Шифр “БІОІДЕНТИФІКАТОР”

МЕТОД ІНТЕЛЕКТУАЛЬНОЇ АВТЕНТИФІКАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ НА ОСНОВІ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ

АНОТАЦІЯ

наукової роботи під шифром “БІОІДЕНТИФІКАТОР”

У роботі отримано рішення актуальної науково-практичної задачі забезпечення безпеки санкціонованого доступу до інформаційно-телекомунікаційних систем (ІТС), зокрема запропоновано перспективний метод інтелектуальної автентифікації на основі біометричної ідентифікації користувачів за геометрією обличчя.

Значну увагу в роботі приділено практичній (програмній) реалізації та дослідженню її ефективності та надійності. Результати розроблення програмного додатку автентифікації користувачів ІТС на основі біометричної ідентифікації за геометрією обличчя підтвердили достовірність теоретичних положень.

Робота складається зі вступу, 3 розділів, висновку, списку використаних джерел і додатків. Повний обсяг роботи становить 23 сторінки, 9 – рисунків, список використаних джерел із 14 найменувань.

ЗМІСТ

ВСТУП

Останні події, які спостерігаються на світовій арені, супроводжуються процесом перерозподілу зон впливу у технологічному та економічному просторі, розвитком інформаційних технологій (ІТ), які породжують нові способи отримання інформації. У зв'язку з цим, забезпечення захисту секретної інформації є актуальним питанням та вимагає від держав, незалежно від їх розвитку, постійного зміцнення національної безпеки, а також спроможності протидіяти загрозам і мінімізувати ризики реального витоку важливих відомостей та даних.

З початком збройної агресії з боку Російської Федерації (РФ), яка безпрецедентно створює напружену оперативну обстановку як в Україні, так і навколо неї, потреба у впровадженні адекватної комплексної системи забезпечення безпеки інформації та протидії кіберзагрозам та атакам набула особливої актуальності. Тому не викликає сумніву, що кожна теоретична чи прикладна спроба удосконалення механізмів охорони державної таємниці повинна визнаватися необхідною, своєчасною та актуальною.

Враховуючи досвід технологічного розвитку ІТ, одним із потенційно можливих методів надійного захисту інформації та об'єктів інформаційної діяльності (ОІД) від несанкціонованого доступу (НСД) – ідентифікація та/або автентифікація користувачів, який є необхідним заходом для запобігання матеріального та нематеріального витоку інформації [1]. При цьому важливо враховувати ефективність роботи автоматизованих підсистем управління доступом та захисту даних для забезпечення безпеки певної системи інформаційної інфраструктури, у тому числі ІТС.

Отже, наукова робота, **метою** якої є удосконалення методу інтелектуальної біометричної ідентифікації/автентифікації користувачів ІТС та його новітня програмна реалізація є актуальною, своєчасною та становить науково-практичний інтерес дослідження.

РОЗДІЛ 1. АНАЛІЗ НАУКОВИХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ В ГАЛУЗІ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ/АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ

На даний момент розвитку інформаційних технологій парольні, які базуються на унікальній персональній інформації, та атрибутні методи ідентифікації, – на використанні персонального предмету: ключа, перепустки тощо, втрачають свою актуальність, проте користуються великим попитом серед користувачів. Дані методи забезпечення доступу мають суттєві технологічні недоліки, які стають все більш вираженими. Одною з проблем виступає неточність ідентифікації користувача у системі та велика ймовірність порушення її безпеки в результаті НСД, імітації певного атрибута або зламу паролю тощо. Також важливою проблемою цих методів є відсутність функціоналу для виявлення підміни авторизованого “легітимного” користувача. Тобто, порушник режиму доступу до інформації, сторонні особи можуть незаконно увійти до системи чи/або ОІД у той момент, коли “легітимний” користувач залишає її без контролю після етапу проходження авторизації. Однак, неперервний прихований моніторинг дає можливість своєчасно виявити відсутність “легітимного” користувача та унеможливити доступ до системи та/або об’єкта з обмеженим доступом для порушників.

Порівняно з попередніми методами, біометричні характеристики користувача, як спосіб автентифікації, можуть гарантувати підвищений рівень безпеки, враховуючи невід’ємність біометричних даних конкретної особи (користувача) [2].

Біометрична ідентифікація – це технології розпізнавання за окремими специфічними біометричними ознаками (ідентифікаторами), які властиві конкретній особі або користувачу.

Ці технології базуються на вимірюванні унікальних характеристик особи, отриманих від народження (ДНК, відбитки пальців, райдужна оболонка ока), набутих з віком або в результаті зовнішнього впливу (почерк, голос тощо).

Існують дві групи методів біометричної ідентифікації: статистичні та динамічні.

Методи першої групи ґрунтуються на аналізі фізіологічної (статичної) характеристики особи, даній від народження.

До цієї групи відносять методи ідентифікації: за відбитками пальців, на основі геометрії обличчя, за кодом ДНК, за особливостями долоні, за райдужною оболонкою або сітківкою ока тощо.

З метою вибору базового методу проведемо узагальнений їх аналіз.

Ідентифікація за відбитками пальців. В основі даного методу покладено унікальність капілярних узорів на пальцях, зображення (відбитки) яких отримуються за допомогою спеціальних сканерів та перетворюються у спеціальний цифровий код (згортку). Далі відбувається його порівняння з шаблонами, які зберігаються у базі авторизації користувачів [3, 4].

