Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента *Корнєва Андрія Дмитровича*

академічної групи *125-20-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему ***Системи голосової автентифікації для розмежування повноважень користувачів десктопних Windows-додатків***

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	доц. Сафаров О.О.	95	відмінно	
розділів:				
спеціальний	доц. Сафаров О.О.	95	відмінно	
економічний	к.е.н., доц. Пілова Д.П.	90	відмінно	
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2024

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту ***Корнєву Андрію Дмитровичу*** **академічної групи** ***125-20-2***
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Системи голосової автентифікації для розмежування повноважень користувачів десктопних Windows-додатків***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 23.05.2024 № 469-с

Розділ	Зміст	Термін виконання
Розділ 1	Аналіз еволюції голосової автентифікації від початкових концепцій до сучасних технологій. Глибокий аналіз технічних характеристик та функціональності сучасних систем голосової автентифікації. Розгляд відповідності голосової автентифікації законодавству та визначення етичних проблем у зв'язку з її використанням. Аналіз перспектив розвитку голосової автентифікації та ідентифікація основних викликів, які можуть виникнути на шляху її розвитку.	15.03.2024
Розділ 2	Дослідження ефективності голосової автентифікації на прикладі конкретних систем. Розробка та впровадження системи голосової автентифікації в реальному середовищі. Аналіз результатів тестування та впровадження	10.05.2024
Розділ 3	Розрахунок капітальних витрат, річних експлуатаційних витрат, аналіз економічної ефективності.	11.06.2024

Завдання видано _____ Олександр САФАРОВ
(підпис керівника) (ім'я, прізвище)

Дата видачі: 01.04.2024р.

Дата подання до екзаменаційної комісії: 28.06.2024р.

Прийнято до виконання _____ Андрій КОРНЄВ
(підпис студента) (ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка: 96 с., 19 рис., 2 табл., 5 додатка, 20 джерел.

Об'єкт розробки: методи застосування системи голосової автентифікації для розмежування повноважень користувачів десктопних Windows-додатків.

Предмет розробки: рекомендації для використання системи голосової автентифікації для розмежування повноважень користувачів десктопних Windows-додатків

Мета роботи: вдосконалити ефективність використання автентифікації голосу для розпізнавання мовлення та запропонувати рекомендації, щодо покращення інформаційної безпеки в цифровому середовищі.

У першому розділі була розглянута історія та еволюція голосової автентифікації, основні принципи роботи, переваги та недоліки цього методу біометричної ідентифікації.

У другому розділі було описано процес розробки системи голосової автентифікації для розмежування повноважень користувачів десктопних Windows-додатків, а також результати тестування та аналіз ефективності системи.

У третьому розділі було здійснено аналіз економічної ефективності впровадження системи голосової автентифікації, включаючи оцінку витрат на розробку, впровадження та підтримку, а також потенційні економічні вигоди для організацій.

Практична цінність розробки полягає у забезпеченні ефективного та безпечного керування доступом користувачів до різних функцій та даних у десктопних Windows-додатках за допомогою голосової автентифікації.

ГОЛОСОВА АВТЕНТИФІКАЦІЯ, БІОМЕТРИЧНА ІДЕНТИФІКАЦІЯ, КІБЕРБЕЗПЕКА, РОЗПІЗНАВАННЯ ГОЛОСУ, РОЗМЕЖУВАННЯ ПОВНОВАЖЕНЬ, МОДЕЛІ АНАЛІЗУ ГОЛОСУ, ШУМОВІ ПЕРЕШКОДИ, ЗАХИСТ ВІД АТАК, ЕКОНОМІЧНА ЕФЕКТИВНІСТЬ.

ABSTRACT

Explanatory note: 96 pp., 19 pic., 2 table, 5 app, 20 sources.

Object of the development: methods of applying a voice authentication system for the differentiation of user privileges in desktop Windows applications.

Subject of the development: recommendations for the use of a voice authentication system for the differentiation of user privileges in desktop Windows applications.

Objective of the work: to enhance the efficiency of using voice authentication for speech recognition and to propose recommendations for improving information security in the digital environment.

In the first section, the history and evolution of voice authentication, the main principles of operation, and the advantages and disadvantages of this biometric identification method were reviewed.

In the second section, the process of developing a voice authentication system for the differentiation of user privileges in desktop Windows applications was described, along with the testing results and system efficiency analysis.

In the third section, an analysis of the economic efficiency of implementing a voice authentication system was carried out, including an assessment of development, implementation, and maintenance costs, as well as the potential economic benefits for organizations.

The practical value of the development lies in ensuring effective and secure user access management to various functions and data in desktop Windows applications using voice authentication.

VOICE AUTHENTICATION, BIOMETRIC IDENTIFICATION, CYBERSECURITY, VOICE RECOGNITION, PRIVILEGE DIFFERENTIATION, VOICE ANALYSIS MODELS, NOISE INTERFERENCE, ATTACK PROTECTION, ECONOMIC EFFICIENCY.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

AI – Artificial Intelligence;
API – Application Programming Interface;
ASR – Automatic Speech Recognition;
CD – Continuous Deployment;
CI – Continuous Integration;
EER – Equal Error Rate;
FAQ – Frequently Asked Questions;
FAR – False Acceptance Rate;
FRR – False Rejection Rate;
GUI – Graphical User Interface;
HCI – Human-Computer Interaction;
ID – Identification;
IoT – Internet of Things;
БІ – біометрична ідентифікація;
ІБ – інформаційна безпека;
МС – мультимодальні системи;
ПЗ – програмне забезпечення;
УІ – унікальний ідентифікатор;
ФР – фоновий рівень;
ЦА – цифрова аутентифікація.

ЗМІСТ

с.

ВСТУП

Об'єкт розробки: методи застосування системи голосової автентифікації для розмежування повноважень користувачів десктопних Windows-додатків.

Предмет розробки: рекомендації для використання системи голосової автентифікації для розмежування повноважень користувачів десктопних Windows-додатків

Мета роботи: вдосконалити ефективність використання автентифікації голосу для розпізнавання мовлення та запропонувати рекомендації, щодо покращення інформаційної безпеки в цифровому середовищі.

Розглянути сучасні системи автентифікації голосу: аналізувати характеристики, переваги та недоліки різних систем автентифікації голосу.

Розглянути технічні принципи систем розпізнавання мовлення: розглянути технічні аспекти систем розпізнавання мовлення, включаючи акустику та біометрію, методи обробки сигналів і алгоритми розпізнавання.

Оцінити ступінь надійності та точності методів автентифікації голосу: проаналізувати надійність і точність різних методів автентифікації голосу, щоб визначити їх здатність виявляти шахрайство та розширювати ідентифікацію користувача.

Аналіз загроз кібербезпеці та інформаційній безпеці: дослідити потенційні загрози та проблеми, пов'язані з використанням голосової автентифікації в цифровому середовищі, та запропонувати стратегії захисту від цих загроз.

Визначити рекомендації щодо вдосконалення систем голосової автентифікації: на основі отриманих результатів сформулювати рекомендації щодо підвищення ефективності та безпеки систем голосової автентифікації у сфері кібербезпеки.

Постановка проблеми: визначення ефективності та доцільності використання голосової автентифікації у сфері кібербезпеки. Зокрема, розглядаються проблеми та обмеження, пов’язані з використанням розпізнавання мовлення для захисту інформації, а також можливості подальшого розвитку цього методу для забезпечення високого рівня безпеки в цифрових середовищах.

Ця тема є актуальною в умовах зростання кіберзагроз та необхідності розробки надійних та ефективних методів захисту інформації. Останніми роками голосова автентифікація стає все більш популярним інструментом для підтвердження особи користувача, але її ефективність і стійкість до атак залежать від багатьох факторів і вимагають ретельного дослідження й аналізу.

Для системи голосової автентифікації, стійкість до підробки голосу є однією з найбільш серйозних загроз. Зловмисники можуть спробувати відтворити голос користувача або використати запис голосу з раніше здійсненого дзвінка чи відеоролика. Для боротьби з цими проблемами потрібно досліджувати технології, що будуть дозволяти визначити живого користувача та знайти підробки, такі як заміна акустичних характеристик та частоти голосу.

Обхід системи голосової автентифікації при використанні зловмисниками технологічних вразливостей. Це може бути експлуатація програмних помилок або вразливостей у алгоритмах розпізнавання голосу. Дослідження таких вразливостей допомагає розробникам покращити безпеку систем та уникнути можливих атак.

Ефективність голосової ідентифікації. Ідентифікація за голосом вважається одним з найпотужніших методів біометричної ідентифікації завдяки унікальним характеристикам голосу кожної людини. Однак ефективність цього методу залежить від різних факторів, таких як: надійність і точність ідентифікації; відмінність голосових характеристик; стійкість до обману; вплив зовнішніх факторів.

Таким чином, постановка проблеми полягає у вивченні потенціалу автентифікації голосу як інструменту підвищення інформаційної безпеки в цифровому суспільстві та визначенні факторів, що впливають на її ефективність, і проблем, пов'язаних з її впровадженням.

Обґрунтування актуальності теми: важливим елементом будь-якого дослідження є обґрунтування актуальності сучасних викликів кібербезпеки та необхідності розробки нових методів верифікації.

Зростання кіберзагроз – сучасний цифровий світ стикається з дедалі більшою кількістю кіберзагроз, зокрема хакерські атаки, фішинг та віруси. У цьому випадку захист інформації від несанкціонованого доступу стає критично важливим.

Постійний розвиток технологій – швидкий розвиток технологій створює нові можливості для кіберзлочинців. Існуючі методи автентифікації можуть бути вразливими до нових методів атак.

Попит на зручність і безпеку – користувачі вимагають не тільки високого рівня захисту даних, але й простоти використання. Голосова автентифікація може поєднувати ці два елементи, поєднуючи простоту використання з високим рівнем безпеки.

Нормативні вимоги – зростаючі нормативні вимоги щодо захисту персональних даних і конфіденційності змушують компанії шукати нові, ефективніші методи автентифікації.

Зростання онлайн-шахрайства –оскільки онлайн-платежі та інші онлайн-сервіси стають все більш популярними, спроби онлайн-шахрайства зростають. Забезпечення надійної автентифікації користувачів, стає ключовим фактором у запобіганні фінансовому шахрайству та іншим кіберзлочинам.

Важливість цього дослідження полягає в тому, що кіберзагрози постійно зростають, а стандартні методи автентифікації, такі як паролі, стають менш ефективними. Оскільки голос є унікальним біометричним показником, який важко підробити, голосова автентифікація може стати важливим інструментом забезпечення безпеки та захисту конфіденційності даних. Подальші дослідження в цій галузі допоможуть виявити потенційні загрози та розробити ефективні методи захисту, щоб убезпечити користувачів у цифровому середовищі.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Теоретичний огляд

1.1.1 Тенденція розвитку голосової автентифікації

Перші наукові дослідження з 1960 по 1970 рік:

Перші дослідження голосової ідентифікації були опубліковані в 1960-х роках. У цей період дослідження були зосереджені на розробці методів аналізу голосу та встановленні особливостей голосового сигналу.

Одним із перших відомих досліджень був проєкт "Speaker Independent Digits Recognition" (SIDR), який вивчав здатність розпізнавати цифри, вимовлені будь-яким говорящим, незалежно від акценту чи тембру голосу.

Вважається, що цей проєкт був великим досягненням у галузі обробки мовлення та машинного навчання. Створення такої системи вимагало розробки нових алгоритмів обробки сигналів і аналізу голосу. Тим не менш, через обмежену обчислювальну потужність і обмежений обсяг даних для навчання моделей SIDR має обмежені можливості та точність.

Принципи «індивідуальної незалежності», які вперше були висвітлені в проєкті в голосовому розпізнаванні, означали, що система могла ідентифікувати будь-який голос, не маючи попереднього навчання цьому голосу.

Спроможність працювати з обмеженим обсягом даних була важливою характеристикою SIDR. Він міг розпізнавати цифри, навіть якщо для кожної цифри було доступно лише невелика кількість записів голосу. Це було значним досягненням, особливо враховуючи обмеження технологій, які були тоді.

SIDR відіграла важливу роль у вивченні та розвитку технологій голосового розпізнавання, хоча її не використовували широко в бізнесі. Її ідеї та підходи стали основою для подальших досліджень у галузі голосової автентифікації [3].

Перші комерційні системи (1980-х – 1990х років):

Перші комерційні системи голосової ідентифікації були запущені в 1980-х роках у промислових і урядових організаціях для контролю доступу та ідентифікації співробітників.

У 1980-1990-х роках урядові та військові органи запровадили системи голосової ідентифікації. Голосові системи ідентифікації в Україні ще не використовувалися широко в 1980-1990-х роках. Тим не менш, ці технології вважалися важливими для безпеки та ідентифікації, і вони були застосовані в багатьох країнах по всьому світу.

Наприклад, у Сполучених Штатах армія, спеціальні військові підрозділи та урядові агентства, такі як Центральне розвідувальне агентство (CIA) або Національна аеронавтична і космічна адміністрація (NASA), використовують системи голосової ідентифікації.

У 1986 році NEC Corporation розробила передову систему голосової ідентифікації Voice Password System, яка дозволяє користувачам ідентифікуватися за їхнім голосом. Ця технологія базується на складних алгоритмах мовленнєвого синтезу та аналізу голосу, які дозволяють системі ідентифікувати особливості голосу кожного користувача. Система Voice Password запобігає несанкціонованому доступу до конфіденційної інформації та ресурсів у багатьох сферах бізнесу, таких як підприємства, фінансові установи та урядові організації.

Основною перевагою Voice Password System є простота використання. Голосова ідентифікація не вимагає використання фізичних пристроїв аутентифікації або запам'ятовування складних паролів, що робить її зручним і ефективним способом аутентифікації. Крім того, система є надзвичайно безпечною, оскільки голосові шаблони кожного користувача ідентифікуються.

Voice Password System може бути корисним у багатьох сферах бізнесу. Ця технологія підвищує безпеку користувачів цифрової безпеки та є важливим кроком у розвитку біометричних систем ідентифікації [4].

Розвиток алгоритмів і штучних нейронних мереж у 2000-ті роки:

Алгоритми та штучні нейронні мережі продемонстрували значний прогрес у 2000-х роках, які стали ключовими для подальшого розвитку голосової автентифікації. У цей період відбувалися значні досягнення в машинному

навчанні та обробці сигналів, що призвело до інновацій у галузі голосової технології.

Вдосконалення алгоритмів розпізнавання голосу було важливим досягненням, яке призвело до більшої точності та надійності голосової автентифікації. Глибоке навчання та нейронні мережі відкрили нові можливості для аналізу голосових характеристик і вдосконалення методів ідентифікації.

Зокрема, були розроблені нові архітектури нейронних мереж, які забезпечують високу швидкодію та точність розпізнавання при роботі з великими кількостями даних. Крім того, глибоке навчання дозволило враховувати більшу кількість голосових ознак, що поліпшило адаптивність системи до різних умов і типів голосу користувачів.

Деякі з найбільш поширених нейронних мереж включали:

Глибокі нейронні мережі (DNN): Використовувалися для вирішення задач розпізнавання голосу, оскільки вони мають високу точність і можуть адаптуватися до складних шаблонів голосу.

Згорткові нейронні мережі (CNN): вони аналізують спектрограми та інші голосові ознаки, щоб покращити розпізнавання голосу в різних ситуаціях.

Рекурентні нейронні мережі (RNN): використовувалися для моделювання часових залежностей у голосових даних для врахування динаміки та інтонації мовлення.

Крім того, у 2000-ті роки відбувся значний прогрес у розробці голосового програмного забезпечення. Це включало в себе створення більш простих для розробників і підприємств інтегрованих платформ для розпізнавання голосу.

У програмному забезпеченні в 2000-ті роки було розроблено кілька інтегрованих платформ для розпізнавання голосу:

Sphinx – це відкрите програмне забезпечення для розпізнавання мовлення, яке широко використовується як у комерційних проєктах, так і в наукових дослідженнях.

Microsoft Speech API (SAPI): розроблений компанією Microsoft, він допомагає програмам і платформам синтезувати мову та розпізнавати мовлення.

Google Cloud Speech-to-Text: хмарна платформа для розпізнавання мовлення, яка надає API для інтеграції голосового розпізнавання в програми та сервіси.

Загалом, двадцять перше сторіччя відзначилися інтенсивними дослідженнями та інноваціями в галузі голосової автентифікації. Це призвело до нових можливостей застосування голосової автентифікації в різних сферах життя, від бізнесу до розваг і медичних додатків [5].

Зростання популярності серед звичайних споживачів з 2010 року:

Починаючи з 2010 року голосова автентифікація стає все більш популярною серед звичайних споживачів. Це зростання відбулося завдяки кільком основним причинам. По-перше, голосова автентифікація та розпізнавання мови стали більш доступними для звичайних користувачів завдяки появі голосових асистентів, таких як Apple Siri, Google Assistant, Amazon Alexa та Microsoft Cortana. Ці асистенти використовували голосову автентифікацію для захисту даних користувачів і персоналізації послуг. По-друге, удосконалення мобільних технологій і зростання потужності мобільних пристроїв, таких як смартфони та планшети, дозволило реалізувати складні алгоритми голосового розпізнавання прямо на мобільних пристроях. Дозволяючи користувачам взаємодіяти зі своїми гаджетами за допомогою голосу, це значно підвищило їх зручність і ефективність використання.

Крім того, точність розпізнавання голосу значно покращилася завдяки розвитку машинного навчання та глибоких нейронних мереж. Завдяки цьому голосові технології стали більш надійними, оскільки вони мають меншу схильність до помилок і працюють краще в складних акустичних умовах. Багато людей тепер використовують голосову автентифікацію в повсякденних пристроях IoT, таких як розумні колонки, телевізори, автомобільні системи, розумні годинники та інші. Популярність голосової автентифікації зросла завдяки простоті використання, яка дозволяє швидко отримати доступ до особистих даних і сервісів без використання фізичних ключів або паролів.

Підвищення рівня безпеки за допомогою ідентифікації за допомогою унікальних голосових ознак є особливо важливим у сучасному світі цифрових загроз.

Голосові технології стали більш доступними для більшої кількості користувачів по всьому світу завдяки розширенню підтримки різних мов і діалектів. Це підвищило їхню популярність серед споживачів з різних країн і культур. Таким чином, з 2010 року голосова автентифікація стає все більш популярною серед звичайних споживачів завдяки різноманітним технологічним досягненням і перевагам, які вона пропонує користувачам. Це пояснює, чому голосові технології є важливою частиною сучасних цифрових послуг і пристроїв, які є частиною повсякденного життя мільйонів людей.

Участь у фінансових і інших послугах (сучасність):

Завдяки технологічним досягненням і зростаючій потребі в безпеці та зручності для користувачів використання голосової автентифікації значно зросла у фінансових і інших послугах. Голосова автентифікація стала важливою частиною систем безпеки багатьох банків і фінансових установ у фінансовому секторі. Банки, такі як HSBC, CitiBank і Barclays, використовують голосову автентифікацію, щоб ідентифікувати клієнтів під час телефонних дзвінків або взаємодії через мобільні додатки. Це швидко та безпечно підтверджує особу клієнта без використання традиційних паролів або PIN-кодів.

