[17]. «Digital signature». Wikipedia, (2024), [Електронний ресурс]. https: // en.wikipedia.org / wiki/Digital_signature. Дата доступу 27 березня 2024.
[18]. Golub O.S., Grigorenko O.G., Repa F.M. (2023). "Data confidentiality in information communication networks and means of ensuring it" (https://ela.kpi.ua/ server / api / core / bitstreams/2c8ad1be-8812-4195-a5a5-f68ca0d5b974/content)

SECURITY SYMBOLS: INTEGRATING CRYPTOGRAPHY WITH CYBER SECURITY TO PROTECT DIGITAL SYSTEMS

Cyber security is a set of procedures aimed at protecting computer systems, networks and data from unauthorized access. In today's digital environment, cyber security has become critical for business, administration and management, as well as for private individuals, as threats from cyber-attacks are ever increasing. The modern world is inextricably linked with the latest technologies that permeate all spheres of our lives. However, the growing dependence on digital technologies leads to cyber threats that can affect the security and stability of society. Integrating cryptography with cybersecurity is the answer to these challenges. A strategic approach to ensuring the security of information technology is the integration of cryptography, which is based as security against unauthorized access and to ensure authentication and inaccessibility of data or systems. The merger of cryptography with cyber security allows to create a comprehensive approach to the protection of digital systems, taking into account modern risks and problems. The increase in the number and complexity of threats requires constant improvement of methods that will allow adapting to modern and future attacks, ensuring effective protection of digital systems and the relevance of the problem in today's digital world. Let's consider the importance of the role of the human factor in ensuring cyber security and possible approaches to take this aspect into account when developing and implementing cryptographic solutions. In addition, an analysis of Ukrainian qualified electronic signatures is conducted, which is an improved form of electronic signature, ensuring a high level of protection and authenticity of electronic documents in a technological environment.

Keywords: security symbols, cryptography, cyber security, authentication, digital signature, encryption, network security, digital systems, hash function, privacy.

Михайлишин Катерина Василівна, студентка кафедри захисту інформації Національного університету «Львівська політехніка».

Kateryna Mykhailyshyn, student at the Department of Information Security, Lviv Polytechnic National University.
E-mail: Kateryna.mykhailyshyn.kb.2022@lpnu.ua.
Orcid ID: 0009-0009-4835-6958.

Опірський Іван Романович, д.т.н., професор, завідувач кафедри захисту інформації Національного університету «Львівська політехніка».

Ivan Opirskyy, Doctor of Technical Sciences, Professor, Head of the Department of Information Security, National University "Lviv Polytechnic".
E-mail: ivan.r.opirskyi@lpnu.ua.
Orcid ID: 0000-0002-8461-8996.

DOI: 10.18372/2410-7840.26.18839
УДК 681.3.06

МОДЕЛЬ ПРОЦЕДУРИ РОЗПІЗНАВАННЯ ОСОБИ ЗА ЗОБРАЖЕННЯМ ОБЛИЧЧЯ ТА РАЙДУЖНОЮ ОБОЛОНКОЮ ОКА ПРИ БІОМЕТРИЧНІЙ АВТЕНТИФІКАЦІЇ ПЕРСОНАЛУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ІЗ ЗАСТОСУВАННЯМ НЕЙРОМЕРЕЖЕВИХ ЗАСОБІВ

Олександр Корченко, Олег Терейковський

Виклики сьогодення визначають необхідність вдосконалення засобів біометричної автентифікації персоналу об'єктів критичної інфраструктури. Поширені засоби біометричної автентифікації, що як правило базуються на використанні нейромережевих технологій аналізу зображення обличчя, в багатьох випадках не достатньо адаптовані до умов розпізнавання під час виконання персоналом своїх функціональних обов'язків, що характеризуються впливом різноманітних завад при відеореєстрації та підвищенням ймовірності атак за допомогою муляжів. Ще один перспективний напрямок вдосконалення визначається доступністю сучасних засобів відеореєстрації, які забезпечують додаткову можливість розпізнавання особи за райдужною оболонкою ока та можливість розпізнавання емоцій, що дозволяє оцінити психоемоційний стан представників персоналу. Показано, що першим етапом вдосконалення нейромережевих засобів біометричної автентифікації є розробка формалізованого опису процедури розпізнавання, яка враховує перспективні напрямки вдосконалення. Запропоновано відповідну модель, що забезпечує формалізований опис і критерії оцінки ефективності кожної із операцій та процедури розпізнавання в цілому. При цьому вперше обґрунтовано перелік критеріїв оцінки якості попередньої обробки зображень, що підлягають нейромережевому аналізу в системі біометричної автентифікації та вперше запропоновано підходи до визначення параметрів завад та розпі-

знавання атак за допомогою муляжів. Підхід до визначення параметрів завад передбачає співставлення параметрів завад з місцезнаходженням та кількістю ключових і контрольних обличчя, які вони перекривають. Розпізнавання атак пропонується реалізовувати на основі аналізу динаміки базових емоцій, динаміки параметрів руху очей та навколишнього середовища. Результати цього дослідження є важливими в контексті розробки ефективних засобів біометричної автентифікації, оскільки забезпечують формалізований опис вимог до функціональних можливостей основних складових цієї процедури розпізнавання особи та емоцій персоналу об'єктів критичної інфраструктури.

***Ключові слова**: модель, критична інфраструктура, зображення обличчя, райдужна оболонка ока, нейронна мережа, біометрична автентифікація, захист інформації, безпека інформації.*

ВСТУП

В умовах сучасного світу навіть незначне порушення безпеки об'єктів критичної інфраструктури може викликати суттєвий негативний вплив на соціальну та економічну сфери держави, рівень її обороноздатності та національної безпеки [26]. Так в [26] 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 об'єкту критичної інфраструктури (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 [26]. Безпека ОКІ забезпечується в тому числі і за рахунок здійснення заходів забезпечення кіберзахисту що регулюється окремим законом України [27]. 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. 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 [28].

Для забезпечення ефективної ідентифікації та автентифікації персоналу використовується широкий спектр засобів, зокрема, на сьогодні відоме використання систем біометричної автентифікації (БА) за зображенням обличчя (ЗО) та райдужної оболонки ока (РОО) [23]. Це передусім пояснюється широким розповсюдженням та доступністю відеокамер, які здатні з високою якістю реєструвати відповідні біометричні параметри, що забезпечує можливість достатньо точної ідентифікації та автентифікації персоналу. Водночас результати [23] та практичний досвід вказують на недостатню точність таких систем автентифікації в ракурсі розпізнавання особи при негативному впливі типових завад. Крім того, в сучасних умовах для якісного 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 в напрямку підвищення рівня безпеки об'єктів критичної інфраструктури за рахунок розробки та впровадження систем біометричної автентифікації, що забезпечують розпізнавання особи й емоційного стану персоналу об'єктів критичної інфраструктури.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

В процесі аналізу науково-практичних робіт присвячених розробці засобів розпізнавання особи та емоційного стану людини увага акцентувалась на визначенні перспективних рішень, які можливо використати для забезпечення ефективного функціонування систем БА персоналу ОКІ.

В роботі [25] розглянута задача виділення обличчя людини у потоці відео з метою контролю за дотриманням безпеки у процесі роботи та навчання. Досліджено використання технології MobileSSD для виділення обличчя людини у відеопотоці в режимі реального часу. Експерименти проводились в умовах різних перешкод, серед яких – наявність на обличчі окулярів, наявність на обличчі сторонніх предметів, які заважають фіксації характерних точок обличчя та ін. Також ефективність технології визначалась у різних умовах рівню освітлення, відстані від обличчя до камери. Наведено результати експериментальних досліджень, що відображають залежність впевне-

ності системи виділення у результатах виділення обличчя під впливом перешкод і зміни умов. Визначено, що поворот обличчя найчастіше призводить до неможливості його виділення, також є доцільною періодична перевірка положення обличчя для уточнення, що зафіксовано саме обличчя людини, а не її фотографія. В статті [10] означено використання технологій комп'ютерного зору для вирішення задачі розпізнавання обличчя, очей і РОО в режимі реального часу. Авторами запропоновано застосування підходу Blob Analysis для ідентифікації обличчя та очей на зображенні, для сегментації – використання порогової функції, яка ізолює пікселі у фоновому режимі, а для виділення райдужної оболонки ока – застосування підходу Circle Hough. Задекларовано, що використання даних рішень дозволяє досягнути високих результатів розпізнавання на зображеннях низької якості.

