних кроків:

- 1.1-1.2 – розраховуються показники відображення кадру та проводиться перевірка придатності кадру до подальшої обробки;
- 2.1-2.2 – корегуються характеристики кольору та здійснюється фільтрація зображення;
- 2.3-2.4 – вхідне зображення масштабується до розміру вхідного поля НММ та проводиться нормалізація кольору;
- 3.1-3.3 – будується НМЗ семантичної сегментації, реалізується семантична сегментація ЗО та відбувається інтеграційна обробка ЗО, результатом якої являється екстрактоване ЗО та екстрактовані зображення правої і лівої РОО, що містить лише пікселі, які належать об'єкту сегментації;
- 4.1-4.3 – проводиться детектування спуфінг-атак на основі візуальних артефактів, артефактів зовнішнього оточення та за живучістю;
- 5.1-5.2 – визначаються контрольні точки ЗО (включаючи РОО) та проводиться фільтрація контрольних точок у зоні завад;
- 6.1-6.2 – проводиться побудова НМЗ для розпізнавання емоцій та визначається інтенсивність відображення на ЗО семи базових емоцій;
- 4.4 – проводиться детектування спуфінг-атак на основі природності розпізнаних емоцій;
- 7.1-7.3 – проводиться розпізнавання особи за ЗО, за РОО та розраховується інтегральна оцінка результатів розпізнавання;

- 8.1-8.2 – відповідно до заданої специфікації проводиться формування результатів виконання та формується вихідний сигнал методу.

Таким чином, запропоновано метод, що реалізує багатокрокову адаптивну обробку відеопотоку та забезпечує комплексне виконання ключових процедур, необхідних для забезпечення ефективної автентифікації в варіативних умовах застосування.

3.4. Висновки до третього розділу

Даний розділі присвячено вирішенню науково-практичної задачі розробки методів біометричної автентифікації в інформаційних системах об'єктів критичної інфраструктури. Основні результати розділу наступні:

- Вперше розроблено метод побудови нейромережевих засобів семантичної сегментації зображення обличчя при біометричній автентифікації, що за рахунок поетапної адаптації типу та параметрів нейромережевого енкодера та нейромережевого декодера до розміру зображення, кількості каналів кольору, допустимої мінімальної точності сегментації, допустимої максимальної обчислювальної складності реалізації процесу сегментації, допустимої максимальної обчислювальної складності та допустимого терміну навчання нейромережевої моделі в напрямку зменшення архітектурної складності та за рахунок використання механізму динамічного коригування параметрів навчання, забезпечує можливість вже на першому етапі експериментів оцінити придатність базової архітектури до досягнення цільових показників, досягти стабільної збіжності навчання і уникнути перенавчання, що в результаті забезпечує можливість підвищити точність виділення недеформованих завадами контурів зображення обличчя та зменшити обсяг складних довготривалих експериментів, спрямованих на визначення архітектурних параметрів нейромережевої моделі.

- Отримав подальший розвиток нейромережевий метод біометричної автентифікації за зображенням обличчя та райдужною оболонкою ока в інформаційних системах об'єктів критичної інфраструктури, що реалізує

багатокрокову адаптивну обробку відеопотоку та забезпечує комплексне виконання ключових процедур, необхідних для забезпечення ефективної автентифікації в варіативних умовах застосування. Етапи методу із застосуванням нейромережових рішень структуровано як послідовність процедур, що відповідають типовим завданням біометричної автентифікації, які зазвичай реалізуються окремими нейромережовими моделями. Вперше в межах єдиної архітектури реалізовано багаторівневий аналіз ознак спуфінг-атак з урахуванням візуальних артефактів зображення обличчя, артефактів зовнішнього оточення, динаміки параметрів живучості та динаміки емоційного стану. При цьому реалізовано механізм адаптивної обробки відеопотоку, який передбачає автоматичне оцінювання показників відображення, динамічне формування множини зображень, придатних для подальшої обробки, а також попередню обробку зображень з метою підвищення якості їх відображення. Фільтрацію зображення обличчя та райдужної оболонки від типових завад забезпечено за рахунок застосування процедури семантичної сегментації з наступним поелементним маскуванням піксельних значень, що дозволяє виключити з обробки ділянки зображення, які містять завади, та уникнути врахування хибно визначених контрольних точок у зонах перекриття, тіней або сторонніх об'єктів. Однією з ключових особливостей методу є цілеспрямоване використання доступних, апробованих наперед навчених нейромережових моделей з відкритим кодом, інструментальне забезпечення яких адаптовано до умов відеореєстрації на об'єктах критичної інфраструктури.

- Шляхи подальших досліджень в області вдосконалення розроблених методів доцільно співвіднести з застосуванням в методі семантичної сегментації новітніх типів нейромережових моделей семантичної сегментації та з проведенням експериментальних досліджень, пов'язаних з уточненням характеристик нейромережових моделей, котрі використовуються на різних етапах методу біометричної автентифікації за зображенням обличчя та райдужною оболонкою ока.

РОЗДІЛ 4. СИСТЕМА БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ТА ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ

4.1. Архітектура системи біометричної автентифікації

Відповідно до загальноприйнятої технології розробки інформаційних систем в якості базису опису архітектури НМС БА в інформаційній системі ОКІ використано UML-діаграми прецедентів. Розроблені UML-діаграми прецедентів базуються на представлений в п. 2.2 модульній НММ БА персоналу ОКІ за ЗО та РОО, представленому в п. 3.3 нейромережевому методі БА за ЗО та РОО, із застосуванням НМЗ та передбачає формалізацію архітектурних компонентів, потоків обробки біометричних даних та специфічних вимог до захисту від спуфінг-атак. Також при розробці UML-діаграм прецедентів були враховані нормативні вимоги до систем БА [133-136]. Відповідно до рекомендацій [109, 148], 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 НМС, 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 НММ, зокрема ініціалізації процесу навчання, налаштування його параметрів, збору необхідних даних та оцінювання результатів. Таким чином, на цьому етапі модель відображає здатність НМС 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 семантичної сегментації ЗО 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 деталізації архітектури та алгоритмів її реалізації. На першому рівні деталізації системи БА, що відповідає показаній на рис. 4.1 діаграмі прецедентів, враховано чотири основні актори, які взаємодіють із системою:

- «Підконтрольний об'єкт» – ініціює процедуру аутентифікації та є джерелом біометричних даних.
- «Сканер» – здійснює відеореєстрацію потоку даних.
- «Контролер доступу» – відповідає за прийняття рішення щодо надання або відмови у доступі.
- «Адміністратор» – виконує налаштування параметрів функціонування системи.

Зазначимо, що актори «Адміністратор» та «Підконтрольний об'єкт» є діючими особами, а актори «Контролер доступу» та «Сканер» являються технічними засобами.

При цьому базовий варіант діаграми включає такі прецеденти:

- «Провести розпізнавання» – 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.
- «Інтегрувати результати розпізнавання» – прецедент, що визначає остаточне рішення про результати розпізнавання на основі інтеграції результатів розпізнавання за ЗО та за РОО.
- «Детектувати ЗО» – прецедент, пов'язаний із захопленням ЗО у відеопотоці.

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

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

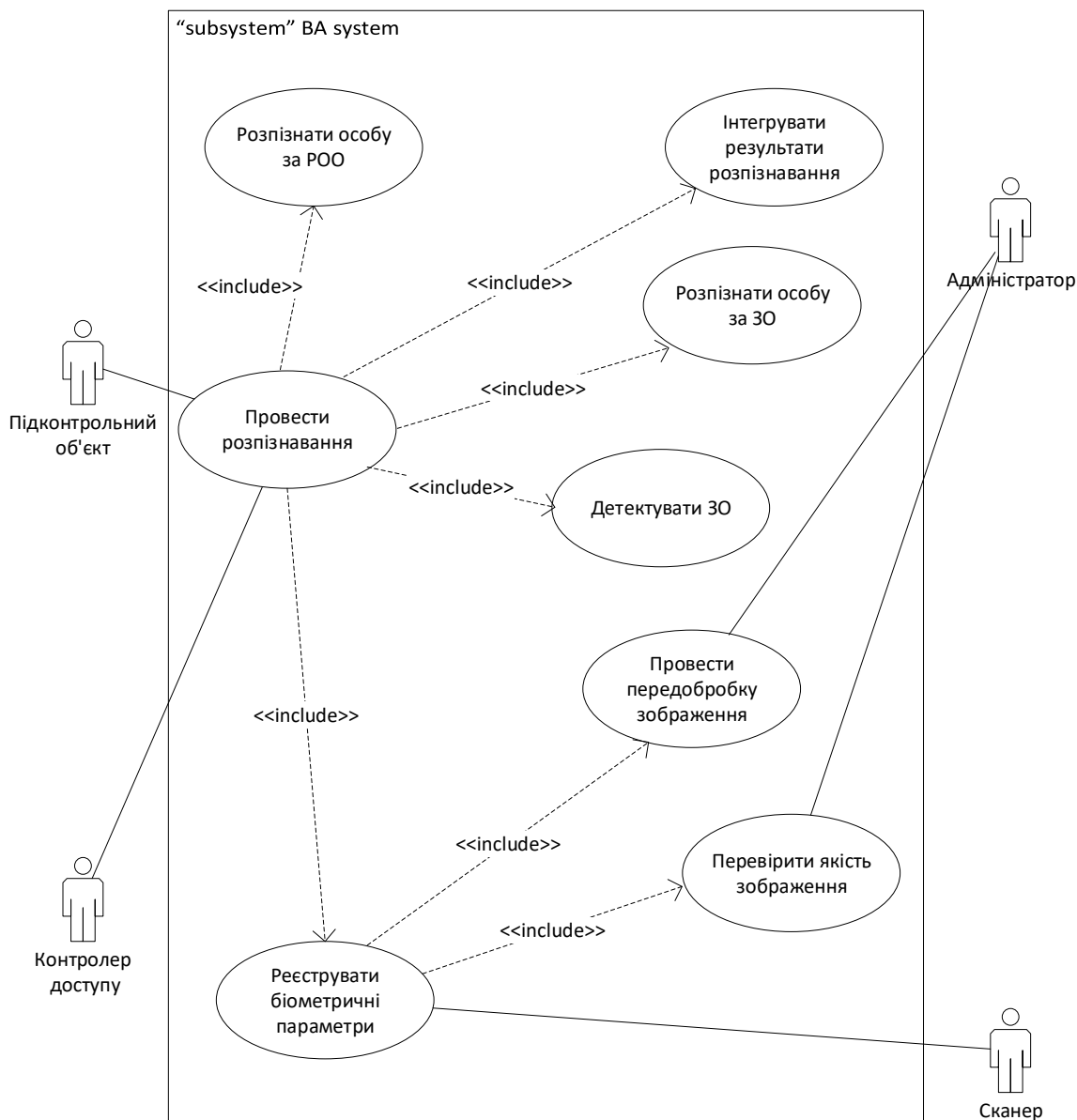


Рис. 4.1. Базовий варіант діаграми прецедентів

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

Прецедент «Провести розпізнавання» включає в себе прецеденти: «Розпізнати особу за ЗО», «Розпізнати особу за РОО», «Інтегрувати результати

розпізнавання», «Виділити ЗО», «Реєструвати біометричні параметри». Функціонал означених прецедентів відповідає їх назвам.

Прецедент «Реєструвати біометричні параметри» включає прецеденти:

– «Перевірити якість зображення» – прецедент реалізується, оскільки розпізнавання особи представника персоналу ОКІ здійснюється лише за умови відповідної якості вхідного зображення.

– «Провести передобробку зображення» – забезпечує нормалізацію кольорових характеристик зображення, узгодження розмірів зображення з розмірами вхідних полів НММ, що використовуються в системі БА, та фільтрацію шуму.

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 системи БА розглядаються додаткові можливості, пов'язані з семантичною сегментацією ЗО. Показаний на рис. 4.2 розширений варіант діаграми включає всі прецеденти базового рівня, а також прецеденти, що розширюють функціональні можливості даної системи аутентифікації.

Додані прецеденти та їх призначення:

- «Виділити ЗО» – виділення ЗО за допомогою прямокутної рамки.
- «Провести семантичну сегментацію» – передбачає визначення масок, що відповідають природнім контурам ЗО та РОО.
- «Отримати інтегроване зображення» – інтеграція отриманих масок з початковим ЗО, в результаті якої отримуються не перекриті завадами ЗО та РОО.
- «Отримати фонове зображення» – інтеграція отриманих масок з початковим ЗО, в результаті якої отримується зображення, на фоні якого було зареєстроване початкове ЗО.

Остаточний варіант діаграми прецедентів, що представлено на рис. 4.3, розширює модель системи, подану на другому рівні деталізації (рис. 4.2), за

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

– «Розпізнати спуфінг-атаки за артефактами довкілля», 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 визначення інтенсивності відображення на 3D семи базових емоцій, що асоціюється з прецедентом «Розпізнати емоції». Отже, остаточний варіант діаграми прецедентів забезпечує формалізований опис функціональних вимог не лише до процесів розпізнавання особи представника персоналу ОКІ за 3D та РОО, як це було в розширеному варіанті, а й вимог до розпізнавання емоцій та 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.

Таким чином, в результаті проведених досліджень розроблено UML-діаграму прецедентів, яка відображає формалізований опис функцій мультимодальної системи БА за 3D та РОО, що є ключовим етапом проєктування та формує основу для її подальшої програмно-апаратної реалізації. До основних переваг розробленої діаграми слід віднести наявність формалізованого опису функціональних вимог щодо семантичної сегментації 3D та необхідності розпізнавання спуфінг-атак за природністю емоцій, відображених на обличчі людини, та за артефактами зовнішнього оточення, що забезпечує підґрунтя для підвищення ефективності системи БА в ракурсі впровадження в неї нових відповідних сервісів.

4.2. Експериментальна оцінка ефективності методу побудови неймережевих засобів семантичної сегментації зображення обличчя

Відповідно до рекомендацій [96, 99, 147], ефективність запропонованого в п. 3.2 методу побудови НМЗ семантичної сегментації ЗО при БА оцінювалася на основі порівняння точності і обчислювальної складності побудованого на його основі НМЗ з відповідними показниками відомих НМЗ аналогічного призначення. Крім того оцінювалася ресурсоемність процесу побудови НМЗ у випадку застосування запропонованого методу та у випадку емпіричного підбору архітектурних параметрів.

Зважаючи на результати [153, 167, 168], прийнято, що умови застосування НМЗ характеризуються наступними параметрами: максимально доступний обсяг пам'яті для зберігання параметрів моделі $V_{CR}^d=100$ МБ, прийнятний обсяг пам'яті $V_{CR}^s=50$ МБ, допустимий термін процесу семантичної сегментації $\Delta_{Tss}=200$ мс, мінімально допустиме значення показника точності сегментації Jaccard Index (IoU) $\Delta_A=0,9$, допустима кількість епох навчання $\Delta_{TL}=100$. Інші умови застосування співвіднесено з характеристиками використаного набору навчальних даних LaPa, доступного за посиланням <https://www.kaggle.com/datasets/dnayan/human-face-segmentation>. В даному наборі міститься 22200 прикладів, що відповідають анотованим ЗО. Анотації представлені у вигляді піксельних масок, де кожному пікселю зображення відповідає мітка класу від 0 до 10, що позначає належність до певної області обличчя. При цьому до класу, який відповідає фону зображення, віднесено всі об'єкти, що не належать до ЗО.

Побудований за допомогою запропонованого методу НМЗ базується на НММ AFSegNet, що має симетричну енкодер-декодерну архітектуру типу Attention U-Net++, на основі блоків VGG. При побудові використано комп'ютерну програму [143] (лістинг наведено в додатку Б). Енкодер складається з п'яти рівнів, кожен з яких містить 2 згорткові блоки ($\text{Conv2D} \rightarrow \text{BatchNorm} \rightarrow \text{ReLU}$), завершені операцією MaxPooling2D , що в сумі дає 10 основних згорткових шарів у енкодері. Декодер також має п'ять рівнів з

відповідною кількістю транспонованих згорткових шарів (Conv2DTranspose) та згорткових блоків після кожного об'єднання (Concatenate), що формує ще близько 10 згорткових шарів. Додатково, у декодері реалізовані механізми уваги через операції Add і Multiply, які створюють залишкові та елементно-зважені з'єднання. Вихідний шар має форму $(128 \times 128 \times 11)$ і забезпечує піксельну багатокласову сегментацію обличчя. Загальна кількість параметрів - близько 8,8 млн, що відповідає приблизно 33,7 МБ пам'яті при зберіганні у форматі float32 (4 байти на параметр).

Зазначимо, що на початку виконання методу в якості базової була використана нейромережева модель Attention U-Net++ з енкодером та декодером на базі VGG-16. Модифікація параметрів енкодера та декодера здійснена внаслідок виконання шостого етапу запропонованого методу, асоційованого з запуском процедури адаптації архітектурних параметрів до умов застосування. При цьому, відповідно до етапу 5, процедура навчання характеризувалась наступними значеннями основних параметрів: функція втрат - Categorical Cross-Entropy; оптимізатор - Adam; learning rate = 0,0005; Dropout=0,3. Процес навчання моделі AFSegNet проілюстровано за допомогою рис. 4.4 та рис 4.5, на яких показано графіки залежностей значень Loss (рис. 4.4) і IoU (рис. 4.5) від кількості епох навчання на тренувальній та на валідаційній вибірках.

Аналіз наведених графіків свідчить про стабільну збіжність навчання, відсутність перенавчання та високу здатність моделі до узагальнення, що підтверджується низькими значеннями функції втрат (Loss) і високими значеннями показника IoU як на тренувальній, так і на валідаційній вибірці. Зокрема, модель досягла точності сегментації за метрикою Intersection over Union (IoU) на рівні 96,67 % на тренувальній вибірці та 93,12 % на валідаційній вибірці, що також підтверджує узгодженість архітектурних параметрів моделі з умовами застосування. Верифікація моделі AFSegNet на тестовій вибірці показала, що точність сегментації за показником IoU становить приблизно 0,92, що перевищує встановлений пороговий рівень і підтверджує відповідність побудованого на її основі НМЗ поставленим вимогам.

