Міністерствоосвіти і науки України
ТернопільськийнаціональнийтехнічнийуніверситетіменіІванаПулюя
(повненайменуваннявищогонавчального закладу)
Факультет прикладнихінформаційнихтехнологій та електроінженерії
(назва факультету)
Кафедра радіотехнічних систем
(повназвакафедри)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проекту (роботи)

магістр
(освітньо-кваліфікаційнийрівень)

на тему: Обгрунтування методу ідентифікації особи у телекомунікаційній мережі

Виконав: студент (ка) VI курсу, групи РРм-61
напрямупідготовки (спеціальності)
172 «Телекомунікації та радіотехніка»
(шифр і названапрямупідготовки, спеціальності)
Макар С.М.
(прізвище та ініціали)

Керівник Яськів В.І.
(прізвище та ініціали)
Рецензент Стрембіцький М.О.
(прізвище та ініціали)
Нормо-контроль Дедів І.Ю.
(прізвище та ініціали)

м. Тернопіль – 2019

АНОТАЦІЯ

Макар С.М. Обгрунтування методу ідентифікації особи в телекомунікаційній мережі. – Рукопис. Кваліфікаційна робота магістра, Тернопільський національний технічний університет імені Івана Пулюя, Тернопіль, 2019.

Роботу присвячено обґрунтуванню методу ідентифікації особи у телекомунікаційній мережі.Розглянуто існуючі методи ідентифікації особи за характеристиками біометричних даних та встановлено, що такі методи вирізняються вищою точністю. Обґрунтовано метод ідентифікаціїособи за голосовим сигналом, який є надійним та дешевим у реалізації.Застосовуючи у такому методі оптимальні способи обробки аудіо сигналів ідентифікація здійснюється з високою достовірністю. В якості інформативних параметрів голосових сигналів запропоновано використати формантні частоти амплітудного спектру голосових сигналів та значення частоти основного тону.

Ключові слова: сигнал, голосовий сигнал, біометричні дані, ідентифікація, розпізнавання, спектральний аналіз, автокореляційна функція, частота основного тону.

ABSTRACT

The work is devoted to thesubstantiation of the method of identification of the person in the telecommunication networks. Existing methids of indification of a person by th characteristics of biometric data are considered and it is established that such methods are of higher accuracy. The method of identification of a person by voice signal is justified, which is reliable and cheap in implementation. Using this method of optimal audio signal processing, identification is performed with high accuracy.As informative parameters of voice signals, it is proposed to use the formant frequencies of the amplitude spectrum of the voice signals and the value of the frequency of the main tone.

Key words:signal, voice signal,biometric data, identification, recognition, spectral analysis, autocorrelation function.frequency of the main tone.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ ТА ПОЗНАЧЕНЬ

АЦП – аналогоцифровий перетворювач;

ЕОМ – електронно-обчислювальні машини;

ОТ – основний тон;

ПК – персональний комп’ютер;

ПОТ – період основного тону;

ПП – первинний перетворювач;

ЧОТ – частота основного тону;

EER – Equal Error Rate (коефіцієнт помилок).

ЗМІСТ

ВСТУП.....10

РОЗДІЛ 1.....14

ВИБІР НАПРЯМКУ ТА ТЕМИ НАУКОВОГО ДОСЛІДЖЕННЯ.....14

1.1 Завдання ідентифікації та аутентифікації користувача..... 14

1.2 Актуальні способи ідентифікації особи..... 22

1.3 Основні засади роботи систем біометричної ідентифікації..... 36

1.4 Описовий аналіз проблематики голосової ідентифікації..... 43

1.5 Висновки до розділу 1..... 45

РОЗДІЛ 2.....47

МЕТОДОЛОГІЇ ОБРОБКИ ГОЛОСОВИХ СИГНАЛІВ ДЛЯ ЗАДАЧІ ІДЕНТИФІКАЦІЇ ОСОБИ 47

2.1 Завдання ідентифікації особи 47

2.2. Аналіз процедури утворення голосового сигналу та моделей процесу породження голосу..... 48

2.3 Основні вимоги до методології обробки аудіо сигналів для задачі голосової ідентифікації особи 55

2.4 Метод дослідження голосового сигналу з метою ідентифікації користувача 57

2.5 Висновки до розділу 2..... 61

РОЗДІЛ 3.....62

ЕКСПЕРИМЕНТ З ВІДБОРУ ГОЛОСОВИХ СИГНАЛІВ.....62

3.1 Обгрунтування структури експерименту з відбору голосових сигналів ... 62

3.2 Обгрунтування відбору параметрів мікрофона 63
3.3 Обгрунтування відбору параметрів АЦП у звуковій карті 64
3.4 Висновки розділу 3 66
РОЗДІЛ 4 67
ОБРОБКА ГОЛОСОВИХ СИГНАЛІВ З МЕТОЮ ІДЕНТИФІКАЦІЇ ОСОБИ 67
4.1 Визначення частотних параметрів формант голосових сигналів 67
4.2 Обчислення значень періоду основного тону голосових сигналів 69
4.3 Висновки до розділу 4 74
РОЗДІЛ 5 76
СПЕЦАЛЬНА ЧАСТИНА 76
5.1 Метрологічне забезпечення наукового дослідженя 76
5.2 Побудова прикладного програмного забезпечення для розв’язування наукової задачі 77
РОЗДІЛ 6 84
ОБҐРУНТУВАННЯ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ 84
6.1. Визначення стадій технологічного процесу та загальної тривалості проведення науково-дослідних робіт 84
6.2. Визначення витрат на оплату праці та відрахувань на соціальні заходи 87
6.3. Розрахунок витрат на електроенергію 91
6.4 Розрахунок витрат на матеріали 91
6.5 Розрахунок суми амортизаційних відрахувань 92
6.6 Обчислення накладних витрат 93
6.7 Складання кошторису витрат та визначення собівартості науково-дослідних робіт 94

6.8 Розрахунок ціни науково-дослідних робіт..... 95

6.9 Визначення економічної ефективності і терміну окупності капітальних вкладень..... 95

6.10 Висновок до розділу 6..... 97

РОЗДІЛ 7.....98

ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ 98

7.1 Охорона праці..... 98

7.2 Безпека в надзвичайних ситуаціях 108

РОЗДІЛ 8.....113

ЕКОЛОГІЯ.....113

8.1 Електромагнітне забруднення довкілля, його вплив на людину, шляхи його зменшення 113

8.2 Джерела шуму і вібрацій, методи їх знешкодження 115

ВИСНОВКИ 118

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 120

ВСТУП

Актуальність роботи. Актуальною технічною задачею в галузі телекомунікаційних систем, інтернет-технологій тощо, є забезпечення функцій контролю доступу, що полягають у формуванні дозволу або забороні доступу до певних визначених баз даних чи приміщень. Такий контроль ґрунтується на ідентифікації суб'єктів, яким потрібен доступ і об'єкта даних, що є метою доступу. В галузі інформаційної безпеки під ідентифікацією розуміється процедура розпізнавання користувача в системі шляхом сприйняття системою ідентифікаторів користувача, які формуються на основі апріорної інформації про нього. При цьому, особливо актуальним є обґрунтування вибору типів ідентифікаторів виходячи із технічної складності реалізації системи контролю доступу, економічної обґрунтованості та захищеності.

Особливо поширеним сьогодні є розроблення для задачі ідентифікації особи автоматизованих методів і засобів, що ґрунтуються на оцінюванні її фізіологічних або поведінкових характеристик – методів біометрії, що пояснюється їхньою винятковістю та низькою ймовірністю помилки ідентифікації. При цьому, всі методи біометричної ідентифікації можна розділити на статичну і динамічну. До першої групи належать методи ідентифікації зарайдужною оболонкою ока,сітківкою ока, відбитком пальця, формою долоні, розташуванням вен на тильній стороні долоні, формою обличчя, термограмою особи тощо. Методи динамічної ідентифікації ґрунтуються на поведінковій (динамічній) характеристиці людини, зокрема ідентифікація проводиться за рукописним почерком, клавіатурним почерком, голосом, рухом губ тощо [1]. Із усіх зазначених методів біометричної ідентифікації найбільш перспективним при ймовірності відмови у доступі чи помилкової ідентифікації (0,5….5)% є метод голосової ідентифікації, якому

властива простота технічної реалізації та низька собівартість порівняно з іншими методами отримання біометричних параметрів. Однак точність цього методу в знаній мірі залежить від методів відбору та опрацювання голосових сигналів, степені врахування впливу зовнішніх та внутрішніх факторів, що спричинюють зростання складових завад в структурі голосових сигналів, появи артефактів тощо. Важливою при цьому є задача обґрунтування методу опрацювання голосових сигналів та виділення інформативних ознак, оцінки яких носили б індивідуальний характер та давали б можливість проведення ідентифікації особи.

Відомими є неодноразові спроби побудови коду для ідентифікаціх особи за голосом. Як правило, це різноманітні поєднання статистичних і частотних характеристик голосового сигналу. При цьому, голосовий сигнал розглядається як стаціонарних випадковий процес з подальшим застосуванням методів спектрально кореляційного аналізу. Проте таке подання голосових сигналів не придатне для опису коливнох структури голосових сигналів людини, які результатом роботи голосових складок і проявляється наявністю основного тону – характерної повторюваності, що може бути використана для задачі ідентифікації особи. Протягом останніх 70 років актуальною задачею є визначення основного тону голосового сигналу. Поширеними методами оцінювання основного тону є кепстральний, фільтровий , піковий метод, тощо. Однак цим методам притаманні недоліки, пов’язані з затраченим на опрацювання часом, низькою чутливістю, роздільною здатністю (ще може призвести до помилкового дозволу доступу).

Отже, обґрунтування мотоду опрацювання голосових сигналів для задаці ідентифікації особи, алгоритм якого можна було б реалізувати у вигляді елемента програмного забезпечення біометричних систем, є актуальною задачею.

Мета і задачідостідження:*метою дослідження є* обґрунтування вибору

методу ідентифікації особи в телекомунікаційній мережі. Для вирішення поставленої мети потрібно виконати такі задачі:

1. Провести огляд та аналіз літературних джерел за тематикою наукового дослідження.
2. Розглянути існуючі методи ідентифікації особи.
3. Обгрунтування вибору математичної моделі голосових сигналів для задачі ідентифікації особи.
4. Розробка методу статистичного опрацювання голосових сигналів на основі вибраної математичної моделі для виявлення нових персональних інформативних параметрів.
5. Обгрунтування застосовності нових інформативних параметрів для задачі ідентифікації особи.
6. Розробка програмного забезпечення для проведення експериментального дослідження голосових сигналів для задачі ідентифікації особи.

*Об'єкт дослідження:*голосовий сигнал людини.

Предмет дослідження: метод розпізнавання голосового сигналу для задачі автентифікації особи.

Методи дослідження: статистичні, імовірнісні та кореляційні методи, цифрова обробка сигналів.

Наукова новизна одержаних результатів: вперше обгрунтовано метод розпізнавання голосового сигналу для задачі ідентифікації особи.

Практичне значення отриманих результатів: обґрунтований метод може бути використаний для проектування автоматизованих систем ідентифікації особи за голосовими сигналами.

Публікації. Викладенні в роботі, результати якої доповідались і обговорювалися на IVВсеукраїнській науково-технічній конференції Теоретичні та прикладні аспекти радіотехніки, приладобудування і копм'ютерних

технологій –Тернопіль 20-21 червня 2019.

РОЗДІЛ 1
ВИБІР НАПРЯМКУ ТА ТЕМИ НАУКОВОГО ДОСЛІДЖЕННЯ

1.1 Завдання ідентифікації та аутентифікації користувача

Під терміном ідентифікація можна розуміти процес який являє собою розпізнавання (визначення) користувача (особи) за певними ідентифікаторами в системі [1].

Термін автентифікація являє собою процес перевірки автентичності, або запропонованого ідентифікатора на відповідність об’єкта в системі.

В основному, область IT використовує даний термін найчастіше [1-3].

Виходячи з термінів політика безпеки та ступінь довіри системи, перевірка автентичності буває двох видів – одностороння та взаємна. Найчастіше перевірку проводять криптографічними засобами.

Не варто плутати автентифікацію з авторизацією (процесом надання визначених повноважень користувачу в системі) чи ідентифікацією (процесом перевірки ідентифікатора суб’єкта).

Стандарти автетнифікації визначаються такими документами як [1-3]:

1) ДСТУ ISO/IEC 9594-8-98 – «Основи аутентифікації»

Цей стандарт:

- вказує формат інформації аутентифікації, що зберігається довідником;
- описує спосіб отримання з довідника інформації аутентиікації;
- встановлює передумови про способи формування і розміщення в довіднику інформації аутентифікації;
- визначає способи, за допомогою яких прикладні програми можуть використовувати таку інформацію аутентифікації для виконання аутентифікації,

і описує, яким чином за допомогою аутентифікації можуть бути забезпеченні інші послуги захисту.

У цьому стандарі викладено два види аутентифікації: просто – виконує пароль як перевірку збережених даних ідентичності; і сувора – використовує посвідчення особи, яке створене криптографічними методами.

2) FIPS 113 – COMPUTER DATA AUTHENTICATION

У цьому стандарті визначено Алгоритм Автентифікації Даних (DAA), який зручно використовувати під час детектування випадкових та навмисних змін у даних неповноваженою особою. Даний стандарт базується на відомому криптографічному алгоритмі DataEncryptionStandard (DES).

Цей стандарт застосовується для контролю над цілісністю інформації, яка передається засобами криптографічної аутентифікації.

Кожна система автентифікації містить у собі такі елементи:

В будь-якій системі аутентифікації як правило можна виділити декілька елементів:

- особа, що проходитиме процедуру
- характерні особливості особи, як індивідуальна риса
- власник, що контролює роботу та несе відповідальність за систему автентифікації
- власне самі принципи роботи, що являє собою сам алгоритм автентифікації
- система управління доступом, яка регламентує порядок права особи на доступ до системи.

Рушійні сили аутентифікації. Задовго до створення ЕОМ використовувались різні індивідуальні особливості особи, тобто її відмінні характеристики. Нині захищеність, надійність та вартість впровадження системи насамперед становить певну залежність відносно використання певних характеристик. Існує кілька чинників автентифікації [1]:

1) Те, що нам відомо – тобто пароль. Він являє собою конфіденційну інформацію, що відома лише авторизованому користувачу. Пароль буває у текстовому виді, буквинно-циферної комбінації, вербальним текстом чи індивідуальним ідентифікаційним номером (PIN). Достовірний алгоритм буде легко впроваджуваним і дешевим. Нажаль даний метод вирізняється доволі важливими недоліками: дуже тяжко забезпечити надійне зберігання паролю, щодня створюються інноваційні методи викрадення, зламу та генерації паролів, що негативно впливає на захищеність парольної системи.

2) Те, що у нас є – прилад автентифікації. Важливою обставиною є володарювання користувачем певним неповторюваним предметом. Таким «щось» можна вважати замочні ключі, індивідуальні печатки, інформаційний файл з певними властивостями для ПК. Такі властивості зазвичай використовують для інтеграції з певним засобом для автентифікації. Такими засобами можна назвати пластикові та смарт картки, тощо. Дістати такий пристрій стає набагато складніше для порушника, аніж підробити пароль, а користувач негайно повідомить про крадіжку засобу. Виходячи з вище сказаного вказаний спосіб отримує вищий рівень захищеності, аніж система паролів, але така система є набагато дорожчою.

3) Те, що являється частинкою нас – «біометрика». В біометриці основною властивістю є біологічні особливості особи. Такою характеристикою можна вважати відбитки пальців чи долонь, голосові дані особи, портрет чи індивідуальність ока. На думку користувача, цей спосіб вважається найпростішим, що означає, що немає необхідності носити з собою пристрій автентифікації, ні запам’ятовувати пароль. Проте система біометричної ідентифікації мусить бути дуже чутливою, для підтвердження автентичності зареєстрованої особи, та ігнорувати порушника з подібними параметрами біометрії. Така система є також дуже дорогою. Проте, не зважаючи на такі

негативні фактори біометрика буде доволі сприятливим в майбутньому чинником.

Методи автентифікації. Автентифікація за допомогою електронного підпису [3]

Федеральний закон від 06.04.2011 $N_{\underline{o}}$ 63 «Про електронний підпис» (зі змінами) передбачає наступні види електронного підпису:

Простий електронний підпис – підтверджує випадок створення електронного підпису валідного користувача з використанням засобів кодування та паролювання.

Некваліфікований електронний підпис являє собою такі пункти:

- виведений за допомогою криптографічних перетворень даних обрахованих з ключем електронного підпису;
- унеможливлює відмову від авторства особи, що підписувала документ;
- забезпечує цілісність електронного документа та показує останні модифікації з моменту підпису;
- для створення використовуються тільки засоби електронного підпису;

Кваліфікований електронний підпис – електронний підпис, що підпадає під всі ознаки некваліфікованого електронного підпису та ще деяким ознакам:

- лише у кваліфікованому сертифікаті вказується ключ для перевіряння електронного підпису;
- механізми електронного підпису, що використовуються для перевіряння та створення електронного підпису повинні бути відповідні вимогам, які встановлює даний Закон.

Форма введення пари логін-пароля

Відомим способом автентифікації у комп’ютерних системах є введення користувацького ідентифікатора, який називається «логіном» і пароля – деяких

конфіденційних відомостей. Для зберігання пари «логін та пароль» використовують спеціальну базу даних.

Алгоритм простої автентифікації [3]:

1) Користувач, щоб увійти у систему вносить особисті пароль і логін.

2) Дані, які ввів користувач перевіряються і порівнюються з оригінальними на сервері автентифікації.

3) Якщо дані збігаються, то таку автентифікацію називають успішною, після проходження користувач проходить перший крок.

Існує два способи, за якими пароль, який був введений користувачем можна передавати по мережі:

- Незашифрований спосіб, заснований на протоколі парольної автентифікації.

- Зашифрований спосіб, який базується на використанні SSL чиTLS. Дані, які ввів користувач у даному шифруванні будуть передаватися в мережу захищеними.

Автентифікація з використанням одноразових паролів

Щоб отримати постійний доступ до інформації з обмеженним доступом зловмиснику достатньо зламати багаторазовий пароль. Для вирішення цієї проблеми застосовуються одноразові паролі (OTP - One Time Password). Сутністю даного способу буде варіант, в якому для авторизації у системі надається пароль, який дійсний одноразово, кожен наступний запит потребує нового пароля. Алгоритм автентифікації за допомогою одноразового паролювання можна реалізовувати як програмним так і апаратним способом.

Методології користування одноразовими паролями поділяються на:

- Використання бази випадкових паролів, єдиної для користувача і автоматизованої системи

- Генератор псевдовипадкових чисел повинен бути єдиним для системи та користувача
- Застосування тимчасових прапорців в унісон з системою єдиного часу.

Перший спосіб базується на загальній парольній базі для системи та користувача і володіє високоточною синхронізацією. В такому випадку всі паролі зі списку можуть використовуватись лише одноразово. Такий принцип дозволяє зробити недійсним пароль користувача, який зловмиснику вдалося перехопити.

Другий метод засновується на використанні генератора псевдовипадкових чисел з ідентичними значеннями для користувача та системи. Таким методом користувачем генерується пароль, що під час послідовного використання функції без відповіді або з кожним новим запитом, що базується на унікальних даних що були у попередніх запитах, передається системі.

Третій метод

В третьому методі застосовуються тимчасові мітки. Прикладом даної технології може бути SecureID. Ця система бере за основу застосування апаратні ключі та часовій синхронізації. Така автентифікація засновується на генеруванні випадкових чисел який генерує в певних часових інтервалах. Секретний унікальний ключ зберігається тільки в апаратному пристрої суб’єкта та в базі системи. Система пропонує суб’єкту ввести PIN-код і число що згенеровано випадково, яке у даний момент зображене на пристрої. Секретний ключ особи та PIN-код із бази системи, співставляється системою, після чого генерується випадковим чином число, що базується на особливостях таємного ключа, що є у базі та поточного часу. Тоді використовується перевірка ідентичності згенерованого та введеного чисел.

В порівнянні із використанням багаторазових паролів такі одноразові паролі надають користувачу вищий ступінь захисту [1-3].

Аутентифікація за допомогою SMS

На сьогоднішній день забезпечення безпеки мобільних засобів комунікації є дуже актуальним, що стимулює розробкам нових способів у цій галузі. Серед них можна згадати аутентифікацію за допомогою SMS-повідомлень.

Така аутентифікація включає в себе такі кроки:

- Введення імені користувача та його пароля
- Одразу ж після введення служба безпеки (PhoneFactor) надсилає одноразовий ключ для аутентифікації, який має вигляд текстового SMS-повідомлення.
- Отриманий користувачем ключ використовується для аутентифікації

Великим плюсом такого методу є те, що канал який використовується для виходу ключа є відмінний від того де проводиться автентифікація. Це робить майже неможливим такий тип атаки, як «людина посередині».

Вимога ввести PIN-код на мобільному засобі буде додатковим рівнем безпеки.

У банківських операціях за допомогою інтернету та у подвійній автентифікації цей метод дуже широко поширений.

Біометричка аутентифікація [3,4]

Способи аутентифікації, які засновуються на вимірах параметрів біометрії людини, показують 99% точність ідентифікації, що вирішує проблематику втрати пари «логін-пароль».

Відомим прикладом використання таких способів будуть системи

розпізнавання особи за допомогою відбитків пальців, відбитком долоні, малюнку райдужної оболонки ока, формі вух, інфрачервоній картині капілярних судин, по почерку, по запаху, за голосом та навіть по ДНК [4].

Використання біометричних характеристик є інноваційним напрямом в елементах стільникового зв'язку, індивідуальних розрахункових картах та жетонах-пропусках. Прикладом такого використання можна вважати прикладання пальця на сканер при розрахунку в магазині, для підтвердження автентичності власника картки.

Найпоширеніші біометричні атребути та відповідні їм системи у використанні [3, 4]:

Введення з клавіатури [4]. У такому методі при введенні, наприклад, пароля відслідковується інтервали між натисканням та швидкість.

Рукописний підпис [4]. Пристрої для введення рукописного підпису у цифровому вигляді використовуються для контролю.

Відбитки пальців [4]. Сканери відбитку пальців мають невеликий розмір, вони є універсальними та відносно недорогими. Відбиток пальця дорослої особи має імовірність біологічного повторення 5-10 %. На сьогодні правоохоронні органи пропагують за допомогою великих фінансувань до електронних архівів відбитків пальців.

Геометричні особливості руки [4]. Пристрої для сканування рук використовуються у випадках, коли через травми чи бруд тяжко застосувати пристрої сканування відбитків пальців. Геометрія людської руки має відсоток схильності до повторювання близько 2 відсотків.

Розпізнавання за особливостями обличчя людини [4]. Системи основані на розпізнаванні обличчя дають змогу розпізнати персону за деяких умов з точністю 97%. Залежно який спосіб розпізнавання вони дають змогу розпізнати особу, що знаходиться на відстані від півметра до кількох десятків. Зручність цього методу полягає в тому, що можна реалізовувати звичними засобами

(камера). Складніші методи вимагають більш чутливих та якісних пристроїв.

Райдужна оболонка ока [4]. Такі пристрої мають найвищу точність. Теоретично існує імовірність співпадіння райдужок ока дорівнює 1 із 10^{78}.

Голосові характеристики [4]. Перевіряння голосу є зручним в застосуванні телекомунікаційними пристроями. Це потребує конденсаторний мікрофон та 16-бітну звукову плату, які коштуватимуть менше 25 $.Ймовірність помилки такої системи становить 2-5 %. Така технологія підходить для верифікації за допомогою голосу по телефонних каналах зв'язку, вона є надійнішою в порівнянні з цифровим набором індивідуального номеру. На даний час покращуються русла ідентифікації особи та її голосових властивостей, таких як: правдивість слів, хворіє, збудження і т.д.

Попри свої переваги методи біометричної автентифікації маютьтакі недоліки:

- Шаблон біометричних даних особи порівнюють відносно тих, які надійшли на місце порівняння, а не з результатом первісної обробки характеристик користувача.
- Шаблонна база характеристик користувача доступна для змін зловмисникам.
- Важливою є різниця застосування біометрії людини на визначеній зоні та в неконтрольованих випадках.
- Багато біометричних даних людини змінюються (наприклад під час старіння та через отримання різних порізів, опіків, хвороб і т.д.), тому шаблонна база повинна мати постійний супровід, що може створювати деякі незручності як користувачам так і модераторам.

1.2 Актуальні способи ідентифікації особи

Ідентифікувати людину можна за її фізіологічнимипоказниками, щоточнорозпізнаютьїї. Такими ознаками є: почерк «від руки», комп'ютерні та клавіатурні почерки, дактилоскопічні особливості, геометрична будова руки, особливості ока, особливі ознаки мовлення та інші.

Особливості розпізнавання за параметрами біометрії людини беруть за основу їх винятковість. Існує дуже мала імовірність знаходження двох людей з ідентичними особливостями (така імовірність рівна приблизно 1/24 млн для відбитків пальців).

В таблиці 1.1 наведено головні властивості вище описаних методологій ідентифікації за біометричними ознаками [5].