Оскільки голос кожної людини є унікальним і важко підроблюваним біометричним маркером, голосова автентифікація забезпечує високий рівень безпеки. Крім того, вона значно покращує користувацький досвід, забезпечуючи швидкий доступ до рахунків або фінансові операції. Це особливо важливо в умовах зростаючої кількості транзакцій через Інтернет і мобільні пристрої.

Голосова автентифікація також широко використовується в страхових компаніях. Вона використовується для перевірки особи клієнтів, коли вони звертаються до служби підтримки або оформляють страхові випадки. Це полегшує спілкування з клієнтами та знижує ризик шахрайства.

Голосова автентифікація широко використовується в інших сферах послуг, окрім фінансового сектору. Це використовується компаніями телекомунікацій,

такими як AT&T та Verizon, для ідентифікації абонентів під час звернень до служби підтримки. Це гарантує безпечний і швидкий доступ до персональних даних і послуг.

Голосова автентифікація полегшує швидкий доступ до медичних записів і зберігає конфіденційність пацієнтів у медичному секторі. Під час телефонних консультацій або доступу до електронних медичних карток вона використовується для підтвердження особи пацієнта.

Голосова автентифікація також буде використана в державних послугах. Урядові установи використовують цю технологію для ідентифікації громадян, які звертаються за різними службами, наприклад, для отримання соціальних виплат або доступу до електронних урядових послуг.

Таким чином, використання голосової автентифікації в фінансових і інших послугах сьогодні значно підвищує безпеку та зручність користувачів. Вона дозволяє швидко та безпечно отримати доступ до багатьох сервісів, зменшуючи ризик шахрайства та покращуючи досвід користувачів у багатьох сферах життя[6].

Аналіз історії голосової автентифікації свідчить про значний технологічний прогрес у цій області. Починаючи з 1960-1970-х років, було зафіксовано значний прогрес у наукових дослідженнях і використанні голосу як біометричного ідентифікатора, що привело до розвитку сучасних технологій, впроваджених у мобільних пристроях і онлайн-сервісах. З'явлення нових алгоритмів обробки сигналів, використання штучних нейронних мереж та інших інновацій сприяли покращенню продуктивності і точності систем голосового розпізнавання. Популярність мобільних пристроїв і голосових асистентів у 2010-х роках значно збільшила використання голосової автентифікації серед звичайних користувачів. Однак впровадження голосової автентифікації у фінансових і інших онлайн-сервісах породжує питання щодо безпеки даних користувачів і приватності, що вимагає розробки нових заходів захисту та підвищення безпеки голосових систем ідентифікації.

Таблиця 1.1 – Таблиця історії голосової автентифікації

Період	Опис	Основні досягнення
1960-1970-ті роки	Перші наукові дослідження з розпізнавання голосу. Проєкт "Speaker Independent Digits Recognition" (SIDR).	Створення алгоритмів для аналізу голосу та розпізнавання цифр.
1980-1990-ті роки	Запуск перших комерційних систем голосової ідентифікації у промислових та урядових організаціях.	NEC Voice Password System для контролю доступу.
Початок 2000-х	Значний прогрес у машинному навчанні та обробці сигналів.	Вдосконалення алгоритмів розпізнавання голосу.
Середина 2000-х	Розробка глибоких нейронних мереж, згорткових та рекурентних нейронних мереж для покращення аналізу голосових характеристик.	Використання DNN, CNN та RNN у розпізнаванні голосу.
З 2010 року	Поява голосових асистентів, таких як Apple Siri, Google Assistant, Amazon Alexa та Microsoft Cortana.	Голосові асистенти стають доступними для широкого загалу.
Середина 2010-х	Покращення точності розпізнавання голосу завдяки глибокому навчанню.	Голосові технології стають надійнішими та доступнішими.
Сучасність	Використання голосової автентифікації у фінансових установах, страхових компаніях, телекомунікаційних компаніях, медичних установах та державних службах.	Впровадження голосової автентифікації у різні сфери бізнесу та послуг.
Майбутнє	Розширення застосування голосової автентифікації у нових галузях, інтеграція з іншими біометричними технологіями.	Інтеграція з IoT-пристроями, розвиток голосових технологій для розумних будинків.

1.1.2 Основні поняття та методи голосової автентифікації

Основні поняття:

1) Голосовий відбиток, також відомий як Voiceprint, – це цифрове відображення особливостей голосу людини, яке використовується для

ідентифікації та автентифікації особи. Голосовий відбиток, як і відбитки пальців або сітківки ока, є біометричним маркером з особливостями, які роблять його унікальним для кожної людини. Для створення голосового відбитку акустичні характеристики, такі як частота, інтонація, тембр і ритм, аналізуються [7].

2) Алгоритми розпізнавання голосу – це програми, які використовуються для аналізу та обробки голосових сигналів з метою ідентифікації або порівняння людей. Вони обробляють та порівнюють голосові характеристики за допомогою різноманітних статистичних і математичних моделей. Розвиток машинного навчання та штучного інтелекту призвів до значного підвищення точності та надійності сучасних алгоритмів розпізнавання голосу.

3) Моделі мовлення є важливими компонентами систем розпізнавання голосу. Вони забезпечують розуміння та обробку мовленнєвих сигналів, а також ідентифікацію, розпізнавання та синтез мовлення. Моделі мовлення, які можуть бути статистичними або нейронними, використовуються для моделювання структури мовлення та багатьох його компонентів.

4) Фонеми, найменші звукові одиниці мови, відрізняються від інших звуків і впливають на їхнє значення. Розпізнають і моделюють мову.

5) Мовленнєві функції (Speech Features): особливості звукових сигналів, які аналізуються та розпізнаються. Вони включають спектральні характеристики, частоту, амплітуду тощо [8].

6) Мовленнєві граматики – це стандарти та обмеження, які визначають, як правильно поєднувати слова та фрази в мовленні. Використовуються, щоб покращити розпізнавання мовлення.

7) Мовленнєві корпуси, також відомі як мовленнєві корпуси, представляють собою значні набори записаних мовленнєвих даних, які використовуються для навчання та тестування мовленнєвих моделей.

8) Мовленнєві кодеки – це алгоритми для стиснення та передачі мовленнєвих сигналів, щоб збільшити пропускну здатність мережі або зберегти місце на пристроях з обмеженими ресурсами.

Основні методи голосової автентифікації:

Статичне голосове розпізнавання:

Одним із поширених методів голосової автентифікації є статичне розпізнавання голосу. У цьому способі користувач вимовляє слово або фразу, які вже були визначені як пароль. Для порівняння з аудіоданими, що надходять під час автентифікації, введені слова або фрази зберігаються в системі. Оскільки він не потребує складних технічних знань, цей метод досить простий у використанні та зручний для користувачів. Але для забезпечення високого рівня безпеки фрази або паролі повинні бути складними та унікальними. Одним із недоліків цього методу є те, що фраза чи пароль можуть бути підслухані чи відтворені. Отже, для забезпечення найвищого рівня захисту даних рекомендується використовувати статичне розпізнавання голосу як додатковий захист у поєднанні з іншими методами аутентифікації, такими як двофакторна аутентифікація.

Динамічне розпізнавання голосу:

Динамічне розпізнавання голосу – це передова техніка голосової автентифікації, яка базується на аналізі динамічних аспектів мовлення користувача. Цей метод відрізняється від інших тим, що він враховує як статичні, так і динамічні аспекти мовлення, такі як інтонація, темп, тон та інші акустичні характеристики. Це робить результати ідентифікації користувача більш точними та надійними.

Динамічне розпізнавання голосу має багато переваг, включаючи більшу точність ідентифікації, вищу стійкість до шахрайства, зменшення чутливості до шумів і акустичних перешкод і підвищення рівня безпеки. Системи динамічного розпізнавання можуть ефективно відрізняти справжній голос власника від підробленого або штучного за допомогою складного аналізу динамічних характеристик мовлення, які включають інформацію про ритм, інтонацію та інші характеристики.

Гібридні підходи:

Гібридні підходи до голосової автентифікації покращують продуктивність і безпеку процесу. Використання переваг кожного методу, компенсуючи його недоліки та підвищуючи загальну стійкість системи, є основною ідеєю.

Комбінація динамічного та статичного розпізнавання голосу є одним із прикладів гібридного підходу. Для більш точної ідентифікації користувача в цьому випадку система аналізує не тільки сам голосовий зразок, але й динамічні елементи мовлення, такі як темп, інтонація та ритм. Це підвищує стійкість до спроб обману або підробки голосу, оскільки потенційний зловмисник стикається з труднощами.

Гібридні підходи також використовують голосову автентифікацію з різними біометричними та небіометричними методами, такими як відбитки пальців, розпізнавання обличчя або кодові комбінації. Мультифакторна аутентифікація може бути створена за допомогою цієї комбінації, що робить її більш ефективною та надійною, оскільки для зламу системи потрібно зламати кілька видів захисту одночасно.

Гібридні підходи можуть підвищити безпеку та стійкість голосової автентифікації та забезпечити більш гнучку та індивідуалізовану систему автентифікації, яка може бути адаптована до потреб користувачів[9].

1.1.3 Технології та методи аналізу голосу

Розбір технологій та методів аналізу голосу:

1) Глибокі нейронні мережі (DNN):

Глибокі нейронні мережі (DNN), засновані на концепціях штучних нейронних мереж і глибокого навчання, є потужним інструментом у галузі голосової автентифікації. Ця технологія широко використовується для розпізнавання та аналізу голосових сигналів, що покращує процес ідентифікації особи за її голосом.

Глибокі нейронні мережі мають багатошарові архітектури, які складаються з великої кількості штучних нейронів, розташованих у послідовності різних шарів. Усі штучні нейрони отримують вхідні дані, обробляють їх за допомогою внутрішніх параметрів і передають оброблену інформацію наступному шару. Під час тренування на великих кількостях даних глибокі нейронні мережі вчаться

виконувати складні завдання шляхом автоматичного визначення найкращих параметрів і ваг для кожного штучного нейрона.

Глибокі нейронні мережі використовуються в голосовій автентифікації для виконання багатьох завдань, таких як розпізнавання голосу, ідентифікація користувачів і верифікація особи за її голосом. Ці мережі можуть точно визначити особливості голосу кожної людини, аналізуючи різні елементи голосового сигналу, такі як частотні характеристики, мел-кепстральні коефіцієнти, спектрограми тощо.

Завдяки здатності до автоматичного визначення складних і абстрактних особливостей голосу глибокі нейронні мережі можуть покращити точність і надійність систем автентифікації. Крім того, глибокі нейронні мережі можуть бути ефективно треновані на великих кількостях реальних голосових даних. Це дозволяє їм покращити продуктивність і адаптуватися до різних умов і мовних особливостей.

Незважаючи на це, необхідно враховувати, що навчання глибоких нейронних мереж вимагає значних обчислювальних ресурсів і великого обсягу даних. Крім того, недостатня кількість прикладів може призвести до проблеми перенавчання. Точність роботи глибоких нейронних мереж також може залежати від якості вхідних даних і параметрів тренування.

2) Рекурентні нейронні мережі (RNN):

Одним із найважливіших типів нейронних мереж є конкуруючі нейронні мережі (RNN), які спеціалізуються на обробці послідовних даних, таких як мовлення, текст або часові ряди. Здатність RNN обробляти послідовності змінних довжин за допомогою внутрішнього стану (пам'яті) є її основною характеристикою. Це робить їх надзвичайно корисними для завдань, у яких важлива контекстуальна інформація зберігається протягом тривалого часу.

У традиційній нейронній мережі всі обчислення виконуються незалежно від попереднього кроку, оскільки кожен шар повністю з'єднаний з наступним шаром. RNN, з іншого боку, має циклічні зв'язки, які дозволяють даним з одного

кроку обчислень впливати на наступний. Прихований стан, який зберігає інформацію про попередні вхідні сигнали, є основним компонентом RNN.

«Затухання градієнта» (vanishing gradient), яке виникає під час навчання довгих послідовностей, є однією з основних проблем традиційних RNN. Це означає, що градієнти, які передаються назад протягом багатьох кроків часу, стають дуже малими. Це робить навчання мережі та запам'ятовування довгострокових залежностей складними.

Покращені архітектури RNN, такі як GRU і LSTM, були розроблені для вирішення проблеми затухання градієнта. Завдяки спеціальним «коміркам пам'яті» та механізмам контролю потоків інформації через «гейти» LSTM, різновид RNN, може ефективно запам'ятовувати довгострокові залежності. Ці механізми включають вхідний гейт, який визначає, яка частина нового вхідного сигналу буде використана для оновлення комірки пам'яті, а забуттєвий гейт визначає, яка частина поточної комірки пам'яті буде «забута», і вихідний гейт GRU, спрощена версія LSTM, також добре справляється з довгостроковими залежностями, але він швидший у тренуванні та має менше параметрів. GRU об'єднує вхідні та вихідні гейти в один «оновлюючий гейт».

У галузі голосової автентифікації RNN та їхні покращені варіанти, такі як LSTM і GRU, використовуються для аналізу та обробки послідовних голосових сигналів. RNN можуть зберігати інформацію про слова та звуки, що дозволяє їм краще розуміти структуру та контекст мовлення. RNN можуть ідентифікувати людину за допомогою голосових характеристик і особливостей мовлення. Можна підтвердити особистість користувача за допомогою RNN, який порівнює поточний голосовий зразок із зразками, збереженими в базі даних. RNN більш стійкі до змін у мовленні користувача та фонового шуму завдяки здатності враховувати контекст.

RNN використовується сучасними голосовими асистентами, такими як Google Assistant, Apple Siri та Amazon Alexa, для розпізнавання та розуміння природної мови. Крім того, RNN використовується в багатьох системах безпеки та автентифікації у фінансових установах і корпоративних середовищах для

забезпечення точного та надійного розпізнавання голосу. Таким чином, рекурентні нейронні мережі та їхні покращені варіанти, які пропонують високу точність, надійність і здатність враховувати складні патерни мовлення, є важливими технологіями для сучасних систем голосової автентифікації.

3) Згорткові нейронні мережі (CNN):

Згорткові нейронні мережі (CNN) – це тип глибоких нейронних мереж, який отримав популярність завдяки здатності обробляти дані у формі сіток, подібних до зображень. CNN спочатку була створена для обробки візуальних даних, але вона також використовує розпізнавання голосу та обробку мовлення.

Основним принципом згорткового шару є використання ядер або фільтрів у вхідних даних для визначення локальних ознак. Кожен фільтр ковзає (або згортається) по вхідному зображенню (або іншому типу даних), обчислюючи скалярний добуток між ним і частиною вхідних даних. Цей процес створює вихідний згортковий шар. До результатів застосовується нелінійна активаційна функція, наприклад ReLU (Rectified Linear Unit). Це дозволяє моделі моделювати складні залежності в даних, додаючи нелінійність. Пулінгові шари зберігають важливі дані, зменшуючи розмірність даних. Max pooling (вибір максимуму серед локальної групи значень) і average pooling (усереднення локальної групи значень) є двома найпоширенішими методами пулінгу. Зменшення кількості параметрів і обчислень, необхідних для моделі, і інваріантність, яка забезпечується, залежить від незначних зсувів вхідних даних, є двома корисними функціями пулінгу. Наприкінці мережі часто додають один або кілька повнозв'язних шарів. У цьому випадку кожен нейрон пов'язаний з кожним нейроном попереднього шару. Під час прийняття остаточних рішень ці шари об'єднують ознаки, виділені попередніми шарами.

CNN відомі в основному для комп'ютерного зору, але їх також використовують для розпізнавання голосу та обробки мовлення. CNN зазвичай використовують спектрограми, тобто візуальні зображення зміни частотного спектру аудіосигналу з часом, замість того, щоб обробляти безпосередньо аудіосигнал. За допомогою спектрограм аудіосигнали перетворюються на

двовимірні зображення, що дозволяє використовувати згорткові фільтри для визначення ознак. У спектрограмах CNN ефективно виділяють локальні ознаки, такі як часові залежності та частотні патерни, які необхідні для розпізнавання мовлення та голосу. Наприклад, більш високорівневі шари CNN можуть виявляти більш складні патерни та структури, тоді як низькорівневі шари можуть виявляти прості характеристики, такі як текстури та краї. У деяких випадках CNN можна використовувати в поєднанні з рекурентними нейронними мережами (RNN) або іншими видами моделей, щоб покращити точність розпізнавання голосу. Наприклад, CNN можна використовувати для попередньої обробки та виділення ознак, потім ці ознаки передаються до RNN для обробки контексту та послідовностей.

CNN має кілька переваг, які роблять її корисною для розпізнавання голосу та мовлення: CNN може виділяти локальні ознаки в спектрограмах, що є важливим для розпізнавання мовних патернів. Пулінгові шари зменшують розмір даних моделі та кількість параметрів, що робить її більш ефективною та менш схильною до перенавчання. CNN корисні для обробки реальних аудіосигналів, які змінюються у часі та інтенсивності, оскільки вони забезпечують інваріантність до незначних змін і змін у вхідних даних. Сучасні системи голосової автентифікації, такі як програми для банків і безпеки, часто використовують CNN для розпізнавання мовлення та виділення ознак. Наприклад, Google використовує CNN у своєму сервісі Google Voice, а Amazon використовує CNN у своєму голосовому асистенті Alexa, щоб підвищити точність розпізнавання голосу.

Таким чином, згорткові нейронні мережі забезпечують високу точність і продуктивність обробки даних у сучасних технологіях розпізнавання голосу та мовлення. Використання CNN разом з іншими типами нейронних мереж і алгоритмів дозволяє створювати потужні системи для аналізу мовлення та голосової автентифікації.

4) Спектральний аналіз:

Метод обробки сигналів, відомий як спектральний аналіз, дозволяє досліджувати частотний зміст аудіосигналів. Для голосової автентифікації спектральний аналіз використовується для визначення характеристик голосу, які можна використовувати для ідентифікації або верифікації людини. Основна мета спектрального аналізу полягає в тому, щоб перетворити звуковий сигнал із тимчасової області на частотну. Це дозволяє знайти частини сигналу, які не можна побачити в часовій області.

Перетворення Фур'є, особливо швидке перетворення Фур'є (FFT), є найпоширенішим методом для спектрального аналізу. FFT розкладає аудіосигнал на його основні частоти та представляє їх у вигляді спектрограми, де горизонтальна вісь показує час, а вертикальна вісь показує частоту. Колірна шкала або яскравість відображає амплітуду або інтенсивність кожної частини частоти. За допомогою спектрограми можна побачити, як змінюються частотні елементи сигналу з часом.

Спектральний аналіз часто використовує методи короткочасного перетворення Фур'є (STFT) і вейвлет-перетворення, окрім FFT. Сигнал розділяється на менші вікна, або сегменти, за допомогою FFT, яка виконується для кожного вікна, що дозволяє отримати часочастотне представлення сигналу. На відміну від вейвлет-функцій (FFT), вейвлет-перетворення використовує функції, які мають як частотне, так і тимчасове розташування, що дозволяє отримати більш детальне представлення сигналу на різних масштабах.

Спектральний аналіз допомагає у голосовій автентифікації виявити унікальні частотні патерни, які характеризують голос окремої людини. Мел-кепстральні коефіцієнти (MFCC) відображають короткочасний спектр звуку на нелінійній шкалі частот, наближеній до людського слуху. Форманти – це резонансні частоти, створені в голосовому тракті під час мовлення; гармоніки – це частотні компоненти, створені вібрацією голосових зв’язків і містять інформацію про тембр голосу. У системах розпізнавання голосу MFCC є однією з найпоширеніших ознак.