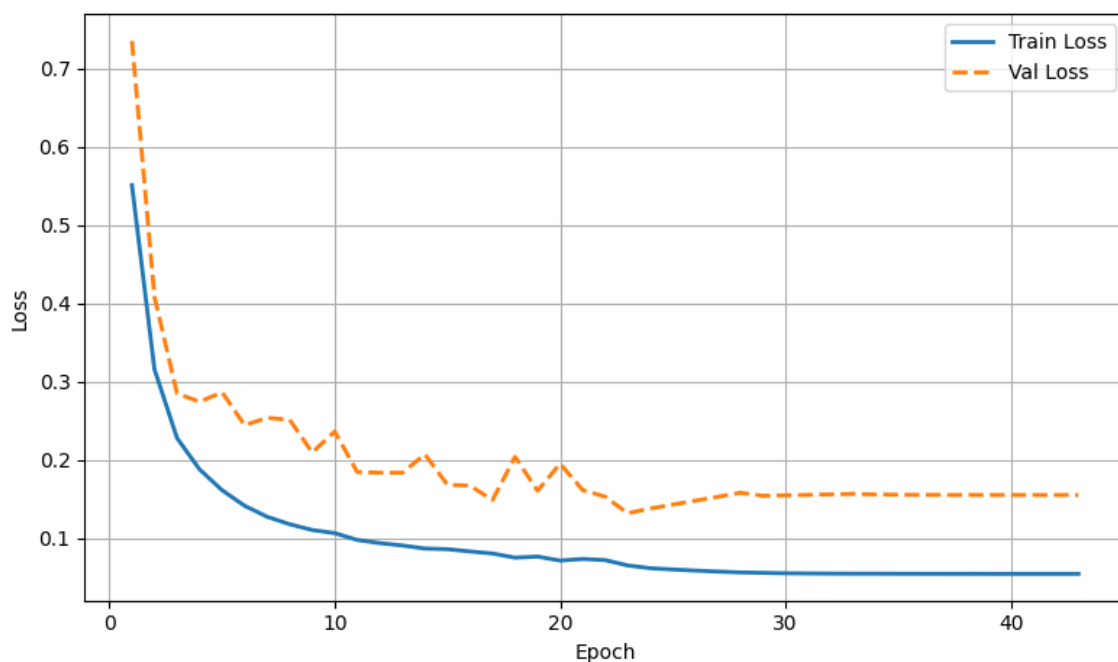


Рис. 4.4. Графіки залежності значень Loss від кількості епох навчання на тренувальній та валідаційній вибірках

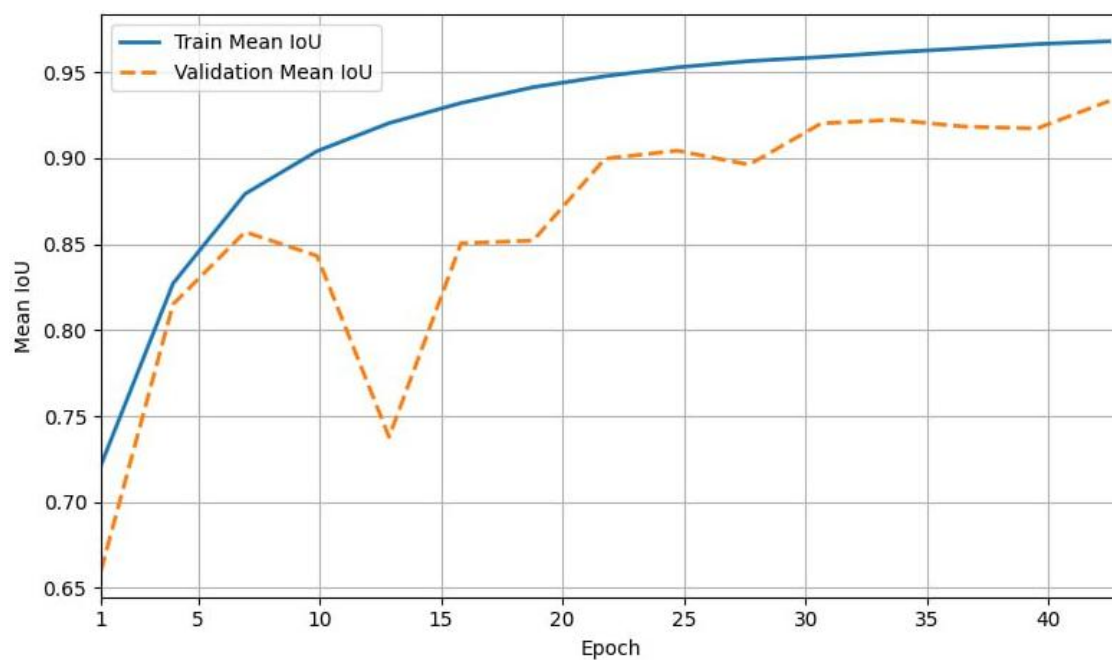


Рис. 4.5. Графіки залежності значень IoU від кількості епох навчання на тренувальній та валідаційній вибірках

Для порівняння з відомими рішеннями проведено оцінювання точності сегментації тестових даних, виконане з використанням НМЗ, побудованих на основі вільнодоступних НММ BiSeNet V1 та Selfie Segmentation. Отримані

показники точності і ресурсоемності для розробленого НМЗ та НМЗ на основі вільнодоступних НММ, що застосовувалися для порівняння, наведено в табл.4.1.

Таблиця 4.1

Порівняння точності і ресурсоемності нейромережових засобів сегментації
обличчя

Назва моделі	Кількість параметрів	Точність сегментації
AFSegNet	$\approx 9 \times 10^6$	0,92
BiSeNet V1	$\approx 12 \times 10^6$	0,83
Selfie Segmentation	$\approx 1,9 \times 10^6$	0,75

Як свідчать дані, наведені в табл. 4.1, точність розробленого НМЗ відповідає вимогам системи БА ОКІ та перевищує точність відомих НМЗ семантичної сегментації. При цьому хоча ресурсоемність AFSegNet і перевищує ресурсоемність Selfie Segmentation, однак знаходиться в допустимих межах. Зазначимо, що визначення прийнятних значень архітектурних параметрів розробленої НММ AFSegNet призвело до необхідності реалізації 6 серій експериментальних досліджень, кожна з яких вимагала проведення 50 епох навчання НММ. Слід відзначити, що на основі оціночних експертних висновків, у випадку використання загальноновживаних підходів для визначення архітектури НММ, визначення архітектурних параметрів моделі семантичної сегментації призвело б до необхідності реалізацій 50-80 експериментів, кожен з яких пов'язаний з необхідністю проведення близько 50 епох навчання НММ. Це пояснюється необхідністю оцінювання ефективності 5–8 базових архітектур та від 10 до 20 варіантів конфігурацій архітектурних параметрів для кожної з них. Таким чином, застосування розробленого методу дозволяє приблизно на порядок зменшити кількість експериментальних досліджень, пов'язаних з визначенням архітектурних параметрів НММ, на якій базується НМЗ. Ілюстрацією застосування розробленого НМЗ для сегментації чоловічого та жіночого ЗО з метою їх обробки перед подачею в інші модулі системи БА являються рис. 4.6-

4.11, на яких показано: оригінальні зображення обличчя (рис. 4.6), зображення, сегментовані за допомогою розробленого НМЗ AFSegNet (рис. 4.7), зображення, сегментовані за допомогою НМЗ на основі моделі BiSeNet V1 (рис. 4.8) та моделі Selfie Segmentation (рис. 4.9), ЗО, виділені прямокутною рамкою за допомогою YOLOv8n (рис. 4.10), а також ЗО, отримані внаслідок інтеграції оригінального зображення з маскою, створеною за допомогою AFSegNet (рис. 4.11).



Рис. 4.6. Зображення обличчя, що підлягають сегментації

Зазначимо, що на рис. 4.6 показано синтетичні ЗО чоловіка та жінки,

згенеровані за допомогою вільнодоступних засобів штучного інтелекту. Крім незашумлених, на рис. 4.6 показано 30 частково перекриті такими об'єктами, як борода, головний убір, медична маска, сонцезахисні (темні окуляри), прозорі окуляри, сережки та комбінацією вказаних об'єктів.

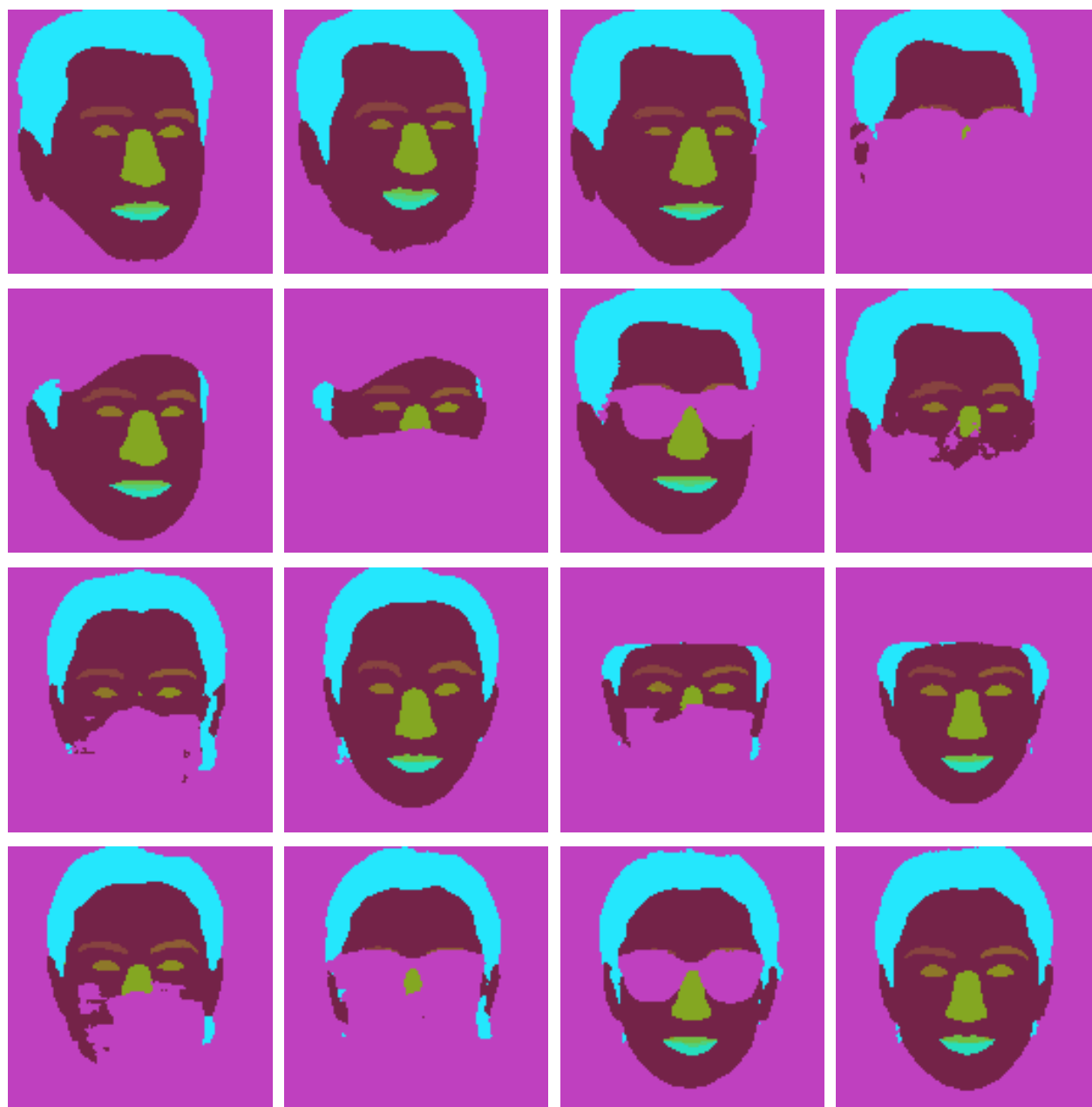


Рис. 4.7. Зображення обличчя, сегментовані за допомогою розробленого HM3 AFSegNet

Як свідчить візуальний аналіз рис. 4.6-4.7, у порівнянні з загальновідомими HM3 BiSeNet V1 та Selfie Segmentation, розроблений HM3 AFSegNet дозволяє

якісніше забезпечити вимоги до результату семантичної сегментації ЗО. Порівняно з Selfie Segmentation, отримана за допомогою AFSegNet маска точніше відповідає природним контурам обличчя, тоді як результати сегментації за допомогою BiSeNet V1 виявляються надлишковими, охоплюючи області, які в подальшому не використовуються при БА.

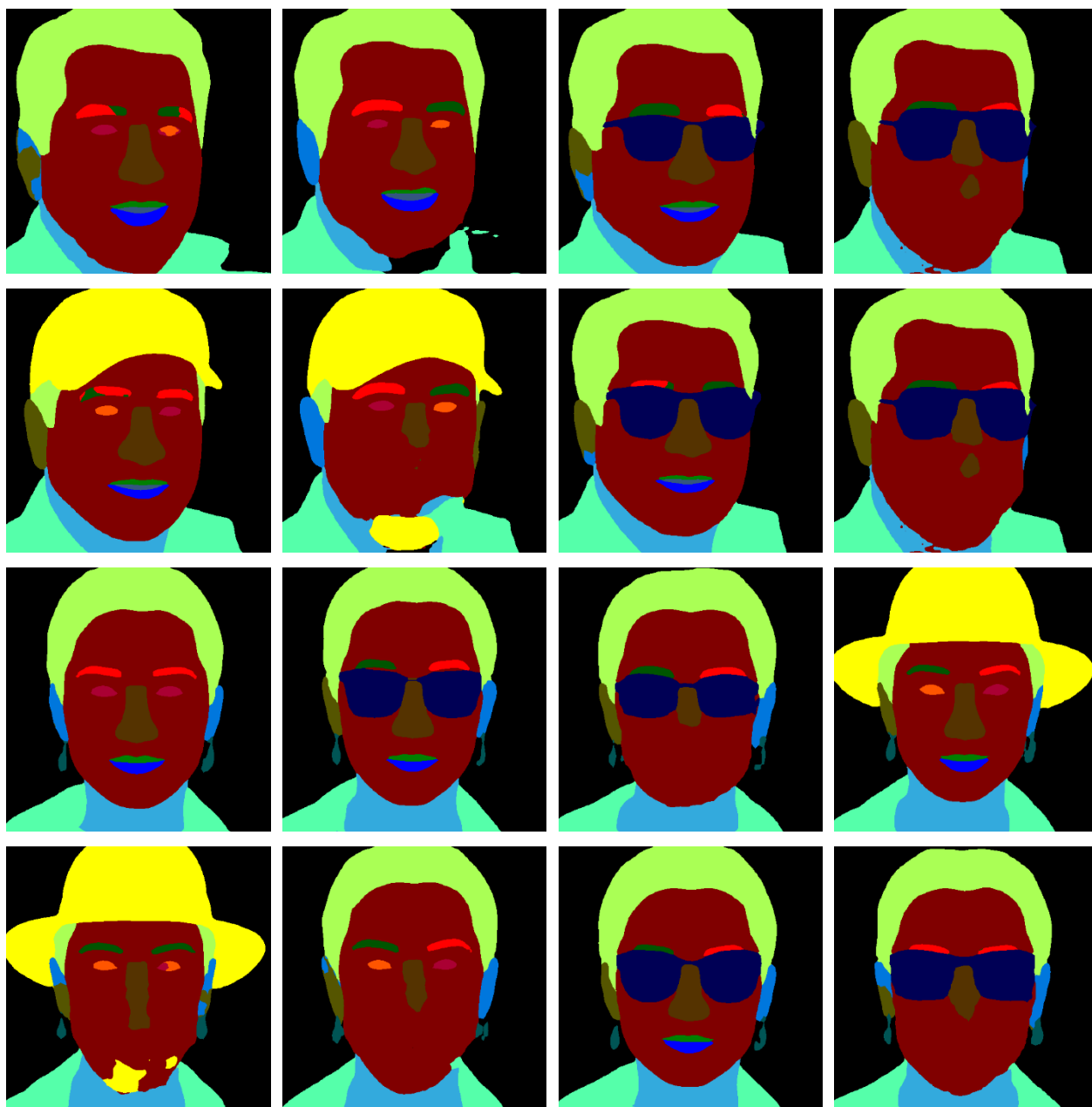


Рис. 4.8. Зображення обличчя, сегментовані за допомогою HM3 на основі BiSeNet V1

При цьому HM3 BiSeNet V1 не у всіх випадках забезпечує коректну

сегментацію брів; відносить медичну маску до ЗО, хоча і не сегментує верхню та нижню губу; однаково сегментує прозорі та сонцезахисні окуляри, що не дозволяє виділити зображення очного яблука.