Таблиця 1.1

Головні властивості методологій ідентифікації за біометричними ознаками

Метод отримання біометричних параметрів	Ймовірність відмови у доступі %	Ймовірність помилкової ідентифікації «чужого» (без використання муляжу) %	Ймовірність помилкової ідентифікації «чужого» (з використанням муляжу) %	Збереження таємниці образу у процесі ідентифікації абонента	Вартість технічної реалізації в грошовому еквіваленті, у.о.
Геометрична будова руки	0,2…4	0,2….1	10…75	неможливо приховати	Від 600 до 3000
Відбитки пальців	2...6	0,0001	10...70	неможливо приховати	Від 60 до 600
Особливості малюнка сітківки ока	0,4	6...10	_____	неможливо приховати	приблизно 4000
Райдужна оболонка ока	0,2…2	0,0001	_____	неможливо приховати	Від 500 до 6000
Портрет обличчя	1…9	_____	_____	неможливо приховати	55000
Рукописний почерк	0,5…5	0,5…5	0,5...5	8-10…10-40	_____
Клавіатурний та комп'ютерний почерк	3…9	3...9	_____	6-10…10-12	_____
Характеристики і особливості мови	0,5...5	0,5...5	25...90 (запис)	10-16…10-30	1...60

Існує дві групи методів біометричної ідентифікації:

- статичні методи – це методи, що беруть за основу фізіологічні характеристики людини;
- динамічні методи – це методи, які беруть за основу особливості поведінки людини – послідовних рухів під час будь-якої дії.

Два вище згадані методи є взаємопов'язаними та взаємодоповнюючими напрямами. В статистичних методах біометричної ідентифікації основними перевагами є малі затрати зусиль користувача, та незалежність їх від психологічного стану людини, і, як наслідок, можливість організувати біометричну ідентифікацію великих потоків людей [6].

Біометрична ідентифікація основана на динамічних характеристика, зазвичай простіше реалізується, тому, що, зазвичай, не потребує високо вартісного технічного забезпечення і буває обмеженим лише засобами програмного забезпечення, що потребує мінімальних зусиль фахівця в процесі

супроводу та користування [7].

Статистичні біометричні властивості

Загальні статистичні біометричні властивості та способи їхньої реалізації наведенні у таблиці 1.2.

Таблиця 1.2

Способи використання особливостей фізіології біометричних характеристик

Біометрична характеристика	Реєструючий пристрій	Зразок	Досліджувані риси
Геометрична будова руки	Запатентований настінний пристрій	Тривимірне зображення зверху і боків кисті	Висота і ширина кісток і суглобів кисті і пальців
Відбиток пальця	Периферійний пристрій настільного комп'ютера, карта стандарту PC card, миша, мікросхема або зчитувальний пристрій, вбудований в клавіатуру	Зображення відбитку пальців (оптичне, на кремнієвому фотоприймачі, ультразвукове, або безконтактне)	Розташування і напрям гребінчастих виступів і розгалужень на відбитку пальців, дрібні деталі
Особливості малюнка сітківки ока	Запатентований настільний або настінний пристрій	Зображення сітківки	Розташування кровоносних судин на сітківці
Райдужна оболонка ока	Відеокамера, здатна працювати в інфрачервоному діапазоні, камера для ПК	Чорно-біле зображення райдужної оболонки ока	Смужки і борозенки на райдужній оболонці ока
Портрет обличчя	Відеокамера, камера для ПК, фотоапарат	Зображення особи (оптичне або теплове)	Відносне розташування і форма носа, розташування скул

На даний час нові біометричні технології знаходяться у стадії розробки, пов’язані із ще деякими фізіологічними ознаками.

- Порівняльний аналіз ДНК, на сьогоднішній день є найдосконалішою біометричною технологією, яка вказує на ідентичність людини (окрім одно яйцевих близнюків, які мають одинаковий генотип). Такий спосіб часто називають дактилоскопією ДНК. Така назва легко може збити з пантелику, тому, що унікальні візерунки на пальцях людини не визначаються на

генному рівні. На сьогодні біометричні системи, які беруть основу на порівняннях ДНК поки що не використовуються.

- Відбиток візерунку долоні – у таких системах застосовують положення складок на людській долоні, такі біометричні технології є аналогічними до тих, що і у перевірці відбитків пальців.
- Рисунки кровоносних судин – така система сканує розміщення кровоносних судин по тілу людини, зовнішню сторону долоні та зап’ястя.
- Продуковані серцем сигнали – така система вимагає постійного короткого контакту (не більше 8с.) користувача з датчиком «біометричного підпису» («Biodynamic signature» sensor). Під час контакту проходить ідентифікація індивідуальних параметрів людини.

Форма кисті руки як параметр ідентифікації

Такий статистичний метод ґрунтується на розпізнанні геометричних даних кисті руки, з використанням спеціалізованих пристроїв, які дозволяють отримати 3D модель кисті руки. Дані які отримали таким способом використовуються того, щоб отримати унікальну згортку, яка безумовно розпізнає особу. Геометричні характеристики кистей рук мають пару основних підходів. Один метод побудований за допомогою геометричних характеристик рук. Інший метод використовує ще й образні характеристики руки.

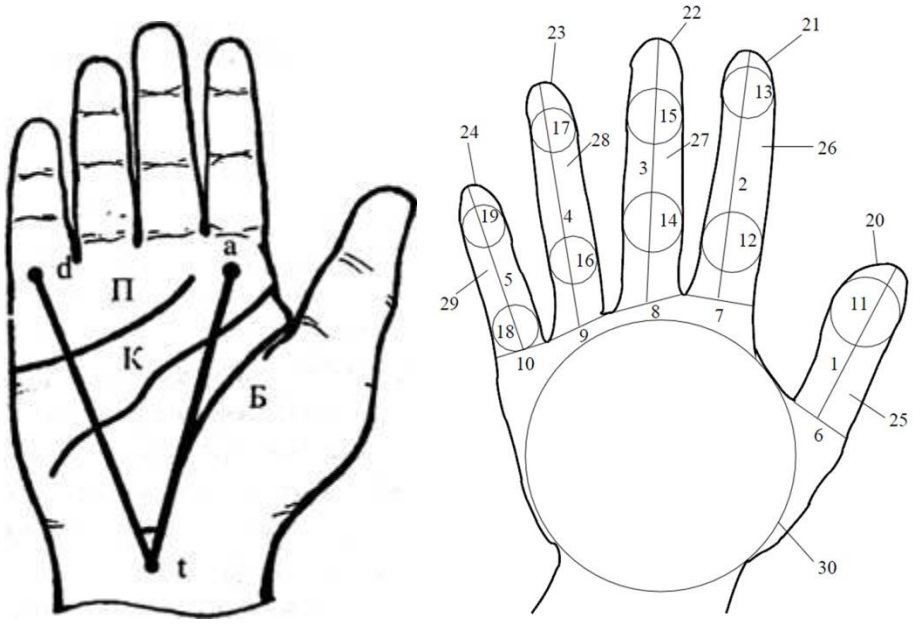


Рис 1.1. Зображення долоні людини

Рис. 1.1 відображає візерунки на долонях, які у своєму складі мають зліва основні лінії та контрольні точки, та справа сімнадцять геометричних особливостей рук. Виділяють кілька основних геометричних ознак: розміри пальців та долоні, діаметр кола, що вписується в долоню, три точки, у яких вимірюється висота кистей. Усі вище переліченні ознаки формують собою в нормаль значень. Доволі простим можна вважати векторний метод ідентифікації.

Насамперед, кілька разів сканують руку користувача. Кожна відсканована проекція створює власний вектор. Основою кількох таких векторів утворюється особливий клас. Потім обраховується середнє значення всіх ознак, що містить клас, та створюється еталонний образ. Вихідні данні часто модифікуються під час роботи. Якщо порівняти еталонний та новий образи і результат буде успішним, то такий образ може включатись до класу вихідних ознак. Два образи можна порівнювати між собою за декількома критеріями.

Найочевиднішим критерієм – можна вважати найменшу відстань еталону

до досліджуваного образу. У складнішому методі передбачено отримання чотирьох характеристик та їх порівняльний аналіз. Три позиції займають розміри, а останнє показує зображення ліній на шкірі на згинах між фалангами пальців. Таким чином даний спосіб робить нульову можливість обману пристрою.

Дактилоскопія.

Характерні ознаки, які потім зручно використовувати для ідентифікації можна отримати за допомогою зчитувача.

Зазвичай системи ідентифікації використовують лише два види особливостей малюнку:

- точки розгалуження – точки в котрих папілярні лінії роздвоюються;
- кінцеві точки – точки, в котрих папілярні лінії «виразно» закінчуються.

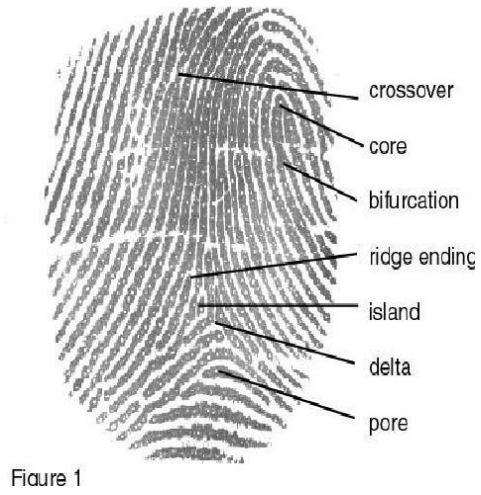


Figure 1

Рис. 1.2. Відбиток пальця з позначеними порами та точками

Зображення показує поверхню пальця просканованого високоточним сканером. На зображенні чітко видно усі особливості папілярних ліній і також потові залози. Їхнє розташування можна використати для ідентифікації. Однак такий метод мало поширений через складність отримань зображень такої якості

в не лабораторних умовах.

На відміну від звичайної дактилоскопії при автоматичному розпізнаванні відбитків пальців виникає значно менше проблем, зв’язаних з різними зовнішніми чинниками, які впливають на процес розпізнання. При отриманні фарбовим методом зображення відбитків пальців неможливо виключи чи, принаймні максимально мінімізувати, зміну тиску, поворот чи зміну положення пальця, пошкодження шкіри, та ін.

Для обробки з достатньою якістю можна за допомогою безфарбових електронних сканерів отримати зображення візерунків на поверхні пальців. Одним із важливих критеріїв можна вважати якість зображення папілярних ліній пальця, що є рушійною силою під час вибору механізму створення згортки відбитку пальця, та врешті, розпізнавання особи.

Ідентифікація за особливістю сітківки ока

Сітківка ока сканується за допомогою світла інфрачервоного спектру з низькою інтенсивністю, яке направляється зіницею у кровоносні судини задньої стінки ока. Імовірність надання допуску не вповноваженній особі під час сканування сітківки ока рівна 0,0001% (помилка першого роду). Помилка другого роду має високу імовірність – приблизно 0,1%. Така імовірність має лише одне пояснення – найжорсткіші обмеження до помилок першого роду були заявлені військовими, для яких розроблялись такі системи. До того ж, було передбачено кількаразове повторення процедури аутентифікації.

Динамічні характеристики біометрії людини

Головні динамічні характеристики біометрії людини та їх застосування показано в табл.. 1.3.

Таблиця 1.3

Реалізація динамічних біометричних характеристик

Біометрична характеристика	Реєструючий пристрій	Зразок	Досліджувані риси
Голос	мікрофон, телефон	запис голосу	частота, модуляція і тривалість голосового образу
Підпис	планшет для підпису, перо для введення даних	зображення підпису і значення відповідних динамічних вимірів	швидкість, порядок ліній, тиск і зовнішній вигляд підпису
Динаміка натискання клавіш	клавіатура	ритм машинопису	час затримки (проміжок часу, протягом якого користувач утримує конкретну клавішу) час «польоту» (проміжок часу, який потрібний користувачеві для переходу з однієї клавіші на іншу)
Динаміка роботи з маніпулятором «миша»	маніпулятор «миша»	Образ характерної траєкторії	характерні точки траєкторії Та інші параметри траєкторії

Розпізнання людини за особливими характеристиками голосу

Розпізнавання людини за допомогою особливих характеристик голосу є привабливою з декількох факторів. Першим фактором є розвиненість телефонних мереж, а іншим – звукові плати, які є звичним модулем в нинішніх ПК. Важкість зберігання парольної фрази таємничою є головним недоліком систем, які проводять ідентифікацію за особливістю голосових даних.

Завдяки сучасним засобам аудіо-прослуховування можна успішно несанкціовано копіювати парольні фрази. Можна очікувати, що буде знівельовано злочинне перехоплення акустичних сигналів технічними каналами зв’язку завдяки переходу до розпізнавання користувача за рандомними реченнями.

Потенційною протидією перехопленню акустичних сигналів – є використання комбінування з різними методами біометричної ідентифікації. Імовірність похибки у голосових системах рівна 1-2%.

Щоб ідентифікувати користувача за голосовими даними, потрібно володіни наявним мовним шаблоном, який дозволить порівнювати введені в систему голосі ключі. Ключ та шаблон можна порівнювати загалом, чи використовуючи кілька особливостей мовного сигналу після оцифрування і обробки: (амплітуди та потужності, частоти, енергетичних, часових та фазових характеристики) [9].

Щоб спростити аналіз мовного сигналу спочатку проводять дискретизацію за допомогою частотних чи Вейвлет перетворень.

Розпізнання користувача виконується за допомогою таких показників:

- визначення енергії та періодичних властивостей сигналів;
- за допомогою вікон Хеммінга можна визначити короткочасну енергію сигналу [9];
- кепстральні коефіцієнти;
- кількість переходів сигналу через нульову позначку.

Розпізнавання завдяки динаміці рукописного підпису

Проблематику розпізнання особи завдяки його факсимільному підписі [11, 12] варто розрізняти як дві відмінні задачі:

- розпізнавання особи за траекторією руху пера у підписі, що перевіряється на відповідність еталонному;
- розпізнавання особи з допомогою динаміки написання автором підпису та відслідковування почерку.

Такі задачі є суттєво відмінними, проте їх вирішення можна проводити одночасно і окремо. Перша задача описує способи порівнювання зображень, що вже були відтворені раніше у невідомому порядку. Друга задача проводить аналіз даних параметрів коливань пера автора коли той відтворює підпис на 3D пристрої.

Навіть за допомогою сучасних технологій задачу номер один дуже тяжко реалізувати. Зазвичай можна вважати дані системи напівавтоматичними, це

означає, що системи дозволяє спрощувати роботу експерта, він може порівнювати відповідні числові властивості підходящих фрагментів підпису з еталоном, але останнє слово за людиною. Через це виробники не будуть надавати звітну статистику появи помилок обох видів.

Задача номер два показує, що головна роль належить ЕОМ, у якої є суттєво більше даних, в порівняні з експертами. Тому, системи розпізнання особи, які проводять аналіз динаміки напсання автографа, завдяки своїм статистичним характеристикам є значно кращими ніж експерти.

Варто знати, що окремі системи розпізнання особи за підписом замість функцій використовують їхню першу чи другу похідну.

Також важливо те, що помилка першого роду чи помилкова відмова справжньому автору яка має ймовірність 0,01 – це прийнятно характеристика для вимог сьогодення.

Ідентифікація за клавіатурним почерком

В звичних системах захисту інформації здійснюється доступ завдяки паролям. При збільшені пароля, можна спостерігати характерний для користувача клавіатурний почерк при введенні ним пароля. Наприклад, паролем може використовуватись наступна фраза: «Способом захисту інформації є пароль». Під час введення подібної фрази біометрична система фіксує інтервали між настисканням кожної наступної клавіші та відпуском попередньої і час натиснення кожної клавіші. Графік співвідношень інтервалів часу натиснення та відпускання кнопок у слові «Пароль» показано на рис. 1.3.

На рис. 1.3. показано, що моменти натискання кнопок t1, t2, t3, …., tN відрізняються, одже, такі параметри можна використовувати під час знаходження властивостей, які характерні лише індивідуальному клавіатурному почерку автора. Також можна використовувати контрольні періоди між натисканням поставлених поруч кнопок τ1, τ2, τ3 ...., τN-1, як контрольовані параметри. Такі контрольовані параметри є залежними від того, скількома

пальцями та чи однією рукою друкує користувач, від поєднання рухів усіх пальців і рук характерних для користувача під час набору. Можна сказати що клавіатурний почерк може позбутись індивідуальності через те, що користувач буде працювати лише за допомогою одного пальця однієї руки. Базуючись на вище сказаній інформації можна сказати, що для різних людей час натиснень клавіш не буде індивідуальним.

Будуть пропорційними до віддалі клавіш інтервали їх натискань, та стає неможливим перекриття натиснень сусідніх клавіш. Тому зі збільшенням навиків роботи з клавіатурою та переходу до «сліпого набору» усіма пальцями двох рук, індивідуальність клавіатурного почерку у будь-якого користувача зростає.

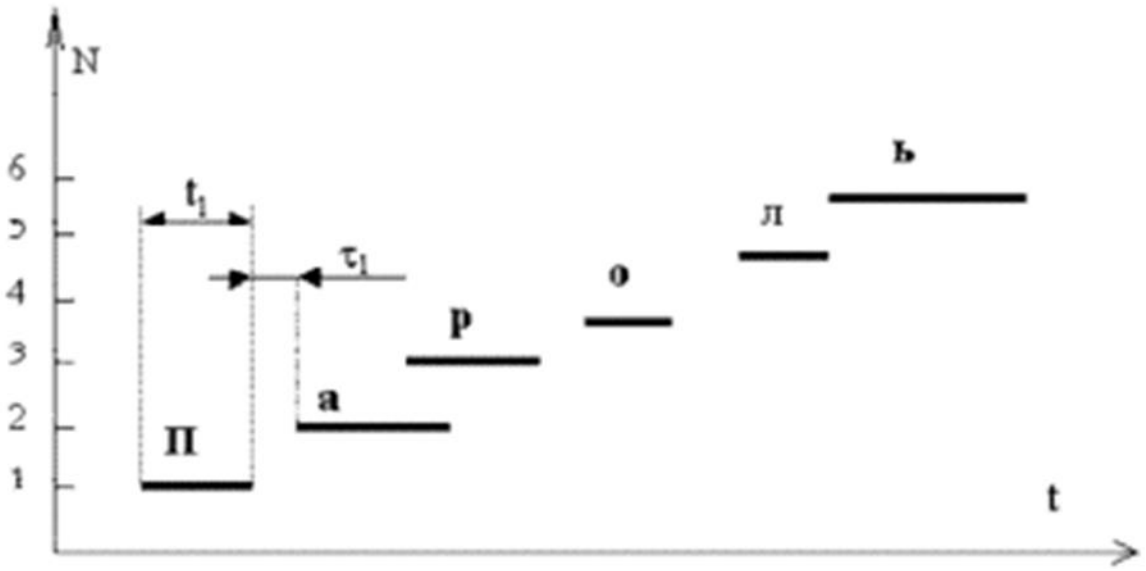


Рис. 1.3. Часова діаграма введення слова «Пароль»

Довжина парольної фрази для такої технології біометричної ідентифікації є важливою характеристикою.

Як показує практика парольна фраза повинна бути такою, щоб вона легко запам’ятовувалась та містила від 21 до 42 нажимань клавіш. Для синтезу

парольних фраз допустимо використовувати слова з сенсом зі словника. Під час набору парольної фрази можна допустити помилку в один два символи, через що суттєво погіршується стійкість такої фрази [13].

Завдяки обчисленням математичних сподівань і дисперсії параметрів, які піддані контролю, можна отримати біометричні еталони для введень парольних фраз. У обчисленнях важливим є фільтрування з вибірки дефектних прикладі чи аномальних викидів [14-15]. Питання про присутність в користувача індивідуального клавіатурного почерку для такої технології біометричної ідентифікації є, мабуть, найскладнішим. Для відповіді на дане запитання та виявлення міри стабільності та індивідуальних ознак клавіатурного почерку кожного користувача розробляються спеціальні обчислювальні процедури.

Ідентифікація за почерком миші

Наявні дослідження по моніторингу маніпулятора мишки під час роботи користувача в системі демонструють надійність розпізнавання 0,8 – 0,9. Тут відбувається розбиття екрану на зони, в яких найчастіше знаходиться курсор миші, та піддаються аналізу параметри руху миші між цими зонами кожні дві хвилини.

У праці [16] запропоновано моніторити весь процес розвитку системи «користувач-миша» на протязі «потенційно необмеженого» періоду свостережень за користувачем.

В першу чергу потрібно визначитись зі способомвідображення наборів числових значень використовуючи ідентифікацію за динамічними характеристики. Для аналізу почерку може бути виділення координат певних точок (екстремуми – це такі точки, які характеризуються розриви почерку) і інші особливості траекторії. Накопичення бази зразків характеристик зразків можна розпочати після вибору ключових значень. Так на підставі порівнянь з цими значеннями (еталонними зразками) здійснюватиметься ідентифікація.

Крім того, потрібно встановити необхідні правила: усі траекторії будуть

вважатись осмисленими. У цьому випадку здійснені траєкторії обумовлені наступними чинниками: антропологічними, психологічними та фізіологічними.

Зрозуміло, що антропологічні характеристики людини (розміри зап'ястя та довжина ліктьового суглоба) впливають на характеристику радіусу кривизни траєкторії. Фізіологічні ж дані, тобто структура м'язів плечового та ліктьового суглобів, впливають на динаміку руху (швидкість та прискорення руху курсору). Проте і психологічні чинники теж мають вплив на вище згадані характеристики, що вводить ще і елементи звички під час виконання роботи. Відповідно, згадані чинники є у взаємозв'язку між собою та завжди впливають на процес утворення траєкторії. В загальному в задачі аналізу вказаних траєкторій є аналоги з задачами аналізу рукописного тексту чи рукописних підписів. Однак комп'ютерні системи дають змогу розглянути такий процес в динаміці та скористатись додатковою інформацією про динаміку курсору.

Сьогодні розроблено декілька підходів для аналізу отриманих на цьому етапі характеристик:

- застосування байєсівських мереж;
- застосування нейронних мереж;
- застосування прихованих моделей Маркова;
- статистичний аналіз: даний аналіз здійснює обчислення середнього значення кожного із головних, середньоквадратичного відхилення та здійснює перевірку належності головних значень еталону, який пред'являється, довірчим інтегралом, отриманих у результаті аналізу еталонів.

Аналіз почерку миші можна здійснювати як повністю, так і виконуючи попередню сегментацію почерку з наступним аналізом цих сегментів. Можна застосовувати спектральний аналіз, при аналізі почерку як цілісного об'єкту.

Результатом огляду способів біометричної ідентифікації особи встановлено, найперспективнішими для подальших досліджень та найневивченішими є динамічні методи ідентифікації особи за біометричними

даними, які грунтуються на аналізі індивідуальності підсвідомих рухів.

Скожімо, методи, які проводять аналіз особливостей інформаційного (комп'ютерного) почерку. Сьогодні це дуже актуально, коли неможливо уявити майже кожне робоче місце без персональних комп'ютерів.

Дешевизна та простота в реалізації є однією з головних привабливих сторін динамічних методів ідентифікації особи за біометрією і, скажімо, розпізнанні особи за динамікою комп'ютерного почерку, тому, що в такому випадку дороге устаткування, наприклад, як для сканування зіниці ока, не потрібне. Ефективно протидіяти інформативному шпигунству та витоку інформації дозволить реалізація таких систем, які здійснюватимуть контроль за допущенням користувачів до конфіденційної інформації. Однак, ідентифікація за комп'ютерним підписом виграючи в дешевизні та простоті, програє у точності розпізнавання.

Потрібно зазначити, що найефективнішими системами захисту є такі системи, у котрих поєднані як біометричні способи, так і апаратні засоби аутентифікації, чи ті, в яких поєднані різні способи біометричного розпізнавання. Так, комбінуванням різних способів біометричної аутентифікації можна створити дуже надійну захисну систему. Доказом чого є зацікавленість провідними виробниками програмних забезпечень до таких технологій.

Відповідно у наступних дослідженнях доцільним буде сконцентрування уваги на підвищенні якості розпізнавання користувача за допомогою динамічних методів ідентифікації особи за біометричними показниками з застосуванням інноваційних методик статистичного та ймовірнісного моделювання.

1.3 Основні засади роботи систем біометричної ідентифікації

Координація діяльності комерційних фірм, державних організацій та

лабораторії, які займаються проблемами біометрії, здійснюється біометричним Консорціумом (APICosorcium). Є такі провідні виробники біометричних систем: BioLink Technologies, Bioscrypt, Ethentica, DigitalPersona, Identix, Neurotechnologiya, Precise Biometrics, Staflink, Veridicom та ін.

Задля автоматичної реалізації процедур ідентифікації, зазвичай, розробляються біометричні системи, які реалізують такі основні функції:

- фіксація (реєстрація) біометричних характеристик;
- попередня обробка матеріалів реєстрації;
- витяг біометричних ознак з матеріалів реєстрації;
- порівняння отриманих біометричних даних із заздалегідь сформованим еталоном (шаблоном, макетом);
- прийняття рішення про допуск (не допускаючи) користувача до заданих ресурсів та послуг.

Зважаючи на перераховані функції, в біометричній системі можна підкреслити два канали та, згідно з чим, два режими (чи етапи) роботи. Структурна схема біометричної системи представлена на рис 1.4. [17-19]

Перший етап (канал системи) відповідає за навчання системи ідентифікації для кожного користувача. Результатом даного етапу – є формування біометричного зразка (шаблону) користувача.

На другому етапі здійснюється ідентифікація користувача за результатами порівняння еталонними (збереженими в базі) характеристиками з його поточними біометричними характеристиками та визначається спектр його прав та можливостей.

