РОЗДІЛ 1

ДОСЛІДЖЕННЯ ІСНУЮЩИХ ПІДХОДІВ ДО ІДЕНТИФІКАЦІЇ ВІДБИТКІВ ПАЛЬЦІВ

* 1. **Актуальність задач ідентифікації**

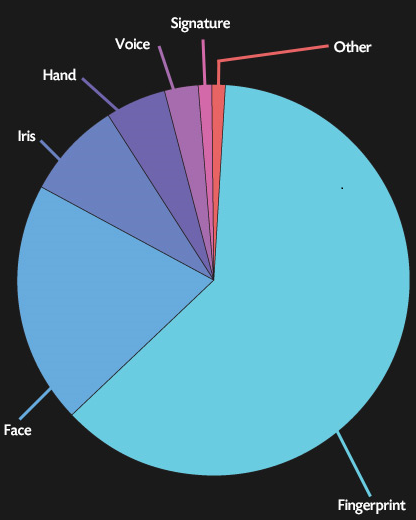
Теми ідентифікації особистості людини обумовлена активною інформатизацією сучасного суспільства та збільшенням потоків конфіденційної інформації. Аналіз сучасних систем контролю доступу свідчить про очевидний рух у бік біометричних методів завдяки їх зручності, надійності та достовірності.

Біометричною характеристикою людини (БХЛ) є її виміряна фізична або персональна поведінкова риса, в процесі порівняння якої з аналогічною БХЛ, зареєстрованою раніше, реалізується процедура розпізнавання. Як основні джерела БХЛ використовуються відбитки пальців та/або долоні, райдужна оболонка та/або сітківка очей, голос, обрис обличчя, манера роботи на клавіатурі комп'ютера, підпис тощо.

Біометричні технології (БТ) містять методи та технічні засоби рішення задач двох суттєво відмінних режимів - ідентифікації та аутентифікації особистості на основі БХЛ.

Для біометричної ідентифікації застосовуються характеристики та риси людини, які поділяють на статичні, пов'язані з її унікальними фізичними характеристиками, та динамічні, пов'язані з особливостями виконання людиною будь-яких дій. До перших належать, наприклад, відбитки пальців, форма долоні та/або розташування вен на зовнішній стороні долоні, сітківка ока, форма обличчя, термограма особи тощо. До других відносяться, наприклад, темп набирання тексту на клавіатурі комп’ютера, рукописний почерк тощо.

Так як БХЛ не можна легко підробити, вкрасти або змінити, вони вважаються більш надійними у контексті їх застосування до ідентифікації особистості людини, на відміну від традиційних підходів, що використовують електронні пластикові картки або секретні комбінації (паролі, PIN-коди тощо). Основними перевагами використання БХЛ є: зручність (наприклад, видача готівки користувачу банкомата без необхідності використання картки та PIN-коду); покращена безпека (наприклад, лише конкретна людина, яка власником даних БЛХ, має доступ до системи); легше відслідковувати, хто і коли отримував доступ до системи; вища ефективність (наприклад, відпадає необхідність зберігання та управління паролями в системі, так як БХЛ практично не змінюються і вони не можуть бути загублені). Визначний успіх технологій розпізнавання у сфері охорони порядку, зменшення вартості пристороїв для зняття відбитків, покращення та здешевлення обчислювальних можливостей, та збільшення кількості злочинів/шахрайств через проблеми ідентифікаційних систем призвели до поширення технологій розпізнавання на основі відбитків пальців у бізнесі, юридичній, урядовій та фінансовій сфері. Додатково до відбитків пальців застосовуються системи ідентифікації на основі райдужної оболонки ока, форми руки, голосу та обличчя. На Рис.1 можна побачити долі різних біометричниї технологій згідно International Biometric Group у 2009 році.