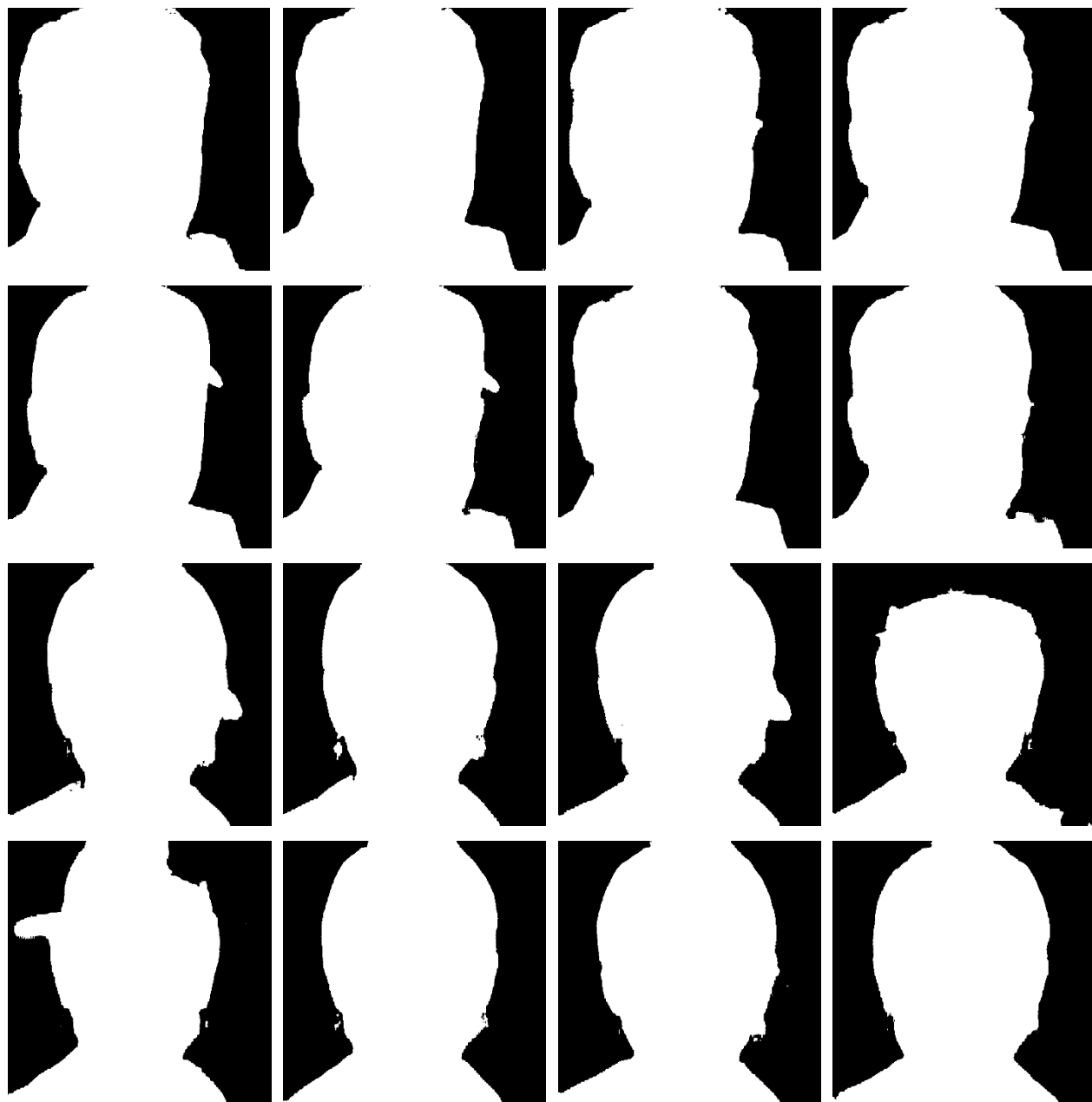


Рис. 4.9. Зображення обличчя, сегментовані за допомогою НМЗ на основі Selfie Segmentation

Щодо Selfie Segmentation, то застосування такого НМЗ не дозволяє виділити такі важливі частини ЗО, як очі, рот та ніс, а також не забезпечує сегментацію головного убору, медичної маски та як прозорих, так і

сонцезахисних окуляр. Ці об'єкти, хоча безпосередньо і не використовуються при БА, однак мають вагоме значення для подальшого аналізу позиціонування голови особи, яка проходить процедуру автентифікації, що безпосередньо впливає на точність розпізнавання та виявлення спуфінг-атак.



Рис. 4.10. Зображення обличчя, виділені прямокутною рамкою за допомогою YOLOv8n

Крім того, порівняння показаних на рис. 4.10 результатів виділення обличчя за допомогою прямокутної рамки із показаними на рис. 4.11

зображеннями, які являються інтеграцією вхідних зображень із масками отриманими за допомогою розробленого НМЗ AFSegNet свідчить про те, що застосування семантичної сегментації дозволяє суттєво зменшити негативний вплив фонові варіативності та наявності завад на ЗО.

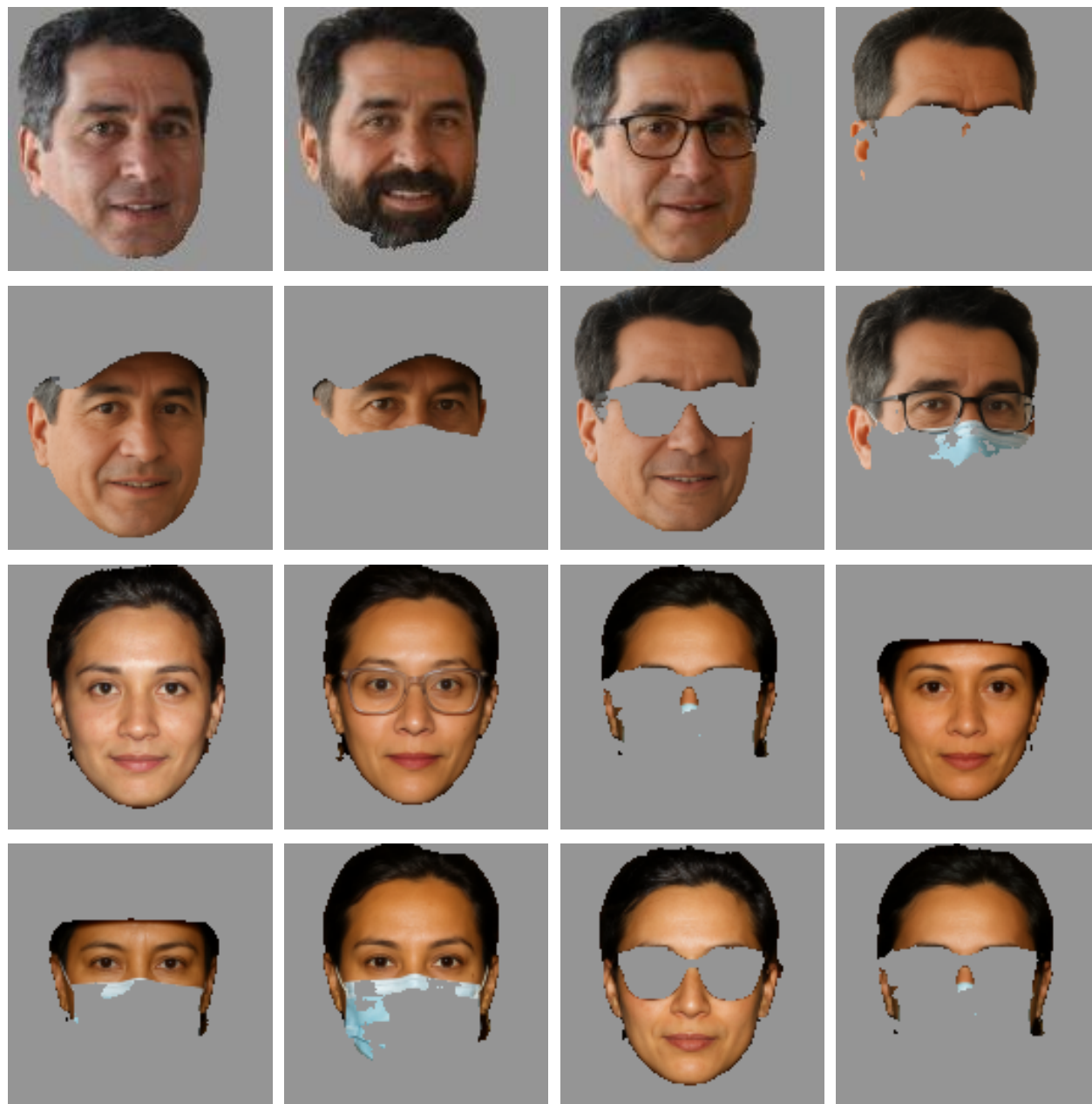


Рис. 4.11. Зображення обличчя отримані внаслідок інтеграції оригінального зображення з маскою, створеною за допомогою AFSegNet

Таким чином, отримані експериментальні результати підтверджують, що НМЗ AFSegNet, розроблений в результаті виконання методу, забезпечує вищу

точність семантичної сегментації ЗО порівняно з відомими моделями і дозволяє зменшити вплив різноманіття фону та завад, що підвищує якість вхідних даних, які в подальшому використовуються для розпізнавання особи.

Також результати експериментів вказують на те, що застосування розробленого НМЗ дозволяє приблизно в 1,2-1,25 рази підвищити точність виділення кордонів обличчя порівняно з поширеними НМЗ, які виділяють область обличчя прямокутною рамкою, внаслідок чого забезпечується можливість зменшення похибки розпізнавання особи, що підлягає автентифікації.

4.3. Експериментальна оцінка ефективності нейромережевого методу біометричної автентифікації за зображенням обличчя та райдужною оболонкою ока в інформаційних системах об'єктів критичної інфраструктури

Зважаючи на рекомендації [50, 98, 146], проведено експериментальні дослідження, спрямовані на оцінку ефективності впровадження в систему БА НМЗ, що базуються на рішеннях, запропонованих в п. 2.2 (крім рішень, що стосуються семантичної сегментації) та дослідження, спрямовані на оцінку ефективності описаного в п. 3.3 методу в цілому. Таким чином, проведено три серії експериментів, в яких досліджено:

- Ефективність НМЗ на базі Siamese Network та Two_channel Networks для розпізнавання особи за РОО та для розпізнавання спуфінг-атак за артефактами зовнішнього оточення.

- Ефективність застосування засобів семантичної сегментації в процесі розпізнавання особи за ЗО та РОО.

- Ефективність НМЗ на базі PNN для розпізнавання спуфінг-атак за природністю емоцій.

Ілюстрацією процесу проведення першої серії експериментів являються рис. 4.12-4.17. Так, на рис. 4.12 та 4.13 показано структурні схеми розроблених НММ. В розробленому варіанті Siamese Network в якості базису окремих гілок

використано LeNet з 4 шарами згортки та 4 шарами пулінгу, адаптовану до аналізу одноканальних зображень розміром 150×150 пікселів, для якої $N_Y=256$.

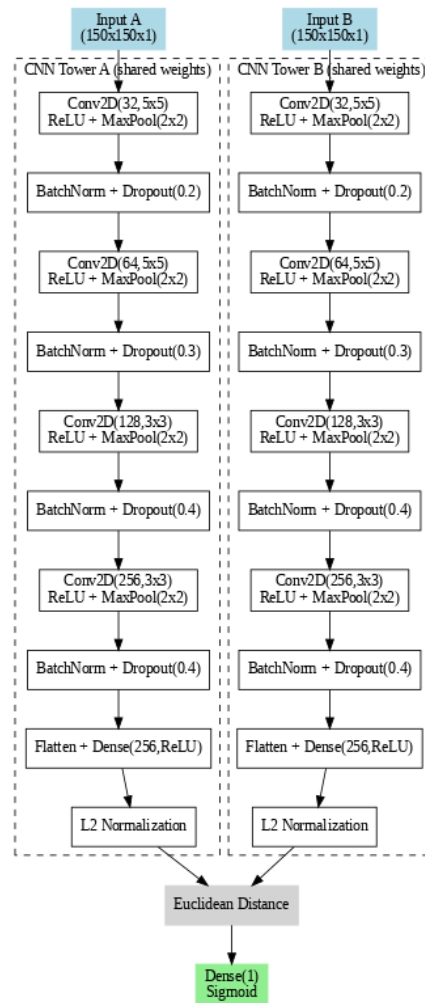


Рис. 4.12. Структура розробленої моделі типу Siamese Network

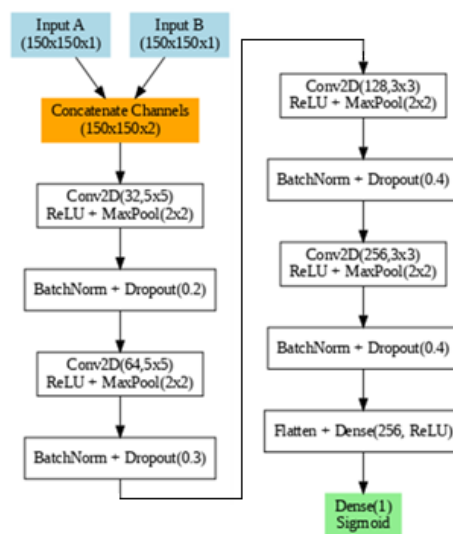


Рис. 4.13. Структура розробленої моделі типу Two_channel Network

Відмінністю розробленої HMM типу Two_channel Network являється адаптація структури до вхідного поля 150×150 пікселів. Для навчання мереж використано набір даних CASIA-Iris-Thousand, доступний за посиланням <https://www.kaggle.com/datasets/sondosaabed/casia-iris-thousand>. Набір даних містить 20000 RGB-зображень 1000 суб'єктів відеореєстрації (по 10 зображень на праве та ліве око). Кожне одноканальне зображення розміром 640×480 пікселів представлене в окремому jpg-файлі. Перед подачею на вхід HMM розміри зображення підлягали масштабуванню методом бікубічної інтерполяції. Графіки зміни показників Accuracy та Loss для розроблених HMM Siamese Network та Two_channel Network, показані на рис. 4.14-4.17.

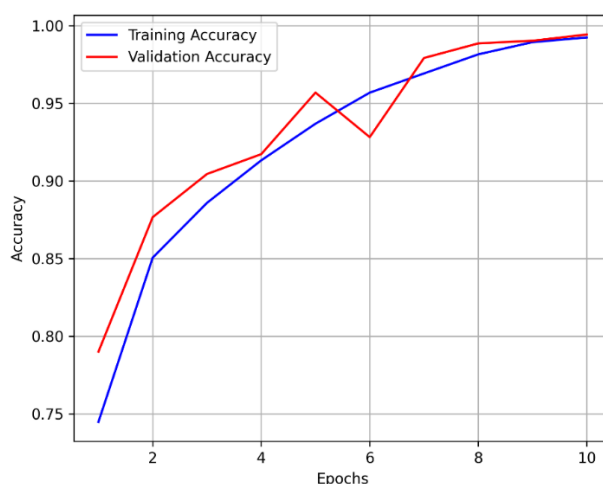


Рис. 4.14. Графіки залежності Accuracy від кількості епох навчання для Siamese Network

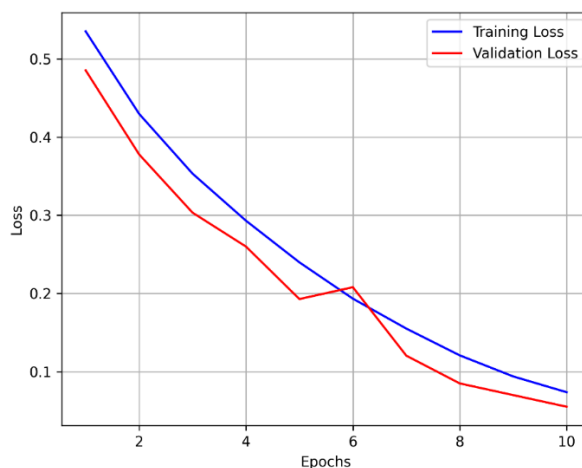


Рис. 4.15. Графіки залежності Loss від кількості епох навчання для Siamese Network

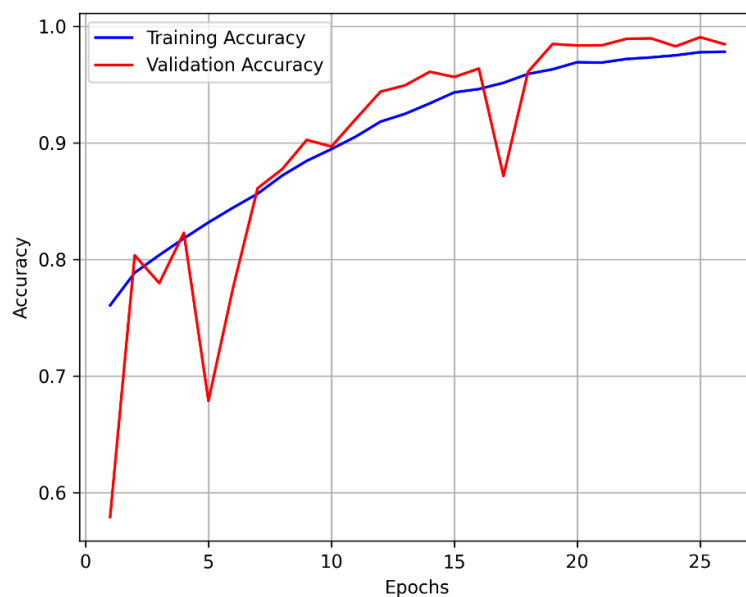


Рис. 4.16. Графіки залежності Accuracy від кількості епох навчання для Two_channel Network

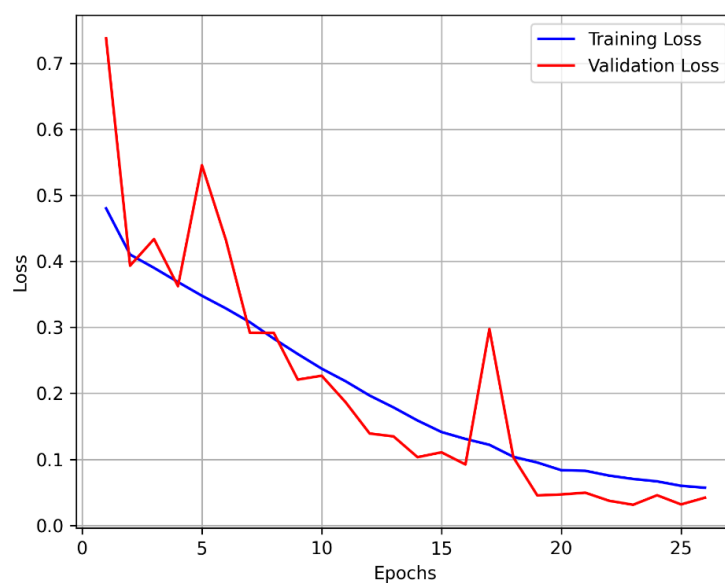


Рис. 4.17. Графіки залежності Loss від кількості епох навчання для Two_channel Network

Як свідчать показані на рис. 4.14-4.17 графіки, процес навчання мереж Siamese Network та Two_channel Network здійснюється за відносно невелику кількість епох. Так, для Siamese Network вже після 10 епохи навчання на валідаційних даних $Loss \approx 0,04$, $Accuracy \approx 0,996$, а для Two_channel Network на валідаційних даних $Loss \approx 0,04$, $Accuracy \approx 0,995$ досягається після 25 епохи

навчання. Досягнуті значення Accurasy відповідають значенням коефіцієнту рівної ймовірності помилок $EER=0,004$ та $EER=0,005$.

В базовому випадку вказані значення Accurasy відповідають оцінкам подібності (r_{IR}) між РОО особи, що підлягає розпізнаванню, та РОО легітимних представників.

Враховуючи, що відповідно до даних п. 2.2, при застосуванні FaceNet $r_{FC} = 0,9963$, розраховане за допомогою (3.21) значення інтегрованої оцінки подібності при застосуванні Siamese Network $r_{RR} = 0,99621$, а при застосуванні Two_channel Network $r_{RR} = 0,99591$. Зазначимо, що досягнуті показники співвідносяться із заявленими показниками найбільш сучасних НМЗ аналогічного призначення [7, 41, 51, 60, 66]. Для проведення експериментів, пов'язаних з застосуванням Siamese Network та Two_channel Networks для детектування спуфінг-атак за артефактами зовнішнього оточення сформовано набір даних, в якому представлено зображення фонових об'єктів, отриманих після вилучення із відеокадрів 30, обмеженого прямокутною рамкою. Отриманий набір даних містив 1000 RGB-зображень розміром 250x250 пікселів з роздільною здатністю 96 dpi і глибиною кольору 24 біт.