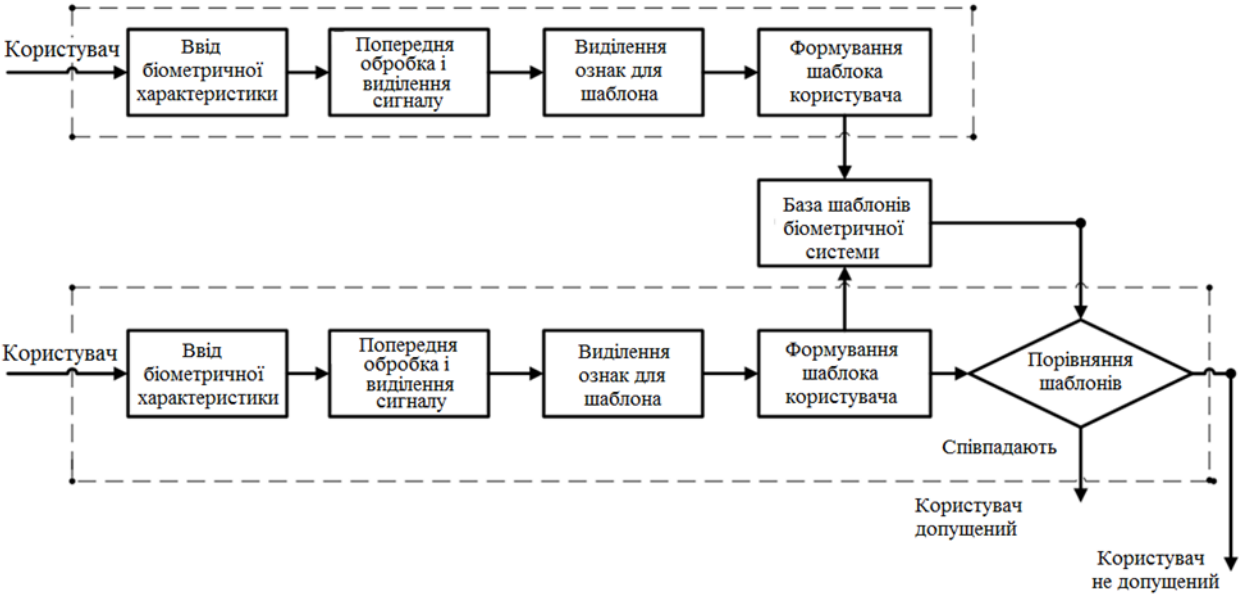


Рис 1.4 Спрощена схема біометричної системи

Відсутність єдиної системи визначення надійності є значною проблемою при побудові біометричних систем. Тому нижче проаналізуємо характеристики біометричних систем.

Основою роботи біометричних систем є математична статистика (а саме, перевірка гіпотез), алгоритми котрої часто використовуються в багатьох сучасних технічних системах, таких як: радіолокація (різні радари), зв'язок, та безліч баєсівських систем. Помилки першого і другого родів можуть бути прийнятими в якості головних ознак біометричної системи, яка будуться на статистичній теорії перевірки гіпотез (тестів). В теорії радіолокації ці помилки мають назву «помилкова тривога» та «пропуск цілі», а в біометричній автентифікації, звичними є поняття – FAR – помилкове розпізнавання та FRR – помилкова відмова. Поняття помилкового розпізнавання охарактеризовує імовірність співпадіння біометричних особливостей двох користувачів. Помилкова відмова ж показує імовірність заперечення у доступі користувачу, у якого є доступ.

Друге поняття – ймовірність відмови доступу користувачу, у якого є доступ.

В якості оптимального варіанту вибору значень вище згаданих помилок багато авторів пропонують використання порівняльної характеристики EER (EqualErrorRate, коефіцієнт помилок). Така характеристика визначає точку, при якій величина FAR таFRR є ріними.

Розглянемо дві щільності ймовірностей, характеризуючих шалон користувача та шаблон некористувача, для пояснень введених характеристик біометричних систем. Звісно можна припустити, що такі шаблони можуть задаватись у вигляді нормальних розподілів. Через те, що шаблон користувача отриманий в процесі навчання системи, його основна характеристика (математичне значення) *q1*матиме велике значення. Шаблон отриманий оперативно у процесі застосування біометричної системи, користувачем-хакером, котрий намагається проникнути в систему, для шаблону матиме характеристику *q0*.

Введемо і третю величину*gh*, ця величина визначатиме рішення, які приймаються. В результаті аналізу біометричних шаблонів, збережених у базі системі та оперативно отриманих біометричних характеристик, потрібно прийняти рішення про віднесення користувача до користувачів системи, тобто допуск поточного користувача, або недопущених до ресурсів системи (користувачів хакерів).

При найпростішому випадку рішення при двох взаємо виключаючих умовах:

- умова A_1 – біометричні характеристики належать користувачу системи;
- умова A_0 – біометричні характеристики належать користувачу, який не має допуску до ресурсів системи (хакеру);

Дані умови є невідомими при автоматичному прийнятті рішення в системі.

Під час аналізу шаблону та біометричних характеристик поточного користувача, для кожної умови відповідають два види рішень:

- Рішення $\widehat{\mathrm{A}}_1$ – біометричні характеристики відповідають шаблону, збереженому в базі системи;
- Рішення $\widehat{\mathrm{A}}_0$ – біометричні характеристики належать недопущеному до ресурсів системи користувачу-хакеру.

В такому випадку є можливих чотири ситуації суміщень випадкових подій «рішення» та «умови»:

- $\widehat{\mathrm{A}}_1\mathrm{A}_1$ – правильний допуск користувача до ресурсів системи;
- $\widehat{\mathrm{A}}_1\mathrm{A}_0$ – помилковий пропуск користувача-хакера до ресурсів системи, помилка 1-го роду (помилкове розпізнавання, FAR,FalseAcceptanceRate);
- $\widehat{\mathrm{A}}_0\mathrm{A}_1$ – помилкова заборона допуску користувача (користувач системи сприйнятий як хакер), помилка 2-го роду (помилкова відмова, FRR,FalseRejectionRate);
- $\widehat{\mathrm{A}}_0\mathrm{A}_0$ – правильна заборона допуску користувача-хакера до ресурсів системи.

Вище перерахованим ситуаціям можуть відповідати чотири ймовірності їх поєднання, сума яких дорівнює одиниці:

$$P\left(\widehat{\mathrm{A}}_1\mathrm{A}_1\right) + P\left(\widehat{\mathrm{A}}_1\mathrm{A}_0\right) + P\left(\widehat{\mathrm{A}}_0\mathrm{A}_1\right) + P\left(\widehat{\mathrm{A}}_0\mathrm{A}_0\right) = 1 \qquad (1.1)$$

Зазвичай, для кожного помилкового рішення ставлять у відповідність деяку ціну – вартість помилки $r_{ik}(i = 0{,}1); k = 0{,}1$. Ціну помилки можна ввадати рівною нулю для безпомилкових рішень, тобто $r_{11} = r_{00} = 0$. В такому випадку біометричну систему можна охарактеризувати середньою ціною (математичним сподіванням ціни) помилкових рішень:

$$M\{r\} = \bar{r} = r_{01} \cdot P\left(\widehat{\mathrm{A}}_0\mathrm{A}_1\right) + r_{10} \cdot P\left(\widehat{\mathrm{A}}_1\mathrm{A}_0\right) \quad (1.2)$$

Із порівнювальних біометричних систем кращою варто вважати таку систему, яка задовольняє мінімуму ціни $M\{r\}$ – критерію мінімуму середнього ризику.

Виходячи з того, що зазвичай, є відсутньою інформація про апріорні (додослідні) ймовірності $P(\mathrm{A}_1)$ та $P(\mathrm{A}_1)$, важким є і розрахунок ймовірностей суміщення $P\left(\widehat{\mathrm{A}}_0\mathrm{A}_1\right)$ та $P\left(\widehat{\mathrm{A}}_1\mathrm{A}_0\right)$. Відповідно у таких випадках варто перейти до умовних можливостей, завдяки чому отримуються якісні показники досліджуваних систем.

Якісними показниками в умовах ідентифікації користувача у системі є умовні ймовірності правильного допуску до ресурсів

$$D = P\left(\widehat{\mathrm{A}}_1\middle|\mathrm{A}_1\right) = P\left(\widehat{\mathrm{A}}_1\mathrm{A}_1\right)/P(A_1) \quad (1.3)$$

та помилкової відмови (помилкової заборони допуску користувача)

$$\widehat{D} = P\left(\widehat{\mathrm{A}}_0\middle|\mathrm{A}_1\right) = P\left(\widehat{\mathrm{A}}_0\mathrm{A}_1\right)/P(A_1). \quad (1.4)$$

$$D + \widehat{D} = 1. \quad (1.5)$$

Умовні ймовірності помилкового розпізнання є якісними показниками для прийняття рішення під час ідентифікації користувача-хакера.

$$F = P\left(\widehat{\mathrm{A}}_1\middle|\mathrm{A}_0\right) = P\left(\widehat{\mathrm{A}}_1\mathrm{A}_0\right)/P(A_0). \quad (1.6)$$

та правильної заборони ідентифікації (допуску)

$$\hat{F} = P\left(\hat{\mathrm{A}}_0 \middle| \mathrm{A}_0\right) = P\left(\hat{\mathrm{A}}_0 \mathrm{A}_0\right)/P(A_0). \quad (1.7)$$

причому

$$F + \hat{F} = 1.$$

Користуючись наведеними вище співвідношеннями (1.3) – (1.7), вираз (1.2) для середньої ціни помилки може бути представленим у вигляді

$$\bar{r} = r_{01} \cdot \hat{D} \cdot P(A_1) + r_{10} \cdot F \cdot P(A_0)$$

або,

$$\bar{r} = r_{01} \cdot P(A_1) \cdot [1 - (D - l_0 \cdot F)], \quad (1.8)$$

де

$$l_0 = \frac{r_{10} \cdot P(A_0)}{r_{01} \cdot P(A_1)}. \quad (1.9)$$

При чому критерій оптимізації системи ідентифікації (доступу) за мінімумом середнього ризику зводиться до вагового критерію

$$D - l_0 \cdot F \to max. \quad (1.10)$$

Біометричні характеристики являються унікальними ідентифікаторами, проте їх не можна зберегти в секреті. Проте цей напрям є перспективним, та активно розвивається, саме тому він розглядається у роботі. У плані точності аутентифікації та собівартості реалізації метод, який оснований на аутентифікації за голосом є найперспективнішим серед усіх можливих типів біометричної аутентифікації.

1.4 Описовий аналіз проблематики голосової ідентифікації

Метод розпізнавання особистості за голосом існує з тих пір, як людина навчилась говорити. Тому переваги та недоліки цього методу відомі всім [1-4].

Перевагами даного методу – є зручність використання та дешевизна пристроїв введення. У методі перевірки голосу є дві позитивні відмінності, у порівнянні з іншими біометричними методами. По-перше, це є ідеальним способом для телекомунікаційних програм. По-друге, майже всі сучасні комп'ютери вже обладнанні необхідними апаратним забезпеченням. Зараз більше 20 компаній пропонує пристрої для голосової аутентифікації.

Ідентифікація за голосом використовує акустичні особливості мови, які відрізняються та в якійсь мірі є унікальними [1-4]. Такі акустичні зразки відображають як анатомію (наприклад, форму та розмір роту і горла), також і набуті звички (манера розмови, гучність голосу). Виконання технологій розпізнавання людини за голосом основане на аналізі наступних характеристик голосу: спектр голосового сигналу, тембр, сила звуку, інтонація, акцент, швидкість мовлення, носові звуки, вібрації в гортані і т.д. Взалежності від необхідності ідентифікації (впізнаванні) чи аутентифікації (підтвердженні) особистості, застосовуються різні методи розпізнання. Перетворення таких зразків у голосові моделі дало даному способу ідентифікації назву «поведінкова біометрія». В біометричній технології відбувається розбиття кожного вимовленого слова на кілька сегментів. Такий голосовий відбиток зберігається математичним кодом. Задля успішної ідентифікації людині потрібно відповісти на кілька запитань, відповіді яких є легко запам'ятовуваними. Наприклад: прізвище, ім'я, по батькові; дата народження, тощо. Окремі сучасні системи можуть створювати модель голосу та мають змогу порівнювати її з будь-якою сказаною фразою.

Недоліком біометричних систем ідентифікації особи за голосом варто

зазначити те, що важко зберігати в таємниці парольну фразу. Сучасні засоби ддя аудіо прослуховування (радіо жучки та інші пристрої прослуховування) дозволяють дають право зловмиснику несанкціоновано копіювати парольну фразу. Очікується, що для виключення небезпеки застосування зловмисника «магнітофонів» варто перейти до ідентифікації особи за довільними фразами. Потенційною протидією «магнітофонам» є використання випадкових розіграшів парольних фраз, та комбінування з іншими методами біометричної аутентифікації.

Основними перевагами голосової аутентифікації є [4]:

- дешевизна та наявність реєстраційних пристроїв в більшості стаціонарних та мобільних комп'ютерних пристроях;
- для обробки застосовуються часові ряди цифрових даних;
- природний та інтуїтивно зрозумілий людині спосіб взаємодії з системою завдяки голосу;
- верифікація за голосом можлива у використанні в темряві, відстані, та по стандартному телефонному каналу;
- верифікація за голосом має практично необмежений потенціал для зниження помилок за рахунок розширення числа ознак для аналізу та використання довших мовних повідомлень.

Недоліками голосової аутентифікації є [4]:

- через реверберацію приміщення створюються амплітудно-частотні характеристики мовного сигналу, а також до тривалого згасання коливань на форматних частотах звуку, через що здійснюється змикання. Також і відлуння породжує хибні піки в сигналі-залишку;
- вплив психофізіологічного стану особи на результати аутентифікації (труднощів у використанні системи може зазнавати людина з застудою чи ларингітом);
- важко зберегти в таємниці парольну фразу.

Аналіз розглянутих систем голосової аутентифікації та наукових робіт у даній галузі показує, що для введення мовної інформації, зазвичай, використовується один мікрофон. В той же час на телефонах, комп'ютерах та інших мобільних гаджетах встановлені двоканальні звукові карти.

Зауважимо, що основні характеристики (помили першого та другого роду) систем голосової аутентифікації, як і в інших біометричних системах, у значній мірі визначаються відношенням сигнал/шум в оброблюваних матеріалах реєстрації. Зауважимо, що дане співвідношення може збільшуватись, як у процесі побудови системи введення сигналу, так і за рахунок реалізації таких наступних процедур для цифрової обробки реєстрації реєстрованих матеріалів. Введення голосового сигналу користувача відбувається, як правила, на фоні зовнішніх заважаючи шумів та перешкоджаючих сигналів, наприклад, акустичних хвиль, зумовлених роботою апаратури комутації, серверів, домашніх пристроїв, автомобілів, кондиціонерів і т. д. Якщо шуми діють у смузі частот мовного сигналу, то ускладнюється завдання компенсації таких сигналів. Експериментальні дослідження спектру сигналу, зумовленого роботою комутаційної апаратури (маршрутизатори, комутатори), показали, що він охоплює велику смугу частот з максимумами в області 1, 3, 4.2 та 5 кГц.

Отже існує наукова задача для підвищення якості введення та виділення мовного сигналу користувача у системах голосової ідентифікації.

1.5 Висновки до розділу 1

Проведено аналіз задачі аутентифікації користувача, розглянуто чинники і способи аутентифікації. Розглянуто переваги і недоліки наявних способів аутентифікації.

Встановлено, що найперспективнішою в плані зниження рівня помилок

під час формування висновку про аутентифікацію є біометрична аутентифікація.

Розглянуто, статичні методи аутентифікації, які засновані на фізіологічних особливостях людини, та динамічні методи, які базуються на індивідуальних характерностях у поведінці людини – підсвідомі рухи у процесі виконання будь-якої дії.

Встановлено, що системи голосової аутентифікації мають низьку собівартість, простоту та ряд інших переваг. Сучасні системи голосової ідентифікації можуть бути суттєво модернізовані за рахунок впровадження методів обробки даних, які раніше досліджені та широко використовуються, і, насамперед, повинні бути модернізовані методи та програмно-апаратні засоби введення та виділення мовного сигналу користувача системи.

РОЗДІЛ 2

МЕТОДОЛОГІЇ ОБРОБКИ ГОЛОСОВИХ СИГНАЛІВ ДЛЯ ЗАДАЧІ ІДЕНТИФІКАЦІЇ ОСОБИ

2.1 Завдання ідентифікації особи

В працях [9, 20] було класифіковано основні області застосування опрацювання голосових сигналів, яку відображено на рис. 2.1. Близькою до задач аналізу/синтезу голосових сигналів є задача діагностики органів голосового апарату, тому, що у решти задач інформація про голосовий апарат, що є присутньою в сигналі, вважається надлишковою і не враховується [9, 21].

Рис. 2.1 Класифікація основних областей застосування опрацювання голосових сигналів.

Підходячи до розв’язання задачі аутентифікації особи за голосовим сигналом варто дослідити сам фізичний процес створення голосового сигналу та існуючі моделі голосових сигналів, які використовуються як в акустиці так і в

задачах їх аналізу/синтезу.

2.2. Аналіз процедури утворення голосового сигналу та моделей процесу породження голосу

Формування та розповсюдження звуків у голосовому тракті відбувається відповідно до основних законів акустики [22-26].Розглядаючи голосовий сигнал як акустичне коливання вчені намагались скласти систему диференційних рівнянь в частинних похідних, що описувала б рух повітря в голосовому тракті [9].Проте, складання та розв’язування таких рівнянь є дуже складним навіть для простих припущень щодо форми і втрат енергії в голосовому тракті [9]. Необхідно включати в рівняння такого типу часові варіації мовного апарату, зокрема зміни форми та твердості стінки, розсіяння потужності мовного сигналу внаслідок в’язкого тертя та переносу тепла для голосового тракту, резонанс в носовій порожнині тощо. Побудова таких рівнянь не отримала широкого поширення. Замість цього розглядають голосовий сигнал, який міг би бути розв’язком таких рівнянь. Головна складність полягає у тому, щоб аналітично описати голосовий сигнал через фізичні параметри системи, яка його утворила. Тому доречно розглянути фізіологічних особливостей процесу створення голосових сигналів та моделей голосового апарату.

В публікаціях [27, 28] мовний сигнал розглядається як остаточний акустичнийпродукт, який визначається станом та зміщеннями органів дихання, піднебуння, губ, щік та зубів, тобто його можна класифікувати як моторну поведінку, якої особа набула внаслідок тренування (навчання). Голосовий тракт моделюється порожнинним циліндром зі змінним перерізом [27]. Один кінець тракту починається з губ, а інший – з щілини яка веде до входу трахеї, утвореною голосовими складками. Зміна поперечного перетину у голосовому тракті відбувається під час руху артикуляційних органів. Якими є губи, щелепа,

язик та піднебінна стінка.

Схематичне зображення голосового апарату людини наведено на рис. 2.1.

Носовий тракт створює допоміжний шлях для розповсюдження звукових коливань. Він бере початок від піднебінної стінки та закінчується ніздрями. Величина акустичного зв’язку між ротовою та носовою порожнинам визначається розмірами проходу біля піднебінної стінки. Звукові хвилі можуть випромінюватись ротом і носом, взалежності від величини акустичного зв’язку.

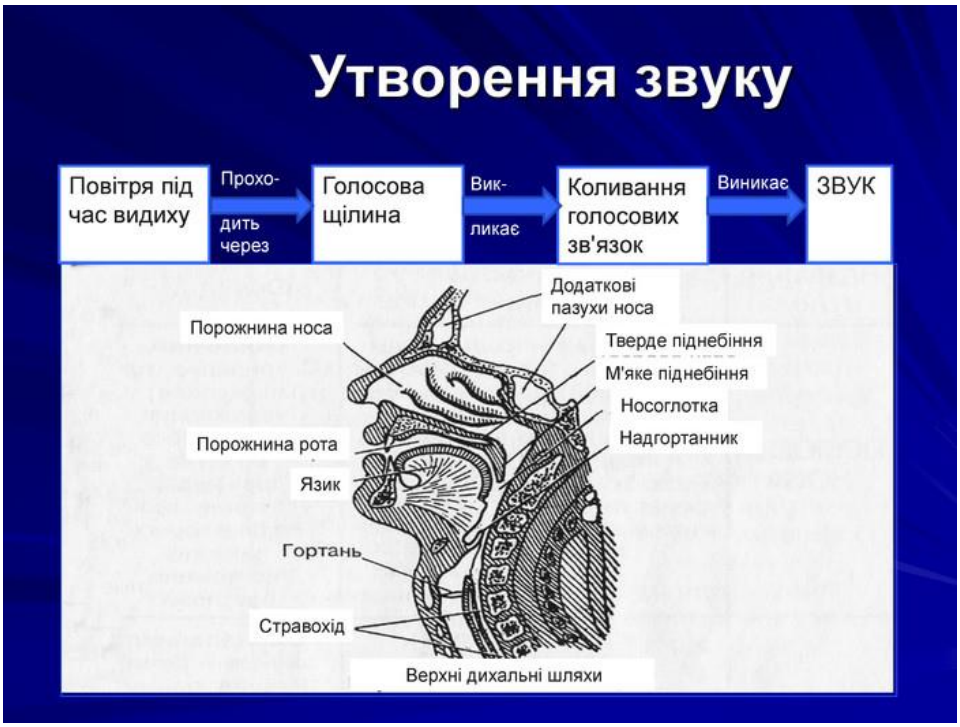


Рис 2.1. Зображення утворення звуку у голосовому апараті людини.

Голосовий та носовий тракти формують неоднорідні за січенням труба з втратами. Коливні процеси в таких трубах важко описати, навіть у випадку відсутності втрат. Через те, що найбільший поперечний розмір тракту є значно меншим за довжину хвилі, також в силу того, що поперечне січення труби не різко зменшується, що породжує відбивання хвиль, акустична система

наближено може бути описано одновимірним хвилевим рівнянням. В такому рівнянні, яке інколи називають рівнянням Вебстера, допускається синфазне розміщення фронтів хвилі по площі поперечного січення. Воно має такий вигляд [27]:

$$\frac{1}{A(x)}\frac{\partial}{\partial x}\left[A(x)\frac{\partial}{\partial x}\right] = \frac{1}{c^2}\frac{\partial^2 p}{\partial t^2}, \tag{2.1}$$

де $A(x)$ – площа поперечного січення голосового тракту, p – звуковий тиск, c – швидкість поширення звуку. В загальному випадку дане рівняння можна розв'язати лише чисельними методами не враховуючи втрат. Проте воно використовувалось для аналізу процесу утворення голосових звуків у працях Чиба і Каджиями, Унгехоера, Гейнца тощо.

Часто застосовується модель голосового тракту у виді трубки з неоднорідностями та залежною від часу площею поперечного перерізу (рис. 2.2). Даний підхід детально описаний в праці [9].

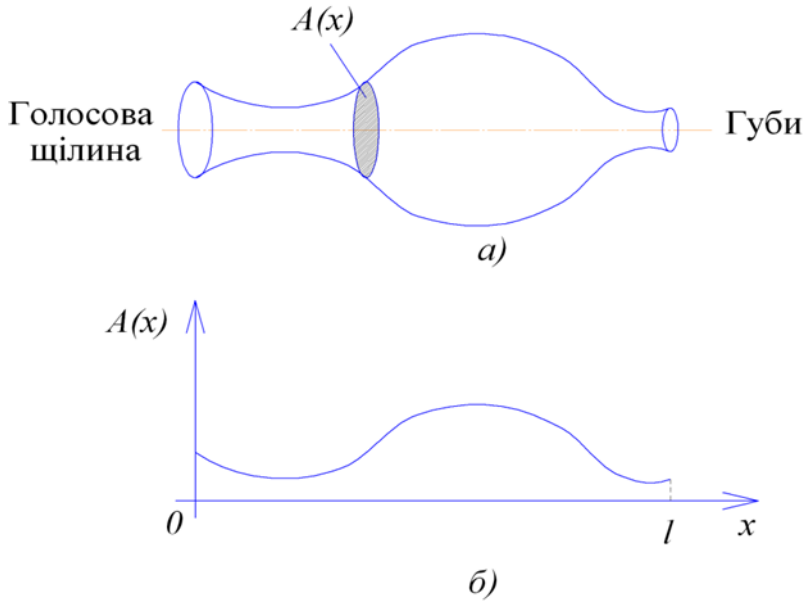


Рис. 2.2 Схематичне зображення голосового тракту у вигляді неоднорідної

труби (а), та функції площі її поперечного січення (б).

Для коливань, довжина хвиль яких перевищує розміри голосового тракту (зазвичай це у частотах нижче 4000 Гц), можна припустити, що взовж повздовжньої осі труби розповсюджується плоска хвиля. Наступний етап опрацювання базується на припущенні, що втрати внаслідок теплопровідності відсутні а в'язкістю у потоці повітря можна знехтувати. Застосовуючи закони збереження енергії та імпульсу Портнов довів [9], що звукові хвилі в голосовому тракті можуть бути описані такими рівняннями:

$$-\frac{\partial p}{\partial x} = p\frac{\partial\left(\frac{u}{A}\right)}{\partial t};$$
$$-\frac{\partial u}{\partial x} = \frac{1}{pc^2}\frac{\partial(pA)}{\partial t} + \frac{\partial A}{\partial t}. \qquad (2.2)$$

де $p = p(x,t)$ – залежить від координати x та часу t звуковий тиск,$u = u(x,t)$ – позначає швидкість потоку повітря, залежну від x і t, p є густиною повітря в певній області, c – швидкість звуку, $A = A(x,t)$ є залежна від координати та часу площі поперечного перерізу голосового тракту.

Навіть для простих форм труби неможливо отримати замкнуте вирішення рівнянь (2.2). Для повного вирішення диференціальних рівнянь мають бути задані тиск і швидкість потоку для значень x і t у областях голосової щілини і при губах, тобто щоб отримати розв'язок повинні бути задані граничні умови біля обох кінців труби. З боку голосової щілини граничні умови повинні відображати характер збудження, а з боку губ – ефект випромінювання.

