МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри Комп'ютеризованих систем захисту інформації

_____ Михайло СТЕПАНОВ
«____»_____ 2023 р.

На правах рукопису
УДК 004.056.6:004.056.65

КВАЛІФІКАЦІЙНА РОБОТА ЗДОБУВАЧА ВИЩОЇ ОСВІТИ ОСВІТНЬОГО СТУПЕНЯ «МАГІСТР»

Тема: Програмний модуль багатофакторної автентифікації для доступу до інформаційних активів.

Виконавець: Андрій КЛИМЕНКО
Керівник: к.т.н. Наталія ГУЛАК
Консультант розділу «Охорона навколишнього середовища»: к.т.н., доцент Тетяна ДМИТРУХА
Нормоконтролер: к.т.н. Наталія ГУЛАК

Київ 2023

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет: Кібербезпеки та програмної інженерії

Кафедра: Комп'ютеризованих систем захисту інформації

Освітній ступінь: Магістр

Спеціальність: 125 «Кібербезпека»

Освітньо-професійна програма: «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ
Завідувач кафедри Комп'ютеризованих систем захисту інформації

_____Михайло СТЕПАНОВ
«__» _____ 2023 р.

ЗАВДАННЯ

на виконання кваліфікаційної роботи

здобувача вищої освіти Клименка Андрія Вікторовича

1. Тема: *Програмний модуль багатофакторної автентифікації для доступу до інформаційних активів*
затверджена наказом ректора від «15» вересня 2023 р. № 1814/ст.
2. Термін виконання: з 16.10.2023 р. по 31.12.2023 р.
3. Вихідні дані: методи автентифікації, автентифікація методами шифрування, біометричні методи автентифікації, архітектура платформи Azure, багатофакторна автентифікація, мова програмування C#
4. Зміст пояснювальної записки: аналіз методів автентифікації на основі нормативно-правової бази України; визначення методів для багатофакторної автентифікації на основі їх порівняльного аналізу; розробка і реалізація програмного модуля багатофакторної автентифікації.

5. КАЛЕНДАРНИЙ ПЛАН

виконання кваліфікаційної роботи

№ з/п	Етапи виконання кваліфікаційної роботи	Термін виконання етапів	Примітка
1.	Уточнення постановки задачі	16.10.2023	*Виконано*
2.	Аналіз літературних джерел	18.10.2023	*Виконано*
3.	Обґрунтування вибору рішення	22.10.2023	*Виконано*
4.	Збір інформації	01.11.2023	*Виконано*
5.	Аналіз методів автентифікації на основі нормативно-правової бази України.	01.11.2023-15.11.2023	*Виконано*
6.	Визначення методів для багатофакторної автентифікації на основі порівняльного аналізу	16.11.2023-20.11.2023	*Виконано*
7.	Розробка і реалізація програмного модуля багатофакторної автентифікації.	21.11.2023-09.12.2023	*Виконано*
8.	Проведення дослідження природних екосистем.	08.12.2023	*Виконано*
9.	Апробація роботи на V міжнародно-практичній конференції: «TRENDS IN SCIENCE REGARDING THE CREATION OF NEW TEACHING METHODS»	09.12.2023	*Виконано*
10.	Перевірка на антиплагіат	06.12.2023	*Виконано*
11.	Оформлення і друк пояснювальної записки	07.12.2023	*Виконано*
12.	Оформлення презентації	10.12.2023	*Виконано*
13.	Отримання рецензій від рецензента	22.12.2023	*Виконано*

6. Консультанти з окремих розділів

Розділ	Консультант (посада, П.І.Б.)	Дата, підпис	
		Завдання видав	Завдання прийняв
Охорона навколишнього середовища	Дмитруха Т.І.		

7. Дата видачі завдання: «16» жовтня 2023 р.

Здобувач вищої освіти Андрій КЛИМЕНКО
(підпис, дата)

Керівник кваліфікаційної роботи Наталія ГУЛАК
(підпис, дата)

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, чотирьох розділів, загальних висновків, списку використаних джерел, додатків і має 80 сторінок основного тексту, 23 рисунка, 13 таблиць, 5 сторінок додатків. Список використаних джерел містить 22 найменувань і займає 2 сторінок. Загальний обсяг роботи 81 сторінок.

Метою даної роботи є розробка, тестування та оцінка підвищення рівня захисту доступу до інформаційних активів методом багатофакторної автентифікації.

В роботі вирішено задачу побудови системи аналізу і оцінки ризиків інформаційної безпеки на основі експертних думок відповідно до вимог НД ТЗІ та інших нормативно-правових документів, сформованих в умовах нечіткості.

В роботі розроблено алгоритм та програмне забезпечення для реалізації багатофакторної автентифікації на основі сканування сітківки ока. Цей метод відноситься до галузі інформаційної безпеки та може бути застосований для підвищення рівня безпеки та автентифікації користувачів.

Розроблений програмний модуль дозволяє впроваджувати багатофакторну автентифікацію, використовуючи сканування сітківки ока як один з ключових факторів ідентифікації особи. Це дозволяє отримати високий рівень безпеки, оскільки сканування сітківки ока є надійним методом біометричної автентифікації.

Можливі напрямки подальшого розвитку цього модуля пов’язані з вдосконаленням та розширенням функціоналу для відповідності міжнародним стандартам безпеки, таким як ISO 27001.

Ключові слова: багатофакторна автентифікація, сканування сітківки ока, інформаційна безпека, розвиток програмного забезпечення, точність і надійність, методи шифрування, біометричні методи, методи автентифікації.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

MFA – багатофакторна автентифікація;

БД – база даних;

ВД – вихідні дані;

ІБ – інформаційна безпека;

ІКС – інформаційно-комунікаційна система;

ІСТ – Інформаційно-комунікаційна система;

SW – Програне забезпечення;

ЗІ – захист інформації;

ЛЗ – лінгвістична змінна;

НЗ – нечітка змінна;

НЛ – нечітка логіка;

Alg – алгоритм;

ПЗ – програмний засіб;

ПК – персональний комп’ютер;

СРОО – сканування райдужної оболонки ока;

МІС – міжнародний стандарт;

ISO – International Organization for Standardization.

ВСТУП

Сучасний світ, повний цифрових технологій і інформаційних активів, вимагає надійного забезпечення безпеки та контролю доступу до цінних інформаційних ресурсів. Завдяки великим обсягам даних та специфічним характеристикам інформаційного середовища, забезпечення безпеки стає важливим завданням для багатьох сфер, включаючи бізнес, державний сектор, науку та освіту.

Багатофакторна автентифікація стала ключовим елементом в системах безпеки, яка дозволяє впевнитися в ідентифікації користувачів та обмеженні доступу лише для авторизованих осіб. Ця технологія базується на використанні декількох методів автентифікації, таких як паролі, біометричні дані, смарт-карти, тощо. Інтеграція багатофакторної автентифікації в системи стала необхідністю, оскільки звичайний логін і пароль вже недостатньо надійні для захисту важливої інформації.[1]

Актуальність теми: Для підвищення безпеки комп'ютерних систем важливо використовувати багатофакторну автентифікацію, яка включає в себе використання біометричних даних користувача. Біометричні дані є унікальними для кожної людини, що робить їх більш надійними, ніж традиційні методи автентифікації, такі як паролі та одноразові коди. Цей двофакторний підхід до автентифікації має великий потенціал у забезпеченні високого рівня безпеки та надійності тому, тема роботи є актуальною.

Метою даної роботи є розробка, тестування та оцінка підвищення рівня захисту доступу до інформаційних активів методом багатофакторної автентифікації.

Для досягнення поставленої мети вирішуються такі **задачі:**

- аналіз методів автентифікації на основі нормативно правової бази України;
- визначення методів для багатофакторної автентифікації на основі їх порівняльного аналізу;

− розробка, тестування та оцінка підвищення рівня захисту інформаційних активів багатофакторної автентифікації

Галузь застосування. Розроблений метод та програмне забезпечення відносяться до галузі інформаційної безпеки і можуть бути використані для підвищення рівня захищеності ІКС за рахунок використання методів біометричної автентифікації та шифрування інформації.

Об’єктом дослідження є процес захисту доступу до інформаційних активів багатофакторною автентифікацією.

Предметом дослідження є методи шифрування і біометричні методи для автентифікації.

Методи дослідження базуються на основі об’єктно-орієнтованого програмування (для програмної реалізації розробленого методу).

Новизна одержаних результатів полягає в наступному:

Було розроблено та протестовано програмний модуль для підвищення захисту інформаційних активів з використанням методів паролів та сканування райдужної оболонки ока, що дало можливість отримати низьку ймовірність проникнення за стандартним розрахунком 0.5%. Коефіцієнт захисту від несанкціонованого доступу складає 99.5%.

Практична цінність: програмний модуль багатофакторної автентифікації має велику практичну цінність у сфері кібербезпеки, так як знижує ризик несанкціонованого доступу до інформації, також значно підвищує безпеку даних користувача.

Апробація. Основні положення роботи доповідалися та обговорювалися на таких конференціях: Клименко А.В. Використання біометричних методів для багатофакторної автентифікації/ Н.К. Гулак, А.В. Клименко //V International Scientific and Practical Conference "Trends in science regarding the creation of new teaching methods", October 16-18, 2023, Madrid, Spain. - С. 179-181.

Розділ 1. АНАЛІЗ МЕТОДІВ АВТЕНТИФІКАЦІЇ НА ОСНОВІ НОРМАТИВНО-ПРАВОВОЇ БАЗИ УКРАЇНИ

1.1. Нормативно-правові документи України

В Україні сучасна реальність вимагає надійних та ефективних засобів захисту особистих даних, оскільки інформаційна безпека стає важливим фактором у всіх сферах життя: від державних інституцій до приватних підприємств і особистих комунікацій. В цьому контексті багатофакторна автентифікація, зокрема за допомогою біометричних ключів, визначається як передовий метод забезпечення інформаційної безпеки, що забезпечує надійний та складний доступ до систем та даних.

Останні технологічні досягнення в галузі біометрії відкривають нові можливості для ідентифікації особи на основі унікальних біологічних показників, таких як відбиток пальця, обличчя, структура радужки ока тощо. Багатофакторна автентифікація, яка комбінує кілька таких біометричних аспектів разом з іншими факторами ідентифікації, стає важливим інструментом для забезпечення високого рівня захисту інформації.

Аналіз правової бази України в контексті використання багатофакторної автентифікації за допомогою біометричних даних важливий для розуміння законодавчого статусу та регулювання цієї технології. З'ясування правових аспектів щодо захисту біометричних даних, нормативно-правового середовища для впровадження таких систем та визначення прав та обов'язків учасників цього процесу є важливим етапом у забезпеченні ефективного та законного використання цієї технології.

Отже, цей аналіз становить ключовий внесок у розвиток та впровадження багатофакторної автентифікації за допомогою біометричних ключів в Україні, сприяючи забезпеченню високого рівня захисту особистих даних та інформаційної безпеки в цифрову епоху.

Розглянемо ключові законодавчі акти, які можуть стосуватися аспектів багатофакторної автентифікації та захисту біометричних даних в Україні.

Закон України "Про захист персональних даних" встановлює загальні принципи та правила збору, обробки та захисту персональних даних громадян. Цей закон має важливе значення для забезпечення інформаційної безпеки та захисту особистих даних, включаючи біометричні дані. [1]

Цей закон встановлює рамки, в межах яких організації та установи повинні здійснювати обробку особистих даних, включаючи біометричні дані, з метою забезпечення конфіденційності та безпеки цих даних.[1]

Деякі ключові аспекти закону про захист персональних даних включають:

- Організації мають право обробляти персональні дані лише на підставі законних підстав, які можуть включати згоду суб'єкта даних або необхідність для виконання угоди чи виконання юридичних обов'язків.[1]
- Обробка персональних даних дозволяється лише для конкретно визначених, законних цілей і не може перевищувати ціль, для якої дані були зібрані.[1]
- Організації збирають ті персональні дані, які необхідні для досягнення визначених цілей обробки та обмежувати обробку лише необхідним обсягом інформації.[1]
- Закон гарантує права громадян на доступ до їх персональних даних, виправлення неточностей, видалення даних та інші права відносно контролю за їхніми даними.[1]
- Організації зобов'язані приймати необхідні технічні та організаційні заходи для захисту персональних даних від несанкціонованого доступу, втрати чи руйнування.[1]

Закон встановлює важливий фундамент для забезпечення прозорості, правової відповідальності та захисту особистих даних громадян, включаючи біометричні дані, і сприяє розвитку інформаційної безпеки в Україні.

Закон України "Про електронний документ і електронний документообіг" визначає правові засади використання електронних документів та електронного

документообігу. Цей закон включає положення, що стосуються електронної підписи, включаючи біометричну підтримку для автентифікації особи. [2]

Біометрична підтримка може означати використання біометричних даних, таких як відбиток пальця, обличчя, голос або інші унікальні біологічні параметри для створення, перевірки або підтвердження електронного підпису в документах чи у сфері електронного документообігу. Це може бути важливим аспектом в сфері інформаційної безпеки та забезпечення надійності електронних документів, оскільки біометрична підтримка може забезпечити більш високий рівень ідентифікації особи, що підписує документ чи бере участь у електронному документообігу. Закон містить норми, що встановлюють вимоги до використання біометричних параметрів у електронних підписах, їхню захищеність та правовий статус у сфері електронного документообігу. Враховуючи швидкий технологічний розвиток, законодавство може вдосконалюватися та адаптуватися до нових вимог та можливостей біометричних технологій у цьому контексті.[2]

Закон України "Про інформацію" встановлює правові норми щодо доступу до інформації, її захисту та розповсюдження. Він має значення для регулювання обробки та захисту інформації, включаючи біометричні дані. Закон містить 5 розділів. [3]

Закон України «Про доступ до публічної інформації», прийнятий 2 жовтня 2011 року, визначає правові та організаційні засади забезпечення доступу до інформації, що знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, а також порядок обмеження доступу до інформації.[4]

Цей закон є важливим гарантом права громадян на доступ до інформації, яка є основою для участі громадян у політичному, економічному та культурному житті суспільства.

Закон визначає такі основні поняття:

публічна інформація - це інформація, що знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, і стосовно якої не встановлено обмеження на доступ;[4]

розпорядник публічної інформації - це фізична або юридична особа, уповноважена законом на здійснення функцій держави або місцевого самоврядування та яка володіє публічною інформацією;[4]

запит на інформацію - це письмове звернення до розпорядника публічної інформації з проханням надати публічну інформацію, що знаходиться у його володінні.[4]

Закон передбачає право кожного на доступ до публічної інформації, крім випадків, передбачених законом.

Розпорядники публічної інформації зобов'язані надавати доступ до запитуваної інформації, якщо інше не передбачено законом.[4]

Доступ до інформації може бути обмежено лише в інтересах національної безпеки, територіальної цілісності або громадської безпеки, з метою запобігання розголошенню інформації, що становить державну таємницю, захисту комерційної таємниці, інтелектуальної власності, а також інформації про особисте життя громадян, за винятком випадків, коли це обмеження не відповідає суті конституційних прав і свобод людини і громадянина.

Обмеження доступу до інформації здійснюється шляхом віднесення інформації до категорії інформації з обмеженим доступом.

Відповідальність за порушення Закону:

За порушення Закону передбачена адміністративна, цивільна та кримінальна відповідальність.

Важливість Закону:

Закон «Про доступ до публічної інформації» є важливим кроком у напрямку утвердження в Україні демократичних цінностей та принципів відкритого суспільства. Він забезпечує громадянам право на доступ до інформації, яка є основою для їх участі у політичному, економічному та культурному житті суспільства.[5]

Сприяє підвищенню прозорості діяльності органів державної влади та місцевого самоврядування, а також сприяє боротьбі з корупцією.

Цей закон визначає правові та організаційні засади забезпечення національної безпеки України, її пріоритети, основні напрями та заходи реалізації. Національна безпека України забезпечується шляхом, зокрема, захисту інформації, що становить державну таємницю.[5]

Закон України «Про державну таємницю», прийнятий 22 травня 1994 року, визначає правові та організаційні засади забезпечення охорони державної таємниці в Україні.[6]

Державна таємниця - це інформація, що становить державну власність і збереження якої є доцільним в інтересах національної безпеки України.

Державна таємниця може бути класифікована за ступенем секретності на:

- особливо таємна;
- таємна;
- неконфіденційна.[6]

Охорона державної таємниці - це комплекс заходів, що здійснюються з метою запобігання розголошенню інформації, що становить державну таємницю.

Відповідальність за порушення Закону

За порушення Закону передбачена адміністративна, цивільна та кримінальна відповідальність.[6]

Основні вимоги Закону до захисту державної таємниці

Інформація, що становить державну таємницю, повинна бути засекречена, доступ до неї повинен бути обмежений, обробка, зберігання, транспортування та знищення інформації, що становить державну таємницю, повинні здійснюватися з дотриманням встановлених вимог.[6]

Інформація, що становить державну таємницю, може бути розсекречена за рішенням Президента України, Кабінету Міністрів України, керівника центрального органу виконавчої влади, уповноваженого на здійснення заходів

щодо охорони державної таємниці, або керівника органу, якому підпорядкований або підзвітний суб'єкт, що має доступ до державної таємниці.

Закон України «Про Державну службу спеціального зв'язку та захисту інформації України»[7]

Цей закон визначає правові та організаційні засади діяльності Державної служби спеціального зв'язку та захисту інформації України, її завдання, функції, структуру, компетенцію та порядок її взаємодії з іншими органами державної влади, органами місцевого самоврядування та фізичними і юридичними особами.[7]

Відповідно до цього закону, Державна служба спеціального зв'язку та захисту інформації України забезпечує, зокрема, захист інформації, що становить державну таємницю, та захист інформації, що є конфіденційною інформацією.[7]

Також важливо розглянути Кримінальний кодекс України (ККУ) та Кримінально-процесуальний кодекс України (КПКУ) які містять положення, які можуть стосуватися порушень інформаційної безпеки та незаконного використання біометричних даних без згоди їх власника. Наприклад, в Кримінальному кодексі України можуть бути включені статті, які передбачають кримінальну відповідальність за такі дії, як:

1. Незаконний доступ до комп'ютерних систем, мереж, баз даних тощо: Це може включати несанкціонований доступ до інформації з використанням технічних засобів без дозволу власника цієї інформації.[8]

2. Крадіжка даних або інформації: Незаконне копіювання, використання або передачі конфіденційної інформації, включаючи біометричні дані, без згоди їх власника.[8]

3. Якщо було порушено вимоги до обробки особистих даних, включаючи біометричні, це також може бути передбачено в ККУ.[8]

4. Дії, спрямовані на отримання доступу до інформації чи біометричних даних шляхом обману, також можуть бути кваліфіковані як злочини.[8]

Ці кодекси визначають різні види злочинів та встановлюють відповідні види відповідальності та покарання за порушення законодавства у сфері інформаційної безпеки та незаконного використання біометричних даних без належної згоди їх власника.

