

# «ІНФОРМАЦІЙНА СИСТЕМА ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ НА ОСНОВІ БІОМЕТРИЧНИХ ДАНИХ»

Виконала: студентка групи ІСТ-18м Волошина В.А..

Керівник: к.т.н., доцент Жуков С.О.



**Об'єктом дослідження** є процес захисту інформації шляхом обмеження доступу в комп'ютерних системах.

**Предмет дослідження** — метод ідентифікації користувача за біометричними даними із подальшим розмежуванням доступу та авторизацією.

**Метою дослідження** є покращення ефективності захисту конфіденційних даних від несанкціонованих дій шляхом розмежування доступу за допомогою ідентифікації користувачів за біометричними даними.



## Задачі дослідження:

- визначено зміст та значення проблеми захисту інформації у процесі ідентифікації користувачів;
- здійснено класифікацію способів ідентифікації;
- проаналізовано недоліки та переваги існуючих підходів до ідентифікації користувачів;
- проаналізовано та обрано методи біометричної ідентифікації
- побудовано базу даних користувачів;
- розроблено програмне забезпечення та інструкцію користувача.

## Актуальність роботи:

Питання захисту інформації в комп'ютерних системах вирішується для того, щоб ізолювати нормально функціонуючу інформаційну систему від несанкціонованих управляючих дій і доступу сторонніх осіб або програм до комп'ютерних даних, що захищаються.

Щоб користувач отримав можливість працювати з програмним продуктом, його має бути авторизовано. Після цього він може запускати від свого імені процес, який інтерпретує введені ним команди і транслює їх у системні виклики, що дає йому змогу виконувати дії з файлами та користування програмним продуктом.

Потреба у дослідженні методів та засобів захисту користувача зумовлена тим, що ідентифікація користувачів є невід'ємним та важливим елементом і основою ефективності будь-якої системи управління доступом до інформаційних ресурсів комп'ютерних систем.

# Способи ідентифікації користувачів



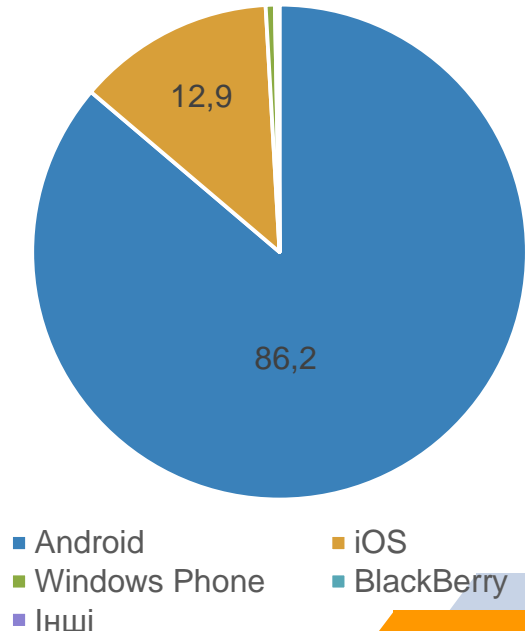
## Переваги і недоліки способів ідентифікації

| Спосіб ідентифікації                        | Парольна | Апаратна | Біометрична | Багатофакторна |
|---|----------|----------|-------------|----------------|
| Надійність                                  |          |          |             |                |
| Можливість випадкового підбору              | ■        |          |             |                |
| Можливість «підглянути»                     | ■        |          |             |                |
| Можливість передати іншій особі             | ■        | ■        |             |                |
| Поширення особистих даних (номера телефону) |          |          |             | ■              |
| Необхідний час на перевірку                 |          |          |             | ■              |
| Дороговизна                                 |          | ■        | ■           | ■              |

# Обґрунтування вибору методу біометричної ідентифікації

Кожен з наведених вище методів має недоліки, але як видно головний недолік біометричної ідентифікації є її дороговизна, адже необхідне додаткове устаткування. Вирішенням даної проблеми є ідентифікація за допомогою смартфон. Операційна система Android була обрана за даними дослідницької та консалтингової компанія Gartner, що спеціалізується на ринках інформаційних технологій.