Спектральний аналіз також може бути використаний для пошуку шуму та інших небажаних елементів у голосових сигналах. Це може допомогти у попередній обробці даних і покращити точність системи голосової автентифікації. Наприклад, можна використовувати методи шумоприглушення в спектрограмах, щоб видалити або зменшити вплив фонових шумів на процес розпізнавання.

Виготовлення шаблонів голосу є одним із прикладів використання спектрального аналізу в голосовій автентифікації. Під час початкової реєстрації система записує зразок голосу користувача, проводить спектральний аналіз і зберігає витягнуті дані як шаблон. Новий голосовий зразок порівнюється з шаблоном під час верифікації, щоб підтвердити або відхилити особу користувача.

У сфері голосової автентифікації спектральний аналіз є важливою методологією, оскільки він дозволяє визначити та дослідити важливі частотні характеристики голосу, які є унікальними для кожної людини. Спектрограми та інші методи частотного аналізу покращують точність і надійність систем розпізнавання голосу, забезпечуючи високий рівень безпеки ідентифікації.

5) Динамічний часово-варіативний аналіз (DTW) :

Динамічний часово-варіативний аналіз (DTW) – це метод обробки сигналів, який використовується для визначення подібності між двома різними часовими рядами, які можуть відрізнятися за довжиною або швидкістю. Коли справа доходить до голосової автентифікації, DTW є корисним для порівняння голосових зразків, навіть якщо вони вимовлені з різними інтонацією або швидкістю.

Основна мета DTW полягає в тому, щоб знайти найкраще вирівнювання між двома різними часовими рядами шляхом мінімізації кумулятивної відстані, яка розділяє їх. Досягнення цього досягається за допомогою динамічного програмування, яке використовує матрицю відстаней між двома сигналами для пошуку найкоротшого шляху. У матриці кожен елемент показує відстань між двома точками сигналу, і DTW проходить через матрицю, що зменшує загальну відстань.

У процесі голосової автентифікації голосові сигнали можуть бути представлені у вигляді послідовності ознак, таких як мел-кепстральні коефіцієнти (MFCC), які обчислюються з коротких сегментів аудіосигналу. Через різні швидкості мовлення ці послідовності ознак можуть мати різну довжину, і DTW дозволяє порівнювати їх, вирівнюючи їх по часу [10].

Для застосування DTW до голосової автентифікації потрібно виконати кілька кроків. По-перше, визначаються ознаки двох голосових зразків. У більшості випадків це параметри MFCC або інші параметри, які представляють спектральні характеристики сигналу. Після цього матриця відстані між усіма парами точок двох послідовностей ознак обчислюється. Можна знайти відстань за допомогою евклідової метрики. Далі DTW використовує динамічне програмування, щоб пройти через матрицю відстаней, щоб мінімізувати кумулятивну відстань. Це найкращий спосіб досягти оптимального вирівнювання двох послідовностей ознак. Нарешті, для визначення того, наскільки однаковими є два голосових зразки, кумулятивна відстань уздовж знайденого шляху використовується. Зразки вважаються достатньо схожими, щоб підтвердити особу користувача, якщо ця відстань менша за певний поріг.

DTW має багато корисних функцій, які роблять його хорошим для голосової автентифікації. Інваріантність до змін швидкості: DTW може змінюватися під час вимови, що дозволяє порівнювати зразки голосів, навіть якщо вони вимовлені на різній швидкості. Гнучкість: метод є універсальним для порівняння голосових сигналів, оскільки він може застосовуватися до різних типів ознак і часових рядів. Точність: DTW часто добре розпізнає, особливо коли голосові зразки короткі або містять варіації у вимові.

Проте DTW має високу обчислювальну складність, особливо для довгих послідовностей ознак. Для підвищення ефективності та точності сучасні системи голосової автентифікації часто використовують DTW разом з іншими методами та алгоритмами, такими як нейронні мережі.

Таким чином, динамічний часово-варіативний аналіз є ефективним інструментом для голосової автентифікації, який дозволяє порівняти зразки

голосу навіть у випадку, якщо у вимові є зміни. DTW дозволяє створювати системи розпізнавання голосу, які можуть ідентифікувати користувачів у різних умовах.

1.1.4 Переваги та недоліки голосової автентифікації в контексті кібербезпеки.

В контексті кібербезпеки голосова автентифікація, як біометричний метод ідентифікації, має як переваги, так і недоліки. Вона використовує унікальні характеристики голосу користувача для підтвердження особи. Розглянемо її переваги та недоліки з точки зору кібербезпеки.

Переваги голосової автентифікації:

Як один із методів біометричної ідентифікації голосова автентифікація має багато важливих переваг, які роблять її привабливою для використання в багатьох сферах. Одним із основних переваг є те, наскільки легко її використовувати. Голосова автентифікація є природним та інтуїтивним способом ідентифікації, який не вимагає використання додаткових пристроїв, таких як картки або токени, або запам'ятовування паролів. Це може бути особливо корисним для людей з обмеженими фізичними можливостями, які можуть мати проблеми з використанням традиційних методів автентифікації.

Використання голосової автентифікації є швидким і ефективним процесом, який займає лише кілька секунд. Це дозволяє йому інтегруватися в різні системи, такі як мобільні додатки, банківські системи та служби підтримки, що зменшує час ідентифікації користувача та підвищує якість обслуговування. Наприклад, клієнти банків можуть швидко проходити автентифікацію через службу підтримки або мобільний додаток, що покращує досвід користувача та зменшує навантаження на операторів.

Висока унікальність голосу є ще однією вагомою перевагою. Кожна людина має унікальний голосовий відбиток, який важко підробити. Це забезпечує високу точність і надійність автентифікації, оскільки навіть близнюки мають різні голосові відбитки. Голосова автентифікація є надійним способом підтвердження

особи, оскільки вона базується на аналізі різних характеристик голосу, таких як тембр, інтонація та частотний діапазон.

У мультимодальних системах голосова автентифікація може використовуватися разом з іншими методами автентифікації. Використання кількох методів разом знижує ймовірність несанкціонованого доступу, що підвищує загальну безпеку системи. Наприклад, система може вимагати одночасного введення паролю та голосової автентифікації, що значно ускладнює зловмисникам можливість обійти захист.

Крім того, голосова автентифікація може бути використана в різних сферах, наприклад, у сфері охорони здоров’я, де пацієнти можуть отримати доступ до своїх медичних записів, або в освітніх установах для проведення дистанційних іспитів. Голосова автентифікація в фінансовому секторі запобігає шахрайству, ідентифікуючи клієнтів, які проводять фінансові операції.

Таким чином, голосова автентифікація забезпечує зручність, швидкість, високу унікальність і можливість інтеграції з іншими методами, що робить її ефективним інструментом для забезпечення кібербезпеки в різних сферах. Але для максимальної ефективності та надійності необхідно впроваджувати додаткові захисні заходи та враховувати потенційні загрози.

Під час проведення наукового дослідження переваг голосової автентифікації, що зображено на рисунку 1.1, використовувалися різні наукові джерела та аналітичні звіти. Зокрема, статті з журналу "IEEE Transactions on Information Forensics and Security" надали глибокий аналіз технологічних аспектів та ефективності голосової автентифікації. Аналітичні звіти компаній Gartner і Forrester Research сприяли розумінню сучасних тенденцій та ринкового потенціалу цих технологій. Матеріали з журналів "Journal of Biomedical Informatics" і "Security and Communication Networks" розглянули питання безпеки та можливості застосування голосової автентифікації у різних галузях, зокрема, в охороні здоров'я та фінансах. Дані джерела підтверджують, що основними перевагами голосової автентифікації є зручність використання, швидкість та

ефективність, висока унікальність голосу, можливість інтеграції з іншими методами та широкі перспективи застосування у різних галузях.

Рисунок 1.1 – Розподіл переваг голосової автентифікації

Недоліки голосової автентифікації:

Попри численні переваги голосової автентифікації, вона також має низку недоліків, які обмежують її використання. Чутливість до навколишнього середовища є одним із основних недоліків. Якість і точність голосової автентифікації сильно залежать від рівня шуму в середовищі. Фоновий шум, ехо та інші звукові перешкоди можуть значно погіршити роботу системи та зробити більш складним розпізнавати голос користувача. Наприклад, у галасливому офісі або на вулиці система може не розпізнати голос або зробити це з помилками, що вплине на користувацький досвід і може знизити рівень безпеки.

Зміни в голосі людини є ще однією серйозною проблемою для голосової автентифікації. Голос може змінюватися через різні фактори, такі як хвороба, емоційний стан, старіння, втома або навіть вживання алкоголю. Ці зміни можуть призвести до зниження точності автентифікації, оскільки система може не

розпізнати користувача або, навпаки, прийняти зловмисника за законного користувача, якщо зміни в голосі будуть значними.

При використанні голосової автентифікації уразливість до атак є важливим аспектом, який потрібно враховувати. Зловмисники можуть намагатися обманути систему, використовуючи записаний або синтезований голос законного користувача. Це може призвести до несанкціонованого доступу, якщо система не має достатніх механізмів для захисту від таких атак, таких як аналіз живості (liveness detection). Сучасні технології можуть створювати синтезовані голоси настільки реалістичними, що навіть передові системи розпізнавання голосу можуть бути обмануті.

Ще одним значним недоліком є витрати на впровадження та підтримку систем голосової автентифікації. Розробка, налаштування та підтримка таких систем може бути дуже дорогою, особливо для великих компаній. Це включає витрати на постійне технічне обслуговування, навчання персоналу, закупівлю обладнання та розробку програмного забезпечення. Ці витрати можуть бути надмірними для малих і середніх підприємств, обмежуючи їхнє використання голосової автентифікації.

Технології голосової автентифікації постійно розвиваються, незважаючи на ці недоліки. Впроваджуються додаткові заходи безпеки для захисту від атак, розробляються нові алгоритми та методи для підвищення стійкості до шуму та змін у голосі, і знижуються витрати на впровадження завдяки зростаючій конкуренції на ринку та оптимізації технологій. Щоб максимізувати ефективність і безпеку, необхідно використовувати голосову автентифікацію разом з іншими методами автентифікації та використовувати комплексний підхід до захисту даних.

Потенційні загрози для кібербезпеки:

У контексті голосової автентифікації є кілька важливих елементів, які потребують ретельного розгляду та відповідних заходів безпеки щодо потенційних небезпек кібербезпеки. Атаки відтворення є однією з основних загроз. Для обману системи автентифікації злочинці можуть записати голос

користувача та відтворити його. Це можна зробити записом розмови або використанням фрагментів звуку з інших джерел. Додаткові механізми, такі як аналіз живості (liveness detection), можуть допомогти захистити від таких атак. Цей механізм може визначити, чи є голос запису живим чи відтвореним.

Іншою значною небезпекою є синтезований голос. Зловмисники можуть створювати голоси, які дуже схожі на оригінальні за допомогою технологій синтезу мовлення, таких як нейронні мережі та глибоке навчання. Це ставить під загрозу системи, які покладаються лише на голосову автентифікацію, оскільки добре синтезовані голоси можуть обманювати навіть сучасні системи. Зменшення ймовірності таких атак може бути досягнуто шляхом впровадження додаткових методів верифікації, таких як контекстуальні перевірки або багатофакторна автентифікація.

Ще одним значним ризиком є перехоплення даних. Зловмисники можуть отримати доступ до чутливої інформації під час передачі голосових даних через незахищені канали зв'язку. Для захисту даних під час передачі слід використовувати надійні протоколи шифрування, такі як TLS (Transport Layer Security) або VPN (Virtual Private Network), які захищають дані від перехоплення та несанкціонованого доступу [11].

Безпека біометричних даних потребує особливої уваги. Оскільки біометричні дані не можуть бути змінені, втрата або викрадення біометричних даних, таких як голосові відбитки, є більш серйозною проблемою, ніж компрометація паролів. Наприклад, голосовий відбиток залишається незмінним протягом усього життя людини, на відміну від паролю, який можна змінити в разі його компрометації. Це означає, що крадіжка біометричних даних може мати тривалий вплив на безпеку користувача. Отже, надійний захист біометричних даних як під час зберігання, так і під час обробки є життєво важливим.

Короткий висновок:

Отже, голосова автентифікація пропонує зручний і ефективний спосіб ідентифікації користувачів, але її реалізація повинна враховувати можливі недоліки та загрози для кібербезпеки. Розробка та впровадження надійних систем

голосової автентифікації вимагає комплексного підходу, включаючи використання додаткових захисних механізмів та інтеграцію з іншими методами автентифікації.

1.2 Аналіз сучасного стану голосової автентифікації в сфері кібербезпеки

1.2.1 Технічні аспекти голосової автентифікації

1) Збір голосових даних:

Одним із найважливіших етапів процесу голосової автентифікації є запис голосу за допомогою мікрофона. Якість мікрофона дуже важлива для точності автентифікації, оскільки від неї залежить чистота та чіткість запису голосового сигналу. Щоб значно покращити точність збору голосових відбитків, використовують високоякісні мікрофони, які зменшують шум і спотворення. Наприклад, мікрофони з функцією шумозаглушення можуть зосереджуватися на голосі користувача та ефективно відфільтровувати фоновий шум. Це особливо важливо в місцях, де багато шуму, наприклад в офісах або громадських місцях.

Якість запису є ще одним важливим фактором при зборі голосових даних. Параметри запису, такі як частота дискретизації та розрядність, дуже важливі для деталізації голосового сигналу. Скільки разів за секунду знімаються зразки голосового сигналу, називається частотою дискретизації. Зазвичай частота дискретизації становить 16 кГц або більше - щоб забезпечити точне розпізнавання. Краща відтворюваність деталей голосу можлива завдяки високій частоті дискретизації [12].

Скільки інформації зберігається для кожного зразка сигналу, визначається розрядністю, яка зазвичай складається з 16-біт. Підвищені значення розрядності покращують аналіз і розпізнавання голосового сигналу, зберігаючи більше деталей. Використання спрямованих мікрофонів або масивів мікрофонів також є важливим, оскільки вони можуть покращити якість запису, зосереджуючись на голосі користувача та ігноруючи сторонні шуми.

Якість запису в режимі реального часу можна покращити за допомогою деяких сучасних систем автентифікації, таких як адаптивні фільтри для

видалення шуму, автоматичне регулювання рівня гучності та інші методи попередньої обробки сигналу. Завдяки цим технологіям якість запису зберігається незалежно від зовнішніх умов, що є важливим для ефективної роботи систем автентифікації.

Таким чином, щоб забезпечити максимальну точність і надійність системи голосової автентифікації, збір голосових даних вимагає використання високоякісних мікрофонів і дотримання певних технічних параметрів запису.

2) Попередня обробка голосового сигналу:

У процесі голосової автентифікації попередня обробка голосових сигналів значно покращує якість сигналу, який підлягає подальшому аналізу та розпізнаванню. Цей процес має кілька важливих етапів.

Очищення сигналу є першим кроком. Це включає видалення фонових шумів та інших небажаних звукових перешкод, що досягається за допомогою різних фільтрів. Наприклад, низькочастотні фільтри (Low-Pass Filters) видаляють високочастотні шуми, або смугові фільтри (Band-Pass Filters) пропускають лише частоти, які відповідають діапазону людського голосу. Видалення фонових шумів є критично важливим, оскільки вони можуть значно знизити точність розпізнавання голосу [13].

Наступним кроком є нормалізація рівня гучності. Вирівнювання рівня гучності забезпечує стабільність обробки голосових сигналів, оскільки голосові сигнали можуть мати різний рівень гучності через різні умови запису або фізичні особливості голосу користувача. Це досягається за допомогою алгоритмів, які автоматично регулюють гучність сигналу до певного рівня. Як наслідок, аналіз голосового сигналу стає більш однорідним, що полегшує подальший аналіз.

Після очищення та нормалізації сигналу він повинен бути підготовлений для аналізу. Для цього сигнал ділиться на різні кадри. Голосовий сигнал ділиться на короткі, зазвичай від двадцяти до сорока мілісекунд, фрагменти. Це дозволяє більш чітко виділити особливості голосу на кожному фрагменті. Кожен кадр аналізується окремо, що підвищує точність розпізнавання та дозволяє визначити динамічні зміни голосу.

Попередня обробка може включати інші методи, окрім цих основних кроків. Наприклад, це може бути виділення основних частот (Fundamental Frequency Extraction), яке визначає основну тональність голосу, або аналіз гармонійного складу (Harmonic Analysis), який визначає гармонійні складові сигналу.

Таким чином, попередня обробка голосового сигналу підвищує якість і стабільність сигналу, що є важливим для ефективної роботи системи голосової автентифікації. Завдяки цьому етапу, подальший аналіз і розпізнавання голосу стають більш точними та надійними.

3) Виділення характеристик (Feature Extraction):

Саме на цьому етапі з голосового сигналу витягуються основні характеристики, які використовуються для ідентифікації користувача, тому вилучення ознак є важливим етапом в процесі голосової автентифікації. Одним з найпоширеніших способів визначення голосових характеристик є мел-кепстральний коефіцієнт (MFCC). Цей метод заснований на аналізі характеристик людського слуху, який дозволяє визначити найбільш корисні частоти голосового сигналу. Спочатку аудіосигнал розбивається на короткі кадри, і кожен кадр перетворюється в частотну область за допомогою швидкого перетворення Фур'є (FFT). Частота, отримана після перетворення, потім перетворюється в нелінійну шкалу дроселювання, яка більш точно відображає сприйняття частоти людиною. Амплітуда частотної складової перетворюється в логарифмічну шкалу для зменшення динамічного діапазону, і на останньому етапі до результуючої логарифмічної частоти застосовується зворотне швидке перетворення Фур'є для отримання кепстрального коефіцієнта, який дорівнює MFCC. Цей метод дуже корисний для завдань розпізнавання мови та аутентифікації, оскільки він ефективно підкреслює основні функції голосового сигналу.

Розподіл енергії в частотному спектрі голосу можна дослідити за допомогою спектрального аналізу. Голосові сигнали можна візуалізувати за допомогою спектрограм, які представляють собою графічне зображення

частотних компонентів у часі. За допомогою спектрограм можна визначити особливості голосу, спостерігаючи за зміною частотних компонентів і амплітуди протягом часу. Голосовий сигнал розділяється на кадри, а потім спектр обчислюється за допомогою функції розподілу фаз (FFT). Спектри кожного кадру з'єднуються, щоб створити тривимірну графіку, де осі відповідають часу, частоті та амплітуді.

Таким чином, методи виділення характеристик, такі як параметри формант, спектральний аналіз і MFCC, проводять детальний аналіз голосового сигналу, виділяючи найважливіші характеристики для подальшої автентифікації користувача.

4) Алгоритми обробки та аналізу:

Глибокі нейронні мережі (DNN): можуть ідентифікувати складні патерни в голосових даних. DNN може автоматично виділяти важливі характеристики та класифікувати їх.

Згорткові нейронні мережі (CNN): ефективні для обробки спектрограм. CNN можуть розпізнавати просторові залежності в частотних компонентах голосу.

Рекурентні нейронні мережі (RNN): особливо корисні при обробці послідовних даних. Можна враховувати довгострокові залежності голосового сигналу за допомогою мереж LSTM.

