Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра комп'ютерних наук
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: Дослідження програмних і апаратних засобів для побудови системи контролю та управління доступом на основі біометричного аналізу відбитку долоні

Виконав: студент II курсу, групи СТд-2
спеціальності 126 Інформаційні системи та технології
(шифр і назва спеціальності)

_____ Кайдик О.Л.
(підпис) (прізвище та ініціали)

Керівник _____ Гром'як Р.С.
(підпис) (прізвище та ініціали)

Нормоконтроль _____ Мацюк О.В.
(підпис) (прізвище та ініціали)

Завідувач кафедри _____ Боднарчук І.О.
(підпис) (прізвище та ініціали)

Рецензент _____ _____
(підпис) (прізвище та ініціали)

Тернопіль
2022

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра комп'ютерних наук
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Боднарчук І.О.
(підпис) (прізвище та ініціали)
«____» _____ 2022 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 126 Інформаційні системи та технології
(шифр і назва спеціальності)

Студенту Кайдику Олегу Леонтійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження програмних і апаратних засобів для побудови системи контролю та управління доступом на основі біометричного аналізу відбитку долоні

Керівник роботи Гром'як Роман Сильвестрович, к.ф.-м.н., доцент кафедри КН
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «_22_» _листопада___ 2022 року № _4/7-953_____

2. Термін подання студентом завершеної роботи 22 грудня 2022р.

3. Вихідні дані до роботи Наукові публікації про ідентифікування суб'єктів доступу за біометричним аналізом відбитку долоні та побудову системи контролю і управляння доступом на його основі

4. Зміст роботи (перелік питань, які потрібно розробити): Вступ. 1 Аналіз предметної області (Біометричне ідентифікування у системах доступу. Технології автентифікації суб'єкта доступу. Розпізнавання за геометрією руки. Система контрою та управління доступом. Програмні методи доступу до баз даних СКУД. Апаратні засоби для організації СКУД. Висновки до першого розділу). 2 Ідентифікування суб'єкта за відбитком долоні (Ідентифікування та реєстрації в СКУД. Задачі детектування та розпізнавання. Методика детектування. Методика розпізнавання. Висновки до другого розділу). 3 Обчислювальний експеримент (Тестова вибірка. Метод оцінювання точності алгоритму. Ідентифікування шляхом простого порівняння із Зразком. Ідентифікування за генеруванням ознак. Висновки до третього розділу). 4 Охорона праці та безпека в надзвичайних ситуаціях (Небезпечні та шкідливі фактори під час виконання робіт із монтування СКУД. Заходи забезпечення сприятливих (безпечних) умов праці. Створення і функціонування системи моніторингу довкілля з метою інтеграції екологічних інформаційних систем). Висновки. Додатки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1 Титульна сторінка. 2 Тема. Мета. Об'єкт. Предмет дослідження. 3 Завдання дослідження. 4 Технології автентифікації СД. 5 Біометричні ознаки руки. 6 СКУД. 7 Модель процесу іденти фікування в СКУД. 8 Формалізований опис завдання ідентифікування. 9 Формування геометричної інформації про долоню. 10 Графічна інтерпретація ознак на основі форми. 11 Метрики порівняння нормалізованих зображень. 12 Алгоритм оцінювання точності ідентифікування. 13 Ідентифікування СД. 14 Розподіл відстаней. 15 Висновки. 16 Апробація результатів валіфіаційної роботи. 17 Завершальний слайд.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Мацюк О.В., доцент		
Безпека в надзвичайних ситуаціях	Клепчик В.М., ст. викладач		

7. Дата видачі завдання 14 листопада 2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	14.11.2022-15.11.2022	*Виконано*
2.	Підбір наукових джерел про ідентифікування суб'єк-		
	тів доступу за біометричним аналізом відбитку долоні		
	та побудову СКУД на його основі	16.11.2022-20.11.2022	*Виконано*
3.	Переклад та опрацювання наукових джерел про іден-		
	тифікуівання суб'єкта доступу за біометричним аналі-		
	зом відбитку долоні та побудову СКУД	21.11.2022-23.11.2022	*Виконано*
4.	Виконання дослідження щодо шляхів реалізації підви-		
	щення точності та якості системи ідентифікування		
	суб'єкта доступу за зображенням відбитка долоні	24.11.2022-27.11.2022	*Виконано*
5.	Оформлення розділу «Аналіз предметної області»	28.11.2022-30.11.2022	*Виконано*
6.	Оформлення розділу «Ідентифікування суб'єкта за		
	відбитком долоні»	01.12.2022-04.12.2022	*Виконано*
7.	Оформлення розділу «Обчислювальний експеримент»	05.12.2022-07.12.2022	*Виконано*
8.	Виконання завдання до підрозділу «Охорона праці»	08.12.2022-09.12.2022	*Виконано*
9.	Виконання завдання до підрозділу «Безпека в надзви-		
	чайних ситуаціях»	10.12.2022-11.12.2022	*Виконано*
10.	Оформлення кваліфікаційної роботи	12.12.2022-13.12.2022	*Виконано*
11.	Нормоконтроль	14.12.2022-15.12.2022	*Виконано*
12.	Перевірка на плагіат	9.12.2022	*Виконано*
13.	Попередній захист кваліфікаційної роботи	16.12.2022	*Виконано*
14.	Захист кваліфікаційної роботи	23.12.2022	

Студент _____ Кайдик О.Л.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Гром'як Р.С.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Дослідження програмних і апаратних засобів для побудови системи контролю та управління доступом на основі біометричного аналізу відбитку долоні // Кваліфікаційна робота освітнього рівня «Магістр» // Кайдик Олег Леонтійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра комп'ютерних наук, група СТд-2 // Тернопіль, 2022 // С. 78, рис. – 30, табл. – 7, додат. – 3, бібліогр. – 59.

Ключові слова: суб'єкт доступу, біометрія, сканер, відбиток долоні, метрика, точність, алгоритм, ідентифікування, управління доступом.

Кваліфікаційна робота присвячена дослідженню систем контролю та управління доступом на основі біометричного аналізу відбитку долоні. В першому розділі кваліфікаційної роботи проаналізовано існуючі підходи до побудови таких систем, висвітлено існуючі технології автентифікації суб'єкта, подано результати аналізу методів ідентифікації відбитків долоні та принципів побудови СКУД за відбитком долоні. В другому розділі кваліфікаційної роботи подано модель процесу ідентифікації в СКУД, методики детектування та розпізнавання відбитку долоні суб'єкта.

В третьому розділі кваліфікаційної роботи запропоновано алгоритм оцінювання точності ідентифікації суб'єкта доступу на основі формування бази зображень відбитків рук та метрика подібності рук між собою, подано результати тестування якості роботи запропонованого алгоритму та оцінка ступеня його стійкості до зміни фону та освітлення. Об'єкт дослідження: процеси збирання та опрацювання біометричних сутностей на прикладі відбитків долоні. Предмет дослідження: методи збирання та аналітичного опрацювання біометричних сутностей на прикладі відбитків долоні.

ANNOTATION

Survey of Software and Hardware Means for Design of Access Control Management System Based on the Palmprint Analysis // Qualification work of the educational level “Master” // Kaidyk Oleh Leontiiovych // Ternopil Ivan Puluj National Technical University,, Faculty of Computer Information Systems and Software Engineering, Department of Computer Science, STd-2 group // Ternopil, 2021 // P. 78, fig. - 30, tables - 7, annexes - 3, references - 59.

Key words: access subject, biometrics, biometric reader, palmprint, metric, accuracy, algorithm, identification, access control.

The qualification work is devoted to the study of access control and management systems based on biometric palmprint analysis. In the first section of the qualification work, the existing approaches to building such systems are analyzed, the existing technologies of subject authentication are highlighted, the results of the analysis of palmprint identification methods and the principles of building an access control management systems based on a palmprint are presented. In the second section of the qualification work, a model of the process of identification in the ACMS, methods of detection and recognition of the subject’s palm print is presented.

In the third section of the qualification work, an algorithm for assessing the accuracy of the identification of the access subject based on the formation of a database of handprint images and a metric of hand similarity is proposed, the results of testing the quality of the proposed algorithm and an assessment of its resistance to changes in the background and lighting are presented. Object of research: processes of collection and processing of biometric entities using the example of palmprints. Subject of research: methods of collection and analytical processing of biometric entities using the example of palmprints.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

EER (англ. Equal Error Rate) – рівна ймовірність помилок.

EMD (англ. Earth Mover`s Distance) – метрика Вассерштейна.

FAR (англ. False Acceptance Rate) – помилка другого роду.

FRR (англ. False Rejection Rate) – помилка першого роду.

PIN (англ. Personal Identification Number) – персоанльний ідентифікаційний номер.

RAD (англ. Rapid Application Development) – швидке розроблення додатків.

RFID (англ. Radio Frequency IDentification) – радіочастотне ідентифікування.

SQL (англ. Structured Query Language) – мова структурованих запитів.

БД – бази даних.

БО – біологічна ознака.

БС – біометрична система.

КУД – контроль та управління доступом.

МЗ – мобільний засіб.

НД – несанкціонований доступ.

ПЗЗ – прилад із зарядовим зв’язком.

ПІА – підсистема ідентифікування та автентифікації.

СД – суб’єкт доступу.

СКУД – система контролю та управління доступом.

СУБД – система управління базами даних.

ТЗ – технічний засіб.

ЗМІСТ

ВСТУП ……. 8

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Біометричне ідентифікування у системах доступу …… 10

1.2 Технології автентифікації суб'єкта доступу ……... 14

1.3 Розпізнавання за геометрією руки ……... 21

1.4 Система контрою та управління доступом ……. 24

1.5 Програмні методи доступу до баз даних СКУД …… 31

1.6 Апаратні засоби для організації СКУД ……... 35

1.7 Висновки до першого розділу …….. 38

2 ІДЕНТИФІКУВАННЯ СУБ'ЄКТА ЗА ВІДБИТКОМ ДОЛОНІ

2.1 Ідентифікування та реєстрації в СКУД ……..…… 39

2.2 Задачі детектування та розпізнавання ……. 45

2.3 Методика детектування …… 46

2.4 Методика розпізнавання ……... 52

2.5 Висновки до другого розділу …….. 55

3 ОБЧИСЛЮВАЛЬНИЙ ЕКСПЕРИМЕНТ

3.1 Тестова вибірка …….. 57

3.2 Метод оцінювання точності алгоритму …….. 58

3.3 Ідентифікування шляхом простого порівняння із зразком …….. 61

3.4 Ідентифікування за генеруванням ознак ……. 63

3.5 Висновки до третього розділу …….. 66

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Небезпечні та шкідливі фактори під час виконання робіт із монтування СКУД ……... 67

4.2 Заходи забезпечення сприятливих (безпечних) умов праці …….. 67

4.3 Створення і функціонування системи моніторингу довкілля з метою інтеграції екологічних інформаційних систем ……. 69

4.4 Висновки до четвертого розділу …….. 71
ВИСНОВКИ …… 72
ПЕРЕЛІК ДЖЕРЕЛ ……. 73
ДОДАТКИ ……... 79

ВСТУП

Актуальність теми. Технології біометричного ідентифікування суб’єктів доступу широко представлені у системах контролю та управління доступом. На практиці застосовують різні підходи, які дозволяють підвищити рівень безпеки. Попит на такі системи з кожним роком тільки зростає, а ідентифікація суб’єкта доступу за його біометричним відбитком долоні є одним із перспективних їх напрямів.

Мета і задачі дослідження. Метою даної кваліфікаційної роботи освітнього рівня «Магістр» є підвищення точності та якості системи ідентифікування суб’єкта доступу за зображенням відбитка долоні, яке дозволить врахувати згрупованість біометричних зображень та оцінити точність ідентифікування за нормалізованим зображенням.

Для досягнення поставленої мети було потрібно виконати наступні завдання:

- провести аналіз досліджень в області ідентифікування суб’єкта доступу за біометричними ознаами;
- дослідити оргацізацію біометричного контролю за відбитком долоні;
- подати модель ідентифікування суб’єкта доступу для СКУД;
- навести узагальнені алгоритми дететування та розпізнавання ознакових описів суб’єкта доступу;
- розробити алгоритм оцінювання точності ідентифікування суб’єкта доступу на основі формування бази зображень відбитків долонь;
- оцінити якість роботи алгоритму ідентифікування за стійкістю зміни фону та освітлення відносно нормалізованого зображення відбитка долоні.

Об’єкт дослідження. Програмні та апаратні засоби для біометричного аналізу зображення відбитка долоні.

Предмет дослідження. Оперативна задача ідентифікування суб’єкта доступу за біометричним відбитком долоні.

Наукова новизна одержаних результатів кваліфікаційної роботи полягає у тому, що отримано результати тестування якості роботи алгоритму оцінювання точності ідентифікування суб'єкта доступу за зображенням відбитків його рук.

Практичне значення одержаних результатів. Описано алгоритм оцінювання точності ідентифікування суб'єкта доступу на основі формування бази зображень відбитків рук та метрика подібності рук між собою.

Апробація результатів магістерської роботи. Основні результати проведених досліджень обговорювались на: III-й міжнародній науково-практичній конференції «Priority Directions of Development of Science fnd Education» (Zdar nad Sazavou, Czech Republic); Всеукраїнській науково-практичній конференції молодих учених і студентів «Інформаційні технології в освіті, техніці та промисловості» (м. Івано-Франківськ); V-й Всеукраїнській науково-практичній конференції «Приладобудування та метрологія: сучасні проблеми, тенденції розвитку» (м. Луцьк).

Публікації. Основні результати кваліфікаційної роботи опубліковано у трьох працях конференції (див. Додаток А, Б, В).

Структура й обсяг кваліфікаційної роботи. Кваліфікаційна робота складається зі вступу, чотирьох розділів, висновків, списку літератури із 59 найменувань та 3 додатків. Загальний обсяг кваліфікаційної роботи складає 78 сторінки, з них 62 сторінки основного тексту, який містить 30 рисунків та 7 таблиць.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Біометричне ідентифікування у системах доступу

На практиці, усі системи забезпечення контрольованого доступу прийнято поділяти на [19]:

- парольний захист – суб’єкт доступу надає/пред’являє системі свої секретні дані;
- застосування ключів – суб’єкт доступу надає/пред’являє системі свій персональний ідентифікатор, який і є фізичним носієм секретного ключа;
- біометрія – суб’єкт доступу надає/пред’являє системі свій особистий параметр, який є невід’ємною його частиною (індивідуальні характеристики).

Враховуючи те, що біометричні системи доступу базуються на наявності індивідуальних людських параметрів, які не можливо втратити, викрасти або скопіювати, то вони є зручними для користувачів.

Зародження біометричних технологій. Біометричні технології набагато давніші, ніж можна собі уявити. Ще у Стародавньому Єгипті переваги ідентифікації робітників визнавались за заздалегідь нанесеними тілесними характеристиками [17]. Дана технологія значно випередили свій час, оскільки протягом наступних чотирьох тисяч років у цій галузі практично нічого нового не відбувалося.

Наприкінці XIX століття почали зароджуватись системи, в основу яких було покладено використання відбитків пальців та інші фізичні характеристики ідентифікації людей. У 1880 році Г. Фоулдс публікує свої роздуми про різноманіття та унікальність відбитків пальців, і припустив, що їх можна використовувати для ідентифікації злочинців, а в 1900 році уже опубліковано систему класифікації відбитків пальців Гальтона-Генрі.

За винятком декількох робіт про унікальність райдужної сітківки ока (перша функціонуюча технологія була представлена в 1985 році),

біометричні технології практично не розвивалися до 1960-х років, коли брати Міллер розпочали впроваджувати пристрій, який автоматично визначав довжину пальців людини. Наприкінці 1960-х та 70-х років були розроблені технології ідентифікування особи за голосом та підписом.

Біометричні системи забезпечення безпеки були спрямовані лише на захист військових таємниць та важливої комерційної інформації. Після терористичного акту 11 вересня 2001 року ситуація різко змінюється [2]. Системами біометричного доступу обладнують аеропорти, великі торгові центри та інші масові скупчення людей. Підвищений попит спровокував дослідження у цій галузі, що, своєю чергою, призвело до появи нових пристроїв та цілих технологій.

Природно, що збільшення ринку біометричних пристроїв призвело до збільшення кількості компаній, які почали займатись ними, а конкуренція спричинила між ними вплинула на зменшення вартості біометричних системи забезпечення інформаційної безпеки.

Основні відомості про біометрію. Біометрія являє собою процедуру ідентифікування суб’єкта доступу за унікальними, властивими лише їй біологічними ознаками [3, 38]. На даний час, системи доступу та захисту інформації, які засновано на таких технологіях, є не тільки надійними, але й зручними для користувачів. СД немає потреби запам’ятовувати складні паролі, постійно носити із собою апаратні ключі. Для того щоб потрапити до приміщення або отримати доступ до інформації необхідно лише прикласти до сканера палець або руку, підставити для сканування очі або щось сказати.

Для ідентифікації людини прийнято використовувати різні біологічні ознаки. Усіх їх розділено на дві групи ознак: статичні та динамічні [32].

До статичних ознак зазвичай відносять відбитки пальців, райдужну оболонку та сітківку ока, форму обличчя, форму долоні, розташування вен на кисті руки тощо. Тобто, цю групу формують лише ті ознаки, які не змінюються у людині із часом, починаючи з моменту її народження.

Динамічні ознаки являють собою голос, почерк, клавіатурний почерк, особистий підпис тощо. Загалом, до цієї групи відносять характеристики поведінки людини, які характеризують підсвідомість рухів під час відтворення будь-якої дії. Цим ознакам характерна поступова зміна їх у часі.

Ідентифікування людини за статичними ознаками більш надійні, у порівнянні із динамічними, хоча ймовірність виникнення помилок першого роду залишається досить великою для обидвох.

Біометричні технології засновані на біометрії, вимірі унікальних характеристик окремо взятої людини. Це можуть бути як унікальні ознаки, отримані з народження, наприклад: ДНК, відбитки пальців, райдужна оболонка ока; так і характеристики, придбані з часом або здатні змінюватися з віком або зовнішнім впливом. Наприклад: почерк, голос або хода.

Зростаючий останнім часом інтерес до цієї тематики у світі прийнято пов'язувати з загрозами народного тероризму, що активізувався. Багато держав у найближчій перспективі планують ввести в обіг паспорти з біометричними даними.

Алгоритм роботи біометричної системи. Робота усіх біометричних систем побудована за одним і тим же принципом. Ідентифікація у них здійснюється за чотири стадії:

- запис – запам’ятовування системою статичних та динамічних ознак суб’єкта доступу;
- виділення – для СД із зразка виокремлюється унікальна інформація, на основі якого формується біометричний зразок;
- порівняння – збережений у БС біометричний зразок СД порівнюють із наданим/пред’явленим;
- співпадіння/неспівпадіння – БС приймає рішення про те чи співпадають біометричні зразки та приймає рішення.

На першому етапі біометрична система запам’ятовує/записує зразок біометричної характеристики (для складання найбільш точного зображення

біометричної характеристики деякі БС пропонують СД зробити декілька зразків). Далі отримана інформація опрацьовується та перетворюється на математичний код (для прописання біометричного зразку конкретному СД деякі БС вимагають додатково виконати деякі дії). Наступний етап вимагає застосування пристрою зчитування біологічного параметра, що дозволяє опрацювати результат та перетворити його в цифровий код, який порівнюється із вмістом спеціальної бази даних.

Переважна більшість людей вважають, що в пам’яті комп’ютера зберігається зразок відбитка пальця, голосу людини або зображення райдужної оболонки його ока. Але насправді у більшості сучасних систем це не так. У спеціальній базі даних зберігається цифровий код довжиною до 1000 біт, який асоціюється з конкретною людиною, яка має право доступу. Сканер або будь-який інший пристрій, який використовується в системі, зчитує певний біологічний параметр людини. Далі він обробляє отримане зображення або звук, перетворюючи їх на цифровий код. Саме цей ключ і порівнюється із вмістом спеціальної бази даних для ідентифікації СД. На останньому етапі БС приймається рішення про допуск ідентифікованого суб’єкта на об’єкт доступу.

Параметри біометричних систем. Ймовірність виникнення помилок FAR/FRR, тобто коефіцієнтів помилкового допуску (False Acceptance Rate – наданий системою доступ незареєстрованому користувачеві) та помилкової відмови у доступі (False Rejection Rate –заборона у доступі зареєстрованій в системі людині). На практиці взаємозв’язок між цими показниками має бути врахованим [44], оскільки зниження рівня «вимогливості» системи FAR дозволяє зменшити відсоток помилок FRR, і навпаки.

На даний час усі біометричні технології відносять до ймовірнісних, оскільки вони не здатні гарантувати повну відсутність помилок FAR/FRR.

Практична реалізація біометричних технологій**.** Активний розвиток біометричних систем забезпечення інформаційної безпеки дозволив

витіснити із ринку інші способи інформаційного захисту. Біометричні технології активно застосовуються у багатьох галузях, які пов’язані із забезпеченням безпеки доступу до інформації, матеріальних об’єктів та ідентифікування суб’єкта доступу.

Застосування біометричних технологій різноманітні: доступ до робочих місць та мережевих ресурсів, захист інформації, забезпечення доступу до певних ресурсів та безпека. На сьогоднішній день біометричні технології застосовуються у різних сферах народного господарства: безпека банків та інших фінансових установ, роздрібної торгівлі, охорони правопорядку, питань охорони здоров’я та надання соціальних послуг.

У майбутньому на біометричні технології будуть покладені основні завдання із персонального ідентифікування у багатьох сферах.