Ринок мобільних пристроїв



# Вибір методів біометричної ідентифікації:

Серед біометричних механізмів ідентифікації можна виділити такі:

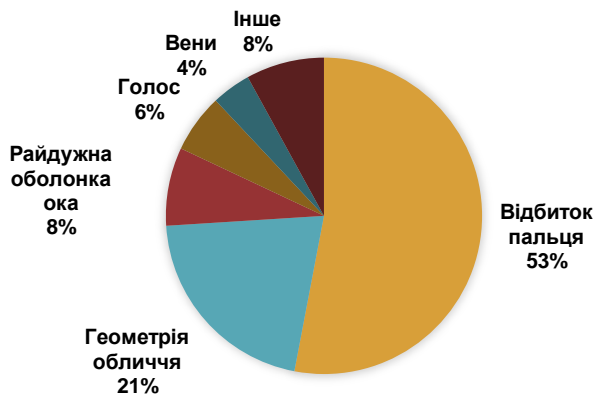
- по статичних ознаках — те, що практично не змінюється з часом, починаючи з народження людини (фізіологічні характеристики);
- по динамічних ознаках — поведінкові характеристики, тобто ті, які побудовані на особливостях, характерних для підсвідомих рухів в процесі відтворення якої-небудь дії. Динамічні ознаки можуть змінюватися з часом, але не різко, а поступово.

Основними методами, які використовують статичні біометричні характеристики людини, є ідентифікація по папілярних малюнку на пальцях, райдужній оболонці, геометрії особи, сітківці ока, малюнку вен руки, геометрії рук.

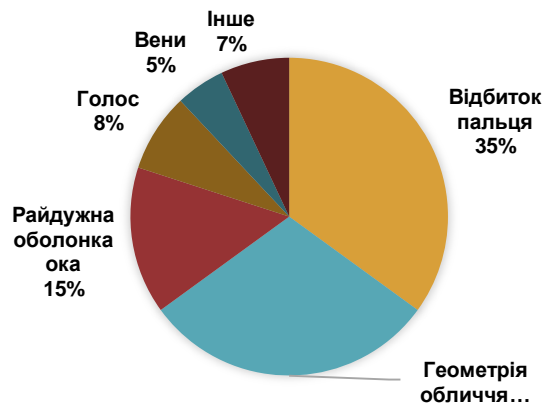
Методи, які використовують динамічні характеристики: ідентифікація по голосу, динаміці рукописного почерку, серцевого ритму, ході.



# Аналіз динаміки розвитку біометричних систем



2014 рік



2020 рік

Світовий ринок біометричних технологій.  
Динаміка розвитку. Прогноз до 2020 р.

## Вибір методів біометричної ідентифікації:

Проаналізувавши переваги та недоліки методів ідентифікації та алгоритм захисту інформації в комп'ютерних мережах на основі біометричних даних було обрано два методи ідентифікації – за відбитками пальців та за геометрією обличчя, адже за динамікою розвитку саме ці методи є найактуальнішими.

Підводячи підсумки можна сказати, що у системах, які вимагають особливих вимог до безпеки, використовуються мультимодальні методи біометричної ідентифікації. Використання біометричних засобів спрощує процедуру ідентифікації особи, а також підвищує надійність систем безпеки. Для підтвердження особи при використанні мобільного телефону, планшета або ноутбука найбільш підходящою ІТ є біометрія за відбитками пальців та геометрією обличчя.

## Вибір методів керування доступом:

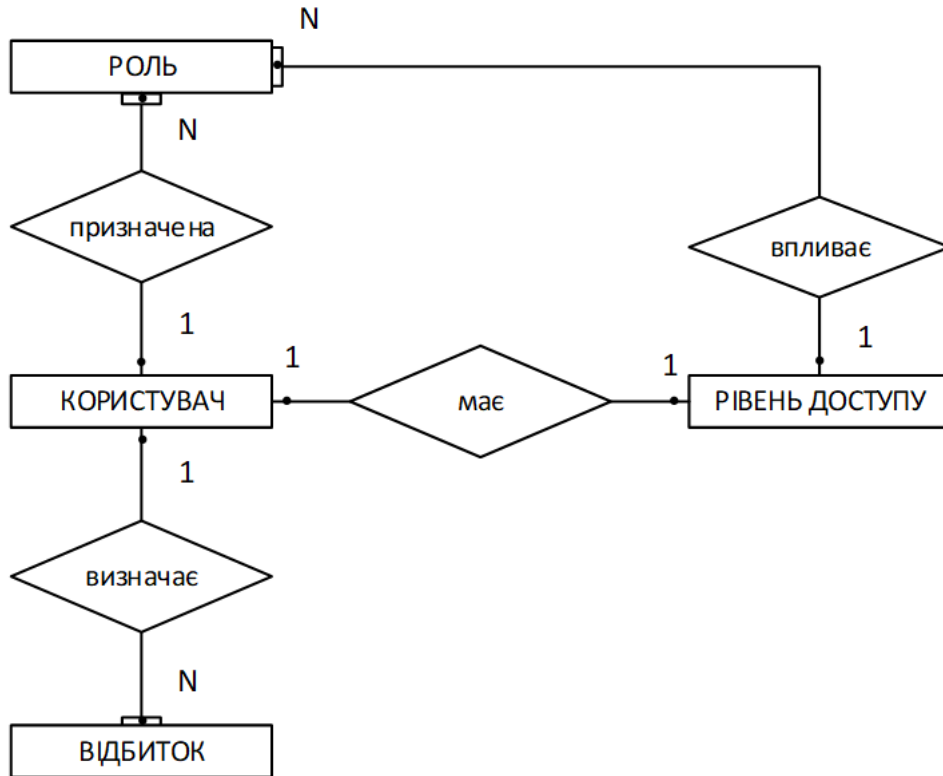
У зв'язку з інтенсивним зростанням потреби в обчислювальних і телекомунікаційних системах, розвитком комп'ютерної техніки і збільшенням числа користувачів, все більша увага приділяється питанням контролю доступу до їх ресурсів. Подібний контроль здійснюється через задані адміністратором обмеження доступу, тобто, можливості виконати певні дії, користувачів по відношенню до ресурсів системи.