Також важливо розглянути стандарти безпеки інформації та кібербезпеки, такі як ISO 27001, які відіграють важливу роль у забезпеченні безпеки і автентифікації користувачів в інформаційних системах підприємств і організацій.[9]

ISO 27001 - це міжнародний стандарт, що встановлює вимоги до систем управління інформаційною безпекою в організаціях. Цей стандарт включає в себе широкий спектр аспектів інформаційної безпеки, у тому числі й автентифікації користувачів. ISO 27001 визначає вимоги до технічних, організаційних та правових заходів для захисту інформації від різних загроз, включаючи несанкціонований доступ та зловживання інформацією. [9]

Стандарт ISO 27001 вимагає впровадження систем управління інформаційною безпекою, які включають політики, процедури, технології та контрольні механізми для ефективного захисту інформації. Ці системи можуть також включати аспекти, пов'язані з автентифікацією користувачів, такі як управління доступом, використанням паролів, багатофакторною автентифікацією та інші методи ідентифікації та автентифікації особистості.[9]

Реалізація стандартів безпеки інформації, таких як ISO 27001, допомагає підприємствам та організаціям встановлювати та підтримувати високий рівень захисту інформації, в тому числі і заходи щодо автентифікації користувачів, що є важливим для забезпечення безпеки в інформаційних системах.

ISO/IEC 27001 є міжнародним стандартом для управління інформаційною безпекою в організаціях. Він встановлює вимоги до систем управління інформаційною безпекою (ISMS - Information Security Management System) і надає рекомендації для захисту конфіденційності, цілісності та доступності інформації.[9]

1. Організації мають ідентифікувати потенційні загрози безпеці інформації та приймати заходи для зменшення цих ризиків.
2. Розробка і впровадження політики безпеки, яка визначає цілі, вимоги та процедури для захисту інформації.
3. Це означає визначення і захист важливих активів інформації, таких як дані клієнтів, інтелектуальна власність тощо.
4. Контроль доступу до інформації та ресурсів, забезпечення правильного використання та обмеження несанкціонованого доступу.
5. Забезпечення відповідних заходів з безпеки, включаючи захист від вірусів, шифрування, безпеку мережі та інші технічні заходи.
6. Розробка планів неперервності бізнесу для забезпечення доступності інформації у надзвичайних ситуаціях або кризових ситуаціях.
7. Постійне вдосконалення системи управління інформаційною безпекою через оцінку ефективності заходів та процесів безпеки.[9]

1.2. Поняття багатофакторна автентифікація та основні фактори його використання

Багатофакторна автентифікація (MFA) - це метод захисту, який вимагає використання двох або більше факторів для підтвердження ідентичності користувача. Це може включати введення пароля, використання біометричних даних, таких як відбиток пальця або розпізнавання обличчя, або використання фізичного пристрою, наприклад, токена або смарт-карти. Багатофакторна автентифікація додає додатковий рівень безпеки, оскільки хакерам значно складніше обійти захист, який використовує кілька факторів. [10]

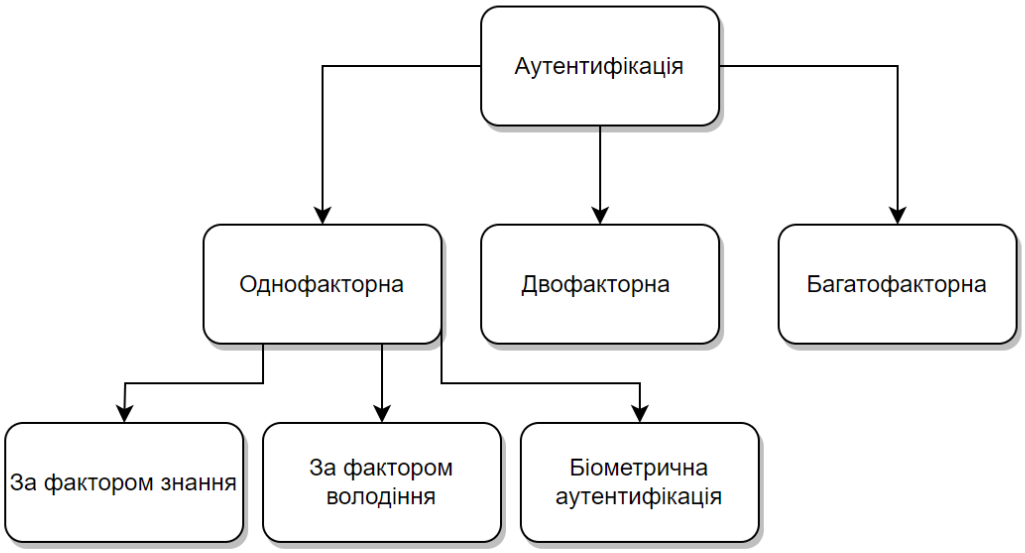


Рис.1.1. Типи автентифікації

Розглянемо, що являє собою автентифікація, а саме фактор автентифікації - це конкретний спосіб підтвердження ідентичності користувача. Багатофакторна автентифікація надає більш високий рівень безпеки порівняно з однофакторною автентифікацією, яка базується лише на паролях чи PIN-кодах.

Виділимо основні фактори автентифікації:

- Фактор знання (щось, що ви знаєте): Наприклад, пароль, PIN-код, відповідь на секретне питання, гасло чи інша інформація, яку тільки користувач повинен знати.
- Фактор володіння (щось, що ви маєте): Це може бути фізичний об'єкт, такий як смарт-карта, ключ USB або мобільний телефон, на якому генеруються одноразові паролі.
- Фактор біометричних даних (щось, що ви є): Включає сканування відбитка пальця, розпізнавання обличчя, голосу, ірису чи інших біологічних характеристик користувача.
- Фактор місцезнаходження (де ви знаходитесь): Іноді інформація про фізичне місцезнаходження користувача може бути використана для автентифікації.

MFA допомагає захищати конфіденційні дані, особисту інформацію і фінансові ресурси користувачів в онлайн-сервісах, банківських системах та корпоративних мережах. Допомагає ускладнити спроби несанкціонованого доступу до систем та послуг шляхом вимоги двох або більше незалежних методів підтвердження ідентичності. Захищає користувачів від атак, таких як перехоплення паролів, фішинг, атаки на ідентифікацію та інші види кіберзлочинності. [10]

В багатьох галузях, таких як фінансові послуги, охорона здоров'я та корпоративний сектор, MFA є обов'язковим стандартом для доступу до критичних ресурсів і даних. Відомі хмарні послуги також використовують багатофакторну автентифікацію для забезпечення безпеки користувачів та їх даних.

Багатофакторна автентифікація дозволяє підвищити рівень безпеки, оскільки вторгнення або несанкціонований доступ стають складнішими. Вона використовується в багатьох сферах, включаючи:

- Інтернет-сервіси, такі як соціальні мережі, електронні поштові скриньки, банківські системи та інтернет-магазини.
- Багато компаній вимагають від своїх співробітників використовувати MFA для доступу до корпоративних мереж, електронної пошти та інших ресурсів з метою забезпечення конфіденційності даних.
- Системи безпеки фізичного доступу до будівель, приміщень та об'єктів також можуть використовувати багатофакторну автентифікацію для забезпечення безпеки.
- Сучасні операційні системи і пристрої підтримують MFA для захисту від несанкціонованого доступу.
- MFA використовується для захисту фінансових транзакцій та особистих даних клієнтів.
- Деякі урядові організації використовують MFA для захисту конфіденційної інформації та доступу до важливих систем.

- Електронні комерційні платформи використовують MFA для захисту особистих даних та фінансових транзакцій покупців.

Багатофакторна автентифікація використовується для безпеки фінансових операцій і доступу до банківських систем в інтернеті.

1.3. Методи автентифікації

Розгляд методів автентифікації є важливою складовою в галузі кібербезпеки та захисту даних. Забезпечення безпеки доступу до систем, ресурсів та конфіденційної інформації є критичною у сучасному цифровому світі. Методи автентифікації визначають, як користувачі можуть підтвердити свою ідентичність для отримання доступу до систем та послуг. [11]

Методи автентифікації визначають основу безпеки в мережі, системі чи додатку. Вони відіграють ключову роль у захисті від несанкціонованого доступу та зловживань з боку несанкціонованих користувачів або зловмисників. Ідентифікація користувачів через методи автентифікації допомагає забезпечити безпеку конфіденційної інформації, такої як особисті дані, фінансові відомості та комерційна інформація, від несанкціонованого доступу. [12]

Метод автентифікації паролем є одним з найбільш поширених способів перевірки ідентичності користувача. При цьому, користувач вводить свій ідентифікатор (наприклад, логін) та пароль, який вже зареєстрований в системі. Система порівнює введені дані зі збереженими і, якщо вони співпадають, надає доступ до ресурсів.

Цей метод має свої переваги та недоліки. До переваг відносяться простота використання, низькі витрати на впровадження та зручність для користувачів. Однак, паролі можуть бути легко підібрані чи вкрадені, особливо якщо вони несильні або якщо користувачі використовують однакові паролі для різних сервісів.

У зв'язку з цим, рекомендується поєднувати метод автентифікації паролем з іншими методами, такими як біометрія, двофакторна автентифікація або

використання апаратних ключів. Це допоможе підвищити рівень безпеки та унеможливить несанкціонований доступ до системи.

Метод автентифікації за допомогою біометричних даних використовує унікальні фізичні характеристики користувача для підтвердження його особи. Зазвичай використовуються такі біометричні дані, як відбитки пальців, розпізнавання обличчя, сканування радужної оболонки ока або голосові відбитки.

Метод автентифікації за допомогою токена є одним з популярних способів забезпечення безпеки в системах. В цьому методі користувачу видається токен - унікальний ідентифікатор, який використовується для підтвердження його ідентичності при доступі до ресурсів або послуг.

При використанні методу автентифікації за допомогою токена, користувач зазвичай спочатку надає свої облікові дані (наприклад, ім'я користувача і пароль) для отримання токена. Потім, замість повторно вводити свої облікові дані, користувач просто представляє токен для підтвердження своєї ідентичності.

Один з важливих аспектів методу автентифікації за допомогою токена полягає в тому, що токени можуть мати обмежений термін дії. Це означає, що після закінчення терміну дії токен потрібно оновити або отримати новий токен, щоб продовжити доступ до ресурсів або послуг.

Цей метод автентифікації широко використовується в різних системах, включаючи мобільні додатки, веб-сайти, API та хмарні послуги. Використання токенів дозволяє забезпечити безпеку і зручність користувачів, а також спрощує керування доступом та забезпечення конфіденційності даних.

Автентифікація за допомогою ключ-карти - це метод автентифікації, який використовує спеціальні картки зберігання даних, відомі як ключ-карти або смарт-карти. Ключ-карти - це безпечні мікроконтролери, які здатні генерувати, зберігати та опрацьовувати криптографічні ключі. Цей метод автентифікації вимагає фізичного володіння та вставки картки в комп'ютер.

За допомогою ключ-карти здійснюється двофакторна автентифікація, оскільки вона вимагає фізичного володіння карткою та знання ПІН-коду. Ключ-

карти є досить складними для підробки, але виникали випадки взлому та клонування. Використання ключ-карт для автентифікації забезпечує високий рівень безпеки, але також може мати обмеження, такі як необхідність наявності читачів карток на кожному пристрої, вартість читачів карток, можливі зниження продуктивності та ризик втрати або поломки карток.

Шифри на основі поведінки, також відомі як шифри на основі динамічних атрибутів, є методом автентифікації, який використовує унікальні характеристики поведінки користувача для визначення його ідентичності. Цей метод заснований на припущенні, що кожна людина має свою унікальну манеру використання клавіатури, миші або смартфона.

Шифри на основі поведінки вимагають від користувача виконання певних завдань, таких як набір тексту, рухи миші або проведення по сенсорному екрану. Система аналізує ці динамічні атрибути і порівнює їх з попередньо встановленим шаблоном, щоб підтвердити особу користувача.

Один з прикладів шифрів на основі поведінки - це аналіз динаміки набору тексту. Система фіксує швидкість та час натискання на клавіші, паузи між натисканнями та інші параметри. Ці дані використовуються для побудови унікального профілю користувача. При наступному вході в систему користувач повинен повторити певний текст, і система порівнює його з попереднім профілем.

Перевагами є їх ненав'язливість та висока точність. Оскільки поведінкові характеристики складно підробити або вкрасти, цей метод автентифікації забезпечує високий рівень безпеки. Однак, варто враховувати, що цей метод може мати деяку помилковість і вимагати певного тренування для досягнення найкращих результатів. Крім того, існує питання щодо зберігання і захисту біометричних даних, оскільки їх скрадення може мати серйозні наслідки.

Автентифікація за допомогою одноразового OTP ключа - це метод автентифікації, в якому користувач отримує спеціальний код, який може використовуватися лише один раз для входу в систему. Цей код може бути

згенерований за допомогою спеціального пристрою або мобільного додатку, які синхронізуються з сервером автентифікації.

Переваги цього методу автентифікації полягають у високому рівні безпеки. Оскільки одноразовий OTP ключ може бути використаний лише один раз, його неможливо підмінити або використати повторно. Це робить його ефективним для захисту від фішингу, підманювання та інших атак.

Однак, використання одноразових OTP ключів також має свої обмеження. Користувачам необхідно мати доступ до пристрою або додатку, щоб отримати OTP код. Це може бути не зручно у випадку, коли користувач не має доступу до свого пристрою або знаходиться в обмеженому середовищі. Крім того, може виникнути проблема зі синхронізацією між сервером автентифікації і пристроєм, що використовується для генерації OTP коду.

Загалом, автентифікація за допомогою одноразового OTP ключа є потужним і ефективним методом, який забезпечує високий рівень безпеки. Втім, перед використанням цього методу необхідно враховувати його обмеження і забезпечити зручність для користувачі.

1.4. Методи шифрування інформації

Звичайне шифрування передбачає застосування математичних алгоритмів для перетворення звичайного тексту в зашифрований, який не може бути прочитаний без спеціального ключа чи пароля. Існують різні методи шифрування, кожен з яких має свої особливості і використовується у відповідних ситуаціях.

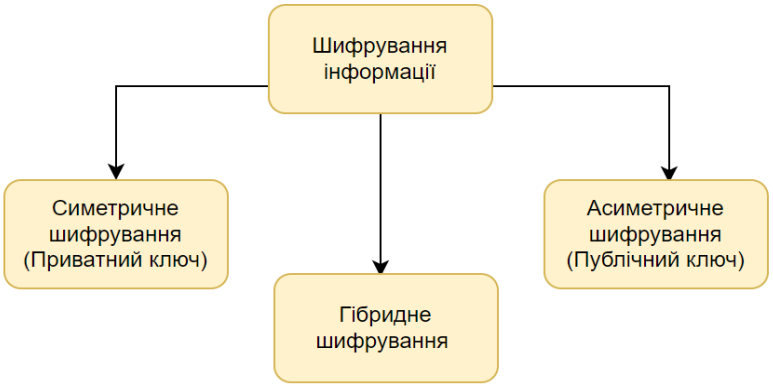


Рис.1.2. Методи шифрування інформації

Симетричне шифрування:

- Алгоритми: AES (Advanced Encryption Standard), DES (Data Encryption Standard), 3DES (Triple DES), і IDEA (International Data Encryption Algorithm).
- Принцип дії: Всі вони використовують один ключ для як шифрування, так і розшифрування. Проблема полягає в безпечному обміні ключа між сторонами.

Асиметричне шифрування (Публічний ключ):

- Алгоритми: RSA (Rivest-Shamir-Adleman), ECC (Elliptic Curve Cryptography), та DSA (Digital Signature Algorithm).
- Принцип дії: Цей метод використовує пару ключів: публічний та приватний. Публічний ключ використовується для шифрування, приватний - для розшифрування.

Гібридне шифрування:

- Принцип дії: Це комбінація симетричного та асиметричного шифрування. Зазвичай використовується симетричне шифрування для швидкості обробки даних і асиметричне - для передачі симетричного ключа.

Кожен з цих методів має свої переваги та обмеження. Важливо обрати той метод шифрування, який найкраще відповідає конкретним потребам захисту інформації в конкретній ситуації. Наприклад, асиметричне шифрування часто

використовується для безпечної передачі симетричних ключів для подальшого симетричного шифрування даних.

1.5.Порівняльний аналіз методів автентифікації

Автентифікація, як ключовий аспект інформаційної безпеки, становить основу для забезпечення доступу до цінних ресурсів, будь то дані, системи чи послуги. За останні роки зростаюча кількість кіберзагроз та технологічні інновації викликали появу різних методів автентифікації, кожен із яких має свої переваги та недоліки.

У цьому порівняльному аналізі будуть досліджені різноманітні методи автентифікації, включаючи традиційні, такі як ідентифікація за допомогою пароля, а також новіші технології, наприклад, біометричну автентифікацію та методи, що базуються на публічних ключах.

Цей аналіз надасть глибше розуміння різних методів автентифікації, їх переваг та недоліків, а також допоможе визначити, які методи найкраще відповідають конкретним потребам безпеки та які можуть забезпечити оптимальний рівень захисту для різних сценаріїв використання.