1.2 Технології автентифікації суб’єкта доступу

Звичайні системи автентифікації не завжди задовольняють вимоги, які висуваються до сучасних систем безпеки. Біометрична автентифікація суб’єкта допуску дозволяє впевнено ідентифікувати суб’єкта за фізіологічними параметрами або характеристики його поведінки [14].

На практиці для автентифікації СД, досить широко, застосовують такі біометричні ознаки як: відбитки пальців; геометрична форма кисті руки; форма та розмір лиця; особливості голосу та узор райдужної оболонки ока.

Автентифікація за відбитками пальців. Ідентифікація за відбитками пальців (див. рисунок 1.1) – найпоширеніша, надійна та ефективна біометрична технологія [12]. Завдяки своїй універсальності її застосовують для вирішення будь-якого завдання, у будь-якій сфері, яке пов’язане із достовірною ідентифікацією суб’єктів доступу. В основі методу покладено унікальність малюнка папілярних узорів на пальцях (відбитки усіх пальців у кожного СД унікальні та не змінюються протягом усього його життя) [13].

Рисунок 1.1 – Ідентифікування суб’єкта допуску за відбитками пальців

Відбиток, який отримують шляхом застосування спеціального сканера (ємнісного, прокатного, оптичного), давача або сенсора та перетворюють на цифровий код і порівнюють із введеним раніше еталоном [30].

Автентифікація за сітківкою ока. Метод автентифікації сітківки ока отримав практичне застосування після того, як у 50-ті роки XX століття було доведено унікальність малюнка кровоносних судин очного дна (рисунок 1.2).

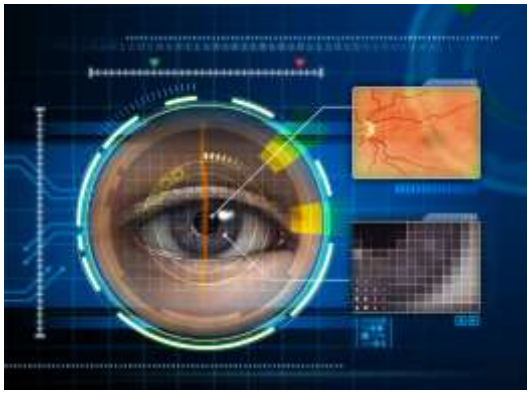


Рисунок 1.2 – Ідентифікування суб’єкта допуску за сітківкою ока

Для сканування сітківки застосовують інфрачервоне випромінювання низької інтенсивності [13, 30, 41], яке спрямовано через зіницю до кровоносних судин на задній стінці ока. З отриманого сигналу виділяють кілька сотень спеціальних точок, інформація про які зберігається у шаблоні.

Така біометрична технологія набула широкого поширення для доступу до надсекретних об’єктів, оскільки забезпечує одну із найнижчих

ймовірностей помилки першого роду (відмова у доступі для зареєстрованого користувача) та майже нульовий відсоток помилок другого роду. Останнім часом даний метод розпізнавання не застосовують, оскільки окрім біометричної ознаки він містить у собі інформацію про здоров’я суб’єкта.

Автентифікація за райдужною оболонкою ока. Технологія розпізнавання за райдужною оболонкою ока була розроблена на противагу методу сканування сітківки ока (сітківка ока змінюється з часом, тоді як райдужна оболонка ока залишається незмінною), при якому використовуються інфрачервоні промені (яскраве світло) [13, 30, 41].

Рисунок 1.3 – Ідентифікація суб’єкта допуску за райдужною оболонкою ока

Для отримання біометричної ознаки за райдужною оболонкою застосовують методику низькоінтенсивного висвітлювання райдужної оболонки ока, що дозволяє відеокамері сфокусуватися на ній (для створення зразка програма сканування використовує біля 260 точок прив’язки.). Райдужна оболонка ока текстурою нагадує мережу із великою кількістю навколишніх кіл і малюнків (рисунок 1.3).

Автентифікація за геометрією руки. Даний біометричний метод було засновано у 70-ті роки минулого століття, а для ідентифікування особистості були вибрані параметри, які характеризують форму (геометрію) руки [12, 41]. Враховуючи те, що окремі параметри є унікальними, то на практиці використовують декілька характеристик одночасно (див. рисунок 1.4).

Рисунок 1.4 – Ідентифікування суб’єкта допуску за геометрією руки

За допомогою сканера скануються такі геометричні параметри руки, як вигини пальців, їх довжина та товщина, ширина та товщина тильного боку руки, відстань між суглобами та структура кістки.

Системи автентифікації за геометрії руки є досить поширеними, що говорить про їх зручність з точки зору користувачів. Процедура отримання зразка досить проста та не потребує високих вимог до зображення. На процес автентифікації не впливають ні температура, ні вологість, ні забрудненість. Розрахунки для порівняння із еталоном є простими та легко автоматизувати.

Рисунок 1.5 – Ідентифікування суб’єкта допуску за геометрією обличчя

Автентифікація за геометрією обличчя. Біометрична автентифікація суб’єкта доступу за геометрією обличчя є досить поширеним способом ідентифікації та автентифікації [12, 13, 30, 41]. Технічна реалізація цієї технології є складною математичною задачею.

Широке використання мультимедійних технологій (застосування відеокамер на вокзалах, аеропортах, площах, вулицях, дорогах тощо) стало вирішальним для розвитку даного напрямку. Для побудови тривимірної моделі СД перш за усе виокремлюють контури його очей, брів, губ, носа та інших елементів обличчя, після чого визначають відстань між ними та будують тривимірну модель (див. рисунок 1.5).

Для формування унікального шаблону, який відповідатиме конкретному суб'єкту потрібно від 12 до 40 характерних елементів. Шаблон повинен враховувати безліч варіацій зображення на випадок повороту обличчя, нахилу, зміни освітленості, зміни виразу. Кількість таких варіантів зменшується у залежності від цілей застосування цього способу.

Деякі алгоритми дозволяють компенсувати наявність у людини окулярів, капелюхів, вусів та бороди.

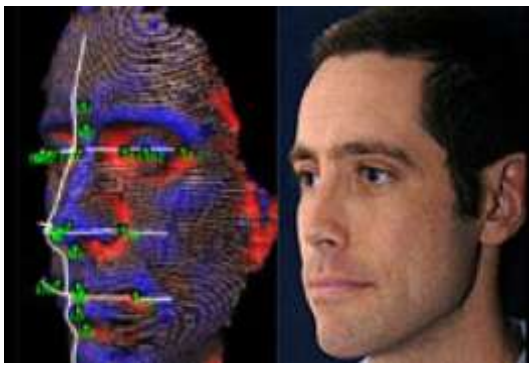


Рисунок 1.6 – Ідентифікація суб'єкта допуску за термограмою його обличчя

Автентифікація за термограмою обличчя. Даний спосіб базується на дослідженнях, які показують, що зображення суб'єкта допуску в інфрачервоному спектрі дозволяє отримати картиний розподіл його температурних полів (термограма) та є унікальним для кожного з них. Термограма (рисунок 1.6) формується за допомогою спеціальних камер, які працюють в інфрачервоному діапазоні [13, 30, 41].

Фізіологічні чинники СД не впливають точність термограми, але цей метод не отримав широкого застосування за рахунок його невисокої якості.

Автентифікація за голосом. Біометричний метод автентифікації за голосом, характеризується простотою застосування. Даному методу не потрібна дорога апаратура, достатньо мікрофона та звукової плати (рисунок 1.7). В наш час ця технологія швидко розвивається, так як даний метод автентифікації широко використовується в сучасних бізнес-центрах.

Рисунок 1.7 – Ідентифікування суб’єкта допуску за голосом

На практиці існує велика кількість способів побудови шаблону за голосом [13, 30]. Зазвичай це різні комбінації частотних і статистичних характеристик голосу (модуляція, інтонація, висота тону тощо).

Основним та визначальним недоліком цього методу є його низька точність методу. Шумова компонента є ще однією важливою і не вирішеною проблемою практичного використання автентифікації за голосом.

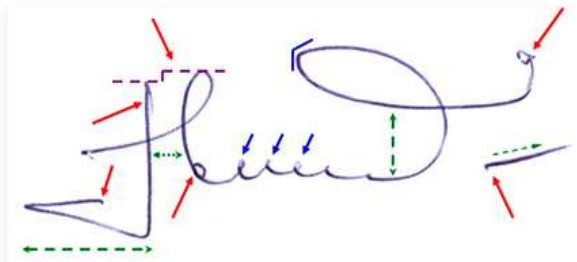
Оскільки ймовірність помилок другого роду під час використання цього методу велика (≈1%), то автентифікацію за голосом застосовується тільки для управління доступом у приміщеннях середнього рівня безпеки.

Автентифікація за почерком. Зазвичай, на практиці, виділяють два способи оброблення даних про підпис [12, 13, 30, 41]:

- аналіз самого підпису, коли використовують ступінь схожості двох картинок (див. рисунок 1.8, *а*);

- аналіз динамічних характеристик напису, коли для автентифікації будують розгортку напису, до якої входить інформація про його тимчасові та статистичні характеристики (див. рисунок 1.8, *б*).

а)



б)

Рисунок 1.8 – Ідентифікування суб’єкта допуску за почерком

Класична верифікація (ідентифікація) СД за почерком полягає у звіренні аналізованого зображення з оригіналом. Зазвичай таку процедуру робить оператор, а тому її точність, з огляду на ймовірність прийняття неправильного рішення (FAR та FRR) невисока. Окрім цього, на розкид значень ймовірності прийняття правильного рішення впливає і суб’єктивний чинник. Принципово нові можливості верифікації за почерком притаманні новим автоматичним методам аналізу почерку та прийняття рішення. Дані методи дозволяють виключити суб’єктивний чинник та значно знизити ймовірність помилок під час ухвалення рішень.

а)

б)

Рисунок 1.9 – Комбінована біометрична система автентифікації

Комбінована біометрична система автентифікації. Комбінована або мультимодальна біометрична система автентифікації (рисунок 1.9, *а*) включає у себе різні доповнення, які дозволяють використовувати декілька типів біометричних характеристик та дозволяє поєднати у собі різні типи біометричних технологій систем автентифікації в одній [13, 30, 41]. Це

дозволяє задовольнити найсуворіші вимоги щодо ефективності організації системи автентифікації (наприклад, автентифікація відбитків пальців легко поєднується зі скануванням руки (див. рисунок 1.9, *б*)). Така структура може використовувати усі види біометричних даних СД і застосовуватись там, де доводиться пришвидшувати обмеження однієї біометричної характеристики. Комбіновані системи є більш надійними з точки зору можливості імітації біометричних даних суб'єкта доступу, оскільки важче підробити низку характеристик, ніж фальсифікувати одна біометрична ознака.

1.3 Розпізнавання за геометрією руки

У загальному випадку з руки можна зняти близько 90 інформаційних ознак, частина з яких, взагалі, не використовується в біометрії. На даний час в біометрії з метою автентифікації суб'єкта доступу використовується просто геометрія руки – розміри, форма, в окремих випадках інформаційні ознаки на зовнішній частині долоні (рисунок шкіри на суглобах між фалангами пальців, рисунок розташування кровоносних судин).

На практиці відомими є два підходи для розпізнавання СД [4, 33]:

- за геометричними параметрами кисті руки (див. рисунок 1.10, *а*);
- за геометричними та образовими параметрами руки.

Перший метод уже добре відомий та застосовується від самого зародження біометричних систем контролю доступу (понад 25 років). З точки зору компактності образу цей клас систем є найекономнішим (найпростіший варіант зберігає лише інформація про довжину та ширину пальців, а для цього необхідно всього 9 байт). Природно, що системи, які працюють лише за ідентифікуванням довжини та ширини пальців можна достатньо легко їх обійти, виготовивши муляж руки оригіналу. Більш складними прийнято вважати системи, які вимірюють профіль руки, що включає об'єм кисті, пальців, нерівності долоні, розташування складок шкіри на згинах.

Другий, більш сучасніший, та заснований на поєднанні геометричних та образових характеристик руки суб'єкта доступу. До останніх відносять образи ділянок шкіри, які формуються фалангами пальців та рисунки підшкірних кровоносних судин. Для даного метода характерним є те, що з руки знімають чотири характеристики, три з яких – скалярні, які відносять до розмірів пальців (рисунок 1.10, *в*).

а) *б*) *в*)

Рисунок 1.10 – Біометричні ознаки руки

а) – 3D геометрія руки (контрольні точки та геометричні ознаки руки); *б*) – відбиток руки (рисунок на долоні, який складається із п'яти основних ліній); *в*) – 2D геометрія руки за чотирьома характеристиками

На рисунку 1.10, *а* подано характеристичні (контрольні) точки, які позначено у вигляді відрізків. Основними вихідними біометричними параметрами руки прийнято вважати: ширину долоні, радіус вписаного в долоню кола, довжину (відстань від верхніх контрольних точок пальців до середин ліній, які з'єднують нижні) та ширину пальців, висота кисті руки на трьох рівнях (*a*, *b* і *c*).

На практиці системами верифікації суб'єкта доступу за геометрією руки застосовуються лише деякі із наведених вище ознак. Допустимим, також, є використання і інших ознак, які отримують із вихідних, шляхом їх математичної обробки: кути між контрольованими точками, середнє значення та дисперсію значень вихідних ознак тощо [5].

Особливістю такого способу отримання біометричних характеристик руки є його простота. При цьому, еталонний параметр руки записується компактно, у вигляді векторних значень ознак і зводиться до наступного [45]:

- у кожного суб'єкта доступу знімають декілька силуетів руки із яких формують векторне значення ознак;
- усі вектори ознак одного СД об'єднують в окремий клас, який буде характерним тільки для цієї ознакової множини;
- за ознаки образу-еталона свого класу прийнято призначати середні значення відповідних ознак усього класу (образ-еталон – вершина класу);
- вихідні ознаки та/або множину вихідних ознак прийнято модифікувати (корегуються на нові шляхом селекції ознак);
- образи-еталони також змінювати за наведеною вище модифікацією;
- новий образ класифікують за множиною вихідних або модифікованих ознак шляхом порівняння із образом-еталоном.

Однією із мір подібності порівнюваних образів може бути метрика L_2 (див. рисунок 1.10, *а*), яка базується на відповідності нового образу СД уже наявним центрам класів: що меншою є ця відстань, то ближчим буде новий образ до відповідного класу. У тому випадку коли в біометричних системах здійснюється процедура автентифікації, то вона оцінює відстань між новим образом та наявними образами-еталонами. При цьому визначена відстань не повинна перевищувати задане значення, в іншому випадку вважають, що автентифікація не підтверджена.

Застосування подібних біометричних систем потребує вкрай обережного ставлення, оскільки застосування різних муляжів кисті руки іншими СД призведе до несанкціонованого доступу в систему.

На рисунку 1.10, *в* подано технологію автентифікації суб'єкта доступу, яка полягає у тому, що з руки знімають тільки чотири характеристики.

Три перших характеристики (ширина вказівного пальця *1*, висота вказівного пальця *2* і довжина середнього пальця *3*) прийнято оцінювати так,

як показано на рисунку 1.10, *в*. Характеристика *4*, у даному випадку, являє собою зображення складок шкіри на згині між середньою і нижньою фалангою вказівного пальця.

Саме наявність додаткової біометричної характеристики руки суттєво ускладнює виготовлення муляжу – який, як правило, застосовують для зламування системи ідентифікації. Зауважимо, що виробники, які постачають такі системи ідентифікації, не надають конкретної інформації про додаткові ознаки (характеристики) руки суб'єкта доступу. Дана перевага зменшує ймовірність фізичного доступу до системи.

1.4 Система контрою та управління доступом

СКУД, на сьогоднішній день, є невід'ємною складовою сучасних систем захисту об'єктів різного рівня [50]. Застосування подібних комплексів дозволяє не тільки запобігти несанкціонованому доступу, але й надає інструментарій для контролю за поведінкою людей на об'єкті, який охороняється. Інтеграція СКУД з іншими технічними засобами захисту дозволяє організувати евакуацію у разі надзвичайних ситуацій.

Варто врахувати те, що технічні можливості таких систем дозволяють автоматизувати процес ідентифікації особистості, однак для більшості випадків вирішення цього завдання потребує залучення людських ресурсів.

Класифікація СКУД. Структура та кількісний склад комплексу технічних засобів забезпечення безпеки можуть змінюватись в залежності від умов функціонування об'єкта та кількості рубежів захисту [23]. Важливим елементом кожного рубежу є СКУД, яка дозволяє забезпечувати безпеку персоналу, а також збереження матеріальних та інформаційних ресурсів підприємства за допомогою організації контрольно-перепускного режиму. Подібні системи успішно застосовуються як на промислових об'єктах, так і в житлових приміщеннях, офісних центрах, магазинах тощо.

До основних завдань СКУД прийнято відносити:

- запобігання несанкціонованому доступу до контрольованих зон із обмеженим доступом, у тому числі реєстрація таких подій;
- організація безперешкодного проходу до зон із вільним доступом;
- забезпечення умов дотримання внутрішньооб'єктного режиму та виконання відповідних обов'язків персоналом об'єкта;
- контроль та облік доступу відвідувачів на об'єкт;
- інтеграція із іншими системами безпеки.

СКУД являє собою сукупність програмно-апаратних засобів, які володіють технічною, інформаційною, програмною та експлуатаційною сумісністю. Пристрої, які входять до таких систем розділяють на групи:

- зчитувальні пристрої – кардридери доступу, біометричні сканери, пристрої розпізнавання автомобільних номерів, кодонабірні пристрої тощо;
- засоби виявлення матеріалів: металодетектори, засоби виявлення вибухових речовин та радіаційних матеріалів;\
- пристрої для оброблення інформації: панелі керування, контролери;
- виконавчі пристрої: турнікети, хвіртки, шлагбауми, електромеханічні, електромагнітні та механічні замки тощо;
- допоміжні пристрої: модулі зв'язку між компонентами СКУД, інжектори живлення, адаптери тощо.

Як було згадано вище, СКУД прийнято реалізувати різними способами, усе залежить від умов функціонування конкретно взятого об'єкта та задач, які при цьому мають вирішуватись (у певних випадах прийнято застосовувати автономні СКУД для кожної точки доступу).

Останнім часом популярності набули розподілені системи [51], які підтримують масштабування під час розширення контрольованої зони. У таких випадках контролери доступу виступають самостійними пристроями, які здійснюють процес управління із використанням спеціалізованих віддалених інтерфейсних модулів.

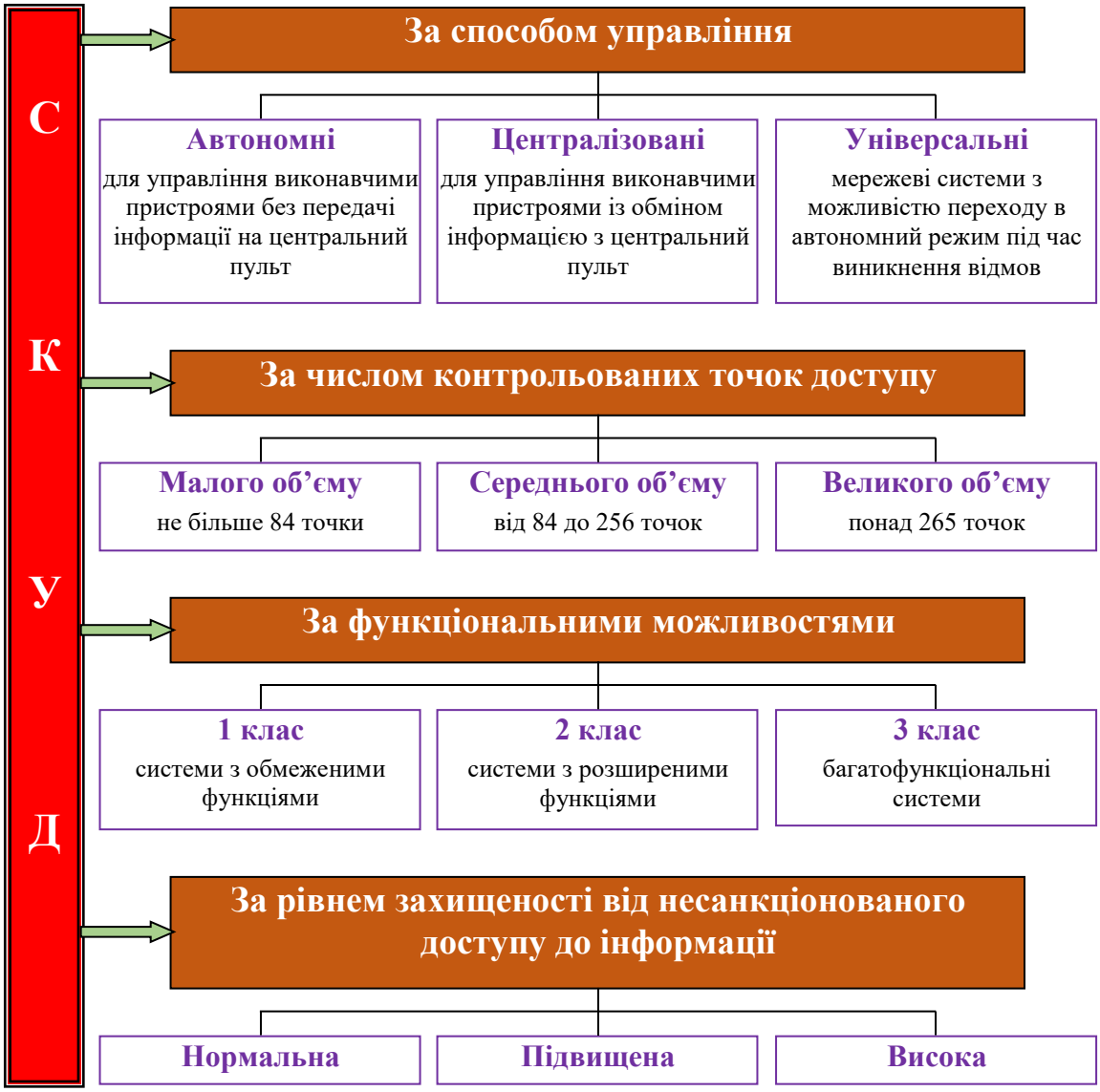


Рисунок 1.11 – Класифікація СКУД

Розподіл засобів та систем контрою та управління доступом на класи прийнято здійснювати на основі порівняльного аналізу ряду функціональних можливостей. У нормативних документах, поряд із загальними технічними вимогами та методами випробувань, зазвичай наводять і класифікацію подібних систем (див. рисунок 1.11). Отже, СКУД класифікують за [7]:

- способом управління;
- числом контрольованих точок доступу;
- функціональним характеристикам;
- видом об'єктів контролю;
- рівнем захищеності системи від несанкціонованого доступу.