В роботі [22] розглянуто використання методів глибокого навчання для розпізнавання емоцій людини за ЗО. Авторами було реалізовано розпізнавання проводилось розпізнавання 7 емоцій - щастя, подив, огида, смуток, гнів, страх та нейтральність. Для виділення обличчя, очей та рота використано попередньо навчений каскадний класифікатор Хаара. Для розпізнавання емоцій автори використали модель згорткової нейронної мережі (НМ) типу LeNet, попередньо провівши її навчання на базі даних FER-2013, що складається із 28709 маркованих зображень у навчальній вибірці та 3589 у тестовій вибірці. Вказано, що мережа навчалась за методом «з вчителем» та «з підкріпленням». Заявлено про точність розпізнавання 0,62 на тестовій вибірці.

В роботі [12] були проведені експериментальні дослідження з метою виявити залежність розпізнавання людиною емоції актора за виразом його обличчя від наявності на обличчі маски. Розпізнавались такі емоції, як щастя, смуток, гнів, здивування, страх, огиду та нейтральність. Було виявлено, що наявність маски погіршує розпізнавання емоції на обличчі приблизно на 20%. Зокрема, найбільше це стосується емоцій огиди, страху, здивування, смутку та щастя. Додатково було виявлено, що експерти, які звикли спілкуватись з людьми із маскою на обличчі, розпізнавали емоції краще.

В статті [9] додатково до впливу наявності маски аналізується також вплив наявності сонцезахисних окулярів на розпізнавання емоції актора та його ідентифікації за обличчям. Було виявлено, що на відміну від наявності маски наявність сонцезахисних окулярів не знижує точність ідентифікації та розпізнавання емоцій. Автори, посилаючись на [9, 12], стверджують, що область очей є найбільш інформативною для ідентифікації та розпізнавання емоцій за обличчям.

Система FaceReader від компанії Noldus Information Technology [https: // www.noldus.com/ facereader] надає можливість розпізнавання емоції людини за ЗО, використовуючи попередньо навчену НМ. Також система фіксує деякі додаткові дані, такі як стать людини, її вік, наявність бороди, напрямок погляду, орієнтація голови та ін. Для навчання НМ було використано понад 20 000 зображень, на яких вручну виділено 468 ключових точок обличчя людини. Для виділення обличчя використовується метод головних компонент.

Система Captemo [https://www.captemo.com] від компанії Logic Pursuits призначена для розпізнавання емоцій людини за її обличчям в режимі реального для оцінки рівня задоволення клієнтів у сфері обслуговування. Використовуючи засоби штучного інтелекту та хмарних обчислень, система здатна розпізнавати емоції до десяти людей одночасно. Додатково Captemo фіксує деякі інші внутрішні і зовнішні дані, зокрема рівень продажів компанії, дані про співробітників, погоду та ін., що дозволяє аналізувати залежність рівня задоволення клієнтів послугами від певного часу доби, часу робочої зміни певного співробітника та інших параметрів.

Система BioObserver [https://hertasecurity.com / advanced – solution-facial-expression-analysis/] від компанії Herta здатна розпізнавати сім базових емоцій людини за її обличчям як в режимі аналізу відео в реальному часі, так і в режимі аналізу попередньо записаного відеоряду. Водночас система розпізнає вісімнадцять мікроекспресій обличчя, таких як нахмуреність, моргання, підняття брів та ін., а також відслідковує направлення напрямку погляду та орієнтацію голови, що дає можливість відслідковувати рівень уваги людини.

Хоча результати проведеного аналізу науково-практичних робіт та відомих програмно-апаратних рішень в області БА за ЗО та РОО вказують на доцільність їх застосування на ОКІ, однак результати [1, 8, 9, 12] та практичний досвід свідчать про ускладнення процедури ідентифікації та автентифікації за ЗО та РОО при впливі завад, пов'язаних з носінням масок, окулярів, зміни зачіски, зміни кута нахилу голови людини відносно об'єктиву відеокамери, недостатнім, занадто високим та нерівномірним освітлення. Та-

кож можливо зробити висновок про найбільшу перспективність аналізу ЗО та РОО за допомогою нейромережевих засобів (НМЗ). Ще одним важливим напрямком вдосконалення засобів БА на основі ЗО та РОО є необхідність підвищення ефективності захисту від атак за допомогою муляжів [23], що зумовлює необхідність їх розпізнавання. При цьому поширені засоби розпізнавання базуються на аналізі якості підконтрольного зображення [4, 13, 14], аналізі його просторових характеристик [11], перевірці динаміки параметрів характерній для ЗО і РОО живої людини [21] та виконанні підконтрольною особою певних команд, що спричиняють зміну параметрів відеореєстрації [3]. 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 відеореєстарції однією камерою. Труднощі визначення просторових характеристик виникають і при застосуванні декількох камерами 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. 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, необхідність визначення особи та емоційного стану персоналу, а також механізму визначення ефективності процесу БА.

Таким чином, метою дослідження є розробка моделі, що забезпечує формалізований цілісний опис процедури розпізнавання особи за зображенням обличчя та райдужною оболонкою ока при біометричній автентифікації персоналу об'єктів критичної інфраструктури з застосуванням нейромережевих засобів з урахуванням необхідності визначення емоцій та виявлення атак за допомогою муляжів.

ОСНОВНА ЧАСТИНА

Як показують результати огляду літературних джерел, в моделі процедури розпізнавання особи за ЗО та РОО при БА персоналу ОКІ з застосуванням НМЗ слід відобразити термінологію, що враховує особливості прикладної області, аналітичні вирази, які відображають перетворення інформації, підходи до реалізації окремих операцій процедури розпізнавання, загальну схему реалізації процедури та критерії оцінювання ефективності основних операцій та процедури в цілому, що враховують сучасні технології їх реалізації.

Використовуючи результати [7, 16, 24] при розробці моделі використано наступні терміни:

- нейромережева модель (НММ) – модель, що описує архітектуру НМ та нейрони, які входять до її складу;
- РОО – це забарвлене кільце в передній частині зіниці, що складається з м'язової та сполучної тканин і пігментних клітин, що змінює розмір зіниці ока;
- 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 базується за рахунок подачі сенсору для зчитування підроблених біометричних даних;
- 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, відраза, сум, страх, здивування, презирство, радість;
- ключові точки – точки обличчя, які використовуються для розпізнавання емоцій;
- контрольні точки – точки голови людини, які використовуються для розпізнавання особи.

В першому наближенні можливо вважати, що множина контрольних точок входить до множини ключових точок. Також результати [5, 24, 29] вказують на те, що до множини як контрольних так і ключових точок входять точки на зображенні очей людини.

Враховуючи специфіку проблеми розробки НМЗ БА персоналу ОКІ, в базовому випадку запропонована модель призначена для опису процесів нейромережевої обробки зареєстрованого відеопотоку для розпізнавання особи персоналу ОКІ і наявності атаки за допомогою муляжів на систему БА за ЗО та РОО. Тому в базовому випадку модель розпізнавання можливо відобразити за допомогою виразів виду:

$$\langle \Theta, C \rangle \overset{NR}{\rightarrow} \langle I, E, A \rangle, \quad (1)$$

де Θ – множина параметрів, що характеризують умови відеореєстрації; C – множина параметрів, що характеризують контент кожного із кадрів відеопотоку; I – множина параметрів, що описують результат розпізнавання особи; E – множина параметрів, що описують результат розпізнавання емоцій; A – результат розпізнавання атаки за допомогою муляжів; N, J, K – потужність множин C, I, A; NR – оператор нейромережевого розпізнавання.

В свою чергу:

$$\Theta = |\theta_1, \dots, \theta_q|, \quad (2)$$

де q –кількість параметрів, що описують якісні характеристики вхідного відеопотоку.

