МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра спеціалізованих комп'ютерних систем

ДОНЧАК Надія Михайлівна

Автоматизована система контролю віддаленого доступу до інформаційних ресурсів/ Automated remote access control system to information resources

спеціальність: 151 – Автоматизація та комп'ютерно-інтегровані технології
освітньо-професійна програма – Автоматизація та комп'ютерно-інтегровані технології

Кваліфікаційна робота

Виконала студентка групи АКІТ - 41
Н.М. Дончак

Науковий керівник
к.т.н., доцент І.Р. Пітух

Кваліфікаційну роботу допущено до захисту:
«____» _____ ___2022 р.

Завідувач кафедри
_____ А.І.Сегін

ТЕРНОПІЛЬ - 2023

Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра спеціалізованих комп'ютерних систем
Освітній ступінь "бакалавр"
Спеціальність: 151 - Автоматизація та комп'ютерно-інтегровані технології
Освітньо-професійна програма – Автоматизація та комп'ютерно-інтегровані технології

ЗАТВЕРДЖУЮ
Завідувач кафедри СКС
_____ А.І.Сегін
"____"_____20__ р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
ДОНЧАК Надії Михайлівні

(прізвище, ім'я по-батькові)

1. Тема кваліфікаційної роботи: __Автоматизована система контролю віддаленого доступу до інформаційних ресурсів/ Automated remote access control system to information resources._____
_____
____керівник роботи_____к.т.н., доцент І.Р. Пітух_____

затверджені наказом по університету від «08» грудня 2020 р. №

2. Строк подання студентом закінченої кваліфікаційної роботи:15.05.2023р.

3. Вихідні дані до кваліфікаційної роботи:
__1. Технології віддаленого доступу._____
__2. Засоби контролю доступу до інформаційних ресурсів._____
__3. Апаратні засоби систем контролю та обмеження доступу._____
__4. Методи ідентифікації користувачів._____

4. Основні питання, які потрібно розробити:
__1. Дослідження технології доступу до віддалених інформаційних ресурсів.___
__2. Аналіз методів ідентифікації користувачів за біологічними ознаками.___
__3. Реалізація автоматизованої системи контролю доступу до інформаційних ресурсів._____
__4. Охорона праці._____

5. Перелік графічного матеріалу у роботі:
_1. Дочірня діаграма IDEF0 ідентифікації користувачів на основі комплексу біометричних параметрів._____
_2. Діаграма IDEF0 декомпозиції блоку А2._____
_3. Алгоритм роботи модуля з використанням звукових сигналів._____
_4. Алгоритм роботи модуля з використанням зображень._____

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Пітух І.Р.		
2	Пітух І.Р.		
3	Пітух І.Р.		
4	Сапожник Г.В.		

7. Дата видачі завдання 20 жовтня 2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назви етапів випускної кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Дослідження технології доступу до віддалених інформаційних ресурсів	11.2022р. – 12.2022р.	
2	Аналіз методів ідентифікації користувачів за біологічними ознаками	01.2023р. – 02.2023р.	
3	Реалізація автоматизованої системи контролю доступу до інформаційних ресурсів	03.2023р. – 04.2023р.	
4	Охорона праці	04.2023р. – 05.2023р.	

Студент _____ Дончак Н.М.
(підпис)

Керівник роботи _____ к.т.н., доцент Пітух І.Р.
(підпис)

РЕФЕРАТ

Робота виконана на 74 сторінках та містить 39 рисунків, 3 таблиці, 5 додатків, 35 джерел за переліком посилань.

Мета роботи. Метою роботи є проектування автоматизованої системи контролю віддаленого доступу до інформаційних ресурсів.

Методи дослідження. Методи, методики та технології створення САУ процесами та комплексами різного призначення. Інструментальні засоби моделювання, планування, математичного, алгоритмічного і програмного забезпечення задач аналізу та синтезу складних розподілених у просторі гнучких комп'ютерно-інтегрованих систем.

Результи роботи. Досліджено засоби та технології контролю доступу, розроблено структуру, функціональну модель та програмне забезпечення автоматизованої системи контролю віддаленого доступу до інформаційних ресурсів, що забезпечить високу надійність, безпеку та зручність використання.

Рекомендації по використанню результатів роботи. Запропонована система може бути використана в різних сферах, наприклад, в установах державної влади, фінансових установах, компаніях тощо, для забезпечення швидкого та безпечного доступу до необхідних інформаційних ресурсів.

Можливі напрямки розвитку. У запропонованій системі можливе вдосконалення системи аудиту дій користувачів та розробка системи сповіщення про їх підозрілу діяльність, а також покращення механізмів аутентифікації та авторизації, розширення функціональності системи та її адаптацію до різних галузей використання.

Ключові слова: АВТОМАТИЗОВАНА СИСТЕМА, КОНТРОЛЬ ДОСТУПУ, ІДЕНТИФІКАЦІЯ, ВІДДАЛЕНИЙ ДОСТУП, ІНФОРМАЦІЙНІ РЕСУРСИ.

ABSTRACT

Work is executed on 74 pages and including 39 illustrations, 3 tables, 5 appendices ,35 sources after the list of references.

Purpose of work. The aim of the work is to design an automated system for remote control of access to information resources.

Research methods. Methods, techniques and technologies for the creation of Automatic control systems for processes and complexes of different purposes. Instrumental means of modeling, planning, mathematical, algorithmic and software problems of analysis and synthesis of complex distributed in the space of flexible computer-integrated systems

Job performances. The means and technologies for access control have been researched, and a structure, functional model, and software for an automated system of remote access control to information resources have been developed. This system ensures high reliability, security, and user convenience..

Recommendations after the use of job performances. The proposed system can be used in various areas, such as government institutions, financial institutions, companies, etc., to provide quick and secure access to the necessary information resources.

Possible development directions. The proposed system can be improved by enhancing user activity auditing and developing a notification system for suspicious activities, as well as improving authentication and authorization mechanisms, expanding the system functionality, and adapting it for various domains of use.

Keywords: AUTOMATED SYSTEM, ACCESS CONTROL, IDENTIFICATION, REMOTE ACCESS, INFORMATION RESOURCES

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

СКУД – система контролю та управління доступом;

АСК – автоматизована система контролю;

ВД – віддалений доступ;

ІР – інформаційні ресурси;

ПЗ – програмне забезпечення;

НСД – несанкціонований доступ;

ОС – операційна система;

КД – контроль доступу;

НСД – несанкціонований доступ;

ЕЗ – еталонний зразок;

ММ – математична модель;

РРЧ – режим реального часу;

НММ – приховані моделі Маркова;

SVM – Support Vector Machines;

SNoW Classifier Networks of One Weight;

АЦП – аналого–цифрове перетворення;

К – контролер;

ВМ – виконавчий механізм;

Д – датчик;

АРМ – автоматизоване робоче місце.

ВСТУП

Актуальність теми. В сучасних умовах, коли більшість процесів відбуваютьюся в онлайн режимі, віддалений доступ до інформаційних ресурсів є надзвичайно важливим. Робота з віддаленим доступом дозволяє користувачам працювати з інформаційними ресурсами з будь–якої локації та в любий час, що дозволяє значно збільшити продуктивність роботи та знизити витрати на забезпечення стаціонарного робочого місця.

Проте, зростання популярності віддаленого доступу також призводить до збільшення кількості кібератак на інформаційні системи та мережі. Такі атаки можуть спричинити втрату конфіденційної інформації, порушення робочих процесів та фінансові збитки. Щоб зменшити ризики таких атак, важливо забезпечити безпеку та захист інформації з використанням систем контролю та управління доступом (СКУД).

Застосування автоматизованих систем контролю (АСК) доступу дозволяє зменшити ці ризики та забезпечити безпеку інформаційних ресурсів. Тому, розробка та використання таких систем для віддаленого доступу є важливою задачею, вирішення якої дозволяє забезпечити високий рівень захисту даних та безпеки діяльності організацій та компаній, оскільки вони дозволяють контролювати доступ до інформації, забезпечуючи ідентифікацію, авентифікацію, авторизацію та аудит дій користувачів.

Мета кваліфікаційної роботи полягає у дослідженні існуючих методів та технологій забезпечення віддаленого доступу, розробку автоматизованої системи, що забезпечує безпеку, конфіденційність та цілісність даних.

Досягнення мети обумовлює вирішення таких завдань:

- дослідження технології доступу до віддалених інформаційних ресурсів;
- дослідження апаратних та програмних засобів систем контролю та обмеження доступу;
- аналіз методів ідентифікації користувачів за біологічними ознаками;
- обґрунтувати вибір методів ідентифікації для реалізації АСК;

- побудувати математичну модель ідентифікації;
- реалізувати алгоритми ідентифікації за різними характеристиками;
- розробити архітектуру АСК;
- реалізувати АСК доступу до інформаційних ресурсів.

Предметом дослідження є автоматизована система контролю доступу до віддалених інформаційних ресурсів.

Об'єктом дослідження процеси та технології забезпечення безпеки дистанційного доступу до даних.

Методи дослідження – методи, методики та технології створення САУ процесами та комплексами різного призначення. Інструментальні засоби моделювання, планування, математичного, алгоритмічного і програмного забезпечення задач аналізу та синтезу складних розподілених у просторі гнучких комп'ютерно–інтегрованих систем, методи та засоби розпізнавання та підтвердження особи в комп'ютеризованих системах.

Практичне значення одержаних результатів. Система може використовуватися в організаціях різного розміру для забезпечення високої швидкості та надійності роботи для користувачів, які працюють з віддалених місць, що сприяє більш ефективному управлінню процесами та знижує виробничі витрати.

Напрямки подальшого розвитку. Можливе розширення функцій запропонованої системи з метою підвищення безпеки даних, покращення механізмів аутентифікації, авторизації, інтеграція з системами електронного документообігу та інших процесів. Також розширити можливості аудиту для відстеження діяльності користувачів, що мають доступ до інформаційних ресурсів.

Публікації.

1. Дончак Н.М. Дослідження та розробка автоматизованої системи контролю доступу. Збірник матеріалів проблемно–наукової міжгалузевої конференції «Автоматизація та комп'ютерно–інтегровані технології» (АКІТ – 2023), Тернопіль, 2023. –с.

1. ДОСЛІДЖЕННЯ ТЕХНОЛОГІЇ ДОСТУПУ ДО ВІДДАЛЕНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

1.1 Віддалений доступ до інформаційних ресурсів

Віддалений доступ (ВД) до інформаційних ресурсів (ІР) організації є дуже важливим елементом для організації роботи в онлайн–режимі, що набув актуальності у останні роки у зв'язку з поширенням пандемії COVID–19 та введенням карантинних заходів, які змусили багато компаній перейти на дистанційну роботу [1–4]. В таких умовах ВД до інформації став необхідним для забезпечення роботи організацій та забезпечення продуктивності співробітників та дозволив організаціям зберігати конкурентну перевагу та адаптуватися до змін у бізнес–середовищі.

Дистанційна робота з даними стає все більш актуальною у сучасному світі, оскільки дозволяє не лише забезпечити ефективну роботу, але й надавати освітні послуги з усіх точок із доступом до Інтернету. Крім того, ВД до ресурсів дозволяє знизити організаційні витрати на обладнання робочого місця, оренду та обслуговування офісних приміщень а також надає можливість працювати з значним обсягом інформації та забезпечувати безпеку інформації за допомогою різноманітних інструментів захисту даних.

Онлайн–режим роботи є це одним зі способів віддаленої роботи, що полягає у використанні ІТ–технологій для взаємодії з колегами, клієнтами, партнерами та іншими стейкхолдерами ВД дозволяє підтримувати зв'язок та комунікацію між користувачами на різних континентах, що збільшує ефективність роботи у великих компаніях з децентралізованою структурою. З урахуванням технологічного розвитку та зростаючої мобільності, ВД до інформації є необхідним компонентом успішної роботи в будь–якій галузі.

Основними перевагами організації ВД до даних та роботи віддалено є:

- Глобалізація бізнесу – завдяки технологічному розвитку та зростанню глобалізації бізнесу, компанії можуть займатися своїм бізнесом в будь–якої локації світу, не обмежуючись географічним положенням. Робота з ВД дозволяє

співробітникам працювати з любого місця, що є особливо зручним для компаній з представництвами в різних країнах.

- Економічні переваги – робота в режимі онлайн, що виконується з місця, яке відмінне від місця розташування організації або робочого місця працівників, дозволяє компаніям скоротити витрати, які пов'язані із орендою офісних приміщень та інфраструктурою, такою як електроенергія, опалення та інтернет–зв'язок.

- Зручність та гнучкість роботи з ВД дозволяє співробітникам працювати в зручний для них час та місце, зменшує час, який витрачається на шлях до роботи та назад, та надає більшу гнучкість в роботі.

- Збільшення продуктивності – віддалена робота дозволяє співробітникам працювати в зручному для них режимі, що зазвичай призводить до збільшення продуктивності. Також, співробітники можуть бути більш зосередженими на своїй роботі, оскільки відсутність зовнішніх відволікаючих факторів може позитивно вплинути на їх концентрацію та ефективність роботи.

- Збільшення доступності робочої сили – віддалена робота дозволяє компаніям залучати співробітників з різних точок світу, що збільшує доступ до більш широкої бази даних (БД) потенційних працівників. Це дозволяє компаніям найняти висококваліфікованих спеціалістів, які можуть знаходитися в інших країнах або регіонах, у яких вони є менш доступними для роботодавців.

Крім того, ВД до IP може забезпечити доступ до більш широкого кола робочих годин. Наприклад, якщо компанія має офіси в різних часових зонах, віддалена робота дозволяє залучати працівників з будьякої зони, що забезпечує більш гнучкий розклад роботи та покращує обслуговування клієнтів у різних частинах світу.

1.2 Засоби контролою доступу до інформаційних ресурсів

В сучасному світі обмін інформацією відбувається за допомогою електроних каналів зв'язку. Розвиток інформаційних технологій та глобальної мережі інтернету [1] зумовлює дедалі більше число компаній та організацій

переходити до онлайн–режиму роботи, що передбачає використання ВД до різного виду інформації (рисунок 1.1).

Рисунок 1.1 – Класифікація інформації

ВД є важливим для підвищення продуктивності роботи однак, збільшує ризики несанкціонованого доступу (НСД) до інформації, який може призвести до втрати конфіденційної та таємної інформації [5–7]. Тому задача інформаційної безпеки, зокрема контролю доступу (КД), є надзвичайно важливою.

Основою цього є перевірка даних про користувача. Розрізняють три елементи КД:

- ідентифікація – є першим етапом на якому відбувається розпізнавання інформації про користувача, наприклад, логін та пароль;
- автентифікація – є другим етапом, зокрема є процесом перевірки інформації про користувача;
- авторизація – третій етап, на якому відбувається перевірка прав користувача та визначення можливості його доступу до ІР.

Для того, щоб раелізувати захистит даиих від НСД, зловмисників та інших загроз існують різноманітні методи захисту, а також засоби КД, що включають апаратні і програмні інструменти [8–10].

До апаратних засобів КД (рисунок 1.2) включають пристрої, які реалізують захист даних високого рівня, оскільки вони забезпечують апаратну автентифікацію та шифрування даних. Вони включають фізичні пристрої, такі як біометричні сканери, смарт–карти, токени та ін.

Рисунок 1.2 – Класифікація апаратних засобів КД

Програмні засоби регулювання доступності ІР (рисунок 1.3) включають різні системи шифрування, паролі та інші методи автентифікації користувачів, інструменти що видаляють залишкову (робочу) інформацію, зокрема тимчасові файли, реалізують тестовий контроль систем захисту, між–мережеві екрани – брандмауери та фаєрволи, антивірусні програми, спеціалізовані програмні засоби, Proxy–сервери, VPN та інші заходи безпеки.

Рисунок 1.3 – Класифікація програмних засобів

Використання зазначених методів захисту та засобів контролю може допомогти забезпечити безпеку інформації та захистити її від небажаних загроз. Крім того, на практиці застосовується комбінація програмних та апаратних елементів управління доступом до ІР, що дозволяє забезпечити найвищий ступінь безпеки та надійності. Це може реалізувати надійний захист конфіденційної інформації в системах електронної торгівлі, банківських операцій, дистанційного

навчання, мережах корпорацій, тощо.

Найбільш критичним елементом системи керування правами доступу є ефективність ідентифікації користувача, що отримує права доступу до конфіденційних даних. У традиційних методів ідентифікації, зокрема таких як парольний захист, є низка недоліків, серед яких можлива витік конфіденційної інформації внаслідок скомпрометованого пароля.

Автентифікація використовується для отримання доступу до різних ресурсів, наприклад, соцмереж, електронного поштового ресурсу, інтернет–магазину, платіжних систем, тощо [10].

Елементами автентифікації є:

- суб'єкт – користувач;
- характеристика суб'єкта – інформація, яку надає користувач для автентифікації;
- власник системи автентифікації – власник ресурсу;
- механізм автентифікації – принцип перевірки;
- механізм авторизації – управління доступом.

Парольні системи є методом, який широко використовується. В системах автентифікація може відбуватися за допомогою одноразового та багаторазових паролів. Багаторазовий – задається користувачем, зберігається у БД системи та є ідентичним під час кожної із сесій. До таких поролів можна віднести PIN–код, слово, цифр, графічний ключ, тощо. На відміну від зазначеного одноразовий пароль буде відрізнятися під час кожної із сесій, прикладом може бути код отриманий за допомогою SMS.

При комбінованих методах автентифікація відбувається з використанням кількох методів, наприклад, парольних та криптографічних сертифікатів. Він потребує спеціального пристрою для зчитування інформації.

Біометричні є найдорожчими методами аутентифікації. Вони запобігаєть витоку або крадіжці персональної інформації. Перевірка проходить за фізіологічними характеристиками користувача, наприклад, по відбитку пальця, сітківці ока, ДНК, тембру голосу тощо.

Інформація про користувача використовується для відновлення логіну або

пароля та для двоетапної автентифікації, для досягнення високого ступеня безпеки. До цього методу належить номер телефону, дівоче прізвище матері, рік народження, дата реєстрації, прізвисько вихованця, місце проживання.