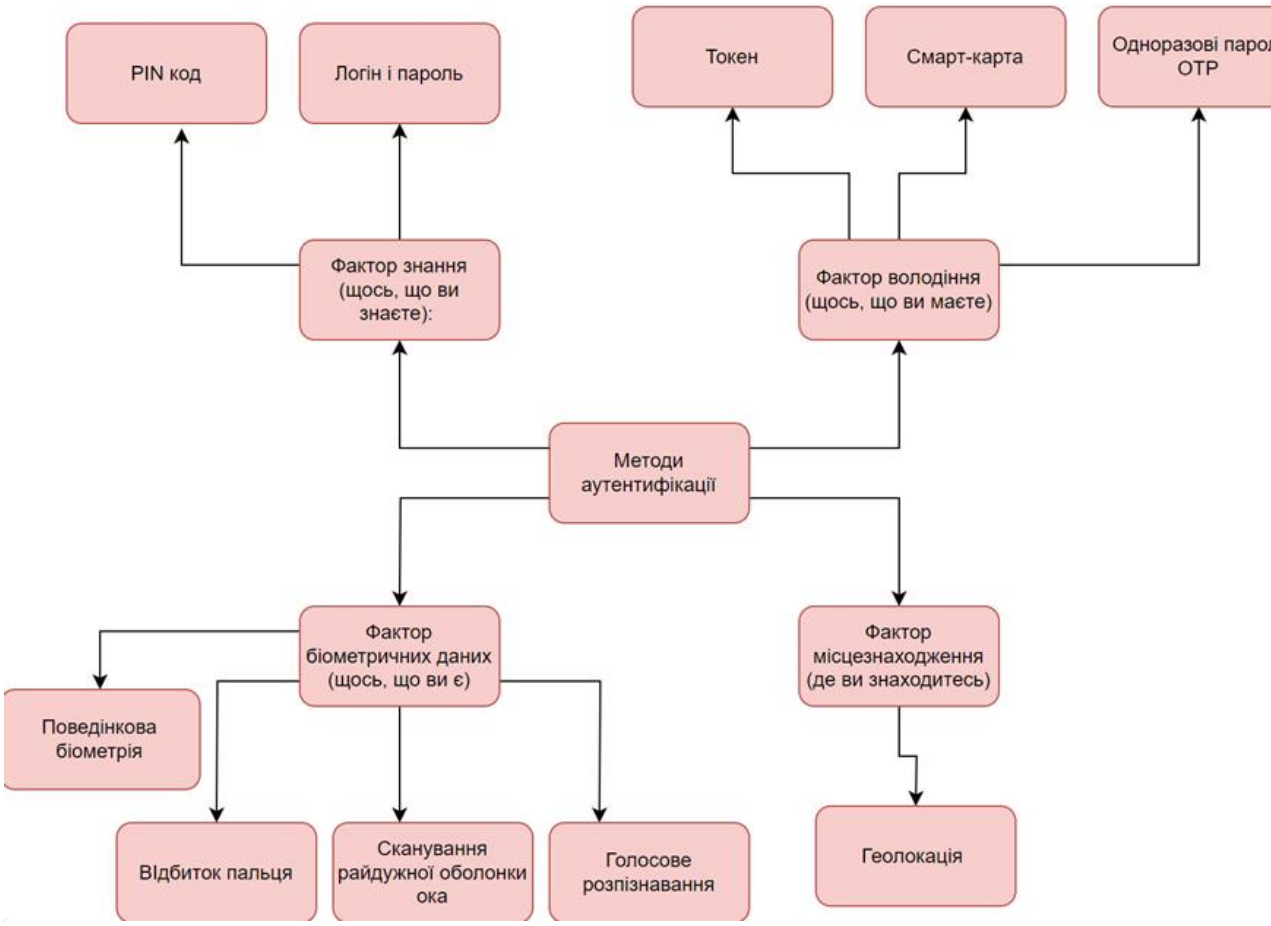


Рис.1.3. Класифікація методів автентифікації

Для порівняння методів автентифікації зробимо порівняльну таблицю:

Таблиця 1.1.

Методи автентифікації

Назва	Опис	Переваги	Недоліки
Паролі	Секретні комбінації символів, які встановлюють користувачі для доступу до системи чи облікового запису.	Просте використання, низька вартість впровадження	Потенційна слабкість, коли використовуються прості паролі; вразливість до атак перебору паролів.
Біометричні дані	Використання фізичних характеристик особи для автентифікації, таких як відбитки пальців, розпізнавання обличчя, сканування сетчатки ока і т.д.	Унікальність, важкість підробки, високий рівень безпеки.	Витрати на обладнання, можливі проблеми з приватністю та точністю.
Токени	Фізичні пристрої або програми, які генерують одноразові паролі або коди для автентифікації.	Додатковий шар безпеки, трудність вторгнення без наявності фізичного токена.	Втрата токена може стати проблемою, витрати на обладнання.
Ключ-карти	Карти або фізичні пристрої, які містять ключі для автентифікації.	Додатковий рівень безпеки, можливість легко замінити або скасувати доступ.	Витрати на виготовлення карт, можливі втрати або крадіжки.
Шифри на основі поведінки	Вивчення унікальних властивостей користувача, таких як швидкість набору тексту, стиль, тощо.	Безпека, що базується на унікальних характеристиках користувача.	Точність, можливі позитиви або відмови.

Для кваліфікаційної роботи буде використано два методи автентифікації за допомогою пароля і біометричних даних.

Комбінація паролю та біометричних даних може підвищити рівень безпеки. Використання паролю в якості одного з факторів автентифікації

забезпечує можливість створення складних та унікальних паролів для кожного користувача. Тим часом, використання біометричних даних (таких як відбиток пальця, розпізнавання обличчя або голосу) дозволяє підтверджувати ідентичність на основі унікальних фізичних характеристик, що ускладнює їхню підробку чи використання без дозволу користувача.

1.6. Висновки до першого розділу

На основі аналізу методів автентифікації за нормативно-правовою базою України визначено методи для багатофакторної автентифікації, був проведений їх порівняльний аналіз. Також ми розглянули загально методи шифрування інформації.

Було показано, що багатофакторна автентифікація є ефективним інструментом для забезпечення безпеки доступу до інформаційних активів. Вона дозволяє підвищити рівень безпеки шляхом використання декількох факторів ідентифікації, таких як пароль, біометричні дані, смарт-карти та інші. Крім того, в цьому розділі були визначені об'єкт та предмет дослідження. Об'єктом дослідження є модулі, які забезпечують вищий рівень безпеки та контролю доступу до цінних інформаційних ресурсів. Предметом дослідження є концепція та практика багатофакторної автентифікації як способу забезпечення безпеки доступу до цінних ресурсів.

Провівши аналіз було визначено, що метод автентифікації паролем і за допомогою біометричних даних є ефективним рішенням для забезпечення безпеки програмного модуля.

Розділ 2. ЗАХИСТ ПРОГРАМНОГО МОДУЛЯ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ

2.1. Визначення біометрики

Біометричні технології відіграють важливу роль у сучасному світі, створюючи унікальні можливості для ідентифікації особистості та забезпечення безпеки. Засновані на унікальних фізичних та поведінкових характеристиках кожної людини, біометричні системи дозволяють впевнено впроваджувати ефективні методи автентифікації, які виключають або мінімізують ризик несанкціонованого доступу.

Біометричні технології включають в себе різноманітні методи ідентифікації, такі як відбитки пальців, розпізнавання обличчя, сканування сетчатки ока, голосове та поведінкове визначення, які стали неодмінною частиною ряду сучасних сфер життя.

Невідомість щодо збереження конфіденційності та захисту особистих даних відкриває дебати та питання щодо приватності при використанні цих технологій. Однак відмінні характеристики біометричних даних, такі як унікальність, складність підробки та високий рівень безпеки, роблять їх привабливим інструментом для розв'язання проблем автентифікації та забезпечення безпеки в різних сферах.

У цьому контексті, дослідження та аналіз ролі біометричних технологій у сучасному світі, їхніх переваг та можливих викликів є ключовими для розуміння ефективності та потенціалу цих інноваційних засобів ідентифікації та захисту даних.

Технології використовуються в різних сферах для підтвердження ідентичності особи на основі унікальних фізичних та поведінкових характеристик.

У сфері безпеки та контролю доступу, біометричні методи, такі як розпізнавання обличчя, сканування відбитків пальців чи сетчатки ока,

застосовуються у важливих місцях, таких як аеропорти, банки, офісні приміщення та системи безпеки, для забезпечення точного та безпечного доступу.

У фінансовій сфері, біометричні технології використовуються для автентифікації платіжних транзакцій, мобільного банкінгу та ідентифікації користувачів у фінансових установах. В медичній галузі вони використовуються для ідентифікації пацієнтів та забезпечення безпеки особистих медичних даних.

Технологічні компанії використовують біометричні сенсори в смартфонах та гаджетах для розблокування пристроїв та захисту особистих даних. Вони також використовуються в урядових службах, особливо у виборчих системах, для забезпечення правдивості та достовірності виборів.

Інші застосування включають використання біометричних технологій у готельному бізнесі для автоматичного заселення гостей, у навчальних закладах для контролю доступу та в різних інших сферах життя. Всі ці застосування відображають значення біометричних технологій у забезпеченні безпеки, зручності та ефективності в сучасному світі.

2.1.1. Методи біометричної автентифікації

Метод автентифікації за допомогою біометричних даних. Їх існує велика кількість:

Відбиток пальця: Це один з найпоширеніших методів. Системи сканують та аналізують унікальні риси відбитку пальця для ідентифікації особи.

Розпізнавання обличчя: Використовує особливості геометрії обличчя або визначає його через аналіз особливих піків і впадин на обличчі.

Сканування радужки або сітківки ока: Аналізує унікальність радужки або сітківки ока. Цей метод вважається одним з найбільш надійних.

Голосовий розпізнавання: Використовує особливості голосу, такі як тон, ритм, частота і т. д., для ідентифікації особи.

Сканування долоні та вен: Аналізує унікальність структури вен у долоні або руці для ідентифікації.

Електрокардіограма (ЕКГ): Використовує особливості серцевого ритму для автентифікації.

Поведінкова біометрія: Оцінює особливості поведінки, такі як манера ходьби, рукопис, клавіатурні манери введення пароля тощо.

Таблиця 2.1.

Порівняння методів біометричної автентифікації

Метод	Опис	Надійність	Зручність в застосуванні
Відбиток пальця	Аналіз унікальних рис відбитка пальця.	Висока	Зручний і швидкий
Розпізнавання обличчя	Визначення особливостей геометрії обличчя або особливих піків і впадин на ньому.	Середня	Зручний для деяких систем
Сканування радужки/сітки	Аналіз унікальних рис радужки або сітківки ока.	Дуже висока	Складніше в застосуванні
Голосове розпізнавання	Використання особливостей голосу для ідентифікації особи.	Висока	Зручний у відповідних умовах
Сканування долоні/вен	Аналіз структури вен або долоні для ідентифікації.	Висока	Зручний і швидкий
Електрокардіограма	Використання особливостей серцевого ритму для автентифікації.	Середня	Зручний у відповідних умовах
Поведінкова біометрія	Оцінка особливостей поведінки, таких як манера ходьби, рукопис, клавіатурні манери введення пароля та ін.	Середня	Залежить від мет

Кожен метод має свої переваги і недоліки. Наприклад, відбитки пальців та розпізнавання обличчя можуть бути швидкими, але менш надійними у деяких умовах освітлення чи стану шкіри. Радужкова автентифікація може бути надійнішою, але складніше з технічної точки зору. Голосовий розпізнавання може бути вразливим до зміни тону чи захворювання голосу.

Розглянемо детальніше методи біометричної автентифікації:

Відбиток пальця - це метод біометричної автентифікації, який використовує унікальні патерни, текстуру та лінії на поверхні пальця для ідентифікації особи. Процес автентифікації на основі відбитка пальця включає сканування папіллярних ліній, розмірів та глибини відбитку. Отримані дані порівнюють з збереженими шаблонами в базі даних для підтвердження особи. Цей метод вважається досить надійним, оскільки відбитки пальців у кожної особи унікальні та майже незмінні протягом життя. Використання відбитків пальців у біометричній автентифікації широко застосовується в пристроях з контролем доступу, смартфонах, системах безпеки та інших сферах для підтвердження особистості.

Розпізнавання обличчя базується на аналізі особливостей геометрії та текстури обличчя для ідентифікації особи. Системи розпізнавання обличчя застосовують алгоритми для виділення ключових точок, контурів, пропорцій обличчя та інших унікальних особливостей, які є властивими кожній особі. За отриманими даними створюються шаблони або хеш-коди обличчя, які потім порівнюються зі збереженими у базі даних для перевірки особи. Розпізнавання обличчя широко використовується в сучасних системах безпеки, смартфонах, системах контролю доступу та відеоспостереження для ідентифікації осіб.[9]

Голосове розпізнавання використовує унікальні особливості голосу людини для ідентифікації особи. Цей процес базується на аналізі фізичних характеристик голосу, таких як тон, ритм, частота, амплітуда звуків та інтонація. Голосові дані перетворюються на числові параметри або хеш-коди, які можна порівняти зі збереженими у базі даних для автентифікації конкретної особи. Голосове розпізнавання використовується у великій кількості додатків, таких як системи голосового керування, аудіодоступу до пристроїв, телефонних систем, банківських послуг та інших сфер, де важлива ідентифікація особи за її голосом.

Сканування сітківки ока, також відомий як ретинова автентифікація, є одним з найбільш передових і надійних способів підтвердження ідентичності особи. Цей метод використовує унікальні характеристики та візуальні ознаки внутрішньої структури ока для ідентифікації особи.

Метод сканування сітківки ока використовує інфрачервоне світло низької інтенсивності для проникнення через зіницю та відображення кровоносних судин на задній стінці ока. Чітке зображення райдужної оболонки є ключовим для ідентифікації особи, тому будь-які аномалії, такі як катаракта, можуть негативно вплинути на якість ідентифікації.

Цей метод став широко вживаним у системах контролю доступу до особливо секретних об'єктів через його високу надійність. Він відзначається одним з найнижчих рівнів відмови у доступі для законних користувачів, при цьому майже ніколи не виникає помилкового надання доступу.

Незважаючи на схожість та майже однакову надійність, важливо зазначити, що цей метод не зовсім аналогічний скануванню райдужної оболонки. Використовуються різні сенсори та методи отримання образу, кожен з яких має свої вимоги та специфікації. Таким чином, вони можуть мати різні аспекти застосування та ефективності в певних умовах або середовищах.

Принцип роботи:

1. Під час процедури сканування око розглядається відмінними технологіями, які можуть використовувати освітлення, інфрачервоні промені, або використовують фотографічні методи для створення високоякісного зображення сітківки ока.

2. Сітківка ока вважається однією з найбільш унікальних частин тіла людини. Вона містить мережу кровоносних судин та нервових волокон, які утворюють унікальні візуальні ознаки, відомі як ретинові мережі.

3. Отримане зображення сітківки ока піддається аналізу алгоритмами комп'ютерного зору. Унікальні властивості сітківки ока перетворюються на числовий шаблон або біометричний "ключ", який кодується та зберігається у безпечній базі даних.

4. Під час спроби автентифікації особи система сканує сітківку ока, створює її біометричний шаблон та порівнює його з збереженим шаблоном у базі даних.

5. Якщо зразок сітківки ока співпадає з збереженим у базі, користувачу надається доступ. В іншому випадку система відмовляє в доступі.

Переваги:

1. Сітківка ока - одна з найбільш унікальних і складних для підробки біометричних характеристик.

2. Сітківка ока залишається майже незмінною протягом усього життя, що робить цей метод досить стійким.

Недоліки:

1. Використання спеціальних пристроїв для сканування та обробки зображень сітківки ока може бути дорогим.

2. Існує ризик захоплення або зламу систем, що зберігають біометричні дані, тому важливо забезпечити безпеку цих систем.

Перейдемо до більш детального розгляду автентифікації за допомогою сканування райдужної оболонки ока який я не зовсім аналогічним методом, методу сканування оболонки ока.

2.1.2. Будова райдужної оболонки ока

Райдужка, що складається з передньої частини судинної оболонки, здається тонкою та майже круглою платівкою, трохи подібною до еліпса. Близько до зіниці виділяється чорна зубчаста межа, що охоплює райдужку і представляє задній пігментний листок.

Райдужна оболонка прилягає до кришталика своєю зіничною зоною, дотикаючись до нього і вільно рухаючись по його поверхні при русі зіниці. Ця зона райдужної оболонки виступає вперед через опуклу задню поверхню кришталика, надаючи їй загальну форму висіченого конуса.

По периметру зіниці розташовується невеликий зубчастий валик, відомий як кільце Краузе або брижі. Тут райдужка має найбільшу товщину. Від цього місця в напрямку до зіниці, райдужка стає тоншою, але найтонша частина відповідає кореневі райдужки.

Кругово Краузе у стромі райдужки розташоване сплетіння судин, що називається малим кругом кровообігу райдужки. Це дозволяє виділити дві топографічні зони райдужки: внутрішню (зіничну) та зовнішню (циліарну).

На передній поверхні райдужки простежується радіальна смугастість, особливо в циліарній зоні. Це обумовлено радіальним розташуванням судин вздовж строми райдужки. По боках кільця Краузе видно щілиноподібні впадини (крипти або лакуни), які проникають у неї. Такі ж крипти, але меншого розміру, є вздовж кореня райдужки.

У зовнішньому відділі циліарної зони помітні складки райдужки, що йдуть від її кореня – контракційні борозенки або борозенки скорочення. Зазвичай вони представляють лише ділянку дуги, але не охоплюють всю райдужку. При скороченні зіниці вони стають менш помітними, при розширенні – найбільш вираженими.

Усі вищеописані структури на поверхні райдужки впливають на її малюнок та рельєф. Райдужка складається з двох листків.

Передня частина райдужки складається з переднього і судинного шарів, що є мезодермальними. Задня частина - це ретинальний шар, який є ектодермальним. У розвитку райдужки задній ектодермальний листок формує дилататор і сфінктер, два м'язи райдужки, відповідальні за розширення або стиснення зіниці.

Прикордонний шар переднього мезодермального листка складається з густої групи клітин, що розташовані паралельно поверхні райдужки, перериваючись біля краю крипта. М'язи райдужки формуються з зовнішнього шару заднього пігментного листка: сфінктер, що звужує зіницю, і дилататор, що розширює її. У процесі розвитку сфінктер переміщується у строму райдужки та розташовується біля краю зіниці, оточуючи її у вигляді кільця.