У результаті проведеного аналізу технологій розмежування доступу було виявлено низку характерних особливостей, переваг і недоліків існуючих напрямів управління доступом. Визначено, що одними з найбільш перспективних напрямів є використання технології рольового розмежування доступу (англ. Role Based Access Control, RBAC).



## Керування доступом на основі ролей



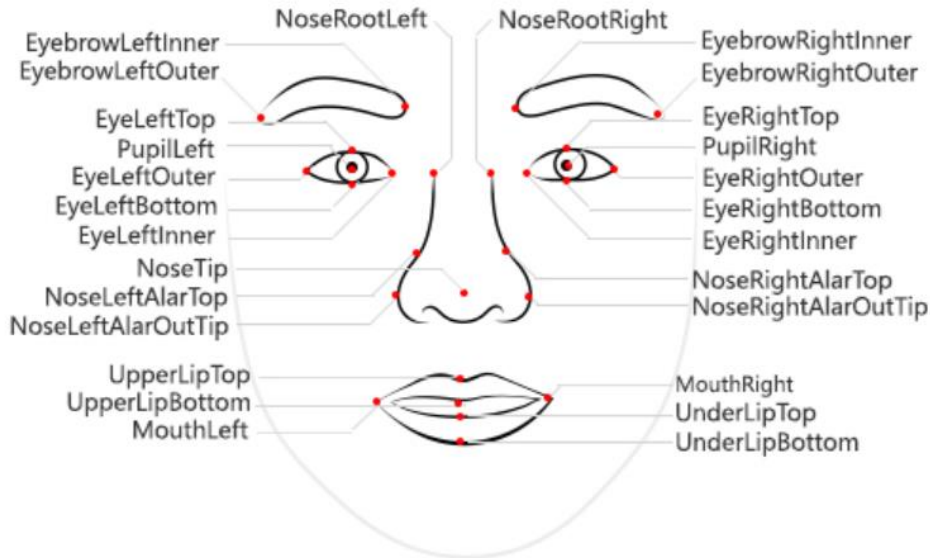


ER-модель

# Azure Face API

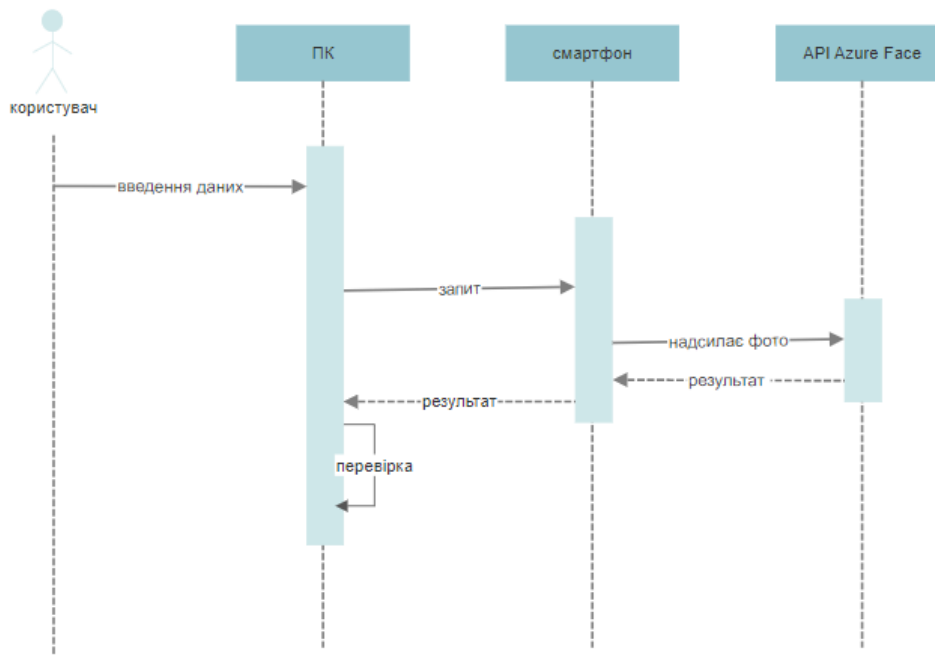
API Face Azure Cognitive Services надає алгоритми, які використовуються для виявлення, розпізнавання і аналізу людських облич на зображенні (2D). API-інтерфейс Face виявляє людські обличчя на зображенні і повертає координати. API ідентифікації використовується для ідентифікації виявленого особи по базі даних людей.