Перевагою цього методу є простота використання, зручність та надійність. Однак, ідентифікація за відбитком пальців володіє низкою недоліків, серед яких:

- капілярний узор легко пошкодити дрібними подряпинами або порізами;
- низький рівень захисту від “підробки” згортки, викликаний широким поширенням використання методу;
- залежність від чистоти пальців;
- низька ефективність розпізнавання у випадку сухості шкіри.

Ідентифікація за ДНК. Встановлено, що в молекулі ДНК є індивідуальні ділянки, неповторні у різних людей. Ймовірність того, що генетичний відбиток (індивідуальний код ДНК) у двох людей буде однаковий, складає менше однієї мільярдної. Таким чином індивідуальні ділянки ДНК можуть стати безпомилковим маркером, які дозволять відрізнити одну людину від іншої.

Переваги даного способу очевидні, проте в даний час методи обробки та аналізу ДНК працюють настільки довго, що такі системи використовуються лише для спеціалізованих експертиз.

Ідентифікація за особливостями долоні. На сьогодні існує два способи ідентифікації людини за особливостями долоні: за формою та за термограмою вен.

Перший метод ґрунтується на розпізнаванні геометричних особливостей долоні. Спеціальний пристрій формує тривимірне зображення кисті руки, який потім перетворюється у згортку. Перевагою методу за геометрією долоні полягає у підвищеній надійності порівняно з ідентифікацією за відбитками пальців.

Другий спосіб ідентифікації – використання термограми розташування вен долоні. Цей спосіб надійний, проте не досить розповсюджений у зв'язку з відсутністю чітких алгоритмів його функціонування.

Наступний метод – **ідентифікація за райдужною оболонкою ока**. Рисунок радужної оболонки ока також є унікальною характеристикою людини, причому для її сканування використовують портативні відео- та фотокамери зі спеціалізованим програмним забезпеченням. Даний програмний засіб дозволяє захоплювати зображення частини обличчя, з якого виділяється рисунок райдужної оболонки ока, за яким будується цифровий код ідентифікації особи [2, 4, 5].

До недоліків методу відносять:

- неможливість ідентифікації за умови низької якості (розмиття) зображення райдужної оболонки, викликана недостатнім фокусуванням;
- низька доступність готових технічних рішень;
- унеможливлення ідентифікації шляхом використання контактних лінз;
- значна залежність від умов зовнішнього середовища, зокрема освітленості.

Даний метод має власний підтип – **розпізнавання за сітківкою ока**. У даному випадку, біометрична технологія сканування сітківки використовується для відображення унікального рисунка сітківки людини. Кровоносні судини всередині сітківки поглинають світло з більшою інтенсивністю, ніж навколишні тканини, тому їх легко ідентифікувати.

Певні труднощі у застосуванні зазначеного методу ідентифікації виникають у разі використання контактних лінз. Крім того, процес розпізнавання доволі суттєво залежить від зовнішніх умов, насамперед від освітленості.

Ідентифікація за геометрією обличчя. Розпізнавання обличчя – один з найпоширеніших способів ідентифікації, заснований на унікальності характерних рис обличчя та форми черепа особи (користувача) [6].

Розпізнавання за геометрією обличчя має низку переваг порівняно з іншими методами біометричної ідентифікації/автентифікації. Серед них:

- відсутня необхідність безпосереднього контакту технічних засобів розпізнавання з користувачем;
- при відповідному обладнанні (потужні характеристики відеокамер) розпізнавання можливе на великих відстанях, навіть в групі людей;
- це єдиний біометричний спосіб, який не вимагає спеціальної техніки;
- для ідентифікації використовується загальнодоступна характеристика (обличчя) користувача;
- ідентифікація проводиться виключно із динамічним зображенням обличчя (фото користувача для розпізнавання ігнорується).

Ефективність та надійність систем ідентифікації користувачів за геометрією обличчя характеризується ймовірністю розпізнавання, на величину якої впливають різні чинники. Так, наприклад, риси обличчя змінюються в залежності від віку, повороту голови, психологічного стану людини, мімічного виразу обличчя, наявності волосяного покрову, косметики, окулярів тощо.

Для підвищення цих показників необхідно збільшити вибірку навчання, тобто кількість фото користувачів при різних психологічних станах. Шляхом формування потужної бази даних шаблонних зображень користувачів вирішено питання ідентифікації користувачів-близнюків.

Другу групу біометричної ідентифікації складають динамічні методи, які ґрунтуються на поведінковій (динамічній) характеристиці людини. До основних методів цієї групи відносять ідентифікацію за: голосом, клавіатурним почерком тощо.

Голосова ідентифікація. У даному випадку використовуються частотні характеристики голосу (тон, тембр), на основі яких створюється цифрова модель. Особливістю цього методу є зручність у використанні. Однак, суттєвою

проблемою є точність ідентифікація. На надійність та ефективність голосової ідентифікації впливають як біологічні, так і технологічні фактори. Наприклад, важко ідентифікувати особу, яка хворіє, наприклад ларингітом, а також голосовий запис можна використати в якості НСД до ІТС [2].

Клавіатурний підпис (почерк). Метод ґрунтується на особливості (індивідуальності) набору тексту на клавіатурі. За рахунок цього можна ідентифікувати користувача з достатньою точністю. Позитивним методу цього типу полягає у відсутності необхідності додаткового обладнання. Однак, головним недоліком використання клавіатурного почерку для ідентифікації особи – тимчасова зміна самого почерку користувачів, наприклад під впливом стресових ситуацій.

На підставі аналізу встановлено, розглянуті методи володіють низкою недоліків нехарактерних ідентифікації користувачів за геометрією обличчя. Розвитку теоретичної та практичної бази в галузі біометричної ідентифікації та автентифікації користувачів присвячено роботи вітчизняних та закордонних вчених.