Крім того, в стромі райдужки поряд зі сфінктером розміщені великі, густо пігментовані клітини, відомі як "глибинні клітини". Ці клітини виникають у результаті зсуву пігментованих клітин з зовнішніх пігментних шарів. За

допомогою зовнішнього шару заднього пігментного листка розвивається дилататор - м'яз, який відповідає за розширення зіниці.

Дилататор райдужки залишається в тому ж місці, де утворився - в задньому пігментному листку райдужки. Він представляє собою тонку пластинку, розташовану між циліарною частиною сфінктера і основою райдужки. Клітини дилататора розташовані радіально відносно зіниці у вигляді одного шару. Ці клітини, які містять міофібрили, направлені в сторону строму райдужки, не мають пігменту і утворюють задню пластинку. Скорочення дилататора зумовлюється міофібрилами і призводить до зміни розміру та форми його клітин.

Завдяки взаємодії сфінктера і дилататора райдужна оболонка здатна рефлекторно змінювати розмір зіниці, регулюючи проникнення світла в очне яблуко. Діаметр зіниці може варіюватися від 2 до 8 мм.

2.1.3. Сканування райдужної оболонки ока

Унікальність райдужної оболонки обумовлена генетикою і виявляється навіть у близнюків. Лікарі використовують малюнок і колір райдужної оболонки для діагностики захворювань та виявлення генетичних відмінностей, що можуть впливати на розвиток деяких захворювань. Деякі хвороби можуть викликати характерні плями та зміни кольору на райдужці. Щоб зменшити вплив стану здоров'я на процес ідентифікації, в технічних системах використовують чорно-білі зображення високої роздільної здатності.

Концепція розпізнавання особи за параметрами райдужної оболонки виникла в 1950-х роках. Джон Даугман, професор Кембриджського університету, розробив технологію розпізнавання, яка використовується в Nationwide ATM. Вчені показали, що кожна райдужна оболонка унікальна, навіть у тих самих осіб, і це підтверджується програмними засобами, що здатні порівнювати скановані зображення. У 1991 році Даугман почав розробку алгоритму розпізнавання райдужної оболонки ока, а в 1994 році отримав патент на цю технологію. Згодом 22 компанії, такі як Sensar, British Telecom і японська OKI, отримали ліцензії на використання цієї технології.

Зображення райдужної оболонки, отримане при скануванні, містить більше інформації, ніж відбиток пальця. Це дозволяє розробляти надійні системи для біометричної ідентифікації особи. Для отримання візерунка райдужної оболонки ока застосовується дистанційний метод сканування.

Існують два основних підходи до розпізнавання райдужної оболонки. Перший - це виділення райдужної оболонки з зображення очей, де представлення образу може бути у вигляді кілець чи прямокутника, отриманого за допомогою перетворення координат. Другий підхід - представлення образу як матриці штрих-кодів, що відповідає райдужці.

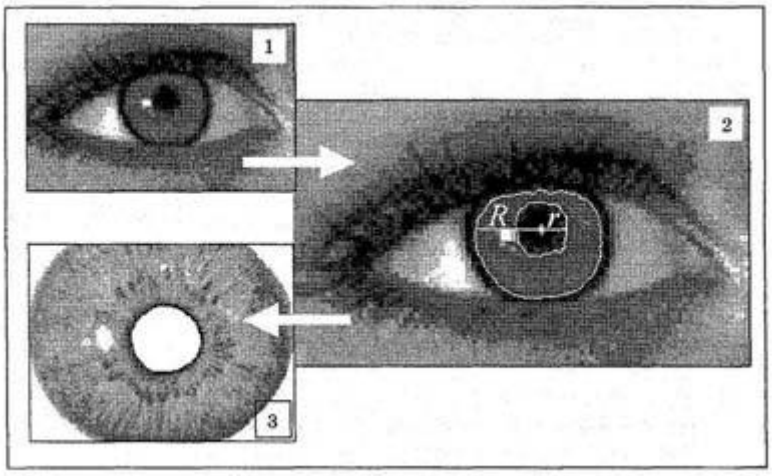


Рис.2.1. Представлення першого способу сканування райдужної оболонки ока

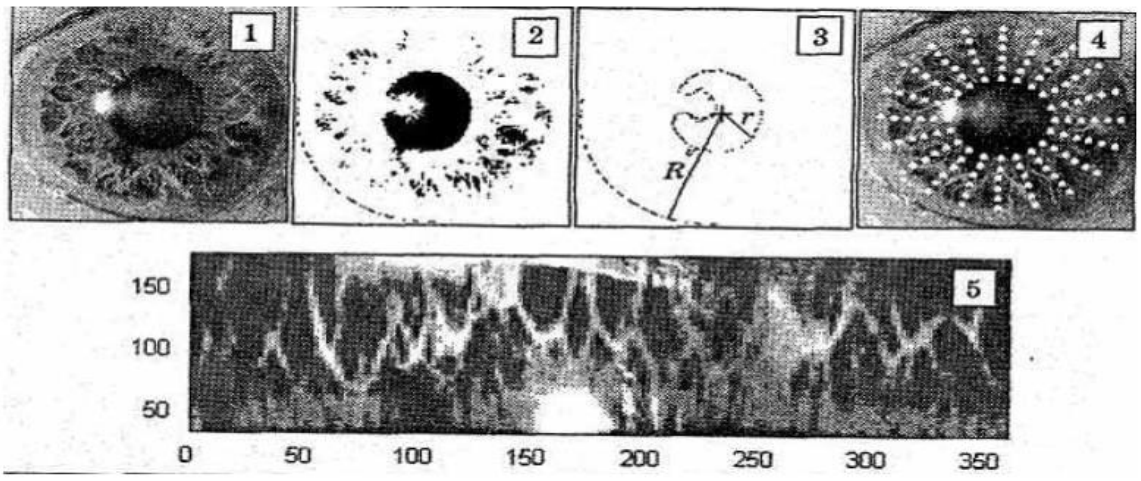


Рис.2.2. Представлення другого способу сканування райдужної оболонки ока

Системи цього типу захоплюють відео зображення очей з використанням звичайних відеокамер на відстані до одного метра. Вони автоматично виділяють зіницю та райдужну оболонку і мають високу пропускну здатність та низьку помилковість. Ці системи мають високу стійкість до різних факторів, таких як окуляри чи сонячні відблиски. Крім того, вони надійно розрізняють реальне око від муляжу.

Цей метод біометричної ідентифікації має великі перспективи для використання в комп'ютерних системах для контролю доступу, оскільки вже існують мультимедійні монітори з вбудованими відеокамерами. Такі системи можна впроваджувати за доступною ціною.

Райдужна оболонка містить більше інформації, ніж будь-який інший орган людського тіла, зокрема, вона містить 266 унікальних точок ідентифікації у порівнянні з 10-60 точками у інших біометричних методах.

Цей метод не вимагає спеціальних умов, наприклад, фокусування уваги користувача на об'єкті, оскільки райдужна оболонка розташована на поверхні ока. Порушення зору чи катаракта не впливають на точність сканування. Патентований код, який використовується у всіх комерційних системах ідентифікації, забезпечує частоту помилок приблизно 1 на 1,2 мільйона. Існуючі рішення дозволяють ідентифікувати користувача навіть при частковому затемненні або пошкодженні райдужної оболонки з ймовірністю помилки 1 до 100 тисяч. [10]

Для реалізації цього методу потрібна лише камера, яка забезпечить достатньо високу якість зображення та спеціалізоване програмне забезпечення для виділення райдужної оболонки ока. Новітні камери здатні сканувати райдужку на відстані до метра, що розширює можливості використання даного методу.

Процес роботи з фотографіями полягає у витягненні інформації про райдужну оболонку за допомогою спеціалізованих алгоритмів комп'ютерного зору та обробки зображень. Алгоритми визначають унікальність райдужної оболонки, враховуючи різноманітні візуальні характеристики, такі як структура

та розташування вен і судин, колір, геометричні особливості та інші унікальні деталі.

Цей процес включає кроки:

1. Алгоритми використовуються для виділення райдужної оболонки зі зображення. Вони можуть використовувати різні техніки обробки зображень, щоб точно визначити райдужку на фотографії.

2. Після виділення райдужної оболонки зображення обробляється для виокремлення унікальних патернів і особливостей, які будуть використані для ідентифікації конкретної особи.

3. Отримана інформація про унікальні особливості райдужної оболонки перетворюється на біометричний шаблон або код, який може бути порівняний з іншими шаблонами для ідентифікації особи.

4. Біометричний шаблон порівнюється з базою даних шаблонів райдужних оболонок для пошуку відповідності. Якщо знайдено відповідність, це дозволяє ідентифікувати особу на фотографії.

Плюси методу розпізнавання особи за райдужною оболонкою ока:

1. Унікальність ідентифікації: Кожна райдужна оболонка є унікальною, що забезпечує високий рівень точності ідентифікації особи.

2. Висока надійність: Завдяки великій кількості унікальних точок ідентифікації (до 266), цей метод забезпечує високу надійність.

3. Невимаганість спеціальних умов: Даний метод не вимагає спеціальних умов для сканування райдужної оболонки, оскільки вона розташована на поверхні ока.

4. Відносна зручність в реалізації: Для впровадження методу потрібні лише відповідні камери та програмне забезпечення, що забезпечує високу швидкість роботи та зручність в застосуванні.

Недоліки методу:

1. Витрати на обладнання: Використання спеціалізованих камер для сканування райдужної оболонки може бути вартісним, особливо для розгорнутих систем.

2. Проблеми із збереженням даних: Як і у випадку інших біометричних методів, інформація про райдужну оболонку може піддатися ризику крадіжки або несанкціонованого доступу.

3. Вплив зовнішніх факторів: Деякі фактори, такі як освітлення або певні захворювання очей, можуть вплинути на точність сканування та процес ідентифікації.

4. Приватність та етичні питання: Існує потенційний ризик порушення приватності, оскільки біометричні дані можуть стати об'єктом зловживання або незаконного використання.

Розглянемо статистичні характеристики методу:

Характеристики FAR (доля помилкових відмов) і FRR (доля помилкових прийняттів) для біометричних систем, що використовують радужку ока, є найкращими у класі сучасних біометричних систем (за винятком, можливо, методу розпізнавання по сітківці ока). У статті приведені характеристики бібліотеки розпізнавання радужкової оболонки за нашим алгоритмом EyeR SDK, які відповідають перевіреному на тих же базах алгоритму VeriEye. Використовувалися бази даних від компанії CASIA, отримані їх сканером.

FAR	FRR(Casia1)	FRR(Casia3)
0,10%	0,05%	0,08%
0,01%	0,05%	0,09%
0,00%	0,13%	0,10%
0,00%	0,13%	0,17%
0,00%	0,13%	0,19%

Рис.2.3. Характеристика FAR

Характерне значення FAR - 0,00001%. Згідно формули

$$FAR \times N^2 \approx 1 => N \approx \sqrt{\frac{1}{FAR}}, \qquad (2.1)$$

N≈3000 - кількість персоналу організації, при якій ідентифікація співробітника відбувається достатньо стабільно.

Варто відзначити важливу особливість, що відрізняє систему розпізнавання по радужці від інших систем. У разі використання камери з роздільною здатністю 1,3 МП можна захопити два очі на одному кадрі. Оскільки

ймовірності FAR і FRR є статистично незалежними, то під час розпізнавання за двома очима значення FAR буде приблизно дорівнювати квадрату значення FAR для одного ока. Наприклад, для FAR 0,001% при використанні двох очей ймовірність помилкового доступу буде дорівнювати 8-10%, при FRR лише вдвічі більше, ніж відповідне значення FRR для одного ока при FAR=0.001%.

2.1.4. Метод автентифікації паролем

Математичний аналіз методу автентифікації за допомогою пароля полягає у вивченні математичних аспектів та безпеки, пов'язаних з цим методом перевірки ідентичності користувача.

Ентропія пароля - це міра випадковості, складності та несподіваності пароля. Це концепція, яка використовується для визначення того, наскільки пароль важко вгадати або зламати. Чим більше ентропія пароля, тим відмінніше ймовірність вгадування або перебору його значення.

Ентропія пароля пов'язана з його складністю та довжиною. У загальному розумінні, чим більше символів у паролі та чим більше різних типів символів (букви верхнього та нижнього регістрів, цифри, спеціальні символи тощо), тим вища ентропія і, отже, вищий рівень безпеки пароля.

Можна визначити ентропію пароля за допомогою формул із теорії інформації, використовуючи наступний підхід:

Ентропія=$log_2(N^l)$

де:

- N - кількість можливих символів (алфавіт, які можуть входити в пароль).
- L - довжина пароля.

Ця формула визначає кількість біт інформації, яку містить пароль. Наприклад, якщо ваш пароль складається з 8 символів (наприклад, літер верхнього та нижнього регістрів, цифр та символів), то припустимо, що кожен тип символу має 64 можливих значення (загалом 26+26+10+2 = 64). Тоді N=64 і, $log_2(2^{48})$=48 біт, що означає, що цей пароль містить 48 біт інформації.

Збільшення довжини паролю або розширення множини символів (більш складні паролі) може значно підвищити ентропію та, відповідно, зробити пароль більш стійким до атак перебору або вгадування.

Також важливе обгрунтування за допомогою теорії ймовірності. Дозволяє розглядати ймовірність вгадування пароля з точки зору математичних концепцій, які оцінюють можливість успішного злому або вгадування пароля. Оцінка ймовірності вгадування пароля залежить від кількох факторів:

1. Довжина пароля: Чим довше пароль, тим складніше його вгадати. Кожен додатковий символ в паролі робить простіше вгадування значно більш складним, оскільки зростає кількість можливих комбінацій.

2. Складність пароля: Паролі, які містять різні типи символів (букви верхнього та нижнього регістрів, цифри, спеціальні символи тощо), важче вгадати, оскільки збільшується кількість можливих комбінацій.

3. Швидкість злому пароля: Визначається час, який потрібно зламати або вгадати пароль при використанні різних методів (наприклад, атаки грубої сили, словникові атаки тощо).

Чим більша довжина пароля та чим більша його складність, тим менша ймовірність того, що пароль буде вгаданий або зламаний за обмежений час.

Наприклад, припустимо, що у нас є пароль довжиною 8 символів із можливими символами латинського алфавіту верхнього та нижнього регістрів, цифрами та спеціальними символами (загалом 94 можливі символи). Ймовірність вгадування цього пароля за допомогою атаки грубої сили залежить від кількості можливих комбінацій, що дорівнює 94^8, що є вкрай великою кількістю. Отже, чим більше символів у паролі та чим більше різних символів використовується, тим менша ймовірність успішного вгадування пароля.

Також для опису використовують атаки перебору паролів, математичний аналіз заходів безпеки і інші. Математичний аналіз методів автентифікації за допомогою пароля допомагає розуміти їхню стійкість, вразливості та розробляти стратегії для підвищення рівня безпеки та уникнення можливих загроз.

2.1.5. Розрахунок коефіцієнту захисту від несанкціонованого доступу методу багатофактороної автентифікації.

На основі отриманих даних можна розрахувати загальний коефіцієнт захисту від несанкціонованого доступу описаного вище методу, для цього скористаємося формулою, яка покаже мовірність несанкціонованого доступу в послідовній струтктурі багатофакторної автентифікації по теоремі множення ймовірностей.

$$\mathrm{P_{нсд}} = \mathrm{P_в^{нсд}} \times \mathrm{P_п^{нсд}} = (1 - \mathrm{P_в}) \times (1 - \mathrm{P_п}) \qquad (2.2.)$$

$\mathrm{P_{нсд}}$–ймовірність несанкціонованого доступу;

$\mathrm{P_в^{нсд}}$–ймовірність підроблення відбитку пальця;

$\mathrm{P_п^{нсд}}$– ймовірність підроблення райдужної оболонки ока;

$\mathrm{P_в}$–ймовірність правильного використання відбитку пальця;

$\mathrm{P_п}$– ймовірність правильного використання райдужної оболонки ока.

Якщо $P_в$ - ймовірність неуспішності радужкової автентифікації, а $P_п$ - ймовірність неуспішності автентифікації за допомогою пароля, то вираз $(1- P_в)\times(1- P_п)$ визначатиме загальну ймовірність того, що обидва фактори автентифікації будуть успішними.

Для обрахунку загальної ймовірності несанкціонованого доступу при використанні сканування райдужної оболонки і пароля потрібно мати значення ймовірностей невдачі кожного окремого методу автентифікації. Нехай:

- $P_в$ - ймовірність неуспішності методу автентифікації за допомогою сканування райдужної оболонки.
- $P_п$ - ймовірність неуспішності методу автентифікації за допомогою пароля.

Загальна ймовірність несанкціонованого доступу обчислюється за формулою:

$\mathrm{P_{нсд}} = P_в \times P_п$

Для прикладу, якщо ймовірність неуспішності методу автентифікації за допомогою сканування райдужної оболонки (радужкової автентифікації) $P_в$ дорівнює 0.05 (тобто 5%), а ймовірність неуспішності автентифікації за допомогою пароля $P_п$ дорівнює 0.1 (або 10%), то:

$\mathrm{P_{нсд}}=0.05\times0.1=0.005$

Отже, загальна ймовірність несанкціонованого доступу при одночасному використанні сканування райдужної оболонки і пароля складає 0.005 або 0.5%.

2.2. Методи асиметричного шифрування

Шифрування — це технічний процес, за допомогою якого інформація перетворюється на секретний код, маскуючи дані, які ви надсилаєте, отримуєте чи зберігаєте.

Історія шифрування сягає давніх часів і має глибокі корені у забезпеченні конфіденційності комунікації та захисту від несанкціонованого доступу до інформації.

Одним з перших відомих прикладів використання шифрування було шифрування в Давньому Єгипті при пануванні фараонів. Їхні редакції щоденних записів були зашифровані у вигляді загадкових символів, що ускладнювало розшифрування іншими особами. [15]

У середньовіччі використовувалися різні методи шифрування для передачі секретної інформації. Одним із найвідоміших методів став шифр Цезаря, де кожна літера у відкритому тексті замінялася літерою, що знаходиться на певну кількість позицій в алфавіті. Цей метод дозволяв передавати повідомлення так, що воно ставало зрозумілим лише особам, які знали правило зсуву літер.[12]

Протягом історії шифрування розвивалося, з'являлися більш складні та ефективні методи, зокрема під час Другої світової війни. Тоді німці використовували шифр "Енігма" для захисту своїх комунікаційних систем. Але завдяки зусиллям британських криптоаналітиків, таких як Алан Тьюрінг, вдалося зламати цей шифр, що відіграло важливу роль у подальшому розвитку криптоаналізу та шифрування.