Метод користувацьких даних ґрунтується на використанні геоданих про розташування користувача з використанням GPS, а також використовує інформацію про точки доступу безпровідного зв'язку. Недоліком є те, що за допомогою проксі–серверів можна підмінити дані.

Види автентифікації можна класифікувати за такими характеристиками:

- в залежності від кількості методів, що використовуються:
  - одно-факторна – використовує лише один метод;
  - багато-факторна – використовує кілька способів.
- в залежності від політики безпеки систем та рівня довіри до користувачів:
  - одностороння – користувачі доводять право доступу до IP їх власнику;
  - взаємна – де відбувається перевірка достовірність прав доступу як користувача так і власника IP, як правило, з використанням методів криптографії.

Процедура авторизації є важливою частиною захисту інформації у інформаційнних системах. Її основною метою є реалізація КД користувачів до IP системи, тобто встановити, які користувачі мають право доступу до яких ресурсів системи та які дії вони можуть виконувати з цими ресурсами. Крім того, дана процедура дозволяє встановити ідентичність користувача та переконатися, є у нього відповідні права на доступ до певних ресурсів системи. Це допомагає забезпечити безпеку інформації та запобігти НСД до неї. Авторизація відбувається після того, як успішно пройшли попередні етапи. Для кожного із користувачів системи визначається певний набір обмежень та правил, що будуть використовуватися при зверненні ним до ресурсів.

Перелічені програмні засоби та апаратні інструменти систем КД характеризуються певними перевагами та недоліками. Їх вибір залежить від конкрентих вимог та потреб користувачів IT-систем.

1.3 Апаратні засоби систем контролю та обмеження доступу

Перевагами апаратних засобів КД IP у порівнянні з програмними є те, що вони забезпечують вищий рівень захисту, оскільки можуть фізично обмежити доступ до IP, що зберігаються в системі. Апаратні засоби не залежать від операційної системи (ОС) і програмного забезпечення (ПЗ), що використовується в системі, а це визначає можливість їх використання на будь якій платформі. Перевагою є відсутність можливості впливу на апаратні засоби ззовні, наприклад вірусів та шкідливих програм, оскільки вони розміщені на апаратному рівні і не залежать від ПЗ [11–13].

Апаратні засоби ВД дозволяють забезпечити високий ступінь безпеки та надійності захисту даних, оскільки вони базуються на апаратних механізмах, які не піддаються зламуванню програмним шляхом. Вони також дозволяють зменшити ризик витоку даних через зовнішні атаки, віруси або шкідливі програми, оскільки вони надійніше захищають доступ до конфіденційних даних. Крім того, апаратні засоби, як правило, працюють у автономному режимі, що дозволяє забезпечувати захист навіть тоді, коли комп'ютер піддається атакам або знаходиться в аварійному режимі.

Прикладом апаратних засобів КД до IP є електронні ключі Touch Memory – це одним із видів електронних ідентифікаторів, що широко застосовуються по всьому світу. Зовнішнім виглядом (рисунок 1.4) цей тип електронного ключа нагадує плоску батарейку, ґудзик або таблетку [14]. Іншою назвою електронних ключів цього типу є ключі iButton, що означає «інформаційна кнопка».

Рисунок 1.4 –Електронний ключ

Функціональність, необхідність ПЗ та кількість вбудованої пам'яті даного тину засобів збільшуються відповідно із зростанням номеру моделі – від DS1990, що не містить пам'яті, ідентифікація за ID-номером, як правило використовується

в домофонах, до DS1996. У моделі DS1996 є вбудований календар.

Технологія RFID – технологією радіочастотної ідентифікації, в основі якої лежить використання радіочастотного електромагнітного випромінювання [15]. RFID-мітка містить мікрочіп, що включає унікальний номер та користувацьку інформацію, та антени, за допомогою якої вона передає та отримує ці дані. При потряплянні мітки до зони реєстрації, спеціальний пристрій-зчитувач може зчитувати та записувати інформацію в мітці (рисунок 1.5).

Рисунок 1.5 – RFID мітки

RFID-мітки класифікуються за типом живлення, видами пам'яті та за виконанням (визначається цілями), а також за умовами їх використання.

NFC це технологія високочастотного безпровідного зв'язку із невеликим радіусом дії (<10 см), яка дозволяє здійснення безконтактного обміну даними між прнстроями, які розташовані на невеликій відстані (рисунок 1.6). Дана технологія заснована, на попередньо розглянутій, технології RFID [16].

Рисунок 1.6 – Технологія NFC

Три найбільш популярні варіанти використання NFC технології в мобільних телефонах:

- емуляція карт – телефон емулює карту, наприклад пропуск або платіжну

картку;

- режим зчитування – телефон зчитує пасивну мітку (Tag), наприклад для інтерактивної реклами;
- режим P2P – два телефони зв'язуються та обмінюються інформацією.

Картки з магнітною стрічкою (рисунок 1.7) також відносять до апаратних засобів захисту IP. У цьому типі картки інформація заноситься на магнітну смугу. Карти із магнітною смугою бувають трьох форматів: ID-1, ID-2, ID-3 [17].

Рисунок 1.7 – Картки з магнітною стрічкою

Магнітна стрічка містить 3 доріжки, на які в закодованому вигляді записують номер карти, її термін дії, прізвище власника картки тощо. Обсяг записаної інформації близько 100 байт. Характеристики смуг магнітних карток представлені в таблиці 1.1.

Таблиця 1.1 – Технічні характеристики магнітних стрічок

Доріжка	Кількість символів	Символи кодування
1	76	QWERTYUIOPASDFGHJKLZXCVBNM 0123456789 : ; = + () - ' - ! @ # ^ & * < > / \
2	37	лише цифри 0 1 2 3 4 5 6 7 8 9 та знак "="
3	104	лише цифри 0 1 2 3 4 5 6 7 8 9 та знак "="

Магнітні стрічки можуть за необхідності виготовлюватися для різної потужності магнітного поля. Відповідно до цього параметру їх класифікують як висококоерцитивний – HiCo і низькокоерцитивний – LoCo [17]. Ступінь коерцитивності має вплив на стійкість до розмагнічування записаних даних. Пластикові карти з магнітною стрічкою HiCo є більш надійними та довговічними,

оскільки інформація на них є менш схильною до розмагнічування шляхом зовнішніх магнітних полів, ніж на стручки LoCo.

Смарт–карти (рисунок 1.8) є пластиковими картками у які вбудовано мікросхему [17]. У переважній більшості, вони оснащені мікропроцесором та ОС, що контролює сам пристрій та управляє доступом до об'єктів, що знаходяться в його запамятовуючому пристрої. Картки мають можливість проводити криптографічні обчислення. Такі карти призначенні для одно- та дво-факторна автентифікація користувачів, збереження важливої інформації та проведення крипто–операцій у захищеному середовищі.

Рисунок 1.8 – Смарт–карта

Такі карти можна класифікувати по способу обміну данми із зчитуючим пристроєм, наприклад:

- контактні із інтерфейсом ISO 7816 – вони мають зону контакту, що має декілька контактних пелюсток невеликих розмірів. Коли картка контактує з зчитувачем, чіп сдоторкається до електричних конекторів, тоді зчитувач може зчитувати або записувати наді на чіп.
- контактні з інтерфейсом USB – зазвичай це мікросхема звичайної ISO 7816 карти, що суміщена з USB–зчитувачем в одному мініатюрному корпусі. Це робить застосування смарт–карт для комп'ютерної автентифікації набагато зручніше.
- безконтактні (RFID) смарт-картки – контакт із зчитувачем відбувається за технологією RFID. Необхідно підносити картку достатньо близько до пристрою, для того щоб здійснити операції. Їх часто застосовують у сферах, де необхідне швидке проведення операцій, зокрема, у транспорті.

Використання смарт-карт для цифрової ідентифікації швидко розвивається. У цій сфері карти застосовуються для забезпечення автентифікації особи.

Штрих-код (рисунок 1.9 а) – це закодована інформація, що наноситься у вигляді штрихів, а зчитування відбувається спеціальними пристроями. За допомогою штрихового коду кодують інформацію про деякі найбільш суттєві параметри об'єкта.

а) б)

Рисунок 1.9 – Штрих код та QR–код

QR-код (quick response – швидкий відгук) (рисунок 1.9 б) є двомірним штрихкодом, розробленим у 1994 році фірмою Denso–Wave (Японія). У ньому кодується інформація, що складається із символів (включаючи кирилицю, цифри та спецсимволи).

Як альтернатива традиційній парольній системі, можна розглядати ідентифікацію користувачів за біометричними характеристиками (рисунок 1.10), що має переваги у порівняні до традиційних методів [18].

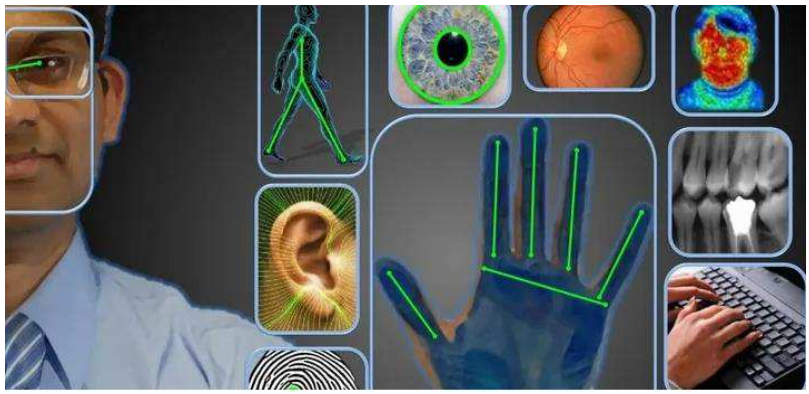

Рисунок 1.10 – Біометричні характеристики

Відмінність біометричного підтвердження від звичайної перевірки пароля полягає в можливості ідентифікувати особу користувача за його фізичними особливостями або поведінкою. Це має ключове значення для розвитку електронної комерції, впровадження нових систем інформаційної безпеки у корпоративні мережі та системи навчання дистанційно.

Сучасні біометричні системи та технології забезпечують розпізнавання людей на основі певних анатомічних особливостей, зокрема відбитків пальців, образ обличчя, форми та ліній на долоні, малюнка очей та голосу, або рис поведінки, наприклад підпис та ходьба [19]. Використання біометричних технологій дозволяє досягнути високого рівня захщеності ІР порівнянно із традиційними способами захисту, такими як паролі, що можуть викрадатися, перехоплюватися або бути вгаданими.

Крім того, біометричні АСК доступу є зручними для користувачів, оскільки не потрібно запам'ятовувати складний пароль або носити з собою ключ–карту для отримання доступу до ІР. Також, неможливо, щоб біометричні дані бути викрадені, перехоплені або загублені.

2. АНАЛІЗ МЕТОДІВ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ЗА БІОЛОГІЧНИМИ ОЗНАКАМИ

2.1 Методи біометричної ідентифікації користувачів

Біометрія – забезпечує розпізнавання та визначення, тобто ідентифікацію людини за біологічними ознаками [18]. Однією з її переваг є висока точність ідентифікації, оскільки біологічні ознаки людини є унікальними та не можуть бути скопійовані. Біометрія також є зручною та швидкою альтернативою для автентифікації користувача в порівнянні зі стандартними методами, такими як використання пароля або картки доступу. Методи такої ідентифікації можна розділити на групу динамічних та статичних, як видно з рисунку 2.1.

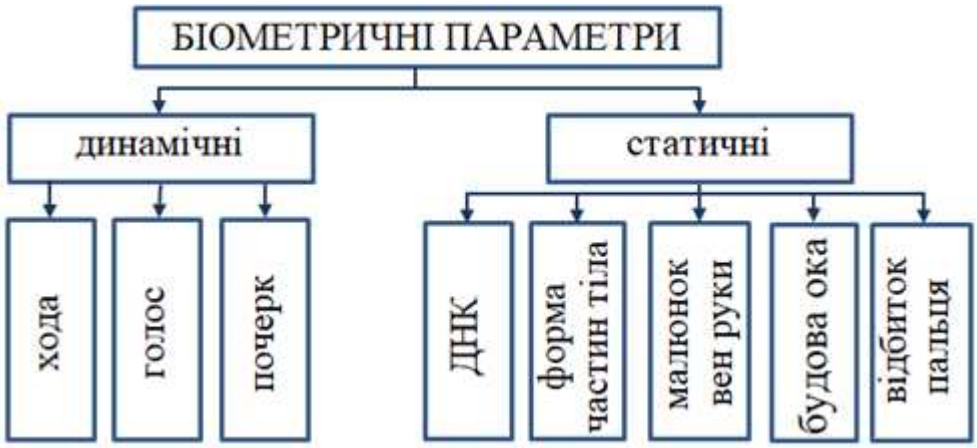

Рисунок 2.1 – Методи біометричної ідентифікації

Статичні методи грунтуються на унікальній фізіологічній характеристиці людини, невід'ємної та даної їй від народження. Розрізнають різні способи ідентифікації користувача [19–23]. Персональна ідентифікація може бути здійснена шляхом аналізу окремих частин тіла, зокрема за формою обличчя. При такому методі створюється тривимірне зображення людини, де виділяються контур губ, брів, очей та інших рис обличчя. За допомогою обчислення відстаней між цими рисами будується образ, який не лише відображає форму обличчя, але й враховує можливі зміни виразу, кутів нахилу та повороту голови.

Також можливе визначення особи за формою долоні. Такий метод базується на геометрії кистей рук, і використовує спеціальний пристрій, який складається із

камери та кількох діодів. Підсвічуючи долонь з різних кутів, пристрій отримує різні проекції кисті руки, з яких будується 3-D-образ. За допомогою цього образу визначається унікальна згортка на долоні, яка використовується для ідентифікації особи. За тим, як розташовані на долоні вени можна проводити ідентифікацію для ВД. Використовуючи інфрачервону камеру для зчитування малюнку вен руки або долоні, даний метод дозволяє отримати цифрову згортку шляхом обробки схеми розміщення вен.

Розпізнати людину можна також за допомогою будови ока, оскільки кожен індивідуум має унікальну будову райдужної оболонки та сітківки ока, що дозволяє використовувати ці біометричні ідентифікатори особи. Для того, щоб провести сканування райдужної оболонки необхідна тільки портативна камера зі спеціалізованим ПЗ, яке дозволить захопити зображення певної зони обличчя, з якого відокремлюється зображення ока і райдужної оболонки, що з них будує код ПЗ що дозволить ідентифікувати людину. «Визначення особи за сітківкою ока полягає у використанні малюнка кровоносних судин очного дна» [21]. Цей малюнок стає видимим під час погляду на віддалену світлову точку, після чого його можна зісканувати спеціальною камерою для створення цифрового коду ідентифікації людини.

Метод ідентифікації на основі відбитку пальців базується на неповторності малюнку папілярних візерунків на кожній людині. За допомогою спеціалізованого пристрою – сканера отримується відбиток, далі він перетворюється у цифрову форму (згортку), і потім відбувається порівняння з вже збереженим еталоном. Ця технологія є найпоширенішою порівняно з рештою методів біометричної ідентифікації.

Використовуються також інші унікальні способи, наприклад ідентифікація за шаром шкіри під нігтем, за кількома вказаними для ідентифікації пальців, формою вушної раковини, за запахом, за розподілом тепла на поверхні обличчя. Даний метод ідентифікації ґрунтується на унікальному розподілі артерій на обличчі, які забезпечують кровообіг і випромінюють тепло. Створення термограми отримується за допомогою спеціальних інфрачервоних камер. У порівнянні з методом ідентифікації за рисами зовнішності, даний – забезпечує

розпізнавання навіть схожих братів та сестер-близнюків. Перевагами методу ідентифікації за ДНК полягають у високій точності ідентифікації, проте його застосування відносно обмежене через затрати часу, необхідні для одержання та обробки ДНК за поточних методів. Тому такі системи використовуються головним чином для вузького кола експертиз.

Методи динамічної ідентифікації засновані на певних особливостях поведінки людини, що проявляються у підсвідомих рухах, що здійснюються нею під час виконання довільної дії. Ідентифікувати людину можна за рукописним почерком. Ця технологія набуває популярності стосовно альтернативи звичайного підпису за допомогою ручки. В даному випадку зразок можна отримати за допомогою спеціальної ручки, або чутливого до тиску планшета, або їх комбінації.

В залежності від потрібного рівня безпеки, біометрична ідентифікація може бути простою, ґрунтуючись на порівнянні двох зображень, або складною, де крім зображень проводиться аналіз динамічних особливостей написання, таких як ступінь тиску, швидкість письма, розподіл зон з більшим або меншим тиском та інші. Використовується також клавіатурний аналіз даних. Для цього не потрібно жодного спеціального обладнання, лише стандартна клавіатура. Основним параметром, за яким відбувається побудова згортки є динаміка з якою відбувається набір кодових слів. Іншимі способом ідентифікації за динамічними характеристиками є, наприклад рух губ під час вимовляння паролю чи врахування динаміки ключа під час його повороту у замку, тощо.

Голосова ідентифікація – це спосіб визначення особи за її голосом. Суть методу в тому, щоб порівняти голос, який поточно записується, з голосом, який збережений в БД. Для цього використовуються різні параметри голосу, такі як частота, інтенсивність, тембр, артикуляція тощо. Для побудови коду ідентифікування по голосу, зазвичай, використовуються різноманітні поєднання таких характеристик голосу, як частотні та статистичні.

Найбільш поширеними способами здійснювати ВД до ІР за допомогою біометричних методів є розпізнавання відбитку пальця, двохвимірного або тривимірного зображення особи або райдужної оболонки ока. Незалежно від

методу, який використовується, вони базуються на порівнянні інформації про об'єкт і певним біометричним еталоном. Щоб таке порівняння було можливим, необхідно записувати та зберігати біометричну інформацію, що створює потребу в документуванні цієї інформації.

2.2 Обгрунтування вибору методу біометричної ідентифікації

В проектованій системі біометрична ідентифікація вибрана як достатньо точний та ефективний метод контролю ВД. Даний метод є зручним у використанні, забезпечує швидку ідентифікацію користувача, а також зменшує ризик помилкової ідентифікації. На вибір конкретного методу біометричної ідентифікації можуть вплинути різні фактори, наприклад які біометричні ознаки доступні для збору, відтворюваність ознак, їх надійність, унікальність тощо.