Автономні системи, як правило, застосовують на об’єктах, де відсутньою є потреба у постійному моніторингу подій та віддаленому управлінні виконавчими пристроями. Централізовані (мережеві) СКУД застосовуються у тому випадку, коли необхідно проводити контроль часу проходження персоналу та керувати конфігурацією будь-якою частиною системи із центрального пульта. Універсальність мережевих СКУД дозволяє їм переходити у режим автономної роботи під час виникнення відмов управляючих процесорів, мережевого обладнання або обриву зв’язку із контролером. Для побудови універсальних СКУД прийнято використовувати централізовану, розподілену та змішану архітектури.

Централізована архітектура передбачає використання центрального контролера, який здійснює процес управління за допомогою спеціалізованих інтерфейсних модулів (контролер зберігає усю базу ідентифікаторів та подій, які накопичуються системою). Таким чином, поділ функції прийняття рішень та безпосереднього управління підвищує рівень безпеки СКУД.

Системи, які побудовано із врахуванням принципів розподіленої архітектури, містять бази даних ідентифікаторів та подій не на одному, а на декількох контролерах (виконують функції керування зовнішніми пристроями та охоронними шлейфами). Особливість типового розташування контролерів, за розподіленої архітектури, дозволяє системі, у разі, обриву лінії зв’язку між ними та процесорами, продовжувати виконувати основні функції управління процесом доступу в автономному режимі.

Найбільш поширеним є підхід до побудови мережевих СКУД за змішаною архітектурою, який передбачає використання спеціалізованих зчитувачів із власним буфером пам’яті ідентифікаторів та подій (інтелектуальні інтерфейсні модулі). Робота такої системи базується на централізованій архітектурі, а тому, під час пошкодження ліній зв’язку між центральним контролером та інтерфейсними модулями управління виконавчими пристроями активується автономний режим керування

доступом із застосуванням вбудованої буферної пам’яті на кожній із проблемних ділянок. Дані системи характеризуються високим рівнем безпеки та надійності.

СКУД прийнято встановлювати на об’єктах різних масштабів, а їх широке поширення залежить від стрімкого розвитку технологій. Вибір і налаштування систем безпеки на кожному об’єкті носить індивідуальний характер, оскільки залежить від багатьох чинників, що зумовлює виробників СКУД до уніфікації застосованих у них технологій.

Таблиця 1.1 – Класифікація засобів контролю та управління доступом

<table>
<tr><th rowspan="2">За функціональним призначенням</th><th colspan="2" rowspan="2">За функціональними характеристиками</th><th colspan="2">Стійкість до несанкціонованого доступу (нормальна, підвищена, висока)</th></tr>
<tr><th>До руйнівного впливу</th><th>До неруйнівного впливу</th></tr>
<tr><td rowspan="4">Пристрої загороджувальні керуючі</td><td rowspan="4">За видом перекриття проходу</td><td>Із частковим перекриттям</td><td rowspan="2">—</td><td>Стійкість до відкриття</td></tr>
<tr><td>Із повним перекриттям</td><td rowspan="3">Стійкість до маніпулювання</td></tr>
<tr><td>Із суцільним перекриттям проходу</td><td>Стійкість до виламування, вибуху та кулестійкість</td></tr>
<tr><td>Із блокуванням об’єкту в проході</td><td>—</td></tr>
<tr><td rowspan="4">Виконавчі пристрої</td><td rowspan="4">За способом закриття</td><td>Електромеханічні замки</td><td rowspan="4">В залежності від конструкції</td><td>Стійкість до відкриття</td></tr>
<tr><td>Електромагнітні замки</td><td rowspan="3">Стійкість до маніпулювання</td></tr>
<tr><td>Електромагнітні засувки</td></tr>
<tr><td>Механізми приводу дверей/воріт</td></tr>
<tr><td rowspan="9">Зчитувальні пристрої</td><td rowspan="4">За способом зчитування</td><td>Із ручним введенням</td><td rowspan="9">—</td><td>Стійкість до нагляду (спостереження) для зчитувачів введення запам’ятованого коду</td></tr>
<tr><td>Контактні</td><td rowspan="5">Стійкість до маніпулювання</td></tr>
<tr><td>Безконтактні</td></tr>
<tr><td>Комбіновані</td></tr>
<tr><td rowspan="5">За видом застосованих ідентифікаційних ознак</td><td>Механічні</td></tr>
<tr><td>Магнітні</td></tr>
<tr><td>Оптичні</td></tr>
<tr><td>Електронні контактні</td></tr>
<tr><td rowspan="4">Ідентифікатори</td><td>Електронні радіочастотні</td><td rowspan="4">—</td><td rowspan="4">Стійкість до маніпулювання</td></tr>
<tr><td>Акустичні</td></tr>
<tr><td>Біометричні</td></tr>
<tr><td>Комбіновані</td></tr>
<tr><td rowspan="2">Засоби керування у складі апаратних пристроїв та програмних засобів</td><td colspan="2">Апаратні засоби</td><td>—</td><td>Стійкість засобів обчислювальної техніки від несанкціонованого доступу до інформації</td></tr>
<tr><td colspan="2">Програмні засоби</td><td>—</td><td>Стійкість до маніпулювання</td></tr>
</table>

Засоби контролю та управління доступом. Відповідно до діючих нормативних документів [26, 27], засоби контролю та управління доступом прийнято класифікувати за функціональним призначенням пристроїв і їх характеристиками та стійкістю до несанкціонованого доступу.

Класифікацію засобів КУД подано у таблиці 1.1.

Для забезпечення повноцінного функціонування та безперебійної роботи СКУД до складу цих систем прийнято включати різні набори додаткових засобів: джерела електричного живлення; пристрої для передачі даних різними каналами; перетворювачі інтерфейсів мереж зв'язку; комп'ютерне обладнання та програмне забезпечення; сповіщувачі; пристрої звукової та світлової сигналізації; доводчики та кнопки ручного управління загороджувальними пристроями тощо.

Варто зауважити, що нормативна база, яка встановлює вимоги, класифікацію, порядок та методи випробувань систем та засобів такого класу, представлена міжнародними стандартами ISO 9000, ГОСТ 26342-89, EN 50065, VDS, VDSG 29023, ГОСТ Р 51241-2008, BSI, UL, VDEO833.

В основу роботи будь-якої СКУД покладено принцип порівняння ідентифікаційних ознак [8], які належать чи притаманні конкретноій фізичній особі (суб'єкту доступу) або об'єкту (предмету, транспортному засобу), з інформацією, що зберігається у базах даних системи.

Незважаючи на те, що для кожної СКУД перелік засобів контролю та управління доступом буде різним, то у загальному випадку їх допустимо об'єднувати у єдину функціональну підсистему. На рисунку 1.12 подано структурну схему, яка відображає взаємодію основних елементів СКУД [11].

Зауважимо, що контрольовані об'єкти, які перебувають на території, що охороняється, та використовуються у якості пунктів пропуску суб'єктів доступу прийнято називати точками доступу, які зазвичай обладнують пристроями зчитування, виконавчими пристроями і керованими загороджувальними пристроями [23].

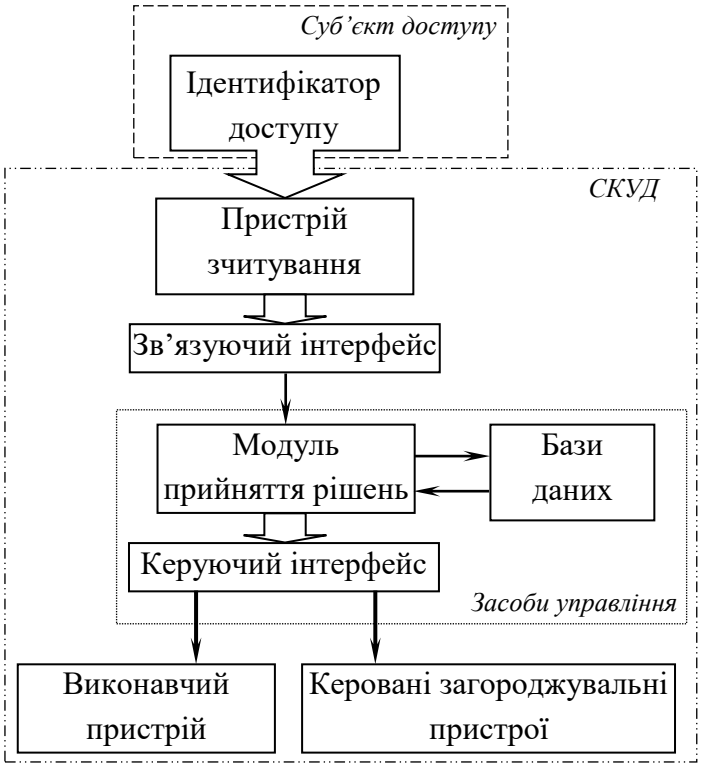


Рисунок 1.12 – Схема взаємодії елементів СКУД

Зауважимо, що контрольовані об'єкти, які перебувають на території, що охороняється, та використовуються у якості пунктів пропуску СД називають точками доступу та зазвичай обладнують пристроями зчитування, виконавчими пристроями і керованими загороджувальними пристроями.

Пристрої ідентифікації в СКУД. Пристрої ідентифікації призначені для зчитування і розкодування інформації, яка була записана на ідентифікаторі користувача, а також встановлює права суб'єктів доступу на переміщення в охоронній зоні (об'єкті) [56].

На практиці прийнято виділяти наступні принципи ідентифікації:

- ідентифікація за запам'ятовуючим кодом, який вводиться вручну за допомогою клавіатури, кодових перемикачів тощо;

- ідентифікація за речовим кодом, який записано на фізичному носії (ідентифікаторі), в якості якого застосовують різні ключі, карти тощо;

- біометрична ідентифікація, яка ґрунтується на визначенні індивідуальних фізичних ознак людини.

На пристрої зчитування, у загальному випадку, покладено такі функції:

- введення запам’ятованого коду / зчитування ідентифікаційної ознаки з ідентифікатора / зчитування біометричних характеристик;
- перетворення отриманої інформації на електричний сигнал;
- передача інформації до засобів управління (контролер СКУД).

Класифікація ідентифікаторів доступу за видом ідентифікаційних ознак наведена у таблиці 1.2.

Таблиця 1.2 – Класифікація ідентифікаторів доступу

Види ідентифікаційних ознак	**Елементи, які покладено в основу принципу роботи**	**Параметри ідентифікаторів**
Механічні	Елементи конструкції ідентифікаторів	Механічні ключі із перфорованими отворами
Магнітні	Намагнічені ділянки поверхні або магнітні елементи ідентифікатора	Картки із магнітною полосою або картки Віганта
Оптичні	Мітки, які нанесено на поверхню або розташовано у середині ідентифікатора, що володіють різноманітними оптичними характеристиками у відбитому або поглиненому оптичному випромінюванні	Картки із штриховим кодом або топографічні мітки
Електронні контактні	Електронний код, який записано в електронній мікросхемі ідентифікатора	Електронні ключі
Електронні радіочастотні	Радіоканал, який застосовується для передачі даних	Безконтактні картки доступу
Акустичні	Кодований акустичний сигнал	Пристрій генерування акустичних сигналів
Біометричні	Індивідуальні фізичні ознаки людини	Відбитки пальців, геометрія долоні, малюнок сітківки ока, голос, динаміка підпису
Комбіновані	Декілька ідентифікаційних ознак	Безконтактна картка доступу та відбитки пальців

1.5 Програмні методи доступу до баз даних СКУД

Концепція організації процесу управління доступом припускає відслідковування переміщення об’єктів допуску, а також надання їм прав на

допуск до конкретних об’єктів як за персональними ідентифікаторами, так і біометрії [47]. Відповідно постає питання зберігання інформації про СД, його біометричний зразок та параметри об’єктів доступу. Отримання даних підсистеми різними суб’єктами шляхом віддаленого доступу дозволяє використати клієнт-серверну архітектуру, як найбільш ефективну, а технологія реляційних баз даних є найбільш вдалою технологією організації зберігання інформації.

Таблиця 1.3 – Порівняльний аналіз систем управління базою даних

Параметр	**Система управління базою даних**			
	FireDird 2.5	MySQL 5.5.	MS SQL 2012	PostgreSQL 9.4
Обмеження на розмір БД	Можливості операційної системи	Можливості операційної системи	524 ПБ, Express – 10 ГБ	Можливості операційної системи
Робота з великою кількістю СД	Обмеження відсутнє	Обмеження відсутнє	Обмеження: 32767	Обмеження відсутнє
Операційна система	Кросплатформа	Кросплатформа	Unix, OS/2, Windows	Кросплатформа
Стандарт SQL	SQL-92 та частково SQL-99	SQL-99	SQL-2011	SQL-2011, SQL-99, SQL-92
Підтримка контролерів домена	Пакет програм Samba	Пакет програм Samba	Служба Active Directory	Пакет програм Samba
Наявність безкоштовного програмного забезпечення	+	Community Edition	Express	+

Критерії вибору системи управління базами даних визначаються, у першу чергу, предметною областю, а їх порівняльний аналіз, на предмет доцільності використання збережених даних суб’єктів доступу з метою їх ідентифікації, здійснюють відповідно до функціональних характеристик [46]:

- обмеження на розмір БД – встановлення проміжку часу, коли можливо надати швидкісний доступ до даних, які містять інформацію про пересування суб’єктів доступу без архівування;

- робота із великою кількістю СД – створення умов для проведення моніторингу на об’єктах із великою кількістю приміщень;

- легке інтегрування із інтерфейсом, який розроблено у RAD-середовищах;

- можливість використання різноманітних операційних систем з метою інтегрування із різноманітними пристроями;

- легкість встановлення та супровід СУБД;

- можливість використання контролера доменів – контроль над комп’ютерною мережею та взаємодією СД з доменом;

- підтримка стандартів SQL.

У таблиці 1.3 наведено порівняльний аналіз систем управління базами даних. Враховуючи необхідність оцінювання можливостей СУБД для вирішення задач управління доступом переміщення СД або їх порівняння за складним образом біометрії, виникає необхідність у технологіях та можливостях надання доступу до даних (таблиця 1.4).

Таблиця 1.4 – Технології та можливості доступу до даних

Засоби доступу до сервера	**Система управління базою даних**			
	FireDird 2.5	MySQL 5.5.	MS SQL 2012	PostgreSQL 9.4
Компоненти	C/C++, Delphi	API для Delphi, C, C++, Java, Perl, PHP, Python, Ruby	C/C++	C, C++, Java через модуль PL/Java
Класи	Для ADO, ODBC, JDBC (Jaibird)	API для Delphi, C, C++, Java, Perl, PHP, Python, Ruby	Для ADO, ODBC, JDBC	Підтримка для PL/Lua, PL/LOL, CODE, PL/Perl, PL/PHP, PL/Python, PL/Ruby
Драйвери	Для Python і PHP, OLE DB, dbExpress, провайдер .NET	ODBC, MyODBC	OLE DB	Підтримка для PL/Lua, PL/LOL, CODE, PL/Perl, PL/PHP, PL/Python, PL/Ruby

Приведений аналіз дозволяє зробити висновок, що використання усіх розглянутих СУБД є можливим для вирішення задач СКУД. Враховуючи це,

під час вибору СУБД не варто забувати про її інтегрування в автоматизовану систему управління доступом. Найбільш оптимальним варіантом є вибір на користь Microsoft-MSSQL Server, оскільки ця система володіє необхідною швидкодією та забезпечує достатньо легке інтегрування із клієнтським додатком за рахунок великої кількості бібліотек, що спрощує їх розроблення в RAD-середовищі.

Під час порівняння засобів розроблення та мови програмування на першому плані будуть знаходитись інструменти та бібліотеки, які, на основі спеціалізованих інструментів аналізу [15, 43], дозволять провести під'єднання до реляційної СУБД, працювати із графічним зображенням та порівняти зображення.

Варто зауважити, що поширені для розроблення web-додатків мови програмування не підходять для роботи із складними обчислювальними алгоритмами. У даному випадку рекомендованим є використання високорівневих мов програмування на кшталт Delphi, C# та Visual C++.

Таблиця 1.5 – Порівняльний аналіз мов програмування

Параметри	**Мови програмування**			
	Java SE9	Visual C++	Visual C# 4.0	Delphi 10 Lite v3.0
Наявність інструментів роботи СУБД	JDBC (Jaibird)	OLE DB, ODBC, MyODBC	OLE DB, ODBC, MyODBC	ADO
Середовище розробки	Visual Studio, Borland Enterprise Studio	Visual Studio	Visual Studio	Turbo Delphi, Borland Enterprise Studio
Наявність механізму роботи із математичним апаратом	MathGL, libfann, fannj, jna, JavaCV	Math.h, numeric.h, OpenCV	Math.h, numeric.h, OpenCV	Math, fann, OpenCV
Простота у використанні	Середня	Середня	Висока	Висока
Наявність безкоштовного програмного забезпечення	Express	Express	Express	Turbo Delphi Explorer

З метою проведення порівняльного аналізу мов програмування, які ставлять за мету вирішити поставлену задачу із розроблення СКУД вибирають наступні параметри (див. таблиця 1.5):

- можливість роботи із реляційною базою даних – база даних використовується для зберігання персональної інформації СД та відповідності біометричного ідентифікатора конкретному суб'єкту;
- необхідність використання сервера додатків – сервер додатків застосовується у тому випадку коли до наявної автоматизованої системи управління додають системи ідентифікації та доступу;
- наявність інструментів для розроблення ергономічного інтерфейсу;
- наявність бібліотек для підтримування математичного апарату, який використовується для порівнювання зображень;
- оцінка застосованих технологій та їх реалізація.

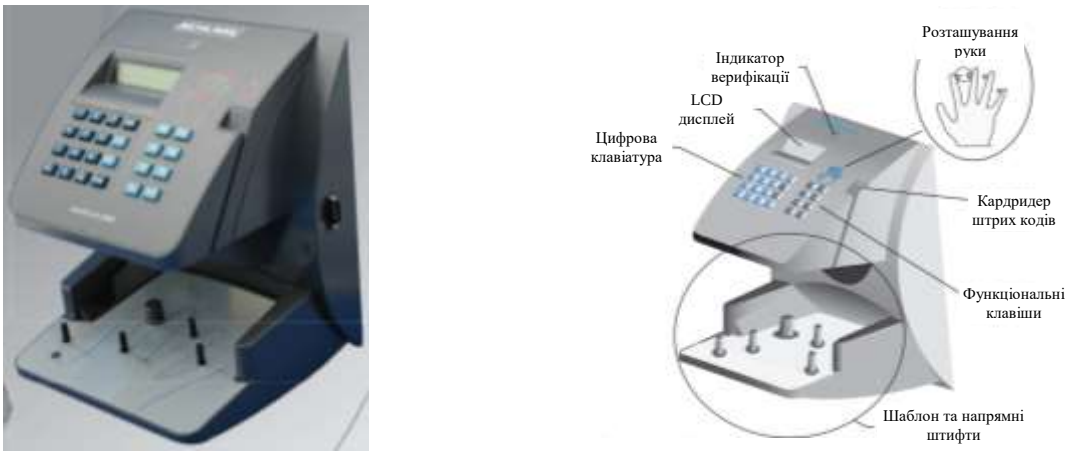
Наведена порівняльна характеристика дозволяє зробити висновок, що найбільш оптимальним, з точки зору вирішення поставленої задачі щодо організації СКУД, є RAD-середовище розробки MS Visual Studio []. Найбільш оптимальною мовою програмування є C# [].

1.6 Апаратні засоби для організації СКУД

Системи біометричного ідентифікування на ринку СКУД представлені широким спектром відповідного апаратного забезпечення. Враховуючи різноманітність методик, за якими здійснюється автентифікація суб'єкта доступу, доцільно виокремити ті, які орієнтовано на біометричний аналіз відбитка долоні (геометрії руки).

Сканер геометрії руки – це пристрій, який дозволяє обробити параметри геометрії руки та створювати її цифровий біометричний шаблон, який застосовують для подальшого встановлення особистості та її перевірки.

Типовий БС (рисунок 1.13) оснащено рідкокристалічним дисплеєм та клавіатурою, що дозволяє полегшити процес реєстрації та перевірки [6]. Для підтвердження особи СД повинен ввести свій особистий ідентифікаційний номер, після чого система розпізнавання готує образ-еталон до порівняння із зображенням відсканованої руки.



а) *б*)

Рисунок 1.13 – Біометрична система HandPunch3000 (HandPunch Guys LLC)

а) – вигляд загальний; *б*) – позначення функціональних вузлів

Для більшості таких систем притаманним є направляюче положення руки за допомогою штифтів (рисунок 1.14), з метою правильного розташування руки у шаблоні. Щодо інших особливих вимог (температура, вологість та чистота рук), то для пристроїв даного класу не висувають.