Враховуючи [17, 19, 22] та специфіку задачі нейромережевого аналізу ЗО та РОО для розпізнавання особи та емоцій прийнято, що умови реєстрації характеризуються відстанню та взаємною орієнтацією в просторі між відеокамерою та об'єктом, освітленістю при відеореєстрації та характеристиками відеокамери. Характеристики та умови відеореєстрації для окремо взятої відеокамери можливо оцінити за допомогою наступних параметрів: θ_1 – мінімально допустимий рівень освітленості (чутливість відеокамери) без використання інфрачервоної підсвітки; θ_2 – максимально допустимий рівень освітленості; θ_3 – кут огляду відеокамери по горизонталі; θ_4 – кут огляду камери по вертикалі; θ_5 – частота кадрів у відеопотоці; θ_6 – формат кольорової гамми; θ_7 – роздільна здатність відеопотоку; θ_8 – дальність дії інфрачервоної підсвітки; θ_9 – максимально можливий кут зміни напрямку відеозйомки по горизонталі при функціонуванні відеокамери в режимі відслідковування об'єкта; θ_{10} – максимально можливий кут зміни напрямку відеозйомки по вертикалі при функціонуванні відеокамери в режимі відслідковування об'єкта; θ_{11} – дальність дії підсвітки у видимому діапазоні світла (біла підсвітка); θ_{12} – відстань від відеокамери до обличчя; θ_{13} – кут між напрямком відеозйомки та проекцією обличчя на площину Oxy; θ_{14} – кут між напрямком відеозйомки та проекцією обличчя на площину Oxz; θ_{15} – кут між напрямком відеозйомки та проекцією обличчя на площину Oyz.

Загальним умовам використання системи відеоспостереження в межах однієї локації відповідають параметри: θ_{16} – освітленість; θ_{17} – кількість відеокамер у системі відеоспостереження на одній площадці; θ_{18} – максимально можлива кількість об'єктів, що підлягають одночасному моніторингу; θ_{19} – наявність завад (окуляри, зачіска, маска і т.ін.).

На основі аналізу стандартних рішень в області відеоспостереження визначено, що параметр θ_5 може приймати значення від 7 до 60 кадрів за секунду. Параметр θ_6 може бути RGB, RGBA, BGR, monochrome або CMYK. Параметр θ_7 може приймати такі значення: VGA (640x480 - 0.3Мп), HD (1280x720 - 1 Мп, 1280x960 - 1.3 Мп), FullHD (1920x1080 - 2Мп), UHD (4K-3840x2160 - 8 Мп, 8K - 7680x4320 - 33 Мп). Крім того сучасні системи відеоспостереження забезпечують можливість зміни просторової орієнтації відеокамери, можливість зміни освітленості, можливість подачі команди для уточнення положення обличчя в просторі та для усунення завад при відеореєстрації. Вказані команди можуть подаватись за допомогою голосових сигналів. Наприклад, може бути озвучена команда «Зняти окуляри». Відповідні параметри позначено як $\theta_{20} - \theta_{23}$. Також слід врахувати дискретний характер вхідної інформації НМЗ аналізу відеопотоку, що співвідноситься із кількістю кадрів в пакеті, на основі якого реалізується розпізнавання та з частотою отримання пакетів відеоданих. Відповідні параметри: розмір пакету відеоданих (θ_{24}) та частота прийому пакетів відеоданих (θ_{25}). Таким чином у виразі (2) значення $q = 25$.

Розглянемо множину параметрів, що характеризують контент кожного із кадрів відеопотоку, параметри якого відображені в елементах множини C. Оскільки кожен із кадрів відеопотоку по суті є статичним монохромним або кольоровим зображенням, то окремий елемент множини C можливо представити у вигляді матриці виду:

$$c_n = \begin{vmatrix} d_{1,1} & \dots & d_{1,X} \\ \dots & \dots & \dots \\ d_{Y,1} & \dots & d_{Y,X} \end{vmatrix} \; n = 1 \dots N, \quad (3)$$

де n – n-ий кадр відепоптоку; N – кількість кадрів вхідного відеопотоку; X – розмір кадру по горизонталі; Y – розмір кадру по вертикалі; $d_{x,y}$ – колір пікселя з координатами (x, y).

Кількість елементів множини C дорівнює кількості кадрів відеопотоку, що підлягають нейромережевому аналізу.

При визначенні множини I враховано, що кожен із її елементів i_j трактується як впевненість у тому, що у відеопотоці розпізнано j-го представника персоналу ОКІ. При цьому $0 \le n_j \le 1$. З

урахуванням необхідності визначення, що у відеопотоці має бути розпізнано нелегітимну особу та може взагалі не бути людини, кількість елементів I розраховується так:

$$J = L + 2, \quad (4)$$

де L – кількість легітимних представників персоналу ОКІ.

У випадку, коли j лежить в межах від 1 до L, i_j представляє собою впевненість в тому, що в зареєстрованому відеопотоці розпізнано j-го представника персоналу ОКІ. Для $j = L + 1$, n_j – впевненість в тому, що в зареєстрованому відеопотоці розпізнано нелегітимну особу, а для $j = L + 2$, n_j – впевненість в тому, що у зареєстрованому відеопотоці люди відсутні.

Елементи множини E описують емоції представника персоналу ОКІ, розпізнані на основі нейромережевого аналізу ЗО. Оскільки в більшості авторитетних роботах прийнято, що до множини базових емоцій відносяться радість, гнів, відраза, страх, смуток, здивування та нейтральність, то спектр базових емоцій доцільно описати за допомогою семи параметрів. Таким чином кожен із семи елементів множини E ($e_i \in E, 0 \leq e_i \leq 1$) співвідноситься з проявом відповідної базової емоції на обличчі.

Базуючись на [2, 11, 23] визначено, що у випадку необхідності розпізнавання наявності або відсутності атаки:

$$A = \{a_1; a_2\}, \quad (5)$$

де a_1, a_2 – величини, що свідчать про наявність чи відсутність атаки за допомогою муляжів.

Як і для елементів множини I, величини a_1 та a_2 знаходяться в межах від 0 до 1. У випадку необхідності розпізнавання типу муляжа множина A повинна бути доповнена відповідними елементами. В першому наближенні вважається, що в якості муляжу буде використано: фотографію, відеозапис, маска обличчя представника персоналу ОКІ, обличчя мертвого представника персоналу ОКІ. Також один із елементів множина A може бути співвіднесено із муляжем невідомого типу. Таким чином, вирази (1-5) являються аналітичним представленням базового варіанту моделі розпізнавання особи при БА персоналу ОКІ за ЗО та РОО. Зазначимо, що в цьому випадку модель не відображає операцій обробки інформації, що здійснюються для визначення I, E та A.

Для деталізації базового варіанту моделі проведено декомпозицію процедури розпізнавання особи за ЗО та РОО при БА персоналу ОКІ з урахуванням необхідності розпізнавання емоцій та атак за допомогою муляжів. Відповідно до [6, 15, 22] при декомпозиції процедури розпізнавання особи увагу акцентувано на специфічних операціях, ефективність яких в сучасних системах БА персоналу ОКІ можливо вважати недостатньою. До вказаних операцій слід віднести:

- виділення ЗО та РОО у відеопотоці;
- виявлення та нівелювання завад розпізнавання;
- виявлення атаки за допомогою муляжів.

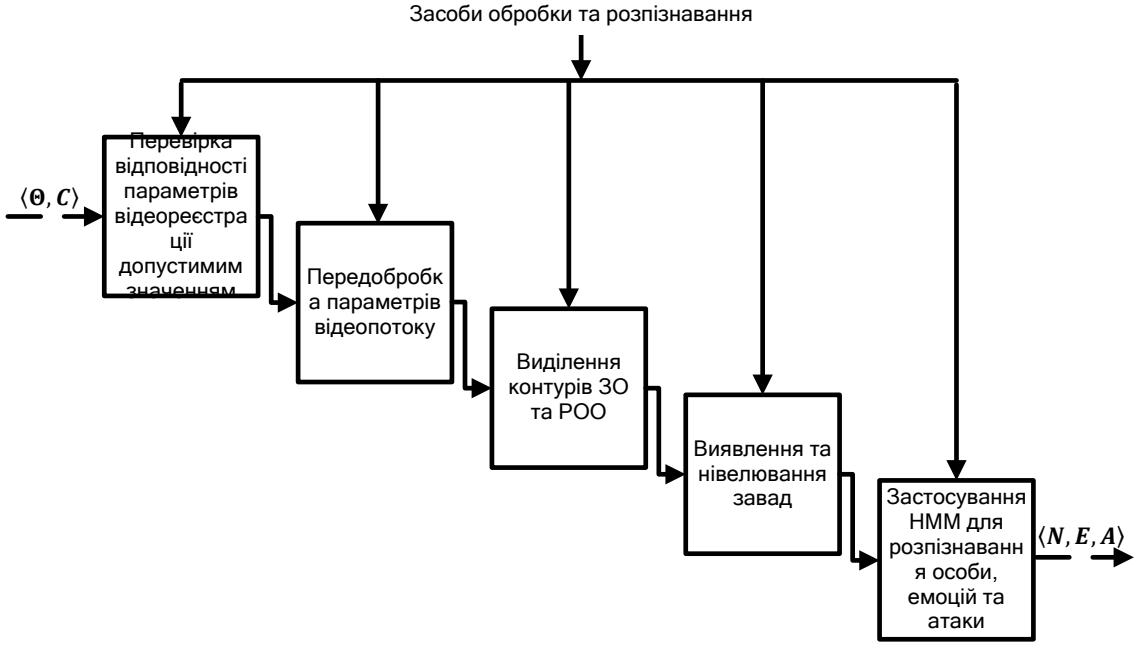

Рис. 1. Діаграма декомпозиції процедури розпізнавання особи за ЗО та РОО при БА персоналу ОКІ з урахуванням необхідності визначення емоцій та виявлення атак за допомогою муляжів