Тому для обґрунтування вибору біометричних характеристик для ідентифікації користувачів в проектованій системі контролю ВД до ІР, необхідно розглянути детальніше різні доступні методи.

2.2.1 Система розпізнавання відбитків пальців

Сканування відбитків пальців є найбільш ранньою методикою з усіх наявних, проте вона все ще вважається однією з кращих. Криміналістична наука і експертна практика довели, кожна людина має унікальні та незмінні візерунки на кінчиках пальців. Рельєфні лінії, які утворюють відбиток пальця, складаються з гребінців – виступів на шкірі, які поділених на борозенки, та формують складні зображення, такі як дуги, петлі, завитки. Ці властивості, такі як індивідуальність, стійкість і відновлюваність, притаманні цілому візерунку.

Метод визначення особи за відбитком пальця [22] (рисунок 2.2) має дуже низький рівень відмов у доступі до ІР, а це значить, що АСК рідко не розпізнає достовірність відбитків пальців зареєстрованого користувача. Однак, при цьому існує певна можливість помилки або підробки доступу до ІР, коли АСК неправильно ідентифікує відбитки пальців користувачів, які не зареєстровані в даній системі.

Рисунок 2.2 – Процес розпізнавання відбитків

2.2.2 Ситема розпізнавання за ознаками зовнішності

Ідентифікація особи за розпізнаванням обличчя – це технологія біометричної ідентифікації, яка полягає в автоматичному розпізнаванні особи за його візуальними ознаками, зокрема за формою і розмірами голови, відстанню між очима, формою брів, носа, губ і т.д. Основною метою технології розпізнавання обличчя [20] є ідентифікація певної особи серед тисяч облич у БД в режимі «один до багатьох». Якість роботи даних систем перебуває в залежності від можливостей відеокамер, які повинні мати високу роздільну здатність (не < 800x600 DPI) та швидкість потоку відео не < 3-5 FPS. Для покращення якості ідентифікації важливо об'єднати камери в мережу з робочими станціями та забезпечити ще більшу швидкість відеопотоку та кращу розподільну здатність.

Технологією ідентифікації за розпізнаванням обличчя використовуються алгоритми машинного навчання і штучного інтелекту для зіставлення зображення обличчя з даними у БД ідентифікації. Ця технологія набула широкого застосовування в системах безпеки, охорони та КД, а також у фотографії та відеозйомці.

Розрізняють кілька основних методів розпізнавання за обличчям, що засновані на аналізі зображень для виявлення відмінних характеристик, серед них:

- проведення аналізу рис обличчя, що відрізняються – найбільш поширений та адаптований до зміни міміки людини;
- проведення аналіз на базі нейронних мереж, який оснований на порівнянні так званих особливих точок, що дозволяє ідентифікувати людину у важких ситуаціях;

- автоматична обробка зображення, яка визначає відстань та їх відношення між встановленими рисами, що визначають особливості обличчя.

На рисунку 2.3 наведено приклад процесу розпізнавання характерних рис на обличчі людини.

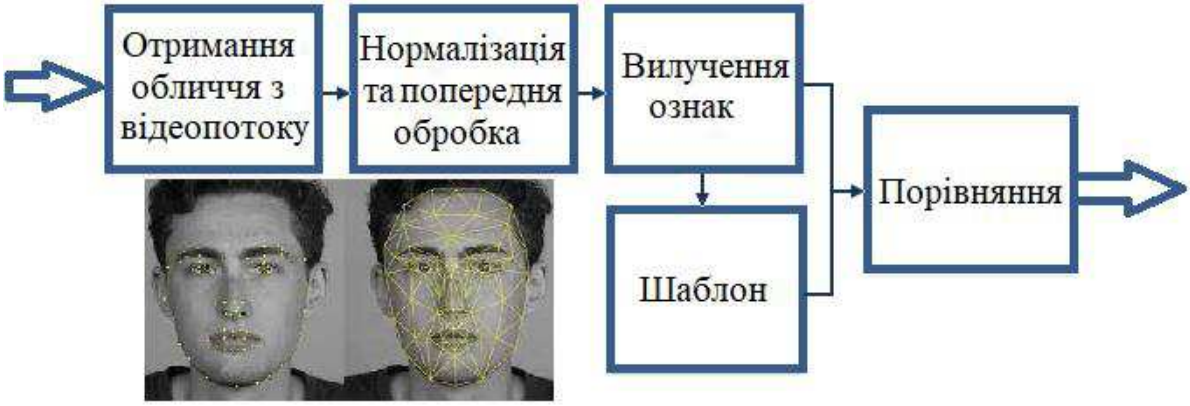

Рисунок 2.3 – Процес розпізнавання людського обличчя

Перевагами технології ідентифікації за розпізнаванням обличчя є швидкість і точність ідентифікації, можливість використання у різних умовах освітлення та змін міміки, а також відсутність необхідності у фізичному контакті з об'єктом ідентифікації.

Однак, серед недоліків можна назвати можливість помилкової ідентифікації при зміні зовнішнього вигляду (наприклад, зміна зачіски або надівання окулярів) та питання приватності даних, які зберігаються в БД ідентифікації.

2.2.3 Система ідентифікації за формою частин тіла

Біометрична ідентифікація за формою вуха базується на геометрії вуха та інших характеристиках (рисунок 2.4), які можуть виокремлюватися з форми вушної раковини [23].

Цей метод може використовуватися для автоматичної ідентифікації особи на основі її вуха. Вухо містить унікальну комбінацію особистих рис, таких як розмір, форма, контури та інші, що застосовуються для розпізнавання.

Сучасні технології дозволяють застосовувати даний метод ідентифікації з високим рівнем швидкості обробки даних й точності. Проте він має недоліки серед яких є необхідність використовувати спеціальне обладнання, що досить є

високовартісним, а також чутливість до дії зовнішніх факторів, як травми, операції, вади слуху або форми, які важко або неможливо сканувати.

Рисунок 2.4 – Процес ідентифікації за формою вуха

Технологія ідентифікації особи за геометрією кисті руки [22] (рисунок 2.5) є подібною до розпізнавання за відбитками пальців в аспекті технологічної структури та рівня надійності, але ще не є широко поширеною. Використовується невелика кількість (9 байт) інформації для математичної моделі ідентифікації, що забезпечує зберігання великого обсягу даних щодо користувачів, для яких потрібно швидко проводити ідентифікацію чи пошук.

Дана система використовує форму та структуру руки для ідентифікації особи та ґрунтується на використанні математичних алгоритмів, які аналізують геометричні параметри руки, наприклад довжину та ширину пальців, відстань між вузькими місцями руки, кут нахилу пальців тощо.

Рисунок 2.5 – Процес ідентифікації за формою руки

Система підтвердження особи за формою кисті руки не може працювати без спеціального пристрою – сканера, який зчитує параметри руки та порівнює їх з

вже збереженими даними. Дані можуть зберігаються у вигляді цифрової моделі руки або у вигляді шаблону, що містить ключові параметри руки.

Як перевагу даної технології ідентифікації можна назвати високу точність ідентифікації, надійність та швидкість роботи системи, а також можливість її використання в умовах, коли інші методи ідентифікації можуть бути недоступні або неефективні, наприклад, коли вимагається ідентифікація в руху або в умовах низької освітленості.

Однак, ця технологія може мати свої недоліки та обмеження, такі як нестабільність результатів при зміні форми руки, поганий розпізнавання в разі наявності травм або інших дефектів на руці тощо.

2.2.4 Системи ідентифікації за будовою ока

Системи ідентифікації за будовою ока базуються на біометричному аналізі окоміркування, форми зіниці, радужки, текстури, кольорових плями та зморшок. Ці системи широко використовуються в різних сферах, включаючи безпеку, медицину, фінанси та технології.

Для ідентифікації особи системи сканують око та збирають детальну інформацію про його форму, розташування, розмір та інші параметри. Одержані дані порівнюються з тими даними, що зберігаються в БД, для визначення особи.

Технологія ідентифікації особи за допомогою аналізу сітківки ока [24] використовує інфрачервоне світло низької інтенсивності, що направляється крізь зіницю до кровоносних судин задньої стінки ока. В таких системах зареєстровані користувачі мають нижчий відсоток помилок і практично завжди отримують доступ до IP об'єкта. Чіткість зображення райдужної оболонки є ключовим аспектом для успішної ідентифікації, але також може бути використаний і малюнок кровоносних судин, які добре відображаються під час освітлення зіниці ока за допомогою зовнішнього джерела світла.

Для ідентифікації особи шляхом сканування сітківки ока (рисунок 2.6), необхідно, щоб особа дивилася на віддалену світлову точку через спеціальний окуляр, при цьому застосовуються інфрачервоні промені для освітлення ока та виділення мережі кровоносних судин. Потім ця мережа порівнюється з еталоном.

Рисунок 2.6 – Процес розпізнавання шляхом сканування сітківки ока

Розглянута технологія ідентифікації є дороговартісною, проте є трудомісткою та має невисоку пропускну здатність, тобто відсутня можливість обробки великої кількость запитів за короткий період часу та працювати з значною кількістю користувачів одночасно. Однак її надійність в рази перевищує інші методи. Вона комбінує найкращі особливості ідентифікації по венозному малюнку та ключовими точками райдужної оболонки, щоб досягти більш точного та надійного результату.

Основною перевагою систем ідентифікації за будовою ока є висока точність ідентифікації, оскільки очі є унікальними для кожної особи і майже неможливо підробити дані ока. Однак, існують деякі недоліки цієї технології, такі як нестійкість до змін міміки, освітлення та інших факторів, що можуть вплинути на точність ідентифікації. Також, ідентифікація може бути ускладнена за наявності очних захворювань або травм.

В результаті проведеного аналізу технологій ідентифікації людини за біометричними характеристиками для АСК доступу до ІР, запропоновано використання багатофакторної ідентифікації для проектованої сиситеми, що є мультимодальним рішенням, та складатиметься з двох характеристик:

- розпізнавання зображення обличчя;
- голосова ідентифікація.

Для того, щоб дати оцінку стосовно точності роботи АСК [25] використовуються характеристичні криві, зокрема крива характеристики роботи приймача – ROC або крива залежності помилок виявлення від порогового

значення рішення – DET. Вони дозволяють визначити оптимальні значення порогу для біометричної системи на основі співвідношення між двома типами помилок: FRR – частотою помилкового відхилення та FAR – частотою помилкового прийняття. Таке рішення також можна оцінити за допомогою DET–кривої (рисунок 2.7).

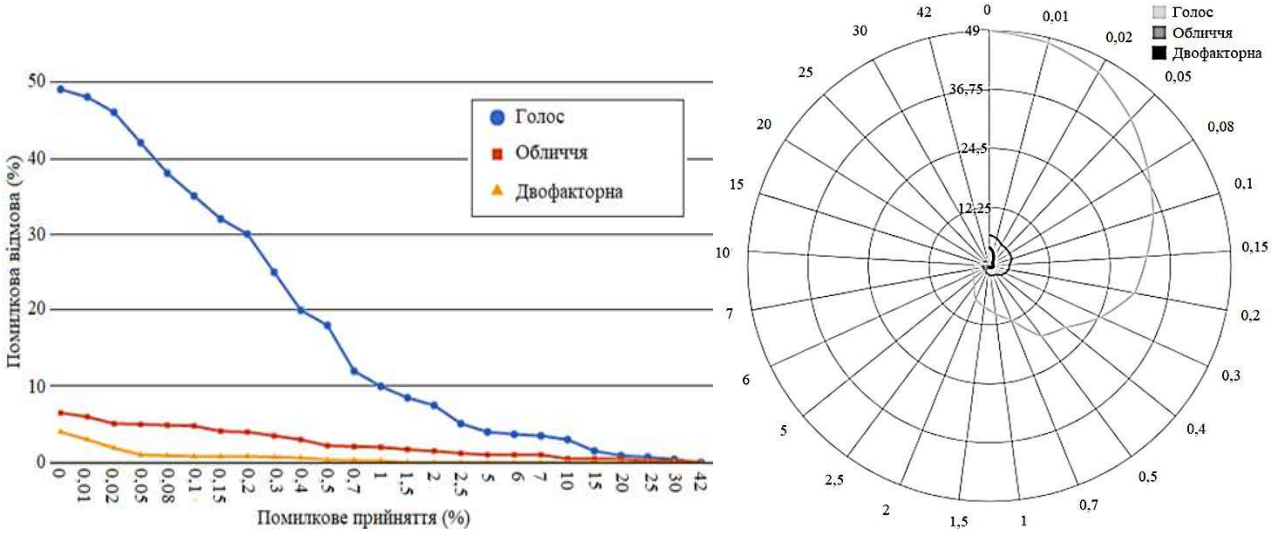

Рисунок 2.7 – Оцінка точності роботи АСК

Ідентифікація може бути здійснена за рисами обличчя у РРЧ, коли особа підходить до пристрою, обладнаного камерою. Для того, щоб зареєструватися, та в подальшому для ідентифікації, потрібно лише три зображення. При реєстрації особи для ідентифікації за голосом потрібно повторити статичну парольну фразу декілька разів. Це робиться з метою досягнення максимальної надійності та визначення варіативності вимови.

Таке рішення (мультимодальне) базується на об'єднанні результатів голосової та ідентифікації за ознаками зовнішності, що передбачає використання математичних ймовірностей схожості еталонного зразка (ЕЗ) користувача в обох модулях.

Для розрахунку мультимодальної ймовірності ідентифікації використовуються значення ймовірностей голосової та лицевої ідентифікації, отримані на основі аналізу вхідного аудіо/відеопотоку. При прийнятті рішення щодо надання доступ користувачу, системою ідентифікації враховуються результати кожного з модулів.

2.4 Побудова математичної моделі ідентифікації

Математичною моделлю (ММ) ідентифікації користувачів в інформаційних системах [21] є комплекс алгоритмів та методів, що забезпечують ідентифікацію користувача та перевірку його доступу до системи. Для цього використовуються такі характеристики, як логін та пароль, ідентифікатор сесії, IP–адреса, відбиток пристрою тощо. Зазвичай така ММ включає трих основні етапи: аутентифікація – полягає в перевірці ідентифікатора користувача та його пароля; авторизація – виконується, в результаті успішного проходження попереднього етапу користувачем, перевірка права доступу до ресурсів та проведення операцій; аудит відповідає за фіксацію дій користувачів в системі з метою забезпечення надійного захисту та перевірки дотримання правил користування.

ММ є ключовим елементом АСК ВД для ідентифікації користувачів. Правильно розроблена модель може запобігти НСД до системи, злому акаунтів та крадіжці даних користувачів. ММ включає набір алгоритмів та методів, які дозволяють здійснити ідентифікацію користувача та перевірити його доступ до системи. Це здійснюється за допомогою таких параметрів, як логін та пароль, ідентифікатор сесії, IP-адреса, відбиток пристрою та інші.

Для забезпечення високої ефективності й точності ідентифікації користувачів в АСК доступу враховуються різні біометричні параметри, наприклад відбитки пальців, риси обличчя, характеристики очей, голосу тощо, оскільки кожен користувач системи має унікальний набір цих параметрів, що використовуються для його ідентифікації. При проектуванні АСК ВД на основі біометричної ідентифікації, необхідно враховувати кількість параметрів, які використовуються для ідентифікації кожного користувача.

Нехай ми маємо n відмінних параметрів людини, тоді для ми повинні їх набір зберегти для кожного користувача. У таблиці 2.1 наведено приклад кількості параметрів P_i, які притаманні одній людині H_j, що використані при розробці ММ ідентифікації користувачів та перевірки доступу користувачів до системи. Враховуючи ці параметри, система може забезпечити високий ступінь безпеки та захисту особистих даних користувачів.

Таблиця 2.1 – Параметри математичної моделі

Персонал, m	Біометричні параметри людини, n				Мінімальна норма для доступу
	P_1	P_2	…	P_n	
L_1	x_{11}	x_{12}	…	x_{1n}	d_1
L_2	x_{21}	x_{22}	…	x_{2n}	d_2
…	…	…		…	…
L_m	x_{m1}	x_{m2}	…	x_{mn}	d_k

Для реалізації даної задачі необхідно визначити множину користувачів H та їхні біометричні параметри P. Крім того, потрібно встановити мінімальну норму для доступу d_k, яка відповідатиме рівню безпеки кожного користувача окремо.

При цьому система обмежень визначатиметься наступним чином: сума значень біометричних параметрів кожного користувача має бути не меншою за мінімальну норму для доступу d_k. Тобто, якщо X – кількість біометричних параметрів однієї людини, то умова обмежень буде наступною:

$$P_1 + P_2 + \cdots + P_x \geq d_k.$$

Крім того, значення c_r системи можна оцінити за формулою:

$$c_r = \sum (c_i \cdot Y_i),$$

де c_i – значення одного біометричного параметра, а Y_i – кількість параметрів, які використовуються для ідентифікації кожного користувача.

Система обмежень матиме вигляд:

$$\begin{cases} x_{11} + x_{12} + \ldots + x_{1n} \geq d_1 \\ x_{21} + x_{22} + \ldots + x_{2n} \geq d_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_{m1} + x_{m2} + \ldots + x_{mn} \geq d_k \end{cases}$$

$$x_{ij} \geq 0, \text{де } i, j = \overline{1, n};\ d_i \geq 0, \text{де } i = \overline{1, k};$$

Мінімум цільової функції визначається виразом:

$$F(X) = c_1 x_1 + c_2 x_2 + c_r x_n \rightarrow min$$

Таким чином, введені змінні для невідомих параметрів X у задачі та встановлено обмеження на їх значення $x_{ij} \geq 0, \text{де } i, j = \overline{1, n};\ d_i \geq 0, \text{де } i = \overline{1, k}$. Створена система обмежень для задачі щодо мінімальної норми доступу dk та

визначено цільову функцію з екстремумом:

$$F(X) = c_1x_1 + c_2x_2 + c_rx_n \rightarrow min.$$

Наведена модель це задача лінійного програмування. Вона має лінійну цільову функцію та лінійні обмеження, тому можна застосувати алгоритми лінійного програмування для її розв'язання.