В результаті експериментів визначено, що після 20 епох навчання для Siamese Network та Two_channel Networks значення показника Accurasy дорівнює близько 0,99, що свідчить про достатньо високу точність порівняння зображень фонових об'єктів, а відповідно вказує на можливість детектувати спуфінг-атаки на основі порівняння зображення зовнішнього оточення, отриманого при відеореєстрації, з очікуваним (еталонним) зображенням зовнішнього оточення. Таким чином, експериментальні дослідження підтвердили доцільність застосування Siamese Network та Two_channel Network для визначення легітимності представника персоналу ОКІ за рахунок розпізнавання РОО та для детектування спуфінг-атак за артефактами зовнішнього оточення. Разом з тим, порівняння динаміки параметрів навчання Siamese Network та Two_channel Network свідчать про те, що з точки зору оперативності навчання більш ефективною являється мережа Siamese Network.

При цьому обчислювальна ресурсоемність Two_channel Network приблизно в 15 разів менша, ніж у Siamese Network, що є перевагою Two_channel Network.

Разом з тим, до переваг Siamese Network слід віднести гнучкість концепції її побудови, яка потенційно дозволяє значно підвищити її ефективність за рахунок використання в якості базису окремих гілок мережі (рис. 4.12) найбільш передових нейромережових архітектур, адаптованих до аналізу ЗО. Наприклад, в блоці CNN замість традиційно використаної архітектури типу LeNet можливо використати архітектуру типу MobileNet, що було підтверджено за допомогою оціночних експериментальних досліджень. Таким чином, за необхідності оперативного розгортання системи БА пріоритет слід віддати мережі Siamese Network, однак при жорстких обмеженнях щодо обчислювальної ресурсоемності доцільно використати Two_channel Network.

Експерименти, пов'язані із дослідженням запропонованих рішень в області застосування засобів семантичної сегментації, полягали у порівнянні точності розпізнавання особи у випадку подачі на НМЗ сегментованого та несегментованого ЗО. В якості засобу розпізнавання використано НМЗ на базі FaceNet, на вхід якої подавались оригінальні ЗО, представлені у вільнодоступному наборі даних LFW (<https://vis-www.cs.umass.edu/lfw/>), що були частково спотворені за рахунок накладання типових завад, та ЗО, отримані внаслідок інтеграції оригінальних зображень з маскою, створеною за допомогою AFSegNet. Результати експериментів вказують, що при застосуванні засобів семантичної сегментації похибка розпізнавання зменшується приблизно в 1,1–1,15 рази, що підтверджує ефективність запропонованих рішень.

З метою узагальнення результатів оцінки ефективності рішень щодо розпізнавання особи та використання засобів семантичної сегментації, на основі правила прийняття рішення (3.21) було побудовано графіки залежності ймовірності помилок FAR та FRR від порогу прийняття рішення у лінійній (рис. 4.18) та напівлогарифмічній (рис. 4.19) шкалі. Крім того, побудовано показаний на рис. 4.20 графік залежності ймовірності хибного відхилення (FRR) від ймовірності хибного допуску (FAR) у логарифмічному масштабі (DET-крива).

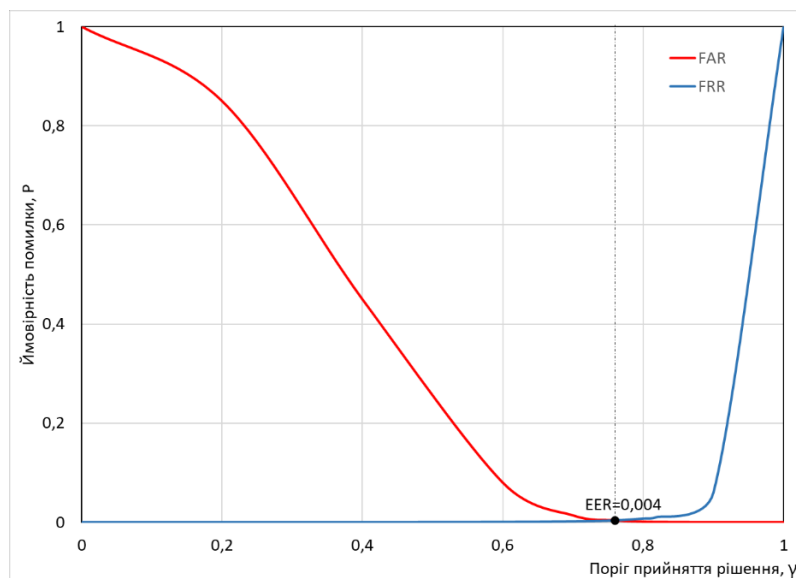


Рис. 4.18. Графіки залежності FAR та FRR від значення порога прийняття рішення

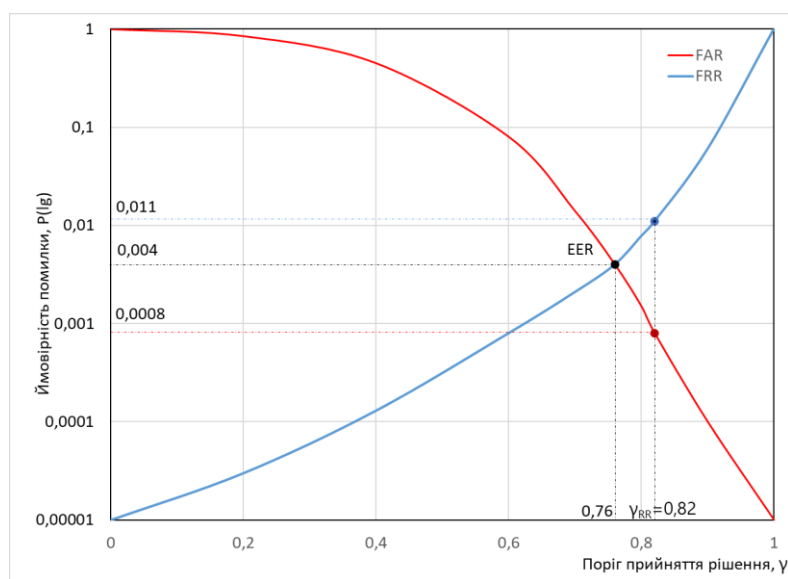


Рис. 4.19. Графіки залежності FAR та FRR від значення порога прийняття рішення у напівлогарифмічному масштабі

Базуючись на аналізі означених графіків та нормативних вимогах до систем БА на ОКІ, значення порогу прийняття рішення встановлено на рівні $\gamma_{RR} = 0,82$. Обраний поріг прийняття рішення знаходиться у стабільній зоні DET-кривої, вище точки рівної помилки ($EER = 0,004$, що відповідає значенню порогу 0,76), забезпечуючи дотримання нормативних вимог щодо ймовірності несанкціонованого доступу та значний відступ від зони деградації системи.

Додатково на основі експериментальних даних чисельним методом розраховано інтегральний показник площі під ROC-кривою, який становить $AUC \approx 0,999$.

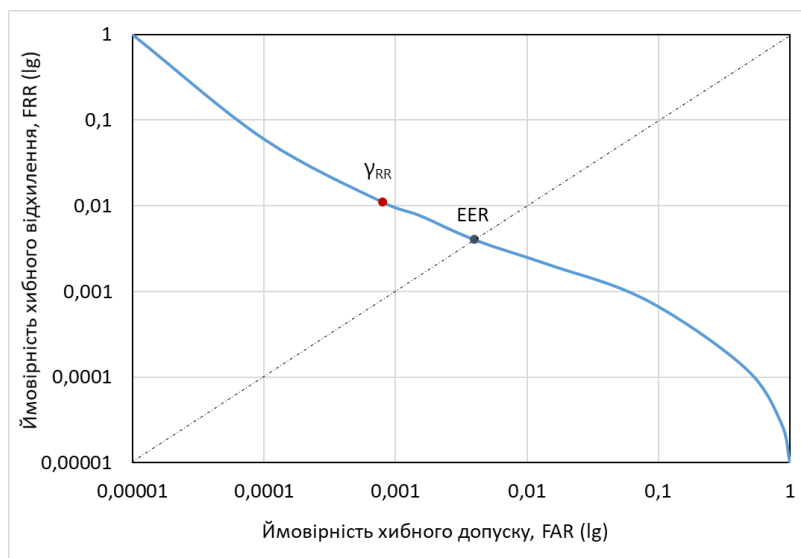


Рис. 4.20. Графік залежності ймовірності хибного відхилення (FRR) від ймовірності хибного допуску (FAR) у логарифмічному масштабі (DET-крива)

Сукупність отриманих результатів, а саме: показники $FAR \approx 0,0008$ та $FRR \approx 0,011$ у робочій точці, форма DET-кривої, що свідчить про високу роздільну здатність системи, а також високе значення показника AUC вказують на дотримання нормативних вимог щодо систем БА на ОКІ та співвідносяться з показниками передових рішень у цій галузі [26, 50, 131, 152, 159].

В наступних експериментах досліджено можливість розпізнавання спуфінг-атак на основі нейромережевого аналізу природності емоцій. Відповідно до результатів п. 2.1, 2.2, 3.3, в якості базису нейромережевого аналізатора використано НММ РNN, на вхід якої передбачено подавати інтенсивність 7 базових емоцій, що відображаються на ЗО на протязі 10 послідовних кадрів. Використовуючи дані [65, 70], сформовано навчальну вибірку обсягом 1200 навчальних прикладів, що відповідають емоціям людини у спокійному стані, стані помірної емоційної напруженості, у стані алкогольного та наркотичного сп'яніння, при перебуванні під стресом. Крім того, враховуючи результати [36, 37] сформовано навчальні приклади, що відображають раптові зміни емоційного

стану, які відповідають змінам інтенсивності більше ніж на 0,4 за один кадр, та аномально тривале збереження емоційного стану, які відповідають змінам інтенсивності менше ніж на 0,15 за кадр. Навчальні приклади, що відповідають спокійному стану, помірній емоційній напруженості та нормальній поведінці людини, марковані як відсутність спуфінг-атаки, а приклади, що відповідають стану алкогольного або наркотичного сп'яніння, підвищеному стресу, а також будь-якому неадекватному емоційному стану, – як спуфінг-атака. Навчальна вибірка розділена на тренувальну та валідаційну. Кількість тренувальних прикладів 1000, кількість валідаційних прикладів – 200. При цьому 500 тренувальних прикладів відповідають класу відсутності спуфінг-атаки, а 500 прикладів – класу наявності спуфінг-атаки. У валідаційній вибірці також у рівних пропорціях представлено два вказаних класи. Враховуючи наведені передумови, структура побудованої НММ типу PNN (див. рис. 4.21) характеризується такими параметрами: кількість входних нейронів (відповідають інтенсивностям базових емоцій) – 70, кількість нейронів у шарі образів – 1000 (відповідають навчальним прикладам), кількість нейронів у шарі додавання – 2 (відповідають класам відсутності та наявності спуфінг-атак).

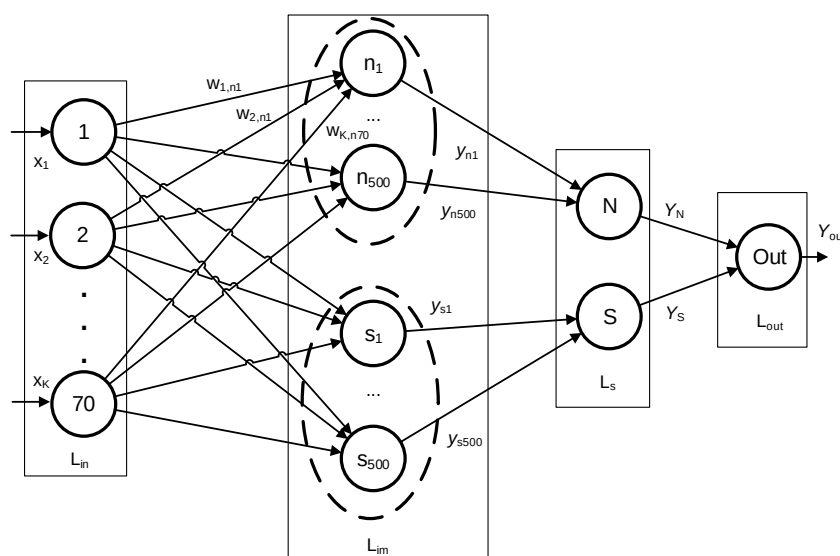


Рис. 4.21. Структура мережі PNN для розпізнавання спуфінг-атак за природністю емоцій

На рис. 4.21 використано наступні позначення: входний шар, шар образів,

шар додавання та вихідний шар – $L_{in}, L_{im}, L_s, L_{out}$; n, s – нейрони шару образів, що відповідають прикладам, які співвідносяться з класами відсутності та наявності спуфінг-атак; w_{ij} – ваговий коефіцієнт між i -им вхідним нейроном та j -им нейроном шару образів; y – вихідний сигнал нейрону шару образів; N, S – нейрони, що відповідають класам відсутності та наявності спуфінг-атак; Y – вихідний сигнал нейрону шару додавання; Y_{out} – вихідний сигнал мережі.

В результаті експериментів визначено, що для розробленої НММ на тестових даних значення показника Accuracy $\approx 0,99$. Це свідчить про достатньо високу точність класифікації емоційного стану, а відповідно вказує на можливість детектування спуфінг-атак за природністю емоцій. На заключному етапі досліджень проведено оцінювання ефективності розробленої системи БА ОКІ. Відповідно до положень п.1.2, при оцінюванні використано критерії, наведені в табл.1.1 та табл. 1.2. Результати оцінювання наведені в табл. 4.2.

Таблиця 4.2

Значення критеріїв ефективності розробленої системи розпізнавання

Позначення	Опис	Значення
Критерії ефективності основної групи		
A_1	Рівень точності розпізнавання особи	0,9
A_2	Стійкість до спуфінг-атак	0,9
A_3	Оперативність розпізнавання особи	0,7
A_4	Оперативність розробки системи розпізнавання	0,9
Критерії ефективності додаткової групи		
B_1	Стійкість до розпізнавання в умовах завад на ЗО	0,9
B_2	Стійкість до зміни умов відеореєстрації	0,7
B_3	Пристосованість до аналізу кадру, що містить декілька ЗО	0,9
B_4	Ресурсоемність процедури розпізнавання	0,5
B_5	Ресурсоемність розробки системи розпізнавання	0,9
B_6	Можливість розпізнавання емоцій	0,8

Крім обґрунтованого використання в процесі БА найбільш ефективних НМЗ, високі значення критеріїв ефективності пояснюється застосуванням запропонованих рішень, що дозволяють:

- підвищити точність виділення кордонів обличчя з урахуванням наявності у відеокадрі можливих завад та декількох ЗО (RetinaFace; AFSegNet, розроблена на основі запропонованої моделі та методу семантичної сегментації);
- забезпечити точність розпізнавання особи за РОО, співрозмірну із точністю найбільш досконалих засобів аналогічного призначення (IrisParseNet; HMM, розроблені на базі Siamese Network та Two_channel Networks);
- детектувати спуфінг-атаки за візуальними артефактами, за живучістю, за артефактами зовнішнього оточення та за природністю емоцій (DeepPixBiS; ModifiedConvNeXtLarge; FaceEmotion_ID; HMM, розроблені на базі Siamese Network, Two_channel Networks та PNN);
- підвищити ефективність розробки НМЗ завдяки модульній структурі, побудованій на основі вільнодоступних та ефективних рішень (RetinaFace, IrisParseNet, DeepPixBiS, ModifiedConvNeXtLarge, FaceEmotion_ID);
- адаптувати параметри попередньої обробки до показників відображення поточного відеокадру (процедури, що відповідають реалізації першого та другого етапу запропонованого методу БА персоналу ОКІ);
- реалізувати розпізнавання емоцій (FaceEmotion_ID).

Середнє значення критеріїв A_3 та B_4 не є критичним обмеженням, оскільки компенсується використанням в більшості систем БА ОКІ сучасного апаратного забезпечення.

Порівняння отриманих оцінок з даними наведеними в табл. 1.3 та табл. 1.4 вказує на те, що за критеріями, які характеризують рівень точності розпізнавання, стійкості до спуфінг-атак та оперативності розпізнавання особи розроблена система БА знаходиться приблизно на одному рівні із найкращими аналогічними рішеннями, а за критерієм оперативності розробки перевершує означені рішення приблизно в 1,2 рази. Крім того, ще однією перевагою розробленої системи являється інтеграція основних функціональних

можливостей, які в відомих засобах БА реалізовані фрагментарно.

Використавши дані табл. 4.2 та вираз (1.3) для розробленої системи БА визначена інтегральна оцінка ефективності (E_{Σ}) та оцінки ефективності по критеріям груп А і В (E_{Σ}^A , E_{Σ}^B). Зазначимо, що при розрахунках за допомогою виразу 1.3 прийнято: $\theta_A = 0,7$; $\theta_B = 0,3$; $\alpha_1 = 0,4$; $\alpha_2 = 0,3$; $\alpha_3 = 0,15$; $\alpha_4 = 0,15$; $\beta_1 = 0,25$; $\beta_2 = 0,2$; $\beta_3 = 0,2$; $\beta_4 = 0,15$; $\beta_5 = 0,1$; $\beta_6 = 0,1$.

Відповідні оцінки розраховані також для рішень, представлених в табл.1.3, 1.4. Отримані результати наведені в табл. 4.3.