а) *б*)

Рисунок 1.14 – Розташування руки в шаблоні із напрямними штифтами

Зображення руки знімають за допомогою ПЗЗ-камери, яка розташована безпосередньо над шаблоном. Зчитувачі геометрії для отримання зображення руки, як правило, використовують інфрачервоне світло та відбивачі.

Процес реєстрації включає у себе багаторазове сканування (не більше трьох послідовних сканувань) руки суб'єкта, після чого система усереднює отримані дані для створення біометричного шаблону користувача. Система розпізнавання створює контурне зображення руки (здійснює не менше 90 вимірювань) із сканованого необробленого зображення за 31 тисячею точок. Обчислення та вимірювання здійснюють за допомогою базового алгоритму розпізнавання геометрії руки, та генерують біометричний шаблон суб'єкта.

Таблиця 1.6 – Порівняльний аналіз біометричних систем

Можливість	**Біометричні системи**			
	Digi-2 *BioMet Partners, Inc*	ID3D HandKey *Recognition Systems, Inc*	HandPunch3000 *HandPunch Guys LLC*	Hand Geometry System *Unicard Technologies Pvt Ltd*
Підтрмувані стандарти	ANCI, INCITS, NIST	ANCI, INCITS, NIST	ANCI, INCITS, NIST	ANCI, INCITS, NIST
Точність	FAR – 0,01 FRR – 0,01	FAR – 0,1 FRR – 0,1 (0,03)	FAR – 10^{-6} FRR – 10^{-2}	Малі помилки FAR і FRR
Сумісність із системами	Крос-платформа	Крос-платформа	Windows	Крос-платформа
Облік робочого часу	Пропускний контроль	Пропускний контроль	Пропускний контроль	Пропускний контроль
Віддалене управління	Автоматичне управління по GPRS	Автоматичне управління по GPRS	Автоматичне управління по GPRS	Автоматичне управління по GPRS
Сумісність із ідентифікаційними системами	Microsoft Dynamics, SAP R/3	Microsoft Dynamics, SAP R/3	Microsoft Dynamics, SAP R/3	Microsoft Dynamics, SAP R/3

У таблиці 1.6 наведено порівняльний аналіз біометричних систем, які здатні автентифікувати суб'єкт доступу за геометрією руки.

На сьогоднішній день, до складу біометричних сканерів геометрії руки (відбитка долоні) входять різноманітні давачі, які дозволяють підвищити ступінь їх захисту, а пройдений постійні вдосконалення зробили їх більш зручними та компактними.

1.7 Висновки до першого розділу

Питання першого розділу спрямовано на організаційно-методичні та програмно-технічні засоби, які дозволять вирішити задачі, які базуються на принципах контролю й управлінні доступом суб’єктів за їх біометричним аналізом відбитку долоні до контрольованих ними об’єктів.

Організація біометричного контролю дозволяє оперативно реагувати на поведінку суб’єктів доступу та підвищити рівень безпеки контрольної ділянки.

Огляд інформаційних джерел дозволяє зробити висновок, що під ідентифікацією суб’єкта доступу за геометрією кисті його руки прийнято розуміти ідентифікацію за формою долоні, оскільки в її основу покладено принцип розпізнавання біометричних ознак руки за геометрію її кисті.

Встановлено, що унікальними ідентифікаторами суб’єктів є їх біометричні характеристики, але питання їх надійного зберігання та захисту від неправомірного застосування, як і раніше залишається відкритим.

Розглянуто та наведено порівняльний аналіз найпоширеніших технологій автентифікації біометричних образів. Встановлено, що із статичних методів перевагу надають технологіям розпізнавання за відбитком пальця, а з динамічних – за рукописним почерком. Суттєвою відмінністю технології автентифікації за відбитком кисті руки, яка на практиці становить особливий інтерес, є малий об’єм електронного шаблону біометричного зразка.

На ринку програмного та апаратного забезпечення системи біометричної ідентифікації представлені достатньо широко. Не дивлячись на різноманіття існуючих методик переважна більшість систем орієнтована на статичні методи ідентифікування суб’єкта доступу. Враховуючи те, що спосіб автентифікації є досить відомим та широко застосовувався у минулому столітті, він не втратив практичного інтересу і сьогодні. Основною його перевагою залишається малий розмір математичного опису геометрії кисті руки (близько 9 байт).

2 ІДЕНТИФІКУВАННЯ СУБ'ЄКТА ЗА ВІДБИТКОМ ДОЛОНІ

2.1 Ідентифікування та реєстрації в СКУД

Формалізований опис завдання ідентифікування. Ідентифікаційна ознака являє собою властивість, значення якої здатне охарактеризувати суб'єкт доступу. Ідентифікатор – це унікальний набір параметрів ідентифікаційних ознак СД, що використовується для ідентифікації СКУД.

У якості ідентифікатора зазвичай застосовують [39]:

- значення імені користувача (логін);
- ідентифікаційний номер користувача у системі;
- номер документа встановленого зразка;
- обліковий номер картки-ідентифікатора чи іншого пристрою.

Процедура ідентифікації являє собою процес розпізнавання СД за індивідуальними його властивими або присвоєними ідентифікаційними ознаками. У ході цієї процедури відбувається порівняння ідентифікатора, наперед зареєстрованого у системі суб'єкта, який надається користувачем, із вмістом/наповненням бази даних СКУД.

Реєстрація СД ставить за мету створити у базі даних СКУД образу ідентифікатора, який, у подальшому, виступатиме еталоном під час його ідентифікації. Сама ж процедура автентифікації виступає перевіркою справжності ідентифікатора, який надається суб'єктом доступу.

Перевірку прийнято проводити шляхом взаємодії автентифікатора із застосуванням певного механізму автентифікації [48, 53]. У залежно від застосованого на практиці механізму, автентифікацію розрізняють:

- автентифікація на основі знання певної закритої інформації, якою володіє суб'єкт доступу – пароль;
- автентифікація на основі володіння деяким унікальним предметом – пристрої автентифікації;

- автентифікація на основі біометричних характеристик – унікальних фізіологічних ознак.

Процедуру проходження СКУД, яка побудовано на базі класичних електронних перепусток, можна розглядати як автентифікацію СД на основі володіння унікальної перепустки або ідентифікатора, а перевірку достовірності здійснює контролюючий персонал [10].

Розглянемо детальніше суть ідентифікації СД. Зробимо припущення, що у підсистемі ідентифікації та автентифікації зареєстровано деяку кількість суб'єктів доступу (n). При цьому в момент реєстрації i-го СД в базі даних СКУД створюється образ його ідентифікатора (p_i), який сформовано набором еталонних значень ідентифікаційних ознак. Враховуючи це, усі зареєстровані образи доцільно подавати у вигляді наступної множини $P=\{p_1, p_2, \ldots, p_n\}$.

Припустимо, що ПІА дозволяє розпізнавати ідентифікаційні ознаки СД (k). Множина $Z=\{z_1, z_2, \ldots, z_k\}$ дозволяє включити до свого складу ті ознаки, за допомогою яких здійснюється процес ідентифікації у межах СКУД. При чому елементами множини Z виступають серія та номер пропуску, PIN-код тощо. У якості біометричної ідентифікації виступають різні способи розпізнавання СД за фізіологічними ознаками або її поведінкою.

У залежності від особливостей об'єкта множина елементів Z є індивідуальною та формується для кожної СКУД оремо. Образу p_i при n=i, …, 1 повинен відповідати набір діапазонів значень ідентифікаційних ознак z_j ($k=j, \ldots, 1$), які було отримано на етапі реєстрації i-го суб'єкта доступу. З метою ідентифікації СД системою такий набір варто подавати у вигляді вектору $D_i=(d_{i1}, d_{i2}, ..., d_{ik})$, що дозволить визначити діапазон, у який потрапляє значення відповідних ознак.

Кожен з елементів d_{ij} для j-ї ідентифікаційної ознаки i-го суб'єкта доступу формує собою наступний діапазон $[d_{ij\,min}, d_{ij\,max}]$. Враховуючи це набір усіх наявних діапазонів варто записувати у вигляді матриці D, яка матиме такий вигляд:

$$D = \begin{pmatrix} d_{11} & d_{12} & \dots & d_{1k} \\ d_{21} & d_{22} & \dots & d_{2k} \\ \dots & \dots & \dots & \dots \\ d_{n1} & d_{n2} & \dots & d_{nk} \end{pmatrix}. \qquad (2.1)$$

Вектор D_i, залежить від архітектури СКУД і типу підсистеми ідентифікації та автентифікації, та окрім діапазонів, здатний визначити конкретні еталонні значення ідентифікаційних ознак. На етапі ідентифікації СД надає свій ідентифікатор, а пристрій зчитування формує його образ, який і використовується для порівняння з образами, які зберігаються у базі даних СКУД. Якщо у цій БД уже існує образ, який повністю відповідає пред'явленому, то суб'єкт доступу вважається ідентифікованим.

Модель процесу ідентифікування в системах контролю та управління доступом. Встановлення дій, які необхідні для ідентифікування суб'єкта допуску в СКУД є основною метою моделювання [52]. Структура та принципи функціонування подібних комплексів дозволяють виокремити їх основні елементи (суб'єкт доступу; об'єкт доступу, ідентифікатор, база даних, пристрій зчитування, засоби управління, виконавчі пристрої, керовані загороджувальні пристрої), а структурний підхід, який застосовують для побудови моделі процесу ідентифікування дозволяє відобразити взаємодію всіх елементів досліджуваного процесу шляхом декомпозиції.

На рисунку 2.1 подано структурну схему процедури ідентифікування.

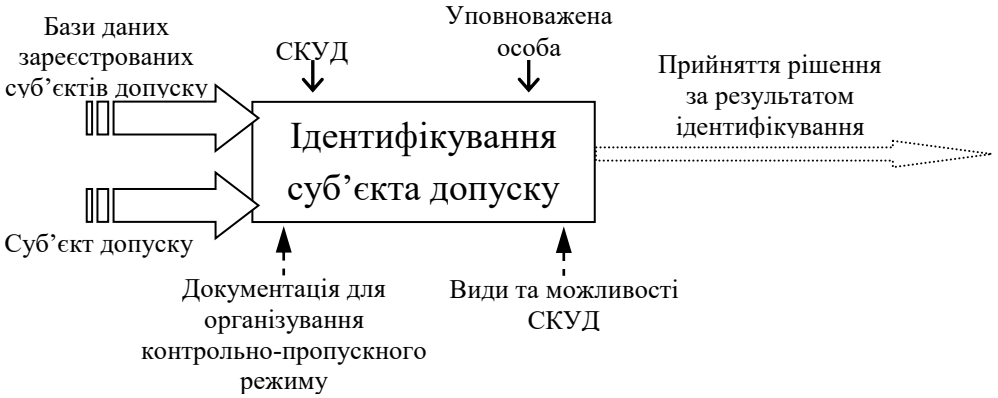


Рисунок 2.1 – Структурна схема процедури ідентифікування

Відповідно до структурної схеми процедури ідентифікування суб’єкта допуску, вхідними даними моделі виступають суб’єкт допуску та база даних зареєстрованих СД. У якості основних механізмів виступає СКУД та уповноважена особа (посадові обов’язки якого дозволяють забезпечувати контрольно-перепускний режим). За підсумками проведеної процедури ухвалюється рішення про ідентифікування суб’єкта допуску.

Аналіз предметної області дозволяє встановити послідовність етапів процесу ідентифікування (рисунок 2.2) [23]. Спершу здійснюється перевірка необхідності реєстрації суб’єкта доступу у системі. Наступний етап – пред’явлення пропуску/ідентифікатора користувача. Враховуючи вид (конфігурацію) СКУД та правил здійснення контрольно-перепускного режиму із наданого для зчитування ідентифікатора виділяється набір ідентифікаційних ознак, який проходить перевірку на наявність подібності із переліком образів *P*.

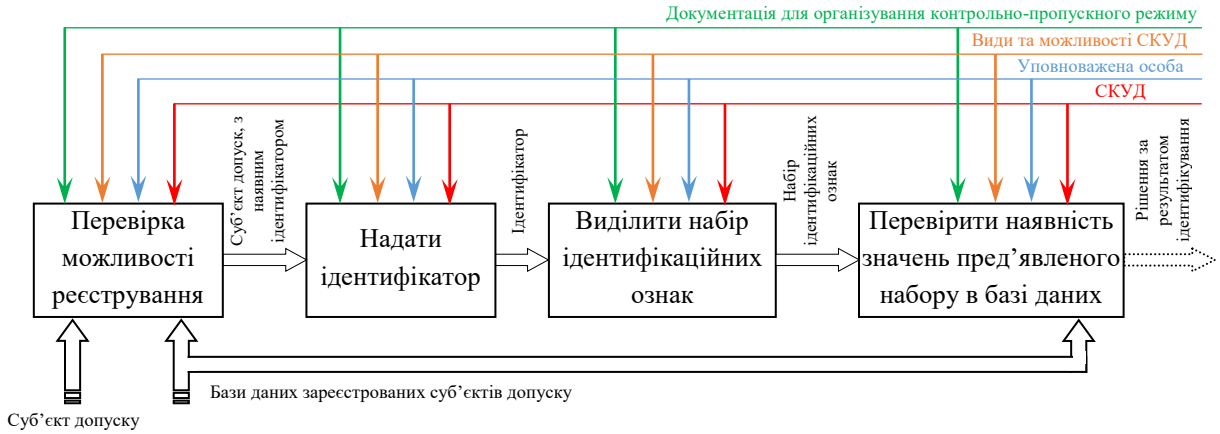


Рисунок 2.2 – Декомпонування процедури ідентифікування

База даних зареєстрованих суб’єктів доступу являє собою деяку множину *P*. Враховуючи, те що, для запропонованої моделі, даний параметр є частиною вхідних даних, то актуальним є питання його формування.

Як зазначалось раніше, образи ідентифікаторів p_i додаються до БД на етапі реєстрації користувача. Для проведення процедури ідентифікування

суб’єкт доступу має надати/пред’явити для зчитування образ p^*. При цьому p^* має бути представленим значенням як мінімум однією із трьох ідентифікаційних ознак $z_j \in Z$.

Пристрій зчитування являє собою засіб, який приймає та обробляє передані йому образи для ідентифікування або перетворення їх у зручний для засобу управління (контролер) формат. Інтерпретуючи роботу пристрою зчитування у вигляді математичного апарату отримаємо:

$$p_k^* = F(p^*), \tag{2.2}$$

де p_k^* – образ, який надається суб’єктом доступу і перетворюється на той формат, який використовується контролером; $F(p^*)$ – функція перетворення образу у формат, який використовується контролером.

Після перетворень пристрій зчитування передає контролеру значення p_k^*. Основним із інструментів, які дозволяють вирішити задачу ідентифікування є контролер.

Для вирішення даної задачі необхідно оперувати поняттям міри близькості між образами p_k^* та p_i ($p_i \in P$), i=1, 2, …, n):

$$Q(p_k^*, p_i). \tag{2.3}$$

Функцію визначення $Q(p_k^*, p_i)$ варто подати, як аналітичний виразу $\Phi(z^*, D_i)$, який дозволить розрахувати числову оцінку критерію порівняння двох образів, як оцінку близькості або розрізнення вектору визначених значень ідентифікаційних ознак z» та векторів діапазонів образу D_i.

Особливості застосованої системи ідентифікування безпосередньо впливають на вибір $\Phi(z^*, D_i)$ від якої буде залежати вибір метрик (відстань Хеммінга, коефіцієнта парної кореляції, ймовірнісні оцінки методу Байєса тощо) міри близькості. Під час аналізу переданого пристроєм зчитування образу p_k» контролер перевіряє наявність у базі даних відповідного образу p_i. У тому випадку, якщо порівнюваний образ існує (зазвичай в єдиному

екземплярі), то формується позитивний результат ідентифікування суб'єкта виявлення, в іншому випадку – СД ідентифіковано не буде.

Процедуру ідентифікування в СКУД прийнято подавати наступним чином [35]:

$$Q(p^*, p_i)=\Phi(z^*, D_i),\ i=1, 2, \ldots, n. \tag{2.4}$$

$$p^* = p_i : \Phi\left(z^*,\ D_i\right) \equiv \begin{cases} \min\left(\Phi\left(z^*,\ D_i\right)\right), & \text{якщо } \Phi - \text{метрика близкості;} \\ \max\left(\Phi\left(z^*,\ D_i\right)\right), & \text{якщо } \Phi - \text{метрика розрізнення,} \end{cases} \tag{2.5}$$

де $p_i \in P$, $D_i \in D$, $i=1, 2, \ldots, n$.

Вираз (2.5) описує правило, за яким віднесення p^* до конкретного образу p_i здійснюється за мажоритарною оцінкою значення функції $\Phi(z^*, D_i)$.

У тому випаду коли обрана метрика оцінювання значення $\Phi(z^*, D_i)$ перевищує чи не досягає певного заданого порога λ (обов'язковою умовою обмеження виступають вирази (2.6) і (2.7)) то ідентифікувати представлений образ у поточній системі неможливо.

$$p_i \notin P : \Phi(z^*, D_i) \leq \lambda,\ p_i \in P,\ D_i \in D,\ i=1, 2, \ldots, n. \tag{2.6}$$

$$p_i \notin P : \Phi(z^*, D_i) > \lambda,\ p_i \in P,\ D_i \in D,\ i=1, 2, \ldots, n. \tag{2.7}$$

Умову (2.5) прийнято застосовувати коли застосовують метрики близькості, а вираз (2.6) – для метрик розрізнення.

У випадку успішної ідентифікації суб'єкта допуску та відсутності додаткових вимог до виконання процедури автентифікації відбувається передача управляючого впливу на виконуючий пристрій або керований загороджувальний пристрій. В іншому випадку, коли політикою безпеки об'єкта та підсистемою ідентифікування та автентифікації передбачено процедуру обов'язкової автентифікації, то тоді необхідно провести додаткову перевірки, під час якої слід перевірити справжність наданого ідентифікатора.

На рисунку 2.3 подано схему процесу ідентифікування в СКУД.

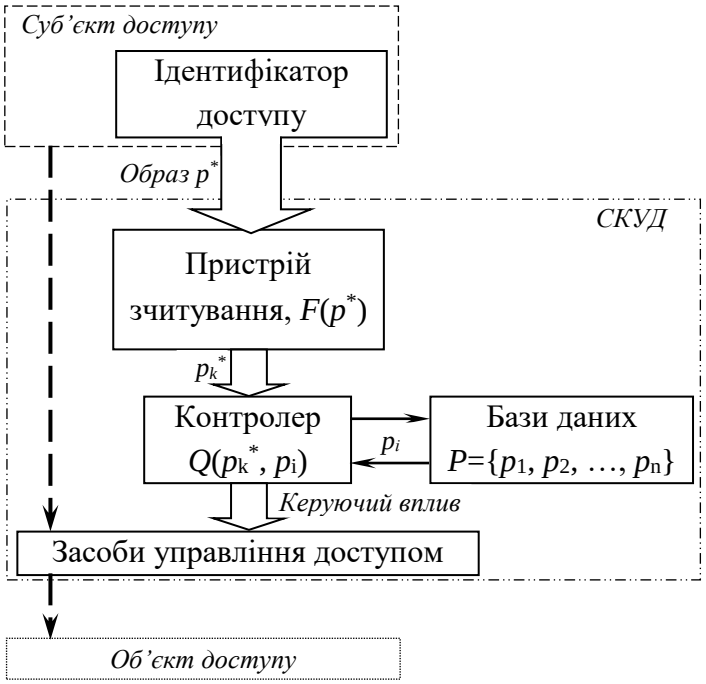


Рисунок 2.3 – Схема процесу ідентифікування в СКУД

Реєстрація користувача ПІА є невід'ємною частиною процесу ідентифікування, а вихідними даними для цієї процедури виступають як суб'єкт доступу, так і база даних зареєстрованих суб'єктів доступу. СКУД та її оператор виступають у якості основних механізмів [22].

Оператор, обравши параметри за якими може ідентифікувати СД, оформляє заявку на реєстрацію. Отримавши відомості, які підтверджують особу відвідувача, оператор верифікує його та отримує значення ідентифікаційних ознак. Отримані значення перевіряють на достовірність та записують до бази даних СКУД, після чого генерують ідентифікатор доступу. Завершальним етапом є видача суб'єкту доступу унікального ідентифікатора (RFID-мітки, електронна картка тощо). За умови використання біометричних систем ідентифікації останній крок відсутній.

2.2 Задачі детектування та розпізнавання

З метою виділення у суб'єкта доступу біометричних ознак необхідно отримати якісну сегментацію зображення його руки.

Існуючі алгоритми [34], враховуючи сучасні вимоги до застосування мобільних технічних засобів середнього цінового діапазону, не дозволяють забезпечити високу якість сегментації під час роботи у реальному часі [58]. Окрім того, у самій БС необхідно зберігати базу біометричних зразків СД. При цьому БД має забезпечувати достатній рівень безпеки, а також доступ до бази усіх суб'єктів доступу. Вирішення цієї проблеми полягає у наявності центрального сервера, у якості якого може виступити персональний комп'ютер або спеціалізоване забезпечення.

Розподіл завдання ідентифікування СД за відбитком долоні на детектування і розпізнавання дозволяє врахувати обмежені обчислювальні можливості мобільних технічних засобів. З метою зменшення навантаження на МТЗ розпізнавання біометричної ознаки СД прийнято проводити на ПК.