Так, науковими співробітниками компанії Facebook опубліковано дослідження з проекту розпізнавання обличчя користувачів даної соціальної мережі (Deep Face) [7]. Учені P. Viola та M. J. Jones розробити алгоритм [8] виявлення та ідентифікації об’єктів на зображеннях у реальному часі. У своїх роботах [9] Бабарика А., Прокопенко Е., Бабій Ю. запропонували комбіновані методи розпізнавання та ідентифікації.

Основу цих методів складають примітиви (ознаки) Хаара [10]. Ці ознаки обчислюються в межах сканувального вікна змінного розміру, що переміщується зображенням, яке під час процесу обробки методом [8] зберігається в так званому інтегральному форматі SAT (від англ. Summed Area Table). У даному алгоритмі використовується так званий бустінг (від англ. Boosting) – комплекс заходів, що сприяють підвищенню точності аналітичних, або посилення “слабких” моделей.

Таким чином, актуальність вивчення методів, способів (алгоритмів) визначення біометричної ідентифікації користувачів ІТС підвищується. Одним

з таких напрямів є застосування біометричних методів автентифікації користувачів, які ґрунтуються на використанні алгоритмів ідентифікації за геометрією обличчя. У даній науковій праці за основу розпізнавання користувачів обрано метод Віоли-Джонса, виходячи із його можливості забезпечення підвищення точності ідентифікації та послаблення “слабких” моделей, що значно зменшує хибні розпізнавання.

РОЗДІЛ 2. МАТЕМАТИЧНА МОДЕЛЬ МЕТОДУ ІНТЕЛЕКТУАЛЬНОЇ АВТЕНТИФІКАЦІЇ В ІТС НА ОСНОВІ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ

Запропонований метод інтелектуальної автентифікації в ІТС на основі біометричної ідентифікації користувачів, загальний алгоритм якого наведено на рис. 2.1., містить такі основні кроки:

Крок 1. Виявлення та локалізація обличчя користувача на зображенні відеопотоку (розрахунок контурів геометрії)

Крок 2. Нормалізація зображення за масштабом, яскравістю тощо.

Крок 3. Обчислення набору базових (характеристик) ознак зображення.

Крок 4. Обчислення набору базових (характеристик) ознак зображення.

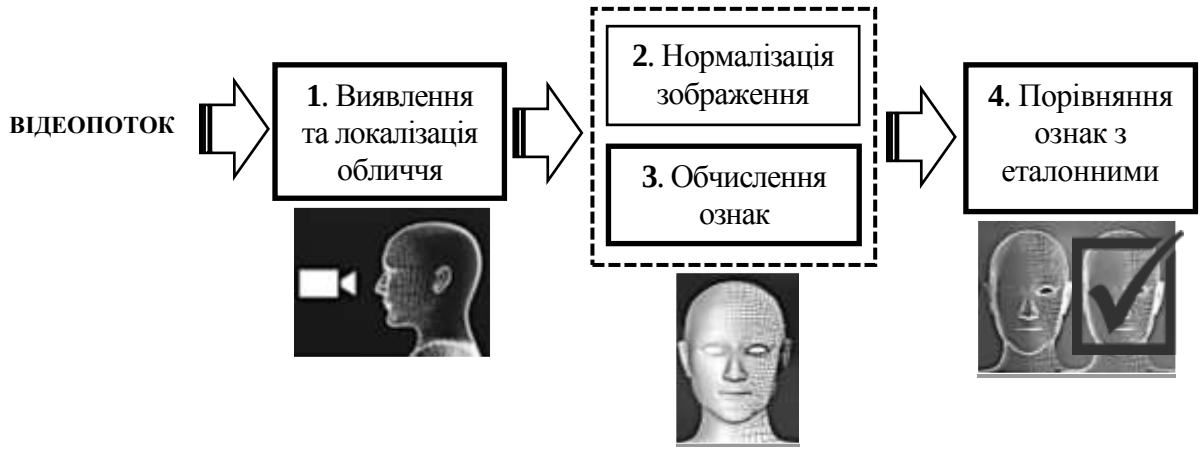


Рисунок 2.1 – Алгоритм ідентифікації користувачів ІТС

На даний час існує значна кількість підходів для вирішення завдання розпізнавання та локалізації обличчя. На підставі аналізу, проведеного у попередньому розділі, у даній роботі використано алгоритм Віоли-Джонса для пошуку геометрії обличчя на зображені систем відеоспостереження. Як правило, пошук геометрії обличчя відбувається швидко, однак інтелектуальне вивчення ознак класифікатором проводиться у достатньо тривалий час. Відповідно, обраний метод є кращим рішенням, порівняно з іншими алгоритмами, за критеріями ефективності та оперативності розпізнавання обличчя [11].

Особливість цього методу полягає у можливості його реалізації у мобільних додатках, що особливо актуально в умовах інформатизації сьогодення.

Основні принципи, на яких базується метод:

- відеозображення подається в інтегральному вигляді для підвищення оперативності аналітичних обчислень та розрахунків;

- використання базових понять теорії розпізнавання об’єктів, зокрема ознак (примітивів) Хаара. Усі ознаки надходять на вхід класифікатора та обробляються з деяким підсилення, так званим бустингом (*від англ.* boost: вдосконалення, посилення);

- застосування каскаду ознак/примітивів для аналізу результату ідентифікації.

Інтегральне подання відеозображення. Інтегральне подання – це матриця (відповідає розмірам зображення, що аналізується), яка дозволяє розраховувати значення сумарної яскравості довільного прямокутника на зображенні, розмір якого не впливає на час проведення аналітичних обчислень. У кожному елементі матриці зберігається значення суми інтенсивності пікселів, які геометрично окреслюють об’єкт зліва та зверху (рис. 2.2) [12].