Орім умов ліміту функції важливо сформувати функцію площі $A(x,t)$. Для протяжних звуків можна припустити, що A не змінне в часі. Однак таке припущення невірне для непротяжних звуків. Детальні вимірювання $A(x,t)$ є

складними та можуть виконуватись тільки для протяжних звуків. Одним із методів проведення таких вимірювань є метод, який оснований на одержані рентгенівських знімків голосового апарату. Ще один метод обчислення форми голосового тракту ґрунтується на акустичних вимірюваннях. Результати прямого вимірювання $A(x,t)$ за голосовим сигналом, вимовленим в нормальних умовах, описані в роботах Атала.

Під час створення голосу мускули грудної клітки та мускули черевної порожнини стають джерелом енергії [27]. Легені втягуються повітря під час розширення грудної клітки та опускання діафрагми. Його виштовхують рухи під час стискання грудної кліки а збільшення легеневого тиску. Внаслідок коливального руху голосових складок утворюються локалізовані звуки.

Повітряний потік має власну силу, з якою проходить голосовою щілиною. Сила являє собою рівняння часу що має залежність від числа добутку ширини на довжину голосової щілини. При застосуванні середніх значень гучності та частоти, хвилі, які створює голосова щілина загалом виглядають як трикутник. Значення частки тривалості імпульсів та загальних періодів коливань становить в межах 0,3-0,7. Це є причиною того, що обертони та гармоніки є частиною частотного спектру голосових складок. Амплітудні значення верхніх частотних складових зі швидкістю 6дБ на октаву зменшуються в наслідок форми імпульсів, близькій до трикутної.

Турбулентний повітряний потік у будь-якій точці збудження, який створюється голосовим трактом слугує іншим джерелом акустичного збудження.

Непрямі вимірювання та основні положення акустичної теорії голосотворення [28] дають підставу вважати, що спектр шуму в точні або в області його генерації відносно широкий та рівномірний. У формуванні спектру звукових хвиль найважливішими є порожники, які знаходяться перед звуженнями.

Наступним джерелом збудження служить тиск, створений в області змички. Під час раптового розкриття гортанної змички голосовий тракт збуджується через перехідний процес, який виникає в ньому. Перше наближення неперіодичного збудження і має властивість представлятись за допомогою стрибків тисків зі спектром, який може спадати оберено пропорційно відносно частоті.

В праці [29] запропоновано модель голосостворення, де на остові системи з динамічною чатотно-імпульсною модуляцією синтезується голосове збудження. Структурно така модель представляє собою послідовне з'єднання імпульсного пристрою з параметричним зворотнім зв'язком, динамічного фільтра, та формозадаючого фільтра. Така модель застосовується в задачах кодування голосових сигналів.

Як згадувалось раніше, задача діагностики голосового апарату є близькою до задачі аналізу/синтезу. Серед моделей аналізу/синтезу відомою є лінійна модель голосотворення, яку було розроблено Фантом в кінці 50-х років [30]. Відповідна структурна схема даної моделі представлена на рис. 2.3.

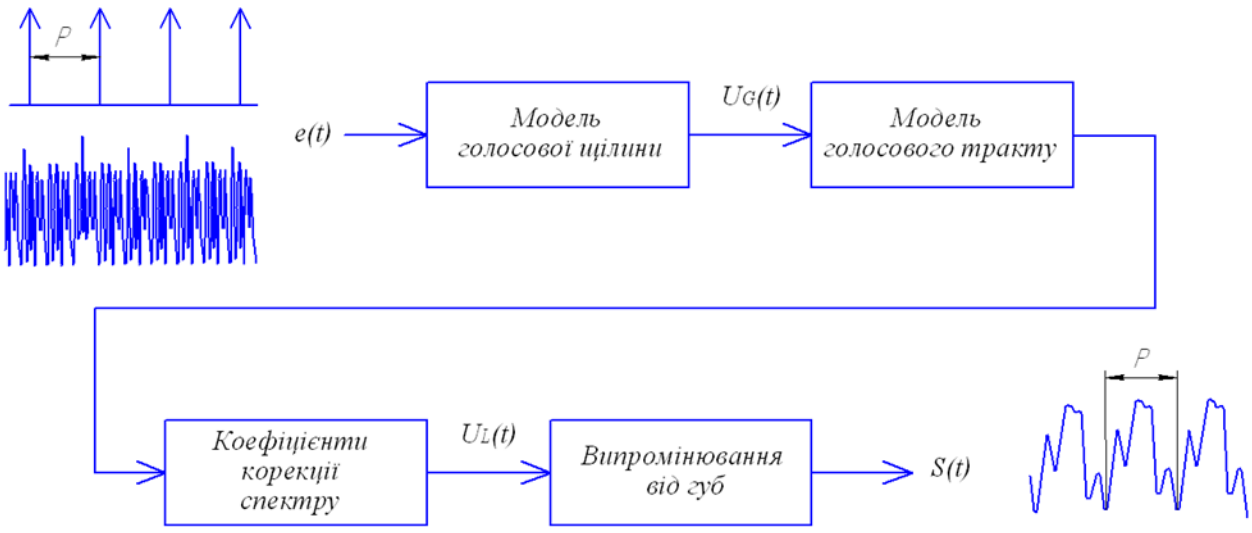


Рис. 2.3. Лінійна модель голосотворення.

Об’ємна швидкість хвилі в районі голосової щілини $U_G(t)$ моделюється вихідним сигналом двополюсного фільтру нижніх частот з часотою зрізу близько 100 Гц. Вхідний сигнал фільтру $e(t)$ є імпульсною послідовність з періодом P для локалізованих звуків та шумом з рівномірним спектром для нелокалізованих звуків. Така модель є окремим випадком більш загальної моделі, оскільки в цій моделі не змішуються імпульсні та шумові сигнали для моделювання локалізованих фрикативних звуків чи під’єднується ще одна гілка з фільтром для моделювання назальних звуків. Голосовий тракт в такій моделі є полюсним фільтром, який складається з невеликої групи каскадно включених двополюсних резонаторів. Кожен резонанс, у цій моделі, визначається як форманта з відповідною частотою та смугою.

Подекуди зручно об’єднати моделі голосового траку, збудження та випромінювання в одну систему, запропоновану Шеноном [9], яка виглядає як на рис. 2.4.

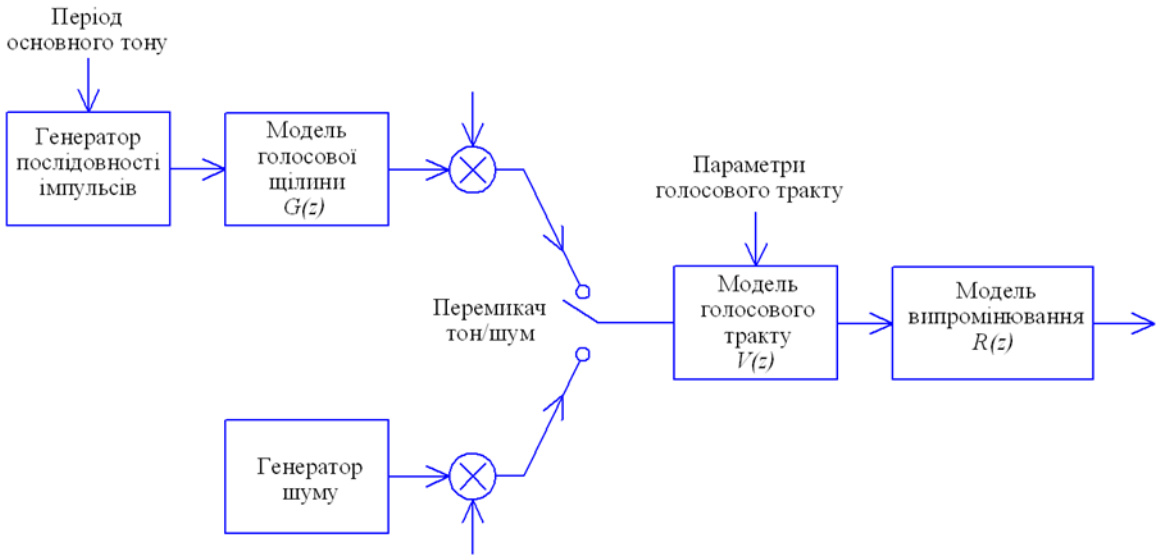


Рис. 2.4. Схема цифрової моделі голосотворення

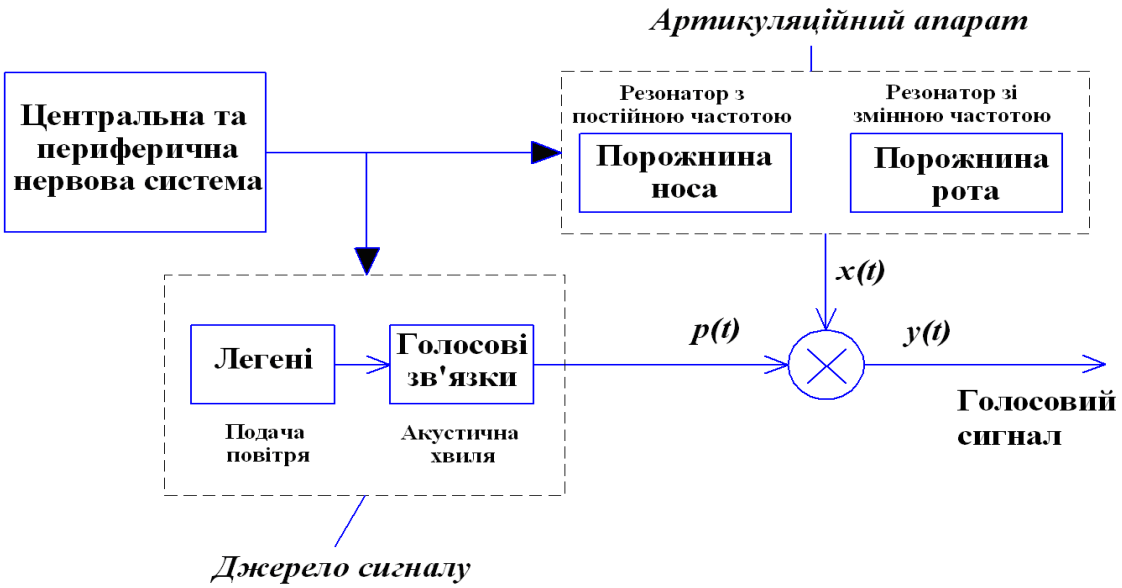
Проте, дана модель має певні обмеження. В основі першого обмеження лежить в характер змін параметрів. При вимовленні протяжних звуків, таких як голосні, зміна параметрів проходить повільно, тому така модель володіє достатньою точністю. Для короткотривалих звуків, модель стає неадекватною. Передбачено, що на інтервалах 10-20 мс параметри модлей є постійними. Для звуки, в яких повільно змінні параметри у часі можна відобразити структуру завдяки функції передавання $V(z)$. Інше обмеження засноване на відсутності нулів функції передавання, які необхідні для точних описів фрикативних та носових звуків. У третьому обмеженні використовується спрощене дихотомічне розділення типів збудження: локалізоване та нелокалізоване. Дихотоміному розділенню не підлягають локалізовані фрикативні звуки. Дуже тяжко усувати такі обмеження за допомогою простих складань сигналів збуджень двох типів, через те, що у фрикативні звуки мають залежність імпульсу основного тону до шумового збудження. Зображена на рис. 2.4 модель має ще один недолік, який полягає у повторюваності поріоду T імпульсів голосових збуджень, кратною з інтервалом дискретизації.

2.3 Основні вимоги до методології обробки аудіо сигналів для задачі голосової ідентифікації особи

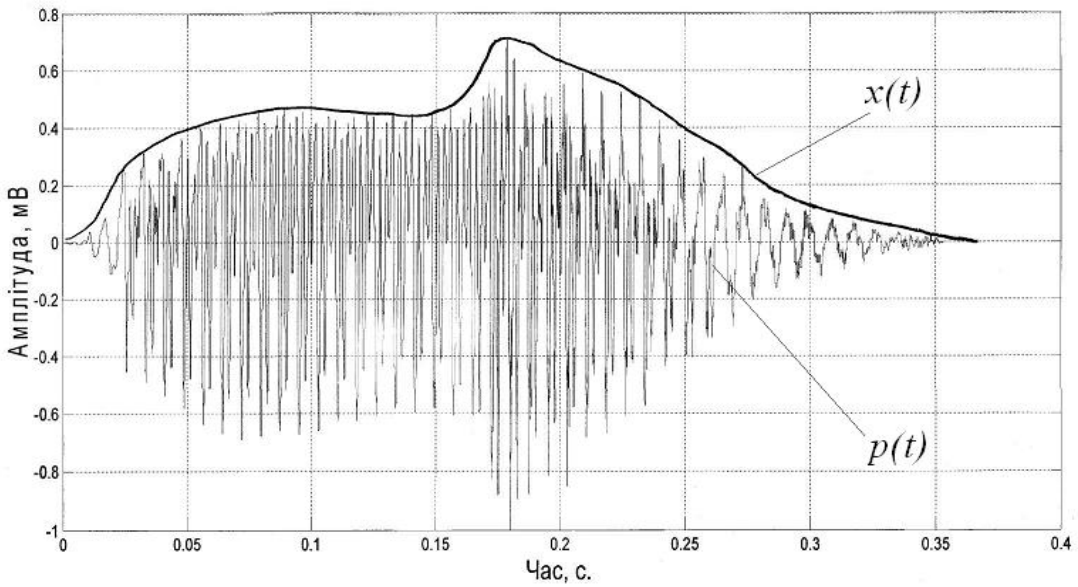
Аналіз голосового сигналу повинен проводитися методом, який дозволить виокремити характерні ознаки сигналу, які не змінюються в часі та служили б унікальними маркерами індивіда, за якими його можна однозначно ідентифікувати. Розглянемо основні способи опрацювання голосових сигналів.

Параметри голосового тракту, які динамічно змінюються в залежності від фізіологічного та емоційного стану особи, розбивають на 4 типи: спектрально-часові, амплітудно-частоні, кепстральні та нелінійно-динамічні.

Мовний апарат людини утворює періодичний звуковий сигнал, взаємодіючи з повітрям, яке виштовхується з легенів. Голосові складки створюють характерний основний тон, характеристики якого визначаються послідовністю нервових імпульсів $p(t)$ (рис. 2.5, а). Артикуляцію можна моделювати як комплекс резонаторів чи фільтрів, з фіксованими або варіабельними частотами, що відтворюють фонетичний профіль сигналу $x(t)$(рис. 2.5, а, б).



а)



б)

Рис. 2.5. Процес створення голосового сигналу:

а) – структурна схема процедури створення голосового сигналу, б) – голосовий сигнал, який є результатом процесу створення голосових звуків

Так, мовний сигнал $y(t)$може бути представлено у вигляді складного сигналу з амплітудною модуляцією, що визначається формулою:

$$y(t) = p(t) \cdot x(t) \tag{2.3}$$

де $y(t)$ є повідомленням (голосовим сигналом, (рис. 2.5, б)); $p(t)$ є несучою хвилею тиску, створеною джерелом; $x(t)$ – є функцією, яка визначає обвідну мовного сигналу в тому часому інтервалі, якому відповідають зміни стану органів артикуляції. Аналізуючи $x(t)$x(t) та $p(t)$ в частотному, часовому, частотно-часовому представленнях, можна однозначно встановити особу користувача. Разом зхарактеристиками основного тону, які є визначальними ознаками конкретної особи, в складі несучої компоненти виділяють так звані форманти – максимуми, властиві спектральній характеристиці. Ці максимуми також можна застосувати з метою аутентифікації особи. В зв'язку з цим, доцільно розглянути способи визначення частот основного тону та формант.

2.4 Метод дослідження голосового сигналу з метою ідентифікації користувача

2.4.1 Методи визначення частоти основного тону мовного сигналу

Ідентифікація основного тону мовного сигналу становить актуальну задачу вже багато десятиліть [31]. Найпростішим методом знаходження періоду

основного тону (ПОТ), значення якого оберненим до ЧОТ, є піковий метод [9, 21], який грунтується на оцінці структури голосового сигналу у часі. Процедура пошуку ПОТ забезпечує здійснення пошуку його значення на першому локалізованому сегменті та початки кожного періоду, який не перевищує значення максимумів амплітуди. Після чого, подальше максимальне значення сигналу знаходять у області можливих значень основного тону. На даному кроці значенням ПОТ вважається відстань між максимальними значеннями. Такий метод є ефективнішим у випадку без шумових сигналів при наявній першій чи другій-третій гармоніці основного тону, метод є дуже чутливим до задання меж максимумів та мінімумів у допустимих значеннях ПОТ.

Також, відомим кепстральний метод обчислення основного тону [9,21]. Кепстральне (гомоморфне) обчислення проводиться чотирьма етапами. Порція відліків оцифрованого голосового сигналу U зважують за допомогою вагового вікна. Переважно використовується вікно Хеммінга

$$K(x) = (0{,}54 + 0{,}46\cos\pi x) \cdot U(1 - |x|) \tag{2.4}$$

Далі, зважену порцію обробляється перетворенням Фур'є. Наступним етапом обчислюється логарифм амплітуди гармоніки. Одержані результати обробляються за допомогою зворотнього перетворення Фур'є (результат даного перетворення носить назву кепстр):

$$C(n) = \frac{1}{2\pi}\int_{-\pi}^{\tau} \log\left|X(e^{j\omega})\right| e^{j\omega n} d\omega \tag{2.5}$$

Виражений максимум кепстра у діапазоні 2-20 мс свідчить про, що ділянка сигналу, яку досліджується, є локалізованою, а період аналізованого сигналу визначається розміщенням максимуму. На ділянці аналізу виконується

зворотне перетворення Фур'є комплексного логарифма спектру потужності сигналу для визначення кепстра.

У запропонованому Рабінеро-Гоулдом методі по виділенню основного тону процедура його виділення відбувається завдяки знаходженню ПОТ через відстань між максимумами, мінімумами, та максимальних і мінімальних часових реалізацій сигналу. Одержані оцінки за трьома відстанями тривалостей ПОТ потрібно розглядати комплексно для поточних, попередніх та наступних ПОТ. Під час порівняння всіх оцінок ПОТ при частому зустрічанні в сукупності оцінок ОТ така оцінка вважається як оцінка поточного ПОТ.

При фільтровому методі визначення ПОТ сигнал перед початком аналізу фільтрується вузько смуговим фільтром нижнього значення частот. Смуга частот пропускання має бути в діапазоні 50-250 Гц – для чоловічого голосу, а при жіночому голосі – 70-450 Гц. Після цього проводиться обробка піковим методом.

Праця [21] описує метод визначення частоти ОТ, який ґрунтується на лінійному передбаченні, такий алгоритм має назву SIFT. У основі даного методу лежить знаходження максимального піку автокореляційної функції.

На першому етапі еліптичним фільтром нижніх частот проводиться виділення частотного діапазону 0-1 кГц, у якому є наявна ЧОТ.

Після чого, за теоремою Котельникова знижується частота дискретизації до 2 кГц методом проріджування сигналу. Такий сигнал за використанням автокореляційного варіанту проходить обробку лінійним передбаченням. Як результат, такого опрацювання будуть визначенні коефіцієнти лінійного передбаченні. На їх основі буде обчислено похибку передавання. Після чого обчислюється автокореляційна функція похибки передавання та знаходяться максимуми похибки, що є виділенням максимальних значень у спектрі аудіо сигналу людини.

Найбільш поширений метод знаходження ПОТ є автокореляційний [32-

36].Початкова оцінка ПОТ визначається місцезнаходженням максимального значення автокореляції в межах визначеного інтервалу [21]:

$$y(t) = \frac{1}{T}\int_{-T/2}^{T/2} x(t)x(t-\tau)d\tau, \quad (2.6)$$

де τ – пробний період, T – інтервал оцінювання.

2.4.2 Метод форматного аналізу [21]

Нині існує два основні варіанти по розпізнаванню мовних сигналів, це фонемний та формантний. У формантному способі розпізнавання здійснюється за формантними частотами (частотами розміщення максимумів обвідної амплітудних спектрів). Активну участь у творенні мови беруть аудіо коливання ні чотирьох частотах, які створюються в результаті роботи порожнин голосового тракту, які резонують. Нинішні засоби розпізнання мови грунтуються на спектральному аналізі, за допомогою якого можна виділяти найінформативніші складові з аудіо сигналів людини. Це формантні частот та шум. На рис. 2.6 зображено вигляд амплітудного спектру голосового сигналу та вказано розміщення перших трьох формант.

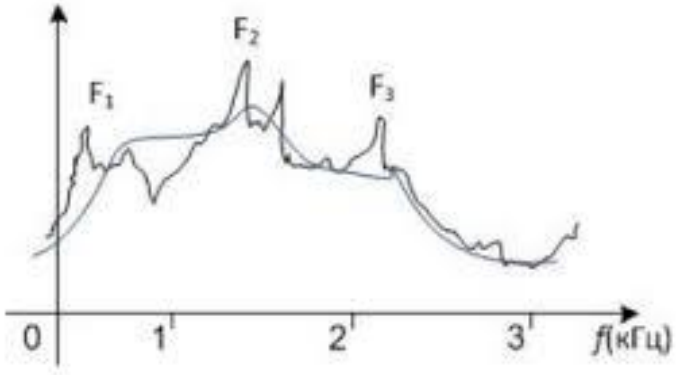


Рис. 2.6. Вигляд амплітудного спектру голосового сигналу та розміщення перших трьох формант.

Метод ідентифікації за формантними частотами придатний до використання проте має недоліки, зумовлені наявноя випадковою складовою у структурі голосових сигналів, що призводить до появи мінливості у розміщенні частот. У такому випадку необхідно застосовувати додаткові ознаки голосового сигналу, однією з яких може бути поряд з частотою основного – обвідна голосового сигналу у часовій області.

2.5 Висновки до розділу 2

Виконано дослідження механізмів і вивчено способи опису генерації голосового сигналу, а також запропоновано вимоги до способів аналізу мовних сигналів з метою аутентифікації користувача. Методика опрацювання мовного сигналу повинна давати змогу встановити інформативні характеристики, незалежні від часу, а залежні лише від особливостей конкретного мовного апарату, таким чином придатні для безпомилкової ідентифікації особи. Можна бачити, що голосовий сигнал є складним амплітудно-модульованим сигналом, для якого дослідження несучої складової у частотному, часовому, частотно-часовому представленнях дозволяє визначити особу.

Основною ознакою користувача є частота основного тону несучої складової сигналу, допоміжними ознаками – форманти (максимуми спктральної характеристики.

Піддано аналізу способи визначення частот основного тону та перших формант.

РОЗДІЛ 3

ЕКСПЕРИМЕНТ З ВІДБОРУ ГОЛОСОВИХ СИГНАЛІВ

3.1 Обгрунтування структури експерименту з відбору голосових сигналів

Перед початком проведення експериментального відбору голосових сигналів потрібно провести планування [37,38]. Воно передбачає організацію експериментальних досліджень, що дасть можливість зібрати необхідні дані, використати статистичні методи для їх аналізу та зробити об’єктивні висновки. Проведення експерименту, відповідно, повинне включати наступні етапи [37]:

- формулювання задачі. На даному етапі необхідно зкоректувати всі уявлення про мету експерименту;
- вибір факторів та рівнів. На даному етапі необхідно визначити незалежні змінні та фактори, які будуть досліджуватись у експерименті, а також значення та рівні цих факорів;
- проведення експерименту;
- аналіз даних.

Перші два етапи проведення експерименту були розглянуті та проаналізовані у першому і другому розділах. На третьому етапі необхідно провести вибір схеми активного експерименту для проведення відбору голосових сигналів і обгрунтувати характеристики технічних засобів, які в неї входять

Рис. 3.1 відображає схему експериментального відбору голосових сигналів

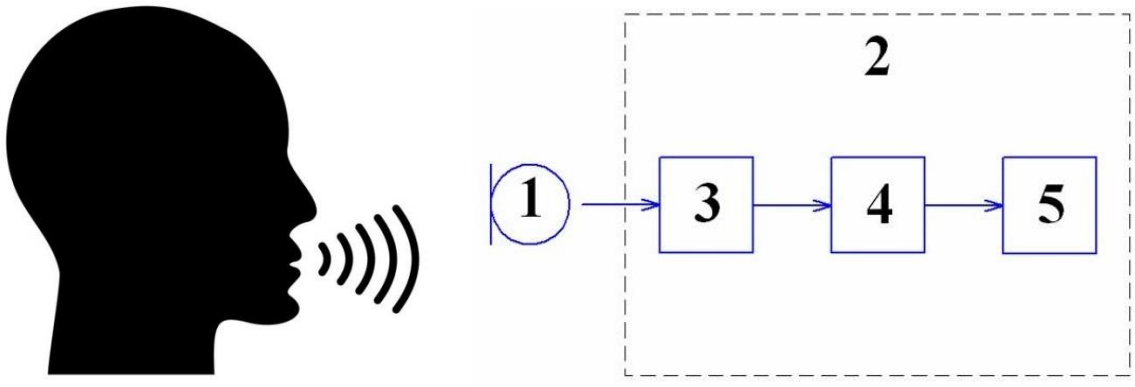


Рис. 3.1. Схема експериментального відбору для визначення спектру мовного сигналу: 1 – приймач (мікрофон); 2 – аналізатор (комп’ютер); 3 – спеціалізований пристрій (звукова карта); 4 – програмна для отимання спектру сигналу; 5 – представлення результату.