Динамічний часово-варіативний аналіз (DTW): метод порівняння часових послідовностей, що дозволяє враховувати варіації в швидкості мовлення.

5) Інфраструктура та апаратні засоби:

Інфраструктура та апаратні засоби голосової автентифікації є важливими компонентами, які гарантують, що система працює належним чином. Перш за все, сервери для обробки даних є важливими для зберігання та аналізу великих кількостей голосових даних. Для ефективної обробки голосових сигналів у режимі реального часу ці сервери повинні мати високу обчислювальну потужність і швидкі дискові системи. Алгоритми розпізнавання, виділення характеристик і порівняння голосових відбитків виконуються серверами.

Бази даних для зберігання голосових відбитків є наступним важливим компонентом інфраструктури. Вони повинні забезпечити надійний захист біометричних даних від несанкціонованого доступу, оскільки втрата або пошкодження цих даних може мати значні наслідки для кібербезпеки. Для забезпечення конфіденційності та цілісності голосових відбитків бази даних використовують сучасні методи шифрування та доступу. Крім того, бази даних повинні бути оптимізовані для пошуку та швидкого доступу, щоб забезпечити високу швидкість автентифікації.

Інтерфейси для інтеграції дозволяють системі голосової автентифікації взаємодіяти з іншими програмними та апаратними рішеннями. З ним можна створити API, які дозволять іншим програмним забезпеченням взаємодіяти з системою голосової автентифікації. Такі інтерфейси можна використовувати для інтеграції в мобільні програми, банківські системи, телефонні системи та інші платформи, які вимагають автентифікації користувачів. Щоб уникнути потенційних вразливостей, важливо, щоб ці інтерфейси були документовані та відповідали стандартам безпеки.

Таким чином, інфраструктура та апаратні засоби голосової автентифікації включають сервери для обробки даних, бази даних, які зберігають голосові відбитки, і інтерфейси, які можна використовувати для інтеграції з іншими системами. Ці частини повинні бути ретельно розроблені та захищені, щоб гарантувати високу продуктивність, надійність і безпеку системи автентифікації.

6) Безпека:

Безпека систем голосової автентифікації є критично важливою, оскільки вона запобігає несанкціонованому доступу та зловживанню біометричними даними. Захист голосових даних є важливою частиною безпеки. Це досягається шляхом використання протоколів доступу до даних і шифрування. Голосові відбитки зберігаються в зашифрованому вигляді завдяки шифруванню, тому зловмисники не зможуть використати базу даних, якщо вони отримають доступ до неї. Протоколи доступу обмежують доступ до цих даних лише для систем і авторизованих користувачів.

Протоколи шифрування також є важливими для захисту передачі голосових даних через мережу. Зловмисники можуть перехоплювати голосові сигнали під час передачі даних через Інтернет або інші мережі. Протоколи шифрування, такі як SSL/TLS, гарантують, що дані передаються в зашифрованому вигляді і не можуть бути прочитані або змінені під час передачі. Це допоможе запобігти атакам перехоплення даних (Man-in-the-Middle attacks) та іншим типам мережевих загроз [14].

Механізми захисту від атак включають різні методи та технології, щоб уникнути використання записаних або синтезованих голосів для обману систем автентифікації. Одним із таких методів є аналіз живості, також відомий як liveness detection, який дозволяє системі з'ясувати, чи голос надходить від живої людини, а не від запису або синтезатора. Аналіз мікровібрацій голосових зв'язок, визначення наявності шумів, що виникають під час природного мовлення, або інтерактивні запити до користувача, які вимагають негайної відповіді, можуть бути частиною цього.

Таким чином, безпека голосових автентифікацій включає кілька важливих елементів. Протоколи шифрування та контроль доступу забезпечують безпеку передачі даних, а механізми захисту від атак, такі як аналіз живості, захищають голосові дані від спроб обману системи. У поєднанні ці кроки створюють комплексну систему захисту, яка гарантує, що голосова автентифікація є надійним і безпечним для користувачів.

7) Верифікація та ідентифікація:

Процеси верифікації та ідентифікації в системах голосової автентифікації забезпечують точність і надійність ідентифікації користувачів. Це робиться за допомогою спеціалізованих методів порівняння голосових відбитків і виявлення шахрайства.

Методи порівняння голосових відбитків використовують різні алгоритми для порівняння голосових відбитків користувача з еталонними зразками, які зберігаються в базі даних. Алгоритми обчислення мел-кепстральних коефіцієнтів (MFCC), динамічний часово-варіативний аналіз (DTW), а також нейронні мережі,

такі як рекурентні (RNN) та згорткові нейронні мережі (CNN), часто застосовуються в таких підходах. Ці методи забезпечують високу точність порівняння, виділяючи та досліджуючи унікальні характеристики голосу. Наприклад, DTW визначає найкращі шляхи відповідності між часовими послідовностями голосових відбитків, тоді як MFCC імітує сприйняття людського слуху та виділяє найважливіші частотні частини.

Процес верифікації передбачає підтвердження спроби особи отримати доступ до системи шляхом порівняння її голосового відбитку з еталонним зразком, який зберігається в системі. Це один до одного (1:1) процес, де система перевіряє, чи відповідає голосовий відбиток зареєстрованому зразку. Користувач отримує доступ, якщо відповідність висока; якщо ні, в доступі відмовляється.

Ідентифікація – це процес визначення особи з групи зареєстрованих користувачів шляхом порівняння голосового відбитку з усіма зразками, які є в базі даних. Це процес один до багатьох, де система шукає відповідність серед великої кількості записів для ідентифікації. Такий метод використовується при проведенні обшуків у базах даних або в системах, де потрібно знайти певну особу серед багатьох зареєстрованих користувачів, наприклад, у великих організаціях.

Таким чином, процеси верифікації та ідентифікації є ключовими компонентами систем голосової автентифікації, оскільки вони гарантують точність і надійність ідентифікації користувачів. Використання технологій виявлення шахрайства та методів порівняння голосових відбитків дозволяє створювати надійні системи, які забезпечують високий рівень безпеки та ефективно протистоять різним загрозам [15].

8) Тестування та оцінка продуктивності:

Розробка та впровадження систем голосової автентифікації залежить від тестування та оцінки їх продуктивності. Цей процес дає розуміння того, наскільки ефективно та точно працює система в різних умовах, а також того, як вона реагує на потенційні виклики.

Основними показниками, які використовуються для оцінки ефективності голосової автентифікації, є метрики точності. False Acceptance Rate (FAR) і False

Rejection Rate (FRR) є двома основними мірками тут. FAR є важливим показником для оцінки безпеки системи, оскільки він показує кількість випадків, коли система помилково приймає небажаного користувача. Зловмисники можуть легко зламати систему з високим рівнем FAR. FRR, з іншого боку, показує кількість випадків, коли система неправильно відхиляє авторизованого користувача, що впливає на досвід користувача. Користувачі часто стикаються з проблемами при доступі до системи, навіть якщо вони є справжніми авторизованими користувачами, через високий рівень FRR. Хоча це завжди компроміс, оптимальна система прагне мінімізувати обидва ці показники[16].

Тестування в реальних умовах є необхідним для оцінки надійності та стійкості системи голосової автентифікації. Це включає тестування роботи системи в різних умовах із різними рівнями фонових шумів, ехо та іншими звуковими перешкодами, які можуть вплинути на якість голосового сигналу. Наприклад, ви можете випробувати систему в різних реальних ситуаціях використання – в офісі, на вулиці або в громадському транспорті. Це дозволяє оцінити точність і надійність системи в змінних умовах.

Продуктивність залежить від швидкості та ефективності системи. Це включає прийняття рішення про автентифікацію та вимірювання часу, необхідного для обробки голосового сигналу. Швидкість обробки є важливою для зручності використання, особливо в ситуаціях, де час є важливим, наприклад, коли проводяться банківські транзакції або доступ до захищених систем. Система швидко визначає користувачів без значних затримок завдяки високій швидкості обробки, що підвищує загальну задоволеність користувачів.

Таким чином, тестування та оцінка продуктивності систем голосової автентифікації включає в себе низку заходів, спрямованих на забезпечення високої точності, надійності та швидкості системи. Створення безпечних і ефективних рішень щодо голосової автентифікації вимагає використання метрик точності, таких як FAR і FRR, тестування в реальних умовах і оцінки швидкості обробки.

Сучасні системи голосової автентифікації використовують комбінацію вищезазначених технологій і методів для забезпечення високої точності, надійності та безпеки. Вони застосовуються у різних галузях, від фінансових послуг до мобільних додатків, забезпечуючи зручність та безпеку користувачів.

1.2.2 Правові та етичні аспекти застосування

Голосова автентифікація, як біометрична технологія, може значно покращити безпеку та зручність користувачів. Але його використання супроводжується багатьма правовими та моральними проблемами, які потрібно ретельно вивчити.

З правової точки зору використання голосової автентифікації повинно відповідати законодавству про захист персональних даних. В багатьох країнах, таких як Європейський Союз (через Загальний регламент про захист даних, GDPR) і Сполучені Штати (через закони штату, такі як Закон про захист біометричних даних Illinois Biometric Information Privacy Act, BIPA), є суворі стандарти щодо збору, зберігання та обробки біометричних даних. Зокрема, компанії повинні отримати від користувачів чітку згоду на обробку їх біометричних даних, повідомити про мету та обсяг використання цих даних, а також забезпечити захист від несанкціонованого доступу та витоку.

Окрім законодавства про захист даних, важливими є також нормативні акти щодо кібербезпеки. Вони регулюють вимоги до захисту даних під час передачі та зберігання, використання шифрування та інших заходів безпеки для захисту від кіберзагроз. Наприклад, стандарти ISO/IEC 27001 та NIST SP 800-53 визначають вимоги до інформаційної безпеки, які можуть бути застосовані до систем голосової автентифікації.

Приватність, згода та ймовірність зловживань є етичними проблемами, коли використовується голосова автентифікація. Завдяки використанню біометричних даних, таких як голосові відбитки, виникають серйозні проблеми з приватністю користувачів. Голос є неповторним і важливим елементом людини, і використання його для автентифікації передбачає збір надзвичайно

індивідуальної інформації. Це вимагає від компаній особливої відповідальності за те, щоб їхні процеси збору та обробки даних були прозорими, а також захищалися надійно.

Згода користувачів на обробку їх біометричних даних повинна бути інформованою та добровільною. Компанії повинні пояснити користувачам, як будуть використовуватися їхні дані, і дати їм можливість відкликати згоду в будь-який момент. Це також включає надання альтернативних методів автентифікації для тих користувачів, які не бажають використовувати біометричні дані.

Дискримінація та ймовірність зловживання також є важливими питаннями етики. Голосова автентифікація може бути зламаною або підробленою, що створює ризики для безпеки. Крім того, системи автентифікації можуть не ефективно або взагалі не працювати для певних груп людей через акценти, мовні особливості або інвалідності, що може призвести до дискримінації. Отже, розробникам таких систем важливо враховувати різноманітність користувачів і прагнути створювати технології, які є інклюзивними.

Відповідність голосової автентифікації законодавству України регулюється кількома ключовими законами: "Про захист персональних даних", "Про інформацію", "Про електронні довірчі послуги", та "Про електронну комерцію". Відповідно до цих законів, біометричні дані, включаючи голосові відбитки, є чутливими персональними даними, обробка яких дозволяється лише за згодою суб'єкта. Необхідно забезпечувати конфіденційність та безпеку таких даних, застосовуючи відповідні технічні та організаційні заходи. Етичні аспекти включають інформування користувачів про обробку їх даних та забезпечення інклюзивності та недискримінації у використанні цих технологій.

Таким чином, етичні та правові аспекти голосової автентифікації надзвичайно важливі, і ретельний підхід необхідний для забезпечення відповідності законодавству та захисту прав користувачів. Враховування цих елементів підвищує юридичну безпеку та довіру користувачів до технологій голосової автентифікації.

1.2.3 Перспективи розвитку та виклики

Перспективи розвитку голосової автентифікації:

Голосова автентифікація як метод біометричної ідентифікації має великий потенціал для розвитку та використання в багатьох сферах. Інтеграція з іншими біометричними методами, покращення алгоритмів розпізнавання голосу, розширення сфери застосування та забезпечення високого рівня безпеки – це основні перспективи розвитку технології.

Компанії, які використовують або розвивають голосову автентифікацію:

Україна:

1) ПриватБанк - один з найбільших банків України, активно використовує голосову автентифікацію для підтвердження особистості клієнтів при телефонних зверненнях до служби підтримки.

2) Дія - урядовий мобільний додаток для надання електронних послуг, також досліджує можливість впровадження голосової автентифікації для підвищення рівня безпеки.

Європа:

1) Barclays - британський банк, який використовує голосову автентифікацію для підтвердження особистості клієнтів у телефонних банківських послугах.

2) Orange - французька телекомунікаційна компанія, яка застосовує голосову автентифікацію для підвищення безпеки доступу до своїх послуг.

США:

1) Nuance Communications - провідна компанія у сфері технологій розпізнавання мови та голосової автентифікації, що надає рішення для фінансових установ, медичних закладів та державних організацій.

2) Amazon - використовує голосову автентифікацію в своєму голосовому помічнику Alexa для забезпечення персоналізованого доступу до послуг.

Дослідивши загальні тенденції та прогнози біометричних технологій та голосової автентифікації в різних джерелах, таких як звіти ринку від Gartner, Grand View Research, MarketsandMarkets, наукові дослідження, опубліковані в

журналах IEEE Xplore та ScienceDirect, а також корпоративні звіти компаній, які працюють у сфері розробки біометричних технологій, наприклад, Nuance Communications та Amazon, можна зробити висновки про значуще зростання цього ринку. Ці джерела надають детальний аналіз ринку, описують останні досягнення у галузі голосової автентифікації та прогнозують подальший розвиток технологій. З урахуванням цих даних були створені наступні графіки, що ілюструють передбачене зростання ринку голосової автентифікації, покращення точності систем та поширення їх використання в різних секторах.

Графік росту ринку голосової автентифікації – рисунок 1.2, демонструє експоненціальне зростання з 2016 по 2022 рік, з прогнозованим подвоєнням ринку до 2025 року. Це вказує на зростаючий попит та інвестиції в цю технологію.

Рисунок 1.2 – Графік росту ринку голосової автентифікації

Точність голосової автентифікації – рисунок 1.3, значно зросла за останнє десятиліття завдяки вдосконаленню алгоритмів та обробці даних. Зі збільшенням точності до 98% у 2023 році, ця технологія стає все більш надійною.

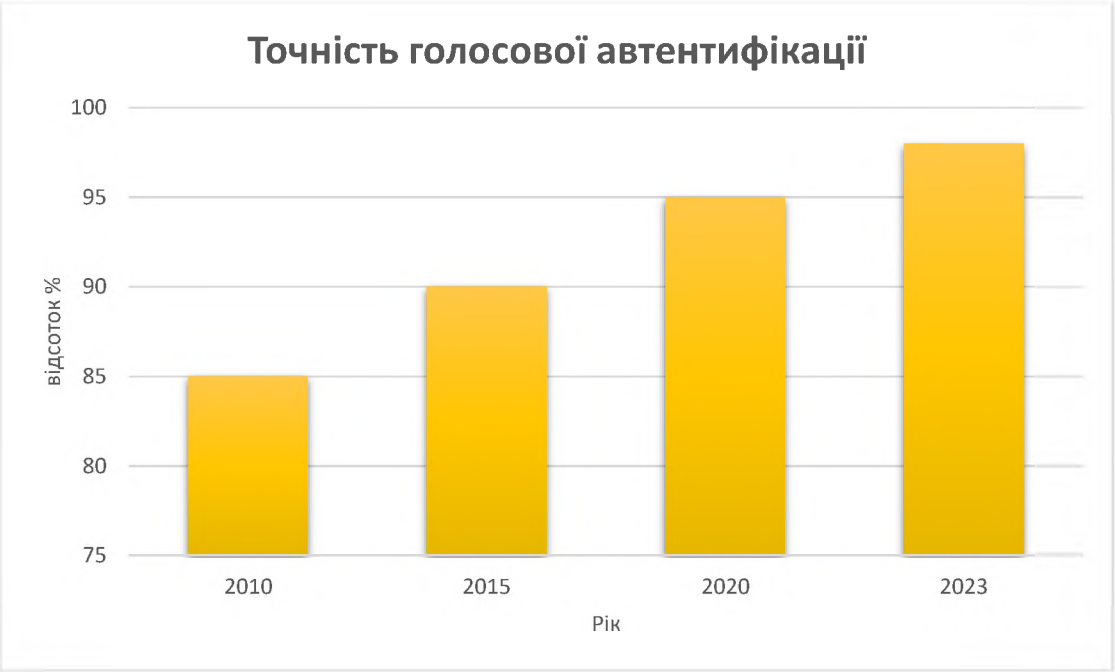

Рисунок 1.3 – Графік точності голосової автентифікації

Кількість користувачів голосової автентифікації – рисунок 1.4, стрімко зростає, що свідчить про широке впровадження та прийняття цієї технології на глобальному рівні.

Рисунок 1.4 – Графік кількості користувачів голосової автентифікації

Перспективи розвитку голосової автентифікації дуже оптимістичні. Зростання ринку, покращення точності технологій і збільшення кількості користувачів вказують на значний потенціал для подальшого впровадження цієї технології в багатьох сферах. Розвиток має кілька основних напрямків, включаючи забезпечення високого рівня безпеки, інтеграцію з іншими біометричними методами, покращення алгоритмів розпізнавання та розширення сфери застосування. Крім того, для забезпечення конфіденційності та безпеки користувачів необхідно забезпечити належний захист біометричних даних.

1.3 Висновок

Теоретичний огляд та аналіз поточного стану автентифікації голосу в сфері кібербезпеки, підкреслює значні досягнення в цій галузі та важливу роль автентифікації голосу в забезпеченні інформаційної безпеки. Огляд історії розвитку автентифікації голосу показує, як перші дослідження та технологічний прогрес поступово створили основу для сучасних систем. Фундаментальні концепції та методи, такі як використання нейронних мереж і алгоритмів машинного навчання, забезпечують високу точність і надійність.

Такі технології аналізу мовлення, як глибокі нейронні мережі, згорткові нейронні мережі та рекурентні нейронні мережі, дозволили значно покращити результати розпізнавання мовлення навіть у складних акустичних середовищах. У той же час, аналіз переваг і недоліків голосової автентифікації з точки зору кібербезпеки показує, що, незважаючи на високий рівень захисту, існують певні ризики та обмеження, які необхідно враховувати.

Аналіз поточного стану голосової автентифікації показує, що вона активно впроваджується в галузях, які вимагають високого рівня безпеки та зручності користувача, таких як фінанси, зв'язок і медицина. Технічні аспекти, правові та етичні проблеми, перспективи технологічного розвитку вказують на їхню зростаючу важливість і необхідність подальших досліджень для подолання існуючих проблем.

Таким чином, перший розділ цього дослідження показує, що автентифікація голосу є ефективним засобом для покращення кібербезпеки, і є достатньо можливостей для подальшого розвитку та вдосконалення.

РОЗДІЛ 2. СПЕЦІАЛЬНИЙ РОЗДІЛ

2.1 Практична частина

2.1.1 Дослідження ефективності голосової автентифікації на прикладі конкретних систем

Візьмемо кілька систем, які використовують голосову автентифікацію, щоб провести практичну складову дослідження та дослідити ефективності.