Основним завданням детектування залишається виявлення на зображенні БО (долоні) та його перевірка для наступного розпізнавання.

Алгоритм детектування дозволяє пропускати до подальшого оброблення тільки придатні зображення, тобто має низьке значення FAR (сегментування дозволяє серверу краще обробляти зображення у реальному часі). Невелике значення параметра FRR дозволяє забезпечити оптимальний час розпізнавання за умови дотримання СД розпізнаваних процедур.

2.3 Методика детектування

Перед процедурою детектування долоні СД варто задатись рядом обмежень, які дозволять сформувати конкретне її зображення [1, 42]. Для того, щоб отримати коректне зображення долоні необхідно щоб:

- долоня разом із зап'ястям знаходилась у зоні формування відбитка;
- сторонні предмети не обмежували видимість долоні (браслети, годинники, довгі рукави тощо);
- були розставленні/розведені усі пальці.

Наступним етапом є формування алгоритму детектування, для якого варто виокремити такі етапи [57]:

1. сегментування – виявлення у зоні формування відбитка об’єкта-кандидата, який виступатиме у ролі долоні;

2. формування скелетового подання долоні, побудова семантичної розмітки та перевірка долоні на коректність її зображення;

3. визначення розфокусованих відбитків (кадрів);

4. формування даних (валідна долоня) для відправлення їх у модуль розпізнавання.

Отже, коректне зображення долоні є необхідною, але не достатньою, умовою її валідності (тільки валідні відбитки долоней розпізнають далі).

Варто пам’ятати, що алгоритм детектування зазвичай працює з відбитками/кадрами у режимі реального часу (продуктивність оброблення одного відбитка/кадру 20 … 40 мс). Враховуючи те, що абсолютна більшість методів сегментування (глибокі нейронні мереж, мінімальних розрізів на графах тощо) не вкладаються у такі часові обмеження.

Враховуючи те, що порогова бінаризації зображення за методом Оцу [37] дає змогу отримати оптимальне поєднання якості сегментування із швидкодією, то це дозволить швидко виділити необхідну ділянку, яка ймовірно буде відноситись до долоні, а потім перевірити її умови її коректного зображення.

Сегментування. На практиці відомою є велика кількість алгоритмів сегментування зображень. Бінарне сегментування цифрового зображення, як правило дозволяє отримати тільки два (переважно білий та чорний) можливі значення для кожного із пікселів, які позначають міткою «об’єкт» і «фон». З поміж наявних методів бінарного сегментування [18], для вирішення даного питання, варто звернути увагу на такі їх групи:

- порогова бінаризація за яскравістю – пікселі поділяють на дві групи та залежать від яскравості тієї або іншої ознаки;

- віднімання фону – зображення або послідовність зображень складається із нерухомого фону та рухомого об’єкту;

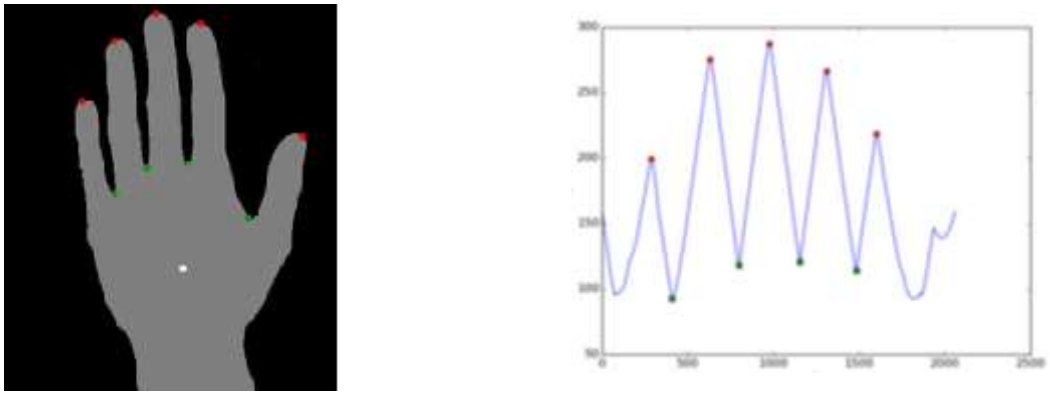
- кластеризація за кольором – пікселі, на основі свого кольору, формують групи;

- мінімізування енергії – розбивання пікселів на групи відбувається шляхом оптимізування певної функції енергії, яка задана на графі, що будується за відбитком (зображенням);

- нейронні мережі – зображення подається на вхід нейронної мережі, яка визначає приналежність кожного пікселя до своєї ознаки.

Формування геометричної інформації про долоню. Після того, як операцію із сегментування долоні виконана (виділено множину пікселів, які їй відповідають), необхідно визначити, чи виділена область є долонею [9].

Для роботи алгоритму, який дозволить встановити коректність зображення долоні необхідно отримати додаткову інформацію про її геометрію. На практиці (рисунок 2.4, *а*) увага акцентується на основі (зелені точки) пальців, їх кінцях (червоні точки) та максимальним вписаним у долоню коло (біла точка).



а) *б*)

Рисунок 2.4 – Формування геометричної інформації про долоню

Одним із найбільш розповсюджених способів є функція відстані, яка базується на формуванні геометричної інформації про долоню за відстанню

між особливою точкою на долоні (центроїд, точка на зап’ясті тощо) та визначеною на точках контуру [16, 21].

Графік такої функції подано на рисунку 2.4, *б*. На графіці по осі X відкладено номер точки на контурі долоні, а по осі Y – відстань від даної точки до центру долоні.

Цей спосіб дозволяє якісно відшуковувати точки кінців пальців та точки між пальцями. Однак він не дає змоги відрізнити коректне зображення долоні від некоректного, оскільки інформації, яка міститься у функції відстані є недостатньо. Більше того, такий метод не здатний відрізнити долоню від будь-якого іншого об’єкта, який володіє необхідним числом виступів та западин. У тому випаду коли сегментування є неідеальним, то такий алгоритм також працює неідеально та формує помилковий результат.

Враховуючи даний недолік, на практиці застосовують такий спосіб, який дає можливість отримання геометричної інформації із форми долоні на основі циркулярних графів (безперервних скелетів) [54].

Скелетом замкнутої фігури називають множину центрів максимально вписаних у неї кіл. Максимальним вписаним колом фігури вважають таке коло, яке не вписано у жодне інше вписане коло цієї фігури.

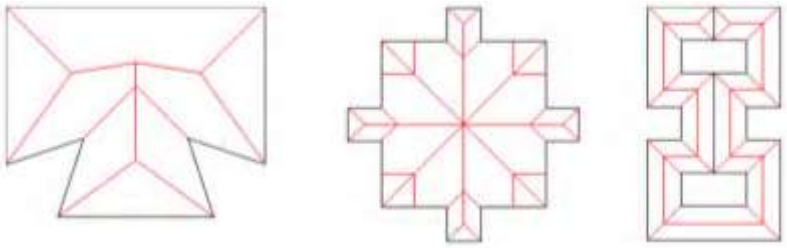


Рисунок 2.5 – Приклад скелетування різних фігур

Скелетна уява про фігуру (рисунок 2.5) відображає її топологічну структуру та не залежить від її деформацій. Побудова скелета здійснюється наступним чином: з бінарного зображення долоні (див. рисунок 2.6, *б*) виокремлюють контур, який приймають за замкнутий багатокутник. На

основі отриманого багатокутника будується діаграма Вороного [28], після чого вибирається підмножина ребер його діаграми, яка і формує скелет (рисунок 2.6, *в*). Цей метод, порівняно просто, за допомогою виділення гілок скелета, які відповідають пальцям долоні, дозволяє провести перевірку долоні на коректність її зображення.

а) *б*) *в*)

Рисунок 2.6 – Етапи процедури детектування

а) – вихідний відбиток руки; *б*) – бінаризація за Оцу; *в*) – контур долоні та її скелет

а) *б*) *в*)

Рисунок 2.7 – Регуляризація (стрижка) побудованого скелета

а) – вихідний відбиток руки; *б*) – скелет руки без стрижки; *в*) – скелет руки зі стрижкою

Рисунок 2.8 – Силует руки із максимальною кількістю вписаних у нього кіл

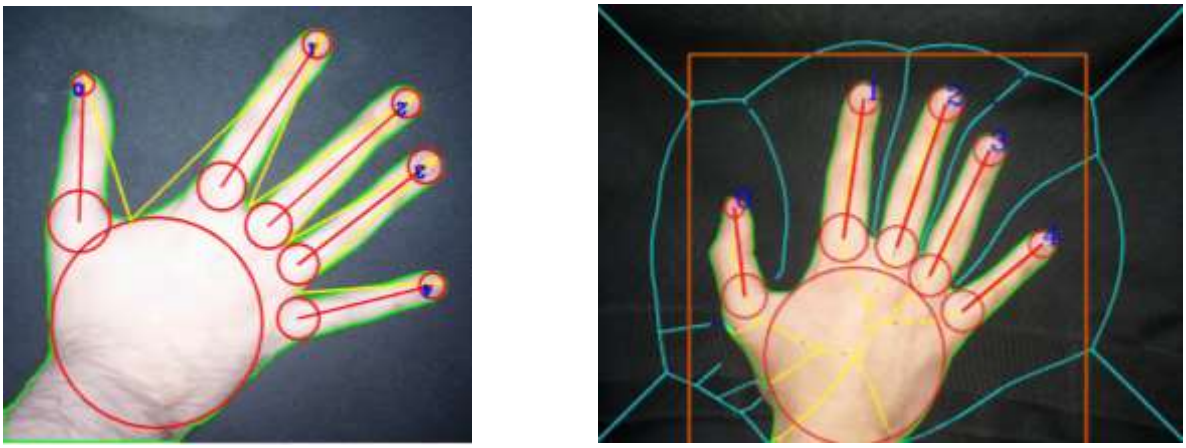
Враховуючи те, що невеликі зміни контуру можуть призвести до суттєвих змін у скелеті фігури, то вводять регуляризацію або стрижку побудованого скелета (див. рисунок 2.7). Силует скелета являє собою об’єднання усіх максимальних вписаних кіл із центрами у точках скелета (див. рисунок 2.8). Силует скелета без регуляризації повністю співпадає із вихідною багатокутною фігурою. Якщо при цьому задано параметр ε, то процес стрижки можна описати так: послідовне видалення вершин скелета 1-го ступеня до тих пір, поки відстань між контуром отриманого скелета та вихідною фігурою за метрикою Хаусдорфа не буде перевищувати ε.

Семантична розмітка долоні. Подальший аналізу даного методу вимагає визначити положення пальців за скелетом долоні (рисунок 2.9, *а*). Дана процедура складається має наступну послідовність:

- виділення гілок-кандидатів у пальці;
- перевірка радіальної функції, яка дає змогу відсіяти гілки-кандидати, які анатомічно не відповідають пальцям через свою товщину;
- виділення основи та кінців пальців;
- базова порогова перевірка відстаней, яка дає змогу відсіяти гілки-кандидати, які анатомічно не можуть бути пальцями через свою довжину, розташування основи та кінців пальців;
- виключення побічних гілок-кандидатів, які відповідають одному пальцю;
- перевірка трійок, які відсіюють гілки, що не лежать у ділянці пальців (гілки з ділянки зап’ястя);
- визначення великого пальця із кандидатів, які залишилися;
- медіанна перевірка, яка дозволяє відсіяти зображення із близько зведеними пальцями;
- пошук вершин зовнішнього скелета між пальцями.

У тому випадку, коли сформоване на відбитку зображення долоні суб’єкта доступу на одному із кроків не проходить перевірку або

залишається менше п’яти гілок-кандидатів у пальці, то процедуру розмітки достроково завершують, а зображення долоні вважається некоректним.



а) *б*)

Рисунок 2.9 – Скелетизоване зображення рук

а) – виділення пальців на скелетизованій долоні; б) – семантична розмітка долоні

У тому випадку коли зображення долоні є коректним, то алгоритмом формується обмежуючий прямокутник, що дозволяє включити долоню і пальці (див. рисунок 2.9, *б*). Дана процедура дозволяє зменшити обчислювальну складність наступного аналізу, так як процедура розпізнавання буде оперувати тільки з областю, яка розташовується всередині прямокутника.

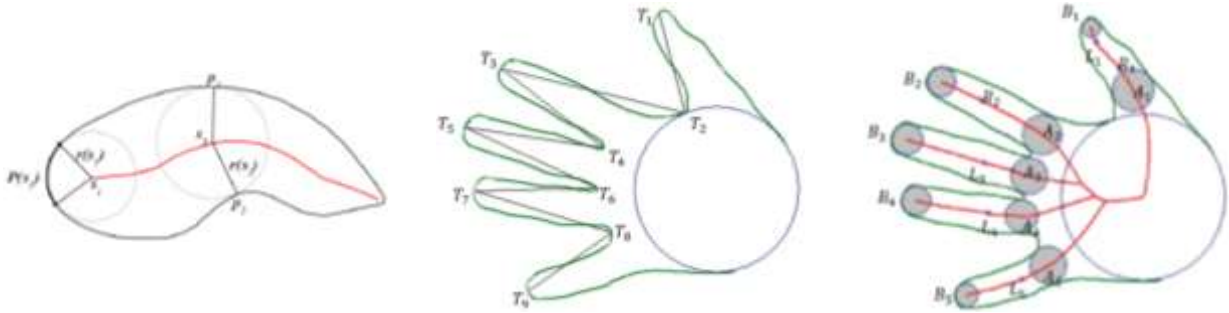
2.4 Методика розпізнавання

Після того, як долоню детектовано, дані про неї передаються у модуль розпізнавання де і розпочинається генерування ознакового опису.

Сегментування. Для точного та якісного сегментування долоні зазвичай застосовують алгоритм мінімізації енергії на основі теорії графів [24, 54]. Такі алгоритми володіють високою обчислювальною складністю, яка, у свою чергу, залежить від розміру зображення відбитка. Отримане бінарне

зображення надходить до модуля отримання ознак форми та застосовуються під час виділення й формування біологічних ознак.

Генерування ознак форми. На виході з алгоритму сегментування за допомогою графів отримують точну маску долоні із гладким контуром, що дозволяє з високою точністю відшукати ті ознаки, які відносяться форми кисті руки [21]. Актуальним залишається завдання підбору таких ознак, – вони мають будуть стійкими та репрезентативними для подальшого використання їх під час класифікації суб'єкта доступу із зображенням долоні.



а) *б*) *в*)

Рисунок 2.10 – Графічна інтерпретація ознак на основі форми

а) – розподіл медіальної ширини; *б*) – ломана; *в*) – кривизна пальців

Генерація ознак форми відбувається за бінарним зображенням (маскою долоні) коли будується скелет долоні та здійснюється семантична розмітка долоні. Після цього визначають наступні ознаки (рисунок 2.10):

- розподіл медіальної ширини (спектр);
- ламану, яка послідовно з'єднує вершини пальців та точки між ними (нормалізовані довжини ланок);
- кривизну пальців (максимальна відстань між точками скелета та віссю пальця по-обидва боки).

Метрика порівняння нормалізованих зображень. Нехай $A1$ та $A2$ – дискретні спектри, P та Z – кількість елементів у них, $K=\min\{P, Z\}$. Найпростішою метрикою є сума поелементних різновидів [24]:

$$d_L = \sum_{i=1}^{K} \left| A1_{(i)} - A2_{(i)} \right|. \quad (2.8)$$

Основною перевагою цієї метрики є простота її інтерпретації. Тобто, чим меншим є значення, тим більша схожість.

Наступна метрика – сума перетинання гістограм:

$$d_{\text{int}} = \sum_{i=1}^{K} \min\left\{ A1_{(i)},\ A2_{(i)} \right\}. \quad (2.9)$$

У тому випадку коли гістограми $A1$ та $A2$ нормовані за одиницею, то значення метрики «1» свідчити про відповідність, а «0» – не відповідність.

Наступною є метрика χ-квадрат (метод порівняння Пірсона):

$$d_{\chi^2} = \sum_{\substack{i=1 \\ A1_{(i)} + A1_{(i)} \neq 0}}^{K} \frac{\left(A1_{(i)} - A2_{(i)} \right)^2}{A1_{(i)} + A2_{(i)}}. \quad (2.10)$$

У даному випадку, чим меншим є значення, тим більшим є схожість («0» відповідає за ідеальне співставлення, а максимальне значення є необмеженим).

Ще однією метрикою виступає відстань Бахаттачарія:

$$d_B = \sqrt{1 - \sum_{i=1}^{K} \frac{\sqrt{A1_{(i)} A2_{(i)}}}{\sum_j A1_{(j)} \sum_j A2_{(j)}}}. \quad (2.11)$$

У ній чим меншим є значення тим більшим є співставлення («0» – свідчить про повне співпадіння, а «0» – не співпадіння).

Важливим класом метрик є EMD-метрики. Дані метрики відображають мінімальні затрати на перетворення однієї гістограми на іншу. Наприклад маємо базову метрику $d_{\text{E}}(i, j)$, $i \in \{1, \ldots, P\}$, $j \in \{1, \ldots, Z\}$. Значення i-го елемента гістограми $A1$ дорівнює $a1_{\text{i}}$, аналогічно значення j-го елемента гістограми $A2$ дорівнює $a1_{\text{j}}$. Тоді EMD-метрика визначаються наступним чином:

$$EMD\left(A1_{(i)},\ A2_{(i)}\right)=\min_{a_{ij}}\sum_{i=1,\dots,P}\sum_{j=1,\dots,Z}a_{ij}d_E(i,\ j),$$

$$\sum_{i=1,\dots,P}a1_i=1,\quad \sum_{j=1,\dots,Z}a2_j=1,\quad \sum_{i=1,\dots,P}\sum_{j=1,\dots,Z}a_{ij}=1, \tag{2.12}$$

$$\forall i,\ j:\ a_{ij}\ge 0,\quad a1_i=\sum_{j=1,\dots,Z}a_{ij},\ a2_j=\sum_{i=1,\dots,P}a_{ij}.$$

У загальному випадку визначення такої відстані зводиться до вирішення задачі лінійного програмування. Однак, коли гістограми дискретні, одномірні та нормовані за одиницею (2.12), то розрахунки максимально спрощуються. Якщо у якості базової метрики вибрати L_1-метрику, то її відстань EMD_{L1} буде рівною:

$$EMD\left(A1_{(i)},\ A2_{(i)}\right)=\int_{-\infty}^{+\infty}\left|F(x)-G(x)\right|dx, \tag{2.13}$$

де $F(x)$ та $G(x)$ – функції розподілу для $A1(x_\mathrm{i})$ та $A2(y_\mathrm{i})$ відповідно:

$$F(x)=\int_{-\infty}^{+\infty}A1(t)dt,\quad G(x)=\int_{-\infty}^{+\infty}A2(t)dt. \tag{2.14}$$

Вираз (2.14) свідчить про те, що таким чином можна отримати лінійну відстань по відношенню до розміру гістограм часу.

2.5 Висновки до другого розділу

Подано формальний опис завдання ідентифікування суб’єкта та модель даного процесу для СКУД. Моделювання основних процесів СКУД дозволяє говорити про те, що інформація, яка зберігається у базах даних є вхідними даними для процедури ідентифікації.

Розглянуті у другому розділі питання дають підстави стверджувати, що біометричну ідентифікацію суб’єкта доступу за відбитком долоні доцільно розглядати у межах методології машинного навчання.

У зв’язку із обмеженими обчислювальними можливостями мобільних технічних засобів та забезпечення безпеки сформованих біометричних ознак задачу ідентифікації варто розділяти на детектування та розпізнавання.

Узагальнено метод детектування, який складається із сегментування долоні, побудови її скелету, сементичної розмітки та перевірки долоні на коректність, формування даних для їх відправлення в модуль розпізнавання.

Запропоновано методику розпізнавання долоні, яка дозволяє встановити ознаковий опис та порівняння його із наявними у базі зразками.

3 ОБЧИСЛЮВАЛЬНИЙ ЕКСПЕРИМЕНТ

Описаний вище алгоритм ідентифікування суб’єкта доступу доцільно тестувати на предмет точності його роботи [49]. Поряд з тим, необхідно звернути увагу на те, як точність алгоритму ідентифікації реагує на зміну умов освітлення/фону. Враховуючи те, що біометричні відбитки долоні суб’єкта доступу у базі даних згруповано за серіями (відбитки знімаються за однакових умов освітлення/фону), то використовують спеціальний метод оцінювання точності ідентифікування, який враховує згрупованість фотографій за серіями. Для різних способів виділення біометричних ознак з відбитка долоні тестування проводиться оремо.

Таблиця 3.1 – Приклад тестової вибірки відбитку долоні суб’єкта доступу

№ суб’єкта доступу	**Номер серії**	**Кількість зображень**	**№ суб’єкта доступу**	**Номер серії**	**Кількість зображень**
1	1 із 3	21	7	1 із 1	13
1	2 із 3	15	8	1 із 1	9
1	3 із 3	15	9	1 із 1	8
2	1 із 1	13	10	1 із 1	12
3	1 із 1	5	11	1 із 1	11
4	1 із 1	13	12	1 із 3	22
5	1 із 1	13	12	2 із 3	29
6	1 із 1	13	12	3 із 3	36
		Всього:	**12**	**16**	**248**

3.1 Тестова вибірка

Для тестування алгоритму ідентифікації необхідно зібрати вибірку зображень відбитків рук декількох суб’єктів доступу. Вважаємо, що наша вибірка складається із відбитків 12 долонь різних СД, при цьому, такі знімки

зроблено за однакових умов освітлення/фону та згруповано за серіями. Для кожного із СД кількість серій відбитків долоні різна.