Цільова функція має вигляд:

$$F(X) = c_1x_1 + c_2x_2 + \cdots + c_rx_n,$$

де x_i – це кількість *i*–го біометричного параметра, а c_i – вартість одиниці і–го параметра. Метою є мінімізувати цю функцію, тобто знайти таке значення хі для кожного *i*, яке забезпечить мінімальну вартість системи.

Обмеження на параметри x_{ij} мають вигляд: $x_{ij} \geq 0$, де $ij = 1,2, \dots, n$. Ці обмеження вказують на те, що кількість кожного біометричного параметра не може бути від'ємною. Також є обмеження на мінімальну норму для доступу $d_j \geq 0$, де $i = 1,2, \dots, k$. Ці обмеження вказують на те, що для кожного зі користувачів понна задаватися норма мінімуму для доступу, яка не має бути від'ємна. Отже, ми отримали задачу лінійного програмування з цільовою функцією $F(X)$ та лінійними обмеженнями $x_{ij} \geq 0$ та $d_j \geq 0$. Вирішення даної задачі є важливий для забезпечення контролю ВД та інформаційної безпеки.

Двофакторна статично–динамічна біометрична ідентифікація за голосом та рисами обличчя базується на перетворенні біометричних параметрів особи у вектор V. Цей вектор представляється у *N*–мірному ортогональному просторі.

$$V = \{v_1, v_2, \dots v_j, \dots v_N\} j = \overline{1, N}.$$

Для того, щоб додати нового користувача до системи на основі наданих зразків створюється біометричний еталон особи у вигляді векторів V_v – голос та V_f – обличчя. При наступних спробах ідентифікації, людиною надаються її біометричні параметри вектором V, і система за її ідентифікатором викликає відповідні ЕЗ V_v та V_f з БД зареєстрованих користувачів. За допомогою порівнювання отриманого вектора V з еталонами V_v та V_f, система здійснює процедуру автентифікації користувача, що може здійснюватися за допомогою різних моделей.

2.5 Розробка структури проектованої системи

Після того, як користувач надіслав свої біометричні дані системі, вони були оброблені та порівняні з вже наявними в БД еталонами. За результатом порівняння система вирішує, чи можна допустити користувача до системи, чи ні. Якщо біометричні характеристики користувача відповідають ЕЗ, то система надає йому доступ до необхідних ресурсів, інакше – відмовляє в доступі. Запропонована модель системи показана на рисунку 2.8.

Рисунок 2.8 – Схема ідентифікації користувачів

Цей процес має важливе значення щодо забезпечення безпеки IP системи. Біометрична ідентифікація дозволяє визначити особу, яка робить спробу отримати доступ до системи, і підтвердити її право на цей доступ. Таким чином, система захищається від НСД та зловживань, що можуть призвести до витоку важливої інформації та інших проблем.

Стуктура проектованої системи наведена на рисунку 2.9. На рисунку 2.9 позначено:

- блоки датчиків (Д) для отримання зображення та голосу для розпізнавання особи, а також можливе підключення до системи інших датчиків, наприклад стану дверей, руху, розбиття, присутності, зчитувачі, тошо;
- блок оповіщувачів (ОП) для сповіщення про нештатні ситуації, наприклад виконувати функції охорони та пожежної сигналізації;
- виконавчі механізми (ВМ) після порівняння біометричних даних з ЕЗ, допомагають контролеру системи (К) прийняти рішення щодо допуску

користувача до інформаційних ресурсів або відмовити у доступі.;

- базу даних (БД) ЕЗ для порівняння з отриманими даними для ідентифікації та авторизації користувачів;

- протоколи обміну інформацією забезпечують зв'язок між різними елементами системи АСК;

- блок обробки даних забезпечує обробку даних, які отримані від блоків датчиків та ВМ, зокрема аналіз зображень обличчя та голосу для визначення біометричних даних користувача, порівняння отриманих біометричних характеристик з ЕЗ в БД, формування результатів обробки даних та передача їх до контролера для подальшої обробки та прийняття рішення;

- головний та резервний сервери інформаційних ресурсів головний та резервний сервери ІР забезпечують надійну та безперебійну роботу системи, збереження резервних копій даних та їх відновлення в разі втрати. Вони також забезпечують доступ до інформаційних ресурсів для користувачів системи та здійснюють КД та аудит дій користувачів;

- територіально розподілені автоматизовані робочі місця.

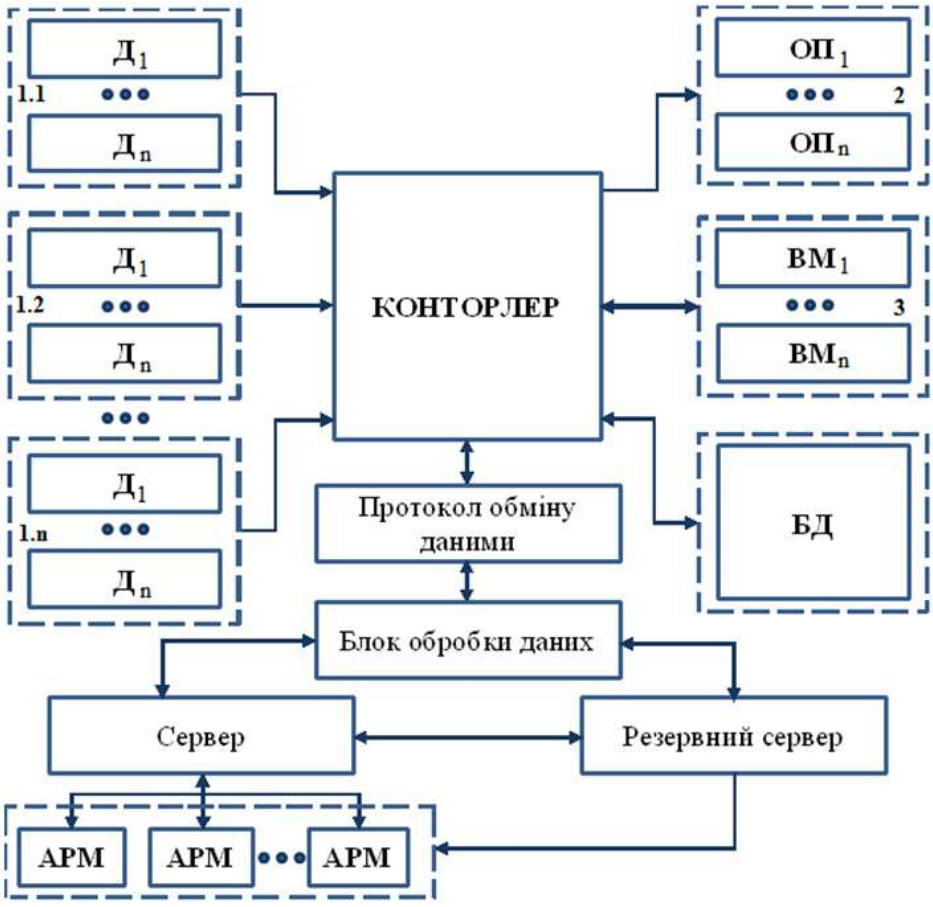

Рисунок 2.9 – Стуктура АСК відаленого доступу

Головний сервер забезпечує зберігання та обробку інформації про користувачів, права доступу до IP, а також здійснює обробку біометричних даних для прийняття рішень щодо доступу користувачів до ресурсів. Резервний сервер виступає як резервне копіювання головного сервера та забезпечує безперебійну роботу системи в разі відмови головного сервера.

В теорії автоматичного управління (ТАУ) [26], така АСК є системою з типовим нелінійним контуром управління та може описуватися набором інтегруючих та диференціюючих ланок з аперіодичною ланкою і передавальними функціями $W_j(p)$, з припщенням деяких умови. У контексті АСУ, такі ланки можуть бути характеризовані як комплекси засобів автоматизації та осіб управління з функціями формування керуючих впливів $W_{\text{КВ}}(p)$, органів та засобів оцінки поточного стану $W_{\text{ПС}}(p)$, виконавчі механізми об'єкта управління $W_{ОУ}(p)$ та засоби збору даних про стан керованих об'єктів $W_{\text{Д}}(p)$ $W_{СД}(p)$).

Передавальна функція безперервної системи $W(p)$ в ТАУ описує відношення перетворення Лапласа між вихідним сигналом $y(t)$ та вхідним сигналом $g(t)$, при нульових початкових умовах. Ця залежність зазвичай описується системою диференціальних рівнянь або матрицею коефіцієнтів, і дозволяє отримати зображення вихідного сигналу системи на основі відомого зображення її вхідного сигналу, за виразом:

$$y(t) = W(p) \cdot g(t).$$

Передавальна функція $W(p)$ є інструментом для оцінки різних властивостей досліджуваної системи, зокрема стійкості, чутливості, ступеня астатизму та характеристики частоти та амплітуди в стаціонарному та перехідному режимах. Для отримання передавальної функції системи в цілому, передавальні функції окремих ланок об'єднуються у відповідності до певних правил (рисунок 2.10).

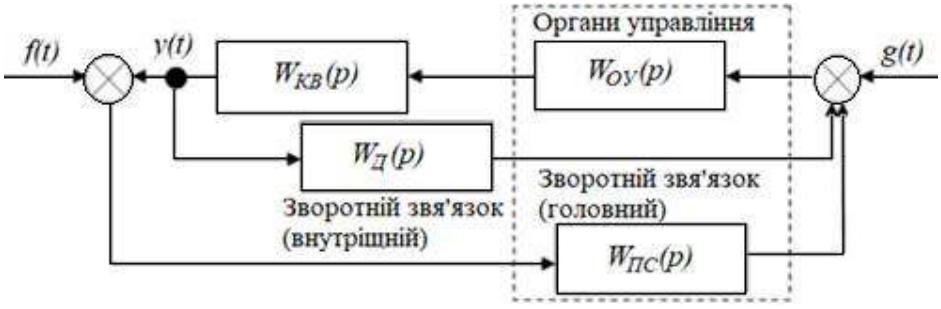

Рисунок 2.10 – Передавальні ланки АСК

На практиці виявляється, що при аналізі особливостей окремих компонентів системи, передавальна функція системи в цілому може бути незручною. У випадках дослідження автоматизованих органів управління, більш зручною для оцінки керованості системи в цілому є передавальна функція розімкнутої системи, яка включає тільки компоненти органів управління та зворотнього зв'язку. Ця передавальна функція забезпечує оцінку функціонування системи в цілому, за винятком її стійкості. Структура розімкнутого контуру системи органи управління – середовище – об'єкт управління, що включає тільки компоненти органів управління, зображена на рисунку 2.11.

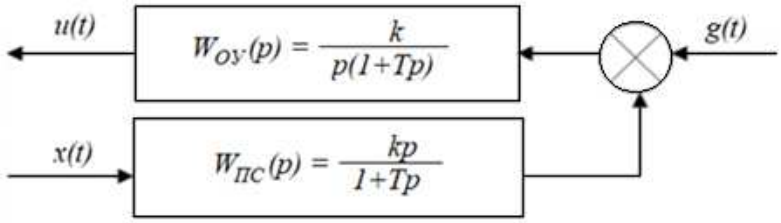

Рисунок 2.11 – Структура розімкнутого контуру

Для спрощення дослідження функціонування системи, при формуванні цієї структури приймається ідеально функціонуюча система збирання даних про стан керованого об'єкта, тобто зі значенням функції $W_{ПС}(p)$ близькою до одиниці.

2.6 Алгоритм ідентифікації за голосом

В сучасному світі ідентифікація за голосом [27–29] є актуальною проблемою, і для її вирішення застосовуються різні алгоритм, однак, використання багатьох з них потребує значних обчислювальних ресурсів, що ускладнює їх застосування в мобільних пристроях та інших обмежених середовищах. Тому відбувається, пошук більш ефективних та оптимізованих методів для ідентифікації за голосом.

Попри це, певні алгоритми є достатньо простими для реалізації їх за допомогою електронних пристроїв, оскільки на кожній з ітерацій виконується невелика кількість операцій. Такі алгоритми пропонуються у якості альтернативи до існуючих методів для розпізнавання голосу в режимі реального часу (РРЧ), особливо у випадках, коли обмеженість обчислювальних ресурсів є серйозною

проблемою. В цілому, розробка ефективних та оптимізованих методів ідентифікації за голосом може покращити безпеку та зручність використання електронних пристроїв та систем.

При вирішенні задач щодо ідентифікації особистості шляхом розпізнавання мови використовуються різні моделі, але однією з основних є моделі з прихованими моделями Маркова (HMM). В таких моделях процес описується набором кінцевих станів, що змінюються у довільному напрямку, але який можна статистично прогнозувати (рисунок 2.12).

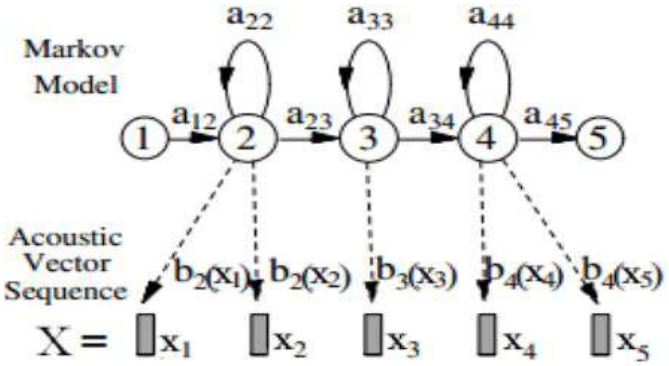

Рисунок 2.12 – Прихована модель Маркова

В основі таких підходів лежить припущення, що мова може розбиватися на деякі сегменти – стани, всередині кожного з яких голосовий сигнал може розглядатися стаціонарним. Такі моделі передбачають миттєвий перехід між станами та те, що ймовірність символів спостереження буде залежати тільки від поточного стану моделі та буде не залежна від попередніх символів. Незважаючи на те, що жодне із названих припущень не будуть повністю справедливим для мовного сигналу, для великого числа автоматизованих систем аудіорозпізнавання HMM є основою.

Метод SVM – опорних векторів – це алгоритм машинного навчання, який використовують для класифікації та регресії. Завданням є пошук оптимальної гіперплощини, що розділяє дані на дві частини різного класу (рисунок 2.13).

Оптимальна гіперплощина – це та, яка забезпечує максимальний проміжок між точками кожного класу (margin), тобто мінімізує кількість помилок класифікації. Опорні вектори – це точки, що лежать на границі проміжку між класами або найближчі до нього точки. SVM є досить ефективним методом для

класифікації, навіть якщо кількість ознак дуже велика, а кількість прикладів досить мала.

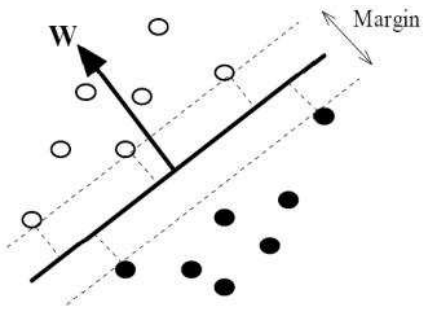

Рисунок 2.13 – Метод опорних векторів

Також він здатний працювати з нелінійними зв'язками між ознаками, використовуючи так зване ядро, що перетворює ознаки в більш високорозмірний простір. SVM використовується у багатьох задачах, включаючи розпізнавання образів, розпізнавання мови, біоінформатику, аналіз даних тощо.

Метод SVM може застосовуватися в задачах розпізнавання голосу для класифікації голосових зразків на два класи: голос особи, яку необхідно ідентифікувати, та інші голоси. Для цього потрібно підготувати набір даних, який включає голосові зразкіи, які належать цим двом класам. На основі цього набору будується модель SVM, яка дозволяє класифікувати нові голосові зразки. Наприклад, голосовий сигнал буде попередньо оброблений та перетворений у векторну форму, а потім використаний у якості вхідних даних для моделі SVM.

Процес опрацювання хвилі звуку наведений схематично на рисунку 2.14.

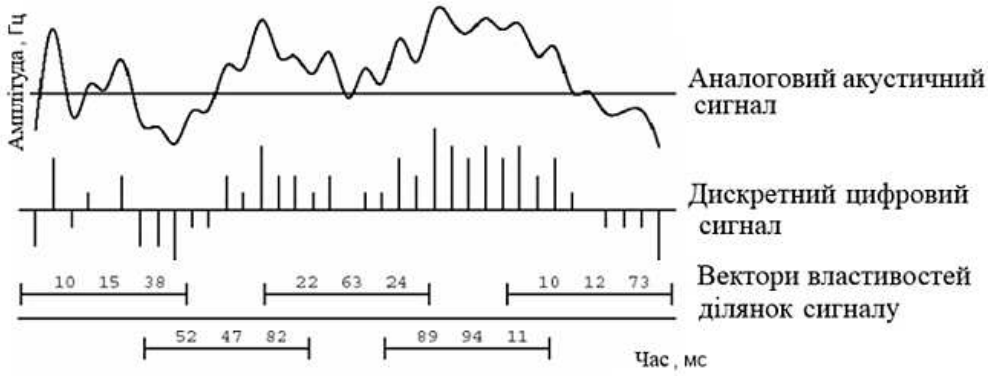

Рисунок 2.14 – Етапи опрацювання звукових хвиль

Цифрова система для опрацювання звукового сигналу в контексті розпізнавання голосу передбачає не тільки перетворення мовного сигналу з

аналогового у цифровий вигляд (АЦП), але і подальшу його обробку використовуючи методи машинного навчання. Для ефективної роботи звуковий сигнал повинен бути коректно представлений у цифровому вигляді, тому важливим є забезпечення якісної дискретизації та квантування сигналу.

Процес дискретизації передбачає розбиття аналогового сигналу на відрізки часу та отримання чисельних значень, що характеризують сигнал у кожній точці. Частота дискретизації визначає, скільки відліків отримується за одну секунду. Чим вищою є частота дискретизації, тим точнішим буде представлення у цифровій формі звукового сигналу.