Показана діаграма декомпозиції процедури розпізнавання особи за ЗО та РОО, побудована з урахуванням означених специфічних операцій (рис. 1). При обґрунтуванні переліку операцій, що входять до складу процедури розпізнавання з позицій обмеженості обчислювальних ресурсів, необхідності оперативного реалізації та можливостей сучасних НМЗ аналізу відеопотоку, визначено доцільність проведення однієї операції попередньої обробки вхідного відеопотоку, що реалізується без використання засобів штучного інтелекту.

Враховуючи загальноприйняту технологію нейромережевого аналізу відеопотоку, до параметрів моделі ($\tilde{C}$), що стосуються виділення контурів ЗО та РОО, слід віднести параметри, які описують такі контури у попередньо обробленому відеопотоці. За аналогією із (3) окремий кадр такого обробленого відеопотоку можливо представити у вигляді матриці виду:

$$\tilde{c}_k = \begin{vmatrix} \tilde{d}_{1,1} & \dots & \tilde{d}_{1,\tilde{X}} \\ \dots & \dots & \dots \\ \tilde{d}_{\tilde{Y},1} & \dots & \tilde{d}_{\tilde{Y},\tilde{X}} \end{vmatrix}, \; k = 1 \dots K, \qquad (6)$$

де k – k-ий кадр відеопотоку; K – кількість кадрів вхідного відеопотоку; $\tilde{X}$ – розмір кадру по горизонталі; $\tilde{Y}$ – розмір кадру по вертикалі; $\tilde{c}_{\tilde{x},\tilde{y}}$ – колір пікселя з координатами $(\tilde{x}, \tilde{y})$.

Зазначимо, що в загальному випадку попередня обробка відеопотоку може призвести до його значного видозмінення, тому складові виразу (6) можуть відрізнятись від виразу (3).

Наявність завад при розпізнаванні особи та емоцій представника персоналу ОКІ передбачено описувати за допомогою множини Z. Зазначимо, що наведені в [9, 12, 23, 24] результати досліджень, які стосуються нівелювання завад для розпізнавання особи та емоцій людини за ЗО та РОО вказують на відсутність загальноприйнятого підходу до визначення параметрів завад, що в свою чергу ускладнює їх виявлення та нівелювання.

Тому для опису завад, що стосуються видимості ключових та контрольних точок запропоновано підхід, що передбачає співставлення параметрів завад з їх місцезнаходженням та кількістю ключових та контрольних точок, які вони перекривають.

Базуючись на нормативних вимогах та рекомендаціях [29] передбачено, що завада потенційно може повністю або частково перекривати показаних одну або декілька зон (рис. 2). Вказані зони позначені літерами A, B, C, D та E.

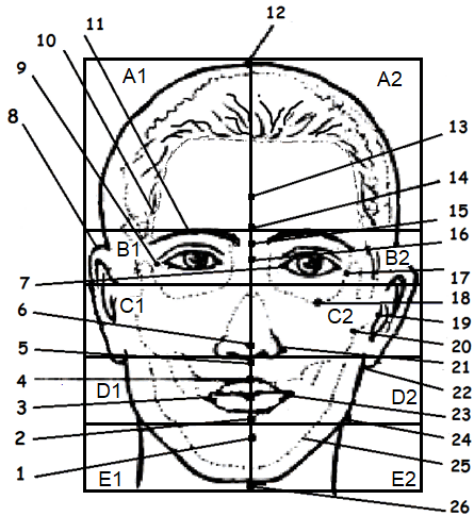

Рис. 2. Зони можливого місцезнаходження завад

Зона А співвідноситься з верхньою частиною голови людини, зона В – з очима, зона С – носом, D – ротом, а Е - нижньою частиною обличчя. Лівій частині обличчя відповідає індекс 1, а правій частині – індекс 2. При визначенні вказаних зон, крім нормативних вимог, враховано що положення ключових та контрольних точок, які використовуються для розпізнавання особи та емоцій визначаються положеннями, показаних на рис. 2 контрольних точок голови людини, а саме: 1 – надпідборідна, 2 –губна нижня, 3 – ротова, 4 – губна верхня, 5 – підносова, 6 – передньоносова, 7 – точка у внутрішньому куті ока, 8 – верхньовушна, 9 – точка у зовнішньому куті ока, 10 – контур лінії росту волосся, 11 – надбрівна лінія, 12 – верхівкова, 13 – точка на перетині лінії, яка з'єднує точки лобних бугрів, що найбільш виступають, 14 – надглабелярна, 15 – точка в ділянці, де сходяться надбрівні дуги, 16 – найбільш глибока точка перенісся, 17 – зовнішньоочна, 18 – нижньоочна, 19 – козелок вуха, 20 – вилицева, 21 – носокрилова, 22 – нижньовушна, 23 – губнокутова, 24 – кутова щелепна, 25 – щелепна, 26 – зона підборіддя.

Інтенсивність завади, локалізованої в певній зоні обличчя пропонується співставити з кількістю ключових та контрольних точок, які вона перекриває. Інтенсивність завади на РОО співвідноситься з площею яку перекриває ця завада. Зазначимо, що запропонований підхід дозволяє адаптувати інтенсивність завади до застосування в моделях з різною кількістю ключових та контрольних точок. Таким чином:

$$Z = \{z_1, z_2, \dots, z_{12}\}, \qquad (7)$$

де $z_1, \dots, z_{10}$ – параметр, що визначає інтенсивність завади, локалізованої в зоні зображення обличчя A1, A2, B1, B2, C1, C2, D1, D2, E1, E2

відповідно; z_{11}, z_{12} – параметр, що визначає інтенсивність завади на райдужній оболонці лівого та правого ока відповідно.

При цьому;

$$z_m = \frac{1}{W_m}\sum_{w=1}^{W_m} r_w,\ 0 \le r_w \le 1, \qquad (8)$$

де m – номер відповідної зони зображення обличчя; W_m – кількість контрольних/ключових точок в зоні m; r_w – ступінь зменшення видимості w-ої контрольної/ключової точки в m-ій зоні обличчя через дію завади.

Множина параметрів завад, пов'язаних з контрольними точками позначається Z_I, а множина параметрів завад, пов'язаних з ключовими точками – Z_E.

Базуючись на результатах [11, 20, 23, 24] запропоновано підходи до виявлення атак на систему БА, що базуються на використанні муляжів обличчя та ока людини. Підхід «за навколишнім середовищем» передбачає виявлення атаки на основі результатів аналізу параметрів, що характеризують зображення навколишнього середовища при відеореєстрації ЗО та РОО. Підхід «за динамікою ЗО» передбачає виявлення атаки на основі результатів аналізу динаміки параметрів ЗО та РОО, що описують базові емоції представника персоналу ОКІ та додаткові параметри, що описують динаміку руху очей. В цьому випадку до додаткових параметрів, що використовуються для розпізнавання атак за допомогою муляжів, віднесено:

- зміну напрямку його погляду;
- зміну розміру зіниці ока;
- наявність пульсацій кровоносних судин на зображенні ока;
- кліпання очей.