У таблиці 3.1 наведено загальну кількість відбитків долонь у кожній серії для кожного із ідентифікованих суб'єктів доступу.

3.2 Метод оцінювання точності алгоритму

Для забезпечення точності оцінювання ефективної роботи наведеного алгоритму біометричної ідентифікації до сформованої бази даних відбитків рук повинні входити зображення долонь одних і тих же суб'єктів доступу, які було зроблено за різних умов. З метою перевірки правильної роботи запропонованого алгоритму формування образу кисті руки необхідно здійснювати для різних кутів повороту долоні по відношенню до засобу фіксації відбитка (камери), освітлення або фону (тла) [44]. Приклади зображення рук одного і того ж суб'єкта доступу, які зроблено за різних умов освітлення, подано на рисунках 3.1 та 3.2.

а) *б*)

Рисунок 3.1 – Приклад відбитку руки суб'єкта доступу №1

а) – серія 1; *б*) – серія 2

а) *б*)

Рисунок 3.2 – Приклад відбитку руки суб'єкта доступу №12

а) – серія 1; *б*) – серія 2

Як бачимо, до бази даних заносять зображення відбитків кисті рук суб'єктів доступу у різних серіях, які володіють суттєвими відмінностями у освітленні та фоні. Тестування алгоритму ідентифікування на зображеннях відбитків рук різних серій дозволяє оцінити ступінь його стійкості до зміни фону та освітлення. Для тестування якості роботи алгоритму на зображеннях відбитків різних серій прийнято використовувати наведений на рисунку 3.3 алгоритм [49].

Вихідні параметри: $p : B \times B \to \boldsymbol{R}$ – міра співпадіння; B – множина зображень відбитків; $s(I)$ – функція зображення відбитка I, яка повертає усі зображення із тієї ж серії, що й I; $u(I)$ – функція зображення відбитка I, яка повертає усі зображення, які належать тому ж суб'єкту доступу, що й I.

Результат: d_{ss} – внутрішньосерійна відстань; d_{sp} – міжсерійна відстань; d_d – відстань між різними суб'єктами доступу.

Цикл $\boldsymbol{I} \in \boldsymbol{B}$ виконувати:

$T_1 \leftarrow s(I) \backslash \{I\}$; // зображення відбитка того ж СД у тій же серії

$T_2 \leftarrow u(I) \backslash s(I)$; // зображення відбитка того ж СД в іншій серії

$T_3 \leftarrow B \backslash u(I)$; // зображення відбитка інших СД

$d_{ss}(I) \leftarrow \min_{\bar{I} \in T_1} p(I, \bar{I})$;

$d_{sp}(I) \leftarrow \min_{\bar{I} \in T_2} p(I, \bar{I})$;

$d_d(I) \leftarrow \min_{\bar{I} \in T_3} p(I, \bar{I})/$

Кінець циклу.

Рисунок 3.3 – Алгоритм оцінювання точності ідентифікування

Вхідними даними цього алгоритму є база зображень відбитків рук та метрика подібності рук між собою. Отже, задаючись такими параметрами, як множина користувачів системи доступу (P), множина зображень відбитків рук суб'єктів доступу (B), загальна кількість зображень відбитків у базі (n), множина усіх підмножин множини зображень відбитків рук (2^B) та

отримавши функції $s: B \to 2^B$ і $u: B \to 2^B$ можна встановити розподіл внутрішньосерійних, міжсерійних та міжсуб'єтних відстаней. Застосовуючи визначені таким чином розподіли, дозволяє вибрати найбільш вдалий поріг класифікації та оцінити ймовірність помилки (похибки) під час ідентифікування СД.

Для оцінювання достовірності класифікації зображення відбитка руки I за умови міжсерійної перевірки необхідно порівнювати між собою значення $d_{sp}(I)$ і $d_d(I)$, а достовірність класифікації зображення відбитка при внутрішньосерійних перевірках, слід порівнювати між собою значення $d_{ss}(I)$ та $d_d(I)$. Зображення I, для міжсерійної перевірки, буде класифікуватись вірно тоді, коли $d_{sp}(I)<d_d(I)$, відповідно для внутрішньосерійної перевірки необхідно дотриматись умови ці, у випадках, коли $d_{ss}(I)<d_d(I)$.

З метою подальшого оцінювання точності ідентифікування суб'єкта доступу за зображенням відбитка його долоні необхідно визначити математичні параметри наступних функції:

- відсоток зображень, у – яких відстань до найближчого зображення руки іншого СД менша за τ:

$$FMR(\tau) = \frac{\left|\left\{I \in B \middle| d_d(I) < \tau\right\}\right|}{|B|}; \qquad (3.1)$$

- відсоток зображень, у яких відстань до найближчого зображення руки того ж СД більша за τ:

$$FNMR_{sp}(\tau) = \frac{\left|\left\{I \in B \middle| d_{sp}(I) > \tau\right\}\right|}{|B|} \quad - \text{ для міжсерійних порівнянь}; \qquad (3.2)$$

$$FNMR_{ss} = \frac{\left|\left\{I \in B \middle| d_{ss}(I) > \tau\right\}\right|}{|B|} \quad - \text{ для внутрішньосерійних порівнянь}. \qquad (3.3)$$

3.3 Ідентифікування шляхом простого порівняння із зразком

Розглянемо простий алгоритм ідентифікування суб'єкта доступу, який ґрунтується на прямому порівнянні зображень відбитків долоні із еталоном у метриці Евкліда без виділення текстурних ознак [40].

Нехай $A=(A^1, \ldots, A^k)$ та $B=(B^1, \ldots, B^k)$ – набори нормалізованих зображень пальців (мізинець, безіменний, середній і вказівний) першої та другої руки відповідно. При цьому, кожне із нормалізованих зображень пальців руки є матрицею розміру $M \times N$ пікселів (для кольорових зображень слід передбачити 3 канали яскравості пікселя). Тоді відстань між двома долонями, обчислюючи Евклідову відстань на відповідних парах пальців, буде визначатись за виразом:

$$M(A,\ B) = \frac{1}{4}\sum_{k=1}^{4}\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(A_{i,\ j}^{k} - B_{i,\ j}^{k}\right)}, \tag{3.4}$$

де A та B – нормалізовані напівтонові зображення пальці долоні (вектори із чотирьох матриць розміром $M \times N$).

Слід пам'ятати, що нормалізовані зображення відбитків долоней можна порівнювати як кольорові, так і напівтонові зображення. За умови порівняння кольорових зображень доцільно порівнювати відповідні канали яскравості:

$$M(A,\ B) = \frac{1}{4}\sum_{k=1}^{4}\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}\left[\begin{array}{c}\left(r\left(A_{i,\ j}^{k}\right) - r\left(B_{i,\ j}^{k}\right)\right)^2 + \left(g\left(A_{i,\ j}^{k}\right) - g\left(B_{i,\ j}^{k}\right)\right)^2 + \\ + \left(b\left(A_{i,\ j}^{k}\right) - b\left(B_{i,\ j}^{k}\right)\right)^2\end{array}\right]}, \tag{3.5}$$

де r, g і b – функції, які формують червоний, зелений та синій канали яскравості зображення відповідно; A та B – нормалізовані кольорові зображення пальців долоні.

Практичний інтерес являють такі випадки:

- коли між собою порівнюють нормалізовані кольорові зображення;
- коли між собою порівнюють нормалізовані напівтонові зображення.

Для кожного випадку будують гістограми:

- у першому – гістограму Евклідових відстаней між руками одного і того ж суб’єкту доступу;
- у другому – гістограму Евклідових відстаней між руками різних СД.

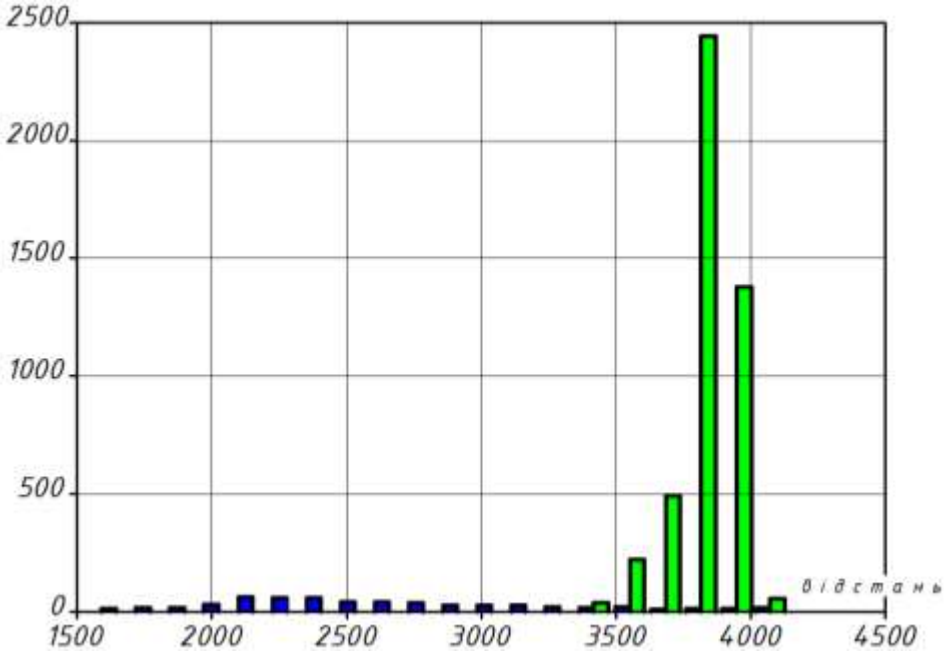


Рисунок 3.2 – Розподіл відстані між кольоровими відбитками зображень

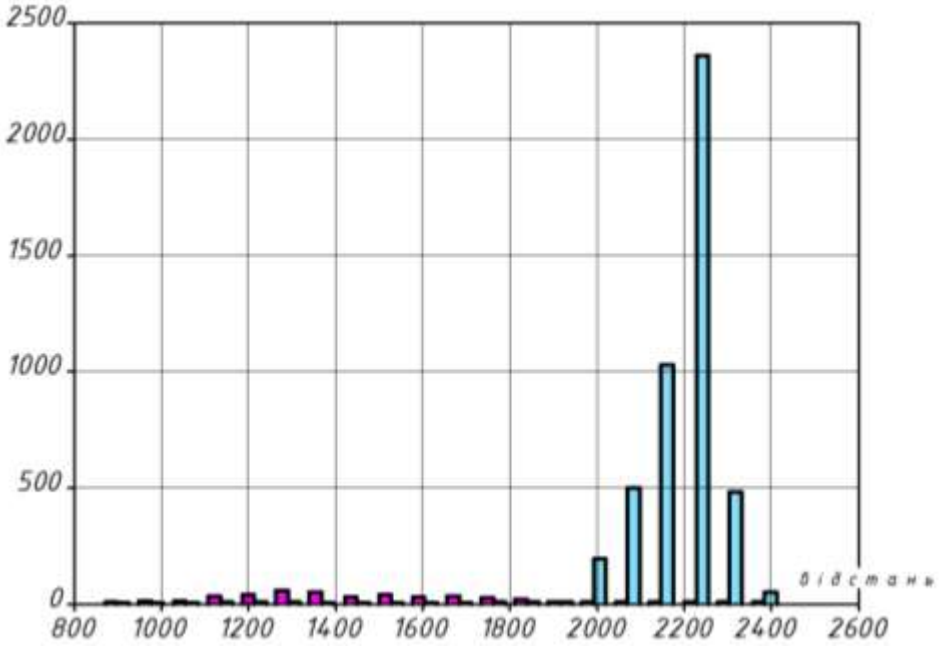


Рисунок 3.3 – Розподіл відстані між напівтоновими відбитками зображень

Гістограму розподілу відстаней між кольоровими нормалізованими зображеннями в метриці Евкліда подано на рисунку 3.2, а для напівтонових – на рисунку 3.3. Аналіз графіків дозволяє зробити висновок, що відстані між руками одного і того ж суб'єкту доступу значно менші, у порівнянні із відстанями відбитків долоней рук різних СД. А недоліком залишається той фат, що ці методи порівняння відбитків зображень є нестійкими до умов освітлення.

3.4 Ідентифікування за генеруванням ознак

Застосовуючи для тестової вибірки метод ідентифікування, який засновано на використанні фільтрів Габора досягають бінарного зображення. У тому випадку коли зображення пальців руки подано в бінарному виді, відстань між ними визначається за метрикою Геммінга [20]:

$$M(A,\ B)=\frac{1}{4}\sum_{k=1}^{4}\sum_{i=1}^{M}\sum_{j=1}^{N}\left|A^{k}_{i,\ j}-B^{k}_{i,\ j}\right|, \tag{3.6}$$

де A і B – нормалізовані та бінарні зображення пальців руки.

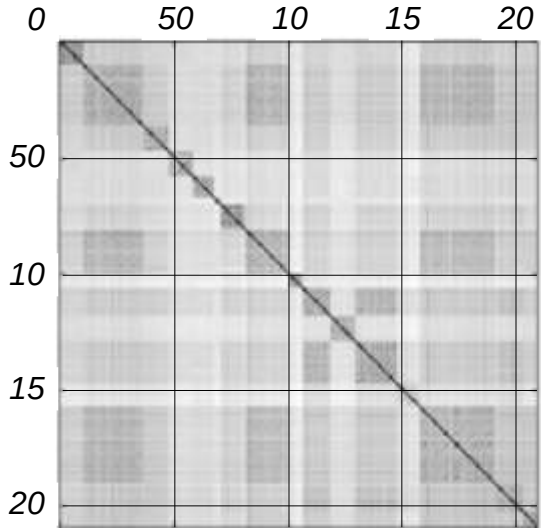
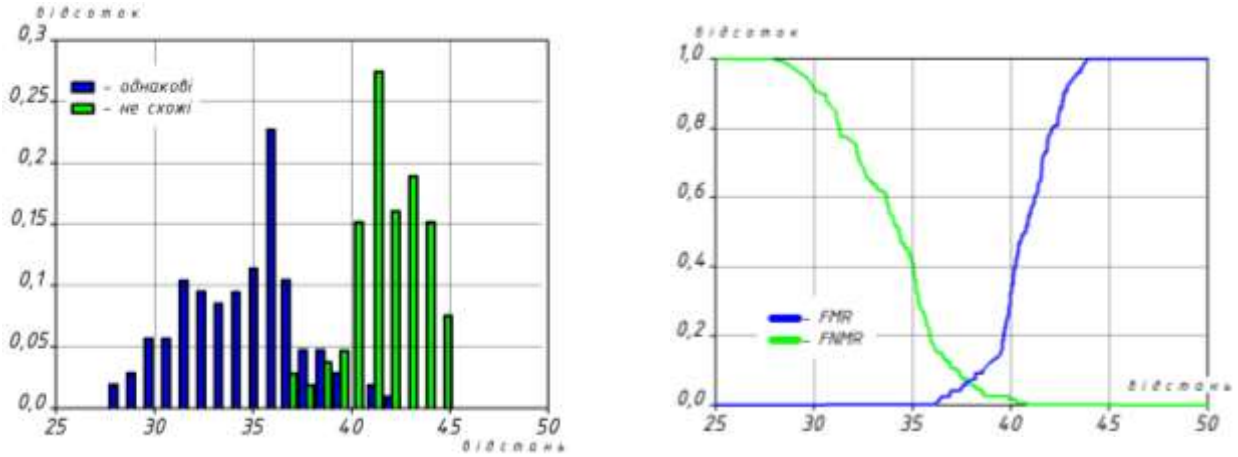


Рисунок 3.4 – Матриця відстаней між зображенням у метриці Геммінга

На рисунку 3.4 наведено матрицю відстаней у метриці Геммінга між усіма парами зображень у вибірці. На даному рисунку меншому значенню метрики присвоєно темніший колір відповідної комірки. Великі блоки темних пікселів на матриці відстаней відповідають зображенням долонь одного СД. Наявність таких блоків свідчить про те, що відстані між відбитками зображень долонь тих самих суб'єктів доступу є значно меншими у порівнянні з відстанями між різними СД.



а) *б*)

Рисунок 3.5 – Розподіл відстаней під час внутрішньосерійних порівнянь

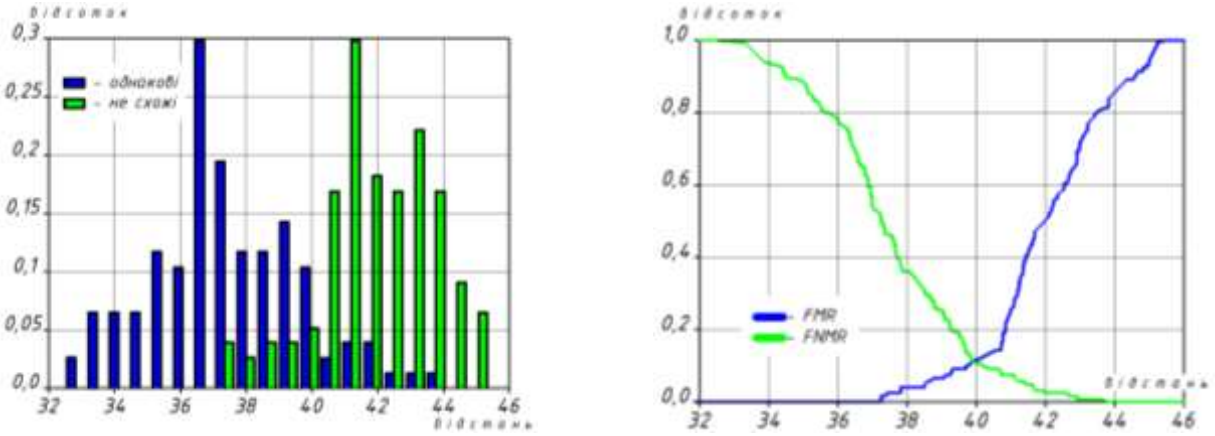
а) – нормалізована гістограма; *б*) – параметри функцій для різних рівнів τ

Внутрішньосерійні порівняння. Достовірність роботи алгоритму ідентифікування оцінюють шляхом визначення внутрішньосерійних відстаней між зображеннями рук суб'єктів доступу, який описано в п. 3.2 даної роботи. Під час внутрішньосерійних порівнянь акцентують уваглі лише на розподілі значень наступних функцій:

- $d_{ss}(I)$ – найкоротша відстань від зображення I до зображень одног і того ж СД тій же серії;

- $d_d(I)$ - найкоротша відстань від зображення I до зображення відбитка руки іншого СД.

На рисунку 3.5, *а* подано нормалізовану гістограму розподілу відстаней, а на 3.5, *б* – значення функцій FMR(τ) і FNMR(τ) для різних рівнів порогових значень τ (значення EER не перевищує 7,5%).



а) *б*)

Рисунок 3.6 – Розподіл відстаней під час міжсерійних порівнянь

а) – нормалізована гістограма; *б*) – параметри функцій для різних рівнів τ

Міжсерійні порівняння. Як і у попередньому випадку, достовірність роботи алгоритму ідентифікування прийнято оцінювати шляхом визначення міжсерійних відстаней між зображеннями рук СД, який описано в п. 3.2. Під час таких порівнянь звертають увагу на розподіл значень наступних функцій:

- $d_{sp}(I)$ – найкоротша відстань від зображення I до зображень того ж самого СД в інший серії;

- $d_{d}(I)$ – найкоротша відстань від зображення I до зображення іншого суб’єкта доступу.

На рисунку 3.6, *а* подано нормалізовану гістограму розподілу відстаней, а на 3.7, *б* – значення функцій FMR(τ) і FNMR(τ) для різних рівнів порогових значень τ (EER – 11%).

Підвищення точності алгоритму ідентифікування можливо досягнути лише шляхом додаткового врахування геометричних ознак долоні (довжина та кривизна пальців, геометрія долоні руки у поєднанні із формою складок шкіри на зовнішній стороні пальців тощо).

3.5 Висновки до третього розділу

У третьому розділі кваліфікаційної роботи застосовано спеціальний метод оцінювання точності ідентифікування, який дозволив врахувати згрупованість біометричних зображень відбитків долоні суб’єкта доступу за серіями.

Запропоновано алгоритм оцінювання точності ідентифікування суб’єкта доступу на основі формування бази зображень відбитків рук та метрика подібності рук між собою. Оцінювання точності ідентифікування суб’єкта доступу за його нормалізованими зображеннями відбитків долонь здійснювалось на основі математичних функцій (метрика Евкліда та метриа Геммінга).

Тестування якості роботи запропонованого алгоритму ідентифікування на зображеннях відбитків долонь різних серій дозволило оцінити ступінь його стійкості до зміни фону та освітлення.

Достовірність ідентифікування суб’єкта доступу за допомогою запропонованого алгоритму біометричного аналізу відбита долоні вказує на те що похибка для внутрішньосерійних порівнянь не перевищує 7,5%, а для міжсерійних – 11%. Підвищення точності алгоритму ідентифікування можливо лише за умови додаткового введення до біометричного ідентифікування суб’єкта доступу геометричних ознак долоні.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Небезпечні та шкідливі фактори під час виконання робіт із монтування СКУД

Тема кваліфікаційної роботи присвячена дослідженню програмних та апаратних засобів для побудови СКУД на основі біометричного аналізу відбитків долоні. Як було зазначено вище, до складу такої типової системи можуть входити елемент обмеження доступу (турнікет, двері тощо), біометричний термінал для зчитування відбитка долоні, контролер доступу, які потребують джерело електроживлення ~220 В [31].

Згідно існуючої класифікації небезпечних та шкідливих чинників за природою дії на людину [25] під час монтажних робіт СКУД присутні небезпечні фізичні чинники.

У нашому випадку небезпечним фізичним чинником є можливість враження електричним струмом напругою в ~220 В та отримання травм від піротехнічного монтажного інструмента [36].