1	1	1
1	1	1
1	1	1

а) вихідне зображення

1	2	3
2	4	7
3	7	14

б) інтенсивність пікселів

Рисунок 2.2 – Інтегральне подання відеозображення

Елементи інтегрального подання розраховуються за формулою:

$$L(x,y)=\sum_{i=0}^{i\le x}\sum_{j=0}^{j\le y} I(i,j), \tag{2.1}$$

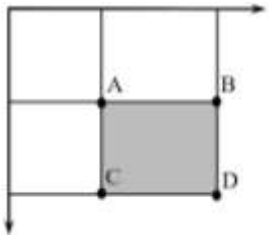
де $I(i,j)$ – яскравість пікселя на зображенні.

Кожен елемент $L(x,y)$ відповідає сумі пікселів, які знаходяться у прямокутнику $(0,0)-(x,y)$. Розрахунок матриці здійснюється за виразом:

$$L(x,y)=I(x,y)-L(x-1,y-1)+L(x,y-1)+L(x-1,y) \tag{2.2}$$

Вираз (2.2) дозволяє обчислити суму пікселів будь-якого заданого прямокутника, використовуючи тільки чотири значення (пікселі в інтегральному поданні, які відповідають кутами прямокутника вхідного зображення).

Візуально результат інтеграційного подання наведено на рис. 2.3.



$$rectangle=D-(B+C)+A$$

Рисунок 2.3 – Графічна інтерпретація
інтегрального подання відеозображення

У загальному вигляді алгоритм здійснює пошук (розпізнавання) обличчя та її контури (геометрію) за допомогою сканування вікна.

Опишемо цей процес. Відеозображення, на якому здійснюється пошук об'єкта, подається у вигляді двовимірної матриця пікселів розміром $x\times y$, кожен піксель якої приймає значення для однотонного зображення grayscale $[0;255]$ та для кольорового зображення формату RGB – $\left[0;255^3\right]$. Пошук здійснюється в активній області зображення прямокутними ознаками (опис користувача та його геометрія обличчя):

$$rectangle=\{(x,y),(w,h),\alpha\}, \tag{2.3}$$

де (x,y) – координати центру i-го прямокутника;

w, h – ширина та висота прямокутника відповідно;

α – кут нахилу прямокутника відносно вертикальної осі зображення.

Ознаки (примітиви) Хаара. Характеристики Хаара – це відображення f :

$$\chi \Rightarrow D_f , \tag{2.4}$$

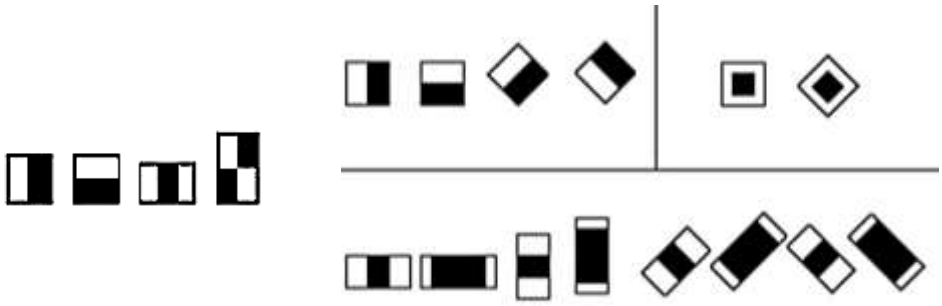
де D_f – множина допустимих значень ознаки.

За умови, що ознака $f_1,...,f_n$ визначена, вираз (2.3) прийме вигляд:

$$\chi \Rightarrow \{ f_1,...,f_n \}, \tag{2.5}$$

який називається ознакою опису об’єкта.

У стандартному методі Віола-Джонса використовуються прямокутні ознаки (примітиви Хаара), а у розширеному – додаткові, яку входять до складу типізованої бібліотеки OpenCV (*від англ.* Open Source Computer Vision Library: бібліотека комп’ютерного зору з відкритим вихідним кодом).



а) примітиви б) додаткові

Рисунок 2.4 – Ознаки Хаара

У процесі пошуку (ідентифікації) обчислювати всі ознаки Хаара практично не можливо, відповідно класифікатор повинен враховувати лише певну підмножину важливих ознак. Таким чином, для досягнення ефективності функціонування алгоритму та надійної роботи необхідно проводити інтелектуальне навчання класифікатора, наприклад з використанням нейронних

мереж. Цей процес є складовою концепції та технології Data Mining (дослідження та інтелектуальний аналіз даних). Машинне навчання в методі Віоли-Джонса вирішує завдання класифікації об'єктів за ознаками.

Тренування класифікатора. В контексті алгоритму, є множина N об'єктів (зображень), які класифікуються за деякими визначеними ознаками**.**

Виконання алгоритму дозволяє класифікувати довільний об'єкт:

- номер (клас), до якого належить даний об'єкт;

- номер або назва класу конкретного об'єкту;

Класифікація проводиться таким чином: є деяка множина $\{O\}$, в якій зберігається опис об'єктів та $\{K\}$ – кінцева множина номерів класів, для яких встановлюється залежність $K^*: O \Rightarrow K$.

Навчальна вибірка (кінцева кількість даних):

$$O_i = \{(o_i, \kappa_i)\},\ i \in [1; n],\ n \in N. \qquad (2.6)$$

У результаті, для $\{O\}$ описується деяка функція, яка для будь-якого можливого значення цієї множини класифікує об'єкт, тобто $o_i \in O$. Дане правило стосується також і нових даних.