У другій половині 20 століття з'явилися нові шифри, такі як шифр RSA та AES, які засновані на складних математичних алгоритмах та використовуються для захисту цифрової інформації. Сьогодні криптографія є ключовою складовою кібербезпеки, забезпечуючи безпеку та конфіденційність у мережах Інтернету,

фінансових операціях, обміні конфіденційною інформацією між урядовими структурами та іншими галузями.

1. Симетричне шифрування: Використовує один ключ для як шифрування, так і розшифрування повідомлень. Приклади алгоритмів: AES (Advanced Encryption Standard), DES (Data Encryption Standard), і IDEA (International Data Encryption Algorithm).

2. Асиметричне (або публічне) шифрування: Використовує пару ключів: публічний ключ для шифрування повідомлень та приватний ключ для їх розшифрування. Приклади алгоритмів: RSA, ECC (Elliptic Curve Cryptography).

4. Гібридне шифрування: Комбінація симетричного та асиметричного шифрування для забезпечення високої швидкодії та безпеки. Наприклад, використання асиметричного шифрування для обміну симетричним ключем, який вже використовується для шифрування даних.

5. Квантове шифрування: Використовує квантові властивості частинок для передачі ключів з високим рівнем захищеності від перехоплення.

6. Протоколи шифрування комунікацій: Такі як SSL/TLS, які забезпечують безпеку під час передачі даних через мережу, зокрема в Інтернеті.

Таблиця 2.2.

Класифікація методів шифрування

Метод шифрування	Опис	Приклади алгоритмів	Рівень безпеки	Швидкодія
1	2	3	4	5
Симетричне шифрування	Використання одного ключа для шифрування та розшифрування повідомлень.	AES, DES, IDEA	Високий	Висока
Асиметричне шифрування	Використання пари ключів: публічний для шифрування та приватний для розшифрування.	RSA, ECC	Високий	Низька
Гібридне шифрування	Комбінація симетричного та асиметричного шифрування для високої	RSA + AES	Високий	Висока

	швидкодії та безпеки. Використовує асиметричне шифрування.			

Продовження табл. 2.2.

1	2	3	4	5
Квантове шифрування	Використання квантових властивостей частинок для передачі ключів із високим рівнем захисту від перехоплення.	BB84, E91	Дуже високий	Дуже висока
Протоколи шифрування	Забезпечують безпеку під час передачі даних через мережу.	SSL/TLS	Високий	Висока

Для нашої дипломної роботи використані асиметричні методи шифрування, де для підтвердження ідентичності використовують асиметричні криптографічні ключі. Ці методи часто використовуються в криптографії для забезпечення безпеки комунікацій і відомі як методи публічного ключа.

Основні методи асиметричної автентифікації включають:

1. RSA метод асиметричного шифрування ґрунтується на складних математичних операціях з великими простими числами. Він використовує два ключі — публічний (який може бути опублікований) та приватний (який лише у власника). Повідомлення, зашифроване публічним ключем, може бути розшифроване лише за допомогою відповідного приватного ключа.

2. ЕЦП метод підпису повідомлень або документів за допомогою приватного ключа для створення унікального підпису, який може бути перевірений за допомогою відкритого ключа. ЕЦП дозволяє підтверджувати автентичність повідомлення та ідентифікацію відправника.

3. DSA Цей алгоритм також використовується для створення електронних цифрових підписів, але він використовується у комбінації з асиметричними ключами для забезпечення цілісності, конфіденційності та автентифікації повідомлень.

4. ECDSA метод базується на використанні еліптичних кривих для створення електронних цифрових підписів, які мають високий рівень безпеки та ефективності.[13]

5. PKI комплексний набір процедур, політик, апаратних засобів та програмного забезпечення, що дозволяє створювати, управляти, розповсюджувати та використовувати ключі та цифрові сертифікати.

Таблиця 2.3.

Методи асиметричного шифрування

Метод	Опис	Приклади	Рівень безпеки	Складність ключів	Потужність обчислень
RSA	Використання двох ключів: публічного та приватного для шифрування та розшифрування повідомлень.	RSA	Високий	Висока	Висока
ЕЦП	Створення унікального підпису за допомогою приватного ключа, який перевіряється відкритим ключем для підтвердження автентичності повідомлення та відправника.	DSA, ECDSA	Високий	Висока	Висока
DSA	Використання для створення електронних цифрових підписів у комбінації з асиметричними ключами для забезпечення цілісності, конфіденційності	DSA	Високий	Висока	Висока
ECDSA	Використання еліптичних кривих для створення електронних цифрових підписів з високим рівнем безпеки та ефективності.	ECDSA	Високий	Висока	Висока
PKI	Комплексний набір процедур, апаратних та програмних засобів	X.509, PGP	Високий	Висока	Висока

Методи асиметричної автентифікації використовуються для забезпечення безпеки та автентифікації в інформаційних системах, електронній комунікації та технологіях, де необхідно забезпечити безпеку та довіру між сторонами.

Історія методів автентифікації свідчить про постійні зусилля створити безпечні та надійні способи перевірки особистості в цифровому середовищі.

У 20-21 столітті з'явилися технології для використання фізичних характеристик для автентифікації особистості. Це включає відбитки пальців, розпізнавання обличчя, сканування сітківки ока тощо. Введення методів асиметричного шифрування та цифрових підписів (RSA, ЕЦП) стало кроком уперед у забезпеченні безпеки комунікацій та автентифікації у цифровій епохі. Ці методи дозволяють безпечно взаємодіяти в мережі, використовуючи публічні та приватні ключі. У сучасному світі важливою частиною автентифікації є публічна інфраструктура ключів. PKI забезпечує видачу, управління та використання цифрових сертифікатів та ключів для безпечного обміну інформацією в мережах.

Розглянемо детальніше використовуваний криптографічний алгоритм RSA, який базується на математичних властивостях простих чисел, конкретно, на проблемі факторизації великих цілих чисел. Основна ідея полягає в утрудненні факторизації дуже великого числа на прості множники.[14]

RSA використовує два ключі — публічний та приватний — для шифрування та розшифрування повідомлень. Ось математичний аспект цього методу:

1. Генерація ключів:

- Вибираються два великих простих числа p та q.
- Обчислюється їхня добуток $n=p\times q$, який використовується як модуль RSA.
- Обчислюється функція Ейлера $\phi(n)=(p-1)\times(q-1)$.
- Вибирається ціле число e, яке є взаємно простим з $\phi(n)$ і менше за $\phi(n)$. Це стає публічним ключем.
- Обчислюється приватний ключ d такий, що $d\times e\equiv 1 (\mathrm{mod}\ \phi(n))$.

2. Шифрування:

- Повідомлення M перетворюється в числове представлення m.
- Шифрування відбувається за формулою: $C=M^e \bmod n$, де C — зашифроване повідомлення.

3. Розшифрування:

- Зашифроване повідомлення C перетворюється у c.
- Розшифрування відбувається за формулою: $M=C^d \bmod n$, де M — вихідне повідомлення.

Математична складність алгоритму RSA полягає у великій довжині чисел p і q та ускладненні факторизації n на прості множники, особливо коли p та q є дуже великими простими числами з десятками або сотнями цифр. Ця проблема факторизації чисел на добуток простих чисел є обчислювально складною для великих чисел і є основною основою для безпеки алгоритму RSA.

2.3. Визначення вимог до програмного модуля

Визначення вимог до програмного модуля є важливим етапом у розробці програмного забезпечення. Цей процес включає аналіз, збір та формулювання вимог, які повинен задовольняти модуль для того, щоб відповідати потребам користувачів та виконувати свої функції ефективно.

2.3.1. Визначення функціональних вимог

Функціональні вимоги визначають, як система чи програмний продукт повинен поводитися, які функції має виконувати та які операції чи сервіси мають бути надані. Вони описують функціональність системи, яка відповідає на питання "Що система повинна робити?"

Необхідність функціональних вимог полягає у визначенні конкретних функцій чи операцій, які програма чи система повинна виконувати для задоволення потреб користувачів або виконання певної бізнес-мети.

Функціональні вимоги визначають межі та поведінку системи, що є ключовим для розробки програмного забезпечення та проведення його тестування.

Розглянемо основні функціональні вимоги.

Таблиця 2.4.

Функціональні вимоги

Функціональні вимоги	Опис
1	2
Автентифікація	Можливість використання сканування райдужної оболонки ока та пароля для підтвердження ідентифікації користувача
Інтеграція зі сховищем даних	Зберігання біометричних даних (сканування райдужної оболонки) та захищене зберігання паролів
Множинна автентифікація	Підтримка можливості використання обох методів автентифікації одночасно для більшої надійності
Відновлення доступу	Механізм відновлення доступу в разі втрати або зміни біометричних даних або пароля
Повторна реєстрація	Можливість зміни, оновлення або додавання нових біометричних даних для покращення точності автентифікації
Аудит автентифікації	Запис подій автентифікації (успішних/неуспішних спроб, часу доступу тощо) для забезпечення безпеки
Захист конфіденційності	Забезпечення шифрування та безпеки передачі біометричних даних та паролів для запобігання несанкціонованому доступу
Система керування користувачами	Можливість управління правами доступу, блокуванням/розблокуванням облікових записів користувачів

Визначення функціональних вимог допоможе нам створити програмний модуль, який відповідає потребам безпеки та контролю доступу до інформаційних активів у нашій роботі.

2.3.2. Визначення нефункціональних вимог

Нефункціональні вимоги визначають характеристики і якості програмної системи, які не стосуються конкретних функцій, але важливі для її успішного функціонування і відповідності вимогам безпеки та продуктивності.

Таблиця 2.5.

Нефункціональні вимоги

Вимога	Значення
1	2
Безпека даних	- Забезпечення високого рівня захисту даних від несанкціонованого доступу та зламу. - Використання шифрування для збереження та передачі конфіденційної інформації.
Спроможність до відновлення	- Можливість швидко відновити роботу системи в разі виникнення непередбачених ситуацій або викидів.
Масштабованість	- Здатність системи обслуговувати різну кількість користувачів та об'єми даних без втрати продуктивності.
Швидкодія та продуктивність	- Забезпечення відповідної швидкодії системи, щоб користувачі не відчували затримок при автентифікації.
Доступність та надійність	- Гарантування доступності системи в усі часи та мінімізація можливих перебоїв.
Легкість використання	- Створення інтуїтивного та зручного інтерфейсу для користувачів.
Тестування безпеки та валідація	- Проведення тестів безпеки та валідації для підтвердження ефективності системи.

Ці нефункціональні вимоги допоможуть забезпечити якість, продуктивність та безпеку нашого програмного модуля та впевнитись, що він відповідає стандартам безпеки та вимогам користувачів.

2.3.3. Інші необхідні вимоги до програмного модуля

Вимоги до інтерфейсів системи багатофакторної автентифікації включають в себе опис користувацького інтерфейсу.

Таблиця 2.6.

Вимоги до інтерфейсу

Вимога	Функціонал
Користувацький інтерфейс	- Розробка інтуїтивного та зручного для користувачів інтерфейсу для введення ідентифікаційних даних. З - абезпечення можливості вибору різних методів багатофакторної автентифікації, таких як паролі, біометричні дані, одноразові паролі тощо. - Відображення інформації про стан автентифікації та сповіщення про неуспішні спроби входу.
Підтримка різних мов	- Забезпечення можливості використання різних мов та форматів для користувачів з різних регіонів.

Таблиця 2.7.

Вимоги до безпеки даних

Вимога	Функціонал
Шифрування даних	- Забезпечення шифрування всіх переданих та збережених даних, включаючи ідентифікаційні дані користувачів, паролі та біометричні дані.
Сповіщення та аудит безпеки	- Збір та збереження журналів подій для відстеження доступу користувачів та виявлення спроб несанкціонованого доступу. - Надсилання сповіщень адміністраторам та користувачам про підозрілі дії або неуспішні спроби входу.
Моніторинг та звітність	- Система моніторингу роботи програмного модуля та генерація звітів щодо подій та активності користувачів.

Вимоги до використання біометричних даних в системі мають на меті забезпечити безпеку та приватність користувачів. Оскільки біометричні дані є

особистою та неповторною інформацією, важливо дотримуватися високих стандартів захисту цих даних.

Таблиця 2.8.

Вимоги до біометричних даних

Вимога	Функціонал
1	2
Збереження біометричних даних	- Забезпечення безпеки зберігання біометричних даних та їхньої таємниці. - Використання шифрування для захисту біометричних даних в покої на стороні сервера.
Система ідентифікації та валідації	- Застосування методів ідентифікації та валідації біометричних даних для запобігання підробці.
Видалення та оновлення даних	- Можливість користувачів видаляти свої біометричні дані або оновлювати їх у будь-який момент.
Передача біометричних даних	- Захист біометричних даних під час їхньої передачі через мережу, використовуючи безпечні канали та шифрування.

Ці всі сформовані вимоги є обов’язковими під час розробки, тестування і експлуатації нашого програмного модуля.

2.4. Опис типів даних, які будуть використовуватися, їх важливість для системи.

Важливість різних типів даних в полягає в їхньому внеску у забезпечення безпеки, валідності і правильного функціонування програмного модуля, оскільки дозволяють системі перевіряти ідентичність користувачів та

відстежувати їхню активність для забезпечення безпеки доступу до інформаційних активів.

Опишимо тезисно кожен з типів даних.

Ідентифікаційні дані користувача є ключовими атрибутами, які система використовує для розпізнавання конкретної особи серед інших користувачів. Ці дані можуть включати ім'я, прізвище, логін, електронну адресу, номер користувача або будь-яку унікальну ідентифікаційну інформацію, яка відокремлює цю особу від інших в системі.

Важливість Висока.

Паролі та пін-коди використовуються для першого фактора автентифікації та мають важливе значення для захисту доступу до системи.

Важливість: Висока

Біометричні дані, скан сітківки ока, є унікальним для кожного користувача та надають високий рівень безпеки.

Важливість: Дуже висока

Одноразові паролі (OTP) мають високу важливість, оскільки вони генеруються та використовуються тільки один раз для кожної автентифікації. Вони мають обмежений строк дії, що підвищує безпеку процесу автентифікації та запобігає використанню старих паролів.

Важливість: Висока

Сертифікати та ключі шифрування використовуються для створення захищених з'єднань та підпису даних, що забезпечує безпеку інформації під час її передачі.

Важливість: Дуже висока

Логи та аудиторська інформація включають дані про активність користувачів та події, що відбуваються в системі. Ця інформація важлива для виявлення можливих спроб несанкціонованого доступу.

Важливість: Висока

Інформація про стан автентифікації включає дані про результати процесу автентифікації, такі як час, місце та використаний метод для входу в систему. Ця інформація має високу важливість для контролю та забезпечення безпеки системи.

Важливість: Висока

Дані, що визначають права та обмеження користувача після автентифікації, містить інформацію про ролі, які має користувач в системі, та набір дозволів, які він має для доступу до різних ресурсів або функцій системи. Ця інформація забезпечує контроль доступу та регулює поведінку користувачів у системі з урахуванням їхніх функціональних обов'язків та відповідальності.

Важливість: Висока

2.5. Висновки до другого розділу

У другому розділі розглянули детально, що являє собою біометрія, також провели аналіз біометричних методів, зробивши порівняльні таблиці, обрали ефективний метод сканування райдужки ока і пароля для програмного модуля. Також обрахували коефіцієнт захисту від несанкціонованого доступу який рівний 0,005, що підтверджує значну безпеку автентифікації за рахунок використання багатофакторної автентифікації.

Також розглянули детальніше методи шифрування інформації, а саме методи асиметричного шифрування, які гарантують високий рівень безпеки, забезпечуючи конфіденційність та цілісність даних у передачі. Методи асиметричного шифрування також слугують основою для створення електронних підписів, забезпечуючи автентифікацію користувача та підтвердження цілісності даних.

Провели аналіз вимог для програмного модуля, визначивши його функціональні, нефункціональні, вимоги до безпеки і інші.

Отже, обговорені методи асиметричного шифрування та біометрична автентифікація на основі сканування райдужної оболонки ока є ефективними та надійними засобами забезпечення безпеки інформації та автентифікації користувачів. Їх використання у поєднанні з іншими заходами безпеки може значно підвищити рівень захисту систем та даних.

Розділ 3. СХЕМАТИЧНА РЕАЛІЗАЦІЯ ПРОГРАМНОГО МОДУЛЯ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ

3.1. Вибір основних підходів і технологій, інструментів які будуть впроваджені у програмний модуль

Для реалізації потрібне використання спеціалізованих пристроїв для збору високороздільних зображень сітківки ока. Проведення обробки зображення, щоб виокремити сітківку ока та видалити шуми і зайві деталі. Використоння методів розпізнавання біометричних особливостей, такі як аналіз текстури та геометричних особливостей сітківки, і відповідно необхіно збереження унікальних характеристик в базі даних і використання їх для порівняння зразків при подальших автентифікаційних процедурах.

Також необхідно створити адаптивний і зручний інтерфейс користувача.

Для реалізації поставлених задач будемо використовувати мову програмування C#.

C# - це об'єктно-орієнтована мова програмування, розроблена компанією Microsoft. Вона входить до складу платформи розробки .NET (переважно в .NET Framework, .NET Core і тепер в .NET 5 і вище) і використовується для створення різноманітних програм, включаючи веб-додатки, настільні програми, ігри, мобільні додатки і багато іншого.

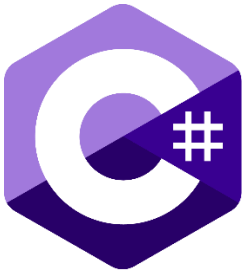


Рис.3.1. Позначення мови програмування C#

Обгрунтуємо вибір даної мови програмування для реалізації нашої задачі.

C# є мовою, яка інтегрована з платформою розробки .NET, що спрощує роботу зі збіркою сміття (garbage collection), обробкою винятків та іншими

важливими аспектами розробки. Також мова відома своєю сильною системою типів, яка допомагає уникати багатьох типових помилок в програмах, зокрема тих, які стосуються обробки біометричних даних.