Акустична хвиля від джерела за допомогою приймача 1 перетворюється у електричний сигнал і направляється до спеціалізованого пристрою 3 на комп’ютері 2. Результат аналізу сигналу 4 відображається на моніторі 5.

3.2 Обгрунтування відбору параметрів мікрофона

Вибір мікрофона повинен забезпечити отримання інформативних характеристик сигналу [39] та має мати достатні

- чутливість – відношення вихідної напруги на мікрофоні до діючого на мембрану звукового тиску;
- динамічний діапазон – тобто різницю між граничним звуковим тиском та власними шумами;
- робочий діапазон частот;
- частотну характеристику;

- відповідну характеристику направленості, тобто – залежність чутливості напрямку до джерела звуку.

Просторова напрямленість у багатьох випадках є визначальною характеристикою. Її можна відобразити діаграмою у полярній системі координат. За типом характеристики направленості розрізняють такі види мікрофонів: ненаправлені, односторонньо та двосторонньо направлені. Щоб отримати мовний сигнал використовують ненаправлений або односторонньо направлений мікрофон, щоб мінімізувати шкідливий вплив акустичних шумів. Важлива також частотна характеристика мікрофона, яка повинна бути достатньо рівномірною в діапазоні частот 20-200 Гц, (характерний для перших формант), та до 14 кГц для свистячих звуків. Відомо, що конденсаторні мікрофони мають набагато більш рівномірну частотну характеристику, ніж електродинамічні. Для електродинамічних мікрофонів, що їх частотний діапазон лежить в області 60-12 кГц, а в низькочастотній області мікрофони частотна характеристика мікрофона значно спадає, через що призводить знижується величина амплітуди першої форманти (70-200 Гц для чоловічого голосу).

На основі попереднього аналізу приймаємо рішення про використання для відбору голосових сигналів конденсаторного мікрофона.

Сигнал з реєструю чого пристрою (мікрофона) надсилається на вхід АЦП у звуковій карті), яка проводить попереднє опрацювання та оцифрування сигналу. Проведемо обгрутнування основних параметрів АЦП звукової карти.

3.3 Обгрунтування відбору параметрів АЦП у звуковій карті

До основних параметрів АЦП у звукових картах відносяться розрядність і частота дискретизації вхідного сигналу [39].

Динамічний діапазон пристрою залежить від розрядності. Він виражається

залежність (3.1)

$$D = 20\lg(N), \tag{3.1}$$

де N – число рівнів квантування, яке має залежність від розрядності пристрою.

Так, для восьмибітного (восьми розрядного) АЦП звукових карт $N = 256, D = 48$ дБ, а для шіснадцятибітного АЦП $N = 65536$, $D = 96$ дБ. Професійні звукові карти які мають АЦП вищої розрядності (18 і 20) використовують для складного комбінованого оброблення звуку, монтажу, конвертування тощо.

Для максимальної похибки квантування відносна величина має дорівнювати $1/N$ для нормального сигналу. Для рівенів шумів квантування АЦП звукових карт оцінювання позначається цією ж величиною, представлено в логарифмічних одиницях (децибелах), та визначається виразом (3.2).

$$D = 20\lg(1/N), \tag{3.2}$$

Для трьох розрядного АЦП $N = 8, D = -18$ дБ; для восьмирозрядного АЦП – $N = 256$, $D = -48$ дБ; для шістнадцятибітного АЦП - $N = 65536$, $D = -96$ дБ; для вісімнадцятибітного АЦП $N = 262144$, $D = -108$ дБ; та для двадцятибітного АЦП $N = 1648576$, $D = -120$ дБ. Дані цифри наочно демонструють, що шум квантування спадає при збільшенні розрядності АЦП. Сьогодні стандартом у відтворенні оцифрованого звуку вважається прийнятним 16-розрядне представлення сигналу. На усунення впливу шумів квантування збільшення розрядності аналого-цифрового перетворювача не матиме вирішального впливу, оскільки визначальну роль відіграють шуми іншого

походження, зокрема теплові та імпульсні, створені елементною базою та контурами електроживлення обчислювальних засобів (типове значення - 96 дБ). Частота дискретизації для сигналу мікрофона може бути знайдена за допомогою теореми про відліки.

На основі теореми про відліки і технічних характеристик мікрофона проведемо вибір частоти дискретизації сигналу.

Людський голос може генерувати звук, частотою до 20кГц. Зважаючи на те, що обраний для запису звуків мікрофон, згідно паспортних даних, працю у діапазоні частот до 16 кГц, то частотна складова дискретизації має бути не меншою як 32 кГц.

Для реєстрації голосових сигналів обрано частоту дискретизації рівну 32 кГц та розрядність АЦП – 16 біт.

3.4 Висновки розділу 3

Обґрунтовано принципову схему експерименту для запису голосового сигналу, критерії вибору обладнання, зокрема мікрофона, АЦП, обчислювальних засобів.

Запропоновано методики реєстрації мовного сигналу та його опрацювання, які дозволять ефективно виділити інформативні параметри для задачі ідентифікації користувачів.

РОЗДІЛ 4

ОБРОБКА ГОЛОСОВИХ СИГНАЛІВ З МЕТОЮ ІДЕНТИФІКАЦІЇ ОСОБИ

4.1 Визначення частотних параметрів формант голосових сигналів

Відбір голосових сигналів однієї особи було проведено з використанням конденсаторного мікрофона і звукової карти персонального комп'ютера. При чому проводився відбір окремих голосових звуків [м] та [е]. Розрядність АЦП – 16 біт, частота дискретизації – 32 кГц. Вигляд реєстрограм відібраних сигналів наведено на рис. 4.1.

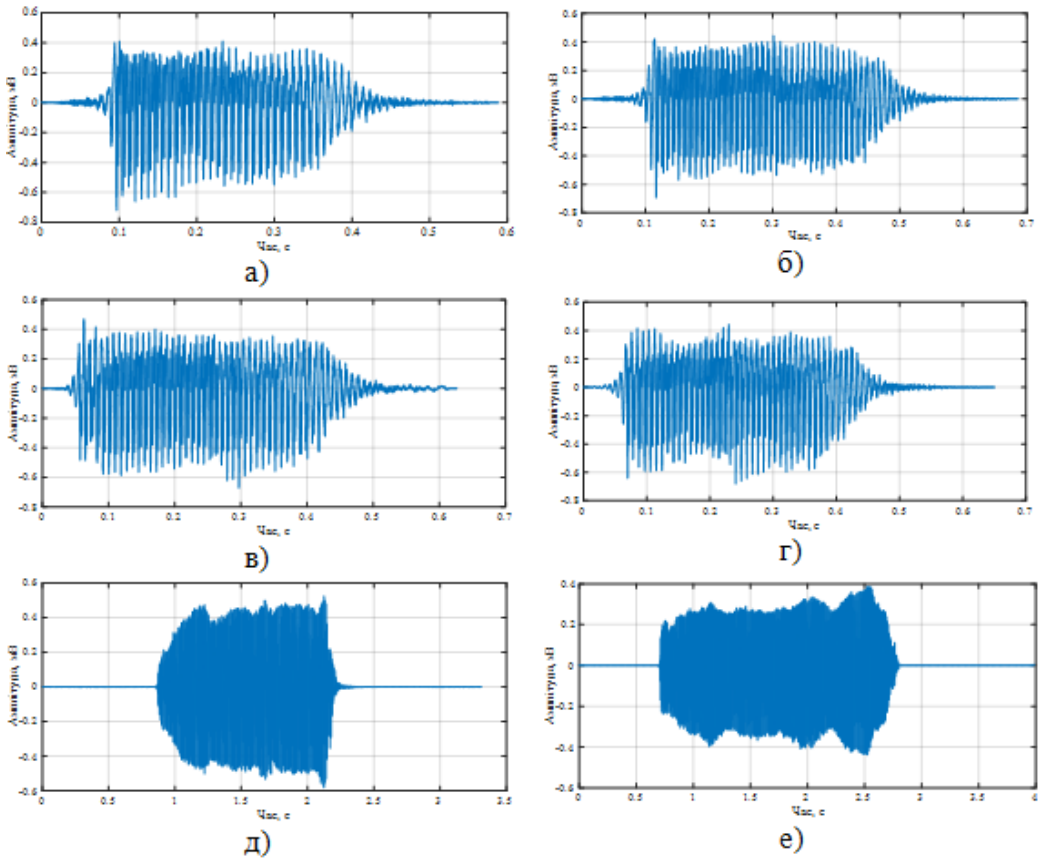


Рис 4.1. Реєстрограми голосових сигналів [м] (а-г) та [е] (д, е)

На основі одержаних характеристик глосового сигналу (рис. 4.1) отримано амплітудні спектри, за якими можна визначити частотні параметри формант. Вони наведені на рис. 4.2.

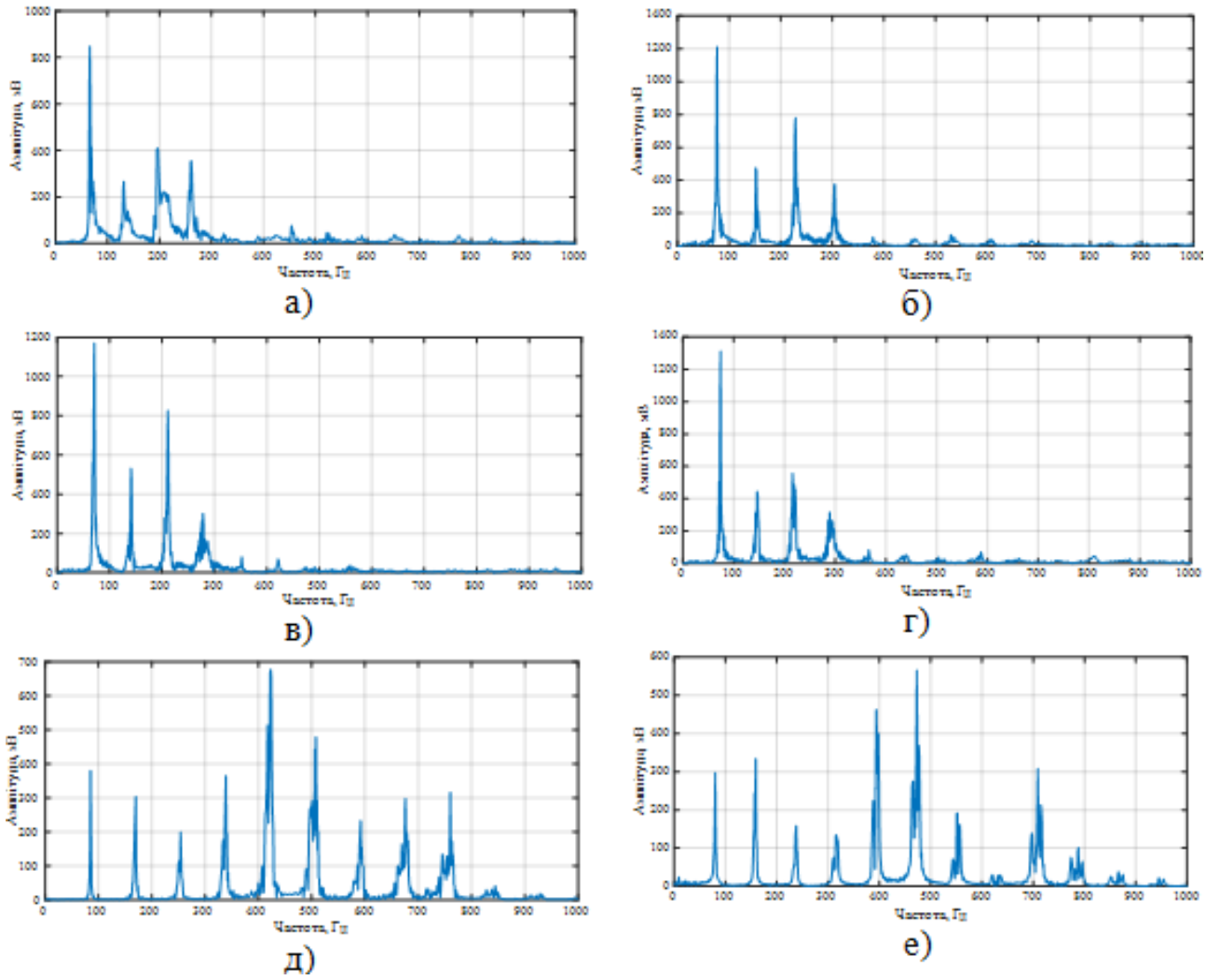


Рис. 4.2. Оцінки амплітудних спектрів реєстрограм голосових сигналів (рис. 4.1): а-г – для сигналу [м], та (д, е) – для сигналу [е]

З рис. 4.2 видно, в амплітудних спектрах голосового сигналу [м] частоти розміщення формант практично співпадають, змінюється амплітуда формат, це пояснюється неоднаковістю умов реєстрації (наявність зовнішніх завад, забезпечити однакову силу звуку важко). Для різних реалізацій голосового

сигналу [е] частоти розміщення формат теж співпадають. Отже, індивідуальними характеристиками особи можуть вважатись оцінки формантних частот, за допомогою значень яких можна проводити ідентифікацію особи. Пропонується разом із оцінками формантних частот використовувати і оцінки періоду основного тону голосових сигналів.

4.2 Обчислення значень періоду основного тону голосових сигналів

Для оцінювання значення ПОТ використаємо автокореляційний метод з певною модифікацією.

Тривалість проміжку часу між амплітудними значеннями автокореляційної функції дозволяє провести оцінювання ПОТ. Значення періоду T_{corr}визначається з виразу (4.1):

$$T_{corr} = M(T_n), n\epsilon Z, \tag{4.1}$$

де T_n – значення ПОТ, які знайдено за автокореляційною функцією, $M(\cdot)$ - математичне сподівання.

Рис. 4.3 демонструє оцінки вибірки функції автокореляції реєстрограм голосового сигналу.

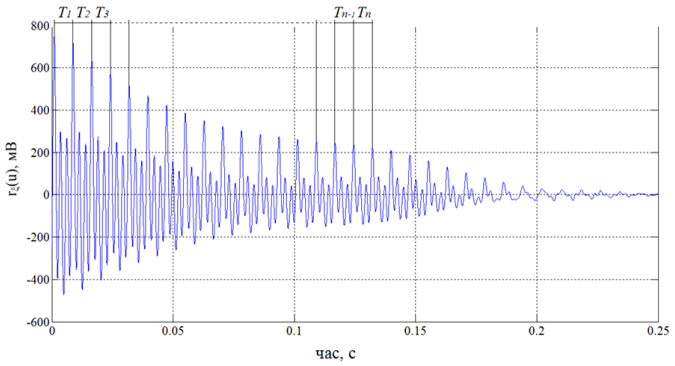


Рис. 4.3. Знаходження періоду основного тону голосового сигналу за оцінками його кореляційної функції

Проте відомо, що обертони, присутні в сигналі, та гармоніки з вищою амплітудою можуть впливати на точність ПОТ за автокореляційною функцією. Обчислення перетворення Фур'є від кореляційної функції дасть змогу вирішити проблему. Спектральні піки, рознесені по частотах, утворюються при перетворенні Фур'є гармонік, з яких складається функція кореляції. Проблематика розділення обертонів та основного тону вирішується перетворенням Фур'є, та відповідно, отримується оцінка спектральної густини потужності сигналу (А. Хінчин, Н. Вінер). Пара перетворень Фур'є, які зв'язують між собою функції кореляції та спектр густини потужності стаціонарного випадкового процесу називається парою перетворень Вінера-Хінчина і має вигляд:

$$\begin{cases} P(f) = \int_{-\infty}^{\infty} K(\tau) \exp(-j2\pi f\tau)\, d\tau, \\ K(\tau) = \int_{-\infty}^{\infty} P(\tau) \exp(j2\pi f\tau) df \end{cases} \quad (4.2)$$

Дещо гірше від очікуваного спетру матиме вигляд оцінка спектру густини потужності, вона буде відрізнятися від дійсного спектру на величину помилки вимірювань, яка містить випадкову та систематичну складові.

З урахуванням співвідношень (4.3), оцінку спектральної густини потужності, можна сформувати у вигляді:

$$\bar{P}(f) = \int_{-T}^{T} \bar{K}(\tau) \cdot e^{-j2\pi f\tau} d\tau, \quad (4.3)$$

де $\bar{P}(f)$ – це оцінка кореляційної функції.

Скінченною тривалістю T відрізка спостережуваного процесу, зумовлена систематична складова похибки оцінки (4.3).

На рис. 4.4 наведено отримані оцінки автокореляційної функції реєстрограм голосових сигналів (рис. 4.1), та відповідні оцінки спектральної густини потужності зображено на рис. 4.5.

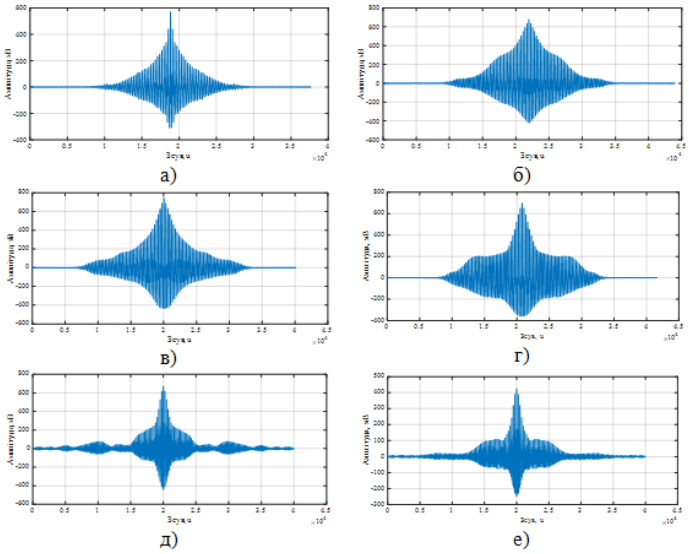


Рис. 4.4. Оцінки автокореляційної функції реєстрограм голосових сигналів (рис. 4.1): а-г – для сигналу [м], д-е – для сигналу [е]

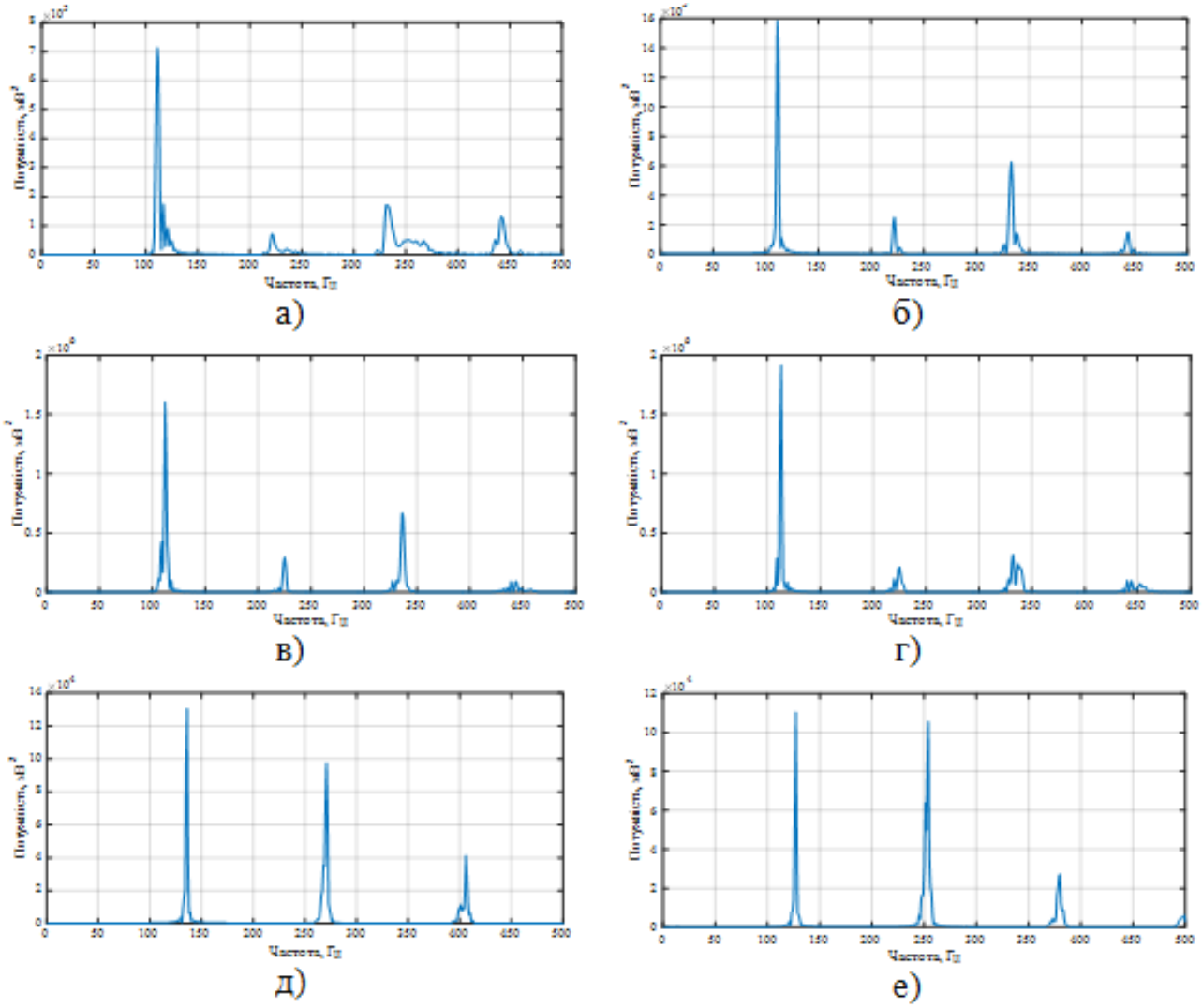


Рис.4.5. Оцінки спектральної густини потужності реєстрограм голосових сигналів(рис. 4.1): а-г – для сигналу [м], д-е – для сигналу [е]

Індивідуальними характеристиками особи у відповідності з рис. 2.4 та рис. 2.5, будуть оцінки ПОТ, які є оберненими до частоти основного тону, яка відповідає частоті розміщення першого максимуму у розподілі спектральної густини потужності (рис. 4.5), які також можуть бути використані для її ідентифікації /ідентифікації особи.

Але важливо перевірити чи будуть різнитися вище описані оцінки формантних частот та ПОТ різним особам відповідно. Щоб це перевірити, у

іншої особи було відібрано голосові сигнали (е). На рисунку 4.6 відображено оцінки амплітудних спектрів, реєстрограми цих сигналів, автокореляційних функцій та розподілів спектральної густини потужності.

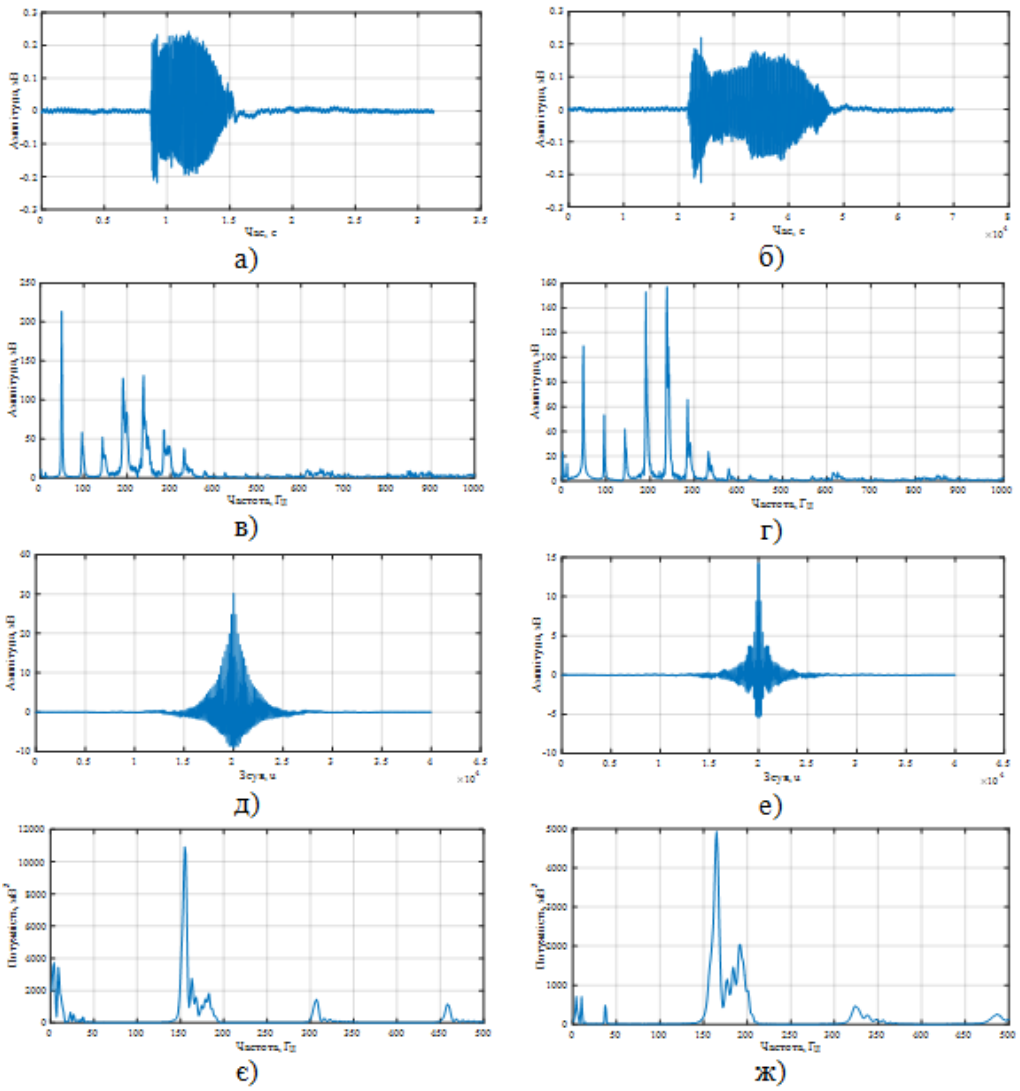


Рис. 4.6. Реєстрограми голосового сигналу [е] (а-б), оцінки амплітудного спектру (в-г), автокореляційні функції (д-е) та розподілу спектральної густини потужності (є-ж)

З Рис. 4.6 видно, що значення формантних частот та ПОТ є індивідуальними ознаками особи (які повторюються у різноманітних

реалізаціях аудіо сигналу) та відрізняються з цими ж оцінками ідентичних звукових сигналів іншої особи. Відповідно, для задачі ідентифікації та аутентифікації особи можуть бути використані оцінки формантних частот та ПОТ.