Процес квантування передбачає визначення точності, з якою представлено чисельне значення сигналу. Квантування дозволяє обмежити кількість можливих значень для кожного відліку та зменшити обсяг зберігання даних. Точність представлення звукового сигналу залежатиме від ширини діапазону одержуваних чисел.

Для цифрової обробки аналогового акустичного сигналу з мікрофону використовується процес дискретизації та квантування за допомогою АЦП. Це дозволяє отримати цифровий запис вимови кодового слова або звуків як послідовності відліків голосового сигналу $\{S_k\}$. Щоб покращити обробку та класифікацію, реалізацію слова (звуку) розбивають на послідовність кадрів $\{X_i\}$. Кожен кадр X складається з послідовності відліків голосового сигналу $S_1, S_2, S_3, \dots, S_n$, довжина якої становить N.

Кадри мають фіксовану в часі довжину, наприклад, коли N=100, а частота дискретизації рівна 8000Гц, кадр триватиме 12,5мс. Зазвичай кадри зміщуються один відносно одного для того, щоб уникнути втрати інформації на межі кадрів. Крок даного зміщення визначається кількістю звукових відліків між початком наступних кадрів.

Якщо крок зміщення буде меншим за довжину кадру N, то кадри будуть перекриватися між собою, що дозволяє не втрачати інформацію на їх кордонах. Для вирішення різних задач, наприклад розпізнати слова, мову чи ідентифікувати особу, кожному з кадрів ставлять у відповідність вектор властивостей або ознак. Цей вектор *RM* може містити набір функцій або бути однією функцією.

Задачею розпізнавання голосу є визначення того класу, до якого належить кожне з слів, які поступили на вхід системи. Для покращення результатів класифікації можуть використовуватись різноманітні методи перед–опрацювання даних, включаючи фільтрацію шуму та згладжування сигналу. На рисунку 2.15 наведений приклад амплітудно–частотної діаграми чистого сигналу. Однак, точність розпізнавання може бути погіршена різними чинниками, такими як стан мовця, шум оточуючого середовища, швидкість вимови фраз тощо.

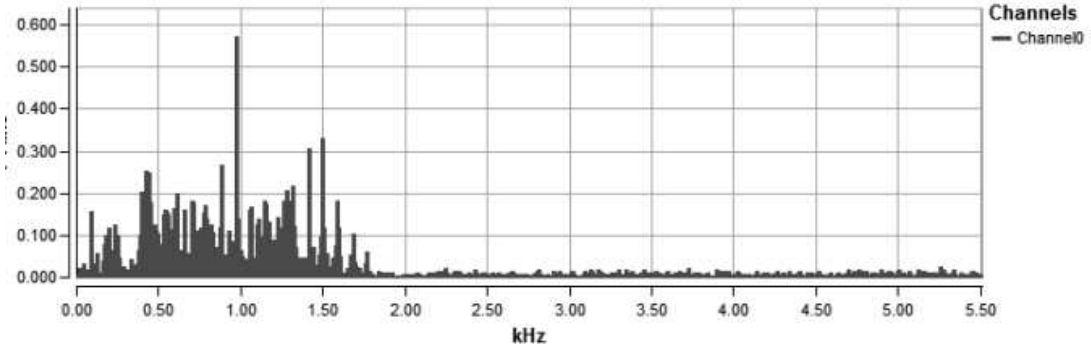

Рисунок 2.15 – Чистий сигнал

Записати чистий сигнал, без сторонніх шумів, дуже складно. На рисунку 2.16 представлено амплітудно–частотну діаграму чистого сигналу, з рисукну 2.15, із додаванням білого шуму, що характеризуються різночастотними звуковими коливаннями в рівній мірі представлені, тобто приблизно однаковою є середня інтенсивність звукових хвиль на різних частотах.

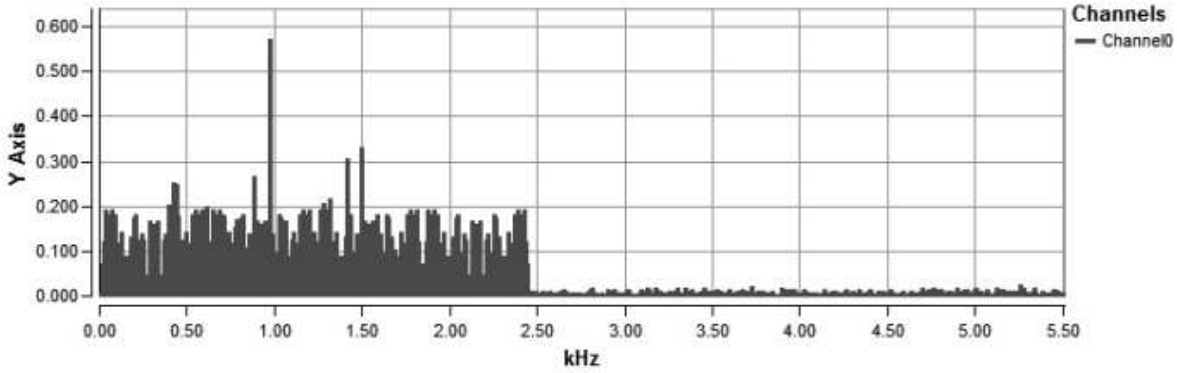

Рисунок 2.16 – Сигнал з білим шумом

З рисунків 2.15 та 2.16 видно, що зашумлений сигнал має відмінності від чистого сигналу. Щоб зменшити негативний вплив шуму, використовують спеціальні частотні фільтри. Ці фільтри забезпечують відбір частот зі звукового

сигналу, які знаходяться в заданій смузі пропускання, та відкидають інші частоти.

Однак, існують різні типи сторонніх шумів, таких як шум вітру, шум машин, шум побутових пристроїв та інші, які можуть ускладнити завдання розпізнавання звуків та збільшити кількість помилок. Для покращення точності розпізнавання звуків необхідно розробляти ефективні методи попередньої обробки сигналу, які дозволяють виділяти корисну інформацію та видуляти сторонні шуми. В проектованій АСК спектральний аналіз голосу виконуватиметься за допомогою швидкого перетворення Фур'є, адже це забезпечує значне зменшення часу розрахунків шляхом скорочення кількості операцій множення, що необхідні для аналізу кривої.

2.7 Алгоритм розпізнавання обличчя

Для проведення тестування ефективності алгоритмів виділення обличчя обрано три різні алгоритми, які реалізовано на БД, що включали набір зображень з обличчями:

- boosting – розроблений П. Віолою та М. Джонсом, заснований на поєднанні багатьох слабких класифікаторів в один сильний класифікатор за допомогою ваг та послідовного навчання;
- SNoW – застосовується для вирішення задач, де важлива точність прогнозування при невеликій кількості вхідних ознак задач класифікації, зокрема, для розпізнавання зображень, обробки природних мов, відновлення сигналів;
- SVM – використовується для класифікації і регресії, а також застосований в інших областях, таких як комп'ютерний зір, біоінформатика, тощо.

Метод бустінгу є важливим для розпізнавання в РРЧ певних об'єктів на зображеннях. Його суть полягає у використанні зображень в інтегральному вигляді для швидкого обчислення необхідних об'єктів та використанні ознак Хаара для пошуку потрібного об'єкта (у даному випадку – обличчя).

Метод використовує бустінг для відбору оптимальних ознак для об'єкта, пошук якого проводиться на зображенні. Ці ознаки поступають на вхід класифікатору, який повертає результат «вірно» або «невірно». Для підвищення

швидкості пошуку вікна, у яких не знайдені обличчя відкидаються використовуючи каскади ознак. Даний метод широко застосовується в сфері обробки зображень та ефективний для розпізнавання облич, зокрема в системах безпеки, медицині та робототехніці.

SNoW базується на алгоритмі Winnow і використовується для розробки «розріджених» (sparse) моделей нейронних мереж, тобто моделей зі значно меншою кількістю вагових коефіцієнтів в порівнянні з традиційними нейронними мережами. Це дозволяє економити пам'ять та підвищувати швидкодію обчислень.

У SNoW кожен вхідний сигнал множиться на ваговий коефіцієнт, і результат вагового додавання обробляється функцією активації. Якщо результат більший від заданого порогового значення, тоді вхідний сигнал вважаєтиметься таким, що належить до даного класу, інакше – ні. У SNoW кожен нейрон відповідає за класифікацію одного з об'єктів. Він дозволяє автоматично відбирати найбільш інформативні ознаки за допомогою «вікна» або порогової межі, яка обчислюється для кожної ознаки.

SNoW є спеціально розробленою архітектурою мережі просівальних елементів, що використовується для виявлення обличчя. Мережа має два шари: вхідний та вихідний. У вхідному шарі кожен вузол відповідає за характеристику вхідного зображення та генерує 1 при наявності особливості і 0, якщо її немає. У вихідному шарі ткаож є 2 вузли, кожен із яких відповідає за клас зображень («обличчя» / «не обличчя»). Характеристики зображення визначаються за значеннями середньої яскравості та дисперсії в кожному прямокутному фрагменті зображення. Зображення розміром 20×20 пікселів, що дозволяє отримати простір ознак розміром 135424. При класифікації до вхідних вузлів надходить інформація стосовно наявності на зображенні певних характеристик. Вузлами вихідного шару обчислюється лінійна комбінація сигналів, що генеруються вхідними вузлами, а значення зв'язків між вхідними і вихідними вузлами задаються коефіцієнтами лінійної комбінації. У випадку перевищення заданого порогу вирішується, чи присутнє на зображенні обличчя.

Аглоритм SVM є ефективним інструментом для зменшення кількості ознак у тренувальному наборі об’єктів без значної втрати інформації. Використання до

набору векторів у лінійному просторі методу головних компонент дозволяє перетворити його до такого базису, де основна дисперсія буде спрямована уздовж кількох головних осей. Такий підпростір є оптимальним, оскільки найкращим чином зображує тренувальний набір.

Суть SVM при виявленні особи зводиться до пошуку гіперплощини у просторі ознак, яка відокремлює зображення облич від інших зображень. Оскільки зображення облич людини та не облич мають складний клас, то можливість їх лінійного розділення є низькою. Після роботи системи виділення облич можуть виникнути два види помилок: обличчя не виділене та помилкове виділення обличчя. Відповідно є два основні параметри, які визначають ефективність: рівень виявлення, який відображає їх відсоток, та рівень хибного виявлення – загальне число помилок у наборі, який тестувався.

Різні алгоритми виділення облич мають різний розмір діапазону виділення. Алгоритм на основі бустінгу захоплює повністю обличчя, включаючи лоб, бороду, щоки. У алгоритмах онові SNoW і SVM виділяються лише центр обличчя, тобто очі, рот, ніс. Різниця в розмірі виділеного обличчя виникає через використання різних наборів навчальних зображень при побудові класифікатора. У першому випадку більш точно відображається реальний розмір обличчя.

На рисунку 2.17 зображено наскільки залежить рівень виділення від імовірності імпульсного шуму.

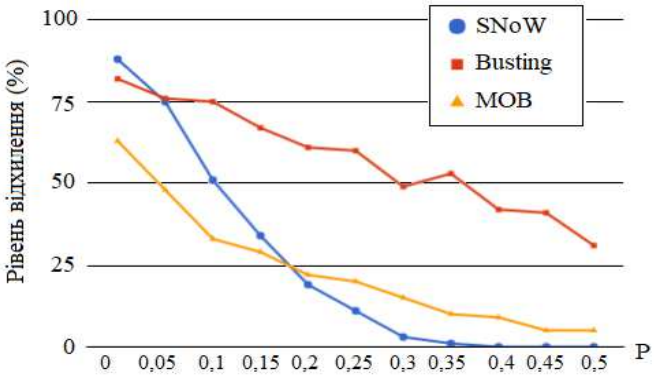

Рисунок 2.17 – Вплив ймовірності імпульсного шуму на рівеньвиділення

Зображення може також бути розмите, і ступінь розмиття визначається використовуючи універсальний індекс якості (УІЯ), який. приймає значення 1 для вихідного зображення і наближається до нуля для сильно розмитого зображення.

Зрізання розмиття зображення не має значного впливу на рівень виділення обличчя, у порівнянні з додаванням шуму (рисунок 2.18).

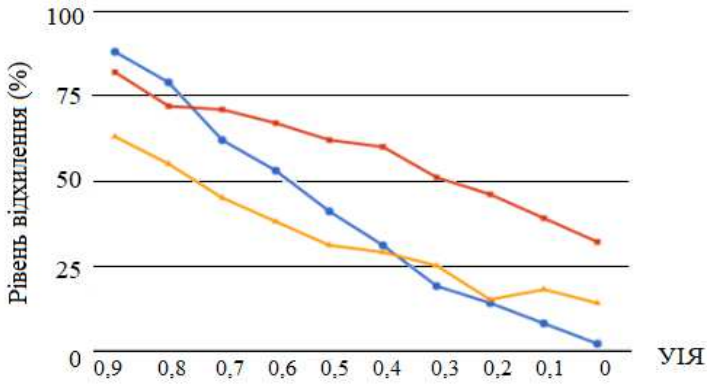

Рисунок 2.18 – Взаємозв'язок між рівнем виділення та ступенем розмиття

Зміна значень УІЯ в межах 1–0,7 призводить до зменшення рівня виділення до 10% для тестованих алгоритмів. Лише при сильному розмитті рівень виділення обличчя відбувається скорочується.

Оскільки алгоритми засновані на SNoW і SVM використовують лише деякі частини зображення (очі, ніс, рот) для виявлення обличчя, тому при розмитті зображення вони можуть помилково виявляти обличчя у зоні, де воно насправді відсутнє. Проте, алгоритм на основі бустінгу використовує більш широкий діапазон ознак для виявлення обличчя, тому є менш вразливим до невеликого розмиття зображення.

Проте при сильному розмитті зображення всі алгоритми показують значне спадання рівня виділення обличчя. Оскільки, при сильному розмитті зображення стає менш чітким і менш інформативним, що ускладнює виявлення обличчя. навіть для алгоритмів, що використовують широкий діапазон ознак. Тому, алгоритм оснований на бустінгу, що показує кращі результати при слабкому розмитті зображення, при сильному розмитті може бути недостатньо ефективним.

Ефективним інструментом для виділення границь на зображеннях, особливо у випадках, де потрібно визначити напрямок і силу зміни яскравості на площині зображення є оператор Собеля. Оскільки він базується на дискретному диференціальному підході, він може давати грубі результати на високочастотних ділянках зображення. Використовуючи малий сепарабельний фільтр у вертикальному та горизонтальному напрямках, оператор Собеля розраховує

наближене значення градієнта або норми градієнта для кожного пікселя зображення (рисунок 2.19). Хоча він не дає точного значення градієнту кожного пікселя, все ж таки забезпечує швидке та ефективне визначення границь на зображеннях.

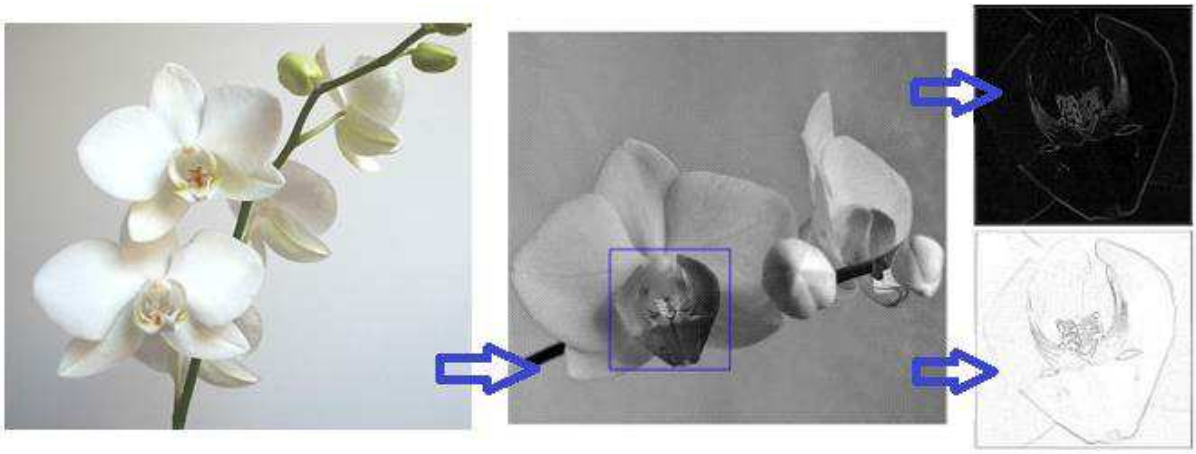

Рисунок 2.19 – Процес створення ЕЗ для ідентифікації об’єкта

Для апроксимації часткових похідних застосовують скінченні різниці, оскільки значення функції на зображенні існують тільки на регулярній сітці. Це дозволяє знаходити наближені значення градієнту кожного пікселя зображення, які використовуються для виділення границь. Даний оператор є одним із найбільш поширених та використовується в різних областях для розпізнавання зоьражень.

«Фільтр Собеля є дискретним диференціальним оператором, який заснований на згортці зображення сепарабельними цілочисельними фільтрами в вертикальному та горизонтальному напрямках» [30]. Він має перевагу перед фільтрами Лапласа, а саме – меншу чутливість до шуму на зображенні. В результаті його застосування (рисунок 2.19), лінії границь не будуть настільки гранульовані, що може покращитсть якість обробки зображення.

3. РЕАЛІЗАЦІЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ ДО ІНФОРМАЦІЙНИХ РЕСУРСІВ

3.1 Алгоритм створення еталонного зразка

Застосування універсального алгоритму роботи із будь–якими об’єктами, заснованого на пропозиціях для покращення існуючих методів оримання ЕЗ, може значно спростити процес обробки зображень та зробити ефективнішим. Результати такого алгоритму наведено на рисунку 3.1.