Динаміку зміни напрямку погляду представника персоналу ОКІ доцільно відслідковувати за динамікою положення обличчя людини та динамікою положення зіниці ока. Враховуючи, що в багатьох випадках комп'ютерні засоби відеоспостереження не забезпечують можливість достатньо точного визначення зміни місцезнаходження представника персоналу, то в першому наближенні доцільно вважати, що динаміку положення обличчя людини та динаміку положення зіниці ока слід описувати за допомогою параметрів, що співвідносяться з динамікою зміни кутових координат відповідних об'єктів в просторі. При цьому врахована просторова обмеженість повороту ока людини. Таким чином реалізацію операції виявлення атаки за допомогою муляжів можливо співвіднести з нейромережевим аналізом множини E та множини Γ, елементи якої співвідносяться з додатковими параметрами, які використовуються для розпізнавання атак за допомогою муляжів. Елементи множини Γ характеризують: $\gamma_1, \gamma_2, \gamma_3$ – кути, що визначають просторову орієнтацію обличчя в площинах Oxy, Oxz, Oyz відповідно; $\gamma_4, \gamma_5, \gamma_6, \gamma_7$ – кути що визначають просторову орієнтацію лівого та правого ока в площинах Oxy, Oxz відповідно; γ_8, γ_9 – розміри зіниць лівого та правого ока відносно розмірів райдужної оболонки; γ_{10}, γ_{11} – наявності пульсацій кровоносних судин на зображенні лівого та правого ока, що можливо оцінити на основі порівняння відповідних зображень, зареєстрованих в різні моменти часу; γ_{12}, γ_{13} – ступінь відкритості повік лівого та правого ока.

У випадку використання підходу «за навколишнім середовищем» до множини додаткових віднесено параметри, що дозволяють розпізнати атаку, яка реалізується шляхом демонстрації відеоряду з представником персоналу ОКІ. Можливо вважати, що для розпізнавання такої атаки слід виявити пристрій на якому відбувається демонстрація ЗО. Для цього достатньо розпізнати межі даного пристрою та характерні зміні якості ділянок ЗО. Крім того доцільно проаналізувати наявність об'єктів, які фіксуються в типових умовах відеореєстрації та відстань від відеокамери до ЗО. Таким чином елементи множини Γ, що використовуються для розпізнавання атак за допомогою муляжів при використанні підходу «за навколишнім середовищем» віднесено: γ_{14} – обрамлення ЗО контурами, характерними для пристроїв демонстрації відеоряду; γ_{15} – наявність на ЗО відблисків, що характерні при демонстрації відеоряду; γ_{16} – зміна якості ЗО, що характерні при демонстрації відеоряду; γ_{17} – відстань від камери до представника персоналу ОКІ, яку у випадку відсутності спеціалізованих засобів вимірювання відстані можливо оцінити на основі кількості пікселів, що співвідносяться з відстанню між контрольними точками.

Передбачається, що величини елементів множини Γ знаходяться в межах від 0 до 1. Значення 0 відповідає мінімальному значенню параметра, а значення 1 – максимальному значенню.

Деталізація специфічних операцій, що здійснюються для розпізнавання особи за ЗО та РОО при БА персоналу ОКІ з урахуванням необхідності визначення емоцій та виявлення атак за допомогою муляжів, забезпечує можливість

модифікації базової моделі розпізнавання. Наведено перелік окремих операцій процесу розпізнавання (табл. 1).

Таблиця 1

Операції, що входять до складу процедури розпізнавання

Номер операції	Позначення оператору	Опис
1	$\overset{Pr}{\rightarrow}$	Попередня обробка зображення
2	$\overset{Sg}{\rightarrow}$	Виділення контурів ЗО та РОО
3	$\overset{DtI}{\longrightarrow}$	Визначення координат контрольних точок
4	$\overset{DtE}{\longrightarrow}$	Визначення координат ключових точок
5	$\overset{DlI}{\longrightarrow}$	Нівелювання завад, які стосуються контрольних точок
6	$\overset{DlE}{\longrightarrow}$	Нівелювання завад, які стосуються ключових точок
7	$\overset{NR_I}{\longrightarrow}$	Нейромережеве розпізнавання особи
8	$\overset{NR_E}{\longrightarrow}$	Нейромережеве розпізнавання емоцій
9	$\overset{NR_\Gamma}{\longrightarrow}$	Нейромережеве Розпізнавання додаткових параметрів для визначення атак за допомогою муляжів
10	$\overset{NR_A}{\longrightarrow}$	Нейромережеве розпізнавання атак за допомогою муляжів

Враховуючи вирази (1-8) та дані табл. 1, модифікована модель розпізнавання може бути представлена наступним чином:

$$if\ \left((\forall\theta \in \Theta)\ \theta \in \theta_{ent}\right) \wedge \left((\forall c \in C)\ c \subset c_{ent}\right) \rightarrow \langle \Theta, C\rangle_{check}\ \ else\ \ stop, \tag{9}$$

$$\langle \Theta, C\rangle_{check} \overset{Pr}{\rightarrow} C_{pr}, \tag{10}$$

$$\langle \Theta, C_{pr}\rangle \overset{Sg}{\rightarrow} \tilde{C}, \tag{11}$$

$$\langle \Theta, \tilde{C}\rangle \overset{DtI}{\longrightarrow} \langle \tilde{C}_I, \mathrm{Z}_I\rangle, \tag{12}$$

$$\langle \Theta, \tilde{C}\rangle \overset{DtE}{\longrightarrow} \langle \tilde{C}_E, \mathrm{Z}_E\rangle, \tag{13}$$

$$\langle \tilde{C}_I, \mathrm{Z}_I\rangle \overset{DlI}{\rightarrow} \langle \tilde{C}_{crI}, \mathrm{Z}_{crI}\rangle, \tag{14}$$

$$\langle \tilde{C}_E, \mathrm{Z}_E\rangle \overset{DlE}{\longrightarrow} \langle \tilde{C}_{crE}, \mathrm{Z}_{crE}\rangle, \tag{15}$$

$$\langle \tilde{C}_{crI}, \mathrm{Z}_{crI}\rangle \overset{NR_I}{\longrightarrow} I, \tag{16}$$

$$\langle \tilde{C}_{crE}, \mathrm{Z}_{crE}\rangle \overset{NR_E}{\longrightarrow} E, \tag{17}$$

$$\langle \tilde{C}_{crI}, \tilde{C}_{crE}, \mathrm{Z}_{crI}, \mathrm{Z}_{crE}\rangle \overset{NR_\Gamma}{\longrightarrow} \Gamma, \tag{18}$$

$$\langle E, \Gamma\rangle \overset{NR_A}{\longrightarrow} A, \tag{19}$$

де θ_{ent} – множина допустимих значень для $\theta \in \Theta$; c_{ent} множина допустимих значень для $c \in C$; $\langle \Theta, C\rangle_{check}$ – кортеж, що складається із множин Θ, C, які пройшли перевірку відповідності параметрів відеореєстрації допустимим значенням; C_{pr} – множина параметрів відеопотоку, що пройшли попередню обробку; $\tilde{C}_I, \tilde{C}_E$ – множини параметрів контрольних та ключових точок; $\mathrm{Z}_I, \mathrm{Z}_E$ – множини параметрів завад при розпізнаванні особи та емоцій персоналу ОКІ; $\tilde{C}_{crI}$, $\tilde{C}_{crE}$ – множини параметрів контрольних та ключових точок після нівелювання завад; Z_{crI}, Z_{crE} – множини параметрів завад при розпізнаванні особи та емоцій персоналу ОКІ після виконання операцій по їх нівелюванню.

Вирази (2-18) складають базис деталізованого опису процесу розпізнавання особи за ЗО та РОО при БА персоналу ОКІ з застосуванням НМЗ.

Формування математичного апарату забезпечила можливість переходу до наступного етапу побудови моделі розпізнавання – визначення множин критеріїв (Λ), що використовуються при побудові засобів розпізнавання для оцінювання ефективності окремих операцій та процедури розпізнавання в цілому. Відповідно до результатів [2, 14, 18] ефективність операцій процедури розпізнавання, окрім операції передобробки параметрів відеопотоку, пропонується оцінювати за допомогою показників точності та ресурсоємності. Щодо операції передобробки параметрів відеопотоку, то для оцінювання її ефективності замість показників точності слід використовувати показники підвищення якості зображення. Множину критеріїв для оцінювання точності позначимо Λ, а множину для оцінювання ресурсоємності – B.