Отже, в даному розділі розглянуто математичний апарат процесу ідентифікації користувачів ІТС, який ґрунтується на використанні розширеного алгоритму розпізнавання геометрії обличчя Віоли-Джонса з використанням основних (допоміжних) ознак Хаара. Для підвищення точності аналітичних обчислень застосовується комплекс методів – бустинг (жадібний алгоритм, який на кожному локальному кроці здійснює вибір рішення таким чином, щоб кінцевий результат був оптимальним).

РОЗДІЛ 3. ПРОГРАМНА РЕАЛІЗАЦІЯ МЕТОДУ ІНТЕЛЕКТУАЛЬНОЇ АВТЕНТИФІКАЦІЇ В ІТС НА ОСНОВІ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ТА ПЕРЕВІРКА ЇЇ ПРАЦЕЗДАТНОСТІ

Структурно-алгоритмічна схема програмної реалізації. Для реалізації спеціалізованого програмного забезпечення (СПЗ) інтелектуальної біометричної ідентифікації/автентифікації користувачів ІТС [14] на основі математичного апарату, розглянутого у попередньому розділі, запропоновано структурно-алгоритмічну схему.

Основні етапи функціонування СПЗ:

1. Авторизація санкціонованих користувачів.

2. Біометрична ідентифікація на основі геометрії обличчя (порівняння поточного користувача із шаблонними даними , які містяться у базі даних) [13].

Схема алгоритму першого етапу програмної реалізації наведено на рис. 3.1.

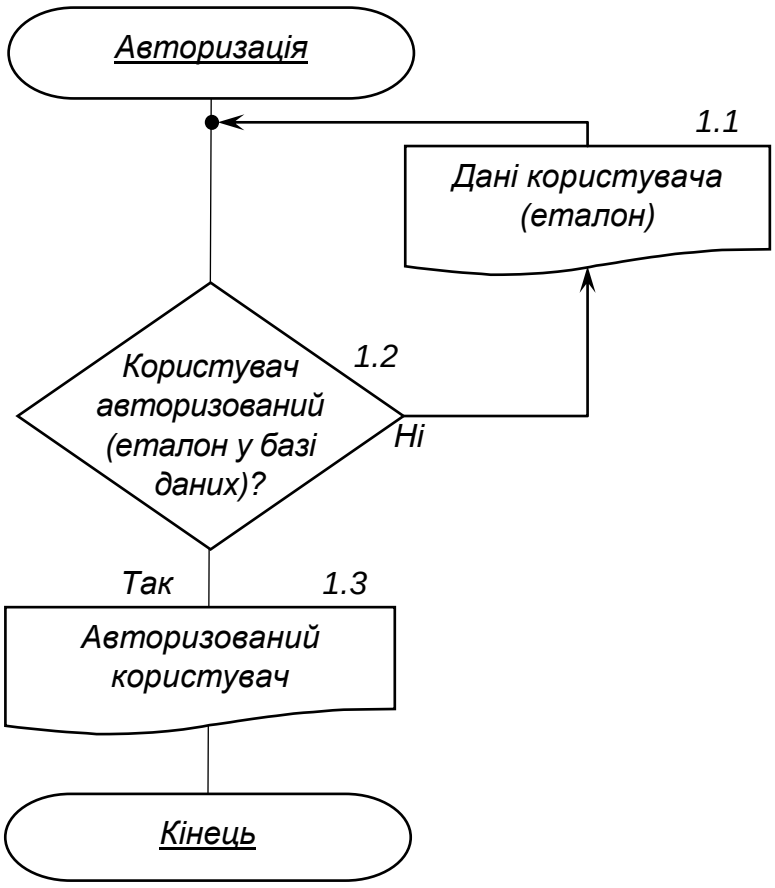


Рисунок 3.1 – Алгоритм авторизації користувачів ІТС

Етап авторизації включає в себе такі блоки:

Блок 1.2. Перевірка користувача на наявність його даних у базі (БД), зокрема шаблонного зображення (фото), прізвища, імені тощо.

Лістинг 3.1.

```
def getImagesAndLabels():
    imagePaths = [os.path.join(path_for_photo, f) for f in os.listdir(path_for_photo)]
    faceSamples = []
    ids = []
    for imagePath in imagePaths:
        PIL_img = Image.open(imagePath).convert('L')
        img_numpy = np.array(PIL_img, 'uint8')
        id = int(os.path.split(imagePath)[-1].split(".")[1])
        faces = detector.detectMultiScale(img_numpy)
        for (x, y, w, h) in faces:
            faceSamples.append(img_numpy[y:y + h, x:x + w])
            ids.append(id)
    return faceSamples, ids
```

Блок 1.1. При необхідності авторизації нового користувача відповідні дані вносяться до існуючої БД:

Лістинг 3.2

```
image = face_recognition.load_image_file(os.path.join(path_for_photo, "User." + str(face_id) + '.' + str(count) + ".jpg"))
            face_encoding = face_recognition.face_encodings(image)[0]
            users[str(face_id)] = [user_name.get(), face_encoding]
            with open('user_list.pickle', 'wb') as f:
                pickle.dump(users, f)
            user_name.set('')
```

Блок 1.3. За умови, що користувач попередньо авторизований, його дані завантажуються з БД для виконання наступного етапу функціонування СПЗ.

Другий етап (рис. 3.2) – власне сам процес ідентифікації/автентифікації користувачів ІТС на основі геометрії обличчя.