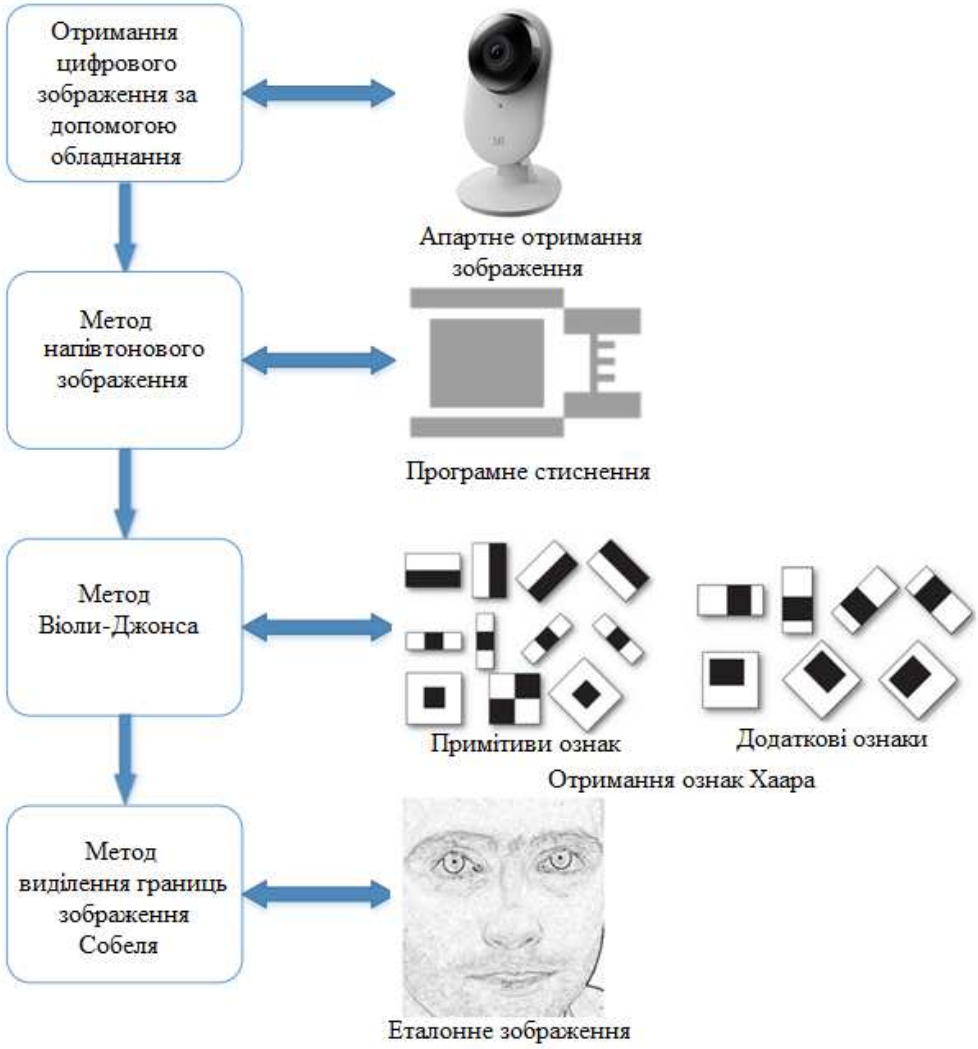

Рисунок 3.1 – Створення еталонного зразка

Після отримання цифрового зображення, використано метод напівтіньового зображення, щоб скоротити розмір зображення та підвищити його якість. Далі використано метод Віоли–Джонса, який базується на каскадному класифікаторі і

забезпечує точне виявлення обличчя на зображенні. Крім того, для виділення границь на зображенні використовувався фільтр Собеля, що зменшує гранулювання та чутливість до шумів зображення у порівняння з іншими фільтрами.

Після проведення зазначених дій, отримано ЕЗ зображення роздільна здатністю якого становить 500×500 пікселів, а розмір – 150кБ, що є оптимальним для зберігання в сучасних БД. Такий ЕЗ забезпечує точну та швидку ідентифікацію об'єктів на зображеннях та може використовуватися в проектованій АСК для ідентифікації осіб та КД.

Однією із найбільш актуальних на сьогоднішній день задач є безпека та конфіденційність, особливо стосовно ідентифікації людини за біометричними характеристиками. Ключовим недоліком даного процесу є ризик витоку даних. У випадку отримання доступу до БД з біометричними ЕЗ зловмисником – змінити їх не вийде, і це викличе значні труднощі. Тому при створенні зразків для забезпечення безпеки і конфіденційності використовується шифрування.

В проектованій АСК забезпечується можливість користувачам системи вибирати свої ЕЗ і здійснювати їх шифрування їх на стороні клієнта використовуючи код доступу. Для реалізації використано HTML5 FileReader API [31]. Головне вікно АСК наведене на рисунку 3.2.

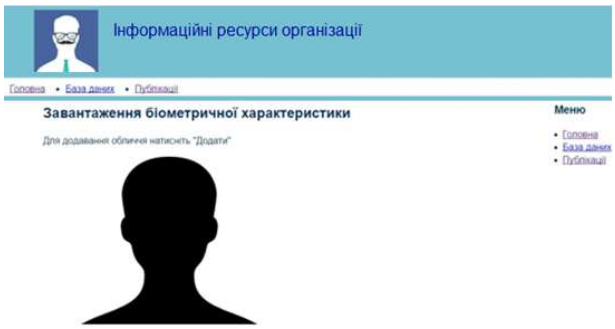

Рисунок 3.2 – Головне вікно системи

В проектованій АСК бібліотека CryptoJS [32] використовується для шифрування ЕЗ біометричних характеристик користувачів на стороні клієнта, що забезпечує їхню безпеку та конфіденційність при передачі через мережу. Це не потребує передачі даних між сервером та клієнтом. Результат шифрування наведено на рисунку 3.3.

```
var CryptoJS=CryptoJS||function(u,p){var d={},l=d.lib={},s=function(){},t=l.Base
={extend:function(a){s.prototype=this;var c=new s;a&&c.mixIn(a);c.hasOwnProperty
("init")||(c.init=function(){c.$super.init.apply(this,arguments)});c.init.
prototype=c;c.$super=this;return c},create:function(){var a=this.extend();a.init
.apply(a,arguments);return a},init:function(){},mixIn:function(a){for(var c in a
)a.hasOwnProperty(c)&&(this[c]=a[c]);a.hasOwnProperty("toString")&&(this.
toString=a.toString)},clone:function(){return this.init.prototype.extend(this)}},
r=l.WordArray=t.extend({init:function(a,c){a=this.words=a||[];this.sigBytes=c!=p
?c:4*a.length},toString:function(a){return(a||v).stringify(this)},concat:
function(a){var c=this.words,e=a.words,j=this.sigBytes;a=a.sigBytes;this.clamp
();if(j%4)for(var k=0;k<a;k++)c[j+k>>>2]|=(e[k>>>2]>>>24-8*(k%4)&255)<<24-8*((j+
k)%4);else if(65535<e.length)for(k=0;k<a;k+=4)c[j+k>>>2]=e[k>>>2];else c.push.
apply(c,e);this.sigBytes+=a;return this},clamp:function(){var a=this.words,c=
this.sigBytes;a[c>>>2]&=4294967295<<
32-8*(c%4);a.length=u.ceil(c/4)},clone:function(){var a=t.clone.call(this);a.
words=this.words.slice(0);return a},random:function(a){for(var c=[],e=0;e<a;e+=4
)c.push(4294967296*u.random()|0);return new r.init(c,a)}}),w=d.enc={},v=w.Hex={
stringify:function(a){var c=a.words;a=a.sigBytes;for(var e=[],j=0;j<a;j++){var k
=c[j>>>2]>>>24-8*(j%4)&255;e.push((k>>>4).toString(16));e.push((k&15).toString(
16))}return e.join("")},parse:function(a){for(var c=a.length,e=[],j=0;j<c;j+=2)e
[j>>>3]|=parseInt(a.substr(j,
2),16)<<24-4*(j%8);return new r.init(e,c/2)}},b=w.Latin1={stringify:function(a){
var c=a.words;a=a.sigBytes;for(var e=[],j=0;j<a;j++)e.push(String.fromCharCode(c
[j>>>2]>>>24-8*(j%4)&255));return e.join("")},parse:function(a){for(var c=a.
length,e=[],j=0;j<c;j++)e[j>>>2]|=(a.charCodeAt(j)&255)<<24-8*(j%4);return new r
.init(e,c)}},x=w.Utf8={stringify:function(a){try{return decodeURIComponent(
escape(b.stringify(a)))}catch(c){throw Error("Malformed UTF-8 data");}},parse:
function(a){return b.parse(unescape(encodeURIComponent(a)))}},
```

```
[Constructor, Exposed=Window,Worker]
  interface FileReader: EventTarget {
    // async read methods
    void readAsArrayBuffer(Blob blob);
    void readAsText(Blob blob, optional DOMString label);
    void readAsDataURL(Blob blob);
    void abort();
    // states
    const unsigned short EMPTY = 0;
    const unsigned short LOADING = 1;
    const unsigned short DONE = 2;
    readonly attribute unsigned short readyState;
    // File or Blob data
    readonly attribute (DOMString or ArrayBuffer)? result;
    readonly attribute DOMError? error;
    // event handler attributes
    attribute EventHandler onloadstart;
    attribute EventHandler onprogress;
    attribute EventHandler onload;
    attribute EventHandler onabort;
    attribute EventHandler onerror;
    attribute EventHandler onloadend;
  };
```

Рисунок 3.3 – Використання CryptoJS

Це відкрита бібліотека криптографічних алгоритмів, яка забезпечує надійність і безпеку даних. Будучи ПЗ з відкритим вихідним кодом, дозволяє переглянути та аналізувати її код. Простий інтерфейс допомагає швидко

реалізувати шифрування та розшифрування даних. Завдяки використанню передових моделей та передового досвіду забезпечує надійність та безпеку даних.

Алгоритм шифрування AES є надійним та використовується для захисту конфіденційної інформації в багатьох сферах, включаючи урядові, комерційні та особисті цілі. Є симетричним алгоритмом блочного шифрування, отже, один ключ використовується для шифрування і дешифрування даних. Використовуються ключі довжиною до 256 біт, а розмір блоку AES – 128 біт.

Вбудований API в браузерах, інтерфейс HTML5 FileReader дозволяє читати вміст файлів на стороні клієнта без необхідності завантажувати їх на сервер. Це дозволяє реалізувати більш зручний та ефективний інтерфейс взаємодії з файловою системою користувача. Проте, він не дозволяє доступатися до вмісту файлів на стороні сервера, і не може використовуватися для читання файлів, що знаходяться в мережі.

Він не підтримується деякими старішими версіями браузерів, тому потребує перевірки підтримки API від користувача. Рисунок 3.4 ілюструє, які браузери підтримують технологію FileReader API [31].

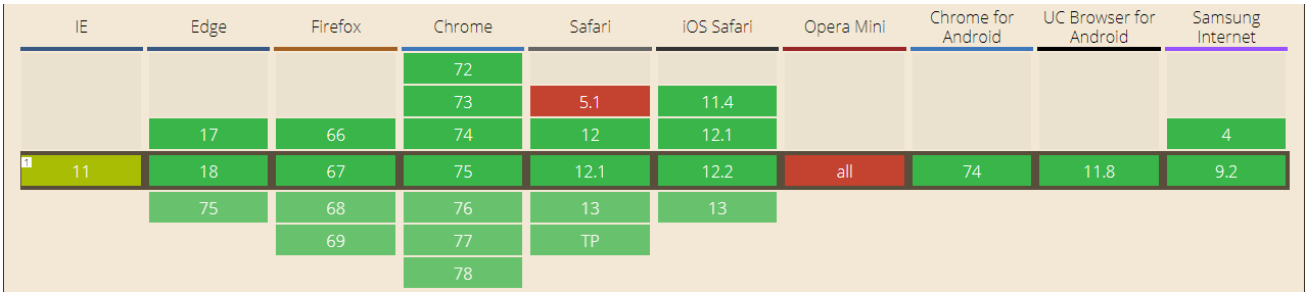

Рисунок 3.4 – Підтримка технології FileReader API

В проектованій АСК даний інтерфейс використовується для зчитування вмісту різноманітних файлів, включаючи тексти, зображення та відео, що може використовуватися також для розробки веб–додатків, які працюють зі змістом файлів на стороні клієнта, таких як редактори зображень або текстові редактори.

Після завантаження файлу ЕЗ біометричних характеристик, він перетворюється у стрічку URI–даних, що дозволяє зберегти його початковий зміст. Далі застосовується шифрування з обраним паролем для збереження файлу у вигляді тексту. При розшифруванні відбувається зворотна процедура. Це

дозволяє зберігати та передавати еталон біометричної характеристики в безпечному форматі.

3.2 Розробка функціональної моделі

Для створення моделі для відображення структури та функцій АСК можна використовувати різні методики графічного представлення, зокрема IDEF0. Ця нотація графічного моделювання дозволяє побудувати функціональну модель, яка відображає також і потоки інформації та матеріальні об'єкти, що пов'язують функції.

Для початку роботи з IDEF0 [33] створюється контекстна діаграма, де об'єкт моделювання зображується як єдиний блок з граничними стрілками, її назва А–0, А мінус нуль. Далі розглядаються окремі функції та їх зв'язки, використовуючи відповідні блоки та стрілки. Така модель використовується для визначення структури та функцій АСК віддаленого доступу до IP. На діаграмі, рисунок 3.5, стрілки показують, як об'єкт моделювання пов'язаний зі своїм оточенням. Вона визначає межі області моделювання.

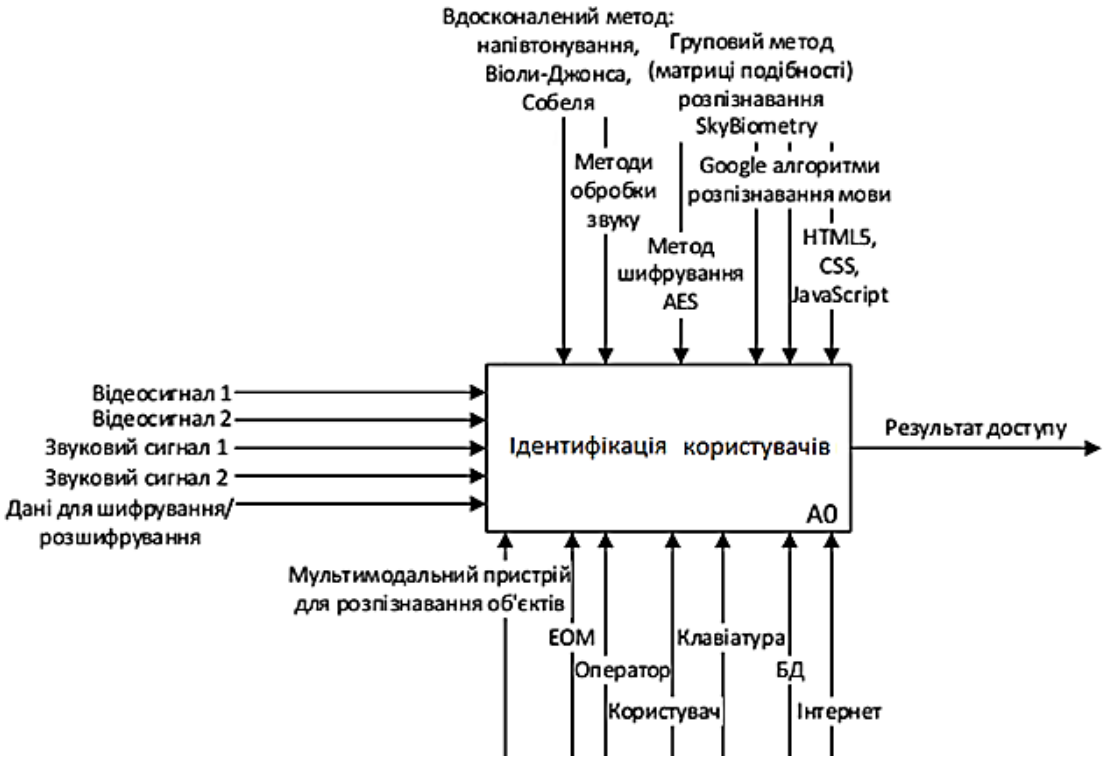

Рисунок 3.5 – Контекстна діаграма ідентифікації користувачів

Далі відбувається процес декомпозиції. За допомогою нотації IDEF0 послідовно розбивається процес на більш детальні рівні. Дочірня діаграма, створюється під час декомпозиції, охоплює область, що й батьківський процес, проте більш детально описує.

Згідно з методологією IDEF0, при декомпозиції батьківського процесу стрілки, які зв'язують його та інші процеси, переносяться до дочірньої діаграми, як граничні стрілки, (додаток А) що вказують на вхідні дані для процесу. Цей підхід дозволяє виключити дублювання даних та забезпечити наочність у подальшому аналізі моделі.

На дочірній діаграмі також можуть з'являтись нові функції та об'єкти моделювання, які потрібні для більш детального опису процесу. Таким чином, декомпозиція дозволяє розглядати процес на різних рівнях деталізації та розуміти його складові частини.

Після декомпозиції продовжується процес моделювання, створенням наступної дочірньої діаграми. У результаті створюється декілька рівнів діаграм, що дозволить детально проаналізувати процес та виявити можливі проблеми або вдосконалити його. Узагальнення всіх діаграм на різних рівнях деталізації дозволяє створити повну функціональну модель процесу, що відображає всі складові частини та зв'язки між ними.

Дана модель використовується для планування та управління процесом, виявлення можливих проблем та їх вирішення, а також для вдосконалення процесу та забезпечення його ефективності.

Блок А2 діаграми IDEF0 характеризується складною внутрішньою функціональністю (додаток Б).

Тому виконується його декомпозиція, оскільки тут попередьо вдбувається обробка зображень та звуку для створення ЕЗ. При цьому враховується, що рівень деталізації на поточному етапі є достатнім для відображення мети моделювання і на нижчих діаграмах будуть використовуватись елементарні функції, які зрозумілі користувачам системи.

3.3 Реалізація проектованої системи

Багатофакторний підхід стосовно КД до ІР дозволяє використовувати кілька характеристик для ідентифікації користувача, що забезпечує більш ефективний та надійний захист від НСД. Цей підхід використовується для подолання обмежень, що випливають з використання однофакторних систем КД, оскільки певні характеристики можуть збалансувати недоліки, притаманні іншим характеристикам. Комбінація багатьох факторів дозволяє підвищити рівень безпеки та надійності системи, зменшити кількість помилок ідентифікації, а також підвищити стійкість до шуму та змін у середовищі.