Таблиця 4.3

Значення інтегральних оцінок ефективності

№	Рішення	E_{Σ}^A	E_{Σ}^B	E_{Σ}
1	2	3	4	5
1	FACETEC (www.facetec.com)	0,825	0,51	0,7305
2	Acuity (www.acuitymi.com)	0,81	0,22	0,633
3	ID R&D (www.idrnd.ai)	0,885	0,3	0,7095
4	VisionLabs (visionlabs.ai)	0,825	0,38	0,6915
5	Neurotechnology (www.neurotechnology.com)	0,765	0,25	0,6105
6	Iridian Tech (www.iridiantech.com)	0,795	0,26	0,6345
7	Blink Identity (www.blinkidentity.com)	0,575	0,585	0,578
8	AxxonSoft (www.axxonsoft.com)	0,62	0,535	0,5945
9	Face ID (Apple)	0,84	0,565	0,7575
10	Face Authentication (Android)	0,77	0,5	0,689
11	Noldus company, FaceReader [39]	0,59	0,595	0,5915
12	Logic Pursuits company, Captemo [41]	0,56	0,48	0,536
13	Herta company, BioObserver [45]	0,56	0,445	0,5255
14	Висоцька О.О., Давиденко А.М., Христович В. [129]	0,635	0,515	0,599

Таблиця 4.3 (продовження)

1	2	3	4	5
15	Долганенко О.Д., Сєверінов О.В., В'юхін Д.О., Коцюба В.П., Крепко А.В. [132]	0,635	0,25	0,5195
16	Яковенко О.О., Кушніренко Н.І., Дорофєєва І.С., Євтушенко А.Р. [168]	0,475	0,3	0,4225
17	Бондарчук А.П., Онисько А.І., Отрох С.І., Шевчук Д.О [126]	0,475	0,3	0,4225
18	Бубенщиков О.В., Лепа Є.В. [127]	0,475	0,3	0,4225
19	Батюк Т., Досин Д. [125]	0,53	0,285	0,4565
20	Ranjith, G., Pallavi, K., Mahendra, V. [77]	0,455	0,41	0,4415
21	Ahmad S., Setumin S. [5]	0,545	0,355	0,488
22	Hamdani N., Bousahba N., Braikia A. [39]	0,6	0,36	0,528
23	Pranav K., Manikandan J. [74]	0,56	0,285	0,4775
24	Hangaragi S., Singh T., Neelima N. [41]	0,58	0,285	0,4915
25	Yergesh A.K. [120]	0,62	0,38	0,548
26	Kumar C., Saranya N., Priyadharshini M. [51]	0,56	0,305	0,4835
27	Li L., Correia P., Hadid, A. [58]	0,71	0,305	0,5885
28	Edmunds T., Caplier, A. [33]	0,69	0,475	0,6255
29	Lokhande M., Khedkar M., Desale N. [63]	0,735	0,475	0,657
30	Розроблена система біометричної автентифікації	0,87	0,79	0,846

Базуючись на даних табл. 4.3, з позицій забезпечення візуального аналізу отриманих результатів побудовано рис. 4.22.

Аналіз даних наведених в табл. 4.3 та представлених на рис. 4.22 свідчить, що ефективність розробленої системи БА за групою критеріїв, які безпосередньо характеризують ефективність процесу розпізнавання, знаходиться приблизно на одному рівні з найбільш досконалими відомими засобами аналогічного призначення, а за групою критеріїв, які дозволяють реалізувати оцінювання з

позицій стійкості до зовнішніх чинників, ресурсоємності та можливості визначення належного функціонального стану представника персоналу ОКІ перевищує ці системи більше ніж у 1,5 рази.

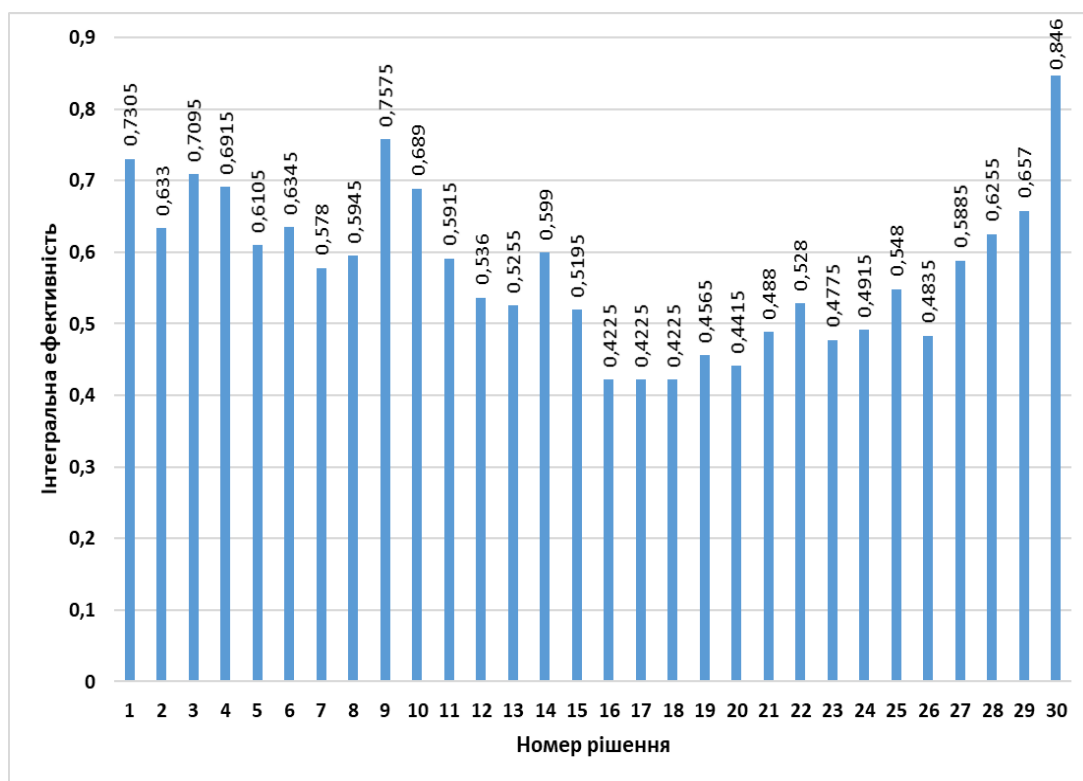


Рис. 4.22. Діаграма інтегральної ефективності рішень в області розпізнавання особи

При цьому інтегральна ефективність розробленої системи БА ОКІ перевищує ефективність найбільш досконалих відомих систем як мінімум в 1,1 рази, що підтверджує доцільність застосування запропонованих рішень задля підвищення ефективності засобів БА в інформаційних системах ОКІ.

4.4. Висновки до четвертого розділу

Даний розділ присвячено вирішенню науково-практичної задачі розробки системи біометричної автентифікації об'єктів критичної інфраструктури та проведенню експериментальних досліджень, спрямованих на перевірку достовірності основних результатів дисертаційного дослідження. Основні результати розділу наступні:

Вперше розроблено архітектуру системи біометричної автентифікації за зображенням обличчя та райдужної оболонки ока об'єктів критичної інфраструктури, в якій, на відміну від відомих, з використанням UML-діаграми прецедентів сформовано формалізований опис функціональних вимог, пов'язаних із семантичною сегментацією зображень обличчя, а також із необхідністю виявлення та розпізнавання спуфінг-атак за природністю емоцій і артефактами зовнішнього оточення, що забезпечує підґрунтя для підвищення ефективності системи біометричної автентифікації в ракурсі впровадження в неї відповідних сервісів.

Проведені експериментальні дослідження дозволяють стверджувати:

- Використання запропонованого методу побудови нейромережових засобів семантичної сегментації зображення обличчя при біометричній автентифікації дозволяє приблизно на порядок зменшити кількість експериментальних досліджень, пов'язаних з визначенням архітектурних параметрів нейромережових моделей, на яких базуються вказані засоби, та в 1,2-1,25 рази підвищити точність виділення кордонів обличчя, внаслідок чого забезпечується можливість в 1,1-1,15 рази зменшити похибку розпізнавання особи. Отримані при цьому показники $FAR \approx 0,0008$ та $FRR \approx 0,011$ у робочій точці, високе значення $AUC \approx 0,999$, а також характер DET-кривої у сукупності підтверджують дотримання нормативних вимог до систем біометричної автентифікації на ОКІ та відповідність запропонованого методу рівню передових рішень у цій галузі.

- Використання запропонованого нейромережового методу біометричної автентифікації за зображенням обличчя та райдужною оболонкою ока в інформаційних системах об'єктів критичної інфраструктури дозволяє приблизно в 1,1 рази підвищити інтегральну ефективність засобів біометричної автентифікації.

ВИСНОВКИ

В дисертаційній роботі вирішено актуальну науково-прикладну задачу розробки ефективних нейромережових моделей та методів біометричної аутентифікації за зображенням обличчя та райдужною оболонкою ока в інформаційних системах об'єктів критичної інфраструктури.

Проведені дослідження дозволяють зробити наступні висновки:

1. Визначено, що перспективи підвищення ефективності нейромережової системи біометричної автентифікації персоналу об'єктів критичної інфраструктури за зображенням обличчя та райдужною оболонкою ока пов'язані з забезпеченням оперативності розробки нейромережових засобів, підвищенням точності виділення кордонів зображення обличчя, зареєстрованого в умовах завад, розширенням переліку ознак розпізнавання спуфінг-атак та доповненням функціональних можливостей системи автентифікації за рахунок розпізнавання емоцій.

2. Розроблено моделі біометричної автентифікації в інформаційних системах об'єктів критичної інфраструктури, що дозволило деталізувати шляхи підвищення ефективності засобів біометричної аутентифікації за зображенням обличчя та райдужною оболонкою ока та забезпечило теоретичний базис розробки методу побудови нейромережових засобів семантичної сегментації зображення обличчя при біометричній автентифікації та нейромережового методу біометричної автентифікації за зображенням обличчя та райдужною оболонкою ока в інформаційних системах об'єктів критичної інфраструктури. Модель процедури розпізнавання особи за зображенням обличчя та райдужною оболонкою ока при біометричній автентифікації персоналу об'єктів критичної інфраструктури з застосуванням нейромережових засобів за рахунок реалізації формалізованого опису процедури розпізнавання, конкретизації завдань та умов застосування нейромережових засобів, обґрунтування доцільності побудови модульної нейромережової моделі, багатовимірного підходу до розпізнавання спуфінг-атак, конкретизації критеріїв оцінювання ефективності та критеріїв

якості попередньої обробки зображення, дозволила деталізувати перспективні шляхи підвищення ефективності нейромережових засобів біометричної автентифікації. Модель семантичної сегментації зображення обличчя за рахунок застосування енкодер-декодерної архітектури нейронної мережі з варіативними конструктивними параметрами, що підлягають адаптації залежно від умов застосування, забезпечила можливість розробки ефективного методу побудови нейромережових засобів семантичної сегментації зображення обличчя. Модульна нейромережева модель біометричної автентифікації за рахунок співвіднесення функціоналу модулів із виконанням завдань біометричної автентифікації, які доцільно виконувати за допомогою окремої нейронної мережі, з урахуванням можливості використання апробованих вільнодоступних нейромережових засобів, адаптованих до очікуваних умов застосування, забезпечила можливість побудови ефективного нейромережевого методу біометричної автентифікації за зображенням обличчя та райдужною оболонкою ока, з урахуванням необхідності розпізнавання спуфінг-атак та забезпечення оперативності розробки відповідних нейромережових засобів.

3. Розроблено метод побудови нейромережових засобів семантичної сегментації зображення обличчя при біометричній аутентифікації, що, за рахунок поетапної адаптації типу та конструктивних параметрів нейромережевої моделі до умов застосування в напрямку зменшення архітектурної складності та за рахунок використання механізму динамічного коригування параметрів навчання, забезпечує можливість вже на першому етапі експериментів оцінити придатність базової архітектури до досягнення цільових показників, досягти стабільної збіжності навчання і уникнути перенавчання, що в результаті дозволяє в 1,2-1,25 рази підвищити точність виділення не деформованих завадами контурів зображення обличчя та приблизно в 10 разів зменшити обсяг складних довготривалих експериментів, спрямованих на визначення архітектурних параметрів нейромережевої моделі.

4. Розроблено нейромережевий метод біометричної автентифікації за зображенням обличчя та райдужною оболонкою ока в інформаційних системах

об'єктів критичної інфраструктури, що, за рахунок адаптації параметрів обробки відеопотоку до поточних значень показників відображення, обґрунтованого використання апробованих наперед навчених нейромережових моделей, фільтрації зображення обличчя та райдужної оболонки від типових завад шляхом застосування процедури семантичної сегментації з наступним поелементним маскуванню піксельних значень та за рахунок аналізу ознак спуфінг-атак, з урахуванням артефактів зовнішнього оточення та динаміки емоційного стану, дозволяє в 1,1-1,15 рази зменшити похибку розпізнавання особи, забезпечує можливість здійснювати розпізнавання спуфінг-атак за розширеним переліком ознак, доповнює функціональні можливості системи біометричної автентифікації за рахунок розпізнавання емоцій та забезпечує можливість оперативної розробки відповідних нейромережових засобів.

5. Розроблено та досліджено систему біометричної автентифікації об'єктів критичної інфраструктури, ефективність якої приблизно в 1,1 рази перевищує ефективність найкращих відомих систем подібного призначення. Ефективність запропонованих рішень підтверджується впровадженням дисертаційних рішень в діяльність Державного університету «Київський авіаційний інститут» при виконанні держбюджетної науково-дослідної роботи «Система забезпечення кібербезпеки та стійкості об'єктів критичної інфраструктури» (№ДР 5-2024/18.02, 2024-2025 рр.) (акт впровадження від 12.01.2026) та в навчальному процесі кафедри кібербезпеки факультету комп'ютерних наук та технологій (акт впровадження від 12.01.2026). Також отримані результати впроваджені в діяльність ТОВ «АНТЕ МЕДІАМ» (акт впровадження від 11.09.2025), Львівської торгово-промислової палати (акт впровадження від 12.03.2026), ТОВ «Науково-виробниче підприємство хімічних продуктів» (акт впровадження від 16.06.2025), ТОВ «Айті Курсор» (акт впровадження від 27.11.2025), ТОВ «ОПТОЕЛЕКТРОНІКА» (акт впровадження від 24.12.2025).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Abraham, J., & Paul, V. (2019). An Imperceptible Spatial Domain Color Image Watermarking Scheme. *Journal of King Saud University – Computer and Information Sciences*, 31, 125–133.
2. Adithya, U., & Nagaraju, C. (2021). Object Motion Direction Detection and Tracking for Automatic Video Surveillance. *International Journal of Education Management Engineering*, 11(2), 32–39.
3. Afchar, D., Nozick, V., Yamagishi, J., & Echizen, I. (2018). *MesoNet: A compact facial video forgery detection network*. Proceedings of the IEEE International Workshop on Information Forensics and Security, Hong Kong, China (pp. 1–7).
4. Agarwal, N., Krohn-Grimberghe, A., & Vyas, R. (2017). *Facial Key Points Detection using Deep Convolutional Neural Network - NaimishNet*. (arXiv:1710.00977v1). arXiv.
5. Ahmad, S., & Setumin, S. (2021). *One-Shot Learning for Facial Sketch Recognition using the Siamese Convolutional Neural Network*. Proceedings of the 11th IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE), Penang, Malaysia (pp. 307–312).
6. Aitchanov, B., Korchenko, A., Tereykovskiy, I., & Bapiyev, I. (2017). Perspectives for using classical neural network models and methods of counteracting attacks on network resources of information systems. *News of the National Academy of Sciences of the Republic of Kazakhstan, Series of Geology and Technical Sciences*, 5(425), 202–212.
7. Arora, S., Bhatia, M. P. S., & Kukreja, H. (2021). A multimodal biometric system for secure user identification based on deep learning. In X. S. Yang, R. S. Sherratt, N. Dey, & A. Joshi (Eds.), *Advances in Intelligent Systems and Computing* (Vol. 1183, pp. 81–90). Springer: Singapore.
8. Avital, N., Egel, I., Weinstock, I., & Malka, D. (2024). Enhancing Real-Time Emotion Recognition in Classroom Environments Using Convolutional Neural Networks: A Step Towards Optical Neural Networks for Advanced Data Processing.

Inventions, 9(6), 113.

9. Avkurova, Z., Gnatyuk, S., Abduraimova, B., & Makulov, K. (2024). Targeted attacks detection and security intruders identification in the cyber space. *International Journal of Computer Network and Information Security*, 16(4), 144–153.

10. Badrinarayanan, V., Kendall, A., & Cipolla, R. (2017). *SegNet: A Deep Convolutional Encoder–Decoder Architecture for Image Segmentation*. arXiv:1511.00561.

11. Baisholan, N., Dietz, J., Gnatyuk, S., Turdalyuly, M., Matson, E. T., & Baisholanova, K. (2025). A systematic review of machine learning in credit card fraud detection under original class imbalance. *Computers*, 14(10), 437.

12. Baltrušaitis, T., Zadeh, A., Lim, Y. C., & Morency, L.-P. (2017). OpenFace 2.0: Facial Behavior Analysis Toolkit. *2017 IEEE International Conference on Automatic Face and Gesture Recognition (FG 2017)* (pp. 262–269). IEEE.

13. Bagitova, K., Tereikovskiy, I., Babayev, I., Tereikovska, L., & Tereikovskiy, O. (2023). Model for processing images of online social networks used to recognize political extremism. *Journal of Mathematics, Mechanics and Computer Science*, 119(3), 91–103.

14. Bao, X., Xiang, W., He, J., Liu, H., Cheng, Z., Li, C., Liu, W., Geng, Y., Sun, J., Luo, B., & Xie, X. (2023). KeyPosS: Plug-and-Play Facial Landmark Detection through GPS-Inspired True-Range Multilateration. *Proceedings of the 31st ACM International Conference on Multimedia (MM '23)* (pp. 3861–3870).

15. Benalcazar, D., Tapia, J., Gonzalez, S., & Busch, C. (2023). Synthetic ID Card Image Generation for Improving Presentation Attack Detection. *Transactions on Information Forensics and Security*, 18, 1814–1824.

16. Bushuyev, S., Tereikovskiy, I., Korchenko, O., Dychka, I., Tereikovska, L., & Tereikovskiy, O. (2024). Conceptual model of the face recognition process based on the image of the face and iris of personnel of critical infrastructure facilities. In *Proceedings of the 5th International Workshop IT Project Management (ITPM 2024)* (Vol. 3709, pp. 278–291). CEUR Workshop Proceedings.

17. Cao, Q., Li, M., Yang, G., Tao, Q., Luo, Y., Wang, R., & Chen, P. (2024).

Urban vegetation classification for unmanned aerial vehicle remote sensing combining feature engineering and improved DeepLabV3+. *Forests*, 15(2), 382.

18. Cao, Q., Shen, L., Xie, W., Parkhi, O. M., & Zisserman, A. (2018). VGGFace2: A dataset for recognising faces across pose and age. In *2018 IEEE International Conference on Automatic Face & Gesture Recognition*, (pp. 67–74).

19. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys*, 41(3), 1–58.