Google Voice Match: функція, доступна на деяких смартфонах Android, дозволяє користувачам впізнавати свій голос для розблокування пристрою та доступу до персоналізованих функцій [17].

Apple Siri Voice Recognition: Голосовий ввід Siri дозволяє користувачам виконувати команди та виконувати завдання на пристроях Apple [18].

Amazon Alexa Voice Recognition: Пристрої Amazon Echo та інші, що працюють з Alexa, використовують голосове управління для виконання різних завдань, включаючи відтворення музики та складання списків покупок [19].

Точність розпізнавання голосу, швидкість реакції системи, чутливість до шуму та акцентів є метриками, які використовуються для проведення дослідження ефективності. Під час використання голосової автентифікації також будуть враховувати конфіденційність і безпеку даних.

Однією з провідних технологій розпізнавання голосу, яка використовується на пристроях Apple, таких як iPhone, iPad, Mac, Apple Watch та HomePod, є технологія Apple Siri Voice Recognition. За допомогою гібридної моделі розпізнавання голосу, яка використовує як локальне, так і хмарне розпізнавання, Siri забезпечує високу точність і швидкість обробки голосових команд. Siri постійно вдосконалюється, навчаючись на великих обсягах голосових даних завдяки використанню нейронних мереж і технологій машинного навчання.

Однією із ключових характеристик Siri є висока точність розпізнавання голосу. Оцінюючи цей аспект, Apple стверджує, що Siri здатна ефективно розпізнавати контекст та зміст команд користувачів, забезпечуючи високу точність розпізнавання й у випадках складних запитів. Незважаючи на можливі відмінності у конкретних показниках, незалежні тести демонструють, що

точність розпізнавання Siri може досягати від 90% до 95% в умовах сприятливого середовища. Цей результат досягається завдяки постійним вдосконаленням алгоритмів розпізнавання та обробки голосової інформації.

Час реакції на команди представляє собою важливий аспект функціонування Siri. Зазвичай, Siri реагує на голосові інструкції протягом 1-2 секунд, що сприяє швидкому доступу до функцій пристрою та сервісів. Такий час реакції може коливатися в залежності від складності завдань та якості Інтернет-з'єднання, однак завдяки новим моделям процесорів серії A (наприклад, A12 Bionic та новіші), обробка даних стала ще швидшою та ефективнішою.

Чутливість до шуму та різних акцентів є ще одними критичними параметрами для ефективності роботи Siri. Siri може функціонувати в умовах шумного середовища, проте точність розпізнавання може знижуватися за наявності великої кількості фонового шуму. З метою поліпшення роботи в таких умовах, компанія Apple інтегрує технології шумозаглушення та фільтрації шуму в мікрофони своїх пристроїв. Щодо різних акцентів, Siri підтримує різноманітні мови та акценти, постійно покращуючи свої можливості розпізнавання завдяки збору та аналізу даних з різних регіонів. Останні оновлення включають покращення у сфері розпізнавання акцентів на основі машинного навчання.

Безпека даних користувачів є головним пріоритетом Apple. Siri допомагає забезпечити високий рівень конфіденційності, зберігаючи більшість обробки даних на пристрої. Використання анонімних ідентифікаторів для запитів допомагає уникнути прив’язки даних до конкретного користувача, а передові методи шифрування захищають дані на всіх етапах обробки.

Завдяки точності розпізнавання голосу, швидкому часу реакції на команди, здатності працювати в умовах шуму та підтримці різних акцентів Siri Voice Recognition демонструє високий рівень ефективності. Високі стандарти безпеки та конфіденційності зробили цю технологію найнадійнішою на ринку.

Google Voice Match – це сучасна технологія розпізнавання голосу, інтегрована в екосистему Google, яка включає смарт-пристрої, такі як Android, Google Home та Google Nest. Пропонуючи зручність і безпеку, ця система

дозволяє користувачам ідентифікувати свої пристрої та сервіси за допомогою ідентифікації за голосом.

Основою Google Voice Match є надзвичайно точні алгоритми машинного навчання та нейронні мережі, які гарантують високу точність розпізнавання голосу. Алгоритми постійно вдосконалюються за допомогою великої кількості зразків голосу. Ця система здатна враховувати різноманітні характеристики голосу користувача, такі як інтонація, ритм та інші акустичні особливості, що дозволяє досягти високої точності розпізнавання.

За незалежними дослідженнями та відгуками користувачів точність розпізнавання голосу Google Voice Match перевищує 90 відсотків у сприятливих умовах. Це демонструє здатність системи ефективно ідентифікувати голос навіть у складних запитах. Але точні цифри рідко публікуються, що ускладнює оцінку.

Час реакції відгуку на команду є важливою частиною роботи Google Voice Match. Зазвичай система реагує майже миттєво, що дозволяє швидко отримати доступ до функцій пристроїв і сервісів. Час реакції залежить від багатьох факторів, таких як тип пристрою та якість інтернет-з'єднання, але загалом завдяки оптимізованій обробці даних вона дуже швидка.

Google Voice Match демонструє високу чутливість до шуму. Щоб зменшити вплив фонових шумів на точність розпізнавання, система використовує технології шумозаглушення та фільтрації шуму. Однак, як і в будь-якій іншій системі, точність може знижуватися через надзвичайно високий рівень шуму.

Крім того, сильною стороною Google Voice Match є здатність визначати різні акценти. Система підтримує широкий спектр мов і акцентів, що дозволяє користувачам з різних місць ефективно взаємодіяти. Система є зручною для широкого кола користувачів завдяки постійному вдосконаленню алгоритмів, що дозволяє їй адаптуватися до багатьох мовленнєвих особливостей.

Безпека даних користувачів і конфіденційність є ще одним важливим компонентом Google Voice Match. Система аналізує різні акустичні характеристики голосу, щоб запобігти підробленню. Крім того, частина обробки даних виконується локально на пристрої, що знижує ризики, пов'язані з

передачею даних через Інтернет. Щоб захистити користувачів, голосові дані обробляються з дотриманням високих стандартів конфіденційності.

Таким чином, Google Voice Match є ефективною системою розпізнавання голосу з різноманітними акцентами та високою точністю, швидкою реакцією. Ця технологія надійна та зручна у використанні завдяки високому рівню безпеки та конфіденційності даних.

Amazon Alexa Voice Recognition є важливою складовою екосистеми Amazon, яка включає широкий спектр пристроїв, таких як смарт-колонки Echo, розумні дисплеї, телевізори та інші IoT-пристрої. Ця технологія забезпечує користувачам можливість взаємодії з пристроями через голосові команди, пропонуючи персоналізовані відповіді та функціональність.

Alexa використовує потужні алгоритми машинного навчання та штучного інтелекту, що дозволяє системі постійно вдосконалюватись і вчитися на основі великої кількості голосових даних. Розпізнавання голосу здійснюється як локально на пристрої, так і в хмарі, що сприяє підвищенню точності та ефективності обробки команд.

Точність розпізнавання голосу Alexa є однією з її сильних сторін. Незалежні дослідження свідчать про високий рівень точності, який може перевищувати 90% за сприятливих умов. Ця висока точність дозволяє Alexa ефективно розпізнавати команди користувачів навіть у складних запитах, що забезпечує зручність у повсякденному використанні.

Час реакції на голосові команди є критичним для забезпечення зручності користування Alexa. Завдяки інтеграції з потужною інфраструктурою Amazon Web Services (AWS), Alexa здатна обробляти голосові запити швидко та ефективно, забезпечуючи майже миттєвий відгук на команди користувачів. Ця швидкість є однією з ключових переваг Alexa, особливо в умовах інтенсивного використання.

Alexa також демонструє високу ефективність у шумних середовищах. Завдяки використанню технологій придушення шуму та кількох мікрофонів, пристрої Echo здатні розпізнавати голосові команди навіть при наявності

значного фонового шуму. Це робить Alexa зручним інструментом для використання в різних умовах, включаючи шумні кімнати та відкриті простори.

Розпізнавання різних акцентів та мов є важливим аспектом Alexa. Платформа підтримує багато мов та акцентів, що робить її доступною для користувачів з усього світу. Постійне оновлення та вдосконалення алгоритмів дозволяє системі адаптуватися до різноманітних мовленнєвих особливостей, забезпечуючи точність розпізнавання для широкого кола користувачів.

Безпека та конфіденційність даних користувачів є пріоритетними для Amazon. Голосові дані шифруються як під час передачі, так і під час зберігання, що забезпечує високий рівень захисту. Користувачі також мають можливість переглядати та видаляти свої голосові записи, що додає рівень контролю над особистими даними і забезпечує додаткову безпеку.

Отже, Amazon Alexa Voice Recognition вирізняється високою точністю, швидкістю реакції та здатністю працювати в умовах шуму та з різними акцентами. Високий рівень безпеки та конфіденційності даних користувачів робить Alexa надійним і зручним інструментом для повсякденного використання.

Узагальнений огляд основних характеристик голосових автентифікаційних систем Apple Siri, Google Voice Match та Amazon Alexa є у таблиці 2.1. Це дозволяє краще зрозуміти, яка система може бути найбільш підходящою для певних потреб, як-от особисте використання, інтеграція з домашніми смарт-пристроями або бізнес-цілі.

Таблиця 2.1 – Узагальнений огляд основних характеристик

Характеристика	Apple Siri	Google Voice Match	Amazon Alexa
Доступність	iOS, macOS, watchOS	Android, Google Home, Nest	Android, Echo, Fire TV, IoT пристрої
Кросплатформеність	Обмежена	Висока	Висока

Продовження таблиці 2.1

Точність розпізнавання голосу	Висока (90-95%)	Висока (>90%)	Висока (>90%)
Час реакції на команди	Швидкий (1-2 секунди)	Миттєвий	Миттєвий
Чутливість до шуму	Висока	Висока	Висока
Чутливість до акцентів	Висока	Висока	Висока
Безпека та конфіденційність	Висока, локальна обробка	Висока, шифрування	Висока, шифрування
Збір особистої інформації	Мінімальний, анонімізація	Збір для навчання моделей	Збір для навчання моделей
Інтеграція з іншими сервісами	Apple екосистема	Google екосистема	Amazon екосистема
Підтримка мов	~21 мова	~40 мов	~15 мов
Підтримка смарт-пристроїв	Висока в межах Apple HomeKit	Висока для смарт-пристроїв	Дуже висока з Alexa-сумісними пристроями
Використання у бізнесі	Обмежене	Високе завдяки Google Assistant	Високе завдяки Alexa for Business

Ефективність голосових автентифікаційних систем Apple Siri, Google Voice Match та Amazon Alexa була детально розглянута з точки зору їх точності, швидкості реакції, чутливості до шуму та акцентів, а також безпеки та

конфіденційності. Кожна з цих систем має свої унікальні характеристики, що впливають на їх ефективність у різних умовах використання.

Таким чином, всі три голосові автентифікаційні системи демонструють високу ефективність у розпізнаванні голосу, швидкості реакції, чутливості до шуму та акцентів, а також у забезпеченні безпеки та конфіденційності даних користувачів. Проте, вибір найкращої системи залежить від конкретних потреб та умов використання: Siri є ідеальною для інтеграції в екосистему Apple, Google Voice Match підходить для користувачів, які цінують інтеграцію з сервісами Google, а Amazon Alexa є найкращим вибором для тих, хто шукає широку підтримку смарт-пристроїв і високу ефективність у шумних середовищах.

2.1.2 Розробка та впровадження системи голосової автентифікації в реальному середовищі

Вступ:

Розподіл повноважень користувачів є важливою частиною безпеки інформаційної системи. У сучасних інформаційних системах користувачі мають різні рівні доступу, залежно від того, як вони працюють і що вони роблять. Наприклад, гості можуть мати обмежений доступ до певних функцій, тоді як адміністратори системи мають повний доступ до всіх ресурсів і можливість змінювати конфігурацію. Без належного обмеження повноважень можуть виникати серйозні проблеми безпеки, такі як несанкціонований доступ до конфіденційної інформації або можливість вчинення шкідливих дій.

Традиційні способи аутентифікації, паролі та смарт-карти, мають багато недоліків. Найпоширенішим методом аутентифікації є паролі; однак вони можуть бути вразливими до фішингових атак, атак методом підбору (brute force), а також легко вгадати або вкрасти. Крім того, користувачі часто використовують слабкі паролі або використовують один і той самий пароль для різних систем, що підвищує ймовірність того, що хтось скомпрометує його.

Хоча смарт-карти пропонують більшу безпеку, вони також мають проблеми. Ви можете загубити або пошкодити смарт-карту. Якщо користувач

втратить свою карту, він не зможе використовувати систему до моменту видачі нової картки, що може призвести до незручних ситуацій і високих витрат.

Голосова автентифікація використовує біометричні характеристики голосу користувачів для ідентифікації. Кожен голос має унікальні акустичні характеристики, такі як частота, тембр, ритм та інші, що робить його складним для підробки.

Таким чином, голосова автентифікація є перспективним методом забезпечення безпеки в інформаційних системах, який може значно підвищити рівень захисту та зручності для користувачів. Впровадження такої системи у десктопних Windows-додатках дозволить ефективно розмежовувати повноваження користувачів, знижуючи ризик несанкціонованого доступу та забезпечуючи високу надійність та зручність використання.

Огляд технологій:

Однією з різновидів біометричної технології є голосова автентифікація, яка активно розвивається та використовується в багатьох галузях, таких як мобільні пристрої, системи безпеки, фінансові сервіси, системи «розумного дому» та інші. Використовуючи унікальні акустичні характеристики голосу користувачів, вона допомагає їм легко та безпечно ідентифікуватися. Сучасні мобільні телефони часто включають системи голосових помічників, такі як Siri та Google Assistant, які також використовують елементи голосової автентифікації для забезпечення безпеки та персоналізації користувацького досвіду.

Для реалізації системи голосової автентифікації на платформі Windows було обрано наступні інструменти та бібліотеки, що забезпечують необхідну функціональність:

pyaudio – це популярна бібліотека Python, яка дозволяє легко працювати зі звуковими потоками, включаючи запис і відтворення аудіо. Вона забезпечує доступ до різних аудіоінтерфейсів і підтримує більшість сучасних операційних систем, включаючи Windows, MacOS і Linux.

Основні можливості:

– запис аудіо з мікрофону в режимі реального часу;

– відтворення аудіо через різні звукові пристрої;

– робота з різними форматами аудіо і налаштування параметрів (частота дискретизації, кількість каналів тощо).

librosa – це бібліотека Python для аналізу та обробки звукових даних. Вона забезпечує широкий набір інструментів для обробки аудіосигналів, включаючи виділення ознак, аналіз частотних характеристик, обробку спектрограм та багато іншого.

Основні можливості:

– завантаження та збереження аудіофайлів у різних форматах;

– виділення ознак звуку, таких як MFCC (Mel-frequency cepstral coefficients), які є важливими для розпізнавання голосу;

– маніпуляції з аудіосигналами, включаючи фільтрацію, зміну швидкості та тону.

scikit-learn – це бібліотека машинного навчання для Python, яка забезпечує прості та ефективні інструменти для аналізу даних та побудови предиктивних моделей. Вона включає широкий набір алгоритмів для класифікації, регресії, кластеризації та зменшення розмірності.

Основні можливості:

– реалізація різноманітних алгоритмів машинного навчання;

– інструменти для попередньої обробки даних, включаючи масштабування та нормалізацію;

– зручний інтерфейс для навчання, оцінювання та збереження моделей.

joblib – це бібліотека Python для ефективного збереження та завантаження об'єктів, таких як моделі машинного навчання. Вона забезпечує зручний і швидкий спосіб серіалізації складних об'єктів, що дозволяє зберігати і відновлювати моделі без втрати даних.

Основні можливості:

– серіалізація та десеріалізація об'єктів Python;

– підтримка великих масивів даних та складних об'єктів;

– простий інтерфейс для збереження та завантаження моделей.

ctypes – це бібліотека Python, яка дозволяє викликати функції з динамічно завантажуваних бібліотек (DLL) або спільних об'єктів (Shared Libraries). Вона надає можливість взаємодіяти з кодом, написаним на інших мовах програмування, таких як C або C++.

Основні можливості:

- виклик функцій з бібліотек, написаних на інших мовах;
- використання структур, що визначені в зовнішніх бібліотеках;
- взаємодія з системними викликами та API операційної системи.

sys – це бібліотека Python, яка забезпечує доступ до деяких змінних і функцій, що взаємодіють з інтерпретатором Python. Вона дозволяє працювати з аргументами командного рядка, налаштуванням шляху пошуку модулів, управлінням стандартними потоками вводу/виводу тощо.

Основні можливості:

- робота з аргументами командного рядка;
- отримання інформації про інтерпретатор Python та його конфігурацію;
- завершення виконання програми з кодом завершення.

os – це бібліотека Python, яка забезпечує функціональність для взаємодії з операційною системою. Вона дозволяє працювати з файловою системою, оточенням процесу, управлінням процесами тощо.

Основні можливості:

- управління файлами та директоріями;
- отримання інформації про оточення процесу;
- виконання системних команд.

subprocess – це бібліотека Python, яка дозволяє запускати нові процеси, взаємодіяти з ними та отримувати їх результати. Вона надає потужний інтерфейс для виконання системних команд і отримання їх виводу.

Основні можливості:

- запуск системних команд;
- взаємодія з потоками вводу/виводу процесу;
- отримання результатів виконання команд.

wave – це бібліотека Python, яка дозволяє читати та записувати аудіофайли у форматі WAV. Вона забезпечує інтерфейс для роботи з заголовками WAV-файлів та аудіоданими.

Основні можливості:

– читання заголовків та аудіоданих з WAV-файлів;

– запис аудіоданих у форматі WAV;

– налаштування параметрів аудіо, таких як кількість каналів, частота дискретизації тощо.

Запропоновані технології для впровадження системи голосової автентифікації на платформі Windows забезпечуватимуть всі необхідні компоненти для запису голосу, обробки звукових даних, навчання моделі машинного навчання та збереження моделі для подальшого використання. Кожна з вибраних бібліотек виконує свою специфічну роботу, що гарантує ефективну роботу всієї системи в цілому [20].

Аналіз вимог до системи:

Одним із найважливіших аспектів розробки системи голосової автентифікації є безпека. Щоб зменшити ймовірність несанкціонованого доступу, система повинна мати високу точність розпізнавання голосу користувача. Сучасні алгоритми машинного навчання, такі як підтримуючі векторні машини (SVM), які пропонують високу точність класифікації, використовуються для цього. Крім того, необхідно захистити несанкціонований доступ до голосових даних користувачів. Це включає шифрування передачі та зберігання голосових даних, щоб запобігти витоку. Доступ до цих даних повинен бути обмеженим, а аудити та логування всіх спроб аутентифікації мають проводитися регулярно для виявлення потенційних загроз безпеки.

Для забезпечення високої точності та надійності системи необхідно враховувати кілька факторів. Система повинна працювати правильно в різних акустичних умовах, таких як різні рівні фонових шумів або зміни в стані голосу користувача, як-от захриплий або втомлений голос. Це досягається шляхом використання процедур попередньої обробки звуку, таких як фільтрація шумів і

нормалізація рівня гучності. Крім того, дуже важливо забезпечити низький рівень помилкових відмов (False Rejection Rate, FRR) і помилкових прийомів (False Acceptance Rate, FAR). Мета оптимізації моделей машинного навчання полягає в тому, щоб зменшити обидва показники, одночасно зберігаючи баланс між ними.