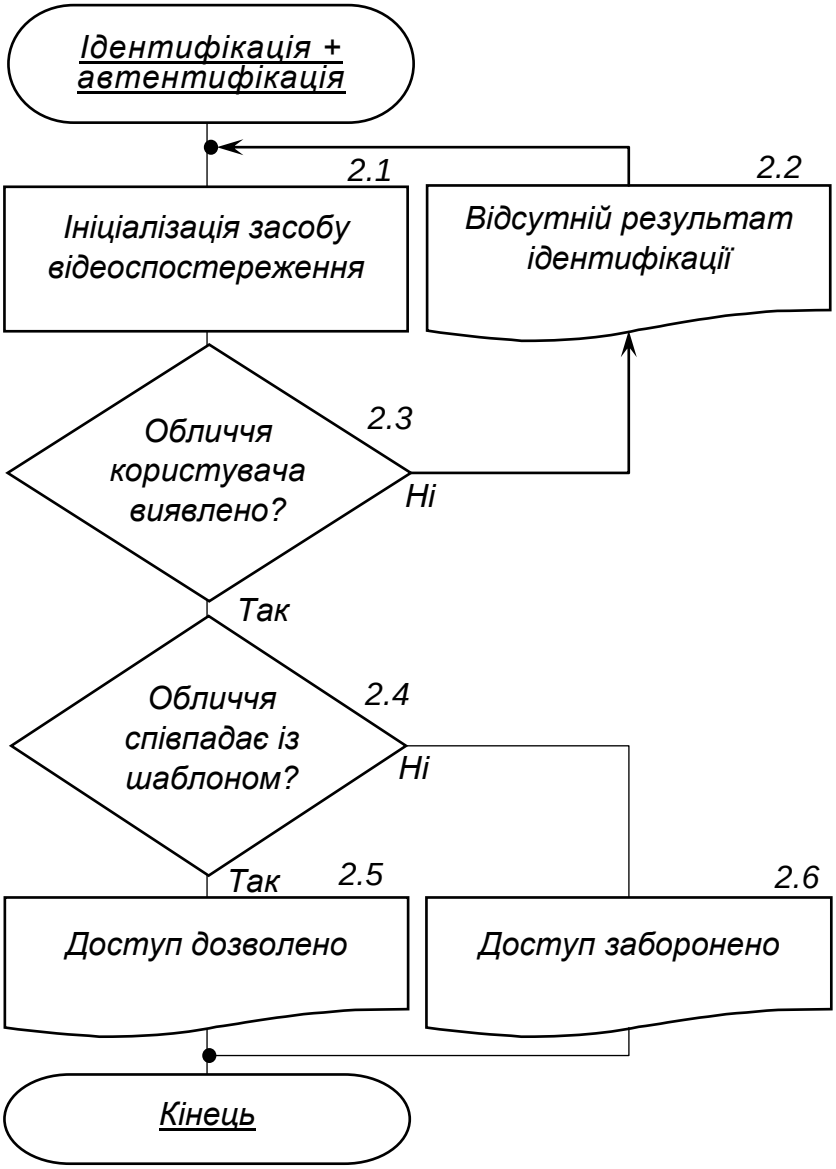


Рисунок 3.2 – Алгоритм ідентифікації/автентифікації користувачів ІТС

Даний етап включає:

Блок 2.1. Ініціалізації відеокамери (інтегрованої або зовнішньої).

Лістинг 3.3

```
video_capture = cv2.VideoCapture(0) or cv2.VideoCapture(1)
   while True: ret, frame = video_capture.read()
      small_frame = cv2.resize(frame, (0, 0), fx=0.25, fy=0.25)
      rgb_small_frame = small_frame[:, :, ::-1]
```

Блок 2.2 – 2.3. Алгоритмічна структура пошуку (виявлення) геометрії обличчя на зображенні відеопотоку в режимі часу, наближеному до реального.

Лістинг 3.4

```
for (top, right, bottom, left), name in zip(face_locations, face_names):
        top *= 4
        right *= 4
        bottom *= 4
        left *= 4
        cv2.rectangle(frame, (left, top), (right, bottom), (119, 172, 152), 2)
        cv2.rectangle(frame, (left, bottom - 35), (right, bottom), (119, 172, 152), cv2.FILLED)
        font = cv2.FONT_HERSHEY_DUPLEX
        cv2.putText(frame, name, (left + 6, bottom - 6), font, 1.0, (0,0,255), 1)
    cv2.imshow('Video', frame)
```

Блок 2.4 – 2.6. Порівняння біометричних даних поточного користувача зі шаблонними даними, які містяться у БД.

Лістинг 3.5

```
    if process_this_frame:
        face_locations = face_recognition.face_locations(rgb_small_frame)
        face_encodings = face_recognition.face_encodings(rgb_small_frame, face_locations)
        face_names = []
        for face_encoding in face_encodings:
            matches = face_recognition.compare_faces(known_face_encodings, face_encoding)
            name = "Unknown"
            face_distances = face_recognition.face_distance(known_face_encodings, face_encoding)
            best_match_index = np.argmin(face_distances)
            if matches[best_match_index]:
                name = known_face_names[best_match_index]
            face_names.append(name)
    process_this_frame = not process_this_frame
```

Програмна реалізація методу. Відповідно до алгоритмічної структури (рис. 3.1 – 3.3) розроблено СПЗ, для реалізації якого використано:

- мову програмування Python 3.6;
- інтегроване середовище розроблення JetBrains PyCharm;
- типізовані пакетні бібліотеки OpenCV, Face_Recognition;
- бібліотеки машинного навчання Dlib.