20. Chen, L. C., Papandreou, G., Kokkinos, I., Murphy, K., & Yuille, A. L. (2018). DeepLab: Semantic image segmentation with deep convolutional nets, atrous convolution, and fully connected CRFs. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 40(4), 834–848.

21. Chen, L. C., Papandreou, G., Schroff, F., & Adam, H. (2017). *Rethinking atrous convolution for semantic image segmentation*. arXiv:1706.05587.

22. Chen, L. C., Zhu, Y., Papandreou, G., Schroff, F., & Adam, H. (2018). Encoder-decoder with atrous separable convolution for semantic image segmentation. In *Lecture Notes in Computer Science* (Vol. 11211, pp. 833–851). Springer: Cham, Switzerland.

23. Cheng, B., Schwing, A. G., & Kirillov, A. (2021). *Per-Pixel Classification is Not All You Need for Semantic Segmentation*. (arXiv:2107.06278v2). arXiv.

24. Cherrat, R. A., & Bouzahir, H. (2020). Score Fusion of Finger Vein and Face for Human Recognition Based on Convolutional Neural Network Model. *International Journal of Computer*, 19(2), 11–19.

25. Chiu, M.-T., Cheng, H.-Y., Wang, C.-Y., & Lai, S.-H. (2021). *High-accuracy RGB-D face recognition via segmentation-aware face depth estimation and mask-guided attention network*. 2021 16th IEEE International Conference on Automatic Face and Gesture Recognition (FG 2021) (pp. 1–8). IEEE: Jodhpur, India.

26. Cui, W., Lan, Y., Li, J., Yang, L., Zhou, Q., Han, G., Xiao, X., & Qiao, Y. (2025). Apple yield estimation method based on CBAM-ECA-Deeplabv3+ image segmentation and multi-source feature fusion. *Sensors*, 25(11), 3140.

27. Davison, A. K., Merghani, W., & Yap, M. H. (2018). Objective Classes for

Micro-Facial Expression Recognition. *Journal of Imaging*, 4(10), 119.

28. Davydenko, A., Korchenko, O., Vysotska, O., & Ivanchenko, I. (2021). Model and method for identification of functional security profile. *Proceedings of the 3rd International Conference on Information Security and Information Technologies (ISecIT 2021)* (Vol. 3200, pp. 274–280). CEUR Workshop Proceedings.

29. Deng, J., Guo, J., Yang, J., Xue, N., Kotsia, I., & Zafeiriou, S. (2022). *ArcFace: Additive Angular Margin Loss for Deep Face Recognition*. (arXiv:1801.07698v4). arXiv.

30. Deshmukh, P., & Mohod, S. (2020). *Biometric Jammer: A Security Enhancement Scheme using SVM Classifier*. Proceedings of the 5th IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE), Jaipur, India (pp. 1–6).

31. Dileep, P., Bolla, B. K., & Ethiraj, S. (2022). *Revisiting Facial Key Point Detection: An Efficient Approach Using Deep Neural Networks*. (arXiv:2205.07121v1). arXiv.

32. Dudnik, A., Vyhovskyi, S., Yaremenko, D., Zhaksigulova, D., Kysil, A., Rakytskyi, V., & Fesenko, A. (2024). *Algorithms for obtaining video and sound data of UAVs in real time*. CH&CMiGIN'24: Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, Kyiv, Ukraine (pp. 193–204).

33. Edmunds, T., & Caplier, A. (2018). Motion-based countermeasure against photo and video spoofing attacks in face recognition. *Journal of Visual Communication and Image Representation*, 50, 314–332.

34. George, A., & Marcel, S. (2019). *Deep Pixel-wise Binary Supervision for Face Presentation Attack Detection*. (arXiv:1907.04047v1). arXiv.

35. Green, K. (2021). *Segmentation in style: Unsupervised semantic image segmentation with StyleGAN and CLIP*. arXiv:2107.12518.

36. Gupta, G., Raja, K., Gupta, M., Jan, T., Whiteside, S. T., & Prasad, M. (2024). A Comprehensive Review of DeepFake Detection Using Advanced Machine Learning and Fusion Methods. *Electronics*, 13(1), 95.

37. Hajare, H., & Ambhaikar, A. (2023). *Face Anti-Spoofing Techniques and Challenges: A short survey*. Proceedings of the 11th International Conference on Emerging Trends in Engineering & Technology-Signal and Information Processing, Nagpur, India (pp. 1–6).
38. Hajizadeh Javaran, M. R., Rajabi, M. M., Kamali, N., Fahs, M., & Belfort, B. (2023). Encoder-decoder convolutional neural networks for flow modeling in unsaturated porous media: Forward and inverse approaches. *Water*, 15(16), 2890.
39. Hamdani, N., Bousahba, N., Bousbai, A., & Braikia, A. (2023). Face Detection and Recognition Using Siamese Neural Network. *International Journal of Computing and Digital System*, 14(1), 889–897.
40. Han, K., Wang, Y., Tian, Q., Guo, J., Xu, C., & Xu, C. (2020). *GhostNet: More Features from Cheap Operations*. (arXiv:1911.11907v2). arXiv.
41. Hangaragi, S., Singh, T., & Neelima, N. (2023). Face Detection and Recognition Using Face Mesh and Deep Neural Network. *Procedia Computer Science*, 218, 741–749.
42. He, S., Luo, H., Wang, P., Wang, F., Li, H., & Jiang, W. (2021). *TransReID: Transformer-based object re-identification* (arXiv preprint arXiv:2102.04378). <https://arxiv.org/abs/2102.04378>.
43. Hu, Z., Tereikovskiy, I., Chernyshev, D., Tereikovska, L., Tereikovskiy, O., & Wang, D. (2021). Procedure for processing biometric parameters based on wavelet transformations. *International Journal of Modern Education and Computer Science (IJMECS)*, 13(2), 11–22.
44. Howard, A., Sandler, M., Chen, B., Wang, W., Chen, L.-C., Zhu, Y., Chu, G., Pang, R., Vasudevan, V., Le, Q. V., Tan, M., & Adam, H. (2019). *Searching for MobileNetV3*. (arXiv:1905.02244v5). arXiv.
45. Htwe, P., & Phyo, T. (2021). Face Recognition System based on Convolution Neural Networks. *International Journal of Image, Graphics and Signal Process (IJIGSP)*, 13(3), 23–29.
46. Kanashev, M., Mukasheva, A., Yedilkhan, D., Rakhmetulaeva, S., Gnatyuk, S., & Nazym, M. (2024). *Research and development of an information system for*

speech recognition based on neural network algorithms metrics. 2024 IEEE 4th International Conference on Smart Information Systems and Technologies (SIST), Astana, Kazakhstan (pp. 314–320).

47. Kolarik, M., Burget, R., & Riha, K. (2019). *Upsampling algorithms for autoencoder segmentation neural networks: A comparison study*. 2019 11th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), Dublin, Ireland (pp. 1–5).

48. Kong, C., Chen, B., Li, H., Wang, S., & Kwong, S. (2022). Detect and locate: Exposing face manipulation by semantic- and noise-level telltales. *IEEE Transactions on Information Forensics and Security*, 17, 1741–1756.

49. Kong, T., Sun, F., Liu, H., Jiang, Y., Li, L., & Shi, J. (2020). FoveaBox: Beyond anchor-based object detection. *IEEE Transactions on Image Processing*, 29, 7389–7398.

50. Korchenko, O., Tereikovskiy, I., Ziubina, R., Tereikovska, L., Korystin, O., Tereikovskiy, O., & Karpinskyi, V. (2025). Modular Neural Network Model for Biometric Authentication of Personnel in Critical Infrastructure Facilities Based on Facial Images. *Applied Sciences*, 15(5), 2553.

51. Kumar, C. R., Saranya, N., Priyadharshini, M., Gilchrist, E. D., & Rahman, M. K. (2023). Face recognition using CNN and siamese network. *Measurement: Sensors*, 27, 100800.

52. Lakhno, V., Akhmetov, B., Kryvoruchko, O., Chubaievskiy, V., Desyatko, A., Bereke, M., & Shalabaeva, M. (2024). Cyber threats to the private academic cloud. *International Journal of Electronics and Telecommunications*, 70(2), 413–420.

53. Lakhno, V., Kozlovskiy, V., Klobukov, V., Kryvoruchko, O., Chubaievskiy, V., & Tyshchenko, D. (2022). Software Package for Information Leakage Threats Relevance Assessment. In R. Silhavy (Ed.), *Cybernetics Perspectives in Systems* (Vol. 503, pp. 290–301). Springer: Cham.

54. Lee, S., Shin, C., Kang, H.-G., & Lee, S. (2025). Recurrent flow update model using image pyramid structure for 4K video frame interpolation. *Sensors*, 25(1), 290.

55. Lee, H. J., & Sediqi, K. M. (2021). A novel upsampling and context convolution for image semantic segmentation. *Sensors*, 21(6), 2170.
56. Li, C., He, Z., Lu, K., & Fang, C. (2025). Bird species detection net: Bird species detection based on the extraction of local details and global information using a dual-feature mixer. *Sensors*, 25(1), 291.
57. Li, D., Yang, J., Kreis, K., Torralba, A., & Fidler, S. (2021). *Semantic Segmentation with Generative Models: Semi-Supervised Learning and Strong Out-of-Domain Generalization*. Proceedings of the 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Nashville, TN, USA (pp. 8296–8307).
58. Li, L., Correia, P. L., & Hadid, A. (2018). Face recognition under spoofing attacks: Countermeasures and research directions. *IET Biometrics*, 7(1), 3–14.
59. Li, R., Zhao, J., & Fan, Y. (2025). Research on CTSA-DeepLabV3+ urban green space classification model based on GF-2 images. *Sensors*, 25(13), 3862.
60. Li, Y., Chang, M. C., & Lyu, S. (2018). *In actu oculi: Exposing ai created fake videos by detecting eye blinking*. Proceedings of the IEEE International Workshop on Information Forensics and Security (WIFS), Hong Kong, China (pp. 11–13).
61. Liu, X.-P., Li, G., Liu, L., & Wang, Z. (2019). Improved YOLOv3 Target Recognition Algorithm Based on Adaptive Edged Optimization. *Microelectron. Comput.*, 36, 59–64.
62. Liu, Z., Lin, Y., Cao, Y., Hu, H., Wei, Y., Zhang, Z., Lin, S., & Guo, B. (2021). *Swin Transformer: Hierarchical vision transformer using shifted windows*. arXiv:2103.14030.
63. Lokhande, M., Khedkar, M., & Desale, N. (2024). *Biometric Liveness Detection Guarding Against Spoofing Attacks using Machine Learning Techniques*. Proceedings of the 8th International Conference on I-SMAC, Kirtipur, Nepal (pp. 2065–2070).
64. Ma, N., Zhang, X., Zheng, H.-T., & Sun, J. (2018). *Practical Guidelines for Efficient CNN Architecture Design*. (arXiv:1807.11164v1). arXiv.
65. Ma, X., Fu, M., Zhang, X., Song, X., Becker, B., Wu, R., Xu, X., Gao, Z., Kendrick, K., & Zhao, W. (2022). Own Race Eye-Gaze Bias for All Emotional Faces

but Accuracy Bias Only for Sad Expressions. *Frontiers in Neuroscience*, 16.

66. Meden, B., et al. (2021). Privacy–Enhancing Face Biometrics: A Comprehensive Survey. *IEEE Transactions on Information Forensics and Security*, 16, 4147–4183.

67. Müller, D., Ehlen, A., & Valeske, B. (2021). Convolutional Neural Networks for Semantic Segmentation as a Tool for Multiclass Face Analysis in Thermal Infrared. *Journal of Nondestructive Evaluation*, 40(1), 9.

68. Muthukumaran, B., Harshavarthanan, L., Dhyaneshwar, S., & Sharief, M. (2023). *Face and Iris based Human Authentication using Deep Learning*. Proceedings of the 4th International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India (pp. 841–846).

69. Nguyen, H. H., Yamagishi, J., & Echizen, I. (2019). *Capsule-forensics: Using capsule networks to detect forged images and videos*. Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing, Brighton, UK (pp. 2307–2311).

70. Noyes, E., Davis, J. P., Petrov, N., Gray, K. L. H., & Ritchie, K. L. (2021). The effect of face masks and sunglasses on identity and expression recognition with super-recognizers and typical observers. *Royal Society Open Science*, 8(3).

71. Osypenko, M., Shymkovych, V., Kravets, P., Novatsky, A., & Shymkovych, L. (2024). Intelligent control system with reinforcement learning for solving video game tasks. *Adaptive Automatic Control Systems*, 2(45), 34–46.

72. Pahuja, S., & Goel, N. (2024). Multimodal Biometric Authentication: A Review. *AI Communications*, 37, 525–547.

73. Pennebaker, J. W., Mehl, M. R., & Niederhoffer, K. G. (2003). Psychological aspects of natural language use: Our words, our selves. *Annual Review of Psychology*, 54(1), 547–577.

74. Pranav, K., & Manikandan, J. (2020). Design and Evaluation of a Real-Time Face Recognition System using Convolutional Neural Networks. *Procedia Computer Science*, 171, 1651–1659.

75. Prilianti, K. R., et al. (2021). Non-Destructive Photosynthetic Pigments

Prediction Using Multispectral Imagery and 2D-CNN. *International Journal of Computer*, 20(3), 391–399.

76. Qi, D., Tan, W., Yao, Q., & Liu, J. (2023). YOLO5Face: Why Reinventing a Face Detector. In L. Karlinsky, T. Michaeli, & K. Nishino (Eds.), *Computer Vision – ECCV 2022 Workshops* (Vol. 13805, pp. 223–238). Springer: Cham, Switzerland.

77. Ranjith, G., Pallavi, K., & Mahendra, V. (2022). Human Face, Eye and Iris Detection in Real-Time Using Image Processing. In *Algorithms for Intelligent Systems* (pp. 383–389). Springer Nature Singapore.

78. Rinck, M., Primbs, M. A., Verpaalen, I. A. M., & Bijlstra, G. (2022). Face masks impair facial emotion recognition and induce specific emotion confusions. *Cognitive Research: Principles and Implications*, 7(1).

79. Ronneberger, O., Fischer, P., & Brox, T. (2015). *U-Net: Convolutional networks for biomedical image segmentation*. arXiv:1505.04597.

80. Royer, J., Blais, C., Charbonneau, I., Déry, K., Tardif, J., Duchaine, B., Gosselin, F., & Fiset, D. (2018). Greater reliance on the eye region predicts better face recognition ability. *Cognition*, 181, 12–20.

81. Saleh, A., Alsafo, F., Ali, D., & Taha, M. (2024). An Effective Face Detection and Recognition Model Based on Improved YOLO v3 and VGG 16 Networks. *International Journal of Computer Methods and Experimental Measurements*, 12(2), 107–119.

82. Sajaad, A. L., & Mir, A. H. (2022). Smartphone-based Biometric Authentication Scheme for Access Control Management in Client-server Environment. *International Journal of Information Technology and Computer Science*, 14(4), 34–47.

83. Schroff, F., Kalenichenko, D., & Philbin, J. (2015). FaceNet: A unified embedding for face recognition and clustering. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition* (pp. 815–823). IEEE.

84. Serengil, Ş. İ., & Özpınar, A. (2024). A Benchmark of Facial Recognition Pipelines and Co-Usability Performances of Modules. *Bilişim Teknolojileri Dergisi*, 17(2), 95.

85. Shelhamer, E., Long, J., & Darrell, T. (2017). Fully convolutional networks

for semantic segmentation. *IEEE Transactions on Pattern Analysis and Mach. Intell.*, 39(4), 640–651.

86. Shen, J. (2014). Motion Detection in Color Image Sequence and Shadow Elimination. In *Visual Communications and Image Processing* (Vol. 5308, pp. 731–740). SPIE: Bellingham, WA, USA.

87. Sindel, A., Maier, A., & Christlein, V. (2022). *Art FacePoints: High-resolution Facial Landmark Detection in Paintings and Prints*. (arXiv:2210.09204v1). arXiv.

88. Štītīlis, D., Laurinaitis, M., & Verenius, E. (2023). The Use of Biometric Technologies in Ensuring Critical Infrastructure Security: The Context of Protecting Personal Data. *Entrepreneurship and Sustainability Issues*, 10(3), 133–150.

89. Taigman, Y., Yang, M., Ranzato, M., & Wolf, L. (2014). DeepFace: Closing the Gap to Human-Level Performance in Face Verification. *2014 IEEE Conference on Computer Vision and Pattern Recognition*, 1701–1708.

90. Tan, M., Chen, B., Pang, R., Vasudevan, V., Sandler, M., Howard, A., & Le, Q. V. (2019). *MnasNet: Platform-Aware Neural Architecture Search for Mobile*. (arXiv:1807.11626v3). arXiv.

91. Tan, M., & Le, Q. V. (2020). *EfficientNet: Rethinking Model Scaling for Convolutional Neural Networks*. (arXiv:1905.11946v5). arXiv

92. Tang, M., He, Y., Aslam, M., Akpokodje, E., & Jilani, S. F. (2025). Enhanced U-Net++ for improved semantic segmentation in landslide detection. *Sensors*, 25(9), 2670.

93. Tarafdar, K. K., et al. (2025). *Multiresolution encoder-decoder convolutional neural network for magnetic resonance image segmentation*. ICASSP 2025 - 2025 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Hyderabad, India (pp. 1–5).

94. Tavrov, D., Temnikova, O., & Temnikov, V. (2019). Perceptual Computing Based Method for Assessing Functional State of Aviation Enterprise Employees. *Advances in Intelligent Systems and Computing*, 836, 61–70.

95. Tereikovskiy, I., AlShboul, R., Mussiraliyeva, S., Tereikovska, L., Bagitova,

K., Tereikovskiy, O., & Hu, Z. (2024). Method for constructing neural network means for recognizing scenes of political extremism in graphic materials of online social networks. *International Journal of Computer Network and Information Security (IJCNIS)*, 16(3), 52–69.

96. Tereikovskiy, I., Korchenko, O., Bushuyev, S., Tereikovskiy, O., Ziubina, R., & Veselska, O. (2023). A neural network model for object mask detection in medical images. *International Journal of Electronics and Telecommunications*, 69(1), 41–46.

97. Tereikovskiy, I., Subach, I., Tereikovskiy, O., Tereikovska, L., Toliupa, S., & Nakonechnyi, V. (2019). *Parameter definition for multilayer perceptron intended for speaker identification*. 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT) (pp. 227–231). IEEE.