# Azure Face API

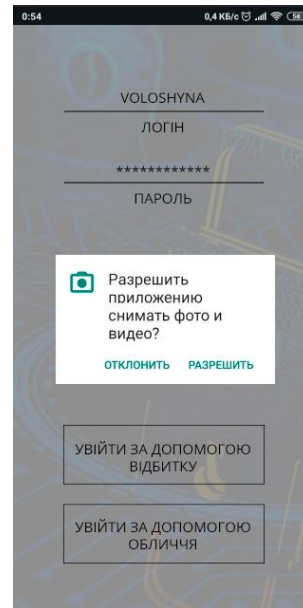
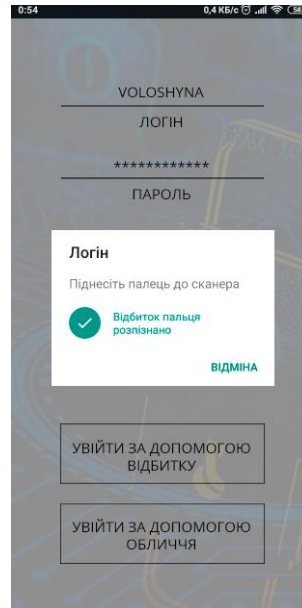
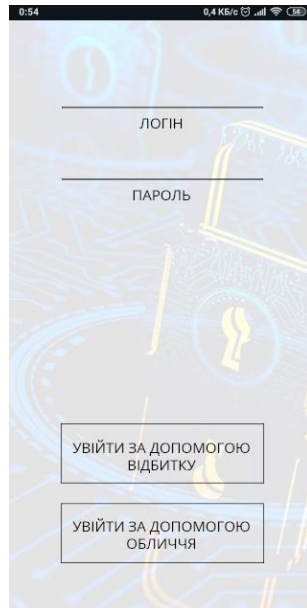


Copyright (c) Microsoft. All rights reserved

# Діаграма послідовності взаємодії ПК додатку з додатком на Android







## Висновки:

У дипломній роботі розглянуто та проаналізовано сучасні підходи до ідентифікації користувачів комп'ютерних систем, які особливо важливі у зв'язку з потребою захисту комп'ютерної інформації шляхом обмеження доступу до інформаційних та технічних ресурсів комп'ютера. Визначено недоліки і переваги кожного підходу та отримано перспективні напрями досліджень. Удосконалено існуючі засоби захисту інформаційних комп'ютерних систем від несанкціонованого доступу з боку неавторизованих користувачів шляхом управління та контролювання доступу за допомогою ідентифікації користувачів – процесом розпізнавання параметрів, що точно визначають користувача, а саме ідентифікація за біометричними даними.

**Наукова новизна** результатів дослідження полягає у вдосконаленні методу ідентифікації користувачів з подальшою авторизацією та розмежуванням доступу шляхом використання біометричних даних, а саме відбитків пальців, який, на відміну від уже створених підходів, розширює функціональні можливості засобів автентифікації, здешевлює їх та підвищує ефективність системи захисту даних.

**Практичне значення** результатів дослідження полягає у розробленні програмного модулю ідентифікації користувача через смартфон із подальшою авторизацією та розмежуванням доступу.

Результати досліджень магістерської кваліфікаційної роботи були опубліковані у збірнику доповідей XII Міжнародної науково-практичної конференції Одеської національної академії харчових технологій (ч.1 стр. 34)



**Дякую за увагу!**