Головне вікно програмної реалізації інтелектуальної ідентифікації та автентифікації користувачів ІТС наведено на рис. 3.3.

Рисунок 3.3 – Інтерфейс СПЗ ідентифікації/автентифікації користувачів ІТС

Інтерфейс СПЗ розроблено відповідно до класичного вигляду програмних додатків операційних систем сімейства Windows:

1. Панель вкладок основних операцій (відкриття, закриття програми, ініціалізація системи відеоспостереження, довідка програми тощо).
2. Панель авторизації (кнопка “Додати” та поле відображення даних авторизації – кількість авторизованих користувачів).
3. Панель управління (кнопка “Ідентифікувати”) та відображення результатів ідентифікації та автентифікації (поле виведення відеопотоку).

Перевірка працездатності та дослідження умов функціонування СПЗ. Апробація розробленого СПЗ проводилась з використанням наявних технічних засобів, основні характеристики яких наведено у табл. 3.1.

Таблиця 3.1

Основні характеристики технічних засобів

Назва	**Параметр (характеристика)**
Засоби обробки інформації	
Дисплей	15.6" Full HD (1920x1080) IPS
Процесор	Intel® Core ™ i5-8300H Processor (8M Cache, up to 4.00 ГГц)
Оперативна пам’ять	8 ГБ DDR4 2666 МГц
Графічний адаптер	Дискретний, nVidia® GeForce® GTX1050Ti, 4 ГБ
Засоби відеоспостереження	
Роздільна здатність	1 Мп
Формат відеопотоку	HDTV 720p

Умови проведення дослідження працездатності розробленого СПЗ:

- до БД занесено 4 записи шаблонних користувачів ІТС (кожен запис містить до 30 зображень, прізвище, ім’я, унікальний номер тощо);

- світла пора доби (13:30 – 14:30);

- природня (достатня та недостатня) освітленість приміщення – 100 – 400 люкс;

- мінімальна відстань між засобом відеоспостереження та об’єктом ідентифікації складає 0.5 метрів, максимальна – 2.5;

- кількість експериментів дослідження – 200;

- тестовими користувачами обрано одного з авторів наукової роботи (його дані занесені до БД) та двох його колег, один з яких авторизований;

- перевірка працездатності одиночної (персональної) та групової ідентифікацій.

Результат апробації наведено у табл. 3.2.

Таблиця 3.2

Результат дослідження працездатності СПЗ

Відстань, (м)	**Результат (точність) ідентифікації, (%) ([0-20] – не ідентифіковано; [21-100] – виявлено)**	
	Недостатня освітленість, до 150 (лк)	Достатня освітленість, 200-400 (лк)
Персональна ідентифікація		
0.5	30	100
1.0	20	98
1.5	20	95
2.0	10	85
2.5	5	20
Групова ідентифікація		
0.5	5	100
1.0	5	95
1.5	0	60
2.0	0	20
2.5	0	0

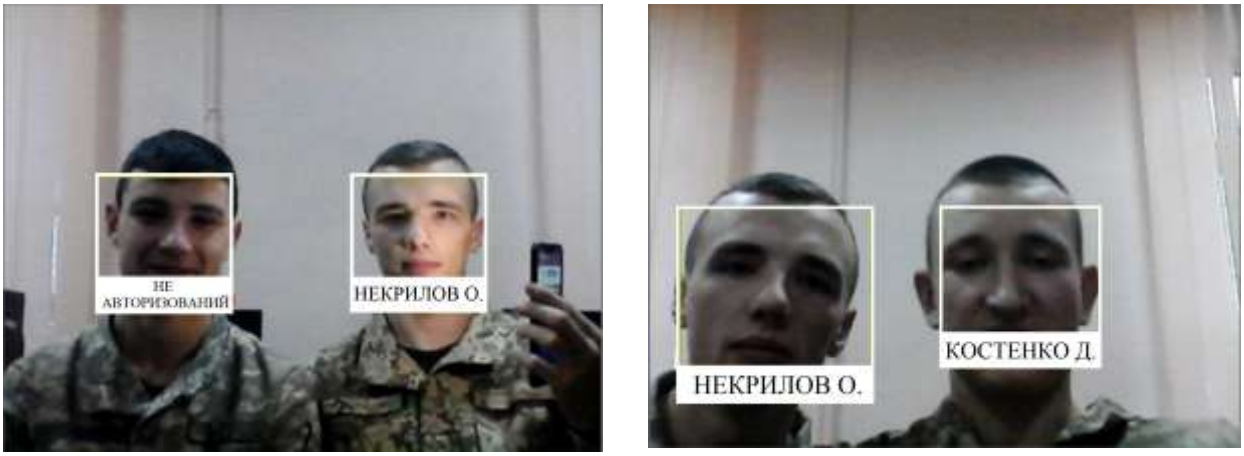
Результати дослідження функціонування СПЗ в залежності від відстані між засобом відеоспостереження та об’єктом ідентифікації наведено на рис. 3.4.

а) відстань 0.5 (м)

б) відстань 2 (м)

Рисунок 3.4 – Персональна ідентифікація при достатній освітленості

Результати роботи СПЗ для групової ідентифікації наведено на рис. 3.5.



а) відстань 0.5 (м)

б) відстань 2 (м)

Рисунок 3.5 – Групова ідентифікація при достатній освітленості

На підставі результатів апробації СПЗ, яке реалізує метод інтелектуальної автентифікації в ІТС на основі геометрії обличчя, встановлено:

- персональна біометрична ідентифікація здійснюється з точністю 85–100 % при достатній освітленості приміщення, середнє значення якої складає 200-400 лк на відстані до 2 метрів та при недостатній – 30 % на відстані лише 0.5;

- групова ідентифікація ефективна лише при достатній освітленості на відстані користувача від засобу відеоспостереження до1.5 метрів.