4.3 Висновки до розділу 4

Проведено відбір голосових сигналів однієї особи. Обчислено оцінки амплітудних спектрів отриманих реєстрограм голосових сигналів для задачі оцінювання частот розміщень формант.

Встановлено, що в амплітудних спектрах аудіо сигналу голосу [м] частоти, на яких розміщуються форманти майже співпадають, зміна амплітуд формант пояснюється через неоднаковість умов реєстрації. Співпадають і частоти на яких розміщуються форманти у різноманітних реалізаціях аудіо сигналу голосу [е]. Відповідно, за значеннями оцінок формантних часто можна проводити ідентифікацію особи, так як їх можна вважати індивідуальними характеристиками особи.

Проте, у окремих реалізаціях аудіо сигналу голосу одного диктора, значення частот розміщення формант дещо різняться між собою через наявність в структурі звукового сигналу випадкової складової. У такому випадку під час ідентифікації користувача можливою стає допущення помилок.

Для збільшення достовірності ідентифікації особи запропоновано збільшити число персональних ознак звукових сигналів голосу, на підставі яких буде прийматись рішення про позитивну чи негативну відповідь про аутентифікацію особи. Запропоновано попри оцінку частот розміщень формант оцінювати період основного тону.

Автокореляційний метод з певною його модифікацією було використано для того, щоб оцінити значення періоду основного тону.

Проте відомо, що обертони, присутні в сигналі та гармоніки з вищою амплітудою можуть мати вплив на точність розрахунку періоду основного тону за функцією автокореляції. Щоб вирішити дану проблему було розраховано оцінки розподілу спектральної густини потужності, де частота основного тону є оберненою до періоду і їй відповідає частота розміщення.

Встановлено, що індивідуальними характеристиками особи будуть значення частот на яких розміщенні форманти та періоду основного тону та відрізняються з ідентичними оцінками голосових сигналів для іншої особи. Відповідно до вище описаного, можна стверджувати, що для задачі ідентифікації та аутентифікації особи можна використовувати оцінки формантних часто та період основного тону.

РОЗДІЛ 5

СПЕЦАЛЬНА ЧАСТИНА

5.1 Метрологічне забезпечення наукового дослідженя

Згідно закону України "Про метрологію та метрологічну діяльність" та ДСТУ 2681-94, метрологічне забезпечення – це установлення та застосування метрологічних норм і правил, а також розроблення, виготовлення та застосування технічних засобів, необхідних для досягнення єдності і потрібної точності вимірювань.

Технічною основою метрологічного забезпечення є:

- система державних еталонів одиниць фізичних величин, яка забезпечує їх відтворення з найвищою точністю;

- система робочих еталонів і зразкових ЗВТ, за допомогою яких здійснюється передача розмірів одиниць фізичних величин робочим ЗВТ;

- система стандартних зразків складу та властивостей речовин та матеріалів, що забезпечує відтворення одиниць фізичних величин, які характеризують склад і властивості речовин і матеріалів;

- система робочих ЗВТ, які використовуються під час розроблення, виробництва, випробувань та експлуатації продукції, наукових досліджень та інших видів діяльності.

Основною метою метрологічного забезпечення є поліпшення якості продукції, підвищення ефективності виробництва, використовування матеріальних цінностей та енергетичних ресурсів, а також наукових досліджень.

При проведенні повірки повинні дотримуватися такі умови:

- температура навколишнього повітря (20 ± 5) ° С;

- атмосферний тиск від 97,3 до 105,3 кПа (від 730 до 790 мм. рт. ст.);

- відносна вологість повітря (65 + 15)%;

- на робочому місці для зменшення електромагнітних перешкод видаляються мережеві кабелі та шнури приладів від схеми перевірки і вхідних ланцюгів ЕК на відстань не менше 1 м;

- потрібно видалити від робочого місця джерела електромагнітних перешкод, що впливають на роботу засобів повірки. [5]

5.2 Побудова прикладного програмного забезпечення для розв’язування наукової задачі

Система Matlab (скорочення від Matrix Laboratory - матрична лабораторія) є інтерактивною комп'ютерною системою для виконання інженерних і наукових розрахунків, орієнтовану на роботу з масивами даних. Система припускає можливість звернення до програм, які написані на мовах FORTRAN, C і C++.

Привабливою особливістю системи є те, що вона містить вбудовану матричну і комплексну арифметику. Система підтримує виконання операцій з векторами, матрицями і масивами даних, реалізує сингулярний і спектральний розклади, підтримує роботу з поліномами алгебри, вирішення нелінійних рівнянь і задач оптимізації, інтеграція функцій в квадратурі, чисельна інтеграція диференціальних і різницевих рівнянь, побудова різноманітних видів графіків, тривимірних поверхонь і ліній рівня. В ній реалізовано зручне операційне середовище, яке дозволяє формулювати проблеми і отримувати рішення в звичайній математичній формі, не вдаючись до рутинного програмування.

Основний об'єкт системи Matlab - прямокутний числовий масив (матриця), який допускає комплексні елементи. Використання матриць не вимагає явної вказівки їх розмірів.

Система Matlab виконує операції з векторами і матрицями навіть в режимі безпосередніх обчислень без якого-небудь програмування. Нею можна користуватися як найпотужнішим калькулятором, в якому разом із звичайними арифметичними і алгебраїчними діями можуть використовуватися такі складні операції, як повернення матриці, обчислення її власних значень і векторів, вирішення систем лінійних рівнянь алгебри і багато іншого. Проте, характерна основна особливість системи - легкість її модифікації і адаптації до конкретних задач користувача. Користувач може ввести в систему будь-яку нову команду, оператор або функцію і користуватися потім ними так само просто, як і вбудованими операторами і функціями.

В базовий набір слів системи входять: спецзнаки; знаки арифметичних і логічних операцій; арифметичні, тригонометричні і деякі спеціальні математичні функції; функції швидкого перетворення Фур'є і фільтрації; векторні і матричні функції; засоби для роботи з комплексними числами; оператори побудови графіків в декартовій і полярній системах координат, тривимірних поверхонь і тому подібне. Matlab надає користувачеві великий набір готових засобів (більше половини з них - зовнішні розширення у вигляді m-файлів).

Matlab має широкі можливості для роботи з сигналами, для розрахунку і проектування аналогових і цифрових фільтрів, для побудови їх частотних, імпульсних і перехідних характеристик. В наявності і засоби для спектрального аналізу та синтезу, зокрема, для реалізації прямого і зворотного перетворення Фур'е. Завдяки цьому система досить зручна для проектування електронних пристроїв.

Робота в середовищі Matlab може здійснюватися в двох режимах:

- в режимі калькулятора, коли обчислення здійснюються відразу після набору чергового оператора або команди Matlab; при цьому значення результатів обчислення можуть привласнюватися деяким змінним, або

результати виходять безпосередньо, без привласнення (як в звичайних калькуляторах);

- шляхом виклику імені програми, написаної на мові Matlab, заздалегідь складеної і записаної на диску, яка містить всі необхідні команди, що забезпечують введення даних, організацію обчислень і виведення результатів на екран (програмний режим).

У обох режимах користувачеві доступні практично всі обчислювальні можливості системи, зокрема по виведенню інформації в графічній формі. Програмний режим дозволяє зберігати розроблені обчислювальні алгоритми і, таким чином, повторювати обчислення при інших вхідних даних.

Середовище Matlab має надзвичайно потужні засоби для проведення цифрової обробки сигналів, що може бути використано для обробки сигналів на виході вимірювального блоку. Розглянемо можливості Matlab в цьому плані.

Цифрова обробка сигналів традиційно включає створення засобів чисельного перетворення масиву заданого (зміряного в дискретні моменти часу) процесу зміни деякої неперервної фізичної величини з метою одержання з нього корисної інформації про іншу фізичну величину, що міститься в зміряному сигналі.

Фізична величина, що є корисною (що несе в собі необхідну інформацію), рідко має таку фізичну форму, що може бути безпосередньо зміряною. Зазвичай вона представляє лише деяку складову (сторону, частину, межу) деякої іншої фізичної величини, яка може бути безпосередньо зміряна. Зв'язок між цими двома величинами позначимо введенням ланки, яку назвемо "первинним перетворювачем" (ПП). Зазвичай закон перетворення відомий заздалегідь, інакше відновити інформаційну складову надалі було б неможливим. Первинний перетворювач вносить залежність сигналу, який може бути зміряний, від деяких інших фізичних величин. Внаслідок цього вихідна його величина містить, окрім корисної інформаційної складової, інші, шкідливі

складові або риси, що спотворюють корисну інформацію. І, хоча залежність виходу ПП від цих інших величин також відома, проте унаслідок неконтрольованої можливої зміни останніх з часом, часто важко спрогнозувати їх вплив на спотворення корисної складової. Назвемо ПП, що вноситься, шкідливу складову шумом ПП.

Хай утворена таким чином безпосередньо вимірювана величина вимірюється деяким вимірювачем. Будь-який реальний вимірювач вносить власні спотворення до вимірюваної величини і додаткових залежностей від деяких інших фізичних величин, що не є об'єктом вимірювання.

Назвемо ці спотворення шумами вимірювача. Не обмежуючи спільності, вважатимемо, що вихідною величиною вимірювача є електричний сигнал (зміряна величина), який можна надалі досить просто перетворювати електричними пристроями.

Для здійснення цифрової обробки зміряна величина має бути перетворена в дискретну форму за допомогою спеціального пристрою, який містить екстраполятор і аналого-цифровий перетворювач (АЦП).

Перший проводить фіксацію окремого поточного значення зміряної величини в окремі моменти часу через певний постійний проміжок часу, званий дискретом часу. Другий переводить це значення в цифрову форму, яка дозволяє надалі здійснювати перетворення за допомогою цифрових ЕОМ. Хоча обидва пристрої можуть вносити при таких перетвореннях власні спотворення до вихідного (дискретного) сигналу, проте ними зазвичай нехтують, оскільки в більшості випадків ці додаткові спотворення значно менші шумів ПП і вимірювача.

Щоб на основі отриманого дискретизованого сигналу отримати корисний сигнал, потрібно розрахувати і створити пристрій (програму для ЕОМ), який здійснював би такі перетворення вхідного дискретного в часі сигналу, щоб на його виході спотворення, внесені шумами ПП і вимірювача були мінімізовані в

деякому розумінні. Цей пристрій називають фільтром.

У загальному випадку створення (проектування) фільтру є задачею невизначеною, яка конкретизується лише на основі попередніх отриманих знань про закономірність утворення вимірюваної величини (моделі ПП), про модель утворення зміряної величини з вимірюваної (моделі вимірювача), про характеристики зміни в часі шкідливих фізичних величин, що впливають на утворення вимірюваної і зміряної величин, і закономірностей їх впливу на спотворення корисної інформації.

Оскільки моделі ПП і вимірювача можуть бути досить різноманітними, традиційно задачу фільтрації вирішують тільки для деяких найбільш поширених на практиці видів таких моделей, найчастіше - для лінійних моделей.

У загальному випадку процес створення фільтру розкладається на такі етапи:

- на основі апріорної інформації про моделі ПП і вимірювача і про характеристики шумів, а також про задачі, які повинен вирішувати фільтр, вибирається деякий тип фільтру з відомих, теорія проектування яких розроблена;

- на основі конкретних числових даних розраховуються числові характеристики вибраного типу фільтру (створюється конкретний фільтр);

- перевіряється ефективність виконання розробленим фільтром поставленого перед ним завдання; для цього необхідне зімітувати на ЕОМ дискретний сигнал, що містить корисну (інформаційну) складову з накладеними на неї передбаченими шумами ПП і вимірювача, "пропустити" його через побудований фільтр і порівняти отриманий на виході сигнал з відомою (в даному випадку) корисною його складовою; різниця між ними характеризуватиме похибки вимірювання на виході фільтру;

- оскільки в реальних умовах деякі характеристики шумів можуть

відрізнятися від прийнятих при проектуванні (створенні фільтру), не зайвими стають випробування ефективності роботи фільтру в умовах наближеніших до реальних, ніж прийняті при проектуванні.

Пакет SignalProcessingToolbox (надалі скорочено Signal) призначений для здійснення операцій по трьом останнім з вказаних етапів. Він дозволяє проектувати (розраховувати конкретні числові характеристики) цифрові і аналогові фільтри по необхідних амплітудно- і фазо-частотних їх характеристиках, формувати послідовності типових часових сигналів і обробляти їх спроектованими фільтрами. У пакет входять процедури, що здійснюють перетворення Фур'є, Гільберта, а також статистичний аналіз. Пакет дозволяє розраховувати кореляційні функції, спектральну щільність потужності сигналу, оцінювати параметри фільтрів по зміряних відліках вхідної і вихідної послідовностей.

У пакеті Signal передбачено декілька процедур для створення послідовності даних, що представляють деякі одиночні імпульсні процеси типових форм.

Процедура rectpuls забезпечує формування одиночного імпульсу прямокутної форми. Вираз вигляду:

y = rectpuls(t, w),

дозволяє утворити вектор y значень сигналу такого імпульсу одиничної амплітуди, шириною w, що центрується відносно t=0 по заданому вектору t моментів часу. Якщо ширина імпульсу w не вказана, її значення за умовчанням набуває рівним одиниці. імпульсів

Формування імпульсу трикутної форми одиничної амплітуди можна здійснити за допомогою процедури tripuls, вираз якої має вигляд

y =tripuls(t, w,s).

Аргументи y, t і w мають той же сенс. Аргумент s (-1<s <1) визначає нахил трикутника. Якщо s=0, або не вказаний, трикутний імпульс має симетричну форму.

РОЗДІЛ 6

ОБҐРУНТУВАННЯ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ

6.1. Визначення стадій технологічного процесу та загальної тривалості проведення науково-дослідних робіт

Економічне обґрунтування дипломної роботи магістра є суттю даного розділу, оскільки, дозволяє встановити доцільність проведення науково-дослідних робіт і економічно обґрунтувати доцільність застосування тих чи інших засобів.

Метою дипломної роботи магістра є дослідження методів та засобів побудови спеціалізованих комп’ютерних систем для аутентифікації особи.

Як відомо, розробка надійної і ефективної системи вимагає значних затрат часу. Слід зауважити, що затрати часу залежать від кваліфікації розробника і його можливостей. Розробник повинен у достатній мірі володіти навиками програмування, вміти адекватно застосовувати математичний апарат, бути добре обізнаним з об’єктом дослідження.

Розробку даної системи можна поділити на такі етапи:

1) постановка задачі;
2) збір інформації по тематиці роботи наступне її опрацювання;
3) прийняття рішень щодо вибору оптимального шляху розв'язання поставленої задачі;
4) аналіз математичної моделі та методів побудови спеціалізованих комп’ютерних систем для аутентифікації особи;
5) розробка алгоритму програми для аутентифікації особи;
6) налаштування середовища розробки і роботи вже готової програми;

7) написання програми;

8) написання і оформлення документації.

Для оцінки тривалості виконання окремих робіт використовують нормативи часу або попередній досвід. До таких нормативів відносять тривалість написання операцій (команд), які в деяких підприємствах становлять: для одної операції - 0,5-1,6 год та 8 годин для п'яти операцій (тривалість зміни).

У разі їх відсутності звертаються до експертних оцінок по встановленню тривалості кожного етапу (стадії):

при трьох оцінках:

$$T_{вс} = (t_{min} + 4_{тн.й} + t_{max}) / 6, \quad (6.1)$$

при двох оцінках:

$$T_{вс} = (3t_{min} + 2t_{max}) / 5, \quad (6.2)$$

де $T_{вс}$ – очікуване (середнє) значення тривалості виконання етапу (стадії); $t_{min.}$, $t_{н.й.}$, t_{max} – відповідно мінімальна, найбільш імовірна і максимальна оцінки тривалості виконання етапу (стадії).

Для визначення загальної тривалості проведення науково-дослідних робіт (розробки програмного продукту) доцільно дані витрат часу на виконання окремих стадій (етапів) звести у таблицю 6.1.

Витрати часу наукового керівника на виконання окремих стадій (етапів) при недостатній кількості інформації доцільно приймати в межах 5% сумарних витрат часу інженерів на виконання цих стадій (етапів).

Таблиця 6.1.

Основні етапи і час їх виконання у НДР

№ з/п	Етап	Середній час виконання етапу, год	
		інженер	керівник
1	2	3	4
1	постановка задачі	3	7
2	збір потрібної інформації і наступне її опрацювання	15	5
3	прийняття рішень щодо вибору оптимального шляху розв'язання поставленої задачі	3	2
4	аналіз математичної моделі та методів побудови спеціалізованих комп’ютерних систем для аутентифікації особи	15	8
5	розробка алгоритму програми для аутентифікації особи	11	5
6	налаштування середовища розробки і роботи вже готової програми	3	1
7	написання програми	85	5
8	написання і оформлення документації	20	7
разом		155	40

6.2. Визначення витрат на оплату праці та відрахувань на соціальні заходи

Відповідно до Закону України «Про оплату праці» заробітна плата – це «винагорода, обчислена, як правило, у грошовому виразі, яку власник або уповноважений ним орган виплачує працівникові за виконану ним роботу».

Розмір заробітної плати залежить від складності та умов виконуваної роботи, професійно-ділових якостей працівника, результатів його праці та господарської діяльності підприємства. Заробітна плата складається з основної та додаткової оплати праці.

Основна заробітна плата нараховується на виконану роботу за тарифними ставками, відрядними розцінками чи посадовими окладами і не залежить від результатів господарської діяльності підприємства.

Додаткова заробітна плата – це складова заробітної плати працівників, до якої включають витрати на оплату праці, не пов’язані з виплатами за фактично відпрацьований час. Нараховують додаткову заробітну плату залежно від досягнутих і запланованих показників, умов виробництва, кваліфікації виконавців. Джерелом додаткової оплати праці є фонд матеріального стимулювання, який створюється за рахунок прибутку.

Основна з/п складається із прямої з/п і доплати, яка при укрупнених розрахунках становить 25% – 35% від прямої з/п. При розрахунку з/п кількість робочих днів в місяці слід приймати – 21 дні/міс., що відповідає 168 год./міс. Розмір місячних окладів керівника та інженерів слід приймати згідно існуючих на даний час норм. Основна заробітна плата розраховується за формулою:

$$З_{осн} = Т_с \times К_г, \tag{6.3}$$

де $Т_с$ – тарифна ставка, грн.;

$К_г$ - кількість відпрацьованих годин.

Посадові оклади (тарифні ставки) за розрядами Єдиної тарифної сітки визначаються шляхом множення окладу (ставки) працівника 1 тарифного розряду на відповідний тарифний коефіцієнт. У разі коли посадовий оклад (тарифна ставка) визначені у гривнях з копійками, цифри до 0,5 відкидаються, від 0,5 і вище - заокруглюються до однієї гривні. У 2019 році посадові оклади (тарифні ставки) розраховуються згідно з Законом України «Про Державний бюджет України на 2019 рік».

Мінімальна зарплата в 2019 р. складає 4173,00 грн., в погодинному розмірі 25,13 грн., приймемо 80,00 грн. для інженера, для керівника – 130,00 грн.

Тарифні ставки: керівник проекту – 130,00 грн./год., інженер – 80,0 грн./год.

Основна заробітна плата становитиме:

$$З_{осн} = Т_{осн} \times К_{ГОД} \quad (6.4)$$

Керівник проекту:

$$З_{осн} = 130{,}00 \text{ грн.} \times 40 \text{ год.} = 5200{,}00 \text{ грн.}$$

Інженер:

$$З_{осн} = 80{,}00 \text{ грн.} \times 155 \text{ год.} = 12400{,}00 \text{ грн.}$$

Додаткова заробітна плата становить 10 – 15% від суми основної заробітної плати:

$$З_{дод} = З_{осн} \times К_{допл}, \quad (6.5)$$

де $К_{допл.}$– коефіцієнт додаткових виплат працівникам 0,1.

Керівник проекту:

$$З_{дод} = 5200{,}00 \text{грн.} \times 0{,}15 = 780{,}00 \text{ грн.}$$

Інженер:

$$З_{дод} = 12400 \text{ грн.} \times 0{,}10 = 1240{,}00 \text{ грн.}$$

Звідси загальні витрати на оплату праці ($В_{ОП}$) визначаються за формулою (6.6) і становлять:

$$В_{ОП} = З_{ОСН} + З_{дод} \quad (6.6)$$

Керівник проекту:

$$В_{ОП} = 5200{,}00 + 780{,}00 = 5980{,}00 \text{ грн.}$$

Інженер:

$$В_{ОП} = 12\ 400{,}00 + 1240{,}00 = 13640{,}00 \text{ грн.}$$

Таким чином загальна сума становить 19620,00 грн. Крім того, слід визначити відрахування на соціальні заходи:

– податок на доходи фізичних осіб: 18% 3531,60 грн.;

– військовий збір 1,5% 294,30 грн.;

– єдиний внесок 22% 4316,40 грн..

У сумі зазначені відрахування становлять 41,5%. Отже, загальна сума відрахувань на соціальні заходи становитиме:

$$B_{С.З.} = ФОП \times 0,415 \quad (6.7)$$

$$B_{С.З.} = 19620,00 \text{ грн.} \times 0,415 = 8142,30 \text{ грн.},$$

де ФОП – фонд оплати праці, грн.

Проведені розрахунки витрат на оплату праці зведемо у наступну табл. 6.2.

Таблиця 6.2.

Зведені розрахунки витрат на оплату праці

№ п/п	Категорія працівників	Основна заробітна плата, грн.			Додаткова заробітна плата, грн.	Нарах. на ФОП, грн.	Всього витрати на оплату праці, грн. 8=5+6+7
		Тарифна ставка, грн.	К-сть відпрацьов. год.	Фактично нарах. з/пл., грн.			
1	2	3	4	5	6	7	8
1.	Керівник проекту	130	40	5200,00	780,00	2481,70	8461,70
2.	Інженер	80	155	12400,00	1240,00	5660,60	19300,60
Разом				17600,00	2020,00	8142,30	27762,30

6.3. Розрахунок витрат на електроенергію

Затрати на електроенергію 1-ці обладнання визначаються за формулою:

$$З_е = W \times T \times S, \quad (6.8)$$

де W – необхідна потужність, кВт;

T– кількість годин роботи обладнання;

S – вартість кіловат-години електроенергії.

Згідно з постановою НКРЕКП України від 05.10.2018 р. № 1177 вартість електроенергії становить 243,71 коп./кВт.год.

Потужність комп'ютера – 380 Вт з підключеним маршрутизатором, кількість годин роботи обладнання згідно таблиці 4.1 – 250 годин.

$$З_е = 0{,}380 \times 250 \times 2.4371 = 231{,}52 \text{ грн.}$$

6.4 Розрахунок витрат на матеріали

Результати розрахунку затрат на матеріали зводяться в таблицю 6.3.

Таблиця 6.3.

Визначення величини затрат на матеріал

Найменування матеріальних ресурсів	Одиниця виміру	Норма витрат	Ціна за одиницю, грн	Затрати матеріалів, грн	Транспортно-заготівельні витрати, грн	Загальна сума витрат на матеріали, грн
Папір А4-80	пачка	1	100,00	100,00	-	100,00
Ватман	шт.	9	10,00	90,00	-	90,00
Заправка картріджа для лазерного принтера	шт.	1	90,00	90,00	-	90,00
Плата за користування Інтернетом	Грн.	1	170,00	170,00	-	170,00
Разом						450,00

6.5 Розрахунок суми амортизаційних відрахувань

Характерною особливістю застосування основних фондів у процесі виробництва є їх відновлення. Для відновлення засобів праці у натуральному виразі необхідне їх відшкодування у вартісній формі, яке здійснюється шляхом амортизації.

Амортизація – це процес перенесення вартості основних фондів на вартість новоствореної продукції з метою їх повного відновлення.

Комп’ютери та оргтехніка належать до четвертої групи основних

фондів. Для цієї групи річна норма амортизації дорівнює 60 % (квартальна – 15 %).

Для визначення амортизаційних відрахувань застосовуємо формулу:

$$A = \frac{Б_в \cdot Н_А}{100} \tag{6.9}$$

де A – амортизаційні відрахування за звітний період, грн.,

$Б_в$ – балансова вартість комп'ютера, на початок звітного періоду, грн..

$Н_а$ – норма амортизації, %.

$$A = \frac{22000{,}00 * 15\%}{100\%} = 3300{,}00 грн.$$

6.6 Обчислення накладних витрат

Накладні витрати пов'язані з обслуговуванням виробництва, утриманням апарату управління підприємства (фірми) та створення необхідних умов праці.