Існує два найпопулярніших способа класифікації застосувань біометричних технологій для ідентифікації: горизонтальний та вертикальний. У горизонтальній класифікації окремі категорії поєднують у собі застосування, які містять конкретні вимоги до системи розпізнавання. Вертикальна класифікація базується на вимогах окремих секторів виробництва або урядових установ. Основними категоріями горизонтальної класифікації є:

* Контроль фізичного доступу: доступ обмеженний до таких установ як АЕС, банківські сховища, роздягальні тощо
* Контроль логічного доступу: доступ до персональних комп’ютерів, серверів та баз даних дозволяється лише для конкретних авторизованих користувачів
* Автентифікація транзакцій: транзакції можуть проводитися між банком та банкоматом, або між банками. Системи розпізнавання відбитків пальців використовуються для забезпечення захищеності транзакції та відстеженнями їх учасників
* Контроль доступу до пристороїв: ноутбуки, мобільні телефони та інші електронні пристрої часто містять персональну та важливу інформацію. Для захисту цих даних використовують автоматичні системи ідентифікації відбитків (АСІВ), за допомогою яких проводиться управління доступом до пристрою.
* Час роботи та відвідуванність: системи, що відслідковують час роботи працівників використовуються на різноманітних підприємствах з метою автоматичного обрахунку заробітньої платні, згідно відробленних працівником годин, збільшення ефективності роботи та запобігання різноманітних шахрайств
* Адміністративна ідентифікація: необхідно забезпечити відсутність дуплікатів серед різноманітних документів (паспорт, водійські права тощо) та уникнути зайвих ідентифікаційних документів
* Криміналістика: відбитки пальців знайдені на місці злочину використовуються для ідентифікації особи, яка причетна до цього злочину

Вертикальна класифікація містить такі категорії:

* Охорона здоров’я
* Фінансова сфера
* Ігрова сфера та туризм (казино, готелі тощо)
* Торгівля
* Освіта
* Виробництво
* Високі технології та телекомунікації
* Транспорт
* Урядові та юредичні сфери
* Військовий сектор
  1. **Існуючі проблеми впровадження та застосування АСІВ**

АСІВ надають гарне поєднання засобів безпеки, приватності та зручності. Хоча кількість провадженних систем такого типу постійно збільшується, поточний рівень їх використання дещо менший ніж можна було б очікувати. В першу чергу, це пов’язано з відсутністю чіткого розуміння можливостей та переваг технологій розпізнавання відбитків. Іншою причиною є те, що часто запровадження АСІВ у бізнесі виявлялося складною задачею (з точки зору інвестиційного аналізу) у зв’язку з наступними причинами:

* Рівні шахрайств і результуючі збитки для великого бізнесу та урядових систем не є добре вивченеми та обрахованими
* АСІВ, які є дуже новими технологіями, часто зустрічаються нереальними вимогами до їх ефективності і не можуть бути справедливо порівнянними з існуючими альтернативами (наприклад, електронні картки та паролі), з незручністю та дороговизною яких бізнес навчився миритися
* Якість наявних технологій розпізнвання відбитків дуже сильно відрізняється від одного постачальника до іншого. Клієнти часто просто не можуть отримати доступ до правдоподібних результатів тестування різних технологій у зв’язку з відсутністю стандартизованих тестових сценаріїв для АСІВ. Тому клієнт сам змушений проводити аналіз існуючих технологій, що потребує додаткових коштів, або сподіватися на достовірність існуючих результатів аналізу

АСІВ, якщо вона належним чином реалізована, надає кращу захищеність, зручність та ефективність ніж будь-які інші можливі засоби ідентифікації. Жодна інша технологія не має можливості гарантувати, що особа, яка автентифікується, фізично присутня у місці автентифікації. Системи на основі розпізнавання відбитків вже замінили паролі та електронні картки у багатьох сферах. У деяких інших – вони використовуються на додачу до паролів та карток. Використання АСІВ значно зменшує рівень шахрайств та крадіжок пов’язаних з автентифікацією та приватними даними.