98. Tereikovskiy, I., Tereikovska, L., Kryvoruchko, O., Tereikovskiy, O., Tyshchenko, D., & Franchuk, T. (2022). *Speaker's emotions recognition module based on the GoogleLeNet neural network*. 2022 IEEE International Conference on Smart Information Systems and Technologies (SIST) (pp. 45–50). IEEE.

99. Tereikovskiy, I., Hu, Z., Chernyshev, D., Tereikovska, L., Korystin, O., & Tereikovskiy, O. (2022). The method of semantic image segmentation using neural networks. *International Journal of Image, Graphics and Signal Process (IJIGSP)*, 14(6), 1–14.

100. Tereikovskiy, I. A., Chernyshev, D. O., Tereikovska, L. A., Mussiraliyeva, S. Z., & Akhmed, G. Z. (2019). The procedure for the determination of structural parameters of a convolutional neural network to fingerprint recognition. *Journal of Theoretical and Applied Information Technology*, 97(8), 2381–2392.

101. Tereikovskiy, I., Parkhomenko, I., Toliupa, S., & Tereikovska, L. (2018). *Markov model of normal conduct template of computer systems network objects*. 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET 2018) – Proceedings (pp. 498–501). IEEE: Lviv-Slavske, Ukraine.

102. Tereikovska, L., Tereikovskiy, I., Aytkhozhaeva, E., Tynymbayev, S., &

Imanbayev, A. (2017). Encoding of neural network model exit signal that is devoted for distinction of graphical images in biometric authentication systems. *News of the National Academy of Sciences of the Republic of Kazakhstan, Series of Geology and Technical Sciences*, 6(426), 217–224.

103. Tereikovskiy, O. (2024). Characteristics of personnel authentication means in information systems of critical infrastructure facilities. *У XII Міжнародна науково-практична конференція...* (с. 181–182). Кропивницький.

104. Tereikovskiy, O. (2025). Development of the architecture of the neural network model of biometric authentication based on the face and iris image. *У POLIT. Challenges of Science Today...* (pp. 82–83). Kyiv.

105. Tereikovskiy, O. (2025). Model of semantic segmentation of face images. *У 2-га Міжнародна науково-практична конференція... (IST 2025)* (с. 260–263). Київ: Факультет інформаційних технологій КНУ імені Тараса Шевченка.

106. Toliupa, S., Kulakov, Y., Tereikovskiy, I., Tereikovskiy, O., Tereikovska, L., & Nakonechnyi, V. (2020). *Keyboard dynamic analysis by AlexNet type neural network*. 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET) (pp. 416–420). IEEE: Lviv-Slavske, Ukraine.

107. Toliupa, S., Tereikovska, L., Tereikovskiy, I., Doszhanova, A., & Alimseitova, Z. (2020). *Procedure for Adapting a Neural Network to Eye Iris Recognition*. IEEE International Conference on Problems of Infocommunications, Science and Technology (pp. 167–171).

108. Udaheemuka, G., Djouani, K., & Kurien, A. M. (2024). Multimodal Emotion Recognition Using Visual, Vocal and Physiological Signals: A Review. *Applied Sciences*, 14(17), 8071.

109. Unified Modeling Language Specification Version 2.5.1. (2025). Object Management Group (OMG).

110. Vinette, C., Gosselin, F., & Schyns, P. (2004). Spatio-temporal dynamics of face recognition in a flash: it's in the eyes. *Cognitive Science*, 28(2), 289–301.

111. Viswanath Reddy, D. A., Aswini Reddy, A., & Bindyashree, C. A. (2021).

Facial Emotions over Static Facial Images Using Deep Learning Techniques with Hysterical Interpretation. *Journal of Physics: Conference Series*, 2089(1), 012014.

112. Vysotska, O., Davydenko, A., & Potenko, O. (2023). Modeling the mindfulness people's function based on the recognition of biometric parameters by artificial intelligence elements. *Radioelectronic and Computer Systems*, 3, 136–149.

113. Wang, J., Sun, K., Cheng, T., Jiang, B., Deng, C., Zhao, Y., Liu, D., Mu, Y., Tan, M., Wang, X., Liu, W., & Xiao, B. (2020). Deep High-Resolution Representation Learning for Visual Recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*.

114. Wang, L., Chang, Y., & Wang, K. (2024). Dual-Branch Multimodal Fusion Network for Driver Facial Emotion Recognition. *Applied Sciences*, 14(20), 9430.

115. Wang, Y., Tan, T., & Jain, A. K. (2003). Combining Face and Iris Biometrics for Identity Verification. In J. Kittler & M. S. Nixon (Eds.), *Audio- and Video-Based Biometric Person Authentication* (Vol. 2688, pp. 805–813). Springer: Berlin, Heidelberg.

116. Wang, Y., Yang, L., Liu, X., & Yan, P. (2024). An improved semantic segmentation algorithm for high-resolution remote sensing images based on DeepLabv3+. *Scientific Reports*, 14(1), 9716.

117. Wood, E., Baltrušaitis, T., Hewitt, C., Dziadzio, S., Johnson, M., Estellers, V., Cashman, T. J., & Shotton, J. (2021). *Fake it till you make it: Face analysis in the wild using synthetic data alone*. arXiv:2109.15102.

118. Xiao, T., Liu, Y., Huang, Y., Li, M., & Yang, G. (2023). Enhancing multiscale representations with Transformer for remote sensing image semantic segmentation. *IEEE Transactions on Geoscience and Remote Sensing*, 61, 5605116.

119. Xie, E., Wang, W., Yu, Z., Anandkumar, A., Alvarez, J. M., & Luo, P. (2021). *SegFormer: Simple and efficient design for semantic segmentation with Transformers*. arXiv:2105.15203.

120. Yergesh, A. K. (2024). Development of an advanced biometric authentication system using iris recognition based on a convolutional neural network.

Herald of Science, 2(5), 615–625.

121. Yudin, O., Toliupa, S., Korchenko, O., Tereikovska, L., Tereikovskiy, I., & Tereikovskiy, O. (2020). Determination of signs of information and psychological influence in the tone of sound sequences. *2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT)* (pp. 276–280). IEEE: Kyiv, Ukraine.

122. Zheng, Q., Deng, J., Zhu, Z., Li, Y., & Zafeiriou, S. (2022). *Decoupled multi-task learning with cyclical self-regulation for face parsing*. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), New York, NY, USA (pp. 4156–4165).

123. Zhou, A., Ma, Y., Ji, W., Zong, M., Yang, P., Wu, M., & Liu, M. (2022). Multi-head attention-based two-stream EfficientNet for action recognition. *Multimedia Systems*, 29(1), 1–12.

124. Zhang, H., et al. (2024). HF-HRNet: A simple hardware friendly high-resolution network. *IEEE Transactions on Circuits and Systems for Video Technology*, 34(8), 7699–7711.

125. Батюк, Т., & Досин, Д. (2024). Реалізація надійної та ефективної автентифікації в інтелектуальних системах шляхом використання методів візуальної біометрики. *Information Systems and Networks*, 15, 23–42

126. Бондарчук, А. П., Онисько, А. І., Отрох, С. І., & Шевчук, Д. О. (2023). Система двофакторної аутентифікації користувача за допомогою розпізнавання обличчя. *Телекомунікаційні та інформаційні технології*, 3(80), 79-85.

127. Бубенщиков, О.В. & Лепа, Є.В. (2019). Використання згортальних нейронних мереж для ідентифікації обличчя людини. *Вісник ХНТУ*, 1(68), 136-142.

128. Бушуєв, С.Д., Кулаков, Ю.О., Терейковська, Л.О., Терейковський, І.А. & Терейковський О.І. (2022). Нейромережева модель детектування кордонів обличчя людини. *Управління розвитком складних систем*, 51, 5-11.

129. Висоцька, О. О., Давиденко, А. М., & Христович, В. (2022). Виділення обличчя людини у відеопотоці для контролю за дотриманням співробітниками стану безпеки в процесі роботи та навчання. *Захист інформації*,

24(2), 94–107.

130. Власенко, В. О. (2024). Застосування сіамських нейронних мереж для порівняння аерофотознімків із картами місцевості. *Вісник Національного технічного університету "ХПІ", 1-2(11–12)*, 153–161.

131. Гаврилович, М. П. (2024). *Верифікація користувача методами глибокого навчання на основі поведінкових та біометричних характеристик* [Дисертація доктора філософії, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»].

132. Долганенко, О. Д., Сєверінов, О. В., В'юхін, Д. О., Коцюба, В. П., & Крепко, А. В. (2023). Аналіз методів виявлення атак біометричної автентифікації за обличчям у мобільних пристроях. *Radiotekhnika*, 215, 13–21.

133. ДСТУ ISO/IEC 19989-1:2023. *Інформаційна безпека. Критерії та методологія оцінювання безпеки біометричних систем. Частина 1. Структура (ISO/IEC 19989-1:2020, IDT)*. (2023). ДП «УкрНДНЦ».

134. ДСТУ ISO/IEC 19989-2:2023. *Інформаційна безпека. Критерії та методологія оцінювання безпеки біометричних систем. Частина 2. Структура (ISO/IEC 19989-2:2020, IDT)*. (2023). ДП «УкрНДНЦ».

135. ДСТУ ISO/IEC 2382-37:2018. *Інформаційні технології. Словник термінів. Частина 37. Біометрія (ISO/IEC 2382-37:2017, IDT)*. (2018). ДП «УкрНДНЦ».

136. ДСТУ ISO/IEC 24745:2023. *Інформаційні технології. Кібербезпека та захист конфіденційності. Захист біометричної інформації (ISO/IEC 24745:2022, IDT)*. (2023). ДП «УкрНДНЦ».

137. Закон України. (2017). Про основні засади забезпечення кібербезпеки України (№ 2163-19). *Відомості Верховної Ради (ВВР)*, 45, ст. 403.

138. Закон України. (2023). Про критичну інфраструктуру (№ 1882-20). *Відомості Верховної Ради (ВВР)*, 5, ст. 13.

139. Ільєнко, А., Ільєнко, С., Яковенко, О., Галич, Є., & Павленко, В. (2024). Перспективи інтеграції штучного інтелекту в системи кібербезпеки. *Кібербезпека: освіта, наука, техніка*, 1(25), 318–329.

140. Ільєнко, А., Телющенко, В., & Дубчак, О. (2025). Сучасні кіберзагрози критичної інфраструктури України та світу. *Кібербезпека: освіта, наука, техніка*, 3(27), 150–164.

141. Кабінет Міністрів України. (2019). Постанова Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури (№ 518). Отримано 19 жовтня 2025, з <https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF>.

142. Квашук, Д., Гріненко, С., Гріненко, О., Фесенко, В., Фесенко, А., & Дуднік, А. (2023). Моделі та методи визначення проникнення в охоронні об'єкти засобами бездротових сенсорних мереж. *European Science*, 1(sge21-01), 161–171.

143. Корченко, О. Г., & Терейковський, О. І. (2024). Neural network analysis of images [Свідоцтво про авторське право на твір (комп'ютерна програма) № 123672]. *Бюлетень № 80*.

144. Корченко, О. Г., & Терейковський, О. І. (2024). Модель процедури розпізнавання особи за зображенням обличчя та райдужною оболонкою ока при біометричній автентифікації персоналу об'єктів критичної інфраструктури із застосуванням нейромережових засобів. *Захист інформації*, 26(1), 157–170.

145. Корченко, О. Г., & Терейковський, О. І. (2024). Модульна нейромережева модель біометричної автентифікації персоналу об'єктів критичної інфраструктури за зображенням обличчя та райдужною оболонкою ока. *Безпека інформації*, 30(2), 339–347.

146. Корченко, О., & Терейковський, О. І. (2025). Метод біометричної автентифікації персоналу об'єктів критичної інфраструктури за зображенням обличчя та райдужною оболонкою ока із застосуванням нейромережових засобів. *Кібербезпека: освіта, наука, техніка*, 1(29), 92–106.

147. Корченко, О., & Терейковський, О. І. (2025). Семантична сегментація зображення обличчя в системах біометричної аутентифікації персоналу об'єктів критичної інфраструктури. *Кібербезпека: освіта, наука, техніка*, 4(28), 385–399.

148. Корченко, О. Г., Козловський, В. В., Міщенко, А. В., & Терейковський, О. І. (2025). Визначення функціональних вимог до

мультимодальної системи біометричної аутентифікації персоналу об'єкта критичної інфраструктури з використанням UML-діаграм прецедентів. *Сучасний захист інформації*, 2(62), 68–75.

149. Корченко, О. Г., & Терейковський, О. І. (2023). Аналіз та оцінювання засобів біометричної аутентифікації за зображенням обличчя та райдужної оболонки ока персоналу об'єктів критичної інфраструктури. *Кібербезпека: освіта, наука, техніка*, 1(21), 136–148.

150. Козловський, В. В., Міщенко, А. В., Варченко, О. І., & Левінсон, Г. С. (2016). Метод оперативного управління комплексною системою захисту інформації авіатранспортного комплексу. *Зв'язок*, 48–52.

151. Маслова, Н. О., & Полуніна, Д. О. (2019). Методи біометричної автентифікації при ідентифікації особи. *Науковий вісник ДонНТУ*, 1(2)–2(3), 12–20.

152. Медвінський, С. В. (2026). *Система ідентифікації користувача комп'ютерної системи за динамічними біометричними параметрами* [Дисертація доктора філософії, Чорноморський національний університет імені Петра Могили].

153. Міщенко, А. В., Іщенко, Н. Ф., & Ліщиновська, Н. О. (2023). Безпека держави в енергонезалежності об'єктів критичної інфраструктури. *Наука і техніка сьогодні*, 2(16), 401–416.

154. Міщенко, А. В., & Сидоренко, Л. П. (2023). Моделі управління інноваціями в організаціях: адаптація до сучасних викликів. *Вісник менеджменту та інновацій*, 7(1), 37–51.

155. Назаркевич, М., Возний, Я., & Назаркевич, Г. (2021). Розроблення методу машинного навчання при біометричному захисті із новими методами фільтрації. *Кібербезпека: освіта, наука, техніка*, 3(11), 16–30.

156. Оксіюк, О. Г., Фесенко, А. О., Вялкова, В. І., & Швець, В. А. (2019). Алгоритми виділення текстурних ознак райдужної оболонки ока. *Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка*, 65, 55–63.

157. Про затвердження Методичних рекомендацій щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами: Наказ Адміністрація Держспецзв'язку України від 29.05.2023 № 463. (2023).

158. 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. (2017).

159. Руда, Х. С. (2025). *Удосконалення методів та засобів біометричної автентифікації за голосом з застосуванням технологій машинного навчання* [Дисертація доктора філософії, Національний університет «Львівська політехніка»].

160. Терейковський, І. А., Чернишев, Д. О., Корченко, О. Г., Терейковська, Л. О., & Терейковський, О. І. (2022). Процедура застосування нейронних мереж для сегментації растрових зображень. *Кібербезпека: освіта, наука, техніка*, 2(18), 25–38.

161. Терейковський, О. І. (2022). Проблематика біометричної автентифікації в інформаційних системах об'єктів критичної інфраструктури. У *Матеріали IX Міжнародної науково-технічної Internet-конференції «Сучасні методи, інформаційне, програмне та технічне забезпечення систем керування організаційно-технічними та технологічними комплексами»* (с. 126–127). Київ: НУХТ.

162. Терейковський, О. І. (2023). Характеристика засобів автентифікації персоналу в інформаційних системах об'єктів критичної інфраструктури. У *Матеріали X Міжнародної науково-технічної Internet-конференції «Сучасні методи, інформаційне, програмне та технічне забезпечення систем керування організаційно-технічними та технологічними комплексами»* (с. 140–141). Київ: НУХТ.

163. Терейковський, О. І. (2025). Застосування нейронних мереж при вирішенні завдань біометричної автентифікації на об'єктах критичної інфраструктури. У *Теорія модернізації в контексті сучасної світової науки:*

збірник наукових праць з матеріалами IV Міжнародної наукової конференції, м. Мукачево, 24 січня, 2025 р. (с. 320–323). Вінниця: ТОВ «УКРЛОГОС Груп».

164. Указ Президента України. (2021). Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" (№ 447/2021).

165. Шимкович, В., Чимшир, В., Знова, К., Ювженко, Д., Новаковський, Г., & Теленик, С. (2025). Синтез архітектури сервісів на основі нейромережі з глибоким навчанням. *Адаптивні системи автоматичного управління*, 2(47), 231–249.

166. Шостак, А. В. (2024). Про особливості формування вхідних даних у сіамській нейронній мережі. *Системи управління, навігації та зв'язку*, 3, 193–195.

167. Шульга, В., Міщенко, А., Моркляник, Б., Лазаренко, С., & Ліщиновська, Н. (2023). План управління безпекою інформаційних активів об'єктів авіатранспортного комплексу України. *Захист інформації*, 25(4), 213–221.

168. Яковенко, О.О., Кушніренко, Н.І., Дорофєєва, І.С. & Євтушенко, А.Р. (2019). Розробка системи розпізнавання осіб на основі згорткової нейронної мережі. *Інформатика та математичні методи в моделюванні*, 9 (1-2), 77-87.

Додаток А. Акти впровадження результатів дисертаційного дослідження

ЗАТВЕРДЖУЮ

Декан Факультету комп'ютерних та
технологій Державного університету
«Київський авіаційний інститут»
Андрій ФЕСЕНКО
2026 р.

АКТ

впровадження результатів дисертаційної роботи

Комісія у складі: голова - завідувач кафедри кібербезпеки Факультету комп'ютерних та технологій (далі – ФКНТ), к.т.н., доцент Ільєнко А.В.; члени комісії - професор кафедри кібербезпеки ФКНТ, д.т.н., професор Ахрамович Володимир Миколайович, доцент кафедри кібербезпеки ФКНТ, к.т.н. Висоцька Олена Олександрівна склали цей акт про те, що результати дисертаційного дослідження здобувача ступеня доктора філософії за спеціальністю 125 «Кібербезпека» Терейковського Олега Ігоревича «Нейромережеві методи та моделі біометричної автентифікації в інформаційних системах об'єктів критичної інфраструктури» впроваджені в Державному університеті «Київський авіаційний інститут» при виконанні держбюджетної науково-дослідної роботи «Система забезпечення кібербезпеки та стійкості об'єктів критичної інфраструктури» (№ДР 5-2024/18.02, 2024-2025 рр.). Зокрема, у ході виконання науково-дослідної роботи використано метод побудови засобів семантичної сегментації зображення обличчя, що забезпечив підвищення точності виділення контурів обличчя в 1,2-1,25 рази та забезпечив можливість приблизно в 10 разів зменшити обсяг експериментальних досліджень, спрямованих на визначення архітектурних параметрів нейромережевої моделі.