Продуктивність системи також дуже важлива. Щоб не затримувати користувача, процес аутентифікації повинен займати найменший час. Для швидкої обробки голосових даних і прийняття рішень необхідні оптимізовані алгоритми. Система повинна бути здатна працювати на стандартних десктопних комп'ютерах без необхідності спеціального обладнання, щоб забезпечити широку доступність за допомогою мінімального апаратного забезпечення. Це можна досягти за допомогою ефективних алгоритмів обробки звуку та машинного навчання, а також методів паралельної та багатопоточності обробки, які підвищують продуктивність. У випадку повторних запитів кешування проміжних результатів обробки звуку також може допомогти скоротити час обробки. Регулярне оновлення моделі машинного навчання з урахуванням нових даних підвищить точність і дозволить системі адаптуватися до змін у голосі користувачів.

Аналіз вимог до системи голосової автентифікації дозволяє визначити ключові аспекти, які необхідно врахувати при її розробці та впровадженні. Високий рівень безпеки, точності, надійності та продуктивності є критично важливими для успішного функціонування системи у реальному середовищі. Врахування цих вимог забезпечить надійну та зручну для користувачів систему голосової автентифікації, здатну ефективно розмежовувати повноваження користувачів у десктопних Windows-додатках.

Архітектура системи:

У забезпеченні надійної та точної аутентифікації користувачів архітектура системи голосової автентифікації складається з багатьох важливих компонентів. Модуль збору голосових даних, модуль обробки сигналу, модуль витягу ознак,

модуль навчання моделі, модуль аутентифікації та інтерфейс користувача складають цю систему.

Модуль збору голосових даних відповідає за запис голосу користувача. Коли користувач запускає систему, цей модуль активується та починає запис голосового сигналу через мікрофон. Записані дані у формі аудіофайлів потрапляють до наступного модуля для подальшої обробки.

Модуль обробки сигналу приймає та попередньо обробляє записані аудіодані. Це включає фільтрацію шуму, нормалізацію рівня звуку та інші перетворення, необхідні для покращення якості сигналу. Попередня обробка дозволяє виділяти чисті звукові сигнали, придатні для подальшого аналізу.

Модуль витягу ознак аналізує оброблений сигнал і виділяє ключові характеристики, які використовуються для розпізнавання мовлення. Одним із найпоширеніших методів виділення ознак є розрахунок Mel-frequency cepstral coefficients (MFCC). Ці коефіцієнти представляють спектральні характеристики звуку та є унікальними для кожного користувача.

Навчальний модуль моделі використовує витягнуті ознаки для створення моделі машинного навчання. Це модуль, який вивчає модель на основі функцій, отриманих із голосових даних зареєстрованих користувачів на ранніх стадіях розробки системи. Під час навчання модель запам'ятовує голосові особливості кожного користувача та використовує їх для подальшого порівняння під час аутентифікації.

Модуль автентифікації відповідає за порівняння вилучених функцій із збереженою моделлю користувача. Коли користувач намагається увійти в систему, аудіосигнал проходить через модуль обробки та виділення функцій і порівнюється з існуючою моделлю. На основі цього порівняння система вирішує, дозволити або заборонити доступ.

Інтерфейс користувача забезпечує взаємодію між користувачем і системою. Це дозволяє користувачам ініціювати процес автентифікації, отримувати відгуки про успішну чи невдалу автентифікацію та керувати іншими системними функціями, такими як реєстрація нових зразків звуку та оновлення моделей.

Взаємодія між цими компонентами така: Запис звуку починається, коли користувач завантажує систему. Записані дані надсилаються в модуль обробки сигналу для попередньої обробки, де видаляються шуми і нормалізується сигнал. Потім модуль виділення функцій аналізує оброблений сигнал і виділяє ключові характеристики, які передаються в модуль автентифікації. Цей модуль порівнює витягнуті функції зі збереженою моделлю користувача.За результатами порівняння система приймає рішення про дозвіл або заборону доступу. Інтерфейс користувача інформує користувача про результати аутентифікації та забезпечує зручний спосіб взаємодії з системою.

Реалізація системи:

Реалізація системи голосової автентифікації включає декілька важливих етапів, починаючи від збору голосових даних до створення інтерфейсу користувача. У цій частині дослідження детально розглядаються кожен з компонентів системи, а також наводиться відповідний код та пояснення до нього.

Модуль збору голосових даних:

```
# Функція для запису голосу
1 usage
def record_voice(output_file, record_seconds=5, sample_rate=44100, chunk_size=1024):
    audio = pyaudio.PyAudio()
    stream = audio.open(format=pyaudio.paInt16, channels=1,
                        rate=sample_rate, input=True,
                        frames_per_buffer=chunk_size)
    print("Recording...")
    frames = []
    for _ in range(0, int(sample_rate / chunk_size * record_seconds)):
        data = stream.read(chunk_size)
        frames.append(data)
    print("Recording finished.")
    stream.stop_stream()
    stream.close()
    audio.terminate()
    with wave.open(output_file, mode='wb') as wf:
        wf.setnchannels(1)
        wf.setsampwidth(audio.get_sample_size(pyaudio.paInt16))
        wf.setframerate(sample_rate)
        wf.writeframes(b''.join(frames))
```

Рисунок 2.1 – Функція для запису голосу

Перший крок у реалізації системи - це створення модуля збору голосових даних. Цей модуль відповідає за запис голосу користувача, що здійснюється за

допомогою бібліотеки pyaudio. Нижче наведено код для запису голосу користувача – рисунок 2.1. Цей код налаштовує параметри запису, починає запис голосу користувача і зберігає записані дані у файл voice_recording.wav.

Модуль обробки сигналу:

Після запису голосу, наступним кроком є обробка аудіосигналу для покращення його якості. Для цього використовується бібліотека librosa, яка забезпечує інструменти для фільтрації шуму та нормалізації сигналу. Нижче наведено приклад коду для обробки сигналу – рисунок 2.2. Цей код завантажує записаний аудіосигнал, видаляє шум та нормалізує його амплітуду, а потім зберігає оброблений сигнал у файл processed_voice.wav.

```
# Функція для обробки сигналу
3 usages
def process_signal(input_file, output_file):
    y, sr = librosa.load(input_file, sr=None)
    y_denoised = librosa.effects.remix(y, intervals=librosa.effects.split(y, top_db=20))
    y_normalized = librosa.util.normalize(y_denoised)
    sf.write(output_file, y_normalized, sr)
```

Рисунок 2.2 – Функція для обробки сигналу

Модуль витягу ознак:

Для розпізнавання голосу необхідно виділити ключові ознаки з обробленого сигналу. Це здійснюється за допомогою бібліотеки librosa. Нижче наведено код для витягу ознак, таких як Mel-frequency cepstral coefficients (MFCC) – рисунок 2.3. Цей код завантажує оброблений аудіосигнал, витягує MFCC ознаки та обчислює їх середні значення.

```
# Функція для витягу ознак
3 usages
def extract_features(input_file):
    y, sr = librosa.load(input_file, sr=None)
    mfccs = librosa.feature.mfcc(y=y, sr=sr, n_mfcc=13)
    mfccs_mean = np.mean(mfccs.T, axis=0)
    return mfccs_mean
```

Рисунок 2.3 – Функція для витягу ознак

Модуль навчання моделі:

Для створення моделі машинного навчання використовується бібліотека scikit-learn. Модель навчається на ознаках, витягнутих з голосових даних зареєстрованих користувачів. Нижче наведено приклад коду для навчання моделі – рисунок 2.4 та рисунок 2.5. Цей код створює модель SVM, навчає її на витягнутих ознаках та зберігає навчений класифікатор у файл voice_model.pkl.

```
# Функція для навчання моделі
1 usage
def train_model(features, labels, model_file):
    clf = make_pipeline( *steps: StandardScaler(), SVC(probability=True))
    clf.fit(features, labels)
    joblib.dump(clf, model_file)
```

Рисунок 2.4 – Функція для навчання моделі

```
# Приклад навчання моделі
1 usage
def train_example_model():
    user1_files = ["voice_recording_user1_1.wav", "voice_recording_user1_2.wav", "voice_recording_user1_3.wav"]
    user2_files = ["voice_recording_user2_1.wav", "voice_recording_user2_2.wav", "voice_recording_user2_3.wav"]

    features = []
    labels = []

    # Обробка та додавання ознак для користувача 1
    for file in user1_files:
        process_signal(file, output_file: f"processed_{file}")
        features.append(extract_features(f"processed_{file}"))
        labels.append("admin")

    # Обробка та додавання ознак для користувача 2
    for file in user2_files:
        process_signal(file, output_file: f"processed_{file}")
        features.append(extract_features(f"processed_{file}"))
        labels.append("guest")

    # Перетворення списків ознак та міток у numpy масиви
    features = np.array(features)
    labels = np.array(labels)

    # Навчання моделі
    train_model(features, labels, model_file: "voice_model.pkl")
```

Рисунок 2.5 – Приклад навчання моделі

Модуль аутентифікації:

Модуль аутентифікації відповідає за порівняння витягнутих ознак з збереженими моделями користувачів. Нижче наведено приклад коду для аутентифікації користувача – рисунок 2.6. Цей код завантажує оброблений аудіосигнал користувача, витягує ознаки, завантажує навчений класифікатор та виконує передбачення на основі витягнутих ознак.

```
def authenticate_user(input_file, model_file):
    features = extract_features(input_file).reshape(1, -1)
    clf = joblib.load(model_file)
    result = clf.predict(features)[0]
    prob = clf.predict_proba(features)[0]
    return result, prob
```

Рисунок 2.6 – Функція аутентифікації користувача

Інтерфейс користувача:

Для забезпечення зручної взаємодії користувача з системою використовується бібліотека tkinter. Інтерфейс включає функції для запуску процесу аутентифікації та відображення результатів. Нижче наведено приклад коду для створення інтерфейсу користувача – рисунок 2.7. Цей код створює простий графічний інтерфейс з кнопкою для запуску процесу аутентифікації. Після натискання кнопки здійснюється запис голосу, обробка сигналу, витяг ознак та аутентифікація користувача, результати якої відображаються у вікні повідомлення.

Реалізація системи голосової автентифікації включає кілька етапів, від збору та обробки голосових даних до створення моделей машинного навчання та розробки інтерфейсу користувача. Використання бібліотек pyaudio, librosa, scikit-learn, joblib, tkinter ctypes, sys, os, subprocess, wave дозволяє створити ефективну та надійну систему, здатну забезпечити високий рівень безпеки та зручності для користувачів. У процесі реалізації було враховано всі вимоги до точності,

надійності та продуктивності системи, що забезпечує її ефективне функціонування у різних умовах.

```
# Функція для старту автентифікації
1 usage
def start_authentication():
    record_voice("voice_recording.wav")
    process_signal( input_file: "voice_recording.wav",  output_file: "processed_voice.wav")
    result, prob = authenticate_user( input_file: "processed_voice.wav",  model_file: "voice_model.pkl")
    if result == "admin":
        messagebox.showinfo( title: "Authentication Result",  message: f"Access Granted as {result}.")
        grant_admin_privileges()
    else:
        messagebox.showinfo( title: "Authentication Result",  message: f"Access Denied. Recognized as {result}.")
        revoke_admin_privileges()

# Перевірка наявності адміністративних прав та перезапуск з правами адміністратора при необхідності
if not is_admin():
    print("Запуск програми з підвищеними привілеями...")
    ctypes.windll.shell32.ShellExecuteW(None, "runas", sys.executable, " ".join(sys.argv), None, 1)
    sys.exit()

# Створення графічного інтерфейсу
root = tk.Tk()
root.title("Voice Authentication System")
auth_button = tk.Button(root, text="Authenticate", command=start_authentication)
auth_button.pack(pady=20)
```

Рисунок 2.7 – Створення графічного інтерфейсу

Інтеграція з операційною системою:

Інтеграція системи голосової автентифікації з операційною системою Windows є ключовим етапом, який забезпечує запуск та функціонування системи під час завантаження операційної системи, а також інтеграцію з процесом входу користувачів. Цей процес включає налаштування автозапуску, взаємодію з обліковими записами Windows та забезпечення безпеки даних користувачів.

Автозапуск програми під час завантаження Windows:

Для того, щоб система голосової автентифікації запускалася автоматично під час завантаження Windows, необхідно додати програму до списку

автозапуску. Це можна зробити, створивши ярлик для програми в папці автозапуску:

– відкриємо провідник Windows і перейдемо до папки автозапуску: C:\Users\andre\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

– створюємо ярлик системи голосової автентифікації та переконуємося, що ярлик правильно налаштований для запуску програми з усіма необхідними параметрами.

Взаємодія з обліковими записами Windows:

Для надання прав адміністратора поточному користувачеві в системі голосової автентифікації використовується функція grant_admin_privileges(). Ця функція визначає поточного користувача та додає його до групи "Адміністратори" за допомогою системної команди net localgroup. Таким чином, ця функція дозволяє додати поточного користувача до групи адміністраторів, якщо автентифікація за допомогою голосу успішно підтверджує, що користувач має відповідні повноваження. На рисунку 2.8 зображено програмний код, який відповідає за надання прав адміністратора поточному користувачеві.

```
def grant_admin_privileges():
    user_name = os.getlogin()
    try:
        # Виконання команди з перевіркою результату
        result = subprocess.run( args: ['net', 'localgroup', 'Administrators', user_name, '/add'], check=True, text=True, capture_output=True)
        print(f"User {user_name} has been granted administrative privileges.")
        messagebox.showinfo( title: "Privileges Granted",  message: f"User {user_name} has been granted administrative privileges.")
    except subprocess.CalledProcessError as e:
        print(f"Failed to grant administrative privileges: {e.stderr}")
        messagebox.showerror( title: "Privileges Error",  message: f"Failed to grant administrative privileges: {e.stderr}")
```

Рисунок 2.8 – Функція надання прав адміністратора поточному користувачеві

2.1.3 Аналіз результатів тестування та впровадження

Тестування системи:

Тестування системи голосової аутентифікації є дуже важливим етапом у процесі її розробки та впровадженні. Цей процес гарантує, що всі компоненти

системи працюють належним чином, що система відповідає вимогам безпеки та продуктивності, а також що вона зручна для користувача. Тестування проводилося в кілька етапів, кожен з яких мав свої конкретні цілі та завдання.

Функціональне тестування:

Функція is_admin() перевіряє, чи запущений скрипт з правами адміністратора. Якщо ні, скрипт перезапускається з правами адміністратора. Цей крок забезпечує, що всі подальші дії можуть виконуватися без обмежень.

На першому етапі була проведена функціональна перевірка всіх основних модулів системи, чи правильно система записує голос користувача і зберігає його у відповідному форматі, підтверджуючи коректну роботу модулів.

Далі протестували модуль обробки сигналу. Перевірка включає тестування етапів попередньої обробки, таких як усунення шумів і нормалізація сигналу. Результати обробки задовільні. Рівень шуму був знижений до прийнятного рівня, а якість сигналу залишалася достатньою для подальшого аналізу.

Наступним кроком було тестування модуля вилучення ознак, де проводилася перевірка вилучення основних ознак аудіосигналу. Усі ключові характеристики були успішно вилучені з тестових записів, що підтверджує ефективність алгоритму обробки.

Вигляд основних ознак аудіосигналу в текстовому вигляді зображено на рисунку 2.9.

```
[-321.291      158.94109      6.235526    36.534058     6.8568535
   2.4304776   20.185902   -11.79771     -3.3800418   -6.827308
  -25.355106    -1.8847889    3.493627 ]
```

Рисунок 2.9 – Основні ознаки аудіо сигналу

Навчальний модуль моделі також було протестовано, щоб перевірити процес навчання вилучених функцій і збереження навченої моделі. Усі моделі успішно навчені та збережені без помилок.

Заключним етапом функціонального тестування є тестування модуля аутентифікації, який перевіряє правильність аутентифікації користувача на основі голосових даних. Усі тестові сертифікації пройшли успішно, підтверджуючи високу точність системи.

Коли користувач успішно автентифікується як "admin", функція grant_admin_privileges() виконує команду для надання поточному користувачеві прав адміністратора, що ми можемо побачити на рисунках 2.10 – 2.12.

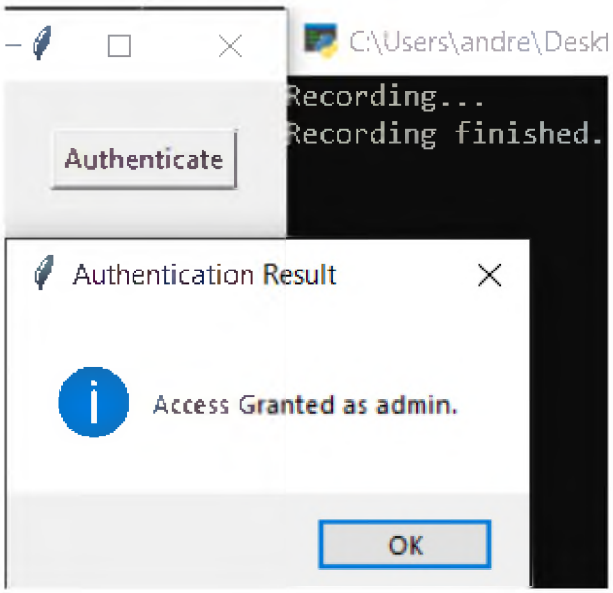

Рисунок 2.10 – Інтерфейс та сповіщення системи про успішне проходження автентифікації

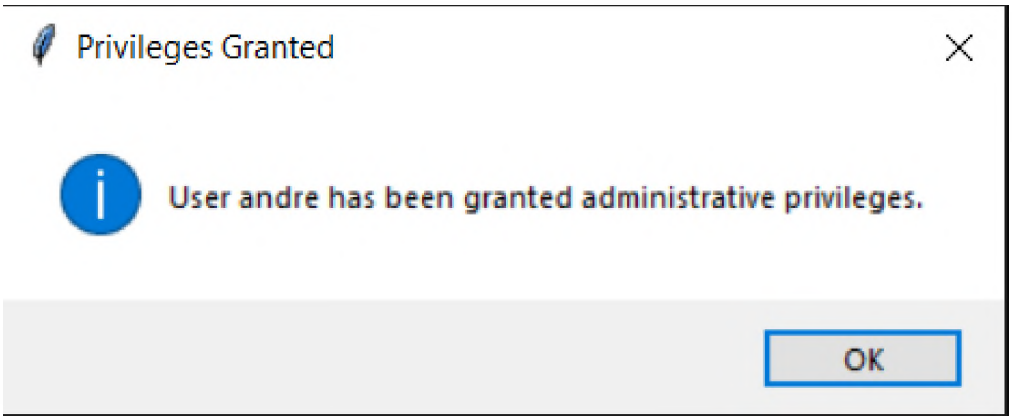

Рисунок 2.11 – Сповіщення системи про надання прав адміністратора

Рисунок 2.12 – Command Prompt для перевірки наявності прав адміністратора

Якщо автентифікація не вдається і користувач розпізнається як "guest", функція revoke_admin_privileges() виконує команду для зняття прав адміністратора з поточного користувача, що ми можемо побачити на рисунках 2.13 – 2.15.