У C# доступні потужні бібліотеки, які спрощують обробку зображень і біометричних даних, що є критичними для алгоритму розпізнавання сітківки ока. Також синтаксис C# вважається більш зручним для багатьох розробників, особливо для тих, хто працює з платформою Windows.

Важливо, що дана мова чудово підходить під інтеграцію з базами даних і для створення гарного інтерфейсу користувача.

Вибір бази даних для зберігання інформації, пов'язаної з розпізнаванням сітківки ока, є важливим етапом розробки нашого програмного модуля. Правильно підібрана база даних допоможе забезпечити надійне зберігання даних, їхну доступність і безпеку. Для нашої задачі чудово підійде Microsoft Sql Server

Microsoft SQL Server – це реляційна система управління базами даних (РСУБД), розроблена і підтримувана компанією Microsoft. Вона призначена для зберігання, керування та обробки даних в реляційному форматі. SQL Server є однією з найпопулярніших і потужних систем управління базами даних у світі і використовується для різноманітних застосувань, включаючи веб-додатки, корпоративні системи, звітність, аналітику та багато іншого.

Рис.3.2. Microsoft SQL Server

Важливою складовою даної бази даних є те, що можливо інтегрувати у хмарне середовище, Microsoft пропонує Microsoft Azure SQL Database, яка є повністю керованою службою для роботи з базами даних в хмарі.

Microsoft Azure ми будемо використовувати для побудови архітектури нашого програмного забезпечення, і відповідно інтеграції у хмарне середовище.

Рис.3.3. Microsoft Azure

Також розглянемо інші програми які ми будемо використовувати у процесі створення програмного продукту.

Рис.3.3. Draw.io

Draw.io - це онлайн-інструмент для створення схем, діаграм, блок-схем, організаційних структур, мережевих планів та інших візуальних представлень інформації. Це безкоштовний інструмент, який дозволяє користувачам створювати графічні візуалізації для різних потреб, від проектів інформаційних технологій до бізнес-процесів та академічних досліджень.

За допомогою цієї програми реалізуємо необхідні нам діаграми для програмної системи.

Також будуть використовуватись офісні пакети від Microsoft, а саме:

- Microsoft PowerPoint: Для створення інформативних презентацій, можна представити ключові результати та візуалізації своїх досліджень.

- Microsoft Word: використовується для написання звіту, пояснювальної записки та іншої документації, що супроводжує магістерську роботу.

Завдяки цьому різноманітному інструментарію можна здійснити розробку, тестування, аналіз та документування програмного модуля для багатофакторної автентифікації, а також презентувати результати дослідження в чіткій та зрозумілій формі. Використання цих інструментів сприяє успішному виконанню магістерської роботи та досягненню її мети.

3.2. Розробка архітектури Azure

Створення архітектури програмного продукту - це комплексний процес, що включає аналіз, планування та організацію структури системи. Його мета полягає у визначенні основних компонентів, їх взаємозв'язків та принципів взаємодії для досягнення поставлених цілей проекту. Під час розробки архітектури важливо враховувати потреби користувачів, необхідність майбутнього розширення системи, безпеку, продуктивність та інші аспекти, що впливають на ефективність роботи програмного продукту. Основною метою архітектурного процесу є створення ефективної та масштабованої структури системи, яка відповідає вимогам клієнта та забезпечує стабільну та ефективну роботу програмного продукту в майбутньому.

Архітектура Azure включає в себе створення інфраструктури, налаштування мережі, вибір підходящих сервісів та розміщення додатків у хмарі. Структура Azure може бути реалізована за допомогою встановлених патернів та практик, які надаються Azure Architecture Center

Процес роботи нашого програмного модуля можна описати покроково

1. Вхід до модуля за допомогою пароля.
2. Авторизація за допомогою пароля.
3. При вдалому вводі пароля іде запит на цифровий підпис.

4. Беремо файловий або фізичний пристрій із підписом, і для його підтвердження просить біометричну автентифікацію.

5. При вдалому вводі нас допускають до обробки даних.

Побудуємо діаграму Azure

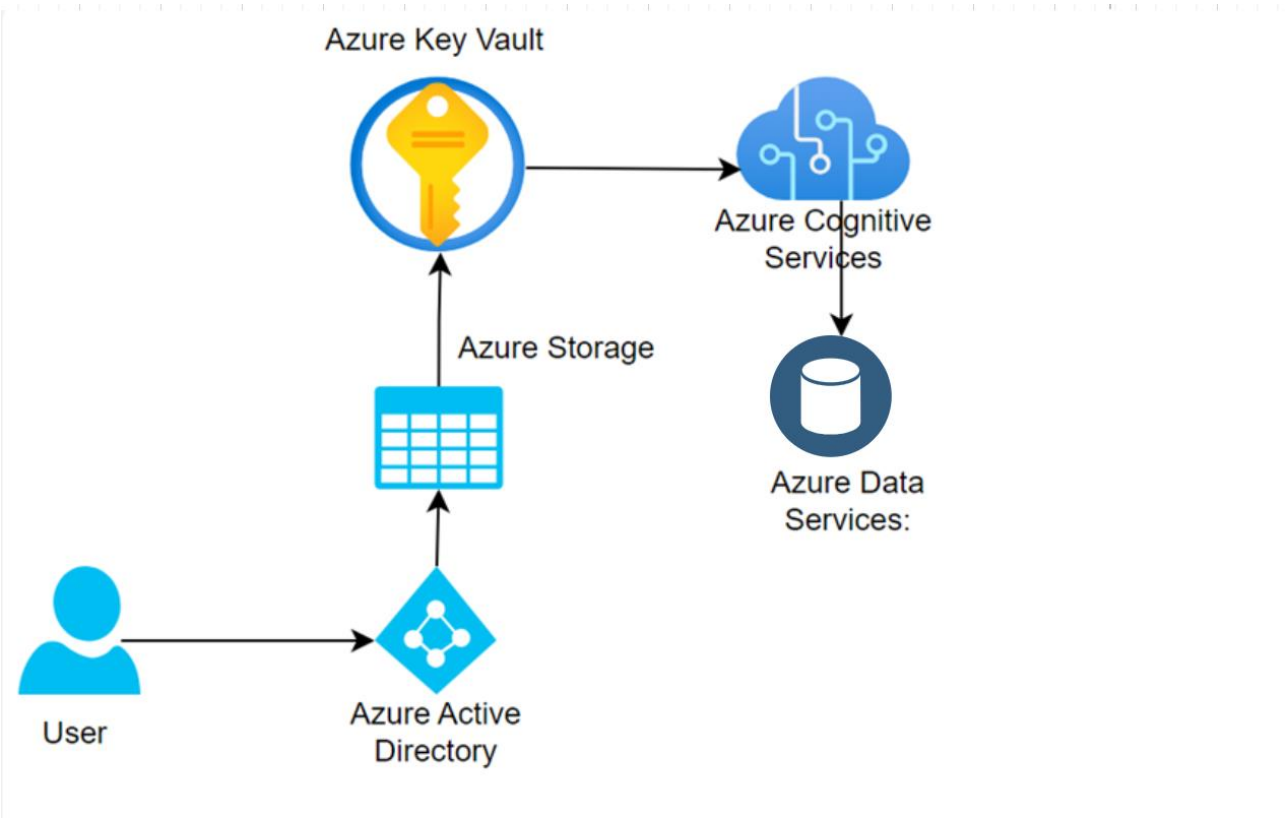


Рис.3.4. Діаграма Azure для програмного модуля

Розглянемо кожен компонент більш детальніше.

Azure Active Directory (Azure AD): Azure AD може бути використаний для автентифікації користувача за допомогою пароля. Користувачі вводять свій пароль, і Azure AD перевіряє його вірність. [4]

Azure Key Vault: Azure Key Vault може використовуватися для збереження ключів і підписів. Під час цифрового підпису Azure може використовувати Key Vault для збереження та управління ключами.

Azure Cognitive Services: Для біометричної автентифікації можна використовувати Azure Cognitive Services, такі як Azure Face API або Azure Fingerprint Recognition. Ці сервіси дозволяють виконувати біометричну автентифікацію на основі зображень обличчя, відбитків пальців тощо.

Azure Data Services: Для обробки даних можна використовувати різні Azure Data Services, такі як Azure Databricks для аналізу даних, Azure Machine Learning для машинного навчання та інші послуги для обробки та аналізу даних.

3.3. Побудова діаграм для програмної системи

Побудова діаграм для програмного модуля є важливим етапом у процесі розробки програмного забезпечення. Ці діаграми є графічними зображеннями, які надають візуальне уявлення про структуру, компоненти та взаємозв'язки модуля чи системи в цілому. Включає в себе ретельний аналіз вимог до програмного модуля та його функціональності. Визначення ключових елементів, що потрібно відобразити у діаграмах, забезпечує правильне представлення модуля та його функцій.

Створення діаграм дозволяє чітко уявити структуру модуля, його компоненти, взаємозв'язки та взаємодію з іншими частинами програми чи системи. Це сприяє кращому розумінню логіки роботи модуля, спрощує процес розробки, спільної роботи команди, а також підвищує чіткість та зрозумілість для всіх учасників проекту.

3.3.1. Діаграма класів і послідовності

Діаграма класів є важливим інструментом для візуального представлення структури та взаємозв'язків між класами в програмному коді. Ось деякі ключові причини, чому створення діаграм класів є необхідним:

Діаграма класів допомагає розуміти, як класи пов'язані між собою в програмі. Вона відображає класи, їхні атрибути та методи, а також зв'язки між класами, такі як спадкування, асоціація, агрегація та композиція. Діаграма класів може сприяти у процесі розробки програмного забезпечення, оскільки дозволяє програмістам легше розуміти внутрішню структуру системи, допомагаючи у виявленні потреби в нових класах, інтерфейсах або взаємодії між ними.

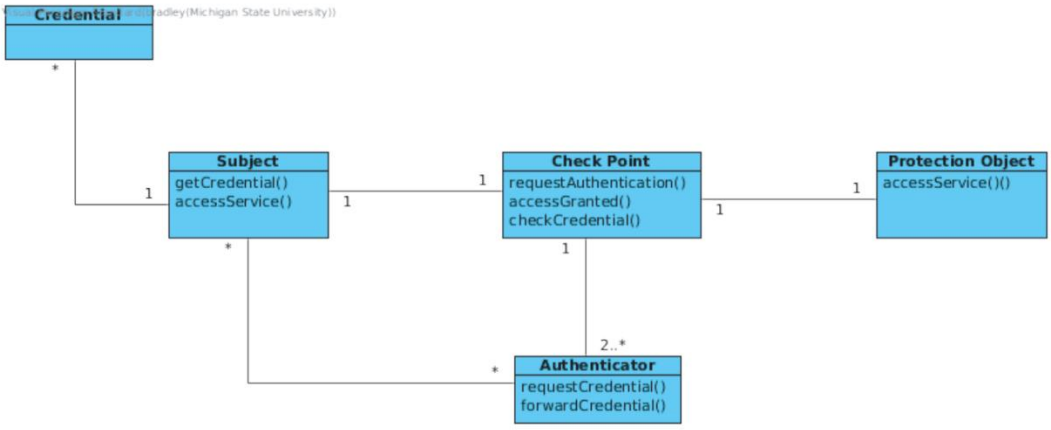


Рис.3.5. Діаграма класів для багатофакторної автентифікації

Діаграма послідовності — це тип UML-діаграми, який показує послідовність обміну повідомленнями між об'єктами або компонентами системи для виконання певної функціональності або сценарію. У випадку багатофакторної автентифікації, діаграма послідовності може відобразити взаємодію різних факторів автентифікації та системи, що виконує перевірку.

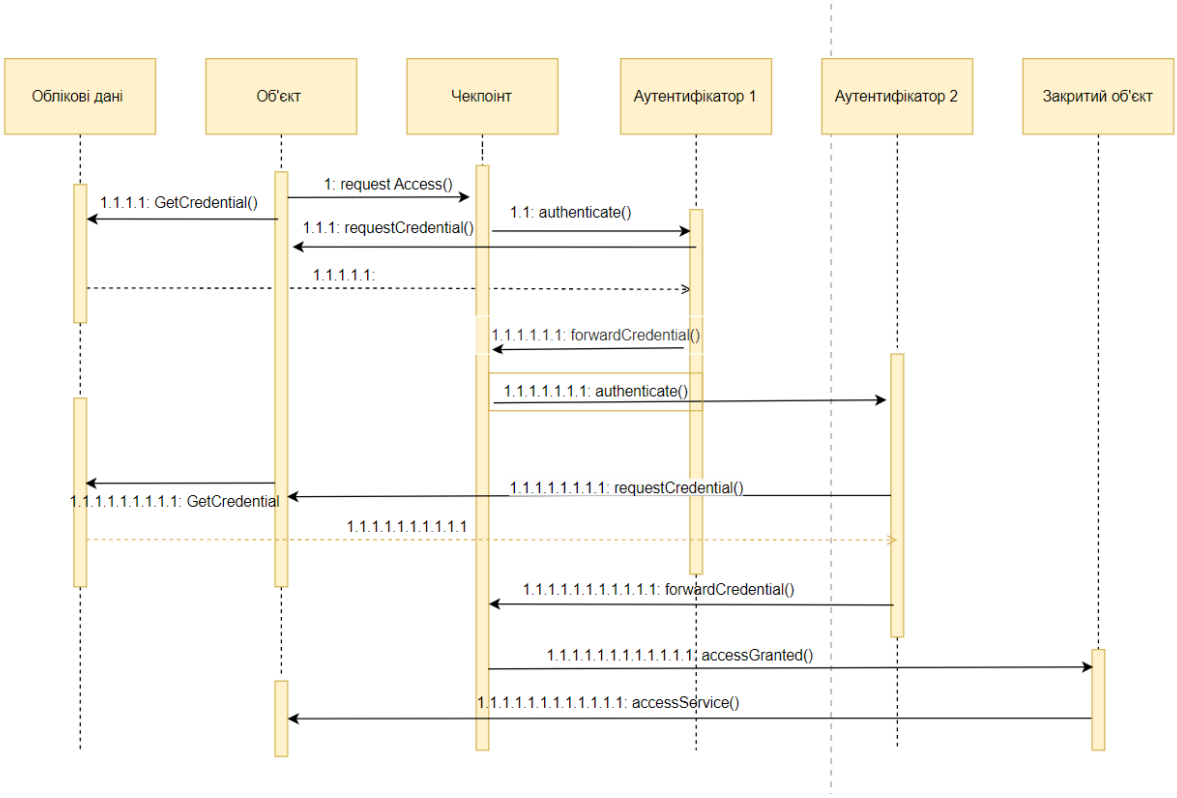


Рис.3.6. Діаграма послідовності для програмного модуля

3.3.2 Діаграма розгортання

Діаграма розгортання - це один із видів діаграм, який використовується в інженерії програмного забезпечення для візуалізації архітектури системи та

способу, як різні компоненти системи розгортаються на фізичних або логічних пристроях (серверах, віртуальних машинах, контейнерах тощо). Вона є необхідною для коректного зображення роботи нашого модуля. [5]

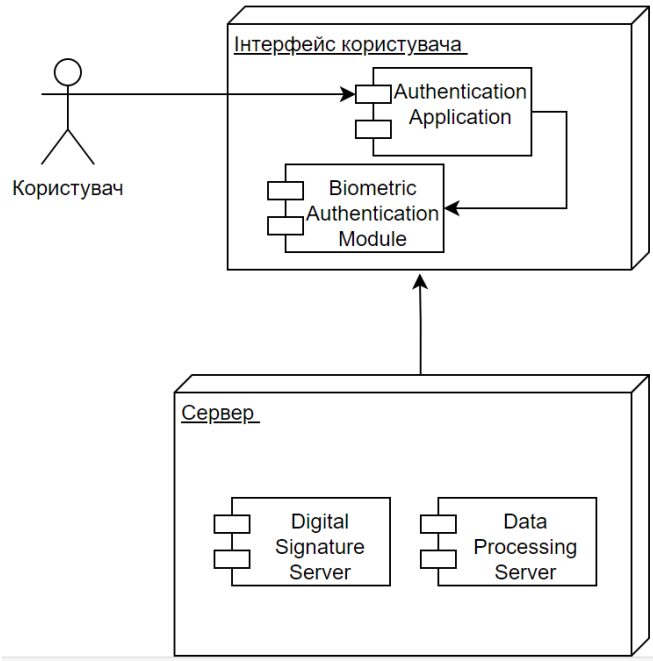


Рис.3.7. Діаграма розгортання

Користувачі взаємодіюють з системою та надають автентифікаційні дані (пароль та біометричні дані).

Інтерфейс користувача (User Interface):

- Authentication Application: В цьому компоненті відбувається автентифікація користувачів за допомогою пароля.
- Модуль для біометричної автентифікації (Biometric Authentication Module): Компонент відповідає за захоплення біометричних даних та їхню подальшу автентифікацію.

Сервер (Server):

- Сервер для цифрового підпису (Digital Signature Server): В цьому компоненті зберігаються ключі та підписи для цифрового підпису даних. Сервер обробки даних
- (Data Processing Server): Цей компонент відповідає за обробку та аналіз даних після проходження автентифікації.

Так ми показали візуально повністю роботу нашої програмної системи.

3.3.3. Проектування алгоритму роботи програми

Проектування алгоритму передбачає розробку структури та послідовності кроків, необхідних для досягнення очікуваного результату в програмі. Для візуалізації алгоритму можна використовувати різні модельні інструменти, такі як блок-схеми, псевдокод чи UML-діаграми.