В теорії НМ при вирішенні задач класифікації базовим критерієм оцінки точності є Accuracy (λ_1). Для розрахунку цієї метрики у випадку необхідності розпізнавання класів True та False використовується вираз виду:

$$\lambda_1 = \frac{N_t}{N_\Sigma}, \tag{20}$$

де N_t – кількість правильно розпізнаних об'єктів; N_Σ – загальна кількість об'єктів.

Використання критерію λ_1 має обмеження, пов'язані з необхідністю пропорційного предста-

влення 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 [2] визначено, що крім accuracy в першому наближенні в якості критеріїв доцільно використовувати Recall (λ_2), Precision (λ_3), F1-score (λ_4):

$$\lambda_2 = \frac{N_{tp}}{N_{tp}+N_{fp}}, \quad (21)$$

$$\lambda_3 = \frac{N_{tp}}{N_{tp}+N_{fn}}, \quad (22)$$

$$\lambda_4 = \frac{N_{tp}}{N_{tp}+\frac{1}{2}(N_{fp}+N_{fn})}, \quad (23)$$

де N_Σ – загальна кількість прикладів; N_{tp} – кількість правильно розпізнаних прикладів, що відносяться до класу True; N_{tn} – кількість правильно розпізнаних прикладів, що відносяться до класу False; N_{fp} – кількість неправильно розпізнаних прикладів, що відносяться до класу True; N_{fn} – кількість неправильно розпізнаних прикладів, що відносяться до класу False.

Критерії, задані виразами (20-23), доцільно використовувати для оцінювання точності результатів операцій $\overset{NR_I}{\longrightarrow}$, $\overset{NR_E}{\longrightarrow}$, $\overset{NR_A}{\longrightarrow}$.

У випадку, коли операція $\overset{NR_E}{\longrightarrow}$ передбачає необхідність розпізнавання більше двох класів емоцій, вирази (20-23) підлягають модифікації з позицій мультикласової класифікації.

Результатом виконання операції $\overset{NR_\Gamma}{\longrightarrow}$ є множина дискретних значень параметрів, що знаходяться в межах від 0 до 1.

Відповідно до даних [14, 19] у цьому випадку для оцінки точності доцільно використовувати середню абсолютну похибку (λ_5), що розраховується за допомогою виразу:

$$\lambda_5 = \frac{1}{N_\Sigma}\sum_{n=1}^{N_\Sigma}\left|\frac{y_{t,n}-y_{m,n}}{y_{t,n}}\right|, \quad (24)$$

де $y_{t,n}, y_{m,n}$ – істинне та модельне значення параметру для n-го прикладу.

Відповідно до [2] операції $\overset{Sg}{\rightarrow}$, $\overset{DtI}{\longrightarrow}$, $\overset{DtE}{\longrightarrow}$, $\overset{DlI}{\rightarrow}$, $\overset{DlE}{\longrightarrow}$ можна віднести до області семантичної сегментації зображень, що дозволяє оцінити точність їх реалізації за допомогою коефіцієнта Дайтса (λ_6) та коефіцієнта Жаккара (λ_7):

$$\lambda_6 = 2\sum_{k=1}^{K}(y_{t,n}y_{m,n})/\left(\sum_{k=1}^{K}y_{t,n}^2+\sum_{k=1}^{K}y_{m,n}^2\right), \quad (25)$$

$$\lambda_7 = \sum_{k=1}^{K}(y_{t,n}y_{m,n})\Big/\begin{pmatrix}\sum_{k=1}^{K}y_{t,n}+\\ \sum_{k=1}^{K}y_{m,n}-\\ \sum_{k=1}^{K}(y_{m,n}-y_{t,n})\end{pmatrix}, \quad (26)$$

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 і-го пікселя очікуваного вихідного сигналу.

При обґрунтуванні критерію оцінки якості попередньої обробки зображення при реалізації операції операція $\overset{Pr}{\rightarrow}$ 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 масштабування розмірів, корекції яскравості та контрастності. Також у цьому випадку при виборі критерію оцінювання якості попередньої обробки слід очікувати недоступність еталону зареєстрованого зображення. Ще одним важливим фактором, що впливає на вибір критерію, є необхідність його оперативного розрахунку. Враховуючи вказані передумови та результати досліджень в області оцінки якості обробки статичних зображень та відеопотоку визначено перелік критеріїв до складу якого входять PSNR (λ_8), контраст Міхельсона (λ_9) та контраст Вебера (λ_{10}), що визначаються виразами (27-30):

$$Br_{mse} = \frac{1}{XY}\sum_{x=1}^{X}\sum_{y=1}^{Y}\big(Im_e(x,y) - Im_r(x,y)\big)^2, \quad (27)$$

$$if\ Br_{mse} \neq 0 \implies \lambda_8 = 10\lg(Br_{max}/Br_{mse}),\ else\ \lambda_8 = \lambda_{8,max}, \quad (28)$$

$$\lambda_9 = \frac{Br_{max}-Br_{min}}{Br_{max}+Br_{min}}, \quad (29)$$

$$\lambda_{10} = \frac{|Br_{ob}-Br_{bg}|}{Br_{bg}}, \quad (30)$$

де Im_e, Im_r – еталонне та зареєстроване зображення; Br_{max}, Br_{min}, – максимальне та мінімальне значення яскравості пікселів; Br_{mse} – середнє квадратичне відхилення яскравості пікселів; Br_{ob}, Br_{bg} – середня яскравість об'єкту та фону; $Im_e(x,y)$, $Im_r(x,y)$ – яскравість пікселя з координатами x, y для зображень Im_e та Im_r відповідно; X, Y – розмір зображення по горизонталі та вертикалі, відповідно.

Вважається, що значення параметрів X, Y, Br_{max}, Br_{min}, Br_{ob}, Br_{bg} не дорівнюють 0, оскільки перед реалізацією операції $\overset{Pr}{\rightarrow}$ відеопотік проходить перевірку на допустимість. Особливість розрахунку виразу (28) полягає у тому, що значення Br_{mse} може дорівнювати 0. Відповідно до виразу (28), $Br_{mse} = 0$ при тотожності Im_e та Im_r, тобто тотожності еталонного та обробленого зареєстрованого зображення. Це відповідає випадку максимально якісної попередньої обробки, що і пояснює значення $\lambda_8 = \lambda_{8,max}$. Передбачено, що критерій λ_8 використовується для обробки ЗО у випадку проведення автентифікації персоналу ОКІ при вході в систему, коли розпізнавання особи зводиться до задачі класифікації зображення обличчя, а умови відеореєстрації є чітко визначеними, що передбачає необхідність масштабування з масштабним коефіцієнтом в межах від 0,7 до 1,3. Критерій λ_9 передбачено використовувати у випадку розпізнавання особи при виконанні персоналом ОКІ своїх функціональних обов'язків при відсутності еталонів зареєстрованих зображень, а λ_{10} передбачено використовувати при передобробці зображення для виділення контурів обличчя та контурів райдужної оболонки ока. Критерії λ_8, λ_9, λ_{10} призначені для оцінки якості обробки монохромних або напівтонових зображень. При їх застосуванні до оцінки якості обробки кольорових зображень слід провести оцінку якості зображення по кожному із каналів та розрахувати середнє значення. В підсумку вирази (20-30) визначають множину критеріїв для оцінювання точності операцій Λ.