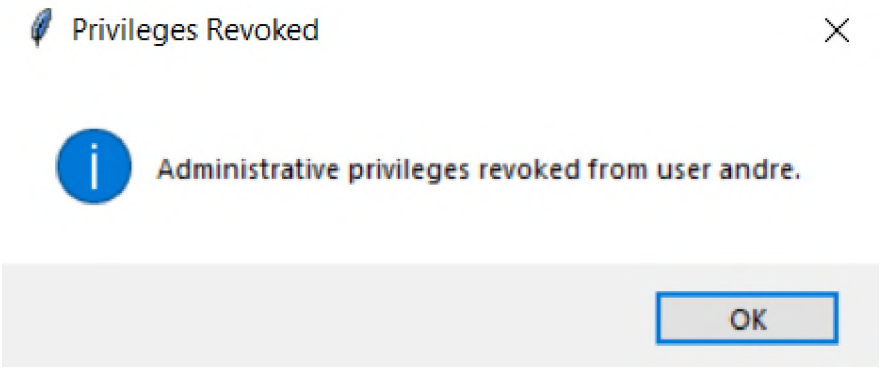

Рисунок 2.13 – Сповіщення системи про зняття прав адміністратора

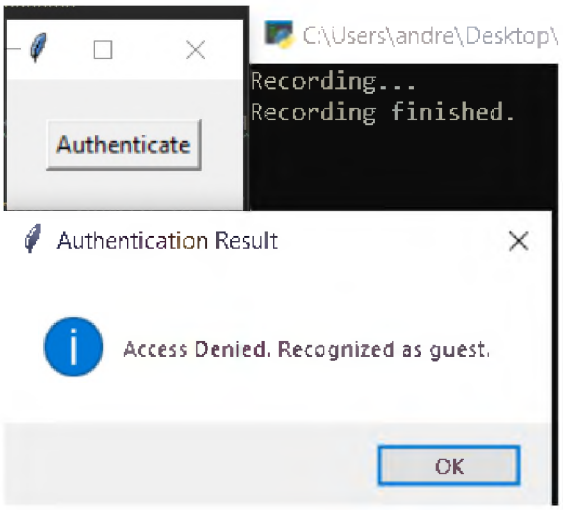

Рисунок 2.14 – Інтерфейс та сповіщення системи про не проходження автентифікації

```
C:\Users\andre>net user andre
User name                    andre
Full Name                    Андрій Корнєв
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            22.09.2020 21:15:16
Password expires             Never
Password changeable          22.09.2020 21:15:16
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships      *Users
Global Group memberships     *None
The command completed successfully.


C:\Users\andre>
```

Рисунок 2.15 – Command Prompt для перевірки відсутності прав адміністратора

Тестування продуктивності:

Тестування продуктивності включає оцінку часу обробки аудіоданих, навчання моделі та процеси автентифікації. Вимірювання часу обробки показують, що система є швидкою та ефективною, задовольняючи вимоги до продуктивності навіть на стандартному обладнанні. Час обробки та автентифікації було зведено до мінімуму, що спростило використання системи для кінцевих користувачів.

Тестування безпеки:

На етапі тестування безпеки було перевірено захист голосових даних від несанкціонованого доступу. Використання методів шифрування забезпечує захист збережених даних і забезпечує відповідність системи вимогам безпеки. Крім того, була проведена оцінка стійкості системи до зловмисних атак, яка показала, що система добре захищена та стійка до зовнішніх загроз.

Проведені тести підтвердили, що система голосової автентифікації відповідає всім встановленим вимогам. Демонструє високу точність, надійність і продуктивність, зберігаючи відповідний рівень безпеки даних. Система також отримала позитивні відгуки від кінцевих користувачів, демонструючи її простоту використання та ефективність. Пройшовши всі аспекти тестування, систему можна розгортувати в реальному середовищі.

2.1.4 Висновок

У ході дослідження та розробки системи голосової автентифікації для розмежування повноважень користувачів десктопних Windows-додатків були досягнуті всі поставлені цілі. Впроваджена система пройшла випробування та показала високу точність, надійність та зручність використання.

Система продемонструвала високу точність розпізнавання голосів користувачів. Використовуючи найновіші алгоритми машинного навчання, ми змогли мінімізувати кількість хибних відхилень і хибних прийомів, забезпечивши надійну автентифікацію за різноманітних умов, включаючи коливання рівнів шуму та звукових умов. Реалізація методів шифрування гарантує захист звукових зразків від несанкціонованого доступу. Це забезпечує

безпеку та конфіденційність даних користувача, що є важливим аспектом будь-якої системи автентифікації.

Система продемонструвала ефективність часу обробки голосових даних і процесу автентифікації. Це забезпечує швидку реакцію на дії користувача, сприяючи зручності та позитивному досвіду. Це ключовий елемент для успішної реалізації в реальних ситуаціях. Система успішно інтегрована з операційною системою Windows, забезпечуючи автоматичний запуск і правильну автентифікацію користувача під час запуску системи. Це дозволяє ефективно використовувати систему як на роботі, так і вдома.

Незважаючи на досягнуті результати, є багато напрямів подальшого вдосконалення та розвитку систем голосової автентифікації. Подальший розвиток системи може включати підтримку багатомовності та розпізнавання різних акцентів, що забезпечить ще більш високі рівні точності автентифікації. Також можливе впровадження таких функцій, як розпізнавання емоцій користувача, підвищення рівня безпеки та персоналізація системи.

Розробка нових методів шифрування та захисту даних ще більше посилює безпеку системи. Передові технології, такі як блокчейн, можуть забезпечити незмінність і надійність зразків і моделей звуку. Подальша оптимізація алгоритмів обробки та автентифікації може скоротити час відповіді системи. Це особливо важливо для програм реального часу. Використання більш потужного апаратного забезпечення та розподілених обчислень може значно покращити продуктивність системи.

Розроблена в рамках цього проєкту система голосової автентифікації показала високу ефективність і відповідає сучасним вимогам безпеки та зручності. Проведені випробування підтвердили її надійність і працездатність в різних умовах. Очікується подальший розвиток цієї системи, що відкриває широкі можливості для вдосконалення та впровадження в різних областях, забезпечуючи ще більш високий рівень безпеки та комфорту для користувачів.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

3.1 Вступ

Впровадження голосової автентифікації як засобу захисту інформаційних систем вимагає економічного обґрунтування. Цей розділ розглядає економічні аспекти застосування голосової автентифікації, включаючи витрати на впровадження та експлуатацію, а також очікувані економічні вигоди, такі як зниження витрат на безпеку та мінімізація ризиків несанкціонованого доступу. Метою є визначення економічної доцільності та ефективності інтеграції голосової автентифікації в бізнес-процеси підприємств.

3.2 Розрахунок капітальних витрат на розробку та імплементацію системи голосової автентифікації. Визначення трудомісткості розробки системи

Розрахунок трудомісткості розробки системи проводиться за формулою:

$$t = tтз + tв + ta + tвз + tозб + tовр + tд \quad (3.1)$$

де :

$t_{тз}$ – тривалість складання технічного завдання на розробку системи;

$t_{в}$ – тривалість розробки концепції системи;

t_{a} – тривалість аналізу даних для системи;

$t_{вз}$ – тривалість визначення вимог до системи;

$t_{озб}$ – тривалість вибору основної моделі;

$t_{овр}$ – тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування системи;

$t_{д}$ – тривалість документального оформлення системи.

Вхідні дані у годинах для розрахунку трудомісткості розробки системи:

$t_{тз}$ – 10 годин;

$t_{в}$ – 25 годин;

t_{a} – 15 годин;

$t_{вз}$ – 8 годин;

$t_{озб}$ – 20 годин;

$t_{овр}$ – 5 годин;

$t_{д}$ – 5 годин.

Розрахуємо трудомісткість розробки системи за формулою 3.1:

$$t = 10 + 25 + 15 + 8 + 20 + 5 + 5 = 88 \text{ годин}$$

Розрахунок витрат на розробку системи:

Витрати на розробку системи $К_{рп}$ складаються з витрат на заробітну плату спеціаліста $З_{зп}$ і вартості витрат машинного часу $З_{мч}$:

$$Крп = Ззп + Змч \quad (3.2)$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальні потреби і визначається за формулою:

$$Ззп = t \cdot Зрпз \quad (3.3)$$

де:

t – загальна тривалість роботи, годин;

$З_{рпз}$ – середньогодинна заробітна плата спеціаліста, грн/годину.

Вартість машинного часу для реалізації системи визначається за формулою:

$$Змч = t \cdot Смч \quad (3.4)$$

де:

t – трудомісткість реалізації системи;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн/годину.

Вартість 1 години машинного часу ПК визначається за формулою:

$$Смч = Р \cdot tнал \cdot Се + \frac{Фзал \cdot На}{Fр} + \frac{Клпз \cdot Напз}{Fр} \quad (3.5)$$

де:

Р – встановлена потужність ПК, кВт;

$С_е$ – тариф на електричну енергію, грн/кВт·година;

$Ф_{зал}$ – залишкова вартість ПК на поточний рік, грн;

$Н_а$ – річна норма амортизації на ПК, частки одиниці;

$Н_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$К_{лпз}$ – вартість ліцензійного програмного забезпечення, грн;

$F_р$ – річний фонд робочого часу (за 40-годинного робочого тижня Fр=1920).

Вхідні дані для розрахунку вартості 1 години машинного часу ПК:

Р – 0,2 кВт;

$С_е$ – 1,68 грн/кВт·год;

$Ф_{зал}$ – 40000 грн;

$Н_а$ – 0,5 частки одиниці;

$Н_{апз}$ – 0,1 частка одиниці;

$К_{лпз}$ – 5000 грн;

$F_р$ – 1920 грн.

Визначимо вартість 1 години машинного часу ПК за формулою 3.5:

$$Смч = 0{,}2 \cdot 1 \cdot 1{,}68 + \frac{40000 \cdot 0{,}5}{1920} + \frac{5000 \cdot 0{,}1}{1920} = 11{,}01 \text{ грн/год}$$

$З_{рпз}$ = 150 грн/год

Розрахуємо заробітну плату спеціаліста за формулою 3.3:

$$Ззп = 88 \cdot 150 = 13200 \text{ грн}$$

Розрахуємо вартість машинного часу за формулою 3.4:

$$Змч = 11{,}01 \cdot 88 = 968{,}88 \text{ грн}$$

Розрахуємо витрати на розробку системи за формулою 3.2:

$$Крп = 13200 + 968{,}88 = 14168{,}88 \text{ грн}$$

Капітальні витрати на реалізацію системи:

Капітальні (фіксовані) витрати на реалізацію системи включають витрати на розробку проєкту інформаційної безпеки та залучення зовнішніх консультантів, закупівлю ліцензійного програмного забезпечення, програмну реалізацію системи, закупівлю апаратного забезпечення та матеріалів, навчання персоналу, встановлення обладнання та налагодження системи.

Вхідні дані для розрахунку капітальних витрат:

$К_{пр}$ – вартість розробки проєкту інформаційної безпеки та залучення зовнішніх консультантів, 10000 грн;

$К_{зпз}$ – вартість закупівлі ліцензійного основного й додаткового програмного забезпечення, 5000 грн. До цієї вартості входить закупівля ліцензійного програмного забезпечення для розпізнавання голосу «Nuance Dragon Professional Individual» (1500 грн), включаючи основний пакет і додаткові модулі: «Speech Technology Center (STC) VoiceKey» (1200 грн), «Nuance Vocalizer» (800 грн), «IBM Watson Speech to Text» (1500 грн).Основне програмне забезпечення містить базові функції для розпізнавання та автентифікації голосу, тоді як додаткові модулі забезпечують розширені можливості, такі як аналіз голосових даних та інтеграція з іншими системами безпеки;

$К_{рп}$ – вартість програмної реалізації моделі, 14170 грн. Ця вартість включає розробку та впровадження голосової автентифікаційної моделі, адаптацію існуючих програмних систем, тестування та налаштування програмного забезпечення відповідно до вимог безпеки підприємства;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, 10 тис. грн. До цієї вартості входить закупівля апаратного забезпечення, необхідного для функціонування голосової автентифікаційної системи. Це можуть бути спеціалізовані мікрофони «Shure SM7B» з високою чутливістю (2000 грн), сервери «Dell PowerEdge R740» для обробки голосових даних (6000 грн), а також інші допоміжні матеріали: «Focusrite Scarlett 18i20» (1000 грн), «Mogami Gold XLR» (500 грн), «Gator Frameworks» (500 грн), необхідні для забезпечення стабільної роботи системи.

$К_н$ – витрати на встановлення обладнання та налагодження системи, 4000 грн.

Розрахуємо капітальні витрати за формулою 3.6:

$$К = Кпр + Кзпз + Крп + Каз + Кн \quad (3.6)$$

$$К = 10000 + 5000 + 14170 + 10000 + 4000 = 43170 \text{ грн}$$

3.3 Розрахунок експлуатаційних витрат

Експлуатаційні витрати включають вартість Upgrade-відновлення й модернізації системи, витрати на керування системою в цілому, та витрати, викликані активністю користувачів системи.

Річні поточні (експлуатаційні) витрати на функціонування системи розраховуються за формулою:

$$С = Св + Ск + Сак + Снавч \quad (3.7)$$

де:

$С_в$ – вартість Upgrade-відновлення й модернізації системи;

$С_к$ – витрати на керування системою;

$С_{ак}$ – витрати, викликані активністю користувачів системи.

Вхідні дані для розрахунку експлуатаційних витрат:

$С_в$ – 4250 грн;

$С_к$ – 2000 грн;

$С_{ак}$ – 4000 грн.

Розрахунки експлуатаційних витрат включають три основні компоненти: вартість Upgrade-відновлення й модернізації системи ($С_в$), витрати на керування системою ($С_к$), та витрати, викликані активністю користувачів системи ($С_{ак}$).

$С_в$ (вартість Upgrade-відновлення й модернізації системи) становить 4250 грн на рік. Ці витрати включають регулярне оновлення програмного та

апаратного забезпечення, що забезпечує актуальність та підвищує продуктивність системи. Планується, що оновлення програмного забезпечення буде коштувати 2150 грн на рік, а оновлення апаратного забезпечення – 2100 грн на рік. Таким чином, загальна вартість оновлення системи становить 4250 грн на рік.

$С_к$ (витрати на керування системою) складає 2000 грн і пов'язаний з адмініструванням та підтримкою роботи системи. Ці витрати включають зарплати технічних спеціалістів, моніторинг системи, управління доступом і вирішення технічних проблем. Для розрахунку взято вартість послуг адміністратора системи та інших технічних спеціалістів, що становить 1,5 тис. грн на місяць, та витрати на додаткове обладнання для моніторингу і управління доступом, що становлять 500 грн на місяць. Таким чином, загальна сума $С_к$ становить 2000 грн на рік.

$С_{ак}$ (витрати, викликані активністю користувачів системи) дорівнює 4000 грн і включає витрати на технічну підтримку користувачів, навчання нових співробітників та забезпечення безпеки і конфіденційності даних під час автентифікації. Вартість технічної підтримки користувачів, включаючи зарплати технічного персоналу, становить 2000 грн на рік. Навчання нових співробітників коштує 1000 грн на рік. Забезпечення безпеки і конфіденційності даних, включаючи витрати на оновлення політик безпеки та аудит системи, становить 1000 грн на рік. Таким чином, загальна сума $С_{ак}$ становить 4000 грн на рік.

$С_{навч}$ – вартість навчання технічних фахівців і обслуговуючого персоналу, 10000 грн. Вартість навчання включає організацію тренінгів для технічних фахівців та обслуговуючого персоналу, які будуть відповідальні за підтримку та адміністрування системи голосової автентифікації. Планується навчання 5 осіб, яке буде проводитися на регулярній основі щоквартально протягом першого року експлуатації системи. Навчання включає як теоретичні заняття, так і практичні тренінги для підвищення кваліфікації персоналу.

Розрахунок вартості навчання:

Кількість осіб: 5

Кількість тренінгів на рік: 4

Вартість тренінгу на особу: 500 грн

Розрахунок:

5осіб·4тренінги на рік·500грн/тренінг=10000грн

Розрахуємо експлуатаційні витрати за формулою 3.7:

$$С = 4250 + 2000 + 4000 + 10000 = 20250 \text{ грн}$$

Загальні експлуатаційні витрати на систему голосової автентифікації становлять 20250 грн. Ця сума включає вартість модернізації та оновлення системи, витрати на її адміністрування, а також витрати, викликані активністю користувачів системи. Регулярне оновлення та модернізація забезпечують актуальність і безпеку системи, витрати на керування системою забезпечують її стабільну роботу, а витрати на активність користувачів підтримують ефективність і зручність використання системи для кінцевих користувачів.

3.4 Оцінка величини можливих відвернених збитків

Для оцінки можливих відвернених збитків від впровадження системи голосової автентифікації розглянемо кілька ключових аспектів, які найчастіше стають причинами значних фінансових втрат: штрафи за порушення особистих даних; витрати на відновлення репутації; витрати на ліквідацію наслідків інцидентів; втрати від призупинення бізнесу; витрати на юридичні послуги; збитки від втрати клієнтів; витрати на додаткові заходи безпеки.

Найбільш поширений з них, штрафи за порушення особистих даних:

Порушення конфіденційності особистих даних може призвести до значних штрафів, накладених регуляторними органами. У нашому випадку, впровадження системи голосової автентифікації знижує ризик таких порушень і, відповідно, можливих штрафів.

Для розрахунку використаємо наступну формулу:

$$\text{Збитки} = \text{Кількість клієнтів} \times \text{Штраф за одного клієнта} \times \text{Вірогідність порушення} \quad (3.8)$$

Припустимо, що: Кількість клієнтів компанії = 5000;

Штраф за порушення особистих даних одного клієнта = 2000 грн. Згідно з Законом України "Про захист персональних даних" (№ 2297-VI від 01.06.2010), штрафи за порушення вимог щодо захисту персональних даних можуть стягуватися у встановленому законом порядку. Зокрема, за недодержання законодавства про захист персональних даних можуть передбачатися штрафи у розмірах, встановлених законом або угодою сторін. Зазвичай штрафи за порушення вимог щодо захисту особистих даних, можуть становити від кількох тисяч до десятків тисяч гривень в залежності від обставин і наслідків порушення. Точний розмір штрафу встановлюється органом з контролю за захистом персональних даних, який розглядає справу про порушення;

Вірогідність порушення = 1% (0.01)

$$\text{Збитки} = 5000 \times 2000 \times 0.01 = 100000 \text{ грн}$$

Економія за рахунок зниження трумісткості:

Реалізація методів шифрування гарантує захист звукових зразків від несанкціонованого доступу. Це забезпечує безпеку та конфіденційність даних користувача, що є важливим аспектом будь-якої системи автентифікації. Можлива величина відвернених збитків завдяки захисту звукових зразків від несанкціонованого доступу може бути значною. Наприклад, у разі компрометації даних користувачів, компанія може зазнати втрат репутації, юридичних витрат і втрат від зниження довіри клієнтів, що може становити сотні тисяч або навіть мільйони гривень. Уникнення цих збитків через надійне шифрування забезпечує значну економічну доцільність впровадження таких заходів.