Представимо алгоритм роботи програми багатофакторної автентифікації:

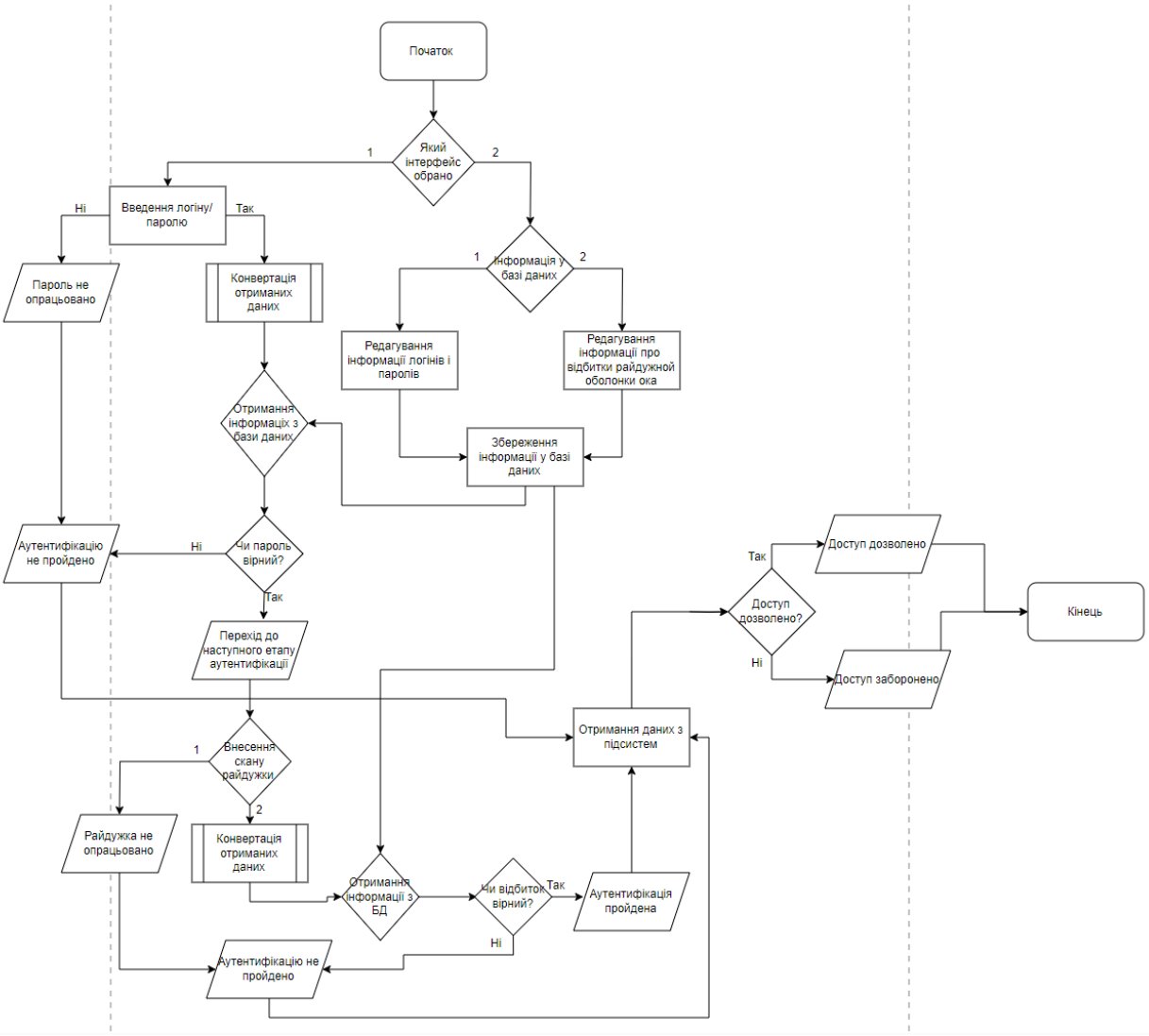


Рис.3.8. Алгоритм роботи програми багатофакторної автентифікації

- Користувач подає запит на доступ до системи, вимагаючи перевірки своєї ідентичності.
- Це є традиційний метод автентифікації, такий як пароль чи PIN-код. Система перевіряє коректність введеного пароля або іншого ідентифікатора.

- Цей фактор може включати в себе використання біометричних даних, таких як відбиток пальця, розпізнавання обличчя, голосове підтвердження або інші біометричні характеристики. Система збирає та перевіряє ці біометричні дані.
- Обидва фактори ідентифікації (наприклад, пароль і біометричні дані) перевіряються системою. Якщо обидва фактори визнані як вірні, ідентифікація користувача успішна.
- Якщо обидва фактори ідентифікації успішні, користувачеві дозволяється отримати доступ до системи. У випадку невдачі хоча б одного з факторів, доступ може бути відмовлено.
- Успішні та невдалі автентифікації фіксуються в системному журналі для подальшого аналізу безпеки та контролю доступу.

3.4. Розробка інтерфейсу користувача.

Інтерфейс користувача для програмного модулю багатофакторної автентифікації необхідно зробити зручним, інтуїтивно зрозумілим та забезпечувати безпеку під час процесу автентифікації.

Розглянемо вимоги до інтерфейсу користувача програмного модуля:

Таблиця 3.1.

Вимоги до інтерфейсу користувача програмного модуля

Вимога	Функціонал
1	2
Зручність та Інтуїтивність	- Інтерфейс є легким для розуміння і використання для будь-якого користувача без особливих технічних знань. Навігація має бути інтуїтивно зрозумілою та простою.
Адаптивність до пристроїв	- Інтерфейс є адаптованим до різних типів пристроїв (комп'ютери, планшети, мобільні телефони) та розмірів екранів.

Продовження табл.3.1.

1	2
Безпека і конфіденційність	- Забезпечення захисту конфіденційності даних під час введення чутливої інформації (наприклад, паролів або біометричних даних). - Використання шифрування та інших методів безпеки для захисту інформації під час взаємодії з користувачем.
Система повідомлень та статусів	- Надання користувачу чітких повідомлень про статус автентифікації або помилок, які можуть виникнути під час процесу.

Користувач на вході повинен ввести логін і пароль, який береться з хмарної бази даних

Рис.3.9. Вкладка авторизації у систему

При не правильному введені логіна чи пароля, модуль повідомляє про це

Рис.3.10. Повідомлення “Не правильний логін чи пароль”

При успішній автентифікації паролем відбувається перехід до наступного етапу. До автентифікації за допомогою біометричних даних.

Рис.3.11. Автентифікація за допомогою сканування сітківки ока

При успішній автентифікації (співпадінню зображень райдужної оболнки ока), система повідомить про успішну авторизацію користувача у програмному модулі.

3.5. Реалізація компонентів програмного модуля

Для початку потрібно реалізувати автентифікацію логіном і паролем:

```
using System;
using System.Data.SqlClient;
using System.Windows.Forms;
using static System.Net.Mime.MediaTypeNames;

class Program
{
   static void Main()
   {

      // Текстове поле для введення імені користувача
      TextBox usernameTextBox = new TextBox();
      usernameTextBox.Location = new System.Drawing.Point(50, 30);
      usernameTextBox.Width = 200;
      form.Controls.Add(usernameTextBox);

      // Текстове поле для введення пароля
      TextBox passwordTextBox = new TextBox();
      passwordTextBox.Location = new System.Drawing.Point(50, 60);
      passwordTextBox.Width = 200;
      passwordTextBox.PasswordChar = '*'; // Пароль відображається символами *
      form.Controls.Add(passwordTextBox);

      // Кнопка для авторизації
      Button loginButton = new Button();
      loginButton.Text = "Вхід";
      loginButton.Location = new System.Drawing.Point(100, 100);
      form.Controls.Add(loginButton);

      // Обробник події для кнопки
      loginButton.Click += (sender, e) =>
      {
         string conStr = "Andrey_Azure_Database";
         string username = usernameTextBox.Text;
         string password = passwordTextBox.Text;

         using (SqlConnection conn = new SqlConnection(conStr))
         {
            string query = "SELECT COUNT(*) FROM UsersTable WHERE Username = @Username AND Password = @Password";

            using (SqlCommand cmd = new SqlCommand(query, conn))
            {
               cmd.Parameters.AddWithValue("@Username", username);
               cmd.Parameters.AddWithValue("@Password", password);

               conn.Open();

               int count = (int)cmd.ExecuteScalar(); // Отримуємо кількість користувачів з таким ім'ям та паролем


            }
         }
      };


   }
}
```

Рис.3.12. Авторизація паролем у систему

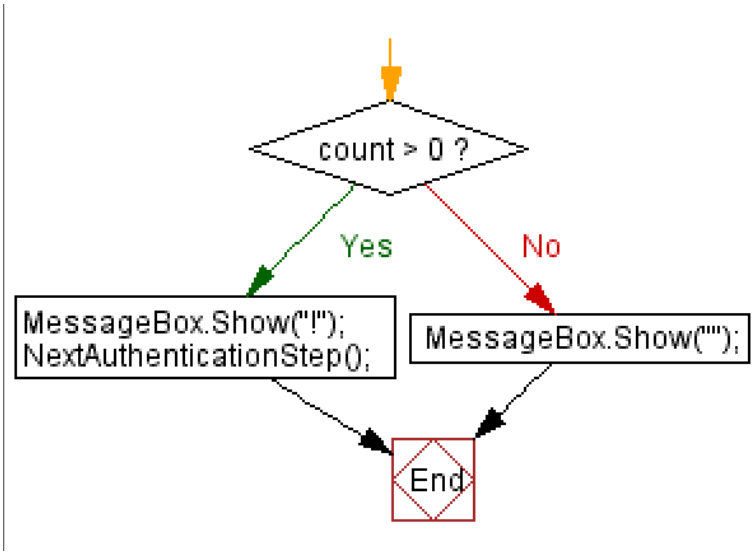


Рис.3.13. Блок-схема результату перевірки співпадіння даних

У коді створюються три елементи: два текстові поля для введення імені користувача та паролю, і кнопка для авторизації.

Кнопка має обробник події Click, який викликається при натисканні на неї. У цьому обробнику перевіряється введене ім'я користувача та пароль за допомогою SQL-запиту до бази даних Azure. Запит перевіряє наявність користувача з введеними даними. Якщо такий користувач знайдений, відбувається виклик наступного кроку автентифікації (метод NextAuthenticationStep()). У протилежному випадку виводиться повідомлення про помилку.

Реалізація ауетентифікації за допомогою біометричних даних можлива тільки за умови використання спеціального обладнання, тому ми можемо тільки описати логіку і алгоритми, уявивши, що цей сканер у нас є,

```
using System;
using System.Security.Cryptography;

namespace BiometricAuthentication
{
    public class IrisAuthentication
    {
        private readonly byte[] storedIrisData; // Збережені дані сканування райдужної оболонки ока

        public IrisAuthentication(byte[] storedIrisData)
        {
            this.storedIrisData = storedIrisData;
        }

        public bool Authenticate(byte[] scannedIrisData)
        {
            // Порівнюємо скановані дані зі збереженими
            return CompareByteArrays(storedIrisData, scannedIrisData);
        }

        private bool CompareByteArrays(byte[] array1, byte[] array2)
        {
            if (array1.Length != array2.Length)
                return false;

            for (int i = 0; i < array1.Length; i++)
            {
                if (array1[i] != array2[i])
                    return false;
            }

            return true;
        }
    }

    public class Program
    {
        public static void Main(string[] args)
        {
            // Симулюємо сканування ока
            byte[] scannedIrisData = GetScannedIrisData();

            // Збережені дані сканування райдужної оболонки ока
            byte[] storedIrisData = GetStoredIrisData();

            // Створюємо об'єкт автентифікації
            IrisAuthentication irisAuth = new IrisAuthentication(storedIrisData);

            // Проводимо автентифікацію
            bool isAuthenticated = irisAuth.Authenticate(scannedIrisData);

            // Виводимо результат автентифікації
            if (isAuthenticated)
                Console.WriteLine("Автентифікація успішна");
            else
                Console.WriteLine("Автентифікація неуспішна");
        }

        private static byte[] GetScannedIrisData()
        {
            // Зчитуємо і повертаємо скановані дані райдужної оболонки ока

            return new byte[] { 0x01, 0x02, 0x03, 0x04, 0x05 }; // Приклад даних
        }

        private static byte[] GetStoredIrisData()
        {
            // Зчитуємо і повертаємо збережені дані сканування райдужної оболонки ока
            return new byte[] { 0x01, 0x02, 0x03, 0x04, 0x05 }; // Приклад даних
        }
    }
}
```

Рис.3.14. Логіка реалізації сканування райдужної оболонки ока

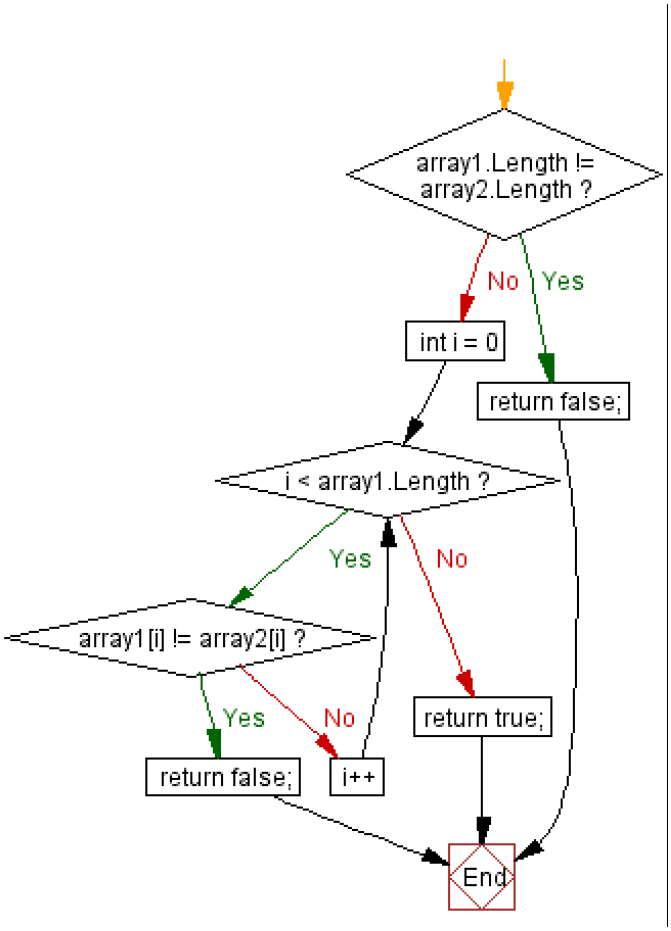


Рис.3.15. Порівняння двох масивів байтів

Розглянемо, компоненти даного коду:

IrisAuthentication - клас, який містить логіку автентифікації за допомогою сканованих даних райдужної оболонки. Конструктор цього класу приймає збережені дані сканування райдужної оболонки. Authenticate - метод класу IrisAuthentication, який порівнює скановані дані зі збереженими для проведення автентифікації. Використовується метод CompareByteArrays для порівняння двох масивів байтів.

Program - клас, який містить Main метод. У цьому методі спочатку симулюється отримання сканованих та збережених даних райдужної оболонки ока, створюється об'єкт IrisAuthentication зі збереженими даними, а потім проводиться автентифікація за допомогою методу Authenticate. Результат автентифікації виводиться на екран.

3.6. Висновки до третього розділу

Для програмного модуля багатофакторної автентифікації розробили архітектуру за допомогою компонентів Azure, також описали діаграми необхідні для чіткого розуміння роботи програми (діаграма компонентів, послідовності, розгортання), також реалізували алгоритм роботи програми. Описали інтерфейс користувача. Розробка інтерфейсу передбачає створення інтуїтивного дизайну та функціоналу, що відповідають потребам користувачів.

Процес реалізації компонентів програмного модуля включає в себе конкретне втілення цього інтерфейсу через програмні засоби. Це означає побудову елементів керування, їх програмування та забезпечення функціональності, визначеної на етапі розробки інтерфейсу.

Важливо зазначити, що успішність будь-якого програмного продукту в значній мірі залежить від якості його інтерфейсу. Грамотно спроектований та реалізований інтерфейс дозволяє користувачам ефективно та комфортно взаємодіяти з програмою чи системою, забезпечуючи задоволення від використання продукту.

Отже, розробка інтерфейсу користувача та його подальша реалізація є критичними складовими процесу розробки програмного забезпечення, спрямованими на створення зручного, функціонального та привабливого для користувача інтерфейсу.

Розділ 4. ОХОРОНА НАВКОЛИШНЬОГО СЕРЕДОВИЩА. ПРИРОДНІ ЕКОСИСТЕМИ.

Екосистема - це складна система, що складається з живих організмів (рослин, тварин, мікроорганізмів) і неживих складників середовища (ґрунт, вода, повітря), які взаємодіють між собою у певному обмеженому просторі.

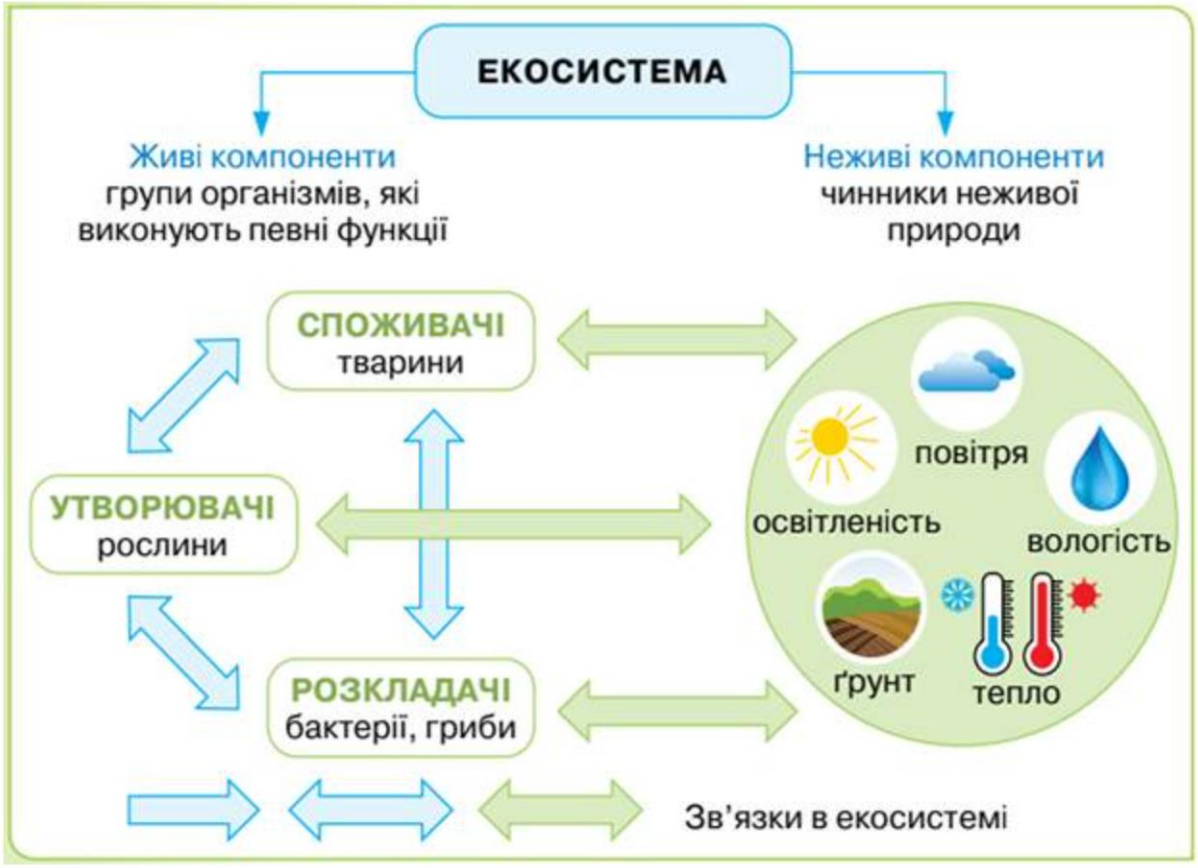


Рис.4.1. Структура екосистеми

Екосистеми можуть бути дуже різноманітними: ліси, степи, пустелі, океани, гори тощо - кожна має свою унікальну структуру, склад елементів та функції. Вони також можуть перебувати у різних станах - бути здоровими, деградованими або відновлюваними.