В загальному випадку для оцінювання обчислювальної ресурсоємності кожної із операцій, наведених в табл. 1, використовують обчислювальну складність та обсяг пам'яті, необхідний для їх виконання. На практиці провести розрахунок вказаних показників достатньо складно через необхідність враховувати великий обсяг різноманітних факторів, наприклад – підходу до сегментації зареєстрованого зображення або до підходу до визначення ключових точок обличчя. Разом з тим з позицій розробки біометричних засобів автентифікації можливо стверджувати, що операції 2-4, 7-10 базуються на використанні нейромережевих рішень. Враховуючи результати [18] можливо вважати, що в першому наближенні в якості критерію оцінювання обчислювальної ресурсоємності кожної з цих операцій можливо використовувати кількість вагових коефіцієнтів відповідної нейронної мережі K_w. Тобто для всіх операцій 2-4, 7-10, $\beta_i = K_{w,i}$, де індекс i відповідає номеру операції в табл. 1. Враховуючи дані [18, 25] для операції 1, 5, 6 критерій оцінювання обчислювальної ресурсоємності в базовому випадку можливо співвіднести з обчислювальною складністю алгоритму її виконання. Загальну обчислювальну ресурсоємність процедури розпізнавання особи можливо розрахувати так:

$$\beta_\Sigma = \sum_{i=1}^{10} \beta_i. \quad (31)$$

Очевидно, що діапазони допустимих значень критеріїв, що входять до складу Λ та B і стосуються операцій розпізнавання особи, емоцій та атак за допомогою муляжів повинні визначатись у вимогах до засобів БА. Разом з тим, діапазони допустимих значень критеріїв, що асоціюються з реалізацією проміжних операцій процедури розпізнавання в першому наближенні можливо визначити та основі загальноприйнятних вимог. Так, відповідно до даних [2, 15, 23, 24], допустимі значення критеріїв λ_8, λ_9, λ_{10}, що використовуються для оцінки якості попередньої обробки зображень, відповідно дорівнюють $\lambda_{8,adm} = 20$ дБ, $\lambda_{9,adm} = 0{,}6$, $\lambda_{10,adm} = 0{,}9$. Також слід відзначити, що з позицій зручності інтерпретації отриманих результатів можливо вихідний сигнал НМЗ представити у ймовірнісному вигляді. Разом з тим, у вимогах до НМЗ слід передбачити порогові значення вихідних сигналів, що забезпечать можливість остаточного визначення величин елементів множин I, E та A.

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 [11], а також матеріальні ресурси, що виділяються на розробку та впровадження таких засобів. Також слід відзначити, що, відповідно до загальновизнаної методології створення НМЗ захисту інформації, розробка моделі процедури розпізнавання забезпечує базис розробки НММ та

нейромережевих методів, призначених для розпізнавання особи, емоцій та атак за допомогою муляжів на основі відеопотоку, зареєстрованого в умовах ОКІ.

ВИСНОВКИ

В результаті аналізу науково-практичних робіт показано, що однією із основних перешкод підвищення ефективності систем БА персоналу ОКІ являється недостатня адаптованість сучасних НМЗ розпізнавання особи за ЗО та РОО до очікуваних умов застосування. З'ясовано, що для побудови вдосконалених НМЗ необхідно доповнити методологічну базу шляхом розробки моделі, яка забезпечить формалізований опис відповідної процедури розпізнавання.

Визначено, що до складу процедури розпізнавання входять операції перевірки допустимості параметрів відеореєстрації, передобробки параметрів відеопотоку, виділення контурів ЗО та РОО, виявлення та нівелювання завад та застосування НМЗ. Для кожної із означених операцій обґрунтовано перелік критеріїв оцінки ефективності, адаптований до характеристик сучасних засобів її реалізації. При цьому вперше обґрунтовано перелік критеріїв оцінки якості попередньої обробки ЗО, що підлягає нейромережевому аналізу в системі БА.

Також вперше запропоновано підходи до визначення параметрів завад для розпізнавання особи і емоцій та розпізнавання атак за допомогою муляжів. Підхід до визначення параметрів завад передбачає співставлення параметрів завад з місцезнаходженням та кількістю ключових і контрольних обличчя, які вони перекривають. Підходи до розпізнавання атак за допомогою муляжів передбачають виявлення таких атак на основі аналізу динаміки базових емоцій, динаміки параметрів руху очей та навколишнього середовища при відеореєстрації.

Розроблено аналітичні вирази, які надають формалізований опис кожної із операцій, а в сукупності з розробленою діаграмою, формують модель процедури розпізнавання особи за ЗО та РОО при БА персоналу ОКІ із застосуванням НМЗ з урахуванням необхідності визначення емоцій та виявлення атак за допомогою муляжів. З використанням розробленої моделі розпізнавання визначено перспективність вдосконалення НМЗ систем БА за рахунок використання запропонованих підходів до визначення параметрів завад та розпізнавання атак за допомогою муляжів.

ЛІТЕРАТУРА

[1]. Ali M., Thakur K., Tappert C. User authentication and identification using neural network. I-manager's Journal on Pattern Recognition. 2015. No 2. pp. 28-39.

[2]. Bagitova K., Tereikovskyi I., Babayev I., Tereikovska L., Tereikovskyi O. Model for processing images of online social networks used to recognize political extremism. Journal of Mathematics, Mechanics and Computer Science. Vol. 119 No. 3 (2023): Journal of Mathematics. pp. 91-103. ISSN 1563–0277, eISSN 2617-4871. DOI: 10.26577/JMMCS2023v119i3a8.

[3]. Batista J.C., Albiero V., Bellon O.R., Silva L. AUMPNet: Simultaneous Action Units Detection and Intensity Estimation on Multipose Facial Images Using a Single Convolutional Neural Network. 12th IEEE International Conference on Automatic Face & Gesture Recognition. 2017. pp. 866-871.

[4]. Callet P., Viard-Gaudin C., Barba D. (2006). A Convolutional Neural Network Approach for Objective Video Quality Assessment. IEEE Transactions on Neural Networks. pp. 1316-1327.

[5]. Chandrani S., Washef A., Soma M., Debasis M. Facial Expressions: A Cross-Cultural Study. Emotion Recognition: A Pattern Analysis Approach. Wiley Publ., 2015. pp. 69-87. DOI:10.1002/9781118910566.

[6]. Connaughton R., Bowyer K. W., Flynn P. J. Fusion of Face and Iris Biometrics. Handbook of Iris Recognition. Springer, 2013. pp. 219-237.

[7]. Dychka I., Chernyshev D., Tereikovskyi I., Tereikovska L., Pogorelov V. Malware Detection Using Artificial Neural Networks. In: Hu Z., Petoukhov S., Dychka I., He M. (eds) Advances in Computer Science for Engineering and Education II. ICCSEEA 2019. Advances in Intelligent Systems and Computing. Vol 938. Springer, Cham. pp. 3-12. DOI: 10.1007/978-3-030-16621-2_1.

[8]. Ma X., Fu M., Zhang X., Song X., Becker B., Wu R., Xu X., Gao Z., Kendrick K. and Zhao W. Own Race Eye-Gaze Bias for All Emotional Faces but Accuracy Bias Only for Sad Expressions. 2022. Frontiers in Neuroscience. Vol. 16. pp. 1-11.

[9]. Noyes E., Davis J., Petrov N., Gray K., Ritchie K. The effect of face masks and sunglasses on identity and expression recognition with super-recognizers and typical observers. Royal Society Open Science. 2021. Vol. 24. № 8(3):201169. pp. 1-18. DOI: 10.1098/rsos.201169.

[10]. Ranjith, G., Pallavi K., Mahendra V. Human Face, Eye and Iris Detection in Real-Time Using Image Processing. In: Mandal, J.K., Hinchey, M., Rao, K.S. (eds) Innovations in Signal Processing and Embedded Systems. Algorithms for Intelligent Systems. Springer, Singapore. 2023. doi.org/10.1007/978-981-19-1669-4_34.

[11]. Ratha N. Enhandcing security and privacy in biometrics-based autentication system / Ratha N., Conneli J., Bolle R. // IBM System Journal. Vol. 40, №3. 2001. pp. 614-634.

[12]. Rinck M., Primbs M.A., Verpaalen A.M., Bijlstra G. Face masks impair facial emotion recognition and induce specific emotion confusions. Cognitive Research: Principles and Implications. 2022. Vol. 7(1):83. doi: 10.1186/s41235-022-00430-5.

[13]. Royer J., Blais C., Charbonneau I., Déry K., Tardif J. Greater reliance on the eye region predicts better face recognition ability. Cognition. 2018. Vol. 181. pp. 12-20. DOI: 10.1016/j.cognition.2018.08.004.

[14]. Tariq U., Lin K., Li Z., Zhou Z., Wang Z., Le V., Huang T.S., Lv X., Han T.X. Emotion Recognition from an Ensemble of Features. Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions, 2012, vol. 42 (4), pp. 1017-1026.

[15]. Tereikovskyi I., Hu Z., Chernyshev D., Tereikovska L., Korystin O., Tereikovskyi O. The Method of Semantic Image Segmentation Using Neural Networks. International Journal of Image, Graphics and Signal Processing (IJIGSP), 2022. Vol. 14, No.6. pp. 1-14. DOI: 10.5815/ijigsp.2022.06.01.

[16]. Tereikovskyi I., Korchenko O., Bushuyev S., Tereikovskyi O., Ziubina R., Veselska O. A Neural Network Model for Object Mask Detection in Medical Images. International Journal of Electronics and Telecommunications. 2023. Vol. 69. No 1. pp. 41-46. DOI: 10.24425/ijet.2023.144329.