Накладні витрати можуть становити 20% від суми основної та додаткової заробітної плати працівників:

$$Н_в = В_{О.П} \text{ х. } 0{,}2 , \tag{6.10}$$

$$Н_в = 19620{,}00 \text{ грн. х } 0{,}2 = 3924{,}00 \text{ грн.}$$

де $Н_в$ – накладні витрати, грн.,

$В_{О.П}$ – суми основної та додаткової заробітної плати працівників, грн..

6.7 Складання кошторису витрат та визначення собівартості науково-дослідних робіт

Результати проведених вище розрахунків зведемо у табл. 6.4. Собівартість ($С_В$) науково-дослідних робіт розрахуємо за формулою:

$$Св=Во.п.+Вс.з.+Зм.в.+Зе+Тв+А+Нв\ , \quad (6.11)$$

$С_в$ = 19620,00 + 8142,30 + 450,00 + 231,52 + 3 300,00 + 3924,00 = 35667,82 грн.

Таблиця 6.4.

Кошторис витрат на науково-дослідних робіт

Зміст витрат	Сума, грн.	В % до загальної суми
1	2	3
Витрати на оплату праці (основну і додаткову заробітну плату)	19620,00	55,01
Відрахування на соціальні заходи	8142,30	22,83
Матеріальні витрати	450,00	1,26
Витрати на електроенергію	231,52	0,65
Амортизаційні відрахування	3 300,00	9,25
Накладні витрати	3924,00	11,00
Собівартість	35667,82	100

6.8 Розрахунок ціни науково-дослідних робіт

Ціну науково-дослідних робіт можна визначити за формулою:

$$Ц = \frac{C_в \cdot (1 + P_{рен}) + К \cdot B_{н.і.}}{К} \quad (6.12)$$

$P_{рен.}$ – рівень рентабельності, 30 %;

$К$ – кількість замовлень;

$B_{і.н.}$ – вартість носія інформації, грн.

Таким чином ціна рівна 46518,17 грн.

Визначимо величину прибутку:

$$П = Ц - Св \quad (6.13)$$

Згідно формули 6.13 отримаємо 10850,35 грн.

6.9 Визначення економічної ефективності і терміну окупності капітальних вкладень

Ефективність виробництва – це узагальнене і повне відображення кінцевих результатів використання робочої сили, засобів та предметів праці на підприємстві за певний проміжок часу.

Економічна ефективність ($E_р$) полягає у відношенні результату виробництва до затрачених ресурсів:

$$E_Р = П/C_в, \quad (6.14)$$

де $П$ – прибуток;

C_B – собівартість.

$$E_P = 10850,35 / 35667,82 = 0,30$$

Поряд із економічною ефективністю розраховують термін окупності капітальних вкладень (T_p):

$$T_P = E_P \quad (6.15)$$

$$T_P = 1 / 0,30 = 3,33 \text{ р.}$$

Про доцільність розробки програми можна сказати при врахуванні наступних критеріїв:

Таблиця 6.5.

Техніко-економічні показники НДР

№ п/п	Показник	Значення
1	Собівартість, грн	35667,82
2	Плановий прибуток, грн	10850,35
3	Ціна, грн	46518,17
4	Економічна ефективність	0,30
5	Термін окупності, рік	3,33

У результаті проведення розрахунків можна зробити висновок: розробка матиме оптимальну економічну ефективність 0,3 і термін окупності становитиме 3,33 року.

6.10 Висновок до розділу 6

Варто зазначити, що дані розрахунки носять номінальний характер і основна їх мета оцінити приблизну вартість дослідження та створення даного продукту. Номінальний характер розрахунків зумовлений тим, що даний програмний продукт має дослідницьке призначення.

РОЗДІЛ 7
ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

7.1 Охорона праці

7.1.1 Планування заходів з охорони праці. Види планування та контролю стану охорони праці. Виявлення, оцінка та зменшення ризиків небезпечних подій.

Метою планування заходів з охорони праці є визначення необхідних вкладень у заходи з охорони праці для ефективного впливу на стан охорони праці.

Система планів з охорони праці окремого підприємства може включати:

- перспективне планування (на період, більший одного року) ;
- поточне планування (на рік) ;
- оперативне планування (детальні плани, спрямовані на вирішення конкретних питань працеохоронної діяльності на підприємстві в короткостроковому, до одного року, періоді).

Планування в охороні праці може включати:

- визначення цілей діяльності з охорони праці на підприємстві та засобів їх досягнення;
- вибір методів і базових показників, за допомогою яких може здійснюватися оцінка необхідних вкладень в охорону праці;
- розрахунок суми вкладень у заходи з охорони праці та раціональний розподіл цієї суми за напрямками діяльності;
- забезпечення організації контролю виконання плану (при необхідності здійснення коригування запланованих показників) ;
- здійснення постійного контролю умов і безпеки праці на підприємстві та оперативне реагування на відхилення від нормативних вимог.

Перспективне планування вміщує найбільш важливі, трудомісткі і довгострокові за терміном виконання заходи з охорони праці, виконання яких, як правило, вимагає сумісної роботи кількох підрозділів підприємства. Можливість виконання заходів перспективного плану повинна бути підтверджена обґрунтованим розрахунком необхідного матеріально-технічного забезпечення і фінансових витрат з зазначенням джерел фінансування.

До перспективних планів належить комплексний план покращення умов праці і санітарно-оздоровчих заходів, що передбачає створення, відповідно до нормативних актів з охорони праці, умов праці, пов’язаних з перспективними змінами підприємства. Таке планування, як правило, розраховане на термін від 2 до 5 років. Реалізація цих планів забезпечується через річні плани номенклатурних заходів з охорони праці, які вносяться до угоди, що є невід’ємною частиною колективного договору.

Поточне планування здійснюється у межах календарного року через розроблення відповідних заходів у розділі «Охорона праці» колективного договору.

Поточні плани передбачають реалізацію заходів із покращення умов праці, створення кращих побутових і соціальних умов на виробництві. Ці плани обов’язково забезпечуються фінансуванням згідно з розробленими кошторисами.

Питання охорони праці можуть віддзеркалюватися в інших поточних планах, які підприємства та організації можуть складати на вимогу трудових колективів:

- план соціального розвитку колективу;
- наукової організації праці;
- механізації важких і ручних робіт;
- охорони праці жінок;
- підготовки підприємства до робіт в осінньо-зимовий період;

- підвищення культури виробництва та ін.

Оперативне планування роботи з охорони праці здійснюється за підсумками контролю стану охорони праці в структурних підрозділах і на підприємстві в цілому.

Оперативні плани складаються для швидкого виправлення виявлених в процесі державного, відомчого і громадського контролю недоліків в стані охорони праці, а також для ліквідації наслідків аварій або стихійного лиха.

Оперативні заходи щодо усунення виявлених недоліків зазначаються безпосередньо у наказі власника підприємства, який видається за підсумками контролю, або у плані заходів, як додатку до наказу.

Організаційно-методичну роботу щодо складання перспективних, поточних та оперативних планів здійснює служба (спеціаліст) охорони праці.

7.1.2 Особливості розслідування та обліку нещасних випадків невиробничого характеру

Розслідування та облік нещасних випадків, професійних захворювань і аварій на виробництві організовує роботодавець відповідно до Положення про порядок розслідування та ведення обліку нещасних випадків, професійних захворювань і аварій на виробництві, затвердженого постановою Кабінету Міністрів України від 21 серпня 2001 року №1094.

Розслідуванню підлягають раптові погіршення стану здоров'я, поранення, травми, у тому числі отримані внаслідок тілесних ушкоджень, заподіяних іншою особою, гострі професійні захворювання і гострі професійні та інші отруєння, теплові удари, опіки, обмороження, утоплення, ураження електричним струмом, блискавкою та іонізуючим випромінюванням, інші ушкодження, отримані внаслідок аварій, пожеж, стихійного лиха (землетруси, зсуви, повені, урагани та інші надзвичайні події), контакту з тваринами,

комахами та іншими представниками фауни і флори, що призвели до втрати працівником працездатності на один робочий день чи більше або до необхідності переведення потерпілого на іншу (легшу) роботу терміном не менш як на один робочий день, а також випадки смерті на підприємстві.

До гострих професійних отруєнь належать випадки, що сталися після одноразового (протягом не більше однієї робочої зміни) впливу небезпечних факторів, шкідливих речовин.

Гострі професійні захворювання спричиняються дією хімічних речовин, іонізуючого та неіонізуючого випромінювання, значним фізичним навантаженням та перенапруженням окремих органів і систем людини. До них належать також інфекційні, паразитарні, алергійні захворювання тощо.

Визнаються пов'язаними з виробництвом, і складається акт за формою Н-1 про нещасні випадки, що сталися з працівниками під час виконання трудових (посадових) обов'язків, у тому числі у відрядженнях, а також ті, які сталися під час:

- перебування на робочому місці, на території підприємства або в іншому місці роботи протягом робочого часу, починаючи з моменту приходу працівника на підприємство і до його виходу (який повинен фіксуватися відповідно до правил внутрішнього трудового розпорядку) або за дорученням роботодавця в неробочий час, під час відпустки, у вихідні та святкові дні;

- приведення в порядок знарядь виробництва, засобів захисту, одягу, виконання заходів особистої гігієни перед початком роботи і після її закінчення;

- проїзду на роботу чи з роботи на транспортному засобі підприємства або на транспортному засобі іншого підприємства, яке надало його згідно з договором (заявкою), за наявності розпорядження роботодавця;

- використання власного транспортного засобу в інтересах підприємства з дозволу або за дорученням роботодавця відповідно до встановленого порядку;

- проведення дій в інтересах підприємства, на якому працює потерпілий,

тобто дій, які не входять до кола виробничого завдання чи прямих обов'язків працівника (надання необхідної допомоги іншому працівникові, дії щодо попередження можливих аварій або рятування людей та майна підприємства, інші дії за наявності розпорядження роботодавця тощо);

- ліквідації аварій, пожеж та наслідків стихійного лиха на виробничих об'єктах і транспортних засобах, що використовуються підприємством;

- надання підприємством шефської допомоги;

- перебування на транспортному засобі або на його стоянці, на території вахтового селища, у тому числі під час змінного відпочинку, якщо причина нещасного випадку пов'язана з виконанням потерпілим трудових (посадових) обов'язків або з дією на нього небезпечних чи шкідливих виробничих факторів або середовища;

- прямування працівника до (між) об'єкта (ми) обслуговування за затвердженими маршрутами або до будь-якого об'єкта за дорученням роботодавця;

- прямування до місця відрядження та в зворотному напрямку відповідно до завдання про відрядження.

Нещасні випадки визнаються пов'язаними з виробництвом, і складається акт за формою Н-1 також у випадках:

- природної смерті працівника під час перебування на підземних роботах;

- нанесення тілесних ушкоджень іншою особою або вбивство працівника під час виконання чи у зв'язку з виконанням ним трудових (посадових) обов'язків незалежно від порушення кримінальної справи;

- які сталися з працівниками на території підприємства або в іншому місці роботи під час перерви для відпочинку та харчування, яка встановлюється згідно з правилами внутрішнього трудового розпорядку, а також під час перебування працівників на території підприємства у зв'язку з проведенням роботодавцем наради, отриманням заробітної плати, обов'язковим

проходженням медичного огляду тощо, а також у випадках, передбачених колективним договором (угодою).

За висновками роботи комісії з розслідування не визнаються пов'язаними з виробництвом, і не складається акт за формою Н-1 про ті нещасні випадки, що сталися з працівниками:

- під час прямування на роботу чи з роботи пішки, на громадському, власному або іншому транспортному засобі, який не належить підприємству і не використовувався в інтересах цього підприємства;

- за місцем постійного проживання, на території польових і вахтових селищ;

- під час використання ними в особистих цілях транспортних засобів, а також устаткування, механізмів, інструментів підприємства без дозволу роботодавця, крім випадків, що сталися внаслідок несправності цього устаткування, механізмів, інструментів;

- внаслідок отруєння алкоголем, наркотичними або іншими отруйними речовинами, а також унаслідок їх дії (асфіксія, інсульт, зупинка серця тощо) за наявності медичного висновку, якщо це не викликано застосуванням цих речовин у виробничих процесах або порушенням вимог безпеки щодо їх зберігання і транспортування, або якщо потерпілий, який перебував у стані алкогольного чи наркотичного сп'яніння, був відсторонений від роботи згідно установленого порядку;

- під час скоєння ними злочинів або інших правопорушень, якщо ці дії підтверджені рішенням суду;

- у разі природної смерті або самогубства, що підтверджено висновками судово-медичної експертизи та органів прокуратури.

Якщо за висновками роботи комісії з розслідування прийнято рішення, що про нещасний випадок не повинен складатися акт за формою Н-1, про такий нещасний випадок складається акт за формою НТ (невиробничий травматизм)

відповідно до Порядку розслідування та обліку нещасних випадків невиробничого характеру.

7.1.3 Пожежна сигналізація і зв'язок. Засоби гасіння пожеж. Протипожежне водопостачання. Первинні засоби пожежогасіння. Автоматичні засоби пожежогасіння на об'єктах галузі

Система пожежної сигналізації складається з пожежних сповіщувачів (пристроїв для формування сигналу про пожежу), які включені у сигнальну лінію (шлейф або промінь), приймально-контрольного приладу, ліній зв'язку.

Пожежні сповіщувачі перетворюють прояви пожежі (тепло, світло полум'я, дим) в електричний сигнал, який по лініях зв'язку надходить до контрольно-приймального приладу. Контрольно-приймальний прилад здійснює приймання інформації від пожежних сповіщувачів, виробляє сигнал про виникнення пожежі чи несправності, передає цей сигнал та видає команди на інші пристрої (наприклад, включає автоматичні установки пожежогасіння чи димовидалення).

В залежності від проявів процесу горіння сповіщувачі можуть бути:

- теплові, які реагують на певне значення температури та (чи) швидкість її наростання ;
- димові, які реагують на аерозольні продукти горіння;
- полум'я, які реагують на електромагнітне випромінювання полум'я.

В залежності від можливості зазначати свій номер (адресу) сповіщувачі поділяються на:

- адресовані, які реагують на фактори, супровідні пожежі, в місці їх встановлення і постійно або періодично активно формують сигнал про стан пожежонебезпечності в приміщенні, що захищається та власну працездатність із зазначенням свого номера (адреси);

- неадресовані, які реагують на фактори, супровідні пожежі, в місці їх встановлення та формують сигнал про виникнення пожежі в приміщенні, що захищається без зазначенням свого номера (адреси);

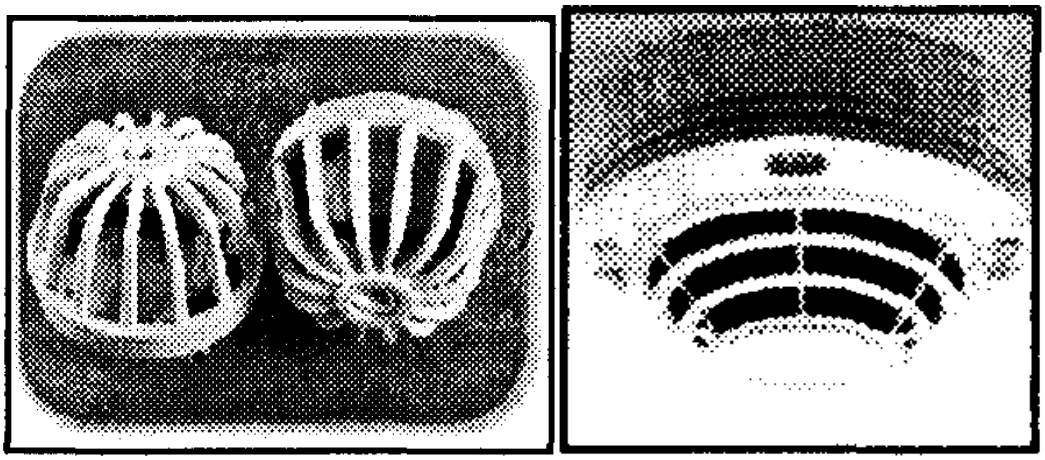


Рис. 1. Зовнішній вигляд пожежних сповіщувачів:

1 - тепловий максимально-диференцьований сповіщувач;

2 — сповіщівачі пожежні теплові магнітні;

Вибір пожежних сповіщувачів здійснюється в залежності від характерних приміщень, виробництв та технологічних процесів. В даний час розвивається тенденція заміни з метою зниження інерційності спрацювання теплових сповіщувачів на димові.

Враховуючи, що вода є основною вогнегасною речовиною, необхідно приділити особливу увагу створенню та працездатності надійних систем протипожежного водопостачання.

Система притипожежного водопостачання являє собою комплекс інженерних водопровідних пристроїв та споруд, призначених для забору води з вододжерела, її транспортування, зберігання запасів та подавання до місця пожежі. Призначення системи протипожежного водопостачання полягає в

забезпеченні подавання необхідних об'ємів води потрібного напору протягом нормативного часу гасіння пожежі за умови достатнього ступеня надійності всього комплексу водопровідної споруди.

Кожне підприємство повинно бути забезпечене необхідно кількістю води для цілей пожежогасіння.

Систему протипожежного водопостачання поділяють на дві частини: зовнішню (ззовні будівель) та внутрішню (всередині будівель). Протипожежний водопровід (зовнішній та внутрішній) є одним з найбільш важливих елементів системи протипожежного водопостачання.

До зовнішнього водопроводу належать усі пристрої та споруди для забору, очищення, зберігання та розподілу води мережею до вводу в будівлю.

Внутрішні водопроводи являють собою сукупність трубопроводів та пристроїв, які забезпечують постачання води із зовнішньої мережі та її подавання до місця відбору води для гасіння пожеж, що можуть виникнути в будівлі.

Для відбору води із зовнішнього водопроводу на ньому встановлюють пожежні гідранти. Кришки люків колодязів підземних пожежних гідрантів рекомендується фарбувати в червоний колір.

Біля місць розташування пожежних гідрантів і водойм повинні бути встановлені покажчики (об'ємні зі світильником або плоскі із застосуванням світловідбивних покриттів) з нанесеними на них:

для пожежного гідранта - літерним індексом ПГ, цифровими значеннями відстані в метрах від покажчика до гідранта, внутрішнього діаметра трубопроводу в міліметрах, зазначенням виду водогінної мережі (тупикова чи кільцева);

для пожежної водойми — літерним індексом ПВ, цифровими значеннями запасу води в кубічних метрах та кількості пожежних автомобілів, котрі можуть одночасно встановлюватися на майданчику біля водойми.

Кожний пожежний кран повинен бути укомплектований пожежним рукавом однакового з ним діаметра та стволом, а також важелем для полегшення відкривання вентиля, Будова внутрішнього пожежного крана показана на рис. 2.

Пожежні крани повинні розміщуватись у вбудованих або навісних шафках, які мають отвори для провітрювання і пристосовані для опломбування та візуального огляду їх без розкривання.

Влаштовуючи шафки, слід враховувати можливість розміщення в них двох вогнегасників.

На дверцятах пожежних шафок із зовнішнього боку повинні бути вказані після літерного індексу «ПК» порядковий номер крана та номер телефону для виклику пожежної охорони.

До первинних засобів пожежогасіння відносяться: вогнегасники, пожежний інвентар (покривала з негорючого теплоізоляційного полотна, грубововняної тканини або повсті, ящики з піском, бочки з водою, пожежні відра, совкові лопати) та пожежний інструмент (гаки, ломи, сокири тощо).

Вони використовуються для локалізації та ліквідації пожеж у початковій стадії розвитку.

Організаційні заходи щодо забезпечення пожежної безпеки. Відповідно до Закону України "Про пожежну безпеку" забезпечення пожежної безпеки підприємств, установ, організацій (далі - підприємств) покладається на їх керівників та уповноважених керівниками осіб, якщо інше не передбачено відповідним договором.

Забезпечення пожежної безпеки під час проектування та забудови населених пунктів, будівництва, розширення, реконструкції та технічного переоснащення підприємств, будівель і споруд покладається на органи архітектури, забудовників, проектні та будівельні організації.

Забезпечення пожежної безпеки в житлових будинках державного,

громадського житлового фонду, фонду житлово-будівельних кооперативів (далі - ЖБК) покладається на власників цих будинків або на уповноважені ними органи, а в житлових приміщеннях (квартирах) – також і на квартиронаймачів (членів ЖБК). Взаємні зобов’язання власника і квартиронаймача щодо забезпечення пожежної безпеки повинні визначатися договором житлового найму, а членів ЖБК – статутом.

Забезпечення пожежної безпеки в житлових будинках (квартирах) приватного житлового фонду та інших приватних, окремо розташованих господарських спорудах і гаражах, на територіях, а також у дачних будинках, на садових ділянках покладається на їх власників чи наймачів, якщо інше не обумовлено договором найму.

Обов'язки сторін щодо забезпечення пожежної безпеки орендованого майна повинні бути визначені у договорі оренди.

Повноваження у галузі пожежної безпеки асоціацій, корпорацій, концернів, інших виробничих об'єднань повинні визначатися їх статутами або договорами між підприємствами, що утворили об'єднання.

За порушення вимог Правил, невиконання приписів та постанов посадових осіб органів державного пожежного нагляду або створення перешкод для їх діяльності, посадові та фізичні особи притягуються до відповідальності згідно з чинним законодавством України.

7.2 Безпека в надзвичайних ситуаціях

7.2.1 Здійснення заходів щодо зниження дії радіоактивних випромінювань на апаратуру телекомунікаційної мережі

Дія радіації на матеріали і деталі апаратури залежить від виду випромінювання, дози радіації, природи опромінюваної речовини та умов навколишнього середовища.

В РЕА використовуються елементи, до складу яких входять матеріали: метали, неорганічні матеріали, напівпровідники та різні органічні сполуки (діелектрики, смоли та ін.). Серед цих матеріалів метали найбільш чутливі до радіації, оскільки їм властива висока концентрація вільних носіїв.

В радіоелектронній апаратурі радіація викликає зворотні і незворотні процеси, внаслідок яких можуть бути порушення роботи елементів схеми, що приведе до пошкодження апаратури.

Якщо потік гамма-опромінення проходить через елементи РЕА, то в них виникають вільні носії електричних зарядів, внаслідок переміщення яких виникає хибний імпульс, який може призвести до включення пристрою.

Найбільш чутливі до дії радіації напівпровідники, оптичні прилади і фотоматеріали.

В елементній базі РЕА внаслідок дії іонізаційних випромінювань можлива зміна майже всіх електричних та експлуатаційних характеристик, залежних від проходження процесів іонізації і порушення структури матеріалів.

Практика експлуатації РЕА в умовах дії радіоактивних випромінювань дає можливість зробити висновки:

1. РЕА може раптово втратити працездатність при певних рівнях радіації (критичних).

2. В елементах схем РЕА можуть початись зворотні або незворотні процеси через деякий час після випадання радіоактивних опадів при рівнях радіації значно нижчих критичних, тобто $p_{гр} < p_{кр}$.

Для інженерної практики найбільший інтерес має перший випадок, тобто оцінка стійкості роботи РЕА при знаходженні її на забрудненій радіоактивними речовинами місцевості тривалістю однієї години після випадання радіоактивних речовин на даній місцевості.

Оцінка стійкості роботи РЕА ведеться в послідовності:

1. РЕА аналізується і визначаються всі елементи, від яких залежить її

робота (функціонуються) наприклад: мікросхеми ТТЛ, транзистори, резистори та ін.

2. З табл. 2.4 додатка 2 для кожного елементу визначаються максимально допустимі потужності дози гамма-випромінювання (p_i) або експозиційні дози (ДІ). Отримані дані заносяться в таблицю 7.1,

Таблиця 7.1

Результати стійкості роботи РЕА

Елементи РЕА	P_i, Р/с	$Д_i$, Р	$p_{гр}$, р/с ; $Д_{гр}$Р
Напівпровідники	$\mathbf{p_1}$	$\mathbf{Д_1}$	$p_{гр}$ ($Д_{гр}$)
Мікросхеми	$\mathbf{p_2}$	$\mathbf{Д_2}$	
Конденсатори	$\mathbf{p_3}$	$\mathbf{Д_3}$	

3. Дані табл. 7.1 аналізуються і за мінімальним значенням $\mathbf{p_1}Д_i$ визначається межа стійкості $p_{гр}$ ($Д_{гр}$) роботи РЕА.

4. Граничне значення потужності гамма-випромінювання ($p_{гр}$) або експозиційної дози ($Д_{гр}$) порівнюється з $\mathbf{p_{1max}}$ ($Д_{max}$), що очікується на об'єкті і робиться висновок про стійкість роботи РЕА:

$$\left.\begin{matrix} p_{гр} \geq \mathbf{p_{1max}} \\ Д_{гр} \geq \mathbf{Д_{1max}} \end{matrix}\right\} \text{– РЕА стійка до радіації;}$$

$$\left.\begin{matrix} p_{гр} < \mathbf{p_{1max}} \\ Д_{гр} < \mathbf{Д_{1max}} \end{matrix}\right\} \text{– РЕА нестійка до радіації;}$$

Можливу дозу опромінення (Дм=Дmax) за встановлений час можна визначити за формулами 3.10, 3.11,3.12 .

Допустимий час роботи РЕА в заданих умовах можна визначити за допомогою виразів:

$$t_{\partial} = \left(\frac{Д_{гр} \cdot К_{пос} + 1{,}33\rho_{1max} \cdot \sqrt[4]{t_n^3}}{1{,}33\rho_{1max}} \right)^{4/3}, \text{ год}$$

$$t_{\partial} = \left(\frac{Д_{гр} \cdot К_{пос} + 2\rho_{1max} \cdot \sqrt[4]{t_n}}{2\rho_{1max}} \right)^{2}, \text{ год}$$

5. На підставі висновку про стійкість розробляються заходи з радіаційної стійкості РЕА (пристроїв, блока та ін.).