До переваг багатофакторного підходу можна віднести зменшення ризику крадіжки або втрати одного із факторів, оскільки їх комбінація робить процес аутентифікації більш складним для зловмисників. Більш складний процес аутентифікації також дозволяє зменшити ймовірність використання зловмисниками програмного забезпечення для обходу системи безпеки.

Вибір факторів для багатофакторного підходу в АСК доступу є ключовим етапом, який визначає ефективність та надійність системи. Правильно вибрані та налаштовані фактори можуть усунути обмеження однофакторних систем та забезпечити більш точну ідентифікацію та авторизацію об'єктів. У проектованій системі використано наступні біометричні характеристики: голос та обличчя, що дозволить забезпечити більш точну ідентифікацію об'єктів та призвести до зменшення помилок хибних розпізнавань завдяки використанню кількох модальностей. Такий багатофакторний підхід дозволяє покращити ефективність та надійність АСК доступу, але вимагає правильного вибору та налаштування факторів.

У проектовані АСК доступу до ІР реалізовано алгоритм для роботи аудіомодуля (додаток В), який передбачає можливість вибору режиму роботи:

- процес створення ЕЗ – приймається звуковий стереосигнал, шумопоглинання та запис спектрограми еталону у БД;
- процес ідентифікації – прийом звукового стереосигналу в РРЧ, здійсненя поглинання шумів та порівняння його із ЕЗ.

У випадку не відповідності запису ЕЗ, користувачу не надається доступ.

У АСК реалізовано алгоритм для роботи відеомодуля (додаток Г), у якому також передбаченає вибору режиму роботи:

- зберігання ЕЗ – приймається 3D відеосигнал, відбувається накладання зображень та зберігання до БД системи;

- ідентифікація – прийом 3D відеосигналу в РРЧ, здійснюється накладання зображень та порівнянняїх із ЕЗ, що записаний у БД АСК.

Якщо отримане зображення користувача не збігається з еталоном, тоді він не отримує доступ до ресурсів.

Запропоновані модулі біометричної ідентифікації можуть працювати окремо або в комбінації один з одним для більш точної ідентифікації. Наприклад, якщо звуковий модуль не може впевнено ідентифікувати особу через шумне середовище або проблеми з голосом, зображення обличчя може допомогти в розпізнаванні. Така комбінація дозволяє знизити помилки ідентифікації та зробити систему більш надійною.

Запропонована АСК доступу до IP має переваги, зокрема можливість отримання зображень у двох діапазонах – звичайному та в ІЧ, що дозволяє змінювати динамічний діапазон зображення при обробці. Крім того, система оснащена двома мікрофонами для запису стереозвуку та регульованим світлодіодним підсвічуванням і дозволяє знімати в умовах низької освітленості або вечірнього часу.

АСК легко інтегрується до робочоїї станції АРМ через USB та до мікрофонів за допомогою 3,5 мм роз'єму MiniJack, при цьому не потребує додаткового джерела живлення (рисунок 3.6).

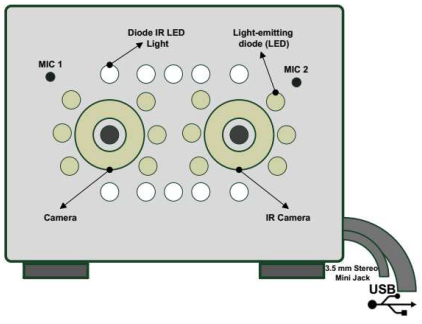

Рисунок 3.6 – Пристрій мультимодальної ідентифікації

Застосування АСК на базі біометричних методів для розпізнавання об'єктів має значні переваги. Використання кількох різних біометричних технологій або модальностей, дозволяє враховувати кілька характеристик одночасно, що значно зменшує кількість людей, яких неможливо ідентифікувати біометрично, і значно підвищує захист ІР та знижує ризик НСД.

Використання кількох модальностей для розпізнавання об'єктів, дозволяє подолати обмеження унімодальних систем, оскільки різні параметри компенсують недоліки один одного. Він об'єднує дві характеристики – звукове та візуальне розпізнавання – і збирає багатопотокову цифрову інформацію у формі відео та звукового сигналу в реальному часі. Це розширює сфери застосування пристрою і зменшує помилки неправильного розпізнавання та чутливість до шуму.

Для роботи з АСК користувачу потрібно виконати додавання біометричної характеристики, натиснувши кнопку «Додати». Або, якщо користувач планує завантажити нову біометричну характеристику, він може скористатися кнопкою «Очистити» (рисунок 3.7).

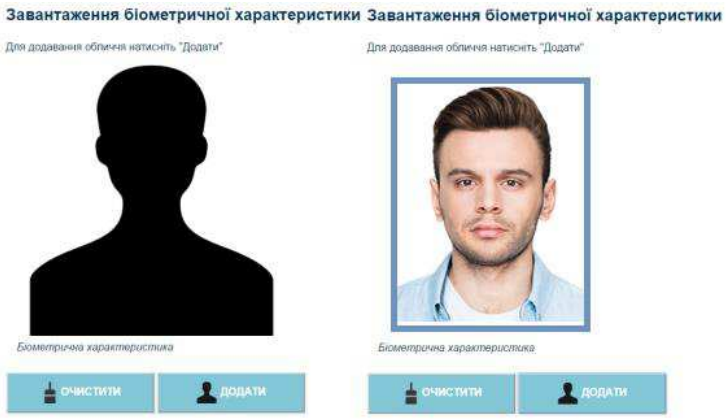

Рисунок 3.7 – Додавання характеристик

Після того, як зображення з'явиться у вікні, користувач може переходити до наступних етапів. Наприклад, він може ввести додаткову інформацію про зображення, яка буде збережена разом з біометричним зразком у БД. Також АСК забезпечує можливість переглянути раніше додані біометричні зразки. Зокрема, користувач може перейти на сторінку БД та переглянути перелік доданих біометричних характеристик. Крім того, у АСК доступні інструменти для захисту конфіденційної інформації. Наприклад, є можливість зашифрувати біометричні

зразки, щоб забезпечити їх безпеку під час передавання та зберігання.

Попередня обробка зображення (рисунок 3.8) в розробленому алгоритмі пов'язана зі знебарвленням, для забезпечення однорідності. Після знебарвлення виконується виділення області ідентифікації. Для цього користувач повинен виділити область на зображенні за допомогою миші або тачпаду. Ця область буде використовуватись для подальшої обробки та створення ЕЗ.

Рисунок 3.8 – Попередня обробка

На наступному етапі, після успішного виділення біометричних даних, проводиться процес виділення кордонів та додавання ЕЗ до БД, що ілюструє рисунок 3.9.

Рисунок. 3.9 – Додавання ЕЗ

На останньому кроці, виконується шифрування еталону (рисунок 3.10), щоб забезпечити безпеку та конфіденційність даних, з використанням бібліотеки CryptoJS. Під час шифрування, ЕЗ перетворюється на незрозумілий для сторонніх символьний рядок, який зберігається в БД.

Рисунок 3.10 – Захист еталону

В АСК реалізовано захист від НСД до конфіденційних даних користувачів, що гарантує їх безпеку. Крім того, це допомагає запобігти можливим атакам на сайт та забезпечити стабільну роботу його функцій.

3.4 Реалізація програмного забезпечення

Група математичних методів, які дозволяють визначати контури на цифрових зображеннях, де яскравість змінюється різко або має інші види неоднорідностей мають назву виділення кордонів. Ці методи дуже важливі для обробки та розпізнавання зображень, зокрема для виявлення та виділення ознак. Дані методи застосовуються у різних областях та дозволяють визначати різні форми та контури на зображеннях, що можуть мати важливе значення для різних додатків, таких як розпізнавання об'єктів на зображеннях, аналіз медичних зображень та багато іншого.

Застосування фільтрів виділення кордонів забезпечує зменшення обсягу оброблюваних даних, видаливши зображення менш значущі деталі. Однак, не завжди можна виділити кордони на зображеннях реального світу з середньою складністю, особливо у випадках, коли зображення має нерегулярну форму або вміщує в собі багато складних об'єктів. Тому, при використанні цих методів, необхідно ретельно аналізувати кожен конкретний випадок та враховувати особливості зображення для досягнення найкращих результатів.Межі, які виділяються на зображеннях інколи мають недоліки, зокрема, криві кордонів не з’єднані в одну лінію, відсутня межа або присутні межі об’єкта, який не відповідає досліджуваному.

Згортка є математичною операцією, яка застосовується у багатьох алгоритмах обробки зображень. При цьому, два масиви чисел різних розмірів перемножуються, щоб створити третій масив чисел тієї ж розмірності. У зображеннях, зазвичай один з масивів представляє відтінки сірого кольору, а другий масив, який називається ядром, містить значення, які використовуються для обчислення значення вихідного пікселя. Згортка дозволяє реалізувати оператори обробки зображень, такі як розмивання, відокремлення країв та виявлення ознак. Застосування згортки до зображення може допомогти покращити його якість, зменшити шум та підсилити важливі ознаки.

Дискретний оператор Лапласа є важливим інструментом в обробці зображення, особливо для виявлення кордонів та оцінки руху. Цей оператор визначається як сума других похідних виразу та зазвичай використовується для зменшення шуму та виділення граней у зображенні. Даний оператор можна також використовувати для виявлення дефектів у матеріалах або для покращення роздільної здатності мікроскопічних зображень. Для 1–, 2– і 3–вимірних сигналів його можна представити як згортку з певними ядрами:

$$\text{Фільтр } 1D\colon D_x^2 = [1 \ -2 \ 1]; \qquad \text{Фільтр } 2D\colon D_{xy}^2 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & -4 & 1 \\ 0 & 1 & 0 \end{bmatrix}.$$

Матриці ядер отримуються шляхом дискретних похідних. Зміни в матриці ядра матимуть різні наслідки, від незначних до помітних.

У наступному прикладі розглянуто матриця ядер: 3 × 3:

```
public static Bitmap
Laplacian3x3Filter(this Bitmap sourceBitmap,
bool grayscale = true){
      Bitmap resultBitmap =
      ExtBitmap.ConvolutionFilter(sourceBitmap,
      Matrix.Laplacian3x3,
      1.0, 0, grayscale);
      return resultBitmap;
      }
public static double[,] Laplacian3x3{
      get{
            return new double[,]
            { { -1, -1, -1, },
            { -1, 8, -1, },
            { -1, -1, -1, }, };
      }
```

Матриця Лапласа розміром 5 × 5 може створювати зображення з помітними

відмінностями, в той час як виділення кордону виражається в дрібних деталях. Однак, ця матриця може бути чутливою до шуму на зображенні. У наступному прикладі розглянуто матриця ядер Лапласа 5 × 5:

```
public static Bitmap
Laplacian5x5Filter(this Bitmap sourceBitmap,
bool grayscale = true){
      Bitmap resultBitmap =
      ExtBitmap.ConvolutionFilter(sourceBitmap,
      Matrix.Laplacian5x5,
      1.0, 0, grayscale);
      return resultBitmap;
      }
public static double[,] Laplacian5x5{
      get{
            return new double[,]
            { { -1, -1, -1, -1, -1, },
            { -1, -1, -1, -1, -1, },
            { -1, -1, 24, -1, -1, },
            { -1, -1, -1, -1, -1, },
            { -1, -1, -1, -1, -1 }
      }
```

Метод Гауса–Лапласа є загальною варіацією фільтра Лапласа, яка призначена для протистояння шумовій чутливості звичайного фільтра Лапласа. Для видалення шуму на зображенні метод Гауса–Лапласа використовує згладжування за допомогою Гаусового розмиття.

Для оптимізації продуктивності можна обчислити єдину матрицю, яка має вигляд Гаусового розмиття та матриці Лапласа.

```
public static Bitmap
LaplacianOfGaussian(this Bitmap sourceBitmap){
      Bitmap resultBitmap =
      ExtBitmap.ConvolutionFilter(sourceBitmap
      Matrix.LaplacianOfGaussian,
      1.0, 0, true);
      return resultBitmap;
      }
public static double[,] LaplacianOfGaussian{
      get{
            return new double[,]
            { { 0, 0, -1, 0, 0 },
            { 0, -1, -2, -1, 0 },
            { -1, -2, 16, -2, -1 },
            { 0, -1, -2, -1, 0 },
            { 0, 0, -1, 0, 0 } };
            }
      }
```

Ще одним методом загального застосування для виділення кордонів є метод Собеля.

```
public static Bitmap
Sobel3x3Filter(this Bitmap sourceBitmap,
bool grayscale = true) {
      Bitmap resultBitmap =
      ExtBitmap.ConvolutionFilter(sourceBitmap,
      Matrix.Sobel3x3Horizontal,
      Matrix.Sobel3x3Vertical,
      1.0, 0, grayscale);
      return resultBitmap;
      }
public static double[,] Sobel3x3Horizontal {
      get {
            return new double[,]
            { { -1, 0, 1, },
            { -2, 0, 2, },
            { -1, 0, 1, }, };
            }
      }
public static double[,] Sobel3x3Vertical {
      get {
      return new double[,]
      { { 1, 2, 1, },
      { 0, 0, 0, },
      { -1, -2, -1, }, };
      }
}
```

Даний метод використовується для обробки зображень з метою відокремлення границь. Оператор Собеля є дискретним диференціальним оператором, що наближено обчислює значення градієнту або норми градієнту для яскравості зображення. «Для виконання операції Собеля, зображення згортається з невеликими сепарабельними цілочисельними фільтрами у вертикальному та горизонтальному напрямках» [30].

Фільтр Собеля є менш чутливим до шуму зображення у порівняні з фільтром Лапласа. Це зумовлено тим, що фільтр Собеля використовує дві окремі ядра (для горизонтального та вертикального напрямку), які згладжують зображення перед виконанням диференціювання, тобто виконують згладжування за допомогою розмиття. Це допомагає позбавитися від шуму та інших непотрібних деталей в зображенні. Таким чином, фільтр Собеля дозволяє знайти границі на зображенні з високою точністю та мінімальним шумом.

У порівнянні з фільтрами Лапласа, які були розглянуті раніше, метод Собеля дає істотно відмінні результати. Фільтр Собеля має меншу чутливість до шуму на зображенні, порівняно з фільтром Лапласа.

Після проведення дослідження та реалізації методів виділення кордонів зображення можна стверджувати, що найкращим для задачі розпізнавання особи є оператор Собеля, оскільки він проявляє меншу чутливість до шуму на зображенні та кордони не є такими гранульованими, як у інших розглянутих фільтрах.

Лістинг модулів системи наведено в додатку Д.

В результаті запропоновано АСК доступу до ІР, яка дозволяє створювати ЕЗ біометричної характеристики, шифрувати та зберігати його. Також забезпечено візуальне представлення АСК. Проведена апробація та тестування системи показало, що завдяки застосуванню сучасних мов програмування, система є ефективною та має високу продуктивність.

4. ОХОРОНА ПРАЦІ

4.1 Основні поняття електробезпеки

Основні поняття електробезпеки є ключовими для забезпечення безпечної експлуатації електроенергетичних систем та обладнання. В сучасному виробництві, де використовується значна кількість електроенергії, особливо важливим є захист персоналу, що працює з електричним устаткуванням, від потенційно небезпечного впливу електричного струму.

Система електробезпеки включає в себе широкий спектр заходів, таких як «правові, соціально–економічні, організаційно–технічні, санітарно–гігієнічні, лікувально–профілактичні та реабілітаційні» [34]. Правила електробезпеки регулюються відповідними юридичними та технічними документами, які складають нормативно–технічну базу в цій галузі. Основна мета електробезпеки полягає в збереженні здоров'я, а у деяких випадках і життя працівників, які працюють з електричними установками та обладнанням. Для персоналу, який працює з електроустановками та електрообладнанням, необхідно мати достатні знання з основ електробезпеки, щоб забезпечити безпечну роботу та уникнути потенційних небезпек.

«Електричний струм – це упорядкований спрямоване рух заряджених частинок у провіднику. Електричний струм характеризується силою струму (I), яка в системі СІ вимірюється в амперах [A], і щільністю струму (j), яка в системі СІ вимірюється в амперах на квадратний метр [A / m^2]» [35].

Сила струму є величиною, що чисельно рівна заряду, δ_q який протікає за одиницю часу δ_t крізь переріз провідника:

$$I = \frac{\delta_q}{\delta_t}.$$

Закон Ома є основним принципом, що описує взаємозв'язок сили струму, напруги та опору в електричному колі:

$$I = \frac{U}{R},$$

де: U – напруга електричного струму між кінцями провідника (вольт, В); R – опір провідника (Ом).

«Електрична дуга – це фізичне явище, при якому електрони, рухаючись в провіднику від негативного полюса до позитивного, між електричними контактами, утворюють електричний ланцюг» [34].

Провідник – це матеріал, який дозволяє протікання електричного струму. Коли електричний струм проходить крізь провідник, він зтикається з опором, який спричиняє часткову конвертацію електричної енергії в тепло. Його опір, як правило, залежить від матеріалу, розміру, форми та інших факторів.

При надзвичайно низьких температурах деякі матеріали можуть перейти в стан, що називається надпровідністю. У такому стані провідник втрачає майже весь свій опір та майже без втрати переносить електричний струм. Проте, в більшості матеріалів, які ми зустрічаємо у повсякденному житті, провідники виявляють опір току. Наприклад, метали, які часто використовуються як провідники, мають певний рівень опору, який залежить від їхніх фізичних властивостей. Окрім провідників, існують інші матеріали, що не можуть проводити струм, і вони називаються діелектриками.

Електричний струм буває постійний або змінний. Середні значення порогових струмів наведені в таблиці 4.1 [34].