[17]. Tereykovska L., Tereykovskiy I., Aytkhozhaeva E., Tynymbayev S., Imanbayev A. Encoding of neural network model exit signal, that is devoted for distinction of graphical images in biometric authenticate systems // News of the national academy of sciences of the republic of Kazakhstan series of geology and technical sciences. 2017. Vol. 6, No 426, pp. 217-224.

[18]. Toliupa S., Kulakov Y., Tereikovskyi I., Tereikovskyi O., Tereikovska L., Nakonechnyi V. Keyboard Dynamic Analysis by Alexnet Type Neural Network, 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), Lviv-Slavske, Ukraine, 2020. pp. 416-420.

[19]. Toliupa S., Tereikovska L., Tereikovskyi I., Doszhanova A., Alimseitova Z. Procedure for Adapting a Neural Network to Eye Iris Recognition. IEEE International Conference on Problems of Infocommunications, Science and Technology. 2020. pp. 167-171. DOI: 10.1109/PICST51311.2020.9468020.

[20]. Toliupa S., Tereikovskiy I., Dychka I., Tereikovska L., Trush A. (2019). The Method of Using Production Rules in Neural Network Recognition of Emotions by Facial Geometry. 3rd International Conference on Advanced Information and Communications Technologies (AICT). 2019, 2-6 July 2019, Lviv, Ukraine. pp. 323-327.

[21]. Vinette C., Gosselin F., Schyns P. Spatio-temporal dynamics of face recognition in a flash: it's in the eyes. Cognitive Science. Vol. 28(2) pp. 289-301. doi. org/10.1016/j.cogsci.2004.01.002.

[22]. ViswanathReddy A. et al. Facial Emotions over Static Facial Images Using Deep Learning Techniques with Hysterical Interpretation. Journal of Physics: Conference Series. 2021. Vol. 2089. pp. 1-17. DOI: 10.1088/1742-6596/2089/1/012014.

[23]. Wu Z., Cheng Y., Yang J., Ji X., Xu W. DepthFake: Spoofing 3D Face Authentication with a 2D Photo. 2023 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2023. pp. 917-933. DOI: 10.1109/SP46215.2023.10179429.

[24]. Zhuravlov D., Polshakova O. Detection of face spoofing attacks on biometric identification systems. Interdepartmental scientific and technical collection "Adaptive automatic control systems». No 1 (42) 2023. pp. 108-114.

[25]. Висоцька О.О., Давиденко А.М., Христевич В. Виділення обличчя людини у відеопотоці для контролю за дотриманням співробітниками стану безпеки в процесі роботи та навчання. Захист інформації. 2022. Т. 24, №2. С. 94-107. DOI: 10. 18372/2410-7840.24.16934.

[26]. Закон України «Про критичну інфраструктуру» від 01.01.2024.

[27]. Закон України «Про основні засади забезпечення кібербезпеки України» від 01.01.2024.

[28]. Постанова Кабінету міністрів України «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» від 19.06.2019.

[29]. Способи зіставлення особи з її фотозображенням. Міністерство цифрової трансформації України.

MODEL OF THE FACIAL RECOGNITION PROCEDURE MODEL AND THE IRIS OF THE EYE DURING BIOMETRIC AUTHENTICATION OF PERSONNEL OF CRITICAL INFRASTRUCTURE FACILITIES USING NEURAL NETWORK TOOLS

Today's challenges determine the need to improve the means of biometric authentication of personnel of critical infrastructure facilities. Common means of biometric authentication, which are usually based on the use of neural network technologies for facial image analysis, in many cases are not sufficiently adapted to the conditions of recognition during the performance of the personnel's functional duties, which are characterized by the influence of various interferences during video recording and an increase in the probability of attacks using dummies. Another promising direction of improvement is determined by the availability of modern means of video registration, which provide an additional possibility of recognizing a person by the iris of the eye and the possibility of recognizing emotions, which allows assessing the psycho-emotional state of staff representatives. It is shown that the first stage of improving neural network means of biometric authentication is the development of a formalized description of the recognition procedure, which takes into account promising areas of improvement. An appro-

priate model is proposed that provides a formalized description and criteria for evaluating the effectiveness of each of the operations and the recognition procedure as a whole. At the same time, for the first time, the list of criteria for assessing the quality of pre-processing of images, subject to neural network analysis in the biometric authentication system, has been substantiated, and for the first time, approaches to determining the parameters of interference and recognizing attacks using dummies have been proposed. The approach to determining the parameters of obstacles involves comparing the parameters of obstacles with the location and number of key and control faces that they overlap. Recognition of attacks is proposed to be implemented based on the analysis of the dynamics of basic emotions, the dynamics of eye movement parameters and the environment. The results of this study are important in the context of the development of effective biometric authentication tools, as they provide a formalized description of the requirements for the functionality of the main components of this procedure for recognizing the identity and emotions of personnel of critical infrastructure facilities.

Keywords: model, critical infrastructure, face image, iris, neural network, biometric authentication, information protection, information security.

Корченко Олександр Григорович, лауреат Державної премії України в галузі науки і техніки, Заслужений діяч науки і техніки України, доктор технічних наук, професор, перший проректор Державний університет інформаційно-комунікаційних технологій, професор Університету Комісії Народної Освіти (Краків, Польща).

Oleksandr Korchenko, laureate of the State Prize of Ukraine in the field of Science and Technology, Honored Worker of Science and Technology of Ukraine, Dr Hub. (Eng), Professor, Vice-Rector for Research, National Aviation University, Professor of the National Education Commission of the University, Krakow, Poland.
E-mail: icaocentre@nau.edu.ua.
Orcid ID: 0000-0003-3376-0631.

Терейковський Олег Ігорович, аспірант, Національний авіаційний університет.

Oleh Tereikovskyi, PhD student, National Aviation University.
E-mail: tereikovskyio@gmail.com.
Orcid ID: 0000-0001-5045-0163.

DOI: 10.18372/2410-7840.26.18840
УДК 004.056.5

ОСОБЛИВОСТІ ВИКОРИСТАННЯ AMAZON INSPECTOR ДЛЯ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ ХМАРНИХ ДОДАТКІВ

Андрій Партика, Богдан Недодус

Основними проблемами з якими може зіштовхнутись бізнес можуть слугувати вразливості до різноманітних кібератак, втрати конфіденційності даних, збільшення кількості збоїв і зменшення стабільності інформаційної інфраструктури, збільшення капітальних витрат, нові вимоги до незалежності даних, проблеми з масштабуванням інформаційної інфраструктури бізнесу. Зазначені вище проблеми можуть слугувати підґрунтям для міграції на хмарні технології, що в свою чергу забезпечить зменшення видатків на підтримку інфраструктури, підвищить ефективність управління інформаційної інфраструктури в порівнянні з роботою в локальному середовищі, збільшить гнучкість організації. Актуальність дослідження полягає в покращенні інформаційної безпеки, забезпечення конфіденційності, цілісності і доступності, виявленню вразливостей додатку і середовища завдяки використання вбудованих служб AWS. Метою даної роботи є впровадження оцінки і покращення безпеки робочого середовища і додатку, розгорнутому на базі хмарних сервісів, шляхом автоматизації сканування і аналізу робочого навантаження AWS.

***Ключові слова**: Amazon Web Services, AWS, Amazon Inspector, IAM, хмарні технології, вразливість, інфраструктура, моніторинг.*

ВСТУП

За умов стрімкого і безперервного розвитку інформаційних технологій різні мотиви можуть стимулювати бізнес-перетворення, які підштовхують власників підприємств до переходу на хмарні технології. Хмарні обчислення – це технологія, яка розширює сфери комп'ютерної мережі, створюючи середовище, яке пропонує масштабованість, краще використання апаратного забезпечення, програми на вимогу та сховище, а також нижчі витрати в довгостроковій перспективі завдяки створенню віртуальних серверів, клонованих із існуючих екземплярів, кожна з яких пропонує майже миттєве підвищення продуктивності, що дозволяє компаніям швидко й динамічно реагувати на нові вимоги [1]. «Хмара» може розміщуватися на території компанії або за її межами. Однак із зростанням попиту потреба в конфіденційності, цілісності та доступності даних стала однією з найважливіших проблем у хмарних об-