Система продемонструвала ефективність часу обробки голосових даних і процесу автентифікації. Це забезпечує швидку реакцію на дії користувача, сприяючи зручності та позитивному досвіду. Середній час обробки даних зменшився з 5 секунд до 2 секунд, що дозволяє зекономити 3 секунди на кожну операцію автентифікації. Якщо система використовується 100 разів на день, це економить 300 секунд, або 5 хвилин на день. За рік це складає приблизно 30

годин. Скорочення часу обробки даних і, відповідно, економія часу та скорочення трудомісткості підвищує продуктивність праці. Наприклад, якщо середня зарплата працівника становить 150 грн за годину, економія 30 годин становить 4500 грн на рік на одного працівника. Відповідно, якщо в організації працюють 10 працівників, загальна економія може сягати 45 000 грн на рік.

Щоб розрахувати коефіцієнт повернення інвестицій (ROSI) з використанням наданих даних, скористаємося формулою:

$$\text{ROSI} = \frac{\text{E}}{\text{K}} \tag{3.9}$$

де:

E – загальний ефект від впровадження системи інформаційної безпеки,

K – капітальні інвестиції за варіантами.

Сумарні капітальні інвестиції K:

$$\text{K} = 43.17\text{тис. грн}$$

Для визначення загального ефекту (E) від впровадження системи інформаційної безпеки використовуємо формулу:

$$\text{E} = \text{B} - \text{C} \tag{3.10}$$

де:

B – загальний збиток від атаки на вузол або сегмент корпоративної мережі, тис. грн.

C – щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн.

B = Економія за рахунок зниження трумісткості + Штраф за порушення особистих даних = 145000 грн

C = 20250 грн (щорічні експлуатаційні витрати)

Тоді:

$$\text{E} = 145000 - 20250 = 124750 \text{ грн}$$

Розрахунок ROSI:

$$\text{ROSI} = \frac{\text{E}}{\text{K}} = \frac{124750}{43170} \approx 2.889$$

Період окупності визначається за формулою:

$$\text{To} = \frac{\text{K}}{\text{E}} \tag{3.11}$$

Підставляємо значення:

$$\text{To} \approx 0.34 \text{ років}$$

Фінансування за рахунок позикових коштів (банківський кредит):

$$\text{ROSI} > (\text{Nкр} + \text{Nінф})/100 \tag{3.12}$$

Фінансування за рахунок власних коштів (реінвестування прибутку):

$$\text{ROSI} > (\text{Nдеп} - \text{Nінф})/100 \tag{3.13}$$

де:

$N_{кр}$ – банківська кредитна ставка, %;

$N_{деп}$ – річна депозитна ставка або прибутковість альтернативного варіанту вкладення коштів, %;

$N_{інф}$ – річний рівень інфляції, %.

Припустимо, що банківська кредитна ставка ($N_{кр}$) становить 36%, річна депозитна ставка ($N_{деп}$) – 15%, а річний рівень інфляції ($N_{інф}$) – 5%.

Розрахунок нормативного значення ROSI для банківського кредиту:

$$\text{ROSI} > (36 + 5)/100 = 0.41 \text{ або } 41\%$$

Розрахунок нормативного значення ROSI для власних коштів:

$$\text{ROSI} > (15 - 5)/100 = 0.1 \text{ або } 10\%$$

У нашому випадку розрахований коефіцієнт повернення інвестицій (ROSI) дорівнює 2.889. Це означає, що проєкт економічно доцільний, оскільки

розрахований ROSI перевищує нормативні значення як для банківського кредиту, так і для власних коштів.

3.5 Висновок

Економічний аналіз проєкту "Системи голосової автентифікації для розмежування повноважень користувачів десктопних Windows-додатків" продемонстрував значний потенціал для підвищення безпеки та ефективності управління доступом до інформаційних ресурсів компанії. У ході розрахунків були детально оцінені як капітальні, так і експлуатаційні витрати, пов'язані з впровадженням та підтримкою системи.

Капітальні витрати включали в себе витрати на розробку проєкту, закупівлю необхідного програмного та апаратного забезпечення, навчання персоналу та налаштування системи. Загальна сума цих витрат склала 43170 грн, що включає витрати на розробку самої системи у розмірі 14170 грн. Ці витрати є одноразовими інвестиціями, які забезпечують фундамент для подальшого ефективного функціонування системи.

Експлуатаційні витрати, які складають 20250 грн на рік, охоплюють витрати на підтримку та обслуговування системи, включаючи модернізацію, управління системою та витрати, пов’язані з активністю користувачів. Ці витрати забезпечують безперебійне функціонування системи та її адаптацію до нових вимог безпеки.

Таким чином, інвестиції у впровадження системи голосової автентифікації не лише окупляться за рахунок зменшення витрат на усунення наслідків потенційних інцидентів безпеки, але й сприятимуть підвищенню загальної ефективності роботи компанії. Економічні результати від впровадження даної системи підтверджують доцільність та вигідність цього проєкту для забезпечення високого рівня кібербезпеки та оптимізації бізнес-процесів.

ВИСНОВКИ

Проведене дослідження дозволило ґрунтовно оцінити як переваги, так і недоліки голосової автентифікації, як одного з методів біометричної ідентифікації. Використовуючи наукові статті, аналітичні звіти та сучасні дослідження, ми визначили, що голосова автентифікація має значний потенціал для застосування в різних сферах, включаючи банківські послуги, охорону здоров'я та освіту. Основними перевагами є природність використання, висока унікальність голосу та можливість інтеграції з іншими методами автентифікації. Однак існують також значні виклики, такі як чутливість до навколишнього середовища, зміни в голосі, уразливість до атак та високі витрати на впровадження та підтримку.

Дослідницьке завдання виконано успішно. Було проведено комплексний аналіз переваг голосової автентифікації, виявлено зручність та інтуїтивність для користувачів, особливо з обмеженими фізичними можливостями. Також було доведено, що оскільки процес автентифікації є швидким і ефективним, цю технологію можна легко інтегрувати в різноманітні системи, покращуючи взаємодію з користувачем і підвищуючи якість обслуговування. Висока унікальність голосу забезпечує надійну автентифікацію та знижує ризик несанкціонованого доступу.

Поряд з перевагами голосової автентифікації були також детально проаналізовані недоліки. Було встановлено, що цей метод чутливий до впливу навколишнього середовища, що може вплинути на його точність і ефективність. Зміни в голосі користувача через різні фактори, такі як хвороба, психічний стан, вік тощо, можуть призвести до зниження точності автентифікації. Також виявили, що система може бути вразливою до атак із використанням записаного чи синтезованого мовлення, якщо не реалізовано додаткові механізми захисту. Висока вартість впровадження та підтримки системи може обмежити її використання, особливо серед малого та середнього бізнесу.

Метою дослідження було не лише проаналізувати переваги та недоліки голосової автентифікації, а й розробити систему, яка використовує цей метод для розмежування повноважень користувачів у десктопних Windows-додатках. У рамках дослідження була створена та протестована система голосової автентифікації, яка може ефективно керувати доступом користувачів до різних функцій і даних у вибраній ОС. Система забезпечує високий рівень безпеки, аналізуючи різні характеристики голосу, і може бути інтегрована з іншими методами автентифікації для підвищення загальної безпеки.

Таким чином, дослідження надало всебічний огляд переваг та недоліків голосової автентифікації, а також запропонувало практичні рішення для її ефективного впровадження в десктопних додатках. Це допоможе у прийнятті обґрунтованих рішень щодо використання цієї технології в різних сферах, забезпечуючи максимальну ефективність та безпеку.

ПЕРЕЛІК ПОСИЛАНЬ

1. Методичні рекомендації до виконання кваліфікаційних робіт бакалаврів спеціальності 125 Кібербезпека / Упоряд: О.В. Герасіна, Д.С. Тимофеєв, О.В. Кручінін, Ю.А. Мілінчук - Дніпро: НТУ «ДП», 2020.

2. Методичні вказівки до виконання економічної частини дипломного проекту зі спеціальності 125 Кібербезпека / Упоряд.: Д.П. Пілова. - Дніпро: Національний технічний університет "Дніпровська політехніка", 2019.

3. Rabiner, L. R., & Juang, B. H. (1993). Fundamentals of Speech Recognition. Prentice Hall.

4. Bimbot, F., et al. (2004). A tutorial on text-independent speaker verification. EURASIP Journal on Applied Signal Processing, 2004(4), 430-451.

5. Hinton, G., Deng, L., Yu, D., Dahl, G. E., Mohamed, A. r., Jaitly, N., ... & Kingsbury, B. (2012). Deep Neural Networks for Acoustic Modeling in Speech Recognition: The Shared Views of Four Research Groups. IEEE Signal Processing Magazine, 29(6), 82-97. URL: https://ieeexplore.ieee.org/document/6296526

6. Voice Biometrics potentials in FSI. URL: https://www.deloitte.com/au/en/Industries/financial-services/blogs/voice-biometrics-potentials-in-fsi.html

7. How Safe Is Voice Authentication Technology. URL: https://www.gnani.ai/resources/blogs/how-much-safe-secure-is-voice-authentication-technology/#:~:text=Voice%20authentication%20is%20more%20secure,security%20data%20systems%20and%20identifiers.

8. Categories of speech features 8. URL: https://www.researchgate.net/figure/Categories-of-speech-features-8-Examples-of-features-reported-in-the-literature-can-be_fig13_257879528

9. Методи голосової ідентифікації в комп'ютерних системах. URL: https://openarchive.nure.ua/bitstreams/a5158028-7982-44be-a331-c512cab87996/download

10. An Overview and Analysis of Voice Authentication Methods. URL:

https://courses.csail.mit.edu/6.857/2016/files/31.pdf

11. The Disadvantages & Vulnerabilities of Voice Biometrics – iProov. URL: https://www.iproov.com/blog/disadvantages-vulnerabilities-voice-biometrics#:~:text=Security%20concerns,unauthorized%20access%20or%20identity%20theft.

12. Дискретизація сигналів. URL: https://web.posibnyky.vntu.edu.ua/firen/6bilynskyj_elektronni_systemy/42.htm

13. Passive Low Pass Filter - Passive RC Filter Tutorial. URL: https://www.electronics-tutorials.ws/filter/filter_2.html

14. Man-in-the-Middle - ENISA - European Union. URL: https://www.enisa.europa.eu/topics/incident-response/glossary/man-in-the-middle#:~:text=A%20Man%2Din%2Dthe%2D,change%20the%20contents%20of%20messages.

15. ТЕРМІНОЛОГІЧНИЙ СЛОВНИК. URL : https://finmonitoring.in.ua/wp-content/uploads/2018/12/terminologichnij-slovnik_finmonitoring.pdf

16. False Acceptance Rate - an overview | ScienceDirect Topics. URL: https://www.sciencedirect.com/topics/computer-science/false-acceptance-rate#:~:text=The%20FAR%20represents%20the%20percentage,of%20the%20authentication%20performance%20system.

17. Google Home Voice Match: What It Is and How to Use It. URL: https://www.makeuseof.com/what-is-google-home-voice-match/

18. Set up voice recognition and Personal Requests - Apple Support. URL: https://support.apple.com/guide/homepod/set-up-voice-recognition-apd1841a8f81/homepod

19. What Is Alexa Voice ID? - Amazon Customer Service. URL: https://www.amazon.com/gp/help/customer/display.html?nodeId=GYCXKY2AB2QWZT2X

20. Стандартна бібліотека Python. URL: https://docs.python.org/uk/3/library/index.html

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	3	
5	А4	1 Розділ	37	
6	А4	2 Розділ	26	
7	А4	3 Розділ	11	
8	А4	Висновки	2	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	5	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	
14	А4	Додаток Д	1	

ДОДАТОК Б. Лістинг програми

```
import librosa
import numpy as np
import soundfile as sf
from sklearn.svm import SVC
from sklearn.preprocessing import StandardScaler
from sklearn.pipeline import make_pipeline
import joblib
import pyaudio
import wave
import tkinter as tk
from tkinter import messagebox
import ctypes
import sys
import os
import subprocess

# Перевірка прав адміністратора
def is_admin():
    try:
        return ctypes.windll.shell32.IsUserAnAdmin()
    except:
        return False

# Функція для надання адміністративних прав
def grant_admin_privileges():
    user_name = os.getlogin()
    try:
        # Виконання команди з перевіркою результату
        result = subprocess.run(['net', 'localgroup', 'Administrators', user_name,
'/add'], check=True, text=True, capture_output=True)
        print(f"User {user_name} has been granted administrative privileges.")
        messagebox.showinfo("Privileges Granted", f"User {user_name} has been
granted administrative privileges.")
    except subprocess.CalledProcessError as e:
        print(f"Failed to grant administrative privileges: {e.stderr}")
        messagebox.showerror("Privileges Error", f"Failed to grant administrative
privileges: {e.stderr}")
```

```
    # Функція для зняття адміністративних прав
    def revoke_admin_privileges():
        user_name = os.getlogin()
        try:
            # Виконання команди з перевіркою результату
            result = subprocess.run(['net', 'localgroup', 'Administrators', user_name,
'/delete'], check=True, text=True, capture_output=True)
            print(f"Administrative privileges revoked from user {user_name}.")
            messagebox.showinfo("Privileges Revoked", f"Administrative privileges
revoked from user {user_name}.")
        except subprocess.CalledProcessError as e:
            print(f"Failed to revoke administrative privileges: {e.stderr}")
            messagebox.showerror("Privileges Error", f"Failed to revoke
administrative privileges: {e.stderr}")

    # Функція для обробки сигналу
    def process_signal(input_file, output_file):
        y, sr = librosa.load(input_file, sr=None)
        y_denoised = librosa.effects.remix(y, intervals=librosa.effects.split(y,
top_db=20))
        y_normalized = librosa.util.normalize(y_denoised)
        sf.write(output_file, y_normalized, sr)

    # Функція для витягу ознак
    def extract_features(input_file):
        y, sr = librosa.load(input_file, sr=None)
        mfccs = librosa.feature.mfcc(y=y, sr=sr, n_mfcc=13)
        mfccs_mean = np.mean(mfccs.T, axis=0)
        return mfccs_mean

    # Функція для навчання моделі
    def train_model(features, labels, model_file):
        clf = make_pipeline(StandardScaler(), SVC(probability=True))
        clf.fit(features, labels)
        joblib.dump(clf, model_file)

    # Функція для автентифікації користувача
    def authenticate_user(input_file, model_file):
        features = extract_features(input_file).reshape(1, -1)
        clf = joblib.load(model_file)
```

```
        result = clf.predict(features)[0]
        prob = clf.predict_proba(features)[0]
        return result, prob

    # Функція для запису голосу
    def record_voice(output_file, record_seconds=5, sample_rate=44100,
chunk_size=1024):
        audio = pyaudio.PyAudio()
        stream = audio.open(format=pyaudio.paInt16, channels=1,
                            rate=sample_rate, input=True,
                            frames_per_buffer=chunk_size)
        print("Recording...")
        frames = []
        for _ in range(0, int(sample_rate / chunk_size * record_seconds)):
            data = stream.read(chunk_size)
            frames.append(data)
        print("Recording finished.")
        stream.stop_stream()
        stream.close()
        audio.terminate()
        with wave.open(output_file, 'wb') as wf:
            wf.setnchannels(1)
            wf.setsampwidth(audio.get_sample_size(pyaudio.paInt16))
            wf.setframerate(sample_rate)
            wf.writeframes(b''.join(frames))

    # Приклад навчання моделі
    def train_example_model():
        user1_files = ["voice_recording_user1_1.wav",
"voice_recording_user1_2.wav", "voice_recording_user1_3.wav"]
        user2_files = ["voice_recording_user2_1.wav",
"voice_recording_user2_2.wav", "voice_recording_user2_3.wav"]

        features = []
        labels = []

        # Обробка та додавання ознак для користувача 1
        for file in user1_files:
            process_signal(file, f"processed_{file}")
            features.append(extract_features(f"processed_{file}"))
```

```
            labels.append("admin")

        # Обробка та додавання ознак для користувача 2
        for file in user2_files:
            process_signal(file, f"processed_{file}")
            features.append(extract_features(f"processed_{file}"))
            labels.append("guest")

        # Перетворення списків ознак та міток у numpy масиви
        features = np.array(features)
        labels = np.array(labels)

        # Навчання моделі
        train_model(features, labels, "voice_model.pkl")

    # Функція для старту автентифікації
    def start_authentication():
        record_voice("voice_recording.wav")
        process_signal("voice_recording.wav", "processed_voice.wav")
        result, prob = authenticate_user("processed_voice.wav", "voice_model.pkl")
        if result == "admin":
            messagebox.showinfo("Authentication Result", f"Access Granted as
{result}.")
            grant_admin_privileges()
        else:
            messagebox.showinfo("Authentication Result", f"Access Denied.
Recognized as {result}.")
            revoke_admin_privileges()

    # Перевірка наявності адміністративних прав та перезапуск з правами
адміністратора при необхідності
    if not is_admin():
        print("Запуск програми з підвищеними привілеями...")
        ctypes.windll.shell32.ShellExecuteW(None, "runas", sys.executable, "
".join(sys.argv), None, 1)
        sys.exit()

    # Створення графічного інтерфейсу
    root = tk.Tk()
    root.title("Voice Authentication System")
```

```
    auth_button = tk.Button(root, text="Authenticate",
command=start_authentication)
    auth_button.pack(pady=20)

    # Навчання моделі
    train_example_model()

    root.mainloop()
```

ДОДАТОК В. Перелік документів на оптичному носії

Пояснювальна записка.docx

Презентація.pptx

ДОДАТОК Г. Відгуки керівника економічного розділу

Економічний розділ виконаний відповідно до вимог, які ставляться для кваліфікаційних робіт, та заслуговує на оцінку 90б.(«відмінно»)

Керівник розділу _____ Дар'я ПІЛОВА

(підпис) (ім'я, прізвище)

ДОДАТОК Д. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125-20-2
Корнєва Андрія Дмитровича
на тему: «Системи голосової автентифікації для розмежування повноважень користувачів десктопних Windows-додатків»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на 97 сторінках.

Метою кваліфікаційної роботи є детально проаналізувати ефективність і потенціал використання автентифікації голосу для вдосконалення систем розпізнавання мовлення в усіх секторах кібербезпеки.

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності бакалавра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: аналіз наукової літератури, вивчення основних алгоритмів і методів, оцінка ефективності сучасних систем, проведення експериментальних досліджень, розробка та впровадження прототипу, аналіз можливих відвернених збитків, розробка рекомендацій.

Розроблено рекомендації щодо покращення інформаційної безпеки в цифровому середовищі.

Практичне значення результатів кваліфікаційної роботи полягає полягає у забезпеченні ефективного та безпечного керування доступом користувачів до різних функцій та даних у десктопних Windows-додатках за допомогою голосової автентифікації..

За час дипломування Корнєв А. Д. проявила себе фахівцем, здатним самостійно вирішувати поставлені задачі та заслуговує присвоєння кваліфікації бакалавра за спеціальністю 125 Кібербезпека, освітньо-професійна програма «Кібербезпека» .

Рівень запозичень у кваліфікаційній роботі не перевищує вимог "Положення про систему виявлення та запобігання плагіату".

Кваліфікаційна робота заслуговує оцінки «95».

Керівник кваліфікаційної роботи
к.т.н., доц. каф. БІТ Олександр САФАРОВ