Недотримання правил безпеки та необережне поводження із електротехнічним обладнанням призводить як до тяжких наслідків, так і летальних.

4.2 Заходи забезпечення сприятливих (безпечних) умов праці

Зовнішні елементи конструкції турнікетів, які в процесі роботи можуть опинитись під напругою, заземлюють.

Захисне заземлення може бути штучне або природне [59]. Природним заземленням можуть служити металеві трубопроводи або елементи залізних конструкцій, що входять глибоко в землю. В жодному випадку не можна використовувати нафтогазопроводи, труби опалення і відведення блискавки.

Забороняється також застосування алюмінієвих предметів. Якщо не має можливості використати існуючі мережі для заземлення, то створюють штучну систему. Для цього потрібні сталеві стержні або труби, а на кислих ґрунтах – мідні або оцинковані, які вертикально заглиблюють в землю. Глибина заглиблення залежить від типу матеріалу і його поперечного перерізу. Наприклад, у разі використання металевих стержнів діаметром 10 мм їх довжина повинна бути 10 м і більше, а для металевих труб діаметром 3 см і товщиною стінки 4 мм – понад 3 м.

Всі елементи заземлення з'єднують зварюванням. В місці контакту дротів заземлення з корпусом апарату допускається болтове з'єднання діаметром більше 5 мм.

Підключення турнікетів до загальної електромережі обов'язково здійснюється через кабель, що входить до комплекту монтажних частин, через індивідуальний щит, укомплектований пристроєм вмикання-вимикання і запобіжниками. Цей щит повинен забезпечити, в разі потреби, повне його знеструмлення. Щит встановлюють на такій відстані від пульта управління, щоб оператор елементарним рухом руки міг його вимкнути.

Забороняється:

- користуватись несправними електричними розетками та вилками;
- використовувати запобіжники завищених номіналів;
- експлуатувати турнікет зі знятими кожухами і кришками;

Перед початком роботи оператор повинен перевірити візуально стан проводів заземлення, цілісність блоку турнікету.

З появою запаху тліючої ізоляції роботу зупиняють до перевірки обладнання електромонтером.

При аварії персонал повинен, в першу чергу, відключити головний рубильник, а тоді діяти у залежності від ситуації:

- при виникненні пожежі викликати пожежну команду і повідомити керівництво установи; до прибуття пожежної команди пожежа ліквідовується первинними засобами гасіння;

- при інших аварійних ситуаціях (коротке замикання тощо) повідомити керівництво зміни (установи) і зупинити роботу.

По закінченню роботи оператор приводить в порядок робоче місце: встановлює в початкове положення ручки керування апаратом і вимикає рубильник, записує до контрольно-технічного журналу («повідомити техніку») всі неполадки, які помічені під час роботи.

4.3 Створення і функціонування системи моніторингу довкілля з метою інтеграції екологічних інформаційних систем

У наш час питання екології набувають першочергового значення. Сучасні технології дозволяють визначати екологічні проблеми ще стадії їх виникнення, тим самим полегшуючи антропогенне навантаження на довкілля [29]. У світовій практиці наявний значний досвід у галузі відстеження шкідливих впливів діяльності людини на довкілля.

Одним з основних методів відстеження впливу на навколишнє середовище та змін, що відбуваються в ньому, є його моніторинг. Основними складовими моніторингу є: точки спостереження, система індикаторів, датчики, блоки обробки та відображення інформації.

До основних об’єктів моніторингу довкілля належать:

- природні середовища;
- джерела антропогенного впливу, які призводять до зміни середовищ;
- природні ресурси.

Система моніторингу довкілля є багаторівневою інформаційною системою, яка відстежує всі цикли антропогенних впливів. Для комплексного підходу до визначення допустимих рівнів на організм, популяцію,

екосистему, біосферу загалом треба знати критичні показники і ланки, що характеризують стан екосистем. Велику увагу при цьому приділяють методам математичного моделювання, в основу якого закладається принцип багаторівневості.

Цей принцип екологічного моніторингу реалізується у двох напрямках. Перший передбачає поступовий перехід від простих датчиків до складних, де на першому рівні використовують прості датчики для реєстрації відхилення параметрів контролю від встановленої норми. На кожному наступному вищому рівні контролю кількість датчиків зменшується. Останній рівень містить певну невелику кількість універсальних високочутливих приладів.

Другий напрям пов’язаний з реалізацією багаторівневого моніторингу, що діє за принципом «космічного древа», і передбачає космічний, літаковий та наземний рівні спостережень.

Під час організації моніторингу довкілля враховують певні пріоритети. Так, стосовно територій вищий пріоритет віддають містам, зонам питної води та місцям нерестовищ риб; стосовно середовищ – атмосферному повітрі та воді прісноводних водойм тощо.

Основні труднощі в організації моніторингу довкілля пов’язані з вирішенням наступних завдань: створення мережі пунктів спостереження, оперативний контроль об’єктів, вибір контрольованих параметрів та показників для адекватного опису стану екосистеми.

Концепція комплексної системи моніторингу довкілля базується на оперативному екологічному контролі. Побудова такої системи потребує створення відповідної методології та апаратури оперативного стеження.

У світі створено регіональні моніторингові геоінформаційні системи, які збирають інформації про дійсні значення параметрів геосистем, обробку цієї інформації в імітаційних моделях екологічних та кліматичних процесів.

Розгляд існуючих можливостей для розвитку моніторингу довкілля в світі дає уяву про значні розробки в цій галузі. Проте практичне

використання різних комплексів і систем цьому історичному етапі розвитку України здійснюється вкрай повільно. Такій ситуації сприяє комплекс супутніх проблем, що охоплює широкий перелік питань – від бюрократичних до економічних.

4.4 Висновок до четвертого розділу

У четвертому розділі кваліфікаційної роботи сконцентровано увагу на небезпечних та шкідливі факторах, які виникають під час монтування СКУД.

Встановлено, що основним небезпечним фізичним чинником є ураження електричним струмом.

Передбачено захисне заземлення, для зовнішніх елементів конструкції СКУД, яке дозволить забезпечити безпечні умов праці та експлуатування системи.

Запропоновано застосувати системи моніторингу довкілля, яка дозволить зменшити вплив антропогенного навантаження на довкілля.

ВИСНОВКИ

В першому розділі кваліфікаційної роботи освітнього рівня «Магістр»:

– описано біометрична ідентифікація у системах доступу;

– висвітлено технології автентифікації суб’єкта доступу;

– розглянуто біометричні ознаки руки;

– проаналізовано методи ідентифікації відбитків долоні та принципи побудови СКУД за відбитком долоні.

В другому розділі кваліфікаційної роботи:

– проведено формалізований опис завдання ідентифікації;

– подано модель процесу ідентифікації відбитка долоні в СКУД;

– розкрито методики детектування та розпізнавання відбитку долоні суб’єкта.

В третьому розділі кваліфікаційної роботи:

– описано алгоритм оцінювання точності ідентифікації суб’єкта доступу на основі формування бази зображень відбитків рук та метрика подібності рук між собою,.

– подано результати тестування якості роботи запропонованого алгоритму та оцінка ступеня його стійкості до зміни фону та освітлення.

У розділі «Охорона праці та безпека в надзвичайних ситуаціях» проаналізовано небезпечні й шкідливі фактори під час виконання робіт із монтування СКУД. Запропоновано заходи із забезпечення сприятливих (безпечних) умов праці. Описано сутність створення і функціонування системи моніторингу довкілля з метою інтеграції екологічних інформаційних систем, що охоплюють певні території.

ПЕРЕЛІК ДЖЕРЕЛ

1. 3 самых важных метрики в Data Science. URL: https://itnan.ru/post.php?c=1&p=479390 (дата звернення: 21.11.2022).

2. Alyson J. K. Bailes. Terrorism and the International Security Agenda since 2001. *Combating Terrorism and Its Implications for the Security Sector*. – Sweden, 2005. P. 12–25. URL: https://dcaf.ch/sites/default/files/publications/documents/Combat_Terrorism_webb.pdf (дата звернення: 21.11.2022).

3. Biometrics. URL: https://translated.turbopages.org/proxy_u/en-ru.ru.78ff3eaa-6384a386-e495006c-74722d776562/https/www.dhs.gov/biometrics (дата звернення: 21.11.2022).

4. Daniel Martinkovic. Is Hand Geometry Identification Still Relevant? URL: https://www.m2sys.com/blog/guest-blog-posts/about-hand-geometry-identification/ (дата звернення: 21.11.2022).

5. Hand Geometry Recognition Biometrics: All You Need to Know. URL: https://www.bayometric.com/hand-geometry-recognition-biometrics/ (дата звернення: 21.11.2022).

6. HandPanch 3000. URL: https://www.handpunchguys.com/HandPunch-3000-Manual.pdf (дата звернення: 21.11.2022).

7. Oleh Kaidyk, Taras Terletskyi, Vitalii Ptashenchuk, Viktor Denysiuk. About Question of Organising of Physical Access Control System. *Priority Directions of Development of Science fnd Education* : materials of the III international research and practical internet conference. Zdar nad Sazavou. 24 December 2021. Zdar nad Sazavou : “DEL a.s.”. P. 56–58/

8. Peter Varchol, Dušan Levický. Using of Hand Geometry in Biometric Security Systems. URL: https://www.radioeng.cz/fulltexts/2007/07_04_082_087.pdf (дата звернення: 21.11.2022).

9. Stephen Mayhew. Explainer: Hand Geometry Recognition. URL: https://translated.turbopages.org/proxy_u/en-ru.ru.ec7c5b8b-6384a440-0461d537-

74722d776562/https/www.biometricupdate.com/201206/explainer-hand-geometry-recognition (дата звернення: 21.11.2022).

10. Алгоритмы прохода в СКУД. URL: http://sio.su/down_017_2_def.aspx (дата звернення: 21.11.2022).

11. Алгоритмы работы СКД. URL: http://www.glavsetstroy.ru/articles.php?id=337 (дата звернення: 21.11.2022).

12. Андреев В.О. Биометрические методы идентификации и аутентификации пользователя. URL: https://www.yaneuch.ru/cat_22/biometricheskie-metody-identifikacii-i-autentifikacii/215689.2096933.page1.html (дата звернення: 21.11.2022).

13. Антти Суомалайнен. Биометрическая защита: обзор технологии – Москва : ДМК Пресс, 2019. – 104с.

14. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам : учеб. пособие / А.А. Афанасьев и др. – Москва : Горячая линия – Телеком, 2012. – 550 с.

15. Биометрическая аутентификация в Windows. URL: https://www.kv.by/forum/biometricheskaya-autentifikatsiya-v-windows (дата звернення: 21.11.2022).

16. Биометрическая идентификация и аутентификация. URL: https://zarplatto.ru/biometrisheskaya-identifikatsiya-i-autentifikatsiya/ (дата звернення: 21.11.2022).

17. Биометрические технологии. URL: https://ru.wikipedia.org/wiki/Биометрические_технологии (дата звернення: 21.11.2022).

18. Бінарне зображення. URL: https://uk.wikipedia.org/wiki/Бінарне_зображення (дата звернення: 21.11.2022).

19. Біометрія. URL: https://uk.wikipedia.org/wiki/Біометрія (дата звернення: 21.11.2022).

20. Відстань Геммінга. URL: https://uk.wikipedia.org/wiki/Відстань_Геммінга (дата звернення: 21.11.2022).

21. Воложанин А.И. Технология распознавания по геометрии кисти руки. URL: https://bms.ucoz.ru/statii/tekhnologija_raspoznavanija_po_geometrii_kisti_ruk.pdf (дата звернення: 21.11.2022).

22. Ворона В.А., Тихонов В.А. Концептуальные основы создания и применения системы защиты объектов. – Москва : Горячая линия – Телеком, 2015. – 184 с.

23. Ворона В.А., Тихонов В.А. Системы контроля и управления доступом. – Москва : Горячая линия – Телеком, 2015. – 272 с.

24. Выбор метрики в машинном обучении. URL: http://blog.datalytica.ru/2018/05/blog-post.html (дата звернення: 21.11.2022).

25. ГОСТ 12.0.003-2015. Система стандартов безопасности труда. Опасные и вредные производственные факторы. Классификация. URL: https://dou.su/files/docs/GOST120003_2015.pdf (дата звернення: 21.11.2022).

26. ГОСТ Р 51241-2008. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний. URL: https://armo-training.ru/assets/files/gost/gost-r-51241.pdf (дата звернення: 21.11.2022).

27. ГОСТ Р 54412-2011. Информационные технологии. Биометрия. Обучающая программа по биометрии. URL: https://meganorm.ru/Data2/1/4293788/4293788152.pdf (дата звернення: 21.11.2022).

28. Діаграма Вороного. URL: https://uk.wikipedia.org/wiki/Діаграма_Вороного (дата звернення: 21.11.2022).

29. Екологічний моніторинг довкілля. URL: https://mepr.gov.ua/content/ekologichniy-monitoring-dovkillya.html (дата звернення: 21.11.2022).

30. Захаров В.П., Рудешко В.І. Біометричні технології в XXI столітті та їх використання правоохоронними органами : посібник. Львів : ЛьвДУВС, 2015. 492 с.

31. Инструкция по технике безопасности при монтаже, ТО и наладке слаботочных сетей. URL: https://vizart.pro/upload/files/instrukciya_po_tehnike.pdf (дата звернення: 21.11.2022).

32. Кайдик О.Л., Терлецький Т.В., Меус О.С. До питання біометричної автентифіації. *Інформаційні технології в освіті, техніці та промисловості* : зб. тез доп. учасн. Всеукр. наук.-практ. конф. молодих учених і студ. Івано-Франківськ, 13 жовт. 2022 р. Івано-Франківськ : ІФНТУНГ. С. 56–57.

33. Кайдик О.Л., Терлецький Т.В., Меус О.С., Садовий М.О, Бас Р.В. Про технологію та методи розпізнавання за геометрією кисті руки. *Приладобудування та метрологія: сучасні проблеми, тенденції розвитку* : зб. матеріалів доп. учасн. V Всеукр. наук.-практ. конф. Луцьк, 20-22 жовт. 2022 р. Луцьк : ЛНТУ. С. 37–39.

34. Классификация механизмов аутентификации пользователей и их обзор. URL: https://habr.com/ru/post/177551/ (дата звернення: 21.11.2022).

35. Кухарев Г.А. Биометрические системы. Методы и средства индентификации личности человека. – Санкт-Петербург : Политехника, 2001. 240 с.

36. Меры безопасности при монтаже приборов СКУД. URL: https://studbooks.net/2346492/tehnika/mery_bezopasnosti_montazhe_priborov_skud (дата звернення: 21.11.2022).

37. Метод Оцу. URL: https://uk.wikipedia.org/wiki/Метод_Оцу (дата звернення: 21.11.2022).

38. Методическое руководство по биометрии. URL: https://studfile.net/preview/10058920/ (дата звернення: 21.11.2022).

39. Методы идентификации, системы идентификации. Биометрические технологии. URL: https://www.idexpert.ru/technology/119/th1/ (дата звернення: 21.11.2022).

40. Метрика Евкліда. URL: https://ru.wikipedia.org/wiki/Евклидова_метрика (дата звернення: 21.11.2022).

41. Обзор биометрических методов идентификации. URL: https://monomah.org/archives/4602 (дата звернення: 21.11.2022).

42. Обзор метрик для использования в системе управления клиентским опытом. URL: https://vc.ru/u/1313487-apeks-berg/513470-obzor-metrik-dlya-ispolzovaniya-v-sisteme-upravleniya-klientskim-opytom (дата звернення: 21.11.2022).

43. Обзор СКУД с бесплатным программным обеспечением. URL: https://habr.com/ru/company/intems/blog/316728/ (дата звернення: 21.11.2022).

44. Оценка качества биометрических систем. URL: https://studfile.net/preview/5282722/page:14/ (дата звернення: 21.11.2022).

45. Понкратов А.Ю., Лобов Д.В., Осауленко Р.Н. Идентификация личности по рисунку внутренней стороны ладони посредством искусственной нейронной сети. URL: https://applied-research.ru/ru/article/view?id=12786 (дата звернення: 21.11.2022).

46. Программное обеспечение СКУД. URL: https://housechief.ru/skud-sistemy.html (дата звернення: 21.11.2022).

47. Программы ядра СКУД. URL: https://sevenseals.ru/upload/information_system_34/3/4/3/item_343/TSS0202_Ядро%20СКУД.pdf (дата звернення: 21.11.2022).

48. Прудник А.М., Власова Г.А., Рощупкин Я.В. Биометрические методы защиты информации : учеб.-метод. пособие. – Минск : БГУИР, 2014. – 123 с.

49. Серебряная Л.В. Методы и алгоритмы принятия решений : учеб.-метод. пособие. – Минск : БГУИР, 2016. 64.

50. Система контроля и управления доступом (СКУД). URL: http://fors.gtechs.ru/sites/all/forsdocs/gilyakova/SKUD120514.pdf (дата звернення: 21.11.2022).

51. СКУД – система контроля и управления доступом. URL: https://smarthomegadget.ru/skud-sistema-kontrolya-i-upravleniya-dostupom/ (дата звернення: 21.11.2022).

52. СКУД і забезпечення її надійності. URL: https://worldvision.com.ua/articles/skud-i-obespechenie-ee-nadezhnosti (дата звернення: 21.11.2022).

53. Способы идентификации личности по биометрическим параметрам. URL: https://studfile.net/preview/5282722/page:15/ (дата звернення: 21.11.2022).

54. Теорія графів. URL: https://uk.wikipedia.org/wiki/Теорія_графів (дата звернення: 21.11.2022).

55. Типовые алгоритмы доступа на примере одной двери. URL: http://secuteck.ru/articles2/sys_ogr_dost/tipovie-algoritmi-dostypa-na-primere-odnoi-dveri (дата звернення: 21.11.2022).

56. Требования к системе контроля и управления доступом. URL: https://naoxrane.ru/r78_36_018-2011_35.html (дата звернення: 21.11.2022).

57. Хабаров С. Интеллектуальные информационные системы. URL: http://www.habarov.spb.ru/new_es/exp_sys/ai_11.pdf (дата звернення: 21.11.2022).

58. Чабан Л.Н. Теория и алгоритмы распознавания образов : учебн. пособ. Москва : МИИГАиК. 2004. 70с.

59. Шудренко І.В. Основи охорони праці : навч. посіб. Житомир : О.О. Євенок, 2016. – 214 с.

ДОДАТКИ

Додаток А

Тези конференції

THE COMPANY "DEL a.s." (CZECH REPUBLIC)
NES NOVA DUBNICA sro (SLOVAK REPUBLIC)
UNIVERSITY OF MALAYSIA PAHANG (MALAYSIA)
UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO (MÉXICO)

PRIORITY DIRECTIONS OF DEVELOPMENT OF SCIENCE AND EDUCATION

MATERIALS
OF THE III INTERNATIONAL RESEARCH
AND PRACTICAL INTERNET CONFERENCE

December, 24, 2021

Zdar nad Sazavou, 2021

Пелипась Д.С.
Історичний аспект філософії олімпізму 39

ФІЛОЛОГІЯ І ЖУРНАЛІСТИКА

Mariia Zavorina
Cognitive Linguistics as Modern School of Linguistics 41
Ліана МАКАР, Анжеліка ШУЛЬЖЕНКО
Висвітлення в засобах масової інформації проблеми порушення прав жінок від домашнього насильства 44
Пасічник Ольга, Пирко Софія, Міщенко Т.М.
Особливості невербальної комунікації в професійній діяльності медичних працівників 47
Пономарь О.А.
Система жіночих образів у детективному романі Бориса Крамера «Зламані сходи» 49
Рула Н.В., Волканова Т.І.
Спростування як метод контрпропаганди в програмі «Антифейк» 52

ТЕХНІЧНІ НАУКИ

Osman Adiguzel
The Low-Cost Technology of Wastewater Treatment from Organic Dyes by Modified Natural Clay Minerals 55
Oleh Kaidyk, Taras Terletskyi, Vitalii Ptashenchuk, Viktor Denysiuk
About Question of Organising of Physical Access Control System 56
Гонгало Н.В., Яцкевич В.Ю.
Приклад розв'язання задачі мережевого планування 59
Зеленькевич А.И.
Обоснование критериев технико-экономической оптимизации конструктивных параметров силового трансформатора 62
Прищепов М.А., Зеленькевич А.И., Збродыга В.М.
Алгоритм технико-экономической оптимизации методом покоординатного поиска конструктивных параметров трансформатора со схемой соединения обмоток «звезда-двойной зигзаг с нулевым проводом» 65

ABOUT QUESTION OF ORGANISING OF PHYSICAL ACCESS CONTROL SYSTEM

Oleh Kaidyk
Ph.D., Associate Professor
Taras Terletskyi
Ph.D., Associate Professor
Vitalii Ptashenchuk
Ph.D., Associate Professor
Viktor Denysiuk
Ph.D., Associate Professor
(Lutsk National Technical University, Ukraine, Lutsk)

Traditional methods of personal identification, nowadays, have begun to lose their effectiveness, which is not the case with modern facility protection complexes, which are hard to imagine without physical access control systems (PACS). The use of such means allows, first of all, to solve the task based on the control and management of premises (prevention of unauthorised access), or to carry out operational control over the movement (residence time) of personnel in the controlled area.

Identification of the subject who is granted access to the protected premises/object is the initial PACS, and the extension of its technical capabilities enables automation of the identification process, however, for a number of cases the solution of the identity verification task is carried out with the involvement of human resources.