Таким чином, розроблене СПЗ – ефективний засіб біометричної ідентифікації/автентифікації користувачів ІТС, обробки інформації та боротьби з несанкціонованими інсайдер-користувачам. Умовами використання програмної реалізації методу інтелектуальної автентифікації в ІТС є середнє значення освітленості приміщення або ОІД, яке складає 200–400 люкс. Ефективність СПЗ свого максимального значення досягає при відстані між користувачем та засобом відеоспостереження до 2 метрів (при персональній ідентифікації) та до 1.5 (при груповій).

Отже, СПЗ – працездатний, надійний та ефективний програмний засіб, який доцільно застосовувати при вирішенні важливих завдань у галузі кібербезпеки та технічного захисту інформації.

ВИСНОВКИ

У науковій роботі наведено результати вирішення актуального наукового завдання, яке полягало в удосконаленні методу інтелектуальної біометричної ідентифікації/автентифікації користувачів ІТС та його новітній програмній реалізації.

У ході аналізу технологічного розвитку ІТ встановлено, що одним із потенційно можливих методів надійного захисту інформації та ОІД від НСД є біометрична ідентифікація та/або автентифікація користувачів, зокрема на основі аналізу геометрії обличчя.

У другому розділі наведено та детально розглянуто математичну модель реалізації методу інтелектуальної біометричної ідентифікації/автентифікації користувачів, який ґрунтується на використанні відомого алгоритму Віоли-Джонса. З урахуванням поданого у розділі математичного апарату розроблено спеціалізоване програмне забезпечення, яке є надійним програмно-апаратним інструментом захисту інформації та ОІД від НСД до них.

Практичне значення одержаних результатів полягає в можливості: впровадження методу в сучасні системи контролю та пропускного режиму ОІД; інтеграції програмного забезпечення в системи автентифікації засобів обчислювальної техніки, у тому числі персональних комп'ютерів; блокування доступу до інформації та засобів її обробки для несанкціонованих інсайдер-користувачів тощо.

Таким чином, мети роботи досягнуто.

Перспективи подальших наукових досліджень полягають в удосконаленні запропонованого методу шляхом реалізації мультиідентифікації груп осіб на основі отриманих зображень їх обличь у відкритих серверах мережі Інтернет.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. “Концепція створення національної системи ідентифікації громадян України, іноземців та осіб без громадянства”. Розпорядження Кабінету Міністрів України № 1428-2015-р від 23.12 2015. Режим доступу: https://zakon.rada.gov.ua/
laws/main/1428-2015-%D1%80.

2. Бугаєнко Х., Горбенко І. Аналіз трьох біометричних методів автентифікації особи // Прикладная радиоэлектроника. 2012, Т. 11, № 2. С. 262–266.

3. Царьов Р., Лемеха Т. Біометричні технології: навч. посіб. [для вищих навчальних закладів]. Одеса : ОНАЗ ім. О.С. Попова. 2016. 140 с.

4. Мороз А. Биометрические технологии идентификации человека. Обзор систем. Математические машины и системы. 2011, № 1. С. 39–45.

5. Бідюк П., Бондарчук В. Сучасні методи біометричної ідентифікації // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2009, № 1 (18). С. 137–146.

6. Нечипоренко О., Корпань Я. Біометрична ідентифікація і автентифікація особи за геометрією обличчя // Вісник Хмельницького національного університету. Технічні науки. 2016, № 4. С. 133–138.

7. Prihasto B., et al. A survey of deep face recognition in the wild // International Conference on Orange Technologies (ICOT). 2016. pp. 76–79.

8. Viola P., JonesM. Rapid object detection using a boosted cascade of simple features // IEEE Conf. on Computer Vision and Pattern Recognition. 2001, Vol. 1. pp. 511–518.

9. Бабарика А., Прокопенко Є., Бабій Ю. Дослідження алгоритмів розпізнавання в системі оптико-електронного спостереження охорони державного кордону // Збірник наукових праць Національної академії Державної прикордонної служби України. Сер.: Військові та технічні науки. 2017, № 1. С. 294–305.

10. Тимошин Ю., Орленко С. Алгоритм розпізнавання обличчя людей на базі згорткової нейронної мережі // Адаптивні системи автоматичного управління. 2018, № 1. С. 166–173.

11. Левенець Т., Кравець І. Дослідження методів розпізнавання облич при використанні мобільних технологій // Наукові праці Чорноморського державного університету імені Петра Могили комплексу "Києво-Могилянська академія". Серія : Комп'ютерні технології. 2016, Т. 283, Вип. 271. С. 28–35.

12. Jensen O. Implementing the Viola-Jones face detection algorithm // Informatics and Mathematical Modelling, Denmark : Technical University of Denmark. 2008. 36 p.

13. Гуменюк І., Басараба М., Некрилов О. Біометрична ідентифікація у кіберпросторі на основі розпізнавання обличчя // Проблеми теорії та практики інформаційного протиборства в умовах ведення гібридних війн : наук.-практ. конф., 24–25 жовт. 2019 р. : тези доповідей. Житомир : ЖВІ, 2019. С. 205–207.

14. Спеціалізоване програмне забезпечення біометричної ідентифікації/автентифікації користувачів інформаційно-телекомунікаційних систем на основі геометрії обличчя (Face_ID 1.0.0.0). Свідоцтво про реєстрацію авторського права на твір № 94744, Дата реєстрації 13.12.2019.