Використання зазначених результатів дозволило підвищити рівень кіберзахисту інформаційних систем об'єктів критичної інфраструктури та забезпечити оперативність розробки спеціалізованих нейромережевих засобів.

Голова комісії
к.т.н., доц.

Анна ІЛЬЄНКО

Члени комісії
д.т.н., проф.

Володимир АХРАМОВИЧ

к.т.н.

Олена ВИСОЦЬКА

ЗАТВЕРДЖУЮ

Декан Факультету комп'ютерних та
технологій Державного університету
«Київський авіаційний інститут»
Андрій ФЕСЕНКО
«12» лютого 2026 р.

АКТ

впровадження результатів дисертаційної роботи Терейковського Олега Ігоровича на тему
«Нейромережеві методи та моделі біометричної автентифікації в інформаційних системах
об'єктів критичної інфраструктури» на здобуття наукового ступеня доктора філософії за
спеціальністю 125 «Кібербезпека»

Комісія у складі: голова - завідувач кафедри кібербезпеки Факультету комп'ютерних та технологій (далі – ФКНТ), к.т.н., доцент Ільєнко А.В.; члени комісії - професор кафедри кібербезпеки ФКНТ, д.т.н., професор Ахрамович Володимир Миколайович, доцент кафедри кібербезпеки ФКНТ, к.т.н. Висоцька Олена Олександрівна цим Актом засвідчує, що результати дисертаційного дослідження Терейковського Олега Ігоровича використані співробітниками кафедри кібербезпеки Державного університету «Київський авіаційний інститут» при підготовці і викладанні курсу лекцій і лабораторних робіт навчальної дисципліни «Технології безпечного доступу» для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Безпека інформаційних і комунікаційних систем» спеціальності 125 «Кібербезпека та захист інформації»

Зокрема впроваджено:

1. Модель процедури розпізнавання особи за зображенням обличчя та райдужною оболонкою ока при біометричній автентифікації персоналу об'єктів критичної інфраструктури з застосуванням нейромережевих засобів.
2. Нейромережевий метод біометричної автентифікації за зображенням обличчя та райдужною оболонкою ока в інформаційних системах об'єктів критичної інфраструктури.
3. Архітектуру системи біометричної автентифікації за зображенням обличчя та райдужної оболонки ока персоналу об'єктів критичної інфраструктури.

Голова комісії
к.т.н., доц.

Члени комісії
д.т.н., проф.

к.т.н.

Анна ІЛЬЄНКО

Володимир АХРАМОВИЧ

Олена ВИСОЦЬКА



Товариство з обмеженою відповідальністю «АНТЕ МЕДІАМ»
 01601, м. Київ, Паркова дорога, буд. 16 А, поштова адреса: а/с 367, м. Київ, 01001
 код ЄДРПОУ 37815293

АКТ

впровадження результатів дисертаційної роботи
 «Нейромережеві методи та моделі біометричної автентифікації в
 інформаційних системах об'єктів критичної інфраструктури»
 на здобуття наукового ступеня доктора філософії
 за спеціальністю 125 «Кібербезпека» аспіранта
Терейковського Олега Ігоревича

Комп'ютерна програма «Neural network analysis of images», яка була розроблена в результаті виконання дисертаційної роботи «Нейромережеві методи та моделі біометричної автентифікації в інформаційних системах об'єктів критичної інфраструктури», використана в процесі вдосконалення системи біометричної автентифікації Датацентру «ПАРКОВИЙ» для визначення найбільш ефективної архітектури нейромережевої моделі, що призначена для виділення цільових об'єктів на кольорових, напівтонових та монохромних зображеннях.

Використання вказаної комп'ютерної програми дозволило автоматизувати процедуру визначення архітектурних параметрів нейромережевої моделі, використання якої забезпечило можливість приблизно в 1,2 рази підвищити точність виділення недеформованих завадами контурів зображення обличчя.

Таким чином, результати, отримані Терейковським О.І. під час виконання дисертаційної роботи, дозволили підвищити ефективність системи біометричної автентифікації датацентру «ПАРКОВИЙ».

Директор
 ТОВ «АНТЕ МЕДІАМ»



Володимир ПОКАТІЛОВ



Київ, Паркова дорога 16А,
 01601, а/с 367, 01001



Код ЄДРПОУ 37815293
 +38 (044) 377-77-77



info@datapark.com.ua



datapark.ua

ЗАТВЕРДЖУЮ:
ЛЬВІВСЬКА ТОРГОВО-ПРОМИСЛОВА
ПАЛАТА
Віцепрезидент В. Б. КОРУД



«12» березня 2026 р.

АКТ

про впровадження результатів дисертаційної роботи
«НЕЙРОМЕРЕЖЕВІ МЕТОДИ ТА МОДЕЛІ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ В
ІНФОРМАЦІЙНИХ СИСТЕМАХ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ»
на здобуття наукового ступеня доктора філософії за спеціальністю 125 «Кибербезпека»
аспіранта Державного університету «Київський авіаційний інститут»
Терейковського Олега Ігоревича

Цей акт складено комісією на чолі з Володимиром Богдановичем Корудом, про те, що запропоновані в дисертаційній роботі рішення, а саме - модель процедури розпізнавання особи за зображенням обличчя та райдужною оболонкою ока при біометричній автентифікації персоналу об'єктів критичної інфраструктури з застосуванням нейромережових засобів та модульна нейромережева модель біометричної автентифікації були використані в Львівській торгово-промисловій палаті в процесі вдосконалення комплексної системи захисту інформації. Зокрема, використано:

- підхід до співвіднесення функціоналу модулів із виконанням завдань біометричної автентифікації, які доцільно виконувати за допомогою окремої нейронної мережі, з урахуванням можливості використання апробованих вільнодоступних нейромережових засобів;
- підхід до розпізнавання спуфінг-атак за природністю емоцій та артефактами зовнішнього оточення
- розроблену множину критеріїв, що використовуються при побудові засобів розпізнавання особи для оцінювання ефективності процедури розпізнавання.

Використання запропонованих рішень дозволило приблизно в 10 разів зменшити обсяг експериментів, необхідних для визначення архітектурних параметрів нейромережевої моделі біометричної автентифікації, підвищити ефективність розпізнавання спуфінг-атак та деталізувати напрямки вдосконалення засобів біометричної автентифікації, що входять до складу комплексної системи захисту інформації.

Голова комісії

Віцепрезидент ЛТПП

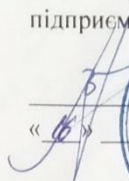
Члени комісії:

Радник президента

Володимир КОРУД

Владислав Хвостенко

ЗАТВЕРДЖУЮ

Директор ТОВ «Науково-виробниче
підприємство хімічних продуктів»


 Володимир ЩЕРБАНЬ

АКТ

 впровадження результатів дисертаційної роботи аспіранта
 Державного університету «Київський авіаційний інститут»
 Терейковського Олега Ігоревича

Комісія у складі голови - провідного фахівця інформаційних технологій Бондарцева П.Є. та членів комісії - фахівця інформаційних технологій Зуя В.Ф., цим Актом засвідчує, що результати дисертаційного дослідження аспіранта кафедри кібербезпеки Державного університету «Київський авіаційний інститут» Терейковського Олега Ігоревича на тему: «Нейромережеві методи та моделі біометричної автентифікації в інформаційних системах об'єктів критичної інфраструктури», поданої на здобуття наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека», впроваджено на ТОВ «Науково-виробниче підприємство хімічних продуктів» в процесі вдосконалення архітектури системи біометричної автентифікації. При цьому використано модель процедури розпізнавання особи за зображенням обличчя та райдужною оболонкою ока при біометричній автентифікації персоналу об'єктів критичної інфраструктури з застосуванням нейромережевих засобів, модульну нейромережеву модель біометричної автентифікації та архітектуру системи біометричної автентифікації за зображенням обличчя та райдужної оболонки ока персоналу об'єктів критичної інфраструктури. Використання означених рішень забезпечило підґрунтя для впровадження в систему біометричної автентифікації спеціалізованих сервісів, які дозволяють проводити розпізнавання спуфінг-атак за розширеним переліком ознак та реалізовувати визначення відповідності поточного психоемоційного стану персоналу щодо належного виконання службових обов'язків на об'єкті критичної інфраструктури.

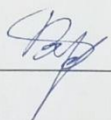
Комісія вважає, що запропоновані рішення мають вагому теоретичну та практичну значимість для підвищення ефективності систем біометричної автентифікації на об'єктах критичної інфраструктури.

Голова комісії



Павло БОНДАРЦЕВ

Члени комісії



Віталій ЗУЙ

ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ «АЙТІ КУРСОР»

Ідентифікаційний код за ЄДРПОУ: 40123706. Юридична адреса: 03124, м. Київ, бульвар Вацлава Гавела, 8. Фактична адреса: 03124, м. Київ, бульвар Вацлава Гавела, 8.

Поточний рахунок: UA74 305299 00000 26007025022694 в ПАТ КБ «ПРИВАТБАНК» МФО: 305299

<http://www.itcursor.com.ua> E-mail: info@itcursor.com.ua тел/факс +38(044) 501-12-03



ЗАТВЕРДЖЕНО

« 27 » листопада 2025 р.

АКТ

впровадження результатів дисертаційної роботи аспіранта
Державного університету «Київський авіаційний інститут»
Терейковського Олега Ігоревича

Комісія у складі голови - директор, Сенчіло Ярослав В'ячеславович та членів комісії, головний інженер Сєдих Денис Сергійович і Остапчук Валентин Віталійович, цим Актом засвідчуює, що результати дисертаційного дослідження аспіранта Київського авіаційного інституту Терейковського Олега Ігоревича на тему: «Нейромережеві методи та моделі біометричної автентифікації в інформаційних системах об'єктів критичної інфраструктури», поданої на здобуття наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека», впроваджено на ТОВ «Айті Курсор» в процесі вдосконалення архітектури системи біометричної автентифікації. При цьому використано модель процедури розпізнавання особи за зображенням обличчя та райдужною оболонкою ока при біометричній автентифікації персоналу об'єктів критичної інфраструктури з застосуванням нейромережевих засобів, модульну нейромережеву модель біометричної автентифікації та архітектуру системи біометричної автентифікації за зображенням обличчя та райдужної оболонки ока персоналу об'єктів критичної інфраструктури. Використання означених рішень забезпечило підґрунтя для впровадження в систему біометричної автентифікації спеціалізованих сервісів, які дозволяють проводити розпізнавання спуфінг-атак за розширеним переліком ознак та реалізовувати визначення відповідності поточного психоемоційного стану персоналу щодо належного виконання службових обов'язків на об'єкті критичної інфраструктури.

Комісія вважає, що запропоновані рішення мають вагомий теоретичний та практичний значимість для підвищення ефективності систем біометричної автентифікації на об'єктах критичної інфраструктури.

Голова комісії
Члени комісії

Сенчіло Я.В.

Остапчук В.В.

Сєдих Д.С.



АКТ ВПРОВАДЖЕННЯ

результатів дисертаційного дослідження здобувача ступеня доктора філософії за спеціальністю 125 «Кібербезпека» Терейковського Олега Ігоревича «Нейромережеві методи та моделі біометричної автентифікації в інформаційних системах об'єктів критичної інфраструктури»

Цим актом підтверджується, що результати дисертаційного дослідження аспіранта кафедри кібербезпеки Державного університету «Київський авіаційний інститут» Терейковського О. І. на тему «Нейромережеві методи та моделі біометричної автентифікації в інформаційних системах об'єктів критичної інфраструктури» використано в діяльності ТОВ «ОПТОЕЛЕКТРОНІКА» для оцінювання відповідності характеристик світлодіодного освітлення встановленим вимогам. Зокрема використано рішення щодо оцінювання якості та попередньої обробки зображення, наведені в описі моделі процедури розпізнавання особи за зображенням обличчя та райдужною оболонкою ока при біометричній автентифікації персоналу об'єктів критичної інфраструктури з застосуванням нейромережевих засобів та в описі нейромережевого методу біометричної автентифікації за зображенням обличчя та райдужною оболонкою ока в інформаційних системах об'єктів критичної інфраструктури.

Директор ТОВ «ОПТОЕЛЕКТРОНІКА»

«24» грудня 2025р



Інна ШОХІНА

**ДОДАТОК Б. Лістинг (код) програмного застосунку для сегментації
зображення**

```
from pathlib import Path
import keras
import cv2
from glob import glob
import numpy as np
import os
import matplotlib.pyplot as plt
import tensorflow as tf
from tensorflow import keras
from tensorflow.keras.layers import Conv2D, BatchNormalization, MaxPool2D,
Dense, Activation, Conv2DTranspose, Concatenate, Input
from tensorflow.keras.models import Model
from tensorflow.keras.models import load_model
import matplotlib.cm as cm

def conv_block(inputs, num_filters):
    x = Conv2D(num_filters, 3, padding = 'same')(inputs)
    x = BatchNormalization()(x)
    x = Activation("relu")(x)

    x = Conv2D(num_filters, 3, padding = 'same')(x)
    x = BatchNormalization()(x)
    x = Activation("relu")(x)

    return x

def encoder_block(inputs, num_filters):
```

```
x = conv_block(inputs, num_filters)
p = MaxPool2D((2,2))(x)
```

```
return x, p
```

```
def attention_block(s, g, num_filters):
    ws = Conv2D(num_filters, 1, padding = 'same')(s)
    ws = BatchNormalization()(ws)

    wg = Conv2D(num_filters, 1, padding = 'same')(g)
    wg = BatchNormalization()(wg)

    res = Activation('relu')(ws + wg)
    res = Conv2D(num_filters, 1, padding = 'same')(res)
    res = Activation('sigmoid')(res)

    return res * s
```

```
def decoder_block(inputs, skip_feat, num_filters):
    x = Conv2DTranspose(num_filters, 3, 2, padding = 'same')(inputs)
    s = attention_block(x, skip_feat, num_filters)
    s = Concatenate()([x,s])
    s = conv_block(s, num_filters)

    return s
```

```
def unet_model(input_shape):
    inputs = Input(input_shape)

    # Encoder Block
```

```

skip1, res1 = encoder_block(inputs, 64)
skip2, res2 = encoder_block(res1, 128)
skip3, res3 = encoder_block(res2, 256)

b1 = conv_block(res3, 512)

# Decoder Block
out1 = decoder_block(b1, skip3, 256)
out2 = decoder_block(out1, skip2, 128)
out3 = decoder_block(out2, skip1, 64)

# Output
final = Conv2D(num_classes, 1, padding='same', activation='softmax')(out3)

model = Model(inputs, final, name="UNET_Model")

return model

def read_image(path, W=128, H=128):
    x = cv2.imread(path, cv2.IMREAD_COLOR)
    x = cv2.resize(x, (W, H))
    x = x/255.0
    x = x.astype(np.float32)
    return x

H = 128
W = 128
num_classes = 11

custom_objects = {
    "conv_block": conv_block,

```

```

"encoder_block": encoder_block,
"attention_block": attention_block,
"decoder_block": decoder_block,
}

def process_segmented_dataset(
    src_path,
    dest_path,
    bg_color="black"
):
    """
    Args:
        src_path (str): Path to 'lfw_arcface_experiment'
        dest_path (str): Path to save results
        model_wrapper (keras.Layer): Your loaded TFSMLayer
        bg_color (str): "black", "white", or "mask_only"
    """
    source_base = Path(src_path)
    output_base = Path(dest_path)

    new_model_path = "./new_format_models/new_model_path"
    model_wrapper = keras.layers.TFSMLayer(new_model_path,
call_endpoint='serving_default')
    print("Model loaded successfully.")
    # Create base output directory
    output_base.mkdir(parents=True, exist_ok=True)

    print(f"Starting segmentation. Target Background: {bg_color}")

    for person_folder in source_base.iterdir():

```

```

if not person_folder.is_dir():
    continue
# Create subfolder for the person
target_person_dir = output_base / person_folder.name
target_person_dir.mkdir(exist_ok=True)

for image_file in person_folder.glob("*.jpg"):
    # 1. Load and Preprocess
    img_bgr = cv2.imread(str(image_file))
    # Your model expects 128x128 based on your previous snippet
    img_input = cv2.resize(img_bgr, (128, 128))
    check = (img_input.reshape((1, 128, 128, 3)).astype(np.float32)) / 255.0
    # 2. Inference
    pred_output = model_wrapper(check)
    pred = pred_output["conv2d_23"].numpy()[0]
    mask = np.argmax(pred, axis=-1) # Shape (128, 128)
    # 3. Create Binary Mask (Assuming class 0 is background, others are face)
    # Adjust '0' if your model uses a different index for background
    binary_mask = np.where(mask > 0, 1, 0).astype(np.uint8)
    # 4. Apply Background Logic
    if bg_color == "mask_only":
        # Save the halftone/viridis as you did before
        final_output = (mask * (255 / 11)).astype(np.uint8)
    else:
        # Expand mask to 3 channels for multiplication
        mask_3ch = np.dstack([binary_mask] * 3)

        if bg_color == "white":
            bg = np.ones_like(img_input) * 255
        else: # default black

```

```

        bg = np.zeros_like(img_input)
        # Combine: (Face * Mask) + (Background * Inverse Mask)
        final_output = (img_input * mask_3ch) + (bg * (1 - mask_3ch))
        # 5. Save Result
        file_name = f"{image_file.stem}_{bg_color}.png"
        cv2.imwrite(str(target_person_dir / file_name), final_output)

    print(f"Done! Results saved to {dest_path}")

# --- EXAMPLE USAGE FOR YOUR PHASING ---
# P6 - Variant 1: Black Background
process_segmented_dataset(

src_path="../../../ImageComparison/ArcFace_experiments_5_04_2026/code_python/l
fw_arcface_experiment_one_face",

dest_path="../../../ImageComparison/ArcFace_experiments_5_04_2026/code_python/
lfw_arcface_experiment_one_face_segmented/lfw_segmented_black",
    bg_color="black"
)
# P6 - Variant 2: White Background
process_segmented_dataset(

src_path="../../../ImageComparison/ArcFace_experiments_5_04_2026/code_python/l
fw_arcface_experiment_one_face",

dest_path="../../../ImageComparison/ArcFace_experiments_5_04_2026/code_python/
lfw_arcface_experiment_one_face_segmented/lfw_segmented_white",
    bg_color="white"
)

```