Formation of an integrated object protection system implies, first of all, development of its security concept, which will allow to prevent and reduce consequences from threats of different nature. The development of information technology and the emergence of new algorithms for pattern recognition and subject identification allow for the intelligence of this procedure. Modern physical access control systems make it possible not only to transfer as many functions as possible to accumulate and process information, but also to make appropriate decisions on security, information leakage and personnel performance control.

An analysis of the existing literature suggests that in addition to increasing the level of security in the protected area by preventing unauthorised access, PACS also enables a prompt response to the behaviour of staff and visitors in crowded places.

The main objectives of the PACS are as follows:

– to prevent unauthorised access in the controlled area where access restrictions are imposed;

– to enable unobstructed passage/traffic in an area with free access;

– organise monitoring and recording of staff/visitors access to the site;

– provide conditions for compliance with the intrinsic regime;

– integrate with other security systems.

PACS is first of all a complex of hardware and software compatible with each other by technical, informational, software and operational factors. The main components of such systems usually include the following groups of devices: readers;

means of detecting materials; devices for processing information; executive and auxiliary devices.

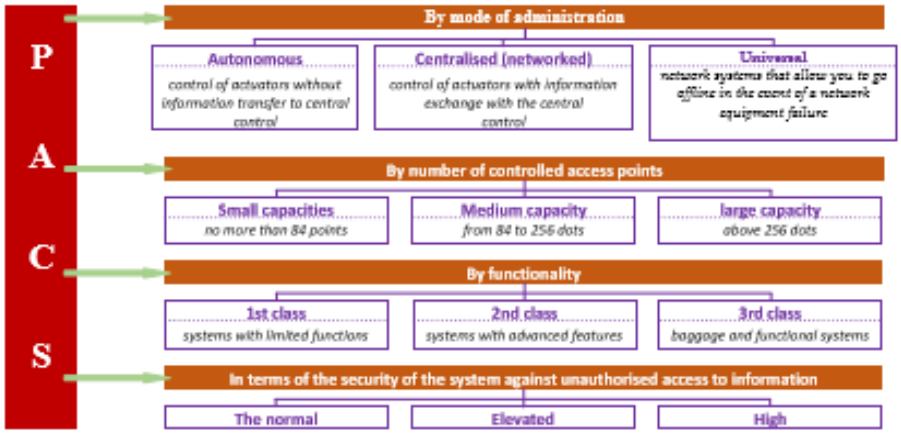


Fig. 1. Classification of physical access control systems

Physical access control systems are classified (fig. 1) into autonomous, centralized and universal according to the way of their operation and depending on the conditions of a particular object and the tasks to be solved.

Autonomous PACS are usually used at those objects where there is no necessity for permanent event monitoring and remote control of executive devices. As for centralized (networked) systems, they are used when it is necessary to control passage time/stay of an access subject and manage any PACS components from a central desk. Universal access control systems are network systems that can switch to autonomous operation mode in case of failure of PACS servers, network equipment or loss of communication with controller.

Universal PACS are based on centralised, distributed and mixed architecture.

The centralized architecture is based on the central controller that performs control process through specialized interface modules. The controller, in this case, is the storage of the whole database of identifiers and events that occurred in the system. In this case the separation of decision-making and direct control increases the level of PACS security, because the controller itself is installed, as a rule, at a considerable distance from the partition device controlling it. If the controller fails to communicate with the PACS server, the system continues to operate in stand-alone mode.

Systems based on a distributed architecture contain several controllers and the ID and event databases are separate from each other. This feature (location of controllers) does not help to reduce the probability of unauthorized access to the monitored objects, and the PACS itself is responsible for controlling external devices and security loops. This approach minimizes the disruption of communication between the controller and the interface module, i.e. the failure of one controller will not affect the operation of the other controllers, and if the communication line between controllers and PACS servers

is broken the system will continue to perform its basic functions – access process control in standalone mode.

Network physical access control systems based on mixed architecture with intelligent interface modules (specialized reader with its own memory buffer of identifiers and events) are the most popular. Such system is based on the centralized architecture, where in case of communication line failure between the central controller and the interface modules of end devices control, an autonomous mode of access control is activated with the use of built-in buffer memory at each of the problematic sites. Such systems are characterised by a high level of safety and reliability.

It should be noted that PACS integrates quite well with other security systems: video surveillance, security and fire alarm systems. For example, access control together with video surveillance provides absolute control over the secured premises. When PACS and intruder alarms are combined, it is possible to configure the overall response of the system to unauthorized intrusion in a particular room. Integration of PACS with fire alarm system allows automatic unblocking of doors, turnstiles and passageways in case of fire.

The study of physical access control systems capabilities, issues of their functioning, and analysis of technical solutions that are commonly used in identification tasks is relevant, as it will allow modeling, and then, organizing the process of complex security provision in a room or facility as a whole.

Додаток Б


МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Інститут модернізації змісту освіти
Івано-Франківський національний технічний
університет нафти і газу
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ
В ОСВІТІ, ТЕХНІЦІ
ТА ПРОМИСЛОВОСТІ
МАТЕРІАЛИ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ
Івано-Франківськ, 2022

М. В. Шавранський, М. Т. Яцура	Автоматизована система процесу буріння свердловин із складною траєкторією	37
В. С. Борин, Р. М. Лещій	Автоматизація технологічного процесу низькотемпературної сепарації газу	39
В. С. Борин, А. І. Димкар	Експериментально-аналітичне обґрунтування автоматизації керування температурно-вологісними режимами холодильного зберігання плодоовочевої продукції	41
М. І. Горбійчук, Н. Т. Лазорів, А. М. Лазорів	Автономна система автоматичного керування температурним режимом муфельної печі	42
В. С. Борин, М. М. Лазорів	Автоматизоване управління газоперекачувальним агрегатом на базі мікропроцесорної системи обробки технологічної інформації	45
М. І. Горбійчук, Н. Т. Лазорів	Емпіричні моделі муфельних печей	47
М. І. Когутяк, О. Р. Корчинський	Розроблення цифрових двійників об'єктів керування на PLC	49
В. М. Кулаківський, О. М. Давидов	Використання рекурсивної маршрутизації для резервування та балансування навантаження між каналами на прикладі локальної обчислювальної мережі ІНМ НАН України	51
В. Ю. Денисюк, Л. О. Гуменюк	Автоматизована система управління кліматичними випробуваннями гумотехнічних виробів	54
О. Л. Кайдик, Т. В. Терлецький, О. С. Меус	До питання біометричної автентифіації	56
В. О. Лось	Синтез нечіткого регулятора для системи автоматичного регулювання тиску в ректифікаційній колоні	58
А. О. Соломчак, М. Я. Николайчук	Вдосконалення алгоритмів керування статичними компенсаторами реактивної потужності (постановка задачі)	60
Т. В. Терлецький, О. Л. Кайдик	Особливості автоматизації проектування CCTV	61

УДК 004.3+004.93

ДО ПИТАННЯ БІОМЕТРИЧНОЇ АВТЕНТИФІАЦІЇ

О. Л. Кайдик, Т. В. Терлецький, О. С. Меус

Луцький національний технічний університет, м. Луцьк, Україна, o.kaidyk@lntu.edu.ua

На даний час біометрична ідентифікація людини є додатковим рівнем захисту, оскільки її біометричні дані складно підробити. При цьому біометричні дані окремовзятої особи залишаються незмінними та унікальними протягом усього її життя.

З-поміж основних переваг автентифікації за біометричними параметрами достатньо зупинитись на особистих даних, які неможливо забути, втратити, передати іншим особам або викрасти, відтворити у повному об'ємі [2].

Щодо самих методів біометричної автентифікації, то на практиці широко використовують як статистичні, так і динамічні характеристики особистості. Класифікацію біометричних методів за принципом їх дії подано на рисунку 1.

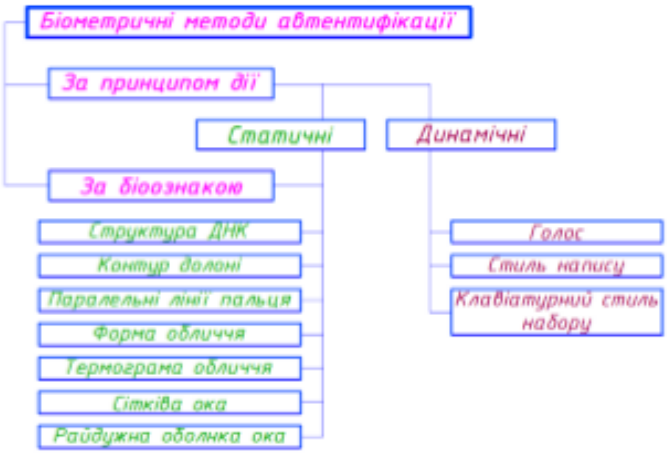


Рисунок 1 – Біометричні методи автентифікації

До біометричних характеристик людини зазвичай відносять: голос, обличчя, структуру ДНК, відбитки пальців, контур долоні, малюнок вен руки, сітківка ока, особливості підпису, хода тощо.

Методи біометричної автентифікації поділяють на два види [1]:

- статистичні – методи, які засновано на вивченні та аналізі характеристик, які не змінюються протягом усього життя людини (відбитки пальців, малюнок райдужної оболонки ока, структура ДНК тощо);
- динамічні – методи, які побудовано на аналізі характеристик людини, які можуть змінюватись протягом її життя (хода, стиль напису, характер набору на клавіатурі).

Ідеальна біометрична характеристика повинна володіти наступними властивостями:

- універсальність – можливість представлення людини однією/єдиною характеристикою;

• унікальність – виключення можливості існування двох осіб з ідентичними характеристиками;

• сталість – незалежність характеристики/показника відносно часу та зовнішніх умов;

• вимірювання/зчитування – можливість швидкого та легкого отримання характеристики.

Аналіз біометричних показників людини (таблиця 1) дозволить сформувати експертну оцінку її властивостей, яка дозволить прискорити процес призначення процедури надання доступу в інформаційній системі.

Таблиця 1 – Оцінювання якостей біометричних показників людини

Характеристика	Універсальність	Унікальність	Сталість	Вимірювання
Форма обличчя	*висока*	*висока*	*середня*	*висока*
Термограма обличчя	*висока*	*висока*	*низька*	*висока*
Відтиск пальця	*середня*	*висока*	*висока*	*середня*
Геометрія руки	*середня*	*середня*	*середня*	*висока*
Райдужна оболонка ока	*висока*	*висока*	*висока*	*середня*
Сітківка	*висока*	*висока*	*середня*	*низька*
Підпис	*низька*	*низька*	*низька*	*висока*
Голос	*середня*	*низька*	*низька*	*середня*
Відтиск губ	*висока*	*висока*	*середня*	*низька*
Особливості вушної раковини	*середня*	*середня*	*середня*	*середня*
Динаміка напису	*висока*	*висока*	*низька*	*висока*
Хода	*висока*	*середня*	*низька*	*низька*

Варто зауважити, що передумовою до впровадження процедури біометричної автентифікації є біометрична ідентифікація (основне завдання біометричних систем). Принциповою відмінністю ідентифікації та автентифікації є рівень довіри до користувача.

На попередньому етапі ідентифікації системи рівень довіри до реєстрованого користувача апріорно високий. При цьому біометрична ідентифікація здійснюється під прямим контролем її власника, що підтверджує повноваження реєстрованої особи. Режим біометричної автентифікації, навпаки, передбачає низький рівень довіри до особи. Під час біометричної автентифікації власник-заявник повинен довести справжність своєї заявленої характеристики шляхом надання унікальних біометричних образів.

Відзначимо, що біометрична автентифікація є потенційно вразливою, у тому випадку, коли її використовують незалежно від методів класичної автентифікації, які базуються на протоколах із використанням паролів та ключів. Достатній рівень інформаційної безпеки забезпечують лише шляхом поєднання методів класичної та біометричної автентифікації.

Літературні джерела

1 Болл Р.М., Коннел Дж.Х., Панканти Ш., Ратха Н.К., Сеньор Э.У. Руководство по биометрии. – Москва : Техносфера, 2007. – 368 с.

2 Шаньгин В.Ф. Комплексная защита информации в корпоративных системах. – Москва : ИД «Форум», 2012. – 592 с.

Додаток В


МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
Матеріали
V Всеукраїнської науково-практичної конференції
"ПРИЛАДОБУДУВАННЯ ТА МЕТРОЛОГІЯ:
СУЧАСНІ ПРОБЛЕМИ, ТЕНДЕНЦІЇ РОЗВИТКУ"
20-22 жовтня 2022 р.
Materials
V Ukrainian scientific conference
"Instrumentation and metrology:
contemporary issues, trends"
October 20-22, 2022
м. Луцьк, 2022

ЄФІМЕНКО Н.А., ЄФІМЕНКО В.С., БАНЗАК О.В., БАНЗАК Г.В., ЛЕЩЕНКО О.І.
АНАЛІЗ НАУКОВИХ ПІДХОДІВ ЗАБЕЗПЕЧЕННЯ КОНТРОЛЮ ЯКОСТІ ПРОДУКЦІЇ НА МАШИНОБУДІВНИХ ПІДПРИЄМСТВАХ..... 29
ЄФІМЕНКО Н.А., ЄФІМЕНКО В.С., БАНЗАК О.В., БАНЗАК Г.В., ЛЕЩЕНКО О.І.
ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ КОНТРОЛЮ ЯКОСТІ ВИГОТОВЛЕННЯ МАШИНОБУДІВНОЇ ПРОДУКЦІЇ..... 31
ІВАНСЬКИЙ Д.І., ТКАЧУК В.М.
НОВІ МЕТОДИ ВИМІРЮВАННЯ ПАРАМЕТРІВ НАНОШОРСТКИХ ПОВЕРХОНЬ..... 33
ІМБІРОВИЧ Н.Ю., ФЕДОСОВ С.А.
СУЧАСНІ ПРОБЛЕМИ ДОСЛІДЖЕНЬ ГАЛЬМІВНИХ СИСТЕМ В УКРАЇНІ..... 35
КАЙДИК О.Л., ТЕРЛЕЦЬКИЙ Т.В., МЕУС О.С, САДОВИЙ М.О, БАС Р.В.
ПРО ТЕХНОЛОГІЮ ТА МЕТОДИ РОЗПІЗНАВАННЯ ЗА ГЕОМЕТРІЄЮ КИСТІ РУКИ..... 37
OLEH KAIDYK, TARAS TERLETSKYI, VITALII PTASHENCHUK, MYKOLA SADOVUY
ABOUT THE ASSIGNMENT OF THE VERIFICATION INTERVAL..... 39
КЕПЕЩУК Т.В., КЕПЕЩУК Д.Т.
МЕТОДИКА КАЛІБРУВАННЯ ТРУБОПОРШНЕВИХ ПОВІРОЧНИХ УСТАНОВОК ЗА ДОПОМОГОЮ КОМПАКТ-ПРУВЕРА З КОМПАРАТОРОМ..... 40
КУДРЯШОВ В.О., ЛЕЩЕНКО О.І., ЛЮБИМОВ А.Я.
АНАЛІЗ МОЖЛИВОСТІ ВДОСКОНАЛЕННЯ МЕТРОЛОГІЧНИХ ХАРАКТЕРИСТИК ДЕТЕКТОРНИХ БЛОКІВ СИСТЕМИ «СЦИНТИЛЯТОР - P-I-N ФОТОДІОД»..... 42
ЛАПЧЕНКО Ю.С.
ІНФОРМАЦІЙНІ КРИТЕРІЇ, ЩО ВИКОРИСТОВУЮТЬСЯ ПРИ ДІАГНОСТИЦІ ПАТОЛОГІЙ ОКА..... 44
ЛИСА О.В., МІДИК А.-В.В.
ВІДДАЛЕНЕ АДМІНІСТРУВАННЯ РОБОТОЮ ГРУПИ ТЕПЛИЦЬ..... 46
МОРОЗ С.А., ТКАЧУК А.А., ЛИШУК В.В.
ОСОБЛИВОСТІ ВИКОРИСТАННЯ ПІРОЕЛЕКТРИЧНИХ ПРИЙМАЧІВ ВИПРОМІНЮВАННЯ ДЛЯ ЕЛЕКТРОННИХ ПРИСТРОЇВ ТЕХНОЛОГІЇ SMART CITY..... 47

ПРО ТЕХНОЛОГІЮ ТА МЕТОДИ РОЗПІЗНАВАННЯ ЗА ГЕОМЕТРІЄЮ КИСТІ РУКИ

Кайдик О.Л., Терлецький Т.В., Меус О.С., Садовий М.О, Бас Р.В.
Луцький національний технічний університет

На сьогоднішній день біометричні характеристики людини відносять до додаткових параметрів захисту, що дозволяє забезпечити носію даної інформації безпеку та комфорт у різних сферах її діяльності. Узагальнено таку технологію ідентифікації/автентифікації особи прийнято називати біометричною.

Біометрія являє собою сукупність автоматизованих методів і засобів ідентифікації людини, які засновано на її фізіологічних характеристиках або поведінці. На систему біометричної ідентифікації покладено наступні функції:

- реєстрація – за декількома параметрами (залежить від методу увтентифікації) формують цифрову модель/шаблон біометричної характеристики окремовзятої людини;
- ідентифікація – вимірювання/зчитування біометричної характеристики з її носія та порівняння з наявним шаблоном/моделлю.

На практиці розрізняють статичні та динамічні методи біометричної автентифікації. Перші методи ґрунтуються на фізіологічній характеристиці людини, а другі – на її поведінці (характерні для підсвідомості рухи під час відтворення будь-якої дії).

Розпізнавання за геометрією кисті руки, яка є унікальною біометричною характеристикою людини, зазвичай відносять до статичних методів розпізнавання. За допомогою спеціального пристрою (сканера), який дозволяє отримувати тривимірний образ кисті руки формують модель унікальної цифрової розгортки, яка дозволяє ідентифікувати людину.

Варто зауважити, що саме системи ідентифікації людини за геометрією (контуром) руки з'явилися одними із перших. З огляду на його компактність образу цей клас систем є найекономічнішим (найпростіший варіант зберігає інформація про довжину та ширину пальців). Більш складними є системи, які здатні вимірювати профіль руки, який включає у себе об'єм кисті, пальців, нерівності долоні, розташування складок шкіри на згинах. Дані про об'ємні параметри руки отримують за допомогою телевізійних камер та інфрачервоного підсвічування руки. Послідовне включення світлодіодів, які розташовано під різними кутами, дозволяє отримати проекцію кисті руки у різних площинах та сформувати інформацію про її об'єм.

Технологію розпізнавання за контуром кисті руки прийнято застосовувати для реалізації контролю доступу за різними рівнями безпеки: низьким, середнім і високим. Окрім цього, таку технологію застосовують і у системах, які здатні реєструвати факт присутності. Точність та швидкодія цього методу ідеально підходять для розпізнавання великої кількості людей. У деяких біометричних технологіях закладено ймовірність помилки до 4%, що не є глобальною проблемою, якщо системою користується мала кількість осіб. В протилежному випадку, коли розпізнавати необхідно десятки тисяч людей, необхідно більш надійніша

технологія. Сканування кисті руки гарантує отримання результату розпізнавання з похибкою не більше 0,01%.

Як уже зазначалось вище, для будь-яких біометричних систем/додатків, в основу яких покладено унікальні біометричні характеристики людини, необхідно створити її ідентифікуючий шаблон/модель (код). Чим меншим буде розмір такого шаблону, тим легше буде реєструвати велику кількість людей, інтегрувати таку систему в існуючі системами управління доступом.

Геометрія кисті руки відрізняється, перш за все, мінімальним розміром шаблону (не більше 9 байт), що робить її ідеальною з точки зору збереження цієї інформації на носії. Зауважимо, що з руки можна зняти до 90 інформаційних параметрів (наприклад, у біометриці не використовують інформацію про візерунок на долоні, який також є унікальним для кожної людини).

Існуючі методи розпізнавання за геометрією кисті руки базуються на таких принципах:

- перший – засновано на геометричних характеристиках кисті руки;
- другий – засновано на змішаних (геометричних і образових) характеристиках кисті руки.

Перший метод порівняно старий, існує понад 25 років. Інформація про біометричні характеристики людини (довжина та ширина пальців) дозволяла керувати їй доступом до приміщення за допомогою систем контролю доступу. За рахунок своєї простоти та недосконалості методики автентифікації цей метод став неефективним. Більш складними є системи, які розпізнають (вимірюють) профіль руки за об'ємом кисті, пальців, нерівності долоні, розташування складок шкіри на згинах. Другий метод більш сучасний (знімається чотири характеристики, три з яких є скалярами та відносяться до розмірів пальців) та базується на формуванні моделі біометричних образів за згинами між фалангами пальців, візерунком (розташуванням) підшкірних кровоносних судин.

Аналіз контрольних (характеристичних) точок контуру руки та її вихідних геометричних ознак дозволяють виокремити наступні біометричні характеристики: ширина долоні, радіус вписаної в долоню кола, довжини пальців, ширина пальців та висота кисті руки у трьох точках. Варто зауважити, що в існуючих системах верифікації особистості людини за геометрією руки використовуються не усі наявні ознаки, частину вихідних параметрів отримують з їх математичного оброблення (кути між контрольними точками, середні значення та дисперсія значень вихідних ознак).

Присутність у біометричній характеристиці руки напівтонового зображення дозволяє суттєво ускладнити процедуру обходу (зламу) системи ідентифікації. При цьому комерційні системи ідентифікації людини, не конкретизують інформації про характерні ознаки (характеристики) руки, які застосовано у системі.

З-поміж основних переваг даного способу автентифікації людини варто виділити його простоту (відсутність особливих вимог до чинників навколишнього середовища та чистоти рук), яка не викликає у них дискомфорт та не займає багато часу.