Заходи щодо підвищення стійкості роботи радіоелектронних систем (РЕС)

Дослідження, які здійснені як в нашій державі, так і за кордоном, показали, що зміна параметрів РЕС може мати місце в широкому діапазоні доз (рівнів радіації) іонізуючих випромінювань. Тому в багатьох випадках виникає необхідність приймати дії щодо підвищення радіаційної стійкості роботи апаратури (пристроїв, блоків), що розробляється. Основними заходами щодо підвищення радіаційної стійкості можуть бути: використання в апаратурі радіаційно стійких елементів і матеріалів; застосування для ОЦ різних апаратних масивних екранів або активного захисту від дії радіації. При імпульсній дії іонізаційних випромінювань крім перерахованих заходів використовують: схеми малочутливі до зміни електричних параметрів; зменшення чутливості перемикальних схем до зміни вхідних сигналів і напруг джерел живлення; зниження напруги живлення на аноді і збільшення негативного зміщення сіток газорозрядних приладів; застосування пристроїв, що вимикають радіотехнічні схеми на час дії радіації; збільшення відстані між елементами, які знаходяться під навантаженням та ін.

Висновок. Розглянуто питання здійснення заходів щодо зниження дії радіоактивних випромінювань на апаратуру телекомунікаційної мережі. Зроблено відповідні висновки з практики експлуатації РЕА в умовах дії радіоактивних випромінювань, визначено найбільш чутливі до дії радіоактивних випромінювань елементи РЕА. Запропоновано заходи щодо підвищення стійкості роботи радіоелектронних систем (РЕС).

РОЗДІЛ 8
ЕКОЛОГІЯ

8.1 Електромагнітне забруднення довкілля, його вплив на людину, шляхи його зменшення

Електромагнітне поле (ЕМП) – особлива форма матерії, за допомогою якої зійснюється взаємодія між електрично зарядженими частинками. Воно складається з двох окремих полів – електричного та магнітного. Силові лінії цих полів взаємно перпендикулярні. Через електромагнітне поле передаються всі види електромагнітного випромінювання – від низькочастотного (радіохвилі) до високочастного (рентгенівське та гамма-випромінювання).

Основними фізичними параметрами електромагнітного поля є швидкість поширення електромагнітної хвилі, довжина хвилі та частота коливань, які зв'язані між собою співвідношенням. Спектр електромагнітних коливань радіочастот за частотою коливань та довжиною хвилі умовно поділяють на діапазони. За частотою коливань електромагнітні хвилі мають діапазони низьких (НЧ), середніх (СЧ), високих (ВЧ), дуже високих (ДВЧ), ультрависоких (УВЧ), надвисоких (НВЧ) та надзвичайно високих частот (НЗВЧ). За довжиною розрізняють кілометрові, гектометрові, декаметрові, метрові, дециметрові та інші діапазони хвиль.

Електромагнітна енергія використовується у радіо-, радіорелейному і космічному зв'язках, телебаченні, радіолокації, радіонавігації. Вона застосовується у металургії та металообробних галузях промисловості для індукційного плавлення, зварювання, напилення металів, у деревообробній, текстильній, легкій та харчовій промисловості, у радіоспектроскопії, сучасній обчислювальній техніці, медицині (терапевтичні і діагностичні установки) тощо.

Ступінь опромінення працівників залежить від кількості передатчиків (у деяких зонах, радіо- та телецентрах їх може бути до 20), їх потужності, екранування, розміщення окремих їх блоків усередині та поза приміщенням.

Для всіх видів зв’язку джерелом електромагнітного випромінювання є передавальні станції. Дії енергії зверхвисокочастотного діапазону працівники зазнають при регулюванні, настроюванні та випробовуванні радіопередавальних та радіолокаційних станцій.

Як реагує на електромагнітне поле організм людини

Електромагнітні поля особливо негативно впливають на організм людини, яка безпосередньо працює з джерелом випромінювання. В діапазоні промислових частот більше негативний вплив на біологічний об’єкт має електрична складова поля. Найчутливішими до ЕМП є нейродинамічні процеси, які прямо чи побічно перемикають хронобіологічні процеси організму на патологічний або стресовий режим функціонування.

Для зменшення впливу електромагнітних полів на персонал, який знаходиться у зоні дії деяких радіоелектронних засобів необхідним є ряд захисних заходів: організаційні, інженерно-технічні та лікувально-профілактичні.

Слід сказати, що ще на етапі проектування взаємне розміщення об’єктів має бути забезпечено таким чином, щоб інтенсивність опромінення була мінімальною. Також треба заздалегідь попіклуватися про зменшення часу перебування персоналу у зоні опромінення. Потужність джерел випромінювання повинна бути найменшою з можливих.

Радимо скористатися деякими корисними порадами для профілактики наслідків впливу електромагнітного випромінювання мобільного телефону і базових станцій стільникового зв'язку:

• будьте пильні, вибираючи житло на верхніх поверхах;

• при покупці телефону віддавайте перевагу моделям зі значенням

питомої коефіцієнта поглинання не більше 1 Вт / кг;

• не використовуйте блютуз гарнітуру, адже вона підвищує рівень електромагнітного випромінювання мобільного телефону;

• намагайтеся менше говорити і користуйтеся гучномовцем, щоб не тримати трубку занадто близько до тіла;

• якщо у вас є сумніви щодо вашого телефону, зверніться за консультацією до фахівців.

Отож, є досить багато методів захисту свого здоров’я від небезпеки на робочому місці з підвищеним електромагнітним фоном. Крім того, потрібно дотримуватись Державних стандартів України та не порушувати їх норм.

8.2 Джерела шуму і вібрацій, методи їх знешкодження

Вібрація – коливання, тремтіння. Переміщення точки або механічної системи при якому відбувається почергове зростання й зменшення в часі значень хоча б однієї координати називають вібрацією

Вібрація серед всіх видів механічних впливів для технічних об'єктів найбільш небезпечна. Знакозмінні напруження, викликані вібрацією сприяють накопиченню пошкоджень в матеріалах, появі тріщин та руйнуванню. Найчастіше і досить швидко руйнування об'єкта настає при вібраційних впливах за умов резонансу. Вібрації викликають також й відмови машин, приладів.

Вібрація викликає порушення фізіологічного та функціонального станів людини. Стійкі шкідливі фізіологічні зміни називають вібраційною хворобою. Симптоми вібраційної хвороби проявляються у вигляді головного болю, заніміння пальців рук, болю в кистях та передпліччі, виникають судоми, підвищується чутливість до охолодження, з'являється безсоння. При вібраційній хворобі виникають патологічні зміни спинного мозку, серцево-судинної системи, кісткових тканин та суглобів змінюється капілярний кровообіг.

Функціональні зміни, пов'язані з дією вібрації на людину-оператора - погіршення зору, зміни реакції вестибулярного апарату, виникнення галюцинацій, швидка втомлюваність. Негативні відчуття від вібрації зникають при прискореннях, що складають 5% прискорення сили ваги, тобто при 0,5 м/с2. Особливо шкідливі вібрації з частотами, близькими до частот власних коливань тіла людини, більшість котрих знаходиться в межах 6... 30 Гц.

Резонансні частоти окремих частин тіла наступні:
очі - 22... 27; горло - 6... 12; грудна клітка - 2... 12; ноги, руки - 2... 8; голова - 8... 27; обличчя та щелепи - 4... 27; поясничная частина хребта - 4... 14; живіт - 4... 12.

Вібрації, що впливають на операторів різних машин, поділяються на категорії згідно ГОСТ 12.1. 012-90.

Гігієнічні характеристики та нормування вібрацій. Гігієнічне нормування вібрацій забезпечує вібробезпеку умов праці. Дія вібрації на організм людини визначається наступними характеристиками: інтенсивністю, спектральним складом, тривалістю впливу, напрямком дії.

Захист від вібрацій. Загальні методи боротьби з вібрацією базуються на аналізі рівнянь, котрі описують коливання машин у виробничих умовах і класифікуються наступним чином: зниження вібрацій в джерелі виникнення шляхом зниження або усунення збуджувальних сил; відлагодження від резонансних режимів раціональним вибором приведеної маси або жорсткості системи, котра коливається; вібродемпферування - зниження вібрацій за рахунок сили тертя демпферного пристрою, тобто переведення коливної енергії в тепло; динамічне гасіння - введення в коливну систему додаткових мас або збільшення жорсткості системи; віброізоляція - введення в коливну систему додаткового пружного зв'язку, з метою послаблення передавання вібрацій, суміжному елементу конструкції або робочому місцю; використання індивідуальних засобів захисту.

Роботу щодо знешумлення діючого виробничого обладнання в

приміщенні розпочинають зі складання шумових карт та спектрів шуму, обладнання і виробничих приміщень, на підставі котрих виноситься рішення щодо напрямку роботи.

Нормування шумів. В Україні і в міжнародній організації зі стандартизації застосовується принцип нормування шуму на основі граничних спектрів (граничне допустимих рівнів звукового тиску) в октавних смугах частот.

Граничні величини шуму на робочих місцях регламентуються ГОСТ 12.1. 003-86. В ньому закладено принцип встановлення певних параметрів шуму, виходячи з класифікації приміщень за їх використанням для трудової діяльності різних видів.

В нормах передбачаються диференційовані вимоги до допустимих рівнів шуму в приміщеннях різного призначення в залежності від характеру праці в них. Шум вважається допустимим, якщо вимірювані рівні звукового тиску у всіх октавних смугах частот нормованого діапазону (63-8000 Гц будуть нижчі, ніж значення, котрі визначаються граничним спектром.

Висновок. Розглянуто питання електромагнітного забруднення довкілля, його вплив на людину, шляхи його зменшення. Розглянуто джерела шуму і вібрацій та методи їх знешкодження.

ВИСНОВКИ

1. Проведено аналіз задачі аутентифікації користувача телекомунікаційної мережі, розглянуто чинники і способи аутентифікації. Розглянуто переваги і недоліки наявних способів аутентифікації. Встановлено, що найперспективнішою в плані зменшення рівня помилок під час формування висновку про аутентифікацію є біометрична аутентифікація. Розглянуто, статичні методи аутентифікації, які засновані на фізіологічних особливостях людини, та динамічні методи, які базуються на індивідуальних характерностях у поведінці людини – підсвідомі рухи у процесі виконання будь-якої дії.

2. Встановлено, що системи голосової аутентифікації мають низьку собівартість, простоту у виконанні та ряд інших переваг. Нинішні системи ідентифікації за голосом людини можуть бути значно модернізованими за рахунок впровадження методів обробки даних, які вже є дослідженими та широко використовуються, і, насамперед, мають бути модернізовані методи та програмно-апаратні засоби введення голосового сигналу користувача та його виділення.

3. Виконано дослідження механізмів і вивчено способи опису генерації голосового сигналу, а також запропоновано вимоги до способів аналізу мовних сигналів з метою аутентифікації користувача. Методика опрацювання мовного сигналу повинна давати змогу встановити інформативні характеристики, незалежні від часу, а залежні лише від особливостей конкретного мовного апарату, таким чином придатні для безпомилкової ідентифікації особи. Можна бачити, що голосовий сигнал є складним амплітудно-модульованим сигналом, для якого дослідження несучої складової у частотному, часовому, частотно-часовому представленнях дозволяє визначити особу.

4. Основною ознакою користувача є частота основного тону несучої складової сигналу, допоміжними ознаками – форманти (максимуми спктральної характеристики.

5. Піддано аналізу способи визначення частот основного тону та перших формант.

6. Обґрунтовано принципову схему експерименту для запису голосового сигналу, критерії вибору обладнання, зокрема мікрофона, АЦП, обчислювальних засобів.

7. Запропоновано методики реєстрації мовного сигналу та його опрацювання, які дозволять ефективно виділити інформативні параметри для задачі ідентифікації користувачів.

8. Проведено відбір голосових сигналів однієї особи. Обчислено оцінки амплітудних спектрів отриманих реєстрограм голосових сигналів для задачі оцінювання частот розміщень формант.

9. Автокореляційний метод з певною його модифікацією було використано для того, щоб оцінити значення періоду основного тону.

Встановлено, що індивідуальними характеристиками особи будуть значення частот на яких розміщенні форманти та періоду основного тону та відрізняються з ідентичними оцінками голосових сигналів для іншої особи. Відповідно до вище описаного, можна стверджувати, що для задачі ідентифікації та аутентифікації особи можна використовувати оцінки формантних часто та період основного тону.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ричард Э. Смит. Аутентификация: от паролей до открытых ключей = Authentication: From Passwords to Public Keys First Edition. — М.: Вильямс, 2002. — С. 432.

2. под. редакцией А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева. Аутентификация. Теория и практика обеспечения доступа к информационным ресурсам. = Authentication. Theory and practice of ensuring access to information resources.. — М.: Горячая линия – Телеком, 2009. — С. 552.

3. https://ru.wikipedia.org/wiki/Аутентификация

4. Біометричні технології в XXI столітті та їх використання правоохоронними органами: посібник / В. П. Захаров, В. І. Рудешко; Львів. держ. ун-т внутр. справ. — 2-ге вид., допов. — Львів: ЛьвДУВС, 2015. — 491 с.

5. Дворянкин С. В. Речевая подпись / Под ред. заслуженного деятеля науки РФ, д.т.н. проф. А. В. Петракова. – М.: РИО МТУСИ, 2003 – С. 183 – 184.

6. Голубев Г. А., Габриелян Б. А. Современное состояние и перспективы развития биометрическихтехнологий // Нейрокомпьютеры. Разработка. Применение. № 10, 2004, – С. 39 – 46.

7. Иванов А. И. Биометрическая идентификация личности по динамике подсознательных движений – Пенза: Издательство Пензенского государственного университета, 2000, С. 188.

8. Resources Related to Biometrics and People with Disabilities. The International Center for Disability Resources on the Internet. http://www.icdri.org/biometrics/biometrics.htm.

9. Рабинер Л. Р., Шафер Р. В. Цифровая обработка речевых сигналов: Пер. с англ./Под ред. М. В. Назарова, Ю. Н. Прохорова.– М.: Радио и связь, 1981.– 495 с.

10. Диденко С. М. Автореферат дисертации: «Разработка и исследование компьютерной модели динамики системы «пользователь-мышь»». Тюмень 2007. – 25 с.

11. Беленков В. Д. Электронные системы идентификации подписей // Защита информации. Конфидент. 1997, № 6, – С.39 – 42.

12. Plomondon R., Lorette G. Automatic signature verification and writer identification – the state of the art // Pattern Recognition 1999 – Vol. – 22, № 2, p. 107 – 131.

13. Колядин Д. В., Савин А. А. О проблеме верификации подписи в системах контроля доступа. http://cs.mitp.ru/docs.research/signature.html

14. Расторгуев С. П. Программные методы защиты информации в компьютерах и сетях. М.:“Яхтсмен”, 1993. – 150 с. 7. Рыбченко Д. Е. Критерии устойчивости и индивидуальности клавиатурного почерка при вводе ключевых фраз // Специальная техника средств связи. Серия. Системы, сети и технические средства конфиденциальной связи. Пенза, ПНИЭИ, 1997, Выпуск № 2. – С.104 –107.

15. Рыбченко Д. Е., Иванов А. И. Анализ клавиатурного почерка аппаратом нечетких множеств для целей ограничения доступа и аудита // Специальная техника средств связи. Серия. Системы, сети и технические средства конфиденциальной связи. Пенза, ПНИЭИ, 1996, Выпуск №1., – С.116 – 119.

16. Широчин В. П., Кулик А. В., Марченко В. В. Динамическая аутентификация на основе анализа клавиатурного почерка. – http://www.masters.donntu.edu.ua/2002/fvti/aslamov/files/bio_autentification.htm

17. Болл Р.М. Руководство по биометрии: пер. с англ. Н.Е. Агаповой / Р.М. Болл – М.:Техносфера, 2007. – 368 с.

18. Сорокин В.Н. Распознавание личности по голосу: аналитический обзор / В.Н.Сорокин, В.В.Вьюгин, А.А.Тананыкин // Информационные

процессы. М.: РАН. 2012. Т. 12. № 1. С. 1–30.

19. ГОСТ Р 54412 – 2011/ ISO/IEC/TR 24741:2007 Информационные технологии. Биометрия, М.: Стандартинформ, 2012. – 58 с.

20. Максимов Е.М. Актуальные задачи речевой акустики / Е.М. Максимов, Ю.Н. Ромашкин, С.А. Лопатина // Речевые технологии. – 2008. – №2. – С. 66-71.

21. Маркел Дж. Д. Линейное предсказание речи : пер. с англ. / Дж. Д. Маркел, А. Х. Грэй ; [под ред. Ю. Н. Прохорова, В. С. Звездина]. – М., Связь, 1980. – 308 с.

22. Ремизов А.Н. Медицинская и биологическая физика: учеб. для вузов / А.Н. Ремизов, А.Г. Максина, А.Я. Потапенко. – 4-е изд., перераб. и дополн. – М. : Дрофа, 2003. – 560 с.: ил. – ISBN 5-7107-5001-8

23. Физическая акустика. Под ред. У. Мэзона / пер. с англ. ; [под ред. Л.Д. Розенберга.]. – М. : Мир, 1966. – 589 с.

24. Исакович М.А. Общая акустика : учеб. пособ. / М.А. Исакович. – М. : Наука, 1973. – 496 с.

25. Сорокин В.Н. Фундаментальные исследования речи и прикладные задачи речевых технологий / В.Н. Сорокин // Речевые технологии. – 2008. – №1. – С. 18-49.

26. Бархатов А.Н. Акустика в задачах. Учеб. рук-во. : для вузов / А.Н. Бархатов, Н.В. Горская, А.А. Горюнов и др. ; [под ред. С.Н. Гурбатова, О.В. Руденко.]. – М. : Наука, 1996. – 336 с. – ISBN 5-02-014742-7.

27. Фланаган Джеймс. Анализ, синтез и восприятие речи : пер. с англ. / Джеймс Фланаган ; [под ред. Пирогова А. А.]. – М. : “Связь”, 1968. – 396 с.

28. Физиология речи. Восприятие речи человеком / Л.А. Чистович., А. В. Венцов., М. П. Гранстрем и др. – Ленинград, изд-во Наука, 1976. – 388 с.

29. Медведев О. Н. Разработка методов эффективного кодирования речи на основе новых моделей источника речеобразования : автореф. дис. на

соискание ученой степени канд. техн. наук : 05.12.13 “Системы, сети и устройства телекоммуникаций” / Медведев Олег Николаевич ; Моск. техн. ун-тет. связи и информатики – М., 2007. – 19 с.

30. Фант Гунер. Акустическая теория речеобразования : пер. с англ. / Гунер Фант ; [под ред. Григорьева В. С.]. – М. : Наука, 1964. – 284 с.

31. Sadaoki Furui. Digital speech. Processing, synthesis and recognition. / Furui Sadaoki. – Tokyo : Tokyo institute of technology, 2000. – 439 с. – ISBN 0-8247-0452-5.

32. Федоров Е.Е. Выделение длины периода основного тона речевого сиґнала. / Е.Е. Федоров // Искуственный интелект. – 2004, №1. – С. 237-242. – ISSN 1561-5367.

33. Пирогов А.А. Устройство для автоматического определения частоты основного тона. Реестр изобретений СССР. Авторское свидетельство №129739 с приоритетом от 08.06.1958 г. Бюллетень изобретений и товарных знаков. 1960. № 13. С. 38.

34. Аграновский А.В. Теоретические аспекты алгоритмов обработки и классификации речевых сиґналов / А.В. Аграновский, Д.А. Леднов. – М. : Радио и связь, 2004. – 164 с. – ISBN 5-256-01743-8.

35. Баронин С.П. Автокорреляционный метод выделения основного тона речи / С.П. Баронин // Сб. трудов Гос. НИИ Мин. связи СССР. Вып. 3(24) – М., 1961. С. 93–102.

36. Баронин С.П. Автокорреляционный метод выделения основного тона речи. Пятьдесят лет спустя / С.П. Баронин // Речевые технологии. – 2008. – №2. – С. 3-13.

37. Монтгомери Д.К. Планирование эксперимента и анализ данных : пер. с англ. / Д.К. Монтгомери. – Л. : Судностроение, 1980. – 384 с.

38. Налимов В.В. Теория експеримента / В.В. Налимов. – М. : Наука, 1971. – 207 с.

39. Сидоров И.Н. Отечественные и зарубежные микрофоны и телефоны. Справочное пособие / И.Н. Сидоров. – М. : Горячая линия-Телеком, 2004. – 283 с.: ил. – (Массовая радиобиблиотека; Вып.1273). – ISBN 5-93517-18-5

40. Дедів І. Ю. Обгрунтування методу голосової ідентифікації особи / Ірина Дедів, Леонід Дедів, С. Макар // Матеріали Ⅳ Міжнародної науково-технічної конференції „Теоретичні та прикладні аспекти радіотехніки, приладобудування і комп’ютерних технологій“ присвячена 80-ти річчю з дня народження професора Я.І. Проця, 20-21 червня 2019 року. — Т. : ФОП Паляниця В. А., 2019. — С. 90–91. — (Обчислювальні методи та засоби в радіотехніці і приладобудуванні).

ДОДАТКИ

Додаток А

Текст програми оцінювання характеристик голосових сигналів

```
clear all;
x=wavread('E1');
t=(0:(length(x)-1))./32000;
figure(1);
plot(t,x);
xlabel('Час, с');
ylabel('Амплітуда, мВ');
grid on

ff=abs(fft(x(40000:60000)));
figure(2);
plot(ff(1:1000));
xlabel('Частота, Гц');
ylabel('Амплітуда, мВ');
grid on

a=xcorr(x(40000:60000));
figure(3);
plot(a);
title('автокореляція');
xlabel('Зсув, u');
ylabel('Амплітуда, мВ');
grid on;
z=abs(fft(a,32000));
w=z(1:500);
figure(4);
plot(w);
title('спектр потужності');
xlabel('Частота, Гц');
ylabel('Потужність, мВ^2');
grid on;
[f1,f2]=max(w(1:200));
```

Додаток Б

Матеріали IV Всеукраїнської науково-технічної конференції ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ РАДІОТЕХНІКИ, ПРИЛАДОБУДУВАННЯ І КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ 2019

УДК 621.391

Ірина Дедів, к.т.н, Леонід Дедів, к.т.н., доц., С. Макар
Тернопільський національний технічний університет імені Івана Пулюя, Україна

ОБГРУНТУВАННЯ МЕТОДУ ГОЛОСОВОЇ ІДЕНТИФІКАЦІЇ ОСОБИ

Розглянуто відомі методи ідентифікації особи за біометричними характеристиками. Обґрунтовано метод голосової ідентифікації, який є відносно простий та дешевий у реалізації та при застосуванні оптимальних методів опрацювання голосових сигналів може з достатньо високою достовірністю здійснювати ідентифікацію особи.

Ключові слова: біометрія, голосовий сигнал, спектрльний аналіз, автокореляційна функція.

Iryna Dediv, Leonid Dediv, S. Makar

THE REASONING OF THE METHOD OF VOICE IDENTIFICATION

There are considered well-known methods for identifying a person by biometric characteristics. The method of voice identification is substantiated, which is relatively simple and cheap in realization and when using the optimal method of processing of voice signals with sufficiently high reliability to conduct identification of a person.

Keywords: biometrics, voice signal, spectral analysis, autocorrelation function.

Актуальною технічною задачею в галузі телекомунікаційних систем, інтернет-технологій тощо, є забезпечення функцій контролю доступу, що полягають у формуванні дозволу або забороні доступу до певних визначених баз даних. Такий контроль ґрунтується на ідентифікації суб'єктів, яким потрібен доступ і об'єкта даних, що є метою доступу. В галузі інформаційної безпеки під ідентифікацією розуміється процедура розпізнавання користувача в системі шляхом сприйняття системою ідентифікаторів користувача, які формуються на основі апріорної інформації про нього. При цьому, особливо актуальним є обґрунтування вибору типів ідентифікаторів виходячи із технічної складності реалізації системи контролю доступу, економічної обґрунтованості та захищеності.

Особливо поширеним сьогодні є розроблення для задачі ідентифікації особи автоматизованих методів і засобів, що ґрунтуються на оцінюванні її фізіологічних або поведінкових характеристик – методів біометрії, що пояснюється їхньою винятковістю та низькою ймовірністю помилки ідентифікації. При цьому, всі методи біометричної ідентифікації можна розділити на статичну і динамічну. До першої групи належать методи ідентифікації за відбитком пальця, формою долоні, розташуванням вен на тильній стороні долоні, сітківкою ока, райдужною оболонкою ока, формою обличчя, термограмою особи тощо. Методи динамічної ідентифікації ґрунтуються на поведінковій (динамічній) характеристиці людини, зокрема ідентифікація проводиться за рукописним почерком, клавіатурним почерком, голосом, рухом губ тощо [1]. Із усіх зазначених методів біометричної ідентифікації найбільш перспективним при ймовірності відмови у доступі чи помилкової ідентифікації (0,5….5)% є метод голосової ідентифікації, якому властива простота технічної реалізації та низька собівартість порівняно з іншими методами отримання біометричних параметрів. Важливою при цьому є задача обґрунтування методу опрацювання голосових сигналів та виділення інформативних ознак, оцінки яких носили б індивідуальний характер та давали б можливість проведення ідентифікації особи.

Ідентифікація користувача може виконуватися за такими показниками: короткочасна енергія сигналу (визначається функцією короткочасної енергії з використанням вікон Хеммінга [3]; автокореляційна функція (дозволяє визначити