Таблиця 4.1 – Середні значення порогових струмів

Струм	Пороговий відчутний струм, мА	Пороговий невідпускаючий струм, мА	Пороговий фібриляційний струм, мА
Змінний	0,5 ... 1,5	6 ... 10	50 ... 100
Постійний	5 ... 20	50 ... 80	300

У постійного струму постійноюими є величина та напрямок і створюється він за допомогою постійної напруги. Змінний струм змінює величину і напрямок з певною частотою, і його генерація зазвичай пов'язана зі змінною напругою. Також, існує явище статичної електрики, коли на поверхні та в об'ємі діелектриків, провідників та напівпровідників відбувається накопичення вільного

електричного заряду. Це явище може призводити до виникнення неприємних електростатичних розрядів, але воно не представляє прямої небезпеки для здоров'я людини, за винятком неприємних відчуттів, які можуть виникати при доторканні до заряджених предметів.

4.2 Вплив електричного струму на організм людини

Людиною майже не відчутним є електричний струм з нормою в 1 мА. Струм величиною приблизно 0,01 А стає небезпечним для життя людини, а сила струму близько 0,1 А є смертельною.

При проходженні крізь живий організм, струм проявляє такі ефекти [35]:

1. Термічний ефект – відбувається «нагрівання тканин, органів, кровоносних судин і біологічних середовищ організму» [34]. Це може призвести до перегрівання усього організму й порушення обмінних процесів в ньому.

2. Електролітичний ефект – відбувається розкладання фізіологічних розчинів організму, зокрема крові, плазми тощо, що призводить до порушення їх функцій.

3. Біологічний ефект викликає роздратування та збудження нервових волокон й тканин. Він також впливає на інші тканини організму, що може супроводжуватись непереборними м'язовими скороченнями.

Електричний струм, діючи на організм, може спричинити різноманітні порушення його життєдіяльності, включаючи повну зупинку серця та пригнічення роботи легенів.

Порушення, викликані електричним струмом, можуть бути різноманітними, але їх можна умовно розділити на категорії, зокрема місцеві електротравми і загальні електротравми, відомі як електричні удари.

Місцеві електротравми виникають, коли в деякому конкретному місці організму виникає ушкодження. Загальні електротравми, або електричні удари, впливають на весь організм шляхом порушення нормального функціонування органів та систем, що є життєвонеобхідними.

Ці різновиди електротравм можуть мати серйозні наслідки для здоров'я

людини, включаючи смертельні наслідки, як–то зупинку серця і проблеми з диханням.

Від впливу електричного струму можуть відбуваьтися два типи уражень:

- Місцевої дії (електрична травма) – пошкодження тканин організму, спричинене електричним струмом або електричною дугою. Це може включати пошкодження шкіри, зв'язок і кісток. Травми бувають різних типів, включаючи електричний опік, електричний знак, металізацію шкіри і електроофтальмію. Інколи електричні травми можуть бути смертельними.
- Загальної дії (електричний удар) – збудження тканин організму під час проходження через них струму, що супроводжується судомними скороченнями м'язів. Електричні удари класифікуються за чотирма ступенями важкості: від спазматичного скорочення м'язів без втрати свідомості до клінічної смерті, яка характеризується відсутністю дихання та кровообігу.

Зазвичай розглянуті види травм виявляються разом, проте вони відрізняються і потрібно розглядати їх окремо. Ступінь важкості ураження струмом перебуває у залежності від кількох факторів, зокрема це сила струму, електричний опір тіла людини, тривалість протікання струму крізь тіло, вид струму, індивідуальні властивості організму, шлях проходження струму по тілу, умови навколишнього середовища та площа контакту зі струмоведучими частинами.

4.3 Заходи захисту від ураження електричним струмом

Ураження електричним струмом людини можуть виникати в наступних випадках [35]: дотик до струмоведучих частин електроустановок під напругою; наближення до незахищених ізольованих струмоведучих частин електроустановок на небезпечну відстань; дотик до неструмоведучих частин електроустановок, що виявилися під напругою в результаті замикання на їх корпус. Також ураження може статися внаслідок помилкового прийняття обладнання, яке відключене, як електрично напружене; пошкодження ізоляції; удару блискавки; дії електричної дуги; або випуску іншої людини, що перебуває

під напругою.

У разі замикання на землю фазового проводу, виникає напруга на поверхні землі. Якщо людина опиняється в зоні ураження, вона стає під дією крокової напруги, яка набуває небезпечних значень, прямуючи до дроту. Розмір крокової напруги знаходиться в залежності від відстані між точками контакту людини з землею. Рекомендується рухатися від проводів дрібними кроками. На відстані понад 20 метрів від проводу вона спадає до нуля.

Серед основних заході захисту можна виділити [35]:

- Застосування колективних засобів захисту, які дозволяють унеможливити доступ до струмоведучих частин, що знаходяться під напругою. Це включає в себе використання огороджень, блокувальних пристроїв, сигнальних знаків та інших засобів безпеки. Для уникнення небезпеки контакту зі струмоведучими частинами устаткування унеможливити до них вільний доступ. Це можна досягти шляхом встановлення огороджень або розташування струмопровідних елементів на висоті або в місцях, недоступних для контакту.

- Заземлення – полягає у спеціальному з'єднанні металевих неструмоведучих частин електроустановки із землею. Опір такого заземлення повинен бути мінімальним (до 4Ом у мережах із напругою до 1000 В і до 10Ом для інших мереж). Існують два типи заземлення. Виносне пр якому елемент заземлення, що контактує з землею, розташований за межами майданчика, на якому знаходиться обладнання. Контурне – кілька з'єднаних заземлювачів, розташованих по контурі майданчика, що захищається. Контурне заземлення застосовується в установках з напругою більше 1000В. Для електроустановок з напругою менше 1000В площа заземлювального провідника має бути мінімум 4мм^2. Заземлювати електричні прилади строго заборонено до батарей опалення та водопровідних труб, оскільки можлива травма при контакті з ними.

- Занулення – це намірене електричне з'єднання нульового захисного провідника з металевими неструмоведучими частинами, що можуть виявитися під напругою. Вважається одним із основних засобів реалізації безпеки в трьохфазних мережах. «Занулення перетворює замикання фази на корпус на однофазне коротке замикання, що спричиняє спрацювання захисту (перегоряння запобіжника) та

відключення пошкодженої ділянки мережі» [34].

Пристрої захисного відключення є складовою частиною системи, що автоматично відключає електроустановки в разі виникнення небезпеки ураження струмом. Вони складаються з датчиків, перетворювачів і виконавчих органів.

Мала напруга визначається як напруга, що не перевищує 42 В і використовується для зниження ризику ураження електричним струмом. Найвищий рівень безпеки досягається при напрузі до 10 В. У промисловості часто використовуються мережі з напругою 12 В і 36 В, для створення яких використовуються знижувальні трансформатори.

Ізоляція включає застосування діелектричного шару на поверхні струмопровідних елементів або використання непровідних конструкцій для відокремлення струмоведучих частин від інших частин електрообладнання. Виділяють такі типи ізоляції: робоча, додаткова, подвійна і посилена.

До основних засобів ізоляційного захисту належать ізолюючі штанги, ізолюючі вимірювальні кліщі, покажчики напруги, діелектричні рукавички, діелектричні калоші, килимки та інші. Загальні заходи захисту від статичної електрики включають загальне та місцеве зволоження повітря.

4.4 Розрахунок пристрою захисного відключення

Для визначення припустимого часу спрацювання пристрою захисного відключення в приміщенні, де він буде встановлений, в разі контакту людини з проводом мережі, де існує ізольована нейтраль, при нормальному режимі, необхідно враховувати ряд факторів. Один з таких факторів – це реакція людського організму на електричний струм, опір тіла людини R_h = 2 кОм. Час, необхідний для спрацювання захисного відключення, повинен бути достатнім, щоб уникнути серйозних ушкоджень людині в разі контакту з проводом. Такі параметри, як сила струму, тривалість контакту та індивідуальна реакція організму, можуть впливати на визначення цього часу. Параметри мережі: $U_Л$ = 380 В; $R_{L1} = R_{L2} = R_{L3} = R$ = 200 кОм; $C_{L1} = C_{L2} = C_{L3} = C$ = 10 мкФ.

Ємність фазних проводів відносно землі є дуже великою – 10 мкФ, то вплив

їх повного опору на струм, який протікає через тіло людини при прямому однофазному дотику, можна ігнорувати. Тому його значення можна визначити за простою формулою [35]:

$$I_h = \frac{U_\varphi}{P_h} = \frac{220}{2} = 110\text{мА}.$$

Час спрацювання пристрою захисного відключення визначається відповідно до співвідношення:

$$I_{h_{max}} = \frac{50}{T}.$$

Оскільки, $I_h = 110\text{мА}$, тоді

$$T = \frac{50}{110} = 0{,}45c.$$

В рпезультаті проведених розрахунків, можна зробити висновок, що пристрій захисного відключення відповідає нормативним вимогам.

ВИСНОВКИ

Проведено дослідження технології доступу до віддалених інформаційних ресурсів. В контексті сучасних реалій, віддалений доступ стає все більш актуальним та важливим. Класифіковано інформацію за різними аспектами, що дозволило систематизувати та організувати дані, які використовуються при віддаленому доступі. В результаті проведених досліджень встановлено важливість забезпечення безпеки та контролю доступу.

Основою контролю доступу є процеси ідентифікації, автентифікації та авторизації. В результаті досліджень виявлено, що ідентифікація відіграє важливу роль у ефективності СКІД, оскільки є основою для подальшої автентифікації, яка підтверджує правомірність ідентифікованої особи або пристрою, та авторизації, яка визначає, які ресурси, функції або дії може виконувати автентифікована особа або пристрій.

Досліджено та класифіковано апаратні та програмні засоби контролю доступу до інформаційних ресурсів. Виявлено, що альтернативою традиційним засобам контролю є використання ідентифікації користувачів за допомогою біометричних характеристик, оскільки їх унікальність забезпечує високий рівень надійності системи.

Проведений аналіз статичних та динамічних методів ідентифікації за біометричними характеристиками дозволив виявити їх переваги, недоліки та обмеження. Розроблено математичну модель ідентифікації користувачів. Визначено, що використання комбінації біометричних характеристик, дозволяє підвищити надійність та точність ідентифікації користувачів, а також подолати обмеження унімодальних систем, оскільки різні параметри компенсують недоліки один одного.

Розроблено алгоритм створення еталонного зразка, що дозволяє збирати та обробляти біометричні дані з метою створення унікального шаблону для кожного користувача, та подальшого його шифрування та зберігання. На основі аналізу методів розпізнавання відео та аудіо сигналів реалізовано алгоритми роботи моділув АСК для ідентифікації за голосом та обличчям.

Розроблено архітектуру АСК віддаленого доступу, що визначає взаємозв'язок між різними компонентами системи. Реалізовано функціональну модель проектованої системи, яка відображає потоки інформації та матеріальні об'єкти, що пов'язують функції. Розроблено програмне забезпечення роботи модулів системи.

Реалізована автоматизована система контролю віддаленого доступу до інформаційних ресурсів, яка забезпечує високу надійність, безпеку та зручність використання, що може використовуватися організаціями, які потребують ефективного та безпечного доступу до своїх інформаційних ресурсів з віддаленої локації.

В роботі розглянуто основні поняття електробезпеки, проаналізовано вплив електричного струму на організм людини. Визначено різні шляхи захисту від ураження електричним струмом, а також запобігання потенційним нещасним випадкам, що пов'язані із електрообладнанням. Проведено розрахунок пристрою захисного відключення, який є важливим елементом електробезпеки.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Перехід до інформаційного суспільства. [Електронний ресурс]. – Режим доступу: https://osvita.ua/vnz/reports/econom_pidpr/9175/

2. Інформаційні технології і засоби навчання. [Електронний ресурс]. – Режим доступу: http://journal.iitta.gov.ua/index.php/itlt/index

3. Реденок А.І, Петяк О.В, Ханецька Н.В. Дистанційна робота в умовах карантину та самоізолязії в період пандемії COVID–19. Габітус, Випуск № 16. – 2021. – с. 204–208.

4. Гнатюк О.В. Дистанційне навчання: проблеми, пошуки, виклики. [Електронний ресурс]. – Режим доступу: https://lib.iitta.gov.ua/Текст.pdf

5. Stallings, W., & Brown, L. Computer Security: Principles and Practice. Pearson. – 2017. – 848 с.

6. Бурячок В.Л. та ін. Інформаційна та кібербезпека: соціотехнічний аспект / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. – Київ: ДУТ,2015. – 288с.

7. Abbaszadeh M., Zemouche A. Security and Resilience in Cyber–Physical Systems: Detection, Estimation and Control.– Cham: Springer, 2022. – 383 p

8. Трегуб В.Г. Проектування систем автоматизації: Навч. посібник. − К.: Видавництво Ліра–К, 2017. − 344 с.

9.Писаренко Д.Г. Сучасна система контролю та управління доступом [Електронний ресурс] / Д.Г. Писаренко, Ю.Ю. Нестюк, А.С. Васюра // Матеріали XLIX науково–технічної конференції підрозділів ВНТУ, Вінниця. – 2020. [Електронний ресурс]. – Режим доступу: https://conferences.vntu.edu.ua/index.php/all–fksa/all–fksa–2020/paper/view/9077.

10. Лісовська Ю.П. Кібербезпека: ризики та заходи: навч. посібник. – К.: Видавничий дім «Кондор», 2019. – 272 с.

11. Юдін О.К. Аналіз та класифікація систем контролю та управління доступом на підприємстві / О.К. Юдін, О.М. Весельська // Наукоємні технології. – 2018. – № 2(38). – С. 220 – 225.

12. Гапак О.М. Захист інформації в комп'ютерних системах / О.М. Гапак,

С.І. Балога. – Ужгород : ПП "АУТДОР–ШАРК, 2021. – 184 с.

13. Sennewald Charles, Baillie Curtis. Effective Security Management. – 7th edition. – Buttwrqorth–Heinemann, 2020. – 392 p.

14. Зчитувачі Touch Memory. [Електронний ресурс]. – Режим доступу: https://worldvision.com.ua/schityvateli–touch–memory/

15. RFID стандарти та протоколи. [Електронний ресурс]. – Режим доступу: http://rfidukraine.com.ua/rfid–standarts/

16. Зв'язок ближнього поля (Nfc): корисний протокол у транзакціях. [Електронний ресурс]. – Режим доступу: https://cqr.company/ua/wiki/protocols/near–field–communication–nfc–a–useful–protocol–in–transactions/

17. Пластикові карти. [Електронний ресурс]. – Режим доступу: https://bankchart.com.ua/plastikovi_kartki/statti/plastikovi_karti_vid_a_do_ya

18. Царьов Р.Ю. Біометричні технології навч. посіб. [для вищих навчальних Ц18 закладів] / Р.Ю. Царьов, Т. М. Лемеха. – Одеса: ОНАЗ ім. О.С. Попова, 2016. – 140 с.

19. Коваль Л.Г., Злепко С.М., Новіцький Г.М., Крекотень Є.Г., Методи і технології біометричної ідентифікації за результатами літературних джерел. Вчені записки ТНУ імені В.І. Вернадського. Серія: технічні науки. 2019.Том 30 (69) Ч. 1. № 2. С. 104–112

20. Біометричний контроль та управління доступом. [Електронний ресурс]. – Режим доступу: https://octagram.in.ua/solutions/biometricheskiy–kontrol–i–upravlenie–dostupom–skud/

21. Bilan S., Elhoseny M., Hemanth D. Biometric Identification Technologies Based on Modern Data Mining Methods.– Springer, 2021. – 203 p.

22. Smith M., Miller S. Biometric Identification, Law and Ethics. – Springer, 2021. – 105 p.

23. Метод локалізації вушної раковини на зображенні людини у профіль. [Електронний ресурс]. – Режим доступу: http://journals.khnu.km.ua/vestnik/pdf/tech/2014_4/19.pdf

24. Jaswal Gaurav, Kanhangad Vivek, Ramachandra Raghavendra (Eds.) AI and Deep Learning in Biometric Security: Trends, Potential, and Challenges. – CRC Press,

2021. – 378 p.

25. Новіцький Г.М. Аналіз помилок ідентифікації й шляхи підвищення точності систем біометричної ідентифікації / Г.М. Новіцький, С.М. Злепко, Л.Г. Коваль, І.О. Криворучко.– Автоматика та інформаційно–вимірювальна техніка. – Наукові праці ВНТУ. – 2020, № 2. – с. 1–9.

26. Гоголюк П.Ф. Теорія автоматичного керування. Навчальний посібник /П.Ф.Гоголюк, Т.М. Гречин. – Львів: Видавництво Львівської політехніки, 2009. – 280с.

27. Король А.В. Проектування та реалізація систем контролю та управління доступом / А.В. Король, Д.О. Гордієнко, В.О. Пашинський. – Вид–во "КІМ".– 2019.– 224 с.

28. Технології і програми розпізнавання та розуміння мовлення. [Електронний ресурс]. – Режим доступу: https://www.cybermova.com/speech/розпізнавання–мовлення.html

29. Автоматичне розпізнавання мови. [Електронний ресурс]. – Режим доступу: https://bolcheknig.ru/uk/encyclopedia/avtomaticheskoe–raspoznavanie–rechi–kak–ispolzovat–raspoznavanie–golosa–v/

30. Arokia Priya P., Patil A.V., Bhende M., Wagh S., Thakare A.D. (eds.) Object Detection by Stereo Vision Images. – Beverly: Wiley–Scrivener, 2022. – 283 p.

31. HTML5 FileReader API to Upload Image and Text Files. [Електронний ресурс]. – Режим доступу: https://www.positronx.io/understand–html5–filereader–api–to–upload–image–and–text–files/

32. Crypto–js JavaScript library of crypto standards. [Електронний ресурс]. – Режим доступу: https://cdnjs.com/libraries/crypto–js

33. IDEF0 Visio [Електронний ресурс]. – Режим доступу: https://www.conceptdraw.com/examples/idef0–visio

34. Основи охорони праці / А.І. Ткачук, С.М. Богомаз–Назарова.– Кропивницький: ПП"Центр оперативної поліграфії "Авангард". – 2017. – 156с.

35. Голінько В.І. Основи охорони праці: підручник / В.І. Голінько; М–во освіти і науки України; Нац. гірн. ун–т. – 2–ге вид. – Д.: НГУ, 2014. – 271 с.