Центральними поняттями в екосистемі є поняття продуцентів (організмів, які виробляють органічну речовину з неорганічних речовин), споживачів (які харчуються продуцентами або іншими споживачами), та розкладачів (організмів, що розкладають органічний матеріал на неорганічні речовини).

Природні екосистеми надають значні матеріальні та нематеріальні вигоди, що мають вирішальне значення для людей. Ці екосистеми забезпечують такі переваги, як чисте повітря, утримання води, регулювання рівня води, а також запобігання повеней та пом'якшення посух. Успішність врожаїв багатьох сільськогосподарських культур залежить від комах-запилювачів, наприклад, джмелів, які розвиваються на природних територіях з великим різноманіттям трав.

Екологічні послуги, надані природними екосистемами, мають значну економічну цінність і можуть оцінюватися в грошових термінах. Громадяни, що свідомі та віддані екологічним питанням, мають важливе значення у просуванні збереження біорізноманіття та охорони природи через освітні програми та інформаційну діяльність. Урожайність більшості сільськогосподарських культур залежить від комах-запилювачів, наприклад джмелів. Для розвитку цих комах потрібні природні території з травами .

Екологічні служби сприяють підвищенню обізнаності населення та залученню людей до охорони природи через освітні програми та інформаційну роботу. Велику роль у збереженні біорізноманіття та підтриманні екологічної рівноваги відіграють природні парки та заповідники. Ці природоохоронні території також сприяють відновленню природних екосистем, що є важливим для надання екологічних послуг . Заповідники є центрами наукових досліджень, де вивчається вплив діяльності людини на види та екосистеми, а також надають екологічні послуги . Тому екологічні послуги мають вирішальне значення не лише для збереження природних екосистем, а й для проектів післявоєнної реконструкції .

Що таке біорізноманіття і чому воно важливо?

Біорізноманіття - це надзвичайно важливий аспект природи, який відображає різноманіття життя на Землі на всіх рівнях: генетичному, видовому та екосистемному. Воно охоплює різноманітність рослин, тварин, грибів та інших живих організмів, а також їхніх середовищ існування. Екосистеми, що

включають в себе це багатство біорізноманіття, є ключовими для підтримання життя на планеті.

Унікальність кожної екосистеми полягає в її різноманітті видів та функцій. Екосистеми взаємодіють між собою, утворюючи складні взаємозв'язки та взаємозалежності між різними видами. Ця взаємодія створює стійкі та стабільні системи, які забезпечують життя на планеті.

Важливість біорізноманіття полягає в його здатності забезпечувати екосистемні послуги. Екосистеми, багаті на різноманіття видів, забезпечують чисте повітря, воду та ґрунт, регулюють клімат, забезпечують запилення та полінізацію рослин, а також служать джерелом їжі та ліків.

Проте головною причиною зменшення біологічного різноманіття є діяльність людини. Руйнування середовища існування, зміна клімату та забруднення є головними загрозами для біорізноманіття. Парки та заповідники відіграють вирішальну роль у збереженні біорізноманіття шляхом захисту середовищ існування та видів та відновлення деградованих екосистем. Тому збереження біорізноманіття є необхідним для екологічно збалансованого соціально-економічного розвитку, а також для покращення стану довкілля України. Збереження та невтомне використання біорізноманіття визнано одним із пріоритетів державної політики у сфері природокористування, екологічної безпеки та охорони навколишнього середовища.

Які наслідки втрати природних екосистем?

Втрата природних екосистем має численні наслідки, які впливають не лише на довкілля, але й на здоров’я людей та економічне процвітання. Коли природні екосистеми втрачаються, послуги, які вони надають безкоштовно, також втрачаються, що призводить до необхідності платити за технології, щоб компенсувати ці втрати та втрату здоров’я через погіршення навколишнього середовища. Пошкодження є ще одним наслідком втрати природних екосистем, який може бути спричинений військовими діями, вибухами різних боєприпасів і токсичних речовин, таких як залишки вибухових речовин, нафтопродуктів і важких металів . Втрата природних екосистем також може призвести до загибелі

величезної кількості особин різних видів фауни і флори . Крім того, це може призвести до забруднення атмосферного повітря сполуками сірки, азоту, незгорілих вуглеводнів і важких металів, накопичених у біомасі . Втрата природних екосистем ставить під загрозу економічне процвітання та безпечне майбутнє, оскільки може спричинити викиди великих обсягів вуглекислого газу (CO2) і зробити неможливим проведення наукової та природоохоронної діяльності. Принесення в жертву природних екосистем заради економічного зростання може мати негативні наслідки. Воно призводить до прямої шкоди установам ПЗФ та майну заповідних установ, а також збільшенню рівня браконьєрства. Зростаюча потреба в адаптації та пом'якшенні змін клімату загострює проблему . Вплив військових дій на природні екосистеми без охоронного статусу не відрізняється від впливу на природно-заповідний фонд, що може призвести до неможливості повноцінної експлуатації об'єктів із власними адміністраціями .

Тому вкрай важливо вживати активних відновлювальних заходів для відновлення пошкоджених екосистем, оскільки відновлення природних екосистем є досить мінливим і може потребувати значного часу від десятків до більше ніж сотні років . У більшості випадків відновлення пошкоджених екосистем можна здійснити, дозволивши природі самостійно відновити збитки. Однак для відновлення екосистем, які зазнали незворотної шкоди, можуть знадобитися активні заходи відновлення .

ВИСНОВКИ

В даній кваліфікаційній роботі на тему: “Програмний модуль багатофакторної автентифікації для інформаційних активів.” висвітлено:

Проаналізовано методи автентифікації на основі нормативно-правової бази України, що дало можливість обрати найбільш ефективні методи для розробки програмного модуля захисту інформаційних активів.

На основі порівняльного аналізу криптографічних методів, методів шифрування, та біометричних методів було обрано наступне: метод пароля і метод сканування райдужної оболонки ока, як найбільш стійкими до несанкціонованого доступу до інформаціної системи

Розроблено, протестовано та проведена оцінка програмного модуля на основі програмного модуля багатофакторної автентифікації на основі райдужної оболонки ока та методу пароля для доступу до інформаційних активів, що дало можливість підвищити рівень захисту доступу до них. За розрахунком загального коефіцієнту захисту від несанкціонованого доступу він склав 99,5%

Ця робота створює фундамент для подальших досліджень у галузі кібербезпеки та автентифікації та може бути використана для розробки та впровадження програмних модулів у різних областях, де безпека та доступ до даних є критичними.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 05 липня 1994 року № 1020-XII
2. Закон України «Про державну таємницю» від 21 липня 1993 року № 3855-12
3. Закон України «Про захист персональних даних» від 01 червня 2010 року № 2297-V
4. Закон України «Про основи національної безпеки України» від 19 червня 2003 року № 964-IV
5. Закон України "Про електронні документи та електронний документообіг" від 22 травня 2004 року № 1280-IV
6. Інструкція з організації захисту інформації в інформаційних системах, що містять інформацію з обмеженим доступом, затверджена постановою Кабінету Міністрів України від 15 березня 2006 року № 268
7. ГОСТ 34.10.11-90 "Системи захисту інформації. Комплекс заходів захисту інформації. Основні положення"
8. ГОСТ Р 56926-2015 "Информационная безопасность. Защита информации. Основные термины и определения"
9. Гаврилов В.В., Гаврилова О.О., Іванов В.В. Захист інформації в інформаційно-телекомунікаційних системах. Навчальний посібник. Київ: Видавництво НТУУ "КПІ", 2015. 224 с.
10. Клебанов В.А., Сафонов В.В. Безпека інформаційних систем. Навчальний посібник. Київ: Видавництво НТУУ "КПІ", 2016. 240 с.
11. Кібербезпека: сучасні проблеми та перспективи розвитку: монографія / за ред. В.А. Клебанова. Київ: Видавництво НТУУ "КПІ", 2022. 320 с.
12. Кушнаренко Н.М., Сотникова І.В., Сидоренко В.В. Безпека інформаційних систем. Навчальний посібник. Київ: Видавництво НТУУ "КПІ", 2014. 192 с.

13. Макаренко В.А., Панасюк В.М., Таран В.В. Безпека інформаційних систем. Навчальний посібник. Київ: Видавництво НТУУ "КПІ", 2013. 208 с.
14. Морозов В.І., Піскун Н.В., Савчук В.В. Безпека інформаційних систем. Навчальний посібник. Київ: Видавництво НТУУ "КПІ", 2012. 224 с.
15. "Аналіз вимог до програмного забезпечення", автори: О. М. Поліщук, О. С. Кінаш, Т. В. Снігур, О. М. Чумак, О. М. Бєляєв.
16. "Аналіз вимог до програмного забезпечення: практичний підхід", автори: Т. Д. Ланцова, В. І. Морозов.
17. "C#: від основ до майстерності", автор: Н. А. Іванов.
18. "UML. Введення", автор: Г. Крол.
19. "UML. Проєктування програмного забезпечення"
20. Microsoft Azure documentation: Multi-factor authentication (MFA)
21. Google Cloud Platform documentation: Multi-factor authentication (MFA)
22. Amazon Web Services documentation: Multi-factor authentication (MFA)

Додаток А

Таблиця А.1.

Експертна оцінка біометричних технологій

Назва системи / Критерій	Універсальність	Відмінність	Збірність	Постійність	Продуктивність	Прийнятність	Стійкість
Відбиток пальця	A	A	B	B	A	A	B
Обличчя	A	B	A	B	B	A	B
Райдужна оболонка ока	A	A	B	A	A	B	B
Геометрія руки	A	B	A	B	A	A	A
Сітківка ока	A	A	B	A	A	C	A
Хода	A	B	A	B	C	B	B
Відбиток руки	B	A	B	A	A	B	B
Структура вуха	B	B	B	B	A	B	B
Підпис	C	C	A	B	B	A	B
Голос	B	C	B	C	B	A	C
Частота набору тексту	C	C	B	C	C	B	B

A – висока оцінка, B – середня оцінка, C – низька оцінка.

Таблиця А.1.2.

Порівняння біометричних методів за ефективністю

Критерій	Відбиток пальця	Обличчя	Райдужна оболонка ока	Геометрія руки	Сітківка	Голос	Частота набору тексту
FAR	0,001 %	0,103 %	0,009 %	2 %	0,0001%	2 %	7 %
FRR	0,001 %	0,047 %	$1*10^{-6}$ %	2 %	$1*10^{-5}$ %	10 %	0,10 %
CER	0,01 %	0,75 %	0,021 %	1 %	0,80 %	5-6 %	1,8 %
FTE	1 %	0,2 %	0,5 %	0,9 %	0,80 %	0,01%	-

Продовження додатку А

Таблиця 1.3.

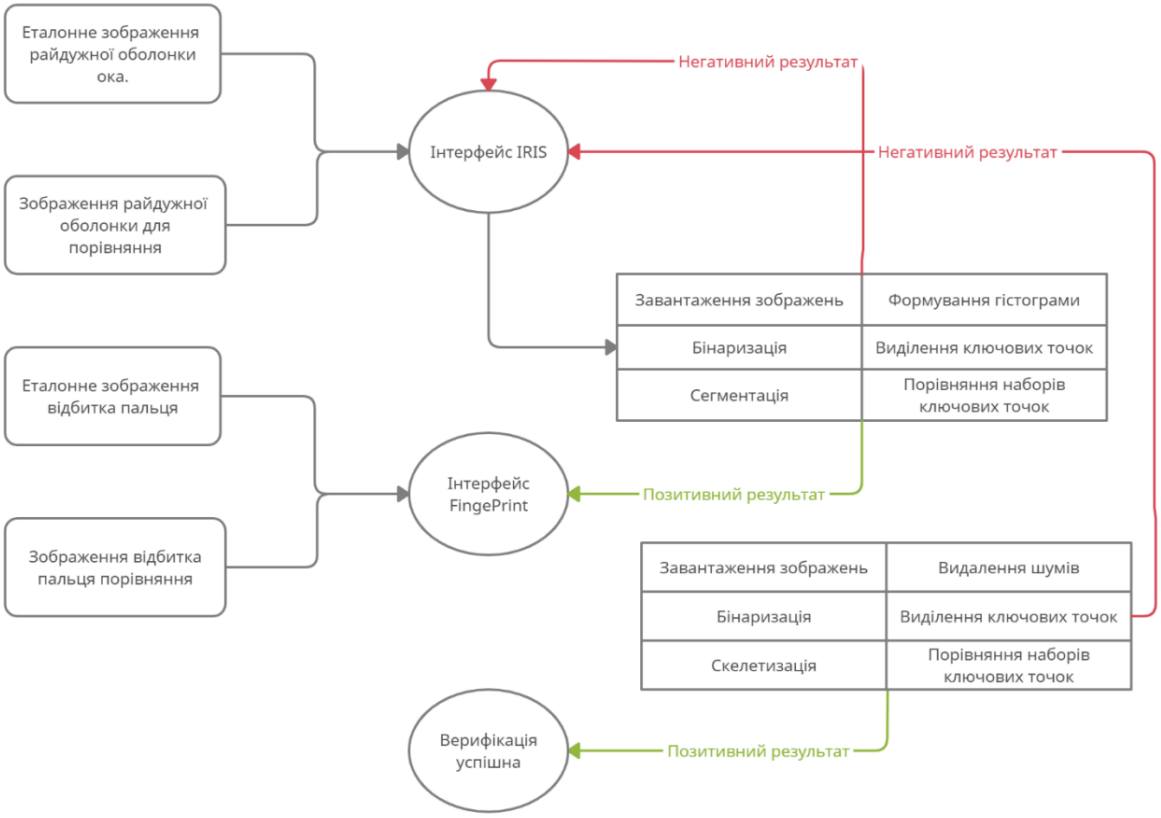
Порівняння біометричних технологій за загальними аспектами.

Аспект	Відбиток пальця	Обличчя	Райдужна оболонка	Геометрія руки	Сітківка	Підпис	Голос	Частота набору тексту
Представлений	1981	2000	1995	1986	1999	1970	1998	2005
Ціна	C	B	A	A	A	-	C	C
Популярність	A	A	A	C	C	A	B	C
Зручність	A	A	A	B	C	A	A	B
Швидкість	A	B	B	A	B	A	B	C
Безпека	B	B	A	B	A	B	B	C
Фактори помилок	Вік, вологість, забруднення, травма	Вік, освітлення, окуляри, волосся	Окуляри, погане освітлення	Вік, травма	Окуляри, контактні лінзи	Зміна підпису	Простуда, грип	Зміна клавіатури, травма пальця

A – висока оцінка, B – середня оцінка, C – низька оцінка.

Додаток Б

Загальна схема можливої програмної реалізації



Додаток В

Фрагмент коду для реалізації алгоритму шифрування RSA

```
using System;
using System.Security.Cryptography;

namespace RsaCryptoExample
{
    static class Program
    {
        static void Main()
        {
            var csp = new RSACryptoServiceProvider(2048);
            var privKey = csp.ExportParameters(true);


            var pubKey = csp.ExportParameters(false);


            string pubKeyString;
            {

                var sw = new System.IO.StringWriter();

                var xs = new
System.Xml.Serialization.XmlSerializer(typeof(RSAParameters));

                xs.Serialize(sw, pubKey);

                pubKeyString = sw.ToString();
            }


            {
                var sr = new System.IO.StringReader(pubKeyString);

                var xs = new
System.Xml.Serialization.XmlSerializer(typeof(RSAParameters));

                pubKey = (RSAParameters)xs.Deserialize(sr);
            }


            csp = new RSACryptoServiceProvider();
            csp.ImportParameters(pubKey);


            var plainTextData = "foobar";


            var bytesPlainTextData =
System.Text.Encoding.Unicode.GetBytes(plainTextData);


            var bytesCypherText = csp.Encrypt(bytesPlainTextData, false);

            var cypherText = Convert.ToBase64String(bytesCypherText);


            bytesCypherText = Convert.FromBase64String(cypherText);


            csp = new RSACryptoServiceProvider();
            csp.ImportParameters(privKey);
```

Додаток Г

Фрагмент коду переходу до наступного етапу авторизації

```
loginButton.Click += (sender, e) =>
 {
 string conStr = "Andrey_Azure_Database";
 string username = usernameTextBox.Text;
 string password = passwordTextBox.Text;

 using (SqlConnection conn = new SqlConnection(conStr))
 {
    string query = "SELECT COUNT(*) FROM UsersTable WHERE Username = @User AND Password = @Password";

    using (SqlCommand cmd = new SqlCommand(query, conn))
    {
       cmd.Parameters.AddWithValue("@User", username);
       cmd.Parameters.AddWithValue("@Password", password);

       conn.Open();

       int count = (int)cmd.ExecuteScalar();

       if (count > 0)
       {

          // Завершення автентифікації та перехід до наступного кроку
          IrisAuthenticationProcess();
       }
       else
       {
          MessageBox.Show("Не правильний логін чи пароль");
                                                                }
```